ON A CLASS OF BINARY SEQUENCES[1]

NEAL ZIERLER[2]

Foreword. In certain applications involving digital computing machines one wishes to generate a sequence of 0's and 1's with given properties; often the sequence is to be pseudo-random in a suitable sense. One common way of producing such a sequence is to combine in some fashion a number of given periodic sequences that are stored or generated in the machine. An important class of such sequences consists of those obtained by a time-invariant method of combining given sequences.

Our immediate objective is to determine the number of elements of this class if the periods of the original sequences are preassigned and pairwise coprime. To achieve this objective, we examine questions of duplication and periodicity within the class.

1. **Introduction.** Let $K=\{0, 1\}$ be a field with two elements, let $V_1=K$ and let $V_n=K\times V_{n-1}$, $n=2, 3, \cdots$. Each element of V_n is an n-tuple $u=\langle u(1), \cdots, u(n)\rangle$ of elements of K; $u(k)$ is called the kth *component* of u. An *A-sequence* is a sequence $x=\{x(i): i=0, 1, \cdots\}$ of elements of a nonempty set A; we say x *covers* A if every element of A occurs as an $x(i)$. The *complement* of a K-sequence x is the K-sequence $\{1+x(i): i=0, 1, \cdots\}$ and is denoted by $1+x$. Fix the integer $n>0$, let $V=V_n$ and let F be the set of all functions defined on all of V with values in K. If $f\in F$ and x is a V-sequence, $f(x)$ denotes the K-sequence $\{f(x(i)): i=0, 1, \cdots\}$. If x is a V-sequence we write $x(i, j)$ for the jth component of $x(i)$ and call the K-sequence $x(-, j)=\{x(0, j), x(1, j), \cdots\}$ the jth *component sequence of* x, $j=1, \cdots, n$.

It is evidently necessary and sufficient for the V-sequence x to be periodic that $x(-, j)$ be periodic for all $j=1, \cdots, n$. We suppose given n integers $p_1, \cdots, p_n$ all greater than unity and such that $(p_i, p_j)=1$ if $i\neq j$. Let X be the set of all V-sequences x such that the ith component sequence of x has p_i as a period for all i. The elements of X are called *admissible* V-sequences.

Let $Q=\{f(x): f\in F, x\in X\}$ and let m denote the number of ele-

Received by the editors December 15, 1954 and, in revised form, June 12, 1955.

[1] The research in this paper was supported jointly by the United States Army, Navy, and Air Force under contract with Massachusetts Institute of Technology.

[2] Staff Member, Lincoln Laboratory, Massachusetts Institute of Technology.

ments of Q. Since F contains 2^{2^n} elements and X contains $2^{p_1+\cdots+p_n}$ elements, $m \leqq 2^{2^n+p_1+\cdots+p_n}$. The number m is, in fact, always less than 2^{-n} times this upper bound because there are many pairs f, g of functions in F and pairs x, y of elements of X such that $f(x) = g(y)$ but $f \neq g$ or $x \neq y$. Such duplication occurs under the following circumstances. If $f \in F$ let $N(f)$ denote the set of all $i = 1, \cdots, n$ such that $f(u)$ is independent of the ith component of u in V; i.e., such that $f(u) = f(\langle u(1), \cdots, u(i-1), 1+u(i), u(i+1), \cdots, u(n)\rangle)$ for all u in V. Let $f \in F$ and $x \in X$ such that $x(-, j)$ covers K whenever $j \notin N(f)$. Let $y \in X$ such that $y(-, j) = x(-, j)$ or $1+x(-, j)$ whenever $j \notin N(f)$. Define $g'(y(i)) = f(x(i))$, $i = 0, 1, \cdots$, and suppose $y(i) = y(k)$. If $j \notin N(f)$, $s+x(i, j) = y(i, j) = y(k, j) = s+x(k, j)$ for some $s \in K$ so $x(i, j) = x(k, j)$. It follows that $f(x(i)) = f(x(k))$ and hence that g' is consistently defined as a function from part of V to K. Let g be an arbitrary extension of g' to all of V with values in K; then $g \in F$ and $g(y) = f(x)$.

We shall investigate the composition of Q as to the periodicity of its elements. In particular, we shall show that under the above assumptions, duplication occurs only in the stated way and deduce that

$$m = T(0) + T(1) \sum q_i + T(2) \sum q_i q_j + \cdots + T(n) q_1 q_2 \cdots q_n$$

where the sigmas denote elementary symmetric functions, $q_i = 2^{p_i - 1} - 1$, $i = 1, \cdots, n$, and

$$T(k) = \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} 2^{2^j}, \qquad k = 0, 1, \cdots.$$

2. Some basic lemmas.[3]

2.1. Let s be a positive integer, let $p_1, \cdots, p_s$ be pairwise relatively prime positive integers and let $j_1, \cdots, j_s$ be integers. Then there exists a non-negative integer j such that $j \equiv j_i \bmod p_i$ for all i simultaneously.

PROOF. If $s = 1$ the result is trivial. Assume $s > 1$ and that there exists $j' \geqq 0$ such that $j' \equiv j_i \bmod p_i$, $i = 1, \cdots, s-1$. Since $r = p_1 \cdots p_{s-1}$ is prime to p_s, we can find k such that $kr \equiv j_s - j' \bmod p_s$. Then $j = j' + kr + k' r p_s$ has the desired property if k' is chosen so large that $j \geqq 0$.

2.2. Let s and $p_1, \cdots, p_s$ be as in 2.1. Let x be a V_s-sequence of least positive period r and let y be the V_s-sequence defined by $y(i) = x(a+bi)$ where a and b are non-negative integers with b prime to r. Then y has least positive period r.

[3] The author is indebted to the referee for simplification of proofs and for improvements in notation and organization.

PROOF. If q is the least positive period of y then, by definition of y, r is a period of y and so q divides r. Since b is prime to r we can find non-negative integers j, k such that $a+bj\equiv 0$, $bk\equiv 1 \bmod r$ and then $x(i)=y(j+ki)$. Hence r divides q, so $q=r$.

2.3. Let $s>1$ and let $p_1, \cdots, p_s$ be as in 2.1. Let the K-sequence x and the V_{s-1}-sequence y have least positive periods r, q respectively where $(r, q)=1$. Let (x, y) denote the V_s-sequence z: $z(i)=\langle x(i), y(i, 1), \cdots, y(i, s-1)\rangle$. Then z has least positive period rq. If x covers K and y covers V_{s-1} then z covers V_s, and conversely.

PROOF. The least positive period of z is the least common multiple of r and q which is rq. If x, y cover K, V_{s-1} respectively let t, u be in K, V_{s-1} respectively. Then $x(i)=t$, $y(j)=u$ for some i, j. By 2.1, there exists a non-negative k such that $k\equiv i \bmod r$, $k\equiv j \bmod q$ and then $z(k)=\langle t, u(1), \cdots, u(n-1)\rangle$. The converse is obvious. Repeated application of 2.3 yields

2.4. Let k be a positive integer and let x be a V_k-sequence with periodic component sequences. Let r_i be the least positive period of $x(-, i)$, $i=1, \cdots, k$, and suppose $(r_i, r_j)=1$ if $i\neq j$. Then x has least positive period $r_1 \cdots r_n$. Furthermore, x covers V if and only if $x(-, i)$ covers K for $i=1, \cdots, n$.

2.5. Let $1\leqq i\leqq n$ and let $f\in F$ for which there exists $v\in V$ such that

(a) $\quad f(v)\neq f(\langle v(1), \cdots, v(i-1), 1+v(i), v(i+1), \cdots, v(n)\rangle)$.

Let $x\in X$ such that $x(-, j)$ covers K if $j\neq i$ and let r_j be the least positive period of $x(-, j)$, $j=1, \cdots, n$. Let $r=r_1 \cdots r_{i-1}r_{i+1} \cdots r_n$. Then $f(x)$ has least positive period $r_i r'$ where r' divides r.

PROOF. We assume, without essential loss of generality, that $i=1$. Let x' be the V_{n-1}-sequence: $x'(j)=\langle x(j, 2), \cdots, x(j, n)\rangle$. Then x' covers V_{n-1} by 2.4 and so, for some $k\geqq 0$, $x'(k)=\langle v(2), \cdots, v(n)\rangle$. Let z be the K-sequence: $z(j)=f(x(k+jr))$. Since $x(k+jr)=\langle x(k+jr, 1), v(2), \cdots, v(n)\rangle$ for all $j=0, 1, \cdots$, $z(j)=s+x(k+jr, 1)$ for all j for some fixed s in K. Clearly z and the sequence $\{x(k+jr, 1): j=0, 1, \cdots\}$ have the same least positive period which, by 2.2, is r_1. We may write the least positive period of $f(x)$, which divides $r_1 r$, in the form $r_1' r'$ where r_1' divides r_1 and r' divides r. Now r_1' is a period of z, for $z(j+r_1')=f(x(k+r_1' r+jr))=z(j)$ since $r_1' r$ is a period of $f(x)$. Hence r_1 divides r_1' and so $r_1=r_1'$.

2.6. Under the hypothesis of 2.5 let y be an admissible V-sequence with $r_i r$ as a period. Suppose that $y(-, i)$ has least positive period r_i and that g is an element of F such that $g(y)=f(x)$. Then $x(-, i)=y(-, i)$ or $1+y(-, i)$. If $r_i>1$ there exists u in V such that (a) of 2.5 holds for g and u.

PROOF. We again assume, without essential loss of generality, that $i=1$. If $r_1=1$ the result is obvious so suppose $r_1>1$. In the notation of the proof of 2.5, $g(y+jr)=s+x(k+jr, 1)$ for all j. Then, since $y(k+jr, a)=y(k, a)$ for $a>1$ by hypothesis, (a) of 2.5 holds for g and $u=\langle 0, y(k, 2), \cdots, y(k, n)\rangle$. Further, $g(y(k+jr))=s'+y(k+jr, 1)$ for all j for some fixed s' in K and so, on setting $t=s+s'$, we have

$$x(k+jr, 1) = t + y(k+jr, 1), \qquad j = 0, 1, \cdots. \tag{b}$$

Since r_1 and r are coprime, there exist non-negative integers a and b such that $k+ra\equiv 0$, $rb\equiv 1 \bmod r_1$. Then from (b) with j replaced by $a+bj$, $x(-, 1)=y(-, 1)$ or $1+y(-, 1)$.

3. **A partial ordering of** X. In the following let $x, y, \cdots$ denote elements of X, $f, g, \cdots$, elements of F.

3.1. Given x let $Q(x)=\{f(x): f\in F\}$. We introduce a partial ordering in X by defining $x<y$ to mean that $Q(x)\subseteq Q(y)$. If $Q(x)=Q(y)$ we write $x\equiv y$, x is equivalent to y. The set of all $\langle x, y\rangle$ such that $x\equiv y$ is an equivalence relation for X.

3.2. $x<y$ if and only if $y(j)=y(k)$ implies $x(j)=x(k)$.

PROOF. If $y(j)=y(k)$ and $x(j)\neq x(k)$ choose f so that $f(x(j))\neq f(x(k))$. Since $g(y(j))=g(y(k))$ for all g, $x\not<y$. Conversely suppose $y(j)=y(k)$ implies $x(j)=x(k)$. Given f define $g'(y(i))=f(x(i))$; by the hypothesis we can extend g' to an element g of F and then $g(y)=f(x)$. Thus $x<y$.

3.3. $x<y$ if and only if there is a mapping α of V in itself such that $y(i)\alpha=x(i)$, $i=0, 1, \cdots$.

PROOF. If such an α exists and $y(j)=y(k)$ then $x(j)=y(j)\alpha=y(k)\alpha=x(k)$ and so $x<y$ by 3.2. Now suppose $x<y$ and define α' by $y(i)\alpha'=x(i)$, $i=0, 1, \cdots$; α' is consistently defined by 3.2 and we may let α be any extension of α' to all of V.

3.4. Let M be the set of all maximal elements of X, $M=\{x: x<y$ implies $x\equiv y\}$. Then x is maximal if and only if x covers V.

PROOF. Suppose x covers V and $x<y$. By 3.3 there exists a mapping α of V in itself such that $y(i)\alpha=x(i)$, $i=0, 1, \cdots$. Then α is onto V by hypothesis, hence is one-one and its inverse β is a permutation of V such that $x(i)\beta=y(i)$, all i. Hence $y<x$ by 3.3 and x is maximal. Suppose now that x does not cover V. Then by 2.4 there exists some $i=1, \cdots, n$ such that $x(-, i)$ does not cover K. Since $p_i>1$, there exist sequences y in X such that $y(-, k)=x(-, k)$ if $k\neq i$ while $y(-, i)$ covers K. Then if $y(j)=y(k)$, $x(j)=x(k)$ so $x<y$ by 3.2. Since $y(-, i)$ covers K, we can choose j' and k' such that $y(j', i)\neq y(k', i)$. By 2.1 we can find j and $k\geqq 0$ such that $j\equiv j'$ and $k\equiv k' \bmod p_i$ while $j\equiv 0\equiv k \bmod p_s$ for $s\neq i$. Then $x(j)=x(k)$ but $y(j)\neq y(k)$ so $y\not<x$ by 3.2 and x is not maximal. An immediate corollary is

3.5. x is maximal if and only if no component sequence of x has period one. Hence M contains

$$\prod_{i=1}^{n} (2^{P_i} - 2)$$

elements.

If α is a permutation of V and $x \in X$ let $x\alpha$ denote the V-sequence $\{x(j)\alpha: j=0, 1, \cdots\}$. An immediate consequence of 3.3 and 3.4 is

3.6. Let x and y be maximal. Then $x \equiv y$ if and only if there is a permutation α of V such that $x\alpha = y$.

3.7. Let G be the set of all permutations α of V such that $x\alpha \in X$ for all $x \in X$. The permutation α of V is in G if and only if there exist permutations $\alpha_1, \cdots, \alpha_n$ of K such that $u\alpha = \langle u(1)\alpha_1, \cdots, u(n)\alpha_n \rangle$ for all u in V.

PROOF. Suppose such α_i exist for the permutation α of V. Then if $x \in X$, $x\alpha(-, j) = x(-, j)$ or $1 + x(-, j)$ for $j = 1, \cdots, n$ so $x\alpha \in X$. Conversely, suppose $\alpha \in G$ and $x \in M$. Let $y = x\alpha$ and, defining addition componentwise in V, let $u = x(0) + y(0)$. Let z be the V-sequence: $z(j) = u + x(j)$, $j = 0, 1, \cdots$. Then

(a) $$z(0) = y(0),$$

(b) $$z(j) = z(0) \text{ if and only if } y(j) = y(0).$$

The result now follows from the next remark and the fact that x covers V on defining α_i, $i = 1, \cdots, n$: $s\alpha_i = s + u(i)$ for $s \in K$.

3.8. Let z and y be elements of X satisfying (a) and (b) of 3.7. Then $z = y$.

PROOF. Let $j \geqq 0$, $1 \leqq i \leqq n$. By 2.1 we can find a non-negative integer s such that $s \equiv 0 \bmod p_k$, $k \neq i$, and $s \equiv j \bmod p_i$. Then for $k \neq i$, $z(s, k) = z(0, k) = y(0, k) = y(s, k)$ while $z(s, i) = z(j, i)$ and $y(s, i) = y(j, i)$. Hence $z(j, i) = z(0, i)$ if and only if $z(s) = z(0)$ and similarly for y. Since $z(0, i) = y(0, i)$ by hypothesis, $z(j, i) = y(j, i)$; since this is true for arbitrary j, i, $z = y$. An immediate consequence of 3.6 and 3.7 is

3.9. Let x and y be maximal. Then $x \equiv y$ if and only if $x(-, i) = y(-, i)$ or $1 + y(-, i)$, $i = 1, \cdots, n$.

3.10. G contains 2^n elements by 3.7 and so it follows from 3.6 that each equivalence class of elements of M has 2^n members. Hence, by 3.5, the elements of M fall into exactly

$$\prod_{i=1}^{n} (2^{p_i - 1} - 1)$$

distinct equivalence classes.

4. Functions nontrivial on V.

4.1. We say f is *nontrivial on* V if for each $i=1, \cdots, n$ there exists $u \in V$ depending on i such that

(a) $f(u) \neq f(\langle u(1), \cdots, u(i-1), 1+u(1), u(i+1), \cdots, u(n)\rangle)$.

In other words, f is nontrivial on V if and only if $N(f)$ is empty.

4.2. f is nontrivial on V if and only if $f(x)$ has the same least positive period as x for every x in M.

PROOF. Let f be nontrivial on V and let $x \in M$. If r_i is the least positive period of $x(-, i)$, $i=1, \cdots, n$, and q is the least positive period of $f(x)$ then every r_i divides q by 2.5 and so $r=r_1 \cdots r_n$, which is the least positive period of x by 2.4, divides q. Since r is obviously a period of $f(x)$, q divides r and so $q=r$.

Conversely, suppose that, for a given f, (a) of 4.1 holds for no u in V for a certain i. Let x be the V-sequence such that $x(j, k)=0$ for $k=1, \cdots, n; j=0, \cdots, p_k-2, x(p_k-1, k)=1, k=1, \cdots, n$. Then $x(-, k)$ has least positive period p_k, x is in M and has least positive period $p=p_1 \cdots p_n$ while $f(x)$ has least positive period at most p/p_i, and the proof is complete.

REMARK. If $x \notin M$ there exists f nontrivial on V such $f(x)$ has period one. (Since $x \notin M$ there exists $v \in V$ that does not occur as an $x(i)$ by 3.4. Let f be the element of F such that $f(u)=1$ if and only if $u=v$.)

4.3. Let $T(n, j)$ denote the number of elements f of F for which $N(f)$ contains $n-j$ elements, $j=0, \cdots, n$. Then

$$T(n, j) = \binom{n}{j} T(j)$$

if we define $T(j)=T(j, j)$. Thus we may obtain $T(n)$, $n=0, 1, \cdots$, recursively from the formula

$$\prod_{j=0}^{n} \binom{n}{j} T(j) = 2^{2^n}.$$

5. Duplication, periodicity and the formula for m.

5.1. Let x and y be any two nonequivalent elements of M and let f and g be nontrivial on V. Then $f(x) \neq g(y)$.

PROOF. Suppose $f(x)=g(y)$. Then by 4.2, x and y have the same least positive period and 2.6 applies for every i. That is, $x(-, i) = y(-, i)$ or $1+y(-, i)$ for $i=1, \cdots, n$ and so $x \equiv y$ by 3.9.

5.2. Let $f \in F$ such that $N(f) \neq \{1, \cdots, n\}$ and let $x \in X$ such that $x(-, j)$ covers K whenever $j \notin N(f)$. Let the least positive period of $x(-, j)$ be r_j. Then the least positive period of $f(x)$ is

$$r = \prod_{j \notin N(f)} r_j.$$

PROOF. The statement reduces to part of 4.2 if $N(f)$ is empty. We assume that $N(f)$ has $n-k$ elements where $1 \leqq k \leqq n$. Without loss of generality we may assume that $N(f) = \{k+1, \cdots, n\}$. Then the function f' on V_k such that $f'(u) = f(\langle u(1), \cdots, u(k), 0, \cdots, 0\rangle)$ is nontrivial on V_k. Let x' be the V_k-sequence $x'(j) = \langle x(j, 1), \cdots, x(j, k)\rangle$. Then x' covers V_k and so by 4.2, the least positive periods of $f'(x') = f(x)$ and x' are the same; namely, by 2.4, $r_1 \cdots r_k$.

5.3. Let f and x be as in 5.2. Let g and y be such that $f(x) = g(y)$. Then $N(g) \subseteq N(f)$ and $x(-, i) = y(-, i)$ or $1 + y(-, i)$ if $i \notin N(f)$.

PROOF. Clearly, if $j \in N(g)$ or $z(-, j)$ has period one then the least positive period of $g(z)$ is prime to p_j for all z in X. Hence, by 5.2, $N(g) \subseteq N(f)$, $y(-, j)$ covers K if $j \notin N(f)$ and does not if $j \in N(f) - N(g)$. If $N(f)$ is empty, so is $N(g)$ and the result follows from 5.1. Suppose that $N(f)$ is not empty and, without essential loss of generality, that $N(f) = \{k+1, \cdots, n\}$ for some k: $1 \leqq k \leqq n$. We may consistently define a function g' on V_k by: $g'(u) = g(\langle u(1), \cdots, u(k), y(0, k+1), \cdots, y(0, n)\rangle)$. Then g' is nontrivial on V_k and $g'(y') = g(y)$ if we define $y'(j) = \langle y(j, 1), \cdots, y(j, k)\rangle$. Define f' and x' analogously; then $f'(x') = f(x)$, f' is nontrivial on V_k and x' and y' cover V_k. The second result now follows from 5.1 with n replaced by k. This proves the assertion of the introduction on duplication in Q. An immediate corollary of 5.3 is

5.4. Let x and y be maximal and suppose $f(x) = g(y)$ for some f and g. Then $N(f) = N(g)$ and $x(-, i) = y(-, i)$ or $1 + y(-, i)$ for $i \notin N(f)$.

5.5. Let $q_i = 2^{p_i - 1} - 1$, $i = 1, \cdots, n$, and let A be a subset of M with $q_1 \cdots q_n$ elements, one representative chosen from each equivalence class of elements of M. Then $Q = \{f(x): x \in A, f \in F\}$ by definition of the partial ordering in X. Let D be a proper subset of $B = \{1, \cdots, n\}$ and let $Q(D) = \{f(x): x \in A, N(f) = D\}$. If D has $n-k$ elements, it follows from 5.4 that $Q(D)$ contains exactly $T(k) \prod_{i \notin D} q_i$ distinct sequences. If D and D' are distinct subsets of B then, by 5.4, $Q(D) \cap Q(D')$ is empty. Thus, the number of distinct sequences in $\cup Q(D)$ taken over all D with $n-k$ elements is $T(k)C_k$ where C_k denotes the sum over all products of k distinct factors chosen from among the q_i. Finally, $Q(B) = 2 = T(0)$ and so we may write $m = T(0) + C_1 T(1) + \cdots + C_n T(n)$.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY