Existence of Ideal Matrices

W.C. Shiu and Y.P. Tang
Department of Mathematics
Hong Kong Baptist University
224, Waterloo Road
Kowloon, Hong Kong

ABSTRACT. An $m \times n$ ideal matrix is a periodic $m \times n$ binary matrix which satisfies the following two conditions: (1) each column of this matrix contains precisely one 1 and (2) if it is visualized as a dot pattern (with each dot representing a 1), then the number of overlapping dots at all actual shifts are 1 or 0. Let $s(n)$ denote the smallest integer m such that an $m \times n$ ideal matrix exists. In this paper, we reduce the upper bound of $s(n)$ which was found by Fung, Siu and Ma. Also we list an upper bound of $s(n)$ for $14 \leq n \leq 100$.

1 Introduction

A *periodic* $m \times n$ *binary array* is an infinite matrix $\tilde{A} = (a(i,j))$, $i,j \in \mathbb{Z}$, $a(i,j) = 0$ or 1 such that $a(i,j) = a(i+m,j) = a(i,j+n)$ for any $i,j \in \mathbb{Z}$. Since the $m \times n$ matrix $A = (a(i,j))$, $0 \leq i \leq m-1$, $0 \leq j \leq n-1$ can generate the infinite matrix $\tilde{A}$, therefore we may identify A and $\tilde{A}$. A periodic $n \times n$ binary array $A = (a(i,j))$ is called an *ideal matrix* if it satisfies the following two constraints:

1) each column of A contains precisely one 1,

2) its binary periodic autocorrelation function

$$BP(r,s) = \sum_{i \in \mathbb{Z}_n} \sum_{j \in \mathbb{Z}_n} a(i,j)a(i+r,j+s) \leq 1 \text{ for } (r,s) \neq (0,0) \text{ in } \mathbb{Z}_n \times \mathbb{Z}_n$$

An ideal matrix has a direct application to frequency-hopping multiple-access communication systems [4].

ARS COMBINATORIA 47(1997), pp. 87-92

It can be shown that $BP(0,0) = n$, $BP(r,0) = 0$ for $r \not\equiv 0 \pmod{n}$, and $BP(r,s) = 1$ for $s \not\equiv 0 \pmod{n}$ [5].

If the arrays $\tilde{A}$ (the infinite array defined above) and A are visualized as dot patterns (with each dot representing a 1) then these patterns have the following property. We move A around on $\tilde{A}$. For certain periodic shifts, when the patterns coincide, n dots will overlap. For purely vertical shifts (i.e., along the columns) from these positions, no dots will overlap and for any other shift exactly one pair of dots will overlap.

Up to now no $n \times n$ ideal matrix is found except n is an odd prime [5]. Ganley, Kumar, Fung, Siu and Ma [1, 2, 3, 5, 6] obtained some nonexistence results of $n \times n$ ideal matrix. We summarize as follows:

Theorem 1.1. *Suppose n is composite.*

(1) *(Ganley [3], Fung [2]) An $n \times n$ ideal matrix exists only if n is odd.*

(2) *(Fung, Siu and Ma [1], Fung [2]) An $n \times n$ ideal matrix exists only if n is square-free.*

(3) *(Fung [2], Kumar [5]) Let n be square-free. If for some prime factor q and some proper factor m of n with $(q,m) = 1$, there exists $h \in \mathbb{Z}$ such that $q^h \equiv -1 \pmod{m}$, then no $n \times n$ ideal matrix exists.*

(4) *(Ma [6]) If $n = pq$ where p and q are distinct primes then no $n \times n$ ideal matrix exists.*

Thus by using a PC under conditions above, Ma [6] got the following proposition:

Proposition 1.2. *Except for the four undecided cases $n = 15655, 29523, 35855,$ and 42627, there is no ideal matrix if n is a composite and $n \leq 50000$.*

In the following we relax the condition on square ideal matrix, but retain the condition that there be exacly one 1 per column and $BP(r,s) \leq 1$ for $(r,s) \neq (0,0)$.

2 Some known results of non-square ideal matrices

An $m \times n$ matrix $A = (a(i,j))$ is called an *ideal matrix* if it is a periodic $m \times n$ binary array and satisfies the following two constraints:

1) each column of A contains precisely one 1,

2) its binary periodic autocorrelation function

$$BP(r,s) = \sum_{i \in \mathbb{Z}_m} \sum_{j \in \mathbb{Z}_n} a(i,j)a(i+r, j+s) \leq 1 \text{ for } (r,s) \neq (0,0) \text{ in } \mathbb{Z}_m \times \mathbb{Z}_n$$

Clearly $m \geq n$. It is not hard to convince that an $m \times n$ ideal matrix corresponds to a function $f : \mathbb{Z}_n \to \mathbb{Z}_m$ for which $f_\ell(j) = f(j+\ell) - f(j)$ gives an injection for each $\ell \in \mathbb{Z}_n \backslash \{0\}$. Such function is called a *planar function* [6] and f_ℓ, $1 \leq \ell \leq n-1$, is called an *induced function of* f.

Theorem 2.1. *A function $f : \mathbb{Z}_n \to \mathbb{Z}_m$ is a planar function if and only if the induced functions $f_\ell(j) = f(j+\ell) - f(j)$ are injective functions for $1 \leq \ell \leq \lfloor \frac{n}{2} \rfloor$.*

Proof: It suffices to show that f_ℓ is injective if and only if $f_{n-\ell}$ is injective. It follows from the fact

$$-f_{n-\ell}(k+\ell) = f_\ell(k) \text{ for each } k \in \mathbb{Z}_n$$

immediately. □

Fung, Siu and Ma [1] found that when $m = n(n-1)$, an $m \times n$ ideal matrix exists by defining $f(j) = \frac{1}{2}j(j+1)$. Note that the formula of f_ℓ in [1] is incorrect. It must be

$$f_\ell(j) = \begin{cases} j\ell + \frac{1}{2}\ell(\ell+1) & \text{if } 0 \leq j \leq n-1-\ell \\ j(\ell-n) + \frac{1}{2}(\ell-n)(\ell-n+1) & \text{otherwise} \end{cases},$$

where $1 \leq \ell \leq \lfloor \frac{n}{2} \rfloor$.

Let $s(n)$ denote the smallest m such that an $m \times n$ ideal matrix exists. Hence $s(n) \leq n(n-1)$. It is known that $s(p) = p$ when p is an odd prime and $s(p-1) = p$ when p is a prime [1, 2]. $s(n)$ is known when $2 \leq n \leq 13$ by computer search [1, 2]. Namely $s(8) = 12$ and $s(9) = 12$. Up to now we only know that $22 < s(14)$ by computer search.

3 The upper bound of $s(n)$

In this section we shall show that the upper bound of $s(n)$ can be reduced by about a quarter of the original one given in [1]. From now on we fix n and $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$. Let $t = \lfloor \frac{n}{2} \rfloor$.

Lemma 3.1. *Let $f : \mathbb{Z}_n \to \mathbb{Z}_m$ and $f_\ell(j) = f(j+\ell) - f(j)$. Then for $1 \leq \ell \leq n-1$ we have*

(1) $f_\ell(j) = \sum_{k=0}^{\ell-1} f_1(j+k)$ *(in $\mathbb{Z}_m$) for each $j \in \mathbb{Z}_n$ and*

(2) $\sum_{j=0}^{n-1} f_\ell(j) = 0$ *(in $\mathbb{Z}_m$).*

Proof: (1) follows from the definition. Obviously, $\sum_{j=0}^{n-1} f_1(j) = 0$ and hence (2) follows. □

Lemma 3.2. *Define* $g_1 : \mathbb{Z}_n \to \mathbb{Z}$ *by*

$$g_1(j) = \begin{cases} j & \text{if } j \neq n-1 \\ (n-t)t & \text{if } j = n-1 \end{cases}$$

and define $g_\ell : \mathbb{Z}_n \to \mathbb{Z}$ *by* $g_\ell(j) = \sum_{k=0}^{\ell-1} g_1(j+k)$, $1 \leq \ell \leq t$ *(the value of* $j+k$ *is taken in* $\{0, 1, 2, \ldots, n-1\}$*). Then* g_ℓ *is an injection.*

Proof: Obviously, g_1 is a strictly increasing function. Therefore, g_ℓ is strictly increasing on $0 \leq j \leq n-\ell$ and is strictly decreasing on $n-\ell \leq j \leq n-1$. Hence g_ℓ has a global maximum at $n-\ell$ for $1 \leq \ell \leq t$. It suffices to show the proposition "$g_\ell(n-1) > g_\ell(n-\ell-1)$" holds for $1 \leq \ell \leq t$. We shall prove it by reduction on ℓ.

For $\ell = t$, we have

$$\begin{aligned} g_t(n-1) - g_t(n-t-1) &= g_1(n-1) + \sum_{k=1}^{t-1} g_1(n-1+k) \\ &\quad - \sum_{k=0}^{t-1} g_1(n-t-1+k) \\ &= (n-t)t + \sum_{k=1}^{t-1} g_1(k-1) - \sum_{k=0}^{t-1} g_1(n-t-1+k) \\ &= (n-t)t + \sum_{k=1}^{t-1} (k-1) - \sum_{k=0}^{t-1} (n-t-1+k) = 1. \end{aligned}$$

Thus when $\ell = t$ the proposition holds. Assume the proposition holds when $\ell = u+1$, where $1 \leq u \leq t-1$, that is, $g_{u+1}(n-1) > g_{u+1}(n-(u+1)-1) = g_{u+1}(n-u-2)$. This implies that

$$\begin{aligned} g_1(n-u-2) + \sum_{k=1}^{u} g_1(n-u-2+k) &< \sum_{k=0}^{u-1} g_1(n-1+k) + g_1(n-1+u) \\ &= \sum_{k=0}^{u-1} g_1(n-1+k) + g_1(u-1) \end{aligned}$$

and

$$(n-u-2) + \sum_{k=1}^{u} g_1(n-u-2+k) < \sum_{k=0}^{u-1} g_1(n-1+k) + (u-1).$$

Since $t < \frac{1}{2}(n+1)$ and $1 \leq u \leq t-1$, $n-u-2 > u-1$. Hence we have $g_u(n-1) > g_u(n-u-1)$. □

Theorem 3.3. *There exists an $m \times n$ ideal matrix, where $m = \frac{1}{2}(n-1)(n-2) + (n-t)t$ and $t = \lfloor \frac{n}{2} \rfloor$.*

Proof: Define $f : \mathbb{Z}_n \to \mathbb{Z}_m$ by $f(j) = \frac{1}{2}j(j-1)$. Let f_ℓ be the induced function of f. It is easy to see that $g_1(j) \equiv f_1(j) \pmod{m}$, $0 \leq j \leq n-2$. Also we have

$$f_1(n-1) = f(0) - f(n-1) = -\tfrac{1}{2}(n-1)(n-2) \equiv (n-t)t = g_1(n-1) \pmod{m}.$$

Hence $g_1 \equiv f_1 \pmod{m}$. By the definition of g_ℓ and Lemma 3.1 we have $g_\ell \equiv f_\ell \pmod{m}$ for $1 \leq \ell \leq t$. For $1 \leq \ell \leq t$, since $\sum_{j=0}^{n-1} g_1(j) = m > g_\ell(i)$ for each i and g_ℓ are injections, f_ℓ are injections. □

Remark 3.4: Suppose $f_1 : \mathbb{Z}_n \to \mathbb{Z}_k$ and $\sum_{j=0}^{n-1} f_1(j) \equiv 0 \pmod{k}$. Then we can construct a function $f : \mathbb{Z}_n \to \mathbb{Z}_k$ with specified value $f(0)$ such that f_ℓ, $1 \leq \ell \leq n-1$, are the induced functions of f.

When a $k \times n$ exists, it does not guarantee the existence of a $(k+1) \times n$ ideal matrix. For example, a 7×7 ideal matrix exists, but by computer search there is no 8×7 ideal matrix.

Proposition 3.5. *Let m be defined in Theorem 3.3. Then there is an $(m+k) \times n$ ideal matrix for $k \geq 0$.*

Proof: Define $g_1 : \mathbb{Z}_n \to \mathbb{Z}$ by $g_1(j) = \begin{cases} j & \text{if } j \neq n-1 \\ (n-t)t + k & \text{if } j = n-1 \end{cases}$. By the same proofs of Lemma 3.2, Theorem 3.3 and Remark 3.4, we get the proposition. □

4 Some computer search results

Let $f : \mathbb{Z}_n \to \mathbb{Z}_k$ defined by $f(j) = \frac{1}{2}j(j-1)$. We check that whether f represent an ideal matrix or not. If not we increase k by 1 each time until an ideal matrix exists. Hence we shall get an upper bound of $s(n)$. Also we can use another function, for example $f(j) = \frac{1}{2}j(j+1)$, to find an upper bound of $s(n)$. We list an upper bound of $s(n)$ for $14 \leq n \leq 100$ as follows:

n	14	15	20	21	24	25	26	27
$s(n) \leq$	38^{1}	53^{11}	116^{2}	125^{2}	149^{4}	212^{1}	176^{5}	217^{3}

n	32	33	34	35	38	39	44	45
$s(n) \leq$	291^{5}	283^{6}	292^{5}	334^{4}	370^{6}	485^{1}	651^{3}	583^{4}

n	48	49	50	51	54	55	56	57
$s(n) \leq$	631^{7}	975^{10}	822^{1}	838^{1}	838^{5}	1069^{1}	905^{7}	1057^{3}

n	62	63	64	65	68	69	74	75
$s(n) \leq$	1268^{2}	1352^{3}	1295^{4}	1464^{1}	2191^{11}	1688^{1}	1902^{1}	1691^{5}

n	76	77	80	81	84	85	86	87
$s(n) \leq$	1985^{3}	2876^{11}	1823^{8}	3280^{11}	2336^{1}	3603^{11}	2340^{6}	2734^{1}

n	90	91	92	93	94	95	98	99
$s(n) \leq$	2354^{9}	4336^{11}	4351^{11}	4502^{11}	4468^{11}	3223^{1}	3092^{5}	5138^{11}

The number indicates which of the following functions is used to find an upper bound.

1. $f(j) = \frac{1}{2}j(j+1)$; 2. $f(j) = \frac{1}{2}j(j-1)$; 3. $f(j) = \frac{1}{2}(j-1)(j-2)$;
4. $f(j) = \frac{1}{2}(j-2)(j-3)$; 5. $f(j) = \frac{1}{2}(j-3)(j-4)$;
6. $f(j) = \frac{1}{2}(j-4)(j-5)$; 7. $f(j) = \frac{1}{2}(j-5)(j-6)$;
8. $f(j) = \frac{1}{2}(j-6)(j-7)$; 9. $f(j) = \frac{1}{2}(j-7)(j-8)$;
10. $f(j) = \frac{1}{2}(j-11)(j-12)$; 11. $f(j) = \frac{1}{2}(j-12)(j-13)$.

References

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

[2] C.I. Fung, On arrays with small autocorrelation, M. Phil. Thesis, The University of Hong Kong, 1991.

[3] M.J. Ganley, On a paper of Dembowski and Ostrom, *Arch. Math.*, **27** (1976), 93–98.

[4] P.V. Kumar, Frequency-Hopping Code Sequence Designs Having Large Linear Span, *IEEE Trans. Inform. Theory*, **34** (1988), 146–151.

[5] P.V. Kumar, On the Existence of Square Dot-Matrix Patterns Having a Special Three-Valued Periodic-Correlation Function, *IEEE Trans. Inform. Theory*, **34** (1988), 271–277.

[6] S.L. Ma, Planar Functions, Relative Difference Sets and Character Theory, to appear in *Journal of Algebra.*