SETS GENERATED BY ITERATION OF A LINEAR OPERATION

BY

DAVID A. KLARNER

STAN-CS-72-275

MARCH 1972

COMPUTER SCIENCE DEPARTMENT
School of Humanities and Sciences
STANFORD UNIVERSITY

SETS GENERATED BY ITERATION OF A LINEAR OPERATION

David A. Klarner

Abstract

This note is a continuation of the paper "Arithmetic properties of certain recursively defined sets," written in collaboration with Richard Rado. Here the sets under consideration are those having the form $S = \langle m_1x_1 + \ldots + m_rx_r: 1\rangle$ where $m_1,\ldots,m_r$ are given natural numbers with greatest common divisor 1. The set S is the smallest set of natural numbers which contains 1 and is closed under the operation $m_1x_1 + \ldots + m_rx_r$. Also, S can be constructed by iterating the operation $m_1x_1 + \ldots + m_rx_r$ over the set $\{1\}$. For example, $\langle 2x + 3y: 1\rangle = \{1, 5, 13, 17, 25, \ldots\} = (1 + 12N) \cup (5 + 12N)$ where $N = \{0,1,2,\ldots\}$. It is shown in this note that S contains an infinite arithmetic progression for all natural numbers $r-1, m_1, \ldots, m_r$. Furthermore, if $(m_1,\ldots,m_r) = (m_1 \ldots m_r, m_1 + \ldots + m_r) = 1$, then S is a per-set; that is, S is a finite union of infinite arithmetic progressions. In particular, this implies $\langle mx+ny: 1\rangle$ is a per-set for all pairs $\{m,n\}$ of relatively prime natural numbers. It is an open question whether S is a per-set when $(m_1,\ldots,m_r) = 1$, but $(m_1 \ldots m_r, m_1 + \ldots + m_r) > 1$.

This research was supported in part by the National Science Foundation under grant number GJ-992, and the Office of Naval Research under contract number N-00014-67-A-0112-0057 NR 044-402. Reproduction in whole or in part is permitted for any purpose of the United States Government.

1. Introduction

This note is a continuation of Section 3 of "Arithmetic properties of certain recursively defined sets," written in collaboration with Richard Rado. All of the special notation used in this note is defined there. Besides using the notation of [1], we shall require also several results proved there.

The significance of the present note in relation to [1] is as follows: Let $r-1, m_1, \ldots, m_r$ denote natural numbers. There exists a smallest set S denoted $\langle m_1x_1 + \ldots + m_rx_r : 1\rangle$ which contains 1 and is closed under the operation $\rho = m_1x_1 + \ldots + m_rx_r$. The set S can be constructed by iterating ρ over the set $\{1\}$; that is, $S = \{1\} \cup \rho\{1\} \cup (\{1\} \cup \rho\{1\} \cup \rho(\{1\} \cup \rho\{1\})) \cup \cdots$. Among other things, it was shown in [1] that S is an affine transformation of the set $\langle m_1x_1 + \ldots + m_rx_r + b : a\rangle$, and S is closed under multiplication. We use these results in the present note to show that S contains an infinite arithmetic progression, thus resolving Conjecture 2 of [1] in the affirmative. Also, we show that if $(m_1, \ldots, m_r) = (m_1 \cdots m_r, m_1 + \ldots + m_r) = 1$, then S is a per-set; that is, S is a finite union of infinite arithmetic progressions. This settles affirmatively infinitely many cases of Conjecture 1 in [I]. In particular, this completely settles the case $r = 2$ of Conjecture 1.

The main idea developed here is as follows. We show that S contains an affine transformation of a set T having the form $\langle mx_1 + \ldots + mx_k : 1\rangle$ where $k = r!$ and $m = m_1 \cdots m_r$. Next, we show that T contains an infinite arithmetic progression A. This implies S contains an affine transformation of A, so S contains an infinite arithmetic progression, $a + d\mathbb{N}$ say. We show that if $(a,d) = (m_1,\ldots,m_r) = 1$, then S is a per-set. The condition $(a,d) = 1$ is met when $(m_1 \ldots m_r, m_1 + \ldots + m_r) = 1$, and this is the route to our main result.

2. Results

THEOREM 1: Suppose $k,m \in \mathbf{P}$, and let

(1) $$S = \langle mx_1 + \ldots + mx_k + 1 : 0 \rangle ,$$

(2) $$T = \{c_0 + c_1 m + \ldots + c_h m^h : h \in \mathbb{N},\ c_0 \in \{0,1\},\ c_i \le kc_{i-1},\ i \in [1,h]\} .$$

Then

(3) $$S = T.$$

PROOF: First, we show that

(4) $$1 + mT + \ldots + mT \subseteq T \quad .$$

To see this, suppose $x^{(j)} \in T$ and let $x^{(j)} = c_0^{(j)} + c_1^{(j)} m + \ldots$ for $j = 1,\ldots,k$, then by definition of T

(5) $$c_0^{(j)} \in \{0,1\} \quad , \quad c_i^{(j)} \le c_{i-1}^{(j)} \qquad (i \in \mathbf{P},\ j = 1,\ldots,k) ;$$

there exists a number t such that $c_i^{(j)} = 0$ for all $i \ge t$ and $j = 1,\ldots,k$. Now let

(6) $$x = 1 + m \sum_{j=1}^{k} x^{(j)} = \sum_{i=0}^{\infty} c_i m^i$$

where $c_0 = 1$, and

(7) $$c_i = \sum_{j=1}^{k} c_{i-1}^{(j)} \qquad (i \in \mathbf{P}) .$$

It follows from (5) that

(8) $$c_i \le kc_{i-1} \quad (i\in P) \;;$$

also, $c_i = 0$ for all $i \ge t+1$ since $c_{i-1}^{(j)} = 0$ for all $i-1 \ge t$ and $j = 1,\dots,k$. Hence, $x\in T$, and this proves (4).

Next, we show that

(9) $$T \subseteq \{0\} \cup (1 + mT + \dots + mT) \, .$$

Suppose the contrary, and let y denote the smallest number in T not contained in the set defined on the right in (9). We have

(10) $$y = c_0 + c_1 m + \dots + c_h m^h$$

where $c_0 \in \{0,1\}$ and $c_i \le kc_{i-1}$ for $i = 1,\dots,h$. Suppose c_j has the form

(11) $$c_j = \sum_{i=1}^{k} c_{j-1}^{(i)}$$

with $c_{j-1}^{(i)} \in N$ for $i = 1,\dots,k$, then since $c_{j+1} \le kc_j$, there exist $c_j^{(i)} \in N$ with $c_j^{(i)} \le c_{j-1}^{(i)}$ for $i = 1,\dots,k$, such that

(12) $$c_{j+1} = \sum_{i=1}^{k} c_j^{(i)} \, .$$

Hence, we can construct k-vectors $(c_{j-1}^{(1)}, \dots, c_{j-1}^{(k)})$ recursively for $j = 1,\dots,h$ such that $c_j^{(i)} \le c_{j-1}^{(i)}$ and (11) holds for $j = 1,\dots,h-1$. Also, since $c_1 \le k$, we can select $c_0^{(i)} \in \{0,1\}$ for $i = 1,\dots,k$. It follows that $c_0^{(i)} + c_1^{(i)}m + \dots \in T$ for $i = 1,\dots,k$. Also, (11) implies

$$(13) \qquad y = \sum_{j=0}^{h} c_j m^j = c_0 + m \sum_{j=1}^{h} \sum_{i=1}^{k} c_{j-1}^{(i)} m^{j-1} .$$

Since 0 is an element of the set on the right in (9), and we are supposing y is not an element of this set, it follows that $c_0 \neq 0$. Hence, $c_0 = 1$, and (13) implies

$$(14) \qquad y > y^{(i)} = c_0^{(i)} + c_1^{(i)} m + \ldots + c_{h-1}^{(i)} m^{h-1} \qquad (i = 1,\ldots,k) .$$

The numbers $y^{(i)}$ have the proper form so that we can conclude $y^{(i)} \in T$ for $i = 1,\ldots,k$, and (13) shows that $y = 1 + my^{(1)} + \ldots + my^{(k)}$. But this means y is an element of the set on the right in (9), a contradiction. So (9) is true.

Together (4) and (9) imply

$$(15) \qquad 1 + mT + \ldots + mT = T .$$

Since $1 + mx_1 + \ldots + mx_k$ is an increasing operation, we can apply the Corollary of Theorem 3 proved in [1] to conclude from (15) that $T = S$. This completes the proof.

THEOREM 2: Suppose $k-1, m \in P$, and let ℓ be an integer satisfying $k^{\ell} - k^{\ell-1} \geq m-1$, then

$$(16) \qquad \frac{k^{\ell} m^{\ell} - 1}{km-1} + m^{\ell} N \subseteq \langle mx_1 + \ldots + mx_k + 1 : 0 \rangle = S .$$

PROOF: Suppose $h \in N$, $d_0 \in [0, k^{\ell}]$, and $d_i \leq kd_{i-1}$ for $i = 1, \ldots, h$, then it follows from Theorem 1 that $1 + km + \ldots + k^{\ell-1} m^{\ell-1} + d_0 m^{\ell} + \ldots + d_h m^{\ell+h}$ is an element of S . That is,

$$(17) \qquad \frac{k^{\ell} m^{\ell} - 1}{km-1} + m^{\ell} D \subseteq S ,$$

where

(18) $$D = \{d_0 + d_1 m + \ldots + d_h m^h : h \in N,\ d_0 \in [0,k^\ell],\ d_i \le k d_{i-1} \text{ for } i = 1,\ldots,h\} .$$

We want to show $D = N$. Of course, $D \subseteq N$, so it has to be shown that $N \subseteq D$. Suppose the contrary, and let y denote the smallest non-negative integer not contained in D. Note that

(19) $$[0,k^\ell] \subseteq D ,$$

(20) $$[k^{\ell-1},k^\ell] + mD \subseteq D .$$

Since $k^\ell - k^{\ell-1} \ge m-1$, there exists $r \in [k^{a-1},k^\ell]$ such that $y = qm+r$. But (19) implies $y > k^\ell$, so $0 \le q < y$. Because y was chosen minimal, it follows that $q \in D$, and (20) implies $y = r+qm \in D$, a contradiction. This completes the proof.

COROLLARY OF THEOREM 2:

(21) $$k^a m^a + (km-1)m^\ell N \subseteq \langle mx_1 + \ldots + mx_k : 1\rangle .$$

PROOF: This follows from (16) and Corollary 1 of Theorem 9 proved in [1].

THEOREM 3: Suppose $r-1, m_1, \ldots, m_r \in P$, let $k = r!$, let $m = m_1 \ldots m_r$, and let $S = \langle m_1x_1 + \ldots + m_rx_r : 1\rangle$,

(22) $$T = \langle (m_1 + \ldots + m_r)^r - km + mx_1 + \ldots + mx_r : 1\rangle \subseteq S .$$

PROOF: It was shown in [1] that S is closed under multiplication. Hence, since

(23) $$m_1S + \ldots + m_rS \subseteq S$$

we have

$$(24) \qquad (m_1 S + \ldots + m_r S)^t \subseteq S$$

for all $t \in P$. In particular, (24) holds for $t = r$. Writing $t = r$ in (24), we have

$$(25) \qquad \sum_{i_1=1} \sum_{i_r=1} m_{i_1} \cdots m_{i_r} S^r \subseteq S \;;$$

but, since $1 \in S$ and $S^r \subseteq S$, (25) implies

$$(26) \qquad (m_1 + \ldots + m_r)^r - r!\, m_1 \ldots m_r + \sum_{i=1}^{r!} m_1 \ldots m_r S \subset S .$$

Hence, S is closed under the operation $(m_1 + \ldots + m_r)^r - km + m_1 x_1 + \ldots + m_r x_r$; also, $1 \in S$. Now we use the fact that T is a subset of every set X closed under this operation provided $1 \in X$. Since S satisfies these conditions, we have $T \subset S$, and this completes the proof.

COROLLARY OF THEOREM 3: Suppose $\ell \in P$ satisfies $k^{\ell} - k^{\ell-1} > m-1$. Then

$$(27) \qquad 1 + ((m_1 + \ldots + m_r)^r - 1)\left(\frac{k^{\ell} m^{\ell} - 1}{km-1}\right) + ((m_1 + \ldots + m_r)^r - 1) m^{\ell} N \subseteq S .$$

PROOF: The set T defined in (22) is an affine transformation of the set $R = \langle mx_1 + \ldots + mx_k : 1 \rangle$. In fact, using Corollary 1 of Theorem 9 proved in [1], we have

$$(28) \qquad T = \frac{((m_1 + \ldots + m_r)^r - 1) R - (m_1 + \ldots + m_r)^r + km}{km-1}$$

Furthermore, (21) asserts that R contains an arithmetic progression A. Thus, T contains the set obtained by replacing R with A in the right number of (28), and this gives (27).

THEOREM 4: Suppose $a, d, r-1, m_1, \ldots, m_r \in \mathbf{P}$, $(a,d) = (m_1, \ldots, m_r) = 1$, and let $S = \langle m_1x_1 + \ldots + m_rx_r : 1 \rangle$. If $a + dN \subseteq S$, then S is a per-set.

PROOF: Let $a_1, \ldots, a_h \in \mathbf{P}$ denote representatives of all the residue classes modulo d entered by S. We suppose the a's are ordered so that $a_1 \equiv 1 \pmod{d}$, and for each $j \in [2,h]$ there exist elements $b_1, \ldots, b_r \in \{a_1, \ldots, a_{j-1}\}$ such that $a_j \equiv m_1b_1 + \ldots + m_rb_r \pmod{d}$. Now we show by induction on t that $aa_t + dN \subseteq S$. Since $a_1 \equiv 1 \pmod{d}$, $aa_1 \equiv a \pmod{d}$, and

(29) $$a_1a + dN \subseteq a + dN \subseteq S.$$

Suppose $a_ia + dN \subseteq S$ for $i = 1, \ldots, t$ where $t \geq 1$. We have $a_{t+1} \equiv m_1b_1 + \ldots + m_rb_r \pmod{d}$ for certain elements $b_1, \ldots, b_r \in \{a_1, \ldots, a_t\}$; also, we have supposed $b_ia + dN \subseteq S$ for $i = 1, \ldots, r$. Using the fact that $m_1N + \ldots + m_rN \doteq N$, and applying Lemma 5 of [1] we have

(30) $$a_{t+1}a + dN \doteq \sum_{i=1}^{r} m_i(ab_i + dN) \subseteq S.$$

It follows by induction that

(31) $$a_ta + dN \subseteq S$$

for $t = 1, \ldots, h$.

Recall that S is closed under multiplication. Hence, for each $i \in \mathbf{P}$ there exists $c_i \in \{a_1, \ldots, a_h\}$ such that $a^i \equiv c_i \pmod{d}$. In particular, if u is the order of $a \pmod{d}$, then $a^{u-1} \equiv c_{u-1} \pmod{d}$ and $c_{u-1}a \equiv 1 \pmod{d}$. But $c_{u-1}a + dN \subseteq S$ by (31), and this implies $1 + dN \subseteq S$.

The numbers $a_1, \ldots, a_h$ were selected so that

$$(32) \qquad S \subseteq \bigcup_{i=1}^{h} (a_i + dN) \quad .$$

Furthermore, since $1 + dN \subset S$ we can write $a = 1$ in (31) and conclude that

$$(33) \qquad \bigcup_{i=1}^{h} (a_i + dN) \not\subset S \quad .$$

Together (32) and (33) imply

$$(34) \qquad \bigcup_{i=1}^{h} (a_i + dN) \doteq S \quad ,$$

so S is equal to a per-set with a finite subset deleted from it. It follows from Lemma 2 of [1] that S is a per-set. This completes the proof.

THEOREM 5: Suppose $r-1, m_1, \ldots, m_r \in \mathbf{P}$ with $(m_1, \ldots, m_r) = (m, m_1 + \ldots + m_r) = 1$ where $m = m_1 \ldots m_r$. Then $S = \langle m_1 x_1 + \ldots + m_r x_r : 1\rangle$ is a per-set.

PROOF: Let $a + dN$ denote the arithmetic progression given in (27), and note that $(m, m_1 + \ldots + m_r) = 1$ implies $(a,d) = 1$. This is easily checked by noting that $a \equiv 1 \bmod((m_1 + \ldots + m_r)^r - 1)$, and $a \equiv (m_1 + \ldots + m_r)^r (\bmod m)$ since $(k^\ell m^\ell - 1)/(km-1) \equiv 1 (\bmod m)$. Since $(m_1, \ldots, m_r) = 1$, we can apply Theorem 4 to conclude that S is a per-set. This completes the proof.

COROLLARY OF THEOREM 5: If $m, n \in \mathbf{P}$ with $(m,n) = 1$, then $\langle mx + ny : 1\rangle$ is a per-set.

PROOF: If $(m,n) = 1$, then $(m,m+n) = (n,m+n) = (mn,m+n) = 1$, and the result follows from Theorem 5.

There are infinitely many sets $\langle m_1x_1 + \ldots + m_rx_r : 1\rangle$ with $r-1, m_1, \ldots, m_r \in \mathbf{P}$ and $(m_1, \ldots, m_r) = 1$ whose status as a per-set or non-per-set is left open by Theorem 5 or Theorem 10 of [1]. For example, neither Theorem 5 nor Theorem 10 applies to sets $\langle m_1x_1 + m_2x_2 + m_3x_3 : 1\rangle$ where $m_1 = ab(ay+bz)$, $m_2 = acy$, $m_3 = bcz$ with a, b, c, y, z natural numbers chosen so that $(m_1, m_2, m_3) = 1$.

Reference

[1] D. A. Klarner and R. Rado, "Arithmetic properties of certain recursively defined sets," to appear.