The Combinatorics of Binary Arrays

Man Keung SIU

Department of Mathematics

The University of Hong Kong

August 25, 1995

Abstract. This paper gives an account of the combinatorics of binary arrays, mainly concerning their randomness properties. In many cases the problem reduces to the investigation on difference sets.

AMS Subject Classification: 05B10, 05B99

Key words: autocorrelation, binary arrays, difference sets

1. INTRODUCTION

This paper is an expanded and updated version of Siu (1993), which in turn can be regarded as a synoptic version of the sequel to the survey by Siu (1989) on binary sequences, promised therein but long overdue as a result of procrastination on the author's part. The subject of discussion in this paper is the two-dimensional analogue of a periodic binary sequence, viz. a periodic binary array, i.e. an infinite array $\boldsymbol{a} = (a_{ij})$ with $a_{ij} \in \mathbb{F}_2$, i, j running through all non-negative integers and $a_{ij} = a_{i+r,j} = a_{i,j+s}$ for all i, j. We will call such an array a periodic $\boldsymbol{r \times s}$ **array**. (Sometimes we actually require r, s to be the smallest such integers.) Throughout this paper we will omit the adjective "periodic" and even regard a periodic $r \times s$ array as a binary $r \times s$ matrix whenever that proves convenient.

We will also omit the adjective "binary" because we will not discuss any case other than that, although it should be noted that many results have their q-ary analogues.

To keep this paper within reasonable length we have not included illustrative examples, and we do not claim to have given full documentation on the results. For details reader can consult references cited together with their bibliographies. For applications readers can consult relevant items in the bibliographies of references cited, most of which are in the area of telecommunication or computer science, (but in Clapham (1986), Grünbaum and Shepherd (1980) readers will find applications in a totally different direction). In this paper we will treat only the mathematical content of these problems.

2. WINDOW PROPERTY

In this section our objective is to recover every possible $m \times n$ array as a subarray in an $r \times s$ array in a most economical way, i.e. construct (if possible) an $r \times s$ array with $rs = 2^{mn}$ in which all $m \times n$ subarrays are distinct. In Fan and Siu (1989) such an array is called an $(\boldsymbol{r}, \boldsymbol{s}\,; \boldsymbol{m}, \boldsymbol{n})$-$\boldsymbol{M}$-**array**. (The topic was treated under different names by various authors. See Chung, Diaconis and Graham (1992), Clapham (1986), Cock (1988), Hurlbert and Isaak (1993), Iványi and Toth (1988).) The special case when $r = m = 1$ (or $s = n = 1$) is the well-known topic of a **de Bruijn sequence**. (See Fredricksen (1982) for a comprehensive account of it.) Reed and Stewart (1962) gave the first example which is a $(4, 4; 2, 2)$-M-array (under the name of a **perfect map**). Ma (1984) took the next significant step in constructing a $(2^m, 2^{m(n-1)}; m, n) - M-$array $(n \geq 3)$ from a de Bruijn sequence of span m. Using a graph-theoretic language on cycles in the "2-dimensional de Bruijn graph" and extending the idea of the Lempel homomorphism (in Lempel (1970)), Fan, Fan, Ma and Siu (1985) succeeded in constructing certain M-arrays from smaller ones. In particular, it is proved that there exists an $(r, s; m, n)$-M-array for some r, s

when m, n are given, and that there is an $(r, r; m, m)$-M-array if and only if m is even. The last result settles a special case completely since a necessary condition for existence of an $(r, s; m, n)$-M-array is clearly $rs = 2^{mn}$. For $r > 1$, $s > 1$, this necessary condition is no longer sufficient since we must also have $r > m$ and $s > n$. Etzion (1988) gave a construction for a large class of M-arrays. Combining the construction by Etzion and that by Fan, Fan, Ma and Siu, and making use of linear complexity of binary sequences (discussed in Chan, Games and Key (1982)), Paterson (1994) proved that, with that additional conditions amended, we have a necessary and sufficient condition for existence of M-arrays. The "aperiodic" analogue of the problem was formulated and solved by Mitchell (1995).

Techniques used in treating the problem above are purely combinatoric in nature. But when we ask a similar question, viz. look for an $r \times s$ array with $rs = 2^{mn} - 1$ in which all $m \times n$ subarrays are distinct and NONZERO, we can bring in linear algebra to our rescue. In Fan and Siu (1989) such an array is called an $(\boldsymbol{r}, \boldsymbol{s}\,; \boldsymbol{m}, \boldsymbol{n})$-$\boldsymbol{m}$-**array**. Again, the necessary condition $rs = 2^{mn} - 1$ is not sufficient in general. But for $r = m = 1$ (resp. $s = n = 1$), $s = 2^n - 1$ (resp. $r = 2^m - 1$) is a necessary and sufficient condition. Indeed, take a de Bruijn sequence of span n and delete one zero from the (unique) n-tuple of zeros, one obtains a $(1, s; 1, n) - m$-array. However, there is another well-known object called a **maximal length sequence** (see MacWilliams and Sloane (1976), Zierler (1959)) which also serves this purpose but which has a strong algebraic flavour. Although an M-array is a 2-dimensional analogue of a de Bruijn sequence, an m-array is, strictly speaking, NOT a 2-dimensional analogue of a maximal length sequence. The strict analogue of a maximal length sequence is an $(r, s; m, n)$-m-array satisfying a "linear recurrence", usually referred to as an $\boldsymbol{LR}$-$\boldsymbol{m}$-**array**. In the 2nd Chinese Combinatorial Conference in 1985 Fan and Siu (1989) gave a general formulation that includes all the previously known constructions of LR-m-arrays discussed in Gordon (1966), MacWilliams and Sloane (1976), Nomura,

Miyakawa, Imai and Fukuda (1972). Let r, s be relatively prime positive integers such that $rs = 2^{mn} - 1$, and let α be a primitive element of $\mathbb{F}_{2^{mn}}$. Let $\varphi : \mathbb{Z}_r \times \mathbb{Z}_s \to \mathbb{Z}_{rs}$ be a group isomorphism. If $\{\alpha^{\varphi(i,j)} | 0 \le i < m, 0 \le j < n\}$ is a basis for $\mathbb{F}_{2^{mn}}$ (as a vector space over $\mathbb{F}_2$) and $L : \mathbb{F}_{2^{mn}} \to \mathbb{F}_2$ is a nonzero linear functional, then $A = (a_{ij})$ where $a_{ij} = L(\alpha^{\varphi(i,j)})$ can be verified to be an $(r, s; m, n)$-m-array. (Geometrically, we are "folding up" a maximal length sequence of length $2^{mn} - 1$ into an $r \times s$ array.) As a corollary, there exists an $(r, s; m, n)$-m-array for some r, s when m, n are given. The author posed in 1985 the natural question: Are all LR-m-arrays obtained in this way? Lin and Liu (1988, 1993) settled the query in the affirmative and showed that indeed a necessary and sufficient condition for this to happen is that r, s are relatively prime positive integers with $rs = 2^{mn} - 1$. In this sense the study of LR-m-arrays is reduced to the study of maximal length sequences. But of course there are $(r, s; m, n)$-m-arrays which are not LR-m-arrays.

3. AUTOCORRELATION PROPERTY

A maximal length sequence possesses certain characteristic features of pseduo-randomness (see MacWilliams and Sloane (1976), Siu (1989)), one of which is the autocorrelation property, viz. the numbers of $0*\cdots*0$, $0*\cdots*1$, $1*\cdots*0$, $1*\cdots*1$ (asterisks in between signify an arbitrary string of prescribed length) are nearly equal. This has its natural extension to an array $\boldsymbol{a} = (a_{ij})$. The **real periodic autocorrelation function**, defined by

$$RP(u, v) = \sum_{i=0}^{r-1} \sum_{j=0}^{s-1} b_{ij} b_{i+u, j+v} \ , \quad u, v \in \mathbb{Z}^+ \cup \{0\}$$

where $b_{ij} = (-1)^{a_{ij}}$, measures the number of coinciding entries (both 0 or both 1) minus the number of non-coinciding entries between $\boldsymbol{a}$ and its (u, v)-translate, i.e. the array

$(a_{i+u,j+v})$. The **binary periodic autocorrelation function**, defined by

$$BP(u,v) = \sum_{i=0}^{r-1}\sum_{j=0}^{s-1} a_{ij}a_{i+u,j+v} \ , \quad u,v \in \mathbb{Z}^+ \cup \{0\} \ ,$$

measures the number of coinciding 1's between $\boldsymbol{a}$ and its (u,v)-translate. The objective is to construct $\boldsymbol{a}$ with $|RP(u,v)|$ or $BP(u,v)$ small for $(u,v) \not\equiv (0,0) \bmod (r,s)$, and in some applications we even want $RP(u,v)$ or $BP(u,v)$ to take on exactly two values, i.e. a common off-phase value. We call the latter **two-level autocorrelation property**. Suppose k is the number of 1's in $\boldsymbol{a}$, i.e. the **weight** of $\boldsymbol{a}$, then by counting it is not hard to see that $RP(u,v) = rs - 4k + 4BP(u,v)$. Hence $RP(u,v)$ takes on two values if and only if $BP(u,v)$ takes on two values.

Let us look at an array $\boldsymbol{a}$ with two-level autocorrelation property, viz. $RP(u,v) = c$ (or $BP(u,v) = \lambda$) for all $(u,v) \not\equiv (0,0) \bmod (r,s)$. Note that $c = rs - 4k + 4\lambda = rs - 4n$ where $n = k - \lambda$. If we let $D = \{d_1, \ldots, d_k\}$ be a subset of $\mathbb{Z}_r \times \mathbb{Z}_s$ defined by $d = (i,j) \in D$ if and only if $a_{ij} = 1$, then this is equivalent to saying that the family of $d_i - d_j$ $(i \neq j)$ consists of all nonzero elements of $\mathbb{Z}_r \times \mathbb{Z}_s$, each repeated λ times. Such an object is well-known in combinatorial mathematics and is called a **difference set** in the group $\mathbb{Z}_r \times \mathbb{Z}_s$ with parameters (rs, k, λ). (Some standard references for difference sets are Baumert (1971), Beth, Jungnickel and Lenz (1983), Jungnickel (1989), Lander (1983). For surveys on difference sets, see Arasu (1990), Ma (1994), Jungnickel (1992), and the recent monograph by Pott (1995).). The parameter $n = k - \lambda$ is called its **index**. ¿From this interpretation it is easy to see a necessary condition, viz. $k(k-1) = \lambda(rs-1)$. A **perfect $r \times s$ array** is an array with two-level autocorrelation and $c = 0$. Since $rs = \sum_{u=0}^{r-1}\sum_{v=0}^{s-1} RP(u,v) = \big(\sum_{i=0}^{r-1}\sum_{j=0}^{s-1} b_{ij}\big)^2 = [(\text{number of } 0) - (\text{number of } 1)]^2$ and $rs = 4n$, we see that a necessary condition for a perfect $r \times s$ array is $rs = 4N^2$ where $N^2 = n = k - \lambda$. Actually, a perfect $r \times s$ array corresponds to a difference set in $\mathbb{Z}_r \times \mathbb{Z}_s$ with parameters $(4N^2, 2N^2 \pm N, N^2 \pm N)$. Menon (1962) investigated difference sets of index n in an abelian group of order $4n$. (The definition for a difference set given above is valid for an abelian

group word for word, and with obvious modification it applies to a non-abelian group as well.) It turns out $n = N^2$ and the parameters are $(4N^2, 2N^2 \pm N, N^2 \pm N)$. Such a difference set is therefore known as a **Menon difference set**. (Some authors prefer to call such an object an **Hadamard difference set**, although confusion may arise from the fact that this name had already been used in earlier times to refer to a difference set with parameters $(4n-1, 2n-1, n-1)$!) When $(r,s) = 1$, the situation reduces to a Menon difference set in $\mathbb{Z}_{rs}$ or to a perfect sequence. A conjecture says that there is no Menon difference set in a cyclic group except $\mathbb{Z}_4$, or in terms of perfect arrays, the only perfect $r \times s$ arrays with $(r,s) = 1$ are (0001) or (1110) or their transpose. An account on the relationship between this conjecture and a number of other conjectures in combinatorial designs was given by Siu (1989). Despite several purported proofs, this conjecture remains open (see Jedwab and Lloyd (1992), Lin and Wallis (1993) for further clarification). We now turn to the case when $(r,s) > 1$. Calabro and Wolf (1968) gave the first example of a 2×2 and a 4×4 perfect array. Chan, Siu and Tong (1979), by relating the object to a difference set, gave examples of 6×6 and 3×12 perfect arrays a decade later. There began a surge of interest in perfect arrays from engineers in the late 1980s (see Lüke and Bömer (1989) for an account in engineering, and Chan and Siu (1991) for a brief survey up to 1990). In the meantime, mathematicians approached the same topic in the language of Menon difference sets. Menon (1962) showed that a Menon difference set of index $4n_1n_2$ in $G_1 \times G_2$ can be constructed from a Menon difference set of index n_1 in G_1 and a Menon difference set of index n_2 in G_2. Turyn (1984) proved the existence of Menon difference sets of index $3^{2s} (s \geq 1)$. Therefore Menon difference sets of index $(2^a \cdot 3^b)^2$ exist for all $a \geq 0$, $b \geq 0$. McFarland conjectured that this sufficient condition on the index is also necessary, but recently this was, to the great surprise of many, refuted by Xia (1992), who gave an example of a Menon difference set in the direct product of $\mathbb{Z}_4$ and a finite number of $\mathbb{Z}_{p_i}$ where each p_i is a prime satisfying $p_i \equiv 3 (\mathrm{mod} 4)$. (Smith (1995) gave a counter-

example in the case of a non-abelian group by finding a difference set with parameters $(100, 45, 20)$ using group representation. His example is particularly interesting, since it has been shown that no Menon difference set exists in an ABELIAN group of order 100.) The construction of Xia involves complicated calculation with cyclotomic classes. Recently Xiang and Chen (1994) gave a character theoretic proof of Xia's example from a new viewpoint. In the direction of nonexistence, the classic result is a theorem of Turyn (1965), giving upper bounds on the exponent of certain Sylow subgroups of an abelian group containing a Menon difference set. (This seminal paper of Turyn (1965) initiated the use of character theory in the study of the subject of difference sets, which reduces the problem to the solution of a certain equation in an integral group ring. See Pott (1995) for a succinct account of the detailed mathematics.) McFarland (1989) proved a result in favour of his conjecture (which we now know is incorrect), viz. if an abelian group G of order $4p^2$ (p a prime number) has a Menon difference set, then $p = 2$ or 3. Interpreting Turyn's basic theorem in the case of $\mathbb{Z}_r \times \mathbb{Z}_s$, we obtain necessary conditions on the size of $r \times s$ perfect arrays with $rs = 4N^2$, $N = p^d$ where p is a prime number, viz. (i) $2^{d+1} \times 2^{d+1}$ or $2^d \times 2^{d+2}$ $(d \geq 0)$; (ii) $2 \cdot 3^d \times 2 \cdot 3^d$ or $3^d \times 4 \cdot 3^d$ or $2 \cdot 3^{d-1} \times 2 \cdot 3^{d+1}$ or $3^{d+1} \times 4 \cdot 3^{d-1}$ or $3^{d-1} \times 4 \cdot 3^{d+1}$ $(d \geq 1)$; (iii) $2 \cdot p^d \times 2 \cdot p^d$ or $p^d \times 4 \cdot p^d$ for $p \geq 5$ $(d \geq 1)$. In recent years various authors have constructed perfect arrays for certain cases among those allowable cases listed above (see Arasu, Davis, Jedwab and Sehgal (1993), Davis (1991), Dillon (1990), Jedwab, Mitchell, Piper and Wild (1994)) or proved nonexistence in other cases (see Arasu and Jedwab (1992), Chan (1993), Chan and Siu (1991), Chan, Siu and Ma (1994), Jedwab (1991)). For an updated survey see Davis and Jedwab (1994).

We now turn to the case of $BP(u, v) = \lambda$ for all $(u, v) \not\equiv (0, 0) \bmod (r, s)$. Since $k(k-1) = \lambda(rs-1)$, we see that only trivial cases (no 1 in $\boldsymbol{a}$, or exactly one 1 in $\boldsymbol{a}$) can satisfy the condition $\lambda = 0$. The next best to hope for is when $\lambda = 1$. This happens if and only if $rs = n^2 + n + 1$ where $n = k - 1$. Hence we are looking for a difference

set of index n in $\mathbb{Z}_r \times \mathbb{Z}_s$ with parameters $(n^2+n+1, n+1, 1)$. Using finite projective geometry Singer (1938) constructed such difference sets in $\mathbb{Z}_{n^2+n+1}$. For $rs = n^2+n+1$ with $(r,s)=1$ this yields $r \times s$ arrays with $\lambda = 1$. For the special case of a square array (i.e. $r = s$), this is impossible unless $r = s = 1$. However, in some applications we relax the condition to $BP(u,v) \leq 1$ for all $(u,v) \not\equiv (0,0) \bmod (s,s)$ (so the array has three-level autocorrelation rather than two-level). It can be shown that in this case the weight k of $\boldsymbol{a}$ cannot exceed s. In the optimal case when $k = s$, $BP(u,v)$ takes on the value k once, the value 0 $s-1$ times and the value 1 s^2-s times (see Fung, Siu and Ma (1990)). In those applications we also require that the s 1's are so placed that each column has exactly one 1. Such a matrix is called an **ideal matrix** by Kumar (1988). An alternative formulation is to construct a function $f : \mathbb{Z}_s \to \mathbb{Z}_s$ satisfying the condition that f_v is injective for all $v \neq 0$, where $f_v(j) = f(j+v) - f(j)$. The correspondence is to put $f(j) = i$ if and only if $a_{ij} = 1$. In the literature such a function is called a **planar function** on $\mathbb{Z}_s$. When $s = p$ is a prime number, f can be expressed as a polynomial function of degree ℓ less than p (by Lagrange Interpolation). Obviously if $p > 2$ and $\ell = 2$, f_v is injective for all $v \neq 0$, i.e. f is planar. Actually, this is the only possible case for f to be planar, as proved independently by Gluck (1990), Hiramine (1989), Rónyai and Szönyi (1989). There is no planar function on $\mathbb{Z}_s$ with s odd because $0 = \sum_{j=0}^{s-1} f_v(j) = 1+2+\cdots+(s-1) = s(s-1)/2$. Translating back to the language of ideal matrix, this means that for the case $s = p$ (p a prime number), we know everything about an $s \times s$ ideal matrix. What about the case when s is an odd composite number? The main conjecture is: An $s \times s$ ideal matrix exists if and only if s an odd prime (and hence corresponds to a quadratic function). Kumar (1988) had shown that a finite projective plane of order s can be constructed from an $s \times s$ ideal matrix. A long-standing conjecture says that the order of a finite projective plane must be a power of a prime. (The case of order 10 was confirmed by Lam, Thiel and Swiercz (1989).) By formulating the problem in a group algebra and using factorization

of ideals in cyclotomic fields, Fung, Siu and Ma (1990) proved that existence of an $s \times s$ ideal matrix implies s is square-free. Hence, granting the conjecture on finite projective plane, the conjecture on ideal matrix will be settled in the affirmative. Hiramine (1992) proved (in a setting which is somewhat more general) that if there exists a planar function on $\mathbb{Z}_{3p}$ (p a prime number), then $p < 5$. Hence there does not exist a $3p \times 3p$ ideal matrix where p is an odd prime number. Besides planar functions and finite projective planes, ideal matrices are also intimately related to difference sets. Indeed, an $s \times s$ ideal matrix is equivalent to a so-called relative difference set of parameters $(s, s, s, 1)$ in $\mathbb{Z}_s \times \mathbb{Z}_s$ relative to the subgroup $0 \times \mathbb{Z}_s$. (More generally, $D = \{d_1, \ldots, d_k\}$ is a **relative difference set** of parameters (m, n, k, λ) in an abelian group G of order mn relative to a subgroup H of order n if the family $d_i - d_j$ $(i \neq j)$ consists of all elements of $G \setminus H$, each repeated λ times.) Very recently, Ma (1995) gave another proof of Hiramine's result by applying character theory to the problem formulated as a problem in relative difference sets, and extended the nonexistence to $s = pq$ where p, q are prime numbers. In particular, it is now known that if an $s \times s$ ideal matrix exists for $s \leq 50,000$, then s is a prime number except for the four undecided cases $s = 15655, 29523, 35855$ or 42627. Hence the first unsettled case concerning the conjecture stands now at $s = 15655$ instead of the previous $s = 55$.

4. APERIODIC CASE

We now turn to investigate the analogous problem of autocorrelation of an array $\boldsymbol{a} = (a_{ij})$ with attention confined to the overlapping part only. The **real aperiodic autocorrelation function**, defined by

$$RA(u, v) = \sum_{i=0}^{r-1} \sum_{j=0}^{s-1} b'_{ij} b'_{i+u, j+v} \ , \quad u, v \in \mathbb{Z}$$

where $b'_{ij} = (-1)^{a_{ij}}$ if $0 \leq i \leq r-1$, $0 \leq j \leq s-1$ and $b'_{ij} = 0$ otherwise, measures the number of coinciding entries (both 0 or both 1) minus the number of non-coinciding

entries between $\boldsymbol{a}$ and its (u, v)-translate on the overlapping part. The **binary aperiodic autocorrelation function**, defined by

$$BA(u, v) = \sum_{i=0}^{r-1} \sum_{j=0}^{s-1} a'_{ij} a'_{i+u, j+v} \ , \quad u, v \in \mathbb{Z}$$

where $a'_{ij} = a_{ij}$ if $0 \leq i \leq r-1$, $0 \leq j \leq s-1$ and $a'_{ij} = 0$ otherwise, measures the number of coinciding 1's between $\boldsymbol{a}$ and its (u, v)-translate on the overlapping part.

Since $BA(u, v) \leq BP(u, v)$, an ideal matrix (See section 3) will satisfy $BA(u, v) \leq 1$ for all $(u, v) \not\equiv (0, 0) \bmod (r, s)$. (The converse is not true.) Costas (1966) investigated, in connection with SONAR signals, $s \times s$ arrays with exactly one 1 in each column and exactly one 1 in each row such that $BA(u, v) \leq 1$ for all $(u, v) \not\equiv (0, 0) \bmod (s, s)$. Today such an array is known as a **Costas array**. For a survey on Costas arrays, see Golomb and Taylor (1982, 1984), Golomb (1991). Constructions by Golomb, Lempel, Welch and Taylor, reported in Golomb (1984), Golomb and Taylor (1982, 1984), guarantee the existence of a Costas array when $s = p - 1$ or $q - 2$ where p is a prime and $q(> 2)$ is a power of a prime. The basic idea can been seen in Welch's construction in which $a_{ij} = 1$ if and only if $j = \alpha^i$ $(0 < i, j < p)$ where α is a preassigned primitive element of $\mathbb{F}_p$. Lempel gave a twist in setting $a_{ij} = 1$ if and only if $\alpha^i + \alpha^j = 1$ $(0 < i, j < q-1)$ where α is a preassigned primitive element of $\mathbb{F}_q$. Golomb further extended the construction by setting $a_{ij} = 1$ if and only if $\alpha^i + \beta^j = 1$ $(0 < i, j < q-1)$ where α, β are preassigned primitive elements of $\mathbb{F}_q$. The last construction has an interesting feature, viz. when $\alpha + \beta = 1$, one obtains a $(q-3) \times (q-3)$ Costas array by deleting the leftmost column and the topmost row. This triggers off concern over a purely algebraic query known as the **Golomb Conjecture:** In any finite field with more than two elements, there exist primitive elements α, β such that $\alpha + \beta = 1$. Various authors contributed to this query since the mid 1980s, and the conjecture (plus some variants of it) was settled in the affirmative around 1990. (see Chang and Kang (1991), Cohen and Mullin (1991), M.H. Le (1990), J.P. Wang (1988) and papers referred to therein.) With this conjecture settled, the first undecided case of existence of

a Costas array is $s = 32$ (the two exceptional cases of $s = 19$ and $s = 31$ were constructed by a sporadic method by Golomb and Taylor (1984)). It is believed (but not yet proved) that an $s \times s$ Costas array exists for each s. A similar question which allows more 1's in the array is more difficult . For instance, as reported in Golomb and Taylor (1982), the largest number of 1's in a 3×3 array with $BA(u, v) \leq 1$ for all $(u, v) \not\equiv (0, 0) \bmod (3, 3)$ is 5 (while a 3×3 Costas array has only 3 1's). It is an open question to know the maximum number of 1's and how to construct such an array.

A related object is the so-called **SONAR array** which is an $r \times s$ array $\boldsymbol{a} = (a_{ij})$ with exactly one 1 in each column satisfying $BA(u, v) \leq 1$ for all $(u, v) \not\equiv (0, 0) \bmod (r, s)$. It corresponds to a **SONAR sequence** (a_i) (with $a_{ij} = 1$ if and only if $i = a_j$) in which $a_j \in \{0, 1, \ldots, r-1\}$ and $a_{i+k} - a_i$ are distinct for all $i \in \{1, 2, \ldots, s-k\}$ for each fixed $k \in \{1, 2, \ldots, s-1\}$ (see Golomb and Taylor (1982)). It is not hard to see that for a given r, the largest value s can attain is $2r$, but known data reported in Robbins and Taylor (1984) seem to purport the fact that the actual attainable value is nearer to r than to $2r$. This is asymptotically confirmed by the bound $s < r + 3r^{2/3} + 2r^{1/3} + 9$ established in Erdös, Graham, Ruzsa and Taylor (1992). Games (1987) constructed certain $r \times s$ SONAR array when s is a power of a prime, using the properties of maximal length sequence and GMW-sequence. (GMW-sequence, related to difference sets constructed by Gordon, Mills and Welch (1962) and hence its name, was discussed in Scholtz and Welch (1984).) For a brief recent survey on sonar sequence, see Moreno, Games and Taylor (1993). Etzion (1990) has applied Costas arrays and sonar sequences to construct arrays with window property (see Section 2).

For the case of $RA(u, v)$, we like to find $r \times s$ array for which $|RA(u, v)| \leq 1$ for all $(u, v) \not\equiv (0, 0) \bmod (r, s)$. Such an array is known as a **Barker array**, discussed in Alquaddoomi and Scholtz (1989). By a counting argument Alquaddoomi and Scholtz (1989) showed that there does not exist an $r \times s$ Barker array where r is an even in-

teger congruent to 2 mod 4 and s is an odd integer larger than 1. Further analysis by Alquaddoomi and Scholtz (1989), Jedwab (1993), Jedwab, Lloyd and Mowbray (1993) revealed a connection between a Barker array and a difference set, viz. (i) when r or s is even, then the existence of an $r \times s$ Barker array implies the existence of a Menon difference set in $\mathbb{Z}_r \times \mathbb{Z}_s$ with parameters $(4N^2, 2N^2 - N, N^2 - N)$, $rs = 4N^2$; (ii) when $rs \equiv 1 (\mathrm{mod} 4)$, the existence of an $r \times s$ Barker array implies the existence of a difference set in $\mathbb{Z}_r \times \mathbb{Z}_s$ with parameters $(2N^2 + 2N + 1, N^2, N(N-1)/2)$, $2rs - 1 = (2N+1)^2$; (iii) when $rs \equiv 3 (\mathrm{mod} 4)$, the existence of an $r \times s$ Barker array implies the existence of a Hadamard difference set in $\mathbb{Z}_r \times \mathbb{Z}_s$ with parameters $(4N-1, 2N-1, N-1)$, $rs = 4N-1$. Results on nonexistence of certain difference sets will thus yield results on nonexistence of certain Barker arrays. The main conjecture stated in Alquaddoomi and Scholtz (1989) is: Apart from $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ (and their obvious derived arrays), there does not exist another $r \times s$ Barker array with $r > 1$, $s > 1$. The case for $r = 1$ or $s = 1$ already arose in the early 1950s when Barker (1953) investigated such sequences, now known as **Barker sequences**, in connection with group synchronization. Up to now we know the existence of Barker sequences of length $1, 2, 3, 4, 5, 7, 11$ or 13. Turyn and Storer (1961) proved that for odd s, the known Barker sequences are the only possible cases, while for even s, the existence of a Barker sequence of length s implies $s = 2$ or $4N^2$ and that furthermore it implies the existence of a Menon difference set in $\mathbb{Z}_s$. (See Siu (1989) for a discussion on its relationship to other conjectures.) Turyn (1968) reported that if a Barker sequence of even length exists, its length must be at least $12100 = 4 \times 55^2$. There is strong evidence that there does not exist any Barker sequence apart from the known cases in view of the conjecture on nonexistence of cyclic Menon difference set with index larger than 1 (see Section 3). Many authors have contributed results on this query (see Eliahou and Kervaire (1992), Eliahou, Kervaire and Saffari (1990), Fredman, Saffari and Smith (1989), Jedwab and Lloyd (1992), Saffari and Smith (1988)). Eliahou and Kervaire (1992) hold the record

to date that there exists no Barker sequence (apart from the known cases) of length less than $4 \times 689^2 = 1898884$, based on the striking result in Eliahou, Kervaire and Saffari (1990) which rules out Barker sequence of even length s having a prime divisor congruent to 3 modulo 4.

References

Alquaddoomi, S. and Scholtz, R.A. (1989). On the nonexistence of Barker arrays and related matters. IEEE Trans. Inform. Theory. IT-35, 1048-1057.

Arasu, K.T. (1990). Recent results on difference sets. In: Ray-Chaudhuri, D., Ed., *Coding Theory and Design Theory, Part II: Design Theory*, Springer-Verlag, Heidelberg, 1-23.

Arasu, K.T. and Davis, J.A. and Jedwab, J. (1992). A nonexistence result for abelian Menon difference sets using perfect binary arrays, HPL-92-140, Hewlett Packard, Bristol.

Arasu, K.T. and Davis, J.A. and Jedwab, J. and Sehgal, S.K. (1993). New constructions of Menon difference sets. J. Comb. Theory. A-64, 329-336.

Barker, R.H. (1953). Group synchronizing of binary digit systems. In: Jackson, W., Ed., *Communication Theory*, Butterworths, London, 273-283.

Baumert, L.D. (1971). *Cyclic Difference Sets*. Springer-Verlag, Heidelberg.

Beth, T. and Jungnickel, D. and Lenz, H. (1983). *Design Theory*. Cambridge University Press, Cambridge.

Calabro, D. and Wolf, J.K. (1968). On the synthesis of two-dimensional arrays with desirable correlation properties. Inform. Control, 11, 537-560.

Chan, A.H. and Games, R.A. and Key, E.L. (1982). On the complexities of de Bruijn

sequences. J. Comb. Theory. A-33, 233-246.

Chan, W.K. (1993). Necessary conditions for Menon difference sets. Designs, Codes and Cryptography. 3, 147-154.

Chan, W.K, and Siu, M.K. (1991). Summary of perfect $s \times t$ arrays, $1 \leq s \leq t \leq 100$. Electron. Lett. 27, 709-710 (correction (1991), Electron. Lett. 27, 1112).

Chan, W.K. and Siu, M.K. and Ma, S.L. (1994). Nonexistence of certain perfect arrays. Discrete Math. 125, 107-113.

Chan, Y.K. and Siu, M.K. and Tong, P. (1979). Two-dimensional binary arrays with good autocorrelation. Inform. Control. 42, 125-130.

Chang, Y.X. and Kang, Q.D. (1991). A representation of nonzero elements in finite fields. Science in China (Series A). 34, 641-649.

Chung, F.R.K. and Diaconis, P. and Graham, R.L. (1992). Universal cycles for combinatorial structures. Discrete Math. 110, 43-59.

Clapham, C.R.J. (1986). Universal tilings and universal $(0, 1)$-matrices. Discrete Math. 58, 87-92.

Cock, J.C. (1988). Toroidal tilings from de Bruiju-Good cyclic sequences. Discrete Math. 70, 209-210.

Cohen, S.D. and Mullen, G.L. (1991). Primitive elements in finite fields and Costas arrays. Appl. Alg. in Engin. Comm. and Comp. 2, 45-53.

Costas, J.P. (1966). Project Medior – A medium-oriented approach to SONAR signal processing, HMED Tech. Publ. R66EMH12, General Electric Co. (originally classified; see also Costas, J.P. (1975). Medium constraints on SONAR design and performance, EASCON Conv. Rec., 68A-68L).

Davis, J.A. (1991). Difference sets in abelian 2-groups. J. Comb. Theory. A-57, 262-286.

Davis, J. and Jedwab, J. (1994). A survey of Hadamard difference sets. HPL-94-14, Hewlett Packard, Bristol.

Dillon, J.F. (1990). Difference sets in 2-groups. In: Kramer, E.S., Ed., *Finite Geometries and Combinatorial Designs*, Contemporary Mathematics. 111, 65-72.

Eliahou, S. and Kervaire, M. (1992). Barker sequences and difference sets. L'Enseignement Math. 38, 345-382. (corrigendum (1994). L'Enseignement Math. 40, 109-111).

Eliahou, S. and Kervaire, M. and Saffari, B. (1990). A new restriction on the lengths of Golay complementary sequences. J. Comb. Theory. A-55, 49-59.

Erdös, P. and Graham, R.L. and Ruzsa, I. and Taylor, H. (1992). Bounds for arrays of dots with distinct slopes or lengths. Combinatorica. 12, 1-6.

Etzion, T. (1988). Constructions for perfect maps and pseudo-random arrays. IEEE Trans. Inform. Theory. IT-34, 1308-1316.

Etzion, T. (1990). On pseudo-random arrays construced from patterns with distinct differences. In: Capocelli, R.M., Ed., *Sequences I: Combinatorics, Compression, Security, and Transmission*, Springer-Verlag, Heidelberg, 195-207.

Etzion, T. (1990). Combinatorial designs derived from Costas arrays. In: Capocelli, R.M., Ed., *Sequences I: Combinatorics, Compression, Security, and Transmission*, Springer-Verlag, Heidelberg, 208-227.

Fan, C.T. and Fan, S.M. and Ma, S.L. and Siu, M.K. (1985). On de Bruijn arrays. Ars Combinatoria. 19A, 205-213.

Fan, S.M. and Siu, M.K. (1989). Construction of m-arrays and M-arrays (in Chinese). Math. in Practice and Theory. 1, 77-86.

Fredman, M.L. and Saffari, B. and Smith, B. (1989). Polynômes réciproques: conjecture d'Erdös en norme L^4, taille des autocorrélations et inexistence des codes de Barker. C.R. Acad. Sci. Paris. 308, Sér I, 461-464.

Fredricksen, H.M. (1982). A survey of full length nonlinear shift register cycle algorithms. SIAM Review. 24, 195-221.

Fung, C.I. and Siu, M.K. and Ma, S.L. (1990). On arrays with small off-phase binary autocorrelation. Ars Combinatoria. 29A, 189-192.

Games, R.A. (1987). An algebraic construction of SONAR sequences using M-sequences. SIAM J. Alg. Discrete Math. 8, 753-761.

Gluck, D. (1990). A note on permutation polynomials and finite geometries. Discrete Math. 80, 97-100.

Golomb, S.W. (1984). Algebraic constructions for Costas arrays. J. Comb. Theory. A-37, 13-21.

Golomb, S.W. (1991). Construction of signals with favourable correlation properties. In: Keedwell, A.D., Ed., *Surveys in Combinatorics, 1991*, Cambridge University Press, Cambridge, 1-39.

Golomb, S.W. and Taylor, H. (1982). Two-dimensional synchronization patterns for minimum ambiguity. IEEE Trans. Inform. Theory. IT-28, 600-604.

Golomb, S.W. and Taylor, H. (1984). Constructions and properties of Costas arrays. Proc. IEEE. 72, 1143-1163.

Gordon, B. (1966). On the existence of perfect maps. IEEE Trans. Inform. Theory. IT-12, 486-487.

Gordon, B. and Mills, W.H. and Welch, L.R. (1962). Some new difference sets. Canadian

J. Math. 14, 614-625.

Grünbaum, B. and Shepherd, G.C. (1980). Satins and twills: An introduction to the geometry of fabrics. Math. Magazine. 53, 139-161.

Hiramine, Y. (1989). A conjecture on affine planes of prime order. J. Comb. Theory. A-52, 44-50.

Hiramine, Y. (1992). Planar functions and related group algebras. J. Algebra. 152, 135-145.

Hurlbert, G. and Isaak, G. (1993). On the de Bruijn torus problem. J. Comb. Theory. A-64, 50-62.

Iványi, A. and Toth, Z. (1988). Existence of de Bruijn words. In: *Proceedings of 2nd Conference on Automata, Languages and Programming Systems*, Salgótarján, Hungary, 165-172.

Jedwab, J. (1991). On the nonexistence of perfect binary arrays. Electron. Lett. 27, 1252-1254.

Jedwab, J. (1993). Barker arrays I — Even number of elements. SIAM J. Disc. Math. 6, 294-308.

Jedwab, J. and Lloyd, S. (1992). A note on the nonexistence of Barker sequences. Designs, Codes and Cryptography. 2, 93-97.

Jedwab, J. and Lloyd, S. and Mowbray, M. (1993). Barker arrays II — Odd number of elements. SIAM J. Disc. Math. 6, 309-328.

Jedwab, J. and Mitchell, C.J. and Piper, F. and Wild, P. (1994). Perfect arrays and difference sets. Discrete Math. 125, 241-254.

Jungnickel, D. (1989). Design theory: An update. Ars Combinatoria. 28, 129-199.

Jungnickel, D. (1992). Difference sets. In: Dinitz, J.H. and Stinson, D.R., Eds., *Contemporary Design Theory: A Collection of Surveys*, Wiley, New York, 241-324.

Kumar, P.V. (1988). On the existence of square dot-matrix patterns having a specific three-valued periodic-correlation function. IEEE Trans. Inform. Theory. IT-34, 271-277.

Lam, C.W.H. and Thiel, L.H. and Swiercz, S. (1989). The non-existence of finite projective planes of order 10. Canadian J. Math. 41, 1117-1123.

Lander, E.S. (1983). *Symmetric Design: An Algebraic Approach*. Cambridge University Press, Cambridge.

Le, M.H. (1990). On Golomb's conjecture. J. Comb. Theory. A-54, 304-308.

Lempel, A. (1970). On a homomorphism of the de Bruijn graph and its applications to the design of feedback shift registers. IEEE Trans. Computers. C-19, 1204-1209.

Lin, C.T. and Wallis, W.D. (1993). On the circulant Hadamard matrix conjecture. In: Jungnickel, D. and Vanstone, S.A., Ed., *Coding Theory, Design Theory, Group Theory: Proceedings of the Marshall Hall Conference*, Wiley, New York, 213-217.

Lin, D.D. and Liu, M.L. (1988). Linear recurring m-arrays. In: Günther, C.G., Ed., *Advances in Cryptology – UROCRYPT '88*, Springer-Verlag, Heidelberg, 351-357.

Lin, D.D. and Liu, M.L. (1993). Structure and properties of linear recurring m-arrays. IEEE Trans. Inform. Theory. IT-39, 1758-1762.

Lüke, H.D. and Bömer, L. (1989). Perfect binary arrays. Signal Process. 17, 69-80.

Ma, S.L. (1984). A note on binary arrays with certain window property. IEEE Trans. Inform. Theory. IT-30, 774-775.

Ma, S.L. (1994). A survey of partial difference sets. Designs, Codes and Cryptography. 4, 221-261.

Ma, S.L. (1995). Planar functions, relative difference sets and character theory. Preprint.

MacWilliams, F.J. and Sloane, N.J.A. (1976). Pseudo-random sequences and arrays. Proc. IEEE. 64, 1715-1729.

McFarland, R.L. (1989). Difference sets in abelian groups of order $4p^2$. Mitt. Math. Sem. Giessen. 192, 1-70.

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

Mitchell, C.J. (1995). Aperiodic and semi-periodic perfect maps. IEEE Trans. Inform. Theory. IT-41, 88-95.

Moreno, O. and Games, R.A. and Taylor, H. (1993). Sonar sequences from Costas arrays and the best known sonar sequences with up to 100 symbols. IEEE Trans. Inform. Theory. IT-39, 1985-1987.

Nomura, T. and Miyakawa, H. and Imai, H. and Fukuda, A. (1972). A theory of two-dimensional linear recurring arrays, IEEE Trans. Inform. Theory. IT-18, 775-785.

Paterson, K.G. (1994). Perfect maps. IEEE Trans. Inform. Theory. IT-40, 743-753.

Pott, A. (1995). *Finite Geometry and Character Theory*. Springer-Verlag, Heidelberg.

Reed, I.S. and Stewart, R.M. (1962). Note on the existence of perfect maps. IRE Trans. Inform. Theory. 8, 10-12.

Robbins, J. and Taylor, H. (1984). SONAR sequences and PPM sequences. Part I. CSI-84-12-01, Comm. Sci. Inst., University of Southern California.

Rónyai, L. and Szönyi, T. (1989). Planar functions over finite fields. Combinatorica. 9, 315-320.

Saffari, B. and Smith, B. (1988). Inexistence de polynômes ultra-plats de Kahane à

coefficients ±1, Preuve de la conjecture d'Erdös. C.R. Acad. Sci. Paris. 306, Sér. I, 695-698.

Scholtz, R.A. and Welch, L.R. (1984). GMW sequences. IEEE Trans. Inform. Theory. IT-30, 548-553.

Singer, J. (1938). A theorem in finite projective geometry and some applications to number theory. Trans. Amer. Math. Soc. 43, 377-385.

Siu, M.K. (1989). From binary sequences to combinatorial designs, J. Math. Res. and Expos. 9, 605-621.

Siu, M.K. (1993). The combinatorics of binary arrays. In: *Proceedings of International Workshop on Discrete Mathematics and Algorithms*, Hong Kong, 13-27.

Smith, K.W. (1995). Non-abelian Hadamard difference sets. J. Comb. Theory. A-70, 144-156.

Turyn, R. (1965). Character sums and difference sets, Pacific J. Math. 15, 319-346.

Turyn, R. (1968). Sequences with small correlation. In: Mann, H.B., Ed., *Error Correcting Codes*, Wiley, New York, 195-228.

Turyn, R. (1984). A special class of Williamson matrices and difference sets. J. Comb. Theory. A-36, 111-115.

Turyn, R. and Storer, J. (1961). On binary sequence. Proc. Amer. Math. Soc. 12, 394-399.

Wang, J.P. (1988). On Golomb's conjectures. Scientia Sinica (Series A). 31, 152-161.

Xia, M.Y. (1992). Some infinite classes of special Williamson matrices and difference sets. J. Comb. Theory. A-61, 230-242.

Xiang, Q. and Chen, Y.Q. (1994). On Xia's construction of Hadamard difference sets. Preprint.

Zierler, N. (1959). Linear recurring sequences. J. Soc. Ind. Appl. Math. 7, 31-48.

Correspondence address:

Man-Keung SIU,

Department of Mathematics,

The University of Hong Kong,

Pokfulam Road,

HONG KONG.

e-mail: MATHSIU@HKUCC.HKU.HK