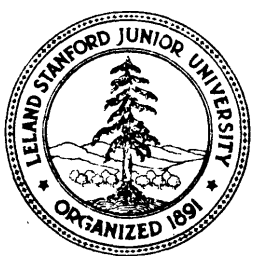
ARITHMETIC PROPERTIES OF CERTAIN RECURSIVELY DEFINED SETS

BY

D. A. KLARNER
R. RADO

STAN-CS-72-269
MARCH 1972

COMPUTER SCIENCE DEPARTMENT
School of Humanities and Sciences
STANFORD UNIVERSITY



ARITHMETIC PROPERTIES OF CERTAIN RECURSIVELY DEFINED SEX'S

D. A. Klarner
Computer Science Department
Stanford University
Stanford, California 94305 . .

R. Rado */
Department of Mathematics
University of Reading
Reading, England

Abstract

Let R denote a set of linear operations defined on the set P of positive integers; for example, a typical element of R has the form $\rho(x_1,\ldots,x_r) = m_0 + m_1x_1 + \ldots + m_rx_r$ where $m_0,\ldots,m_r$ denote certain integers. Given a set A of positive integers, there is a smallest set of positive integers denoted (R:A) which contains A as a subset and is closed under every operation in R . The set $\langle R:A\rangle$ can be constructed recursively as follows: Let $A_0 = A$, and define

$$A_{k+1} = A_k \cup \{\rho(\bar{a}): \rho\in R, \bar{a}\in A_k \times \ldots \times A_k\} \quad (k = 0,1,\ldots) ,$$

then it can be shown that $(R:A) = A_0 \cup A_1 \cup \ldots$. The sets (R:A) sometimes have an elegant form, for example, the set $\langle 2x+3y: 1\rangle$ consists of all positive numbers congruent to 1 or 5 modulo 12 . The objective is to give an arithmetic characterization of elements of a set $\langle R:A\rangle$, and this paper is a report on progress made on this problem last year. Many of the questions left open here have since been resolved by one of us (Klarner).

This research was supported by the Office of Naval Research under number N-000%67-A-0112-0057 NR 044-402, and by the National Science Foundation under grant number GJ-992. Reproduction in whole or in part is permitted for any purpose of the United States Government.

*/ Currently Visiting Professor, Faculty of Mathematics, Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, Canada.

ARITHMETIC PROPERTIES OF CERTAIN RECURSIVELY DEFINED SETS

by

D. A. Klarner and R. Rado

1. Introduction

We begin with a rough description of the kind of problem treated in this paper. This will be followed with a review of certain notions from universal algebra which are going to be used in the precise formulation of our problems. We would like to point out at the outset that only the language and very little of the theory of universal algebra seem to enter our work.

Consider a set R of finitary operations defined on a set X , and suppose A is a subset of X . It can be shown that there is a "smallest" set $\langle R:A\rangle$ with $A \subseteq \langle R:A\rangle \subset X$ such that $\langle R:A\rangle$ is closed under all operations in R . This is a rough version of the "definition from above" of the set $\langle R:A\rangle$. However, there is an alternative "definition from below" which involves iteration of the operations in R . We define a sequence of sets $A_0, A_1, \ldots$ recursively so that

$A = A_0 \subseteq A_1 \subseteq \ldots$ and $A_0 \cup A_1 \cup \ldots = (R:A)$.

Even though we have a constructive definition of (R:A) it is often very difficult to decide whether a given element x of X is an element of $\langle R:A\rangle$. Such a situation may lead to a search for a simple characterization of the elements of $\langle R:A\rangle$ which avoids the recursive construction. For example, it will be shown later on that the subset $\langle 2x+3y:1\rangle$ of the

natural numbers consists precisely of all positive integers congruent to 1 or 5 modulo 12 . This case is typical of the class of problems which will be considered. In general, we seek an arithmetic characterization of sets (R:A) of natural numbers where R is a finite set of finitary linear operations defined on the set of natural numbers, and A is a finite set of natural numbers.

Let us introduce some notation from universal algebra and give a precise formulation to our problem. Henceforth, X denotes a set. Let X^r , for every natural number r , denote the set of all r-tuples of elements of X . A mapping ρ which sends X^r into X is called an r-ary operation on X . For every $Y \subseteq X$ we put

$$(1) \qquad \rho(Y) = \{\rho(\bar{y}) : \bar{y} \in Y^r\} \ .$$

In particular, $\rho(\emptyset) = \emptyset$. A finitary operation on X is an r-ary operation on X for some unspecified natural number r . Henceforth, R denotes a set of finitary operations on X . For $Y \subset X$, let

$$(2) \qquad R(Y) = \bigcup_{\rho \in R} \rho(Y) \ .$$

Henceforth, A denotes a fixed subset of X . Let $\mathscr{I}(R:A)$ denote the set of all subsets of X which contain A and are closed under all operations in R . In other words,

$$(3) \qquad \mathscr{I}(R:A) = \{Y : A \subseteq Y \subseteq X \ ; R(Y) \subset Y\} \ .$$

Finally, for $\mathcal{T} \subseteq \mathscr{I}(R:A)$, $\mathcal{T} \neq \emptyset$, we define the meet of $\mathcal{T}$ by

$$(4) \qquad \bigwedge \mathcal{T} = \bigcap_{T \in \mathcal{T}} T \ ,$$

and if $\mathcal{T} = \emptyset$, then we define $\bigwedge \mathcal{T} = X$.

The join of $\mathcal{T}$ is defined by

$$(5) \qquad \bigvee \mathcal{T} = \bigwedge \mathscr{S}(R:\bigcup_{T\in\mathcal{T}} T) \quad .$$

It is easy to check that $\bigwedge \mathcal{T} \in \mathscr{S}(R:A)$. Clearly, $\bigvee \mathcal{T} \in \mathscr{S}(R:A)$ for all $\mathcal{T} \subseteq \mathscr{S}(R:A)$. Because of its importance, we have a special notation for the set $\bigwedge \mathscr{S}(R:A)$, namely,

$$(6) \qquad \langle R:A\rangle = \bigwedge \mathscr{S}(R:A) \quad .$$

This brings us to the first noteworthy result in the theory of universal algebra (see Kurosh [1, pp. 93-99]).

THEOREM 1. The set $\mathscr{S}(R:A)$, ordered by set inclusion, forms a complete lattice with meets and joins defined by (4) and (5) respectively. The greatest element of $\mathscr{S}(R:A)$ is X , and the least element is $(R:A)$ as defined in (6).

The next result provides a construction for $\langle R:A\rangle$.

THEOREM 2. Let $A_0 = A$, and $A_{i+1} = A_i \cup R(A_i)$ for $i = 0,1,\ldots$, and put $A_\infty = A_0 \cup A_1 \cup \ldots$. Then

$$(7) \qquad \langle R:A\rangle = A_\infty \quad .$$

Proof. By definition, $A = A_0 \subseteq A_\infty \subseteq X$. Next, let ρ be an r-ary operation in R , and select elements $x_1,\ldots,x_r$ of A_∞. Then there exists a number $k \geq 0$ such that $x_1,\ldots,x_r \in A_k$. Hence, in view of $A_{k+1} = A_k \cup R(A_k)$, we have $\rho(x_1,\ldots,x_r) \in A_{k+1} \subseteq A_\infty$. This proves $A_\infty \in \mathscr{S}(R:A)$.

An easy proof by induction on k establishes that $A_k \subseteq Y$ for $k = 0,1,\ldots$ whenever $Y \in \mathscr{S}(R:A)$. Hence $Y \in \mathscr{S}(R:A)$ implies $A_\infty \subseteq Y$. In particular, $A_\infty \subseteq \langle R:A\rangle$. But $(R:A)$ is the least element of $\mathscr{S}(R:A)$. Therefore $A_\infty = (R:A)$, and the proof is complete.

THEOREM 3. Let $Y \in \mathscr{S}(R:A)$. Then $A \cup R(Y) \in \mathscr{S}(R:A)$ and

$$(8) \qquad (R:A) = A \cup R((R:A)) .$$

Proof. Since $A \cup R(Y) \subset Y$ we have $R(A \cup R(Y)) \subseteq R(Y)$ which implies the first assertion. Put $S = \langle R:A\rangle$ and, for every $X' \subseteq X$, $\varphi X' = A \cup R(X')$. Then S is the intersection of all $X' \subseteq X$ with $X' \supseteq \varphi X'$. Consider one such X' . By definition of S , $S \subseteq X'$, which implies $\varphi S \subseteq \varphi X' \subseteq X'$. Therefore, by definition of S , $\varphi S \subseteq S$ and so $\varphi\varphi S \subseteq \varphi S$. Again, by definition of S , we have $S \subseteq \varphi S$ so that, finally, $S = \varphi S$, which is (8).

We introduce the following notation:

$$P = \{1,2,3,\ldots\} \; ; \; N = \{0,1,2,\ldots\} \; ; \; J = \{0,1,-1,2,-2,\ldots\} \; ;$$

$$[a,b] = \{x: x \in J \; ; \; a \leq x \leq b\} \text{ for } a,b \in J .$$

Henceforth, X is assumed to be the set P . We shall also severely limit the scope of the set R . An r-ary operation ρ on P is said to be linear if there exist numbers $a,m_1,\ldots,m_r$ such that

$$(9) \qquad \rho(x_1,\ldots,x_r) = a + m_1x_1 + \bullet \; .+mrxr$$

for all $x_1,\ldots,x_r \in P$. If $a = 0$ then ρ is said to be homogeneous. Henceforth, unless the contrary is stated, R is assumed to be a finite set of finitary linear operations on P . Usually, the elements of R

will be listed explicitly, say in the form $R = \{\rho_i : i\in[1,k]\}$, and in this case we write $\langle \rho_i(i\in[1,k]) :A\rangle$ instead of $(R:A)$. A similar convention is adopted when the elements of A are listed. For example, we shall consider sets such as $\langle 2x+1,3x+1:1\rangle$ and $\langle 2x+3y:1\rangle$. An r-ary operation ρ is called strictly increasing if $\rho(x_1,\ldots,x_r) > x_1,\ldots,x_r$ for all $x_1,\ldots,x_r \in P$. An important corollary of Theorem 3 can be derived for sets R consisting of operations of this kind.

Corollary of Theorem 3. Let R be a set of strictly increasing operations on P, and $A \subseteq P$. Then the equation $Y = A \cup R(Y)$ holds if and only if $Y=(R:A)$.

Proof. In view of (8), we only have to show that $Y = A \cup R(Y)$ implies $Y = \langle R:A\rangle$. Cur assumption implies $Y \in \mathscr{P}(R:A)$, so that $(R:A) \subseteq Y$. If $(R:A) \neq Y$ then there is a least element x of $Y\backslash(R:A)$. Then $x\notin A$, since otherwise we would have $x \in (R:A)$. But the relations $Y = A \cup R(Y)$ and $x\notin A$ imply the existence of an r-ary operation ρ in R together with elements $x_1,\ldots,x_r$ of Y such that $\rho(x_1,\ldots,x_r) = x$. By hypothesis, ρ is strictly increasing, so that $x > x_1,\ldots,x_r$. Hence $x_1,\ldots,x_r \in (R:A)$, and $x = \rho(x_1,\ldots,x_r) \in \langle R:A\rangle$, which is the required contradiction. This completes the proof.

Another notational convenience we shall employ concerns the addition and multiplication of sets of numbers. For $n\in J$ and $A,B \subseteq J$ we define

$$n+A = \{n+a: a\in A\} ,$$

$$A+B = \{a+b: a\in A;\ b\in B\} ,$$

$$nA = \{na: a\in A\} ;\ AB = \{ab: a\in A;\ b\in B\} .$$

For example, the set $\{a+dn: n\epsilon N\}$, which forms an arithmetic progression, may be written as $a+dN$.

Sets expressible as a finite union of arithmetic progressions enter our investigations in a natural way. For example, consider the set $S = \langle x+ \rho(x_1,\ldots,x_r):a\rangle$ where $a,r\epsilon P$, and ρ is an r-ary operation on P such that, with $d = \rho(a,a,\ldots,a)$, we have $\rho(x_1,\ldots,x_r) \equiv \rho(y_1,\ldots,y_r)(\mathrm{mod}\ d)$ whenever $x_i \equiv y_i(\mathrm{mod}\ d)$ for $i\epsilon[1,r]$. Under these circumstances all elements of S are congruent to a modulo d , so that

$$S \subseteq a + dN . \tag{10}$$

On the other hand, a simple induction on k establishes that $a+kd \epsilon S$ for all $k\epsilon N$, in view of $a+(k+1)d = a+kd+ \rho(a,\ldots,a)$. Hence there is equality in (10). Furthermore, one can show under various conditions that if $\langle R:A\rangle$ contains an infinite arithmetic progression, then $\langle R:A\rangle$ is expressible as a finite union of arithmetic progressions. For example, see Theorem 4 below. Before proving Theorem 4 we must discuss some general properties possessed by sets expressible as finite unions of arithmetic progressions.

A set $A \subseteq P$ is called a <u>per-set</u> if A is expressible as a finite union of infinite arithmetic progressions. This means that A has the form

$$A = \bigcup_{i=1}^{k} (a_i + d_iN) , \tag{11}$$

where $k\epsilon N$ and $a_i,d_i \epsilon P$ for $i\epsilon[1,k]$. It is easy to see that a set $A \subseteq P$ is a per-set if and only if $A = F+dN$ where F is a finite subset of P and $d\epsilon P$. The name "per-set? is used to remind us of the periodicity property of such sets which is expressed in the following lemma.

Lemma 1. A set $A \subseteq P$ is a per-set if and only if there exists $d \in P$ such that $d+A \subset A$.

Proof.

(i) Let A be a per-set defined by (11) with $k > 0$. Let d be the least common multiple of $d_1,\ldots,d_k$. Since $a_i+d_i n+d = a_i + d_i(n + (d/d_i))$ for $i \in [1,k]$ and $n \in N$ it follows that $d+A \subseteq A$.

(ii) Suppose that $A \subseteq P$ and $d+A \subseteq A$ for some $d \in P$. For $x \in A$ put $f(x) = \min(A \cap (x+dJ))$. Then the set $F = \{f(x): x \in A\}$ has at most d elements, and if $F = \{a_1,\ldots,a_k\}$ then $A = U\,(i \in [1,k])(a_i + dN) = F+dN$. This completes the proof.

We conclude from (ii) that per-sets are the sets of the form $F + dN$ with F finite and $d \in P$.

We note that the relations $d+A \subseteq A$ and $d'+A \subseteq A$ imply $(d+d')+A = d+(d'+A) \subset d+A \subset A$.

Let ρ denote the set of all per-sets. Our next result shows that ρ has a nice structure.

Lemma 2. Let $A,B \in \rho$. Then $A \cup B, A \cap B \in \rho$. Also, for every finite set $F \subset A$, we have $A \setminus F \in \rho$

Proof. By Lemma 1, there are numbers $d,d' \in P$ such that $d+A \subseteq A$ and $d'+B \subset B$. Then $dd' + (A \cup B) \subseteq A \cup B$, $dd' + (A \cap B) \subset A \cap B$, and the sets $A \cup B$ and $A \cap B$ are in ρ by Lemma 1. There exists $n \in P$ such that $F \subseteq [1,nd]$. Then $nd+(A\setminus F) \subseteq A \setminus F$, and $A \setminus F \in \rho$ by Lemma 1. This completes the proof.

For any sets X,Y we say that X is almost contained in Y, and we write

$$X \subseteq Y ,$$

if $X \backslash Y$ is finite. We say that X and Y are almost equal, and we write

$$X \doteq Y ,$$

if $X \subseteq Y \subseteq X$. Clearly, the relation $\subseteq$ is reflexive and transitive, and $\doteq$ is an equivalence relation. The set $A \subseteq P$ is called a near per-set if A is almost equal to a per-set. Thus, a near per-set is a set which is expressible as a finite union of arithmetic progressions, each progression being allowed to be finite or infinite. The set of all near per-sets has a structure similar to that of P as given in Lemma 2. It is easy to see that a set $A \subseteq P$ is a near per-set if and only if there is $d \in P$ such that $d+A \subseteq A$. We are now ready to state and prove a result which shows how per-sets enter our theory.

THEOREM 4. Let A be a per-set and R a set of operations of the form $a+m_1x_1+\ldots+m_rx_r$, where $a,r,m_1,\ldots,m_r \in P$, such that the highest common factor $(m_1,\ldots,m_r)$ has the value 1. Then $(R:A)$ is a per-set.

Proof. Assume $A,R \neq \emptyset$. There is $d \in P$ with $d+A \subseteq A$. Put $S = (R:A)$;

$$s = (R:A) ;$$

$$f(x) = \min(S \cap (x+dJ)) \quad (x \in S) ;$$

$$S' = \{f(x): x \in S\} .$$

Then S' is finite and

$$SC \bigcup_{X \in S'} (x+dN) = S' + dN .$$

We can write S' in the form $S' = \{s_1, \ldots, s_k\}$, such that $k \in P$, and there is $m \in [0,k]$ such that (i) $s_1, \ldots, s_m \in A+dJ$, (ii) for each $\lambda \in [m+1,k]$ there is an operation $\rho(x_1, \ldots, x_r) \in R$ and indices $\lambda_1, \ldots, \lambda_r \in [1,\lambda-1]$ such that $\rho(s_{\lambda_1}, \ldots, s_{\lambda_r}) \in s_\lambda + dJ$. Then $s_\lambda + dN \subseteq A \subseteq S$ for $\lambda \in [1,m]$. Now assume, using an inductive argument, that $\sigma \in [m+1,k]$ and $s_\lambda + dN \subseteq S$ for all $\lambda \in [1,\sigma-1]$. We shall deduce $s_\sigma + dN \subseteq S$. There are indices $\lambda_1, \ldots, \lambda_r \in [1,\sigma-1]$ and an operation $\rho(x_1, \ldots, x_r) = a + m_1 x_1 + \ldots + m_r x_r \in R$ such that $\rho(s_{\lambda_1}, \ldots, s_{\lambda_r}) \in s_\sigma + dJ$. Then $s_\sigma \in a + m_1 s_{\lambda_1} + \ldots + m_r s_{\lambda_r} + dJ$; $s_{\lambda_i} + dN \subseteq S (i \in [1,r])$. There are indices $\lambda_1, \ldots, \lambda_r \in [1,\sigma-1]$ and an operation $\rho(x_1, \ldots, x_r) = a + m_1 x_1 + \ldots + m_r x_r \in R$ such that $\rho(s_{\lambda_1}, \ldots, s_{\lambda_r}) \in s_\sigma + dJ$. Then $s_\sigma \in a + m_1 s_{\lambda_1} + \ldots + m_r s_{\lambda_r} + dJ$; $s_{\lambda_i} + dN \subseteq S (i \in [1,r])$. There are numbers $p_i \in P$ such that $s_{\lambda_i} + dp_i + dN \subset S$ for $i \in [1,r]$. Then $a + \sum m_i s_{\lambda_i} + d\sum m_i p_i + d\sum m_i N \subseteq S$. There is $q \in P$ such that $q+N \subseteq \sum m_i N$. This is a well known consequence of $(m_1, \ldots, m_r) = 1$. There is $t \in J$ such that $a + \sum m_i s_{\lambda_i} = s_\sigma + td$. Now we have

$$s_\sigma + td + d\sum m_i p_i + d(q+N) \subseteq s_\sigma + td + d\sum m_i p_i + d\sum m_i N$$

$$= a + \sum m_i s_{\lambda_i} + d\sum m_i p_i + d\sum m_i N \subseteq .$$

This implies $s_\sigma + dN \subseteq S$. Thus we have proved, by induction, that $s_\lambda + dN \subseteq S$ for each $\lambda \in [1,k]$. Therefore $S' + dN \subseteq S$, and there is a finite set $F \subset S' + dN$ satisfying $(S' + dN) \setminus F \subseteq S \subseteq S' + dN$. Then $S = (S' + dN) \setminus F'$ for some $F' \subseteq F$. Since $S' + dN \in \mathcal{P}$ it follows from Lemma 2 that $S \in \mathcal{P}$, and Theorem 4 is proved.

It is worth noting that if the set $\langle R':A' \rangle$ contains an infinite arithmetic progression, and R' contains a non-empty set R satisfying the hypothesis of Theorem 4, then $\langle R':A' \rangle$ contains a non-empty per-set but possibly may not be equal to a per-set.

Before going on to special cases of sets of the form (R:A) we prove one more fairly general result concerning the multiplicative structure of sets $\langle R:A \rangle$. For the moment we drop the requirement that the elements of R be linear operations. An r-ary operation ρ on R is now said to be homogeneous if

$$\rho(ax_1, ax_2, \ldots, ax_r) = a\rho(x_1, \ldots, x_r) \tag{12}$$

for all $a, x_1, \ldots, x_r \in P$. We shall show that under certain conditions the set (R:A) is closed under multiplication.

THEOREM 5. Let $A \subseteq P$, and let R be a set of homogeneous operations on P. Put $S = \langle R:A \rangle$. Then $AS \subseteq S$ implies $SS \subseteq S$. In particular, if $A = \{1\}$, then $SS = S$.

Proof. Let $AS \subseteq S$ and $t \in SS$. Then there is $a \in S$ such that

$$t \in aS = a\langle R:A \rangle = \langle R:aA \rangle \subseteq (R:SA) \subseteq (R:S) \subseteq S,$$

which proves $SS \subseteq S$. If, in addition, $A = \{1\}$ then $S = 1S \subseteq SS$, and the theorem follows.

In subsequent sections we shall focus attention on a very restricted class of sets $\langle R:A \rangle$ where R denotes a finite set of finitary linear operations on P, and $A \subseteq P$. Section 2 deals mainly with sets of the form

(13) $\langle mx + n_i (i \in [1,k]) : a \rangle$,

where $a,k,m,n_1,\ldots,n_k \in P$. These are sets generated by unary linear operations on P . In Section 3 we study the sets $\langle mx+ny:1\rangle$ with $m,n \in P$. The cases $(m,n) = 1$ and $(m,n) > 1$ differ significantly and are treated separately; most of our results relate to the case $(m,n) = 1$.

2. Sets generated by unary linear operations

A unary linear operation on P is a function of the form $\rho(x) = mx+n$ with $m \in P$ and $n \in N$. Throughout this section we deal exclusively with sets $(R:A)$ where $A \subseteq P$ and R is a set of unary linear operations on P , finite except possibly in Theorem 8. We may suppose, without loss of generality, that R does not contain the identity operation. If R contains an element $x+d$ with $d \in P$ then $\langle R:A\rangle$ is a per-set. We note that for unary operations

(1) $$\langle R:A\rangle = \bigcup_{a \in A} (R:a) .$$

Hence, it is natural to focus attention on the case when A contains exactly one element. The problem treated in this section is to find a satisfactory arithmetic characterization of the elements of a set of the form

(2) $\langle m_i x + n_i (i \in [1,k]) : a \rangle$,

where $k,a,m_i-1 \in P$ and $n_i \in N$ for $i \in [1,k]$. The case k = 1 in (2) is particularly easy. We have to consider the set $\langle mx+n:a \rangle$ with $m-1 \in P$; $n \in N$; $a \in P$. Using the construction given in Theorem 2 we find

$$\langle mx+n:a \rangle = \{a, am+n, am^2+n(m+1), \ldots\}$$

$$= \{am^t + n(m^t-1)/(m-1) : t \in N\} \ .$$

Thus, the set $\langle mx+n:a \rangle$ has the form $G-T$, where G is a geometric progression with positive rational terms, and τ is a positive rational number. This procedure can be carried out for arbitrary k in (2) and shows that--the elements of (2) are precisely the numbers of the form

$$(3) \qquad \begin{cases} \nu_1 + \mu_1(\nu_2 + \mu_2(\ldots + \mu_{t-1}(\nu_t + \mu_t a)\ldots)) \\ \\ = \nu_1 + \mu_1\nu_2 + \mu_1\mu_2\nu_3 + \ldots + \mu_1\ldots\mu_{t-1}\nu_t + \mu_1\ldots\mu_t a \ , \end{cases}$$

where $t \in N$; $\mu i = m_{\lambda(i)}$; $\nu_i = n_{\lambda(i)}$; $\lambda(1),\ldots,\lambda(t) \in [1,k]$. This characterization, though not very satisfactory in itself, is often a step towards something better. For example, the next theorem is an immediate consequence of (3).

THEOREM 6. Let $a,d,k,m \in P$ and $b \in N$. Then

$$(4) \qquad \begin{cases} \langle mx + b + id(i \in [0,k-1]) : a \rangle \\ \\ = \bigcup_{t \in N} (b(m^0 + \ldots + m^{t-1}) + am^t + d\sum_{i=0}^{k-1} m^i[0,k-1]) \ . \end{cases}$$

Proof. The set corresponding to t = 0 on the right of (4) is to be interpreted as {a} . Let $t \in P$. In (3) put $\mu_1 = \ldots = \mu_t = m$. We

note that each ν_i ranges over the set $b+d[0,k-1]$. Thus, in our case all the numbers of the form (3) comprise the set

$$am^t + \sum_{i=0}^{t-1} m^i(b+d[0,k-1])$$
$$= b(m^0 + \ldots + m^{t-1}) + am^t + d\sum_{i=0}^{t-1} m^i[0,k-1] \ ,$$

for each $t\in N$. This establishes (4) .

We can derive an interesting corollary from this theorem with the help of the following lemma which deals with representation of numbers in the m-ary number system.

Lemma 3. Let $k,m,t\in P$ and $k \geq m$. Then

$$(5) \qquad \sum_{i=0}^{t-1} m^i[0,k-1] = [0,(k-1)(m^0 + \ldots + m^{t-1})] \ .$$

Proof. Let $j\in[1,(k-1)(m^0 + \ldots + m^{t-1})]$ and suppose that

$$j-1 = a_0m^0 + \ldots + a_{t-1}m^{t-1} \ ,$$

where $a_0, \ldots, a_{t-1} \in [0,k-1]$. Then there is a number $s = \min\{i: a_i < k-1\}$, and we have

$$j-1 = (k-1)(m^0 + \ldots + m^{s-1}) + a_sm^s + \ldots + a_{t-1}m^{t-1} \ ,$$

where $a_s < k-1$. Then

$$j = ((k-1)+(1-m))(m^0 + \ldots + m^{s-1}) + (a_s+1)m^s + \sum_{s<i<t} a_im^i \ .$$

Since $k-m, a_s+1 \in [0,k-1]$ this proves, by induction, that the left hand side of (5) is contained in the right hand side. The opposite inclusion holds trivially.

Corollary of Theorem 6. If $k \geq m \geq 2$ in Theorem 6, then

$$(6) \qquad \begin{cases} \langle mx + b + id(i\epsilon[0,k-1]) : a) \\ = \bigcup_{t\epsilon N} \left(am^t + b\left(\frac{m^t-1}{m-1}\right) + d[0,(k-1)\ \frac{(m^t-1)}{(m-1)}\ ]\right) \end{cases} .$$

Proof. Use Lemma 3 to re-write the sum $\sum(i\epsilon[0,t-1])$ in (4), and (6) is the result. For a future application we note that (6) remains true if $a = 0$.

Cur next result shows that if in Theorem 6 the number k is sufficiently large with respect to given values of a,b,d,m , then the set (6) is a near per-set, and under certain conditions even a per-set.

THEOREM 7. Let $a,d,m-1 \epsilon P$ and $b\epsilon N$. Then there exists a number $\kappa = \kappa(a,b,d,m)$ such that whenever $k \geq \kappa$ then the set

$$S = \langle mx + b + id(i\epsilon[0,k-1]) : a\rangle$$

is a near per-set. Furthermore, if d divides the number $(am+b-a)(m^t-1)/(m-1)$ for some $t\epsilon P$ then S is a per-set. Finally,

$$(7) \qquad \kappa(a,b,d,m) \leq 2 + (am + b - a)(m^d-1)/d \ .$$

Proof. Define, for $t\epsilon N$,

$$(8) \qquad \alpha(t) = b(m^0 + \ldots + m^{t-1}) + am^t \ .$$

It follows that

$$(9) \qquad \alpha(t+1) = m\alpha(t) + b$$

for $t\epsilon N$. Since the sequence $(a(t): t\epsilon N)$ satisfies a linear recurrence

relation it is eventually periodic modulo d ; moreover, if d divides $\alpha(t)-\alpha(0)$ for some $t\epsilon P$, the sequence is periodic modulo d . More precisely, there are numbers q,r such that $q\epsilon N$; $r\epsilon[1,d]$,

$$\alpha(t+r) \equiv \alpha(t) (\mathrm{mod}\ d) \tag{10}$$

for all $t \geq q$, and if d divides the number

$$\alpha(t) - \alpha(0) = (am + b - a)(m^t - 1) / (m-1)$$

for some $t\epsilon P$, then $q = 0$.

Now let--us suppose $k \geq m$ and use the Corollary of Theorem 6. We find that

$$\begin{cases} S = \bigcup_{t=0}^{q-1} (\alpha(t) + d[0,\ (k-1)(m^t-1) / (m-1)] \\ \bigcup_{t=q}^{q+r-1} \bigcup_{j\epsilon N} (\alpha(t+rj) + d[0,\ (k-1)(m^{t+rj}-1) / (m-1)]) \end{cases} \tag{11}$$

Now choose a fixed $t\epsilon[q,q+r-1]$ and consider the set

$$\bigcup_{j\epsilon N} (\alpha(t+rj) + d[0,(k-1)(m^{t+rj}-1) / (m-1)]) , \tag{12}$$

which, as we know, is a subset of $\alpha(t) + dN$. In fact, the set corresponding to a fixed j in (12) is a block of consecutive elements of the arithmetic progression $\alpha(t) + dN$. We want to show that the set (12) is almost equal to $\alpha(t) + dN$, i.e., that neighboring blocks in (12) abut or overlap for all large values of j . To achieve this it suffices to make k so large that

$$\alpha(t+rj) + d(k-1)(m^{t+rj}-1) / (m-1) \geq \alpha(t + rj + r) - d \tag{13}$$

for all large j . But (13) is equivalent to a condition of the form

$$k \geq 1 + (am + b - a)(m^r - 1)/d + \delta_j \ , \tag{14}$$

where $\delta_j \to 0$ as $j \to \infty$. Thus, if j is sufficiently large, the right hand side of (14) is less than

$$2 + (am + b - a)(m^d - 1)/d = \kappa' \ ,$$

say. Hence, if $k \geq \kappa'$, and $t \in [q, q+r-1]$ then the set (12) is contained in, and almost equal to, $a(t) + dN$. By combining this result with (11) we obtain

$$S \doteq \bigcup_{t=q}^{q+r-1} (\alpha(t) + dN) \ . \tag{15}$$

If d divides $a(t) - \alpha(0)$ for some $t \in P$, so that $q = 0$, then S is actually contained in the set on the right of (15), because in this case the set $\cup (t \in [0, q-1])$ on the right of (11) is the empty set. Hence we conclude that S is a near per-set provided $k \geq \kappa'$, and a per-set if $k \geq \kappa'$ and if d divides $\alpha(t) - \alpha(0)$ for some $t \in P$. This completes the proof, except that we still have to show that $k \geq \kappa'$ implies the condition $k \geq m$ which we imposed just before (17). In fact we have, since $m^d > 2^d \geq d+1$,

$$\kappa' = 2 + (a(m-1)+b)(m^d - 1)d^{-1}$$

$$\geq 2 + (1(m-1)+0)((d+1)-1)d^{-1} = m+1 > m$$

which completes the proof of Theorem 7.

By using (1) and (6) one can obtain results similar to Theorem 7 concerning sets of the form

$$\langle mx + b_i (i\epsilon[1,k]) : A\}$$

with A and $\{b_1, \ldots, b_k\}$ finite arithmetic progressions. So far, we have not found any other class of sets of the form

$$\langle m_i x + n_i (i\epsilon[1,k]) : A)$$

which have a simple or interesting arithmetic structure. For example, we have studied the set

$$S = \langle 2x+1, 3x+1 : 1 \rangle$$

which seems to be fairly complicated.

P. Erdös has kindly communicated to us the essentials of a result which shows that for certain sets R of unary linear operations and certain sets A the set $\langle R:A \rangle$ has density zero and is therefore neither a per-set nor a near per-set. This applies, *for instance, to* $\langle 2x+1, 3x+1 : 1 \rangle$.

THEOREM 8. Let $\emptyset c A, I \subseteq P$; $m_i \epsilon P$; $n_i \epsilon N$ for $i\epsilon I$. Let σ be a positive real number such that $\sum (i\epsilon I) m_i^{-\sigma} < 1$. Then, if $S = \langle m_i x + n_i (i\epsilon I) : A \rangle$, we have, for all $t\epsilon N$,

$$|[1,t] \cap S| \leq (1 - \sum m_i^{-\sigma})^{-1} \sum (a\epsilon[1,t) \cap A)(t/a)^{\sigma} .$$

Corollary of Theorem 8. If, in addition, $\sigma < 1$ and if either the set A is finite, or A is infinite and the series $\sum (a\epsilon A) a^{-\sigma}$ converges, then the set S has density zero and is neither a per-set nor a near per-set. This applies, for instance, to the set $\langle 2x+1, 3x+1 : A \rangle$ whenever $\sum (a\epsilon A) a^{-\tau} < \infty$ for some $\tau < 1$.

Proof. t $(i\epsilon I)m_i^{-\sigma} = 1-\delta$, so that $0 < \delta < 1$. For $t\epsilon N$ denote by L(t) the set of all mappings $\lambda:[1,r] \to I$ with some unspecified $r\epsilon N$, such that $m_{\lambda(1)}m_{\lambda(2)}\cdots m_{\lambda(r)} \leq t$. We now prove that, for all $t\epsilon N$,

(16) $\quad |L(t)| \leq t^{\sigma}/\delta$.

Clearly, (16) holds for $t = 0$. Let $t\epsilon P$ and use induction with respect to t . Then, by noting that L(t) has exactly one element with $r = 0$, and by giving to $\lambda(1)$ in turn each of the possible values, we find that

$$|L(t)| = 1 + \sum |L([t/m_i])| \leq 1 + \sum \delta^{-1}[t/m_i]^{\sigma}$$

$$\leq 1 + \delta^{-1}t^{\sigma}(1-\delta) = \delta^{-1}t^{\sigma} - (t^{\sigma}-1) < \delta^{-1}t^{\sigma} \ ,$$

where [x] denotes the greatest integer not exceeding x . This proves (16) for all $t\epsilon N$. Let $a\epsilon A$ and $t\epsilon N$ and put

$$S_a(t) = [1,t] \cap \langle m_i x + n_i (i\epsilon I) : a \rangle$$

Let $y\epsilon S_a(t)$. Then we can choose $r\epsilon N$ and a mapping $\lambda:[1,r] \to I$ such that

$$t \geq y = n_{\lambda(1)} + m_{\lambda(1)}(n_{\lambda(2)} + m_{\lambda(2)}(n_{\lambda(3)} + \cdots + n_{\lambda(r-1)}(n_{\lambda(r)} + m_{\lambda(r)}a)\cdots))$$

$$\geq m_{\lambda(1)}m_{\lambda(2)}\cdots m_{\lambda(r)}a \ .$$

Hence $\lambda\epsilon L([t/a])$. Put $\varphi(y) = \lambda$. Then $\varphi:S_a(t) \to L([t/a])$ is an injection, and therefore

$$|S_a(t)| \leq |L([t/a])| \ .$$

Now, using (16) we find that, with $A_t = [1,t] \cap A$,

$$|[1,t] \cap S| \leq \sum(a \epsilon A_t) |S_a(t)|$$

$$\leq \sum(a \epsilon A_t) |L([t/a])| \leq \sum(a \epsilon A_t) \delta^{-1} [t/a]^{\sigma}$$

$$\leq \delta^{-1} \sum(a \epsilon A_t) (t/a)^{\sigma}$$

which was to be proved.

3. Sets Generated by One Linear Operation

If linear operations ρ and τ are related, then one might expect the sets $\langle\rho:a\rangle$ and $\langle\tau:b\rangle$ to -be arithmetically related. The first results proved in this section are of this type. We show in Theorem 9 under fairly general conditions that the set $\langle m_0+m_1x_1+\ldots+m_rx_r:a\rangle$ is an affine transformation of the set $(m_1x_1+\ldots+m_rx_r:1\rangle$. Using Theorem 9, we show in Theorem 10 that if ρ and τ are linear operations and $\langle\rho(\bar{x}):1\rangle$ is a per-set, then $\langle\rho(\bar{x})+\tau(\bar{y}):1\rangle$ is also a per-set. All of the results proved in this section were motivated by attempts to prove the following conjecture.

Conjecture 1. Suppose $r\text{-}1,m_1,\ldots,m_r\epsilon P$, and $(m_1,\ldots,m_r)=1$. Then $\langle m_1x_1+\ldots+m_rx_r:1\rangle$ is a per-set.

If $r\text{-}2,m_1,\ldots,m_r\epsilon P$, $(m_1,\ldots,m_{r\ 1})=1$, and $\langle m_1x_1+\ldots+m_{r-1}x_{r-1}:1\rangle$ is a per-set, then it follows from Theorem 10 that $\langle m_1x_1+\ldots+m_rx_r:1\rangle$ is also a per-set. Thus, to test Conjecture 1 it is only necessary to consider r-sets $(r\geq 2)$ of relatively prime numbers having no proper subset of relatively prime numbers. The following conjecture is weaker than Conjecture 1.

Conjecture la. Suppose $r\text{-}1,m_1,\ldots,m_r\epsilon P$ with $(m_1,\ldots,m_r)=1$. Then $\langle m_0+m_1x_1+\ldots+m_rx_r+n_1y_1+\ldots+n_sy_s:a\rangle$ is a per-set for all $m_0,n_1,\ldots,n_s\epsilon N$ and $a\epsilon P$.

Most of our efforts to prove Conjecture 1 have been concentrated on trying to show that $\langle mx+ny:1\rangle$ is a per-set whenever $(m,n)=1$. For example, we have succeeded in showing (Theorem 11) that $\langle 2x+ny:1\rangle$ is a per-set for all odd numbers n .

It would be interesting to know whether the set $\langle mx+ny:1\rangle$ contains an infinite arithmetic progression for all $m,n\epsilon P$. In fact, a proof along the lines of the proof of Theorem 4 can be given that if $a,d,r-1,m_1,\ldots,m_r\epsilon P$ with $(a,d) = (m_1,\ldots,m_r) = 1$, and $a+dN \subseteq \langle m_1x_1+\ldots+m_1x_r:1\rangle = s$, then S is a per-set. This motivates a second conjecture.

Conjecture 2. The set $\langle mx+ny:1\rangle$ contains an infinite arithmetic progression for all $m,n\epsilon P$.

The truth of Conjecture 2 is not enough to prove Conjecture 1. In fact, R.--Graham has shown that $\langle 3x+3y:1\rangle$ is not a near per-set, but it is easy to prove that $36+45N$ is contained in this set. Evidence in favor of Conjecture 2 is given in Theorem 12 in which it is shown that $\langle mx+ny:1\rangle$ contains arbitrarily long arithmetic progressions for all $m,n\epsilon P$. This is an interesting result because it can be shown in a way similar to that used in the proof of Theorem 7 that if $(m,n) = 1$, and $\langle mx+ny:1\rangle$ contains a sufficiently long arithmetic progression, then $\langle mx+ny:1\rangle$ is a per-set. The sufficiency of the length of the progression depends on m , n , the size of the initial term, and the common difference of the terms of the progression. Now we present our results.

In order to exhibit the essentially very simple idea behind our next result we temporarily abandon our restriction to linear operations on P and readmit general operations on J . We also introduce the convention that if $\underline{x}$ denotes a vector of any dimension, with components $x_i\epsilon J$, then $\underline{x}-t$ denotes the vector with components x_i-t . In what

follows vectors x , $\underline{y}$, $\underline{z}$, w are assumed to have the appropriate dimensions.

Theorem 9. Let I be a set and let, for each $i\in I$, $\rho_i(\underline{x})$ and $\sigma_i(\underline{x})$ be r_i-ary operations on J . Let $\alpha,\beta\in J\setminus\{0\}$; $\alpha',\beta'\in J$; $A,B\subseteq J$. Then

$$(1)\qquad \alpha\langle\rho_i(\underline{x})(i\in I):A\rangle + \alpha' = \beta\langle\sigma_i(x)(i\in I):B\rangle + \beta'$$

provided that

$$(2)\qquad \alpha A + \alpha' = \beta B + \beta'$$

and, for each $i\in I$ and each w over J ,

$$(3)\qquad \alpha\rho_i\left(\frac{1}{\alpha}(\underline{w}-\alpha')\right) + \alpha' = \beta\sigma_i\left(\frac{1}{\beta}(\underline{w}-\beta')\right) + \beta' \quad .$$

Proof. Put

$$S = \langle\sigma_i(\underline{x})(i\in I):B\rangle \ .$$

On account of symmetry it suffices to prove that the left hand side of (1) is contained in the right hand side of (1), that is, that

$$\langle\rho_i(\underline{x})(i\in I):A\rangle \subseteq R \ ,$$

where

$$R = \frac{\beta}{\alpha} S + \frac{\beta'-\alpha'}{\alpha} \quad .$$

First of all we have, by (2),

$$R \supseteq \frac{\beta}{\alpha} B + \frac{\beta'-\alpha'}{\alpha} = A \ .$$

Next, if $\underline{z}$ is a vector over R then αz lies over $\beta S+\beta'-\alpha'$ and $\frac{1}{\beta}(\alpha\underline{z}+\alpha'-\beta')$ lies over S . Hence, for every $i\in I$, $\sigma_i\left(\frac{1}{\beta}(\alpha\underline{z}+\alpha'-\beta')\right)\in S$, so that

$$\frac{\beta}{\alpha}\,\sigma_i\left(\frac{1}{\beta}(\alpha z+\alpha'-\beta')\right)+\frac{\beta'-\alpha'}{\alpha}\in R\ .$$

Put $\alpha z+\alpha' = w$. Then

$$\frac{1}{\alpha}\left(\beta\sigma_i\left(\frac{1}{\beta}(w-\beta')\right)+\beta'\right)-\frac{\alpha'}{\alpha}\in R\ .$$

By (3), this yields

$$\frac{1}{\alpha}\left(\alpha\rho_i\left(\frac{1}{\alpha}(w-\alpha')\right)+\alpha'\right)-\frac{\alpha'}{\alpha}\in R\ ,$$

that is, $\rho_i(z)\in R$. Thus, R contains A and is closed under each ρ_i , which implies (1).

Corollary 1 of Theorem 9. Let $r,m_1,\ldots,m_r\in P$ with $m = m_1+\bullet\bullet\bullet >1$, and $a,b\in J$. Then

(5) $$(m-1)\langle b+m_1x_1+\bullet\bullet\bullet+m_rx_r:a\rangle+b = (b+am-a)\langle m_1x_1+\ldots+m_rx_r:1\rangle\ .$$

It is easily verified that the conditions (2) and (3) hold in the case presented by (5).

Corollary 2 of Theorem 9.

(6) $$(m-1)\langle 1+m_1x_1+\ldots+m_rx_r:0\rangle+1 = \langle m_1x_1+\ldots+m_rx_r:1\rangle\ .$$

This is the case $a=0$; $b=1$ of (5).

Corollary 3 of Theorem 9. The set $\langle m_1x_1+\ldots+m_rx_r:1\rangle$ is closed under multiplication for all $r,m_1,\ldots,m_r\in P$.

Proof. This result already follows from Theorem 5; however, if we put $b=0$ in (1), we get

$$\langle m_1x_1+\ldots+m_rx_r:a\rangle = a\langle m_1x_1+\ldots+m_rx_r:1\rangle$$

which is a key element in the proof of Theorem 5.

Theorem 10. If $m_1,\ldots,m_r \in P$ with $(m_1,\ldots,m_r) = 1$, and $S = \langle m_1x_1 + \ldots + m_rx_r : 1\rangle$ is a per-set, then $T = \langle m_1x_1 + \ldots + m_rx_r + n_1y_1 + \bullet$ o.?nsys+b:a) is a per-set for all $a,b,n_1,\bullet$,nseN .

Proof. First, note that if an affine transformation maps a per-set into a set of integers, then this set is also a per-set, Hence, it follows that the set

$$Q = \langle m_1x_1 + \ldots + m_rx_r + (n_1 + \ldots + n_s)a + b : a\rangle$$

(which is an affine transformation of S according to Theorem 9) is a per-set. Furthermore, $a \in Q$ and $Q \subseteq T$, so

$$\langle m_1x_1 + \bullet \quad +mrxr+nlyl+\ldots+nsys+b:Q) = T .$$

But, since Q is a per-set, and $(m_1,\ldots,m_r) = (m_1,\ldots,m_r,n_1,\ldots,n_s) = 1$, Theorem 4 applies, and we can conclude that T is a per-set. This completes the proof.

A simple special case of the next result is crucial for the proof of Theorem 11. However, the reader is referred to [1] for a proof of a more general result.

Lemma 4. Suppose $m_1,m_2 \in P$ with $(m_1,m_2) = 1$, and let u_1, v_1, u_2, v_2 denote integers such that $v_1-u_1 \geq m_2-1$ and $v_2-u_2 \geq m_1-1$. Then

$$(7) \qquad [m_1u_1 + m_2u_2 + (m_1-1)(m_2-1), m_1v_1 + m_2v_2 - (m_1-1)(m_2-1)] \subseteq m_1[u_1,v_1] + m_2[u_2,v_2] .$$

Theorem 11. If n is odd and $n \in P$, then $\langle 2x + ny : 1\rangle$ is a per-set. Also,

(8) $$\langle 2x+ny:1\rangle \doteq \bigcup_{i=0}^{r-1} (2^i n + 2^i - n + (n^2+n)\mathbb{N}) \ ,$$

where r denotes the order of 2 modulo n, and the symbol $\doteq$ was defined in Section 1.

Proof. Using the First Corollary of Theorem 9, we have

(9) $$\langle 2x+ny:1\rangle = 1 + (n+1)\langle 2x+ny+1:0\rangle \ .$$

From now on we work with the set $T = \langle 2x+ny+1:0\rangle$; also, let

$$S = \bigcup_{i=0}^{r-1} (2^i - 1 + n\mathbb{N}) \ ,$$

where r denotes the order of 2 modulo n . Note that

$$2(2^u - 1 + n\mathbb{N}) + n(2^v - 1 + n\mathbb{N}) + 1 \subset 2^{u+1} - 1 + n\mathbb{N}$$

for all $u,v \in \{0,\ldots,r-1\}$. It follows that S is closed under the operation $2x+ny+1$; furthermore, $0 \in S$, so

(10) $$\langle 2x+ny+1:0\rangle = T \subseteq S \ .$$

Now we show that $T \doteq S$. Since $0,1 \in T$, we have $(2T+1)\cup(2T+n+1)\cup\{0\} \subseteq T$; hence,

(11) $$R = \langle 2x+1, 2x+n+1:0\rangle \subseteq T$$

The Corollary of Theorem 6 with $a = 0$ implies

$$R = \bigcup_{t=0}^{\infty} (2^t - 1 + n[0,2^t-1]) = \bigcup_{i=0}^{r-1} \bigcup_{t=0}^{\infty} (2^{rt+i} - 1 + n[0,2^{rt+i} - 1]) \ .$$

Since $R \subseteq T$, we have

(12) $$T \supseteq 1 + 2(2^{2r-1} - 1 + n[0,2^{2r-1} - 1]) + nR$$

$$= 2^{2r} - 1 + n\Big(\bigcup_{t=0}^{\infty} \bigcup_{i=0}^{r-1} (2^{rt+i} - 1 + 2[0,2^{2r-1} - 1] + n[0,2^{rt+i} - 1])\Big) \ .$$

But n divides 2^r-1, so $|[0,2^{2r-1}-1] > n$; also, $(2,n) = 1$. Thus, Lemma 4 applies to the linear combination of intervals which appears on the right in (12), so we can conclude that

$$T \supseteq 2^{2r} - 1 + n\Big(\bigcup_{t\in N} \bigcup_{i=0}^{r-1} (2^{rt+i} - 1 + [n-1, 2^{2r} + n2^{rt+i} - 2n - 1])\Big) \tag{13}$$

$$= 2^{2r} - 1 + n \bigcup_{t\in N} \bigcup_{i=0}^{r-1} [a_{ti}, b_{ti}] \ ,$$

where $a_{ti} = 2^{rt+i} + n - 2$; $b_{ti} = (n+1)2^{rt+i} + 2^{2r} - 2n - 2$. Let t be fixed, $t\in N$. The union of the r intervals $[a_{ti}, b_{ti}]$ will form a single interval of integers provided that $a_{t,i+1} \le b_{ti}+1$ for every $i\in[0,r-2]$. Now we have for $i\in N$, since $2^r-1 > n$,

$$b_{ti} + 1 - a_{t,i+1} = (n+1)2^{rt+i} + 2^{2r} - 2n - 2 + 1 - 2^{rt+i+1} - n + 2 \tag{14}$$

$$= (n-1)2^{rt+i} + 2^{2r} - 3n + 1 \ge (n-1) + (n+1)^2 - 3n + 1 = n^2 + 1 > 0 \ .$$

Thus (13) yields

$$T \supseteq 2^{2r} - 1 + n \bigcup_{t\in N} [a_{t0}, b_{t,r-1}] \ .$$

Again, this last union constitutes a single interval since we have

$$b_{t,r-1} + 1 - a_{t+1,0} = (n+1)2^{rt+r-1} + 2^{2r} - 2n - 2 + 1 - 2^{rt+r} - n + 2 \tag{15}$$

$$= (n-1)2^{rt+r-1} + 2^{2r} - 3n + 1 > (n-1)2^{r-1} + 2^{2r} - 3n + 1$$

$$\ge (n-1)\cdot\tfrac{1}{2}(n+1) + (n+1)^2 - 3n + 1 = \tfrac{3}{2}\left(n - \tfrac{1}{3}\right)^2 + \tfrac{4}{3} > 0 \ .$$

Thus, finally,

$$T \supseteq 2^{2r} - 1 + n(a_{00} + N) \ , \tag{16}$$

so that

(17) $nN \subseteq T$.

Now we show

(18) $2^i - 1 + nN \subset T$

for $i = 0,\ldots,r-1$ by induction on i ; in fact, we have the case $i = 0$ in (17). Suppose (18) holds for some $i \geq 0$. Then

$$T \supseteq 1 + 2(2^i - 1 + nN) + n(nN)$$

$$= 2^{i+1} - 1 + n(2N + nN) \doteq 2^{i+1} - 1 + nN \ .$$

Here we have implicitly used Lemma 5 which we will state and prove at the conclusion of this proof. Hence, (18) holds also for $i+1$, and this means (18) holds for $i = 0,\ldots,r-1$. It follows that

(19) $$S = \bigcup_{i=0}^{r-1} (2^i - 1 + nN) \subset T \ ,$$

and this together with (10) implies $S \doteq T$. This result together with (9) implies (8) . It remains to prove the following lemma.

Lemma Suppose $m_1, \ldots, m_k$, k-$1 \epsilon P$ with $(m_1, \ldots, m_k) = 1$, let $S = (m_1 x_1 + \ldots + m_k x_k : 1)$, and let $A_1,\ldots,A_k$ denote per-sets such that $A_i \subseteq S$ for $i = 1,\ldots,k$. Then

(20) $m_1 A_1 + \ldots + m_k A_k \subseteq S$.

Proof. It is enough to prove this for per-sets $A_1,\ldots,A_k$ having the special form $A_i = a_i + dN$ with a_i , $d \epsilon P$ for $i = 1,\ldots,k$. Suppose N_i is maximal with $N_i \subset N$ such that $a_i + dN_i \subseteq S$, then since $A_i \subseteq S_1$ we have $N_i \subseteq N$. Because S is closed under the operation

$m_1x_1 + \ldots + m_kx_k$, and $a_i + dN_i \subseteq S$, we have

$$(21) \qquad \sum_{i=1}^{k} m_i(a_i + dN_i) \subseteq S \ .$$

Now, using the fact that $N \doteq N_i$ for $i = 1,\ldots,k$, note that

$$(22) \qquad N \doteq \sum_{1-1}^{k} m_iN \subseteq \sum_{i=1}^{k} m_iN_i \doteq \ .$$

Hence,

$$(23) \qquad \sum_{i=1}^{k} m_iA._1 = \sum_{i=1}^{k} m_ia_i + d \sum_{i=1}^{k} m_iN$$

$$\subseteq \sum_{i=1}^{k} m_ia_i + d \sum_{i=1}^{k} m_iN_i = \sum_{i=1}^{k} m_i(a_i + dN_i) \ ,$$

and this together with (11) implies (20). The proof is complete.

Theorem 12. If $r\text{-}1,m_1,\ldots,m_r \in P$, then $\langle m_1x_1 + \ldots + m_rx_r:1\rangle$ contains an arithmetic progression with k terms for all $k \in P$.

Proof. The set $\langle m_1x_1 + \ldots + m_rx_r:1\rangle$ contains the set $\langle m_1x_1 + m_2x_2 + m_3 + \ldots + m_r:1\rangle$ which is an affine transformation of the set $\langle m_1x_1 + m_2x_2:1\rangle$. Thus, if $\langle m_1x_1 + m_2x_2:1\rangle$ contains an arithmetic progression of length k for all $k \in P$, then this is also true for the set $\langle m_1x_1 + \ldots + m_rx_r:1\rangle$. However, it is easy to show by induction that

$$(24) \qquad (m+n)^{u+v} + (m+n-1)m^un^v[0,\binom{u+v}{v}] \subset \langle mx + ny:1\rangle$$

for all $u,v \in N$, so the proof is complete.

References

[1] D. A. Klarner and R. Rado, "Linear combinations of sets of consecutive integers," to appear.

[2] A. G. Kurosh, General Algebra, Chelsea, 1963.