PACIFIC JOURNAL OF MATHEMATICS
Vol. 83, No. 1, 1979

SETS OF INTEGERS CLOSED UNDER AFFINE OPERATORS-THE FINITE BASIS THEOREMS

D. G. HOFFMAN AND D. A. KLARNER

This paper is a continuation of investigations of sets T of integers closed under operations f of the form $f(x_1, \cdots, x_r) = m_1x_1 + \cdots + m_rx_r + c$, where $r, m_1, \cdots, m_r, c$ are integers satisfying $r \geqq 2$, $0 \notin \{m_1, \cdots, m_r\}$, and $\gcd(m_1, \cdots, m_r) = 1$. We have two goals here:

(1) to prove that $T = \langle f \mid A \rangle$ for some finite set A, where $\langle f \mid A \rangle$ denotes the "smallest" set containing A and closed under f, and

(2) to show that unless $|T| = 1$, T is a finite union of infinite arithmetic progressions, either all bounded below, or all bounded above, or all doubly infinite.

We shall lean heavily on the notation, definitions, and results of [1].

DEFINITION 1. Let $r \in \boldsymbol{P}$. An *r-ary affine* operator f on $\boldsymbol{Z}$ is an operator of the form

$$f(x_1, \cdots, x_r) = m_1x_1 + \cdots + m_rx_r + c ,$$

where $m_1, \cdots, m_r \in \boldsymbol{Z}\backslash\{0\}$, and $c \in \boldsymbol{Z}$. Let $\sigma(f) = m_1 + \cdots + m_r$, let $\rho(f) = r$.

We call f a *positive* operator if each $m_i \in \boldsymbol{P}$, a *prime* operator if $r \geqq 2$ and $\gcd(m_1, \cdots m_r) = 1$, and a *linear* operator if $c = 0$. Denote by $\mathscr{P}$ the set of all positive, prime, linear operators, and by $\mathscr{H}$ the set of all prime linear operators that are not positive. For each $f \in \mathscr{P}$, $\langle f + 1 \mid 0 \rangle$ is a periodic set by Theorem 12 of [1]; let $\delta(f)$ be its smallest eventual period.

LEMMA 1. *Let $f \in \mathscr{P}$, let $a, s, t \in \boldsymbol{Z}$, with $(\sigma(f)-1)a + s \in \boldsymbol{N}$, and $(\sigma(f)-1)a + t \in \boldsymbol{P}$. Then $T = \langle f + \{s, t\} \mid a \rangle$ has an eventual period $\delta(f)\gcd(t - s, (\sigma(f)-1)a + t) = \delta(f)\gcd((\sigma(f)-1)a + s, (\sigma(f)-1)a + t)$.*

Proof. Define a sequence $(T_n \mid n \in \boldsymbol{P})$ of subsets of $\boldsymbol{Z}$ as follows: let $T_1 = \langle f + t \mid a \rangle$, and for $k \in \boldsymbol{P}$, let $T_{2k} = \langle f + s \mid T_{2k-1} \rangle$ and $T_{2k+1} = \langle f + t \mid T_{2k} \rangle$. Then certainly each T_n has an eventual period $\delta(f)((\sigma(f)-1)a + t)$, and further $T = \bigcup_{n \in P} T_n$. Thus T has an eventual period $\delta(f)((\sigma(f)-1)a + t)$. If $(\sigma(f)-1)a + s = 0$, we are done. Otherwise, we may interchange the roles of s and t in the argument above to conclude that T also has an eventual period of $\delta(f)((\sigma(f)-1)a + s)$.

THEOREM 1. *Let $f \in \mathscr{P}$. Then there exists $v \in \boldsymbol{P}$ such that for all $a \in \boldsymbol{N}$, $b \in \boldsymbol{P}$, $T = \langle f \mid a, b \rangle$ has an eventual period $v \cdot \gcd(a, b)$.*

Proof. We may assume $\gcd(a, b) = 1$. If $f(x_1, \cdots, x_r) = m_1x_1 + \cdots + m_rx_r$, then T is closed under the two operators $g + k\{a, b\}$, where $g(x_1, \cdots, x_r) = m_1^2x_1 + m_2x_2 + \cdots + m_rx_r$, and $k = m_1(m_2 + \cdots + m_r)$. Let $v = \delta(g)k(\sigma(g) - 1 + k)$. By Lemma 1, the set $T_a = \langle g + k\{a, b\} \mid a \rangle$ has an eventual period $\delta(g)\gcd(k(b - a), (\sigma(g) - 1 + k)a)$, which divides v. Similarly, $T_b = \langle g + k\{a, b\} \mid b \rangle$ has an eventual period v, thus $T = \langle f \mid T_a \cup T_b \rangle$ does also.

DEFINITION 2. For each $f \in \mathscr{P}$, we denote by $\nu(f)$ the smallest positive integer such that for all $a \in \boldsymbol{N}$, $b \in \boldsymbol{P}$, $\langle f \mid a, b \rangle$ has an eventual period $\nu(f)(\sigma(f) - 1)\gcd(a, b)$.

Theorem 12 of [1] considered sets $\langle f + c \mid A \rangle$, where $(\sigma(f) - 1)A + c \subseteqq \boldsymbol{P}$. We remark that Theorem 1 above can be used to extend Theorem 12 of [1] to the case $\{0\} \neq (\sigma(f) - 1)A + c \subseteqq \boldsymbol{N}$.

THEOREM 2. *Let $f \in \mathscr{P}$, let $c \in \boldsymbol{Z}$, let $A \subseteqq \boldsymbol{Z}$, with $\{0\} \neq (\sigma(f) - 1)A + c \subseteqq \boldsymbol{N}$. Then $\langle f + c \mid A \rangle$ is a periodic set with an eventual period $\nu(f)\gcd((\sigma(f) - 1)A + c)$.*

Proof. By Theorem 1 of [1], we may assume $c = 0$. Let $a \in A \cap \boldsymbol{P}$. For each $b \in \boldsymbol{N}$, $T_b = \langle f \mid a, b \rangle$ has an eventual period $\nu(f)(\sigma(f) - 1)\gcd(a, b)$, thus $T = \bigcup_{b \in A} T_b$ has an eventual period $\nu(f)(\sigma(f) - 1)a$, and so does $\langle f + c \mid A \rangle = \langle f + c \mid T \rangle$.

LEMMA 2. *Let f be a prime operator, let $t \in \boldsymbol{Z}$. Then there is a positive, prime operator g such that for any $T \subseteqq \boldsymbol{Z}$ with $t \in T$, if T is closed under f, then T is closed under g.*

Proof. If f is the operator $m_1x_1 + \cdots + m_rx_r + c$, then let $g = m_1^2x_1 + \cdots + m_r^2x_r + 2t\sum_{i<j} m_im_j + (\sigma(f) + 1)c$.

THEOREM 3. *Let $A \subseteqq Z$, let f be a prime operator. Then $\langle f \mid A \rangle = \langle f \mid B \rangle$ for some finite subset $B \subseteqq A$.*

Proof. Let $t \in A$, produce g as in Lemma 2. Let $\alpha = g(0)/(1 - \sigma(g))$, let $P = \{n \in Z \mid n \geqq \alpha\}$. By Theorem 12 of [1], and its extension noted above, there are finite sets B_1 and B_2 such that $\langle f \mid A \rangle \cap P = \langle g \mid B_1 \rangle$ and $(-\langle f \mid A \rangle) \cap P = \langle g \mid B_2 \rangle$. But then $\langle f \mid A \rangle = \langle g \mid B_1 \cup (-B_2) \rangle$, and clearly $\langle f \mid B_1 \cup (-B_2) \cup \{t\} \rangle = \langle f \mid A \rangle$. Finally, we need only choose a finite $B \subseteqq A$ so that $B_1 \cup (-B_2) \cup \{t\} \subseteqq \langle f \mid B \rangle$.

With Theorem 3, we have achieved goal (1).

We now turn our attention to sets of residue classes in the ring $\boldsymbol{Z}_d$. We make the convention that any integer divides 0; hence $a \equiv b \pmod 0$ if and only if $a = b$, and $\gcd\phi = \gcd\{0\} = 0$. Further, if $d \in N$, and A, $B \subseteqq Z$, define $A \subseteqq B \pmod d$ if for all $a \in A$, there is some $b \in B$ with $a \equiv b \pmod d$, and $A \equiv B \pmod d$ if $A \subseteqq B \subseteqq A \pmod d$. Finally, define $\gamma(A) = \gcd(A - A)$; and if C is a set of residue classes, define $\gamma(C) = \gamma(\bigcup_{A \in C} A)$.

The following theorem is essentially Theorem 10 of [1].

THEOREM 4. *Let $d \in \boldsymbol{P}$, let f be a prime operator, let $A \subseteqq \boldsymbol{Z}$ with $f(A) \subseteqq A \pmod d$. Then $f(A) \equiv A \pmod d$.*

DEFINITION 3. Let R be a family of finitary operators on a set X, let $A \subseteqq X$. We denote by $[R, A]$ the following family of operators: let $f \in R$ be an r-ary operator, let K, L be a partition of $[1, r]$ with $K \neq \phi$, let τ: $L \to \langle R \mid A \rangle$; define a $|K|$-ary operator g on X as follows:

$$g(x_i \mid i \in K) = f(y_1, \cdots, y_r) ,$$

where

$$y_i = \begin{cases} x_i & \text{if } i \in K \\ \tau(i) & \text{if } i \in L . \end{cases}$$

Let $[R, A]$ be the set of all such operators g. Thus $T = \langle [R, A] \mid B \rangle$ is the smallest set containing B, and with the property that if f is an r-ary operator in R, and $x_1, x_2, \cdots, x_r \in \langle R \mid A \rangle \cup T$, and at least one $x_i \in T$, then $f(x_1, \cdots, x_r) \in T$. In particular, $\langle R|A \rangle \cup \langle [R, A]|B \rangle = \langle R \mid A \cup B \rangle$.

THEOREM 5. *Let $f \in \mathscr{P} \cup \mathscr{H}$, let $c \in \boldsymbol{Z}$, let $d \in \boldsymbol{P}$, let A, $B \subseteqq \boldsymbol{Z}$. Then, if $B \neq \phi$,*

$$\langle [f + c, A] \mid B \rangle \equiv \langle f + c \mid A \cup B \rangle \pmod d .$$

Proof. We need only show, for all a, $b \in \boldsymbol{Z}$, that $a \equiv a_1 \pmod d$ for some $a_1 \in \langle [f + c, a] \mid b \rangle$. We may further assume $f \in \mathscr{P}$, and $(\sigma(f) - 1)a + c$, $(\sigma(f) - 1)b + c \in P$. Let $s = d\nu(f)\gcd((\sigma(f) - 1)a + c, (\sigma(f) - 1)b + c)$, let $t = \delta(f)((\sigma(f) - 1)a + c)$, and suppose first $s < t$. By Theorem 2, $a + sN \subseteqq \langle f + c \mid a, b \rangle$. (Recall that for sets X and Y, $X \subseteqq Y$ means $X \backslash Y$ is finite, and $X \doteq Y$ means $X \subseteqq Y \subseteqq X$.) Thus we need only show

$$a + sN \cap \langle [f + c, a] \mid b \rangle \neq \phi .$$

But if the above intersection is empty, then $a + sN \subseteqq \langle f +$

$c|a\rangle = T$ and so T has an eventual period s by Theorem 4 of [3]. But T has smallest eventual period t, so t divides s, contradicting $s < t$.

In the general case, let $a' = a + kd((\sigma(f)-1)b + c)$, where $k \in \boldsymbol{P}$ is chosen so large that $\delta(f)((\sigma(f)-1)a' + c) > s$. Since

$$s = d\nu(f)\gcd((\sigma(f)-1)a' + c, (\sigma(f)-1)b + c) ,$$

the special case above shows $a' \equiv a_1 \pmod d$ for some $a_1 \in \langle [f+c, a'] \,|\, b\rangle$. But $a' \equiv a_1 \pmod d$.

The innocent Lemma 3 lead to the fundamental Theorem 3 on closed subsets of $\boldsymbol{Z}$. The following lemma, with analogous hypotheses, will lead to the fundamental Theorem 6 below on closed subsets of $\boldsymbol{Z}_d$, $d \in P$.

LEMMA 3. *Let $d \in \boldsymbol{P}$, let $a, b \in \boldsymbol{Z}$, let $A \subseteqq z$, let f be a prime operator with*

$$f(A) + \{a, b\} \subseteqq A \pmod d .$$

Then $A + (a - b) \equiv A \pmod d$.

Proof. By Theorem 4, $A - a \equiv f(A) \equiv A - b \pmod d$.

COROLLARY 1. *Let $d \in \boldsymbol{P}$, let f be a prime operator, let $A, B \subseteqq \boldsymbol{Z}$. If $f(A) + B \subseteqq A \pmod d$, then $A + \gamma(B) \equiv A \pmod d$.*

DEFINITION 4. If f is the r-ary affine operator $m_1x_1 + \cdots + m_rx_r + c$, let

$$\theta_1(f) = \gcd(m_1, \cdots, m_r) ,$$

and let

$$\theta_2(f) = \gcd(m_im_j \,|\, 1 \leqq i < j \leqq r) .$$

LEMMA 4. *Let f be a linear operator, let $A \subseteqq \boldsymbol{Z}$. Then $\gamma(f(A)) = \theta_1(f)\gamma(A)$.*

Proof. Certainly $\theta_1(f)\gamma(A)$ divides each element of $f(A) - f(A) = f(A - A)$; thus $\theta_1(f)\gamma(A)$ divides $\gamma(f(A))$.

For the converse, let f be the operator $m_1x_1 + \cdots + m_rx_r$; let $a, b \in A$, as we may suppose $A \neq \phi$.

Then, for each $1 \leqq i \leqq r$,

$$\begin{aligned} m_i(a - b) &= (m_1a + \cdots + m_ra) \\ &\quad - (m_1a + \cdots + m_{i-1}a + m_ib + m_{i+1}a + \cdots + m_ra) , \end{aligned}$$

so $m_i(a - b) \in f(A) - f(A)$. Thus $\gamma(f(A))$ divides each $m_i(a - b)$, and hence divides $\theta_1(f)(a-b)$. This holds for all $a, b \in A$, thus $\gamma(f(A))$ divides $\theta_1(f)\gamma(A)$.

THEOREM 6. *Let f be a prime operator, let $A \subseteqq \boldsymbol{Z}$, let $d \in \boldsymbol{P}$. If $f(A) \subseteqq A \pmod d$, then $A + \theta_2(f)\gamma(A) \equiv A \pmod d$.*

Proof. Let f be the r-ray operator $m_1x_1 + \cdots + x_rx_r + c$, let $R = [1, r]$. For each $K \subseteqq R$, with $K \neq \phi$, define an r-ary, linear prime operator f_K, a $|K|(r-1)$-ary linear operator g_K, and an integer c_K as follows:

$$f_K(x_1, \cdots, x_r) = \sum_{i \in K} m_i^2 x_i + \sum_{i \in R \setminus K} m_i x_i ,$$

$$g_K(x_{i,j} \mid i \in K,\, j \in R,\, i \neq j) = \sum_{\substack{i \in K \\ j \in R \\ i \neq j}} m_i m_j x_{i,j} ,$$

$$c_K = c\left(1 + \sum_{i \in K} m_i\right) .$$

Thus any set closed under f is closed under the $r + |K|(r-1)$-ary operator $f_K + g_K + c_K$, so $A \subseteqq \langle f_K + g_K(A) + c_K \mid A \rangle \subseteqq \langle f + c \mid A \rangle$. By Lemmas 3 and 4, and by Theorem 2 of [1], (we may assume the hypotheses there apply), $A + \theta_1(g_K)\gamma(A) \equiv A \pmod d$. As this holds for all $K \neq \phi$, the theorem is proved, since $\gcd(\theta_1(g_K) \mid \phi \neq K \subseteqq R) = \theta_2(f)$.

By virtue of the above theorem, and Theorem 1 of [1], the calculation of $\langle f \mid A \rangle \pmod d$, where f is a prime operator, and $d \in \boldsymbol{P}$ can be reduced to the special case $d = \theta_2(f)$. We are thus lead to considering sets closed $(\bmod\, \theta_2(f))$; before we do so, we briefly investigate unary operators in the residue class rings.

Let $m, M \in \boldsymbol{Z}$, with $\gcd(m, M) = 1$.

DEFINITION 5. For each $a \in \boldsymbol{N}$ let $m^{[a]} = \sum_{j=0}^{a-1} m^j$. Thus $m^{[0]} = 0$, and $m^{[1]} = 1$.

LEMMA 5. *Let $a, b \in \boldsymbol{N}$. Then*

(i) $m^a = (m-1)m^{[a]} + 1$.

(ii) $m^{[a]} = \begin{cases} a & \text{if } m = 1 \\ \dfrac{m^a - 1}{m - 1} & \text{if } m \neq 1. \end{cases}$

(iii) $m^{[a+b]} = m^a m^{[b]} + m^{[a]}$.

(iv) $m^{[ab]} = (m^b)^{[a]} m^{[b]}$.

LEMMA 6. *There is a unique $t \in \boldsymbol{N}$ such that for all $a, b \in \boldsymbol{N}$, $m^{[a]} \equiv m^{[b]} \pmod M$ if and only if $a \equiv b \pmod t$. In fact,*

$$t = \begin{cases} 0 & \textit{if } M = 0,\ m = 1 \\ 2 & \textit{if } M = 0,\ m = -1 \\ \dfrac{s\,|M|}{\gcd(M, m^{[s]})} & \textit{if } M \neq 0, \end{cases}$$

where s is the order of m modulo M. Thus s divides t; and $t = 0$ if and only if $M = 0$, $m = 1$. Also, if $t \neq 0$, $m^{[t-1]} \equiv -m^{s-1} \pmod{M}$.

Proof. We can assume $M \neq 0$. Let $a, b \in N$, with $a \leqq b$; let $t = s\,|M|/\gcd(M, m^{[s]})$. Then $m^{[b]} - m^{[a]} = m^a m^{[b-a]}$, so $m^{[a]} \equiv m^{[b]} \pmod{M}$ if and only if $m^{[b-a]} \equiv 0 \pmod{M}$.

If $m^{[b-a]} \equiv 0 \pmod{M}$, then $m^{b-a} \equiv (m-1)m^{[b-a]} + 1 \equiv 1 \pmod{M}$, so $b - a = ks$ for some $k \in N$. Then

$$0 \equiv m^{[b-a]} \equiv m^{[ks]} \equiv (m^s)^{[k]} m^{[s]} \equiv k m^{[s]} \pmod{M}\ ,$$

so $k \equiv 0 \pmod{M/\gcd(M, m^{[s]})}$, so $a \equiv b \pmod{t}$.

Conversely, if $b - a = kt$ for some $k \in N$, then

$$\begin{aligned} m^{[b-a]} &= m^{[kt]} = m^{[sk|M|/\gcd(M, m^{[s]})]} = (m^s)^{[k|M|/\gcd(M, m^{[s]})]} m^{[s]} \\ &= k\,|M|\,\frac{m^{[s]}}{\gcd(M, m^{[s]})} \equiv 0 \pmod{M}\ . \end{aligned}$$

Finally, $m \cdot m^{[t-1]} + 1 \equiv 0 \pmod{M}$, thus $m^{[t-1]} \equiv -m^{s-1} \pmod{M}$, since the map $x \to mx + 1$ is a bijection on Z_M.

Let $T = \{m^{[n]} \mid 0 \leqq n < t\}$.

LEMMA 7. *T contains t elements, all distinct modulo M. For each $a \in N$, $m^a T \equiv T - m^{[a]} \pmod{M}$.*

Proof. The first statement is a direct consequence of Lemma 6. Also, $m^a T = \{m^a m^{[n]} \mid 0 \leqq n < t\} = \{m^{[n+a]} \mid 0 \leqq n < t\} - m^{[a]} \equiv T - m^{[a]}$ (modulo M) by Lemma 6.

THEOREM 7. $T \equiv \langle mx + 1 \mid 0 \rangle \pmod{M}$.

Proof. By Lemma 7, $mT + 1 \equiv T \pmod{M}$, so T is closed under $mx + 1$, $\pmod{M}$. A simple induction on n shows $m^{[n]} \in \langle mx + 1 \mid 0 \rangle$ for each $0 \leqq n < t$.

COROLLARY 2. *For each $a, c \in Z$,*

$$\langle mx + c \mid a \rangle \equiv ((m-1)a + c)T + a \pmod{M}\ .$$

Proof. $\langle mx + c \mid a \rangle = ((m-1)a + c)\langle mx + 1 \mid 0 \rangle + a$.

COROLLARY 3. *For each* $c \in \boldsymbol{Z}$, *and* $A \subseteq \boldsymbol{Z}$,

$$\langle mx + c \mid A \rangle \equiv \bigcup_{a \in A} [((m-1)a + c)T + a] \,(\mathrm{mod}\, M) \,.$$

Proof. If f is any unary operator, $\langle f \mid A \rangle = \bigcup_{a \in A} \langle f \mid a \rangle$.

We now turn our attention to r-ary operators on $\boldsymbol{Z}_d$.

Let $r \in \boldsymbol{N} + 2$, let $R = [1, r]$. Let $m_1, \cdots, m_r \in \boldsymbol{Z}\backslash\{0\}$, with $\gcd(m_1, \cdots, m_r) = 1$. Let f be the operator $m_1x_1 + \cdots + m_rx_r$, let $\theta = \theta_2(f)$. For each $i \in R$, let

$$M_i = \gcd\{m_j \mid j \in R,\, j \neq i\} \,.$$

The proof of the following lemma is straightforward.

LEMMA 8. *For each* $i \in R$, $\gcd(m_i, M_i) = 1$, *and* $\theta = \gcd(\theta, m_i)M_i$. *For each* $i, j \in R$, *with* $i \neq j$, M_i *divides* m_j, *but* $\gcd(M_i, M_j) = 1$. *Finally*, θ *is the product of the* M_i'*s*.

For each $i \in R$, let s_i be the order of m_i modulo M_i, let $t_i = s_iM_i/\gcd(M_i, m_i^{[s]})$.

LEMMA 9. *Let* $x, k_1, \cdots, k_r \in \boldsymbol{Z}$, *let* $a_1, \cdots, a_r \in \boldsymbol{P}$. *Then* $k_1m_1^{a_1} + \cdots + k_rm_r^{a_r} \equiv x \,(\mathrm{mod}\, \theta)$ *if and only if, for all* $i \in R$, $k_i \equiv xm^{a_i(s_i-1)} \,(\mathrm{mod}\, M_i)$.

Proof. This is a chain of equivalent statements:

$$k_1m_1^{a_1} + \cdots + k_rm_r^{a_r} \equiv x \,(\mathrm{mod}\, \theta)$$

$$k_1m_1^{a_1} + \cdots + k_rm_r^{a_r} \equiv x \,(\mathrm{mod}\, M_i) \qquad \text{for all } i \in R$$

$$k_im_i^{a_i} \equiv x \,(\mathrm{mod}\, M_i) \qquad \text{for all } i \in R$$

$$k_i \equiv xm_i^{a_i(s_i-1)} \,(\mathrm{mod}\, M_i) \qquad \text{for all } i \in R \,.$$

COROLLARY 4. *Let* $k_1, \cdots, k_r \in \boldsymbol{Z}$, *let* $a_1, \cdots, a_r \in \boldsymbol{P}$. *Then* $k_1m_1^{a_1} + \cdots + k_rm_r^{a_r} \equiv 0 \,(\mathrm{mod}\, \theta)$ *if and only if* $k_i = 0 \,(\mathrm{mod}\, M_i)$ *for all* $i \in R$.

COROLLARY 5. $m_1^{s_1} + \cdots + m_r^{s_r} \equiv 1 \,(\mathrm{mod}\, \theta)$.

COROLLARY 6. *Let* $a_1, \cdots, a_r, b_1, \cdots, b_r \in \boldsymbol{N}$. *Then* $m_1m_1^{[a_1]} + \cdots + m_rm_r^{[a_r]} \equiv m_1m_1^{[b_1]} + \cdots + m_rm_r^{[b_r]} \equiv (\mathrm{mod}\, \theta)$ *if and only if* $a_i \equiv b_i \,(\mathrm{mod}\, t_i)$ *for each* $i \in R$.

Proof. Note that $m_1m_1^{[a_1]} + \cdots + m_rm_r^{[a_r]} \equiv m_1m_1^{[b_1]} + \cdots + m_rm_r^{[b_r]}$

(mod θ) if and only if $m_i^{[|b_i-a_i|]} \equiv 0 \pmod{M_i}$ for each $i \in R$, and the rest follows from Lemma 6.

For each $i \in R$, let $T_i = \{m_i^{[n]} \mid 0 \leqq n < t_i\}$. Let $T = m_1T_1 + \cdots + m_rT_r + 1$. Note that T contains $\prod_{i \in R} t_i$ elements, all distinct modulo θ.

THEOREM 8. $T \equiv \langle f+1 \mid 0\rangle \pmod{\theta}$.

Proof. By Theorem 4,

$$\langle f+1 \mid 0\rangle \equiv m_1\langle f+1 \mid 0\rangle + \cdots + m_r\langle f+1 \mid 0\rangle + 1 \pmod{\theta} .$$

But for each $i \in R$,

$$m_i\langle f+1 \mid 0\rangle \equiv m_i\langle m_ix+1 \mid 0\rangle \equiv m_iT \pmod{\theta} .$$

COROLLARY 7. *Let a, $c \in \boldsymbol{Z}$. Then, modulo θ,*

$$\begin{aligned}\langle f+c \mid a\rangle &\equiv ((\sigma(f)-1)a+c)T+a \\ &\equiv c + \sum_{i \in R}[((m_i-1)a+c)T_i+a] .\end{aligned}$$

THEOREM 9. *Let $c \in \boldsymbol{Z}$, let $A \subseteqq \boldsymbol{Z}$. Then*

$$\langle f+c \mid A\rangle \equiv c + \sum_{i \in R} m_i \bigcup_{a \in A}[((m_i-1)a+c)T_i+a] \pmod{\theta} .$$

Proof. This is a consequence of Corollary 3.

This concludes our investigation of sets of residue classes closed under a prime operator. We now apply these results to closed sets of integers.

DEFINITION 6. A set $A \subseteqq \boldsymbol{Z}$ is *doubly periodic*, with a *double period* $d \in \boldsymbol{P}$ if A is a union of residue classes modulo d. The following analogue of Theorem 2 of [1] is proved in an analogous fashion:

THEOREM 10. *Let f be a prime operator, let A be a doubly periodic set with double period d. Then $\langle f \mid A\rangle$ has double period d.*

THEOREM 11. *Let A and B nonempty periodic sets with eventual period d, let f be a positive, prime operator. Then $T = \langle f \mid A \cup (-B)\rangle$ is a doubly periodic set with double period d.*

Proof. We may assume $f \in P$. Further we may assume A, $B \subseteqq \boldsymbol{P}$; for if that special base be true, it can be applied, for general A,

B, to the set $T' = \langle f \mid (A \cap \boldsymbol{P}) \cup (-(B \cap \boldsymbol{P}))\rangle$, thus A, $B \subseteqq T'$, so $T = T'$.

Let $D = \{t \in \boldsymbol{Z}_d \mid t \cap T \neq \phi\}$,
let $D^+ = \{t \in \boldsymbol{Z}_d \mid t \cap \boldsymbol{P} \subseteqq T\}$,
let $D^- = \{t \in \boldsymbol{Z}_d \mid t \cap (-\boldsymbol{P}) \subseteqq T\}$,
let $D^0 = \{t \in \boldsymbol{Z}_d \mid t \subseteqq T\}$.

Thus $D^0 \subseteqq D^+ \cap D^-$, and $D = D^+ \cup D^-$. Moreover, if T is closed under any positive operator h, then D, D^+, D^- and D^0 are all closed under h. In particular, $f(D^+ \cap D^-) \subseteqq D^0$, thus $D^+ \cap D^- = f(D^+ \cap D^-) \subseteqq D^0 \subseteqq D^+ \cap D^-$, so $D^0 = D^+ \cap D^-$. By hypothesis, $D^+ \neq \phi \neq D^-$; let $s \in D^+$, let $t \in D^-$. Note that $\langle [f, s] \mid t\rangle \subseteqq D^- \pmod d$. But $\langle [f, s] \mid t\rangle \equiv \langle f \mid s, t\rangle \pmod d$ by Theorem 5, thus $s \in D^-$, and $D^+ \subseteqq D^-$. Similarly, $D^- \subseteqq D^+$, thus $D = D^0 = D^+ = D^-$.

THEOREM 12. *Let $f \in P$, let $c \in \boldsymbol{Z}$, let $A \subseteqq \boldsymbol{Z}$, with $((\sigma(f)-1)A + c) \cap \boldsymbol{P} \neq \phi \neq ((\sigma(f)-1)A + c) \cap (-\boldsymbol{P})$. Then $T = \langle f + c \mid A\rangle$ is a doubly periodic set.*

Proof. We may assume $c = 0$. Since both $T \cap \boldsymbol{P}$ and $(-T) \cap \boldsymbol{N}$ are nonempty periodic sets, $T = \langle f \mid (T \cap \boldsymbol{P}) \cup (T \cap (-\boldsymbol{N}))\rangle$ is a doubly periodic set by Theorem 11.

COROLLARY 8. *Let $f \in \mathscr{H}$, let $c \in \boldsymbol{Z}$, let $A \subseteqq \boldsymbol{Z}$, with $((\sigma(f)-1)A + c) \nsubseteqq \{0\}$. Then $T = \langle f + c \mid A\rangle$ is a doubly periodic set.*

Proof. By Lemma 2, T is a closed under a positive, prime operator g. Clearly, T is neither bounded below, nor bounded above; thus $T = \langle g \mid T\rangle$ is doubly periodic by Theorem 12.

DEFINITION 7. Let $A \subset \boldsymbol{Z}$, let $d \in \boldsymbol{P}$. We say that A is a *regular* set, with *regular period d*, if either

Type 1. A is a periodic set with eventual period d, or
Type 2. $-A$ is a set of type 1, or
Type 3. A is a doubly periodic set with double period d.

THEOREM 13. *Let $T \subseteqq \boldsymbol{Z}$, let f be a prime operator, with $f(T) \subseteqq T$. Then either $|T| \leqq 1$, or T is a regular set with regular period $\theta_2(f)\gamma(T)$.*

Proof. If $|T| > 1$, then T is a regular set by Theorem 2, Theorem 12, or Corollary 8. By Theorem 6, T has a regular period $\theta_2(f)\gamma(T)$.

With Theorem 13, we have achieved goal (2).

Now let f be the prime operator $f(x_1, \cdots, x_r) = m_1x_1 + \cdots + m_rx_r + c$, and let $A \subseteqq \boldsymbol{Z}$. How can we calculate $\langle f \mid A\rangle = T$?

Fisrt, let the reader show that for any $a \in A$, $\gamma(T) = \gcd(A - f(a))$. Hence we may use Theorem 1 of [1] to reduce to the case $\gamma(T) = 1$; we simply replace T by $1/\gamma(T)(T - a) \subseteqq \boldsymbol{Z}$. (*Note* $\gamma(T) = 0$ if and only if $((\sigma(f)-1)A + c) \subseteqq \{0\}$, if and only if $|T| \leqq 1$; in this case $T = A$. Thus we assume $\gamma(G) \neq 0$.) By Theorem 13, T has a regular period $\theta = \theta_2(f)$. The next step is to calculate the set $T_\theta = \{t \in \boldsymbol{Z}_\theta \mid t \cap T \neq \phi\}$; this finite calculation can be readily carried out with the aid of Theorem 9.

The type of T can be found as follows. If f is not positive, T is of type 3. If f is positive, then, $\sigma(f) > 1$; let $\alpha = c/1 - \sigma(f)$, let $J = \{u \in A \mid u < \alpha\}$, let $K = \{u \in A \mid u > \alpha\}$. If $J \neq \phi \neq K$, then f is again of type 3. If $J = \phi$, f is of type 1, and if $K = \phi$, f is of type 2.

If T is of type 3, our troubles are over, as $T = \bigcup_{t \in T_\theta} t$. If T is not of type 3, we may assume, (by replacing T with $-T$ if necessary), that T is of type 1. In this case, let

$$S = \{u \in Z \mid u > \alpha,\, u \in t \text{ for some } t \in T_\theta\} \cup \begin{cases} \{\alpha\} & \text{if } \alpha \in A \\ \phi & \text{if } \alpha \notin A \end{cases},$$

then clearly S is a periodic set with $A \cup f(s) \subseteqq S$, and $T \subseteqq S \subset T$. Thus S is only a "little bit too big"; for many applications, this is sufficient information.

We have a method for producing T from S, details will appear elsewhere.

References

1. D. G. Hoffman and D. A. Klarner, *Sets of integers closed under affine operators-the closure of finite sets*, to appear.

2. D. G. Hoffman, *Sets of integers closed under affine operators*, Ph. D. thesis, University of Waterloo, 1976.

3. D. A. Klarner and R. Rado, *Arithmetic properties of certain recursively defined sets*, Pacific J. Math., **53** (1974), 445-463.

4. D. A. Klarner, *Sets generated by interation of a linear operation*, Starr—CS—72—275, Computer Science Department, Stanford University, March 1972.

Received October 12, 1977 and in revised form November 1, 1978.

AUBURN UNIVERSITY
AUBURN, AL 36830
AND
SUNY
BINGHAMTON, NY 13901