EQUIVALENCE CLASSES OF PERIODIC SEQUENCES[1]

BY
ROBERT C. TITSWORTH

1. Introduction

Fine [1], in 1958, and Gilbert and Riordan [2], in 1961, treated the following "necklace" problem [3]: if two periodic sequences a and a' can be made alike either by a shift in origin or a permutation of states, or both, how many inequivalent symmetry types of sequences are there? A finite-state sequential machine capable of generating a sequence a is capable of also generating any sequence a' equivalent to a, since shifts in the origin can be set by proper initial conditions fed into the machine, and since permutations of the states are mere relabelings of the output states. The solution to the necklace problem is then the number of finite-state machines required to generate all sequences having a given period.

If f is a real or complex function on the sequence objects, the autocorrelation of a relative to f is defined as

$$R_f(m) = (1/p) \sum_{n=1}^{p} f(a_n) f^*(a_{n+m}),$$

where p is the period of a. This function f represents, for example, the way sequence states are interpreted as signal voltages for transmission through a communications channel, and the values of $R_f(m)$ are related to the probability that an optimum receiver makes an error when attempting to determine the origin of a in the presence of noise [4].

By considering periodic sequences generated under the mapping

$$a_n \longrightarrow a_{kn+t},$$

one can show, when $(k, p) = 1$, that

$$R_f(m) \longrightarrow R_f(km).$$

Such a mapping is thus important in coding theory, because the values assumed by the autocorrelation function of a are left invariant, signifying that these sequences have the same correlation properties.

If a and a' are called *equivalent* whenever there exist t and k, $(k, p) = 1$, such that $a_n = a'_{kn+t}$, then all sequences in an equivalence class have the same correlation values. By application of Pólya's lemma [5] to all such transformations of the type $a_n \longrightarrow a_{nk+t}$, it is possible to count the number of these equivalence classes.

Received October 19, 1962.

[1] This paper presents the results of one phase of research carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract sponsored by the National Aeronautics and Space Administration.

2. Equivalent sequences

Let $a = \{a_n\}$ be a cyclic sequence of period p, each of whose elements a_n may assume one of b values. Any sequence having period p also has period mp; the least positive period is hence called the primitive period of a. Define the operators g_k^t on $A = \{a : a \text{ has period } p \text{ and } b \text{ states}\}$ as follows:

$$g_k^t\{a_n\} = \{a_{nk+t}\}.$$

Obviously, k, t, and $kn + t$ may be treated as integers modulo p, because the sequences are cyclic. The set

$$G = \{g_k^t : (k, p) = 1; t, k \bmod p\}$$

is a group of $p\phi(p)$ elements, not unlike the affine group of matrices (for example, see [6]).

Two sequences a and a' are equivalent under G if there exists a g_k^t in G such that $g_k^t a = a'$. The number of elements a in A with the property

$$g_k^t a = a$$

for given t and k we will denote by $I(g_k^t)$. The constraints made upon a sequence by invariance under g_k^t are that $a_m = a_n$ whenever m and n are in the same cycle of the decomposition of the integers mod p by the permutation $n \to kn + t$. If we denote by $C(k, t)$ the number of disjoint cycles in the decomposition of g_k^t, the number of degrees of freedom in choosing invariant elements of A is precisely $C(k, t)$, and, consequently,

$$I(g_k^t) = b^{C(k,t)}.$$

When this is inserted into Pólya's formula, the number of equivalence classes is readily exhibited:

$$N(p) = \frac{1}{p\phi(p)} \sum_{t=0}^{p-1} \sum_{\substack{k=1 \\ (p,k)=1}}^{p-1} b^{C(k,t)}.$$

To find the number $N'(p)$ of primitive elements of A, we can apply the Möbius formula

$$N'(p) = \sum_{d|p} \mu(p/d) N(d),$$

where $\mu(d)$ is the Möbius function: $\mu(1) = 1$, $\mu(d) = (-1)^n$ if d is the product of n distinct primes, and $\mu(d) = 0$ otherwise.

It remains only to calculate the cycle numbers $C(k, t)$.

3. The cycle numbers of G

If $(k, L) = 1$, let $M(k, L)$ denote the least positive integer M such that

$$1 + k + \cdots + k^{M-1} \equiv 0 \pmod{L}.$$

LEMMA. *If* $(k, L) = 1$ *and* $E_k(L)$ *denotes the exponent of* k *modulo* L,

$$M(k, L) = LE_k(L)/(L, 1 + k + \cdots + k^{E_k(L)-1}).$$

Proof. $1 + k + \cdots + k^{M-1} \equiv 0 \pmod{L}$ implies $k^M - 1 \equiv 0 \pmod{L}$, and hence, that $E_k(L)$ divides M. If we put $M = rE_k(L)$, then since

$$0 \equiv 1 + \cdots + k^{M-1} \equiv r(1 + \cdots + k^{E_k(L)-1}) \pmod{L},$$

it follows that the smallest value of r is

$$r = L/(L, 1 + k + \cdots + k^{E_k(L)-1}).$$

LEMMA. *The number of elements in the cycle of g_k^t containing the residue class u is $M[k, p/(p, u(k-1) + t)]$.*

Proof. Let the cycle have x elements. Then x is the least positive integer such that

$$uk^x + t(k^{x-1} + \cdots + k + 1) \equiv u \pmod{p},$$

because the elements in this cycle are the residue classes

$$u, \quad uk + t, \quad uk^2 + kt + t, \quad \cdots,$$

until u appears again at the x^{th} step. Now

$$[u(k-1) + t](k^{x-1} + \cdots + 1) \equiv 0 \pmod{p}.$$

If we define $v = (p, u(k-1) + t)$, then x is the least integer such that $k^{x-1} + \cdots + 1 \equiv 0 \pmod{p/v}$, and therefore,

$$x = M(k, p/v).$$

THEOREM. *The number of disjoint cycles of g_k^t is*

$$C(k, t) = \sum_{u=0}^{p-1} M^{-1}(k, p/(p, u(k-1) + t)).$$

Proof. Let $U = \{u_1, u_2, \cdots, u_C\}$ be a set of representatives from the cycles of g_k^t, each u_i from a different cycle. Denote by

$$M(u) = M(k, p/(p, u(k-1) + t))$$

the number of elements in the cycle to which u belongs. If we sum $1/M(u)$ over all residue classes u in the same cycle as u_i, we get $M(u_i)/M(u_i) = 1$. Hence, there is a unit contribution to the sum above for each cycle of g_k^t. Thus the theorem is proved.

If $t = 0$, a simpler formula can be given than that provided by the theorem. To obtain this, note that the integers u between 0 and $p - 1$, inclusive, can be classified according to the value of (u, p). For any divisor d of p, there are exactly $\phi(d)$ values of u for which $(u, p) = p/d$, namely those of the form $u = vp/d$, where $(v, d) = 1$ and $0 \leqq v < d$. Each such u is part of a cycle of length e, where e is the smallest positive integer such that $uk^e \equiv u \pmod{p}$, or $vk^e \equiv v \pmod{d}$, or $k^e \equiv 1 \pmod{d}$, that is, where $e = E_k(d)$. Thus the $\phi(d)$ values of u for which $(u, p) = p/d$ fall into exactly $\phi(d)/E_k(d)$ cycles each of length $E_k(d)$, so that

$$C(k, 0) = \sum_{d|p} \phi(d)/E_k(d).$$

TABLE I

Number of Equivalence Classes under G

p	$N(p)$	$N'(p)$
1	2	2
2	3	1
3	4	2
4	6	3
5	6	4
6	13	8
7	10	8
8	24	18
9	22	18
10	45	38
11	30	28
12	158	142
13	74	72
14	245	234
15	368	360
16	693	669
17	522	520
18	2,637	2,606
19	1,610	1,608
20	7,341	7,293
30	4,500,267	4,499,852
31	2,311,470	2,311,468

Note that whenever $(p, k-1)$ divides t, there exists a residue c such that $ck + t \equiv c \pmod{p}$. Consequently, $uk + t \equiv (u - c)k + c \pmod{p}$ for every residue u, so that g_k^t is the image of g_k^0 under an appropriate inner automorphism, $g_k^t = g_1^c g_k^0 (g_1^c)^{-1}$. Thus g_k^t and g_k^0 have the same cycle structure. Hence, if $(p, k-1)$ divides t, we have

$$C(k, t) = C(k, 0) = \sum_{d|p} \phi(d)/E_k(d).$$

4. Some calculations

In the special case that p is prime, $k - 1$ is relatively prime to p for all k other than $k = 1$, so that in this case

$$N(p) = (1/p(p-1))[b^p + (p-1)b + pb \sum_{k=2}^{p-1} b^{(p-1)/E_k(p)}].$$

Now, if g is a primitive root modulo p,

$$E_{g^i}(p) = (p-1)/(p-1, i),$$

and so the preceding formula for $N(p)$ (valid when p is prime) can be written

$$N(p) = (1/p(p-1))[b^p + (p-1)b + pb \sum_{d|(p-1), d \neq p-1} b^d \phi((p-1)/d)].$$

For any p, since $C(1, 0) = p$ and $C(k, t) \leqq p$ for any pair k, t, it is imme-

diate that[2]

$$b^p/p^2 < b^p/p\phi(p) < N(p) < b^p.$$

Hence, given any $\varepsilon > 0$, there exists a p_0 such that

$$b^{(1-\varepsilon)p} < N(p) < b^p$$

whenever $p > p_0$.

Table I presents the numbers of equivalence classes for periods up to $p = 31$, and for $b = 2$ (binary sequences).

References

1. N. J. Fine, *Classes of periodic sequences*, Illinois J. Math., vol. 2 (1958), pp. 285–302.
2. E. N. Gilbert and J. Riordan, *Symmetry types of periodic sequences*, Illinois J. Math., vol. 5 (1961), pp. 657–665.
3. J. Riordan, *An introduction to combinatorial analysis*, New York, Wiley, 1958.
4. R. C. Titsworth, *Correlation properties of cyclic sequences*, Ph.D. Thesis, California Institute of Technology, Pasadena, California, 1962.
5. G. Pólya, *Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen*, Acta Math., vol. 68 (1937), pp. 145–254.
6. G. Birkhoff and S. MacLane, *A survey of modern algebra*, New York, Macmillan, 1953.

California Institute of Technology
Pasadena, California

[2] The author is grateful to Professor Paul T. Bateman for pointing out this relation.