INFORMATION AND CONTROL 42, 125–130 (1979)

Two-Dimensional Binary Arrays with Good Autocorrelation

Y. K. CHAN, M. K. SIU, AND P. TONG

Department of Mathematics, University of Hong Kong, Hong Kong

Calabro and Wolf (1968, *Inform. Contr.* 11) investigate the autocorrelation properties of certain periodic two-dimensional arrays. This note points out a relationship between periodic $p \times q$-arrays with two-level autocorrelation and difference sets in the group $C(p) \times C(q)$, where $C(n)$ denote the cyclic group of order n. This observation enables us to construct several families of such arrays, some of which are perfect.

1. Calabro and Wolf (1968) investigate the autocorrelation properties of certain periodic two-dimensional arrays. This note points out a relationship between periodic $p \times q$-arrays with two-level autocorrelation and difference sets in the group $C(p) \times C(q)$, where $C(n)$ denotes the cyclic group of order n. This observation enables us to construct several families of such arrays, some of which are perfect, i.e. with zero autocorrelation for all out-of-phase shifts.

A periodic binary $p \times q$-array is an infinite matrix $A = (a(i,j))$ with $i, j = 0, 1, 2, \ldots$, where $a(i,j)$ is either 0 or 1 and where p, q are the smallest positive integers such that

$$a(i,j) = a(i, j+q) = a(i+p, j) \qquad \text{for all } i, j.$$

When no confusion can arise we sometimes regard it as a $p \times q$-matrix $A = (a(i,j))$ with $i = 0, 1, 2, \ldots, p-1$, $j = 0, 1, 2, \ldots, q-1$. Since this is the only type of arrays we shall be looking at in this note, we simply call them $p \times q$-arrays. The autocorrelation function of A is given by

$$R_A(r,s) = \sum_{i=0}^{p-1} \sum_{j=0}^{q-1} b(i,j)\, b(i+r, j+s)$$

where $b(i,j) = 1 - 2a(i,j)$. We say A has two-level autocorrelation if R_A is of the form

$$R_A(r,s) = \begin{cases} pq & \text{if } r \equiv 0 \pmod p \text{ and } s \equiv 0 \pmod q \\ c & \text{if otherwise.} \end{cases} \tag{1}$$

A is said to be *perfect* if c (in (1)) is equal to zero.

A subset $D = \{g_1, \ldots, g_k\}$ of a group G of order v is called a (v, k, λ)-difference set if the equation $g_i g_j^{-1} = g$ has exactly λ solutions for every $g \neq 1$ in G. In what follows we shall be looking at the case $G = C(p) \times C(q)$, and we shall use the additive notation.

0019-9958/79/080125-06$02.00/0

2. It is well-known (see Baumert, 1971, Chap. I) that periodic binary sequences with two-level autocorrelation correspond to cyclic difference sets (i.e. difference sets in cyclic groups). The following result is a natural generalization.

PROPOSITION 1. (a) Let D be a (pq, k, λ)-*difference set in* $C(p) \times C(q)$, *and let* $A = (a(i,j))$ *be defined by*

$$a(i,j) = \begin{cases} 0 & \text{if } (i,j) \in D \\ 1 & \text{if otherwise,} \end{cases}$$

then A *has two-level autocorrelation with* c *(in* (1)*) equal to* $pq - 4(k - \lambda)$.

(b) *Let* $A = (a(i,j))$ *be a* $p \times q$*-array with two-level autocorrelation (see* (1)*), then* $pq + pqc - c$ *is a perfect square, say* m^2, *and* $D = \{(i,j) \in C(p) \times C(q) \mid a(i,j) = 0\}$ *is a difference set with parameters* $(pq, \frac{1}{2}(pq - m), \frac{1}{4}(pq + c - 2m))$ *or* $(pq, \frac{1}{2}(pq + m), \frac{1}{4}(pq + c + 2m))$. *If we restrict our attention to* $p \times q$*-arrays with more* 1*'s than* 0*'s, then the former is the case.*

Proof. (a) Let $\lambda(r,s)$ be the number of matching 0's between A and the (r,s)-translate of A (i.e. with (i,j)th entry equal to $a(i+r, j+s)$). It is not hard to see that, for $r \not\equiv 0 \pmod{p}$ or $s \not\equiv 0 \pmod{q}$, $\lambda(r,s)$ is equal to the number of solution pairs (d_i, d_j) with $d_i, d_j \in C(p) \times C(q)$ and $d_i - d_j = (r,s)$, which is a constant $(= \lambda)$ by hypothesis. From this we can compute c, which turns out to be $pq - 4(k - \lambda)$.

(b) Note that

$$pq + (pq - 1)c = \sum_{r=0}^{p-1} \sum_{s=0}^{q-1} R_A(r,s) = m^2,$$

where $m = \sum_{i=0}^{p-1} \sum_{j=0}^{q-1} b(i,j)$ is the difference between the number of 0's and 1's. Again, by similar argument as in (a), we have $c = pq - 4(k - \lambda(r,s))$ where k is the number of 0's. This implies $\lambda(r,s)$ is a constant for $r \not\equiv 0 \pmod{p}$ or $s \not\equiv 0 \pmod{q}$. Finally, k can be computed from m and pq. Q.E.D.

EXAMPLE I. Let $f: G \to G'$ be an isomorphism of groups. It is clear that D is a difference set in G if and only if $f(D)$ is a difference set in G'. We thus obtain $p \times q$-arrays with two-level autocorrelation when $(p,q) = 1$ by choosing cyclic difference sets with parameters (pq, k, λ), using the isomorphism f: $C(pq) \to C(p) \times C(q)$ given by $f(s) = (xs, ys)$ where $xq + yp = 1$. In particular, case (b) of Theorem 2 in Calabro and Wolf (1968) is obtained by choosing the twin-prime set (see Baumert (1971), Theorem 5.27) when p, q are twin primes.

If D is a difference set in a group G, then for $g \in G$, its g-translate $D + g = \{d + g \mid d \in D\}$ is also a difference set. Two difference sets D_1, D_2 are said to be equivalent if $D_2 = f(D_1) + g$ for some g in G and some automorphism $f: G \to G$.

When $G = C(p) \times C(q)$, $D + (r, s)$ corresponds to the $(-r, -s)$-translate of the array corresponding to D. For $(p, q) = 1$, any automorphism of $C(p) \times C(q)$ sends (x, y) to (rx, sy) where $(r, p) = (s, q) = 1$, and its effect on the corresponding array amounts to forming the new array whose (i, j)th entry is $a(r'i, s'j)$ with $rr' \equiv 1 \pmod{p}$ and $ss' \equiv 1 \pmod{q}$. For $(p, q) \neq 1$, the effect of an automorphism of $C(p) \times C(q)$ on the corresponding array may be more complicated.

EXAMPLE II. McFarland (1973) constructs $\frac{1}{2}(q^s + 1)$ inequivalent difference sets in the group $E \times K$ where E is an elementary abelian group of order q^{s+1} and K is any group of order $[(q^{s+1} - 1)/(q - 1)] + 1$, where q is an odd prime power. By taking q to be an *odd prime*, $s = 1$ and K to be $C(q + 2)$, and observing that $C(q) \times C(q) \times C(q + 2)$ is isomorphic to $C(q) \times C(q(q + 2))$, we obtain $\frac{1}{2}(q + 1)$ inequivalent difference sets in $C(q) \times C(q(q + 2))$ and hence $\frac{1}{2}(q + 1)$ $q \times q(q + 2)$-arrays with two-level autocorrelation with c (in (1)) equal to $q^2(q - 2)$.

The explicit construction is as follows. It is obtained by tracing the isomorphism $f: C(q) \times C(q) \times C(q + 2) \to C(q) \times C(q(q + 2))$ given by $f(x, y, z) = (x, y(q + 2) + zq)$. For a given $t = -1, 0, 1, 2, \ldots, \frac{1}{2}(q - 3)$, we put $A_t = (a_t(i, j))$ where

$$a_t(i, j) = \begin{cases} 0 & \text{if } (i, j) = (sl + 1, (q + 2)s + ql) \\ & \quad \text{or } (sk, (q + 2)s + qk) \\ & \quad \text{or } (s, q^2) \\ & \quad \text{with } l = 0, 1, \ldots, t,\ k = t + 1, \ldots, q - 1, \\ & \qquad s = 0, 1, \ldots, q - 1 \\ 1 & \text{if otherwise.} \end{cases}$$

(For $t = -1$, it is to be understood that l does not appear in the description of (i, j) and k ranges from 0 to $q - 1$). Altogether this gives $\frac{1}{2}(q + 1)$ arrays with two-level autocorrelation.

When q is an odd prime with $q + 2$ a perfect square, say n^2 (e.g. $(q, n) = (7, 3), (23, 5), (47, 7), \ldots$), then by choosing K to be $C(n) \times C(n)$ we obtain in a similar manner $\frac{1}{2}(q + 1)$ $qn \times qn$-arrays with two level autocorrelation with $c = q^2(q - 2)$.

3. It is desirable to obtain perfect $p \times q$-arrays, which corresponds to $(4N^2, 2N^2 - N, N^2 - N)$-difference sets in $C(p) \times C(q)$ by Proposition 1. Again we restrict our attention to arrays with more 1's than 0's.

For $(p, q) = 1$, the group $C(p) \times C(q)$ is isomorphic to $C(pq)$. It is conjectured that no cyclic $(4N^2, 2N^2 - N, N^2 - N)$-difference set exists except for $N = 1$. Turyn (1968) has verified the conjecture for $N < 55$. Thus it seems that (1 1 1 0) is the only possible perfect $p \times q$-array with $(p, q) = 1$.

For $(p, q) \neq 1$, Calabro and Wolf (1968) give the two perfect arrays

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

which are obtained from (1 1 1 0). We shall now produce two more families of perfect arrays.

EXAMPLE III. Spence (1977) constructs three inequivalent (36, 15, 6)-difference sets in $C(6) \times C(6)$ and four inequivalent (36, 15, 6)-difference sets in $C(3) \times C(12)$. Thus we obtain three corresponding perfect 6×6-arrays and four corresponding perfect 3×12-arrays. An example of each type is given below.

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

EXAMPLE IV. Let D_1 be a (36, 15, 6)-difference set in $C(3) \times C(12)$, and let D_2 be the trivial (4, 1, 0)-difference set in $C(4)$. The subset $D = (D_1, \bar{D}_2) \cup (\bar{D}_1, D_2)$, where $\bar{D}_1$ and $\bar{D}_2$ denote the complementary difference sets of D_1 and D_2 respectively, is a (144, 66, 30)-difference set in $C(3) \times C(12) \times C(4)$ by Theorem 2 of Menon (1962). As $C(3) \times C(12) \times C(4)$ is isomorphic to $C(12) \times C(12)$, we obtain four perfect 12×12-arrays from the four inequivalent difference sets in $C(3) \times C(12)$ in Spence (1977) by this method. Again we just give one example below.

$$\begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

If we take both D_1 and D_2 to be the trivial (4, 1, 0)-difference set in $C(4)$, we obtain via this method the perfect 4×4-array given by Calabro and Wolf (1968) mentioned at the beginning of this section.

4. We summarize the preceding results in Table I (for $v \leqslant 200$ and $p \leqslant q$). Most of the entries come from Table 6.1 of Baumert (1971). We shall omit all $1 \times v$-arrays (which are simply sequences of period v) and all trivial cases (which correspond to trivial difference sets with $k - \lambda = 0$ or 1). The last column in Table 1 refers to the type of example described in this note.

TABLE I

v	p	q	c	Type
4	2	2	0	Calabro and Wolf (1968)
15	3	5	−1	I
16	4	4	0	IV
21	3	7	5	I
35	5	7	−1	I
36	3	12	0	III
36	6	6	0	III
40	5	8	4	I
45	3	15	9	II
57	3	19	29	I
63	7	9	−1	I
85	5	17	21	I
91	7	13	55	I
133	7	19	89	I
133	7	19	33	I
143	11	13	−1	I
144	12	12	0	IV
156	3	52	56	I
156	4	39	56	I
156	12	13	56	I
175	5	35	75	II
183	3	61	131	I

ACKNOWLEDGMENT

The authors wish to thank the referee for suggesting many helpful comments.

RECEIVED: June 3, 1977; REVISED: March 24, 1978

Note added in proof. The authors wish to thank the referee for pointing out the following additional references. Turyn, R. (1965), Character sums and difference sets, *Pacific J. Math.* **15**, 319–346; MacWilliams, F. J., and Sloane, N. J. A. (1976), Pseudo-random sequences and arrays, *Proc. IEEE.* **64**, 1715–1729.

REFERENCES

BAUMERT, L. D. (1971), "Cyclic Difference Sets," Springer–Verlag, New York.

CALABRO, D., AND WOLF, J. K. (1968), On the synthesis of two-dimensional arrays with desirable correlation properties, *Inform. Contr.* **11**, 537–560.

MCFARLAND, R. L. (1973), A family of difference sets in non-cyclic group, *J. Combinatorial Theory Ser. A* **15**, 1–10.

MENON, P. K. (1962), On difference sets whose parameters satisfy a certain relation, *Proc. Amer. Math. Soc.* **13**, 739–745.

SPENCE, E. (1977), A family of difference sets, *J. Combinatorial Theory Ser. A* **22**, 103–106.

TURYN, R. (1968), Sequences with small correlations, *in* "Error Correcting Codes" (H. B. Mann, Ed.), pp. 195–228, Wiley, New York.