CS109B Notes for Lecture 6/5/95

Why Tautologies Again?

- Same reason: they embody logical principles that do not depend on the meaning (i.e., interpretation) of the symbols.
- But predicate logic is richer in tautologies than propositional logic, because there are new concepts to incorporate: quantifiers and predicates with arguments.

What is Lost Moving From Propositional to Predicate Logic?

- While there is a finite (although exponential-time) test for tautologyhood in propositional logic (truth tables), *there is no such test for predicate logic.*
- Thus, the only ways to prove a tautology in predicate logic are:

1. Reason about all interpretations using some ad-hoc argument, or
2. Deduce the tautology from other known tautologies, using the four transformations: substitution principle, substitution of equals for equals, commutativity of $\equiv$ and transitivity of $\equiv$.

Tautologies of Predicate Logic

A major source is substitution of predicate logic expressions for the variables of *propositional* logic tautologies.

- Laws unique to predicate logic follow below.

"Infinite DeMorgan's laws"

(a) $(\forall X)E \equiv \texttt{NOT}\big((\exists X)(\texttt{NOT}E)\big)$
(b) $(\exists X)E \equiv \texttt{NOT}\big((\forall X)(\texttt{NOT}E)\big)$

Example: We can say:

1. 'G is a complete graph if for every pair of distinct nodes u and v there is an edge $\{u, v\}$." We could also say

2. "G is a complete graph if for no pair of distinct nodes u and v is edge $\{u, v\}$ missing."

- These are equivalent statements.

- Formally, let $ne(U, V)$ stand for "$U \neq V$" and let $p(U, V)$ stand for "there is an edge $\{U, V\}$." Then the above statements are:

(1) $(\forall U)(\forall V)\big(ne(U, V) \rightarrow p(U, V)\big)$

(2) $\texttt{NOT}\Big((\exists U)(\exists V)\big(ne(U, V) \texttt{ AND NOT } p(U, V)\big)\Big)$

- Let $E = ne(U, V) \texttt{ AND NOT } p(U, V)\big)$. Then we can rewrite (2) as:

(2′) $\texttt{NOT}\big((\exists U)(\exists V)E\big)$

- Use infinite DeMorgan (b) on $(\exists V)E$:

(3) $\texttt{NOT}\Big((\exists U)\big(\texttt{NOT}(\forall V)(\texttt{NOT } E)\big)\Big)$

- Use infinite DeMorgan (a) backwards on (3).

(4) $(\forall U)(\forall V)(\texttt{NOT } E)$

- By "finite" DeMorgan and "double negation," $\texttt{NOT } E$ is equivalent to

$$\texttt{NOT } ne(U, V) \texttt{ OR } p(U, V)$$

which is in turn equivalent to

$$ne(U, V) \rightarrow p(U, V)$$

Thus, (4) is transformed into (1).

- By substitution of equals for equals, we have proved (1) is equivalent to (2).

Renaming

$(\forall X)E \equiv (\forall Y)F$ provided

- □ F is E with all free occurrences of X changed to Y.

- □ There are no free occurrences of Y in E.

- Similar law for $\exists$.

Example: $(\forall X)p(X,Y)$.

- We may replace X by Z to get $(\forall Z)(p(Z,Y)$. That is,

  $$(\forall X)p(X,Y) \equiv (\forall Z)p(Z,Y)$$

  is a tautology.

- However, we may not replace X by Y, because Y is free in $p(X,Y)$. That is,

  $$(\forall X)p(X,Y) \equiv (\forall Y)p(Y,Y)$$

  is *not* a tautology.

Moving quantifiers inside/outside of AND, OR

$$E \texttt{ AND } (\forall X)F \equiv (\forall X)(E \texttt{ AND } F)$$

provided there is no free use of X in E.

- 7 similar rules: AND can be OR, $\forall$ can be $\exists$, and the order of E and F can be switched.

- Compare with making a local C variable x global. OK unless the scope of x now includes some function that used to refer to another global x.

Example: $(\forall X)\big(p(X) \texttt{ OR } q(Y)\big)$.

- We can move the $(\forall X)$ to the left operand of the OR to get $(\forall X)p(X)$ OR $q(Y)$. That is,

  $$(\forall X)\big(p(X) \texttt{ OR } q(Y)\big) \equiv (\forall X)p(X) \texttt{ OR } q(Y)$$

  is a tautology.

- However, if X were free in q — e.g., $q(X,Y)$ — then we could not move the quantifier. That is,

  $$(\forall X)\big(p(X) \texttt{ OR } q(X,Y)\big) \equiv (\forall X)p(X) \texttt{ OR } q(X,Y)$$

  is *not* a tautology.

Default Universal Quantification

Any free variables in an expression (not a subexpression of some larger expression) are implicitly universally quantified.

- $(\forall X)E$ is a tautology iff E is a tautology.

Example: To say "$p(X)$" is the same as saying "$(\forall X)p(X)$."

- Both say "p is true no matter what X is."