Experiments in Automatic Theorem Proving

by

Gianluigi Bellin
Jussi Ketonen

Department of Computer Science
Stanford University
Stanford, CA 94305
Experiments in Automatic Theorem Proving
by
Gianluigi Bellin and Jussi Ketonen

Research Sponsored by
Advanced Research Projects Agency
and
National Science Foundation

Department of Computer Science
Stanford University
Stanford, CA 94305

This version of the PERM was printed on December 20, 1986.
1. Introduction ....................................... 1
  1.1. Motivation and general comments ................. 4
  1.2. The Proofs in EKL .............................. 5
  1.2.1. The Language specified by EKL ................. 5
  1.2.2. Proofs and Lines in EKL ....................... 6
  1.2.3. Lines and dependencies ....................... 8
  1.2.4. Controlling the Rewriting Process ............... 8
  1.2.5. EKL and Natural Deduction .................... 10
  1.2.6. Remembering Lines in EKL ..................... 12
  1.3. Rudiments of LISP ................................ 13
  1.4. Permutations and the Pigeon Hole Principle .......... 14
  1.5. The Representation of Permutations in LISP ........ 16
  1.5.1. A Remark on Sets and Lists ................... 16
  1.5.2. Permutations as Association Lists ................ 18
  1.5.3. Permutations as Lists of Numbers ................ 21
  1.5.4. Application of the Pigeon Hole Principle to Permutations 26
  1.6. Outline of the Paper ............................ 27
2. Preliminaries: Basic Tools ........................ 33
  2.1. Educating EKL about propositional Logic ............ 33
  2.2. Educating EKL about first grade Arithmetic ........ 36
  2.3. LISP and the Bound Quantifier Allp ............... 37
  2.4. Facts of elementary set theory .................... 38
  2.5. Putting things together .......................... 41
  2.6. Properties of Nth ................................ 41
  2.7. Properties of Nthcdr ............................ 45
  2.8. Properties of Fstposition ....................... 47
  2.9. The Lemmata Nth Fstposition and Fstposition Nth .... 48
  2.10. Injectivity and Uniqueness ..................... 52
  2.11. The notions of Finite Union and Finite Sum ........ 53
  2.12. The notion of Multiplicity ........................ 54
  2.12.1. Multiplicity Implies Injectivity ............... 57
  2.12.2. The Multiplicity of a. Disjoint Union is the Sum of Multiplicities 58
3. Notions of Application .......................... 60
  3.1. Function Application using Association Lists ....... 60
  3.2. Function Application using Lists of Numbers ........ 63
  2.13. Conclusion of Part I ........................... 65
4. The Pigeon Hole Principle ........................ 71
  4.1. The Pigeon Hole Principle in Second Order Arithmetic .... 71
  4.2. Corollary for Application to Lists ................ 76
  4.3. Application of the Pigeon Hole Principle to Lists ..... 77
  4.3.1. Application of the Pigeon Hole Principle to Alists ... 78
  4.3.2. Step 1: Injectivity implies Disjointness .......... 79
  4.3.3. Step 2: Positive Multiplicity .................. 80
  4.3.4. Step 3: The Sequence partitions the Range .......... 81
  4.3.5. The Main Result for Association Lists: Every Permutation is an Injection 83
  4.4. Application of the Pigeon Hole Principle to Lists of Numbers 85
  4.4.1. Step 1: Disjointness .......................... 85
CONTENTS

4.4.3.  Step 2: Onteness Implies Multiplicity ........................................... 86
4.4.3.  Step 3: Onteness Implies Multiplicity ........................................... 86
4.4.4.  The Main Result for Lists: Every Permutation is an Injection .......... 87
5.   Representation using Association Lists ........................................ ..... 89
5.1.   Definitions of Composition, Inverse and Identity ........................... 89
5.2.   Almost All the Facts ................................................................. 90
5.3.   The Composition of Permutations is a Permutation ........................... 95
5.3.1.  Proof Range Compose, First Part ................................................. 95
5.3.2.  Proof of Range Compose, Second Part ......................................... 98
5.3.3.  Conclusion of the Proof of Permutp Compose ............................... 100
5.4.   Associativity of Composition ....................................................... 101
5.5.   The Identity Alist ................................................................. 102
5.6.   Inverse of a Permutation is a Permutation .................................... 104
6.   Representation using Lists of Numbers ............................................ 108
6.1.   General Comments on the Choice of the LISP Functions or Predicates 108
6.2.   Definitions of Composition, Identity, Inverse ................................ 112
6.2.1. Functions as Lists: Using Predicates .......................................... 112
6.2.2. Functions as Lists: Using Functions ........................................... 113
6.3.   Preliminaries ......................................................................... 114
6.3.1. Preliminaries: Condition for Definiteness and Sorts of the Functions 114
6.3.2. Preliminaries: Length of Compose ............................................. 116
6.3.3. Preliminaries: Length of Ident .................................................. 117
6.3.4. Preliminaries: Length of Inverse ................................................ 118
6.4.   Theorem 1: Composition of Permutations ...................................... 120
6.4.1. Using predicates: Composition of Permutations is a Permutation .... 121
6.4.2. Using Predicates: Composition is Associative .............................. 124
6.4.3. Using Functions: the Lemma Nth Compose .................................... 127
6.64. Using Functions: Theorem 1 ......................................................... 128
6.5.   Theorem 2: The Identity Permutation ............................................ 128
6.5.1. Using Predicates ................................................................. 129
6.5.2. Using Functions: the Lemma Main Id .......................................... 132
6.5.3. Using Functions: Identity is a Permutation .................................. 133
6.5.4. Using Functions: Right Identity ................................................ 134
6.5.5. Using Functions: Left Identity .................................................. 136
6.6.   Theorem 3: the Inverse of a Permutation ..................................... 137
6.6.1. Using Predicates: the Inverse of a Permutation is a Permutation .... 137
6.6.2. Using Predicates: the Right Inverse Theorem ................................ 137
6.6.3. Using Predicates: the Theorem Left Inverse ................................ 139
6.6.4. Using Functions: the Lemma Main Inv ........................................ 141
6.6.5. Using Functions: the Inverse of a Permutation is a Permutation ...... 143
7.   Conclusion ....................................................................................... 146
8.   APPENDIX ...................................................................................... 151
8.1.   A Summary of Natural Deduction .................................................... 151
8.2.   Organization of the Files ............................................................... 162
8.3.   file NORMAL .................................................................. 163
8.4.   file NATNUM ................................................................ 164
8.4.1. More Arithmetic .................................................................. 167
CONTENTS

S.4.2. Subtraction ................................................. 169
S.5. file LISPAX .................................................... 172
S.5.1. file ALLP .................................................... 175
S.6. file SET ........................................................ 176
S.7. file LENGTH .................................................... 177
S.8. file NTH: Some Appropriate Inductive Principles .......... 178
S.9. Nth .............................................................. 179
S.9.1. Member Nth ................................................... 180
S.10. Nthcdr ......................................................... 180
S.10.1. Nthcdr Induction ............................................ 182
S.11. Fstposition ..................................................... 184
S.11.1. Fstposition and Nth ......................................... 184
S.12. Injectivity ....................................................... 185
S.13. Nth, Allp and Mkset .......................................... 187
S.14. file APPL: Functions Represented by Association Lists .... 188
S.14.1. Alist Induction .............................................. 189
S.14.2. Facts About Association Lists .............................. 189
S.14.3. Samemap Definition ........................................ 190
S.15. Functions Represented by Lists of Numbers .................. 191
S.15.1. Extensionality ............................................... 191
S.16. file SUMS: Finite Union and Finite Sum ...................... 192
S.16.1. Bound Quantifiers ......................................... 193
S.16.2. Facts About Sums and Unions ............................... 193
S.17. file MULT: Multiplicity ....................................... 195
S.17.1. Multiplicity Implies Injectivity ............................ 196
S.17.2. The Multiplicity of Union is the Sum of Multiplicities ... 197
S.18. file PIGEON: the Pigeon Hole Principle in II Order Arithmetic 198
S.19. file ALPIG: Application to Alists 1: Disjointness .......... 199
S.20. Application to Alists 2: the Multiplicity is Positive .......... 200
S.21. Application to Alists 3: Multiplicities in Dom and Range .... 201
S.22. Application to Alists: a Permutation is an Injection .......... 201
S.23. file LPIG: Application to Lists 1: Disjointness ............. 203
S.25. Application to Lists: a Permutation is an Injection .......... 204
S.26. Operations on Functions Represented by Association Lists .... 205
S.26.1. file ASSOC: Functions Represented by Association Lists ...... 205
S.26.2. Lemma Nonempty Range ..................................... 207
S.26.3. Lemma Nonempty Domain .................................... 207
S.26.4. Lemma Range Compose, Part 1 ................................ 208
S.26.5. Lemma Range Compose, Part 2 ................................ 210
S.26.6. Conclusion of Theorem 1 ...................................... 211
S.26.7. Associativity of Composition .................................. 212
S.26.8. Samemap Left ............................................... 213
S.26.9. Theorem 2, on Identity Alist .................................. 213
S.26.10. Lemma Atomrange .......................................... 215
S.26.11. Theorem 3, on Inversion of Alists .......................... 215
S.27. file PERMP: Functions Represented by Lists, Using Predicates 217
Contents

8.27.1. Composition of Permutations is a Permutation ................................. 217
8.27.2. Composition is Associative ............................................................. 219
8.27.3. Using Predicates: Identity ............................................................. 221
8.27.4. Using Predicates: the Inverse Permutation Theorem ......................... 223
8.27.5. Using Predicates: the Right Inverse Theorem .................................. 225
8.27.6. Using Predicates: the Left Inverse Theorem .................................... 226
8.28. file PERMF: Functions Represented by Lists, Using Functions .............. 228
8.29. Condition for Definiteness and Sorts of the Functions ......................... 228
8.30. Length Compose .................................................................................. 229
8.30.1. Length Ident ..................................................................................... 230
8.30.2. Length Inverse .................................................................................. 230
8.30.3. Compose ........................................................................................... 231
8.30.4. Compose Permutation ....................................................................... 231
8.30.5. Identity ............................................................................................. 234
8.30.6. Right Identity .................................................................................... 235
8.30.7. Left Identity ....................................................................................... 236
8.30.8. Inverse ............................................................................................... 236
8.30.9. Inverse Permutation .......................................................................... 238
8.30.10. Right Inverse .................................................................................. 239
8.30.11. Left Inverse ...................................................................................... 241
9. Bibliography .............................................................................................. 243
9.1. Index of Examples .................................................................................. 244
10. Index of SIMPINFO .................................................................................. 245
10.1. Index of Definitions .............................................................................. 250
INTRODUCTION
1. Introduction.

1.1. Motivation and general comments.

The best guarantee is to find programs which are not too hard to execute, but can be applied to very "many" instances of interest. G. Kreisel [1981]

The question of finding convenient representations for mathematical facts is one of the most interesting challenges in the field of mechanical theorem proving. A solution should lead naturally to other applications. Thus, given a problem instead of simply asking whether one can find a particular representation that enables a machine to solve it, one should also ask:

- Are we learning something else from this experiment, besides the fact that the (usually well known) theorem is true?
- Is our representation abstract enough to allow applications of the result to similar problems?

For otherwise, given the well known present limitations of mechanical theorem provers, it is hard to imagine that the natural customer of the technology of automatic proof-checking, i.e. the working mathematician or teacher of mathematics, may ever find any appeal in it.

In the experiments described in this paper we have tried to meet this challenge by using the proof checker EKL, a system whose flexibility is increased by the use of high order logic. Using the expressive power of EKL we abstractly represent a result in second order language, prove it and then apply it in a natural way to different contexts.

The focus of our experiment is the basic theory of permutations. A permutation is a bijection of a (finite) set into itself. Our aim is to prove that permutations of a finite set, with the operation of composition of functions, form a group. Specifically, given a finite set \( S \), we want to show that

1. The composition \( f \circ g \) of two permutations \( f \) and \( g \) on \( S \) is a permutation on \( S \) and composition is associative;
2. The identity function \( i \) on \( S \) is a permutation; for any permutation \( f \) on \( S \), \( i \circ f = f \) (left identity) and \( f \circ i = f \) (right identity)
3. If \( f \) is a permutation on \( S \), then there is a permutation \( f^{-1} \) of \( S \) such that \( f^{-1} \circ f = i \) (left inverse) and \( f \circ f^{-1} = i \) (right inverse).

EKL can easily express such facts in first or higher order logic. We can simply prove the facts stated above using elementary set theory. In the proof we need the 'pigeon hole' principle of elementary arithmetic: if we want to fill each of \( n \) holes and we have only \( n \) objects, then no hole can contain more than one object. The proof of this fact is not entirely trivial. Although it can be formulated in the language of first order logic with symbols for order, successor and a function symbol, it cannot be proved in the fragment of arithmetic having the usual axioms for order and successor plus induction applied to unary formulas only [Goad 1979]. Our proof of the pigeon hole principle, expressed in second order arithmetic, presents no such difficulties, since we do not restrict the inductive principle available to EKL.

The mathematical notions considered here do not require higher order logic in an 'essential way'. Any fact stated herein could be rephrased in terms of first order logic. Rather, the expressive power of EKL is used to emphasize the freedom in the choice of representations and flexibility proving facts.
There are many ways of representing finite functions. Having chosen one, we must define the operations of composition of functions, the identity function and the operation of taking the inverse of a function. Then we must prove the facts (1) - (3) using that interpretation.

We can always assume that a representation of a finite set of objects gives also an enumeration of it. Therefore we may represent finite functions as lists and use the axioms of LISP to prove facts about them.

We give two different representations of permutations, one using association list $s$ and the other using lists of numbers. In the first case the association list contains the graph of the function. Domain and range are represented by lists obtained in the obvious way from the given association list. In the second case the list contains the range in the order given by the domain. The domain is not represented by a list: rather it is a segment of the set of natural numbers. In this sense we have a more abstract representation, in which it is slightly easier to apply the pigeon hole principle as an abstract fact of arithmetic. This representation has been traditionally used in mathematics in order to talk about finite permutations.

The application of the pigeon hole principle occurs at similar points of the proofs, but the second order statement expressing it is instantiated by different functions. The improvement of efficiency obtained by higher order logic is particularly obvious here.

We also give two versions of the results for representations using lists of numbers. In the first version the operations of composition, identity and inverse are defined by predicates: we shall call it PERM-Fun-Predicate or PERMP. In the second these operations are defined by functions: we shall call this approach PERMF, for Permutation-Function.

The contrast between the representations through predicates and through functions is an aspect of the tension between extensional and intensional approaches to mathematics. This is relevant in general to automatic verification of the correctness of programs. The way we dealt with this tension can be taken, in some sense, as the ‘moral’ of our experiment. We try to summarize our point iii the following (idealized) history of the project.

Suppose we have written a LISP program for permutations, using any representation and we want to prove it correct ‘by pencil and paper’. If we are willing to assume the pigeon hole principle as evident and to justify the inferences by the label ‘evident by elementary arithmetic’, then the ‘proof of correctness is fairly simple, no matter what representation one chooses. Only the forms of the intuitions require some thought.

On the other hand, if we try to check our proof mechanically, say using EKL, and have in our proof library only simple facts of arithmetic and of LISP, then the task may look discouraging. Too many facts of elementary arithmetic and LISP functions may be needed, especially if we stick to the original form of our recursive programs in a ‘too constructive’ fashion.

This feeling of uneasiness is well known and perhaps unavoidable in the early stage of such enterprise as ours: since the first efforts of large scale formalization of elementary mathematics (e.g. Russell and Whitehead’s “Principia”), it became obvious that the amount of innocent presuppositions hidden in intuitive arguments grows to the size of tropical forest iii a full formalization. However, our experiments and many others show that some nontrivial results are indeed provable, when the basic proof libraries are reasonably furnished. It is also likely that, simple improvements of EKL -more semantic attachments—will make our task easier.

Minor details in the choice of the representation and in the formulation of the results may have major consequences in terms of length of the proofs and feasibility of the project. For instance, the representation of permutations in terms of association lists makes most proofs easy applications of one induction principle, induction on association lists. However, more work is needed to show that these facts on association lists actually establish the desired facts about permutations: indeed the
represent at ion by association list—unlike that by lists of numbers—is not unique. A permutation is represented by an equivalence class of association lists, not by a single association list. Hence one needs a canonical way to choose represent atives, a normal form, that can be obtained e.g. by ordering the field of the permutations. It is reasonable to consider other representations having the uniqueness property.

At first sight there seems to be no question that it is better to represent our operations by functions rather than by predicates. One can test this assumption by comparing our two versions PERMP and PERMF: to find a confirmation, one just looks at the treatment of composition of permutations and the proof that composition is associative. The operation on lists that represents composition of functions is better represented as a binary function, defined by recursion on the first list, rather than a ternary predicate. Indeed in the first case we can use a straightforward proof by induction on the recursive definition of the functions, whereas in the second case predicates require some relatively complicated substitutions. Finding these substitutions would require a huge number of random attempts if they were done without human direction.

Interestingly enough, many other proofs employing list representa- tion axe easier when the notions in question are formulated using predicates rather than functions. This is true especially of proofs about the identity and the inverse of a permutation. In the version PERMP, such proofs are simply obtained by expanding the assumptions and the definitions. In the version PERMF, the recursive definitions may be quite complicated, and the inductive proofs become quite involved.

This situation is in many ways analogous to problem in various areas of mathematics. In the representation through functions the intensional features of our programs are closely represented. On the contrary, the representation through predicates only the extensional properties of our functions are relevant. It is well known that in most mathematical practice only extensional facts are considered. We may say that predicates allow slightly more abstract definitions of the operations than functions. In mathematics often a small progress towards abstr action simplifies the present at ion considerably.

If we start our proof of correctness with the definitions contained in the version PERMF, we may find it convenient to look at the definitions of the operations in PERMP and to prove them first as lemmata. One can then use these facts in different contexts instead of going through longer direct proofs.

Abstracting lemmata and breaking arguments into suitable parts is the basis for mathematical communication: it makes proof `easy to take and easy to remember'. This remark by Kreisel (a variation on a theme by Wittgenstein) is highly appropriate here. The readability of mechanical proofs depends on such devices even more than the readability of `pencil and paper' proofs. An automatic proof of correctness of previously written program may be too long and tedious for human consumption. A better organization of the problem, based on more abstract consideration of the facts in question, may significantly increase the readability of such proofs.

Some objections may be raised to our remarks. On one side, one may argue that it is not clear what counts as evidence in favour of our claims: isn't it after all just a quest ion of mathematical taste?

On the other side, even granting our claims, one may be a priori skeptical about the relevance of our investigation: Haven't we simply verified, through mechanical proof checking of mathe- matically trivial examples the well known fact that there are good and bad styles of mathematical presentation? Can we expect any interesting theoretical discovery to result from experiments of this kind?

In our experiments we search for methods to effectively use the given technology and for guidelines to improve it. Current practice of informal mathematics and theoretical results from logic.
do not immediately provide all the relevant information. Proof checking is a practice of interaction between a user and a given technology, in which human capacities, technical possibilities, linguistic features and methods of interaction are all relevant. For instance, we know from the Normalization Theorem in Proof Theory that direct proofs are generally longer than those using lemmata. It is very well possible that different languages or different theorem provers may suggest different strategies of proof checking. In particular, we cannot rule out the possibility that language may be created, a technology produced and experiment exhibited in which, say, most of our lemmata have convenient direct proofs. Only experience can decide. But given a certain technology, practice does indeed show what directions are convenient and what projects feasible. Strategies and methods of proofs, not only the subjective qualities of the user, are decisive in determining the success of a project.

On the other hand, no matter how plausible the reasons of the skeptic may look, the performance of automatic proof checkers has been remarkably improved since the first experiments. Instruments are available that allow a ‘microscopic analysis of mathematical proofs: a certain amount of experimentation has already been performed. The analysis of what is usually regarded as ‘style’ of presentation may possibly disclose important features of proofs, that have been overlooked so far. Above all, this work is a necessary preliminary step to start applying automatic proof transformations (e.g. extraction of bounds, transformation of non elementary proofs into elementary ones, cut elimination and functional interpretation, etc.) to mathematically significant examples. And there, for a logician, the real fun begins.

1.2. The-Proofs in EKL.

EKL is a proof checker and constructor that uses a typed language, a rewriting system, a decision procedure and semantic attachments.

The language of EKL is described in detail in the user's manual [Hietonen and Weening 1984]. For the sake of completeness, we will describe some of the basic facets of this system.

**Remark 1.** EKL does not distinguish between uppercase and lowercase. As a convention, in this paper we will use lowercase typewriter-like font for commands and formulas occurring within a command, and uppercase typewriter-like font for the formulas returned by EKL. The output of EKL is preceded by semicolon. Thus

```
(trw |P2P|)
```

is a command (asking EKL to verify a tautology) and

```
:P is unknown.
;the symbol P declared to have type TRUTHVAL
;P2P
```

is the answer by EKL. The first, two lines inform us that a default declaration has been made: the third tells that EKL has verified the tautology.

We thank J. McCarthy for his constant support and encouragement. We owe C. Talcott many ideas and suggestions at various stages of the work. Thanks to R. Casley and J. Weening for their fundamental TeXnical help. This research was supported by grants NSF MCS 82-06365 and ARPA N000-39-82-C-0250.
SECTION 1

Remark 2. EKL commands use the LISP syntax

(funct arg1 . . . argn)

where the function (command) funct is applied to the arguments arg1 . . . argn. In describing such commands we use the expressions &optional and &rest.

(funct arg1 . . . &optional argj . . . &rest param)

'&optional' indicates that all arguments following it are optional and are given a default value if omitted. '&rest' means that 'param' indicates the the list of all arguments following it, rather than a single parameter.

1.2.1. The Language specified by EKL.

A list of linguistic attributes, i.e. a declaration, is associated with every atom. The main attributes of a declaration are the type, the syntype and the sort.

The type of an EKL object tells how that object can be applied. For example, an object of type ground + ground can be applied to objects of type ground resulting in an object of type ground. An object of type ground* + ground can be applied to any number of objects of type ground resulting in an object of type ground. Thus objects of this type could be regarded as having variable arity. A sentence is an object of type truthval. A unary predicate is an object of type ground + truthval. Sets can also be represented as objects of this type.

In declaring the type of a new entity, the operator @ gives the type of a (previously defined) object. Thus

(decl setseq (type: |@n+@set|))

establishes that setseq has the type of a sequence of sets, i.e. the type of a function from objects of the type of natural numbers to objects of the type of sets. Since natural numbers have type ground and sets have type ground+truthval, the above declaration is the same as

(decl setseq (type: |ground+(ground+truthval)|)).

The syntype specifies whether a linguistic object is a variable — so that it can be quantified — a constant — so that it cannot be quantified — or a bindop, an operator binding variables.

A sort in EKL is simply a unary predicate. Every EKL symbol has a sort. The default is universal — the most general sort, of any type.

Typically we may have a variable n of sort natnum and a variable x of sort universal. Then statements like \( \forall n . P(n) \) are equivalent to \( \forall x . \text{natnum}(x) \subset P(x) \).

In existential generalization, X-abstraction etc. EKL checks whether the term in question satisfies sort restrictions. For example, the formula \( \forall n . A(n) \supset \forall x . A(x) \) is not provable in the above situation, unless facts like \( \forall x . \text{natnum}(x) \) are in use.

The information that a function is defined for a certain argument (or that, a program terminates) can be given as a fact about sorts. In the following example, to prove that numseq(m) is of the sort natnum is to show that the function numseq is defined for m as an argument. Of course EKL has cannot determine this just from the declaration of numseq.
(proof sums)
(decl i j k m n (sort: natnum))
(decl numseq (type: [n->n]))

(derive [\forall m. natnum(numseq(m))])
; failed to derive
NATNUM(NUMSEQ(N))

(trw [\forall m. natnum(numseq(m))])
;(\forall . NATNUM(NUMSEQ(M)))=(\forall . NATNUM(NUMSEQ(M)))

Some EKL symbols are predeclared: we cannot modify their attributes. We can introduce linguistic objects using the EKL command DECLARE:

(1) (decl <symbol> . <attributes>).

If we introduce a new symbol without declaring it, EKL tries a default declaration and tells us what it is.

A context is simply a list of declarations for atoms.

1.2.2. Proofs and Lines in EKL.

A proof in EKL consists of lines. Each line in a proof is a result of a command. There are several different types of lines:

(1) Lines that result from declarations. These have the effect of setting the context of a line and adjoining the declaration to the current context.

(2) Lines resulting from other commands.

- Examples:

(II) (assume wff)

The formula wff is assumed true, with the above line introduced as a dependency.

(III) (axiom wff)

The formula wff is assumed as true, with no visible dependencies introduced.

(IV) (defax symbol wff)

The formula wff is assumed as true and regarded as the definition of symbol.

(V) (define symbol wff &optional rewriter)

The formula wff is regarded as the definition of symbol, provided that the truth of symbol.wff follows using the rewriter. The formula wff must contain symbol.
(VI)  
(trw term &optional rewriter)

The term term is rewritten using standard rewriting, the lines labeled previously as simpinfo o and the instructions given by rewriter.

Let term1 be the result of such rewriting. If term is a term then the formula term = term1 is given as conclusion; if term is a formula, then term = term1 is derived, unless term1 is true, in which case term is derived, or false, in which case ¬term is derived.

(VII)  
(rw &optional line rewriter)

The line line is rewritten using standard rewriting, the lines labeled previously as simpinfo o and the instructions given by rewriter.

(VIII)  
(derive term &optional linerange rewriter)

The formula term is derived from the formulas in linerange. using the decision procedure, lines previously labeled as simpiinfo st andard rewriter and rewriting according to the instructions given by the rewriter.

IX)  
(cases line linerange)

The lines in linerange must contain the same formula, say A; line must be a disjunction. This command corresponds to the conclusion of a “proof by cases”. Suppose we are able to derive A from A1 and also from A2 and ... and also from A. Suppose we prove A1 v A2 v ... v An. Then we can conclude A “independently of” A1, ..., An.

(X)  
(ci linerange &optional line rewriter)

Let the lines in linerange contain the formulas A1, ..., An. Let the formula in line be B. Then the result of this command is

A1 A2 ... An ⊃ B,

and this formula will not “depend on” A1, ..., An.

(XI)  
(ue termslst &optional linedg rewriter)

This corresponds to the instantiation of a universal statement. If termslst contains the pair (x t), t is of the same type and sort as x and linedg is of the form ∀x . A(x), then the UE command will yield A(t). rewritten according to rewriter (and the lines previously labeled as simpiinfo).

Let us say that the variable x is explicitly universally quantified in ∀x . A(x). We define below what it means for x to be implicitly universally quantified in a line. The UE command is extended to the case of implicitly quantified variables and also to the case of multiple substitution, with termslst being a list of pairs.
1.2.3. Lines and dependencies.

Each line has associated to it its contest and dependencies. If a line contains a formula, then its contest is the set of all declarations needed to make sense of that formula, and parsing of the commands leading into it.

The dependencies are established using rules similar to Gentzen's Natural Deduction System.

- A line resulting from a command assume depends on itself.
- A line resulting from a command define or trw inherits the dependencies of the lines quoted by the rewriter plus the lines that are used automatically, having previously been labeled as simpinf 0.
- A line resulting from a command rw inherits the dependencies of the lines quoted in line. rewriter and those labeled simpinf 0.
- A line resulting from a command derive inherits the dependencies of the lines quoted in linerange, rewriter and those labeled simpinf 0.
- The dependencies of the line line1 resulting from a command cases are determined as follows. Suppose the formula of the line is \( A_1 \lor \ldots \lor A_n \) and suppose linerange is \( \text{line}_1 \ldots \text{line}_n \); then the dependencies of \( \text{line}_0 \) are the union, for \( j = 1, \ldots, n \), of the dependencies of the line, that are different from \( A_j \).
- The dependencies of the line line1 resulting from a command Cl are determined as follows. Let all the formulas in linerange result from the command assume. Then \( \text{line}_0 \) inherits the dependencies of line and of rewriter, except for those inherited from linerange.
- A line resulting from a command ue inherits the dependencies of linedg and rewriter.

An variable occurring in a line is implicitly universally quantified if it does not occur free in any of the dependencies of the line in question. This condition corresponds to the restriction on the application of \( \forall \)-introduction in Natural Deduction System. As noted above, implicitly universally quantified variables behave exactly as explicitly universally quantified variables: in particular, the ue command applies to them. We cannot allow implicitly universally quantified variables in lines coming from the axiom or def ax command. EKL must regard an axiom as creating dependencies, although it is instructed to be silent about them. Carefully writing all the universal quantifiers in the axioms saves many unpleasant surprises to the user. The variable defined by define or def ax is not implicitly universally quantified: it is to be regarded as the eigenvariable of an \( \exists \)-elimination in Natural Deduction.

1.2.4. Controlling the Rewriting Process.

Certain substitutions are automatically performed by EKL in rewriting. For instance:

- If \( A \) and \( B \) differ only in the name of the bound variables and the corresponding names have the same sort, then \( A=B \) and \( A\#B \) are simplified to \( \text{TRUE} \).
- \( P\#\text{TRUE}, P=\text{TRUE}, \text{PTRUE}, \text{TRUE}P, \text{FALSE}P, \neg P \). IF \( \text{TRUE} \) THEN \( P \) ELSE \( Q \) are all simplified to \( P \). etc.

Other cases of standard rewriting are listed in the user's Manual.

Control over the rewriting process is one of the most important features of EKL. The commands to specify rewriters are described in the user's Manual. We recall only the ones most frequently used in this paper.
The command

(use linerange &rest options)

tells EKL that all lines in linerange are to be applied to the term being rewritten, in the order given by linerange. A line is 'applied' to a term as follows.

-EKL identifies terms that differ only for the names of bound variables of the same sort. Let A be the term being rewritten: if the formula of the line is A, then A is replaced by TRUE; if the formula of the line is \( \neg A \) then A is replaced by FALSE.

-If the formula of the line is a conjunction, both conjuncts are successively applied to the term being rewritten.

-EKL performs 'conditional rewriting': if the formula of the line is \( B \lor A \), then the term A is replaced by TRUE, provided that the decision procedure derives B from the current context.

-If the formula of the line is universally quantified, then instances of the formula, the bound variables being replaced by suitable terms, are applied to the term.

-If the formula of the line is an equality of the form \( a=b \) and let the term being rewritten be a formula containing a. If in the command the list of options is empty, then the left member of the equality a is replaced by b in the formula, provided that b is 'simpler than a.

The notion of 'simplicity can be roughly described as follows. The expressions of the language of EKL are ordered lexicographically: we say that f is 'simpler than g and \( a+b \) is 'simpler' than \( b+a \). Moreover the expression \( f(x, f(x)) \) is 'simpler' than \( f(x, y) \) since it contain fewer basic symbols. The usual recursive definitions of terms from basic symbols and of propositions from atomic propositions give a natural measure of complexity of the expressions: we say that \( f(x) \) is 'simpler' than \( f(x, f(x)) \).

A list of options is available to make substitutions in other ways:

(i) direction: reverse
(ii) direction: simpler
(iii) mode: exact
(iv) mode: always
(v) uc: \((\text{var1. term1}) \ldots (\text{varj. termj})\)

By (i), we ask EKL to apply equalities in the reverse of the normal direction (replace in the term under consideration an occurrence of b, the right member of the equality, by a, the left member), or, by (ii), in whichever direction will make the formula simpler. By (iii), we ask EKL to make the substitution no matter whether the result will be simpler, without applying the line again to the terms produced by the first application, or, by (iv), applying the line as many times as possible. The option (v) allows us to apply the UE command to the line and then to apply the modified line to the term being rewritten.

We can restrict the range of application of the line to parts of the term being rewritten by using the command

(part subpart &rest rewriter)

Loosely speaking, we can regard the set of parts of an expression as a tree and denote a part by any label of the path that leads to it. For instance, the parts of

\( \forall x. p(a) \land (q(a) \lor r(x)) \)
can be denoted as follows:

\[
\begin{align*}
1 & \quad p(a) \land (q(a) \lor r(x)) \\
1\#1 & \quad p(a) \\
1\#2 & \quad q(a) \\
1\#2\#1 & \quad q(a) \\
1\#2\#2 & \quad r(x)
\end{align*}
\]

Example:

1. (assume \( \forall x. p(a) \land (q(a) \lor r(x)) \))
2. (assume \( a=b \))
3. (rw 1 (use 2))
   \( \forall x. P(A) \land (Q(A) \lor R(X)) \)
4. (rw 1 (use 2 mode: exact))
   \( \forall x. P(B) \land (Q(B) \lor R(X)) \)
5. (rw 1 (part 1\#2\#1 (use 2 mode: exact)))
   \( \forall x. P(A) \land (Q(B) \lor R(X)) \)

The command

\[
\text{open \&rest symbols}
\]

is equivalent to

\( \text{use linerange mode: exact} \),
where linerange consists of all the lines involved in the definition of the symbols in the list symbols.

We may want to call the decision procedure to rewrite a subformula of a line to TRUE. This is done by the command

\( \text{der \&rest linerange} \)

Finally, we may use several rewriters within a single command.

1.2.5. EKL and Natural Deduction.

A derivation in Gentzen-style Natural Deduction can be extracted from any EKL proof (although most of the time we don’t see it).

Let us disregard the fact that EKL lines may result from declarations, i.e. that EKL proofs contain also some language specifications and are, in this respect, similar to Martin-Löf-style derivations.
Some commands of EKL corresponds to rules of Natural Deduction systems:

\begin{itemize}
\item \texttt{assume} \rightarrow \texttt{\& introduction}
\item \texttt{\& elimination}
\item \texttt{\forall introduction}
\item \texttt{\forall elimination}
\item \texttt{\exists introduction}
\item \texttt{\exists elimination}
\item \texttt{\Pi introduction}
\item \texttt{\Pi elimination}
\end{itemize}

The missing rules are replaced by the \texttt{derive} command. Commands for the quantifiers include higher order quantification.

If we want to write EKL proofs in terms of Natural Deduction, we must also include some form of equational calculus corresponding to the rewriting process. EKL does not display all the steps of substitutions in the process of rewriting. It displays only the result of such process. We can ask EKL to show us all of the steps executed while rewriting by typing the command
\begin{verbatim}
(setq rewritemessages t)
\end{verbatim}

(Examples are given in Sections 2.1, 2.6 and 2.9). Each step of rewriting corresponds to an application of a rule of equality in equational calculus. The rewriting of a nontrivial line may involve a huge number of substitutions. It is clear, then, why we do not want always to see the natural deduction derivation corresponding to an EKL proof.

More generally, to simulate the flexibility of informal reasoning through (mechanical simulation of) formal reasoning is an important aim in the field of automatic theorem proving. The details of the formalization of informal arguments may be ignored once we are convinced that the mechanical procedure is correct.

Since the rewriting process applies to logical simplification as well, we can replace applications of natural deduction rules with rewriting. In other words, we tend to apply rules of substitution and of replacement, perhaps repeatedly in a single command, instead of expanding the proof according to the rules of natural deduction. This makes the EKL proofs much shorter. We shall show later some useful techniques to help the rewriting process and derive lines in one step.
1.2.6. **Remembering Lines in EKL.**

Forgetting is no mere vis inertiae as the superficial imagine: it is rather an active and in the strictest sense positive faculty of repression... The man in whom this apparatus of repression is damaged and ceases to function properly may be compared... with a dyspeptic - he cannot ‘have done’ with anything. 

EKL is capable of remembering and forgetting. The command

\[
\text{(label name \&optional linerange)}
\]

tags the lines in linerange with label name. Linerange defaults to the last line of the current proof.

\[
\text{(unlabel name \&optional linerange)}
\]

removes the label name from the tags associated to each line. Linerange defaults to the last line of the current proof.

A state in EKL consists of the currently active proof, the currently active context, the currently active linename contest and the currently active rewriter name contest.

A *linename context* is a list of symbolic names associated to lines. These associations may be set by the `LABEL` command.

A *rewriter name context* is a list of symbolic names associated to rewriters. These associations may be set by the `REWRITENAME` command.

The label simpinfo has special meaning to the rewriter. The lines labeled simpinfo are assumed to be lines that are always used in rewriting for simplification purposes or for verifying sorts.

We can call lines not only by name, but also by their number. The command

\[
\text{(use f oo#3)}
\]

means: use the third line of the proof f oo. The command

\[
\text{(use -3)}
\]

means: use the third line in the current, proof before the one being written. The symbol * stands for -1, i.e., it denotes the last line.

The *currently active context* is the cumulative subtotal of all the contest manipulation that has happened in the currently active proof.

A typical command several lines may be cited. We first of all combine the contests of the cited lines. If an incompatibility turns up, the command is aborted. This contest is then combined with the previous active contest; all the incompatible declarations from the previous contest are thrown out. The resulting contest is then used for parsing of terms etc. in the command. If no contest lines are cited, we default to the previous contest. This is sufficient most of the time.

It follows that we can use conflicting declarations in different parts of the of the same proof provided that we do not try to refer to these lines within the same command: the language that is used is ultimately local to the line in question.

---

1.3. Rudiments of LISP.

We shall use lists to represent, finite functions. Let us quickly recall the basic notions of LISP. (The following may also be regarded as a commentary to the file LISPAX, containing the Axioms of LISP, to be found in the Appendix.)

Given a set $A$ of atoms, including the empty list NIL, the set $S$ of symbolic expressions (S-expressions), is the set built from the atoms using the pairing operation “*”:

(i) $A \cup S$
(ii) if $x$ and $y$ are S-expression then $x \cdot y$ is an S-expression.

In other words,

$$S = A + S \times S.$$  

The unary operations car and cdr are the first and the second projections, defined on $S \setminus A$. It is convenient for our purpose to define

$$\text{car nil} = \text{nil} = \text{cdr nil}.$$  

The set $L$ of lists is a subset of the set $S$ of S-expressions. $L$ is defined inductively by the clauses

(iii) NIL is a list.
(iv) if $u$ is a list and $x$ is an S-expression then $x \cdot u$ is a list.

As usual, we abbreviate $(a_1 \cdot (a_2 \cdot \ldots \cdot (a_n \cdot \text{NIL}) \ldots))$ as $(a_1 a_2 \ldots a_n)$. The variables $x$, $y$ and $z$ always range over S-expressions (i.e. are of sort atom)? $x$, $y$ and $z$ range over S-expressions (sort sexp) and $u$, $v$, $w$ range over lists (sort listp).

These inductive definitions suggest principles to define functions by recursion on the definitions of $S$ (recursion on S-expressions) and $L$ (recursion on lists). Using higher order logic we can formulate the principle Listinductiondef of recursion on lists as

$$\forall \text{df nilcase def.}$$

$$(\exists \text{fun.} (\forall \text{pars x u.} \text{fun(nil,pars)} = \text{nilcase(pars)} \wedge \text{fun(x,u,pars)} = \text{def(x,u,\text{fun(u,df(x,pars)),pars})))$$

Here $\text{pars}$ is a list of $n$ parameters, $\text{df}$ is a given auxiliary $(72 + 1)$-ary function, giving a list of $n$ parameters as value, $\text{nilcase}$ is a given $n$-ary function and $\text{def}$ is a given $n \cdot 3$-ary function. for each $n$. Actually the type structure of EKL plays a major role here, since it. can be used to transform any list of $n$ arguments into a single argument. For example, $\text{fun}$ is declared to have type

$$\text{ground} \cdot \text{ground} \Rightarrow \text{ground}.$$  

We can also formulate the principle of Listinduction to prove facts about functions defined by recursion on $L$:

$$\forall \phi. \phi(\text{nil}) \wedge (\forall x \cdot \phi(u) \Rightarrow \phi(x,u)) \Rightarrow (\forall u. \phi(u))$$

Here $\phi$ is any predicate taking lists as argument. The principles of recursion and induction on S-expressions are similar.

The type structure of the language of EKL is a limit to the inductive strength of the system. In the situation described above
pars is of type ground*.
-df of type (ground@ground*)+ground*.
-nilcase of type ground*+ground*.
so that fun will be of type (ground@ground*)+ground*, too.
The device of variable types is a way to overcome such limitation. Consider the following **High Order Definition**

\[
\text{Vbigfun atom\_fun.}\exists\text{defined\_fun.}
\forall x. y. \text{ (atom } x \exists \text{ defined\_fun}(x) = \text{atom\_fun}(x)\land
\text{ (defined\_fun}(x,y)=
\text{bigfun}(x,y,\text{defined\_fun}(x),\text{defined\_fun}(y)))}
\]

Here
- arb is a variable type with name ?arbitrary,
- biginfun is of type ground@ground@arb@arb@arb+arb.
- defined fun and atom\_fun are of type ground+arb.

In this way we allow EKL to postpone the decision about the type of the function defined\_fun to the time of application of the principle to define a particular function in a given context: then arb can be specialized to an object of any type. Therefore we have a primitive recursive schema for definition on all higher type functionals.

1.4. Permutations and the Pigeon Hole Principle.

Let \( A \) be a finite set and let \( \beta \) be the set of all surjections on \( A \), i.e. the set of all functions mapping \( A \) onto itself. The following fact is an easy consequence of the Pigeon Hole Principle.

**Lemma.** Every surjection on a finite set is an injection.

The proof will be considered in section below. Assuming the Lemma, it is not hard to prove the following Theorem.

**Theorem.** (3. o), where o is the operation of composition of functions, is a group.

**Proof.** It is easy to check that the composition of two surjections on \( A \) is a surjection on \( A \) and that composition of functions is an associative operation. The identity map \( i \) is a surjection and is the two-sided identity with respect to o. Finally, given \( f \in \mathcal{F} \), the inverse map

\[
f^{-1} : f(a) \mapsto a.
\]

for all \( a \in A \), is a well defined function. Since \( f \) is an injection: \( f^{-1} \) has \( A \) as domain, since \( f \) is a surjection on \( A \): \( f^{-1} \) is a surjection on \( A \), since the domain of \( f \) is \( A \). Clearly, for all \( f \in \beta \)

\[f^{-1} \circ f = i = f \circ f^{-1}. \blacksquare^\dagger\]

\dagger We use \( \square \) for the end of a proof (both informal and mechanical) and \( \blacksquare \) for the end of an example.
The pigeon hole principle is usually formulated as follows: if we put $n + 1$ pigeons in $n$ holes, then at least one hole gets more than one pigeon. Equivalently, 

If we have $n$ pigeons and $n$ holes and each hole contains at least one pigeon, then each hole contains exactly one pigeon.

More formally, let $N_n$ be the segment of $N$ bound by $n$, i.e. the set of natural numbers less than $n$.

**Theorem.** Let $f$ be a function on natural numbers, $f : N_n \rightarrow N$, such that for all $m$,

(i) $f(m) > 0$

and

(ii) $\sum_{m=0}^{n-1} f(m) = n$.

Then for all $m < n$,

$f(m) = 1$.

**Proof.** We use induction on $n$, employing the following facts of arithmetic: for all $k,m,n$.

(iii) $m \geq n \land k \geq 1 \supset m + k \geq n + 1$,

- for all $k,m,n$,

(iii) $m \geq n \land k \geq 1 \land m + k = n + 1 \supset m = n \land k = 1$.

We use (i) and (iii) to show, by induction on $n$, that for all $n$,

(v) $\sum_{m=0}^{n-1} f(m) \geq n$.

Now, in the induction step, we assume

$\sum_{m=0}^{n} f(m) = n + 1$.

- and use (iv) and (v) to prove

(vi) $\sum_{m=0}^{n-1} f(m) = n \land f(n) = 1$;

then we apply the induction hypothesis. 

Now we can prove
Lemma. Every surjection on a finite set is an injection.

Proof. Let $|A| = n$ be the cardinality of $A$ and let $a_m$ be the $m$-th element, for some enumeration without repetition of $A$. For any sequence of pairwise disjoint sets $B_i$,

$$\sum_{i<n} |B_i| = \bigcup_{i<n} B_i.$$  

Let $f \in 3$ and for each $m < n$, let $A_m = f^{-1}(\{a_m\})$, the inverse image of $\{a_m\}$. The $A_i$'s are pairwise disjoint and their union is $A$. Therefore, by (vii),

$$\sum_{m<n} |A_m| = |A| = n.$$  

Moreover, since $f$ is surjective, for all $A$, and all $m < n$,

$$|A_m| > 0.$$  

The Pigeon Hole Principle says that, if (viii) and (ix), then for all $m < n$,

$$|A_m| = 1.$$  

We conclude, for all $i, j < n$,

$$a_i \neq a_j \supset f(a_i) \neq f(a_j),$$

by applying (m) to $A_{f(i)}$.\]

1.5. The Representation of Permutations in LISP.

We turn now to the representation of finite functions in terms of LISP structures and the operations on finite functions as LISP programs. We will consider the representation of the above mathematical facts as properties of LISP programs and formally state the facts to be proved by EKL.

1.5.1. A Remark on Sets and Lists.

A set, according to Cantor's explanation, is an aggregate of objects, regarded as an entity that can itself be an element of other sets. In Set Theory sets may be constructed out of a given stock of basic objects, the urelements, but abstraction is made from the particular features of the urelements as well as from the order in which the urelements may be given to us. (In fact, in mainstream Set Theory urelements are ignored and the entire universe of sets is generated out of nothing, from the empty set.)

In formalizing Set Theory within, say, first order logic, a distinction is made between sets and classes in order to avoid paradoxes: unlike sets, classes cannot be regarded as elements of other sets or classes and axioms (say, Zermelo-Frankel axioms) determine if a property, expressed by a predicate, actually denotes a set or only a class.
If the formal language is a typed language, as the language of EKL, we may disregard the distinction between sets and classes, for the strict, restriction imposed by the type structure already guarantee from paradoxes. Thus instead of

\[ \{x : P(x)\} \]

we may write (using the lambda notation)

\[ \lambda x. P(x) \]

or simply

\[ P \]

to denote the set of objects having the property \( P \). The \( \epsilon \) relation can then be defined as

**Definition. (Epsilon)**

\[ \forall x v. x v \in \epsilon v = \epsilon v (x v) \]

We will use the epsilon notation applied only to the relation between urelements and sets of urelements.

The set

\[ \{x\} \]

can be represented as

\[ \lambda y. y = x. \]

This is our notation for the singleton set:

**Definition. (Mkset)**

\[ \forall x v. \text{mkset}(x v) = (\forall y v. y v = x v). \]

Given an aggregate, if we abstract only from the particular features of the elements we have an ordered set; if the set is finite we speak of a list. In the LISP language the term ‘list’ has a technical meaning, and membership in a list is represented by the recursive predicate `member`.

**Definition. (Member)**

\[ \forall x y u. \neg \text{member}(x, \text{nil}) \land \text{member}(x, y, u) = (x = y \lor \text{member}(x, u)) \]

Conceptually, the distinction between a list \( u \) and the set

\[ \{x : x \text{ is a member of } u\} \]

amounts to the distinction between a finite ordered set and a set. Our notation for the set \((*)\) is

**Definition. (Mklset)**

\[ \forall u. \text{mklset}(u) = \lambda x. \text{member}(x, u) \]

The functional mklset maps a lists into the set of its members.
1.5.2. Permutations as Association Lists.

Let \( f : A \rightarrow B \) be any finite function, i.e. a function defined on a finite set \( A \). Its graph, i.e. the set \( \{(a, f(a)) : a \in A\} \), can be written as

\[
\begin{pmatrix}
  a_1 & a_2 & \cdots & a_n \\
  f(a_1) & f(a_2) & \cdots & f(a_n)
\end{pmatrix}
\]

A finite function can be represented by an association list, i.e. by writing the graph of the function as a list. For instance the above function \( f \) can be represented by the list \( \text{alist}_f \)

\[
( (a_1 \cdot f(a_1)) \cdot (a_2 \cdot f(a_2)) \cdots (a_n \cdot f(a_n)) )
\]

The notation \( (*) \) is slightly ambiguous: the graph of a function is a set of pairs, but \( (*) \) seems rather to denote a list of pairs. Strictly speaking, the graph of \( f \) is correctly represented by \( \text{mklist}(\text{alist}_f) \), not by \( \text{alist}_f \). It is more informative to represent \( f \) by an equivalence class of association lists rather than by a predicate. We give an appropriate equivalence relation below.

Using \( \text{alist}_f \), we can represent the operation ‘apply \( f \) to an element \( a_k \) in the domain of \( f \)’ as follows: take the cdr of the S-expression in \( \text{alist}_f \) whose car is \( a_k \). Moreover, if \( f \) and \( g \) are finite functions such that the composition \( g \circ f \) of \( f \) and \( g \) is defined and \( \text{alist}_f \) and \( \text{alist}_g \) are the association lists representing \( f \) and \( g \), then we can find a list \( \text{alist}_{g \circ f} \)

\[
( (a_1 \cdots a_c \cdots c_2) \cdots (a_n \cdot a_n) )
\]

representing \( g \circ f \) as follows: “given \( a_k \), in order to find \( c_k \) go through \( \text{alist}_f \) searching for the S-expression, whose car is \( a_k \) and take its cdr, say \( b_k \); next go through \( \text{alist}_g \) searching for the S-expression, whose car is \( b_k \) and take its cdr as \( c_k \).”

The identity and inverse operations have an easy representation using association lists. The following list \( \text{alist}_{id} \) represents the identity function on \{\( a_1, \ldots, a_n \)\}:

\[
( (a_1 \cdot a_1) \cdot (a_2 \cdot a_2) \cdots (a_n \cdot a_n) )
\]

The ‘inverse’ of \( \text{alist}_f \) is given by the list \( \text{alist}_{f^{-1}} \):

\[
( (f(a_1) \cdot a_1) \cdot (f(a_2) \cdot a_2) \cdots (f(a_n) \cdot a_n) )
\]

The result of ‘composing’ \( \text{alist}_{f^{-1}} \) with \( \text{alist}_f \) is \( \text{alist}_{id} \). The result of ‘composing’ \( \text{alist}_{f^{-1}} \) with \( \text{alist}_f \) is the following list \( \text{alist}_{id1} \):

\[
( (f(a_1) \cdot f(a_1)) \cdot (f(a_2) \cdot f(a_2)) \cdots (f(a_n) \cdot f(a_n)) )
\]

If \( f \) is a bijection (and \( \text{alist}_{id}, \text{alist}_{id1} \) “don’t contain garbage”) then both \( \text{alist}_{id} \) and \( \text{alist}_{id1} \) represent the identity function on the same set.

The official EKL definition of \( \text{alist} \) is given by the following axiom. Here \( \text{alist} \) is a variable of type ground and sort. \( \text{alistp} \).

**Definition.** (\text{Alistdef})

\[ \forall x y \ \text{alist}. \text{alistp} \ nil \ A \ \text{alistp} \ (x a y). \text{alist} \]
The following is the definition of the operation of application using association lists.

**Definition.** (\(\text{Appalist}\))

\[ \text{Valist } y.\text{appalist}(y, \text{alist}) = \text{cdr } \text{assoc}(y, \text{alist}) \]

where \(\text{assoc}\) has been defined in the LISP library file as follows:

\[ \forall x \; x a \; y \; \text{alist} \; \text{assoc}(x, \text{nil}) = \text{nil} \]
\[ \text{assoc}(x, (x a \; y) \; \text{alist}) = \begin{cases} x a \; y \; \text{alist} & \text{if } x = x a \\ \text{assoc}(x, \text{alist}) & \text{else} \end{cases} \]

Given an association list \(\text{alist}\), let \(\text{dom(alist)}\) be the list containing the first element of each pair and \(\text{range(alist)}\) the list of all the second elements.

**Definition.** (\(\text{Dom}\))

\[ \forall x a \; y \; \text{alist} \; \text{dom \; nil} = \text{nil} \]
\[ \text{dom}((x a \; y) \; \text{alist}) = x a \; \text{dom \; list} \]

**Definition.** (\(\text{Range}\))

\[ \forall x a \; y \; \text{alist} \; \text{range \; nil} = \text{nil} \]
\[ \text{range}((x a \; y) \; \text{alist}) = y \; \text{range \; list} \]

The recursive predicate uniqueness is true of a list \(u\) iff every element of \(u\) occurs only once.

**Definition.** (\(\text{Uniqueness}\))

\[ \forall u \; x. \; \text{uniqueness \; nil} \]
\[ \text{uniqueness}(x, u) = \text{member}(x, u) \land \text{uniqueness} \; (u) \]

The fact that (the equivalence class of) \(\text{alist}\) represents a function is given by the property of \(\text{uniqueness}\) of \(\text{dom(alist)}\):

**Definition.** (\(\text{Funcp}\))

\[ \forall \text{alist.\;funcp}(\text{alist}) = \text{uniqueness \; dom(alist)} \]

and the fact that (the equivalence class of) \(\text{alist}\) represents an injection can be characterized as follows:

**Definition.** (\(\text{Injectp}\))

\[ \forall \text{alist.\;injectp}(\text{alist}) = \text{funcp}(\text{alist}) \land \text{uniqueness \; range(alist)} \]

Finally, (the equivalence class of) \(\text{alist}\) represents a permutation if and only if \(\text{dom(alist)}\) and \(\text{range(alist)}\) are the same as sets and have the same length as lists. The second property is of course obviously true for any \(\text{alist}\).

**Definition.** (\(\text{Permutp}\))

\[ \forall \text{alist.\;permutp}(\text{alist}) = \text{funcp}(\text{alist}) \land \text{mklset \; (dom(alist)) = mklset(range(alist))} \]
We don't need to include in our definition of permutation the fact that (the equivalence class of) \textit{alist} represents an injection, namely \texttt{injectp(alist)}. The fact that the property \texttt{injectp} follows from our definition \texttt{permtp} corresponds to the Lemma in Section 1.4.

Composition of functions is then represented by the following \textbf{LISP} function \texttt{ ○} (notice the order — \texttt{alistf ○ alisti} is the function \texttt{g ○ f}):

\textbf{Definition.} \texttt{(Compalist)}

\begin{verbatim}
Valist \texttt{alist2 x a y nil m alist2\texttt{=}nilA
    (((xa.y).alist1) \texttt{=} alist2=}
     (xa.appalist(y,alist2)).(alist1 \texttt{=} alist2)
\end{verbatim}

Identity is represented by the following predicate:

\textbf{Definition.} \texttt{(Idalistp)}

\begin{verbatim}
Valist \texttt{xa y . idalistp(nil)A
    (idalistp((xa.y).alist)\texttt{=}xa=y\texttt{}}idalistp alisti)
\end{verbatim}

Inversion is represented by the \textbf{LISP} function:

\textbf{Definition.} \texttt{(Invalist)}

\begin{verbatim}
Valist \texttt{xa y . invalist nil\texttt{=}nilA
    invalist((xa.y).alist)=(y.xa).invalist alisti)
\end{verbatim}

An unpleasant feature of this approach is that any association list consisting exactly of the \textit{S}-expressions \((a_k \cdot f(a_k))\), for all \(k\), is also a representation of \(f\), independently of the order in which they occur. The function \(f\) is not represented by a single association list, but by the class of all association lists that have the same members and give the same result, with respect to the operation of “application”.

The equivalence relation is represented by the following predicate:

\textbf{Definition.} \texttt{(Samemap)}

\begin{verbatim}
Valist \texttt{alist1.samemap(alist,alist1)\texttt{=}mklist dom(alist)=mklist dom(alisti)A
    (vy.y\texttt{}}mklist dom(alist))\texttt{}}
    appalist(y,alist)=appalist(y,alist1))
\end{verbatim}

The Theorem to be proved consists of the following statements:

\textbf{Theorem 1.} (i) \texttt{(Permutp Compalist)}

\begin{verbatim}
VALIST \texttt{ALIST1.PERMUTP(ALIST)A}PERMUTP(ALIST1)A
    MKLSET(DOM(ALIST))=MKLSET(DOM(ALIST1))A
    PERMUTP(ALIST ○ ALIST1)
\end{verbatim}

\textbf{Theorem 1.} (ii) \texttt{(Compalist Associativity)}

\begin{verbatim}
VALIST \texttt{ALIST1 ALIST2.MKLSET(RANGE(ALIST))CMKLSET(DOM(ALIST1))A}
    ALIST ○ (ALIST1 ○ ALIST2)=(ALIST ○ ALIST1) ○ ALIST2
\end{verbatim}
Theorem 2. (i) \( (\text{Idalist}\ \text{Permutp}) \)
\[
\forall \text{ALIST.\ FUNCTP(ALIST)} \cdot \text{IALISTP(ALIST)} \triangleright \text{PERMUTP(ALIST)}
\]

Theorem 2. (ii) (Right \( \text{Idalistp} \))
\[
\forall \text{VALIST.\ IDALISTP(ALIST)} \triangleright \text{PERMUTP}(\text{INVALIST(ALIST)})
\]
\[
(\forall \text{VALIST.\ MKLSET(RANGE(ALIST))} \triangleright \text{MKLSET(DOM(ALIST))}) \triangleright \text{ALIST} \circ \text{ALIST} = \text{ALIST}
\]

Theorem 2. (iii) (Left \( \text{Idalistp} \))
\[
\forall \text{VALISTID ALIST.\ IDALISTP(ALISTID)} \land
\]
\[
\text{MKLSET(DOM(ALISTID))} = \text{MKLSET(DOM(ALIST))} \triangleright \text{SAMESMAP(ALISTID} \circ \text{ALIST,ALIST)}
\]

Theorem 3. (i) \( (\text{Permutp}\ \text{Invalid}) \)
\[
\forall \text{VALIST.\ PERMUTP(ALIST)} \triangleright \text{PERMUTP(INVALID(ALIST))}
\]

Theorem 3. (ii) (Right \( \text{Invalid} \))
\[
\forall \text{VALIST.\ ALLP}(\lambda \text{X.\ ATOM X,\ RANGE(ALIST)}) \triangleright \text{INJECTP(ALIST)} \triangleright
\]
\[
\text{IALISTP(ALIST) \circ INVALIST(ALIST)}
\]

Theorem 3. (iii) (Left \( \text{Invalid} \))
\[
\forall \text{VALIST.\ ALLP}(\lambda \text{X.\ ATOM X,\ RANGE(ALIST)}) \triangleright \text{INJECTP(ALIST)} \triangleright
\]
\[
\text{IALISTP(INVALID(ALIST) \circ ALIST)}
\]

1.5.3. Permutations as Lists of Numbers.

Let \( \mathbb{N}_n \) be the segment of \( \mathbb{N} \) up to \( n \), i.e. the set \( \{m : m \in \mathbb{N}, m < n\} \). If \( A \) is the set \( \mathbb{N}_n \) and \( f \) is a function with domain \( A \) then \( f \) is called a (finite) sequence.

We can represent arbitrary finite functions using finite sequences. Given \( f : A \rightarrow B \) and suitable bijections \( i : \mathbb{N}_n \rightarrow A, j : \mathbb{N}_m \rightarrow B \) where \( n \) is the cardinality of \( A \) and \( m \) is the cardinality of the range of \( f \), there is a finite function \( g : \mathbb{N}_n \rightarrow \mathbb{N}_m \) such that the diagram

\[
\begin{array}{ccc}
\mathbb{N}_n & \xrightarrow{g} & \mathbb{N}_m \\
A & \xrightarrow{f} & B \\
i & \downarrow & \downarrow j \\
\mathbb{N}_n & \xrightarrow{g} & \mathbb{N}_m
\end{array}
\]

commutes. Thus, we need only consider functions from segments of \( \mathbb{N} \) to segments of \( \mathbb{N} \).

Although lists and finite sequences are essentially the same kind of mathematical object, a function is usually understood as a method to associate an element of the range to each element of the domain in a unique way.
When finite functions are represented by lists, we specify a method as follows. Given the finite function \( h : \mathbb{N}_n \rightarrow \mathbb{N} \), "list the range" of \( h \) in the order given by the domain, i.e., construct the list \( \mathbf{v}_h \):

\[
(h(0), h(1) \ldots h(n-1)).
\]

Thus \( h \) associates to each number in \( \mathbb{N}_n \) the \( n \)-th element of \( \mathbf{v}_h \). (To "list the domain" in the order given by the range is another possibility.)

The LISP function \( \text{nth} \) is defined as follows:

**Definition.** \( (N\text{th}) \)

\[
\forall x \in \mathbb{N} \, \forall n. \text{nth}(\text{nil}, n) = \text{nil} \land \text{nth}(\text{car}(x), 0) = \text{nth}(x, \text{nth}(x, 0))
\]

The equation

\[
\text{nth}(\mathbf{v}_h, k) = h(k)
\]

explains how the function \( \text{nth} \) represents the operation of applying a function to a number.

If \( \mathbf{v}_h \) represents \( h \), and \( u \) is any list of numbers, then \( \mathbf{v}_h \) can be "applied" to \( u \), by applying \( \mathbf{v}_h \) successively to all the members of \( u \). The operation "applying \( \mathbf{v}_h \)" to \( u \) is defined if all members of \( u \) are numbers less than the length of \( \mathbf{v}_h \).

This motivates our official definition of application, using lists of numbers:

**Definition.** \( (A\text{pp1}) \)

\[
\forall u. \text{appl}(u, i) = \text{nth}(u, i)
\]

The following predicate specifies the condition for \( v \) to be defined as an application on \( u \) as the domain:

\[
\forall v. \text{def appl}(v, u) = \text{allp}(\lambda x. \text{num}(x) \land x < \text{length}(v), u)
\]

Here \( \text{allp} \) is a recursive predicate, checking whether all members of a list have a certain property:

\[
\forall \phi. \forall u. \text{allp}(\phi, \text{nil}) A \text{allp}(\phi, x. u) = \text{if} \, \phi(x) \, \text{then} \, \text{allp}(\phi, u) \, \text{else} \, \text{false}
\]

The fact that a list \( u \) represents an injection is naturally represented by the predicate \( \text{inj} \): if every element of \( u \) occurs just once in \( u \), then two applications of \( u \) give the same value only for the same argument.

**Definition.** \( (I\text{nj}) \)

\[
\forall u. \text{inj}(u) = \forall n. m. n < \text{length}(u) A m < \text{length}(u) \land \text{nth}(u, n) = \text{nth}(u, m) \implies n = m
\]

On the other hand, the fact that \( u \) represents a surjection on \( \mathbb{N}_{\text{length}(u)} \) is given by the property onto, namely the fact that all members of \( u \) are numbers in \( \mathbb{N}_{\text{length}(u)} \) and, conversely, all numbers in \( \mathbb{N}_{\text{length}(u)} \) are members of \( u \). In such case every number in \( \mathbb{N}_{\text{length}(u)} \) will be the result of an application of \( u \) to some argument.
Definition. (Onto)
\[ \forall u. \text{onto}(u) = (\forall n. n < \text{length } u \land \text{nth}(u, n) < \text{length } u) \]
\[ \forall u. \text{onto}(u) = (\text{into}(u) \land (\forall n. n < \text{length } u \land \text{member}(n, u))) \]

Definition. (Perm)
\[ \forall u. \text{perm}(u) = \text{onto}(u) \]

As above, we don't need to include in our definition of permutation the fact that \( f \) is 1-1: the proof that \( \text{perm}(u) \) implies \( \text{inj}(u) \) will be described in Section 1.5.4.

Composition of functions can be represented by the following LISP function:

Definition. (Compose)
\[ \forall u \forall v \forall x. (u \circ \text{nil}) = \text{nil} \land (u \circ (x \circ v)) = (\text{nth}(u, x)) \circ (u \circ v) \]

Equivalently, the following predicate \( \text{comp} \) gives the condition for an application of \( u \) to be the same as an application of \( w \) followed by an application of \( v \).

Definition. (Comp)
\[ \forall u \forall v \forall w. \text{comp}(u, v, w) = \land \text{length } u = \text{length } w \land (\forall n. n < \text{length } u \land \text{nth}(u, n) = \text{nth}(v, \text{nth}(w, n))) \]

The representation of the identity function and the inversion of permutations are discussed in Section 6.1. It is clear that the predicate \( \text{id} \) gives the condition for the result of an application of \( u \) to be the same as its argument:

Definition. (Id)
\[ \forall u. \text{id}(u) = (\forall n. n < \text{length } u \land \text{nth}(u, n) = n) \]

We will choose the following function to construct the list representing the identity function:

Definition. (Ident)
\[ \forall x \forall u \forall n. \text{ident}(i, 0) = \text{nil} \land \text{ident}(i, n') = \text{ident}(i, n) \land \text{ident}(n) = \text{ident}(0, n) \]

Consider the function \( \text{Au x .f stposition}(u, x) \) that returns a number \( n \), with \( 0 \leq n < \text{-length}(u) \), corresponding to the position of the first occurrence of \( x \) in \( u \), if \( x \) occurs in \( u \) and NIL otherwise.

\[ \forall u \forall y. \text{fstposition}(\text{nil}, y) = \text{nil} \land \text{fstposition}(x . u, y) = \begin{cases} \text{nil} & \text{if } \neg \text{member}(y, x . u) \\ \text{nil} & \text{if } x = y \\ 0 & \text{else if } x = y \\ \text{add1}(\text{fstposition}(u, y)) & \text{else} \end{cases} \]

This function is our candidate for the inverse operation of \( \text{nth} \). If \( x \) occurs in \( u \), then
nth(u, fstposition(u, x)) = x.

By applying this for \( x = \text{nth}(u, n) \) and \( n < \text{length}(u) \), we get

\[
\text{fstposition}(u, \text{nth}(u, n)) = m,
\]

with \( m < \text{length}(u) \). Here \( m \) need not be equal to \( n \). However, this will certainly be the case if \( x \) occurs only once in \( u \), or in other words if \( u \) has the injectivity property \( \text{inj}(u) \).

Notice the asymmetry here: the function \( \text{fstposition} \) is the right inverse of \( \lambda n. \text{nth}(u, n) \) for any \( u_h \), i.e., for any function \( \lambda 12 \) represented by \( u_h \). However, \( \text{fstposition} \) is the left inverse of \( \lambda n. \text{nth}(u, n) \) only if \( u_h \) has the injectivity property, i.e., if the function \( h \) represented by \( u_h \) is a permutation.

Using this property of \( \text{fstposition} \), we can give the condition for \( u \) to represent the inverse function of the permutation \( v \):

**Definition. (Inv)**

\[
\forall u \in \text{inv}(u, v) \equiv (\forall n. n < \text{length } u \cap \text{nth}(u, n) = \text{fstposition}(v, n))
\]

and, as argued below, the following is a convenient way of constructing such inverse:

**Definition. (Inverse)**

\[
\forall u \in \text{invers}1(u, i, 0) = \text{nil} \land \text{invers}1(\text{nil}, i, n) = \text{nil} \land \\
\text{invers}1(u, i, n') = \begin{cases} 
\text{nil} & \text{if null(fstposition}(u, i)) \\
\text{else fstposition}(u, i) \cdot \text{invers}1(u, i', n) 
\end{cases}
\]

\[
\forall u. \text{inverse}(u) = \text{invers}1(u, 0, \text{length}(u))
\]

Using predicates, the results to be proved are:

**Theorem 1.** (i) **(Composition)**

\[
\forall u \in \text{Perm}(V) \land \text{Perm}(W) \land \text{length } V = \text{length } W \land \text{Comp}(u, v, w) \land \text{Perm}(u)
\]

**Theorem 1.** (ii) **(Uniqueness)**

\[
\forall u \in \text{Comp}(u, v, w) \land \text{Comp}(u_1, v, w) \land u = u_1
\]

**Theorem 1.** (iii) **(Associativity)**

\[
\forall u \in \text{Comp}(u_1, v_1, w_1) \land \text{Comp}(w_2, w_3) \land \text{length } w_2 = \text{length } w_3 \land \\
\text{Comp}(v, w_1, w_2) \land \text{Comp}(u, v, w_3) \land \text{Comp}(v_1, w_2, w_3) \land \text{Comp}(u_1, w_1, v_1) \land u = u_1
\]

**Theorem 2.** (i) **(Identity)**

\[
\forall u \in \text{ID}(u) \land \text{Perm}(u)
\]

\[
\forall u \in \text{Comp}(u, v, w) \land \text{Comp}(v, w, u) \land \text{length } w = \text{length } u \land v = w
\]
Theorem 2. (ii) (Right Identity)
\[ VU \forall W. \text{ID}(U) \circ \text{PERM}(W) \circ \text{LENGTH} W = \text{LENGTH} U \circ \text{COMP}(V, W, U) \circ W = V \]

Theorem 2. (iii) (Left Identity)
\[ \forall VU \forall W. \text{ID}(U) \circ \text{PERM}(W) \circ \text{LENGTH} W = \text{LENGTH} U \circ \text{COMP}(V, U, W) \circ W = V \]

Theorem 3. (i) (Inverse)
\[ \forall VU \forall V. \text{PERM}(U) \circ \text{INV}(V, U) \circ \text{LENGTH} V = \text{LENGTH} U \circ \text{PERM}(V) \]

Theorem 3. (ii) (Right Inverse)
\[ \forall VU \forall W. \text{PERM}(W) \circ \text{INV}(U, W) \circ \text{COMP}(V, W, U) \circ \text{LENGTH} U = \text{LENGTH} W \circ \text{ID}(V) \]

Theorem 3. (iii) (Left Inverse)
\[ \forall VU \forall W. \text{PERM}(W) \circ \text{INV}(U, W) \circ \text{COMP}(V, U, W) \circ \text{LENGTH} W = \text{LENGTH} U \circ \text{ID}(V) \]

Using functions, the results can be stated as follows:

Theorem 1. (i) (Perm Compose)
\[ \forall VU \forall V. \text{PERM} U \circ \text{PERM} V \circ \text{LENGTH} U = \text{LENGTH} V \circ \text{PERM}(U \circ V) \]

Theorem 1. (ii) (Associativity of Composition)
\[ \forall VU \forall W. \text{PERM}(V) \circ \text{PERM}(U) \circ \text{LENGTH} V = \text{LENGTH} U \circ \text{LENGTH} W = \text{LENGTH} U \circ \text{COMP}(W \circ V) \circ \text{COMP}(U \circ V) \]

Theorem 2. (i) (Perm Ident)
\[ \forall N. \text{PERM}(\text{IDENT}(N)) \]

Theorem 2. (ii) (Right Identity)
\[ \forall U. U \circ \text{IDENT}(\text{LENGTH} U) = U \]

Theorem 2. (iii) (Left Identity)
\[ \forall U. \text{INT}(U) \circ \text{IDENT}(\text{LENGTH} U) \circ U = U \]

Theorem 3. (i) (Perm Inverse)
\[ \forall U. \text{PERM}(U) \circ \text{PERM}(\text{INVERSE}(U)) \]

Theorem 3. (ii) (Right Inverse)
\[ \forall U. \text{PERM}(U) \circ \text{INVERSE}(U) = \text{IDENT}(\text{LENGTH}(U)) \]

Theorem 3. (iii) (Left Inverse)
\[ \forall U. \text{PERM}(U) \circ \text{INVERSE} U \circ U = \text{IDENT}(\text{LENGTH} U) \]
1.5.4. Application of the Pigeon Hole Principle to Permutations.

We have two representations of finite functions; thus we will have prove two facts representing the theorem that every finite surjection is an injection. In the representation by alists the fact is:

**Theorem (PermutpInjectp)**

\[
\forall \text{alist}. \text{permtp}(\text{alist}) \Rightarrow \text{injectp}(\text{alist})
\]

Under the assumption \text{permtp(alist)}, we need to show uniqueness range (\text{alist}).

In the representation by lists of numbers we show:

**Theorem (Perm Injectivity)** \[\forall U. \text{perm}(U) \Rightarrow \text{inject}(U)\]

As explained above, \textit{uniqueness} and \textit{injectivity} are equivalent predicates, asserting that every element of a list occurs just once. Although the theorems in question can be formulated in terms of the definition of permutation and of the predicates above, we need more information when we try to prove them.

The argument for theorem \textit{Permutp Injectp} can be summarized as follows. Since by definition \text{dom(alist)} has the uniqueness property, there are \(n\) different \textit{kinds} of objects (\(n\) ‘holes’) in \text{dom(alist)} and also in \text{range(alist)}, since \text{dom(alist)} and \text{range(alist)} have objects of the same kinds (i.e., each ‘hole has at least one object (‘pigeon’) of \text{range(alist)}). The number of (distinct) objects in range \text{alist} (‘pigeons’) is at most the length of \text{range(alist)} and at least the number of different kinds of objects. Therefore it is exactly \(n\). Therefore each kind of object occurs just once in \text{range(alist)} and this implies that range \text{alist} has the uniqueness property.

Despite the apparent triviality of this informal argument, some work is needed to formalize it. To speak of ‘kinds’ of objects is to speak of sets. We need a function counting the multiplicity of elements of \(u\) belonging to the set \(a\):

**Definition (Multiplicity):**

\[
\forall x\ u.\ \text{a.mult}(\text{nil},a)\equiv 0 \land \\
\text{mult}(x.u.a)\equiv \begin{cases} \text{if}\ a(x)\ \text{then}\ \text{mult}(u,a) & \text{else}\ \text{mult}(u,a) \end{cases}
\]

Next we must show that the list \text{dom(alist)}, considered as a set, can be partitioned into disjoint sets, i.e., the sets

\[
A_n = \{x: x = \text{nth(dom alist, }n)\}
\]

for all \(n, n < \text{length(dom(alist))}\).

Therefore we need a recursive predicate to decide whether the sets of a sequence are pairwise disjoint:

**Definition (Disjoint):**

\[
\forall n. \text{setseq}.\ \\
\text{disjoint}(\text{setseq,0}) \land \\
\text{disjoint}(\text{setseq, n'}) = (\text{disjoint (setseq,n)} \land \\
\text{disj_pair(un(setseq,n),setseq(n)))}
\]

where \text{disj_pair} is defined as
**SECTION I**

\[ \forall a \ b. \text{disj_pair}(a, b) = \text{emptyp}(a \land b) \]

To count the distinct objects in range(alist) we need the notions of finite union and finite sum:

**Definition (Finite Union):**
\[ \forall n \ \text{setseq.un}(\text{setseq}, 0) = \text{emptyset} \]
\[ \text{un} (\text{setseq}, n') = \text{un} (\text{setseq}, n) \cup \text{setseq}(n) \]

**Definition (Finite Sum):**
\[ \forall n \ \text{numseq.sum} (\text{numseq}, 0) = 0 \]
\[ \text{sum} (\text{numseq}, n') = \text{sum} (\text{numseq}, n) + \text{numseq}(n) \]

and, moreover, the following

**Lemma (Mult of Un is Sum Mult)**
\[ \forall \text{SETSEQ} U \ N. \ \text{DISJOINT} (\text{SETSEQ}, N) \Rightarrow \]
\[ \text{MULT} (U, \text{UN} (\text{SETSEQ}, N)) = \text{SUM} (\forall x \ 1 \cdot \text{MULT} (U, \text{SETSEQ}(x)), N) \]

The argument for Theorem Perm Inj is similar, but simpler. As before we prove the rather obvious fact that \( N_n \) can be partitioned into the disjoint sets

\[ \{ x : x = m \} \]

for each \( m < \text{length}(u) \). We need to show that for each \( m < \text{length}(u) \) the multiplicity in \( u \) of the set \( \{ x : x = m \} \), is exactly 1; then the injectivity of \( u \) follows. The pigeon-hole principle is used to prove this fact.

The pigeon-hole principle as such is an easy matter also for EKL. We use simple numeric induction to prove that for any function \( f : N_n \rightarrow N \) if the values of \( f \) are at least 1 and the sum of \( n \) values is \( n \) then each value is exactly 1. In both applications the function in question is

\[ \lambda m. \text{mult}(v, a(m)) \]

In the case of association lists, \( v \) is \text{range(alist)}; in the other case it is the given list \( u \). In the case of association lists, \( a(m) \) is the set \( \{ x : x = \text{nth} (\text{dom} \ \text{alist}, m) \} \); in the case of numeric lists we can take the set \( \{ x : x = m \} \) for \( a(m) \) and this is the reason why in this case proofs are simpler.

### 1.6. Outline of the Paper.

All the proofs are given in the Appendix. The organization of proofs in files and the dependence of the files are described at the beginning of the Appendix.

**Part I**, i.e. Sections 2 and 3 can be regarded as an introductory guide to automatic deduction of facts about LISP through experiments and examples.

**Section 2** is devoted to the definition of the LISP functions nth, nthcdr, fstposition and mult and to the proof of basic facts about them. It also contains facts of set theory and arithmetic.
Some useful techniques to replace "deriving" by "rewriting" through tautologies of second order propositional logic are explained and illustrated with an example.

We prove, among other things, the following facts connecting member and nth...

Lemma 2.1. (Nth Member)
\[ \forall U \forall N. N < \text{LENGTH } U \rightarrow \text{MEMBER}(\text{NTH}(U, N), U) \]

Lemma 2.2. (Member Nth)
\[ \forall U \forall Y. \text{MEMBER}(Y, U) \land (\exists N. N < \text{LENGTH } U \land \text{NTH}(U, N) = Y) \]

...and the following properties of nthcdr:

Lemma 2.3. (Nthcdr Car Cdr)
\[ \forall U \forall N. N < \text{LENGTH } U \rightarrow \text{NTHCDR}(U, N) = \text{NTH}(U, N) \cdot \text{NTHCDR}(U, N') \]

Lemma 2.4. (Nth in Nthcdr)
\[ \forall U \forall M. M < \text{LENGTH } U \rightarrow \text{MEMBER}(\text{NTH}(U, M), \text{NTHCDR}(U, N)) \]

Facts about nth and fstposition:

Lemma 2.5. (Nth Fstposition)
\[ \forall U \forall N. \text{MEMBER}(N, U) \rightarrow \text{NTH}(U, \text{FSTPOSITION}(U, N)) = N \]

Lemma 2.6. (Fstposition Nth)
\[ \forall U \forall N. \text{UNIQUENESS}(U) \land N < \text{LENGTH } U \rightarrow \text{FSTPOSITION}(U, \text{NTH}(U, N)) = N \]

The set of elements of a list is the finite union of the sets obtained using nth:

Lemma 2.7. (Mkset Un)
\[ \forall U \lambda N. \text{Mkset}(\text{NTH}(U, N)), \text{LENGTH}(U) = (\lambda X. (\text{Mkset}(U))(X)) \]

Moreover we show the following facts concerning the function mult:

Lemma 2.8. (Length Mult)
\[ \forall U \forall A. \text{MULT}(U, A) \cdot \text{LENGTH } U \]

Lemma 2.9. (Member Mult)
\[ \forall U \forall Y. \forall A. \text{MEMBER}(Y, U) \land (A \cdot Y) \leq \text{MULT}(U, A) \]

Lemma 2.10. (Mult Nthcdr)
\[ \forall N \forall A. U. N < \text{LENGTH } U \cdot \text{MULT}(\text{NTHCDR}(U, N), A) \leq \text{MULT}(U, A) \]

Lemma 2.11. (Mult Inj)
\[ \forall V. (\forall K. K < \text{LENGTH } V \rightarrow \text{MULT}(V, \text{Mkset}(\text{NTH}(V, K))) = 1) \rightarrow \text{INJ}(V) \]

The following facts about finite sums and unions are also needed:

Lemma 2.12. (Mdstsum)
\[ \forall U \forall N. \text{DISJ_PAIR}(A, B) \land \text{MULT}(U, A \cup B) = \text{MULT}(U, A) + \text{MULT}(U, B) \]

Lemma 2.13. (Mult of Un is Sum Mult)
\[ \forall \text{SETSEQ } U \forall N. \text{DISJOINT}(\text{SETSEQ}, N) \rightarrow \text{MULT}(U, \text{UN}(\text{SETSEQ}, N)) = \text{SUM}(\lambda X. \text{MULT}(U, \text{SETSEQ}(X)), N) \]
Section 3 contains the definitions of application and permutation, in both representations. It contains also some facts needed for the representation through association lists. In particular, since this representation is not unique, we have the predicate samemap that is true of two alists if they represent the same function. We show that samemap is an equivalence relation on alists:

Lemma 3.1. (Samemap Equivalence)

(i) $\forall \text{ALIST}. \text{SAMEMAP}(\text{ALIST}, \text{ALIST})$

(ii) $\forall \text{ALIST} \text{ALIST1}. \text{SAMEMAP}(\text{ALIST}, \text{ALIST1}) \land \text{SAMEMAP}(\text{ALIST1}, \text{ALIST})$

(iii) $\forall \text{ALIST} \text{ALIST1 ALIST2}. \text{SAMEMAP}(\text{ALIST}, \text{ALIST1}) \land \text{SAMEMAP}(\text{ALIST1}, \text{ALIST2}) \Rightarrow \text{SAMEMAP}(\text{ALIST}, \text{ALIST2})$

Part 2 contains the three mathematical facts, namely

— the proof of the Pigeon Hole Principle, and two proofs that every finite surjection is an injection (Section 4);
— the proof that permutations represented as association lists form a group (Section 5);
— the proof that permutations represented as lists of numbers form a group (Section 6).

Section 4 contains

Theorem. (Pigeonfact)

$\forall F. (\forall M. M < N \land F(M)) \land (\forall M. M < N \land F(M)) \Rightarrow (\forall M. M < N \land F(M))$

Corollary. (Pigeonlist)

$\forall U. \text{DISJOINT}(\text{SETSEQ}, \text{LENGTH} U) \Rightarrow$

$((\forall M. M < \text{LENGTH} U \land \text{MULT}(U, \text{SETSEQ}(M))) \Rightarrow$

$(\forall M. M < \text{LENGTH} U \land \text{MULT}(U, \text{SETSEQ}(M)))$

and the two applications of the pigeon hole principle. In both cases the proof takes three steps. In the version representing functions as association lists the desired result...

Theorem. (Permutp Injectp)

$\forall \text{ALIST}. \text{PERMUTP}(\text{ALIST}) \Rightarrow \text{INJECTP}(\text{ALIST})$

.. is proved through the following steps:

Lemma 4.1. (Inj Disj)

$\forall U. \text{INJ}(U) \Rightarrow \text{DISJOINT}(\lambda M. \text{MKSET}(\text{NTH}(U, M)), \text{LENGTH} U)$

Lemma 4.2. (Permutp Injectp Lemma)

$\forall V. \text{MKLSET}(U) \land \text{MKLSET}(V) \Rightarrow$

$(\forall M. M < \text{LENGTH}(U) \land \text{MULT}(V, \text{MKSET NTH}(U, M)))$
The conclusion follows by the lemma *Mult Inj*.

In the version representing functions as lists the result...

**Theorem.** *(Perm Injectivity)*

\[ \forall U \, \text{PERM}(U) \supset \text{INJ}(U) \]

...is proved again in three steps:

**Lemma 4.4.** *(Disjoint Number)*

\[ \forall N \, \text{DISJOINT}(\lambda X. \text{MKSET}(X), N) \]

**Lemma 4.5.** *(Onto Mult)*

\[ \forall U \, \text{ONTO}(U) \supset (\forall N \in \text{LENGTH}(U) \subseteq \text{MULT}(U, \text{MKSET}(N))) \]

**Lemma 4.6.** *(Into Mult)*

\[ \forall U \, \text{INTO}(U) \supset (\forall K \in \text{LENGTH}(U) \subseteq \text{MULT}(U, \text{MKSET}(K))) \supset (\forall I \in \text{LENGTH}(U) \subseteq \text{MULT}(U, \text{MKSET}(\text{NTH}(U, I)))) \]

The conclusion follows using the lemma *Mult Inj*.

**Sections 5 – 6** contain definitions of the operation *composition* of functions, of the *identity* function and of the operation taking the *inverse* of a permutation and proofs of the following theorems:

**Theorem 1.** (i) The composition of permutations is a permutation.
(ii) Composition of functions is associative.

**Theorem 2.** (i) The identity function \( i \) is a permutation.
(ii) For every permutation \( f \), \( f \circ i = f \).
(iii) For every permutation \( f \), \( i \circ f = f \).

**Theorem 3.** (i) For every permutation \( f \), the inverse function \( f^{-1} \) is a permutation.
(ii) For every permutation \( f \), \( f \circ f^{-1} = i \).
(iii) For every permutation \( f \), \( f^{-1} \circ f = i \).

In **Section 5** we work with association lists. In the proof of the theorems we need the following facts:

**Lemma 5.1** *(App Compalist)*

\[ \text{VALIST} \text{ALIST1} \in \text{MEMBER}(X, \text{DOM} \text{ALIST})) \supset \text{APPALIST}(X, \text{ALIST} \in \text{ALIST1}) = \text{APPALIST}(\text{APPALIST}(X, \text{ALIST}), \text{ALIST1}) \]
In *Section 6* first we discuss the choice of LISP functions and predicates for the representation through lists of numbers. Then the proofs of the theorems in the representations PERMP, using predicates, and PERMF, using LISP functions, are shown in parallel.

In the version PERMF we need first to prove some facts about length.

**Lemma 6.1.** (*Length Compose*)

\[ \forall U \exists W. \text{DEF} \rightarrow \text{APPL}(W, U) \land \text{LENGTH}(W@U) = \text{LENGTH}(U) \]

**Lemma 6.2.** (*Length Ident*)

\[ \forall N. \text{LENGTH}(\text{IDENT}(N)) = N \]

**Lemma 6.3.** (*Length Inverse*)

\[ \forall U. \text{PERM}(U) \land \text{LENGTH}(\text{INVERSE}(U)) = \text{LENGTH}(U) \]

In the version PERMF by proving first the following facts, we make it possible to follow the proofs of the version PERMP.

**Lemma 6.4.** (*Nth Compose*)

\[ \forall U. \exists V, N. \text{DEF} \rightarrow \text{APPL}(V, U) \land \text{NTH}(V@U, N) = \text{NTH}(V, \text{NTH}(U, N)) \]

**Lemma 6.5.** (*Main Id*)

\[ \forall N. \exists N. \text{NTH}(\text{IDENT}(N), N) = N \]

**Lemma 6.6.** (*Main Inv*)

\[ \forall U. \exists N. \text{PERM}(U) \land \exists N. \text{LENGTH}(U) \land \text{NTH}(\text{INVERSE}(U, N)) = \text{FSTPOSITION}(U, N) \]
ABOUT PERMUTATIONS IN LISP AND EKL
PART 1

2.1. Educating EKL about propositional Logic.

One of the unique features of EKL is the ability to describe procedures like bringing formulas into disjunctive normal form (where other rewriters can then be applied) as a set of simple rewriters. However, since this is often not appropriate and may cause combinatorial explosions, we do not add these to the default rewrite facts denoted by simpinfo; instead we want to call those lines as rewriters when needed.

; propositional schemata, used by the rewriter to normalize expressions (proof normal)

1. \text{\texttt{(trw \mid \forall p \ q \ r . ((pvq)\alpha r) \equiv ((pA\alpha r)v(qA\alpha r)) \mid)}}
   \text{\texttt{(label normal)}}

2. \text{\texttt{(trw \mid \forall p \ q \ r . (\exists \alpha(pvq)) \equiv ((\exists \alpha p)v(\exists \alpha q)) \mid)}}
   \text{\texttt{(label normal)}}

3. \text{\texttt{(trw \mid \forall p \ q \ r . ((pvq)\alpha r) \equiv ((pA\alpha r)v(qA\alpha r)) \mid)}}
   \text{\texttt{(label normal)}}

4. \text{\texttt{(trw \mid \forall p \ q \ r . (pvq\alpha r) \equiv (p\alpha r)\lambda(q\alpha r)) \mid)}}
   \text{\texttt{(label normal)}}

5. \text{\texttt{(trw \mid \forall p \ q . (\neg(pvq)) \equiv ((\neg p)\lambda(\neg q)) \mid)}}
   \text{\texttt{(label demorgan)}}

6. \text{\texttt{(derive \mid \forall p \ q \ . (\neg(pAq)) \equiv (\neg p)v(\neg q) \mid)}}
   \text{\texttt{(label demorgan)}}

Now the rewriter will be able to normalize expressions, distributing conjunction over disjunction, eliminating disjunctions in the antecedent of an implication and negations of disjunctions.

The pure rewriter, however, finds it difficult to make certain inferences in conditional rewriting. This problem may be overcome by introducing propositional facts to be used later as rewriters.

7. \text{\texttt{(derive \mid \forall p \ q . p \equiv (q\exists p)\lambda(\neg q\exists p) \mid)}}
   \text{\texttt{(label excluded-middle)}}

8. \text{\texttt{(derive \mid \forall p \ q \ r . (q\alpha r)\lambda(if \ p \ then \ q \ else \ r)\alpha r) \mid)}}
   \text{\texttt{(label trans_cond)}}

Remark. Example 1. The use of the lines labeled NORMAL is an interesting example of use of second order unification. Since sentences are just terms of type truthval, we can apply to them the rewriting procedure in a uniform way. This is made possible, of course, by the use of the higher order unification. We give an example of its application. The fact to prove is the transitivity of $\leq$, assuming the transitivity of $\leq$. Using our technique we collapse into one line a 16 line long Natural Deduction style proof. We will present the Natural Deduction Style proof first.
About Permutations in \textsc{Lisp} and \textsc{Eki.}

(wipe-out)
(get-proofs nth prf prm glb)
(proof example)

(setq rewritemessages t)

;labels: TRANSITIVITY-OF-ORDER
;\forall n k n<m \land k<n \rightarrow k<n

;labels: LESSEQDEF
;\forall n. n \leq n \equiv (n = n \lor n < n)

(\text{Remember: (open lesseq) is the same as use: lesseqdef mode: exact.})

0. (trw |\forall n m k. n \leq m s k \land n \leq s k| (open lesseq)
\text{transitivity-of-order})
\text{the term } N \leq M \text{ is replaced by:}
N = N \lor N < M
\text{the term } M \leq S K \text{ is replaced by:}
M = K \land M < K
\text{the term } N \leq S K \text{ is replaced by:}
N = K \land N < K
(\forall n m k. n \leq m s k \land n \leq s k) \equiv (\forall n m k. (n = m \lor n < m) \land (m = k \lor m < k) \land n < k)

We do not go very far by simply expanding the definition of \textless, because the rewriter does not know what to do with the disjunctions in the antecedent.

Instead, we can construct a derivation and use two arguments by cases to handle the disjunctions (lines 1-1 and 15).

(setq rewritemessages nil)

1. (assume |n \leq m|)
\text{(label example1)}

2. (assume |m \leq s k|)
\text{(label example2)}

3. (rw example1 (open lesseq))
N = N \lor N < M
\text{(label example3)}
\text{deps: (EXAMPLE1)}

Argue by cases. First case:

4. (assume |n = m|)

5. (rw example2 (use \ast mode: exact direction: reverse>>
N \leq K
\text{(label example4)}

Second case:
6. (assume \( |n<m| \))
   (label example5)

7. (rw example2 (open lesseq))
   \( M=KV_M<K \)
   (label example6)
   ;deps: (EXAMPLE2)

Within the second case, we need another argument by cases.

8. (assume \( |m=k| \))

9. (rw example5 (use * mode: exact))
   \( N<K \)

10. (trw \( |nsk| \) (open lesseq) *)
    \( NSK \)
    (label example7)

11. (assume \( |m<k| \))

12. (derive \( |n<k| \) (transitivity-of-order example5 *))

13. (trw \( |nsk| \) (open lesseq) *)
    \( NSK \)
    (label example8)

14. (cases example6 example7 example8)
    \( NSK \)
    (label example10)
    ;deps: (EXAMPLE2 EXAMPLE5)

This concludes the second case. So we can conclude our first argument.

15. (cases example3 example4 example10)
    \( NSK \)
    ;deps: (EXAMPLE1 EXAMPLE2)

16. (ci (example1 example2))
    \( NKMAMSK\not\subseteq K \)

This concludes the Natural Deduction style proof of the transitivity of \( \leq \). However, using the rewriter NORMAL we can do all this in one step.

0. (trw \( \forall n \ m \ K.\nsK\not\subseteq K \) (open lesseq) (use normal mode: always)
   transitivity-of-order)
   \( \forall n \ m \ K.\nsK\not\subseteq K \)
   (label example)

For after expanding the definition of \( \leq \) the rewriter uses lines 1 and 2 of the proof NORMAL
;the term \(N=MvN<M\) is replaced by:
\[N=MA(M=KvM<K)vN<MA(M=KvM<K)\]
;the term \(N=Mh(M=KvM<K)\) is replaced by:
\[N=MA(M=KvM<K)\]

So in the first disjunct;
;the term \(M\) is replaced by:
\(K\)

Similarly
;the term \(N<MA(M=KvM<K)\) is replaced by:
\[N<AM=KvN<AM<K\]
;the term \(M\) is replaced by:
\(K\)

Later the rewriter uses line 4 of the proof NORMAL. This corresponds to argument by cases.
;the term \(N=AM=KvN<A(M=KvM<K)\) is replaced by:
\[(N=AM=KvN<A(M=KvM<K))\]

Now standard rewriting does the job for the first conjunct:
;the term \(N=K\) is replaced by:
\(TRUE\)
;the term \(TRUEvN<K\) is replaced by:
\(TRUE\)
;the term \(N=KvN<K\) is replaced by:
\(TRUE\)

\(\text{etc.}\)

2.2. 

\textbf{Educationing EKL about first grade Arithmetic.}

First we ask EKL to read the proofs contained file MINUS, namely the proofs "minus" and "lesseq". They in turn contain the instruction of reading the files NATNUM and NORMAL (see the Appendix).

\(\text{(wipe-out)}\)
;Done.Proof?

\(\text{(get-proofs minus)}\)
;file read in
;switched to MINUS
;the proof LESSEQ read in.
;the proof INDUCTION read in.
;the proof MINUS read in.
;the proof NATNUM read in.
;the proof NORMAL read in.

\(\dagger\) We use \(\Box\) for the end of an example and \(\mathbf{I}\) for the end of a proof (both informal and mechanical).
2.3. **LISP and the Bound Quantifier Allp.**

Similarly we ask EKL to learn about LISP by reading the file LISPAX (see the Appendix).

```
(wipe-out)
; Done. Proof?
(get-proofs lispax)
; file read in
; switched to LISPAX
; the proof LISPAX read in.
```

In defining function&, the language of EKL gives us the option between a definition by recursion and a definition using bounded quantifiers.

Consider the predicate \( \text{allp}(\phi, u) \), to be interpreted as "for all members \( x \) of \( u \), \( \phi(u) \). It could be defined as:

```
(define allp (\forall \phi x u. allp(\phi, u) \equiv (\forall x. \text{member}(x, u) \implies \phi(x)))
```

The definition by recursion \( \text{Allpdef} \)

\[
\forall \phi x u. \text{allp}(\phi, \text{nil}) =
\text{allp}(\phi, x . u) = \text{if } \phi(x) \text{ then } \text{allp}(\phi, u) \text{ else false}
\]

simplifies its use in proofs by induction on lists: consider for instance the proof's of the Lemma \textit{Nth} \textit{Compose} or of Theorem \textit{Assoc Compose}. In contests where a straightforward proof by induction is not possible, we may use the other definition, having proved the equivalence.

```
; facts about allp
(proof allp)
;a reformulation of the definition of allp
1 (trw [\forall \phi x u. \text{allp}(\phi, x . u) \implies \phi(x) \land \text{allp}(\phi, u)] (open allp))
; \forall \phi x u. \text{ALLP}(\phi, x . u) \implies \phi(x) \land \text{ALLP}(\phi, u)
(label allp_introduction)

2 (ue (\phi \lambda u. (\forall y. \text{member}(y, u) \implies \phi_1(y) \land \text{allp}(\phi_1, u)))
; listinduction
    (open allp member) (use normal mode: always))
(label allp_introduction)
; \forall u. (\forall y. \text{MEMBER}(y, u) \implies \phi_1(y) \land \text{ALLP}(\phi_1, u))

; allp_elimination

3 (ue (\phi \lambda u. \text{member}(x, u) \land \text{allp}(\phi_1, u) \implies \phi_1(x)))
; listinduction
    (part 1 (open member allp) (use normal mode: always))
(label allp_elimination)
; \forall u. \text{MEMBER}(x, u) \land \text{ALLP}(\phi_1, u) \implies \phi_1(x)

; allp_implication
```
4. (ue (phi |\a.u.\a1.allp(a,u)A(\a.x.a(x)\a1(x))\a1.allp(a1,u)|)
lisinduction (open allp))
(label allp_implication)
;\a\U \a1.ALLP(\a,u)A(\a.x.a(x)\a1(x))\a1.allp(a1,u)

Similarly for the predicate somep:

\V phi x u.\neg somep(phi,nil)A

somep(phi,x.u)=if phi(x) then true else somep(phi,u)

(proof somepprop)

1. (ue (phi |\a.u.member(y,u)\a1(phi1(y)\a1.somep(phi1,u)|)
lisinduction
(open somep member) (use normal mode: always))
;\a\U.MEMBER(Y,U)\a1(phi1(y)\a1.somep(phi1,u))

2. (derive |\a.u.\exists y.member(y,u)\a1(phi1(y))\a1.somep(phi1,u)| *)

3. (ue (phi |\a.u.somep(phi1,u)\a1(\exists x.member(x,u)\a1(phi1(x)))|)
lisinduction
(part 1 (open member somep) (use normal mode: always) (der)))
;\a\U.somep(phi1,u)\a1(\exists x.member(x,u)\a1(phi1(x)))

4. (derive |\a.u.somep(phi1,u)\a1(\exists x.member(x,u)\a1(phi1(x)))| (* -2))
(label somep_fact)

2.4. Facts of elementary set theory.

Next we introduce some useful notations of elementary set theory. We do not distinguish between sets and predicates: our variables av, bv for sets will allow us to speak only about very few sets (only sets of "urelements", sets of objects of type ground—see the file 1.5.1).

Remark. Example 2. The following example shows that some care is needed in dealing with default declarations. In guessing the declaration for a term, EKL looks for syntactical similarities with previously defined terms: thus if x has been previously declared, EKL tries the same declaration for xl or xv.

If we start a new proof, without access to the previous ones, then the expression xv receives default declaration type: ground syntype : variable sort: universal.

(proof sets)

1. (decl (av bv) (type: ground+truthval))
2. (decl epsilon (type: ground+av+truthval)
   (infixname: $\epsilon$) (bindingpower: 925))
3. (define epsilon |\forall av xv.xv$\in$av=av(xv)|)
   ;XV is unknown.
   ;the symbol XV declared to have type GROUND
On the other hand, in the proof \textsc{Lispax} the term \( x \) has already been declared: its declaration is type: ground syntype: variable sort: sexp. Therefore, if we give EKL access to the proof \textsc{lispax} first, then \( xv \) becomes a variable of the sort sexp (line 3 below).

Since in this paper we will consider only sets of S-expressions, such default declaration is convenient.

\begin{verbatim}
(get-proofs allp)
; file read in
; switched to ALLP
; the proof ALLP read in.
; the proof LISPAX read in.

(proof sets)

1. (decl (av bv) (type: lground+truthval))
2. (decl epsilon (type: lground@av+truthval)
   (inf ixname : x) (bindingpower: 925))

3. (define epsilon (\forall xv . xv\in av\Rightarrow av(xv)))
   (label epsilondef)
   ; XV is unknown.
   ; the symbol XV is given the same declaration as X

However, there is a more elegant way to obtain this result; we can declare \( xv \) to be of some sort, say urelement:

\begin{verbatim}
(wipe-out)
(proof set)

(decl (xv yv zv) (type: lgroundl) (sort: urelement))

Then we establish, by axioms, that urelements and S-expressions are the same class.

(axiom (\forall x . x \in x))
(label simpinfo)

(axiom (\forall xv . xv \in exp xv))
(label simpinfo)
\end{verbatim}

Thus we can create the two files separately and later give EKL access to both files and assume the above axioms, if needed. \( \square \)

\begin{verbatim}
; useful set theory
(wipe-out)
(get-proofs allp)
(proof sets)

; all urelements will be S-expressions
; all S-expressions will be urelements

1. (decl (xv yv zv) (type: lgroundl) (sort: urelement))
2. (decl (av bv) (type: lground+truthval))
\end{verbatim}
3. (axiom \( \forall x.\text{urelement} \; x \))
   (label simpinfo)

4. (axiom \( \forall xv.\text{sexp}(xv) \))
   (label simpinfo)

5. (decl epsilon (type: [ground\(\rightarrow\)av\(\rightarrow\)truthval])
   (inf ixname: \( \epsilon \)) (bindingpower: 925))

6. (define epsilon \( \forall av \; xv.\epsilon av = av(xv) \))
   (label epsilondef)

7. \( \forall A \; B. (\forall xv. \; xv \in A \lor xv \in B) \implies A = B \)
   (label set,extensionality)

8. (decl intersection (type: [set\(\rightarrow\)set\(\rightarrow\)set])
   (inf ixname: \( n \)) (bindingpower: 950)
   (pref ixname: intersection)

9. (define intersection \( \forall a \; b. a \cap b = \lambda xv. (a(xv) \land b(xv)) \))
   (label interdef)

10. (decl union (type: [set\(\rightarrow\)set\(\rightarrow\)set])
    (inf ixname: \( U \)) (bindingpower: 950)
    (prefixname: union))

11. (define union \( \forall a \; b. a \cup b = \lambda xv. (a(xv) \lor b(xv)) \))
    (label uniondef)

12. (decl inclusion (type: [set\(\rightarrow\)set\(\rightarrow\)truthval])
    (inf ixname: \( C \)) (bindingpower: 920)
    (pref ixname: inclusion)

13. (define inclusion \( \forall a \; b. a \subseteq b = \forall xv. (a(xv) \implies b(xv)) \))
    (label inclusiondef)

14. (defax emptyset \( \text{emptyset} = \lambda xv. \text{false} \))
    (label emptysetdef)

15. (defax emptyp \( \forall a. \text{emptyp}(a) = \forall xv. \neg a(xv) \))

We want to be able to talk of the set of occurrences of an S- expressions \( x \) as well as of the set of elements of a list \( u \).

16. (decl mkset (type: [ground\(\rightarrow\)set])

17. (define mkset \( \forall xv.\text{mkset}(xv) = (\lambda yv. yv = xv) \))
    (label mkset,def)

    ; the set of members of a list

18. (decl mklset (type: [ground\(\rightarrow\)av])

19. (define mklset \( \forall u.\text{mklset}(u) = \lambda x.\text{member}(x,u) \))
    (label mklsetdef)
2.5. **Putting things together.**

The basic ground domain will contain both S-expressions and natural numbers. We need both to define the function length

\[ \text{Vu } x. (\text{length } nil = 0) \land \text{length}(x.u) = (\text{length } u), \]

(see the Appendix).

```
(get-proofs length)
;file read in
;switched to SETFACTS
;the proof SETFACTS read in.
;the proof ALLP read in.
;the proof LESSEQ read in.
;the proof INDUCTION read in.
;the proof LENGTH read in.
;the proof MINUS read in.
;the proof NATNUM read in.
;the proof NORMAL read in.
;the proof SETS read in.
;the proof LISPAX read in.
```

In such context, the following principle (*Doubleinduction*) of double induction for lists and numbers will be very useful:

\[ \forall \nu, x. \Phi \nu(\text{NIL}, N) \land \Phi \nu(U, 0) \land (\Phi \nu(U, N) \land \Phi \nu(x, u, N')) \implies (\nu U, \Phi \nu(U, N)) \]

Numbers and S-expressions are ground objects of different sorts.

```
(axiom \(\forall \nu. \text{sexp } \nu\))
(label simpinfo)

(axiom \(\forall \nu. \text{null}(\nu)\))
(label simpinfo)
```

We remarked above that, some care is needed to give the database the proper structure of types and sorts. In our experiment, no artificial limitation of expressive power is imposed by the type structure of EKL. Now we are ready to introduce the main LISP functions needed for our representations of permutations.

2.6. **Properties of Nth.**

The LISP function nth plays a key role in our representation. nth and nthcdr are defined as total functions, with the default value NIL. We shall present facts about these functions as examples of simple inferences in EKL.
Example 3. The well-definedness of nth is an immediate consequence of its definition by double induction on lists and numbers. We show the rewriting process in detail. Without the use of simpinfo the following statement is obtained.

\begin{verbatim}
(setq rewritemessages t)
0. (ue (phi3 |λu n.sexp nth(u,n)|) doubleinductionl (nuse simpinfo))
  ;(∀N X.SEXP NTH(NIL,N)∧SEXP NTH(U,O)∧
   ; (SEXP NTH(U,N)∧SEXP NTH(X.U,N )))\top
  ;(∀N.SEXP NTH(U,N))

The information in simpinfo, including the definition of nth, is enough to obtain the result.

3. (ue (phi3 |λu n.sexp nth(u,n)|) doubleinductionl)
  ;the term NTH(NIL,N) is replaced by:
    NIL
  ;the term SEXP NIL is replaced by:
    TRUE
  ;the term SEXP NTH(U,O) is replaced by:
    TRUE
  ;the term NTH(X.U,N') is replaced by:
    NTH(U,N)
  ;the term SEXP NTH(U,N) is replaced by:
    TRUE
  ;the term SEXP NTH(U,N)∧TRUE is replaced by:
    TRUE
  ;the term TRUE∧TRUE∧TRUE is replaced by:
    TRUE
  ;the term W N X.TURE is replaced by:
    TRUE
  ;the term TRUE∧(∀N.SEXP NTH(U,N)) is replaced by:
    W N.SEXP NTH(U,N)
  ;∀N.SEXP NTH(U,N)
  (label simpinfo) (label sexp_nth)
\end{verbatim}

Lemma 2.1. (Nth Member)

\[ W \ N \ N<LENGTH \ U \ \text{MEMBER}(NTH(U,N),U) \]

Proof. We use double induction also the membership of the values of nth in the original list. The first base case, when \( n = 0 \), is proved by listinduction. For \( u = \text{NIL} \) we obtain a contradiction.
in the antecedent (the line \texttt{ZEROLEAST1}, proof \texttt{NATNUM}, is in simpinfo). For \( u = x.u \) we apply definitions of \texttt{nth} and of \texttt{member}.

\[
(ue (phi \lambda u.0<\text{length }u) \land \text{member}(\text{nth}(u,0),u)) \text{ listinduction } \\
(\text{open member}) \\
; \forall u.0<\text{LENGTH }u \land \text{member}(\text{nth}(u,0),u)
\]

. The other base case gives again a. contradiction and the inductive step is immediately reduced to the induction hypothesis. Indeed, \( n'<\text{length}(x.u) \) reduces to \( n'<(\text{length}(u)) \) and by \texttt{SUCCESSORLESS} (proof \texttt{NATNUM}) to \( n<\text{length}(u) \). By definition, \( \text{nth}(x.u,n') = \text{nth}(u,n) \).

\[
(ue (phi \lambda u.n.n<\text{length }u) \land \text{member}(\text{nth}(u,n),u)) \text{ doubleinduction} \\
(\text{use memberdef mode: always}) (\text{use *}) \\
: \forall W.\forall N.\forall N<\text{LENGTH }u \land \text{member}(\text{nth}(u,N),u) \\
(\text{label nthmember})
\]

We need a converse of \texttt{NTHMEMBER}:

\textbf{Lemma 2.2 (Member Nth)}

\[ W \land \text{member}(Y,U) \land (\exists N.\forall N<\text{LENGTH }U \land \text{nth}(U,N) = Y) \]

\textbf{Proof.} Since \texttt{Member Nth} is an existential statement, we have to expand the proof. We use induction on the list \( u \). In order to prove that

\[ \exists n.n<\text{length}(x.u) \land \text{nth}(x.u,n) = y, \]

assume the induction hypothesis (line 1) and the antecedent for the inductive step (line 2), (line 11).

\[
(\text{proof member,nth}) \\
1. (assume \{ (\text{member}(Y,U) \land (\exists N.\forall N<\text{LENGTH }U \land \text{nth}(U,N) = Y) ) \}) \\
\text{ (label m_n1) ; deps: (1)} \\
2. (assume \{ \text{member}(y,x.u) \}) \\
\text{ (label m_n2) ; deps: (2)} \\
3. (rw * (open member)) \\
\text{ (label m_n3) ; Y=x \text{member}(Y,U) ; deps: (M_N2)}
\]

This requires a proof by cases.

\[
4. (assume \{ y=x \}) \\
\text{ (label m_n4) ; deps: (4)}
\]
If \( y = x \), one can take 0 for the desired \( n \). It is enough to expand the definitions of \( \text{length} \) and \( \text{nth} \) in line 5 to verify that
\[
0 < \text{length}(x.u) \quad \text{and} \\
0 < \text{nth}(x.u,0) = y.
\]

5. (trw \( 0 < \text{length}(x.u) \quad \text{and} \quad \text{nth}(x.u,0) = y \))
\; \text{deps:} \; (M\_N4)

6. (derive \( \exists n. \, n < \text{length}(x.u) \quad \text{and} \quad \text{nth}(x.u,n) = y \))
\; \text{label m\_n5}
\; \text{deps:} \; (M\_N4)

Second case:

7. (assume \( \text{member}(y,u) \))
\; \text{label m\_n6}
\; \text{deps:} \; (7)

8. (define nv \( \text{invclength } u \quad \text{and} \quad \text{nth}(u,nv) = y \))
\; (m\_n1 * )
\; \text{NV} is unknown.
\; \text{the symbol NV} is given the same declaration as N
\; \text{deps:} \; (M\_N1 \_M\_N6)

The command DEFINE allows the introduction of an eigenvariable. This is EKL’s way to deal with existential elimination. Now take \( n' \) for \( n \):

9. (trw \( n' < \text{length}(x.u) \quad \text{and} \quad \text{nth}(x.u,nv) = y \))
\; \text{NV' < length} \quad \text{and} \quad \text{nth}(x.u,nv') = y
\; \text{deps:} \; (M\_N1 \_M\_N6)

10. (derive \( \exists n. \, n < \text{length}(x.u) \quad \text{and} \quad \text{nth}(x.u,n) = y \))
\; \text{label m\_n7}
\; \text{deps:} \; (M\_N1 \_M\_N6)

Existential introduction is performed in lines 6 and 10 by the DERIVE command. In both cases we have reached the desired conclusion.

11. (cases m\_n3 m\_n5 m\_n7)
\; \text{3N.} \, n < \text{length} \quad \text{and} \quad \text{nth}(x.u, n) = y
\; \text{deps:} \; (M\_N1 \_M\_N2)

Cases derives the formula of lines 6 and 10 (the formula must be the same) and discharges the open assumptions of lines 4 and 7, respectively, by using line 3. We use conditional introduction to discharge assumptions and to write down the induction step (line 13). In line 14 the inductive argument is performed as a rewriting procedure, using line 13 as a rewriter.

12. (ci m\_n2)
\; \text{MEMBER}(y,x.u) \cap \text{3N.} \, n < \text{length} \quad \text{and} \quad \text{nth}(x.u, n) = y
\; \text{deps:} \; (M\_N1)

13. (ci M\_N1)
\; \text{MEMBER}(y,u) \cap \text{3N.} \, n < \text{length} \quad \text{and} \quad \text{nth}(u,n) = y
\; \text{MEMBER}(y,x.u) \cap \text{3N.} \, n < \text{length} \quad \text{and} \quad \text{nth}(x.u, n) = y

The base case is trivial since NIL has no members. Therefore:

14. \((\text{ue } (\phi \mid \lambda u.\text{member}(y,u) \vee (\exists n. n < \text{length } u \land \text{nth}(u,n) = y))) \text{ list induction (open member) } *)\)

\(\forall U. \text{member}(y,u) \vee (\exists n. n < \text{length } u \land \text{nth}(u,n) = y)\)

2.7. Properties of Nthcdr.

(proof nthcdr)

1. (decl nthcdr (syntype: constant) (type: \([\text{ground} \oplus \text{ground}]\))

2. (defax nthcdr \(\forall x u n. \text{nthcdr}(\text{nil},n) = \text{nil}\) \(\land\) \(\text{nthcdr}(u,0) = u\)
\(\land\) \(\text{nthcdr}(x,u,n') = \text{nthcdr}(u,n)\)
(label simpinfo) (label nthcdrdef)

The proofs of the following facts are quite easy and can be found in the Appendix.

3. \(\forall U. \text{LISTP} \text{NTHCDR}(U,N)\)
(label simpinfo)

4. \(\forall U. 0 < \text{LENGTH } U \land \text{nth}(U,0) = U\)
(label nth,nthcdr,zero)

5. \(\forall U. N < \text{LENGTH } U \land \text{CAR} \text{NTHCDR}(U,N) = \text{NTH}(U,N)\)
(label car,nthcdr)

6. \(\forall U. \text{CDR} \text{NTHCDR}(U,N) = \text{NTHCDR}(U,N')\)
(label cdr-nthcdr)

Lemma 2.3. (Nthcdr Car Cdr)

7. \(\forall U. N < \text{LENGTH } U \land \text{NTHCDR}(U,N) = \text{NTH}(U,N) \land \text{NTHCDR}(U,N')\)
(label nthcdr,car,cdr)

The proof of the following Lemma is of some interest. We give it here.

Lemma 2.4. (NthinNthcdr)

\(\forall U. M. N < M < \text{LENGTH } U \land \text{MEMBER}(\text{NTH}(U,M), \text{NTHCDR}(U,N))\)

Proof. First, we show

\(\forall U. M. (N < M < \text{LENGTH } U \land \text{MEMBER}(\text{NTH}(U,M), \text{NTHCDR}(U,N)))\)

by double induction on numbers and lists, i.e. on \(n\) and on \(u\) (line 13). For \(n = 0\) the result is just the lemma Nthmember. For \(u = \text{NIL}\) we have a false antecedent.

As the inductive hypothesis we need an explicitly universally quantified formula:

1. (assume \(\forall M. (N < M < \text{LENGTH } U \land \text{MEMBER}(\text{NTH}(u,m), \text{NTHCDR}(u,n)))\))
(label nincdr)
The inductive step is proved by a secondary induction on \( m \). The case \( m = 0 \) gives a false antecedent. When \( \mathbf{172} \) is a successor the inductive formula is rewritten to an instance of line 10, using the definitions of \( \text{nth}, \text{nthcdr}, \text{length} \) and the fact \( \text{Successorless} \), file \text{NATNUM}, which is in \text{simpinfo}.

Notice that we must tell EKL not to use the definitions of \( \text{nth}, \text{nthcdr} \) and \( \text{length} \) in the part of the formula that corresponds to the conclusion.

2. \((\lambda m. (n' < m \text{Am} \text{length}(x, u)) \text{member}(\text{nth}(x, u, m), \text{nthcdr}(x, u, n')))) >\)

proof-by-induction
(part 2 (nuse nthdef nthcdrdef lengthdef))
nincdr zero-non-less-successor)

\( \forall n' < n \forall n < \text{LENGTH} (x, u) \text{MEMBER}(\text{nth}(x, u, n), \text{nthcdr}(x, u, n')) \)

3. \((\text{nincdr})\)

\( \forall m < n < \text{LENGTH} u \text{MEMBER}(\text{nth}(u, m), \text{nthcdr}(u, n)) \)

\( \forall n' < n \forall n < \text{LENGTH} u' \text{MEMBER}(\text{nth}(x, u, n), \text{nthcdr}(x, u, n')) \)

We can conclude the main induction.

4. \((\lambda u. \forall n < m < \text{length}(u) \text{member}(\text{nth}(u, m), \text{nthcdr}(u, n))) \)

doubleinduction
(use nthmember mode: exact) (use * mode: exact)

\( \forall u \text{N M} < m < \text{length} u \text{MEMBER}(\text{nth}(u, m), \text{nthcdr}(u, n)) \)

It is interesting to notice that the above argument can be replaced by a one line proof using proof-by-induction as a rewriter.

0. \((\lambda u. \forall n < m < \text{length} u \text{member}(\text{nth}(u, m), \text{nthcdr}(u, n))) \)

doubleinduction
(use nthmember mode: exact)
(use proof-by-induction
ue: ((\lambda m. (n' < m < \text{length}(u)) \text{member}(\text{nth}(x, u, m), \text{nthcdr}(x, u, n)))))

mode: exact)

\( \forall u \text{N M} < m < \text{length} u \text{MEMBER}(\text{nth}(u, m), \text{nthcdr}(u, n)) \)

In the last step an argument by cases is avoided by our technique of using second order unification (line \text{Normal}).

5. \((\text{trw} \forall u n m < m < \text{length}(u) \text{member}(\text{nth}(u, m), \text{nthcdr}(u, n))) \)

(open lesseq member)(use normal mode: always)

(use * nthcdr, car, cdr mode: exact)

\( \forall u \text{N M} < m < \text{length} u \text{MEMBER}(\text{nth}(u, m), \text{nthcdr}(u, n)) \)

(label nth, in, nthcdr)

The proofs of the following facts are easy and left to the Appendix.
1. \( VU N M \cdot N < \text{LENGTH} U A M < \text{LENGTH} (\text{NTHCDR}(U, N)) \)
   \( \text{NTH}(\text{NTHCDR}(U, N), M) = \text{NTH}(U, M+N) \)
   (label nth,nthcdr)

2. \( \forall U N \cdot N < \text{LENGTH} U \cdot \text{LENGTH} (\text{NTHCDR}(U, N)) = \text{LENGTH} U-N \)
   (label length,nthcdr)

3. \( \forall U \cdot \text{NTHCDR}(U, \text{LENGTH} U) = \text{NIL} \)
   (label last,nthcdr)

4. \( \forall U N \cdot \text{LENGTH}(U) \neq \text{NTHCDR}(U, N) = \text{NIL} \)
   (label trivial,nthcdr)

5. \( \forall A \cdot \forall U \cdot \text{ALLP}(A, U) \supset \text{ALLP}(A, \text{NTHCDR}(U, N)) \)
   (label allp,nthcdr)

The principle of nthcdr induction can be viewed as a trick to reduce induction on lists to finite induction on numbers. More interestingly, it is induction on lists localized to a given list, i.e. induction on the tails of a given list. Assume a list \( u \) is given; we can prove that \( u \) has a certain property \( \phi \) from the fact that the null list has property \( \phi \) and that if \( x, v \) is a tail of \( u \) and \( v \) has the property \( \phi \) then \( x, v \) has the property \( \phi \). Using the functions nth and nthcdr we can formulate this method of proof as finite descent from \( \phi(\text{nthcdr}(u, \text{length}(u))) \) to \( \phi(\text{nthcdr}(u, 0)). \)

The mechanical derivation of this inductive principle is not terribly interesting and is left to the Appendix.

6. \( \forall \phi U \cdot \phi(\text{NIL}) \wedge \)
   \( (\forall N \cdot N < \text{LENGTH}(U) \supset (\phi(\text{NTHCDR}(U, N')) \supset \phi(\text{NTH}(U, N) \cdot \text{NTHCDR}(U, N')))) \supset \phi(U) \)
   (label nthcdr,induction)

2.8. **Properties of Fstposition.**

In the representation of permutations the function \( \text{fstposition} \) plays the role of the inverse operation of \( \text{nth} \). Here we give the definition of \( \text{fstposition} \) and some facts about it.

\[ \text{fstposition} \]
(proof \text{fstposition})

\[ 1. \text{(decl (fstposition) (type: |ground@ground|))} \]
\[ 2. \text{(define \text{fstposition}} \]
\[ |\forall x u y. \text{fstposition}(nil, y) = \text{nil} \wedge \text{fstposition}(x . u, y) = \text{if \text{member}(y, x . u)} \]
\[ \text{then nil} \]
\[ \text{else if } x = y \]
\[ \text{then 0} \]
\[ \text{else addl(fstposition}(u, y)\} \]
(listinductiondef)
(label \text{fstposition}def)
2.9. The Lemmata Nth Fstposition and Fstposition Nth.

Since these facts are very basic, we comment the proofs in detail.

**Lemma 2.5 (Nth Fstposition)**

\[ \forall U. \forall N. \text{MEMBER}(N, U) \Rightarrow \text{NTH}(U, \text{FSTPOSITION}(U, N)) = N \]

The proof that f stposition is the right inverse of nth is a simple induction on lists.

1. \( \forall U. \forall n. \text{MEMBER}(n, U) \Rightarrow \text{NTH}(U, \text{FSTPOSITION}(U, N)) = N \)

To obtain the fact that f stposition is the left inverse of nth we need the additional hypothesis that \( u \) has the uniqueness property.

**Lemma 2.6 (Fstposition Nth)**

\[ \forall U. \forall N. \text{UNIQUENESS}(U) \land \text{LENGTH}(U) < \text{FSTPOSITION}(U, \text{NTH}(U, N)) = N \]

**Proof.** By double induction on \( u \) and \( n \).

(i) If \( u = \text{NIL} \), then \text{LENGTH}(u) is 0, and we obtain a contradiction in the antecedent.

(ii) If \( n = 0 \), we prove by induction on \( u \) that
\section{2}

\forall u. \text{UNIQUENESS}(u) \land 0 < \text{LENGTH} u \land \text{FSTPOSITION}(u, \text{CAR}(u)) = 0.

The base case is like \( i \), and the induction step is given by

\[
\text{FSTPOSITION}(x.\, u, \text{CAR}(x.\, u)) = \text{FSTPOSITION}(x.\, u, x) = 0.
\]

(iii) Assume the induction hypothesis

\[
\text{UNIQUENESS}(u) \land 0 < \text{LENGTH}(u) \land \text{FSTPOSITION}(u, \text{NTH}(u, n)) = n.
\]

We want:

\[
\text{UNIQUENESS}(x.\, u) \land 0 < \text{LENGTH}(x.\, u) \land \text{FSTPOSITION}(x.\, u, \text{NTH}(x.\, u, n')) = n'.
\]

Assume \text{UNIQUENESS}(x.\, u)\) and \( n' < \text{LENGTH}(x.\, u) \), which are rewritten as

\[
\neg \text{MEMBER}(x.\, u) \land \text{UNIQUENESS}(u) \quad \text{and} \quad n < \text{LENGTH}(u),
\]
respectively.

(iv) Now

\[
\text{FSTPOSITION}(x.\, u, \text{NTH}(x.\, u, n'))
\]

rewrites to

\[
\text{if } x = \text{NTH}(u, n) \text{ then } 0 \text{ else } \text{FSTPOSITION}(u, \text{NTH}(u, n')).
\]

We have only to show that \( x \neq \text{NTH}(u, n) \): for then we can apply the induction hypothesis. But if \( x = \text{NTH}(u, n) \) with \( n < \text{LENGTH}(u) \), then \( x \) is a member of \( u \), by \text{NTHMEMBER}, contradicting (iii).

\begin{enumerate}
\item (\text{proof } \text{FSTPOSITION-NTH})
\item (\text{derive } n < \text{LENGTH} u \land \text{NTH}(u, n) \land \text{MEMBER}(x, u) \land \text{NTHMEMBER})
\item (\text{derive } \text{UNIQUENESS}(x.\, u) \land 0 < \text{LENGTH} u \land x = \text{NTH}(u, n) \land \text{NTHMEMBER})
\item (\text{derive } \text{UNIQUENESS}(x.\, u) \land 0 < \text{LENGTH} u \land \text{FSTPOSITION}(x.\, u, \text{NTH}(u, n)) = n \land \text{NTHMEMBER})
\end{enumerate}

Remark. Example 4. The last line is a compact proof obtained by an interesting combination of rewriting steps. Let us look at the details of the rewriting process. The following statement must be verified:
Using simpinf 0, without specifying any rewriter, only few substitutions are made. by the definition of nth and the fact Successorless.

Let us see how the rewriting process simulates the above argument.

(i) First base case:

; the term UNIQUENESS(NIL) is replaced by: TRUE
; the term LENGTH NIL is replaced by: 0
; the term N<0 is replaced by: FALSE
; the term TRUEAFALSE is replaced by: FALSE
; the term FALSEFSTPOSITION(NIL,NTH(NIL,N)=N is replaced by: TRUE

Here EKL has found a contradiction in the antecedent.

(ii) Nest EKL does the second base case, by expanding the definition of nth and using line 1:

; the term NTH(U,O) is replaced by: CAR U
; the term FSTPOSITION(U,CAR U) is replaced by: 0
; the term 0=0 is replaced by: TRUE
; the term UNIQUENESS(U)AO<LENGTH UFSTPOSITION(U,NTH(U,N))=N is replaced by: TRUE

(iii) Now EKL starts the induction step. It expands the definitions of uniqueness, length and uses the fact Successorless (which is in simpinf 0).
; the term UNIQUENESS(X.U) is replaced by:
\neg MEMBER(X,U) \land UNIQUENESS(U)

; the term \( N' < \text{LENGTH}(X.U) \) is replaced by:
\( N < \text{LENGTH} U \)

; the term \( (\neg MEMBER(X,U) \land UNIQUENESS(U)) \land N < \text{LENGTH} U \) is replaced by:
\( \neg MEMBER(X,U) \land UNIQUENESS(U) \land N < \text{LENGTH} U \)

(iv) In expanding \textsc{fstposition}, \textsc{ekl} finds two nested \textsc{lisp} conditionals:

; the term \textsc{fstposition}(X.U,\textsc{nth}(X.U,N')) is replaced by:
\begin{verbatim}
IF \neg MEMBER(\textsc{nth}(X.U,N'), X.U) THEN NIL ELSE (IF X=\textsc{nth}(X.U,N') THEN 0 ELSE FSTPOSITION(U,\textsc{nth}(X.U,N')))
\end{verbatim}

; the term \textsc{member}(\textsc{nth}(X.U,N'), X.U) is replaced by:
\textsc{nth}(X.U,N')=X \lor \textsc{member}(\textsc{nth}(X.U,N'), U)

; the term \textsc{nth}(X.U,N') is replaced by:
\textsc{nth}(U,N)

; the term \textsc{nth}(U,N)=X is replaced by:
FALSE

Line 3 has been used here.

; the term \textsc{nth}(X.U,N') is replaced by:
\textsc{nth}(U,N)

; the term \textsc{member}(\textsc{nth}(U,N), U) is replaced by:
TRUE

Here \textsc{ekl} has used the fact \textit{nthmember}.

; the term FALSEvTRUE is replaced by:
TRUE

; the term \neg TRUE is replaced by:
FALSE

The if clause of the outermost conditional is therefore false (see the first line after (iv)). Now \textsc{ekl} moves to the else clause and finds the innermost conditional.

; the term \textsc{nth}(X.U,N') is replaced by:
\textsc{nth}(U,N)

; the term X=\textsc{nth}(U,N) is replaced by:
FALSE

Line 3 has been used here again to see that the if clause of the innermost conditional is false.

Hence \textsc{ekl} considers the else clause, i.e.

\textsc{fstposition}(U,\textsc{nth}(X.U,N'))

(see the first line after (iv)).

; the term \textsc{nth}(X.U,N') is replaced by:
\textsc{nth}(U,N)

; the term \textsc{fstposition}(U,\textsc{nth}(U,N)) is replaced by:
\textsc{N}

Here the induction hypothesis has been used.
; the term IF FALSE THEN 0 ELSE N’ is replaced by:
N’
; the term IF FALSE THEN NIL ELSE N’ is replaced by:
N’

This concludes the evaluation of the term FSTPOSITION(X.U,NTH(X.U,N’)). The result follows by standard rewriting.

; the term N’=N’ is replaced by:
TRUE
; the term -MEMBER(X,U)\&UNIQUENESS(U)\& LENGTH U\& TRUE is replaced by:
TRUE
; the term (UNIQUENESS(U)\& LENGTH U\& FSTPOSITION(U,NTH(U,N))=N)\& TRUE is replaced by:
TRUE
; the term TRUE\& TRUE\& TRUE is replaced by:
TRUE
; the term VU N X.TRUE is replaced by:
TRUE
; the term VU N TRUE is replaced by:
TRUE
; the term TRUE\&(\&TRUE\& VU N UNIQUENESS(U)\& LENGTH U\& FSTPOSITION(U,NTH(U,N))=N) is replaced by:
VU N UNIQUENESS(U)\& LENGTH U\& FSTPOSITION(U,NTH(U,N))=N
; VU N UNIQUENESS(U)\& LENGTH U\& FSTPOSITION(U,NTH(U,N))=N

EI

2.10. **Injectivity and Uniqueness.**

We already pointed out that, in order to represent the property ‘each member of a list u occurs just once in the list u’, we can use either the recursively defined predicate uniqueness

V u x.uniqueness nil \&
(uniquness(x.u)=\neg member(x,u)\& uniqueness(u)),
or the predicate inj, defined using a bounded quantifier.

; injectivity
; another predicate for uniqueness
(proof inj)

(decl (inj) (type: [ground-truthval]))
(defn inj)
|\forall u.inj(u)=\forall n.m.n<length(u)\& m<length(u)\& nth(u,n)=nth(u,m)\& n=m| (label injdef)

The proof of equivalence of the two predicates can be found in the Appendix.

\forall U.UNIQUENESS(U)=INJ(U)
(label uniqueness,injectivity)

Clearly the predicate uniqueness is more convenient, in a. proof by induction on lists. An example is the previous Lemma Fstposition,Nth: a. direct proof of

VU N.INJ(U)\& LENGTH U\& FSTPOSITION(U,NTH(U,N))=N

would be much longer.
2.11. The notions of Finite Union and Finite Sum.

We introduce functions that perform finite sums and finite unions, i.e. given $f : \mathbb{N} \rightarrow \mathbb{N}$, the operation

$$\sum_{m<n} f(m)$$

and given $F : \mathbb{N} \rightarrow A$, where $A$ is a collection of sets, the operation

$$\bigcup_{m<n} F(m).$$

The recursively defined predicates all and some can be used instead of the bounded quantifiers “for all $m < n, a(m)$” and “for some $m < n, a(m)$”. The proof of Pigeonfact shows an effective use of all.

(proof sums>

1. (decl allnum (type: constant))
   (syntype: constant))
2. (decl somenum (type: constant))
   (syntype: constant))
3. (decl (numseq $f$) (type: constant))
4. (decl sum (type: constant))
   (syntype: constant))
5. (decl setseq (type: constant))
6. (decl un (type: constant))
   (syntype: constant))

; axiom for allnum
7. (defax allnum $\forall n a. allnum(0,a) \land (allnum(n',a) \land a(n) \land allnum(n,a))$)
   (label allnumdef)

; axiom for somenum
8. (defax somenum $\forall n a. \sim somenum(0,a) \land (somenum(n',a) \land a(n) \land somenum(n,a))$)
   (label somenumdef)

9. (defax sum
   $\forall n \text{numseq}. \text{sum}(\text{numseq},0) = 0 \land$
   $\text{sum}(\text{numseq},n') = \text{sum}(\text{numseq},n) + \text{numseq}(n))$
   (label sumdef)

10. (defax un
    $\forall n \text{setseq}. \text{un}(\text{setseq},0) = \emptyset \land$
    $\text{un}(\text{setseq},n') = \text{un}(\text{setseq},n) \cup \text{setseq}(n))$
    (label undef)

Finally we have a recursive predicate to identify finite sequences of disjoint sets. 
9. (decl disj.pair (type: ![set→truthval]))
10. (define disj.pair ![forall a b.disj_pair(a,b)=emptyp(a∩b)])
   (label disj.pair,def)

11. (decl disjoint (type: ![ground→ground→truthval]))
12. (defax disjoint ![forall setseq.
      disjoint(setseq,0)=disj.pair(un(setseq,n),setseq(n)))
   (label disjoint,def)

The following line gives the condition for sum to be defined:

:sumsort
3. (ue (a ![∀n.allnum(n,∀m.natnum numseq(m))natnum sum(numseq,n)])
   proof-by-induction (open allnum sum))
   ![∀n.(∀M<Nh:natnum(numseq(M)))natnum(sum(numseq,N)))
   (label sumsort)

2.12. The notion of Multiplicity.

The function mult counts the number of members in a list u that satisfy the predicate a.

(proof multiplicity)
1. (decl mult (type: ![ground→ground]))
2. (defax mult ![forall x u.a.mult(nil,a)=0∧
      mult(x.u,a)=if a(x) then mult(u,a) else mult(u,a)])
   (label mult,def)

The following fact about multiplicity is easy to prove.

3. (ue (phi ![∀u.∀a.natnum(mult(u,a)])] listinduction
   (use mult,def mode: always))
   (label simpinfo) (label multfact)

Lemma 2.8. (Length Mult)

VU a.MULT(U,A)≤LENGTH U

Proof. There are two cases in the inductive step. If x does not satisfy a then

mult(x.u,a)=mult(u,a)≤length(x.u)

follows from the definitions and the induction hypothesis.
Otherwise

\[ \text{mult}(x, u, a) \leq \text{length}(x, u) \]

follows from the definitions and the induction hypothesis (using \text{SUCCESSORLESSEQ}, which is in \text{simpinfo}).

\[
\begin{align*}
\text{; multiplicity is lesseq length} \\
\text{; labels: LESSEQ, LESSEQ, SUCC} \\
\forall n. n \leq m \\
\text{; labels: SIMPINFO, SUCCESSORFACTS, SUCCESSORLESSEQ} \\
\forall n. n' \leq m
\end{align*}
\]

4. (\text{ue (phi | } \forall u. \text{mult}(u, a) \leq \text{length}(u) | ) \text{ list induction} \\
\text{(open \text{mult length}) (use \text{lesseq_lesseq_succ})} \\
\text{(part 1 #1 (open lesseq))} \\
\forall u. \text{MULT}(u, a) \leq \text{LENGTH} U \\
\text{(label \text{length_sum})}

\textbf{Lemma 2.9. (Member Mult)}

\[ \forall U Y A. \text{MEMBER}(Y, U) \land A(Y) \land A(Y) \leq \text{MULT}(U, A) \]

\text{; if there is a member, multiplicity is not zero}

5. (\text{ue (phi | } \forall u. \forall y. \text{a.member}(y, u) \land A(y) \land A(y) \leq \text{mult}(u, a) | ) \text{ list induction} \\
\text{(open \text{mult member}) (use normal mode: always)} \\
\forall U Y A. \text{MEMBER}(Y, U) \land A(Y) \leq \text{MULT}(U, A)

6. (\text{rw * use \text{less-lesseqsucc mode: always})} \\
\forall U Y A. \text{MEMBER}(Y, U) \land A(Y) \leq \text{MULT}(U, A) \\
\text{(label \text{member_mult})}

\textbf{Lemma 2.10. (Mult Nthcdr)}

\[ \forall n. U. n < \text{LENGTH} U \land \text{MULT}(U, a) \leq \text{MULT}(U, a) \]

\text{Mult Nthcdr} is only slightly more difficult. Line 8 is needed to help the rewriter in line 9. The problem in line 9 is the following: we \textbf{want} to expand the definition of mult in the following argument for the induction step: if \( a(nth(u, n)) \), then

\[ \text{mult}(nthcdr(u, n), a) = \text{mult}(nth(u, n). nthcdr(u, n'), a) = \text{mult}(nthcdr(u, n'), a) \]

otherwise

\[ \text{mult}(nthcdr(u, n), a) = \text{mult}(nth(u, n). nthcdr(u, n'), a) = \text{mult}(nthcdr(u, n'), a) \]

But

\[ \text{mult}(nthcdr(u, n'), a) \leq \text{mult}(u, a) \]
implies, using the fact \( \text{Succ Lesseq Lesseq} \).

\[
\text{mult(nthcdr(u,n'),a) \leq mult(u,a)}
\]

Therefore, in both cases

\[
\text{mult(nthcdr(u,n),a) \leq mult(u,a)}
\]

implies

\[
\text{mult(nthcdr(u,n'),a) \leq mult(u,a)}.
\]

This involves a combination of rewriting and logical reasoning: the definition of \( \text{mult} \) is expanded into a \textit{if} \ldots \textit{then} \ldots \textit{else} form and the instance of \( \text{Succ Lesseq Lesseq} \) is an implication. We help \text{EKL} by giving the logical step described above as a separate rewriter (line 8) using \( \text{Trans Cond} \).

8. \texttt{(ue ((q.|mult(nthcdr(u,n'),a),mult(u,a)) (r.|mult(nthcdr(u,n'),a),mult(u,a)) (p.|a(nth(u,n)))) trans,cond (use succ_lesseq_lesseq ue: ((m.|mult(nthcdr(u,n'),a),mult(u,a))) (n.|mult(u,a))) mode: exact )) ;IF A(NTH(U,N)) THEN MULT(NTHCDR(U,N'),A) \leq MULT(U,A) ;ELSIF MULT(NTHCDR(U,N'),A) \leq MULT(U,A)) ;MULT(NTHCDR(U,N'),A) \leq MULT(U,A) ;\texttt{;conclusion}

9. \texttt{(ue (a |\lambda a u.n<length(u)\text{mult(nthcdr(u,n),a)\leq mult(u,a)}) proof-by-induction (part 1#1 (open lesseq)) succ,less-less (part 1#2#1#1 (use nthcdr,car,cdr mode: always)) (open mult) *) ;\forall A U.N<LENGTH U\text{MULT(NTHCDR(U,N),A)\leq MULT(U,A)} (label mult_nthcdr) ■}

\texttt{;mult emptyset}

\texttt{(ue (phi \mid a.u.multip(u,emptyset)=0) listinduction (part 1 (open emptyset mult))) ;\forall U.MULT(U,EMPTYSET)=0 (label simpinfo) (label emptyfacts) ■}
2.12.1. **Multiplicity Implies Injectivity.**

The following Lemma embodies the main use of the notion of multiplicity. If the number of occurrences of every member of a list \( v \) is 1, then the list has the **injectivity** property: for \( i, j < \text{length}(v) \).

\[
\text{nth}(v, i) = \text{nth}(v, j) \Rightarrow i = j.
\]

We use the following fact: if \( \text{nth}(v, i) = \text{nth}(v, j) \) and \( i < j \), then the multiplicity of the set \( \text{mkset}(\text{nth}(v, i)) \) is at least 2.

\[
\forall v \forall i, j \ (i < j \land \text{length}(v) > 0 \land \text{nth}(v, i) = \text{nth}(v, j)) \Rightarrow 2 \leq \text{mult}(v, \text{mkset}(\text{nth}(v, i)))
\]

The proof of **Multinj Computation**, a consequence of the lemmata, **Nth in Nthdr** and **Member Mult**, is left to the Appendix.

**Lemma 2.11.** (**Mult Inj**)

\[
\forall v \forall k \ (\text{length}(v) \leq \text{length}(v) \land \text{mult}(v, \text{mkset}(\text{nth}(v, k))) = 1) \Rightarrow \text{INJ}(v)
\]

**Proof.** At lines 3 and 4 we instantiate **Multinj Computation** and we use line 1 to derive that if \( i < j \) or \( j < i \), then \( 2 \leq 1 \). Now we exploit semantic attachment: EKL knows that \( 2 < 1 \) and \( 2 = 1 \) are false. An application of the trichotomy concludes the proof.

1. (assume \( \forall k \ (\text{length}(v) \leq \text{length}(v) \land \text{mult}(v, \text{mkset}(\text{nth}(v, k))) = 1) \))
   (label mil)

2. (assume \( i \leq \text{length}(v) \land j \leq \text{length}(v) \land \text{nth}(v, i) = \text{nth}(v, j) \))
   (label mi2)

3. (use \( ((v, v)(i, i)(j, j)) \) multinj-computation mi2
   (use mil ue: \( ((k, i)) \) mode: exact) (open leqseq))
   \( i < j \)
   ;deps: (MI1 MI2)

4. (use \( ((v, v)(i, j)(j, i)) \) multinj-computation mi2
   (use mil ue: \( ((k, j)) \) mode: exact) (open leqseq))
   \( j < i \)
   ;deps: (MI1 MI2)

5. (derive \( i = j \) (trichotomy \( * -2) \))
   ;deps: (MI1 MI2)

6. (ci mi2)
   \( i \leq \text{length}(v) \land j \leq \text{length}(v) \land \text{nth}(v, i) = \text{nth}(v, j) \land i = j \)
   ;deps: (MI1)

7. (trw linj v) (open inj \( * \))
   \( \text{INJ}(v) \)
   ;deps: (MI1)
8. (ci mil)
   \( \forall K. K < \text{LENGTH} \forall V. \text{MULT}(V, \text{MKSET}(\text{NTH}(V, K))) = 1 \) \( \Rightarrow \text{INJ}(V) \)
   (label mult_inj)

2.12.2. The Multiplicity of a Disjoint Union is the Sum of Multiplicities.

Consider a list and two sets (say, the sets of occurrences of two different S-expressions in the list). If the sets are disjoint, then the sum of multiplicities is the multiplicity of the union (Lemma. Multsum). Lemma Multsum generalizes to any finite sequence of disjoint sets (Lemma. Mult of Un is Sum Mult).

**Lemma 2.12. (Multsum)**

\( \forall U. \text{DISJ_PAIR}(A, B) \Rightarrow \text{MULT}(U, A \cup B) = \text{MULT}(U, A) + \text{MULT}(U, B) \)

**Proof:** By induction on \( u \). For \( u = \text{NIL} \), all values of mult are 0. Assume the result for \( u \). The assumption that \( a \) and \( b \) are a disjoint pair of sets means that the intersection of \( a \) and \( b \) is empty. If not \( x \in a \) and not \( x \in b \), then induction hypothesis gives the result. If either \( x \in a \) or \( x \in b \), then

\[
\text{mult}(x. u, a \cup b) = \text{mult}(u, a \cup b) = (\text{mult}(u, a) + \text{mult}(u, b)) = \text{mult}(x. u, a) + \text{mult}(x. u, b)
\]

- the induction hypothesis is used to establish the second equality.

The mechanical proof is one line long:

1. (ue (phi lambda u. disj_pair(a,b) mult(u,aub)=mult(u,a)+mult(u,b)) I)
   listinduction
   (part 1 (open mult union disj_pair emptyp intersection)
   (use normal mode: always))
   (part 1 (der))
   (label multsum)

The lemma, Multsum is used in the induction step in the proof of the next fact:

**Lemma 2.13. (Mult of Un is Sum Mult)** If all the sets of the sequence setseq are pairwise disjoint, then

\[
\text{mult}(u, \bigcup_{m<n} \text{setseq}(m)) = \sum_{m<n} \text{mult}(u, \text{setseq}(m)) \ :
\]

\[
\forall \text{SETSEQ U} \text{DISJOINT(SETSEQ,N)} \Rightarrow \\
\text{MULT}(U, \text{UN(SETSEQ,N)}) = \text{SUM}(\lambda X1. \text{MULT}(U, \text{SETSEQ}(X1)), N)
\]

**Proof:** By induction on \( n \). For \( n = 0 \),

\[
\bigcup_{m<0} \text{setseq}(m)
\]
is the empty set, whose multiplicity is 0 (by 'simpinfo'). and
\[
\sum_{m<0} \text{mult}(u, \text{setseq}(m))
\]
is 0 too.

Assume the result for 12. Now

\[
\text{disjoint(setseq, n')}
\]
implies

\[
\text{disjpair(un(setseq,n),setseq(n))};
\]
this implies, using MULTSUM

\[
\text{mult}(u, \bigcup_{m<n'} \text{setseq}(m)) = \text{mult}(u, \bigcup_{m<n} \text{setseq}(m)) + \text{mult}(u, \text{setseq}(n)),
\]
which is, by definition of un and induction hypothesis

\[
= \sum_{m<n} \text{mult}(u, \text{setseq}(m)) + \text{mult}(u, \text{setseq}(n)) = \sum_{m<n+1} \text{mult}(u, \text{setseq}(m)).
\]

Here the mechanical proof is again one line long!

(proof mult_of_un_is_sum_mult)

1. (ue ( a \forall n. \text{disjoint(setseq,n)})
\[
\text{mult}(u, \text{un(setseq,n)})=\text{sum}(\lambda x1. \text{mult}(u, \text{setseq}(x1)), n))
\]
   proof-by-induction
   (open disjoint un sum mult ) multfact
   (use multsum mode: exact) (use normal mode: always))
   ;\forall N. \text{DISJOINT(SETSEQ,N)}
\[
;\text{MULT}(U, \text{UN(SETSEQ,N)})=\text{SUM}(\lambda X1. \text{MULT}(U, \text{SETSEQ}(X1)), N)
\]
   (label mult_of_un_is_sum_mult) ■
3. **Notions of Application.**

We give the basic facts about application, injection and permutation using two representations for finite functions: functions as association lists and functions as lists of numbers.

3.1. **Function Application using Association Lists.**

Our first approach uses association lists. We recall the recursive definition of \( \text{alist} \) (see the Appendix) and present the main definitions (see also the Introduction 1.5.2).

55. \( \text{decl} \ (\text{alist}) \ (\text{type: ground}) \ (\text{sort: listp}) \)
56. \( \text{axiom} \ [\text{alist} \ . \ listp \ \text{alist}] \)

57. \( \text{axiom} \ [\forall u. \ \text{alist} \ u \equiv (\neg \ \text{null} \ u \ \land \ \neg \ \text{atom} \ \text{car} \ u \ \land \ \text{atom} \ \text{car} \ (\text{car} \ u)) \land \ \text{alistp} (\text{cdr} \ u)] \)

58. \( \text{axiom} \ [\forall x, y. \ \text{alist} \ . \ \text{alistp} \ \text{nil} \ \land \ \text{alistp} (x, y) \ . \ \text{alist} \ \]

1. \( \text{decl} \ \text{dom} \ (\text{type: GROUND + GROUND}) \)
2. \( \text{defax} \ \text{dom} \ [\forall x, y. \ \text{alist} \ . \ \text{dom} \ \text{nil} \ \land \ \text{dom} (x, y, \text{alist}) = x. \ \text{dom} \ \text{alist}] \)

3. \( \text{decl} \ \text{range} \ (\text{type: GROUND + GROUND}) \)
4. \( \text{defax} \ \text{range} \ [\forall x, y. \ \text{alist} \ . \ \text{range} \ \text{nil} \ \land \ \text{range} (x, y, \text{alist}) = y. \ \text{range} \ \text{alist}] \)

5. \( \text{decl} \ \text{functp} \ (\text{type: GROUND + TRUTHVAL}) \)
6. \( \text{define} \ \text{functp} \ [\forall x, y. \ \text{alist} \ . \ \text{functp} (\text{alist}) \ \land \ \text{uniqueness} \ \text{dom} (\text{alist})] \)

7. \( \text{decl} \ \text{injunctp} \ (\text{type: GROUND + TRUTHVAL}) \)
8. \( \text{define} \ \text{injunctp} \ [\forall x, y. \ \text{alist} \ . \ \text{injunctp} (\text{alist}) \ \land \ \text{uniqueness} \ \text{range} (\text{alist})] \)

9. \( \text{decl} \ \text{appalist} \ (\text{type: GROUND + GROUND}) \)
10. \( \text{define} \ \text{appalist} \ [\forall x, y. \ \text{appalist} (y, \text{alist}) = \text{cdr} \ \text{assoc} (y, \text{alist})] \)

Let \( \text{alist}_f \) represent the function \( f \). As noticed above, \( \text{dom} (\text{alist}_f) \) and \( \text{range} (\text{alist}_f) \) do not give the domain and the range of \( f \); rather they list the domain and the range of the function in the ordering given by the association list \( \text{alist}_f \). To abstract from such ordering we use the
functional \texttt{mklset}. (Given a list \texttt{u}, \texttt{mklset (u)} is the set of members of \texttt{u}-identified, as usual, with the predicate \(\lambda x. \text{member}(x,u)\)).

As we pointed out in the introduction, the same function can be represented by several association lists, in fact by the equivalence class of association lists. The predicate \texttt{samemap} is the appropriate equivalence relation: two association lists \texttt{alist1} and \texttt{alist2} represent the same map if

(i) they are 'defined' on the same set, i.e. their domains are the same as sets, and
(ii) for all \(y\), \texttt{appalist (y,alist1) = appalist (y,alist2)}, i.e. if they 'map' the same elements into the same elements.

Both conditions are needed: \texttt{appalist (y,alist)} may be \texttt{NIL} either because the pair \((y,\text{NIL})\) belongs to \texttt{alist} or because \(y\) does not belong to \texttt{dom(alist)}; we do not want to identify the two cases.

11. \texttt{(decl (samemap) \{type: [ground@ground+truthval]\})}
12. \texttt{(define samemap}
   \texttt{(define samemap}
   \texttt{\{\forall \texttt{alist \texttt{alist1}}. samemap(alist,alist1)=}
   \texttt{mklset \texttt{dom(alist)=mklset \texttt{dom(alist1)\}}}
   \texttt{(\forall y.y\in mklset \texttt{dom(alist)}}
   \texttt{\texttt{\}}
   \texttt{\texttt{appalist(y,alist)=appalist(y,alist1)\})})

13. \texttt{(define permutp \{\forall \texttt{alist. permutp(alist)=}
   \texttt{\texttt{functp(alist)\}}}mklset(\texttt{dom(alist))=mklset(\texttt{range(alist)))\})}

14. \texttt{(axiom \{\forall \texttt{chi.chi(nil)\}(\forall x y \texttt{alist.chi(alist)\}\}\texttt{chi((xa.y).alist)))\}}

\texttt{(label \texttt{alistinduction})}

\texttt{Alist Induction} is easily derivable from \texttt{Listinduction} (see the Appendix).

The following facts are very easy to prove:

\texttt{(proof \texttt{alistfacts})}

\texttt{\{\texttt{domsort}\}}

1. \texttt{(ue \texttt{(chi \{\lambda \texttt{alist.listp \texttt{dom(alist)}}\}) \texttt{alistinduction (open \texttt{dom})})\}\
   \texttt{\{\texttt{VALIST.LISTP \texttt{DOM(ALIST)}}\}}
\texttt{(label \texttt{domsort}) (label simpinfo)}

\texttt{\{\texttt{rangesort}\}}

2. \texttt{(ue \texttt{(chi \{\lambda \texttt{alist.listp \texttt{range(alist)}}\}) \texttt{alistinduction (open \texttt{range})})\}\
   \texttt{\{\texttt{VALIST.LISTP RANGE(ALIST)}}
\texttt{(label \texttt{rangesort}) (label simpinfo)}

\texttt{\{\texttt{domlength}\}}

3. \texttt{(ue \texttt{(chi \{\lambda \texttt{alist.length \texttt{dom \texttt{alist=\texttt{length \texttt{alist}}}}\}) \texttt{alistinduction (open \texttt{dom})})\}}
;VALIST.LENGTH (DOM(ALIST))=LENGTH ALIST
  (label domlength)

;domrangelength

4. (ue (chi |alist.length(dom alist)=length(range alist)|)
   alistinduction
   (open dom range))
;VALIST.LENGTH (DOM(ALIST))=LENGTH (RANGE(ALIST))
  (label domrangelength)

;appalistsort

5. (ue (chi |alist.SEXP APPALIST(Y,ALIST)|)
   alistinduction
   (part 1 (open appalistsort assoc)))
;VALIST.SEXP APPALIST(Y,ALIST)
  (label appalistsort)(label simpinfo)

;trivial appalistsort

6. (ue (chi |alist.¬(y∈mklist dom(alist))¬appalist(y,alist)=nil|)
   alistinduction
   (part 1 (open epsilon mklist dom appalistsort assoc member)))
;VALIST.¬y∈MKLIST(DOM(ALIST))¬APPALIST(Y,ALIST)=NIL
  (label trivial, appalistsort)

samemap is an equivalence relation:

7. (trw |samemap(alist,alist)| (open samemap))
   (label samemap_equivalence)

8. (trw |samemap(alist,alist1)¬samemap(alist1,alist)|
    (open samemap mklist dom))
   ;SAMEMAP(ALIST,ALIST1)¬SAMEMAP(ALIST1,ALIST)
   (label samemap, equivalence)

9. (trw |samemap(alist,alist1)¬samemap(alist1,alist2)|
    samemap(alist,alist2)|
    (open samemap mklist dom))
   ;SAMEMAP(ALIST,ALIST1)¬SAMEMAP(ALIST1,ALIST2)¬SAMEMAP(ALIST,ALIST2)
   (label samemap_equivalence)

The restriction to elements of the domain in the definition of appalistsort is not necessary:
appalistsort has a default value, as shown in the line Trivial Appalistsort. The easy proof of equivalence
is in the Appendix.

10. ∀ALIST1 ALIST2.SAMEMAP(ALIST1,ALIST2)=
    (MKLIST(DOM(ALIST1))=MKLIST(DOM(ALIST2))∧
    (∀X.APPALIST(X,ALIST1)=APPALIST(X,ALIST2))))
    (label samemap,defl)
3.2. Function Application using Lists of Numbers.

Our second representation of functions uses lists of numbers.

; definition of application

(proof appl)

1. (define appl |∀u i.appl(u,i)=nth(u,i) |)
   (label appldef)
   ; predicates for functions

2. (decl (into) (type: |ground+truthval|))
3. (define into |∀u.into(u)=(∀n.n<length u)natnum nth(u,n)<length u|)
   (label intodef)

4. (decl (onto) (type: |ground+truthval|))
5. (define onto |∀u.onto(u)=(into(u)∧(∀n.n<length u)member(n,u))|)
   (label ontodef)

6. (decl (perm) (type: |ground+truthval|))
7. (define perm |∀u.perm(u)=onto(u) |)
   (label permdef)

Extensionality is proved using Doubleinduction. To do the inductive step, we instantiate twice the assumption of line 3, by replacing i first with 0 (line 4) and then with i' (line 5).

(proof extensionality)

(show doubleinduction)

; labels: DOUBLEINDUCTION
; ∀PHI2.(∀U V X Y.PHI2(NIL,U)∧PHI2(U,NIL)∧(PHI2(U,V)→PHI2(X.U,Y.V)))

; first attempt:
0. (ue (phi2 |λu v.length u=length ∀A

   (∀i.i<length u)nth(u,i)=nth(v,i))∪u=v|)
   doubleinduction (open nth)
   (VU V X Y.(LENGTH U=LENGTH ∀A
   (∀i.i<LENGTH V)nth(U,i)=nth(V,i))∪U=V)\)
   (LENGTH U=LENGTH ∀A
   (∀i.i<LENGTH V)nth(X.U,i)=nth(Y.V,i))∪X.U=Y.V)\)
   (VUV.LENGTHU=LENGTHV∀(∀i.i<LENGTHV)nth(U,i)=nth(V,i))∪U=V)

1. (assume |LENGTH U=LENGTH ∀A(∀i.i<LENGTH V)nth(U,i)=nth(V,i))∪U=V|)
   (label extl)

2. (assume |LENGTH U=LENGTH V|)
   (label ext2)

3. (assume |∀i.i<LENGTH V)nth(X.U,i)=nth(Y.V,i)|)
(label ext3)

4. (ue (i 0) * ext2)
   ;X=Y
   (label ext4)
   ;deps: (EXT2 EXT3)

5. (ue (i |i'|) ext3 ext2)
   ;I<LENGTH V<\text{NTH}(U,I)=\text{NTH}(V,I)
   (label ext5)
   ;deps: (EXT2 EXT3)

6. (derive |u=v| (ext1 ext2 ext5))
   (label ext6)
   ;deps: (EXT1 EXT2 EXT3)

7. (trw |x.u=y.v| (use ext4 ext6 mode: exact))
   ;X.U=Y.V
   ;deps: (EXT1 EXT2 EXT3)

8. (ci (ext2 ext3))
   ;LENGTHU=LENGTHV\forall I<LENGTHU'\forall I<LENGTHV.X(U,I)=Y(V,I))X.U=Y.V
   ;deps: (EXT1)

9. (ci ext1)
   ;(LENGTHU=LENGTHV\forall I<LENGTHU'\forall I<LENGTHV.X(U,I)=Y(V,I))X.U=Y.V
   ;(LENGTHU=LENGTHV\forall I<LENGTHU'\forall I<LENGTHV.X(U,I)=Y(V,I))X.U=Y.V

10. (ue (phi2 |u v.length u=length v\forall
    (\forall i<length u\forall nth(u,i)=nth(v,i))u=v|)
    doubleinduction (open nth) *)
    ;\forall U.V.LENGTHU=LENGTHV\forall I<LENGTHU'\forall I<LENGTHV.X(U,I)=Y(V,I))X.U=Y.V
    (label extensionality)

11. (trw |\forall u.i<length u \forall sexp(appl(u,i))\forall member(appl(u,i),u)|
    (open appl) nthmember)
    ;\forall U.I<LENGTH U\forall SEXP APPL(U,I)\forall MEMBER(APPL(U,I),U)
    (label simpinfo) (label applfacts)
2.13. **Conclusion of Part I.**

It may be appropriate to conclude the first part by some remarks and guidelines for the heuristics of particular proofs of EKL. In the second part we will make some suggestions how to choose among mathematical representations and linguistic variants, how to organize the proofs, how to break them into lemmata and how to improve the efficiency of proofs.

How should a user proceed?

1. First, we must make sure that we understand the mathematical notions and have a proof strategy that works on paper. In particular:
   - If a proof by induction is needed, EKL will not give hints on the form of induction.
   - Even if the result follows by expanding the definitions and making appropriate substitutions, we cannot expect the rewriting process to find the right substitutions by itself.

   As a proof checker, EKL is not designed to cope with the danger of combinatorial explosion. EKL commands give the user many ways to control and direct the rewriting process according to her (his) proof strategy.

2. Two methods are available in searching for a proof.
   - Search by trial and error. Try to obtain a proof in a single line. If this does not succeed, use the output of EKL to establish what other information is needed and try again.
   - Expand the proof, using explicitly the logic decision procedure in the style of Natural Deduction. This is safer, but time consuming.

3. Suppose that, according to the first alternative, we ask EKL to rewrite a certain formula \( A \) to true (or a certain term \( t \) to \( t' \)) and EKL gives instead some error message or returns \( A \equiv B \) (of \( t \equiv u \)). The output of EKL and the form of \( B \) (or of \( u \)) always give useful information. Rewriting may fail because
   - Type conditions are not satisfied. In this case EKL will return an error message. There may be a parsing error. Or we need to modify some definition. Otherwise, we tried to prove something that cannot be expressed by EKL.

\[
\text{(proof foo)}
\]

\[
\text{(trw \{p\Rightarrow p\})}
\]

; \( P \) is unknown.
; type-check: 3
; does not apply in \( \text{P}\Rightarrow \text{P} \)

; it currently has type \( (\text{TRUTHVAL}\Rightarrow \text{TRUTHVAL})\Rightarrow \text{TRUTHVAL} \)

\[
\text{(trw \{f(f)\})}
\]

; \( \text{FOO} \) started.
1. ; \( F \) is unknown.
   ; type-check: \( F \)
   ; does not apply in \( F(F) \)
   ; it currently has type \( \text{GROUND}\Rightarrow \text{GROUND} \)
(ii) Sort conditions are not satisfied. If something totally obvious didn’t work, this may be the reason. A sorted language is more flexible, but some information is left implicit. To check sorts is of course an essential step: it amounts to check that a term has the intended meaning or that a function is defined for the given argument.

(proof f 00)

1. (decl (m n) (type: ground) (sort: natnum))
2. (decl plus (type: [ground*ground*+ground])
   (infixname: [+]) (bindingpower: 930))

3. (decl (f) (type: [ground+ground]))
4. (define f [\forall n.f(n)=1])

5. (decl (g) (type: [ground+ground]))
6. (define g [\forall n.g(n)=n])
7. (trw If (f (n)+1) I (open f))
   ;F(F(N)+1)=1
8. (trw [f(g(n)+1)] (open f g))
   ;F(G(N)+1)=F(N+1)

What’s wrong here? Of course we have forgotten the information that n+1 is of the sort natnum, so iii line 8 the rewriting cannot continue. As soon as this information is available, the rewriting is completed (line 10).

9. (axiom [\forall n.natnum(n+1)])
   (label simpinfo)
10. (trw [f(g(n)+1)] (open f g))
    ;F(G(N)+1)=F(N+1)

One may wonder why the rewriter was successful in line 7. Although we have not defined plus, by semantic attachment 1+1 has its intended meaning and natnum(2) is true.

(setq rewritermessages t)

7. (trw [f(f (n)+1)] (open f))
   ;the term F(N) is replaced by:
   1
   ;the term 1+1 is replaced by:
   2
   ;the term F(2) is replaced by:
   1
   ;F(F(N)+1)=1

(iii) There are conditions on the rewriting that are not satisfied. Often the conditions are satisfied, but cannot be verified directly by EKL decision procedure and we need to construct an additional rewriter. (See Example 5.)

(iv) The use of a line is blocked, because we are rewriting in mode: exact. In this case we may try the same rewriting in mode: always. If the rewriter mode: always causes an infiniteloop, then expanding the proof may be our only choice.
(v) The expression produced by the rewriting is not simpler, and we are rewriting in the default mode. For instance, at line 12 the line is not applied when rewriting in default mode, since the expression \( g(g(n)) \) resulting from its application would be more complex than \( f(x) \). Here it is enough to specify the mode of the rewriting (line 13).

11. (assume \( f(x) = g(g(n)) \))
   (label line)

12. (trw \( f(x) \) line (open \( g \))
    ; F(X) = F(X)
    ; deps : (LINE)

13. (trw \( f(x) \) (use line mode: exact)(open \( g \))
    ; F(X) = N
    ; deps: (LINE)

(vi) The line is not applicable, because of a conflict of context.

14. (define \( g \) \( \forall x. g(x) = f(x) \))
   (label gdef)

15. (trw \( g(x) \) (open \( g \) line)
    ; context of line GDEF cannot be adjoined: the atom G in line GDEF has two definitions: one from line 6 and the other from GDEF

4. The following is a nontrivial example, in which there is additional logical structure to be considered in rewriting. We consider the proof of Lemma 2.10 \( \text{Mult\ Nthcdr} \). Section 2.12. Here the rewriting line is found by interaction with EKL, and from this rather involved expression a general propositional schema is abstracted, to be used in similar contexts.

Example 5.

\[
\forall n \, A \, u \, n < \text{LENGTH} \, u \, \text{MULT}(\text{NTHCDR}(u, n), A) \preceq \text{MULT}(u, A)
\]

This is a statement about the sublists of a given list \( u \) formulated in terms of the function \( \text{nthcdr} \). It may be convenient to use a proof by induction on \( n \). In the base case, since \( \text{nthcdr}(u, 0) \) is \( u \), EKL has to know only what \( \text{nthcdr} \) and \( \preceq \) mean. It is enough, therefore, to say (open \( \text{lesseq} \)) in the part of the induction axiom corresponding to the base case (the definition of \( \text{nthcdr} \) is in \( \text{simpinfo} \)). To do the induction step one can formalize the informal argument given in the test. Assuming

\[
n < \text{LENGTH} \, u \, \text{MULT}(\text{NTHCDR}(u, n), a) \preceq \text{MULT}(u, a)
\]

and deriving

\[
n' < \text{LENGTH} \, u \, \text{MULT}(\text{NTHCDR}(u, n'), a) \preceq \text{MULT}(u, a)
\]

To avoid an explicit proof, we notice that we can easily induce EKL to rewrite the inductive step as

\[
(\forall n' \, \text{LENGTH} \, u \, \text{MULT}(\text{NTH}(u, n''), \text{NTHCDR}(u, n'), A) \preceq \text{MULT}(u, A))
\]
Then \texttt{mult} is expanded and the conditional clause is pushed out; hence the same line rewrites to

\[(N \text{ LENGTH } U)
\begin{align*}
\text{IF } & A(\text{NTH}(U, N)) \\
\text{THEN} & \text{MULT} (\text{NTHCDR}(U, N'), A) \leq \text{MULT} (U, A) \\
\text{ELSE} & \text{MULT} (\text{NTHCDR}(U, N'), A) \leq \text{MULT} (U, A))
\end{align*}
\]

This is not very perspicuous. The key point is to realize that the structure of the logical argument can be summarized in the formula \textit{Trans Cond}:

\[
\forall P \in Q. (\forall R. \text{A}(\text{IF } P \text{ THEN } Q \text{ ELSE } R)) \forall R,
\]

where \(Q\) is

\[
\text{mult}(\text{nthcdr}(u, n'), a) \leq \text{mult}(u, a),
\]

where \(R\) is

\[
\text{mult}(\text{nthcdr}(u, n'), a) \leq \text{mult}(u, a),
\]

and \(P\) is

\[
a(\text{nth}(u, n)).
\]

Clearly \(QR\) follows from elementary arithmetic (fact \textit{Succ Lessq Less}). To do the inductive argument in one step we need only prepare one rewriter (line 8 in the test.):

\[
\text{IF } A(\text{NTH}(U, N))
\begin{align*}
\text{THEN} & \text{MULT} (\text{NTHCDR}(U, N'), A) \leq \text{MULT} (U, A) \\
\text{ELSE} & \text{MULT} (\text{NTHCDR}(U, N'), A) \leq \text{MULT} (U, A))
\end{align*}
\]

and use the following fact of elementary arithmetic (\textit{Succ Less Less}):

\[
N' \text{ LENGTH } U \leq N \text{ LENGTH } U
\]

The simplification of this proof is certainly worth the effort. Indeed the argument used here is quite common in proofs about recursively defined objects. There is a good chance that the rewriter \textit{Trans Cond} may be applied in similar cases.

5. Finally it may be the case that, despite our attempts, we cannot find by trial and error the appropriate rewriter. Then we expand our proof in a 'Natural Deduction style': e.g. in a proof by induction we try to prove the base case, we assume the induction hypothesis and try to prove the conclusion of the inductive step. If the latter is in turn an implication, we assume the antecedent etc. In the process, we may expand definitions, perform substitutions, etc. Moreover, we may need to prove other lemmata also by induction. The process is not easily described in general terms, since there is no general analysis of higher order inductive proofs in Natural Deduction, as we remarked earlier. In practice it is quite clear what to do, although several options may be open, especially when we are engaged in a proof by contradiction.

6. Once the derivation is found we may try to collapse it in few steps. For example, it may be clear which formulas could be taken as rewriters.

In trying to replace logical deduction by rewriting, we find some steps harder to handle than others.
(i) A line resulting from the cases command, i.e. the conclusion of a proof by cases, corresponds to rewriting a disjunction in the antecedent of an implication. This can be handled by using the rewriter NORMAL as explained in Example 1.

(ii) Argument by contradiction and steps involving negation may require some help. For instance, although EKL can easily derive $\neg B \supset \neg A$ from $A \supset B$, it may not do this step in the contest of conditional rewriting.

(iii) Quantifiers may require additional lines, in particular the existential one. If the result involves a bound quantifier, it may be convenient to replace it by a recursively defined predicate. For instance

$$\forall m. m < n \exists A(m), \quad \exists m. m < n \forall A(m), \quad \forall x. \text{member}(x, u) \exists A(x), \quad \exists x. \text{member}(x, u) \forall A(x).$$

are equivalent to the recursive predicates

$$\text{allnum}(n, \lambda m. A(m)), \quad \text{somenum}(n, \lambda m. A(m)), \quad \text{allp}(\lambda x. A(x), u), \quad \text{somep}(\lambda x. A(x), u).$$

In the contest of inductive proofs, it is convenient to formulate the result by using the recursive predicate and prove this formula first. This method is presented in Examples 6 and 7.

The proof of $\text{Fstposition} \ Nth$, already examined in Example 4, Section 2.9, is an instance of the process of collapsing a long proof in few lines. First of all, in later applications we use

$$(\ast)\quad VU \ N. \text{INJ}(U) \land \langle \text{LENGTH} U \supset \text{FSTPOSITION}(U, \text{NTH}(U, N)) = N$$

rather than

$$(\ast\ast)\quad VU \ N. \text{UNIQUENESS}(U) \land \langle \text{LENGTH} U \supset \text{FSTPOSITION}(U, \text{NTH}(U, N)) = N$$

and we may be tempted to prove directly $(\ast)$, inj and uniqueness are equivalent predicates, but the latter is a recursively defined predicate, whereas the former has an explicit definition using quantifiers. In the spirit of our suggestion (iii), we should try a proof of $(\ast\ast)$ and indeed we find one four lines long. Moreover, notice that we derive line 3 of the proof from line 2, to allow the use of $\neg x = \text{nth}(u, n)$, a negative formula, in rewriting. This is in accordance to our suggestion (ii).

Looking at the proof, it is completely clear that line 3 will do the job, by considering its effects of the rewriting of line 3. But the form of 3 or the possibility of proving it in two steps may not have occurred to us at first sight, before a more detailed proof.

In conclusion, one learns to control the rewriting process of EKL by trial and error: it may be necessary first to write some explicit proofs in order to understand with total clarity the single step of rewriting. Then one may succeed in collapsing the proof into a single step, using a suitable line to reduce logical inferences to steps of rewriting. Several proofs in this paper were obtained in this way and some more may be reduced to a few lines with some additional effort. To make the proofs shorter doesn't mean to make them clearer. As in informal mathematical presentations, a balance has to be found between the necessity of formal precision and the need for clarity. One has to admit, however, that at the present stage it is premature to worry about mechanical proofs being too concise.
PART 2
4. **The Pigeon Hole Principle.**

In this section we prove the Pigeon Hole principle in second order arithmetic and apply it to show that every finite surjection is an injection, in our two representations.

4.1. **The Pigeon Hole Principle in Second Order Arithmetic.**

**Theorem. *(Pigeonfact)*

\[
\forall F. (\forall N. \text{NATNUM}(F(N))) \implies \\
(\forall M. M < N \implies F(M) = 1)
\]

We give two versions of the proof. In the former we prove directly

\[
\forall N. (\forall M. M < N \implies F(M) = 1) \implies \text{SUM}(\lambda K. F(K), N) = N \land (\forall M. M < N \implies F(M) = 1);
\]

the presence of quantifiers requires a proof in the style of Natural Deduction.

In the latter we assume \( \forall N. \text{NATNUM}(F(N)) \) and we prove

\[
\forall N. \text{ALLNUM}(N, \lambda K. 1 \leq F(K)) \implies (\forall M. M < N \implies F(M) = 1);
\]

the use of the recursively defined predicate \( \text{allnum} \) allows a straightforward proof by induction.

**First Proof.** We need a preliminary fact: if \( f \) is defined and has positive values on \( 0, \ldots, n-1 \), then the function

\[
\sum_{m<n} f(m)
\]

is strictly increasing. The proof is a straightforward induction, using in the induction step the lemma \( \text{Add Lesseq} \) (line 7).

1. (wipe-out)
2. (get-proofs sums)
3. (proof pigeonfact)
4. (assume \( (\forall m < n \text{natnum } f(m) A 1 \leq f(m)) \implies \text{sums}(\lambda k.f(k), n) \) )
   (label si_indh hyp)
5. (assume \( (\forall m < n \text{natnum } f(m) A 1 \leq f(m)) \) )
   (label si hyp)
6. (trw \( (\forall m < n \text{natnum } f(m) A 1 \leq f(m)) \) )
   (* transitivity-of-order successor1)
   (label si)
7. (ue ((numseq. |\( \lambda k.f(k) | \) ) (n. n)) sums sort *)
   (label si sort)
8. (NATNUM(SUM(\lambda K. F(K), N))
   (label si sort)
5. (derive \(\text{in} \sum (\lambda k.f(k), n) \mid (\text{si1}, \text{si}, \text{indhyp})\))
   (label \(\text{si1}\))

6. (ue (m n) \(\text{si}, \text{hyp} \text{ successor1}\))
   ; \(\text{NATNUM}(F(N)) \land \text{lessF}(N)\)
   (label \(\text{si3}\))
   ; \(\text{deps: (SI, HYP)}\)

We need Add Less eq:

\[
\begin{align*}
\text{labels: ADD, LESS EQ} \\
\forall M. \text{NatNum}(M) \land \text{lessEq}(M, M + K)
\end{align*}
\]

7. (ue ((n, n) \((k, f(n))\)) \(\text{m} \mid \text{sum}(\lambda k.f(k), n)\))
   \(\text{add, lesseq (sisort si2 si3)}\)
   ; \(\text{N' \leq \sum (\lambda k.f(k), N + F(N)}\)
   ; \(\text{deps: (SI, INDHYP, SI, HYP)}\)

8. \(\text{(ci si, hyp)}\)
   ; \(\forall M. \text{NatNum}(F(M)) \land \text{lessEq}(M, N') \leq \sum (\lambda k.f(k), N + F(N)}\)
   ; \(\text{deps: (SI, INDHYP)}\)

9. \(\text{(ci si, indhyp)}\)
   ; \(\forall M. \text{NatNum}(F(M)) \land \text{lessEq}(M, N') \leq \sum (\lambda k.f(k), N + F(N)}\)
   ; \(\forall M. \text{NatNum}(F(M)) \land \text{lessEq}(M, N') \leq \sum (\lambda k.f(k), N + F(N)}\)

10. (ue \((a \mid \text{n} (\forall m \text{NatNum} f(m) \land \text{lessEq}(m, N') \leq \sum (\lambda k.f(k), n))\))
    \(\text{proof-by-induction}\)
    \(\text{(open sum) zeroleast (use * mode: always))}\)
    ; \(\forall N. (\forall m \text{NatNum} F(M) \land \text{lessEq}(M, N) \land \text{sum}(\lambda k.f(k), N)}\)
    (label strictly-increasing)

Next we want to show that if the values of \(f\) are greater than or equal to 1 and, in addition, the value of
\[
\sum_{m=0}^{n-1} f(m)
\]
is bounded by \(n\), then the values of \(f\) must be equal to 1.

The proof is another simple induction, using in the induction step the lemma. Add One (line 19).

- ;use
  ; labels: ADD-ONE
  ; (AXIOM \(\forall X. N. M \cdot 1 \leq F \land N = M + K \land M \leq M \lor K \land N = M\))

We will replace \(f(n)\) for \(k\) and \(\sum (\lambda k.f(k), n)\) for \(m\). Lines 15, 17 and 18 are all the conditions in the antecedent of the Lemma to apply the lemma. At line 18 we use the first part Strictly Increasing.
Section 4

11. (assume (∀m. m < n) (∀ n ∈ natnum. f(m) ≤ f(m)) \( \sum\) (∀k. f(k), n) = \( \sum\) (∀m. m < n) f(m))
   (label pf indhyp)

12. (assume (∀m. m < n) (∀ n ∈ natnum. f(m) ≤ f(m))
   (label pf _assume)

13. (derive (∀m. m < n) (∀ n ∈ natnum. f(m) ≤ f(m))
   (pf, assume transitivity_of_order successor1))
   (label pf0)

14. (ue ((numseq. (∀k. f(k))) (n. n)) sumsort * )
   ; NATNUM(SUM(\( \lambda k. F(k)\), N))
   (label pfsort)
   ; deps : (PF, ASSUME)

   The following is the first fact needed for the application of the lemma AddOne. We obtain it
   as an immediate consequence of the assumption of the inductive step.

15. (ue (m n) pf, assume successor11
   ; NATNUM(F(N)) \( \leq\) F(N)
   (label pf 1)
   ; deps : (PF, ASSUME)

   - The second fact,
     \[ n' = \sum_{m=0}^{n-1} f(m) + f(n), \]
     is also an assumption of the inductive step.

16. (assume \[ \sum(\lambda k. f(k), n') = n' \])
   (label pf _assume)

17. (rw * (open sum)>
   ; SUM(\( \lambda k. F(k)\), N) + F(N) = N'
   (label pf2)
   ; deps: (PF, ASSUME)

   The third fact,
   \[ n \leq \sum_{m=0}^{n-1} f(m), \]
   is a direct consequence of Strictly Increasing.

18. (derive \[ n \leq \sum(\lambda k. f(k), n) \]) (strictly-increasing pf0 pfsort))
   (label pf3)
   ; deps: (PF_ASSUME)

19. (ue ((k. f(n)) (n. n) (m. \[ \sum(\lambda k. f(k), n) \])) add-one
   (pf1 pf2 pf3 pfsort))
   ; 1=F(N) \( \leq\) SUM(\( \lambda k. F(k)\), N)
   (label pf4)
   ; deps: (PF_ASSUME)
We use the second conjunct to apply the induction hypothesis.

20. (derive |∀m. m<n⇒f(m) | (pfindhyp pf0 *))
   (label pf5)
   ;deps: (PF,ASSUME PFINDBYP)

21. (derive |n0=n⇒f(n0) | pf4)
   ;deps: (PF,ASSUME)

22. (trw |∀m. m<n⇒f(m) | (use less,succ,lesseq mode: exact)
        (open lesseq) (use normal mode: always) pf5 *)
   ;∀m. m<n⇒f(m)
   ;deps: (PF,ASSUME PFINDBYP)

23. (ci pf,assume)
    ;(∀m. m<n⇒F(M)∧∀f(m)∧sum(λk.f(k),n)=n⇒(∀m. m<n⇒F(M))
    ;deps: (PF,ASSUME)

24. (ci pfindhyp)

25. (ue (a |λn. (∀m. m<n⇒natnum f(m)∧∀f(m))∧sum(λk.f(k),n)=n)
        (∀m. m<n⇒f(m)) I)
    proof-by-induction * )
    ;∀N. (∀m. m<n⇒natnum f(M)∧∀f(m))∧sum(λk.f(k),n)=N⇒(∀m. m<n⇒f(M))
    ;deps: (PFINDHYP)

Check that the result holds for any f:

26. (trw |∀f. n. (∀m. m<n⇒natnum f(m)∧∀f(m))∧sum(λk.f(k),n)=n)
        (∀m. m<n⇒f(m)) I*)
    ;∀f N. (∀f. n. (∀m. m<n⇒natnum f(m)∧∀f(m))∧sum(λk.f(k),n)=N)
    ;∀m. m<n⇒f(M))
    (label pigeonfact)

**Second Proof.** Using the inductive predicate allnum instead of quantifiers, the theorem is proved very quickly.

   (wipe-out)
   (get-proofs sums)
   (proof pigeonfact)

1. (assume |∀n. natnum f(n) |)
   (label sort1)

2. (ue ((numseq. |λk.f(k) |)(n.n)) sumsort *)
   ;natnum(sum(λk.f(k),n))
   (label sort2)

3. (ue (a |∀m. allnum(n,λk.1≤f(k))⇒∃sum(λk.f(k),n))
        proof-by-induction
        (open allnum sum) zeroleast (use sort1 sort2 mode: always)
        (use add,lesseq
         ue: ((n.n)(k.|f(n)|)(m.|sum(λk.f(k),n)|)))
    (label strictly-increasing)
4. \(\forall n. \text{allnum}(n, \lambda k. 1 \leq f(k)) \cap \text{sum}(\lambda k. f(k), n)\)

\(\text{deps: (SORT1)}\)

\((\text{ue (a \ | n. \text{allnum}(n, \lambda k. 1 \leq f(k)) \cap \text{sum}(\lambda k. f(k), n)) = n_3\text{allnum}(n, \lambda k. 1 = f(k))})\)

\(\text{proof-by-induction (open allnum sum) strictly-increasing sort1 sort2 (use add-one (ue: ((k. f(n)) (n.n) (m. lsum(\lambda k. f(k), n) l)) mode: always))}\)

\(\forall n. \text{allnum}(n, \lambda k. 1 \leq f(k)) \text{sum}(\lambda k. f(k), n) = n_3\text{allnum}(n, \lambda k. 1 = f(k))\)

;in more conventional notation:

5. \((\text{rw * (use allnumfact (ue: ((a. \lambda k. 1 \leq f(k))) (n.n))) mode: always direction: reverse (use allnumfact (ue: ((a. \lambda k. 1 = f(k))) (n.n)) mode: always direction: reverse))}\)

\(\forall m. m < n \leq f(m) \text{sum}(\lambda k. f(k), n) = n_3\forall m. m < n \leq f(m)\)

\(\text{deps: (SORT1)}\)

6. \((\text{ci sort1})\)

\(\forall n. \text{natnum}(f(n))\)

\(\forall n. \text{natnum}(f(n)) \text{sum}(\lambda k. f(k), n) = n_3\forall n. \text{natnum}(f(n))\)

(lab: pigeonfact)

**Remark. Example** 6. Let us consider the heuristics of this theorem. If we formulate *Strictly Increasing* using the inductive predicate 'allnum', and expand the definitions we obtain:

0. \(\forall n. \text{allnum}(n, \lambda k. \text{natnum} f(k) \lambda f(k) \leq f(k)) \cap \text{sum}(\lambda k. f(k), n)\)

\(\text{proof-by-induction (open allnum sum) (use add-lesseq)}\)

\(\forall n. \text{natnum}(f(n)) \text{natnum}(\text{sum}(\lambda k. f(k), n))\)

\(\forall n. \text{natnum}(f(n)) \cap \text{natnum}(\text{sum}(\lambda k. f(k), n))\)

\(\forall n. \text{natnum}(f(n)) \text{natnum}(\text{sum}(\lambda k. f(k), n))\)

\(\text{sum}(\lambda k. f(k), n) = n_3\forall n. \text{natnum}(f(n)) \cap \text{natnum}(\text{sum}(\lambda k. f(k), n))\)

The main point is to formulate the fact *Add Lesseq*. In other words, we must recognize that the following line would do the job (once we guarantee that \(f(n)\) and \(\text{sum}(\lambda k. f(k), n)\) are natural numbers):

0. \(\forall n. \text{allnum}(n, \lambda k. \text{natnum} f(k) \lambda f(k) \leq f(k)) \cap \text{sum}(\lambda k. f(k), n)\)

\(\text{proof-by-induction (open allnum sum) (use add-lesseq)}\)

\(\forall n. \text{natnum}(f(n)) \text{natnum}(\text{sum}(\lambda k. f(k), n))\)

\(\forall n. \text{natnum}(f(n)) \cap \text{natnum}(\text{sum}(\lambda k. f(k), n))\)

\(\forall n. \text{natnum}(f(n)) \text{natnum}(\text{sum}(\lambda k. f(k), n))\)

Similarly, the theorem is:

0. \(\forall n. \text{allnum}(n, \lambda k. \text{natnum} f(k) \lambda f(k) \leq f(k)) \cap \text{sum}(\lambda k. f(k), n)\)

\(\text{proof-by-induction (open allnum sum) (use add-lesseq)}\)

\(\forall n. \text{natnum}(f(n)) \text{natnum}(\text{sum}(\lambda k. f(k), n))\)

\(\forall n. \text{natnum}(f(n)) \cap \text{natnum}(\text{sum}(\lambda k. f(k), n))\)

\(\forall n. \text{natnum}(f(n)) \text{natnum}(\text{sum}(\lambda k. f(k), n))\)
Again the key idea is the fact Add One. We need only to construct the following line as a rewriter (and make sure that \( f(n) \) and \( \text{sum}(\lambda k. f(k), N) \) are natural numbers).

\[
\begin{align*}
0. & \quad (\text{ue } ((k, \text{if}(n,l))(n, n)(m, \text{sum}(\lambda k. f(k), n))) \text{ add-one}) \\
& \quad \text{NATNUM}(F(N)) \land \text{NATNUM}(\text{SUM}(\lambda k. F(K), N)) \\
& \quad (1 \leq F(N) \land \text{SUM}(\lambda k. F(K), N) + F(N) = N \land \text{SUM}(\lambda k. F(K), N)) \\
& \quad 1 = F(N) \land \text{SUM}(\lambda k. F(K), N))
\end{align*}
\]

A priori, it may seem irrelevant for our capacity of discovering the appropriate steps whether these facts are expressed by bound quantifiers or by recursive predicates. Intuitively, we can say that the second representation helps us to ‘think recursively’ and to focus our attention towards the right inductive step. The mechanization of the proof makes it clear that the second representation is indeed more economical and gives more precise content to our intuition.

4.2. Corollary for Application to Lists.

As an application we prove the following corollary. Let \( \{a_1, \ldots, a_r\} \) be a sequence of pairwise disjoint sets, given by the functional \( \lambda m. \text{setseq}(m) \) and let \( w \) be any list of length \( n \).

If the function we consider associates any set \( a_i \) with the number of occurrences in \( w \) of elements of \( a_i \), then we can certainly define it as a total function and the sum of the values is certainly bound by \( n \), the length of \( w \). In our terminology:

**Corollary. (Pigeonlist)**

\[
\forall U. \text{DISJOINT}(\text{SETSEQ}, \text{LENGTH } U) : \\
(\forall m. m < \text{LENGTH } U \Rightarrow \text{MULT}(U, \text{SETSEQ}(m))) : \\
(\forall m. m < \text{LENGTH } U \Rightarrow \text{MULT}(U, \text{SETSEQ}(m)))
\]

**Proof** Consider the function \( \lambda k. \text{mult}(w, \text{setseq}(k)) \) from \( \mathbb{N} \) to \( \mathbb{N} \).

\[
(1) \quad \lambda k. \text{mult}(w, \text{setseq}(k))
\]

is a total function. This is certainly true, no matter what \( \text{setseq} \) is by definition of \( \text{mult} \) (see Multfact).

Since the sets \( \text{setseq}(i) \), for \( i < \text{length}(w) \), are pairwise disjoint, then

\[
\sum_{m < \text{length}(w)} \text{mult}(w, \text{setseq}(m)) \leq \bigcup_{i < \text{length}(w)} \text{setseq}(i)
\]

by the Len-ma 4.7. (Mult of Un is Sum Mult). Also by the Lemma 2.8. (Length Mult)

\[
\bigcup_{i < \text{length}(w)} \text{setseq}(i) \leq \text{length}(w).
\]
Therefore

\[ \sum_{m < \text{length}(w)} \text{mult}(w, \text{setseq}(m)) \leq \text{length}(w) \]

Hence we can apply the Theorem \textit{Pigeonfact} to obtain the Corollary.

(proof pigeonlist)

1. (assume \(|\text{disjoint(setseq, length w)}|\))
   (label pl1)
   ; multiplicity less than length

2. (ue ((u.w)(a.lun(setseq, length w)!!)) length_mult)
   ; MULT(U, UN(SETSEQ, LENGTH U)) \leq \text{LENGTH U}
   (label pl2)

3. (derive \(|\text{sum(\text{Am.mutil}(w, \text{setseq}(m))), length w}\| \leq \text{length w}|
   (mult_of_un_is_sum_mult pl1 pl2))
   (label pl3)

4. (ue ((f. |\text{Am.mutil}(u, setseq(m))|)(n. |length u|))) pigeonfact
   pl3 multfact)
   ; (\forall M < \text{LENGTH U} \exists M \text{MULT}(U, \text{SETSEQ}(M)))
   ; (\forall M < \text{LENGTH U} \exists M \text{MULT}(U, \text{SETSEQ}(K)))
   (deps: (PL1))
   : the pigeon hole principle on lists

5. (ei pl1)
   ; \text{DISJOINT(SETSEQ, LENGTH U)\circ}
   ; (\forall M < \text{LENGTH U} \exists M \text{MULT}(U, \text{SETSEQ}(M)))
   ; (\forall M < \text{LENGTH U} \exists M \text{MULT}(U, \text{SETSEQ}(K)))
   (label pigeonlist) ■

4.3. \textbf{Application of the Pigeon Hole Principle to Lists.}

Having proved the Pigeon Hole Principle, we will conclude that every map \( f \) of a finite set \( A \) onto itself is an injection, using our two different representations of finite functions. We could formalize the informal proof, given as a Lemma in the Introduction, Section 1.4. Actually, we could prove a more general result for surjective mappings \( f : A \rightarrow B \) between finite sets of the same cardinality. (The mechanical proof is described as Example 10 in the Conclusion.) (This approach is described as Example 0 in the Conclusion.)

By restricting ourselves to permutations, we can slightly simplify our proof as follows.

First, let

\[ \{x_1, \ldots, x_n\} \]
be an enumeration without repetition of the set \( \text{domain}(f) \) and let \( v \) be the list
\[
(y_1 \ldots y_n)
\]
where
\[
y_j = f(x_i)
\]
for some \( i, v \) lists \( \text{range}(f) \), possibly with repetitions. Finally, consider the sequence of sets
\[
\{x_1\} \ldots \{x_n\}.
\]
These sets are disjoint.

— Second. since \( f \) is onto \( A \), for each \( \{x_i\} \) there is some \( y_j \) such that \( x_i = y_j \), i.e.
\[
|\{j : y_j = x_i\}| \geq 1,
\]
or, in our terminology.
\[
\text{mult}(v, \text{mkset}(x_i)) \geq 1.
\]
Therefore by the Pigeon Hole Principle.
\[
|\{j : y_j = x_i\}| = 1.
\]
— Finally. since \( f \) is into \( A \), each \( y_i \) is some \( x_j \). It follows that the set of all sets \( \{x_i\} \) is a partition of \( v \). i.e. of \( \text{range}(f) \). Every element \( y_j \) of \( \text{range}(f) \) belongs to one and only one class \( [y_j]. \) By the second step, each \( [y_j] \) has cardinality 1. It follows easily that if \( f(x_i) = f(x_j) \) then \( i \neq j \).

The two representations for finite functions cause some variations in the argument. In both cases. the fact that \( f \) is an injection is represented by the fact that, each element of \( S \) occurs just once in a certain list \( v \). In both cases we use the function \( \text{mult} \) to count the number of occurrences of elements of a set in a list. i.e. \( |\{j : y_j = x_i\}| \).

### 4.3.1. Application of the Pigeon Hole Principle to Alists.

In this subsection we give the proof that every map of a finite set onto itself is an injection. using the representation of functions by association lists (Theorem \( \text{Permut Injectp. Section 4.3.5} \).)

If \( \text{alist}_f \) represents \( f \), the fact that \( f \) is a map of a finite set onto itself is given by the property \( \text{permup(alist}_f) \). Then the two lists \( u = \text{dom(alist}_f) \) and \( v = \text{range(alist}_f) \) have the same length and contain the same set of elements. The list \( u \) has the uniqueness property since \( f \) is a function. Our ultimate goal is to show that \( v \) has the uniqueness property, too.

We search for a partitioning \( \{a; : i \leq n\} \) of \( v \), where \( n = \text{length}(v) \), namely, a sequence of \( n \) nonempty disjoint sets, such that each element of \( v \) belongs to some set of the sequence. We know more about \( u \) than about \( v \), since \( u \) has the injectivity property. The idea is to consider the sequence of the sets
\[
\{x : x = \text{nth}(u, m)\},
\]
for \( m < \text{length}(u) \): in our notation
\[
\lambda m. \text{mkset(\text{nth}(u, m))};
\]
this is a sequence of nonempty sets, whose union is the set of members of \( u \). We can prove that it is disjoint, since \( u \) is injective. Thus it partitions \( u \). It partitions also \( v \), since \( u \) and \( v \) are the same as sets.
4.3.2. **Step 1: Injectivity implies Disjointness.**

Lemma 4.1. (**Inj Disj**)

$$\forall u. \text{INJ}(u) \Rightarrow \text{DISJOINT}(\lambda m. \text{MKSET}(\text{NTH}(u, m)), \text{LENGTH } u)$$

**Proof.** To show this, we prove

$$\forall n. \text{INJ}(u) \land n \leq \text{LENGTH } u \Rightarrow \text{DISJOINT}(\lambda m. \text{MKSET}(\text{NTH}(u, m)), n)$$

by induction on $$n$$ (line 13). The theorem follows by taking $$n = \text{LENGTH}(u)$$. The essential part of the induction step is proved first as a lemma (line 12).

; inj implies disjoint
(proof inj, disj)

; a main lemma for the induction step

1. (assume inj u)(label injdsj0)

2. (rw * (open inj))(label injdsj1)
   $$\forall n. \text{INJ}(u) \land n \leq \text{LENGTH } u \Rightarrow \text{DISJOINT}(\lambda m. \text{MKSET}(\text{NTH}(u, m)), n)$$

3. (assume inj ul)(label injdsj2)

4. (assume injdsj2)(label injdsj3)
   $$\forall n. \text{INJ}(u) \land n \leq \text{LENGTH } u \Rightarrow \text{DISJOINT}(\lambda m. \text{MKSET}(\text{NTH}(u, m)), n)$$

5. (ue ((u.u)(n.n)) mksetfact (open lesseq) injdsj2)
   $$\forall n. \text{INJ}(u) \land n \leq \text{LENGTH } u \Rightarrow \text{DISJOINT}(\lambda m. \text{MKSET}(\text{NTH}(u, m)), n)$$

6. (rw injdsj2 use * mode: exact) (open mkset) injdsj2)
   $$\forall n. \text{INJ}(u) \land n \leq \text{LENGTH } u \Rightarrow \text{DISJOINT}(\lambda m. \text{MKSET}(\text{NTH}(u, m)), n)$$

7. (define kv injdsj5)

8. (derive injdsj5)
   $$\forall n. \text{INJ}(u) \land n \leq \text{LENGTH } u \Rightarrow \text{DISJOINT}(\lambda m. \text{MKSET}(\text{NTH}(u, m)), n)$$

9. (derive injdsj5)
   $$\forall n. \text{INJ}(u) \land n \leq \text{LENGTH } u \Rightarrow \text{DISJOINT}(\lambda m. \text{MKSET}(\text{NTH}(u, m)), n)$$

10. (rw injdsj5 use * mode: exact) irreflexivity, of-order)
    $$\text{FALSE}$$
    ; deps: (INJDSJO INJDSJ3 INJDSJ2)

11. (ci injdsj3)
    $$\forall n. \text{INJ}(u) \land n \leq \text{LENGTH } u \Rightarrow \text{DISJOINT}(\lambda m. \text{MKSET}(\text{NTH}(u, m)), n)$$
12. \((ci\ (injdsj0\ injdsj2))\)
\(\stackrel{\text{label injdsj,lemma}}{\Rightarrow}((\text{UN}(\lambda\ M.\ \text{MKSET}(\text{NTH}(U,M)),N))(\text{XV})\lambda(\text{MKSET}(\text{NTH}(U,N)))(\text{XV}))\)

The result follows in two lines.

13. \((ue\ (a\ \lambda n.\ \text{inj}(u)\ \text{An}\ \text{length}(u)\ \text{disjoint}(\lambda m.\ \text{mkset}\ \text{nth}(u,m),n))\)
\(\text{proof-by-induction}\)
\(\text{open disjoint disj, pair intersection empty}\)
\(\text{use less, lesseq succ mode: always direction: reverse}\)
\(\text{use id-lemma mode: always (part 1#2#1#1 (open lesseq)))}\)
\(\forall n.\ \text{INJ}(U)\ \text{An}\ \text{LENGTH}\ \text{U}\ \text{disjoint}(\lambda M.\ \text{MKSET}(\text{NTH}(U,M)),N)\)

14. \((ue\ (n\ \text{length}\ u)\ \ast\ \text{open lesseq})\)
\(\text{INJ}(U)\ \text{disjoint}(\lambda M.\ \text{MKSET}(\text{NTH}(U,M)),\text{LENGTH} U)\)
\(\text{label inj, disj}\)

4.3.3. Step 2: Positive Multiplicity.

**Lemma 4.2.** (*Permutp Injectp Lemma*)

\[VU\ V.MKLSET\ U=MKLSET\ V\]
\[\forall n.\ \text{length}(U)\ \text{disjoint}(\lambda M.\ \text{MKSET}\ \text{NTH}(U,M))\]

**Proof.** We want to show that the multiplicity in \(v\) of the set \(\{x : x = \text{nth}(u,m)\}\) is positive (line 8) under the assumption that \(u\) and \(v\) have the same set of elements (line 1). In fact, we obtain a map

\[\begin{align*}
N_{\text{length}(u)} & \rightarrow N_{\text{length}(v)} \\
n & \mapsto kv,
\end{align*}\]

where \(\text{nth}(v,kv) = \text{nth}(u,n)\) (line 6).

(proof permutp, injectp, lemma)

1. (assume \(\text{mkset}\ U=\text{mkset}\ V\))
\(\text{label pill}\)

2. (assume \(n\ \text{length}\ u\))
\(\text{label pi12}\)

The fact that \(\text{nth}(u,n) \in \{x : \text{member}(x,v,u)\}\) is an immediate consequence of \(Nthme mbe\ v\).

3. (trw \(\text{nth}(u,n)\ \text{in}\ \text{mkset}\ U\) (open epsilon mklset)
\(\text{nthmember}\ pi12\)
\;\text{NTH}(U,N)\ \text{MKSET}(U)
\;\text{deps: (PIL2)}\)

Here we apply line 1.

4. (rw \(\ast\) (use pill mode: exact))
\;\text{NTH}(U,N)\ \text{MKSET}(V)
\;\text{deps: (PIL1 PIL2)}\)

Finally, using \(Mklset\ Fact\), we prove the existence of a \(kv\) such that \(\text{nth}(v,kv) = \text{nth}(u,n)\).
5. \( \text{(rw } \ast \text{ (use mklset \_fact mode: exact) (open epsilon mkset))} \)
   \( \exists K \text{ \& LENGTH V} \text{\_ANTH(V,K)=} \text{NTH(U,N)} \)
   \( \text{;deps: (PIL1 PIL2)} \)

6. \( \text{(define kv | \text{kv<length(v)\text{\_ANTH(v,kv)=nth(u,n)| \ast )}} \)} \)
   \( \text{(label pi13)} \)
   \( \text{;deps: (PIL1 PIL2)} \)

7. \( \text{(trw | \text{member(nth(v,kv),v)| nthmember pi13)}} \)
   \( \text{;MEMBER(NTH(V,KV),V)} \)
   \( \text{(label pi14)} \)

Therefore, by the Lemma. \em membermult, the set \{\( xv : xv = \text{nth(u,n)} \}\} has positive multiplicity in \( v \).

a. \( \text{(ue ((u.v)(y.|nth(v,kv)|))(a.|mkset nth(u,n)|)) member\_mult} \)
   \( \text{(part 1(open mkset)) pil2 pil4 (use pi13 mode: always)} \)
   \( ; 1 \leq \text{MULT(V,mkset(NTH(U,N)))} \)
   \( \text{;deps: (PIL1 PIL2)} \)

9. \( \text{(ci (pill pi12))} \)
   \( ; \text{MKLSET(U)=MKLSET(V)\& LENGTH UXI\_\_MULT(V,mkset(NTH(U,N)))} \)

Cosmetics:

10. \( \text{(derive |\nu v.mkset u=mklset v)} \)
    \( \text{(\forall m.<length u\cup1<\text{mult(v,mkset nth(u,m))| \ast )}} \)
    \( \text{;label permutp_injectp_lemma)} \)

### 4.3.4. Step 3: The Sequence partitions the Range.

Using the result of steps 1 and 2, we will apply the corollary \em Pigeonlist to obtain:

\[
\forall m. m < \text{length } u \cup 1 \leq \text{mult(v,mkset nth(u,m))}
\]

In the final step, for each member \( x \) of \( v \) we consider the set \{\( xv : xv = x \}\} – in our notation we take \( \text{mkset(nth(v,i))} \), with \( x = \text{nth(v,i)} \) for some \( i \) – and show that it coincides with some element of the partition constructed in step 2. Hence we can conclude

\[
\text{mult(v,mkset(nth(v,i))}=1
\]

for all \( i < \text{length(v)} \). Injectivity of \( v \) will follow by the Lemma. \em Mult \em \em Inj (Section 2.12.1).

**Lemma 4.3.** \em (Mult Mult)

\[
\forall U.V. \text{MKLSET(U)=MKLSET(V)} \land \\
(\forall M. M < \text{LENGTH U} \cup 1 \leq \text{MULT(V,mkset(NTH(U,M)))}=1) \cup \\
(\forall I. I < \text{LENGTH V} \cup 1 \leq \text{MULT(V,mkset(NTH(V,I)))}=1)
\]
Proof. This step is easy. Since \( u \) and \( v \) are the same as sets, the \( i \)-th element of \( v \) occurs in \( u \). By the inclusion of line 4, we obtain a map

\[
N_{\text{length}(v)} \rightarrow N_{\text{length}(u)}
\]

\[
i \mapsto mv
\]

where \( \text{nth}(u, mv) = \text{nth}(v, i) \) (line 6). It follows from our main hypothesis (line 2) that the \( i \)-th element has just one occurrence in \( v \).

(proof mult_mult)

1. (assume \([\text{mklset } u = \text{mklset } v]\))
   (label mm1)

2. (assume \([\forall m. m < \text{length } u \subset \text{mult}(v, \text{mkset nth}(u, m)) = 1]\))
   (label mm2)

3. (assume \([i < \text{length } v]\))
   (label mm3)

4. (trw \([\text{nth}(v, i) \in \text{mklset } v]\) (open epsilon mklset)
   (use * nthmember mode: exact))
   \( ; \text{NTH}(V, I) \in \text{MKLSET}(V) \)

5. (rw * (use mm1 mode: exact direction: reverse))
   \( ; \text{NTH}(V, I) \in \text{MKLSET}(U) \)

6. (rw * (use mkset, fact mode: exact) (open epsilon))
   \( ; \exists K. K < \text{LENGTH } U \Rightarrow \text{NTH}(U, K) = \text{NTH}(V, I) \)

7. (define mv \([mv < \text{length } u \land \text{nth}(u, mv) = \text{nth}(v, i)] * )\)
   (label mm4)
   ; MV is unknown.
   ; the symbol MV is given the same declaration as M
   ; deps: (MM1 MM3)
   a. (ue (m mv) mm2 (use * mode: always))
      ; \text{MULT}(V, \text{MKSET}(\text{NTH}(V, I))) = 1
      ; deps: (MM1 MM2 MM3)

9. (ci mm3)
   \( ; i < \text{LENGTH } V \Rightarrow \text{MULT}(V, \text{MKSET}(\text{NTH}(V, I))) = 1 \)
   ; deps: (MM1 MM2)

10. (ci (mm1 mm2))
    \( ; \text{MKLSET}(U) = \text{MKLSET}(V) \land (\forall m. m < \text{LENGTH } U \Rightarrow \text{MULT}(V, \text{MKSET}(\text{NTH}(U, m))) = 1) \cap \)
    \( ; (i < \text{LENGTH } V \Rightarrow \text{MULT}(V, \text{MKSET}(\text{NTH}(V, I))) = 1) \)
    (label mult_mult) ■
4.3.5. The Main Result for Association Lists: Every Permutation is an Injection.

The derivation of main result for alists follows.

**Theorem (Permutp Injectp)**

∀alist. permutp(alist)⇒injectp(alist)

**Proof.**

(proof permutp.injectp)

1. (assume lpermutp alist l> (label permutp.injctp1)

2. (rw * (open permutp))
   ;functp(alist)⇒mkset(dom(alist))=mkset(range(alist))
   (label permutp.injctp2)

3. (rw * (open functp))
   ;uniqueness(dom(alist))⇒mkset(dom(alist))=mkset(range(alist))
   (label permutp.injctp3)

First step: disjointness of a suitable sequence of sets (Lemma Inj Disj)

;labels: uniqueness, injctivity
;∀u. uniqueness(u)=injectivity(u)

;labels: inj, disj
;∀u. inj(u)⇒disjoint(∀.mkset(nth(u,m)), length u)

4. (derive |inj(dom(alist))) l (* uniqueness_injectivity))
   ;deps: (permutp.injectp1)

5. (derive |disjoint(∀.mkset(nth(dom(alist),m)), length (dom(alist))) l (* inj, disj))
   (label permutp.injectp4)

Second step: multiplicity of the sets in the sequence is positive (Permutp Injectp Lemma)

;labels: permutp, injectp-lemma
;∀v. mkset(v)=mkset(v)⇒(∀.mkset(nth(u,m))≤mult(v,mkset(nth(u,m))))

6. (ue ((u.|dom alist|)(v.|range alist|)) permutp.injectp.lemma
    (permutp.injectp3 permutp.injectp4))
   ;∀.mkset(nth(dom(alist)))≤mult(range(alist),mkset(nth(dom(alist),m)))
   (label permutp.injectp5)
Now we apply the Pigeon Hole principle:

\[ \forall \text{setseq} \subseteq \text{length } U \] \text{disjoint}(\text{setseq}, \text{length } U) \land \\
\left( \forall k < \text{length } U \right) \left( \exists \text{mult}(U, \text{setseq}(k)) \right) \\
\left( \forall k < \text{length } U \right) \left( \exists \text{mult}(U, \text{setseq}(k)) \right) \]

\[ \text{need also} \]
\[ \forall \text{domrange} \subseteq \text{length } (\text{dom}(\text{alist})) = \text{length } (\text{range}(\text{alist})) \]

7. (\( \forall \text{setseq} \subseteq \text{length } (\text{dom}(\text{alist})) \)) (\( \forall \text{range} \subseteq \text{alist} \)) (\( \text{pigeonlist} \))

(\( \text{use domrange length mode: exact direction: reverse} \))

\( \text{permup, injectp} 4 \text{ permup, injectp} 5 \)

\[ \forall k < \text{length } (\text{dom}(\text{alist})) \]
\[ \exists \text{mult}(\text{range}(\text{alist}), \text{mkset}(\text{nth}(\text{dom}(\text{alist}), k))) \]

Third step: injectivity (using lemmata \text{Mult Mult} and \text{Mult Inj})

\[ \forall u \forall v \text{ mkset}(u) = \text{mkset}(v) \land \\
\left( \forall k < \text{length } u \right) \left( \exists \text{mult}(u, \text{mkset}(\text{nth}(u, k))) = 1 \right) \\
\left( \forall i < \text{length } v \right) \left( \exists \text{mult}(v, \text{mkset}(\text{nth}(v, i))) = 1 \right) \]

8. (\( \forall u \subseteq \text{length } (\text{range}(\text{alist})) \)) (\( \exists \text{mult}(\text{range}(\text{alist})) \))

\( \text{permup, injectp} 3 \)

\( \forall i < \text{length } (\text{range}(\text{alist})) \)
\[ \exists \text{mult}(\text{range}(\text{alist}), \text{mkset}(\text{nth}(\text{range}(\text{alist}), i))) = 1 \]
\( \text{deps: (permup, injectp1)} \)

\[ \forall v \forall \left( \forall k < \text{length } \forall \text{mult}(v, \text{mkset}(\text{nth}(v, k))) = 1 \right) \text{ inj}(v) \]

9. (\( \exists \text{range} \subseteq \text{alist} \)) (\( \text{mult, inj} * \))

\( \text{inj}(\text{range}(\text{alist})) \)
\( \text{deps: (permup, injectp1)} \)

10. (\( \text{derive uniqueness(range} \subseteq \text{alist}) \)) (\( \text{* uniqueness, injectivity} \))

\( \text{deps: (permup, injectp1)} \)

11. (\( \text{derive injectp, list} \subseteq \text{alist} \)) (\( \text{permup, injectp2} \)) (\( \text{open injectp} \))

\( \text{deps: (permup, injectp1)} \)

12. (\( \text{ci permup, injectp1} \))

\( \text{label permup, injectp} \)

\( \text{(label } \text{permup, injectp)} \)
4.4. Application of the Pigeon Hole Principle to Lists of Numbers.

In the second application we give the proof of the theorem:

Any map of a finite set onto itself is 1-1,

by representing functions as lists of numbers.

Here we have a list u of numbers less than length(u) (intones) and we know that every n less than length(u) occurs in u (ontology). This simplifies our problem. First we can consider for each m < length(u) the set \{x : x = m\}. The proof that the sequence λm.mkset(m) is disjoint is fairly straightforward. The second step-the proof that for m < length(u) the multiplicity of the set \{x : x = m\} is positive-is immediate; only the third step-to prove inj(u) assuming that the multiplicity of every such set in u is exactly 1-requires some work.

4.4.1. Step 1: Disjointness.

Lemma 4.4. (Disjoint Number) VN.DISJOINT(XXV.MKSET(XV),N)

Proof. First a useful fact: if m ∈ ∪i<n{i}, then m < n.

(proof disjoint-number)
1. (ue (a |λn.∀m. (un((λxv.mkset(xv)),n))(m)∀m<n))
   proof-by-induction
   (part 1 (open mkset un emptyset union))
   (use normal mode: always)
   (use successor1 transitivity-of-order)
   ;∀N λxv.mkset(N)(xv) < N
   (label dnl)

Therefore

\[ \bigcup_{i<n} \{i\} \cap \{n\} = 0 \]

and so, by induction on n, \(\bigcup_{i<n}\{i\}\) is disjoint.

2. (ue ((n.n)(m.n)) dnl irreflexivity,of-order)
   ;¬(UN(AXV.MKSET(XV),N))(N)

3. (t r w |(un(λyv.mkset(yv),n))(xv)∧(mkset(n))(xv)|
   (part 2 (open mkset)))
   ;¬((UN(λyv.MKSET(YV),N))(XV)∧(MKSET(N))(XV))

4. (ue (a |λn.disjoint(λxv.mkset(xv),n) |) proof-by-induction
   (open disjoint disj.pair emptyp intersection)
   (use * mode: exact)
   ;∀N DISJOINT(AXV.MKSET(XV),N)
   (label disjoint-number) ■

This completes step 1.
4.4.3. **Step 2: Ontoness Implies Multiplicity.**

**Lemma 4.5. (Onto Mult)**

\[
\forall U. \text{ONTO}(U) \supset \\
(\forall N. \text{LENGTH}(U) \geq \text{MULT}(U, \text{MKSET}(N)))
\]

(label onto,mult) ■

This is immediate from the definition of onto and the lemma. *Member Mult.*

4.4.3. **Step 3: Intoness Implies Multiplicity.**

Using the lemma *Pigeonlist.* steps 1 and 2 we will conclude that

\[
\text{PERM}(U) \supset (\forall K. \text{K} \text{LENGTH} U \supset \text{MULT}(U, \text{MKSET}(K)))
\]

Let's look at the last step.

**Lemma 4.6. (Into Mult)**

\[
\forall U. \text{INTO}(U) \land (\forall K. \text{K} \text{LENGTH} U \supset \text{MULT}(U, \text{MKSET}(K))) \supset \\
(K \text{LENGTH} U \supset \text{MULT}(U, \text{MKSET}(\text{NTH}(U, K))))
\]

**Proof.** Assume into(u) and that for all \(k < \text{length}(u)\) the multiplicity of the set \(\{x : x = k\}\) is exactly 1.

(proof into,mult)

1. (assume \(|\text{into}(u)|\)).
   (label im1)

2. (assume \(|\forall k. k < \text{length} u \supset \text{mult}(u, \text{mkset} k)|\)
   (label im2)

3. (assume \(|k < \text{length} u|\))
   (label im3)

4. (rw iml (open into))
   ;\(\forall N. \text{LENGTH} U \supset \text{NATNUM} \text{NTH}(U, N) \land \text{NTH}(U, N) \text{LENGTH} U\)
   ;deps: (IM1)

By intoness, nth(u,k) is a number less than length(u). The result is immediate from line 2.

5. (ue (k |nth(u,k)|) im2 (use im3 * mode: exact))
   - ;i = \text{MULT}(U, \text{MKSET} \text{NTH}(U, K))
   ;deps: (IM1 IM2 IM3)

6. (ci im3)
   ;\(K \text{LENGTH} U \supset \text{MULT}(U, \text{MKSET}(\text{NTH}(U, K))))
   ;deps: (IM1 IM2)

7. (ci (iml im2))
   ;\text{INTO}(U) \land (\forall K. \text{K} \text{LENGTH} U \supset \text{MULT}(U, \text{MKSET}(K))) \supset \\
   (K \text{LENGTH} U \supset \text{MULT}(U, \text{MKSET}(\text{NTH}(U, K))))
   (label into_mult) ■
4.4.4. The Main Result for Lists: Every Permutation is an Injection.

We now give the main result for functions represented as lists of numbers.

**Theorem (Perm Injectivity)** \(\forall U. \text{PERM}(U) \rightarrow \text{INJ}(U)\)

**Proof.**

(proof perm,inj)

1. (assume \(|\text{perm } U|\))(label perm,inj1)

2. (\(\text{rw } *\)(open perm onto))
   \(;\text{INTO}(U)\alpha(\forall N. N < \text{LENGTH } U \cup \text{MEMBER}(N, U))\)
   (label perm,inj2)

Second step: multiplicity is positive

;labels: \text{MEMBER,MULT}
;\(\forall U \alpha \text{MEMBER}(Y, U) \land \alpha(Y) \circ \text{MULT}(U, A)\)

3. (ue ((u.u)(y.n)(a.|\text{mkset } n|))) member-mult
   (part 1 (open \text{mkset}))
   ;\text{MEMBER}(N, U) \circ \text{MULT}(U, \text{MKSET}(N))

4. (\text{derive } \forall N. N < \text{LENGTH } U \circ \text{MULT}(U, \text{MKSET}(N)))(perm_inj2 *)
   (label perm_inj3)
   ;deps: (PERM_INJ1)

Third step: the application of the pigeon hole

5. (ue ((\text{setseq. } |xv. \text{mkset}(xv)|)(u.u))
   \(\text{pigeonlist disjoint-number } \text{perm_inj3})\)
   ;\forall K. K < \text{LENGTH } U \circ \text{MULT}(U, \text{MKSET}(K))
   (label perm_inj4)
   ;deps: (PERM_INJ1)

6. (\text{ci perm_inj1})
   ;\text{PERM}(U) \circ (\forall K. K < \text{LENGTH } U \circ \text{MULT}(U, \text{MKSET}(K)))\)

Fourth step: injectivity (using Lemmata INTO-MULT and MULT-INJ)

;labels: INTO,MULT
;\(\forall U. \text{INTO}(U) \alpha(\forall K. K < \text{LENGTH } U \circ \text{MULT}(U, \text{MKSET}(K))) \circ\)
;\(\forall I. I < \text{LENGTH } U \circ \text{MULT}(U, \text{MKSET}(\text{NTH}(U, I)))\))

7. (\text{derive } \forall I. I < \text{LENGTH } U \circ \text{MULT}(U, \text{MKSET}(\text{NTH}(U, I))))
   (into-mult perm_inj2 *)
   ;deps: (PERM_INJ1)

;labels: MULT-INJ
;\(\forall V. (\forall K. K < \text{LENGTH } V \circ \text{MULT}(V, \text{MKSET}(\text{NTH}(V, K))) = 1) \circ \text{INJ}(V)\)

8. (ue (v u) mult_inj *)
   ;\text{INJ}(U)
;deps: (PERM_INJ1)

(derive \( |\text{inj}(u)| \) \( (\text{perm}_1\text{inj}_1 \text{perm}_1\text{inj}_4 \text{perm}_1\text{inj},1 \text{emma}) \))
;deps: (PERM_INJ1)

9. (ci perm,injl)
;PERM(U)\overset{\circ}\text{INJ(U)}
. (l a b e l \ p e r m , i n j e c t i v i t y )
5. Representation using Association Lists.

In this section we prove that permutations (over a finite domain) form a group using the representation of functions by association lists.

Remark. In this representation we do not need to restrict ourselves to functions from numbers to numbers: we may consider permutations of any finite set. However, it is customary to view association lists as maps from atoms to S-expressions. We keep this convention.

To define our functions as maps from atoms to atoms would slightly simplify some proofs below: notice that we need the assumption that all the members in the range are atoms in order to prove the lemmata \textit{Invalistsort}, \textit{Dom Invalist}, \textit{Range Invalist} as well as Theorem 3 (ii) and (iii). In the case of permutations this condition is a consequence of the definition of permutation (as a map of a domain of atoms onto itself).

5.1. Definitions of Composition, Inverse and Identity.

The following functions and predicates on \texttt{alists} represent composition of functions, the identity function and the inverse of a function. Since the domain of our functions is not, fixed in advance, we must use a predicate rather than a function for identity.

;functions as association lists
(proof assoc)

;composition of functions
1. (decl (compalist) (infixname: \texttt{\textcircled{\lnot}}) (type: \texttt{GROUND\textcircled{\texttt{\lnot}}GROUND\textcircled{\texttt{\lnot}}GROUND})
   (syntype: constant) (bindingpower: 930))
2. (def ax compalist
    |\texttt{Valist1 alist2 xa y.nil alist2=nil\lnot
    ((xa.y).alist1) \texttt{\lnot} alist2=
    (xa.appalist(y,alist2)).(alist1 \texttt{\lnot} alist2)!)
  )

;the inverse function
3. (decl invalist (type: \texttt{GROUND\textcircled{\texttt{\lnot}}GROUND}))
4. (def ax invalist
    |\texttt{Valist xa y.invalist nil=nil\lnot
    invalist((xa.y).alist)=(y.xa).invalist alist)
  )

;the identity function
5. (decl idalistp (type: \texttt{GROUND\textcircled{\texttt{\lnot}}TRUTHVAL}))
6. (def ax idalistp
    |\texttt{Valist xa y.idalistp(nil)\lnot
    (idalistp((xa.y).alist)\texttt{\lnot}xa=y\texttt{\lnot}idalistp alist)\lnot})
Remark. In the present section the reader should keep in mind that

\[ \text{appalist}(x, \text{alist}_m \text{alist}_g) \]

represents \((g \circ f)(x)\). It would be helpful to use left notation \(x(f \circ g)\) for functions in our comments, but we do not want to change our notation just for one section.

5.2. Almost All the Facts.

We collect here some Lemmata of general use. Their proof are remarkably short applications of \text{alistinduction}. The first two Lemmata are used to check sorts for \text{invalidist} and \text{compalist}.

(proof \text{alistf acts})

1. \((\text{ue} (\chi | \lambda \text{alist}. \text{alistp}(\text{alist} \circ \text{alist})))\)
   \[ \text{alist induction} \]
   \[ (\text{part 1} \text{(open} \text{compalist})(\text{use} \text{appalistsort mode: exact})) \]
   \[ ;\text{VALIST.ALISTP ALIST} \circ \text{ALIST} \]
   \[ (\text{label simpinfo}) (\text{label compalistsort}) \]

2. \((\text{ue} (\chi | \lambda \text{alist}. \text{allp}(\lambda x. \text{atom} x, \text{range} \text{alist}) \text{alistp invalidist(alist)}) \text{I})\)
   \[ \text{alist induction} \]
   \[ (\text{open} \text{range member invalidist}) \]
   \[ (\text{use allpf act}) \]
   \[ \text{ue:} ((\phi. | \lambda x. \text{atom} x|)(x,y)(u. |\text{range} \text{alist}|) \text{mode: always}) \]
   \[ ;\text{VALIST.ALLP(AX.ATOM X,RANGE(ALIST))}\]
   \[ \text{ALISTP INVALIDIST(ALIST)} \]
   \[ (\text{label simpinfo}) (\text{label invalidistsort}) \]

We must consider with special care the behavior of the LISP function

\[ x\text{alist} \ x. \text{appalist}(x, \text{alist}). \]

It is defined as \(\lambda \text{alist} x. \text{cdr(assoc(x,alist))}\), so it associates with \(x\) the first \(y\) such that \((x.y)\) belongs to \text{alist} and has default value \text{NIL}, if there is no such \(y\).

In Lemma 5.1, by assuming that \(x\) belongs to \text{dom(alist)}, we ignore the default case; in Lemma 5.2, by taking into account the default case we prove \text{equality} instead of inclusion of domains.

Next, Lemma 5.3 proves that if \(x\) belongs to \text{dom(alist)}, then the value of \text{appalist}(x, \text{alist}) is not the default value \text{NIL}, but an element belonging to \text{range(alist)}: Lemma 5.4 says that if \(z\) belongs to \text{range(alist)}, then there is an \(x\) in \text{dom(alist)} such that \text{appalist}(x, \text{alist}) = z. Observe that this need not be true, unless \text{alist} represents a function, i.e. unless \text{dom(alist)} has the \text{uniqueness} property. Indeed, if some \((x.z1)\) occurs in \text{alist} before \((x.z)\), with \(z1 \neq z\), then \text{appalist (x,alist)} will give \(z1\) as value.
Lemma 5.1 (App Compalist) \((g \circ f)(x) = g(f(x))\):

\[
\text{VALIST ALIST1 X.MEMBER(X,DOM(ALIST))}: \\
\text{APPALIST(X,ALIST \circ ALIST1)=APPALIST(APPALIST(X,ALIST),ALIST1)}
\]

Proof.

3. (ue (chi |alist.member(x,dom(alist))))
   
   appalist(x,alist \circ alist1)=
   
   appalist(appalist(x,alist),alist1))
   
   alistinduction
   (part 1 (use appalistdef mode: always)
   (open dom member compalist assoc))
   (use normal mode: always))
   
   \%;VALIST.MEMBER(X,DOM(ALIST))
   
   ;APPALIST(X,ALIST \circ ALIST1)=APPALIST(APPALIST(X,ALIST),ALIST1)
   
   (label app,compalist) (label alist,lemmal)

The following Lemma says that the domain of \(g \circ f\) is a subset of the domain of \(f\).

Lemma 5.2 (Dom Compalist)

\[
\text{VALIST ALIST1.DOM(ALIST \circ ALIST1)=DOM(ALIST)}
\]

Proof.

4. (ue (chi |alist.dom(alist \circ alist1)=dom(alist))))
   
   alistinduction
   (open compalist dom))
   
   ;\%VALIST.DOM(ALIST \circ ALIST1)=DOM(ALIST)
   
   (label dom,compalist) (label alist,lemma2)

The next two Lemmata will be used in the proof of Theorem 1(i).

Lemma 5.3 (Nonempty Range)

\[
\text{VALIST X.MEMBER(X,DOM ALIST)}
\]

\[
(\exists Y.\text{MEMBER}(Y,\text{RANGE ALIST})\land\text{APPALIST}(X,\text{ALIST})=Y)
\]

The argument is by induction on alists.

(proof alist,lemma3)

1. (ue (chi |alist.member(x,dom alist)))
   
   somep(\lambda y.appalist(x,alist)=y,rang e alist))
   
   alistinduction
   (part 1 (open dom somep range member appalist assoc))
   (use normal mode: always))
   
   ;\%VALIST.MEMBER(X,DOM(ALIST))\land\text{SOME}(\lambda y.\text{APPALIST}(X,\text{ALIST})=Y,\text{RANGE(ALIST)})

2. (rew * (use somepfact mode: exact))
   
   ;\%VALIST.MEMBER(X,DOM(ALIST))
   
   ;(\exists X1.\text{MEMBER}(X1,\text{RANGE(ALIST)})\land\text{APPALIST}(X,\text{ALIST})=X1)
   
   (label nonempty,range) (label alist,lemma3)
Remark. Example 7. We prove first the formula, in line 1 (containing the recursively defined predicate samep instead of the existential quantifier as in line 2). In this way we considerably shorten the proof. Let's analyze the proof and see how the rewriter of EKL simulates it.

The induction step of line 1 is

\[ \forall x a \ A L I S T . ( M E M B E R ( x , D O M ( A L I S T ) ) ) \]
\[ \cdot \ S O M E P ( \lambda y. A P P A L I S T ( x , A L I S T ) = y , R A N G E ( A L I S T ) ) \]
\[ \cdot \ ( M E M B E R ( x , D O M ( ( x a . y ) . A L I S T ) ) ) \]
\[ \cdot \ S O M E P ( \lambda y_1 . A P P A L I S T ( x , ( x a . y ) . A L I S T ) = y_1 , R A N G E ( ( x a . y ) . A L I S T ) ) \]

By expanding

\[ m e m b e r ( x , d o m ( ( x a . y ) . a l i s t ) ) \]

we obtain two cases:

(i) \( x = x a \), in which case \( c d r ( a s s o c ( x , ( x a . y ) . a l i s t ) ) \) is \( y \), and \( y \) is clearly a member of \( r a n g e ( ( x a . y ) . a l i s t ) \);

(ii) \( m e m b e r ( x , d o m \ a l i s t ) \). In this case the induction hypothesis yields \( s o m e p ( \lambda y_2 . a p p a l i s t ( x , a l i s t ) = y_2 , r a n g e ( a l i s t ) ) \).

(The two cases are dealt with separately by using as a rewriter the formula

\[ \forall p \ q \ r . ( p \lor q \land r ) = ( p \lor r ) \land ( q \lor r ) \]

labeled NORMAL, as we saw in previous examples.)

Consider how the rewriting process accomplishes this inference. By expanding \( a p p a l i s t \) and \( a s s o c \) in

\[ \text{SOME}P(\lambda y_1 . A P P A L I S T ( x , ( x a . y ) . A L I S T ) = y_1 , R A N G E ( ( x a . y ) . A L I S T ) ) \]

we have:

\[ \text{the} \ \text{term} \ APPA\text{L}I\text{S}T( x , ( x a . y ) . A L I S T ) \ \text{is replaced by:} \]
\[ \text{CDR} \ ASSOC( x , ( x a . y ) . A L I S T ) \]
\[ \text{the} \ \text{term} \ ASSOC( x , ( x a . y ) . A L I S T ) \ \text{is replaced by:} \]
\[ \text{IF} \ X = x a \ \text{THEN} \ x a . y \ \text{ELSE} \ ASSOC( x , A L I S T ) \]

Now the conditional term is 'pushed outside' the function \( c d r \):

\[ \text{the} \ \text{term} \ C D R \ ( \text{IF} \ X = x a \ \text{THEN} \ x a . y \ \text{ELSE} \ ASSOC( x , A L I S T ) ) \ \text{is replaced by:} \]
\[ \text{IF} \ X = x a \ \text{THEN} \ C D R \ ASSOC( x , A L I S T ) \ \text{ELSE} \ C D R \ ASSOC( x , A L I S T ) \]
\[ \text{the} \ \text{term} \ Y \ \text{is replaced by:} \]
\[ \text{IF} \ X = x a \ \text{THEN} \ Y = y_1 \ \text{ELSE} \ C D R \ ASSOC( x , A L I S T ) = y_1 \]

Now \( \text{somep} \) is expanded:
In the innermost conditional

; the term \( Y = Y \) is replaced by:

TRUE

so that the 'if' case of the outer conditional becomes

; the term IF \( X = X \) THEN TRUE ELSE CDR ASSOC(X,ALIST) = \( Y \) is replaced by:

\( X = X \) \( \vee \) CDR ASSOC(X,ALIST) = \( Y \)

On the other hand in the 'else' case of outer conditionals.

; the term \( X = X \) is replaced by:

FALSE

; the term IF FALSE THEN \( Y = Y \) ELSE CDR ASSOC(X,ALIST) = \( Y \) is replaced by:

CDR ASSOC(X,ALIST) = \( Y \)

In conclusion, the term (*) becomes

\( X = X \) \( \vee \) CDR ASSOC(X,ALIST) = \( Y \) \( \vee \) SOME P(\( \lambda Y \). CDR ASSOC(X,ALIST) = \( Y \), RANGE(ALIST))

and it is this formula that rewrites to true in both cases (i) and (ii).

Similarly, Lemma 5.4 says that if \( z \) belongs to the range of \( f \) then there is an \( x \) in the domain of \( f \) such that \( f(x) = 3 \). The proof is left to the Appendix.

**Lemma 5.4 (Nonempty Domain)**

\[ \text{VALIST Z.UNIQUENESS DOM(ALIST) \& MEMBER(Z,RANGE ALIST) \& (} \exists X . \text{MEMBER}(X,\text{DOM ALIST}) \& APPALIST}(X,\text{ALIST}) = Z) \]

(label compalist_lemma4)

The following Lemma, (describing the behavior of compalist with respect to the second \textit{alist}) is used in the induction step of the proofs of theorems 3(ii) and 3(iii).

; compalist lemma

\[ \text{\& (ue (chi |alist.\text{-}member(za,range alist))}\}

alist \( \omega \) ((za.z).alist1) = alist \( \omega \) alist1)

alistinduction

(open member range compalist assoc) (use demorgan mode: always)

;\text{VALIST.\text{-}MEMBER}(ZA,RANGE(ALIST))\text{ALIST m ((ZA.Z).ALIST1) = ALIST} \omega \text{ ALIST1}

(label compalist_lemma) \]
We easily check that \texttt{samemap} guarantees identity of composition on the right: \textit{(Samemap Right)}

6. \texttt{(ue (chi \texttt{|alist.samemap(alist1,alist2)\&alist \&\&alist1=alist \&\&alist2|})
alistinduction
(part 1 (open compalist \texttt{samemap}))
;\texttt{VALIST.SAMEMAP(ALIST1,ALIST2)\&ALIST \&\&ALIST1=ALIST \&\&ALIST2}
(label simpinfo) (label \texttt{samemap_right}) ■)

When composing on the left, the best possible analogue is the following: \textit{(Samemap Left)}

\begin{align*}
\texttt{VALIST ALIST1 ALIST2.SAMEMAP(ALIST1,ALIST2)\&}
\texttt{SAMEMAP(ALIST1 \&\&ALIST,ALIST2 \&\&ALIST)}
\end{align*}

The proof uses Lemmata 5.1 and 5.2 and is left to the Appendix.

The main property of the identity \texttt{alist} is given by the following:

\textbf{Lemma 5.5 (Main Idalistp)}

\begin{align*}
\texttt{VALIST Y.IDALISTP(ALIST)\&MEMBER(Y,DOM(ALIST))\&CDR ASSOC(Y,ALIST)=Y}
\end{align*}

\textbf{Proof.}

7. \texttt{(ue (chi \texttt{|alist.idalistp(alist)\&memberof(y,domain alist)\&}}
applist(y,alist)=y)
alistinduction
(open idalistp appalist assoc member dom) (use normal mode: always))
;\texttt{VALIST.IDALISTP(ALIST)\&memberof(y,DOM(ALIST))\&CDR ASSOC(Y,ALIST)=Y}
(label idalistp,main) ■

Finally, we prove two lemmata essential for the proof of Theorem 3.
We show that \texttt{domain(invalidist)} is the same as \texttt{range} and that \texttt{range(invalidist)} is \texttt{domain}.

;\texttt{domain invalist}

8. \texttt{(ue (chi \texttt{|alist.allp(\&x.\texttt{atom \&x,range \&alist})\&}}
domain invalist(alist)=range alist)
alistinduction
(open domain range invalist) (use invalistsort)
(use allpfact
ue: \texttt{((phi.(\&x.\texttt{atom \&x})(\&x.\texttt{atom \&x}))(\&x.\texttt{atom \&x}))) mode: always )
;\texttt{VALIST.ALLP(\&X.ATOM X,RANGE(ALIST))\&}
;\texttt{DOMAIN(INVALIDIST(ALIST))=RANGE(ALIST)}
(label domain invalist) ■

;\texttt{range invalist}

9. \texttt{(ue (chi \texttt{|alist.allp(\&x.\texttt{atom \&x,range \&alist})\&}}
range invalist(alist)=domain alist)
alistinduction
(open domain range invalist) (use invalistsort)
(use allpfact
ue: \texttt{((phi.(\&x.\texttt{atom \&x})(\&x.\texttt{atom \&x}))(\&x.\texttt{atom \&x}))) mode: always )
;\texttt{VALIST.ALLP(\&X.ATOM X,RANGE(ALIST))\&}
;\texttt{RANGE(INVALIDIST(ALIST))=DOMAIN(ALIST)}
(label range-invalist) ■
5.3. The Composition of Permutations is a Permutation.

We want to prove that if two alists, \texttt{alist} and \texttt{alist1} are permuti, then also their composition \texttt{alist \& \& alist1} is a permuti: i.e. (by the definition of permuti) we know that the domain of \texttt{alist} and \texttt{alist1} have the \textit{uniqueness} property and their 'domains and 'ranges' are the same set and we want to show that

(i) \textit{uniqueness} holds of \texttt{dom(alist \& \& alist1)};
(ii) the dom and the range of \texttt{(alist \& \& alist1)} are the same set.

To prove (i) it is enough to show that the \texttt{dom(alist \& \& alist1)} is the same as \texttt{dom(alist)}. To prove (ii) we prove inclusion in both directions.

The proof of (ii) is the longest in this section. The reason is that we cannot use induction on alists in proving facts about the range of \texttt{dom(alist \& \& alist1)} as a set.

\textbf{Theorem 1 (i) ( Permuth (Compalist) )}

\begin{align*}
\text{VALIST ALIST1. PERMUTP(ALIST) \& PERMUTP(ALIST1) \&} \\
\text{MKLSET(DOM(ALIST))=} & \text{MKLSET(DOM(ALIST1)) \&} \\
\text{PERMUTP(ALIST \& ALIST1)} \\
\end{align*}

This is proved through a main Lemma:

\textbf{Lemma Range Compose, past 1:}

\begin{align*}
\text{VALIST ALIST1. PERMUTP(ALIST) \&} \\
\text{MKLSET(DOM(ALIST))=} & \text{MKLSET(DOM(ALIST1)) \&} \\
\text{MKLSET(RANGE(ALIST \& ALIST1)) \& MKLSET(RANGE(ALIST1))} \\
\end{align*}

\textbf{Lemma Range Compose, part 2:}

\begin{align*}
\text{VALIST ALIST1. PERMUTP(ALIST) \& PERMUTP(ALIST1) \&} \\
\text{MKLSET(DOM(ALIST))=} & \text{MKLSET(DOM(ALIST1)) \&} \\
\text{MKLSET(RANGE(ALIST1))} \text{ \& MKLSET(RANGE(ALIST \& ALIST1))} \\
\end{align*}

5.3.1. Proof Range Compose, First Part.

In Part 1 we show that if \texttt{permuth(alist)} and \texttt{mkiset dom(alist)=mkiset dom(alist1)}, then \texttt{range(alist \& \& alist1)} is a subset of \texttt{range(alist1)}.

Let \texttt{f} and \texttt{g} be the functions represented by \texttt{alist} and \texttt{alist1}, respectively. The argument can be summarized as follows: given \texttt{z} in the range of \texttt{g \& f}, choose an element \texttt{x \& z} in the inverse image of \texttt{z} by \texttt{g \& f}. Such element is in the domain of \texttt{f}. By definition of composition, if \texttt{z = (g \& f)(x \& z)}, then \texttt{z = g(f(x \& z))}, so \texttt{z} belongs to the range of \texttt{g}.
1. (assume [permutp(alist)])
   (label rcl)

2. (rw * (open permutp functp))
   ;UNIQUENESS(DOM(ALIST))\&MKLSET(DOM(ALIST))=MKLSET(RANGE(ALIST))
   (label rc2)
   ;deps: (RC1)

The next line says that the functions \( f \) and \( g \) represented by \( \text{alist} \) and \( \text{alist} \) 1 have the same domain.

3. (assume [mklset dom(alist)=mklset dom(alist1)])
   (label rc3)

4. (assume [member(z,range(alist m alist1))])
   (label rc4)

By applying Lemma 4 we associate to \( z \) an element \( x_z \) in \( \text{dom(alist m alist1)} \). By Lemma 2 \( x_z \) lies in \( \text{dom(alist)} \) (line 6).

5. (ue ((alist |alist w alist1|)(z.z)) nonempty, domain
   - (use dom, compalist rc2 rc4 mode: exact))
   ;\exists \text{. MEMBER(X,DOM(ALIST))\&APPALIST(X,ALIST w ALIST1)=Z}
   ;deps: (RC1 RC4)

6. (define xxvv
   |member(xxvv,dom alist)\&appalist(xxvv,alist w alist1)=z| *)
   (label rc5)
   ;deps: (RC1 RC4)

Apply Lemma 1:

7. (rw * (use app, compalist mode: always))
   ;MEMBER(X,DOM(ALIST))\&APPALIST(APPALIST(X,ALIST),ALIST1)=Z
   (label rc6)
   ;deps: (RC1 RC4)

This represents the fact that if \( z = (g \circ f)(x_z) \), then \( z = g(f(x_z)) \). The proof is not finished. However, we have to check that the two applications of \text{appalist} do not give default value.

By applying lemma, 3, we associate to \( x_z \) its image \( y_z \) in the \text{range(alist)}.

8. (define yyvv |member(yyvv,range alist)\&appalist(xxvv,alist)=yyvv|
   (nonempty, range rc6))
   (label rc7)
   ;deps: (RC1 RC4)

9. (trw |yyvv \in mklset range(alist)| (open mklset epsilon) rc7)
   ;YYVV\in\text{MKLSET(RANGE(ALIST))}
   ;deps: (RC1 RC4)
By the assumption of line 3 we know that \( y_z \) belongs to \( \text{dom}(\text{alist1}) \).

10. \((\text{rw} \ast (\text{use rc2 mode: exact direction: reverse}) \newline (\text{use rc3 mode: exact}) \newline ;YYVV \in \text{MKLSET}(\text{DOM}(\text{ALIST1}))) \newline ;\text{deps}: (\text{RC1 RC3 RC4})\)

11. \((\text{rw} \ast (\text{open epsilon mkls})) \newline ;\text{MEMBER}(YYVV,\text{DOM}(\text{ALIST1})) \newline ;\text{deps}: (\text{RC1 RC3 RC4})\)

We apply again lemma 3 to pick the image of \( y_z \) in \( \text{range}(\text{alist1}) \).

12. \((\text{define zzvv |member(zzvv,range alist1)\text{APPALIST}(yyvv,alist1)=zzvv|} \newline (\text{label rc8}) \newline ;\text{deps}: (\text{RC1 RC3 RC4})\)

By lines 7 and 8 such an image is \( z \).

13. \((\text{rw rc6 rc7}) \newline ;\text{MEMBER}(XXVV,\text{DOM}(\text{ALIST})) \text{APPALIST}(YYVV,\text{ALIST1})=Z \newline ;\text{deps}: (\text{RC1 RC4})\)

14. \((\text{trw |zzvv=z| \ast (\text{use rc8 mode: always direction: reverse})} \newline ;zzvv=z \newline ;\text{deps}: (\text{RC1 RC3 RC4})\)

Hence, \( z \) is in the \( \text{range}(\text{alist1}) \).

15. \((\text{trw |member(z,range alist1)| rc8} \newline (\text{use \ast mode: exact direction: reverse}) \newline ;\text{MEMBER}(Z,\text{RANGE}(\text{ALIST1})) \newline ;\text{deps}: (\text{RC1 RC3 RC4})\)

16. \((\text{ci rc4}) \newline ;\text{MEMBER}(Z,\text{RANGE}(\text{ALIST} \circ \text{ALIST1})) \text{MEMBER}(Z,\text{RANGE}(\text{ALIST1})) \newline ;\text{deps}: (\text{RC1 RC3})\)

17. \((\text{trw |mklset range(alist \circ alist1)\text{cmklset range(alist1)}| \ast} \newline (\text{open mklset inclusion}) \newline ;\text{MKLSET}(\text{RANGE}(\text{ALIST} \circ \text{ALIST1})) \text{CMKLSET}(\text{RANGE}(\text{ALIST1})) \newline ;\text{deps}: (\text{RC1 RC3})\)

18. \((\text{ci (rc1 rc3)}) \newline ;\text{PERMUTP}(\text{ALIST}) \text{AMKLSET}(\text{DOM}(\text{ALIST}))=\text{MKLSET}(\text{DOM}(\text{ALIST1})) \newline ;\text{MKLSET}(\text{RANGE}(\text{ALIST} \circ \text{ALIST1})) \text{CMKLSET}(\text{RANGE}(\text{ALIST1})) \newline (\text{label range-compose})\)
5.3.2. Proof of Range Compose, Second Part.

In Part 2, again under the assumption that

\[ \text{permutp(alist)} \land \text{mklset dom(alist)} = \text{mklset dom(alist1)}. \]

we prove that

\[ \text{range(alist)} \subseteq \text{range(alist w alist1)} \]

The derivation represents the following argument: suppose that \( f \) and \( g \) are maps of the same finite set onto itself and \( z \) belongs to the range of \( g \). If \( y_z \) is in the inverse image of \( z \) by \( g \), then \( y_z \) is in the range of \( f \). Moreover, if \( x_z \) is in the inverse image of \( y_z \) by \( f \), then \( z = g(f(x_z)) \), i.e. \( z = (g \circ f)(x_z) \). Therefore \( z \) is in the range of \( g \circ f \).

(proof range-compose2)

1. (assume |permutp(alist)|)
   (label rc21)

2. (rw * (open permutp functp))
   ;UNIQUENESS(DOM(ALIST))\land MKLSET(DOM(ALIST)) = MKLSET(RANGE(ALIST))
   (label rc22)

3. (assume |permutp(alist1)|)
   (label rc23)

4. (rw * (open permutp functp))
   ;UNIQUENESS(DOM(ALIST1))\land MKLSET(DOM(ALIST1)) = MKLSET(RANGE(ALIST1))
   (label rc24)

5. (assume |mklset dom(alist) = mklset dom(alist1)|)
   (label rc25)

6. (assume |member(z, range alist1) | >
   (label rc26)

Given \( z \) in \( \text{range(alist1)} \), using lemma -4 we pick a \( y_z \) in \( \text{dom(alist1)} \) such that

\[ \text{appalist}(y_z, \text{alist1}) = z. \]

7. (define yvl |member(yv1, dom alist1) \land \text{appalist(yv1,alist1)=z}|
   (nonempty, domain rc24 rc26))
   (label rc27)

8. (trw |yv1 \in mklset dom(alist1)| * (open epsilon mklset))
   ;YV1\in MKLSET(DOM(ALIST1))
   ;deps: (RC23 RC26)

By our assumptions \( y_z \) is in \( \text{range(alist)} \).
9. (rw * (use rc25 mode: exact direction: reverse)
   (use rc22 mode: exact))
   ;YV1=MKLSET(RANGE(ALIST))
   ;deps: (RC21 RC23 RC25 RC26)

10. (rw * (open epsilon mklset))
    ;MEMBER(YV1,RANGE(ALIST))
    (label rc28)
    ;deps: (RC21 RC23 RC25 RC26)

By applying again lemma 4 we can pick \( x_z \) in \( \text{dom(alist)} \) such that

\[
\text{appalist}(x_z, \text{alist}) = y_z.
\]

11. (define xv1 |member(xv1,dom alist)Aappalist(xv1,alist)=yv1|
    (nonempty-domain rc22 rc28))
    (label rc29)
    ;deps: (RC21 RC23 RC25 RC26)

Apply lemma 2:

12. (trw |member(xv1,dom(alist \& alist))|* (use dom_comalist))
    ;MEMBER(XV1,DOM(ALIST \& ALIST))
    (label rc30)
    ;deps: (RC21 RC23 RC25 RC26)

Now, by rewriting, we derive

\[
z = \text{appalist(appalist}(x_z, \text{alist}), \text{alist}) = \text{appalist}(x_z, \text{alist} \& \text{alist}).
\]

13. (trw |appalist(xv1,alist \& alist)| rc29 rc30
    (use app_comalist rc29 rc27 mode: always))
    ;APPALIST(XV1,ALIST \& ALIST)\&Z
    (label rc31)
    ;deps: (RC21 RC23 RC25 RC26)

We have to check that \( z \) is not the default value of appalist. We apply Nonempty Range:

14. (ue ((alist |alist \& alist)|(x.xv1)) nonempty,range
    (use dom_comalist rc22 rc30 mode: always))
    ;\exists Y.MEMBER(Y,RANGE(ALIST \& ALIST))AAPPALIST(XV1,ALIST m ALIST)=Y
    ;deps: (RC21 RC23 RC25 RC26)

15. (define zv1 |member(zv1,range(alist \& alist))A
    appalist(xv1,alist \& alist)=zv1 | * )
    (label rc32)
    ;deps: (RC21 RC23 RC25 RC26)

16. (trw |zv1=z| rc31 (use * mode: always direction: reverse))
    ;ZV1=Z
    ;deps: (RC21 RC23 RC25 RC26)
100

ABOUT PERMUTATIONS IN LISP AND EKL

So \( z \) belongs to the range(alist \( m \) alistl).

17. (trw \( |\text{member}(z,\text{range(alist} \odot \text{alist1})| \) rc32
   (use \( * \) mode: exact direction: reverse))
   ;MEMBER(Z,RANGE(ALIST \( m \) ALIST1))
   ;deps: (RC21 RC23 RC25 RC26)

18. (ci rc26)
   ;MEMBER(Z,RANGE(ALIST1)) \odot \text{MEMBER}(Z,RANGE(ALIST} \odot \text{alistl})
   ;deps: (RC21 RC23 RC25)

19. (trw \( |\text{mklset range(alist1}) \odot \text{mklset range(alist} \odot \text{alist1})| \) *
   (open inclusion mklset )
   ;MKLSET(RANGE(ALIST1)) \odot \text{MKLSET(RANGE(ALIST} \odot \text{alistl})}
   ;deps: (RC21 RC23 RC25)

20. (ci (rc21 rc23 rc25))
   ;PERMUTP(ALIST) \odot \text{PERMUTP(ALIST} \odot \text{alist1}) \odot \text{MKLSET(DOM(ALIST))}=\text{MKLSET(DOM(ALIST} \odot \text{alist1})})
   ;MKLSET(RANGE(ALIST1)) \odot \text{MKLSET(RANGE(ALIST} \odot \text{alistl})}
   (label range-compose)

5.3.3. Conclusion of the Proof of Permutp Compose.

Now we conclude the theorem: by Lemma Range Compose and extensionality we show that

\[
\text{mklset(range(alist} \odot \text{alist1})) = \text{mklset(range(alist1))}
\]

(line 7). By the definition of permutp and the assumption that the alisl1 and \( \text{alist2} \) are permutations of the same set (line 3), mklset range(alist1) is equal to mklset dom(alist). An application of Lemma 2 (line 10) is enough to reach the conclusion.

(proof permutp,compalist)

1. (assume \( |\text{permutp(alist})| \))
   (label permut,compl)

2. (assume \( |\text{permutp(alist})| \))
   (label permut_comp2)

3. (assume \( |\text{mklset(dom(alist))}=\text{mklset(dom(alist} \odot \text{alist1})}| \))
   (label permut_comp3)

4. (derive \( |\text{mklset(range(alist} \odot \text{alist1})} \odot \text{mklset(range(alist} \odot \text{alist1})}| \)
   \( \text{mklset(range(alist} \odot \text{alist1})} \odot \text{mklset(range(alist} \odot \text{alist1})})
   (permut,compl permut_comp2 permut_comp3 range-compose))
   ;deps: (PERMUT_COMP1 PERMUT_COMP2 PERMUT_COMP3)

5. (rw \( * \) (open inclusion))
   ;(\( \forall \text{X}.(\text{MKLSET(RANGE(ALIST} \odot \text{ALIST1})))(\text{X})\)) \odot \text{MKLSET(RANGE(ALIST1))}(\text{X})\)
   ;(\( \forall \text{X}.(\text{MKLSET(RANGE(ALIST1})))(\text{X})\)) \odot \text{MKLSET(RANGE(ALIST} \odot \text{alistl}))\)
   ;deps: (PERMUT_COMP1 PERMUT_COMP2 PERMUT_COMP3)
6. \[ (\text{derive } \forall x.(\text{mklset range(alist m alist1)})(xv) = (\text{mklset range(alist1)})(xv) \star) \]

Remember \textit{Set Extensionality}:

\begin{verbatim}
;labels: SET, EXTENSIONALITY
; (AXIOM \( \forall A B. (\forall x. x \in A \rightarrow x \in B) \rightarrow A = B \))
\end{verbatim}

7. \[ (\text{ue } ((a.\text{mklset range(alist m alist1)}) \ |
     (b.\text{mklset range(alist1)})))
    \set{set, extensionality}
    \star (open \text{epsilon})
    ;MKLSET(RANGE(ALIST m ALIST1)) = MKLSET(RANGE(ALIST1))
    ;deps: (PERMUT_CMP1 PERMUT_CMP2 PERMUT_CMP3)
    (label permut_comp4)
\]

8. \[ (\text{rw permut_comp1 (open permutp functp)})
    ;UNIQUENESS(DOM(ALIST)) \& MKLSET(DOM(ALIST)) = MKLSET(RANGE(ALIST))
    (label permut_comp5)
\]

9. \[ (\text{rw permut_comp2 (open permutp)})
    ;FUNCTP(ALIST1) \& MKLSET(DOM(ALIST1)) = MKLSET(RANGE(ALIST1))
\]

10. \[ (\text{trw } \text{uniqueness(dom(alist m alist1)))} \&
    \text{mklset dom(alist m alist1)} = \text{mklset range(alist m alist1)}|
    (use dom, comp alist permut_comp4 mode: exact) permut_comp5
    (use \star permut_comp3 mode: always direction: reverse)
    ;MKLSET(RANGE(ALIST m ALIST1)) = MKLSET(RANGE(ALIST m ALIST1))
    ;deps: (PERMUT_CMP1 PERMUT_CMP2 PERMUT_CMP3)
\]

11. \[ (\text{trw } \text{permut(alist m alist1)}) \star (open permutp functp))
    ;PERMUTP(ALIST m ALIST1)
    ;deps: (PERMUT_CMP1 PERMUT_CMP2 PERMUT_CMP3)
\]

12. \[ (\text{ci (permut_comp1 permut_comp2 permut_comp3))}
    ;PERMUTP(ALIST1) \& PERMUTP(ALIST1) \& MKLSET(DOM(ALIST)) = MKLSET(DOM(ALIST1))
    ;PERMUTP(ALIST1 m ALIST1)
    (label permutp, comp alist)
\]

* 5.4. \textbf{Associativity of Composition.}

To show that composition is associative is very straightforward. Line 3 simply helps the rewriter in the inductive step to expand the antecedent of the induction formula (line 4).

\textbf{Theorem 1} (ii) \textit{(Comalist Associativity)}

\[ \text{VALIST ALIST1 ALIST2. MKLSET(RANGE(ALIST))} \& \text{MKLSET(DOM(ALIST1))} \&
\text{ALIST m (ALIST1 m ALIST2)} = (ALIST m ALIST1) m ALIST2 \]
Proof.

(proof compalist-associativity)

1. (trw |mklset(range((xa.y).alist))mklset(dom alist1)\nmember(y,dom alist1)mklset range(alist)mklset dom(alist1)|\n(open mklset inclusion range member)\n(use normal mode: always))\n\;MKLSET(RANGE((XA.Y).ALIST))\;CMKLSET(DOM(ALIST1))\;\;\;MEMBER(Y,DOM(ALIST1))\;AMKLSET(RANGE(ALIST))\;CMKLSET(DOM(ALIST1))

2. (trw |member(y,dom alist1)Amklset range(alist)Cmklset dom(alist1))mklset(range((xa.y).alist))Cmklset(dom alist1)| (der)\n(open mklset inclusion range member)\n(use normal mode: always))

3. (derive |mklset(range((xa.y).alist))Cmklset(dom alist1)=\nmember(y,dom alist1)Amklset range(alist)Cmklset dom(alist1)| (* -2))\n(label helpinduction)

4. (ue (chi |\lambda alist.mklset(range alist)Cmklset(dom alist1))\nalist m (alist m alist2)=(alist m alist1) m alist2|)\nalistinduction\n(part 1 (open compalist) (use app,compalist * mode: always)))\n\;VALIST.MKLSET(RANGE(ALIST))\;CMKLSET(DOM(ALIST1))\;\;\;ALIST m (ALIST1 m ALIST2)=(ALIST m ALIST1) m ALIST2\n(label compalist-associativity) ■

5.5. The Identity Alist.

It is a simple matter to prove that an alist representing an identity function satisfies the property permup.

Theorem 2 (i) (Idalistp Permup)

\forall ALIST.FUNCTP(ALIST)\land ALISTP(ALIST)\land Permup(ALIST)

Proof.

1. (ue (chi |\lambda alist.idalistp(alist)\land dom alist=range alist|) alistinduction\n(open idalistp dom range)).\n\;\forall ALIST.IDALISTP(ALIST)\land DOM(ALIST)=RANGE(ALIST)

2. (trw |\forall list.functp(alist)\land idalistp(alist)\land permup(alist)|\n(open functp permup) (use * mode: always))\n\;\forall ALIST.FUNCTP(ALIST)\land IDALISTP(ALIST)\land PERMUP(ALIST)\n(label idalistp_permup) ■
Using the same 'help' for the rewriter that was used in the preceding section it is easy to prove the main theorem for right identity. We prove that if alist represents the identity function \( i \) and alist represents a function \( f \) (\( i \) and \( f \) being defined on the right domains), then \( \text{alist} \circ \text{alist1} = \text{alist} \), i.e. \( i \circ f = f \).

**Theorem 2** (ii) (*Idalistp Right*)

\[
\forall \text{ALIST1}. \text{IDALISTP} (\text{ALIST1}) \supset
(\text{ALIST}. \text{MKLSET} (\text{RANGE} (\text{ALIST}))) \text{C} \text{MKLSET} (\text{DOM} (\text{ALIST1})) \supset \text{ALIST} \circ \text{ALIST1} = \text{ALIST}
\]

**Proof.**

3. (assume \( \text{Idalistp(alist1)} \))
4. (\( \text{ue (chi \text{alist}. \text{mklset} (\text{range} (\text{alist}))) \text{C} \text{mklset} (\text{dom} (\text{alist1}))) \supset \text{alist} \circ \text{alist1} = \text{alist} \))
   \( \text{alistinduction} \\
   \text{(part 1 (open compalist))} \\
   \text{(use helpinduction idalistp,main * mode: always)} \)
   ;\( \forall \text{ALIST}. \text{MKLSET} (\text{RANGE} (\text{ALIST})) \text{C} \text{MKLSET} (\text{DOM} (\text{ALIST1})) \supset \text{ALIST} \circ \text{ALIST1} = \text{ALIST} \)
   ;deps: (4)
5. (ci -2)
   ;\text{IDALISTP}(\text{ALIST1})
   ;(\( \forall \text{ALIST}. \text{MKLSET} (\text{RANGE} (\text{ALIST})) \text{C} \text{MKLSET} (\text{DOM} (\text{ALIST1})) \supset \text{ALIST} \circ \text{ALIST1} = \text{ALIST} \))
   (label idalistp-right)

Left identity presents a different kind of problem. Here we pay for our sins, namely for the fact that our representation is not unique. What we prove is that if alistid is idalistp then \( \text{alistid} \circ \text{alist} \) is in the relation \text{samemap} with \text{alist}. The proof uses the main fact about identity \text{alist} (lemma, \text{Main Idalistp}).

**Theorem 2** (iii) (*Left Idalistp*)

\[
\forall \text{ALIST}. \text{IDALISTP} (\text{ALISTID}) \supset \text{MKLSET} (\text{DOM} (\text{ALISTID})) = \text{MKLSET} (\text{DOM} (\text{ALIST})) \supset \text{SAMEMAP} (\text{ALISTID} \circ \text{ALIST}, \text{ALIST})
\]

**Proof.**

(proof idalistp-left)

1. (assume \( \text{Idalistp alistid} \))
   (label idal_11)
   ;\text{ALISTID} is unknown.
   ;the symbol \text{ALISTID} is given the same declaration as \text{ALIST}
2. (assume \( \text{mklset dom(alistid)=mklset dom(alist)} \))
   (label idal_12)
3. (assume \( \forall \text{u} \in \text{mklset (dom(alistid \circ \text{alist})})} \))
   (label idal_13)
4. (\( \text{rw * (use dom_compalist mode: exact)} \text{(open epsilon mklset)} \))
5.6. **Inverse of a Permutation is a Permutation.**

We promised short proofs for the inverse operation using association lists. *Et voila!*...
Theorem 3. (ii) *(Right Invalid)*

\[ \forall \text{ALIST} \ . \ \text{ALLP}(\lambda x. \text{ATOM } x, \text{RANGE(ALIST)}) \land \text{INJECTP(ALIST)} \land \text{IDALISTP(ALIST} \circ \text{INVALIST(ALIST)}) \]

**Proof.**

(proof invalist)

1. \( (\text{ue (chi } \lambda \text{alist.allp(} \lambda x. \text{atom } x, \text{range(alist)}) \land \text{INJECTP(alist)} \land \text{IDALISTP(alist } \circ \text{INVALIST(alist)}) )) \)

alistinduction

(part 1)

(use allpfact

ue: \((\phi. (\lambda x. \text{atom } x)) (x,y) (u. \text{range alist}1) \)

(open range injectp functp uniqueness invalist idalistp compalist appalist assoc)

(use invalistsort dom,invalist compalist,lemma mode: exact))

; \( \forall \text{ALIST} \ . \ \text{ALLP}(\lambda x. \text{ATOM } x, \text{RANGE(ALIST)}) \land \text{INJECTP(ALIST)} \land \text{IDALISTP(ALIST} \circ \text{INVALIST(ALIST)}) \)

,label invalist,right) ■

Theorem 3. (iii) *(Left Invalid)*

\[ \forall \text{ALIST} \ . \ \text{ALLP}(\lambda x. \text{ATOM } x, \text{RANGE(ALIST)}) \land \text{INJECTP(ALIST)} \land \text{IDALISTP(INVALIDALIST(ALIST} \circ \text{ALIST})} \]

**Proof.**

2. \( (\text{assume } \lambda \text{allp(} \lambda x. \text{atom } x, \text{range(alist)}) ) \)

3. \( (\text{ue ((alist. } \lambda \text{INVALIST(alist)}) (alist1. } \lambda \text{alist}) (za.xa)(z.y)) \)

   compalist,lemma

   (use invalistsort range,invalist mode: exact))

; \( \text{MEMBER(XA,DOM(ALIST))} \)

; \( \text{INVALIST(ALIST} \circ ((XA.Y).ALIST) = \text{INVALIST(ALIST} \circ \text{ALIST}) \)

4. \( (\text{ci -2}) \)

; \( \text{ALLP(XX.ATOM X, RANGE(ALIST))} \)

; \( \text{MEMBER(XA,DOM(ALIST))} \)

; \( \text{INVALIST(ALIST) } \circ ((XA.Y).ALIST) = \text{INVALIST(ALIST} \circ \text{ALIST}) \)

5. \( (\text{ue (chi } \lambda \text{alist.allp(} \lambda x. \text{atom } x, \text{range(alist)}) \land \text{INJECTP(alist)} \land \text{IDALISTP(alist } \circ \text{INVALIST(alist)}) )) \)

alistinduction

(part 1 (open allp range injectp functp uniqueness invalist appalist compalist assoc idalistp)

invalistsort (use range-invalidist mode: exact) (use \(*\) mode: always))

; \( \forall \text{ALIST} \ . \ \text{ALLP}(\lambda x. \text{ATOM } x, \text{RANGE(ALIST)}) \land \text{INJECTP(ALIST)} \land \text{IDALISTP(INVALIDALIST(ALIST} \circ \text{ALIST})} \)

,label invalist,left) ■

Part (i) of Theorem 3 is also quite easy. We need first a Lemma, to make sure that
dom(invalid(alist))

is made of atoms only. The proof of this lemma is a simple example of method of proof frequently used in this paper: first we prove a property of lists by a convenient induction and then we derive a property of sets (i.e. we abstract from the order given by the list.).

**Lemma (Atomrange)**

\[
\forall \text{ALIST.}\text{MKLSET(DOM(ALIST))=MKLSET(RANGE(ALIST))}\land \\
\text{ALLP}(\lambda X.\text{ATOM }X,\text{RANGE(ALIST)})
\]

**Proof.**

(proof atomrange)

1. (assume \(|\text{mklsed(dom(alist))}=\text{mklsed(range(alist)))}||

(label arl)

2. (ue (chi |\text{alist.allp}(\lambda x.\text{atom(x)},\text{dom alist})|)

alistinduction

(open allp dom)

;\text{VALIST.ALLP}(\lambda X.\text{ATOM }X,\text{DOM(ALIST)})

(label ar2)

3. (ue ((phil.lXx.\text{atom(x)}l)(x.x)(u.ldom

alistl))) allp,elimination *

;MEMBER(X,DOM(ALIST)) \text{ATOM }X

4. (trw |\text{mklsed dom(alist)}C(\lambda x.\text{atom x})| *) (open inclusion mklsed )

;\text{MKLSET(DOM(ALIST))C(AX.ATOM }X)

5. (rw * (use arl mode: exact))

;\text{MKLSET(RANGE(ALIST))C(AX.ATOM }X)

6. (rw * (open inclusion mklsed))

;\forall X.\text{MEMBER(X, RANGE(ALIST))ATOM }X

7. (ue ((phil.lXx.\text{atom(x)}l)(u.|range

alistl)) allp, introduction *)

;\text{ALLP}(\lambda X.\text{ATOM }X,\text{RANGE(ALIST)})

8. (ci arl)

* ;\text{MKLSET(DOM(ALIST))=MKLSET(RANGE(ALIST))\land ALLP(AX.ATOM X,RANGE(ALIST))}

(label atomrange) ■

Now we can prove

**Theorem 3.** (i) (Permtp Invalist)

\[
\forall \text{ALIST.}\text{PERMTP(ALIST)}\supset \text{PERMTP(INVALID(ALIST))}
\]

**Proof.** By our application of the Pigeon Hole Principle we know that

\[
\forall \text{ALIST.}\text{PERMTP(ALIST)}\supset \text{INJECTP(ALIST)}
\]
(see Permut Injectp, Section 4.3.5). Lines 3 and 4 will give permutp(invalist(alist))(line 10), using the fact that

(i) \text{dom(invalist(alist))} is range(alist) (line 6) and
(ii) \text{range(invalist(alist))} is \text{dom(alist)} (line 7);
these are true because of our Lemma Atomrange (line 5).

(proof permutp-invalist)

1. (assume lpermutp alist >
   (label piv1)

2. (derive |injectp alist|(permutp_injectp piv1))
   ;deps: (PIVI)

3. (rw * (open injectp))
   ;\text{FUNCTP(ALIST) UNIQUENESS(RANGE(ALIST))}
   (label piv2)

4. (rw piv1 (open permutp))
   ;\text{FUNCTP(ALIST) MKLSET(DOM(ALIST)) = MKLSET(RANGE(ALIST))}
   (label piv3)

5. (derive |allp(\lambda x.\text{atom x},range alist)|(atomrange *))
   (label piv4)

6. (derive |dom invalist(alist)|range alist|(dom,invalist *)
   (label piv5)

7. (derive |range invalist(alist)|dom alist|(range-invalist piv4))
   (label piv6)

8. (trw |uniqueness dom(invalist(alist))| piv2 (use piv5))
   ;\text{UNIQUENESS(DOM(INVALIST(ALIST)))}
   (label piv7)

9. (trw |mklist set dom(invalist(alist))| mklist set range(invalist(alist))| piv3 (use piv5 piv6))
   ;\text{MKLISTSET(DOM(INVALIST(ALIST))) = MKLISTSET(RANGE(INVALIST(ALIST)))}
   (label piv8)

10. (trw lpermutp invalist(alist)| piv7 piv8
    (open permutp functp) (use invalistsort piv4 mode: exact)
    ;\text{PERMUTP(INVALIST(ALIST))}
    ;deps: (PIVI)

11. (ci piv1)
    ;\text{PERMUTP(ALIST) = PERMUTP(INVALIST(ALIST))}
    (label permutp-invalist) ■
6. Representation using Lists of Numbers.

The rest of this paper contains the proof that permutations (of a finite set) form a group, with functions being represented by lists of numbers.

6.1. General Comments on the Choice of the LISP Functions or Predicates.

After the main features of a certain representation have been chosen, many variations are possible, not all equally desirable. Our representation of permutations by lists of numbers “lists the range” in the order given by the domain. However, given a 1-1 finite function \( h : \mathbb{N} \rightarrow \mathbb{N} \), we could have “listed the domain” in the order given by the range \( \dagger \). We could represent the operation of “applying a list \( v \)” to a number \( k \) in the domain of \( h \) by \((\lambda n. \text{position}(v, n))(k)\) where position gives the number corresponding to the (first) position of the number \( n \) in the list \( u \).

Then we have

\[
\text{position}(v, k) = h(k).
\]

Our representation has the advantage that it allows the representation of any finite function, not only injections and permutations.

Given a certain LISP program, different formal representation are possible. For instance, when we express our programs in the language of EKL, we can either represent them as functions or as predicates. Logically speaking, the representations are equivalent, but one should not expect the matter to be irrelevant for automatic proof checking. There are many programs computing the same function and many properties can be used to characterize them.

Sometimes it seems quite clear what we need: for instance, the operation of composition of two functions, represented as by a LISP function, should be

\[
\text{(define compose } [\forall u \ v. u@v=\text{mapcar}(\lambda i. \text{appl}(u,i),v)])
\]

or, avoiding \text{mapcar},

\[
\text{(define compose } [\forall u \ v \ x.(u@nil)=\text{nil}\wedge}
\]

\[
(u@x.v)=(\text{nth}(u,x)).(u@v) I
\]

\text{listinductiondef})
\]

\[
\text{(label composedef)}
\]

Given our definition of perm, the identity function for permutations of \( n \) elements is the list, \((1 \ldots n)\). The most obvious recursive programs generating it are represented either by

\[
\text{(decl (indent) (type: \[\text{ground}+\text{ground}\])}
\]

\[
\text{(define ident } [\forall n. \text{ident}(0)=\text{nil}\wedge}
\]

\[
\text{ident(n')}=\text{ident}(n)@\text{list}(n') I \text{inductive-definition})
\]

where \( \ast \) is the LISP function \text{append}, or by

\( \dagger \) This representation is practical only if \( h \) is indeed a permutation. If the range is not a segment of \( \mathbb{N} \), we would need some place-holder to mark the places not in the range of \( h \). and, of course, this representation doesn’t make sense if \( h \) is not 1-1.
(define identl \(\forall n. identl(0) = \text{nil} \) \(\) identl(n') = n'.identl(n) \(\) inductive-definition)

(define ident \(\forall n. ident(n) = \text{reverse}(identl(n)) \) \(\) I).

These definitions, however, need not be the best choice from the point of view of automatic proof checking. For we will try to construct proofs by induction on numbers, or lists, or both. The first definition would be all right, except that lists are defined recursively using cons, not append, so one would need some extra lemmata about append. The second definition is perhaps worse, because of the use of reverse. One can use the standard trick of introducing an auxiliary function with an extra parameter:

(defax identl \(\forall x \ u \ n. i. ident1(i,0) = \text{nil} \) \(\) ident1(i,n') = i.identl(i',n) \(\) I)

(label identdef 1)

(define ident \(\forall n. ident(n) = identl(0,n) \) \(\) I)

(label identdef)

If we want to introduce identity by a predicate, we may be tempted to follow the above definition:

(decl (identpl) (type: \(\text{ground} \ast \text{ground} \ast \text{ground} \ast \text{truthval} \))

(defax identpl \(\forall x \ u \ n. i. identpl(nil,i,n) \\ (\land \ identpl(u,i,0) \\ (\land \ identpl(x.u,i,n') = (x=i \land identpl(u,i',n))) \) \(\) I)

(label identdef 1)

(define identpl IVu.identp(u)=identpl(u,O,length(u)) I)

(label identdef)

The definition of identpl is by double recursion on numbers and lists. This complicates the subsequent inductions.

The LISP function inverse is defined using first-position by recursion on numbers:

(def ax inverse 1

|\(\forall u \ i. \ n. \ \text{inverse1}(u,i,0) = \text{nil} \\ (\land \ \text{inverse1}(nil,i,n) = \text{nil} \\ (\land \ \text{inverse1}(u,i,n') = \begin{array}{l}
\text{if} \ \text{null(first-position}(u,i)) \\
\text{then} \ \text{nil} \\
\text{else} \ \text{first-position}(u,i) \cdot \text{inverse1}(u,i',n) \end{array} \) \) \(\) I)

(label inversedef 1)

(define inverseIVu.inverse(u)=inverse1(u,0,length(u)) I)

(label inverse)

One could represent it by the predicate:

(def ax inverspl

|\(\forall u \ v \ i. \ (\text{inverspl}(nil,v,i) = \text{null}(v) \ \land \ \text{null(first-position}(v,i)) \) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\) \(\)
Notice that inverse is defined by recursion on lists. The choice of the definition of a function determines the form of induction to be used in the proofs. (For a systematic use of this remark, see Boyer and Moore [1979].) However, the principle of proof is by no means uniquely determined in this way. For instance two objects with different recursive definitions in the same statement may already produce a puzzle. Often to find the right form of induction is a nontrivial contribution required from human interaction. Consider one of our main facts, say the theorem Right Inverse:

$$\forall u. \text{perm}(u) \land u \circ \text{inverse}(u) = \text{ident}(\text{length}(u))$$

If we have defined our operations as functions, the function compose suggests that we try an induction on lists, or maybe a double induction on lists and numbers, since inverse and ident are defined by recursion on numbers. This cannot work: perm(x . u) does not imply perm(u).

We need to use induction locally, with respect to a single list. We must assume that a list is a permutation and prove facts about it by scanning it, without assuming that its sublists are permutations. Nthcdr Induction is such a local form of induction:

$$\forall \phi. \phi(u, \text{nil}) \land (\forall n. n < \text{length}(u) \rightarrow (\phi(\text{nthcdr}(u, n')) \circ \phi(\text{nth}(u, n) \circ \text{nthcdr}(u, n'))) \circ \phi(u)$$

Yet this doesn't solve our problem. Since inverse and ident are defined by recursion on numbers, a promising route is to use induction on numbers instead of lists and expand the definitions of inverse and ident.

Certainly our search for a proof strategy is not a blind process by trial and errors, guided by some limits from the definition of the objects. We have a purpose and an intuitive idea, namely to construct the identity list using the fact that for all n less than the length of u

$$\text{nth}(u, \text{fstposition}(u, n)) = n.$$ 

Indeed we have defined inverse through fstposition in order to do this. What we are searching is a strategy of proof that accomplishes it. If our search now we know that we cannot use induction on the given list u. To use induction on n seems intuitively right: our theorem asserts that two mathematical objects behave like the identity function, i.e. given a number they return the same number. Our proof should be based upon this property of the identity function.

We are satisfied with such intuitive guidelines in interactive proof checking. For the issue here is still the adequacy of representation, and not the automatic heuristics of mathematical proofs. Guided, say, by the above remarks, we will attempt to prove by induction on n

$$\text{perm}(u) \land m < \text{length}(u) \land (u \circ \text{inverse}(u, m, n)) = \text{ident}(m, n).$$

and we ask whether this is the best strategy for an effective mechanical simulation of the intuitive proof.

Further remarks may give suggestions for the kind of improvement we are interested in, namely the improvement of the efficiency of the entire proof.

Since we want to see that two lists are equal, it is natural to use the lemma. Extensionality for lists:

$$\text{length } u = \text{length } v \land (\forall i. i < \text{length } u \rightarrow \text{nth}(u, i) = \text{nth}(v, i)) \land u = v.$$
This suggests that we break the proof in two parts, proving first something about lengths and second something about $nth$ elements. Indeed, the function $nth$ may be the linking notion that allows to choose induction on numbers rather than on lists as the basic proof strategy.

If we choose to represent our operation by predicates, it is not convenient to use the predicates identpl and inverspl (although they are close to the recursive definition of our programs). It is better to define the predicate 'u is the identity' as

\[
\text{(defax id |} \forall u. \text{id}(u) = (\forall n. n < \text{length } u \exists nth(u, n) = n))
\]

and 'u is the inverse of v' as

\[
\text{(defax inv |} \forall u. \forall v. \text{inv}(u, v) = (\forall n. n < \text{length } u \exists nth(u, n) = \text{fstposition}(v, n)))
\]

Then 'u is the composition of v and w' becomes:

\[
\text{(define comp |} \forall u. \forall v. \forall w. \text{comp}(u, v, w) = \text{length } u = \text{length } w \forall (\forall n. n < \text{length } u \exists nth(u, n) = \text{nth}(v, nth(w, n))))
\]

The proof of our theorem as

\[
\forall u. \forall v. \forall w. \text{perm}(w) \land \text{inv}(u, w) \land \text{comp}(v, w, u) \land \text{length } u = \text{length } w \land \text{id}(v)
\]

then follows simply by expanding the definitions, without a need of complicated inductions.

We consider these definitions as more 'abstract and extensional'; the 'intensional' features of the programs computing our functions are abstracted away. Since $nth$ is the function that interprets our notion of application, they describe the properties of applications, together with the properties of the lists used in our representation.

Therefore, when dealing with functions instead of predicates, it is convenient, to prove these definitions as basic properties of our functions, rather than carrying through the proofs directly. We follow this strategy in the following proofs. In the representation through functions we will prove the lemmata $Nth\ Compose,\ Main\ Id,\ Main\ Inv$, showing that our functions compose, identity and inverse have the properties described by the predicates $comp, id$ and $inv$, respectively.

On the other hand, to represent the operations as primitive recursive functionals and to prove facts by the corresponding induction is in many cases the natural choice: very often representing the operations by functions, rather than by predicates, allows for simpler proofs. (An clear example is the proof that composition of permutations is associative).

In conclusion, inspection of our proof should be convincing evidence that the following strategy is the most efficient in terms of the overall organization of the material.

1) It is convenient to use the function $\text{comp}$ to represent composition of functions, for the proof of associativity is much shorter;

2) It is convenient to characterize the identity permutation by the predicate $\text{id}$ and the predicate $\text{inv}$ for the operation of inversion of permutations. We obtain elegant proofs of the properties of left and right identity and of left and right inverse.

3) Finally, we can easily prove that

\[
\forall n. \text{id}(\text{ident } n)
\]
and

\( \forall u. \text{perm}(u) \text{inv}(\text{inverse } u, u) \)

Using these facts, we can derive theorems 2 and 3 for the specific functions \textit{ident} and inverse as corollaries.

However, in order to give the most convincing evidence for the gain in efficiency obtained in this way, we will consider most of the proofs in the two formulations. Occasionally we will show also how a direct proof looks like in the representation using functions.

6.2. Definitions of Composition, Identity, Inverse.

6.2.1. Functions as Lists: Using Predicates.

;definitions of composition, identity, inverse as predicates
(proof comp_pred)

;composition of functions
1 (decl (comp) (type: [ground*ground*ground+truthval]) (syntype: constant) (bindingpower: 930))

2 (define comp
   (forall u v w. comp(u,v,w)=length u=length wA
   (forall n. n<length u nth(u,n)=nth(v, nth(w,n)))])
   (label compdef )

;the identity function
3 (decl (id) (type: [ground+truthval]))
4 (defax id \( \forall u. \text{id}(u)\equiv(\forall n. n<\text{length } u \text{nth}(u,n)=n) \))
   (label id-def )

;the inverse of a function
5 (decl (inv) (type: [ground*ground+truthval]))
6 (defax inv \( \forall u v. \text{inv}(u,v)\equiv(\forall n. n<\text{length } u \text{nth}(u,n)=\text{fstposition}(v,n)) \))
   (label invdef )

Remark. Using list representation for functions the assumption that the functions are defined on the same domain is represented by the condition that our lists have the same length. In our situation we consider permutations of a finite set. We assume that the lists are of a fixed length. We characterize \( u \) as the composition of \( v \) and \( w \) by the property

\( (\forall n. n<\text{length } u \text{nth}(u,n)=\text{nth}(v, nth(w,n))) \).

In order to speak of the composition of \( u \) and \( w \) we have to add the condition that,

\( \text{length}(u)=\text{length}(w) \).

Similarly for the inverse of a function.
6.2.2. Functions as Lists: Using Functions.

If every element of \( u \) is a number less then length(\( v \)), then it makes sense to apply \( v \) to each element of \( u \) (since we defined \( \text{appl}(v, x) \) to be \( \text{nth}(v, x) \)). In this case we may say that \( v \) is defined as a function over the domain \( u \).

(proof camp, fnct)

1. (decl def _appl (type: \( \text{I } @ u @ u @ \text{truthval} \)) )
2. (define def, appl \( \forall u \ v. \text{def_appl}(v, u) \equiv \text{allp}(\lambda x. \text{natnum}(x) \& x < \text{length}(v), u) \))
   (label def _appl_f act)

Composition of functions:

3. (decl (compose) (infixname: \( \circ \)) (type: \( \text{I } \& \text{ground} @ \text{ground} @ \text{ground} \))
   (syntype: constant) (bindingpower: 930))
4. (define compose \( \forall u \ v \ x. (u @ nil) = nil \&
   (u @ (x . v)) = (\text{nth}(u, x)) . (u @ v) \) | list induction def)
   (label composedef)

The identity function:

5. (decl (identl) (type: \( \text{I } \& \text{ground} @ \text{ground} @ \text{ground} \)))
6. (def ax identl \( \forall x \ u \ n \ \text{identl}(i, 0) = \text{nil} \&
   \text{identl}(i, n’) = \text{identl}(i’, n) \) 1)
   (label identdef 1)
7. (decl (ident) (type: \( \text{I } \& \text{ground} @ \text{ground} \)))
8. (define ident \( \forall n. \text{ident}(n) = \text{identl}(0, n) \))
   (label ident def)

The inverse of a function:

9. (decl (inversl) (type: \( \text{I } \& \text{ground} @ \text{ground} @ \text{ground} @ \text{ground} \)))
10. (def ax inversl
    \( \forall u \ i \ n. \text{inversl}(u, i, 0) = \text{nil} \& \text{inversl}(\text{nil}, i, n) = \text{nil} \&
    \text{inversl}(u, i, n’) = \text{if null(fstposition}(u, i))
    \text{then nil}
    \text{else fstposition}(u, i). \text{inversl}(u, i’, n) \) 1)
    (label inversl def 1)
11. (decl (inverse) (type: \( \text{I } \& \text{ground} @ \text{ground} \)))
12. (define inverse \( \forall u. \text{inverse}(u) = \text{inversl}(u, 0, \text{length}(u)) \))
   (label inversdef)
6.3. Preliminaries.

We collect here facts about definiteness, sort and length of the lists resulting from our operations in the representation using functions. We prove facts about concrete LISP programs that perform the operations 'composing' two lists and taking the 'inverse' of a list: hence we obtain more information than in the proofs using predicates.

Remark. The proofs of in the representation by functions require tedious computations involving the function minus. Typically, in a proof by induction on n for n<LENGTH u the induction step contains an expression like

\[
\text{LENGTH} \left( \text{INVERSE1}(u, (\text{LENGTH} u'-n'), n)\right) = n
\]

to be simplified as

\[
\text{LENGTH} \left( \text{INVERSE1}(u, \text{LENGTH} u-n, n)\right) = n
\]

Such replacement is dependent on the truth of the clause N<LENGTH U.

We have collected in the proof MINUS a sequence of facts of the form

;labels: MINUSFACT10
\[ \forall m.n < m \iff m - n = (m-n') \]

to be used as rewriters in similar cases. In fortunate situations the truth of the condition is immediately recognized by the decision procedure. Often a derivation is needed from other facts, e.g. from

;labels: LESS,LESSEQSUCC
\[ \forall n.m < n \iff m' < n \]

and we may need to do the substitution 'by brute force', with some tedious and pain.

6.3.1. Preliminaries: Condition for Definiteness and Sorts of the Functions.

The condition for v to be applicable to u as domain is formulated recursively in Def.Apl Fact.

Now we give a sufficient condition for Def.Apl Fact.

1. (assume lint0 u)
2. (assume |length u|length v|)
3. (rw -2 (open into))
   \[ \forall n. n<\text{LENGTH u} \iff \text{NATNUM(n) AND (U,N)<LENGTH U} \]
4. (trw |\forall n. n<\text{LENGTH u} \iff \text{NATNUM(n) AND (U,N)<LENGTH V} |
   (less,lesseq-fact1 -2))
   \[ \forall n. n<\text{LENGTH u} \iff \text{NATNUM(n) AND (U,N)<LENGTH V} \]
5. (ue ((phi1 |\forall x. \text{NATNUM x AND x<LENGTH v}|(u.u)) nth, allp *)
   \[ \forall x. \text{NATNUM(x) AND x<LENGTH V,U} \]
6. (trw |def_appl(v,u)| (open def_appl) *)
7. \((ci (-6 \ldots -5))\)
   \(;\text{INTO}(U)\leq \text{LENGTH} \land \text{V}\text{DEF}_-\text{APPL}(V,U)\)
   (label def\_appl\_condition)

   In particular, the same condition holds for permutations of the appropriate length.

   a. \((\text{rw} \text{def}_-\text{appl}\_condition \text{open lesseq}) \text{use normal mode: always})\)
   \(;\forall U. V. (\text{INTO}(U)\leq \text{LENGTH} \land \text{V}\text{DEF}_-\text{APPL}(V,U))\land\)
   \(;\text{INTO}(U)\leq \text{LENGTH} \land \text{V}\text{DEF}_-\text{APPL}(V,U)\))

9. \((\text{derive} \text{perm} u\text{LENGTH} u = \text{length} \text{V}\text{DEF}_-\text{APPL}(v,u))\)
   (def\_appl\_condition*) (open perm onto)
   (label def\_appl\_condition)

   We prove that the results of our operations have the right sorts.

   compose:

10. \((\text{ue} (\phi _I\text{def}_-\text{appl}(v,u)\text{listp }\forall u))\text{listinduction}
    \text{part 1} (\text{open def}_-\text{appl allp compose })))\)
    \(;\forall U. \text{DEF}_-\text{APPL}(V,U)\text{LISTP }\forall U\)
    (label sortcomp) (label simpinfo)

   ident:

11. \((\text{ue} (a _\forall n. \text{listp }\text{ident}(m,n)))\text{proof-by-induction}
    \text{open ident})\)
    \(;\forall N. \text{LISTP }\text{IDENT}(M,N)\)
    (label ident\_sort) (label simpinfo)

12. \((\text{trw }\forall n. \text{listp }\text{ident}(n))\text{open ident}\)
    \(;\forall N. \text{LISTP }\text{IDENT}(N)\)
    (label ident\_sort) (label simpinfo)

   inverse:

13. \((\text{ue} (a _\forall n. \forall i. \text{listp }\text{invers}(u,i,n)))\text{proof-by-induction}
    \text{open invers})\text{posfacts})\)
    \(;\forall N. \text{LISTP }\text{INVERS}(U,I,N)\)
    (label invers\_sort) (label simpinfo)

14. \((\text{trw }\text{listp }\text{inverse}(u))\text{open inverse}\)
    \(;\text{LISTP }\text{INVERSE}(U)\)
    (label inverse\_sort) (label simpinfo)
6.3.2. Preliminaries: Length of Compose.

**Lemma 6.1.** (Length Compose)

\[ \text{VU } W. \text{DEF_APPL}(W,U) \Rightarrow \text{LENGTH}(W \cdot U) = \text{LENGTH}(U) \]

**Proof.** By **Nthcdr Induction** applied to \( u \). For \( u = \text{NIL} \), the result is given by the definition of compose. Assume that

\[ \text{length}(w \cdot \text{nthcdr}(u,n')) = \text{length}(\text{nthcdr}(u,n')) \]

for \( n' \) less than \( \text{length}(u) \). We would like to have:

\[ \text{length}(w \cdot (\text{nth}(u,n) \cdot \text{nthcdr}(u,n'))) = \text{length}(\text{nth}(u,n) \cdot \text{nthcdr}(u,n')). \]

Since \( \text{nth}(u,n) \) is always an S-expression, we can apply the definition of compose: the left hand side becomes

\[ \text{length}(\text{nth}(w,\text{nth}(u,n)) \cdot (w \cdot \text{nthcdr}(u,n'))). \]

The inductive step will be proved if we show that the terms have proper sorts, under the assumption of line 1. Lines 3 – 9 do this.

(proof length-compose)

1. (assume \([\text{def}_\text{appl}(w,u)]\))
   (label 1_c_1)

2. (rw * (open def_appl))
   (label 1_c_2)
   ; ALLP(X:NATNUM(X)AX<LENGTH W,U)

Since \( w \) is defined as an application on \( u \) as domain (line 1), \( \text{nth}(u,n) \) is a natural number less than \( \text{length}(w) \). Therefore \( \text{nth}(w,\text{nth}(u,n)) \) is an S-expression (line 5).

3. (assume \([n<\text{length}(u)]\))
   (label 1_c_3)

4. (ue ((u.u)(x.\text{nth}(u,n)))(\text{phi1}.\lambda x.\text{natnum}(x)\wedge x<\text{length}(w))
   \text{allp_elimination}
   \cdot \text{ninthmember sexp nth 1_c_3 1_c_2)
   ; \text{NATNUM}(\text{NTH}(U,N)) \wedge \text{NTH}(U,N)<\text{LENGTH W}
   (label 1_c_4)

5. (trw \text{sexp nth}(w,\text{nth}(u,n))) \text{sexp nth 1_c_4)
   ; \text{SEXP NTH}(W,\text{NTH}(U,N))
   (label 1_c_sort1)

6. (ci 1_c_3)
   ; N<\text{LENGTH W} \cup \text{SEXP NTH}(W,\text{NTH}(U,N))
   (label 1_c_7)
Moreover, \( w \) is defined as an application on any part of \( u \), since it is defined on \( u \) (using \( \text{Allp} \) \( \text{Nthcdr} \)). Therefore, using \( \text{Sortcomp} \), we see that \( w \circ \text{nthcdr}(u, n') \) is a list.

7. (derive \( \text{allp}(\lambda x.\text{natnum}(x) \land x < \text{length } w, \text{nthcdr}(u, n')) \))
   \( \text{allp}_n(\lambda x.\text{natnum}(x) \land x < \text{length } w, \text{NTHCDR}(u, n')) \)

8. (derive \( \text{listp}(w \circ \text{nthcdr}(u, n')) \))
   (label \( 1_c \_\text{sort2} \))

9. (ci \( 1_c \_3 \))
   ; \( n < \text{LENGTH } u \ldots \text{LISTP } w \circ \text{NTHCDR}(u, n') \)
   (label \( 1_c \_8 \))

The result follows by \( \text{Nthcdr Induction} \).

10. (ue \( ((\phi.(u.\text{length}(w \circ u) = \text{length}(u)))\ |
          \text{nthcdr,induction}
       ) \))
    (part 1 (open compose \text{length} )) \( 1_c \_7 \ 1_c \_8 \)
    ; \( \text{LENGTH } (w \circ u) = \text{LENGTH } u \)

11. (ci \( 1_c \_1 \))
    ; \( \text{DEF APPL}(w, u) \circ \text{LENGTH } (w \circ u) = \text{LENGTH } u \)
    (label \text{length-compose} )

6.3.3. Preliminaries: Length of Ident.

Lemma 6.2. (Length Ident)

\[ \forall u \cdot \text{LENGTH}(\text{IDENT}(N)) = N \]

Proof.

1. (ue \( (a \ |
          \forall m.\text{length ident1}(m, n) = n) \))
   proof-by-induction
   (open \text{ident1})
   ; \( \forall m.\text{LENGTH}(\text{IDENT1}(M, N)) = N \)
   (label \text{length-ident1}) (label \text{simpinfo})

2. (trw \( \forall N.\text{LENGTH}(\text{IDENT}(N)) = N \))
   (label \text{length-ident}) (label \text{simpinfo} )

\[ \square \]
6.3.4. Preliminaries: Length of Inverse.

**Lemma 6.3.** *(Lengthinverse)*

\[ \forall u. \text{PERM}(u) \implies \text{LENGTH}(\text{INVERSE}(u)) = \text{LENGTH } u \]

**Remark. Example 8.** It may be instructive to consider the heuristics of the proof. The first problem is to find the appropriate sublemma. inverse is defined in terms of the auxiliary function inversel and the latter is defined by recursion on its third argument:

\[
\begin{align*}
\text{INVERSDEF1} & \\
VU & \text{INVERS1}(u,i,0) = \text{NIL}, \text{INVERS1}(\text{NIL},i,n) = \text{NIL} \\
\text{INVERS1}(u,i,n') = & \\
(\text{IF NULL FSTPOSITION}(u,i) & \text{ THEN NIL} \\
& \text{ ELSE FSTPOSITION}(u,i), \text{INVERS1}(u,i',n))
\end{align*}
\]

Hence it is reasonable to try a proof by induction on \( n \). The reader should see why it is not reasonable to try induction on \( u \). We assume \( \text{perm } u \) and try to prove

\[ (\forall n. n \leq \text{LENGTH } u \implies \text{LENGTH } (\text{INVERS1}(u, \text{LENGTH } u - n, n)) = n) \]

At this point we immediately see that

(i) the base case follows by expanding the definitions:

(ii) in the inductive step f stposition(\( u, \text{LENGTH } u - n' \)) will not be null since

\[ \text{LENGTH } u - n' < \text{LENGTH } u \]

and onto(\( u \)):

(iii) to apply the induction hypothesis in the inductive step we need the lemma

\[ (\forall n. n \leq \text{LENGTH } u \implies \text{LENGTH } (\text{INVERS1}(u, \text{LENGTH } u - n, n)) = n) \]

This test informs us that EKL has done the base case as expected and has expanded the definition of inversel in the induction step. In both cases of the conditional definition of inversel, t he definition of length has been expanded as desired. giving \( 0 = n' \) if

\[ (*) \quad \text{NULL FSTPOSITION}(u, \text{LENGTH } u - n') \]
and

\[(**): \text{LENGTH(INVERS1}(U, (\text{LENGTH } U - N'))') = N\]

otherwise: so the clause of the form if p then false else q has become \(\neg p \land q\).

Now we are confident that EKL will prove the negation of \((*)\), according to the argument given in (ii) above, with the information contained in \textit{Posfacts} and \textit{Minusfact11}:

;labels: SIMPINFO POSFACTS
\[
\forall U, Y. (\text{NULL FSTPOSITION}(U, Y) \land \text{MEMBER}(Y, U)) \land \text{MEMBER}(Y, U) \land \text{NATNUM}(\text{FSTPOSITION}(U, Y)) \land \text{NATNUM}(\text{FSTPOSITION}(U, Y))
\]

;labels: MINUSFACT11
\[
\forall M, N. M < N \rightarrow N - M' < N
\]

and that EKL will see that the induction hypothesis implies (**), if we add

;labels: MINUSFACT10
\[
\forall M, N. M < N \rightarrow N - M' = (M - N')'
\]

In both cases we need also

;labels: LESS, LESSEQSUC
\[
\forall M, N. M < N \rightarrow M' \leq N
\]

etc. The details of the proof follow. \(\square\)
Proof.

1. (assume |perm(u)|)
   (label li1)

2. (rw lil (open perm onto into))
   ;(∀N. N<LENGTH U) NATNUM(NTH(U,N)) ∧ NTH(U,N)<LENGTH U ∧
   ;(∀N. N<LENGTH U) MEMBER(N,U))
   (label li2)

3. (ue ((u.|ul|)(y.|ln|)) posfacts)
   ;(null FSTPOSITION(U,N) ∨ MEMBER(N,U)) ∧
   ;(MEMBER(N,U) ∨ NATNUM(FSTPOSITION(U,N)))

4. (derive |n<length u|=null fstposition(u,n)| (3 li2))
   (label li3)

5. (ue ((m.|ln|)(n.|length ul|)) minusfact11)
   (part 1 (use less,lesseqsucc mode: exact))
   ;N'<LENGTH U,(LENGTH U-N')<LENGTH U

6. (derive |n'<length u|=null fstposition(u,length u-n')|(5 li3))
   (label li4)

7. (trw |n'<length u| (length u-n')'=length u-n|
   (use minusfact10)
   (use less,lesseqsucc mode: exact direction: reverse)
   ;N'<LENGTH U,(LENGTH U-N')=LENGTH U-N

8. (ue (a |λn.|n|length u| length (invers1(u,length u-n,n))=n|)
    proof-by-induction
    (open invers1) (use succ,lesseq,lesseq) (use 7) (use li4)
    ;∀N. N<LENGTH U,LENGTH (INVERS1(U,LENGTH U-N,N))=N

9. (ue (n |length ul|) * (open lesseq))
   ;LENGTH (INVERS1(U,O,LENGTH U))=LENGTH U

10. (trw |length inverse(u)|=length ul| (open inverse) *
    ;LENGTH (INVERSE(U))=LENGTH U
    ;deps: (LI1)

11. (ci lil)
    * ;PERM(U) ∨ LENGTH (INVERSE(U))=LENGTH U

6.4. Theorem 1: Composition of Permutations.
6.4.1. Using predicates: Composition of Permutations is a Permutation.

We prove the following theorem:

**Theorem 1 (Composition)**

(i) \( VU V W \text{PERM}(V) \land \text{PERM}(W) \land \text{LENGTH} V = \text{LENGTH} W \implies \text{COMP}(U, V, W) \land \text{PERM}(U) \)

(ii) \( VU V W \text{COMP}(U, V, W) \land \text{COMP}(U', V, W) \implies U = U' \)

The proof of (i) is long but not hard.

**Proof.** Assume that \( v \) and \( w \) are permutations (lines 1 and 2), have the same length (line 3) and \( u \) is the result of 'composing' \( v \) and \( w \) (line 4). We show that

(i) \( u \) is into (line 17) and

(ii) \( u \) is onto (line 32).

(i), is a matter of expanding definitions. If \( m \) is less than the length of \( u \) (and so of \( w \) and of \( v \) ). then \( \text{nth}(w, m) \) is a natural number less than the length of \( w \) (line 10) and \( \text{nth}(v, \text{nth}(w, m)) \) is a natural number less than the length of \( v \) (line 11). But this is just \( \text{nth}(u, m) \), by the definition of composition (line 15). 'Intoness' follows.

```verbatim
;composition of permutation is a permutation
(proof comp_perm)

1. (assume \( \text{perm}(v) \) I )
   (label cp_pml)
2. (assume \( \text{perm}(w) \) I )
   (label cp_pm2)
3. (assume \( \text{length } v = \text{length } w \) )
   (label cp_pm3)
4. (assume \( \text{comp}(u, v, w) \) I )
   (label cp_pm4)

Rewrite:

5. (rw cp_pm1 (open perm into onto))
   (label cp_pm5)
   ;(\( \forall N . N < \text{LENGTH } V \implies \text{NATNUM}(\text{NTH}(V, N)) \land \text{NTH}(V, N) < \text{LENGTH } V \) )
   ;(\( \forall N . N < \text{LENGTH } V \implies \text{MEMBER}(N, V) \) )
6. (rw cp_pm2 (open perm into onto))
   (label cp_pm6)
   ;(\( \forall N . N < \text{LENGTH } W \implies \text{NATNUM}(\text{NTH}(W, N)) \land \text{NTH}(W, N) < \text{LENGTH } W \) )
   ;(\( \forall N . N < \text{LENGTH } W \implies \text{MEMBER}(N, W) \) )
7. (rw cp_pm4 (open comp ))
   (label cp_pm7)
   ;\( \text{LENGTH } U = \text{LENGTH } W \implies (\forall N . N < \text{LENGTH } U \implies \text{APPL}(V, \text{NTH}(W, N)) )\)
```

A straightforward verification.
8. (assume \(|m<\text{length}(u)\))
\((\text{label cp\_pm8})\)

9. (rw * (use cp\_pm7 mode: always))
\((\text{label cp\_pm9})\)
\;M<\text{LENGTH} W

PO. (derive \(\text{natnum}(\text{nth}(w,m))\land \text{nth}(w,m)<\text{length} v\) \((\text{cp\_pm6})\))
\((\text{use cp\_pm3 mode: exact})\)

So we can obtain the desired result...

11. (trw \(\text{NATNUM}(\text{NTH}(v,\text{NTH}(w,m)))\land \text{NTH}(v,\text{NTH}(w,m))<\text{LENGTH} v\) \((* \text{cp\_pm5})\))
\((\text{label cp\_pm10})\)

... and open appl in line 7

12. (derive \(\text{NTH}(u,m)=\text{NTH}(v,\text{NTH}(w,m))\) \((\text{cp\_pm7 cp\_pm8})\)
\((\text{open appl}) \; (\text{use -2})\))

13. (rw \text{cp\_pm10} (use * mode: exact direction: reverse))
\;\text{NATNUM}(\text{NTH}(U,M))\land \text{ANTH}(U,M)<\text{LENGTH} V
\((\text{label cp\_pm11})\)

14. (trw \(\text{length} u=\text{length} v\) \((\text{use cp\_pm7 cp\_pm3 mode: always})\)
\;\text{LENGTH} U=\text{LENGTH} V

15. (rw \text{cp\_pm11} (use * mode: exact direction: reverse))
\;\text{NATNUM}(\text{NTH}(U,M))\land \text{ANTH}(U,M)<\text{LENGTH} U
\;\text{deps: (CP\_PM1 CP\_PM2 CP\_PM3 CP\_PM4 CP\_PM8)}

16. (ci \text{cp\_pm8})
\;M<\text{LENGTH} U\land \text{NATNUM}(\text{NTH}(U,M))\land \text{ANTH}(U,M)<\text{LENGTH} U

17. (trw \(\text{into} u\) \((\text{open into}) \ast\))
\((\text{label cp\_into})\)
\;\text{INTO}(U)
\;\text{deps: (CP\_PM1 CP\_PM2 CP\_PM3 CP\_PM4)}

The second part, the proof of (ii), is slightly more complicated. Any \(m\) less than the length of \(u\) (and so of \(v\) and of \(w\)) is a member of \(v\) (line 19), since \(v\) is onto.

\* 18. (rw \text{cp\_pm9} (use cp\_pm3 mode: exact direction: reverse))
\;M<\text{LENGTH} V

19. (trw \(\text{member}(m,v)\) \((* \text{cp\_pm5})\)
\;\text{MEMBER}(M,V)
\((\text{label cp\_pm20})\)

Therefore we can find a number \(jr\) less than the length of \(v\) such that \(m\) is the \(jr\)-th element of \(v\) (line 21).
Section 6

20. (derive \( \exists j. j < |v| \) \( \text{Anth}(v, j) = m \) (\(* \text{member-nth}\))
    (label cp_pm21)
    ; deps: (CP_PM1 CP_PM3 CP_PM4 CP_PM8)

21. (define jv \( |jv| < |v| \) \( \text{Anth}(v, jv) = m \) \*)
    (label cp_pm22)

Again, since \( w \) is onto, \( jw \) is a member of \( w \) (line '23).

22. (rw \* (use cp_pm3 mode: exact))
    ; jv < \( |w| \) \( \text{WANTH}(V, jv) = M \)

23. (trw \( \text{member}(jv, w) \) \* cp_pm6))
    ; MEMBER(JV, W)

And again we can find a number \( kv \) less than the length of \( w \) such that \( jv \) is the \( kv \)-th element of \( w \) (line '25).

24. (derive \( \exists k. k < |w| \) \( \text{Anth}(w, k) = jv \) (\(* \text{member-nth}\))
    ; deps: (CP_PM1 CP_PM2 CP_PM3 CP_PM4 CP_PM8)

25. (define kv \( |kv| < |w| \) \( \text{Anth}(w, kv) = jv \) \*)
    (label cp_pm23)

So \( m \) is \( \text{nth}(v, \text{nth}(w, kv)) \) (line 24); but this is just \( \text{nth}(u, kv) \) (line SO), by the definition of composition.

26. (rw cp_pm22 (use \* mode: always direction: reverse))
    ; \( \text{nth}(w, kv) < \text{LENGTH \text{WANTH}(V, \text{nth}(W, KV)) = M} \)
    (label cp_pm24)

27. (trw \( |kv| < |u| \) | cp_pm23 (use cp_pm7 mode: always))
    ; KV < \( \text{LENGTH U} \)
    (label cp_pm25)

28. (trw \( \text{natnum nth}(w, kv) \) \* cp_pm23)
    ; \( \text{NATNUM} \text{nth}(w, KV) \)

29. (derive \( \text{nth}(u, kv) = \text{nth}(v, \text{nth}(w, kv)) \) (cp_pm7 cp_pm25)
    (open appl)(use \*)

30. (rw \* (use cp_pm24 mode: always))
    ; \text{NTH(U,KV)=M}

The last equation allows us to apply lemma \text{Nthmember} and conclude that \( m \) is a member of \text{u}.
31. (derive |member(m,u)| nthmember
   cp_pm25 (use * mode: exact direction: reverse>)
   ;deps: (CP_PM1 CP_PM2 CP_PM3 CP_PM4 CP_PM8)

32. (ci cp_pm8)
   ;M<LENGTH U|MEMBER(M,U)
   (label cp,onto)

33. (trw |perm u| (open perm onto) cp,into cp,onto)
   ;PERM(U)
   ;deps: (CP_PM1 CP_PM2 CP_PM3 CP_PM4)

34. (ci (cp_pm1 cp_pm2 cp_pm3 cp_pm4))
   ;PERM(V) PERM(W) LENGTH V = LENGTH WCOMP(U, V, W) COMP(U, W)
   (label perm_composition)

Composition of functions is unique:

35. (trw |comp(u,v,w)| comp(u1,v,w) U=U1 (open comp) extensionality)
   ;COMP(U, V, W) = COMP(U1, V, W) U=U1
   (label comp_uniqueness)

6.4.2. Using Predicates: Composition is Associative.

Finally we prove associativity:

Theorem 1 (iii) (Associativity Pred)

\[ VU U1 V VI WI W2 W3. INTO(W3) = LENGTH W2 = LENGTH W3A \]
\[ COMP(V, W1, W2) = COMP(U, V, W3) A \]
\[ COMP(V1, W2, W3) = COMP(U1, V1, W1) \]
\[ U=U1 \]

Proof. The aim is to apply extensionality. In view of an application of Extensionality (line 26), we want to prove that for all \( n < \text{length}(u) \)

\[ \text{nth}(u, n) = \text{nth}(u1, n). \]

The facts needed follow from the definitions. However, a lot of rewriting is required not only to expand definitions, but also to find the right matching (e.g. see the derivation of line 16 from lines 10 and 1.5). The decision procedure is often applied, since the definition contains a conditional clause. More specifically, we have to perform the following substitutions:

\[ \text{nth}(u, n) = \text{nth}(v, \text{nth}(w3, n)) \quad (\text{line 10}) \quad \text{if } n < \text{length}(u) \]

\[ = \text{nth}(w1, \text{nth}(w2, \text{nth}(w3, n))) \quad (\text{line 16}) \quad \text{if } \text{natnum}(\text{nth}, w3) \]
\[ \quad \text{and } \text{nth}(w3, n) < \text{length}(v) \]

\[ = \text{nth}(w1, \text{nth}(v1, n)) \quad (\text{from 16, 18}) \quad \text{if } n < \text{length}(v1) \]

\[ = \text{nth}(u1, n) \quad (\text{line 23}) \quad \text{if } n < \text{length}(u1). \]
It would take a lot of work to mechanically perform all the matching involved in these steps, if all possible substitutions had to be attempted at random. It is reasonable to expect human guidance of the proof checker. Therefore one cannot expect a proof in few lines.

This is in sharp contrast to the proof using functions, consisting of few straightforward inductions on lists and numbers.

```
(proof comp_associative)
1. (assume |into(w3)|)
   (label ca1)
2. (assume |length w2=length w3|)
   (label ca2)
3. (assume |comp(v,w1,w2)|)
   (label ca3)
4. (assume |comp(u,v,w3)|)
   (label ca4)
5. (assume |comp(v1,w2,w3)|)
   (label ca5)
6. (assume |comp(u1,w1,v1)|)
   (label ca6)
7. (assume |n<length u|)
   (label ca7)
8. (rw ca4 (open comp))
   ;LENGTH U=LENGTH W3A(VN.N<LENGTH U=NTH(U,N)=NTH(V,NTH(W3,N)))
   (label ca8)
   ;deps: (CA4)
9. (derive |n<length(w3)| (ca7 ca8))
   (label ca9)
   ;deps: (CA4 CA7)
10. (derive |nth(u,n)=nth(v,nth(w3,n))| (ca7 ca8))
    (label ca10)
    ;deps: (CA4 CA7)
11. (rw ca3 (open into))
    ;VN.N<LENGTH W3A(NATNUM(NTH(W3,N))=NTH(W3,N)<LENGTH W3
    ;deps: (CA1)
12. (derive |natnum(nth(w3,n))=nth(w3,n)<length(w2)| (ca9 * ca2))
    (label ca11)
    ;deps: (CA1 CA2 CA4 CA7)
13. (rw ca3 (open comp))
    ;LENGTH V=LENGTH W2A(VN.N<LENGTH V=NTH(V,NTH(W2,N))
    (label ca12)
```
14. (derive [nth(w3,n)<length(v)] (call ca12))
   (label ca13)
   ;deps: (CA1 CA2 CA3 CA4 CA7)

15. (derive [\forall n.n<length(v) \land nth(v,n) = nth(w1,nth(w2,n))]) ca12)
   (ue (n [nth(w3,n) I] * call ca13)
   ;NTH(V,NTH(W3,N)) = NTH(W1,NTH(W2,NTH(W3,N)))
   ;deps: (CA1 CA2 CA3 CA4 CA7)

16. (rw ca10 (use * mode: exact))
   ;NTH(U,N) = NTH(W1,NTH(W2,NTH(W3,N)))
   (label ca14)
   ;deps: (CA1 CA2 CA3 CA4 CA7)

17. (rw ca5 (open comp))
   (label ca20)
   ;LENCTH V1 = LENGTH W3 \land (\forall n. N<LENGTH V1 \land NTH(V1,n) = NTH(W2,NTH(W3,n)))

18. (derive [nth(v1,n) = nth(w2,nth(w3,n))] (ca9 ca20))
   (label ca21)
   ;deps: (CA4 CA5 CA7)

19. (rw ca6 (open comp))
   ;LENGTH U1 = LENGTH V1 \land (\forall n. N<LENGTH U1 \land NTH(U1,n) = NTH(W1,NTH(V1,n)))
   (label ca22)
   ;deps: (CA6)

20. (rw ca9 (use ca20 ca22 mode: always direction: reverse))
    ;N<LENGTH U1
    ;deps: (CA4 CA5 CA6 CA7)

21. (derive [nth(u1,n) = nth(w1,nth(v1,n))] (ca22 *))
    ;deps: (CA4 CA5 CA6 CA7)

22. (rw * (use ca21 mode: exact))
    ;NTH(U1,N) = NTH(W1,NTH(W2,NTH(W3,N)))
    (label ca23)
    ;deps: (CA4 CA5 CA6 CA7)

23. (rw ca14 (use ca23 mode: exact direction: reverse))
   * ;NTH(U,N) = NTH(U1,N)
   ;deps: (CA1 CA2 CA3 CA4 CA5 CA6 CA7)

24. (ci ca7)
   ;N<LENGTH U1 \land NTH(U,N) = NTH(U1,N)
   (label ca24)
   ;deps: (CA1 CA2 CA3 CA4 CA5 CA6)

25. (trw [length u = length u1] (use ca8 ca22 mode: always)
    (use ca20 mode: always direction: reverse))
    ;LENGTH U = LENGTH U1
    ;deps: (CA4 CA5 CA6)
26. (ue ((u.u)(v.u1)) extensionality ca24 *)
   ;U=U1
   ;deps: (CA1 CA2 CA3 CA4 CA5 CA6)

27. (ci (cal ca2 ca3 ca4 ca5 ca6))
   ;INTO(W3)ALength W2=LENGTH W3A
   ;COMP(V,W1,W2)ACOMP(U,V,W3)A
   ;COMP(V1,W2,W3)ACOMP(U1,W1,V1)U=U1
   (label associativity-pred)

6.4.3. Using Functions: the Lemma Nth Compose.

We prove first the lemma. *Nth Compose*, i.e. the basic property of composition, that was taken as definition of the predicate *comp*.

Lemma 6.4. (*Nth Compose*)

\[ \forall U N \, \text{DEF}_\text{APPL}(V,U) \land N < \text{LENGTH} \Rightarrow \text{U} = \text{NTH}(V \bullet U, N) = \text{NTH}(V, \text{NTH}(U, N)) \]

Proof. By double induction on \( n \) and \( n' \):

(proof *nth-compose*)

;labels: DOUBLEINDUCTION
; (\( \forall U N \, \text{X} \phi_3(T(NIL, N), \phi_3(U, 0), \phi_3(U, N)) \))
; (\( \forall U N \, \phi_3(U, N) \))

One base-case is proved by listinduction:

1. (ue (phi [\lambda u. n \text{null}(u) \land \text{def} _\text{appl}(v, u) \land \text{nth}(v \bullet u, 0) = \text{nth}(v, \text{nth}(u, 0))])
   listinduction
   (part 1 (open compose nth def_appl allp))
   ;\( \forall U \text{-null} U \text{def}_\text{appl}(V, U) \land \text{CAR}(V \bullet U) = \text{NTH}(V, \text{CAR} U) \)
   (label a-c-base1)

...and the other is trivial. So:

2. (ue (phi [\lambda u. n \text{def} _\text{appl}(v, u) \land n < \text{LENGTH} \land \text{nth}(v \bullet u, n) = \text{nth}(v, \text{nth}(u, n))])
   doubleinduction
   (part 1 (open compose def_appl allp)) a-c-base1)
   ;\( \forall U \text{def}_\text{appl}(V, U) \land n < \text{LENGTH} \land \text{U} = \text{NTH}(V \bullet U, N) = \text{NTH}(V, \text{NTH}(U, N)) \)
   (label nth-compose)

Exercise. Prove Theorem 1 in the representation by functions

\[ \forall U V \text{PERM} U \land \text{PERM} V \land \text{LENGTH} U = \text{LENGTH} V \land \text{PERM}(U \bullet V) \]

wing directly Theorem 1 (Composition)

\[ \forall U V W \text{PERM}(V) \land \text{PERM}(W) \land \text{LENGTH} V = \text{LENGTH} W \land \text{COMP}(U, V, W) \land \text{PERM}(U) \]

Theorem 1 (i) (Perm Compose)

\[ \text{Perm}(\text{VU, V.PERM U A, PERM V, 3LENGTH U = LENGTH V C PERM(U@V))} \]

The proof is basically the same as in Section 6.4.1. It can be found in the Appendix.

Theorem 1 (ii) (Associativity of Composition)

\[ \text{Perm(VU, V.W.PERM(V)A, PERM(U)A, LENGTH V=LENGTH UALENGTH W=LENGTH U@)C (W@V)@U=W@(V@U)} \]

Proof of (ii) By listinduction on U:

(proof assoc,compose)

1. \([\text{trw def_appl(w,v)Adef_appl(v,u)C(w@v)@nil=w@(v@nil)}>\]
   \(\text{open compose) sort comp}\)
   \(\text{label ass_comp_base}\)

2. \(\text{ue (phi (lambda u.def_appl(w,v)Adef_appl(v,u)C(w@v)@u=w@(v@u)>)}\]
   \(\text{list induction}\)
   \(\text{part 1#2 (open compose def,appl allp)) sort comp ass-camp,base}\)
   \(\text{use nth,compose ue: } ((\text{v.w})(\text{u.v})) )\)
   \(\text{;VU.DEF_APPL(W,V)ADEF_APPL(V,U)C(W@V)@U=W@(V@U)}\)
   \(\text{label assoc,camp)}\)

In particular, the conditions of definedness are satisfied if u and v are permutations of the

3. \([\text{trw |\text{def_appl(w,v)Adef_appl(v,u)C(w@v)@u=w@(v@u)}>|\text{assoc,comp}\}
   \(\text{use def_appl,condition1 ue: } ((\text{u.u})(\text{v.v})) )\)
   \(\text{use def_appl,condition1 ue: } ((\text{u.v})(\text{v.w})) )\)
   \(\text{;VU.V.W.PERM(V)A, PERM(U)A,LENGTH V=LENGTH UALENGTH W=LENGTH U@)C (W@V)@U=W@(V@U)}\)
   \(\text{(label associativity, of -composition) }\)

Compare with the corresponding result using predicates (Section 6.4.2). An explanation why
this proof is much simpler is: both compose and def-appl have a simple definition by recursion
on lists. The lemma and the theorem can be proved by a straightforward double induction on lists
and numbers. On the other hand, when composition is defined as a predicate, a lot, of rewriting is
required to expand the definitions and to perform the right substitutions, and the decision procedure
is often applied to justify conditional rewriting. This cannot be done in a few lines.

6.5. Theorem 2: The Identity Permutation.
6.5.1. Using Predicates.

We have the following theorem about identity:

**Theorem 2** (i) *(Id Perm)*

\[ \forall U. \text{ID}(U) \supset \text{PERM}(U) \]

**Proof.** Intoness:

1. \( \text{(trw \{id(u)\} into(u)\}) \) (open id into)
   \( \text{ID}(U) \supset \text{INTO}(U) \)
   (label p_i1)

Ontoness:

1. (assume \( \text{id}(u) \))
   (label p_i2)

3. (\( \text{rw } * \) (open id))
   \( \forall N.N < \text{LENGTH} \ U \text{NTH}(U,N) = N \)
   (label p_i3)

4. (assume \( N < \text{length } u \))
   (label p_i4)

5. (\( \text{derive } \text{MEMBER}(\text{nth}(u,n),u)\) (\( \text{o nthmember} \))

6. (\( \text{derive } \text{MEMBER}(n,u)\) (\( \text{* p_i4 p_i3} \))

7. (\( \text{ci p_i4} \))
   \( N < \text{LENGTH} \ U \text{MEMBER}(N,U) \)

8. (\( \text{derive } \text{PERM } u \) (\( \text{p_i1 p_i2} * \) (open perm onto))

9. (\( \text{ci p_i2} \))
   \( \text{ID}(U) \supset \text{PERM}(U) \)
   (label id-perm) \]

Right and left identity are also easy consequences of the definitions

**Theorem 2** (ii) *(Right Id)*

\[ \forall U \forall W. \text{ID}(U) \supset \text{ACOMP}(V,W,U) \supset \text{LENGTH } W = \text{LENGTH } U \supset V = W \]
Proof.

(proof identity-right)

1. (assume |id(u)|)
   (label id-1)

2. (assume |comp(v,w,u)|)
   (label id-r2)

3. (assume |length w=|l|length ul|)
   (label id-r3)

4. (rw id-r1 (open id))
   ;\forall n<|length ul\rangle |nth(u,n)|=n
   (label id-r4)

5. (rw id-r2 (open comp))
   ;|length v=|length ul\rangle |nth(u,n)|=n
   (label id-r5)

6. (rw * (use id-r4 mode: always))
   ;|length v=|length ul\rangle |nth(u,n)|=n
   (label id-r6)

7. (trw |length v=|length w| (use id-r3 id-r5 mode: always))
   ;|length v=|length w|
   a. (derive |v=w| (extensionality id-r6 *))

9. (ci (id-r1 id-r2 id-r3))
   ;|id(u)\&comp(v,w,u)|=|length ul\rangle |nth(u,n)|=n
   (label id-right) ■

**Theorem 2 (iii) (Left Id)**

\[ V U V W. |id(u)\&perm(w)|\&|length w=|length ul\rangle |nth(u,n)|=n \]

Proof.

(proof identity-left)

-1. (assume lid(u))
   (label id-11)

2. (assume |perm w|)
   (label id-12)

3. (assume |length w=|length ul|)
   (label id-13)

4. (assume |comp(v,u,w)|)
   (label id-14)
5. \((\text{rw id-11 (open id)})\)
\[\forall N < \text{LENGTH } U \land \text{NTH}(U, N) = N\]
\((\text{label id-15})\)

6. \((\text{rw id-14 (open comp)})\)
\[\text{LENGTH} V = \text{LENGTH} W \land (\forall N < \text{LENGTH } V \land \text{NTH}(V, N) = \text{NTH}(U, \text{NTH}(W, N)))\]
\((\text{label id-16})\)

7. \((\text{rw id-12 (open perm onto into)})\)
\[\forall N < \text{LENGTH } W \land \text{NTH}(W, N) \leq \text{NTH}(W, N) < \text{LENGTH } W \land (\forall N < \text{LENGTH } W \land \text{MEMBER}(N, W))\]
\((\text{label id-17})\)

8. \((\text{trw } |\forall m < \text{length } \text{U} \land \text{NTH}(W, m)\rangle \land \text{NTH}(W, m) < \text{length } U | \text{id-17})\)
\((\text{use id-13 mode: exact direction: reverse})\)
\[\forall M < \text{LENGTH } W \land \text{NTH}(W, m) \leq \text{NTH}(W, m) < \text{LENGTH } U\]
\((\text{label id-18})\)

We can apply the property of the identity function \(u\)

9. \((\text{trw } |\forall m < \text{length } \text{U} \land \text{NTH}(W, m)\rangle \land \text{NTH}(W, m) < \text{length } U | \text{id-15} \ast\)
\[\forall M < \text{LENGTH } W \land \text{NTH}(W, m) \leq \text{NTH}(W, m) < \text{LENGTH } U\]
\((\text{label id-19})\)

We will use extensionality

10. \((\text{assume } |m < \text{length } V|)\)
\((\text{label id-10})\)

11. \((\text{trw } |m < \text{length } U| \ast\)
\((\text{use id-13 mode: exact direction: reverse})\)
\[; M < \text{LENGTH } U\]
\((\text{label id-11})\)

12. \((\text{derive } |\text{NTH}(U, \text{NTH}(W, m))\rangle \land \text{NTH}(W, m) < \text{length } U | \text{id-19 id-111})\)

We use the fact that \(v\) is the composition of \(u\) and \(w\)

13. \((\text{derive } |\text{NTH}(V, m)\rangle \land \text{NTH}(W, m) < \text{length } U | \text{id-16 id-110})\)
\((\text{use } \ast \text{ mode: exact direction: reverse})\)

14. \((\text{ci id-110})\)
\[; M < \text{LENGTH } V \land \text{NTH}(V, m) = \text{NTH}(W, m)\]

15. \((\text{derive } |w = v| (\text{extensionality id-16 } \ast))\)

16. \((\text{ci id-11 id-12 id-13 id-14})\)
\[; \text{ID}(U) \land \text{PERM}(W) \land \text{LENGTH } W = \text{LENGTH } U \land \text{COMP}(V, U, W) \land W = V\]
\((\text{label id-left})\)
6.5.2. Using Functions: the Lemma Main Id.

The main result about the 'identity' list is the extensional property that was assumed as definition of id.

Lemma 6.5. (Main Id)

\[ \forall n. n < m \iff (\text{Ident}(m), n) = n. \]

Proof. First we show the following fact, \( \text{Nthcdr Ident} \), by induction on \( n \):

\[ \forall n. n < m \iff \text{Nthcdr}(\text{ident}(m), n) = \text{ident}(n, m - n) \]

(line 8). The lemma then follows easily.

(proof id-main)

1. (assume \( n < m \iff \text{Nthcdr}(\text{ident}(m), n) = \text{ident}(n, m - n) \))

(label id-main1)

2. (assume \( n' < m \))

(label id-main2)

3. (derive \( \text{Nthcdr}(\text{ident}(m), n) = \text{ident}(n, m - n) \)

   (id-main1 id-main2 succ_less_less))

; deps: (ID_MAIN1 ID_MAIN2)

Now we use \( \text{Minusfact10} \) to expand the definition of identl in the right member of the equality.

; labels: MINUSFACT10
; \( \forall n. n < m \iff m - n = (m - n') ' \)

4. (rw * (use minusfact10 mode: exact) (open identl)

   (use id-main2 succ_less_less mode: exact))

; NTHCDR(\text{IDENT}(m), n) = \text{IDENT}(n', m - n')

; deps: (ID_MAIN1 ID_MAIN2)

The inductive step is concluded by the use of \( \text{Cdr Nthcdr} \)

; labels: CDR,NTHCDR
; \( \forall n. \text{CDR} \iff \text{NTHCDR}(U, N) = \text{NTHCDR}(U, N') \)

5. (trw \( \text{Nthcdr}(\text{ident m}, n') \))

   (use cdr,nthcdr mode: exact direction: reverse)

   (use * mode: exact))

; NTHCDR(\text{IDENT}(m), N') = \text{IDENT}(N', m - N')

6. (ci id-main2)

; \( n' < m \iff \text{NTHCDR}(\text{IDENT}(m), n') = \text{IDENT}(n', m - n') \)

7. (ci id-main1)

; \( n < m \iff \text{NTHCDR}(\text{IDENT}(m), n) = \text{IDENT}(n, m - n) \))

; \( n' < m \iff \text{NTHCDR}(\text{IDENT}(m), n') = \text{IDENT}(n', m - n') \))
To finish the proof of the lemma we use again Minusfact10...

..and then apply Car Nthcdr. In this last step we use the information about the length of the ident function (see Section 6.3.3) in simpinfo.

Exercise. Prove Theorem 2 in the representation by functions

\[ \forall U.V \cdot IDENT(\text{LENGTH } U) = U \]

\[ \forall U.V \cdot \text{INTO}(U) \cdot IDENT(\text{LENGTH } U) \cdot U = U \]

using directly Theorem 2 (ii) (Right Id) and (iii) (Left Id)

\[ \forall U.V.W.ID(U) \cdot \text{ACOMP}(V, W, U) \cdot \text{LENGTH } W = \text{LENGTH } U \cdot V = W \]

\[ \forall U.V.W.ID(U) \cdot \text{APERM}(W) \cdot \text{LENGTH } W = \text{LENGTH } U \cdot \text{ACOMP}(V, U, W) \cdot W = V \]

6.5.3. Using Functions: Identity is a Permutation.

Using the above lemma, it easy to prove that the 'identity' list is a permutation, following the pattern of the proofs in Section 6.5.1.

Theorem 2 (i) (Perm Ident)

\[ \forall N.\text{PERM}(\text{IDENT}(N)) \]
Proof.

\((\text{proof perm_ident})\)

;only ontoness requires some help

1. (assume \(|n<\text{length ident}(m)|\)
    (label \(\text{prm}, \text{idl}2\))

2. (\((\text{rw } \ast (\text{open ident}))\)
    \(\mid N<M\)
    (label \(\text{prm}_2\))

Again notice that the fact \(\text{Length Ident}:\)

\(\forall N. \text{LENGTH (IDENT(N))}=N\)

is in simpinfo.

3. (\((\text{derive } |N\text{TH IDENT(M),N}=N| (\ast \text{id-main})\))

4. *(\((\text{derive } |\text{member(nth(ident m,n),ident m)}|\)
    (nthmember \(\text{prm}, \text{idl}\) ) )

5. (\((\text{rw } \ast (\text{use -2 mode: exact})\)
    \(\mid \text{MEMBER(N,IDENT(M))}\)

6. (\((\text{ci } \text{prm}_1)\)
    \(\mid N>M\))\text{MEMBER(N,IDENT(M))} .

7. (\((\text{trw } |\forall n.\text{perm(ident n)}| (\text{open perm into onto})\)
    (use id-main mode: always) \ast )
    \(\mid \forall N.\text{PERM(IDENT(N))}\)
    (\(\text{label } \text{perm_ident}\) )

6.5.4. Using Functions: Right Identity.

Using the lemma \(\text{Main Id}\) it is also easy to show that \text{ident} gives the right identity.

**Theorem 2** (ii) (Right Identity)

\(\forall U. U \circ \text{IDENT(LENGTH U)}=U\)

**Remark. Example 9.** We give two proofs of this Theorem, as evidence of our claim that a presentation through abstract lemmata (Proof 1) is more convenient than direct verification (Proof 2). The convenience is not simply in the fact that the first proof is shorter than the second: rather it lies in that we use the lemmata \(N\text{th Compose}\) and \(\text{Main Id}\), having many other applications, instead of proving a lemma, of interest only in this contest.
First Proof.

(proof identity-right)

1. (rw perm.id (open perm onto))
   \[ \forall W.\text{INTO}(\text{id}(N)) \land \neg W.\text{MEMBER}(N,\text{id}(N)) \]
   ;labels: DEF, APPL, CONDITION
   ;\forall V.\text{INTO}(V) \land \text{LENGTH} V = \text{DEF_APPL}(V, U)

2. (ue ((u.|ident(length u)|)(v.u))
   def, appl, condition * (open lesseq)
   ;\text{DEF_APPL}(U,\text{id}(\text{LENGTH} U))

   ;labels: NTH, COMPOSE
   ;\forall V.\text{NTH}(V,\text{IDENT}(\text{LENGTH} U)) = \text{NTH}(V,\text{NTH}(U, N))

3. (ue ((u.|ident(length u)|)(v.u)(n.n)) nth_compose *
   (use id-main mode: exact)
   ;N < \text{LENGTH} U \land \text{NTH}(U, N) = \text{NTH}(U, N)

   ;labels: EXTENSIONALITY
   ;\forall V.\text{LENGTH} U = \text{LENGTH} V \land \forall I.1 < \text{LENGTH} U \land \text{APPL}(U, I) = \text{APPL}(V, I) \lor U = V

4. (ue ((u.|u|ident(length u)|)(v.u)) extensionality (open appl)
   (use length-compose -2 *)
   ;U \land \text{IDENT}(\text{LENGTH} U) = U

Notice that this proof is the same as that given in Section 6.5.1.

Second Proof. Without using the main lemma, we can prove Right Identity by proving first

\[ \forall n. n \leq \text{length} u \land u \ast \text{id}(\text{length} u-n, n) = \text{nthcdr}(u, \text{length} u-n) \]

(proof identity-right)

1. (ue ((u.u)(n.|length ul)) trivial-nthcdr (open lesseq))
   ;\text{NTHCDR}(U, \text{LENGTH} U) = \text{NIL}

2. (trw |u|ident1(length u, 0) = NTHCDR(u, length u) | (open ident1 compose)
   (use * mode: exact))
   ;U \ast \text{id}(\text{LENGTH} U, O) = \text{NTHCDR}(U, \text{LENGTH} U)
   (label ir1)

3. (assume ln|length(u)|u|ident1(length u-n,n)=nthcdr(u,length u-n) |)
   (label ir-hyp)

4. (assume \n'n < \text{length} u | (label ir2)

5. (derive \u|ident1(length u-n,n)=nthcdr(u,length u-n) |)
   (ir-hyp ir2 succ_lesseq_lesseq)
   (label ir3)

6. (derive |\text{length} u-(n') < \text{length} u | (minusfact1 less-lesseq succ ir2))
6.5.5. Using Functions: Left Identity.

Similarly, by applying the Main Lemma for Identity, we can prove that \texttt{ident} gives the left identity by following the pattern of the proof in Section 6.5.1.

\textbf{Theorem 2} (iii) (Left Identity)

\[ \forall u. \text{INTO}(u) \cdot \text{IDENT}[length \ u] \cdot u = u \]

\textbf{Proof.}

(proof identity-left)

1. (assume lint0 u)
   (label il_1)

2. (ue ((u.u)(v. |ident(length u)|)))
   \texttt{def.appl.condition}
   * (open \texttt{lesseq})
   :DEF.APPL(\texttt{IDENT[length \ u]}, u)

\[ \square \]
It is completely clear that, by abstracting the main property of identity, we obtain a uniform treatment of all the parts of theorem 2 and greatly simplify the proofs. Actually the present version is even more elegant than that using predicates, since the expression \( u \circ w \) is easier to read than \( \text{comp}(v, u, w) \) (for humans as well as for computer programs).

6.6. Theorem 3: the Inverse of a Permutation.

6.6.1. Using Predicates: the Inverse of a Permutation is a Permutation.

**Theorem 3 (i) (InvPerm)**

\[ \forall U \ V. \ \text{PERM}(U) \ \text{AINV}(V, U) \ \text{ALENGTH} \ V = \text{LENGTH} \ U \ \text{PERM}(V) \]

The proof of this theorem is obtained by expanding the definitions and making appropriate substitutions, in the style of Theorems 1 (i) and 2 (i). We give it in the Appendix.


**Theorem 3 (ii) (Right Inverse)**

\[ \forall U \ V \ W. \ \text{PERM}(W) \ \text{AINV}(U, W) \ \text{ACOMP}(V, W, U) \ \text{ALENGTH} \ U = \text{LENGTH} \ W \ \text{WID}(V) \]

**Proof.** Assume that \( w \) is a permutation (line 1), \( v \) is the result of composing \( w \) and \( u \) (line 4), where \( u \) is the inverse of \( w \) (line 2), and \( u \) is of the same length as \( w \) (line 3). We need to see that for all \( m < \text{length}(v) \), \( \text{nth}(v, m) = m \) (line 14).

The key point is the application of the lemma \( \text{NthFstposition}(\text{l}3) \). To prepare it, we have only to expand the definitions and perform the right substitutions.
\[\text{nth}(v, m) = \text{nth}(w, \text{nth}(u, m)) \quad \text{(by line 7)} \quad \text{if } m < \text{length}(v) = \text{length}(u)\]

\[= \text{nth}(w, \text{fstposition}(w, m)) \quad \text{(line 10)}\]

\[= m \quad \text{(line 13)}\]

; the theorem right inverse
(proof inverse-right)

1. (assume \text{perm}(w))
   (label invrl)

2. (assume \text{inv}(u, w))
   (label invr2)

3. (assume \text{length}(u) = \text{length}(w))
   (label invr3)

4. (assume \text{comp}(v, w, u))
   (label invr4)

5. (rw invrl (open perm onto into))
   ; (\forall N. N < \text{length } w \land \text{natnum}(\text{nth}(w, N)) \land \text{nth}(w, N) < \text{length } w) \land
   ; (\forall N. N < \text{length } w \land \text{member}(N, w))
   (label invr5)

6. (rw invr2 (open inv))
   ; (\forall N. N < \text{length } u \land \text{nth}(u, N) = \text{fstposition}(w, N))
   (label invr6)

7. (rw invr4 (open comp))
   ; \text{length } v = \text{length } u \land (\forall N. N < \text{length } u \land \text{nth}(v, N) = \text{nth}(w, \text{nth}(u, N)))
   (label invr7)

8. (assume \text{m < length } v)
   (label invr8)

9. (rw * (use invr7 mode: exact))
   ; \text{m < length } u
   (label invr9)

10. (trw \text{nth}(v, m) = \text{nth}(w, \text{fstposition}(w, m))) (invr7 *)
    (use invr6 mode: always direction: reverse)
    ; \text{nth}(V, M) = \text{nth}(W, \text{fstposition}(W, M))
    (label invr10)

11. (rw invr9 (use invr3 mode: exact))
    ; \text{m < length } w

12. (derive \text{member}(m, w)) (invr5 *)
    ; labels: \text{NTH\_FSTPOSITION}

**Theorem**3 (iii) (*LeftInv*)

\[ \forall U \ V \ W. \text{PERM}(w) \ \text{AINV}(u,w) \ \text{ACOMP}(v,u,w) \ \text{ALENGTH} \ W=\text{LENGTH} \ U \ \text{ID}(V) \]

**Proof.** Assume that \( u \) is the inverse of \( w \), \( v \) is the result of composing \( u \) and \( w \), and the length \( w = \text{length}(u) \). We need to prove that

\[ \forall n. n < \text{length}(v) \ \text{NTH}(v, n) = n. \]

Assume that \( n < \text{length}(v) \). After expanding the definitions we know that

\[ \text{length}(v) = \text{length}(w), \]

so \( n < \text{length}(w) \) and \( n < \text{length}(u) \). Similarly, all members of \( w \) are natural numbers less than \( \text{length}(u) \) (lines 9, 13). So the sorts are verified and we can apply the definition of composition to get

\[ \text{NTH}(v, n) = \text{NTH}(u, \text{NTH}(w, n)) \]

(line 14), and the definition of inverse to obtain

\[ \text{NTH}(u \circ w, n) = \text{FSTPOSITION}(w, \text{NTH}(w, n)) \]

(line 15).

We want to conclude that

\[ \text{FSTPOSITION}(w, \text{NTH}(w, n)) = n. \]

This need not be true if \( w \) there are several occurrences of the \( n \)-th element. However, \( w \) is a permutation. By the pigeon hole principle \( w \) is injective; we can apply the lemma \( \text{FSTPOSITIONNTH} \) (lines 8, 16) and obtain the desired conclusion (line 19).
I. (proof compose-inverse-left)
   (assume \( |\text{perm}(w)| \))
   (label invl,1)

2. (assume \( |\text{inv}(u,w)| \))
   (label invl,2)

3. (assume \( |\text{comp}(v,u,w)| \))
   (label invl,3)

4. (assume \( |\text{length}(w) = \text{length}(u)| \))
   (label invl,4)

5. (rw invl,2 (open inv))
   \( \forall n. \text{length} u \cap \text{nth}(u,n) = \text{fstposition}(w,n) \)
   (label invl,5)

6. (rw invl,1 (open perm onto into))
   \( \forall n. \text{length} u \cap \text{nth}(u,n) \land \text{nth}(w,n) < \text{length} w \) 
   \( \land \forall n. \text{length} w \cap \text{member}(n,w) \)
   (label invl,6)
   ;deps: (INVL, I)

7. (rw invl,3 (open comp))
   \( \text{length} v = \text{length} w \cap \forall n. \text{length} v \cap \text{nth}(v,n) = \text{nth}(u, \text{nth}(w,n)) \)
   (label invl,7)

8. (derive \( \forall n. \text{length} w \cap \text{fstposition}(w, \text{nth}(w,n)) = n \) )
   (fstposition, nth perm, injectivity uniqueness injectivity
   invl, I invl, 6)
   (label invl, 8)
   ;deps: (INVL, I)

9. (rw invl, 6 (use invl, 4 mode: exact))
   \( \forall n. \text{length} u \cap \text{natnum}(\text{nth}(w,n)) \cap \text{nth}(w,n) < \text{length} u \) 
   \( \land \forall n. \text{length} w \cap \text{member}(n,w) \)
   (label invl, 9)
   ;deps: (INVL, I INVL_4)

10. (assume \( n < \text{length} v \) )
    (label invl, IO)

11. (rw \* (use invl, 7 mode: always))
    \( n < \text{length} w \)
    (label invl, II)
    ;deps: (INVL, 3 INVL, IO)

12. (rw \* invl, 4)
    \( n < \text{length} u \)
    (label invl_12)
    ;deps: (INVL, 3 INVL, 4 INVL, IO)

13. (derive \( \text{natnum}(\text{nth}(w,n)) \land \text{nth}(w,n) < \text{length} u \) (invl, 9 \*))
    (label invl, 13)
6.6.4. Using Functions: the Lemma Main Inv.

We follow the same strategy for the proof of the facts about the inverse operation. First we prove the main extensional property of inverse (compare with the definition of inv, Section 6.2.1):

**Lemma 6.6. (Main Inv)**

\[ \langle V, U \rangle \in \text{PERM} \land V < \text{LENGTH} \implies \langle \text{INVERSE}(U, N), NK = \text{FSTPOSITION}(U, N) \]

- and then we follow the proof of Theorem 3 in Sections 6.6.1, 6.6.2 and 6.6.3.

**Proof of the Main Lemma.** We show first that if \( u \) is a permutation, then

\[ \forall n. n < \text{LENGTH} \implies \text{nthcdr}(\text{inverse}(u), n) = \text{inverse1}(u, n, \text{LENGTH} u - n). \]

(proof inverse-main)

1. (assume \(|\text{perm } u|\))
   (label inv_main1)
We need to check that \( f \) stposition has the proper value on the intended domain.

2. (rw inv_main1 (open perm onto))
   ; INTO(U)\( \forall N. N < \text{LENGTH } U \supset \text{MEMBER}(N, U) \)
   (label inv_main2)

3. (ue ((u. u)(y. n)) posfacts)
   ; (\text{NULL} FSTPOSITION(U, N) \supset \text{MEMBER}(N, U) \supset 
   ; (\text{MEMBER}(N, U) \supset \text{NATNUM}(\text{FSTPOSITION}(U, N)))

4. (derive |n<length u\( \cap \) null fstposition(u, n)| (inv_main2 *))
   (label inv_main3)

Next we give the inductive argument for our sublemma:

5. (assume |n<length u\( \cap \) nthcdr(inverse(u), n)=inverse1(u, n, length u-n) |)
   (label inv_main5)

6. (assume |n'<length u|)
   (label inv_main6)

7. (derive |n<length u| (* succ, less-less))
   (label inv_main7)

8. (derive |\text{null} fstposition(u, n)| (inv_main3 inv_main7))
   (label inv_main9)

We use Minusfact10 to expand the definition of inverse1 in the right member of the equality.

9. (rw inv_main5
    (use inv_main7 inv_main9)(open inverse1)
    (use minusf act IO mode: always))
   (label inv_main10)
   ; \text{NTHCDR}(\text{INVERSE}(U), N) = \text{FSTPOSITION}(U, N). \text{INVERSE}(U, N', \text{LENGTH } U-N')
   ; deps: (INV, MAIN1 INV, MAIN5 INV, MAIN6)

We use Cdr Nthcdr to conclude the inductive step:

; labels: CDR_NTHCDR
; \text{VU } N. CDR_NTHCDR(U, N) = NTHCDR(U, N')

10. (ue ((u. inverse u)(n. n)) cdr_nthcdr (use * mode: exact))
    ; INVERSE1(U, N', LENGTH U-N') = NTHCDR(INVERSE(U), N')
    ; deps: (INV, MAIN1 INV, MAIN5 INV, MAIN6)

11. (ci inv_main6)
    ; N'<LENGTH U \text{INVERSE}(U, N', LENGTH U-N') = NTHCDR(INVERSE(U), N')

12. (ci inv_main5)

13. (ue (a |n. n<length u\( \cap \) nthcdr(inverse(u), n)=inverse1(u, n, length u-n) |)
    proof-by-induction (part ID1 (open inverse minus)) * )
    ; \text{VU } N. N<LENGTH U \text{NTHCDR}(\text{INVERSE}(U), N) = \text{INVERSE}(U, N, \text{LENGTH } U-N)
    ; deps: (INV, MAIN1)
The main lemma follows. We use again Minusfact10 to expand the definition of invers1...

14. \((\text{rw} \ star \ (\text{use minusfact10 \ mode: \ exact}) \ (\text{open invers1})
\ (\text{use inv_main3 \ mode: \ always}))
\;\forall \;N<\text{LENGTH \ U}\)
\;\text{NTHCDR(\text{INVERSE}(U),N) = \text{FSTPOSITION}(U,N) . \text{INVERS1}(U,N',\text{LENGTH}U-N')}
\;\text{deps: (INV_MAIN1)}

...and then Car Nthcdr.

\;\text{labels: \text{CAR-NTHCDR}}
\;\forall \;U \;N<\text{LENGTH U} \\text{CAR NTHCDR}(U,N) = \text{NTH}(U,N)

15. \((\text{ue} ((\text{u.linverse(u)}))(n.n)) \text{ car-nthcdr}
\ (\text{use \ star \ lengthinverse \ inv_main1 \ mode: \ always}))
\;\forall \;N<\text{LENGTH U} \\text{FSTPOSITION}(U,N) = \text{NTH(\text{INVERSE}(U),N)}
\;\text{deps: (INV_MAIN1)}

16. \((\text{ci inv_main1})
\;\forall \;\text{PERM(U)} \\forall \;N<\text{LENGTH U} \\text{FSTPOSITION}(U,N) = \text{NTH(\text{INVERSE}(U),N)}

17. \((\text{derive} \forall \;u \;n.\text{perm} \;u \text{AN}<\text{LENGTH} \;u \text{N} \text{th(inverse} \;u,\;n) = \text{fstposition(u,n)} \;\text{I} \;\star \;)
\;\text{(label \ inv,main) \ I}

Exercise. Prove Theorem 3 in the representation by functions

\forall \;U . \text{PERM(U) ContINVERSE(U) = IDENT(LENGTH(U))}
\forall \;U . \text{PERM(U) ContINVERSE U U = IDENT(LENGTH U)}

using directly Theorem 3 (ii) (RightInverse) and (iii) (LeftInv)

\forall \;V \;W . \text{PERM(W) ContINVERSE(U, W) ContCOMP(V, W, U) ContLENGTH U = LENGTH W ContID(V)}
\forall \;V \;W . \text{PERM(W) ContINVERSE(U, W) ContCOMP(V, U, W) ContLENGTH W = LENGTH U ContID(V)}

6.6.5. Using Functions: the Inverse of a Permutation is a Permutation.

Theorem3(i) (PermInverse)
\forall \;U . \text{PERM(U) ContPERM(INVERSE U)}

Theorem3(ii) (RightInverse)
\forall \;U . \text{PERM(U) ContINVERSE(U) = IDENT(LENGTH(U))}

Theorem3(iii) (LeftInverse)
\forall \;U . \text{PERM(U) ContINVERSE U U = IDENT(LENGTH U)}
Proof of Theorem 3 (i). The first part of the theorem is the proof of the following fact. Inv INTO:

\[ \forall U. \text{PERM}(U) \rightarrow \text{INTO}(\text{INVERSE}(U)) \]
(proof inverse-perm)

1. (assume |perm(u)|)
   (label inv,pl)

2. (rw * (open perm onto))
   \( \rightarrow \text{INTO}(U) \land (\forall N. N < \text{LENGTH } U \land \text{MEMBER}(N, U)) \)
   (label inv,p2)

3. (ue ((u.u)(y.n)) posfacts)
   \( (\text{NULL FSTPOSITION}(U, N) \rightarrow \text{MEMBER}(N, U)) \land \)\( (\text{MEMBER}(N, U) \rightarrow \text{NATNUM}(\text{FSTPOSITION}(U, N))) \)

4. (derive \{v.n.n<length u\}
   \text{natnum fstposition(u,n)=fstposition(u,n)<length u}\)
   (inv_p2 * pos_length))
   (label inv,p3)

5. (derive \{v.n.n<length u\}
   \text{nth(inverse(u,n))=fstposition(u,n)}\)
   (inv,main inv,pl))
   (label inv_p4)

6. (rw inv_p3 (use * mode: always direction: reverse))
   \( \forall N. N < \text{LENGTH } U \land \text{NATNUM}(\text{NTH}(\text{INVERSE}(U), N)) \land \text{NTH}(\text{INVERSE}(U), N) < \text{LENGTH } U \)

7. (trw (into inverse(u)) *
   (open into) (use lengthinverse inv,pl mode: exact))
   \( \rightarrow \text{INTO}(\text{INVERSE}(U)) \)
   (label into-inverse)

8. (ci inv,pl)
   \( \rightarrow \text{PERM}(U) \rightarrow \text{INTO}(\text{INVERSE}(U)) \)
   (label inv_into)

The second part of the theorem is the proof that inverse(u) is onto, still under the assumption that perm(u) (line 1).

9. (rw inv,pl (open perm into onto))
   \( \forall N. N < \text{LENGTH } U \land \text{NATNUM}(\text{NTH}(U, N)) \land \text{NTH}(U, N) < \text{LENGTH } U) \land \)
   \( \forall N. N < \text{LENGTH } U \land \text{MEMBER}(N, U) \)
   (label inv_p10)

10. (derive \{length inverse(u)=length u\}
    (inv,pl lengthinverse))
    (label inv_p11)

11. (assume \{n<length inverse(u)\})
12. (rw * (use inv_p11 mode: exact))
   ;N<LENGTH U
   (label inv_p13)

   We can apply the main property of the inverse function...

13. (ue (n | nth(u,n)|) inv_p4 (use inv_pl0 * mode: always))
    ;NTH(INVERSE(U),NTH(U,N))=FSTPOSITION(U,NTH(U,N))
    (label inv_p14)

   ...the consequence of the Pigeon Hole principle...

14. (derive linj u|(inv_p1 perm_injectivity))

   ...the basic fact Fstposition Nth...

15. (derive |fstposition(u,nth(u,n))=n|
   (fstposition,nth uniqueness,injectivity * inv_p10 inv_p13))

16. (rw inv_p14 (use *))
    ;NTH(INVERSE(U),NTH(U,N))=N
    (label inv_p15)

   ...and the lemma Nthmember...

17. (derive |natnum nth(u,n)nth(u,n)<length inverse(u)|
   (inv_p10 inv,p11 inv_p13))

18. (trw |member(nth(inverse u,nth(u,n)),inverse u)|
    (nthmember *))
    ;MEMBER(NTH(INVERSE(U),NTH(U,N)),INVERSE(U))

   ...to conclude:

19. (rw * (use inv_p15))
    ;MEMBER(N,INVERSE(U))
    ;deps: (INV_P1 INV_P12)

20. (ci inv_p12)
    * ;N<LENGTH (INVERSE(U)) MEMBER(N,INVERSE(U))
    (label onto-inverse)

21. (trw |perm(inverse u)| (open perm onto)
    into-inverse onto-inverse)
    ;PERM(INVERSE(U))

22. (ci inv_p1)
    ;PERM(U) PERM(INVERSE(U))
    (label perm_inverse) ■

The proofs of the other parts of Theorem 3 are given in the Appendix.
7. Conclusion.

The remarks made in the Introduction and in the text, especially in Section 6.1, are relevant to the heuristics of automatic theorem proving and apply at three stages of the enterprise of mechanically representing mathematical facts.

- First, the choice of a representation determines the basic strategy of proof. It is certainly reasonable to search for a representation that allows simple recursive definitions of the basic objects and hence relatively simple proofs by induction on those recursive definitions. For this reason our representation using association lists is particularly attractive. However, there may be other reasons suggesting a different representation. In our case, we considered the representation by lists of numbers since it has the property of uniqueness.

Since EKL uses higher order language, it does not restrict us to a particular kind of representation: if recursive definitions are not available, or not convenient, we may give abstract definitions and carefully organize the argument so that appropriate mathematical or logical principles apply. As a very simple example, discussing the choice of predicates or of functions in the representation PERMP and PERMF we examined two approaches: explicit definitions, derivations by logic inferences and term substitutions directed by the user versus recursive definitions, proofs by induction and logic inference replaced by rewriting. We considered advantages and limitations of the two methods and saw how a judicious combination of them may give the best results. At the end of Section 6.1. we outlined the optimal choice of definitions and the most effective proof strategy.

Moreover, EKL allows us to prove abstract mathematical facts that are independent of the particular representation: the Pigeon Hole principle was proved in second order arithmetic and then applied to different representations. In general there is no doubt that an essential advantage in proving correctness of programs is given by access to abstract mathematical knowledge.

- Even when the main strategy of proof is chosen, different choices may be possible for the Lemmata. One can use EKL as an heuristic aid and try to find a proof by trial and error, reduce the task to some lemmata, try to prove the Lemmata, etc. (An example is given in the proof LengthInversion Section 6.3.1.) A warning has to be made against this procedure: EKL will be extremely helpful in reminding us of many details we usually take for granted, but we are not yet ready to dismiss pencil and paper as obsolete: indeed it will save us a lot of time to work out a fairly detailed proof by 'pencil and paper' before starting our interaction with EKL.

Let us say that a proof is 'trivial' when the recursive definition of the basic objects and the statement of the theorem determine not only the main strategy of proof of the theorem, but also a natural choice of the lemmata and strategies for their proofs. Presumably, for such 'trivial' proofs some development of Boyer and Moore's techniques will allow entirely automatic heuristics.

There is no reason to think that given a simple recursive definition of some basic objects, one will always find 'trivial' proofs by induction. Often the choice of the Lemmma will not be obvious. Sometimes the lemmata suggested by the recursive definition of the objects and by the statement of the theorem by no means are the most convenient or the most perspicuous.

Consider for instance our definition of inverse. Using invers and firstposition the functions involved here cannot be considered extremely difficult as LISP programs. However, there is room for discussion on how to choose and to prove the lemmata. Indeed, as we argued in the text, the best choice seems to be to consider the abstract properties of the functions ident and inverse and prove the lemmas lemmata. These properties are immediately recognized when we formulate the identity function and the operation of function inversion more abstractly as predicates. They are not the ones that come to mind first if we try to prove the theorems by expanding the definitions.
Finally, there is still room for choice at the stage of performing single inductive proofs, when the necessary lemmata have been proved. One may try to obtain the proof in a single line, by rewriting or expand the proof by using explicitly the logic decision procedure in the style of Natural Deduction. The heuristics of single proofs has been extensively discussed in the Conclusion of Part I, Section 2.13.

**Remark, Example 10.** To consider the different options available in carrying on a relatively long proof, let's look at the problem of formalizing the Lemma in Section 1.4 in full generality. We want to prove that for any \( f : A \rightarrow B \) with \( A \) and \( B \) finite sets of the same cardinality, if \( f \) is a surjection then \( f \) is also an injection. We express this statement in our fragment of Set Theory, using our (higher order) formalization of arithmetic. The following is an outline of the project. The details are left to the reader as an exercise.

1. Formulate the Set Theoretic notions of map, surjection, injection and bijection, and use function abstraction and application to define function composition. For instance:

   \[
   \begin{align*}
   &\text{(decl } f \text{, } g \text{, } h \text{) (type: } |\text{ground-}f\text{ound|})} \\
   &\text{(decl map (type: } |\text{map}|f\text{, }a\text{, }a\text{=}\text{-truthval|})} \\
   &\text{(define map }|\forall g \text{, }a\text{, }b\text{=}\text{=}(\forall x \text{v. } x \text{v} \in a\text{=}g(x)\text{v}b)\text{)} \\
   &\text{(label mapdef)} \\
   &\text{(decl compmap (type: } |\text{compmap}|f\text{, }g\text{, }a\text{, }b\text{=}\text{-+|}) (infixname: } @\text{)} \\
   &\text{(bindingpower: } 960\text{)} \\
   &\text{(define compmap }|\forall f \text{, }g\text{=}\text{=}\text{,(}\lambda x \text{v. } f(g(x))\text{)}} \\
   &\text{(label compmapdef)}
   \end{align*}
   \]

   The fact that a set \( a \) has finite cardinality \( n \) can be expressed as

   \[
   \forall a \text{, } n \text{. } \text{fincard}(a, n) \equiv 3 \text{. } \text{bijection}(f, \text{segm}(n), a)
   \]

   (where \( \text{segm}(n) \) denotes \( N_n \).

   The inverse image of an element \( y \) under a function \( g \) is

   \[
   \forall a \text{, } \text{YINVIM}(G, YV) = XXV.G(XV) = YV
   \]

2. Apply the Pigeon Hole principle to maps \( g : N_n \rightarrow N_n \). Formally, prove \( \text{Ontomap Injmap} \)

   \[
   \forall a \text{, } N \text{. } \text{ONTOMAP}(G, \text{SEG}(N), \text{SEG}(N)) \Rightarrow \text{INJMAP}(G, \text{SEG}(N), \text{SEG}(N))
   \]

   A way to do this is to define a recursive functional \text{card} that counts the intersection of a set \( a \) with the set \( N_n \):

   \[
   \begin{align*}
   &\text{(define card }|\forall a \text{, } n\text{. } \text{card}(a, 0) = 0a} \\
   &\text{card}(a, n') = \text{ifa}(n) \text{ then card}(a, n') \text{ else card}(a, n)} \\
   &\text{inductive-definition)}
   \end{align*}
   \]

   The next step is to prove the analogues for \text{card} of the properties of \( \text{mult} \). The Pigeon Hole principle now takes the form
VSETSEQ N.DISJOINT(SETSEQ,N)
((∀M<N1:CARD(SETSEQ(M),N))
 (∀M<N1=CARD(SETSEQ(M),N)))

Let setseq(m) be invim(g,m): by the properties of the inverse image and of surjective maps
we obtain

∀G N.ONTOMAP(G,SEG(N),SEG(N))
(∀M<N1=CARD(INVIM(G,M),N))

An argument by contradiction, counting cardinalities, gives Ontomap Injmap.

iii) Reduce the problem for arbitrary finite sets to the problem for sets of numbers. Namely,
show that given an onto function g : A → B and suitable bijections f_A : N_n → A, f_B : B → N_n,
there is a (finite) onto function f : N_n → N_n such that the diagram

```
  A                       B
     g                         
  f_A      ↓                   ↓ f_B
  N_n       f               N_n
```

commutes. f is an onto function over N_n, hence Ontomap Injmap applies. This involves some
abstract properties of maps between sets. Conclude:

∀G A B N.FINCARD(A,N)\FINCARD(B,N)\ONTOMAP(G,A,B)\INJMAP(G,A,B)

From this general application of the Pigeon Hole principle one can derive the corresponding
statements using various representations of finite functions. In the representation by association
lists one can show

1. ∀ALIST. PERMUTP(ALIST)\ONTOMAP(λX.APPALIST(X,ALIST),MKLSET(DOM(ALIST)),MKLSET(RANGE(ALIST)))

2. ∀ALIST. PERMUTP(ALIST)\FINCARD(MKLSET(DOM(ALIST)),LENGTH(DOM(ALIST)))

3. ∀ALIST. PERMUTP(ALIST)\BIJECTION(λX.APPALIST(X,ALIST),MKLSET(DOM(ALIST)),MKLSET(DOM(ALIST)))

and derive the familiar result Permutp Injectp

∀ALIST. PERMUTP(ALIST)\INJECTP(ALIST)

by using 1,2,3 and some fact about appalast. For instance, the following fact may be useful:

∀ALIST N.UNIQUENESS(DOM(ALIST))\AND<LENGTH(DOM(ALIST))\APPALIST(NTH(DOM(ALIST),N),ALIST) = NTH(RANGE(ALIST),N)

Clearly the above alternative route to prove Permutp Injectp is elegant and attractive, since
the general facts may be applied in other contexts.
iv) In the same vein, one could want to do the entire project at a more abstract level. Namely, one can use EKL to check that bijections over any (not necessarily finite) set, with composition of functions, form a group. Facts about composition and the identity functions are easy, and one may use the Axiom of Choice to show that every bijection has a right inverse, and some categorical properties of mappings of sets to conclude that the right inverse is a two sided inverse.

The Axiom of Choice, i.e. the statement
\[(\forall x. \exists y. A(x, y)) \supset (\exists f. \forall x. A(x, f(x)))\]
is built in EKL: whenever we have obtained the line
\[; (\forall x. \exists y. A(x, y))\]
we can ask EKL to define a suitable function fv
\[(\text{define } fv \mid \forall x. A(x, f(x)) \mid *)\]

In the case of finite sets, by using iii) one can restrict oneself to prove that surjections form a group. Also the corresponding fact, say, for the representation of finite functions by association lists, can be obtained by proving the following facts:

(I) If \( f \) is a bijection over a finite set \( A \), then there exists an association list \( \text{alist}_f \) that represents \( f \), i.e. such that for all elements \( x \) of \( A \),
\[ f(x) = \text{appalist}(x, \text{alist}_f). \]

(II) If \( f_1 \) and \( f_2 \) are functions for which \( f_2 \circ f_1 \) is defined, and \( \text{alist}_1 \), \( \text{alist}_2 \) represent \( f_1 \), \( f_2 \) respectively, then composition of functions is represented by `composition' of association lists, i.e.
\[ (f_2 \circ f_1)(x) = \text{appalist}(\text{alist}_1 \circ \text{alist}_2, x). \]

This approach is certainly very efficient and elegant. Here, however, we see that there may be a price to be paid for efficiency: by general considerations we only show the existence of an inverse function. We do not obtain the verification that a particular LISP program represents the inverse permutation. In logical terms, we verify that our LISP structures satisfy the axioms of groups using the axioms
\[ \forall x y z. x o (y o z) = (x o y) o z, \]
\[ \exists x. \forall y. y o x = x, \]
\[ \forall x. y o x = y, \]

rather than the universal axioms
\[ \forall x y z. (y o z) = (x o y) o z, \]
\[ \forall x. x o x = e, \]
\[ \forall x. x o x^{-1} = x^{-1} o x = e. \]

If the purpose of the project is mechanical verification of correctness of programs, the verification of a given program representing inversion of permutations has to be done separately.

Despite our emphasis on the use of abstract mathematical tools, the approach to verification of properties of programs that has been followed in this paper could be described as the approach
'from below': given simple LISP programs performing some mathematical constructions, prove 'directly' the properties of programs that correspond to the mathematical facts in question.

The efficiency obtained by working with abstract notions suggests a different approach to mechanical program verification: working 'from above', we may formally prove facts with a maximum of generally and abstraction; only at the end we apply the result to the concrete programs.

In conclusion, our experiment shows that, even when (i) our mathematical objects have simple recursive definitions, (ii) the proofs require no sophisticated methods and (iii) the heuristics itself appears mechanizable for some part of the proofs, it is still convenient to organize the subject through abstract lemmata, rather than to use direct proofs every time.

In Proof Theory procedures of Normalization play an essential role. Roughly speaking, when logical constants and mathematical entities can be appropriately defined according to the pattern
Introduction - Elimination, it is possible to define a normal form for proofs and to find procedures that transform every proof into one in normal form.

In such procedures a sequence of inferences that first establish a general lemma and then apply it to particular conditions is considered a 'detour'. Such sequence must be simplified in favor of a longer but more direct proof. From the point of view of Proof Theory it is essential to establish the possibility of normalization. Important properties of mathematical systems can be established by these methods.

However, Normalization does not seem to be the optimal strategy for proof checking. In formalizing relatively large areas of knowledge it seems necessary to follow the opposite strategy, namely to search for suitable abstract lemmata applicable to different situations.

Using Kreisel's words:

'The particular strategy of organizing an area of knowledge, which serves us here as a model, is the style of Bourbaki: one looks for a few definitions and key theorems that lead to easy solutions of many problems. (No one proof in Bourbaki is long).'

G. Kreisel [1981]
8. APPENDIX.

8.1. A Summary of Natural Deduction.

The aim of the following notes is to remind the reader of the basic features of Gentzen's system of Natural Deduction not only because of its historical importance in the design of EKL and of related systems (e.g. FOL), but also since some familiarity with Natural Deduction may be useful in constructing EKL proofs. The reader already familiar with the subject may want to skip this section.

A Natural Deduction System is a formal system that allows one to derive a formula as consequence of a list of formulas, the assumptions, and to eliminate formulas from a given assumption list. One of the deduction rules in a Natural Deduction system, given a derivation of \( B \) from a set of assumptions of the form \( A \), allows one to construct a derivation of \( A \supset B \), where (some of) the assumptions \( A \) have been discharged (see the \( \supset \) - Introduction rule below).

By contrast a Hilbert style axiomatic system allows one only to derive logical consequences of certain formulas, regarded as axioms. We need a metatheorem to prove that in certain conditions if \( B \) is provable from a set of axioms \( S \) together with the axiom \( A \) then there is a proof of \( A \supset B \) from \( S \) only (Deduction Theorem).

The most successful system of Natural Deduction was defined by Gentzen and later improved by Prawitz [1965, 1971]. In the Prawitz formulation, we are given a language with a symbol \( \bot \) for falsity and the usual connectives and quantifiers \( \land, \lor, \supset, \forall, \exists \). Negation is defined: \( \neg A \) is \( A \supset \bot \). Moreover we use two disjoint sets of symbols for free and bound variables. A system of Natural Deduction is specified by rules of inference and rules of deduction.

A derivation is a finite tree of formulas (with 'leaves' at the top), where

(i) the top formulas ('leaves') are the assumptions.

(ii) the bottom formula is the conclusion.

(iii) every formula not at the top is derived by a rule of inference from the subderivation immediately above it and

(iv) a deduction rule associates to each occurrence of a formula a set of open assumptions, i.e. the set of assumptions, which the formula in question depends on.

Often in the literature the deduction rules are not explicitly specified, but the reader can easily fill in the details. (Actually, dealing with finite trees, an effective specification is always possible.) A useful convention is to divide assumptions of the same form into assumption classes, to mark with the same label an assumption class and the inference by which the assumption class is discharged.

A rule of inference has the form: If \( \Pi_1, \ldots, \Pi_n \) are derivations of \( C_1, \ldots, C_n \), respectively, then

\[
\begin{array}{c}
\Pi_1 \\
\vdots \\
C_1 \\
\ldots \\
C_n
\end{array}
\]
is a derivation of $C$, under certain conditions on the form of the $C_i$'s and $\prod_j$'s. The formulas $C_i$ are called the premises and $C$ the conclusion of the inference.

Thus the set of rules of inference, together with the clause

Every formula is a derivation of itself.

gives an inductive definition of derivations.

The reader will recognize the usual rules of introduction and elimination of the logical connectives and quantifiers in the figures below. More specifically, in each of the figures below, if the symbol(s) above the line denote derivation(s) of the indicated formula(s), then the displayed symbols denote a derivation of the formula below the line.

**$\land$-Introduction**

\[
\begin{array}{c}
\Pi_1 \\
A
\end{array}
\quad
\begin{array}{c}
\Pi_2 \\
B
\end{array}
\quad
\begin{array}{c}
\Pi \\
A \land B
\end{array}
\]

**$\land$-Elimination**

\[
\begin{array}{c}
\Pi
\end{array}
\quad
\begin{array}{c}
\Pi
\end{array}
\quad
\begin{array}{c}
\Pi \land \Pi
\end{array}
\]

**$\lor$-Introduction**

\[
\begin{array}{c}
\Pi
\end{array}
\quad
\begin{array}{c}
\Pi
\end{array}
\quad
\begin{array}{c}
\Pi_1 \\
A
\end{array}
\quad
\begin{array}{c}
\Pi_2 \\
B
\end{array}
\quad
\begin{array}{c}
\Pi \\
A \lor B
\end{array}
\]

**$\lor$-Elimination**

\[
\begin{array}{c}
\Pi
\end{array}
\quad
\begin{array}{c}
\Pi
\end{array}
\quad
\begin{array}{c}
\Pi_1 \\
[A]
\end{array}
\quad
\begin{array}{c}
\Pi_2 \\
[B]
\end{array}
\quad
\begin{array}{c}
\Pi_3 \\
A \lor C
\end{array}
\quad
\begin{array}{c}
C
\end{array}
\]

\[
\begin{array}{c}
\Pi
\end{array}
\quad
\begin{array}{c}
\Pi
\end{array}
\quad
\begin{array}{c}
\Pi_1 \\
A \lor B
\end{array}
\quad
\begin{array}{c}
\Pi_2 \\
C
\end{array}
\quad
\begin{array}{c}
\Pi_3 \\
C
\end{array}
\quad
\begin{array}{c}
C
\end{array}
\]
\( \forall \text{-Introduction} \)
\[
\Pi_0 \\
A(t) \\
\overrightarrow{\forall x. A(x)}
\]

\( \forall \text{-Elimination} \)
\[
\Pi \\
\forall x. A(x) \\
\overrightarrow{A(t)}
\]

where no open assumption of \( \Pi_0 \) contains the free variable \( a \). \( t \) is any individual term.

\( \exists \text{-Introduction} \)
\[
\Pi \\
A(t) \\
\overrightarrow{\exists x. A(x)}
\]

\( \exists \text{-Elimination} \)
\[
\Pi_1 \quad I \text{l}_2 \\
\exists x. A(x) \\
\overrightarrow{C'}
\]

where the free variable \( a \) does not occur in \( C \), in \( \exists x. A(x) \), or in any open assumption of \( \Pi_2 \) different from \( A(a) \). \( t \) is any individual term.

In any elimination rule the first premise, containing the symbol to be "eliminated", is called the major premise. The other premise(s) (if any) are called minor premise(s).

The following rules for negation are needed to formalize Intuitionistic Logic and Classic Logic.

\( \bot_I \text{ (Intuitionistic)} \)
\[
\Pi \\
\bot \\
\overrightarrow{A}
\]

\( \bot_C \text{ (Classic)} \)
\[
\Pi \\
\bot \\
\overrightarrow{A}
\]

Under most rules of deduction the open assumptions associated with the conclusion of an inference are the union of the sets of open assumptions associated with the premises, with the following exceptions:

i) in \( \exists \text{-Introduction} \), the assumption class \([A]\) is discharged;

ii) in \( \forall \text{-Elimination} \), the assumption classes \([A]\) of \( \Pi_2 \) and \([B]\) of \( \Pi_3 \) are discharged;

iii) in \( \exists \text{-Elimination} \), the assumption class \([A(a)]\) of \( \Pi_2 \) is discharged;

iv) in the Classical Rule of Negation, the assumption class \([-A]\) is discharged.
Deduction rules can be specified by writing the set of open assumptions (followed by some symbol, e.g. "\(\vdash\)"") before each formula occurrence in the derivation. Thus, using Greek letters for sets of assumptions, we can write the rules for disjunction as

\[
\begin{align*}
\text{\textbf{\(\lor\)-Introduction}} & \\
\Pi & \Pi \\
\Gamma \vdash A & \Gamma \vdash B \\
\hline
\Gamma, A \lor B & \Gamma \vdash A \lor B
\end{align*}
\]

\[
\begin{align*}
\text{\textbf{\(\lor\)-Elimination}} & \\
\Pi_1 & \Pi_2 & \Pi_3 \\
\Gamma \vdash A \lor B & \alpha, u \{A\} \vdash C & \Delta_2 \cup \{B\} \vdash C \\
\hline
\Gamma \cup \Delta_1 \cup \Delta_2 \vdash C
\end{align*}
\]

**Warning.** A formulation of Natural Deduction along these lines would be only a typographical variant of the above system and not a form of Calculus of Sequents, a related but conceptually different logical calculus.

The restrictions on free variables for \(\lor\)-Introduction and \(\exists\)-Elimination establish a relation between free variables and rules. When performing transformations on proof it is convenient to have a different free variable for each application of such a rule. This can be handled by introducing a special list of variables, called eigenvariables or parameters, to be used in association with \(\lor\)-Introduction and \(\exists\)-Elimination.

One can prove that every derivation can be transformed into an equivalent one in which the eigenvariable associated with a \(\lor\)-I or \(\exists\)-E application occurs only in the ancestors of the conclusion of such rule. (*Lemma on parameters*, Prawitz [1965], p. 29).

A formal system that distinguishes between variables and parameters may be sometimes cumbersome, although the main idea is simple. In the top level language of EKL the distinction is not required (see rules about dependencies below).

The system \(\mathbf{M}\), containing only the rules for \(\land\), \(\lor\), \(\exists\), \(\forall\) and \(\exists\), formalizes Minimal Logic. The system \(\mathbf{I}\), given by \(\mathbf{M}\) plus the Intuitionistic Negation Rule \(\bot\), is (Heyting) Intuitionistic Logic. The system \(\mathbf{C}\), given by \(\mathbf{M}\) plus the Classical Negation Rule, is full Classical Logic. We write \(\Gamma \vdash_I A\) \((\Gamma \vdash_C A)\) to indicate that \(A\) is derivable from the formulas in \(\Gamma\) in the system for Intuitionistic (Classical) Logic.

**Example 1.**

\[
\begin{align*}
(1) & \\
A & \\
\hline
\text{\(\lor\)-I, (1)} \\
\neg (A \lor B) & A \lor B \\
\hline
\text{\(\lor\)-E} & A \lor B \vdash A \lor B \\
\hline
\bot & \\
\text{\(\bot\)-I, (1)} \\
\neg A & \\
\hline
\text{\(\neg\)-I} & \\
\neg A & \\
\hline
\neg A \land \neg B
\end{align*}
\]

\[
\begin{align*}
(2) & \\
B & \\
\hline
\text{\(\lor\)-E} & A \lor B \vdash A \lor B \\
\hline
\bot & \\
\text{\(\bot\)-I, (2)} \\
\neg B & \\
\hline
\text{\(\neg\)-I} & \\
\neg A \land \neg B
\end{align*}
\]
(Here ‘\(\neg\)’ stand for ‘\(\neg\)-Introduction’, ‘\(\neg\)-Elimination’, etc. With the above specification of the deduction rules, we obtain a derivation \(\neg(A \lor B) \vdash I \neg A \land \neg B\).

**Example 2.**

\[
\begin{array}{c}
(1) \quad \neg A \\
(2) \quad A \\
\hline
\neg A \lor B
\end{array}
\]

\[
\begin{array}{c}
B \\
\hline
\bot
\end{array}
\]

\[
\begin{array}{c}
A \supset B \\
\hline
A \supset B
\end{array}
\]

\[
\begin{array}{c}
B \\
\hline
A \supset B
\end{array}
\]

\[
\begin{array}{c}
\neg A \lor B \\
\hline
A \supset B
\end{array}
\]

This is a derivation \(\neg A \lor B \vdash I \neg A \land \neg B\). Notice that we can infer \(A \supset B\) from \(B\) **even** if the assumption class \([A]\) is empty—i.e. \(A\) is not an open assumption, which \(B\) depends on.

**Example 3.a)**

\[
\begin{array}{c}
(1) \quad \forall x.A(x,b) \\
\hline
\forall E
\end{array}
\]

\[
\begin{array}{c}
A(a,b) \\
\hline
\exists I
\end{array}
\]

\[
\begin{array}{c}
\exists_y A(a,y) \\
\hline
\forall I
\end{array}
\]

\[
\begin{array}{c}
\forall x \exists y.A(x,y) \\
\hline
\exists E, (1)
\end{array}
\]

Here we assume that \(\exists_y \forall x . A(x,y)\) does not contain \(a, b\).

**Example 3.b)** What restrictions must \(C\) satisfy in order for the following to be a correct derivation?

\[
\begin{array}{c}
(1) \quad \forall x . A(x,b) \\
\hline
\forall E
\end{array}
\]

\[
\begin{array}{c}
(2) \quad A(a,b) \\
\hline
A-I
\end{array}
\]

\[
\begin{array}{c}
C \land A(a,b) \\
\hline
\land E
\end{array}
\]

\[
\begin{array}{c}
A(a,b) \\
\hline
\exists I
\end{array}
\]

\[
\begin{array}{c}
\exists_y A(a,y) \\
\hline
\forall I
\end{array}
\]

\[
\begin{array}{c}
\forall x \exists y . A(x,y) \\
\hline
\exists E, (1)
\end{array}
\]

\[
\begin{array}{c}
\forall x \exists y . A(x,y) \\
\hline
\forall x \exists y . A(x,y)
\end{array}
\]
Example 4. (i) The rule $\perp_C$ is derivable in the system $\mathbf{I}$ plus the axiom $A \lor \neg A$.

(ii) $\vdash_C A \lor \neg A$. It is easy to see that in the proof we must assume $\neg (A \lor \neg A)$.

It will not be difficult to convince the reader that the derivation in Example 3(a) is 'better' than that in Example 3(b). Not only Example 3(a) is shorter, but also the two successive steps of Introduction and Elimination of $A$ in Example 3(b) do not give us any interesting information: the formula $C$ is simply irrelevant for the derivability of the conclusion from the premises.

This simple remark can be extended to other rules and gives the main idea of Normalization Theorem, one of the most interesting result of Proof Theory.

The occurrence of a formula in a derivation is called maximal if it is at the same time the conclusion of an Introduction and the major premise of an Elimination rule (necessarily, of the same logical symbol). A maximal formula can be removed by a reduction, a transformation of the given derivation that consists essentially of removing the two steps, Introduction and Elimination. Here we give the list of reductions.

$\wedge$-Reduction

\[
\begin{array}{c}
\Pi_1 & \Pi_2 \\
A_1 & A_2 \\
\hline \\
A_1 \wedge A_2 & \text{A-I} \\
[\mathbb{A}_i] & \text{A-E} \\
\hline
\Pi_3
\end{array}
\]

where $i = 1$ or $2$, is reduced to

\[
\begin{array}{c}
\Pi_1 \\
[\mathbb{A}_i] \\
\Pi_3
\end{array}
\]
\[ \text{-Reduction} \]

\[
\Pi_1
\]

\[
\begin{array}{c}
B \\
A \supset B
\end{array}
\quad \text{C-I}
\]

\[
\Pi_2
\]

\[
A
\]

\[
\Rightarrow
\]

\[
\begin{array}{c}
[B] \\
\Pi_3
\end{array}
\quad \text{C-E}
\]

is reduced to

\[
\Pi_2
\]

\[
[A]
\]

\[
\Pi_1
\]

\[
[B]
\]

\[
\Pi_3
\]

\[ \text{V-Reduction} \]

\[
\Pi_0
\]

(1) (2)

\[
A_i
\]

\[
\begin{array}{c}
[A_1] \\
[A_2]
\end{array}
\quad \text{V-I}
\]

\[
\Pi_1
\quad \Pi_2
\]

\[
A_1 \lor A_2
\]

\[
C
\]

\[
C
\]

\[
[K_3]
\quad \text{V-E, (1), (2)}
\]

\[
\Pi_3
\]

where \( i = 1 \) or \( 2 \), is reduced to
\[ \Pi_0 \]
\[ [A_i] \]
\[ \Pi_i \]
\[ [C] \]
\[ \Pi_3 \]

The following derivation assume that \( \Pi_1(a) \) satisfies the restriction for the \( \forall \)-Introduction and contains \( a \) only at some ancestors of \( A(a) \). (One can show that any derivation can be transformed into an equivalent derivation satisfying the last condition.) Then

\textbf{\( \forall \)-Reduction}

\[
\begin{align*}
\Pi_1(a) & \\
A(a) & \\
\forall x. A(x) & \forall\text{-I} \\
[\forall x. A(x)] & \forall\text{-E} \\
\Pi_2 &
\end{align*}
\]

is reduced to

\[
\begin{align*}
\Pi_1(t) & \\
[\forall x. A(x)] & \\
\Pi_2 &
\end{align*}
\]

where \( \Pi_1(t) \) is the result of replacing everywhere \( t \) for \( a \) in \( \Pi_1(a) \).
The following derivations assume that $\prod_2(a)$ satisfies the restriction for the $E$-Elimination and contains $a$ only at some descendants of $A(a)$.

**$E$-Reduction**

\[
\begin{align*}
\Pi_1 & \\
A(t) & \rightarrow [A(a)] \\
\exists I & \rightarrow \Pi_2(a) \\
\exists x. A(x) & \rightarrow C \\
\exists E, (1) & \\
\Pi_3 & \\
\end{align*}
\]

is reduced to

\[
\begin{align*}
\Pi_1 & \\
[A(t)] & \\
\Pi_2(t) & \\
[C] & \\
\Pi_3 & \\
\end{align*}
\]

where $\prod_2(t)$ is the result of replacing everywhere $t$ for $a$ in $\prod_2(a)$.

**Example 5.** The following derivation formalizes a common procedure: first prove a general lemma ($\forall x. (A(x) \supset B(x))$) and then apply it to particular cases.

\[
\begin{align*}
(1) & \\
\Pi_1(a) & \\
B(a) & \rightarrow \forall I, (1) \\
A(a) \supset B(a) & \\
\forall x. (A(x) \supset B(x)) & \rightarrow \forall E \\
A(t) \supset B(t) & \\
A(t) & \rightarrow A(t) \\
B(t) & \rightarrow \forall E \\
\end{align*}
\]
A derivation is said to be normal if it does not contain maximal formulas.

**Normalization Theorem.** Every derivation in the system for Intuitionistic Logic can be transformed into one in normal form.

The reader may have noticed that the normal derivations in Examples 1, 2 and 3(a) are, in some sense, 'among the best possible', but with a difference: the derivation in Example 1 is, in some sense, 'unique', whereas the others are not. Indeed in Example 2 we could permute the the \( \land \)-1 applications and the \( \lor \)-E and still obtain a normal derivation. Similarly in Example 3(a) we could permute the \( \lor \)-1 and the \( \exists \)-E. Of course these remarks could be made precise, but our examples suggest that uniqueness of the normal form may fail in a nontrivial sense.

Normal derivations have a very interesting structure. Their analysis requires some technical notions. Let \( \Pi \) be a derivation. A *path* in \( \Pi \) is a sequence \( A_1 \ldots A_n \) of formula occurrences in \( \Pi \) such that:

1) \( A_1 \) is a top formula that is not discharged by \( \lor \)-Elimination or \( \exists \)-Elimination;
2) \( A_n \) is either the endformula of \( \Pi \) or the minor premise of an \( \exists \)-Elimination: \( A_i \), for \( i < n \), is not the minor premise of \( \exists \)-Elimination;
3) for \( i < n \), one of the following cases applies:
   i) \( A_i \) is a premise of an Introduction, of a Negation rule, of a \( \land \)-Elimination, \( \lor \)-elimination, or the major premise of \( \exists \)-Elimination, and \( A_{i+1} \) is the conclusion of that inference;
   ii) \( A_i \) is a minor premise of an \( \lor \)-Elimination or of an \( \exists \)-Elimination and \( A_{i+1} \) is the conclusion of that inference;
   iii) \( A_i \) is the major premises of an \( \lor \)-Elimination of of an \( \exists \)-Elimination and \( A_{i+1} \) is an assumption discharged by that inference.

*Example 6.* In the derivation of Example 1

\[ \neg (A \land B) \] is a path (i.e. the formula occurrence labeled (1) and the one immediately below it);

\[ \neg (\neg A \lor B), \bot, \neg A, \neg A \land \neg B \] is a path (starting with the leftmost occurrence of \( \neg (A \lor B) \) labeled (3) ).

In the derivation of Example 2

\[ \neg (A \lor B), 7.4, \bot, A \lor B, A \lor B \] is a path (starting with the formula occurrence labeled (4) and continuing with the one labeled (1) ).

In a path there may be consecutive occurrences of the same formula, e.g. the minor premise and the conclusion of an \( \exists \)-Elimination. A *segment* \( \sigma \) in a path of \( \Pi \) is a sequence \( \langle A_1, \ldots, A_k \rangle \) of occurrences of (the same) formula, such that either \( 1 \leq k \) or, if \( k > 1 \), the following conditions are satisfied:

i) for \( i = 2, \ldots, k \), \( A_i \) is the consequence of an \( \lor \)-Elimination or of \( \exists \)-Elimination, and \( A_1 \) is not such a consequence;

ii) for \( i = 1, \ldots, k - 1 \), \( A_i \) is the minor premise of an \( \lor \)-Elimination or of an \( \exists \)-Elimination and \( A_k \) is not such a premise.
Example 7. Every formula occurrence in Example 1 is a segment. In Example 2, the sequence \((-1 \supset B. A \supset 0\) consisting of a minor premise and the conclusion of the final \(\lor\)-Elimination is a segment: the sequence \((A \supset B)\) containing the endformula of Example 2 is not a segment.

With this terminology, one can prove the following theorem, giving a complete characterization of normal deductions in Intuitionistic Logic (see Prawitz [1965], pag. 53):

**Theorem.** Let \(\Pi\) be a normal deduction in the Natural Deduction system for Intuitionistic Logic. Let \(\pi\) be a path in \(\Pi\), and let \(\sigma_1, \ldots, \sigma_n\) be the sequence of segments in \(\pi\). Then there is a segment \(\sigma_i\), called the minimum segment in \(\pi\), which separates two (possibly empty) parts of \(\pi\), called the E-part and I-part of \(\pi\), with the properties:

1) For each \(\sigma_j\) in the E-part (i.e. \(j < i\)), the last formula occurrence in \(\sigma_j\) is a major premise of an E-rule and the formula in \(\sigma_{j+1}\) is a subformula of the formula in \(\sigma_j\).

2) If \(i \neq n\), the formula in \(\sigma_i\) is a premise of an I-rule or of the \(\bot \lor\) Negation rule.

3) For each \(\sigma_k\) in the I-part (i.e. \(i < k < n\)), the last formula occurrence in \(\sigma_k\) is a premise of an I-rule and the formula in \(\sigma_k\) is a subformula of the formula in \(\sigma_{k+1}\).

As a corollary of this analysis, one proves

**Subformula Property.** Every formula occurring in a normal derivation of \(A\) from \(\Gamma\) in the system of Natural Deduction for Intuitionistic Logic is a subformula either of \(A\) or of a formula in \(\Gamma\).

The above result is fundamental in Proof Theory. For our purpose it is essential to notice that if \(\Gamma \vdash_{I} A\), then in the search for a normal derivation we need to consider only subformulas of \(A\) and of the formulas in \(\Gamma\); moreover the above theorem gives directions to build such a proof. A normal deduction is in practice the best choice for a short proof. We may find it convenient to break a long derivation into lemmata either for the sake of readability or in order to highlight some important step in the argument.

By contrast, Example 4 (ii) shows that the Subformula Property fails for full Classical Logic. Indeed we do not have a Normalization for full Classical Logic. In order to overcome the difficulty, Gentzen introduced the Calculus of Sequents and Prawitz [1965, 1971] proves Normalization for the formulation of Classical Logic without \(\lor\) and \(\exists\). However we will use the full system for Classical Logic, and not the Calculus of Sequents, so these results, despite their theoretical relevance, are beyond our immediate concern. For practical purpose, the reader may have noticed that when an argument by contradiction is needed, there may be different ways to obtain one. A good choice of the formula to be contradicted is an essential step to obtain a readable proof and is not given by a mechanistic procedure.

**Remark.** Proofs by induction do not fit well in the pattern Introduction-Elimination of Natural Deduction: one may define what it means for the conclusion of an Induction Rule to be maximal and prove a Normalization Theorem for for first order the Natural Deduction system \(\forall \exists \to\) Peano Arithmetic. (see Troelstra [1973]). The significance of the result, however, is reduced by the fact that in such system the Subformula Property does not hold. For higher order logic Prawitz proved Normalization Theorem (Prawitz [1968]). Again, the Subformula Property does not hold. In practice, if we apply some axiom of induction (or of a corresponding rule) in the context of higher order logic and recursive functionals of higher types, the simple form of normal deductions given by the Normalization Theorem for first order logic is necessarily lost.

As we shall see, we would like to let the computer do the logical steps of our proofs. To a certain extent, we succeeded in replacing logical steps by rewriting. However, a certain familiarity
with Natural Deduction is important for the user of EKL. It suggests a safe procedure, through a lengthy one, to expand proofs. It may help us to understand what additional information is needed for the rewriting process to succeed.

8.2. Organization of the Files.

In practice, proofs are printed in electronically created files, that can be reached either directly by the user or automatically by EKL through the command

\[(\text{get-proofs proofname}).\]

Our proofs are distributed in the files described below.

- **NORMAL** contains rewriters to normalize formulas.
- **NATNUM** gives basic facts of arithmetic, i.e. addition, multiplication and ordering.
- **MINUS** introduces more elementary arithmetic, including subtraction.
- **LISPAX** contains the axioms of LISP.
- **ALLP** allows to use the recursive predicate \texttt{allp} to replace bound quantifiers.
- **SET** contains some notions of set theory.
- **LENGTH** contains the definition of \texttt{length} and facts about it.
- **NTH** contains the definitions of \texttt{nth}, \texttt{nthcdr}, \texttt{fposition} and facts about them.
- **APPL** contains the main definitions of application and permutation, in the two different representations. (I) using association lists, and (II) using lists of numbers.
- **SUMS** contains the notions of finite union, finite sums and bound quantifiers \texttt{allnum} and \texttt{some}.
- **MULT** contains the definition of \texttt{of} the function multiplicity.
- **PIGEON** presents the proof of the pigeon-hole principle.
- **ALPIG** contains the application of the pigeon hole to functions represented by association lists.
- **ALPIF** contains an application of the pigeon hole to functions represented by lists of numbers.
- **ASSOC** contains the definition of the operations of composition, identity and inversion of functions, represented as association lists (representation (I)) and proofs of all the facts about permutations.
- **PERMP** contains the definitions of the operation of composition, identity and inversion of functions, using \textit{predicates} in representation (II) and all the facts about permutations.
- **PERMF** contains the definitions of composition, identity and inversion of functions, using \textit{functions} in representation (II) and the corresponding proofs.

The dependency of the files is as follows:

- \texttt{NORMAL}
- \texttt{NATNUM}
- \texttt{MINUS}
- \texttt{LISPAX}
- \texttt{ALLP}
- \texttt{SET}
- \texttt{LENGTH}
- \texttt{NTH}
- \texttt{APPL}
- \texttt{SUMS}
- \texttt{MULT}
- \texttt{PIGEON}
- \texttt{ALPIG}
- \texttt{ALPIF}
- \texttt{ASSOC}
- \texttt{PERMP}
- \texttt{PERMF}
The reason for this organization of the files is to save memory when running the proofs. For the same reason we state our theorems as axioms, we "save" them for "quick-reference" to EKL and then we prove them.

One should not consider these details as merely 'administrative matter'. Quick access to stored information is very important in practice and the amount of memory involved even in easy proofs is considerable. Moreover, just as humans do not look at all the details when reading a proof (but are supposedly able to reconstruct them, if asked), so a computer program checking a proof should remember the relevant facts, not necessarily their proofs.

In the text most of the results are given with their proofs. Some facts of preliminary character are only quoted; their proofs can be found in this Appendix.

### 8.3. file NORMAL.

; propositional schemata, used by the rewriter to normalize expressions
(wipe-out)
(proof normal)

1. (axiom \( \forall p \, q \, r.((p \lor q) \land r) \iff ((p \land r) \lor (q \land r)) \))
   (label normal)

2. (axiom \( \forall p \, q \, r.((p \land q) \lor (r \land q)) \iff ((p \lor q) \land (r \lor q)) \))
   (label normal)
3. (axiom \( \forall p \, q \, r. (r \land (p \lor q)) \Rightarrow (p \lor r) \lor (q \lor r) \))
   (label normal)
4. (axiom \( \forall p \, q \, r. (p \lor q \lor r) \Rightarrow (p \lor q) \lor (q \lor r) \))
   (label normal)
5. (axiom \( \forall p \, q. (\neg (p \lor q)) \Rightarrow (\neg p \lor \neg q) \))
   (label demorgan)
6. (axiom \( \forall p \, q. (p \land q) \Rightarrow p \lor q \))
   (label demorgan)

It would cause combinatorial explosion, to add these to simplifying, or to put everything, say, in conjunctive normal form. So we call them as rewriters when needed.

A few tricks
7. (axiom \( \forall p \, q \, p \Rightarrow (q \lor p) \land (p \lor q) \))
   (label excluded-middle)
8. (derive \( \forall p \, q \, r. (\text{if } p \text{ then } q \text{ else } r) \Rightarrow d \))
   (label trans-cond)
   (save-proofs normal)

8.4. file NATNUM.

We collect here the most elementary facts of arithmetic, omitting their proofs. Our purpose is to have a collection of facts useful in various contexts, rather than to give a systematic treatment of elementary arithmetic from Peano Axioms. Our basic inductive principles include Second Order Induction Axiom and definition of primitive recursive functions and functionals of higher type.

; basic facts about arithmetic and proofs by Bellin
(proof natnum)
1. (decl lessp (type: |ground|ground-truthval|) (syntype: constant)
   (infixname: <) (bindingpower: 920))
2. (decl add1 (type: |ground|ground|) (syntype: constant) (postfixname: I')
   (bindingpower: 975))
3. (decl plus (infixname: +) (type: |ground|ground|ground|ground|)
   (syntype: constant) (associativity: both) (bindingpower: 930))
4. (decl times (type: |ground|ground|ground|ground|) (syntype: constant)
   (infixname: *) (associativity: both) (bindingpower: 935))
5. (decl (i j k n m) (sort: natnum) (type: ground))
6. (decl (a b c set) (type: |ground|truthval|))

; needed axioms on order
7. (axiom \( \forall n. \neg n < n \))
   (label irreflexivity-of-order)
8. (axiom \( \forall m \, k. k < m \Rightarrow k < mk \))
   (label transitivity-of-order)
9. (axiom \( \forall n. \neg n < 0 \))
   (label zeroleast)

; successor and order
10. (axiom \( \forall n. \text{natnum}(n') \))
   (label simpinf 0)

11. (axiom \( \forall n. n < n' \))
   (label successor11 (label succfacts)

12. (axiom \( \forall n. m < n \iff m < n' \))
   (label successor21 (label succ facts)

13. (axiom \( \forall m. n < m < n' \))
   (label successorless) (label succfacts)

14. (axiom \( \forall m. (n' = m') \iff (n = m) \))
   (label successoreq) (label succ facts)

15. (axiom \( \forall n. n = 0 \iff n' = n \))
   (label zeroleast2) (label succ facts)

16. (axiom \( \forall n. 0 < n' \))
   (label zeroleast3) (label succ facts)

17. (axiom \( \forall n. (n' = 0) \))
   (label zero_not_successor) (label succfacts)

; definition of predecessor

18. (decl pred (type: ground + ground) (syntype: constant))

19. (def ax pred \( \forall n. \text{pred}(n') \))
   (label pred_def) (label simpinfo)

20. (axiom \( \forall n. \text{natnum} \ (\text{pred} n) \))
   (label simpinf 0)

; addition

21. (def ax plus \( \forall n. k. 0 + n = n + k = (k + n)' \))
   (label plusdef) (label simpinfo) (label plus facts)

22. (axiom \( \forall n. n + 0 = n \))
   (label simpinf 0) (label plus facts)

23. (axiom \( \forall n. 1 + n = n' + 1 = n' \))
   (label simpinfo) (label plus facts) (label plusdef)

24. (axiom \( \forall n. k + n = n + k = (n + k)' \))
   (label simpinfo) (label plus facts)

25. (axiom \( \forall n. k + n = (n + k)' \))
   (label simpinfo) (label plus facts)

26. (axiom \( \forall n. m. (k + m + k) = (m + n) \))
   (label lpluscan) (label plus facts)

27. (axiom \( \forall n. m. (m + k + n) = (m + n) \))
   (label rpluscan) (label plus facts)

28. (axiom \( \forall n. k + n = 0 \iff 0 + k = 0 \))
   (label addtozero) (label plus facts)

; the effect of the following axiom is to force sums in basically normal
; form: the "simpler" terms will come first

29. (axiom \( \forall n. k + n = n + k \))
   (label commadd) (label plus facts)

; multiplication
30. `(defax times [\(\forall n \cdot 0 \cdot n = 0\) An' k = (n\(\times\)k)\(\times\)k])
   (label timesdef) (label simpinfo) (label timesfacts)
31. (axiom [\(\forall m \cdot \text{natnum}(m \cdot n)\))
   (label simpinfo)
32. (axiom [\(\forall n \cdot 0 = 0\) An' n = m \(\cdot\) A'n = 1 \(\cdot\) n])
   (label timesfacts)
33. (axiom [\(\forall k \cdot n \cdot k' = n \cdot k] = n\))
   (label timesucc) (label timesfacts)
34. (axiom [\(\forall n \cdot k > 0 \cdot ((k \cdot m = k \cdot n) = (m \cdot n))]\)
   (label timescan) (label timesfacts)
35. (axiom [\(\forall n \cdot k > 0 \cdot ((n \cdot k = n \cdot k) = (m \cdot n))]\)
   (label rtimescan) (label timesfacts)
36. (axiom [\(\forall n \cdot n \cdot m = m\cdot n]\))
   (label commutmult) (label timesfacts)
37. (axiom [\(\forall k \cdot n > 0\) An' n \(\cdot\) k = 0 \(\cdot\) k = 0\))
   (label rtimestozer) (label timesfacts)
38. (axiom [\(\forall k \cdot n > 0\) An' k \(\cdot\) m = 0 \(\cdot\) k = 0\])
   (label rtimeszero) (label timesfacts)
39. (axiom [\(\forall k \cdot (k \cdot m) = n \cdot k + n \cdot m] \))
   (label ldistrib) (label timesfacts) (label plusfacts)
40. (axiom [\(\forall m \cdot k \cdot (k \cdot m) = m \cdot n + k \cdot n]\))
   (label rdistrib) (label timesfacts) (label plusfacts)

; distributivity
41. (axiom [\(\forall a \cdot a(0) \cdot a(n \cdot a(n')) = a(\forall n \cdot a(n))]\)
   (label proof-by-induction)
42. (decl npars (type: ?ground*)\))
43. (decl ndf (type: ?ground* ?ground* ?ground*))
44. (decl zcase (type: ?ground* ?ground*))
   (axiom
   \[\forall n \cdot zcase \cdot n \cdot def.
   \((\exists \text{fun.}(\forall \text{npars} \cdot \text{fun}(0, \text{npars}) = \text{zcase}(\text{npars}) \cdot \text{fun}(n', \text{npars}) = \text{ndef}(\text{fun}(\text{ndef}(n, \text{fun}(n, \text{ndef}(n, \text{npars})), \text{npars}))))\])\)
   (label inductive-definition)

; the following is a form of double induction
45. (axiom [\(\forall a \cdot (a(2, 0) \cdot a(2, n)) = (a(2, n) \cdot a(2, n')) \cdot \forall n \cdot a(2, (n, m))]\)
   (label proof-by-doubleinduction)

; general definitional principle for inductive functions
46. (decl (arb arb1 arb2) (type: ?arbitrary*)\))
47. (decl indfn (type: ?ground* !arb = ?arb*))
48. (decl (def-fun) (type: ?ground * !arb = ?arb*))

; this is the primitive recursive schema for definition on ALL higher type functionals:
; note the use of the variable type in declarations;
; in this way we can specialize to ANY type.

9. (axiom
   \[ \text{indfn arb.3def_fun.vn.def_fun(0)=arb} \]
   \[ \text{def_fun(n')=indfn(n,def_fun(n))} \]
   (label high-order-natnum-definition)

; well-foundedness

10. (axiom \[ \text{3desc.vn.desc(n')<desc(n)} \]
    (label infinite-descent)
    (save-proofs natnum)

8.4.1. More Arithmetic.

; proofs of facts of arithmetic
(wipe-out)
(get-proofs normal)
(get-proofs natnum)
(label simpinfo zero-not-successor) ; add these to simpinfo for now
(label simpinfo zeroleast1)
(label simpinfo successorless)
(label simpinfo successoreq)
(label simpinfo zeroleast3)

(proof lesseq)
; an easy consequence of the axioms in natnum

1. (ue (a [\lambda n. n=n']) proof_by_induction)
   (label simpinfo) (label successorfacts)

2. (decl lesseq (type: [\text{ground*ground=truthval}]) (infixname: \[\leq\])
   (bindingpointer: 920)

3. (define lesseq [\forall m. (m \leq n)=(m=n\lor m<n)]
   (label lesseqdef)

; successorlesseq

4. (trw \forall m. n. m'n'\leqm'n
   (label successorlesseq) (label successorfacts) (label simpinfo)

; trans_lesseq

5. (trw \forall m. k. n\leqm\lor k\leqn
   (label transitivity-of-order)

; \forall m. k. n'\leqm\lor k'
   (label trans_lesseq)

; less_lesseq_fact1

6. (trw \forall m. k. n\leqm\lor k\leqn
   (label transitivity-of-order)

; \forall m. k. n\leqm\lor k
   (label less_lesseq_fact1)

; zeroleast

7. (ue (a [\lambda n. 0\leq n]) proof_by_induction (part 1 (open lesseq)))
   ; \forall n. 0\leq n
(label zeroleast) ■
; oneleastsucc
8. (trw |0 ≤ n | zeroleast)
   ; 0 ≤ n'
9. (trw * (nuse successorlesseq))
   ; 1 ≤ n'
   (label oneleastsucc) ■
   ; zero non less successor
10. (trw |m = 0 ∧ n < m|)
    ; ¬(m = 0 ∧ n < m)
11. (derive |∀ m. n < m → m = 0| * )
    (label simpinfo)(label zero-non-less-successor) ■
    ; a couple of very trivial facts
    ; succ_less_less
12. (trw |∀ m. n < m → m < n| transitivity-of-order successor11
    (label succ-less-less) ■
    ; succ_lesseq_lesseq
13. (derive |M = N ∧ M < N| successor1)
14. (trw |∀ m. m < N ∧ m ≤ m| (open lesseq)
    ; sucless-less * (use normal mode: always)
    ; ∀N. N ≤ N
    (label succ_less_less) ■
    ; lesseq lesseq succ
15. (trw |∀ m. n ≤ m | (open lesseq) (use normal mode: always) (successor1 transitivity-of-order))
    (label lesseq_lesseq_succ)
    ; "m less succ of n" implies "m lesseq n"
16. (ue (a |λn. n < 0 ≤ n|) proof-by-induction
    ; ∀N. n < 1 ≤ N
17. (ue (a2 |λn. m < n ≤ m|) proof-by-doubleinduction zeroleast)
    ; ∀N. M < N ≤ M
    (label less_sucless)
    ; "n less than m" implies "suc of n lesseq m"
18. (ue (a |λn. 0 ≤ n < m|) proof-by-induction
    ; ∀N. 0 < N ≤ 1
19. (ue (a2 |λn. m < m ≤ m|) proof-by-doubleinduction zeroleast)
    (label less_lesseqsuccess)
    ; "n lesseq m" and "m lesseq n" implies "n equal m"
20. (ue (a2 |λn. m ≤ m ≤ m|) proof-by-doubleinduction
    ; ∀N. m ≤ m ≤ m (use normal mode: always))
(label leq_leq_eq) ■
; trichotomy
21. (rew zeroleast (open lesseq))

22. (ue (a2 | \( \lambda \) m. m.m\textless\textless n\textless\textless m.n\lesseq m |) proof-by-doubleinduction
(use normal mode: always) ■)
; \( \forall \) M.M\textless\textless M\textless\textless M
(1 a b e l trichotomy) ■

8.4.2. Subtraction.

; minus
(proof minus)

1. (decl minus (type: |ground*ground=ground|) (infixname: [-])
(bindingpower: 940)) ■

2. (define minus \( \forall \) n.m-0=mm-\( \lambda \) (n')=pred(m-n)| inductive_definition)
(label minusdef)
; minus sort
; the following proof works because pred is a total function

3. (ue (a | \( \lambda \) n.\forall x.\textsf{natnum}(k-n)) proof-by-induction
(part 1 (open minus))
; \( \forall \) N.\textsf{NATNUM}(n-N)
(label simpinfo) (label minus-sort) ■

; minusfact3

4. (ue (a | \( \lambda \) n.m\textlesseq m')=m-n| proof-by-induction
(part 1 (open minus pred))
; \( \forall \) N.M'.\textsf{PRED}(M'-N)=M-N

5. (ue (a2 | \( \lambda \) m.n\textlesseq m\textlesseq n) proof-by-doubleinduction (open minus)
(use * mode; always) succ-less-less)
; \( \forall \) M.M\textlesseq M\textlesseq M
(label minusfact ■)

; minusfact5

6. (ue (a | \( \lambda \) n.\textlesseq m\textlesseq n')=n| proof-by-induction)
; \( \forall \) M.<\textsf{PRED}(M)'=N
(label minusfact5) ■

; successor minus

7. (ue (a | \( \lambda \) n.m\textlesseq m'\textlesseq n=\( \textsf{M-n} \)' |) proof-by-induction
(use -2 -3 successor1 succ-less-less mode: exact)
(use * ue: ((n, m-n)))(part 1 (open minus pred))
; \( \forall \) M.'M'-\textlesseq M = (M-N)

8. (derive \( \forall \) m.n\textlesseq n\textlesseq m\textlesseq m'\textlesseq n=\( \textsf{m-n} \)'| (* less_succ_lesseq))
(label successor-minus) ■

; predCancellation

9. (rew \( \forall \) m.n\textlesseq m\textlesseq m'\textlesseq n=\( \textsf{m-n} \) successor-minus)
; \( \forall \) M.M\textlesseq M\textlesseq M
(label predCancellation) (label minusfact7) ■
10. (trw \(\forall n. m.n<m \Rightarrow (m-n')'=m-n\))(use minusfact ue: ((n.|m-n|)))

11. (rw successor-minus (open lesseq) (use normal mode: always))

12. (derive \(\forall n. m.n<m \Rightarrow (m-n')'=m-n\)*)

13. (ue (a \(\lambda n. 0<n\N\text{pred}(n)<n\)) proof_by_induction successor11

14. (ue (a2 \(\lambda n. m.n<n\N\text{pred}(n)<n\)) proof_by_doubleinduction

15. (rw successor-minus (open lesseq) (use normal mode: always))

16. (derive \(\forall n. m.n=m \Rightarrow (m-n')'=m-n\)*)

17. (ue (a \(\lambda n. n-n=0\)) proof_by_induction

18. (ue (a \(\lambda n. m.n<n\)) successor-minus (open lesseq))

19. (ue (a \(\lambda n. 0<n\N\text{pred}(n)<n\)) proof_by_induction

20. (ue (a \(\lambda n. m.n<n\)) proof_by_induction (open lesseq)

21. (trw \(\forall n. m.n<n\N\text{lesseq}(n)=n\)) (use normal mode: always) *

22. (derive \(\forall k. k<n \Rightarrow (n-k)'=(n-k)\)*)

23. (ue (a2 \(\lambda n. m.n<m \Rightarrow (m-n')'=m-n\)) proof_by_doubleinduction

24. (ue (a2 \(\lambda n. m.n<n\)) proof_by_doubleinduction

25. (rw* (use less-succ-lesseq mode: exact)

\(\forall n. m.n<n\N\text{lesseq}(n)=n\))
The following two facts are needed in the induction step of the proof of the pigeon-hole principle.

**Lemma.** *(Add Lesseq)*

\[ \forall n \, \forall k \, n \in \mathbb{N}, k \in \mathbb{N} \implies n \leq k \]

The lower bound of a sum is the sum of the lower bounds. We use by double induction.

**Proof.**

1. (trw \{ \forall n \, \forall k | \text{use zeroleast} \})

2. (trw * (nse successorlesseq))

The following line gives one base case, by a subordinate induction: the preceding line, with an automatic substitution of \( n + k \) for \( n \), proves the induction step for it.

3. (ue (a \{ \forall n \, \forall k \, n \in \mathbb{N}, k \in \mathbb{N} \implies \}) proof-by-induction *)

The other base case reduces to a tautology, using the next line.

4. (trw \{ \forall n \in \mathbb{N} \implies \})

The induction step follows automatically from the line *Successorlesseq* (proof minus) which is in "simpinfo".

5. (ue (a2 \{ \forall n \, \forall k \, n \in \mathbb{N}, k \in \mathbb{N} \implies \}) proof-by-doubleinduction -2 (use * mode: always))

**Lemma.** *(Add One)*

\[ \forall k \, n \in \mathbb{N} \implies n + k \in \mathbb{N} \]

If the sum of two variables equals the sum of the lower bounds, then the values of the variables must be their lower bounds.

**Proof.** Again we use double induction. One base case (i.e. \( n = 0 \)) is also proved by double induction.

Here the other base case \( (k = 0) \) and the induction step are trivial, since the antecedent becomes false. In the other base case, when \( m = 0 \), we first rewrite \( 1 \leq k \) as \( 1 < k \lor 1 = k \); i.e. we
"open" the symbol \texttt{lesseq} and then normalize. We obtain either a contradiction in the antecedent $(1 < k \land 1 = k)$ or the desired result.

The next line is now easy: the base case $n = 0$ is the last line. In the other base case $m = 0$, we get $n = 0$ after opening $\leq$ (since $n < 0$ is impossible) and therefore also $1 = 0 + k$. The induction step follows from the lines \texttt{Successorlesseq}, (proof \texttt{MINUS}) and \texttt{Successorleq} and \texttt{Plusfacts} (proof \texttt{NATVW}) that are in \texttt{simpinfo}.

\label{add:one}

\ promot-by-doubleinduction
\ (part 1#2 (open \texttt{lesseq}))
\ (part 1#1 (use *))
\ (label \texttt{add-one})

\section{file LISPAX.}

We define the basic functions of LISP and give their properties as axioms. We have basic principles of induction on lists and S-expressions and primitive recursive definition of LISP functions and higher order functionals.

\begin{verbatim}
(proof lispax)

;;;declarations: note that t and nil are not declared - EKL knows about them
;;;since they are attached, we don't need to say things like null nil etc.

1. (decl car (unaryname: car) (type: |ground-ground|) (syntype: constant)
   (bindingpower: 950))

2. (decl cdr (unaryname: cdr) (type: |ground-ground|) (syntype: constant)
   (bindingpower: 950))

3. (decl atom (unaryname: atom) (type: |ground-truthval|) (syntype: constant)
   (bindingpower: 750))

4. (decl null (unaryname: null) (type: |ground-truthval|) (syntype: constant)
   (bindingpower: 750))

5. (decl listp (unaryname: listp) (type: |ground-truthval|) (syntype: constant)
   (bindingpower: 750))

6. (decl alistp (unaryname: alistp) (type: |ground-truthval|)
   (syntype: constant) (bindingpower: 750))

7. (decl sexp (unaryname: sexp) (type: |ground-truthval|) (syntype: constant)
   (bindingpower: 750))

8. (decl (u v a> (type: |ground|) (sort: |listp|))

9. (decl (x y z) (type: |ground|) (sort: |sexp|))

10. (decl (xa ya za) (type: |ground|) (sort: |atom|))

11. (decl (phi) (type: |ground-truthval|))

12. (decl cons (type: |ground-ground|) (syntype: constant)
    (infixname: .) (pref ixname: cons>) (bindingpower: 850))

;;;basic axioms and sort info

13. (axiom |xa.sexp(xa)|)
   (label simpinfo)
\end{verbatim}
14. (axiom \(\forall u.\text{xexp }u\))
   (label simpinfo)

15. (axiom \(\forall x.u.\text{listp }x.u\))
   (label simpinfo)

16. (axiom \(\forall u.\text{null }u \odot \text{listp }cdr u\))
   (label simpinfo)

17. (axiom \(\forall u.\text{null }u \odot \text{sexp }\text{car }u\))
   (label simpinfo)

18. (axiom \(\forall x.\text{atom }x \odot 3 \text{sexp }\text{car }x\))
   (label simpinfo)

19. (axiom \(\forall x.\text{atom }x \odot \text{sexp }\text{cdr }x\))
   (label simpinfo)

20. (axiom \(\forall x.y.\text{xexp }x.y\))
   (label simpinfo)

21. (axiom \(\forall x.y.\text{atom }x.y\))
   (label simpinfo)

22. (axiom \(\forall x.u.\text{null }x.u\))
   (label simpinfo)

23. (axiom \(\forall u.\text{null }u \odot u = \text{nil}\))
   (label simpinfo)

24. (axiom \(\forall x.y.\text{car }x.y = x\))
   (label simpinfo)

25. (axiom \(\forall x.y.\text{cdr }x.y = y\))
   (label simpinfo)

26. (axiom \(\text{car }\text{nil} = \text{nil}\))
   (label simpinfo)

27. (axiom \(\text{cdr }\text{nil} = \text{nil}\))
   (label simpinfo)

28. (axiom \(\forall u.\text{null }u \odot (\text{car }u.\text{cdr }u = u)\))
   (label simpinfo) (label cons-car-cdr)

29. (axiom \(\forall x.\text{atom }x \odot (\text{car }x.\text{cdr }x = x)\))
   (label simpinfo) (label cons-car-cdr)

;; induction

30. (axiom \(\forall \phi.\phi(\text{nil}) \lor (\forall x.\phi(x)) \lor (\forall u.\phi(u))\))
   (label listinduction)

31. (decl pars (type: \text{[\emph{ground}]*})))

32. (decl \(\text{df}1 \text{df}2\) (type: \text{[\emph{ground}*\text{\emph{ground}}]*})))

33. (decl nilcase (type: \text{[\emph{ground}*\emph{ground}]*})))

34. (axiom \(\forall \text{df}1\text{ nilcase }\text{def}.
   (\exists \text{fun}.(\forall x.u.\text{fun}(\text{nil},pars) = \text{nilcase}(pars) \land
   \text{fun}(x.u,pars) = \text{def}(x,u,\text{fun}(u,\text{df}(x,pars)),pars)))))
   (label listinductiondef)

35. (axiom \(\forall \phi.\phi(\text{atom }x \odot \phi(x)) \lor (\forall x.y.\phi(x) \land \phi(y) \land \phi(x.y)) \lor (\forall x.\phi(x))\))
   (label sexpinduction)
36. (axiom

\[ \forall \text{atom} \, \text{defexp} \, \text{df1} \, \text{df2} \, .3\text{fun}. \]

\[ V\text{pars} \, x \, y \, z. \]

\[ (\text{atom} \, z) \]

\[ \text{fun}(z, \text{pars}) = \text{atomcase}(z, \text{pars}) \wedge \]

\[ (\text{fun}(x, y, \text{pars}) = \]

\[ \text{defexp}(x, y, \text{fun}(x, y, \text{pars}), \text{fun}(y, \text{df2}(x, y, \text{pars}), \text{pars}))) \]

\[ (\text{label sexpinductiondef}) \]

; a high order definition schema when above is insufficient

37. (decl (arb arbl arbl2) (type: |?arbitrary|))

38. (decl bigfun (type: |ground|+|ground|+|arb|+|arb|)

39. (decl (defined-fun atom-fun) (type: |ground|+|arb|))

; this is the primitive recursive schema for definition on ALL
; higher type functionals:
; note the use of the variable type in declarations;
; in this way we can specialize to ANY type.

40. (axiom \[ \forall \text{bigfun} \, \text{atom-fun} \, .\text{defined-fun}. \]

\[ \forall x \, y. \]

\[ (\text{atom} \, x) \]

\[ \text{defined-fun}(x) = \text{atom-fun}(x) \wedge \]

\[ (\text{defined-fun}(x, y) = \]

\[ \text{bigfun}(x, y, \text{defined-fun}(x), \text{defined-fun}(y))) \]

\[ (\text{label high-order-definition}) \]

;; lists of variable numbers of arguments don't require special treatment,
;; since we have list types now

41. (decl list (type: |ground|+|ground|+|ground|+|syntype|: constant))

42. (decl lst (type: |ground|+|lst|))

43. (axiom |\forall \text{list}() = \text{nil}|)

\[ (\text{label simpinf o}) \]

44. (axiom |\forall \text{lst}. \text{listp}(\text{list}(\text{lst})))\]

\[ (\text{label simpinf o}) \]

45. (axiom |\forall x \, \text{lst}. \text{list}(x, \text{lst}) = x. \text{list}(\text{lst})|)

\[ (\text{label listdef})(\text{label simpinfo}) \]

;; this is lisp's append. while it can be proved associative, it
;; is convenient in proofs of other theorems to have it declared
;; associative.

46. (decl append (type: |ground|+|ground|+|ground|+|ground|) (syntype: constant)

\[ (\text{associativity: both}) (\text{infixname: *}) (\text{bindingpower: 840}) \]

47. (defax append |\forall x \, u. \text{v.nil} = \text{v} = \text{v} = \text{v} = x. (u*v)|)

\[ (\text{label appenddef})(\text{label simpinf o}) \]

48. (axiom |\forall u. \text{v.listp}(u*v)|)

\[ (\text{label simpinfo})(\text{label listappend}) \]

49. (axiom |\forall u, u*\text{nil} = u|)

\[ (\text{label simpinfo}) \]

50. (axiom |\forall x \, (x.\text{nil})*v = x. v|)

\[ (\text{label simpinfo}) \]

;; map functions on lists

51. (decl (allp somep) (syntype: constant) (type: |(\#phi)\#ground\#truthval|))
52. (defax allp
   : (\( \forall \phi\) \( x.\) allp(\( \phi,\) nil))
   \[ allp(\( \phi,\) x.u) = \text{if } \phi(x) \text{ then allp(\( \phi,u\)) else false} \]
   (label allpdef)
53. (defax somep
   : (\( \forall \phi\) \( x.\) -somp(\( \phi,\) nil))
   \[ somep(\( \phi,\) x.u) = \text{if } \phi(x) \text{ then true else somep(\( \phi,u\))} \]
   (label somepdef)
54. (defax mapcar
   : (\( \forall fn\) \( x.\) mapcar(\( fn,\) nil))=nil\( \land \)mapcar(\( fn,\) x.u)=fn(x).mapcar(\( fn,u\))
   (label mapcardef)
55. (decl (alist) (type: ground) (sort: alistp))
56. (axiom |\( \forall u.\) alistp \( u \equiv (\neg \text{null } u \land \text{atom } \text{car } u \land \text{atom } \text{car } (\text{car } u) \land \text{alistp}(\text{cdr } u)) \)
   (label alistdef)
57. (axiom |\( \forall xa,y.\) alistp nil \( \land \)alistp (\( xa,y.\) alist)\)
   (label simpinf 0)
58. (decl assoc (type: \( |\text{ground}\times \text{ground} \to \text{ground}| \)) (syntype: constant)
59. (defax assoc
   |\( \forall xa,y.\) assoc(x,\( nil \equiv nil\)
   \[ \text{assoc}(x,\( xa,y.\) \( .\) \( alist \)) = \text{if } x=x \text{ then } xa,y \]
   else \( \text{assoc}(x,\( al\)\( ist\)) \)
   (label assocdef)
60. (axiom |\( \forall xa,y.\) \( \text{sexp } \text{assoc}(x,\( \text{alist} \)) \)\)
   (label simpinf 0)
61. (decl member (type: \( |\text{ground}\times \text{ground} \to \text{truthval}| \)) (syntype: constant)
62. (defax member
   |\( \forall x,y,u.\) member(x,\( nil \equiv nil\)
   \[ \text{member}(x,y,u) = (x=y \land \text{member}(x,u)) \]
   (label memberdef)
63. (decl uniqueness (type: \( |\text{ground}\to \text{truthval}| \))
64. (defax uniqueness
   |\( \forall u.\) uniqueness nil \( \equiv \)
   \[ \text{uniqueness}(x,u) \equiv (\text{member}(x,u) \land \text{uniqueness}(u)) \]
   (label uniquenessdef)
65. (ue (\( \phi\) \( \lambda u.\) \( \text{sexp } \text{car}(u)\)) \( \text{listinduction}\)
   (label simpinfo)
66. (ue (\( \phi\) \( \lambda u.\) \( \text{alistp } \text{cdr}(u)\)) \( \text{listinduction}\)
   (label simpinfo)
   (save-proofs lispax)

8.5.1. file ALLP.

:properties of allp
(wipe-out)
(get-proofs lispax)
1. (truv \forall \phi x u. allp(\phi, x, u) \Rightarrow allp(\phi, u) \| (open allp))
   (proof allp)

2. (ue (\phi | \alpha u. \forall y. member(y, u) \Rightarrow \forall \phi y (\forall \phi y member(y, u) \Rightarrow allp(\phi, y)))
   listinduction (open allp member) (use normal mode: always)
   (label allpfact) \]

3. (ue (\phi | \alpha u. member(x, u) \Rightarrow allp(\phi, x, u) \Rightarrow \forall \phi x (\forall \phi x member(x, u) \Rightarrow allp(\phi, u)))
   listinduction (open allp member) (use normal mode: always)
   (label allp-introduction) \]

4. (ue (\phi | \alpha u. member(y, u) \Rightarrow allp(\phi, y))
   listinduction (open allp member) (use normal mode: always)
   (label allp-implication) \]

(proof somepprop)

1. (ue (\phi | \alpha u. member(y, u) \Rightarrow \forall \phi y (\forall \phi y member(y, u) \Rightarrow \forall \phi y somep(\phi, y)))
   listinduction (open somep member) (use normal mode: always)
   (label somepfact) \]

8.6. file SET.

(useful set theory)

(proof sets)

(all urelements will be S-expressions)

(all S-expressions will be urelements)

1. (decl (xv yv zv) (type: [ground]) (sort: urelement))
2. (decl (av bv) (type: [ground-truthval])

3. (axiom \forall x. urelement x)
   (label simpinfo)

4. (axiom \forall xv. exp(xv))
   (label simpinfo)

5. (decl epsilon (type: [ground-truthval]) (infixname: \epsilon) (bindingpower: 925))
6. (define epsilon \forall \epsilon xv. \epsilon x \epsilon x xv (label epsilondef))
7. (axiom \( \forall x \forall y. (x = y \equiv (x \in y)) \) \\
(label set-extensionality)

8. (decl intersection (type: \( \forall a \forall b \forall c \)) \\
(infixname: \( \cap \)) (prefixname: intersection))
9. (define intersection \( \forall x \forall y. (x \in y \equiv (x \cap y)) \)) \\
(label interdef)

10. (decl union (type: \( \forall a \forall b \forall c \)) \\
(infixname: \( \cup \)) (prefixname: union))
11. (define union \( \forall x \forall y. (x \cup y) \equiv (x \cup y) \)) \\
(label uniondef)

12. (decl inclusion (type: \( \forall a \forall b \forall c \forall x \)) \\
(infixname: \( \subseteq \)) (prefixname: inclusion))
13. (define inclusion \( \forall x \forall y. (x \subseteq y) \equiv (x \subseteq y) \)) \\
(label inclusiondef)

14. (defax emptyset \( \forall a \forall b \forall c \)) \\
15. (defax emptytyp \( \forall a \forall b \forall c \)) \\

;the set of occurrences of an S-exp

16. (decl mkset (type: \( \forall a \forall b \forall c \)) \\
17. (define mkset \( \forall x. (\text{mkset}(x) = (x = x)) \)) \\
(label mkset_def)

;the set of members of a list

18. (decl mklset (type: \( \forall a \forall b \forall c \)) \\
19. (define mklset \( \forall u. (\text{mklset}(u) = \text{ax. member}(x, u)) \)) \\
(label mklsetdef)

(proof setfacts)

;fact about mkset and mklset

1. (trw \( \forall u. (\text{member}(x, u) \land \text{mkset}(y) \land \text{mklset}(u)) \)) \\
(open mkset mkset inclusion) (der))

;\text{mkset}(y) = \text{mklset}(u) \\
(label mkset_mklset)

;double inclusion

2. (ue ((av. av)(bv. bv)) set-extensionality (open epsilon)) \\
(\( \forall x. \text{AV} = \text{BV} \)) \\
(proof length)

3. (derive \( \forall c. \text{AV} = \text{BV} \)) \\
(label double-inclusion)

8.7. file LENGTH.

;facts about lengths of lists \\
(get-proofs set) \\
(get-proofs minus)

(proof length)

1. (decl length (type: Iground+ground)) (unaryname: length) \\
2. (define length \( \forall x. (\text{length}(x, u) = (\text{length}(u)) \))

;now we need to tie up natural numbers and s-expressions
(axiom \(\forall n. \text{sexp } n\))
(label simpinf o)
(axiom \(\forall n. \neg \text{null}(n)\))
(label simpinf o)
(proof sets)
;all numbers will be urelements
(axiom \(\forall n. \text{urelement } n\))
(label simpinf o)
;forms of doubleinduction
(proof listinduction)
;a useful principle which follows from listinduction
;corresponds to a proof by cases argument s
(trw \(\forall \phi. (\phi(\text{nil}) \land \forall x. \phi(x,x)) \land \forall u. \phi(u)\)| listinduction)
;\(\forall \phi. (\phi(\text{nil}) \land \forall u. \phi(x,x)) \land \forall u. \phi(u)\))
8.9. Nth.

1. (decl nth (syntype: constant) (type: |ground|ground-|ground|))
2. (defax nth |∀x u n.nth(nil, n) = nil \& nth(u, 0) = car u \& nth(x, u, n') = nth(u, n))
   (label simpinfo) (label nthdef)
   ; prove by double induction the well-definedness of nth
   ; for the obvious range
3. (ue (phi |λu n.sexp nth(u, n)) doubleinduction1 (open nth))
   ; ∀u n.sexp nth(u, n)
   (label simpinfo) (label sexp_nth)
   ; prove by double induction the membership of nth in the original list
4. (ue (phi |λu n.0<length u \& member nth(u, 0), u)) listinduction
   (open length nth member)
   ; ∀u.0<length u \& member nth(u, 0), u)
   (ue (phi |λu n.n<length u \& member nth(u, n), u)) doubleinduction1
   (open length nth) (use memberdef mode: always) (use *)
   ; ∀u n.n<length u \& member nth(u, n), u)
   (label nthmember)
8.9.1. Member Nth.

;member_nth
(proof member-nth)
1. (assume |(member(y,u)\exists n.n<length u\Andth(u,n)=y)|)
   (label m_n1)
2. (assume |y=x|)
   (label m_n2)
3. (trrew |0<length(x.u)\Andth(x.u,0)=y| (open nth) * )
   ;0<LENGTH (X.U)\Andth(X.U,0)=Y
4. (derive |\exists n.n<length(x.u)\Andth(x.u,n)=y| * )
   (label m_n3)
5. (assume |member(y,u)|)
6. (define nv |nv<length u\Andth(u,nv)=y|(m_n1 *))
7. (trrew |nv'<length(x.u)\Andth(x.u,nv')=y| (open nth) * )
   ;NV'<LENGTH (X.U)\Andth(X.U,NV')=Y
8. (derive |\exists n.n<length(x.u)\Andth(x.u,n)=y| * )
   (label m_n4)
9. (assume |member(y,x.u)|)
   (label m_n5)
10. (rew * (open member))
    ;Y=XuMEMBER(Y,U)
11. (cases * m_n3 m_n4)
    ;\exists N<LENGTH (X.U)\Andth(X.U,N)=Y
12. (ci m_n5)
    ;MEMBER(Y,X.U)\exists N<LENGTH U'\Andth(X.U,N)=Y
13. (ci m_n1)
14. (ue (phi |\lambda u.member(y,u)\exists n.n<length u\Andth(u,n)=y|) listinduction
    (open member nth) * )
    ;\lambda u.member(y,u)\exists N<LENGTH U'\Andth(U,N)=Y
    (label member-nth)

8.10. Nthcdr.

(proof nthcdr)
1. (decl nthcdr (syntype: constant) (type: |ground*ground=ground|))
2. (defax nthcdr |\forall x u n.nthcdr(nil,n)=nil\Andthcdr(u,0)=uA
   nthcdr(x,u,n')=nthcdr(u,n)|)
   (label simpinfo) (label nthcdrdef)
3. (ue (phi3 |\lambda u.n.listp nthcdr(u,n) |) doubleinduction)
   ;\lambda u.n.LISTP NTHCDR(U,N)
   (label simpinfo)
4. (ue (phi |\lambda u.0<length u\Andth(u,0).nthcdr(u,0')=u|) listinduction
\section{8}

(part 2 (nuse nthcdr))
\[\forall u.0<\text{length } u \Rightarrow \text{nth}(u,0) = \text{nthcdr}(u,1) = u\]
(label nth_nthcdr_zero)

\text{car nthcdr}

5. \text{(use (phi3 \[\forall u.\text{n\text{-}car}(\text{nthcdr}(u, n)) = \text{nth}(u, n)\]) doubleinduction)}
\[\forall u.\text{car} \text{nthcdr}(u, n) = \text{nth}(u, n)\]
(label car_nthcdr)

\text{cdr nthcdr}

6. \text{(use (phi \[\forall u.\text{cdr}(\text{nthcdr}(u, 0)) = \text{nthcdr}(u, 0')\]) listinduction)}
\[\forall u.\text{cdr} \text{nthcdr}(u, 0) = \text{nthcdr}(u, 0')\]

\text{nthcdr car cdr}

7. \text{(use (phi3 \[\forall u.\text{n\text{-}cdr}(\text{nthcdr}(u, n)) = \text{nthcdr}(u, n')\]) doubleinduction)}
\[\forall u.\text{n\text{-}cdr} \text{nthcdr}(u, n) = \text{nthcdr}(u, n')\]
(label cdr_nthcdr)

\text{nthcdr car cdr}

8. \text{(use (phi \[\forall u.\text{thc}(\text{nthcdr}(u, 0)) = \text{nth}(u, 0) \cdot \text{nthcdr}(u, 0')\]) listinduction)}
\[\forall u.\text{thc} \text{nthcdr}(u, 0) = \text{nth}(u, 0) \cdot \text{nthcdr}(u, 0')\]

\text{nth in nthcdr}

9. \text{(use (phi3 \[\forall u.\text{length}(u) \cdot \text{nthcdr}(u, n) = \text{nth}(u, n) \cdot \text{nthcdr}(u, n')\]) doubleinduction)}
\[\forall u.\text{length}(u) \cdot \text{nthcdr}(u, n) = \text{nth}(u, n) \cdot \text{nthcdr}(u, n')\]
(label nthcdr_car_cdr)

\text{length nthcdr}

10. \text{(use (phi3 \[\forall u.\text{nth}(u, n) = \text{nth}(u, n) \cdot \text{nthcdr}(u, n)\]) doubleinduction)}
\[\forall u.\text{nth}(u, n) = \text{nth}(u, n) \cdot \text{nthcdr}(u, n)\]
(use nthmember mode: exact)

\text{last nthcdr}

11. \text{(use (phi \[\forall u.\text{nth}(u, n) = \text{nth}(u, n) \cdot \text{nthcdr}(u, n)\]) listinduction)}
\[\forall u.\text{nth}(u, n) = \text{nth}(u, n) \cdot \text{nthcdr}(u, n)\]

\text{nth in nthcdr}

12. \text{(use (phi3 \[\forall u.\text{n\text{-}nth}(u) \cdot \text{nth}(u, n) = \text{nth}(u, n) \cdot \text{nthcdr}(u, n)\]) listinduction)}
\[\forall u.\text{n\text{-}nth}(u) \cdot \text{nth}(u, n) = \text{nth}(u, n) \cdot \text{nthcdr}(u, n)\]

\text{nthcdr car cdr}

13. \text{(use (phi3 \[\forall u.\text{length}(u) = \text{length}(u)\]) doubleinduction)}
\[\forall u.\text{length}(u) = \text{length}(u)\]

\text{last nthcdr}

14. \text{(use (phi \[\forall u.\text{nthcdr}(u, \text{length}(u)) = \text{nil}\]) listinduction)}
\[\forall u.\text{nthcdr}(u, \text{length}(u)) = \text{nil}\]
(label last_nthcdr)

; trivial nthcdr

15. (ue (phi3 (lambda (u n) (nthcdr (length u) n)) (nnthcdr u n) = nill))
(doubleinduction)
(part 1 (open lesseq))
(label trivial_nthcdr)

; allp nthcdr

16. (ue (phi3 (lambda (a u) (allp a (nthcdr u n)))) (nallp a (nthcdr u n)))
(doubleinduction)
(open allp)
(label allp_nthcdr)

8.10.1. Nthcdr Induction.

Using induction on n, we show:

\[ \forall n. \phi(\text{nthcdr}(u, \text{length}(u) - n)). \]

For n = 0, nthcdr(u, length(u) - n) is NIL, and we have \( \phi(\text{nill}) \).

Assume \( \phi(\text{nthcdr}(u, \text{length}(u) - n)) \). Since subtraction is defined as a total function on nonnegative integers, we have for \( n_2 \text{length}(u), \)

\[ \text{length}(u) - n = 0 = \text{length}(u) - n'. \]

so in this case the induction step is trivial.

If \( n < \text{length}(u) \), then

\[ \text{length}(u) - n = (\text{length}(u) - n')' \]

by elementary arithmetic and

\[ \forall k. k < \text{length}(u) \Rightarrow (\phi(\text{nthcdr}(u, k')) \cup \phi(\text{nthcdr}(u, k))) \]

is the inductive step of our principle. We can complete the induction step by letting k to be \( \text{length}(u) - n' \):

\[ \phi(\text{nthcdr}(u, \text{length}(u) - n)) \cup \phi(\text{nthcdr}(u, \text{length}(u) - n')). \]

Finally it is convenient to write

\[ \text{nthcdr}(u, k) \]

as

\[ \text{nth}(u, k) . \text{nthcdr}(u, k') \]

( using lemma Nthcdr Car Cdr).
(proof nthcdr_induction)

1. (assume \( \forall n. n < \text{length}(u) \rightarrow \phi(nthcdr(u, n')) \) \( \rightarrow \)
   \( \phi(nthcdr(u, nthcdr(u, n')))) \)
   (label n_i_1)
   ;deps: (N-I-1)

2. (derive \( \forall n. n < \text{length}(u) \rightarrow \)
   \( \phi(nthcdr(u, n')) \) \( \rightarrow \)
   \( \phi(nthcdr(u, nthcdr(u, n')))) \)
   (use nthcdr_car_cdr mode: always)
   (label n-i-2)
   ;deps: (N-I-1)
   ; two cases

3. (derive \( \text{length}(u)x\forall n < \text{length}(u) \rightarrow \) trichotomy2)
   (label n-i-cases)
   ;one completely trivial

4. (assume \( \text{length}(u) \leq n! \))
   (label n-i-cl)
   ;deps: (N_I_C1)

5. (trw \( \phi(nthcdr(u, \text{length}(u)-n)) \)
   \( \rightarrow \)
   \( \phi(nthcdr(u, \text{length}(u)-n')))) \)
   (open minus pred)(use total-subtraction n-i-cl mode: always)
   (label n_i_case1)
   ;PHI(nthcdr(u, length u-N))PHI(nthcdr(u, length U-N'))
   ;deps: (N_I_C1)
   ;the other quite trivial too...

6. (assume \( n < \text{length}(u) \))
   (label n_i_c2)
   ;deps: (6)

7. (ue (n | length(u)-(n')) n - i - 2
   (use n_i_c2)(use minusfactll ue: ((n | length(u))))
   (use minusfact10 mode: exact direction: reverse>)
   (label n_i_case2)
   ;PHI(nthcdr(u, length u-N))PHI(nthcdr(u, length U-N'))
   ;deps: (N-I-1 N_I_C2)

8. (cases n-i-cases n_i_case1 n_i_case2)
   ;PHI(nthcdr(u, length u-N))PHI(nthcdr(u, length U-N'))
   ;deps: (N-I-1)

9. (ue (a | \( n \rightarrow \phi(nthcdr(u, length(u)-n))) \)
   proof-by-induction *
   (part 1 (use last-nthcdr mode: exact) (open minus))
   (label n-i-5)
   ;PHI(NIL)>\( \forall n. \phi(nthcdr(u, length U-N)))
   ;deps: (N-I-1)

;cosmetics

10. (assume \( \phi(nil) \))
    (label n-i-6)
    ;deps: (10)

11. (derive \( \forall n. \phi(nthcdr(u, length u-n)) \rightarrow \) (n-i-5 n-i-6)
    ;deps: (N_I_1 N-I-6)

12. (ue (n | length u)) * )
    ;PHI(())
8.11. Fstposition.

; facts about fstposition
(proof fstposition-prop)

1. (trw \[\forall k \cdot \text{null } k\])
   (label simpinfo)

2. (ue (phi \[\forall u \cdot \text{null} \text{ fstposition}(u, y) \Rightarrow \text{member}(y, u) \land \text{natnum} \text{ fstposition}(u, y) \land \text{natnum} \text{ fstposition}(u, y)])
    (label simpinfo) (label posfacts)

3. (ue (phi \[\forall u \cdot \text{sexp} \text{ fstposition}(u, y)])
    (label simpinfo) (label sortpos)

4. (ue (phi \[\forall u \cdot \text{member}(y, u) \Rightarrow \text{fstposition}(u, y) < \text{length}(u)])
    (label simpinfo) (label pos_length)

8.11.1 Fstposition and Nth.

; lemmata nth-fstposition and fstposition-nth

; lemma nth-fstposition

1. (ue (phi \[\forall n \cdot \text{member}(n, u) \Rightarrow \text{nth}(u, \text{fstposition}(u, n)) = n])
    (use normal mode: always)

2. (ue (phi \[\forall n \cdot \text{member}(n, u) \Rightarrow \text{nth}(u, \text{fstposition}(u, n)) = n])
    (use normal mode: always)

3. (ue (phi \[\forall n \cdot \text{member}(n, u) \Rightarrow \text{nth}(u, \text{fstposition}(u, n)) = n])
    (use normal mode: always)

4. (ue (phi \[\forall n \cdot \text{member}(n, u) \Rightarrow \text{nth}(u, \text{fstposition}(u, n)) = n])
    (use normal mode: always)

5. (ue (phi \[\forall n \cdot \text{member}(n, u) \Rightarrow \text{nth}(u, \text{fstposition}(u, n)) = n])
    (use normal mode: always)

6. (ue (phi \[\forall n \cdot \text{member}(n, u) \Rightarrow \text{nth}(u, \text{fstposition}(u, n)) = n])
    (use normal mode: always)

7. (ue (phi \[\forall n \cdot \text{member}(n, u) \Rightarrow \text{nth}(u, \text{fstposition}(u, n)) = n])
    (use normal mode: always)

8. (ue (phi \[\forall n \cdot \text{member}(n, u) \Rightarrow \text{nth}(u, \text{fstposition}(u, n)) = n])
    (use normal mode: always)

9. (ue (phi \[\forall n \cdot \text{member}(n, u) \Rightarrow \text{nth}(u, \text{fstposition}(u, n)) = n])
    (use normal mode: always)

10. (ue (phi \[\forall n \cdot \text{member}(n, u) \Rightarrow \text{nth}(u, \text{fstposition}(u, n)) = n])
    (use normal mode: always)

11. (ue (phi \[\forall n \cdot \text{member}(n, u) \Rightarrow \text{nth}(u, \text{fstposition}(u, n)) = n])
    (use normal mode: always)

12. (ue (phi \[\forall n \cdot \text{member}(n, u) \Rightarrow \text{nth}(u, \text{fstposition}(u, n)) = n])
    (use normal mode: always)

13. (ue (phi \[\forall n \cdot \text{member}(n, u) \Rightarrow \text{nth}(u, \text{fstposition}(u, n)) = n])
    (use normal mode: always)
8.12. Injectivity.

;injectivity
;another predicate for uniqueness
(proof inj)

1. (decl (inj) (type: [ground-truthval]))
2. (define inj [\( \forall u. inj(u) = \forall m. n < \text{length}(u) \land m < \text{length}(u) \land \text{nth}(u, n) = \text{nth}(u, m) \Rightarrow n = m \) ]
   (label injdef)

We want to show that the following properties of a list, \( u \) are equivalent:
(i) uniqueness: for every member \( x \), \( x \) does not belong to the tail of \( u \) after \( x \);
(ii) injectivity: if \( \text{nth}(u, i) = \text{nth}(u, j) \), then \( i = j \).

The property of uniqueness holds for all the tails of a list, if it holds for the list: the fact is needed later, line 1.4 is easily established by double induction on lists and numbers.

;equivalence of uniqueness and inj
(proof uniqueness-inj)

1. (ue (phi3 \( \forall u. \text{uniqueness}(u) \land \text{uniqueness}(\text{nthcdr}(u, n)) \) ) doubleinduction
   (open uniqueness nthcdr)
   \( \forall u. \text{uniqueness}(u) \land \text{uniqueness}(\text{nthcdr}(u, n)) \)
   (label uniqueness-nthcdr)

Assume uniqueness(u) (line 2). We want to show inj(u). Therefore we assume \( \text{nth}(u, i) = \text{nth}(u, j) \), with \( i \) and \( j \) both less than length(u) (lines 2, 3 and 4). We need to obtain \( i = j \) (line 13). We will derive a contradiction from the assumption that either \( i < j \) or \( j < i \) (lines 9 and 12) and apply the trichotomy:

\[ \forall n. m < n \land m = n \lor n < m. \]

Assume \( i < j \). Then \( \text{nth}(u, j) \) is a member of \( \text{nthcdr}(u, i') \) (line 8). (this is the fact \( \forall t \in \text{Nthcdr} \)). But, this contradicts the fact that \( \text{nthcdr}(u, n) \) enjoys the uniqueness property. So \( -n < m \).

Similarly for \( j < i \).

2. (assume [uniqueness(u)]
   (label ui1)
3. (assume [i < length u])
   (label ui2)
4. (assume [j < length u])
   (label ui3)
5. (assume [nth(u, i) = nth(u, j)]
   (label ui4)
6. (derive [uniqueness(nthcdr(u, i))] (uniqueness_nthcdr ui1))
7. (rw * (use nthcdr_car_cdr ui2 mode: always) (open uniqueness))
    ;labels: NTH_IN_NTHCDR
    ;def: N.M.N<LENGTH U'M<LENGTH U'ANDTH(U,M)=NTH(U,M) M=M
    ;def: (INJ UN2)
    ;def: (INJ UN4)

8. (ue (u.u)(m.1)(m.j)) nth_in_nthcdr
    (use ui4 mode: exact direction: reverse>
    (use ui3 * mode: exact))
    ;labels: LESS-LESSEQSUCC
    ;def: N.M.N<LENGTH

9. (ue ((m.i)(n.j)) less-lesseqsucc *)
    ;labels: UI WAY1
    ;def: (UI1 UI2 UI3 UI4)

10. (ci (ui1 ui2 ui3 ui4))
    ;def: (UI1 UI2 UI3 UI4)

11. (ue ((i.j)(j.i)) *)
    ;def: (UI1 UI2 UI3 UI4)

12. (derive |-j<i (*/ ui1 ui2 ui3 ui4))
    ;def: (UI1 UI2 UI3 UI4)

13. (derive |i=j (trichotomy ui_way1 ui_way2))
    ;def: (UI1 UI2 UI3 UI4)

14. (ci (ui1 ui2 ui3 ui4))
    ;def: (UI1 UI2 UI3 UI4)

15. (trw uniqueness(u) inj(u) *) (open inj))
    ;def: (INJ UN4)

We prove inj (u) uniqueness (u) by listinduction. It is easy to see that inj (x . u) implies inj (u) (line 4) and hence uniqueness (u), by induction hypothesis. We need to show n-member (x . u), in order to conclude uniqueness (x . u). If x was a member of u, it would be the (n0 + 1)-th member of x . u, for some n0, and we would have nth(x . u,(n0 + 1)) = nth(x . u,0) (line 7): by the definition of inj this implies n0 + 1 = 0.

1. (assume inj(u) uniqueness(u))
   (label inj_un1)

2. (assume inj(x.u) >)
   (label inj_un2)

3. (rw * (open inj))
   ;def: (INJ UN3)
   ;def: (INJ UN2)

4. (trw linj u) (open inj) (use * (ue: ((m.1)(m.1'))) inj(u))
   ;def: (INJ UN4)

5. (derive uniqueness u)(* inj_un1))
   (label inj_un4)
SECTION 8


; proof of facts about sets
(proof setfacts)
; nth_allp
1. (assume \( \forall n. n \leq \text{length}(u) \Rightarrow \text{phi1}(n, \text{nth}(u, n)) \))
   (label allp_intri)
2. (ue ((\text{phi1}(\text{nth}(u, n))) \text{nthcdr_induction}
      (open allp) (use * mode: always))
   ALLP(\text{phi1}(u))
3. (ci allp_intri)
   ;(\forall n. n \leq \text{length} u \Rightarrow \text{phi1}(\text{nth}(u, n))) \text{ALLP}(\text{phi1}(u))
   (label nth_allp) ■

; mklset_fact
4. (derive \( \forall x. (\text{mklsset}(u))(x) \equiv (\exists k. k < \text{length } u \land \text{Anth}(u, k) = x) \) )
   \( (\text{nthmember} \; \text{member}_n) \) (open \text{mklsset})

5. (ue ((av. \text{mklsset}(u))) (bv. (\forall x. (\exists k. k < \text{length } u \land \text{Anth}(u, k) = x) ))) \text{set-extensionality}
   * (open epsilon) )
   \( ; \text{mklsset}(u) = (\forall x. (\exists k. k < \text{length } u \land \text{Anth}(u, k) = x) ) \)
   (label \text{mklsset}_fact) \]}

(save-proofs nth)


: function as alists: the notion of application for association lists
(proof appalist)
1. (decl dom (type: ground-ground))
2. (defax dom \( \forall x \; y \; \text{alist}. \text{dom} \; \text{nil} = \text{nil} \)
   \( \text{dom}((\text{xa}. \text{y}). \text{alist}) = \text{xa}. \text{dom} \; \text{alist} \)
   (label domdef)
3. (decl range (type: ground-ground))
4. (defax range \( \forall x \; y \; \text{alist}. \text{range} \; \text{nil} = \text{nil} \)
   \( \text{range}((\text{xa}. \text{y}). \text{alist}) = \text{y}. \text{range} \; \text{alist} \) )
   (label rangedef)
5. (decl functp (type: ground-truthval))
6. (define functp \( \forall \text{alist}. \text{functp}(\text{alist}) = \text{uniqueness} \; \text{dom} \; \text{alist} \))
   (label functpdef)
7. (decl injectp (type: ground-truthval))
8. (define injectp \( \forall \text{alist}. \text{injectp}(\text{alist}) = \text{functp}(\text{alist}) = \text{uniqueness} \; \text{range} \; \text{alist} \))
   (label injectpdef)
9. (decl (appalist) (type: ground-ground-ground))
10. (define appalist \( \forall \text{alist}. \text{appalist}(\text{y}, \text{alist}) = \text{cdr} \; \text{assoc}(\text{y}, \text{alist}) \))
    (label appalistdef)
11. (decl (samemap) (type: ground-ground-ground-
    truthval))
12. (define samemap \( \forall \text{alist}. \text{samemap}(\text{alist}, \text{alist}) = \text{mklsset} \; \text{dom}(\text{alist}) = \text{mklsset} \; \text{dom}(\text{alist}) \))
    \( \forall y. y \in \text{mklsset} \; \text{dom}(\text{alist}) \) \text{appalist}(\text{y}, \text{alist}) = \text{appalist}(\text{y}, \text{alist}) \))
    (label samemapdef)
13. (define permutp \( \forall \text{alist}. \text{permutp}(\text{alist}) = \text{functp}(\text{alist}) = \text{mklsset} \; \text{dom}(\text{alist}) = \text{mklsset} \; \text{range}(\text{alist}) \))
    (label permutp_def)

(proof alistind)

1. (assume |chi(nil)\forall x y alist.chi(alist)\exists(x.a).alist)|)
   (label alind1)
2. (assume alistp u\exists u u)
   (label alind2)
3. (assume alistp (x.u))
   (label alind3)
4. (ue (alist |x.u|) alistdefl *)
   ;;ATOM XATOM CAR XAALISTP U
5. (derive |\forall x y alist.chi(alist)\exists(x.a).alist)| alind1)
6. (ue ((x.a).car x)\forall y cdr(x) (alist.u) \ast -2 alind3 alind2)
   ;CHI(X.U)
   ;deps: (ALIND1 ALIND2 ALIND3)
7. (ci alind3)
   ;ALISTP X.U\exists u u(X.U)
   ;deps: (ALIND1 ALIND2)
8. (ci alind2)
   ;(ALISTP U \exists u u(XU))\exists (ALISTP X.U \exists u u(X.U))
   ;deps: (ALIND1)
9. (ue (phi \exists u.alistp(u)\exists u u) listinduction alind)
   ;\forall U ALISTP U \exists u u
10. (derive \forall alist.chi alist | *)
    ;deps: (ALIND1)
11. (ci alind1)
    ;CHI(NIL)\forall x y ALIST.CHI(ALIST)\exists(xa.y).alist)
    (label alistinduction)


;facts about alists
(proof alistfacts)

;domsort

1. (ue (chi \exists alist.domp(alist)!) listinduction (open dom))
   ;\forallalist.LISTP DOM(ALIST)
   (label simpinfo)(label domsort)
2. (ue (chi \exists alist.domp(alist)!) listinduction (open range))
   ;\forallalist.LISTP RANGE(ALIST)
   (label simpinfo)(label rangesort)
3. (ue (chi \exists alist.length dom alist= length alist |)
   (label domlength)

(proof samemap)

1. (trw |samemap(alist,alist)|(open samemap))
   ;SAMEMAP(ALIST,ALIST)
   (label samemap-equivalence)

2. (tra |samemap(alist,alist1)|samemap(alist1,alist)| (open samemap mklset dom))
   ;SAMEMAP(ALIST,ALIST1)|SAMEMAP(ALIST1,ALIST)
   (label samemap-equivalence)

3. (trw |samemap(alist,alist1)|samemap(alist1,alist2)|samemap(alist,alist2))
   (open samemap mklset dom))
   ;SAMEMAP(ALIST,ALIST1)|SAMEMAP(ALIST1,ALIST2)|SAMEMAP(ALIST,ALIST2)
   (label samemap-equivalence)

;apparently stronger definition of samemap
(proof samemapdef)

1. (assume |samemap(alist1,alist2)|)

2. (ra * (open samemap))
   ;MKLSET(DOM(ALIST1))=MKLSET(DOM(ALIST2))
   ;(yאמלשת(DOM(ALIST1))=APPALIST(Y,ALIST1)=APPALIST(Y,ALIST2))

3. (tra |yאמלשת(dom(alist1))=appalist(y,alist1)=appalist(y,alist2)|
   (use trivial,appalist mode: always)
   (use * mode: exact))
   ;אמלשת(DOM(ALIST1))=APPALIST(Y,ALIST1)=APPALIST(Y,ALIST2)

4. (ue ((q.|yאמלשת(dom(alist1))|p.|appalist(y,alist1)=appalist(y,alist2)|))
   excluded-middle |-2)
   ;APPALIST(Y,ALIST1)=APPALIST(Y,ALIST2)

5. (derive |mklset(dom(alist1))=mklset(dom(alist2))
   ∀y.appalist(y,alist1)=appalist(y,alist2) |-3 *)

6. (ci -5)
   ;SAMEMAP(ALIST1,ALIST2)
8.15. Functions Represented by Lists of Numbers.

;functions as lists of numbers
(wipe-out)
(get-proofs pigeon)
(proof appl)
1 (define appl \[\forall u.\forall i.\text{appl}(u,i) = \text{nth}(u,i)\])
(label appldef)
2 (axiom \[\forall u. \forall i. \text{length } u \geq \text{length } u \implies \text{sexp}(\text{appl}(u,i)) \land \text{member}(\text{appl}(u,i), u)\])
(label applfacts)
(label simpinfo)
;predicates for functions
3 (decl (into) (type: \text{ground-truthval}))
4 (define into \[\forall u. \text{into}(u) = (\forall n. n < \text{length } u \implies \text{nth}(u,n) \land \text{nth}(n,u) < \text{length } u)\])
(label intodef)
5 (decl (onto) (type: \text{ground-truthval}))
6 (define onto \[\forall u. \text{onto}(u) = (\forall n. n < \text{length } u \implies \text{member}(n, u))\])
(label ontdef)
7 (decl (perm) (type: \text{ground-truthval}))
8 (define perm \[\forall u. \text{perm}(u) = \text{onto}(u)\])
;injectivity is given by the predicate inj
(save-proofs appl)

8.15.1. Extensionality.

(wipe-out)
(get-proofs appl)
(proof extensionality)
1. (assume \[\text{length } u = \text{length } v \implies (\forall i. i < \text{length } u \implies \text{nth}(u,i) = \text{nth}(v,i)) \implies u = v\])
(label ext1)
2. (assume \[\text{length } u = \text{length } v\])
(label ext2)
3. (assume \[\forall i. i < \text{length } v \implies \text{nth}(x,u,i) = \text{nth}(y,v,i)\])
(label ext3)
4. (ue (i 0) * ext2)
8.16. file SUMS: Finite Union and Finite Sum.

:the notions of finite union and finite sum
(wipe-out)
(get-proofs appl)
(proof sums>

1. (decl allnum (type: |ground@set-truthval|)(syntype: constant))
2. (decl somenum (type: |ground@set-truthval|)(syntype: constant))
3. (decl numseq f) (type: |ground@ground|)
4. (decl sum (type: |(@numseq)@n=0n|))(syntype: constant))
5. (decl setseq (type: |@n=0set|))
6. (decl un (type: |(@setseq)@n=0set|))(syntype: constant))

;axiom for allnum
7. (defax allnum |Vn.a.allnum(0,a)((allnum(n',a)=a(n)@allnum(n,a)|))
(label allnumdef)

;axiom for somenum
8. (defax somenum |Vn.a.somenum(0,a)((somenum(n',a)=a(n)@somenum(n,a)|))
(label somenumdef)

;axiom for sum
9. (defax sum |Vn.numseq.sum(numseq,0)=0Asum(numseq,n')=sum(numseq,n)+numseq(n)|
(label sumdef)

;axiom for un

8.16. file SUMS: Finite Union and Finite Sum.

:the notions of finite union and finite sum
(wipe-out)
(get-proofs appl)
(proof sums>

1. (decl allnum (type: |ground@set-truthval|)(syntype: constant))
2. (decl somenum (type: |ground@set-truthval|)(syntype: constant))
3. (decl numseq f) (type: |ground@ground|)
4. (decl sum (type: |(@numseq)@n=0n|))(syntype: constant))
5. (decl setseq (type: |@n=0set|))
6. (decl un (type: |(@setseq)@n=0set|))(syntype: constant))

;axiom for allnum
7. (defax allnum |Vn.a.allnum(0,a)((allnum(n',a)=a(n)@allnum(n,a)|))
(label allnumdef)

;axiom for somenum
8. (defax somenum |Vn.a.somenum(0,a)((somenum(n',a)=a(n)@somenum(n,a)|))
(label somenumdef)

;axiom for sum
9. (defax sum |Vn.numseq.sum(numseq,0)=0Asum(numseq,n')=sum(numseq,n)+numseq(n)|
(label sumdef)

;axiom for un
8.16.1. Bound Quantifiers.

(proof allnumprop)

; we can easily prove that 'allnum' does its job

1. (ue (a (\An.allnum(n,a) (m < n a (m))))) proof-by-induction
   (use transitivity-of-order) (use successor1 (open allnum)
   (use less-succ-lesseq normal mode: exact) (open lesseq))
   ; VN.ALLNUM(N,A) -> (M < N)A(M)

2. (ue (a (\An.(\V m.m < n a (M))) allnum(n, a)))) proof-by-induction
   (open allnum) (use normal mode: always)
   (use less-succ-lesseq mode: exact) (open lesseq))
   ; VN.(\V M.(M < N)A(M)) ALLNUM(N,A)

3. (derive (\V n.(\V m.m < n a (m))) allnum(n, a)) I (* -2))
   ; similarly for 'somenum':

4. (ue (a (\An.somenum(n,a) (\E m.m < n a (m))))) proof-by-induction
   (use transitivity-of-order) (use successor1 (open somenum)
   (part 1 (der))
   (use less-succ-lesseq normal mode: exact) (open lesseq))
   ; VN.SOMENUM(N,A) -> (\E M.(M < N)A(M))

5. (ue (a (\An.(\E m.m < n a (m))) somenum(n, a)))) proof-by-induction
   (open somenum) (use normal mode: always) (part 1 (der))
   (use less-succ-lesseq mode: exact) (open lesseq))
   ; VN.(\E M.(M < N)A(M)) SOMENUM(N,A)

6. (derive (\V n.(\E m.m < n a (m))) somenum(n, a)) I (* -2))

8.16.2. Facts About Sums and Unions.

(proof unionprop)

; a property of union

;unionfact1

(ue (a (\An.m < n (\V x.(setseq(m))(xv))(un(setseq,n))(xv))))
   proof-by-induction
   (open un union) (use less-succ-lesseq mode: always)
   (open lesseq) (use normal mode: always))
   ; VN.M < N (\V X.(SETSEQ(M))(XV))(UN(SETSEQ,N))(XV))
about permutations in lisp and ekl

; namely:

2. (trw | vssetq = m.m<n|seteq(m)Cun(setseq,n) | (open inclusion)) (label unionfact)

;a property of sum

; sumsort

3. (ue (a | n.allnum(n),m.natnum numseq(m))Cnatnum sum(numseq,n) |)
   (proof-by-induction (open allnum sum))
   (label sumsort)

; mksetfact

5. (ue (a | n|length u) (un(m.mkset(nth(u,m)),n))(x)=somenum(n,λk.x=nth(u,k)))
   (proof-by-induction (part 1(open un mkset nth somenum union emptyset) (der))
   (use succ_lesseq_lesseq mode: always))
   (label mksetfact)

7. (assume | n|length u)

8. (ue (av.|un(m.mkset(nth(u,m)),n)))
   (bv.|λx.∃k<k<nth(u,k)x) )
   (use * -2 mode: always)
   (label mksetfact)

9. (ci -2)

10. (ue (n|length u) mksetfact (use mkset_fact mode: exact direction: reverse> (open lesseq))
    (label mkset_un)

8.17. file MULT: Multiplicity.

;the notion of multiplicity
(get-proof sums>
(proof multiplicity)

1. (declardata mult (type: |(grounde@set)+groundl|))
2. (defaxmult |\(\forall x. a. mult(nil,a) = 0\))
   \(mul(x,u,a) = if(a(x) then mult(u,a)' else mult(u,a) >\)
   (label mult_def)
3. ;facts about multiplicity
4. (ue (phi |\(\forall u. a. natnum(mult(u,a))\)|) listinduction
   (use mult-def mode: always))
   (label simpinfo) (label multfact) ■

;multiplicity is less or equal to length
5. (ue (phi |\(\forall u. \forall v. a. member(y,v)\ AA(y) <\mult(u,a)\)|) listinduction
   (open mult length) (part 1#1(open lesseq)))
   \(\forall U. MULT(U,A) <\length U\)
   (label length_mult) ■

;if there is a member, multiplicity is not zero
6. (ue (phi |\(\forall u. \forall v. a. member(y,u)\ AA(y) <\mult(u,a)\)|) listinduction
   (use normal mode: always))
   \(\forall V. Y. A. MEMBER(Y,U) <\AA(Y) <\MULT(U,A)\)
   (label member_mult) ■

;multiplicity of the emptyset
7. (ue (phi |\(\forall u. mult(u,emptyset)=0\)|) listinduction
   (part 1(open emptyset mult)))
   \(\forall V. MULT(U,EMPTYSET)=0\)
   (label emptyfacts) ■

;mult_nthcdr
;we prepare a rewriter
8. (ue ((q.\(\forall u. mult(nthcdr(u,n'),a)'\mult(u,a)\)\)
       \(\forall u. mult(nthcdr(u,n'),a)'\mult(u,a)\)
       (p.\(\forall u. mult(nthcdr(u,n'),a)'\mult(u,a)\))
       (use succ_lesseq_lesseq: ((\(\forall u. mult(nthcdr(u,n'),a)'\mult(u,a)\)) mode: exact ))
       (n.\(\forall u. mult(nthcdr(u,n'),a)'\mult(u,a)\))
       (use succ_lesseq_lesseq: ((\(\forall u. mult(nthcdr(u,n'),a)'\mult(u,a)\)) mode: exact ))
     )
   ( conclus) ■
7. (ue (\(\forall u. u<\length(u)\mult(nthcdr(u,n),a)'\mult(u,a)\))) proof-by-induction
   (part 1#1(open lesseq)) succ_less_less
   (part 1#2#1#1(use nthcdr_car_cdr mode: always))
   (open mult) ■
   \(\forall V. A. U. N <\length U. MULT(NTHCDR(U,N),A)'\mult(U,A)\)
   (label mult_nthcdr) ■

(proof multinj_computation)
; a sublemma to compute multiplicity

1. (assume |j|<length v|)
   (label mc0)

2. (assume |i|<j|)
   (label mc1)

3. (assume \(\text{nth}(v,i) = \text{nth}(v,j)\))
   (label mc2)

4. (derive |i|<length v| (mc0 mc1 transitivity-of-order))
   (label mc3)
; deps: (mc0 mc1)
; labels: NTH_IN_NTHCDR
; \(\forall v \, N \cdot N < \text{LENGTH} \Rightarrow \text{MEMBER}(\text{NTH}(U,M), \text{NTHCDR}(U,N))\)

5. (ue ((u,v)(n.i')!)(m.j)) nth_in_nthcdr mc0 mc1
   (use less-leq-suucc mode: exact direction: reverse>)
; MEMBER(\text{NTH}(V,J), \text{NTHCDR}(V,I'))
   (label mc4)
; deps: (MC0 MC1)
; labels: MEMBER_MULT
; \(\forall v \, A \cdot \text{MEMBER}(V, U) \Rightarrow (Y > A) \Rightarrow \text{MULT}(U,A)\)

6. (ue ((u.nthcdr(v,i'))!)(y.nth(v,j)))(a.mkset nth(v,j))
   (member-mult
   (part I(open lesseq mkset)) mc4
   (use mc2 mode: exact direction: reverse>)
; \(\text{MULT}(\text{NTHCDR}(V,I'), \text{MKSET}(\text{NTH}(V,I)))\)
   (label mc5)
; deps: (MC0 MC1 MC2)

7. (trv \(\text{MULT}(\text{NTHCDR}(V,I'), \text{MKSET}(\text{NTH}(V,I)))\)
   (open mult mkset) (use nthcdr_car_cdr mc3 mode: exact))
; \(\text{MULT}(\text{NTHCDR}(V,I'), \text{MKSET}(\text{NTH}(V,I)))\)
; deps: (MC0 MC1 MC2)

8. (ue (n |i| !1 l) mc5)
   ; \(\text{MULT}(\text{NTHCDR}(V,I), \text{MKSET}(\text{NTH}(V,I)))\)
   (label mc6)
; deps: (MC0 MC1 MC2)
; labels: MULT_NTHCDR
; \(\forall v \, A \cdot N < \text{LENGTH} \Rightarrow \text{MULT}(\text{NTHCDR}(U,N), A) \Rightarrow \text{MULT}(U,A)\)

9. (ue ((n.i))!(u,v)(a.mkset nth(v,i)) l>> mult_nthcdr mc3)
   ; \(\text{MULT}(\text{NTHCDR}(V,I), \text{MKSET}(\text{NTH}(V,I)))\)
   ; \(\text{MULT}(\text{V}, \text{MKSET}(\text{NTH}(V,I)))\)
; deps: (MC0 MC1 MC2)
; labels: TRANS_LESEQ
; \(\forall v \, N \cdot N < \text{LENGTH} \Rightarrow \text{MULT}(V, \text{NTH}(V,I))\)

10. (ue ((n.|2 l)!)(m.\text{MULT}(\text{NTHCDR}(v,i), \text{MKSET}(\text{NTH}(v,i)))))(k.\text{mkset nth(v,i))})
    (trans lesseq mc6 * )
; \(\text{MULT}(V, \text{MKSET}(\text{NTH}(V,I)))\)
; deps: (MC0 MC1 MC2)

11. (ci (mc1 mc0 mc2))
; \(\forall i < j \cdot \text{LENGTH} \Rightarrow \text{NTH}(V,I) = \text{NTH}(V,J) \Rightarrow \text{MULT}(V, \text{MKSET}(\text{NTH}(V,I)))\)
8.17.2. The Multiplicity of Union is the Sum of Multiplicities.

;Lemma: if the union is disjoint, then the multiplicity of the union is
; the sum of the multiplicities

(proof multsum)

1. (ue (phi | Au. disjoint(a,b) -> mult(u,a U b) = mult(u,a) + mult(u,b)))
   listinduction
   (part 1 (open mult union disjoint emptyp intersection)
     (use normal mode: always))
   (part 1 (der)))
   ; \forall U. DISJ_PAIR(A,B) -> MULT(U,A U B) = MULT(U,A) + MULT(U,B)
   (label multsum) ■

2. (ue (a | An. disjoint(setseq,n))
   mult(u,un(setseq,n)) = sum(Ax1.multiplicities(u,un(setseq(x1)),n)))
   proof-by-induction (open disjoint un sum mult ) multfact
   (use multsum mode: exact) (use normal mode: always))
   ; \forall U. DISJOINT_SETSEQ(N) -> MULT(U,UNSETSEQ(N)) = SUM(Ax1.MULT(U,SETSEQ(X1)),N)
   (label mult_of_un_is_sum_mult) ■
8.18. file PIGEON: the Pigeon Hole Principle in II Order Arithmetic,

(wipe-out)
(get-proofs sums>
(proof pigeonfact)

1. (assume \( \forall n. \text{natnum } f(n) \))
   (label sort1)

2. 
   (ue ((numseq (\( \forall k. f(k) \)) (n n)) sumsort * )
   \( \text{NATNUM}(\text{SUM}(\forall k. f(k), n)) \)
   (label sort2)

3. 
   (ue (a (\( \forall n. \text{allnum}(n, \forall k. f(k)) \)) \( \text{NATNUM}(\text{SUM}(\forall k. f(k), n)) \))
   proof-by-induction
   (open allnum sum> zeroleast (use sort1 sort2 mode: always)
   (use add-lesseq ue: ((n n) (k.lf(n))) (m. sum((\( \forall k. f(k) \)), n))))
   (label strictly-increasing)
   \( \forall n. \text{NATNUM}(n, \forall k. f(k)) \) \( \Rightarrow \text{SUM}(\forall k. f(k), n) \)
   ;deps: (SORT1)

4. 
   (ue (a (\( \forall n. \text{allnum}(n, \forall k. f(k)) \)) \( \text{NATNUM}(n, \forall k. f(k)) = n \) allnum(n, \( \forall k. f(k) \)) )
   proof-by-induction
   (open allnum sum> strictly-increasing sort1 sort2
   (use add-one
   ue: ((k.lf(n))) (m. sum((\( \forall k. f(k) \)), n))) mode: always)
   \( \forall n. \text{NATNUM}(n, \forall k. f(k)) \) \( \Rightarrow \text{SUM}(\forall k. f(k), n) = n \) allnum(n, \( \forall k. f(k) \))
   ;in more conventional notation:
   \( \forall n. \text{NATNUM}(n, \forall k. f(k)) \) \( \Rightarrow \text{SUM}(\forall k. f(k), n) = n \) allnum(n, \( \forall k. f(k) \))

5. (rew (use allnumfact ue: ((a. (\( \forall k. f(k) \))) (n n))
   mode: always direction: reverse>
   (use allnumfact ue: ((a. \( \forall k. f(k) \)) (n n))
   mode: always direction: reverse>)
   \( \forall n. \text{NATNUM}(n, \forall k. f(k)) \) \( \Rightarrow \text{SUM}(\forall k. f(k), n) = n \) allnum(n, \( \forall k. f(k) \))
   ;deps: (SORT1)

6. (ci sort1)
   ;(\( \forall n. \text{NATNUM}(f(n)) \))
   ;(\( \forall n. \text{NATNUM}(f(n)) \)) \( \Rightarrow \text{SUM}(\forall k. f(k), n) = n \) allnum(n, \( \forall k. f(k) \))
   ;application to lists
   (proof pigeononlist)

1. (assume \( \text{disjoint}((\text{setseq}, \text{length } u)) \)>
   (label pl1)
   ;multiplicity less than length
   -2. (ue \( ((u u)(\text{setseq}, \text{length } u)) \)) length_mult
   \( \text{MULT}(u, \text{UMSETSEQ}, \text{LENGTH } u) \) \( \Rightarrow \text{LENGTH } u \)
   (label pl2)

3. (derive \( \text{SUM}(\text{mult}(u, \text{setseq}(m))), \text{length } u) \) \( \Rightarrow \text{length } u \)
   (\text{mult_of_un_is_sum_mult } pl1 pl2)
   (label pl3)

4. (ue \( (f. (\text{mult}(u, \text{setseq}(m))) (n. \text{length } u)) \)) pigeonfact pl3 multifact)
   \( \forall n. \text{MULT}(u, \text{SETSEQ}(m)) = (\forall m \text{LENGTH } u) \Rightarrow \text{MULT}(u, \text{SETSEQ}(m)) \)
   ;deps: (PL1)
   ;the pigeon hole principle on lists

5. (ci pl1)
8.19. file ALPIG: Application to Alists 1: Disjointness.

;first application: to alists. Lemma: inj implies disjoint
(wipe-out)
(get-proofs appal)
(proof inj_disj)

;a main lemma for the induction step
1. (assume linj u)
   (label injdsj0)
2. (rw * (open inj))
   (label injdsj1)
   ;\forall M. M < LENGTH U \Rightarrow U \cdot M < \text{MULT}(U, \text{SETSEQ}(M))
3. (assume [n < length u])
   (label injdsj2)
4. (assume \{(un(A.mkset(nth(u,m)),n))(xv)\}(mkset(nth(u,n)))(xv))
   (label injdsj3)

;need mksetfact
5. (ue ((u,u)(n,n)) mkset fact (open lesseq) injdsj2)
   ;\forall M. M < \text{LENGTH} U \Rightarrow U \cdot M < \text{MULT}(U, \text{SETSEQ}(M))
6. (rw injdsj2 (use * mode: exact) (open mkset) injdsj2)
   ;(\exists K. K < \text{LENGTH} U \Rightarrow U \cdot K = X)\text{AX} = \text{NTH}(U,N)
   (label injdsj4)
7. (define kv\text{mkset}(nth(u,m)),n)(xv)\text{mkset}(nth(u,n))(xv))
   (label injdsj5)
8. (derive \text{mkset}(nth(u,m)),n)(xv)\text{mkset}(nth(u,n))(xv))
   (* injdsj2 transitivity-of-order)
     (use injdsj4 mode: always direction: reverse*)
9. (derive \text{mkset}(nth(u,m)),n)(xv)\text{mkset}(nth(u,n))(xv))
10. (rw injdsj5 (use * mode: exact) irreflexivity-of-order)
   ;FALSE
   ;deps: (INJDSJ0 INJDSJ3 INJDSJ2)
11. (ci injdsj3)
    ;(\exists\{(un(A.mkset(nth(u,m)),n))(xv)\}(mkset(nth(u,n)))(xv))
12. (ci (injdsj0 injdsj2))
    ;INJ(U)\Rightarrow(U \cdot M < \text{LENGTH} U)\Rightarrow(\exists\{(un(A.mkset(nth(u,m)),n))(xv)\}(mkset(nth(u,n)))(xv))
    (label injdsj-lemma)

;the theorem follows
13. (ue (a [m.inj(u)]Am.length(u)\text{disjoint}(Am.mkset nth(u,m),n))
    (use less-lesseqsucc mode: always direction: reverse)
    (use injdsj-lemma mode: always)(part 1#2#1#1 (open lesseq)))
8.20. **Application to Alists 2: the Multiplicity is Positive.**

```
;the sets in the sequence have positive multiplicity
(proof permutp_injectp_lemma)
(assume lmklset u=mklset v)
(label pill)
2. (assume In<length u)
(label pi12)
:use nthmember
3. (trw |nth(u,n)∈ mklset u| (open epsilon mklset)
nthmember pi12)
;NTH(U,N)∈MKLSET(U)
;deps: (PIL2)
:now use line pill
4. (trw * (use pill mode: exact))
;NTH(U,N)∈MKLSET(V)
;deps: (PIL1 PIL2)
;Finally using MKLSET-FACT, we prove the existence of a kv such that
;nth(v,kv) = nth(u,n)
;labels: MKLSET-FACT
;VU.MKLSET(U>=(~X.(BK.K< LENGTH UANTH(U,K)=X))
5. (trw * (use mklset-fact mode: exact> (open epsilon mkset))
;3K.K< LENGTH VANTH(V,K)=NTH(U,N)
;deps: (PIL1 PIL2)
6. (define kv|kv<length(v)∧ nth(v,kv)=nth(u,n)| *)
(label pi13)
;deps: (PIL1 PIL2)
7. (trw |member(nth(v,kv),v)| nthmember pi13)
;MEMBER(NTH(V,KV),V)
(label pi14)
;Therefore the set mkset(nth(u,n)) has positive multiplicity in v.
;labels: MEMBER_MULT
;VU Y A.MEMBER(Y,U)A(Y)>1SMULT(U,A)
8. (ue ((u,v)(y,lnth(v,kv)))(a.mklset nth(u,n))) member-mult
(part 1(open mkset)) pi12 pi14 (use pi13 mode: always)
;1SMULT(V,MKSET(NTH(U,N)))
;deps: (PIL1 PIL2)
9. (ci (pill pi12))
;MKLSET(U)≠MKLSET(V)∧ N<LENGTH U1SMULT(V,MKSET(NTH(U,N)))
:cosmetics
```
8.21. Application to Alists 3: Multiplicities in Dom and Range.

; lemma mult-mult
; (proof mult_mult)
1. (assume lmklset u = mklset v)
   (label mm1)
2. (assume |vm.m=length u | mult(v, mkset nth(u,m))=|1)
   (label mm2)
3. (assume |i=length v)
   (label mm3)
4. (trw |nth(v,i)€ mklset v | (open epsilon mklset)
    (use nthmember mode: exact)
    ; NTH(V, I)€ MKLSET(V)
5. (rw * (use mm1 mode: exact direction: reverse>)
    ; NTH(V, I)€ MKLSET(U)
6. (rw * (use mklset-fact mode: exact) (open epsilon))
    ; EX.K<LENGTH U ANTH(U,K)=NTH(V, I)
7. (define mv |mv<length u ANth(u,mv)=nth(v,i)| * )
   (label mm4)
   ; mv is unknown.
   ; the symbol mv is given the same declaration as M
   ; deps: (MM1 MM3)
8. (ue (m mv) mm2 (use * mode: always))
   ; MULT(V, MKSET(NTH(V, I)))=1
   ; deps: (MM1 M002 MM3)
9. (ci mm3)
   ; I<LENGTH V MULT(V, MKSET(NTH(V, I)))=1
   ; deps: (MM1 MM2)
10. (ci mm2)
    ; MKLSET(U)=MKLSET(V) \forall M.M<LENGTH U MULT(V, MKSET(NTH(U,M)))=1)
    ; (I<LENGTH V MULT(V, MKSET(NTH(V, I)))=1)
    (label mult-mult) ■

8.22. Application to Alists: a Permutation is an Injection.

; the main result for permutp: theorem permutp-injectp
; (proof permutp_injectp)
1. (assume lpermutp alist l)
   (label permutp_injectp1)
2. (rw * (open permutp))
   ; FUNCTP(ALIST)\forall MKLSET(DOM(ALIST))=MKLSET(RANGE(ALIST))
(label permutp_injectp2)

3. (rw * (open funct))
   ;UNIQUENESS(DOM(ALIST))\& MKLSET(DOM(ALIST)) = MKLSET(RANGE(ALIST))
   (label permutp_injectp3)

   ;first step: disjointness of a suitable sequence of sets
   ;labels: UNIQUENESS - INJECTIVITY
   ;Vu.UNIQUENESS(U) = INJ(U)
   ;labels: INJ_DISJ
   ;Vu.INJ(U) \& \& DISJOINT(MKSET(WHOLE(U,M)), LENGTH U)

4. (derive \(\text{inj}(\text{dom(alist)})\) (\# uniqueness_injectivity))
   ;deps: (PERMUTP_INJECTP1)

5. (derive \(\text{disjoint}(\text{mkset(nth(dom(alist)),m)), length(dom(alist)))\) I
   (\# inj_disj))
   (label permutp_injectp4)

   ;second step: multiplicity of the sets in the sequence is positive
   ;labels: PERMUTP_INJECTP_LEMA
   ;Vu.V.MKLSET(U) = MKLSET(V) (\# VM.LEN(U) \& MULT(V, MKSET(WHOLE(U, M))))

6. (ue ((u.| dom alist)) (v.| range alist)) permutp_injectp_lemma
   (permutp_injectp3 permutp_injectp4)
   ;VM.LEN(U) \& MULT(RANGE(ALIST), MKSET(WHOLE(DOM(ALIST), M)))
   (label permutp_injectp5)

   ;third step: application of the pigeon hole principle
   ;labels: PIGEONLIST
   ;V.SETSEQ U.DISJOINT(SETSEQ, LENGTH U) \& (VK.K.LEN(U) \& MULT(U, SETSEQ(K))))
   ; (VK.K.LEN(U) \& MULT(U, SETSEQ(K))))
   ;need also
   ;labels: DOMRANGELENGTH
   ;VALIST.LEN (DOM(ALIST)) = LENGTH (RANGE(ALIST))

7. (ue ((setseq.| \text{mkset(nth(dom(alist),m))}) (u.| range alist)) pigeonlist
   (use domrangelength mode: exact direction: reverse>
   permutp_injectp4 permutp_injectp5)
   ;VK.K.LEN(DOM(ALIST)) \& MULT(RANGE(ALIST), MKSET(WHOLE(DOM(ALIST), K)))

   ;fourth step: injectivity
   ;labels: MULT_MULT
   ;VU.V.MKLSET(U) = MKLSET(V) (\# VK.K.LEN(U) \& MULT(V, MKSET(WHOLE(U, K))))
   ; (VK.K.LEN(U) \& MULT(V, MKSET(WHOLE(U, K))))

8. (ue ((u.| dom(alist)) (v.| range(alist))) mult_mult
   permutp_injectp3 * )
   ;VI.I.LEN(RANGE(ALIST)) \& MULT(RANGE(ALIST), MKSET(WHOLE(RANGE(ALIST), I))) = 1
   ;deps: (PERMUTP_INJECTP1)

   ;apply mult-inj
   ;labels: MULT_INJ
   ;VV.(VK.K.LEN(V) \& MULT(V, MKSET(WHOLE(V, K)))) = 1 \& INJ(V)

9. (ue (v range alist) mult-inj * )
Section 8

10. (derive uniqueness(range alist) (* uniqueness_injectivity))
    ;deps: (PERMUTP_INJECTP)

11. (derive injectp alist! (permutp_injectp2 *)(open injectp))
    ;deps: (PERMUTP_INJECTP)

12. (ci (permutp_injectp1))
    ;PERMUTP(ALIST) INJECTP(ALIST)
    (label theorem_permutp_injectp)

(save-proofs alpig)

8.23. file LPIG: Application to Lists 1: Disjointness.

;Disjointness
(proof disjoint_number)
;lemma dnl
1. (ue (a|An.Vm.((un((axv.mkset(xv)),n))(m)>m<n))
    proof-by-induction
    (part 1(open mkset un emptyset union))
    (use normal mode: always)
    (use successor1 transitivity-of-order)
    ;VN.M.(UN(XXV.MKSET(XV),(N))((N))>M<N)
    ;lemma disjoint number

2. (ue ((n.n)(m.n)) dnl irreflexivity-of-order)
    ;-(UN(A XV.MKSET(XV),N))(N)

3. (trw ((un(axv.mkset(xv)),n))(axv)(mkset(n))(xv))
    ;-(UN(A XV.MKSET(XV),N))(XV)(AXV.MKSET(N))(XV)

4. (ue (a|An.disjoint(axv.mkset(xv),n)) proof-by-induction
    (open disjoint disjoint_pair emptyp intersection)
    (use * mode: exact))
    ;VN.DISJOINT(A XV.MKSET(XV),N)
    (label disjoint_number)


;lemma into-mul
(proof into-mult)
1. (assume |into(u)|
    label i m1)
2. (assume |vk.k<length u|21=mult(u,mkset k))
    (label i m2)
3. (assume |j<length u|)
    (label i m3)
8.25. Application to Lists: a Permutation is an Injection.

;the main result for perm
;a straightforward application of pigeon hole to onto lists
(proof perm inj)
;vu perm(u) inj(u)

1. (assume perm u)
'(label perm inj1)

2. (rw * (open perm onto))
;into(u) A (vn.v < length u) member(u, v)
(label perm inj2)
;labels: MEMBER Mult
;vu y. member(y, u) >> member Mult(u, y)

3. (ue ((u. u)(y. n)(a. mkset n))) member-mult
(part {open mkset})
;member(u, n) >> member Mult(u, mkset(n))

4. (derive (vn. u < length u) (i. mkset n) (perm inj2 *))
(label onto_mult) (label perm inj3)
;deps: (PERM_INJ1)

5. (ue ((setseq. l. x. mkset(x))) (u. n)) pigeonlist disjoint-number perm inj3
;vk. u < length u >> mult(u, mkset(k))
(label perm inj4)
;deps: (PERM_INJ1)

   ;labels: INTO Mult
   ;vu. into(u) A (vk. u < length u) >> mult(u, mkset(k))

6. (derive (vi. i. u < length u) (mkset(nth(u, i))) (into-mult perm inj2 *))
;deps: (PERM_INJ1)

   ;labels: MULT_INJ
   ;vv. (vk. v < length v) mult(v, mkset(nth(v, k))) = 1 >> inj(v)

7. (ue (v u) mult inj *)
;INJ(u)
;deps: (PERM_INJ1)

; the approach using association lists
(wipe-out)
(get-proofs appal)
(proof assoc)
1. (decl (compalist) (infixname: |m|) (type: |ground|ground|ground|))
   (syntype: constant) (bindingpower: 910)
2. (defax compalist
   |Valist1 alist2 xa y.nil m alist2=nilA
   ((xa,y).alist1) o alist2= (xa.appalist(y,alist2)).(alist1 o alist2))
   (label compalistdef)
3. (decl invalist (type: |ground|ground|))
4. (defax invalist
   |Valist=|xa y.invalist nil m nilA
   invalist((xa,y).alist)leaf=(y,x)a.invalist alist1)
   (label invalistdef)
5. (decl idalistp (type: |ground|truthval|))
6. (defax idalistp
   |Valist m xa y.idalistp(nil)A
   (idalistp((xa,y).alist)leaf=xa=y.idalistp alist1))
   (label idalistpdef)


(proof alistprop)
; prove sorts
; compalist sort
1. (ue (chi |alist.alistp(alist o alist)|)) alistinduction
   (part 1(open compalist)(use appalistsort mode: exact>>>
   ; VALIST. ALISTP ALIST o ALIST
   (label simpinfo) (label compalistsort))
   invalistsort
; invalistsort
2. (ue (chi |alist.allp(\x. atom x, range alist)\alistp invalist(alist)|))
   alistinduction (open range member invalist)
   (use allpfact ue: ((\phi.|\x. atom x|))(x,y)(u.|range alist|) mode: always) )
   ; VALIST. ALLP(AX.ATOM X, RANGE(ALIST))\ALISTP \INALIST(ALIST)
   (label invalistsort)
; prove facts about composition of functions
; three (of five) lemmata
; lemma 1
3. (ue (chi |alist.member(x,dom(alist)))
   appalist(x,alist m alist1)=appalist(appalist(x,alist),alist1))
   alistinduction
   (part 1(use appalistdef mode: always)
     (open dom member compalist assoc)
     (use normal mode: always))
   ;VALIST.MEMBER(X,DOM(ALIST)))
   ;APPALIST(X,ALIST m ALIST1)=APPALIST(ALIST,X),ALIST1)
   (label alist_lemma1) (label app_compalist)

; lemma 2
4. (ue (chi |alist.dom(alist m alist1)=dom(alist)))
   alistinduction
   (open compalist dom)
   ;VALIST.DOM(ALIST m ALIST1)=DOM(ALIST)
   (label alist_lemma2) (label dom_compalist)

; compalist lemma
5. (ue (chi |alist.-member(za,range alist)-alist m ((za).alist1)=alist m alist1))
   alistinduction
   (open member range compalist appalist assoc) (use demorgan mode: always))
   ;VALIST.-MEMBER(ZA,RANGE(ALIST))=ALIST m ((ZA).ALIST1)=ALIST m ALIST1
   (label compalist_lemma)

; samemap right
6. (ue (chi |alist.samemap(alist1,alist2)-alist m alist1=alist m alist2))
   alistinduction
   (part 1(use samemap_def mode: exact)
     (part 1(open compalist samemap)))
   ;VALIST.SAMEMAP(ALIST1,ALIST2)ALIST m ALIST1=ALIST m ALIST2
   (label samamap_right)

; prove a fact about the identity function
; idalistp_main
7. (ue (chi |alist.idalistp(alist)-alistp(y,dom alist)-alistp(y,alist)=y))
   alistinduction
   (open idalistp appalist assoc member dom) (use normal mode: always))
   ;VALIST.IDALISTP(ALIST)-alistp(y,DOM(ALIST))=DOM(ALIST)
   (label idalistp_main)

; prove facts about inversion of functions
; dom invalist
8. (ue (chi |alist.allp(Ax.atom x,range alist)-alist invalalist(x)=range alist))
   alistinduction (open dom range invalist) (use invalistsort)
   (use allpfact ue: ((phi\.Ax.atom x)(x,y)u.range alist)) (mode: always))
   ;VALIST.ALLP(AX.ATOM X,RANGE(ALIST))DOM(INVALIDST(ALIST))=RANGE(ALIST)
   (label dom_invalist)

; range invalist
9. (ue (chi |alist.allp(Ax.atom x,range alist)-alist invalalist(x)=dom alist))
   alistinduction (open dom range invalist) (use invalistsort)
   (use allpfact ue: ((phi\.Ax.atom x)(x,y)u.range alist)) (mode: always))
   ;VALIST.ALLP(AX.ATOM X,RANGE(ALIST))RANGE(INVALIDST(ALIST))=DOM(ALIST)
   (label range_invalist)
8.26.2. Lemma Nonempty Range.

(proof nonempty-range)
;lemma 3
5. (ue (chi |alist.member(x,dom alist)|somep(\exists y.appalist(x,alist)=y.range alist))
   alistinduction
   (part 1 (open dom somep range member appalist assoc))
   (use normal mode: always))
;\forallalist\in\text{DOM}(\text{ALIST})\exists\text{SOME}\in\text{RANGE}(\text{ALIST})
   \exists\text{APP}\in\text{ALIST}(x,\text{ALIST})=\text{X}

6. (rw * (use somepfact mode: exact))
;\forallalist\in\text{DOM}(\text{ALIST})\exists\text{APP}\in\text{ALIST}(x,\text{ALIST})=\text{X}
   (\exists x.\text{MEMBER}(x,\text{RANGE}(\text{ALIST}))\text{APP}(x,\text{ALIST})=\text{X})
   (label nonempty-range)


This lemma says that if $Z$ belongs to $\text{range}(\text{alist})$, then there is an $x$ in $\text{dom}(\text{alist})$ such that $\text{appalist}(x,\text{alist})=z$. As noticed above, this requires the fact that $\text{alist}$ represents a function, i.e. that $\text{dom}(\text{alist})$ has the uniqueness property, for if some $(x,z_1)$ occurs in $\text{alist}$ before $(x,z)$, with $z_1#z$, then $\text{appalist}(x,\text{alist})$ will give $z_1$ as value.

;lemma 4
(proof nonempty-domain)
1. (assume $\exists x.\text{MEMBER}(x,\text{DOM}(\text{ALIST}))\text{APP}(x,\text{ALIST})=z$)
   (label lem41)
2. (assume $\exists x.\text{MEMBER}(x,\text{DOM}(\text{ALIST}))\text{APP}(x,\text{ALIST})=z$)
   (label lem42)
3. (rw * (open uniqueness dom))
   $\exists x.\text{MEMBER}(x,\text{DOM}(\text{ALIST}))\text{UNIQUENESS}(\text{DOM}(\text{ALIST}))$
   (label lem43)
   ;deps: (LEM42)
4. (assume $\exists x.\text{MEMBER}(x,\text{DOM}(\text{ALIST}))\text{APP}(x,\text{ALIST})=z$)
   (label lem44)
5. (rw * (open range member))
   $Z=\exists x.\text{MEMBER}(x,\text{DOM}(\text{ALIST}))\text{APP}(x,\text{ALIST})=z$
   (label lem45)
   ;deps: (LEM44)

We use the last line for a proof by cases. The first case follows by expanding the definitions.

6. (assume $z=y$)
7. (trw $\exists x.\text{MEMBER}(x,\text{DOM}(\text{ALIST}))\text{APP}(x,\text{ALIST})=z$
   open dom member appalist assoc (use * mode: exact))
   $\exists x.\text{MEMBER}(x,\text{DOM}(\text{ALIST}))\text{APP}(x,\text{ALIST})=z$
   (label lem46)
We use the assumption of the second case and the induction hypothesis (line 1) to get an element \( x_2 \) in the inverse image of \( z \) (line 9); then we use the assumption of \textit{uniqueness} (lines 2 and 3) to show that \( x_2 \neq x_a \) (line 10) and

\[
\text{appalist } (x_2, (x_a, y). \text{alist}) = \text{appalist}(x_2, \text{alist}) = z
\]

(line 11).

8. (assume \( \text{member}(z, \text{range}(\text{alist})) \))
   (label lem47)

9. (define xxv \( \text{member}(xxv, \text{dom} \text{alist}) \) \text{appalist}(xxv, \text{alist}) = z)
   (lem41 lem43 lem47)
   (label lem48)
   ;deps: (lem41 lem42 lem47)

10. (derive \( xxv \times x_a \) (lem43 lem48))
    ;deps: (lem41 lem42 lem47)

11. (true \( \text{appalist}(xxv, (x_a, y). \text{alist}) = z \)) (open \text{appalist assoc})
    (use * mode: exact) (use lem48 mode: always direction: reverse>
    ;APPALIST(xxv, (X_A, Y).ALIST) = Z
    ;deps: (lem41 lem42 lem47)

12. (derive \( \exists x_1. \text{member}(x_1, \text{dom}(x_a, y). \text{alist})) \text{appalist}(x_1, (x_a, y). \text{alist}) = z \)
    (lem48 *) (open dom) (use memberdef mode: always)
    (label lem49)
    ;deps: (lem41 lem42 lem47)

13. (cases lem45 lem46 lem49)
    ;\( \exists X_1. \text{MEMBER}(X_1, \text{DOM}((X_A, Y). \text{ALIST})) \) \text{APPALIST}(X_1, (X_A, Y). \text{ALIST}) = Z
    ;deps: (lem41 lem42 lem47)

14. (ci lem42 lem44)
    ;\text{UNIQUENESS}(\text{DOM}((X_A, Y). \text{ALIST})) \text{MEMBER}(Z, \text{RANGE}((X_A, Y). \text{ALIST})))
    ;(3X_1. \text{MEMBER}(X_1, \text{DOM}((X_A, Y). \text{ALIST}))) \text{APPALIST}(X_1, (X_A, Y). \text{ALIST}) = Z
    ;deps: (lem41)

15. (ci lem41)

16. (ue (chi \( \text{alist}. \text{uniqueness} \text{dom}(\text{alist}) \) \text{member}(z, \text{range} \text{alist}))
    (3x. \text{member}(x, \text{dom} \text{alist}) \text{appalist}(x, \text{alist}) = z))
    \text{alistinduction}
    (part #1 (open range member)) (use * mode: exact)
    ;\text{UNIQUENESS}(\text{DOM}(\text{ALIST})) \text{MEMBER}(Z, \text{RANGE}(\text{ALIST})))
    ;(3X. \text{MEMBER}(X, \text{DOM}(\text{ALIST}))) \text{APPALIST}(X, \text{ALIST}) = Z
    (label nonempty-domain)

\[ \star \]

\subsection*{8.26.4. Lemma Range Compose, Part 1.}

;\text{theorem} 1 (i); lemma range compose, part 1
;proof range-compose
1. (assume \( \text{permutp}(\text{alist}) \))
   (label rc1)
2. (rw * (open \text{permutp} \text{functp}))
   ;\text{UNIQUENESS}(\text{DOM}(\text{ALIST})) \text{MKLSET}(\text{DOM}(\text{ALIST})) = \text{MKLSET}(\text{RANGE}(\text{ALIST}))
   (label rc2)
3. (assume lmkls \text{set dom}(alist)\text{=}mklset \text{dom}(alist1)\text{)}
   (label rc3)

4. (assume \text{member}(z,\text{range}(alist \circ \text{alist1}))\text{)}
   (label rc4)

   \text{apply lemma 4 and lemma 2}

      (ue((alist1.alist \circ \text{alist1}})(z.z)) \text{nonempty-domain}
      (use \text{dom\_com\_array} rc2 rc4 mode: \text{exact})
   ; \text{deps: (RC1 RC4)}

6. (define xxvv \text{member}(xxvv,dom alist)\text{Appalist}(xxvv,alist \circ \text{alist1})\text{=z} \text{)}
   (label rc5)
   ; \text{deps: (RC1 RC4)}

   \text{apply lemma 3}

7. (define yyvv \text{member}(yyvv,range alist)\text{Appalist}(yyvv,alist)\text{=}yyvv\text{)}
   (nonempty-range rc6)
   (label rc7)
   ; \text{deps: (RC1 RC4)}

8. (define zzvv \text{member}(zzvv,range alist)\text{Appalist}(yyvv,alist)\text{=}zzvv\text{)}
   (nonempty-range rc8)
   (label rc8)
   ; \text{deps: (RC1 RC3 RC4)}

9. (trn lyyvv \epsilon \text{mklset range}(alist)\text{(open mklset epsilon) rc7})
   (use \text{mklset}(range(alist))
   ; \text{deps: (RC1 RC4)}

10. (define xxvv \text{member}(xxvv,range alist)\text{Appalist}(xxvv,alist \circ \text{alist1})\text{=z}\text{)}
    (label rc9)
    ; \text{deps: (RC1 RC4)}

11. (define xxvv \text{member}(xxvv,range alist)\text{Appalist}(xxvv,alist \circ \text{alist1})\text{=}xxvv\text{)}
    (nonempty-range rc8)
    (label rc8)
    ; \text{deps: (RC1 RC3 RC4)}

12. (define xxvv \text{member}(xxvv,range alist)\text{Appalist}(xxvv,alist \circ \text{alist1})\text{=}xxvv\text{)}
    (nonempty-range rc8)
    (label rc8)
    ; \text{deps: (RC1 RC3 RC4)}

13. (trn lyyvv \epsilon \text{mklset range}(alist)\text{(open mklset epsilon) rc7})
    (use \text{mklset}(range(alist))
    ; \text{deps: (RC1 RC4)}

14. (define xxvv \text{member}(xxvv,range alist)\text{Appalist}(xxvv,alist \circ \text{alist1})\text{=}xxvv\text{)}
    (nonempty-range rc8)
    (label rc8)
    ; \text{deps: (RC1 RC3 RC4)}

15. (define xxvv \text{member}(xxvv,range alist)\text{Appalist}(xxvv,alist \circ \text{alist1})\text{=}xxvv\text{)}
    (nonempty-range rc8)
    (label rc8)
    ; \text{deps: (RC1 RC3 RC4)}

16. (define xxvv \text{member}(xxvv,range alist \circ \text{alist1})\text{Appalist}(xxvv,alist \circ \text{alist1})\text{=}xxvv\text{)}
    (nonempty-range rc8)
    (label rc8)
    ; \text{deps: (RC1 RC3 RC4)}

;theorem 1 (i); lemma range compose, part 2
(proof range_compose2)

1. (assume |permutp(alist)>)
   (label rc21)

2. (rw * (open permutp functp))
   ;UNIQUENESS(DOM(ALIST))<MKLSET(DOM(ALIST))=MKLSET(RANGE(ALIST))
   (label rc22)

3. (assume |permutp(alist1)>)
   (label rc23)

4. (rw * (open permutp functp))
   ;UNIQUENESS(DOM(ALIST1))<MKLSET(DOM(ALIST1))=MKLSET(RANGE(ALIST1))
   (label rc24)

5. (assume |mklset dom(alist)=mklset dom(alist1)>)
   (label rc25)

6. (assume |member(z,range alist1)>)
   (label rc26)

;apply lemma 4

7. (define yv1 |member(yv1,dom alist1)<appalist(yv1,alist1)=z|
   (nonempty-domain rc24 rc26))
   (label rc27)
;deps: (RC23 RC26)

8. (trw |yv1 e mklset dom(alist1)>) * (open epsilon mklset))
   ;YV1E(MKLSET(DOM(ALIST1))
   ;deps: (RC23 RC26)

9. (rw * (use rc25 mode: exact direction: reverse)
   (use rc22 mode: exact>)
   ;YV1E(MKLSET(RANGE(ALIST)))
   ;deps: (RC21 RC23 RC25 RC26)

10 (rw * (open epsilon mklset))
   ;MEMBER(XV1,RANGE(ALIST))
   (label rc28)
;deps: (RC21 RC23 RC25 RC26)

;apply again lemma 4, this time to alist

11. (define xv1 |member(xv1,dom alist)<appalist(xv1,alist)=yv1|
    (nonempty-domain rc22 rc28))
   (label rc29)

(proof permutp_complalist)

1. (assume (permutp (alist)))
   (label permut_compl1)

2. (assume (permutp (alist)))
   (label permut_compl2)

3. (assume (mklset (dom (alist))=mklset (dom (alist))))
   (label permut_compl3)
4.  (derive |mklsset(range(alist @ alist1))|Cmklsset(range(alist1))) | 
   mklsset(range(alist1))Cmklsset(range(alist @ alist1)) | 
   (permut-comp1 permut-comp2 permut-comp3 range-compose) 
   ;deps: (PERMUT-COMP1 PERMUT-COMP2 PERMUT-COMP3)

5.  (derive |mklsset(range(alist @ alist1))=mklsset(range(alist1))) | 
   (* double-inclusion) 
   ;deps: (PERMUT-COMP1 PERMUT-COMP2 PERMUT-COMP3) 
   (label permut_comp4)

6.  (rw permut-comp1 (open permutp functp)) 
   ;UNIQUENESS(DOM(ALIST))XMKLSET(DOM(ALIST))=MKLSET(RANGE(ALIST)) 
   (label permut_comp5)

7.  (rw permut-comp2 (open permutp)) 
   ;FUNCTP(ALIST1)XMKLSET(DOM(ALIST1))=MKLSET(RANGE(ALIST1))

8.  (trw |uniqueness(dom(alist @ alist1))X 
   mklsset dom(alist @ alist1)=mklsset range(alist m alist1)) | 
   (use dom-comparealist permut-comp4 mode: exact) permut-comp5 
   (use * permut-comp3 mode: always direction: reverse>) 
   ;UNIQUENESS(DOM(ALIST) @ ALIST1))X 
   ;MKLSET(DOM(ALIST @ ALIST1))=MKLSET(RANGE(ALIST @ ALIST1)) 
   ;deps: (PERMUT-COMP1 PERMUT-COMP2 PERMUT-COMP3)

9.  (trw |permutp(alist @ alist1)|* (open permutp functp)) 
   ;PERMUTP(ALIST @ ALIST1) 
   ;deps: (PERMUT-COMP1 PERMUT-COMP2 PERMUT-COMP3)

10. (ci (permut-comp1 permut-comp2 permut-comp3)) 
    ;PERMUTP(ALIST)XPERMUTP(ALIST1)XMKLSET(DOM(ALIST))=MKLSET(DOM(ALIST1))X 
    ;PERMUTP(ALIST @ ALIST1) 
    (label permutp_comalist)


;theorem 1 (ii)
(proof compalist_associativity)

1.  (trw |mklsset(range((xa.y).alist))|Cmklsset(dom alist1)) 
   member(y,dom alist1)Amklsset(range(alist)Cmklsset dom(alist1)) | 
   (open mklsset inclusion range member)(use normal mode: always) 
   ;MKLSET(RANGE((XA.Y).ALIST))Cmklsset(DOM(ALIST1)) 
   ;MEMBER(Y,DOM(ALIST1))AMKLSET(RANGE(ALIST))Cmklsset(DOM(ALIST1))

2.  (trw |member(y,dom alist1)Amklsset range(alist)Cmklsset dom(alist1)) | 
   mklsset(range((xa.y).alist))Cmklsset(dom alist1) |(der) 
   (open mklsset inclusion range member)(use normal mode: always) 
   ;MEMBER(Y,DOM(ALIST1))AMKLSET(RANGE(ALIST))Cmklsset(DOM(ALIST1)) 
   ;MKLSET(RANGE((XA.Y).ALIST))Cmklsset(DOM(ALIST1))

3.  (derive |mklsset(range((xa.y).alist))|Cmklsset(dom(alist1))= 
   member(y,dom alist1)Amklsset range(alist)Cmklsset dom(alist1)) |(* -2)) 
   (label helpinduction)

4.  (ue (chi |alist.mklsset(range alist)Cmklsset(dom(alist1)) | 
   alist m (alist1 m alist2)=(alist m alist1) m alist2) | 
   altinduction 
   (part 1 (open compalist)(use app_compalist * mode: always))) 
   ;VALIST.MKLSET(RANGE(ALIST))Cmklsset(DOM(ALIST1)) 
   ;ALIST m (ALIST1 m ALIST2)=(ALIST m ALIST1) m ALIST2 
   (label compalist_associativity)

(proof samemap_left)

1. (assume (samemap (alist1, alist2)))
   (label sml1)

2. (rw * (open samemap))
   ; MKLSET(DOM(ALIST1)) = MKLSET(DOM(ALIST2)) \* 
   ; (<Y, Y> \in MKLSET(DOM(ALIST1)), YAPPALIST(Y, ALIST1) = APPALIST(Y, ALIST2))
   (label sm12)

3. (assume (y \in MKLSET DOM(alist1)))
   (label sm13)

4. (derive (appalist (y, alist1) = appalist (y, alist2) | (sml2 sm13))
   (label sm14)

5. (rw sm13 (use sml2 mode: exact))
   ; Y \in MKLSET(DOM(ALIST2))
   (label sm15)

6. (rw sm13 (open epsilon mklset))
   ; MEMBER(Y, DOM(ALIST1))

7. (rw sm15 (open epsilon mklset))
   ; MEMBER(Y, DOM(ALIST2))

8. (trw (appalist (y, alist1 \at alist) = appalist (y, alist2 \at alist))
   (use app-compalist -2 mode: exact)
   (use app-compalist * mode: exact)
   (use sml4 mode: exact))
   ; APPALIST(Y, ALIST1 \at ALIST) = APPALIST(Y, ALIST2 \at ALIST)
   ; deps: (sm1 sml3)

9. (ci sml3)
   ; Y \in MKLSET(DOM(ALIST1)) \Rightarrow APPALIST(Y, ALIST1 \at ALIST) = APPALIST(Y, ALIST2 \at ALIST)

10. (trw |MKLSET(DOM(ALIST1) \at ALIST) = MKLSET(DOM(ALIST2) \at ALIST)|
    dom_compalist (use sml2 mode: exact))
    ; MKLSET(DOM(ALIST1) \at ALIST) = MKLSET(DOM(ALIST2) \at ALIST))

11. (trw |samemap (alist1 \at alist, alist2 \at alist)|
    (open samemap)
    (dom_compalist * -2))
    ; SAMEMAP(ALIST1 \at ALIST, ALIST2 \at ALIST)
    ; deps: (sm1)

12. (ci sm1)
    ; SAMEMAP(ALIST1, ALIST2) \* SAMEMAP(ALIST1 \at ALIST, ALIST2 \at ALIST)
    (label samemap-left) ■


; theorem 2 (i) (permutp idalistp)
(proof idalistprop)

1. (ue (chi |alist.idalistp(alist) |DOM(alist)=range(alist) |alistinduction
   (open idalistp dom range))
   ; ALIST.IDALISTP(ALIST) = DOM(ALIST) = RANGE(ALIST)

2. (trw |alist.functp(alist) |Aidalistp(alist) = permutp(alist))|
(open tunctp permutp)(use * mode: always))

\(\text{NIL}\)

(theorem 2 (ii) (idalistp right))

1. (assume \(\text{idalistp (alistl)}\))
   (label idal_11)
   \(\text{ALISTID is unknown.}\)
   \(\text{the symbol ALISTID is given the same declaration as ALIST}\)

2. (assume \(\text{mklset dom(alistl)}\)=mklset dom(alist))
   (label idal_12)

3. (assume \(\text{y}\in\text{mklset dom(alistid \aleq alist)}\))
   (label idal_13)

4. (rw * (use dom_mcompalist mode: exact)(open epsilon mklset))
   (label idal_14)
   \(\text{MEMBER Y DOM(ALISTID)}\)
   ;deps: (idal_13)

5. (trw \(\text{appalist(y,alistid \aleq alist)}\)| (use app,compalist * mode: exact))
   \(\text{APPALIST(Y,ALISTID \aleq ALIST)=APPALIST(APPALIST(Y,ALISTID),ALIST)}\)
   (label idal_15)

;labels: IDALISTP MAIN
;VALIST Y IDALISTP ALIST MEMBER Y DOM(ALIST)\(\text{\text{APPALIST}(Y,ALIST)}\)=Y

6. (derive \(\text{appalist(y,alistid)=y}\) (idalistp=main idal_11 idal_14))
   ;deps: (idal_11 idal_13)

7. (rw idal_16 * )
   \(\text{APPALIST(Y,ALISTID \aleq ALIST)=APPALIST(Y,ALIST)}\)
   ;deps: (idal_11 idal_13)

8. (cil idal_13)
   \(\text{MKLSET(DOM(ALISTID \aleq ALIST))\text{APPALIST}(Y,ALISTID \aleq ALIST)=APPALIST(Y,ALIST)}\)
   (label idal_16)
   ;deps: (idal_11)

9. (trw \(\text{mklset dom(alistid \aleq alist)}\)=mklset dom(alist))
   (use dom_compalist idal_12 mode: exact))
   \(\text{MKLSET(DOM(ALISTID \aleq ALIST))=MKLSET(DOM(ALIST))}\)
   ;deps: (idal_12)

;labels: SAMEMAPDEF
;\(\text{VALIST ALIST1.SAMEMAP(ALIST,ALIST)}\)=
### 8.26.10. Lemma Atomrange.

; a lemma: the range of a permutation contains only atoms
(proof atomrange)

1. \((\text{assume}\ \text{mklset}(\text{dom}(\text{alist}))=\text{mklset}(\text{range}(\text{alist})))\)
   (label ar1)

2. \((\text{ue} \ (\chi \ \text{alist.allp}(\lambda x. \text{atom}(x), \text{dom}\ \text{alist}))\)
   \text{alistinduction}
   (open \text{allp} \ \text{dom})
   ; \text{VALIST.ALLP}(Ax. \text{ATOM} X, \text{DOM}(\text{ALIST}))
   (label ar2)

3. \((\text{ue} ((\phi 1. (Ax. \text{atom}(x))) (X.X) (\text{u}. \text{dom}\ \text{alist} \rightarrow \text{allp.elimination} \ *)\)
   ; \text{MEMBER}(X, \text{DOM}(\text{ALIST})) \rightarrow \text{ATOM} X\)

4. \((\text{tra} | \text{mklset} \ \text{dom}(\text{alist}) \subset C(Xx. \text{atom}(x))\)
   (open \text{inclusion} \text{mklset})
   ; \text{MKLSET}(\text{DOM}(\text{ALIST})) \subset C(Ax. \text{ATOM} X)\)

5. \((\text{ra} \ * \ (\text{use} \ \text{ar1} \ \text{mode}: \text{exact}))\)
   ; \text{MKLSET}(\text{RANGE}(\text{ALIST})) \subset C(Ax. \text{ATOM} X)\)

6. \((\text{rn} \ * \ (\text{open} \ \text{inclusion} \ \text{mklset})\)
   ; \forall Xx. \text{MEMBER}(X, \text{RANGE}(\text{ALIST})) \rightarrow \text{ATOM} X\)

7. \((\text{ue} ((\phi 1. (Ax. \text{atom}(x))) (X. \text{u}. \text{range}\ \text{alist})))\)
   \text{allp.introduction} \ *)\)
   ; \text{ALLP}(Ax. \text{ATOM} X, \text{RANGE}(\text{ALIST}))\)

8. \((\text{ci} \ \text{ar1})\)
   ; \text{MKLSET}(\text{DOM}(\text{ALIST}))=\text{MKLSET}(\text{RANGE}(\text{ALIST})) \rightarrow \text{ALLP}(Ax. \text{ATOM} X, \text{RANGE}(\text{ALIST}))\)
   (label atomrange) ■

### 8.26.11. Theorem 3, on Inversion of Alists.

; theorem 3 (i)
(proof permutp- invalist)

; we borrow this result from the proof permutp_injctp

; labels: \text{PERMUTP_INJECTP}
; \text{VALIST.PERMUTP ALIST} \rightarrow \text{INJECTP ALIST}
(proof permutp-invalist)
1. (assume lpermutp alist)
   (label piv1)
2. (derive [injectp alist] (permutp_injectp piv1))
   ;deps: (PIV1)
3. (rw * (open injectp))
   ;FUNCTP(ALIST) = UNIQUENESS(RANGE(ALIST))
   (label piv2)
4. (rw piv1 (open permutp))
   ;FUNCTP(ALIST) = MKLS(T(DOM(ALIST))) = MKLS(T(RANGE(ALIST)))
   (label piv3)
5. (derive [allp (\(\cdot\) x \(\cdot\) x, range alist)] (atomrange *))
   (label piv4)
6. (derive 1dom invalist (alist) = range alist) (dom_invalist *)
   (label piv5)
7. (derive 1range invalist (alist) = dom alist) (range_invalist piv4))
   (label piv6)
8. (trw Iuniqueness dom(invalist (alist))) piv2 (use piv5))
   ;UNIQUENESS(DOM(INVALIST(ALIST)))
   (label piv7)
9. (trw Imkls(T dom(invalist (alist))) mkls(T(range invalist (alist))))
   piv3 (use piv5 piv6))
   ;MKLS(T(DOM(INVALIST(ALIST)))) = MKLS(T(RANGE(INVALIST(ALIST))))
   (label piv8)
10. (trw lpermutp invalist (alist) piv7 piv8)
   (open permutp functp) (use invalistsort piv4 mode: exact))
   ;PERMUTP(INVALIST(ALIST))
   ;deps: (PIV1)
11. (ci piv1)
   ;PERMUTP(ALIST) = PERMUTP(INVALIST(ALIST))
   (label permutp_invalist) ■
   (proof invalistprop)
   ;theorem 3 (ii)
1. (ue (chi |alist.allp (\(\cdot\) x \(\cdot\) x, range (alist)) \(\cdot\) injectp (alist))
   idalistp(alist \(\cdot\) invalist (alist))])
   ;alistinduction
   (part
     (open range injectp functp uniqueness invalist
       idalistp compalist appalist assoc)
     (use invalistsort dom_invalist compalist-lemma mode: exact)
   * [VALIST ATT (\(\cdot\) x \(\cdot\) x, RANGE(ALIST)) \(\cdot\) INJECTP(ALIST))]
   ;IALISTP(ALIST \(\cdot\) INVALIST(ALIST))
   (label invalist-right) ■
   ;theorem 3 (iii)
2. (assume [allp (\(\cdot\) x \(\cdot\) x, range (alist))])
3. (ue ((alist. |invalist (alist)) (alist. |alist) (za.xa)(z.y)) compalist-lemma
   (use * invalistsort range_invalist mode: exact))
   ;\(\cdot\)MEMBER(XA,DOM(ALIST)) \(\cdot\) INVALIST(ALIST) \(\cdot\) ((XA.Y).ALIST) = INVALIST(ALIST) \(\cdot\) ALIST
4. (ci -2)
   ;ALLP (\(\cdot\) x \(\cdot\) x, RANGE(ALIST)))
### Section 8

5. \((\text{ue (chi alist.allp(ax,atom X,range(alist))Ainjectp(alist))}
\text{idalistp(invalid(alist)@alist))alistinduction}
(part 1 (open allp range injectp functp uniqueness
invalid compalist appalist assoc idalistp)
validistsort (use range-invalid mode: exact) (use * mode: always))
\text{validist.allp(ax,atom X,range(alist))Ainjectp(alist))}
\text{idalistp(invalid(alist)@alist))}
(label invalid.left) \]

#### 8.27. file PERMP: Functions Represented by Lists, Using Predicates.

;definitions of composition, identity, inverse as predicates
(proof comp_pred)

;composition of functions

(defc comp (type: [ground@ground@ground@truthvall]) (syntype: constant)
(bindingpower: 930))

(define comp |\forall u,w.\text{comp}(u,v,w)\equiv
\text{length u=\text{length w}}\&\&\text{\forall n<\text{length u}\text{U\text{n}}th(u,n)=\text{n}}\text{th}(v,\text{nth(w,n)))}
(label compdef)

;the identity function

(defc id (type: [ground@truthvall]))
(defax id |\forall u.\text{id}(u)\equiv(\text{\forall n<\text{length u}\text{U\text{n}}th(u,n)=n})
(label id_def)

;the inverse of a function

(defc inv (type: [ground@ground@truthvall]))
(defax inv |\forall v.\text{inv}(u,v)\equiv(\text{\forall n<\text{length u}\text{U\text{n}}th(u,n)=\text{fstposition}(v,n))})
(label invdef)

#### 8.27.1. Composition of Permutations is a Permutation.

(proof comp_perm)

1. (assume \(\text{perm}(v)\))
   (label cp_pm1)

2. (assume \(\text{perm}(w)\))
   (label cp_pm2)

3. (assume \(\text{length v=\text{length w}}\))
   (label cp_pm3)

   (assume \(\text{Icomp}(u,v,w)\))
   (label cp_pm4)

5. (\text{\forall w cp.pm1 (open perm into onto))}
   (label cp_pm5)
   ;(\text{\forall n<\text{length v}\text{\&\&natnum(\text{nth(v,n)})\&\&natural(v,n)<\text{length v})\&\&
   ;(\text{\forall n<\text{length v}\text{\&\&member(w,v)}}})
218 ABOUT PERMUTATIONS IN LISP AND EKL

6. (rw cp_pm2 (open perm into onto))
   (label cp_pm6)
   ;(VN. N<LENGTH W) NATNUM(NTH(W,N)<ANTH(W,N)<LENGTH W)
   ;(VN. N<LENGTH W) MEMBER(N,H)

7. (rw cp_pm4 (open comp))
   (label cp_pm7)
   ;LENGTH U=LENGTH WA(VN. N<LENGTH U=NTH(U,N)<ANTH(V,NTH(W,N)))

8. (assume |m<length(U)|)
   (label cp_pm8)

9. (rw * (use cp_pm7 mode: always))
   (label cp_pm9)
   ;M<LENGTH W

10. (derive |natnum(nth(w,m))<ANTH(w,m)<length v| (cp_pm6 *)
     (use cp_pm3 mode: exact))

11. (trw |natnum(nth(v,nth(w,m)))<ANTH(v,nth(w,m))<length v| (* cp_pm5))
    (label cp_pm10)

12. (derive |nth(u,m)=nth(v,nth(w,m))| (cp_pm7 cp_pm8)
     (open appl) (use -2))

13. (trw cp_pm10 (use * mode: exact direction: reverse>)
    ;NATNUM(NTH(U,M))<ANTH(U,M)<LENGTH V
    (label cp_pm11)

14. (trw |length U=LENGTH v| (use cp_pm7 cp_pm3 mode: always))
    ;LENGTH U=LENGTH V

15. (rw cp_pm11 (use * mode: exact direction: reverse>)
    ;NATNUM(NTH(U,M))<ANTH(U,M)<LENGTH U
    ;deps: (CP_PM1 CP_PM2 CP_PM3 CP_PM4 CP_PM8)

16. (ci cp_pm8)
    ;M<LENGTH U=NATNUM(NTH(U,M))<ANTH(U,M)<LENGTH U

17. (trw lint0 (open into) *)
    (label cp_into)
    ;INTO(U)
    ;deps: (CP_PM1 CP_PM2 CP_PM3 CP_PM4)

18. (rw cp_pm9 (use cp_pm3 mode: exact direction: reverse>)
    ;M<LENGTH V

19. (trw |member(m,v)| (* cp_pm5))
    ;MEMBER(M,V)
    (label cp_pm20)

20. (derive |3j. j<length(v)<ANTH(v,j)=m| (* member_nth))
    (label cp_pm21)
    ;deps: (CP_PM1 CP_PM3 CP_PM4 CP_PM8)

21. (define jv |jv<length(v)<ANTH(v,jv)=m| *)
    (label cp_pm22)

22. (rw * (use cp_pm3 mode: exact))
    ;JV<LENGTH W ANTH(V,JV)=M

23. (trw |member(jv,w)| (* cp_pm6))
    ;MEMBER(JV,W)

24. (derive |3k. k<length(w)<ANTH(w,k)=jv| (* member_nth))
25. (define \( \text{kw} | \text{kv} \leq \text{length}(w) \) \( \text{Anth}(w, \text{kv}) = jv \) *)

(label cp.pm23)

26. (rw cp.pm22 (use * mode: always direction: reverse>)
   \( \text{NTH}(w, \text{kv}) < \text{LENGTH} \) \( \text{VANTH}(v, \text{NTH}(w, \text{kv})) = m \)

(label cp.pm24)

27. (rw \( \text{kv} < \text{length}(u) \) | cp.pm23 (use cp.pm7 mode: always))
   \( \text{KV} < \text{LENGTH} \) \( u \)

(label cp.pm25)

28. (rw lnatnum nth(w, \text{kv}) \( i \) cp.pm23)
   \( \text{NATNUM}(\text{NTH}(w, \text{kv})) \)

29. (derive \( \text{nth}(u, \text{kv}) = \text{nth}(y, \text{nth}(w, \text{kv})) \) | (cp.pm7 cp.pm25)
   (open appl)(use *))

30. (rw * (use cp.pm24 mode: always))
   \( \text{NTH}(u, \text{kv}) = m \)

31. (derive \( \text{member}(m, u) \) | nthmember cp.pm25 (use * mode: exact direction: reverse>)
   ; deps: (CP-PM1 CP-PM2 CP-PM3 CP-PM4 CP-PM8)

32. (ci cp.pm8)
   \( \text{M} < \text{LENGTH} \) \( \text{UMEMBER}(m, u) \)

(label cp-onto)

33. (rw lperm \( w \) (open perm onto) cp.into cp-onto)
   \( \text{PERM}(U) \)

; deps: (CP-PM1 CP-PM2 CP-PM3 CP-PM4)

34. (ci (cp.pm1 cp.pm2 cp.pm3 cp.pm4))
   \( \text{PERM}(V) \) \( \text{APERM}(W) \) \( \text{LENGTH} \) \( \text{V} = \text{LENGTH} \) \( \text{W} \) \( \text{ACOMP}(U, V, W) \) \( \text{PERM}(U) \)

(label perm.composition)

Composition of functions is unique:

35. (rw |comp(u,v,w)Acomp(u1,v,w)\( \text{u} = \text{u1} | \) (open comp) extensionality)
   \( \text{COMP}(U, V, W) \) \( \text{ACOMP}(U_1, V, W) \) \( \text{U} = \text{U}_1 \)

(label comp.uniqueness)

8.27.2. Composition is Associative.

(proof comp.associative)

1. (assume \( \text{into}(w3) \))

(label ca1)

2. (assume \( \text{length} \) \( w_2 = \text{length} \) \( w_3 \))

(label ca2)

3. (assume \( \text{comp}(v, w_1, w_2) \))

(label ca3)

| assume \( \text{comp}(u, v, w_3) \)

(label ca4)

5. (assume \( \text{comp}(v_1, w_2, w_3) \))
(label ca5)

6. (assume [comp(u1,w1,v1)])
   (label ca6)

7. (assume [n<length u])
   (label ca7)

8. (rw ca4 (open comp))
   ;LENGTH U = LENGTH W3A (VN, N < LENGTH U) NTH(U, N) = NTH(V, NTH(W3, N))
   (label ca8)
   ;deps: (CA4)

9. (derive [n<length(w3)]) (ca7 ca8)
   (label ca9)
   ;deps: (CA4 CA7)

10. (derive [nth(u,n)=nth(v,nth(w3,n))]) (ca8)
    (label ca10)
    ;deps: (CA4 CA7)

11. (rw ca1 (open into))
    ;VN, N < LENGTH W3 = NTH(W3, N) NTH(W3, N) < LENGTH W3
    ;deps: (CA1)

12. (derive [nth(w3,n)<length(w2)])
    (label call)
    ;deps: (CA1 CA2 CA4 CA7)

13. (rw ca3 (open comp))
    ;LENGTH V = LENGTH W3A (VN, N < LENGTH V) NTH(V, N) = NTH(W1, NTH(W2, N))
    (label ca12)
    ;deps: (CA3)

14. (derive [nth(w3,n)<length(v)])
    (call ca12)
    (label ca13)
    ;deps: (CA1 CA2 CA3 CA4 CA7)

15. (derive [vn.n<length(v)nth(v,n)=nth(w1,nth(w2,n))])
    (call ca12)

16. (ue (n [nth(w3,n)]) * call ca13)
    ;NTH(V, NTH(W3, N)) = NTH(W1, NTH(W2, NTH(W3, N))
    ;deps: (CA1 CA2 CA3 CA4 CA7)

17. (rw ca10 (use * mode: exact))
    ;NTH(U, N) = NTH(W1, NTH(W2, NTH(W3, N))
    ;deps: (CA1 CA2 CA3 CA4 CA7)

18. (rw ca5 (open comp))
    (label ca20)
    ;LENGTH V1 = LENGTH W3A (VN, N < LENGTH V1) NTH(V1, N) = NTH(W2, NTH(W3, N))

19. (derive [nth(w1,n)=nth(w2,nth(w3,n))])
    (call ca20)
    ;deps: (CA4 CA5 CA7)

20. (rw ca6 (open comp))
    ;LENGTH U1 = LENGTH V1A (VN, N < LENGTH U1) NTH(U1, N) = NTH(W1, NTH(V1, N))
    (label ca22)
    ;deps: (CA6)

21. (cw ca9 (use ca20 ca22 mode: always direction: reverse))
    ;N<LENGTH U1
    ;deps: (CA4 CA5 CA6 CA7)
21. (derive \( \text{nth}(u_1, n) = \text{nth}(w_1, \text{nth}(v_1, n)) \) ; (ca22 *))
   ; deps: (CA4 CA5 CA6 CA7)

22. (rw * (use ca21 mode: exact))
   ; \( \text{nth}(u_1, n) = \text{nth}(w_1, \text{nth}(w_2, \text{nth}(w_3, n))) \)
   ; (label ca23)
   ; deps: (CA4 CA5 CA6 CA7)

24. (rw ca14 (use ca23 mode: exact direction: reverse))
   ; \( \text{nth}(u, n) = \text{nth}(u_1, n) \)
   ; deps: (CA1 CA2 CA3 CA4 CA5 CA6 CA7)

25. (ci ca7)
   ; \( \text{N}<\text{LENGTH} \ u \ \Rightarrow \text{Nth}(u, n) = \text{nth}(u_1, n) \)
   ; (label ca24)
   ; deps: (CA1 CA2 CA3 CA4 CA5 CA6)

26. (trw length \ u = \text{length} \ u_1 \) (use ca8 ca22 mode: always)
    (use ca20 mode: always direction: reverse)
    ; \( \text{LENGTH} \ u = \text{LENGTH} \ u_1 \)
    ; deps: (CA4 CA5 CA6)

27. (ue ((u.u) (v.u1))) extensionality ca24 *)
    ; U = U_1
    ; deps: (CA1 CA2 CA3 CA4 CA5 CA6)

28. (ci (ca1 ca2 ca3 ca4 ca5 ca6))
    ; \( \text{INTO}(W_3) \ \text{LENGTH} \ W_2 = \text{LENGTH} \ W_3 \)
    ; \( \text{COMP}(V, W_1, W_2) \ \text{ACOMP}(U, V, W_3) \)
    ; \( \text{COMP}(V_1, W_2, W_3) \ \text{ACOMP}(U_1, W_1, V_1) \)
    ; U = U_1
    ; (label associativity_pred)

8.27.3. Using Predicates: Identity.

; id implies perm
(proof idperm)

1. (trw id(u) \text{into}(u)) (open id into>>)
   ; \( \text{ID}(U) \ \text{INTO}(U) \)
   ; (label p_11)

2. (assume [id(u)])
   ; (label p_12)

3. (rw * (open id))
   ; \( \text{N}<\text{LENGTH} \ u \ \Rightarrow \text{Nth}(u, n) = n \)
   ; (label p_13)

4. (assume [n<length u])
   ; (label p_14)

5. (derive \( \text{member}(\text{nth}(u, n), u) \)) (* nthmember)

6. (derive \( \text{member}(n, u) \)) (* p_14 p_13)

7. (ci p_14)
   ; \( \text{N}<\text{LENGTH} \ u \ \text{MEMBER}(N, U) \)

8. (derive \( \text{perm} \ u \)) (p_11 p_12 *) (open perm onto)

9. (ci p_12)
   ; \( \text{ID}(U) \ \text{PERM}(U) \)
(label id_perm) •

;Theorem 2 (ii) (id right)
(proof identity-right)
1. (assume |id(u)|)
   (label id_r1)
2. (assume |comp(v,w,u)|)
   (label id_r2)
3. (assume llength w=length u|)
   (label id_r3)
4. (rw id_r1 (open id))
   ;VN.N<LENGTH U|=NTH(U,N)=N
   (label id_r4)
5. (rw id_r2 (open comp))
   ;LENGTH V=LENGTH WA(VN.N<LENGTH U|=NTH(U,N)=NTH(W,NTH(U,N)))
   (label id_r5)
6. (rw * (use id_r4 mode: always))
   ;LENGTH V=LENGTH WA(VN.N<LENGTH U|=NTH(U,N)=NTH(W,N))
   (label id_r6)
7. (trw llength v=length w| (use id_r3 id_r5 mode: always))
   ;LENGTH V=LENGTH W
8. (derive |v=w| (extensionality id_r6 *))
9. (ci (id_r1 id_r2 id_r3))
   ;ID(U) |COMP(V,W,U) |LENGTH W=LENGTH UDV=W
   (label id-right) •

;Theorem 2 (iii) (id left)
(proof identity-left)
1. (assume |id(u)|)
   (label id_11)
2. (assume lperm w l)
   (label id_12)
3. (assume llength w=length u|)
   (label id_13)
4. (assume |comp(v,u,w)|)
   (label id_14)
5. (rw id_11 (open id))
   ;VN.N<LENGTH U|=NTH(U,N)=N
   (label id_15)
6. (rw id_14 (open comp))
   ;LENGTH V=LENGTH WA(VN.N<LENGTH U|=NTH(U,NTH(W,U)))
   (label id_16)
7. (rw id_12 (open perm onto into>)
   ;(VN.N<LENGTH W|NATNUM(NTH(W,N)) NTH(W,N)<LENGTH W) A
   ;(VN.N<LENGTH W|MEMBER(N,W))
   (label id_17)
8. (trw |VN.m<length u|natnum(nth(w,m))nth(w,m)<length u| id-17
8.27.4. Using Predicates: the Inverse Permutation Theorem.

**Theorem 3 (i) (Inv Perm)**

\[ \text{VU V.PERM(U)AINV(V,U)ALENGTH V=LENGTH UCPERM(V)} \]

Part 1: inv implies into

(proof inv_into)

1. (assume |perm(u)|)
   (label i1)

2. (assume |inv(v,u)|)
   (label i2)

3. (assume |length v=length u|)
   (label i3)

4. (rw i11 (open perm into onto) )
   (label i14)
   ;(VM.MLENGTH UDNUM(NTH(U,V)))ANTH(U,W)<LENGTH U
   ;(VN.MLENGTH UDNUM(NTH(V,W))=NTH(W,M))

5. (rw i12 (open inv))
   (label i15)
   ;(VM.MLENGTH V=LENGTH V=LENGTH UCPERM(V)

6. (assume |m=length(v)|)
   (label i16)

7. (derive |nth(v,m)=fstposition(u,m)| (i15 i16))
Part 2. inv implies perm:

(proof inv_onto)
1. (assume lperm u)
   (label io1)
2. (assume |inv(v,u)|)
   (label io2)
3. (assume |length v=length u|)
   (label io3)
4. (rw io1 (open perm into onto))
   ;(vn.n<LENGTH U)∧(NTH(U,V)∧NTH(U,N)∧MEMBER(N,U))
   (label io4)
5. (rw io2 (open inv))
   ;(vn.n<LENGTH U)∧(NTH(V,N)∧FSTPOSITION(U,N)
   (label io5)
6. (derive |vn.n<length u|\(\text{fstposition}(u,\text{nth}(u,n))=n|)
   (fstposition nth perm_injectivity uniqueness_injectivity io1 io4)
   ;deps: (io1)
   (label io6)
7. (assume |n<length v|)
   (label io7)
8. (rw * (use io3 mode: exact))
   ;n<LENGTH U
   (label io8)
9. (derive |natnum(nth(u,n))∧NTH(u,n)<length v| (io3 io4 io8))
   (label io9)
   ;deps: (io1 io3 io7)
We can use the fact that \( v \) is the inverse of \( u \).

10. \( \text{true \{nth(v,nth(u,n))=fstposition(u,nth(u,n))\}} \) \( \{\text{io5 \*}\} \)
   \( \text{;NTH(V,NTH(U,N))=FSTPOSITION(U,NTH(U,N))} \)
   \( \{\text{label io10}\} \)
   \( \text{;deps: (101 102 103 107)} \)

...the lemma \textit{Fstposition Nth}...

11. \( \text{true \{use io6 io8 mode: exact\}} \)
   \( \text{;NTH(V,NTH(U,N))=N} \)
   \( \{\text{label ioll}\} \)
   \( \text{;deps: (101 102 103 107)} \)

...the lemma \textit{Nthmember}...

12. \( \text{true \{member(nth(v,nth(u,n)),v)\}} \) \( \{\text{nthmember io9}\} \)
   \( \text{;MEMBER(NTH(V,NTH(U,N)),V)} \)
   \( \{\text{deps: (101 103 107)} \}

13. \( \text{true \{use ioll mode: exact\}} \)
   \( \text{;MEMBER(N,V)} \)
   \( \{\text{deps: (101 102 103 107)} \}

...and obtain the second condition for \textit{ontoness}.

14. \( \text{ci iol7} \)
   \( \text{;N<LENGTH \ V \ MEMBER(N,V)} \)
   \( \{\text{deps: (101 102 103)} \}

15. \( \text{derivative \ into \ v \{\text{inv_into iol io2 io3}\}} \)
   \( \{\text{deps: (101 102 103)} \}

16. \( \text{true \{lperm v\}} \) \( \{\text{open perm onto \ -2 * } \)
   \( \text{;PERM(V)} \)
   \( \{\text{deps: (101 102 103)} \}

17. \( \text{ci (iol io2 io3)} \)
   \( \text{;PERM(U)AINV(V)ALENGTH V=LENGTH UCURRENT} \)
   \( \{\text{label inv_perm}\} \)

8.27.5. Using Predicates: the Right Inverse Theorem.

;the theorem right inverse
(proof inverse-right)

1. \( \text{assume \ lperm w} \)
   \( \{\text{label invrl}\}

2. \( \text{assume \ inv(u,w)} \)
   \( \{\text{label invr2}\}

3. \( \text{assume \ length u=length w} \)
   \( \{\text{label invr3}\}

4. \( \text{assume \ comp(v,w,u)} \)
   \( \{\text{label invr4}\}

5. \( \text{true \{open perm onto \}} \)
   \( \{\text{V \ N \ < \ LENGTH \ U \ MEMBER(N,W)} \}

;\forall \text{N \ < \ LENGTH \ \ U \ MEMBER(N,W)} \}
8.27.6. Using Predicates: the Left Inverse Theorem.

(proof compose-inverse-left)

1. (assume |perm(w)|)
   (label invl_1)
2. (assume |inv(u,w)|)
   (label invl_2)
3. (assume |comp(v,u,w)|)
   (label invl_3)
4. (assume |length(w)=length(u)|)
   (label invl_4)
5. (rw invl_2 (open inv))
   ;VN.N<LENGTH U=UINV(U,W)=FSTPOSITION(W,U)
   (label invl_5)
6. (rw invl_1 (open perm onto into))
   ;(VN.N<LENGTH W NATNUM(NTH(W,N)) A
   ; VN.N<LENGTH W MEMBER(N,W))
   (label invl_6)
   ;deps: (INVL_1)

7. (rw invl_3 (open comp))
   ;LENGTH V=LENGTH W \ VN.N<LENGTH W\NTH(V,N)=NTH(U,NTH(W,N)))
   (label invl_7)

8. (derive [Vn.N<LENGTH w\fstposition(w,nth(w,n))=n]
   (fstposition-nth perm_injectivity uniqueness-injectivity
   invl_1 invl_6))
   (label invl_8)
   ;deps: (INVL_1)

9. (rw invl_6 (use invl_4 mode: exact))
   ; VN.N<LENGTH U\NATNUM(NTH(W,N)) A
   ; VN.N<LENGTH U MEMBER(N,W))
   (label invl_9)
   ;deps: (INVL_1 INVNL_4)

10. (assume [n<length v])
    (label invl_10)

11. (rw * (use invl_7 mode: always))
    ; N<LENGTH W
    (label invl_11)
    ;deps: (INVL_3 INVNL_10)

12. (rw * invl_4)
    ; N<LENGTH U
    (label invl_12)
    ;deps: (INVL_3 INVNL_4 INVNL_10)

13. (derive [natnum(nth(w,n)) A nth(w,n)<length u](invl_9 *))
    (label invl_13)
    ;deps: (INVL_1 INVNL_3 INVNL_4 INVNL_10)

14. (derive [NTH(V,N)=NTH(U,NTH(W,N)))](invl_7 invl_10))
    (label invl_14)
    ;deps: (INVL_3 INVNL_10)

15. (rw invl_14 (use invl_5 use: ((n.|nth(w,n)|)) invl_13 mode: exact))
    ; NTH(V,N)=FSTPOSITION(W,NTH(W,N))
    (label invl_15)
    ;deps: (INVL_1 INVNL_2 INVNL_3 INVNL_4 INVNL_10)

; want to apply the lemma fstposition-nth

16. (rw invl_15 (use invl_8 invl_11 mode: always))
    ; NTH(V,N)=W
    ;deps: (INVL_1 INVNL_2 INVNL_3 INVNL_4 INVNL_10)

; and so V is the identity function

17. (ci invl_10)
    ; N<LENGTH V\NTH(V,N)=N
    ;deps: (INVL_1 INVNL_2 INVNL_3 INVNL_4)

18. (trw lid v] (open id) *)
    ; ID(V)
    ;deps: (INVL_1 INVNL_2 INVNL_3 INVNL_4)

19. (ci (invl_1 invl_2 invl_3 invl_4))
8.28. file PERMF: Functions Represented by Lists, Using Functions.

:definitions of composition, identity and inverse as functions.
(proof comp_fact)

1. (decl def-appl (type: \texttt{ground@ground-ground}))
2. (define def-appl \texttt{(\forall v u)\texttt{def-appl}(v,u)=\forall x.(\texttt{x.natnum}(x)\land x<\texttt{length}(v),u)})
   (label def_appl_fact)

;composition of functions:

3. (decl (compose) (infixname: \texttt{\textunderscore}) (type: \texttt{ground@ground-ground})
   (syntype: \texttt{constant})(bindingpower: 930))
4. (define compose \texttt{(\forall v x.}(u\texttt{ nil})=\texttt{nil} A
   \texttt{(u\texttt{x.v})=(nth}(u,x)).(u\texttt{v})]\texttt{listinductiondef})
   (label composedef)

;the identity function:

5. (decl (ident1) (type: \texttt{ground@ground-ground}))
6. (defax identl \texttt{(\forall x u n)ident1}(i,0)=\texttt{nil} A
   \texttt{ident1}(i,n')=ident1(i',n))
   (label identdef)

7. (decl (ident) (type: \texttt{ground-ground}))
8. (define ident \texttt{(\forall n)ident}(n)=ident1(O,n))
   (label identdef)

;the inverse of a function:

9. (decl (invers1) (type: \texttt{ground@ground-ground-ground}))
10. (defax invers1 \texttt{(\forall u i n)invers1}(u,i,0)=\texttt{nil} A
    \texttt{invers1}(nil,i,n)=\texttt{nil} A
    \texttt{invers1}(u,i,n')=if \texttt{null}(fstposition}(u,i))
      \texttt{nil}
    \texttt{else} \texttt{fstposition}(u,i).\texttt{invers1}(u,i',n))
    (label inversedef)

11. (decl (inverse) (type: \texttt{ground-ground}))
12. (define inverse \texttt{(\forall u)inverse}(u)=invers1(u,0,\texttt{length}(u)))
    (label inversedef)

8.29. Condition for Definiteness and Sorts of the Functions.

(proof def_appl_condition)

1. (assume \texttt{lint0 u})
2. (assume \texttt{llength u<length v})
3. (rw -2 (open into))
   \texttt{\forall n<length \texttt{u}} \texttt{natnum}(\texttt{nath}(u,n)\land \texttt{nth}(u,n)<\texttt{length} \texttt{u})
4. (trw \texttt{\forall n<length u} \texttt{natnum nth}(u,n)\land \texttt{nth}(u,n)<\texttt{length} \texttt{v} \ast}
(less_lesseq_fact1 -2)
;VN.W<LENGTH U:NATNUM(\nth(U,N)):ANTH(U,N)<LENGTH V
(\ue ((\phi.1.|x|natnum x:\length V|)(u.))(nth_allp * )
;ALLP (AX.NATNUM(X)AX<LENGTH V,U)
6. (\tw |def_app(v,u)| (open def_app) * )
;DEF_APPL(V,U)
7. (ci (-6 -5))
;INTO(U)LENGTH US_LENGTH V:DEF_APPL(V,U)
(label def_app_condition) ■
;check sorts
;compose:
8. (\ue (\phi |u|def_app(v,u)|listp v\cdot u|) listinduction
(part 1 (open def-appl allp compose )))
;\top. DEF_APPL(V,U) LISTP V\cdot U
(label sortcomp) (label simpinfo) ■
;ident:
9. (\ue (a |\lambda n.m.|listp ident1(m,n)|) proof-by-induction
(open ident1))
;\top.M.LISTP IDENT1(M,N)
(label ident_sort1) (label simpinfo) ■
10. (\tw |\forall n.|listp ident(n)| (open ident) * )
;\forall.LISTP IDENT(I)
(label ident_sort) (label simpinfo) ■
;inverse
11. (\ue (a |\lambda w.i.|listp inversi(u,i,n)|)
proof-by-induction
(open inversi) posfacts)
;\forall.LISTP INVERSI(U,I,N)
(label inverser_sort1) (label simpinfo) ■
12. (\tw |\forall n.|listp inverse(u)| (open inverse) * )
;\forall.LISTP INVERSE(U)
(label inverse-sort) (label simpinfo) ■

8.30. Length Compose.

;length compose
(proof length-compose)
(assume |def_appl(w,u)|)
(label l_c-1)
2. (\tw (open def_appl))
(label l-c-2)
;ALLP (AX.NATNUM(X)AX<LENGTH W,U)
3. (assume \n<length(u))
(label l-c-3)
4. (\ue ((u.u)(x.|nth(u,n)|)(\phi.1.|x|natnum(x)Ax<length(w)|)))
allp_elimination
nthmember sexp-nth l-c-3 l-c-2
;NATNUM(NTH(U,N))\& NTH(U,N)<LENGTH W
(label l-c-4)

5. (trw |sexp(nth(w,nth(u,n)))| sexp-nth l-c-4)
;SEXPNTH(W,NTH(U,N))
(label l_c_sort1)

6: (ci l-c-3)
;N<LENGTH U\& SEXP W,NTH(U,N))
(label l-c_7)

7. (derive |allp(λx.natnum(x)\& x<LENGTH W,nthcdr(u,n'))|
(allp_nthcdr l-c-2))
;ALLP(λX.NATNUM(X)\& X<LENGTH W,NTHCDR(U,N'))

8. (derive 1listp(w*nthcdr(u,n'))| (* sortcomp))
(label l_c_sort2)

9. (ci l-c-3)
;N<LENGTH U\& LISTP W\& NTHCDR(U,N'))
(label l-c_9),

10. (ue ((phi.l~u.length(aeu>=length(u)l)(u.u))
nthcdr_induction
(part 1 (open compose length )) l-c-7 l-c-8)
;LENGTH W.U)=LENGTH U

11. (ci l-c-1)
;DEF_APPL(W,U)\& LENGTH (W.U)=LENGTH U
(label length-compose)

8.30.1. Length Ident.

1. (ue (a |An.λm.length identi(m,n)=n))
   proof-by-induction
   (open ident))
;∀N M.LENGTH (IDENTI(M,N))=N
(label length_ident1) (label simpinfo)

2. (trw |∀N.LENGTH (IDENT(N))=N| * (open ident))
   (label: length_ident) (label simpinfo)

8.30.2. Length Inverse.

(proof lengthinverse)

1. (assume lperm(u))
   (label l11)

2. (trw lil (open perm onto into>>)
;∀W.N<LENGTH U\& NATNUM(NTH(U,N))\& NTH(U,N)<LENGTH U)
;∀W.N<LENGTH U\& MEMBER(N,U))
   (label l12)

3. (ue ((u.|u|)(y.|n|)) posfacts)
; (NULL FSTPOSITION(U,N))\& MEMBER(N,U))}


8.30.3. Compose.

(proof nth-compose)

1. (ue (phi | u. null (u)def_appl(v, u)n nth(v u, 0) = nth(v, nth(u, 0)) |)
  listinduction
  (part 1 (open compose nth def-appl allp))
  ; v u. NULL U DEF-APPL(v, u) CAR(v u) = nth(v, CAR U)
  (label a_c_base1)

2. (ue (phi3 | u.n def_appl(v, u)n nth(u)u nth(v u, 0) = nth(v, nth(u, 0)) |)
  doubleinductioni
  (part 1 (open compose def-appl allp) a_c_base1)
  ; v u. DEF-APPL(v, U) N nth(U)u nth(v u, 0) = nth(v, nth(U, U))
  (label nth-compose)

8.30.4. Compose Permutation.

Theorem 1 (i) ( Yerm Compose)

V U VPERM(U)APERM(V)ALength U = LENGTH VQPERM(U O V)
(proof per-m-compose)

1. (assume (perm u))
   (label pc1)

2. (assume (perm v))
   (label pc2)

3. (assume (length u = length v))
   (label pc3)

4. (rw pc2 (open perm onto))
   (label pc4)
   ; INTO(V) = (\forall N. N < length V \rightarrow \exists M. M \in V)
   ; deps: (PC2)

5. (ue (((u v) (v u)) def_appl_condition (open lesseq) pc3 pc4)
   ; DEF,APPL(U, V)
   (label pc5)
   ; deps: (PC2 PC3)

6. (ue (((u v) (v u)) length-compose pc5)
   ; LENGTH (U*V) = LENGTH V
   (label pc6)
   ; deps: (PC2 PC3)

7. (assume (n < length (u v))))
   (label pc7)

8. (rw * (use pc6 mode: exact))
   ; N < LENGTH V
   (label pc8)
   ; deps: (PC2 PC3 PC7)

9. (rw pc2 (open perm into>)
   ; (\forall N. N < length U \rightarrow \exists M. M \in U)
   ; ; (\forall N. N < length U \rightarrow \exists M. M \in V)
   (label pc9)
   ; deps: (PC2)

10. (derive (natnum (nth (v, n)) \& nth (v, n) < length u) pc8 *)
    (use pc3 mode: exact)
    (label pc10)
    ; deps: (PC2 PC3 PC7)

11. (rw pc1 (open perm into>)
    ; (\forall N. N < length U \rightarrow \exists M. M \in U)
    ; (\forall N. N < length U \rightarrow \exists M. M \in V)
    (label pc11)
    ; deps: (PC1)

12. (ue (n | nth (v, n)) * pc10)
    ; NATNUM (NTH (U, NTH (V, N))) \& NTH (U, NTH (V, N)) < LENGTH U \& MEMBER (NTH (V, N), U)
    (label pc12)
    ; deps: (PC1 PC2 PC3 PC7)

13. (derive (nth (u v, n) = nth (u, nth (v, n))) (nth-compose pc5 pc8))
    (label pc13)
    ; deps: (PC2 PC3 PC7)

14. (true 1natnum nth (u v, n) \& nth (u v, n) < length (u v)) pc12
    (use pc13 pc6 mode: exact)
    (use pc3 mode: exact direction: reverse)
    ; NATNUM (NTH (U V, N)) \& NTH (U V, N) < LENGTH (U V)
    ; deps: (PC1 PC2 PC3 PC7)
15. (ci pc7)
  ; N<LENGTH (U@V)<NATNUM(NTH(U@V,N))<NTH(U@V,N)<LENGTH (U@V)
  ; deps: (PC1 PC2 PC3)

16. (trw into(u@v) |* (open into) pc5)
  ; INTO(u@v)
  ; label pc-into
  ; deps: (PC1 PC2 PC3)

: part 2

17. (rw pc8 (use pc3 mode: exact direction: reverse)>
  ; N<LENGTH U
  ; label pc20
  ; deps: (PC2 PC3 PC7)

  ; labels: MEMBER-NTH
  ; VU MEMBER(Y,U)<>(3N N<LENGTH U<LENGTH U>V)=Y

18. (define jv | jv<length u =nth(u,jv)=n|(* pc11 member_nth))
  ; label pc21
  ; JV is unknown.
  ; the symbol JV is given the same declaration as J
  ; deps: (PC1 PC2 PC3 PC7)

19. (derive | jv<length v |* (use pc3 mode: exact direction: reverse)>
  ; deps: (PC1 PC2 PC3 PC7)

20. (define kv | kv<length v =nth(v,kv)=jv|(* pc9 member_nth))
  ; label pc22
  ; KV is unknown.
  ; the symbol KV is given the same declaration as K
  ; deps: (PC1 PC2 PC3 PC7)

  ; labels: NTH_COMPOSE
  ; VV U N<LENGTH U>DEF_APPL(V,U)<V<LENGTH U>V=VTH(U,V)<VTH(U,V)<V TH(U,V)

21. (ue ((v,u)(u,v)(n.kv)) nth-compose pc5
  ; (use ' mode: always)(use pc21 mode: always)
  ; label pc23
  ; NTH(U@V,KV)<N
  ; deps: (PC1 PC2 PC3 PC7)

22. (derive | kv<length(u@v)|(pc22 pc6))
  ; ;deps: (PC1 PC2 PC3 PC7)

  ; labels: NTHMEMBER
  ; VU N<LENGTH U<LENGTH U<LENGTH U<LENGTH U)

23. (trw member(nth(u@v,kv),u@v)|(nthmember pc5 |*))
  ; MEMBER(NTH(U@V,KV),U@V)
  ; deps: (PC1 PC2 PC3 PC7)

24. (rw pc23)
  ; MEMBER(U@V)
  ; deps: (PC1 PC2 PC3 PC7)

25. (ci pc7)
  ; N<LENGTH (U@V)<MEMBER(N,U@V)
  ; ;deps: (PC1 PC2 PC3)

  ; label pc-onto)

26. (trw perm(u@v)|(pc5 pc-into pc-onto) (open perm onto))
  ; PERM(U@V)
  ; ;deps: (PC1 PC2 PC3)
27. \((\text{ci } (\text{pc1 } \text{pc2 } \text{pc3}))\)

; PERM(U) \\& PERM(V) | LENGTH U = LENGTH V \\& PERM(U) \\& V

(label perm-compose)

; Theorem 1 (ii) (associativity of composition)
(proof assoc-compose)

1. \((\text{tw } | \text{def_app1}(w,v) \& \text{def_app1}(v,u) \& (w \& v) = w \& (v \& nil)\))

(open compose) sortcomp

(label ass_comp_base)

2. \((\text{ue } (\phi | \text{def_app1}(w,v) \& \text{def_app1}(v,u) \& (w \& v) = w \& (v \& u)))\)

list induction

(part 1\#2 (open compose \text{def_app1 allp})) sortcomp ass_comp_base

(use nth-compose \text{ue: } ((v.w)(u.v)))

; VU.DEF_APPL(W,V) \& DEF_APPL(V,U) \& (W \& V) = U \& (V \& U)

(label assoc_comp)

3. \((\text{assume } | \text{perm}(v) \& \text{perm}(u) \& \text{length}(v) = \text{length}(u) \& \text{length}(w) = \text{length}(v))\)

4. \((\text{rw } * (\text{open perm onto}))\)

; INTO(V) \& (\text{VN. LENGTH U MEMBER(W,V)} \&)

; INTO(U) \& (\text{VN. LENGTH U MEMBER(W,V)} \&)

; LENGTH V = LENGTH U LENGTH W = LENGTH U

5. \((\text{ue } (u.v)(v.w)) \& \text{def_app1_condition} \* (\text{open lesseq}))\)

; DEF_APPL(W,V)

6. \((\text{ue } (u.u)(v.v)) \& \text{def_app1_condition} -2 (\text{open lesseq}))

; DEF_APPL(V,U)

7. \((\text{derive } (w \& v) = w \& (v \& u)) \text{ (assoc_comp } * -2))\)

8. \((\text{ci } -5)\)

; PERM(V) \& PERM(U) \& LENGTH V = LENGTH U \& LENGTH W = LENGTH U \& (W \& V) = U \& (V \& U)

(label associativity-of-composition)

8.30.5. Identity.

(proof id-main)

; id main

1. \((\text{assume } | n < m \& \text{nthcdr(ident(m),n) = ident1(n,m-n))} \&

(label id_main1)

2. \((\text{assume } | n' < m))\)

; (label id_main2)

3. \((\text{derive } | \text{nthcdr(ident(m),n) = ident1(n,m-n))} \&

(id_main1 id-main2 succ-less-less))

; deps: (ID-MAIN1 ID-MAIN2)

4. \((\text{rw } * (\text{use minusfact10 mode: exact}) (\text{open ident1}))

(use id-main2 succ-less-less mode: exact))

; NTHCDR(IDENT(M),N) = N. IDENT1(N',M-N')

; deps: (ID-MAIN1 ID-MAIN2)

5. \((\text{tw } | \text{nthcdr(ident m,n))}\)

(use cdr_nthcdr mode: exact direction: reverse)

(use * mode: exact))

; NTHCDR(IDENT(M),N') = IDENT1(N',M-N')
6. (ci id_main2)
   \( N' < M \) \( \text{NTHCDR} (\text{IDENT} (M), N') = \text{IDENT} (N', M - N') \) 

7. (ci id_main1)
   \( N < M \) \( \text{NTHCDR} (\text{IDENT} (M), N) = \text{IDENT} (N, M - N) \)
   \( N' < M \) \( \text{NTHCDR} (\text{IDENT} (M), N') = \text{IDENT} (N', M - N') \) 

8. (ue (a | \( n < n' \) \( \text{NTHCDR} (\text{IDENT} (m), n) = \text{IDENT} (n, m - n) \))
   proof by induction
   (part \#1 (open minus ident)) \(*\)
   \( \forall N. N < M \) \( \text{NTHCDR} (\text{IDENT} (M), N) = \text{IDENT} (N, M - N) \)
   (label nthcdr_ident) 

9. (rw * (use minusfact10 mode: exact))
   \( \forall N. N < M \) \( \text{NTHCDR} (\text{IDENT} (M), N) = \text{IDENT} (N, (M - N')') \)

10. (ue ((u | \text{ident } m)) \( n, n' \)) \( \text{car_nthcdr} \) (use * mode: always))
   \( N < M \) \( \text{NTH} (\text{IDENT} (M), N) \)

11. (trw | \( \forall n. n < M \) \( \text{nth} (\text{ident } m, n) = n \) | * )
    (label id_main)
    (proof perm_ident)
    ;only ontoeness requires some help

1. (assume \( n < \text{length} \text{ident} (m) \))
   (label prm_id1) 

2. (rw * (open ident))
   \( N < M \)
   (label prm_id2) 

3. (derive \( \text{nth} (\text{ident} (m), n) = n \) \( \ast\ id_main))

4. (derive \( \text{member} (\text{nth} (\text{ident} m, n), \text{ident} m) \)
   \( \text{nthmember} \text{prm_id1} \))

5. (rw * (use -2 mode: exact))
   \( \text{MEMBER} (N, \text{IDENT} (M)) \)

6. (ci prm_id1)
   \( N < M \) \( \text{MEMBER} (N, \text{IDENT} (M)) \)

7. (trw | \( \forall n. \text{perm} (\text{ident } n) \) \( \text{open perm into onto} \)
   \( \text{use id_main mode: always} \) \( \ast\)
   \( \forall N. \text{PEAM} (\text{IDENT} (N)) \)
   (label perm_ident) 

. . .

8.30.6. Right Identity.

(proof identity_right)

1. (rw perm_id (open perm onto))
   \( \forall n. \text{INTO} (\text{IDENT} (N)) (\forall n. n < N \text{\text{MEMBER} (N, \text{IDENT} (N)))} \)
   ;labels: \text{DEF_APPL_CONDITION}
   ;\( V \text{U INTO} (U) \text{ALength USLENGTH V>DEF_APPL (V, U)} \)

2. (ue ((u | \text{ident(length u)}) (v, u)))
   \text{def_appl_condition} \( \ast\ (\text{open lesseq}) \)
3. \((\text{def-appl}(u, \text{ident}(\text{length } u))(v, u)(n, u)) \text{nth-compose }\star \)  
   (\text{use id-main mode: exact})  
   \(\forall \mathbf{v} \mathbf{u} \mathbf{n}. \text{def-appl}(v, u) \land \mathbf{n} < \text{length } u \land \text{nth}(v \cdot u, \mathbf{n}) = \text{nth}(v, \text{nth}(u, \mathbf{n}))\)

4. \((\text{def-appl}(u, \text{ident}(\text{length } u))(v, u)) \text{extensionality (open appl)} \)  
   (\text{use length-compose -2 } \star \)  
   (\text{label identity_right})

8.30.7. Left Identity.

(proof identity_left)

1. (\text{assume } \text{into } u) \)  
   (\text{label il-1})

2. (\text{ue } (u, u)(v, \text{ident}(\text{length } u))) \)  
   (\text{def-appl_condition})  
   (\text{open lesseq})  
   (\text{label il-2})

3. (\text{ue } (u, u)(v, \text{ident}(\text{length } u))) \text{nth-compose il-2 } \star \)  
   (\text{use id-main ue: } (n, \text{nth}(u, n))(m, \text{length } u)))  
   (\text{label il-2})

4. (\text{ue } (u, u)(v, \text{ident}(\text{length } u))) \text{nth-compose il-2 } \star \)  
   (\text{use id-main ue: } (n, \text{nth}(u, n))(m, \text{length } u)))  
   (\text{label il-2})

5. (\text{ue } (u, u)(v, v)) \text{extensionality} \)  
   (\text{open appl})

6. (\text{ci il-1}) \)  
   (\text{label identity_left})

8.30.8. Inverse.

(proof inverse_main)

1. (\text{assume } \text{perm } u) \)  
   (\text{label inv_main1})

   (\text{check that fstposition has the proper value on the intended domain})

2. (\text{previous steps})  
   (\text{label inv_main2})
3. (ue ((u, u)(y, n)) posfacts)
   ;(NULL FSTPOSITION(U,N)) = MEMBER(N, U)
   ;(MEMBER(N, U) = MAXIMUM(FSTPOSITION(U, N)))

4. (derive [n<length u] null fstposition(u, n) | (inv_main2 *))
   (label inv_main3)
   ;prove by induction a sublemma:

5. (assume [n<length u]
     nthcdr(inverse(u), n) = inversl(u, n, length u - n))
   (label inv_main5)

6. (assume [n'<length u])
   (label inv_main6)
   (derive [n<length u] (* succ_less_less))
   (label inv_main7)

8. (derive [null fstposition(u, n)] (inv_main3 inv_main7))
   (label inv_main9)

9. (rw inv_main5
    (use inv_main7 inv_main9)(open invers1)
    (use minusfact10 mode: always))
   (label inv_main10)
   ;NTHCDR(INVERSE(U), N') = FSTPOSITION(U, N). INVERSl(U, N', LENGTH U-N')
   ;deps: (INV_MAIN1 INV_MAIN5 INV_MAIN6)
   ;labels: CDR_NTHCDR
   ;U N.CDR NTHCDR(U, N') = NTHCDR(U, N')

10. (ue ((u, inverse(u))(n, n)) cdr_nthcdr (use * mode: exact))
    ;INVERSl(U, N', LENGTH U-N') = NTHCDR(INVERSE(U), N')
    ;deps: (INV_MAIN1 INV_MAIN5 INV_MAIN6)

11. (ci inv_main6)
    ;N'<LENGTH U=INVERSl(U, N', LENGTH U-N') = NTHCDR(INVERSE(U), N')

12. (ci inv_main5)

13. (ue (a [n<length u] nthcdr(inverse(u), n) = inversl(u, n, length u - n)])
    proof_by_induction (part 1#1 (open inverse minus) *)
    ;VN.<LENGTH U=NTHCDR(INVERSE(U), N)=INVERSl(U, N, LENGTH U-N)
    ;deps: (INV_MAIN1)
    ;from this the main lemma follows:

14. (rw * (use minusfact10 mode: exact) (open invers1)
    (use inv_main3 mode: always))
    ;VN.<LENGTH U
    ;NTHCDR(INVERSE(U), N)=FSTPOSITION(U, N). INVERSl(U, N', LENGTH U-N')
    ;deps: (INV_MAIN1)
    ;labels: CAR_NTHCDR
    ;U N.<LENGTH U=CAR NTHCDR(U, N)=NTH(U, N)

15. (ue ((u, inverse(u))(n, n)) car_nthcdr
    (use * lengthinverse inv_main1 mode: always))
    ;N.<LENGTH U=FSTPOSITION(U, N)=NTH(INVERSE(U), N)
    ;deps: (INV_MAIN1)

16. (ci inv_main1)
    ;PERM(U)(((N<LENGTH U)=FSTPOSITION(U, N)=NTH(INVERSE(U), N))

17. (derive [Vu n.perm u[n<length u]nth(inverse u, n) = fstposition(u, n)] *)
8.30.9. Inverse Permutation.

- (proof inverse_perm)

1. (assume |perm(u)|)
   (label inv_p1)

2. (rw * (open perm onto))
   ;INTO(\(U\)) \(\forall N. N <\text{LENGTH } U \supset \text{MEMBER}(N, U)\)
   (label inv_p2)

3. (use ((u.u)(y.n)) posfacts)
   ;(NULL \(\text{FSTPOSITION}(U, N)\) \(\supset \text{MEMBER}(N, U)\)) \(\supset \text{MEMBER}(N, U)\) \(\supset \text{NATNUM}(\text{FSTPOSITION}(U, N))\)

4. (derive \(\forall N. N <\text{LENGTH } U \supset \text{NATNUM}(\text{FSTPOSITION}(u, n) \supset \text{FSTPOSITION}(u, n) <\text{LENGTH } u)\))
   (label inv_p3)

5. (derive \(\forall N. N <\text{LENGTH } u \supset \text{NTH}(\text{INVERSE}(u, n)) = \text{FSTPOSITION}(u, n)\))
   (inv_p4)

6. (rw inv_p3 (use * mode: always direction: reverse))
   ;\(\forall N. N <\text{LENGTH } U \supset \text{NTH}(\text{INVERSE}(u, n)) \supset \text{NTH}(\text{INVERSE}(u), N) <\text{LENGTH } U\)

7. (trw into inverse(u))
   ;INTO(\(\text{INVERSE}(u)\))
   (label into_inverse)

8. (ci inv_p1)
   ;PERM(U) INTO(\(\text{INVERSE}(U)\))
   (label into_inverse)

9. (rw inv_p1 (open perm into onto))
   ;\(\forall N. N <\text{LENGTH } U \supset \text{NATNUM}(\text{NTH}(U, N)) \supset \text{NTH}(N, U) <\text{LENGTH } U)\)
   \(\supset \text{MEMBER}(N, U)\))
   (label inv_p10)

10. (derive \(\text{LENGTH } \text{INVERSE}(u) = \text{LENGTH } u\))
    (label inv_p11)

11. (assume |n <\text{LENGTH } \text{INVERSE}(u)|)
    (label inv_p12)

12. (rw * (use inv_p11 mode: exact))
    ;\(N <\text{LENGTH } U\)
    (label inv_p13)

    ;apply the main property of the inverse function...

13. (ue (\(n \mid \text{NTH}(u, n)\)) inv_p4 (use inv_p10 * mode: always))
    ;\(\text{NTH}(\text{INVERSE}(u), \text{NTH}(U, N)) = \text{FSTPOSITION}(U, \text{NTH}(U, N))\)
    (label inv_p14)

    ...the consequence of the Pigeon Hole principle...
14. (derive |inj u| (inv_p1 perm_injectivity))
    ;...the basic fact fstposition nth ...
15. (derive |fstposition(u,nth(u,n))=n|
    (fstposition nth uniqueness_injectivity * inv_p10 inv_p13))
16. (rw inv_p14 (use *))
    :NTH(INVERSE(U),NTH(U,N))=N
    (label inv_p15)
    ;...and the lemma nthmember..
17. (derive |natnum nth(u,n)\<length inverse(u)|
    (inv_p10 inv_p11 inv_p13))
18. (trw |member(nth(inverse u,nth(u,n)),inverse u)|
    (nthmember *))
    :MEMBER(NTH(INVERSE(U),NTH(U,N)),INVERSE(U))
    ;...to conclude:
19. (rw = (use inv_p15))
    :MEMBER(N,INVERSE(U))
    :deps: (INV_P1 INV_P12)
20. (ci inv_p12)
    :N<LENGTH (INVERSE(U))\>MEMBER(N,INVERSE(U))
    (label onto_inverse)
21. (trw |perm(inverse u) \open perm onto)
    into_inverse onto_inverse)
    :PERM(INVERSE(U))
22. (ci inv_p1)
    :PERM(U)\>PERM(INVERSE(U))
    (label perm_inverse)  

8.30.10. Right Inverse.

Theorem 3. (ii) (Right Inverse)

\[ \forall U.\, \text{PERM}(U) \Rightarrow \text{INVERSE}(U) = \text{IDENT}(\text{LENGTH}(U)) \]

Proof. We aim at an application of extensionality (line 12). From line 8 on, we follow the proof given in Section 6.6.2, since all the facts assumed there as definitions have been proved here as properties of our functions.

The additional fact to be proved here is that u is defined as an application on inverse(u) as domain. This follows from the fact that inverse(u) is into (line 5) and has the same length as u (line 3).
(proof compose_inverse_right)

1. (assume |perm u|(label cir1))

2. (rw cir1 (open perm onto))
   ; INTO(U) \(\forall N \lt \text{LENGTH } U \ni \text{MEMBER}(N, U)\)
   (label cir2)
   ; labels: LENGTH_INVERSE
   ; PERM(U) \(\lt \text{LENGTH } (\text{INVERSE}(U)) = \text{LENGTH } U\)

3. (derive |length inverse(u)=length ul| (cir1 lengthinverse))
   (label cir3)
   ; labels: PERM_INVERSE
   ; PERM(U) \(\ni \text{PERM}(\text{INVERSE}(U))\)

4. (derive |perm inverse(u)| (perm_inverse cir1))

5. (rw * (open perm onto))
   ; INTO(\text{INVERSE}(U)) \(\times (\forall N \lt \text{LENGTH } (\text{INVERSE}(U)) \ni \text{MEMBER}(N, \text{INVERSE}(U)))\)
   ; labels: DEF_APPL_CONDITION
   ; \(\forall U \cdot \text{INTO}(U) \land \text{LENGTH } U \lt \text{LENGTH } V \ni \text{DEF_APPL}(V, U)\)

6. (ue ((v.u)(u.inverse ul)))
   def_appl_condition
   (cir3 *) (open lesseq)
   ;DEF_APPL(U, INVERSE(U))
   (label cir4)
   ; labels: LENGTH_COMPOSE
   ; \(\forall W \cdot \text{DEF_APPL}(W, U) \land \text{LENGTH } (W \bullet U) = \text{LENGTH } U\)

7. (trw [length(u*inverse(u))=length ident(length u)]
   (use length-compose ue: ((w.u)(u.inverse ul)) cir4 mode: always)
   (use cir3))
   ;LENGTH(U \bullet \text{INVERSE}(U)) = \text{LENGTH } (\text{IDENT}(\text{LENGTH } U))
   (label cir5)

we can apply \(N\)th Compose...

; labels: NTH_COMPOSE
; \(\forall U \cdot \text{NTH}_0(U, N) \land \text{LENGTH } U \lt \text{NTH}(v \bullet U, N) = \text{NTH}(v, \text{NTH}(U, N))\)

8. (ue ((v.u)(u.inverse ul)))
   nth-compose cir4 cir3
   ; \(\forall N \lt \text{LENGTH } U \ni \text{NTH}(U \bullet \text{INVERSE}(U), N) = \text{NTH}(U, \text{NTH}(\text{INVERSE}(U), N))\)

"...Main Inv..."

; labels: INV_MAIN
; \(\forall U \cdot \text{PERM}(U) \land \text{LENGTH } U \lt \text{NTH}(\text{INVERSE}(U), N) = \text{FSTPOSITION}(U, N)\)

9. (rw * (use inv_main cir1 mode: always))
   ; \(\forall N \lt \text{LENGTH } U \ni \text{NTH}(U \bullet \text{INVERSE}(U), N) = \text{NTH}(U, \text{FSTPOSITION}(U, N))\)

"...Nth Fstposition..."

; labels: NTH_FSTPOSITION
; \(\forall N \cdot \text{MEMBER}(N, U) \land \text{NTH}(U, \text{FSTPOSITION}(U, N)) = N\)

10. (rw * (use nth_fstposition cir2 mode: always))
    ; \(\forall N \lt \text{LENGTH } U \ni \text{NTH}(U \bullet \text{INVERSE}(U), N) = N\)
...to conclude, using *Main Id:

\[ \forall M. N < \text{DEHNTH} (\text{IDENT}(M), N) = N \]

11. \( \text{TRW} \left[ \forall n. \text{LENGTH } u \geq \text{NTH}(u \cdot \text{INVERSE}(u), n) = \text{NTH} (\text{IDENT} (\text{LENGTH } u), n) \right] \)

\( \text{use } * \text{ mode: always} \)
\( \text{use id-main } u : (\text{mode: always}) \)
\( \forall N. N < \text{DEHNTH} (u \cdot \text{INVERSE}(u), N) = \text{NTH} (\text{IDENT} (\text{LENGTH } U), N) \)

(label \( \text{cir6} \))

\( \forall U. \text{LENGTH } U = \text{LENGTH } V \iff (\forall I. \text{LENGTH } U \cdot \text{APPL}(U, I) = \text{APPL}(V, I)) \iff U = V \)

12. \( \text{use } ((u. u \cdot \text{INVERSE}(u))) (v. \text{IDENT}(\text{LENGTH } u)) \)

\( \text{extensionality cir6} \)
\( \text{use cir5 mode: always} \)
\( \text{use sortcomp cir4 mode: always} \)
\( \forall U \cdot \text{INVERSE}(U) = \text{IDENT}(\text{LENGTH } U) \)

13. \( \text{PERM}(U) \iff \forall U \cdot \text{INVERSE}(U) = \text{IDENT}(\text{LENGTH } U) \)

(\( \text{label } \text{inverse_right} \) )

8.30.11. Left Inverse.

**Theorem 3.** \((\text{iii}) \) (Left Inverse)

\( \forall U. \text{PERM}(U) \iff \text{INVERSE } U \cdot U = \text{IDENT}(\text{LENGTH } U) \)

**Proof.** Again we follow closely the pattern of Section 6.6.3.

(proof compose_inverse_left)

1. (assume \( \text{PERM } U \))

(label \( \text{cil1} \))

2. (derive \( \text{LENGTH } \text{INVERSE}(u) = \text{LENGTH } u \cdot (\text{LENGTH } \text{INVERSE } \cdot) \))

(label \( \text{cil2} \))

3. (\( \text{TRW } \text{cil1} \) (open \( \text{PERM } \text{onto} ))

\( \text{INTO}(U) \cdot (\forall N. N < \text{LENGTH } U \cdot \text{MEMBER}(N, U)) \)

(label \( \text{cil3} \))

\( \forall V. \text{INTO}(U) \iff \text{LENGTH } U \cdot \text{LENGTH } V \cdot \text{DEF-APPL}(V, U) \)

4. (\( \text{use } ((v. \text{INVERSE } u) \cdot (u. u)) \) \( \text{DEF-APPL-CONDITION} \)

\( \text{cil2 cil3 (open lesseq)} \)

\( \text{use perm_inverse cil1}) \)

\( \text{DEF-APPL(INVERSE(U), U)} \)

(label \( \text{cil4} \))

5. (\( \text{TRW } \text{cil4 sortcomp} \))

\( \text{LISTP } \text{INVERSE}(U) \cdot U \)

(label \( \text{cil5} \))

6. (derive \( \text{LENGTH } (\text{INVERSE}(u) \cdot u) = \text{LENGTH } \text{IDENT}(\text{LENGTH } u) \))

\( \text{cil4 length-compose}) \)

(label \( \text{cil6} \))

7. (assume \( N < \text{LENGTH } u \)) (label \( \text{cil6} \))
Use the lemma \( N^\text{th} \) Compose...

\[
\text{;labels: NTH_COMPOSE} \\
;\forall V U. N. \text{DEF_APPL}(V, U) \land N < \text{LENGTH } U \implies N \text{TH}(V \bullet U, N) = N \text{TH}(V, N \text{TH}(U, N))
\]

8. \((\text{ue } ((v.]} \text{inverse } u)(u. u)(n. n)) \text{ nth_compose cil4 cil6}

;\text{NTH(INVERSE(U) \bullet U, N) = NTH(INVERSE(U), NTH(U, N))}

(label cil17)

..the main property of inverse...

9. \((\text{rw cil13 open into }))

;\forall V. N. \text{INV_COMPOSE(U) \land N < } \text{LENGTH } U \implies \text{NTH(INVERSE(U), N) = FSTPOSITION(U, N)}

(label cil18)

;labels: INV_MAIN
;\forall V U. N. \text{PERM(U) \land N < } \text{LENGTH } U \implies \text{NTH(INVERSE(U), N) = FSTPOSITION(U, N)}

10. \((\text{ue } ((u. u)(n. nth(u, n))) \text{ inv_main (use cil1 cil6 cil8 mode: always))}

;\text{NTH(INVERSE(U), NTH(U, N)) = FSTPOSITION(U, NTH(U, N))}

(label cil19)

..a. consequence of the Pigeon Hole principle...

11. \((\text{derive inj u} (\text{perm_injectivity cil1}))

(label cil10)

..the lemma \( \text{FSTPOSITION} N^\text{th} \)... \n
;labels: FSTPOSITION_NTH
;\forall V U. N. \text{UNIQUENESS(U) \land N < } \text{LENGTH } U \implies \text{FSTPOSITION(U, NTH(U, N)) = N}

12. \((\text{derive } \text{fstposition(u, nth(u, n)) = n})

(\text{fstposition_nth uniqueness injectivity cil10 cil16}))

13. \((\text{rw cil19 (use *))}

;\text{NTH(INVERSE(U), NTH(U, N)) = N}

..and the main property of \text{ident} to conclude:

;labels: ID_MAIN
;\forall V. N. \text{N < } \text{LENGTH } U \land \text{NTH} \text{(IDENT(U), N) = N}

14. \((\text{trw nth(inverse(u) \bullet u, n) = nth(ident(length u), n))}

(\text{use cil16 cil17 * mode: always})

(\text{use id_main ue: (m. [length u](n. n)) cil6 mode: always}))

;\text{NTH(INVERSE(U) \bullet U, N) = NTH(IDENT(LENGTH U), N)}

15. \((\text{ci cil16})

;\text{N < LENGTH U \implies NTH(INVERSE(U) \bullet U, N) = NTH(IDENT(LENGTH U), N)}

Therefore:

;labels: EXTENSIONALITY
;\forall V. \text{LENGTH } U = \text{LENGTH } V \land \forall I. \text{LENGTH } U \land \text{APPL(U, I) = APPL(V, I)} \implies \text{U = V}

16. \((\text{ue } ((u. [inverse(u) \bullet u](v. [ident(length u)]))}

\text{extensionality}

\text{cil5 * (open appl))}

;\text{INVERSE(U) \bullet U = IDENT(LENGTH U)}

;\text{deps: (cil1)}

17. \((\text{ci cil1})

;\text{PERM(U) \bullet INVERSE(U) \bullet U = IDENT(LENGTH U)}

(label inverse left)

R.S. Boyer and J.S. Moore [1979],
C. Goad [1979],
*Independence of the Pigeon Hole Principle*, manuscript, Stanford.
Jussi Ketonen and Joseph S. Weening [1983]
The Language of an Interactive Proof Checker, Stanford Report STAN-CS-83-992
Jussi Ketonen and Joseph S. Weening [1984]
G. Kreisel [1981],
D. Prawitz [1965],
D. Prawitz [1968],
D. Prawitz [1971],
A.S. Troelstra [1973],
9.1. Index of Examples.

Example 1: Use of the rewriter NORMAL. Section 2.1.
Proof: transitivity of $\leq$.
\[ \forall N \forall M \forall K. N \leq M \leq K \]

Example 2: Default declarations and previous declarations, Section 2.4.
Declaration of the symbol xv.

Example 3: Rewriting using only simpinfo. Section 2.6.
Proof: Sexp Nth.
\[ \forall U N. \text{SEXP NTH}(U, N) \]

Example 4: How the rewriting process reflects an informal argument. Section 2.9.
Proof: Firstposition Nth
\[ \forall U N. \text{UNIQUENESS}(U) \land N < \text{LENGTH} \cup \text{FSTPOSITION}(U, \text{NTH}(U, N)) = N \]

Example 5: Abbreviation of proofs by rewriting. How the rewriter Trans Cond is determined in a 'trial and error' interaction. Section 7.
Proof: Lemma 2.10 Mult Nthcdr,
\[ \forall A U N. N < \text{LENGTH} \cup \text{MULT}(\text{NTHCDR}(U, N), A) \leq \text{MULT}(U, A) \]

Proof: Pigeonfact
\[ \forall F. (\forall N. \text{NATNUM}(F(N))) \land (\forall N. (\forall M. M < N \leq F(M)) \land \text{SUM}(\forall K. F(K), N) = N) \land (\forall M. M < N \leq F(M)) \]

Example 7: Predicate somep. Efficiency of rewriting. Definition by recursion and explicit definitions. Section 5.2.
Proof: Nonempty Range
\[ \forall \text{ALIST} X. \text{MEMBER}(X, \text{DOM ALIST}) \land (\exists Y. \text{MEMBER}(Y, \text{RANGE ALIST}) \land \text{APPALIST}(X, \text{ALIST}) = Y) \]

Example 8: Heuristics of a proof. Section 6.3.4.
Proof: Lemma 6.3. LengthInverse
\[ \forall U. \text{PERM}(U) \supset \text{LENGTH}(\text{INVERSE}(U)) = \text{LENGTH} U \]

Example 9: Use of general lemmata and efficiency. Section 6.5.4.
Proof: Theorem 2 (ii) (Right identity)
\[ \forall U U \circ \text{IDENT}(\text{LENGTH} U) = U \]

Example 10: Discussion of the formalization of an informal argument. Section 7.
Proof: Every surjection of finite sets of the same cardinality is an injection.
10. Index of SIMPINFO.

The following lines are labeled simpinfo in some proof. They are available to EKL in the execution of all proofs that use the proof in question by the command get-proofs (we the graph of file dependency at the beginning of the Appendix).

Simpinfo from file LISPAX
proof LISPAX

13. ∀x.sexp x a
14. ∀u.sexp u
15. ∀x. u.listp x u
16. ∀u. ¬null u u listp cdr u
17. ∀u. ¬null u u exp car u
18. ∀x. ¬atom x u exp car x
19. ∀x. ¬atom x u exp cdr x
20. ∀x y.exp x y
21. ∀x y. ¬atom x y
22. ∀x u. ¬null x u
23. ∀u. null u u = nil
24. ∀x y. car (x y) = x
25. ∀x y. cdr (x y) = y
26. car nil = nil
27. cdr nil = nil
28. ∀u. ¬null u u car u. cdr u = u

; labels: SIMPINFO CONS CAR CDR
29. ∀x. ¬atom x u car x. cdr x = x
30. list(()) = nil
31. ∀lst. listp list(lst)

; labels: SIMPINFO LISTDEF
32. ∀x. list(x. lst) = x. list(lst)
33. listappend
47. ∀x u. v. nil* v = v a x u. v = x. (u v)

; labels: SIMPINFO LISTAPPEND
48. ∀u. v. listp u = v
49. ∀u. u* nil = u
50. ∀x v. x. nil* v = x. v
56. valist. listp a list
About Permutations in Lisp and EKL

;labels: SIMINFO ALISTDEF
58. ∀X Y ALIST ALISTP NIL ALISTP (X A Y) ALIST

61. ∀X ALIST SEXP ASSOC X ALIST

66. ∀U SEXP CAR U

67. ∀U LISTP CDR U

Simpinfo from file SET
proof SETS
3. ∀X URELEMENT X
4. ∀X SEXP(X)

Simpinfo from file NATNUM
proof NATNUM
10. ∀N NATNUM(N')

;labels: SIMINFO PRED_DEF
19. ∀N PRED(N') = N

20. ∀N NATNUM(PRED(N))

;labels: SIMINFO PLUSFACTS PLUSDEF
21. ∀N K 0 + N = N K' + N = (K + N)

22. ∀N M NATNUM(N+M)

;labels: SIMINFO PLUSFACTS
23. ∀N N 0 = N

;labels: SIMINFO PLUSFACTS PLUSDEF1
24. ∀N 1 + N = N' + 1 = N'

;labels: SIMINFO SUCCFACTS ZERO_NOT_SUCCESSOR
17. ∀N ¬N' = 0

;labels: SIMINFO ZEROLEAST
9. ∀N ¬N < 0

;labels: SIMINFO SUCCFACTS SUCCESSORLESS
13. ∀M N M' < N' ⇒ N < N

;labels: SIMINFO SUCCFACTS SUCCESSOREQ
14. ∀M N M' = N' ⇒ N = M

;labels: SIMINFO SUCCFACTS ZEROLEAST3
16. ∀N 0 < N'}
Simpinfo from file MINUS
proof LESSEQ
  1. ∀N. N=N'
  ;labels: SIMPINFO SUCCESSORFACTS SUCCESSORLESSEQ
  4. ∀M. N'M=NNM
  ;labels: SIMPINFO ZERO_NON_LESS_SUCCESSOR
  9. ∀M. N'<M⇒N=0

proof MINUS
  ;labels: SIMPINFO MINUS_SORT
  3. ∀K. NATNUM(K-N)
  ;labels: SIMPINFO N.LESS.N
  9. ∀N. N-N=0

Simpinfo from file LENGTH
proof LENGTH
  ;labels: SIMPINFO LENGTHDEF
  2. ∀U. X.LENGTH NIL=0ALENGTH (X.U)=LENGTH U'
  3. ∀U. NATNUM(LENGTH U)
  4. ∀U. LENGTH U=0⇒NULL U
  ;labels: SIMPINFO LENGTHADD
  5. ∀U. V.LENGTH (U+V)=LENGTH U+LENGTH V
  6. ∀X. LENGTH (XNIL)=1
  ;labels: SIMPINFO HAVE_MEMBER
  8. ∀Y. MEMBER(Y,U)⇒LENGTH U
  ;labels: SIMPINFO HAVE_MEMBER1
  9. ∀Y. MEMBER(Y,U)⇒NULL U

Simpinfo from file NTH
proof LISPAX
  69. ∀W. W=NULL W
  70. ∀W. SEXP W
proof NTH

;labels: SIMPINFO NTHDEF
2. ∀x u n. nth(wil, n) = nilnth(u, 0) = car u nth(x, u, n') = nth(u, n)

;labels: SIMPINFO SEXP_NTH
3. ∀u n. nth(u, n)

proof NTHCDR

;labels: SIMPINFO DEF
2. ∀x u n. nthcdr(wil, n) = nilnthcdr(u, 0) = u nthcdr(x, u, n') = nthcdr(u, n)

3. ∀u n. listp nthcdr(u, n)

proof FSTPOSITION

;labels: SIMPINFO POSFACTS
3. ∀u y. (null fstposition(u, y)) = member(y, u) ∧
   (member(y, u) ∧ natnum(fstposition(u, y))) ∧
   (null fstposition(u, y) ∨ natnum(fstposition(u, y)))

;labels: SIMPINFO SORTPOS
4. ∀u n. listp fstposition(u, n)

Simpinfo from file APPL
proof ALISTFACTS

;labels: SIMPINFO DOMSORT
1. ∀alist.listp dom(alist)

;labels: SIMPINFO RANGESORT
2. ∀alist.listp range(alist)

;labels: SIMPINFO APPALISTSORT
5. ∀alist y. sexp appalist(y, alist)

proof APPL

;labels: SIMPINFO APPLFACTS
3. ∀u i. i < length u sexp appl(u, i) ∨ member(appl(u, i), u)

Simpinfo from file MULT
proof MULTIPLICITY

;labels: SIMPINFO MULTFACT
3. ∀u a. natnum(mult(u, a))

;labels: SIMPINFO EMPTYFACTS
7. ∀u.mult(u, emptyset) = 0

Simpinfo from file ASSOC
proof ALISTFACTS

;labels: SIMPINFO COMPALISTSORT
11. ∀alist a. alistp alist v alist1
Simpinfo from file PERMF
proof PERMFACTS

;labels: SIMPINFO SORTCOMP
2. \forall V . DEF_APPL(V, U) \rightarrow LISTP V \bullet U
3. \forall V . ALLP(\forall X . NATNUM(X) \rightarrow \forall X . LENGTH V, U) \rightarrow LISTP V \bullet U
4. \forall M, N . LISTP IDENT1(M, N)
5. \forall N . LISTP IDENT(N)
6. \forall U, N . LISTP INVERSl(U, I, N)
7. \forall U . LISTP INVERSE(U)

;labels: SIMPINFO IDENT_LENGTH
9. \forall M . LENGTH (IDENT1(M, N)) = N
10. \forall N . LENGTH (IDENT(N)) = N
10.1. Index of Definitions.

Definitions from file LISPAX
proof LISPAX

;labels: LISTINDUCTIONDEF
34. ∀DF NILCASE DEF.
   (3FUN.(∀PARS X U.FUN(WIL,PARS)=NILCASE(PARS)∧
   FUN(X.U,PARS)=DEF(XLU,DEF(U,DF(X,PARS)),PARS)))

;labels: SEXPINDUCTIONDEF
36. ∀ATOMCASE DEFSEXP DF1 DF2.
   (∃FUN.
   (∀PARS X Y Z.(ATOM Z⇒ FUN(Z,PARS)=ATOMCASE(Z,PARS))∧
   FUN(X.Y,PARS)=
   DEFSEXP(X,Y,FUN(X,DF1(X,Y,PARS)),
   FUN(Y,DF2(X,Y,PARS)),PARS)))

;labels: HIGH_ORDER_DEFINITION
40. ∀BIGFUN ATOM_FUN.
   (3DEFUN_FUN.(∀X Y.(ATOM X⇒DEFUN(X)=ATOM_FUN(X))∧
   DEFINED_FUN(X,Y)=
   BIGFUN(X,Y,DEFINED_FUN(X),
   DEFINED_FUN(Y))))

;labels: SIMPINFO LISTDEF
45. ∀X LST.LIST(X,LST)=X.LIST(LST)

;labels: SIMPINFO APPENDEF
47. ∀X U VNIL*V=VX.U*V=X.(U*V)

;labels: ALLPDEF
52. ∀PHI X U.ALLP(PHI,NIL)∧
   ALLP(PHI,X,U)=(IF PHI(X) THEN ALLP(PHI,U) ELSE FALSE)

;labels: SOMEPDEF
53. ∀PHI X U.SOMEP(PHI,NIL)∧
   SOMEP(PHI,X,U)=(IF PHI(X) THEN TRUE ELSE SOMEP(PHI,U))

;labels: MAPCARDEF
54. ∀FN X U.MAPCAR(FN,NIL)=NILAMAPCAR(FN,X,U)=FN(X).MAPCAR(FN,U)

;labels: ALISTDEF
57. ∀ALIST.=NULL ALIST⇒
   =ATOM CAR ALISTAATOM CAR (CAR ALIST)ALISTP CDR ALIST

;labels: SIMPINFO ALISTDEF
58. ∀XA Y ALIST. ALISTP NIL ⇒ALISTP (XA.Y).ALIST

;labels: ASSOCDEF
60. ∀X YA LIST. ASSOC(X,NIL)=NIL∧
   ASSOC(X,(XA.Y).ALIST)=
   (IF X=XA THEN XA.Y ELSE ASSOC(X,ALIST))

;labels: MEMBERDEF
63. ∀X Y U.=MEMBER(X,NIL)©MEMBER(X,Y,U)=(X=VMEMBER(X,U))

;labels: UNIQUENESSDEF
65. ∀U UNIQUENESS(NIL)∧(UNIQUENESS(X,U)=MEMBER(X,U)©UNIQUENESS(U))
Definitions from file SET
proof SETS

6. \( \forall X \forall X \in AV \equiv AV(X) \)

9. \( \forall B \forall B \in AV \cap BV = (\forall X \in AV(X) \land BV(X)) \)

11. \( \forall B \forall B \in AV \cup BV = (\forall X \in AV(X) \lor BV(X)) \)

13. \( \forall B \forall B \in AV \setminus BV = (\forall X \in AV(X) \setminus BV(X)) \)

14. \( \forall X \in AV \setminus BV = (\forall X \in AV(X) \setminus BV(X)) \)

Definitions from file NATNUM
proof NATNUM

19. \( \forall \text{ PRED}(N') = N \)

21. \( \forall \text{ PRED}(K, 0 + N) = N \land \text{ PRED}(K + N) \)

24. \( \forall \text{ PRED}(1 + N) = N \land \text{ PRED}(1) \)

Definitions from file MINUS
proof LESSEQ

3. \( \forall N \cdot M \leq N = (N = N \lor M < N) \)

proof MINUS

2. \( \forall N \cdot M - 0 = M \land M \cdot N = \text{ PRED}(M - N) \)

Definitions from file LENGTH
proof LENGTH

2. \( \forall U \cdot \text{ LENGTH} \ NIL = 0 \land \text{ LENGTH} (X . U) = \text{ LENGTH} U \)
proof INDUCTION
;labels: INDUCTIVE_DEFINITION
5. VNDF ZCASE NDEF.
   (3FUN.(\NPARS N.FUN(0,NPARS)=ZCASE(NPARS)A
           FUN(N',NPARS)=
           NDEF(N,FUN(N,MDF(N,NPARS)),NPARS)))
   ;labels: HIGH_ORDER_NATNUM_DEFINITION
10. \INDFN ARB.
    (3DEF_FUN.(\N.DEF_FUN(0)=ARBA
               DEF_FUN(N')=INDFN(N,DEF_FUN(N))))

Definitions from file NTH
proof NTH
;labels: SIMPINFO NTHDEF
2. VX U N.NTH(NIL,N)=NIL\ANDTH(U,O)=CAR U\ANTH(X.U,N')=NTH(U,N)

proof NTHCDR
;labels: SIMPINFO NTHCDRDEF
2. VX U N.NTHCDR(NIL,N)=NIL\ANDTHCDR(U,O)=U\ANTHCDR(X.U,N')=NTHCDR(U,N)

proof FSTPOSITION
;labels: FSTPOSITIONDEF
2. VX U Y.FSTPOSITION(NIL,Y)=NIL\A
   FSTPOSITION(X.U,Y)=(IF \MEMBER(Y,X.U) THEN NIL
                       ELSE (IF X=Y THEN 0 ELSE FSTPOSITION(U,Y)'))

proof INJ
;labels: INJDEF
2. VU.INJ(U)=(\VN M.N<LENGTH U\ANM<LENGTH U\ANTH(U,N)=NTH(U,M)\N=M)

Definitions from file APPL
proof APPALIST
;labels: DOMDEF
2. VXA Y ALIST.DOM(NIL)=NIL\ADOM((XA.Y).ALIST)=XA.DOM(ALIST)
;labels: RANGEDEF
4. VXA Y ALIST.RANGE(NIL)=NIL\ARANGE((XA.Y).ALIST)=Y.RANGE(ALIST)
;labels: FUNCTDEF
6. \VALIST.FUNCTP(ALIST)=UNIQUENESS(DOM(ALIST))
   * labels: INJECTDEF
8. \VALIST.INJECTP(ALIST)=FUNCTP(ALIST)\AUNIQUENESS(RANGE(ALIST))
;labels: APPALISTDEF
10. \VALIST.Y.APPALIST(Y,ALIST)=CDR ASSOC(Y,ALIST)
;labels: SAMEMAPDEF
12. \VALIST ALIST1.SAMEMAP(ALIST,ALIST1)=
    MKLSET(DOM(ALIST))=MKLSET(DOM(ALIST1))A
    (VY.Y\N\MKLSET(DOM(ALIST1)))\APPLIST(Y,ALIST)=APPALIST(Y,ALIST1))
;labels: PERMUTP_DEF
13. \VALIST.PERMUTP(ALIST)=
    FUNCTP(ALIST)\A MKLSET(DOM(ALIST))=MKLSET(RANGE(ALIST))
proof ALISTFACTS

; labels: SAMEMAP_DEF
10. ∀ALIST1 ALIST2. SAMEMAP(ALIST1, ALIST2) =
    MKLSET(DOM(ALIST1)) = MKLSET(DOM(ALIST2)) 
    (∀X. APPALIST(X, ALIST1) = APPALIST(X, ALIST2))

proof APPL

; labels: APPLDEF
1. ∀U I. APPL(U, I) = NTH(U, I)

; labels: INTO_DEF
5. ∀U. INTO(U) = (∀N. N < LENGTH U ∨ NTH(N) = NTH(U, N)) ∨ LENGTH(U, N) < LENGTH U

; labels: ONTO_DEF
7. ∀U. ONTO(U) = (∀N. N < LENGTH U ∨ MEMBER(N, U))

; labels: PERM
9. ∀U. PERM(U) = ONTO(U)

Definitions from file SUMS

proof SUMS

; labels: ALLNUMDEF
7. ∀N A. ALLNUM(O, A) = ALLNUM(N', A) = A(N') ∨ ALLNUM(N, A)

; labels: SOMENUMDEF
8. ∀N A. ~SOMENUM(O, A) = SOMENUM(N', A) = A(N') ∨ SOMENUM(N, A)

; labels: SUMDEF
9. ∀N NUMSEQ. SUM(NUMSEQ, O) = O
    SUM(NUMSEQ, N') = SUM(NUMSEQ, N) + NUMSEQ(N)

; labels: UNDEF
10. ∀N SETSEQ. UN(SETSEQ, O) = EMPTYSET
    UN(SETSEQ, N') = UN(SETSEQ, N) ∪ SETSEQ(N)

; labels: DIJPAIR_DEF
12. ∀A B. DIJPAIR(A, B) = EMPTY(A ∩ B)

; labels: DISJOINTDEF
14. ∀N SETSEQ. DISJOINT(SETSEQ, O) =
    DISJOINT(SETSEQ, N') =
    (DISJOINT(SETSEQ, N) ∨ DIJPAIR(UN(SETSEQ, N), SETSEQ(N)))

Definitions from file MULT

proof MULTIPLICITY

; labels: MULT_DEF
2. ∀X U A. MULT(NIL, A) = O
    MULT(X, U, A) = (IF A(X) THEN MULT(U, A) ELSE MULT(U, A))
Definitions from file ASSOC

;labels: COMPA LISTDEF
2. VALIST1 ALIST2 XA Y.NIL ALIST2=NIL
   (((XA,Y).ALIST1) ALIST2=
(XA.APPALIST(Y,ALIST2)).ALIST1 ALIST2

;labels: INVALID LISTDEF
4. VALIST XA Y.INVALIDLIST(NIL)=NIL
   INVALIDLIST((XA,Y).ALIST)=(Y,XA).INVALIDLIST(ALIST)

;labels: IDALISTPDEF
6. VALIST XA Y.IDALISTP(NIL)
   (IDALISTP((XA,Y).ALIST)=XA=YIDA LISTP(ALIST))

Definitions from file PERMP
proof COMP PRED

;labels: COMPDEF
2. VU V W.COMP(U,V,W)=LENGTH U=LENGTH WA
   (\forall N<LENGTH U\exists NTH(U,W)=NTH(V,NTH(W,N)))

;labels: ID_DEF
4. VU.ID(U,V)=\forall N<LENGTH U\exists NTH(U,W)=N

;labels: INVDEF
6. VU. INV(U,V)=\forall N<LENGTH U\exists NTH(U,W)=FSTPOSITION(V,N)

Definitions from file PERMF
proof COMP FNCT

;labels: DEF_APBPL_FACT
2. VU V.APPL(V,U)\forall(X.XATNUM(X)AX<LENGTH V,U)

;labels: COMPOSEDEF
4. VU V.X.U NIL\NIL U V\MTH(U,X).U\V

;labels: IDENTDEF1

;labels: IDENTDEF
8. V N.IDENT=N.IDENT1(O,N)

;labels: INVERSDEF1
10. V N.INVERS1(U,I,O)=NIL I N.INVERS1(NIL,I,O)=NIL
    INVERS1(U,I,N')=
    (IF NULL FSTPOSITION(U,I) THEN NIL
     ELSE FSTPOSITION(U,I).INVERS1(U,I',N))

;labels: INVERSDEF
12. VU.INVERSE(U)=INVERS1(U,0,LENGTH U)
INDEX OF FORMULAS
add-lesseq. 171
∀ K M. E(M + 1) ≤ M + K

add-one. 171
∀ K M. E(M + 1) = E(M) + M

addtozero, 165
∀ N B. E(0) = 0

alist-lema1. 91
VALIST ALIST. MEMBER(X, DOM(ALIST)) → APPALIST(X, ALIST = ALIST1) = APPALIST(APPALIST(X, ALIST), ALIST1)

alist_lema2. 91
VALIST ALIST. DOM(ALIST = ALIST1) = DOM(ALIST)

alist_lema3. 91
VALIST X. MEMBER(X, DOM(ALIST)) → (Y. MEMBER(Y, RANGE ALIST) ∧ APPALIST(X, ALIST) = Y)

alist_lema4. 93
VALIST 2. UNIQUENESS DOM(ALIST) ∧ MEMBER(Z, RANGE ALIST) → (EX. MEMBER(X, DOM ALIST) ∧ APPALIST(X, ALIST) = Z)

alistdef. 175
∀ X A LIST A LISTP BIL A ALISTP (X A Y) A LIST

alistdfl. 175
∀ U. ALISTP U = (¬ NULL U) ∧ Atom (CAR(U) ∧ Atom (CAR U) ∧ ALISTP (CDR U))

alistinduction. 61
∀ CHI. BIL CHI (BIL) Ab'XA Y A LIST. CHI A LIST A CHI A X A Y A LIST

allnumdef. 53
∀ A. ALLNUM(0, A) ∧ ALLNUM(W, A) ∧ ALLNUM(W, A)

allp_elimination. 37
∀ U. MEMBER(X, U) → (PHI1(U) ∨ PHI2(U))

allp_implication. 35
∀ U. A. ALLP(A, U) → φ(VX X A XK1(X)) = ALLP(A, U)

allp_introduction. 37
∀ U. (Y. MEMBER(Y, U) = PHI1(Y)) → ALLP(PHI1, U)

allp_nthcdr. 47
∀ U. ALLP(A, U) ⇒ ALLP(A, UTHCDR(U, W))

allp. 175
∀ PHI X U. ALLP(PHI, X U) ⇒ ALLP(PHI, X U) = IF PHI(X) THEN ALLP(PHI, U) ELSE FALSE

allpfact. 37
∀ PHI X U. ALLP(PHI, X U) ⇒ ALLP(PHI, U)

app_compalist. 91
VALIST ALIST. MEMBER(X, DOM(ALIST)) → APPALIST(X, ALIST = ALIST1) = APPALIST(APPALIST(X, ALIST), ALIST1)

appalistsort. 62
VALIST. SEXP APPALIST(Y, ALIST)

appender. 63
∀ U V. VIL = VA (X U) ∨ V = X (U V)

append. 63
∀ U I. APPL(U, I) = WTH(U, I)

appfacts. 61
∀ U I. I ≤ LENGTH U = SEXP APPL(U, I) ∧ MEMBER(APPL(U, I), U)

assoc_comp. 128
∀ U. ∀ W. DEF_APPL(W, V) = DEF_APPL(V, U) ⇒ (W + V) = U + (V + W)

assocdef. 175
∀ X A Y. ALIST. ASSOC(X, WIL) = Ψ Α ASOC(X, (X A Y) ALIST) = (IF X = X THEN X A Y ELSE Α SSOC(X, ALIST))

associativity_of_composition. 128
∀ U W V. PERM(V) ∧ PERM(U) ∧ LENGTH V = LENGTH U = LENGTH W = LENGTH U (W ∗ V) = U ∗ (V ∗ U)

associativity_pred. 124
∀ U1 W1 W2 W3. INTO(W3) = LENGTH W2 = LENGTH W3 ∧ COMP(V, W1, W2) = COMP(U, W1, W2) ∧ COMP(V, W1, W2) = COMP(U, W1, W2) ∨ U1 = U1

255
atomrange, 106
  VALIST (MLKSET (DOM (ALIST)) = MLKSET (RANGE (ALIST))) \#ALLP (ATOM, X, RANGE (ALIST))

car_nthcdr, 45
  \#N <LENGTH (UDCAR NTHCDR (U, N)) = NTH (U, N)

cdr_nthcdr, 45
  \#N \#CDR NTHCDR (U, N) = NTHCDR (U, N')

commutadd, 165
  \#N \#+ = \#N

commutmult, 166
  \#N \#* = \#N

comp_uniqueness, 121
  COMP (U, V, W) = COMP (U1, V, W) \& U1 = U1
compalist_associativity, 101
  VALIST ALIST1 ALIST2 (MLKSET (RANGE (ALIST1)) \#MLKSET (DOM (ALIST1))
    ALIST \# (ALIST1 \& ALIST2) = (ALIST \& ALIST1) \& ALIST2

compalist_asso, 93
  

compalist_sort, 90
  VALIST ALIST ALIST \& ALIST1
compalist_def, 89
  VALIST ALIST1 ALIST2 ((U \& ALIST2) = NIL ((U \& ALIST1) \& ALIST2 = (U \& APPALIST (Y, ALIST2)) (ALIST1 \& ALIST2))

composedef, 113
  \#V \#U (U \& NIL) = NIL ((U \& X) = (NTH (U, X)). (U \& U)

cons-car, cdr
  \#V (CAR U.CDR U = U)

cons-car, cdr
  \#V (CAR X.CDR X = X)

def_appl_condition, 115
  \#V (INTO (U) LENGTH \#LENGTH V) \#DEF_APP(V, U)
def_appl_condition, 115
  \#V (PERM (U) LENGTH \#LENGTH V) \#DEF_APP(V, U)
def_appl_fact, 113
  \#V \#DEF_APP(V, U) = ALLP (AX. NATNUM (X) AX < LENGTH (V), U)
demorgan, 33
  \#V Q. ((~P Q) = (\#P) A (~Q))
demorgan1, 33
  \#P Q. ((P Q) = (\#P) V (~P))
disj_pairdef, 54
  \#B \#DISJ PAIR (A, B) = EMPTY (A \& B)
disjoint_def, 54
  \#V \#SETSEQ. DISJOIN (SETSEQ, 0)
    \#DISJOIN (SETSEQ, 0) = (DISJOIN (SETSEQ, 0) \& DISJ PAIR (U (SETSEQ, 0), SETSEQ, 0))
disjoint, 85
  \#V \#DISJOIN (AX. MLKSET (AX), 0)
dom_compalist, 91
  VALIST ALIST1 ALIST DOM (ALIST \& ALIST1) = DOM (ALIST)
dom_invalist, 94
  \#V \#AILP (AX. ATOM, X, RANGE (ALIST)) \#DOM (INVALIST (ALIST)) = RANGE (ALIST)
domdef, 60
  \#V \#X \#ALIST \#DOM \#NIL = NIL \#DOM (AX. ATOM, X, ALIST) = X \#DOM ALIST
domlength, 62
  VALIST LENGTH (DOM (ALIST)) = LENGTH ALIST
domrangelength, 62
  VALIST LENGTH (DOM (ALIST)) = LENGTH (RANGE (ALIST))
domsort, 61
  VALIST. LISTP DOM (ALIST)
doubleinduction. 179
∀ X . Y . \phi12(M, U) ∧ \phi12(U, M) ∧ \phi12(X, Y, V)∧(\phi12(U, V) ∨ \phi12(X, U, Y, V))

doubleinduction. 179
∀ X . \phi13(M, X) ∧ \phi13(U, M) ∧ \phi13(X, U, W)∧(\phi13(U, W) ∨ \phi13(X, U, W))

duniondef. 40

emptyfacts.
∀ U . MULT(U, EMPTYSET) = 0

emptysetdef. 40
∀ U . EMPTYSET(A) = ∀ X . A(X)

emptysedef. 40
EMPTYSET = XX . FALSE

epsilondef. 39
∀ U . X . \epsilon(A, X, U) = A(X)

epsilondef. 40
∀ U . X . \epsilon(B, A, X, U) = A(X)

example. 35
∀ U . X . \epsilon(A, X, U) = X

excluded-middle. 33
∀ V . Q . P (QP) ∧ (∼ QP)

extensionality. 64
∀ U . V . LENGTH(U) = LENGTH(V) ∧ ∀ X . L. APPL(U, L) = APPL(V, L)∧(LENGTH(U) = V

fstposition_nth. 48
∀ U . N . UNIQUEBESS(U) ∧ LENGTH(U) ∧ X . FSTPOSITION(U, N, X) = N

fstpositiondef. 47
∀ U . V . FSTPOSITION(M, Y, U) = M ∧
FSTPOSITION(X, U, Y) = IF MEMBER(Y, X, U) THEN M ELSE IF M = Y THEN 0 ELSE ADD1(FSTPOSITION(U, Y))

fundef. 60
VALIST . FUNCTP(ALIST) = UNIQUENESS DOM(ALIST)

have-member. 178
∀ U . Y . MEMBER(Y, U) = 0 ∧ LENGTH U

have-member. 178
∀ U . Y . MEMBER(Y, U) = NULL U

highternary-definition. 174
∀ V . DEF-FUN . DEF-FUN(W, Y, (ATOM X ∧ DEF-FUN(X)) = ATOM(W) ∧
(DEF-FUN(X, Y) = DEFINYDEF-FUN(W, X, Y, DEF-FUN(X), DEF-FUN(Y)))

highernaturaldelay. 167
∀ V . DEF-FUN . AR.B.DEF-FUN(W, Y, DEF-FUN(O) = AR.B.DEF-FUN(W, M)) = IND(W, DEF-FUN(M))

id-left. 130
∀ U . V . W . ID(U) ∧ PERM(W) ∧ LENGTH W = LENGTH U ∧ COMPE(V, U, W, V)

id-main. 132
∀ U . (W ∧ X = IDENT(M) ∧ N) = N

id-perm. 120
∀ U . ID(U) ∧ PERM(U)

id-right. 129
∀ U . V . W . ID(U) ∧ COMPE(V, W, U, W) ∧ LENGTH U = V

idalistp-left. 103
VALIST . IDALISTP(ALIST) = MKLET(DOM(ALIST)) = MKLET(DOM(ALIST)) ∧ SAMEP(ALIST = ALIST, ALIST)

idalistp-main. 94
VALIST . IDALISTP(ALIST) ∧ MEMBER(Y, DOM(ALIST)) ∧ CDOM ASSOC(Y, ALIST) = Y

idalistp-permutp. 102
VALIST . FUNCTP(ALIST) ∧ IDALISTP(ALIST) ∧ PERMUTP(ALIST)

idalistp-right. 103
VALIST . IDALISTP(ALIST) ∧ (VALIST . MKLET(RANGE(ALIST)) = MKLET(DOM(ALIST)) ∧ ALIST = ALIST, ALIST)

idalistpdef. 90
VALIST . X . Y . IDALISTP(M) ∧ IDALISTP((X, Y, ALIST)) ∧ X = Y ALISTP ALIST

257
ident_sort.117
   \forall M \cdot LISP IDENT(M)

ident_sortl.115
   \forall M \cdot LISP IDENT1(M, M)

identdef.113
   \forall N \cdot IDENT(N) = IDENT1(0, N)

identdefl.113
   \forall N \cdot IDENT1(1, 0) = NIL \cdot IDENT1(1, N') = IDENT1(1', N)

identity-left.126
   \forall U \cdot INTO(U) \cdot IDENT1(LENGTH U) = U

identity-right.134
   \forall U \cdot IDENT1(LENGTH U) = U

inclusiondef.40
   \forall A, B \cdot ACHEV(A, (XV), \Rightarrow \cdot B(XV))

inductive_definition.166
   \forall N \cdot ZCASE NDEF \cdot (FUN \cdot (\forall PARS, FUNCTION(0, PARS)) = ZCASE(\forall PARS, FUNCTION(M, PARS), NDEF(M, FUNCTION(M, NDEF(M, PARS))))

inequality-law.171
   \forall M, K \cdot K < M \iff K < M \land K = K

infinite-descent.167
   \Rightarrow DESC \cdot \forall N \cdot DESC(N) < DESC(N)

injdef.52
   \forall A, B \cdot INJ(U) = \forall M, M < LENGTH(U) \land M < LENGTH(U) \land M = M

injdsj.lemma.80
   \forall A, B \cdot \forall LENGTH U \cdot ((M \cdot M = M) \land M = (M \cdot M = M) \land M = M)

injectdef.60
   \forall A, B \cdot INJECTP(ALIST) = FUNCTP(ALIST) \land UNIQUENESS RADIUS(ALIST)

interdef.40
   \forall A, B \cdot ANB = XV \cdot (A(XV), B(XV))

into-mult.86
   \forall U \cdot INTO(U) \cdot \forall M \cdot M < LENGTH(U) \iff M < LENGTH(U) \land M = M

intodf.63
   \forall U \cdot INTO(U) = \forall M \cdot M < LENGTH U \land M = M

inv_into.144
   \forall U \cdot PERM(U) \cdot INTO(INVERSE(U))

inv_left.139
   \forall U, V \cdot PERM(W) \land INV(U, W) \land COMP(V, U, W) \land LENGTH W = LENGTH U \land ID(W)

inv_perm.137
   \forall U, V \cdot PERM(U) \land INV(V, U) \land LENGTH V = LENGTH U \land PERM(V)

inv_right.137
   \forall U, V \cdot PERM(W) \land INV(U, W) \land COMP(V, U, W) \land LENGTH U = LENGTH W \land ID(V)

invalid-left.105
   \forall A, B \cdot ALIST \cdot INJECTP(ALIST) \land IDALISTP(INVALIDALIST(ALIST)) \iff ALIST

invalid-right.105
   \forall A, B \cdot ALIST \cdot ALISTP(INVALIDALIST(ALIST)) \iff ALIST

invalid_sort.90
   \forall A, B \cdot ALIST \cdot ALISTP(INVALIDALIST(ALIST)) \iff ALIST

invaliddef.89
   \forall A, B \cdot INVALID \land INVALID = (X, Y) \land ALIST = (X, Y) \land INVALID ALIST

invers_sort1.111
   \forall N \cdot LISTP INVERS1(U, I, M)

inversdef.113
   \forall U \cdot INVERSE(U) = INVERS1(U, 0, LENGTH(U))

inversdef1.113
   \forall U \cdot INVERS1(U, I, O) = \forall M \cdot (\forall I, M) = (Y, I) \land N \iff NULL(FSTPOSITION(U, I)) \land \forall I, M \iff NIL \land INVERS1(U, I, M) = NIL \land INVERS1(U, I, M) = IF NULL(FSTPOSITION(U, I)) \land \forall I, M = (I, I') \land (I, I') = 10
null
main-inv. 141
\[ \text{VON:} \text{PERM U} \rightarrow \text{LENGTH U} = \text{FSTPOSITION(U, U)} \]

mapcarded, 17.5
\[ \text{VFN X U: MAPCAR(FN, NIL) = NIL = MAPCAR(FN, X, U) = FN(X), MAPCAR(FN, U)} \]

member-mult, 55
\[ \text{VU Y A: MEMBER(Y, U) \&\& (Y) \rightarrow MULT(U, A)} \]

member_nth, 43
\[ \text{VU Y MEMBER(Y, U) \&\& (N) \rightarrow LENGTH U = \text{TH(y, U), MULT(U, A)} = Y} \]

memberdef, 175
\[ \text{VX Y U: MEMBER(X, NIL) \&\& MEMBER(Y, X, U) = (X = Y \&\& MEMBER(X, U))} \]

minus_sort, 169
\[ \text{VX K: NATUM(K-N)} \]

minnsi, 170
\[ \text{VX Y (PRED N) = 1} \]

minusdef, 169
\[ \text{VX M: O = M \&\& M = PRED(M-N)} \]

minusfact10, 170
\[ \text{VX M: N < M \&\& M = PRED(M-N)} \]

minusfact11, 170
\[ \text{VX M: N < M \&\& M = N} \]

minusfact3, 169
\[ \text{VX M: X < M \&\& PRED(N) = N} \]

minusfact7, 170
\[ \text{VX M: M < N \&\& PRED(N) = M-N} \]

mklet_fact, 188
\[ \text{VU M: KLSET(U) = (AX.(3K.K < LENGTH U = TH(BTH(U, K))) \rightarrow X))} \]

mklet_un, 194
\[ \text{VU W: WMKSET(WH(U, N)), LENGTH W = KLSET(U)} \]

mklet_def, 40
\[ \text{VU M: KLSET(U) = AX MEMBER(X, U)} \]

mkset_def, 10
\[ \text{VXV: KLSET(U) \&\& (XV \rightarrow (YV=XV)} \]

mkset_unklset, 177
\[ \text{VU V: MEMBER(Y, U) \&\& KLSET(Y) \&\& KLSET(U)} \]

mksetfact, 19-1
\[ \text{VX M: KLLENGTH UD(UW, AM. MKSET(WH(U, M)), N)) = (AX. (3K.K < LENGTH U, K) = X))} \]

mult_inj, 57
\[ \text{VX Y: MULT(V, MKSET(WH(V, X))) = 1) \rightarrow Y(V)} \]

mult_mult, 81
\[ \text{VU M: KLSET(U) \&\& KLSET(V) \&\& (YU: M < LENGTH UDMULT(V, MKSET(WH(U, M))) = 1))} \]
\[ \text{(V1: I < LENGTH V \&\& MULT(V, MKSET(WH(V, I))) = 1)} \]

mult_nthcdr, 55
\[ \text{VX Y: U < LENGTH UDMULT(WTHCDR(U, N), A) \&\& MULT(U, A)} \]

multdef, 54
\[ \text{VX U A: MULT(A, X, U) = O MULT(X, U, A) = IF A(X) THEB MULT(U, A) \&\& ELSE MULT(U, A)} \]

multfact, 54
\[ \text{VU: VU NATUM(MULT(U, A))} \]

multinj_computation, 57
\[ \text{VX I J: I < J \&\& LENGTH V = TH(V, I) \&\& 2 MULT(V, MKSET(WH(V, I)))} \]

n-less-n, 170
\[ \text{VX N = 0} \]

nonempty-domain, 93
\[ \text{VALIST Z: UBIQUEBESS DOM(ALIST) \&\& MEMBER(Z, RANGE ALIST) \&\& (3X MEMBER(X, DOM ALIST) \&\& ALIST = Z)} \]

nonempty-range, 91
\[ \text{VALIST X: MEMBER(X, DOM ALIST) \&\& (3Y MEMBER(Y, RANGE ALIST) \&\& ALIST = Y)} \]

260
normal, 33
V P ⊓ R.((P∩Q)∪R)=((P∪R)∩Q∪R))

normal, 33
V P ⊓ R.(P∩Q∩R)=((P∩R)∩Q)

nth_allp, 187
V P ⊓ U.(U.N E LENGTH U)∩P(U)>(∪Q(U))∩ALLP(U)

nth_compose, 127
V U. H, DEF.APPL(V, U)∩N E LENGTH U∩TH(V∩U, U)=TH(V, TH(U, U))

nth_fstposition, 48
V U. H, MEMBER(U, U)∩TH(U, FSTPOSITION(U, U))=N

nth_in_nthcdr, 45
V U, N. U∩N E LENGTH U)∩MEMBER(U, U)∩THCDR(U, N)

nth_nthcdr_zero, 45
V U, O∩LENGTH U∩THCDR(U, O)=THCDR(U, 1)=U

nth_nthcdr, 47
V U, N. U∩N E LENGTH U)∩THCDR(U, N)=THCDR(U, O∩N)

nthcdr_car_cdr, 45
V U, N. N∩E LENGTH U∩THCDR(U, N)=THCDR(U, E∩N)

nthcdr_ident, 133
V U, N. U∩N E LENGTH U∩THCDR(U, N)=THCDR(U, E∩N)

nthcdr_induction, 47

nthcdrdef, 45
V U, N. U∩THCDR(U, N)=U∩THCDR(U, N)

nthdef, 42
V U, N. U∩N E LENGTH U∩THCDR(U, N)=U∩THCDR(U, N)

nthmember, 43
V U, N. U∩N E LENGTH U∩MEMBER(U, U)∩TH(U, N)

oneleastssucc, 168
1∈N

ontodef, 63
V U. Onto(U)=(INTO(U)∩(U.N E LENGTH U)∩MEMBER(U, U))

perm_compose, 128
V V. Perm U A Perm V A LENGTH U = LENGTH V⊂ Perm(U∩V)

perm_composition, 121
PERM(V)∩PERM(W)⊂ LENGTH V∩LENGTH W⊂ COMP(U, V, W)∩PERM(U)

perm_ident, 133
V U. Perm(IDENT(U))

perm_injectivity, 87
V U. Perm(U)⊂ INJ(U)

perm_inverse, 143
V U. Perm(U)⊂ INVERSE(U)

permdef, 63
V U. Perm(U)=Onto(U)

permtp_def, 61
VALIST. Permtp(ALIST)=Funcp(ALIST)∩Mkset(Dom(ALIST), Kmset(RANGE(ALIST)))

permtp_injectp, 80
V V. Mkset(U)⊂ Mkset(V)∩(U.N E LENGTH U∩J∩ Mult(U, Mkset(U, N)))

permtp_injectp, 83
VALIST. Permtp(ALIST)⊂ INJCTP(ALIST)

pigeonfact, 71
V (V. Natnum(F(U)))⊂ (V. U.N E LENGTH U∩J∩ F(U))∩ORTH(AK.F(K), U)∩N=(U.N E LENGTH U∩J∩ F(U))

pigeonlist, 76
V Disjiniw(Setseq, LENGTH U)⊂ (U.N E LENGTH U∩J∩ Mult(U, Setseq(U)))⊂ (U.N E LENGTH U∩J∩ Mult(U, Setseq(U)))

261
plusdef. 165
\forall K. 0*H=H*H+(K*H)'

plusdef. 165
\forall N. H'=H \wedge H+1=H'

plusfacts. 165
\forall K. M.(K+M+K)=M+M

plusfacts. 165
\forall K. M.(K+M+K)=M+M+M

pos_length. 48
\forall Y. \text{MEMBER}(Y,U) \Rightarrow \text{FSTPOSITION}(U,Y) < \text{LENGTH } U

posfacts. 48
\forall U. (\forall Y. \text{MEMBER}(Y,U) \Rightarrow \text{FSTPOSITION}(U,Y)) \Rightarrow 
\text{FSTPOSITION}(U,Y) = \text{MATNUM}(\text{FSTPOSITION}(U,Y))

pred_cancellation. 170
\forall M. H*H \equiv \text{PRED}(M-H)=M-H

proof_by_doubleinduction. 166
\forall A. (\forall M. A2(O,M) \wedge A2(H,M) \wedge A2(H',M')) \Rightarrow M \not\equiv A2(M,M)

proof-by-induction. 166
\forall A. A(O) \wedge (\forall Y. A(Y)) \wedge (\forall M. A(M))

range-compose. 95
\forall ALIST. \text{PERMUT}(ALIST) \Rightarrow \text{MLSET}((\text{DOM}(ALIST)) \text{MLSET}(\text{DOM}(ALIST)))
\Rightarrow \text{MLSET}((\text{RANGE}(ALIST) \text{MLSET}(\text{RANGE}(ALIST)))

range-compose. 95
\forall ALIST. \text{PERMUT}(ALIST) \Rightarrow \text{MLSET}((\text{DOM}(ALIST)) \Rightarrow \text{MLSET}((\text{RANGE}(ALIST) \text{MLSET}(\text{RANGE}(ALIST)))

range-invalist. 94
\forall ALIST. \text{ALLP}(AX. \text{ATOM}(X) \Rightarrow \text{RANGE}(ALIST) = \text{DOM}(ALIST)

rangedef. 60
\forall Y. \text{ALIST}. \text{RANGE} = \text{RANGE}((U. Y) \Rightarrow \text{RANGE}(ALIST) = Y \Rightarrow \text{RANGE} ALIST

rangesort. 66
\forall ALIST. \text{LISTP} \text{RANGE}(ALIST)

rdistrib. 166
\forall K. M(M+K)=M+M+K

pluscan. 165
\forall K. M. (M+K+K)=M+M

pluscan. 165
\forall K. M. (M+K+K)=M+M

rtimescan. 166
\forall K. M. (M+K)=M+M

rtimescan. 166
\forall K. M. (M+K)=M+M

rtimestozero. 166
\forall K. M. (M=0) \Rightarrow (M+M)=M+M

\forall K. -K=0 \Rightarrow K=0

262
! FORMULA INDEX!

same_map_def. 62
VALIST1 ALIST2. SAMEMAP(ALIST1,ALIST2) = (MKSET(DOM(ALIST1)) = MKSET(DOM(ALIST2)) \& (\forall X. APPALIST(X, ALIST1) = APPALIST(X, ALIST2)))

same_map_equivalence. 62
SAMEMAP(ALIST, ALIST)

same_map_equivalence. 62
SAMEMAP(ALIST, ALIST1) \& SAMEMAP(ALIST1, ALIST2) \Rightarrow SAMEMAP(ALIST, ALIST2)

same_map_equivalence. 62
SAMEMAP(ALIST, ALIST1) \Rightarrow SAMEMAP(ALIST, ALIST2)

same_map_left. 94
VALIST ALIST1 ALIST2. SAMEMAP(ALIST1, ALIST2) \Rightarrow SAMEMAP(ALIST1 \& ALIST2 \& ALIST)

same_map_right. 94
VALIST ALIST1 ALIST2. SAMEMAP(ALIST1, ALIST2) \Rightarrow SAMEMAP(ALIST \& ALIST1 \& ALIST2)

same_mapdef. 61
VALIST ALIST1. SAMEMAP(ALIST, ALIST1) = MKLET(DOM(ALIST)) = MKLET(DOM(ALIST1)) \& (\forall Y. \& MKLET(DOM(ALIST)) \& APPALIST(Y, ALIST) = APPALIST(Y, ALIST1))

set-extensionality. 40
\forall A. (\forall X. X \subseteq A) \Rightarrow A \subseteq A

sexp_nth. 42
\forall U. N SEXP \#TH(U, N)

sexpinduction. 174
\forall PHI. (\forall X. \text{ATOM} X \Rightarrow PHI(X)) \Rightarrow (\forall X. PHI(X) \& PHI(Y) \& PHI(X \& Y)) \Rightarrow (\forall X. PHI(X))

sexpinductiondef. 174
\forall ATOMCASE DEFSEXPEP DF1 DF2. 3FUN \& VPARS \& U \& Z. (ATOM \& \& U \& Z. (FUN(X, Y, Z, PARS) \& \& ATOMCASE(Z, PARS) \& \& (FUN(U, \& U, \& Z, PARS) \& \& DEFSEXPEP(X, U, FUN(X, DF1(X, Y, Z, PARS)), FUN(Y, DF2(X, Y, Z, PARS))), PARS))

some_num_def. 53
\forall N. \& A. \& \& SOMEUM(O, A) \& \& SOMEUM(N, A) \Rightarrow (A \& N)

some_def. 175
\forall PHI \& U. \& SOMEOP(PHI, NIL) \& SOMEOP(PHI, X \& U) = IF PHI(X) THEN TRUE ELSE SOMEOP(PHI, U)

some_fact. 176
\forall U. SOMEOP(PHI1, U) = (\exists X. MEMBER(X, U) \& APHI1(X))

some_fact. 38
\forall U. SOMEOP(PHI1, U) \subseteq (\exists X. MEMBER(X, U) \& APHI1(X))

sortcomp. 115
\forall U. DEF-APL(Y, U) \& LISTP V \& U

sortpos. 48
\forall U. Y. SEXP \& FSTPOSITION(U, Y)

strictly-increasing. 72
\forall M. (M \& N \& M < N \& \& M < N \& \& M < N)

successor_less. 168
\forall M. M \& \& N \& M < N \& \& M < N

successor_less_seq. 168
\forall M. M \& \& N \& M < N

successor_minus. 169
\forall M. M \& \& M \& M = N \& \& M = N

successor1. 165
\forall M. K \& K

successor2. 165
\forall M. \& K \& K

successor_seq. 165
\forall M. (M \& \& M \& \& M \& \& M)

successorfacts. 167
\forall M. M \& \& M \& \& M

successorfacts. 167
\forall N. \& N

successorless. 165
\forall M. M \& \& M 

263
successorlesseq. 167
\forall M, N < M \iff \exists H (M = H + 1)

succfacts. 165
\forall M \leq N < M \iff (N = M)

succfacts. 165
\forall M \leq N < M \iff (N = M)

succfacts. 165
\forall M, N < M \iff (N = M)

succfacts. 165
\forall M, N < M \iff (N = M)

succfacts. 165
\forall M, N < M \iff (N = M)

succfacts. 165
\forall M, N < M \iff (N = M)

succfacts. 165
\forall M, N < M \iff (N = M)

succfacts. 165
\forall M, N < M \iff (N = M)

succfacts. 165
\forall M, N < M \iff (N = M)

succfacts. 165
\forall M, N < M \iff (N = M)

succfacts. 165
\forall M, N < M \iff (N = M)

succfacts. 165
\forall M, N < M \iff (N = M)

succfacts. 165
\forall M, N < M \iff (N = M)

sumdef. 53
\forall M \leq N \iff \sum(N, 0) = \sum(N, M) + \sum(M, N)

sumsort. 54
\forall M \leq N \iff \sumsort(M, 0) = \sumsort(M, N) + \sumsort(N, M)

timesdef. 166
\forall K, O \iff OA \iff (O + 1) = O + 1

timesfact 5. 166
\forall K \leq M < (K + 1) \iff (K + 1) = (K + 1)

timesfacts. 166
\forall K \leq M < (K + 1) \iff (K + 1) = (K + 1)

timesfacts. 166
\forall K \leq M < (K + 1) \iff (K + 1) = (K + 1)

timesfacts. 166
\forall K \leq M < (K + 1) \iff (K + 1) = (K + 1)

timesfacts. 166
\forall K \leq M < (K + 1) \iff (K + 1) = (K + 1)

timesfacts. 166
\forall K \leq M < (K + 1) \iff (K + 1) = (K + 1)

timesfacts. 166
\forall K \leq M < (K + 1) \iff (K + 1) = (K + 1)

timesfacts. 166
\forall K \leq M < (K + 1) \iff (K + 1) = (K + 1)

timesfacts. 166
\forall K \leq M < (K + 1) \iff (K + 1) = (K + 1)

timesfacts. 166
\forall K \leq M < (K + 1) \iff (K + 1) = (K + 1)

timesfacts. 166
\forall K \leq M < (K + 1) \iff (K + 1) = (K + 1)

timesfacts. 166
\forall K \leq M < (K + 1) \iff (K + 1) = (K + 1)

timesfacts. 166
\forall K \leq M < (K + 1) \iff (K + 1) = (K + 1)

timesfacts. 166
\forall K \leq M < (K + 1) \iff (K + 1) = (K + 1)

timesfacts. 166
\forall K \leq M < (K + 1) \iff (K + 1) = (K + 1)

timesfacts. 166
\forall K \leq M < (K + 1) \iff (K + 1) = (K + 1)

timesfacts. 166
\forall K \leq M < (K + 1) \iff (K + 1) = (K + 1)

timesfacts. 166
\forall K \leq M < (K + 1) \iff (K + 1) = (K + 1)

timesfacts. 166
\forall K \leq M < (K + 1) \iff (K + 1) = (K + 1)

timesfacts. 166
\forall K \leq M < (K + 1) \iff (K + 1) = (K + 1)

timesfacts. 166
\forall K \leq M < (K + 1) \iff (K + 1) = (K + 1)

timesfacts. 166
\forall K \leq M < (K + 1) \iff (K + 1) = (K + 1)

timesfacts. 166
\forall K \leq M < (K + 1) \iff (K + 1) = (K + 1)

timesfacts. 166
\forall K \leq M < (K + 1) \iff (K + 1) = (K + 1)

timesfacts. 166
\forall K \leq M < (K + 1) \iff (K + 1) = (K + 1)

timesfacts. 166
\forall K \leq M < (K + 1) \iff (K + 1) = (K + 1)

timesfacts. 166
\forall K \leq M < (K + 1) \iff (K + 1) = (K + 1)

timesfacts. 166
\forall K \leq M < (K + 1) \iff (K + 1) = (K + 1)

timesfacts. 166
\forall K \leq M < (K + 1) \iff (K + 1) = (K + 1)

timesfacts. 166
\forall K \leq M < (K + 1) \iff (K + 1) = (K + 1)

timesfacts. 166
\forall K \leq M < (K + 1) \iff (K + 1) = (K + 1)

timesfacts. 166
\forall K \leq M < (K + 1) \iff (K + 1) = (K + 1)

timesfacts. 166
\forall K \leq M < (K + 1) \iff (K + 1) = (K + 1)

timesfacts. 166
\forall K \leq M < (K + 1) \iff (K + 1) = (K + 1)

trans. cond. 33
\forall Q, R, (Q \iff R) \iff (IF P THEN Q ELSE R) \iff R

trans. lesseq. 167
\forall M, N \iff M < N \iff M \leq N

transitivity, of-order. 166
\forall M, N, K \iff M < N \iff K < N

trichotomy. 169
\forall M, N \iff M < N \iff M = N \iff N < M

trichotomy. 178
\forall U \iff \text{LENGTH}(U) = \text{LENGTH}(U)

264
FORMULA INDEX

trivial_appalist.62
  ∀alist. ¬ emptysel(dom(alist)) ⇒ appalist(y, alist) = nil

trivial_nthcdr.47
  ∀v u. length(u) ≤ # nthcdr(u, v) = nil

undef.53
  ∀u. "setseq. ub(setseq, o) = emptysetau. setseq, u' = ub(setseq, o) " = setseq(u)"setseq, u"

unionfact1.194
  ∀setseq u. m. m < # setseq(m) = setseq(setseq, u)union(setseq, u)

uniqueness_injectivity.52
  ∀v u. uniqueness(u) = inj(u)

uniqueness_def.175
  ∀v u. uniqueness nil a(uniqueness(x, u) = member(x, u) ∧ uniqueness(u))

zero-nonless-successor.168
  ∀v. ¬ x < o

zero_not_successor.165
  ∀v. x = o

zeroleast. 168
  ∀v. x ≤ o

zeroleast1.164
  ∀v. x ≤ o

zeroleast2.165
  ∀v. x = o ≤ 0 < o

zeroleast3. 165
  ∀v. x < o