ON THE ANALYSIS OF AN ALGORITHM TO GENERATE A RANDOM CYCLIC PERMUTATION

HELMUT PRODINGER

ABSTRACT. Sattolo has presented an algorithm to generate cyclic permutations at random. In this note the two parameters "number of moves" and "distance" are analyzed.

1. INTRODUCTION

Sattolo [1] generates a random cyclic permutation as follows: She starts with $12\ldots n$, then a random integer between 1 and $n-1$ is chosen, say i, and the numbers in positions i and n are interchanged. Then a random integer between 1 and $n-2$ is chosen, say j, and the numbers in positions j and $n-1$ are interchanged, and so on. After $n-1$ iterations, a random cyclic permutation has been obtained.

Here is an example, with $n=5$ and the random numbers $4,1,2,1$:

$$
\begin{array}{l}
1\,2\,3\,\underline{4}\,5\\
\underline{1}\,2\,3\,5\,4\\
5\,\underline{2}\,3\,1\,4\\
\underline{5}\,3\,2\,1\,4\\
3\,5\,2\,1\,4
\end{array}
$$

The result is the cyclic permutation $1\to 3\to 2\to 5\to 4\to 1$.

In this note we are interested in the (average) number of times digit k moves; in the example we obtain the numbers 1, 1, 2, 1, 3 for $k=1,\ldots,5$. Altogether that means $1+1+2+1+3=8$ moves, which is clear, since each iteration moves exactly 2 digits.

We are also considering the (average) distance digit k travels. In the example we obtain the numbers 3, 1, 2, 1, 5 for $k=1,\ldots,5$.

ARS COMBINATORIA 65(2002), pp. 75-78

2. The number of moves

The probability generating functions $\varphi_{n,k}(u)$ are defined as follows:

$$\varphi_{n,k}(u) = \sum_l a_{n,k;l} u^l = \sum_l \mathbb{P}\{\text{digit } k \text{ makes } l \text{ moves}\} u^l.$$

The probability that position k is never chosen by the random number generator, is given by

$$\frac{n-2}{n-1} \cdot \frac{n-3}{n-2} \cdots \frac{k-1}{k} = \frac{k-1}{n-1}.$$

If position k is chosen by the random generator, digit k is moved once (to the right) and never moves again. If position k is never chosen by the random generator, it starts moving (to the left) when the positions $k+1, \ldots, n$ have already been dealt with. This leads to the recursion

$$\varphi_{n,k}(u) = \frac{n-k}{n-1} u + \frac{k-1}{n-1} \varphi_{k,k}(u), \qquad 1 \le k < n.$$

It remains to discuss the instance $k = n$. The recursion is

$$\varphi_{n,n}(u) = \frac{u}{n-1} \Big[\varphi_{n-1,1}(u) + \varphi_{n-1,2}(u) + \cdots + \varphi_{n-1,n-1}(u) \Big], \quad n \ge 2,$$
$$\varphi_{1,1}(u) = 1.$$

To understand it, note that one move is made, and, according to the random generator, each position $1, 2, \ldots, n-1$ might be chosen with probability $\frac{1}{n-1}$. Then digit n is in position k, say, and the further moves are described by $\varphi_{n-1,k}(u)$.

Let us start with the numbers $a_{n,k;1}$. It is easy to see that

$$a_{n,1;1} = 1, \quad a_{n,2;1} = 1, \quad a_{n,k;1} = \frac{n-k}{n-1}, \quad k \ge 3, \quad n \ge 2, \quad a_{1,1;1} = 0.$$

The recursions tell us furthermore that

$$a_{n,k;2} = \frac{1}{n-1} \Big[a_{k-1,1;1} + a_{k-1,2;1} + \cdots + a_{k-1,k-1;1} \Big].$$

Hence

$$a_{n,k;2} = \frac{1}{n-1} \Big[\frac{k-1}{2} + \frac{1}{k-2} \Big], \quad n \ge k \ge 3, \quad a_{n,k;2} = 0 \text{ otherwise.}$$

Similarly

$$a_{n,k;3} = \frac{1}{n-1} \Big[a_{k-1,1;2} + a_{k-1,2;2} + \cdots + a_{k-1,k-1;2} \Big]$$

and thus

$$a_{n,k;3} = \frac{1}{(n-1)(k-2)}\Big[-1 + \frac{(k-1)(k-2)}{4} + H_{k-3}\Big], \quad n \geq k \geq 3.$$

We can also compute the next ones as

$$a_{n,k;4} = \frac{1}{(n-1)(k-2)}\Big[-H_{k-3} - \frac{1}{4} + \frac{(k-1)(k-2)}{8} + \frac{1}{2}\Big(H_{k-3}^2 - H_{k-3}^{(2)}\Big)\Big],$$

(for $n \geq k \geq 3$), but it is clear the expressions become very messy.

The numbers $H_n = \sum_{k=1}^{n} \frac{1}{k}$ and $H_n^{(2)} = \sum_{k=1}^{n} \frac{1}{k^2}$ are harmonic numbers of the first and second order.

Now we proceed to the expected numbers of moves $E_{n,k} = \varphi'_{n,k}(1)$. The recursions are

$$E_{n,k} = \frac{n-k}{n-1} + \frac{k-1}{n-1} E_{k,k},$$

and

$$E_{n,n} = 1 + \frac{1}{n-1}\Big[E_{n-1,1} + E_{n-1,2} + \cdots + E_{n-1,n-1}\Big].$$

It is a simple task to find the answers

$$E_{n,k} = \frac{n+2k-5}{n-1}, \qquad k \geq 2, \quad E_{n,1} = 1, \quad n \geq 2, \quad E_{1,1} = 0$$

and prove them by induction. Since this can be done by Maple, it is omitted.

Note that

$$\sum_{k=1}^{n} E_{n,k} = 1 + \sum_{k=2}^{n} \frac{n+2k-5}{n-1} = 2(n-1),$$

as it should.

The second factorial moments can be computed in a similar fashion;

$$\varphi''_{n,k}(1) = \frac{1}{n-1}(8k - 4H_{k-2} - 16)$$

for $k \geq 2$, otherwise 0.

Theorem 1. *The average number of moves of digit k in Sattolo's algorithm and the variance are given by*

$$E_{n,k} = \frac{n+2k-5}{n-1}, \qquad k \geq 2, \quad E_{n,1} = 1, \quad n \geq 2, \quad E_{1,1} = 0,$$

$$V_{n,k} = \frac{2(k-2)(3n+1-2k)}{(n-1)^2} - \frac{4H_{k-2}}{n-1}, \qquad k \geq 2, \quad V_{n,1} = 0. \quad \square$$

3. The distance

It is not too hard to change things appropriately.

The recursions for the probability generating functions are now

$$\varphi_{n,k}(u) = \frac{u^{n-k}}{n-1} + \frac{n-2}{n-1}\varphi_{n-1,k}(u), \qquad 1 \le k < n,$$

$$\varphi_{n,n}(u) = \frac{1}{n-1}\Big[\varphi_{n-1,1}(u)u^{n-1} + \varphi_{n-1,2}(u)u^{n-2} + \cdots + \varphi_{n-1,n-1}(u)u\Big], \qquad n \ge 2,$$

$$\varphi_{1,1}(u) = 1.$$

From this we get the expectation

$$E_{n,k} = \frac{n}{2} - k + 1 + \frac{k(3k-5)}{2(n-1)}, \quad k \ge 2, \quad E_{n,1} = \frac{n}{2}, \quad n \ge 2, \quad E_{1,1} = 0,$$

and the second factorial moment

$$E^{(2)}_{n,k} = \frac{n^2}{3} - n(k - \tfrac{1}{3}) + k(k-1) + \frac{(k-2)(14k^2+k-21)}{18(n-1)}, \quad k \ge 2,$$

$$E^{(2)}_{n,1} = \frac{n(n-2)}{3}, \quad n \ge 2, \qquad E^{(2)}_{1,1} = 0.$$

Theorem 2. *The average distance that digit k travels in Sattolo's algorithm and the variance are given by*

$$E_{n,k} = \frac{n}{2} - k + 1 + \frac{k(3k-5)}{2(n-1)}, \quad k \ge 2, \quad E_{n,1} = \frac{n}{2}, \quad n \ge 2, \quad E_{1,1} = 0,$$

$$V_{n,k} = \frac{n(n-2)}{12} + \frac{7k^3 - 34k + 21}{9(n-1)} - \frac{k^2(3k-5)^2}{4(n-1)^2}, \quad k \ge 2,$$

$$V_{n,1} = \frac{n(n-2)}{12}. \quad \square$$

Averaging over all digits we find the average distance that a random element travels:

$$\frac{1}{n}\sum_{k=1}^{n} E_{n,k} = \frac{n+1}{2} - \frac{1}{n}.$$

References

[1] S. Sattolo. An algorithm to generate a random cyclic permutation. *Information Processing Letters*, 22:315–317, 1986.

Helmut Prodinger, The John Knopfmacher Centre for Applicable Analysis and Number Theory, Department of Mathematics, University of the Witwatersrand, P. O. Wits, 2050 Johannesburg, South Africa,
helmut@gauss.cam.wits.ac.za, http://www.wits.ac.za/helmut/index.htm

On Full Orthogonal Designs in Order 56

S. Georgiou
Department of Mathematics
National Technical University of Athens
Zografou 15773, Athens, Greece

C. Koukouvinos
Department of Mathematics
National Technical University of Athens
Zografou 15773, Athens, Greece

Jennifer Seberry
School of IT and Computer Science
University of Wollongong
Wollongong, NSW, 2522, Australia

Abstract

We find new full orthogonal designs in order 56 and show that of 1285 possible $OD(56; s_1, s_2, s_3, 56 - s_1 - s_2 - s_3)$ 163 are known, of 261 possible $OD(56; s_1, s_2, 56 - s_1 - s_2)$ 179 are known. All possible $OD(56; s_1, 56 - s_1)$ are known.

Key words and phrases: Construction, sequences, circulant matrices, amicable sets, orthogonal designs.

AMS Subject Classification: Primary 05B15, 05B20, Secondary 62K05.

1 Introduction

An *orthogonal design* of order n and type $(s_1, s_2, \ldots, s_u)$ $(s_i > 0)$, denoted $OD(n; s_1, s_2, \ldots, s_u)$, on the commuting variables $x_1, x_2, \ldots, x_u$ is an $n \times n$ matrix A with entries from $\{0, \pm x_1, \pm x_2, \ldots, \pm x_u\}$ such that

$$AA^T = (\sum_{i=1}^{u} s_i x_i^2) I_n$$

Alternatively, the rows of A are formally orthogonal and each row has precisely s_i entries of the type $\pm x_i$. In [2], where this was first defined, it was mentioned that

$$A^T A = (\sum_{i=1}^{u} s_i x_i^2) I_n$$

and so our alternative description of A applies equally well to the columns of A. It was also shown in [2] that $u \leq \rho(n)$, where $\rho(n)$ (Radon's function) is defined by $\rho(n) = 8c + 2^d$, when $n = 2^a b$, b odd, $a = 4c + d$, $0 \leq d < 4$.

A weighing matrix $W = W(n, k)$ is a square matrix with entries $0, \pm 1$ having k non-zero entries per row and column and inner product of distinct rows zero. Hence W satisfies $WW^T = kI_n$, and W is equivalent to an orthogonal design $OD(n; k)$. The number k is called the *weight* of W. If $k = n$, that is, all the entries of W are ± 1 and $WW^T = nI_n$, then W is called an Hadamard matrix of order n. In this case $n = 1, 2$ or $n \equiv 0 (mod\ 4)$.

Given the sequence $A = \{a_1, a_2, \ldots, a_n\}$ of length n the *non-periodic autocorrelation function* $N_A(s)$ is defined as

$$N_A(s) = \sum_{i=1}^{n-s} a_i a_{i+s}, \quad s = 0, 1, \ldots, n-1, \tag{1}$$

If $A(z) = a_1 + a_2 z + \ldots + a_n z^{n-1}$ is the associated polynomial of the sequence A, then

$$A(z)A(z^{-1}) = \sum_{i=1}^{n} \sum_{j=1}^{n} a_i a_j z^{i-j} = N_A(0) + \sum_{s=1}^{n-1} N_A(s)(z^s + z^{-s}), z \neq 0. \tag{2}$$

Given A as above of length n the *periodic autocorrelation function* $P_A(s)$ is defined, reducing $i + s$ modulo n, as

$$P_A(s) = \sum_{i=1}^{n} a_i a_{i+s}, \quad s = 0, 1, \ldots, n-1. \tag{3}$$

The following theorem which uses four circulant matrices in the Goethals-Seidel array is very useful in our construction for orthogonal designs.

Theorem 1 *[3, Theorem 4.49] Suppose there exist four circulant matrices A, B, C, D of order n sati sfying*

$$AA^T + BB^T + CC^T + DD^T = fI_n$$

Let R be the back diagonal matrix. Then

$$GS = \begin{pmatrix} A & BR & CR & DR \\ -BR & A & D^TR & -C^TR \\ -CR & -D^TR & A & B^TR \\ -DR & C^TR & -B^TR & A \end{pmatrix}$$

is a $W(4n, f)$ when A, B, C, D are $(0, 1, -1)$ matrices, and an orthogonal design $OD(4n; s_1, s_2, \ldots, s_u)$ on $x_1, x_2, \ldots, x_u$ when A, B, C, D have entries from $\{0, \pm x_1, \ldots, \pm x_u\}$ and $f = \sum_{j=1}^{u}(s_j x_j^2)$. □

Corollary 1 *If there are four sequences A, B, C, D of length n with entries from $\{0, \pm x_1, \pm x_2, \pm x_3, \pm x_4\}$ with zero periodic or non-periodic autocorrelation function, then these sequences can be used as the first rows of circulant matrices which can be used in the Goethals-Seidel array to form an $OD(4n; s_1, s_2, s_3, s_4)$. We note that if their non-periodic autocorrelation function is zero, then there are sequences of length $n + m$ for all $m \geq 0$.* □

This method for constructing orthogonal designs was used in [1, 6, 7].

Throughought this paper we will use the definition and notation of Koukouvinos, Mitrouli, Seberry and Karabelas [6].

A pair of matrices A, B is said to be amicable (anti-amicable) if $AB^T - BA^T = 0$ ($AB^T + BA^T = 0$). Following [5] a set $\{A_1, A_2, \ldots, A_{2n}\}$ of square real matrices is said to be *amicable* if

$$\sum_{i=1}^{n} \left(A_{\sigma(2i-1)} A_{\sigma(2i)}^T - A_{\sigma(2i)} A_{\sigma(2i-1)}^T \right) = 0 \tag{4}$$

for some permutation σ of the set $\{1, 2, \ldots, 2n\}$. For simplicity, we will always take $\sigma(i) = i$ unless otherwise specified. So

$$\sum_{i=1}^{n} \left(A_{2i-1} A_{2i}^T - A_{2i} A_{2i-1}^T \right) = 0. \tag{5}$$

Clearly a set of mutually amicable matrices is amicable, but the converse is not true in general. Throughout this paper R_k denotes the back diagonal identity matrix of order k.

A set of matrices $\{A_1, A_2, \ldots, A_n\}$ of order m with entries in $\{0, \pm x_1, \pm x_2, \ldots, \pm x_u\}$ is said to satisfy an additive property of type $(s_1, s_2, \ldots, s_u)$ if

$$\sum_{i=1}^{n} A_i A_i^T = \sum_{i=1}^{u} (s_i x_i^2) I_m. \tag{6}$$

Let $\{A_i\}_{i=1}^{8}$ be an amicable set of circulant matrices of order t, satisfying the additive property for $(s_1, s_2, \ldots, s_k)$. Then the Kharaghani array

$$H = \begin{pmatrix} A_1 & A_2 & A_4R_n & A_3R_n & A_6R_n & A_5R_n & A_8R_n & A_7R_n \\ -A_2 & A_1 & A_3R_n & -A_4R_n & A_5R_n & -A_6R_n & A_7R_n & -A_8R_n \\ -A_4R_n & -A_3R_n & A_1 & A_2 & -A_8^TR_n & A_7^TR_n & A_6^TR_n & -A_5^TR_n \\ -A_3R_n & A_4R_n & -A_2 & A_1 & A_7^TR_n & A_8^TR_n & -A_5^TR_n & -A_6^TR_n \\ -A_6R_n & -A_5R_n & A_8^TR_n & -A_7^TR_n & A_1 & A_2 & -A_4^TR_n & A_3^TR_n \\ -A_5R_n & A_6R_n & -A_7^TR_n & -A_8^TR_n & -A_2 & A_1 & A_3^TR_n & A_4^TR_n \\ -A_8R_n & -A_7R_n & -A_6^TR_n & A_5^TR_n & A_4^TR_n & -A_3^TR_n & A_1 & A_2 \\ -A_7R_n & A_8R_n & A_5^TR_n & A_6^TR_n & -A_3^TR_n & -A_4^TR_n & -A_2 & A_1 \end{pmatrix}$$

is an $OD(8t; s_1, s_2, \ldots, s_k)$.

The Kharaghani array which uses amicable sets of eight matrices is also very useful in our constructions for orthogonal designs.

The following lemma applies a lemma given in Georgiou, Koukouvinos, Mitrouli and Seberry [1] to determine the number of possible tuples to be searched determining the size of search space for orthogonal designs in order 56.

Lemma 1 *Let $n = 4m = 56$ be the order of an orthogonal design then the number of cases which must be studied to determine whether all orthogonal designs exist is*

(i) $\frac{1}{4}n^2 = 784$ *when 2−tuples are considered;*

(ii) $\frac{n-2}{72}(2n^2 + 7n + 6) = 5004$ *when 3-tuples are considered;*

(iii) $\frac{1}{576}(n^4 + 6n^3 - 2n^2 - 24n + 64) = 18890$ *when 4−tuples are considered.*

2 New full orthogonal designs from smaller orders

Theorem 2 *There are $OD(56; s_1, s_1, 56-s_1, 56-s_1)$ constructed using the full $OD(28; s_1, 28 - s_1)$ given in [2, 6, 7] for:*

(1, 1, 27, 27)	(5, 5, 23, 23)	(9, 9, 19, 19)	(13, 13, 15, 15)
(2, 2, 26, 26)	(6, 6, 22, 22)	(10, 10, 18, 18)	(14, 14, 14, 14)
(3, 3, 25, 25)	(7, 7, 21, 21)	(11, 11, 17, 17)	
(4, 4, 24, 24)	(8, 8, 20, 20)	(12, 12, 16, 16)	

Proof. We use the amicable orthogonal designs of type $AOD(2; (1, 1), (1, 1))$ in order two with the two variable designs in order 28 to obtain the desired designs in order 56. □

(1, 1, 2, 52)	(2, 2, 13, 39)	(2, 13, 13, 28)	(4, 8, 22, 22)	(7, 14, 14, 21)
(1, 1, 4, 50)	(2, 2, 14, 38)	(2, 13, 15, 26)	(4, 9, 9, 34)	(8, 8, 8, 32)
(1, 1, 6, 48)	(2, 2, 16, 36)	(2, 14, 14, 26)	(4, 12, 20, 20)	(8, 8, 10, 30)
(1, 1, 12, 42)	(2, 2, 18, 34)	(2, 16, 18, 20)	(4, 13, 13, 26)	(8, 8, 16, 24)
(1, 1, 16, 38)	(2, 2, 25, 27)	(2, 16, 19, 19)	(4, 14, 19, 19)	(8, 8, 18, 22)
(1, 1, 18, 36)	(2, 2, 26, 26)	(2, 18, 18, 18)	(4, 16, 18, 18)	(8, 8, 20, 20)
(1, 1, 26, 28)	(2, 3, 3, 48)	(3, 3, 12, 38)	(4, 17, 17, 18)	(8, 10, 10, 28)
(1, 2, 2, 51)	(2, 3, 12, 39)	(3, 3, 14, 36)	(5, 5, 10, 36)	(8, 10, 18, 20)
(1, 2, 3, 50)	(2, 3, 15, 36)	(3, 3, 20, 30)	(5, 5, 18, 28)	(8, 12, 18, 18)
(1, 2, 16, 37)	(2, 4, 25, 25)	(3, 5, 12, 36)	(5, 10, 18, 23)	(8, 14, 14, 20)
(1, 2, 17, 36)	(2, 6, 6, 42)	(4, 4, 4, 44)	(5, 15, 18, 18)	(8, 16, 16, 16)
(1, 2, 26, 27)	(2, 6, 12, 36)	(4, 4, 8, 40)	(6, 6, 6, 38)	(9, 9, 10, 28)
(1, 3, 16, 36)	(2, 6, 18, 30)	(4, 4, 12, 36)	(6, 6, 8, 36)	(9, 9, 18, 20)
(1, 3, 26, 26)	(2, 6, 24, 24)	(4, 4, 16, 32)	(6, 7, 7, 36)	(9, 10, 10, 27)
(1, 6, 12, 37)	(2, 8, 8, 38)	(4, 4, 20, 28)	(6, 10, 10, 30)	(9, 10, 18, 19)
(1, 6, 13, 36)	(2, 8, 10, 36)	(4, 7, 7, 38)	(6, 12, 18, 20)	(9, 11, 18, 18)
(1, 7, 12, 36)	(2, 9, 9, 36)	(4, 8, 8, 36)	(6, 12, 19, 19)	(10, 10, 16, 20)
(1, 18, 18, 19)	(2, 9, 18, 27)	(4, 8, 12, 32)	(6, 14, 18, 18)	(10, 10, 18, 18)
(2, 2, 2, 50)	(2, 12, 18, 24)	(4, 8, 18, 26)	(6, 15, 15, 20)	(10, 14, 14, 18)
(2, 2, 8, 44)	(2, 12, 21, 21)	(4, 8, 20, 24)	(7, 7, 14, 28)	(14, 14, 14, 14)

Table 1: Full 4-variable $OD(56; s_1, s_2, s_3, 56 - s_1 - s_2 - s_3)$ constructed from full three and four variable designs in order 28.

Theorem 3 *There are full* $OD(56; s_1, s_2, s_3, 56 - s_1 - s_2 - s_3)$ *constructed using the full* $OD(28; s_1, s_2, 28 - s_1 - s_2)$ *and* $OD(28; s_1, s_2, s_3, 28 - s_1 - s_2 - s_3)$ *designs in order* 28 *for the 4-tuples given in Table* 2.

Theorem 4 *There are* $OD(56; s_1, s_1, 2s_2, 2s_3, 56 - 2s_1 - 2s_2 - 2s_3)$ *constructed using the Multiplication Theorem [3, Lemma 4.11] with the full* $OD(28; s_1, s_2, s_3, 28 - s_1 - s_2 - s_3)$ *given in [2, 6, 7] for the values given in Table* 2.

(1, 1, 2, 2, 50)	(2, 2, 8, 8, 36)	(2, 9, 9, 18, 18)	(7, 7, 14, 14, 14)
(1, 1, 2, 16, 36)	(2, 2, 13, 13, 26)	(4, 4, 4, 8, 36)	(8, 8, 8, 16, 16)
(1, 1, 2, 26, 26)	(2, 2, 16, 18, 18)	(4, 4, 8, 8, 32)	(8, 8, 10, 10, 20)
(1, 1, 6, 12, 36)	(2, 3, 3, 12, 36)	(4, 4, 8, 20, 20)	(9, 9, 10, 10, 18)
(1, 1, 18, 18, 18)	(2, 6, 6, 6, 36)	(4, 8, 8, 18, 18)	
(2, 2, 2, 25, 25)	(2, 6, 12, 18, 18)	(5, 5, 10, 18, 18)	

Table 2: Full 5-variable designs in order 56 from full 4-variable designs in order 28.

In table 3 we present the new amicable sets of eight matrices which can be used in the Kharaghani array to construct some new full orthogonal designs in order 56. In this table we use the symbol $\bar{x}_i$ to denote $-x_i$.

Type	A_1 A_3 A_5 A_7	A_2 A_4 A_6 A_8	ZERO
(1,1,25,29)	$(a,d,d,\bar{d},d,\bar{d},\bar{d})$ $(b,d,d,\bar{d},d,\bar{d},\bar{d})$ $(\bar{d},d,d,d,d,d,d)$ $(b,b,b,\bar{b},b,\bar{b},\bar{b})$	$(\bar{b},b,b,b,b,b,b)$ $(b,d,d,\bar{d},d,\bar{d},\bar{d})$ $(c,b,b,\bar{b},b,\bar{b},\bar{b})$ $(b,b,b,\bar{b},b,\bar{b},\bar{b})$	PAF n=7
(1,2,3,25,25)	$(a,d,d,\bar{d},d,\bar{d},\bar{d})$ $(a,d,d,\bar{d},d,\bar{d},\bar{d})$ $(\bar{d},d,d,d,d,d,d)$ $(e,h,h,\bar{h},h,\bar{h},\bar{h})$	$(a,d,d,\bar{d},d,\bar{d},\bar{d})$ $(\bar{h},h,h,h,h,h,h)$ $(g,h,h,\bar{h},h,\bar{h},\bar{h})$ $(e,h,h,\bar{h},h,\bar{h},\bar{h})$	PAF n=7
(1,2,8,45)	$(\bar{a},b,b,a,b,a,a)$ $(a,b,b,\bar{a},b,\bar{a},\bar{a})$ $(d,b,b,\bar{b},b,\bar{b},\bar{b})$ $(c,b,b,\bar{b},b,\bar{b},\bar{b})$	$(b,b,b,\bar{b},b,\bar{b},\bar{b})$ $(b,b,b,\bar{b},b,\bar{b},\bar{b})$ $(d,b,b,\bar{b},b,\bar{b},\bar{b})$ $(\bar{b},b,b,b,b,b,b)$	PAF n=7
(1,2,13,40)	$(\bar{a},b,b,a,b,a,a)$ $(\bar{b},\bar{a},\bar{a},b,\bar{a},b,b)$ $(c,a,a,\bar{a},a,\bar{a},\bar{a})$ $(d,b,b,\bar{b},b,\bar{b},\bar{b})$	$(a,a,a,\bar{a},a,\bar{a},\bar{a})$ $(a,a,a,\bar{a},a,\bar{a},\bar{a})$ $(c,a,a,\bar{a},a,\bar{a},\bar{a})$ $(\bar{a},a,a,a,a,a,a)$	PAF n=7
(1,2,14,39)	$(a,b,b,\bar{b},b,\bar{b},\bar{b})$ $(d,b,b,\bar{b},b,\bar{b},\bar{b})$ $(c,b,b,\bar{b},b,\bar{b},\bar{b})$ $(\bar{b},\bar{a},\bar{a},b,\bar{a},b,b)$	$(d,a,a,\bar{a},a,\bar{a},\bar{a})$ $(b,b,b,\bar{b},b,\bar{b},\bar{b})$ $(\bar{b},b,b,b,b,b,b)$ $(\bar{a},b,b,a,b,a,a)$	PAF n=7
(1,2,19,34)	$(\bar{a},b,b,a,b,a,a)$ $(c,b,b,\bar{b},b,\bar{b},\bar{b})$ $(d,b,b,\bar{b},b,\bar{b},\bar{b})$ $(b,a,a,\bar{a},a,\bar{a},\bar{a})$	$(a,b,b,\bar{a},b,\bar{a},\bar{a})$ $(a,a,a,\bar{a},a,\bar{a},\bar{a})$ $(\bar{a},a,a,a,a,a,a)$ $(c,a,a,\bar{a},a,\bar{a},\bar{a})$	PAF n=7

Table 3: New full orthogonal designs in order 56 constructed from new amicable sets of eight matrices.

Type	A_1 A_3 A_5 A_7	A_2 A_4 A_6 A_8	ZERO
(1,3,8,19,25)	$(\bar{a}, b, b, a, b, a, a)$ $(a, b, b, \bar{a}, b, \bar{a}, \bar{a})$ $(e, h, h, \bar{h}, h, \bar{h}, \bar{h})$ $(d, b, b, \bar{b}, b, \bar{b}, \bar{b})$	$(e, h, h, \bar{h}, h, \bar{h}, \bar{h})$ $(e, h, h, \bar{h}, h, \bar{h}, \bar{h})$ $(b, b, b, \bar{b}, b, \bar{b}, \bar{b})$ $(\bar{h}, h, h, h, h, h, h)$	PAF n=7
(1,3,13,14,25)	$(a, d, d, \bar{d}, d, \bar{d}, \bar{d})$ $(\bar{f}, \bar{e}, \bar{e}, f, \bar{e}, f, f)$ $(f, f, f, \bar{f}, f, \bar{f}, \bar{f})$ $(\bar{d}, d, d, d, d, d, d)$	$(\bar{e}, f, f, e, f, e, e)$ $(a, d, d, \bar{d}, d, \bar{d}, \bar{d})$ $(a, d, d, \bar{d}, d, \bar{d}, \bar{d})$ $(g, e, e, \bar{e}, e, \bar{e}, \bar{e})$	PAF n=7
(1,10,18,27)	$(a, d, d, \bar{d}, d, \bar{d}, \bar{d})$ $(a, d, d, \bar{d}, d, \bar{d}, \bar{d})$ $(c, d, d, \bar{d}, d, \bar{d}, \bar{d})$ $(\bar{a}, b.b, a, b, a, a)$	$(d, b, b, \bar{b}, b, \bar{b}, \bar{b})$ $(d, b, b, \bar{b}, b, \bar{b}, \bar{b})$ $(\bar{d}, d, d, d, d, d, d)$ $(a, b, b, \bar{a}, b, \bar{a}, \bar{a})$	PAF n=7
(1,14,14,27)	$(a, d, d, \bar{d}, d, \bar{d}, \bar{d})$ $(b, d, d, \bar{d}, d, \bar{d}, \bar{d})$ $(c, d, d, \bar{d}, d, \bar{d}, \bar{d})$ $(\bar{b}, \bar{a}, \bar{a}, b, \bar{a}, b, b)$	$(d, a, a, \bar{a}, a, \bar{a}, \bar{a})$ $(d, b, b, \bar{b}, b, \bar{b}, \bar{b})$ $(\bar{d}, d, d, d, d, d, d)$ $(\bar{a}, b, b, a, b, a, a)$	PAF n=7
(1,20,35)	$(\bar{a}, a, a, a, a, a, a)$ $(a, a, a, \bar{a}, a, \bar{a}, \bar{a})$ $(a, b, b, \bar{a}, b, \bar{a}, \bar{a})$ $(b, b, b, \bar{b}, b, \bar{b}, \bar{b})$	$(d, a, a, \bar{a}, a, \bar{a}, \bar{a})$ $(\bar{a}, b, b, a, b, a, a)$ $(a, a, a, \bar{a}, a, \bar{a}, \bar{a})$ $(b, b, b, \bar{b}, b, \bar{b}, \bar{b})$	PAF n=7
(2,2,8,8,18,18)	$(\bar{a}, b, b, a, b, a, a)$ $(a, b, b, \bar{a}, b, \bar{a}, \bar{a})$ $(d, b, b, \bar{b}, b, \bar{b}, \bar{b})$ $(h, f, f, \bar{f}, f, \bar{f}, \bar{f})$	$(\bar{e}, f, f, e, f, e, e)$ $(e, f, f, \bar{e}, f, \bar{e}, \bar{e})$ $(d, b, b, \bar{b}, b, \bar{b}, \bar{b})$ $(h, f, f, \bar{f}, f, \bar{f}, \bar{f})$	PAF n=7
(2,4,22,28)	$(\bar{a}, a, a, a, \bar{a}, a, a)$ $(f, e, h, \bar{h}, \bar{h}, h, h)$ $(a, \bar{a}, a, a, a, \bar{a}, \bar{a})$ $(a, a, \bar{a}, a, \bar{a}, a, a)$	$(\bar{f}, h, h, h, \bar{h}, h, h)$ $(a, a, a, \bar{a}, \bar{a}, a, a)$ $(f, \bar{e}, h, h, h, \bar{h}, \bar{h})$ $(f, h, \bar{h}, h, \bar{h}, h, h)$	PAF n=7

Table 3 (cont.)

Type	A_1 A_3 A_5 A_7	A_2 A_4 A_6 A_8	ZERO
(3,22,31)	$(\bar{a},b,b,a,b,a,a)$ $(a,b,b,\bar{a},b,\bar{a},\bar{a})$ $(d,a,a,\bar{a},a,\bar{a},\bar{a})$ $(\bar{a},b,b,a,b,a,a)$	$(d,b,b,\bar{b},b,\bar{b},\bar{b})$ $(d,b,b,\bar{b},b,\bar{b},\bar{b})$ $(a,b,b,\bar{b},b,\bar{b},\bar{b})$ $(\bar{b},\bar{a},\bar{a},b,\bar{a},b,b)$	PAF n=7
(4,4,4,4,10,10,10,10)	$(b,c,a,c,d,d,\bar{d})$ $(b,\bar{c},a,\bar{c},\bar{d},\bar{d},d)$ $(b,d,\bar{a},d,\bar{c},\bar{c},c)$ $(b,\bar{d},\bar{a},\bar{d},c,c,\bar{c})$	$(f,g,e,g,h,h,\bar{h})$ $(f,\bar{g},e,\bar{g},\bar{h},\bar{h},h)$ $(f,\bar{h},\bar{e},\bar{h},g,g,\bar{g})$ $(f,h,\bar{e},h,\bar{g},\bar{g},g)$	NPAF n=7
(4,6,46)	$(c,\bar{c},\bar{c},c,c,b,\bar{a})$ $(c,\bar{c},c,c,c,\bar{c},c)$ $(\bar{c},c,\bar{c},c,a,b,c)$ $(\bar{c},c,c,c,c,b,\bar{c})$	$(\bar{c},c,\bar{c},c,a,b,c)$ $(\bar{c},c,c,c,c,b,\bar{c})$ $(c,\bar{c},\bar{c},c,c,b,\bar{a})$ $(c,\bar{c},c,c,c,\bar{c},c)$	PAF n=7
(4,7,21,24)	$(a,a,\bar{a},a,a,a,d)$ $(f,f,\bar{f},f,\bar{e},f,\bar{f})$ $(f,f,\bar{f},\bar{f},\bar{e},\bar{f},f)$ $(\bar{d},\bar{d},d,a,\bar{a},a,a)$	$(f,f,\bar{f},f,e,f,f)$ $(\bar{a},\bar{a},a,a,d,a,\bar{a})$ $(\bar{a},\bar{a},a,\bar{d},a,\bar{d},a)$ $(f,f,\bar{f},\bar{f},e,\bar{f},\bar{f})$	NPAF n=7
(7,7,7,7,7,7,7,7)	$(\bar{a},a,a,g,a,e,c)$ $(\bar{g},g,g,\bar{a},g,c,\bar{e})$ $(\bar{e},e,e,\bar{c},e,\bar{a},g)$ $(\bar{b},b,b,d,b,\bar{f},\bar{h})$	$(\bar{f},f,f,\bar{h},f,b,\bar{d})$ $(\bar{h},h,h,\bar{f},h,d,b)$ $(\bar{d},d,d,\bar{b},d,\bar{h},f)$ $(\bar{c},c,c,e,c,\bar{g},\bar{a})$	NPAF n=7
(7,7,18,24)	$(a,a,\bar{a},a,c,a,d)$ $(b,b,\bar{b},\bar{b},a,\bar{b},\bar{b})$ $(b,b,\bar{b},\bar{b},\bar{a},\bar{b},b)$ $(b,b,\bar{b},b,a,b,b)$	$(b,b,\bar{b},b,\bar{a},b,\bar{b})$ $(\bar{a},\bar{a},a,a,d,a,\bar{c})$ $(\bar{c},\bar{c},c,\bar{d},a,\bar{d},a)$ $(\bar{d},\bar{d},d,c,\bar{a},c,a)$	NPAF n=7
(8,11,37)	$(\bar{a},b,b,a,b,a,a)$ $(a,b,b,\bar{a},b,\bar{a},\bar{a})$ $(b,b,b,\bar{b},b,\bar{b},\bar{b})$ $(c,b,b,\bar{c},b,\bar{c},\bar{c})$	$(c,b,b,\bar{b},b,\bar{b},\bar{b})$ $(c,b,b,\bar{b},b,\bar{b},\bar{b})$ $(c,b,b,\bar{b},b,\bar{b},\bar{b})$ $(\bar{c},b,b,c,b,c,c)$	PAF n=7

Table 3 (cont.)

Type	A_1 A_3 A_5 A_7	A_2 A_4 A_6 A_8	ZERO
(11,14,31)	$(\bar{a}, b, b, a, b, a, a)$ $(c, a, a, \bar{a}, a, \bar{a}, \bar{a})$ $(\bar{c}, b, b, c, b, c, c)$ $(c, b, b, \bar{c}, b, \bar{c}, \bar{c})$	$(\bar{b}, \bar{a}, \bar{a}, b, \bar{a}b, b)$ $(a, b, b, \bar{b}, b, \bar{b}, \bar{b})$ $(c, b, b, \bar{b}, b, \bar{b}, \bar{b})$ $(c, b, b, \bar{b}, b, \bar{b}, \bar{b})$	PAF n=7

Table 3 (cont.)

Remark 1 We note that amicable sets of eight matrices of type $(4,4,4,4,10,10,10,10)$ and $(7,7,7,7,7,7,7,7)$ which are used for constructing OD's in order 56 are also found in [4].

(1, 2, 3, 50)	(2, 2, 18, 34)	(3, 13, 15, 25)	(4, 10, 10, 32)	(8, 8, 18, 22)
(1, 2, 25, 28)	(2, 2, 26, 26)	(3, 14, 14, 25)	(4, 10, 12, 30)	(8, 8, 20, 20)
(1, 3, 8, 44)	(2, 3, 25, 26)	(4, 4, 4, 44)	(4, 10, 14, 28)	(8, 10, 10, 28)
(1, 3, 13, 39)	(2, 4, 25, 25)	(4, 4, 8, 40)	(4, 10, 18, 24)	(8, 10, 14, 24)
(1, 3, 14, 38)	(2, 8, 8, 38)	(4, 4, 10, 38)	(4, 10, 20, 22)	(8, 10, 18, 20)
(1, 3, 19, 33)	(2, 8, 10, 36)	(4, 4, 14, 34)	(4, 12, 20, 20)	(8, 12, 18, 18)
(1, 3, 25, 27)	(2, 8, 18, 28)	(4, 4, 18, 30)	(4, 13, 14, 25)	(8, 14, 14, 20)
(1, 5, 25, 25)	(2, 8, 20, 26)	(4, 4, 20, 28)	(4, 14, 14, 24)	(10, 10, 10, 26)
(1, 8, 19, 28)	(2, 10, 18, 26)	(4, 4, 24, 24)	(4, 14, 18, 20)	(10, 10, 12, 24)
(1, 8, 22, 25)	(2, 16, 18, 20)	(4, 8, 8, 36)	(4, 16, 18, 18)	(10, 10, 14, 22)
(1, 11, 19, 25)	(2, 18, 18, 18)	(4, 8, 10, 34)	(7, 7, 7, 35)	(10, 10, 16, 20)
(1, 13, 14, 28)	(3, 3, 25, 25)	(4, 8, 14, 30)	(7, 7, 14, 28)	(10, 10, 18, 18)
(1, 13, 17, 25)	(3, 8, 19, 26)	(4, 8, 18, 26)	(7, 7, 21, 21)	(10, 12, 14, 20)
(1, 14, 16, 25)	(3, 8, 20, 25)	(4, 8, 19, 25)	(7, 14, 14, 21)	(10, 14, 14, 18)
(2, 2, 8, 44)	(3, 9, 19, 25)	(4, 8, 20, 24)	(8, 8, 10, 30)	(14, 14, 14, 14)
(2, 2, 16, 36)	(3, 13, 14, 26)			

Table 4: Full 4-variable $OD(56; s_1, s_2, s_3, 56 - s_1 - s_2 - s_3)$ constructed from full designs presented in table 2.

s_1, s_2, s_3	s_1, s_2, s_3	s_1, s_2, s_3	s_1, s_2, s_3	s_1, s_2, s_3
(1, 9, 46)	(4, 15, 37)	(6, 11, 39)	(8, 13, 35)	(11, 12, 33)
(1, 23, 32)	(4, 23, 29)	(6, 16, 34)	(8, 15, 33)	(11, 13, 32)
(1, 24, 31)	(5, 6, 45)	(6, 17, 33)	(8, 17, 31)	(11, 15, 30)
(2, 5, 49)	(5, 7, 44)	(6, 21, 29)	(8, 21, 27)	(11, 16, 29)
(2, 7, 47)	(5, 8, 43)	(6, 23, 27)	(9, 12, 35)	(11, 22, 23)
(2, 11, 43)	(5, 9, 42)	(7, 8, 41)	(9, 14, 33)	(12, 13, 31)
(2, 23, 31)	(5, 11, 40)	(7, 9, 40)	(9, 15, 32)	(12, 15, 29)
(3, 4, 49)	(5, 13, 38)	(7, 10, 39)	(9, 16, 31)	(12, 17, 27)
(3, 6, 47)	(5, 14, 37)	(7, 15, 34)	(9, 17, 30)	(13, 16, 27)
(3, 7, 46)	(5, 16, 35)	(7, 16, 33)	(9, 21, 26)	(13, 19, 24)
(3, 10, 43)	(5, 17, 34)	(7, 17, 32)	(9, 23, 24)	(13, 20, 23)
(3, 11, 42)	(5, 19, 32)	(7, 19, 30)	(10, 11, 35)	(13, 21, 22)
(3, 21, 32)	(5, 20, 31)	(7, 20, 29)	(10, 13, 33)	(15, 17, 24)
(3, 22, 31)	(5, 21, 30)	(7, 22, 27)	(10, 15, 31)	(15, 19, 22)
(3, 24, 29)	(5, 22, 29)	(7, 23, 26)	(10, 17, 29)	(16, 17, 23)
(4, 5, 47)	(5, 24, 27)	(8, 9, 39)	(10, 21, 25)	(17, 19, 20)
(4, 11, 41)	(6, 9, 41)			

Table 5: The existence of these 82 full $OD(56; s_1, s_2, 56 - s_1 - s_2)$ is not yet established.

3 Full designs with even parameters

We note that Seberry [8] showed that if all $OD(n; x, y, n - x - y)$ exist then all $OD(2n; z, w, 2n - z - w)$ exist for $s \geq 0$ an integer. In particular if all $OD(2^t p; x, y, 2^t p - x - y)$ exist, for some odd integer p, then all $OD(2^{t+s} p; z, w, 2^{t+s} p - z - w)$ exist for $s \geq 0$ an integer we observe

Lemma 2 *If all $OD(2^t p; 2x, 2y, 2^t p - 2x - 2y)$ exist, for some odd integer p, then all $OD(2^{t+s} p;\ 2z, 2w, 2^{t+s} p - 2z - 2w)$ exist for $s \geq 0$ an integer.*

Corollary 2 *If $OD(56; 6, 16, 34)$ exist then all $OD(2^{s+3} 7; 2z, 2w, 2^{s+3} 7 - 2z - 2w)$ exist for $s \geq 0$ an integer.*

Proof. A search of full $OD(56; x, y, 56 - x - y)$ show only the parameters indicated are as yet unsolved. □

4 Summary

We have found new designs in order 56 and shown that of 1285 possible $OD(56; s_1, s_2, s_3, 56 - s_1 - s_2 - s_3)$ 163 are known: of 261 possible

$OD(56; s_1, s_2, 56 - s_1 - s_2)$ 179 are known; and all possible $OD(56; s_1, 56 - s_1)$ are known.

References

[1] S. Georgiou, C. Koukouvinos, M. Mitrouli and J. Seberry, Necessary and sufficient conditions for three and four variable orthogonal designs in order 36, *J. Statist. Plann. Inference*, (to appear).

[2] A.V.Geramita, J.M.Geramita, and J.Seberry Wallis, Orthogonal designs, *Linear and Multilinear Algebra*, 3 (1976), 281–306.

[3] A.V.Geramita, and J.Seberry, *Orthogonal Designs: Quadratic Forms and Hadamard Matrices*, Marcel Dekker, New York-Basel, 1979.

[4] W.H. Holzmann, and H. Kharaghani, On the Plotkin arrays, *Australas. J. Combin.*, 22 (2000), 287–299.

[5] H. Kharaghani, Arrays for orthogonal designs, *J. Combin. Designs*, 8 (2000), 166–173.

[6] C.Koukouvinos, M.Mitrouli, J.Seberry, and P.Karabelas, On sufficient conditions for some orthogonal designs and sequences with zero autocorrelation function, *Australas. J. Combin.*, 13 (1996), 197–216.

[7] C. Koukouvinos and J. Seberry, New orhogonal designs and sequences with two and three variables in order 28, *Ars Combinatoria*, 54 (2000), 97–108.

[8] J. Seberry Wallis, On the existence of Hadamard matrices, *J. Combin. Theory Ser. A*, 21 (1976), 188–195.