

ARS

COMBINATORIA

DE LA UNIVERSIDAD

DE CALIFORNIA

BERKELEY, CALIFORNIA

CONSTRUCTION OF PANDIAGONAL MAGIC SQUARES
FROM CIRCULANT PANDIAGONAL MATRICES

Włodzimirz Proskurowski
Andrzej Proskurowski

Abstract

Orthogonal latin squares can be used to construct a magic square of the same order. We consider construction of pandiagonal magic squares from selforthogonal, circulant, pandiagonal, constant sum matrices. We present algorithms to construct such matrices of even multiple of 2 and of odd orders. Pandiagonal constant sum matrices may be considered an analogue of latin squares. However, for oddly even order of matrices, there are no orthogonal pairs of circulant such matrices. A similar statement for latin squares (Euler's conjecture) is known to be false.

1. Introduction.

We are interested in combinatorial structures related to latin squares and magic squares, their construction and existence. A *latin square* is a square matrix with n entries of n different elements, none of them occurring twice within any row or column of the matrix [1, p. 15]. A *magic square* of order n is an arrangement of n^2 consecutive integers in a square, such that the sums of each row, each column and each of the main diagonal are the same [1, p. 194]. If also the sum of each *extended diagonal* (diagonal of the square mapped onto the surface of a torus) is the same, the magic square is called *pandiagonal* (PMS). Two latin squares $A = (a[i,j])$ and $B = (b[i,j])$ of order n are said to be *orthogonal* (*orthogonal mates*) if every ordered pair of symbols occurs exactly once among the n^2 pairs $\langle a[i,j], b[i,j] \rangle$ [1, p. 154]. Two orthogonal latin squares can be used to construct a magic square of the same order by a simple juxtaposition [1, p. 206].

We introduce a notion of a *pandiagonal constant sum* (PCS) matrix which is a square matrix with n^2 entries of n consecutive integers, each appearing exactly n times, and such that the sums of each row, each column and each extended diagonal are the same. We will use these

matrices to construct PMS in a manner similar to that of constructing magic squares from latin squares. More specifically, we will give algorithms to construct *circulant* matrices, i.e., in which the first row is explicitly given and each other row is a cyclic shift of the previous one by a given number of elements. A matrix with a given value m of the shift is called an *m-circulant*. We will show that the pandiagonal and circulant properties required from these "weakened latin squares" (a repetition of elements in columns is allowed) restrict the existence of these structures to odd and evenly even orders. This fact echoes the Euler's conjecture (which has been proved false) about non-existence of orthogonal pairs of latin squares of oddly even order [1, p. 156].

The square matrices considered in our paper have subscripts in the range $0, 1, \dots, n-1$ enclosed in square brackets: $C = (c[i, j])$, $0 \leq i, j < n$. An *m-circulant* matrix based on a permutation p of integers $0, 1, \dots, n-1$ will be denoted ${}^m C_p$. A general entry of ${}^m C_p$ will thus be ${}^m C_p[i, j] = p[(i+m) \bmod n]$, where $p = \langle p[0], p[1], \dots, p[n-1] \rangle$. A square matrix S is said to be *selforthogonal* if it is orthogonal (in the sense of uniqueness of pairs of corresponding entries) to its own transpose S^T .

2. *Main results.*

We will give a characterization of pandiagonal magic squares in terms of their decomposition into orthogonal PCS matrices. Then we will state a series of lemmas leading to a construction algorithm for a subclass of pandiagonal magic squares from circulant PCS matrices.

THEOREM 1. (Decomposition) A square matrix of order n , $A = (a[i, j])$, $0 \leq i, j < n$, is a pandiagonal magic square if there exist two orthogonal PCS matrices $B = (b[i, j])$ and $B' = (b'[i, j])$ of order n such that $A = nB + B'$.

Proof. Orthogonality of B and B' ensures that an element $a[i, j]$, $0 \leq i, j < n$, represents uniquely a two-digit number in base n , $a[i, j] = b[i, j]n + b'[i, j]$, which is a number between 0 and $n^2 - 1$.

The property of constant row, column and pandiagonal sum is preserved by scalar multiplication and matrix addition. Thus A is a pandiagonal magic square. \square

Any PMS can be written in the abovementioned way as the weighted sum of two orthogonal mates. If the matrices are transposes of each other, then they have also the PCS property.

COROLLARY 1. A PMS matrix of order n , $A = (a[i, j])$, $0 \leq i, j < n$, has a decomposition $A = nB + B^T$ iff B is a selforthogonal PCS matrix.

Proof. The necessity follows from the fact that if $A = nB + B^T$ then also $A^T = nB^T + B$ is a PMS. This implies that, for any k , $0 \leq k < n$, $\sum_{0 \leq \ell < n} a[k, \ell] = (n-1)n/2 = nx + y$ and $\sum_{0 \leq \ell < n} a[\ell, k] = (n-1)n/2 = ny + x$, where $x = \sum_{0 \leq \ell < n} b[k, \ell]$ and $y = \sum_{0 \leq \ell < n} b[\ell, k]$. Hence, $x = y = (n-1)n/2$. A similar reasoning holds also for diagonals of B , proving its PCS property. \square

Because of its generality, the above theorem is not a useful tool in constructing pandiagonal magic squares. An algorithm based on the definition of PCS matrices would lead to an exhaustive search which, even on a large computer, would require prohibitively long execution time for $n > 4$. We will now investigate circulant PCS matrices which can be relatively easily constructed and thus would give a simpler algorithm for construction of pandiagonal magic squares. We first explore existence of an appropriate value of a shift and a permutation defining a circulant matrix, sufficient for the constant sum property to hold.

If there is a repetition of elements in a column of a circulant PCS matrix, then the sum of repeated elements must divide the constant sum of the column. This sum is the same as the row sum and thus equals $r = \sum_{0 \leq i < n} 1 = n(n-1)/2$.

LEMMA 1. For an arbitrary non-prime integer $n \geq 4$, there exists an integer m , $1 < m < n-1$, such that the greatest common divisor $g = \gcd(m, n)$ also divides $r = n(n-1)/2$.

Proof. We show existence of such a value by case analysis based on the parity of n . (i) n is odd. Then r is divisible by n and thus by all its divisors. Therefore, any divisor of n fulfills the requirements. (ii) n is oddly even (not divisible by 4). Then $n/2$ is odd and only odd divisors of n divide r . For odd m , $\gcd(m, n) = \gcd(m, n/2)$ divides r . (iii) n is evenly even. Then $n/2$ is even and all even divisors of n divide r as well. Any m for which $\gcd(m, n) = \gcd(m, n/2)$ satisfies the requirements. \square

If m and n are relatively prime then there is no repetition of elements in any column of an m -circulant matrix of order n based on any permutation p of $0, 1, \dots, n-1$ and thus mC_p is a magic square. However, for a general m , we have to ensure the existence of a suitable permutation. Namely, $\{0, 1, \dots, n-1\}$ should admit a partition into $q = \gcd(m, n)$ subsets, each with the same partial sum.

LEMMA 2. Let two positive integers, m and n , $1 < m < n-1$, be such that $q = \gcd(m, n)$ divides n . There exists a permutation p of the integers $0, 1, \dots, n-1$ such that for all values of j , $0 \leq j < n$,

$$\sum_{0 \leq i < q} p[(im+j) \bmod n] = r/q.$$

Proof. For even n/q , a suitable permutation p can be obtained considering a matrix $U = (u[i, j])$, $0 \leq i < n/q, 0 \leq j < q$. A general entry of such a matrix with n elements is given by

$$u[i, j] = qi + j \quad \text{for } 0 \leq i < n/(2q) \text{ and } 0 \leq j < q$$

$$= q(i+1) - (j+1) \quad \text{for } n/(2q) \leq i < n/q \text{ and } 0 \leq j < q.$$

It is easy to see that U contains all integers $0, 1, \dots, n-1$ and has a constant column sum. The corresponding permutation is $p[k] = \lfloor (k/n/q) \rfloor, 0 \leq k < n$, a row-wise linearization

of U . (ix) denotes the smallest integer not greater than x .) For odd n/q , also q is odd (cases (i) and (ii) of the preceding lemma's proof). We define an n/q by q matrix $V = (v[i, j])$ of n elements $0, 1, \dots, n-1$ by arranging the first $q(\lfloor n/(2q) \rfloor - 1)$ integers of the interval and the last $q(\lfloor n/(2q) \rfloor - 1)$ integers will be placed the above matrix U . The remaining "middle" integers will be placed in three rows of V , each permuted so as to preserve constant sum in their three-element parts of columns of V . Specifically, for all j , $0 \leq j < n$,

$$v[i, j] = q + j \quad \text{for } 0 \leq i < \lfloor n/(2q) \rfloor - 1,$$

$$= q + ((2+j)(q-1)/2) \bmod q \quad \text{for } i = \lfloor n/(2q) \rfloor - 1,$$

$$= q + j \quad \text{for } i = \lfloor n/(2q) \rfloor,$$

$$= q + ((1+j)(q-1)/2) \bmod q \quad \text{for } i = \lfloor n/(2q) \rfloor + 1,$$

$$= q + (j+1) - (j+1) \quad \text{for } \lfloor n/(2q) \rfloor + 1 < i < n/q.$$

Again, a row-wise linearization of V yields a permutation p of $0, 1, \dots, n-1$ with the postulated property. \square

We now give examples illustrating the above constructions.

Example 1. $n = 8, m = 4, q = 4, r/q = 7$.

$$U = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 4 & 5 & 6 & 7 \end{pmatrix} \quad p = \langle 0 \ 1 \ 2 \ 3 \ 7 \ 6 \ 5 \ 4 \rangle$$

Example 2. $n = 9, m = 3, q = 3, r/q = 12$.

$$V = \begin{pmatrix} 2 & 0 & 1 \\ 3 & 4 & 5 \\ 7 & 8 & 6 \end{pmatrix} \quad p = \langle 2 \ 0 \ 1 \ 3 \ 4 \ 5 \ 7 \ 8 \ 6 \rangle$$

We observe that any rearrangement of rows and columns of U or V and also any exchange of two pairs of values in two columns within two rows of U , one in the upper half and the other in the lower half of the matrix, preserves sums of columns and is thus equally appropriate as a basis for the permutation p .

Because of the desired constant sum property for extended diagonals as well, we have to consider divisibility properties for $m \pm 1$ and n . As we want to preserve the constant sum of column elements, we have to deal with $m(m-1)(m+1)$.

LEMMA 3. For an integer $n \geq 4$, if n is odd or a multiple of 4 then and only then there exists an integer m , $1 < m < n-1$, such that $s = \gcd(m^3-m, n)$ divides $r = n(n-1)/2$.

Proof. Case analysis depending on the parity of n . (i) n is odd. By definition, s divides n and as such also r . Thus, any m would qualify. (ii) n is oddly even. Either m or $m \pm 1$ are even. Therefore either $q = \gcd(m, n)$ or $q' = \gcd(n^2-1, n)$ are even and thus also s is even. But no even divisor of n divides r (cf. case (ii) in the proof of Lemma 1). This proves the necessity condition. (iii) n is evenly even. By the analysis of Lemma 1, there exists an even m that divides both n and r . For any m such that n/q is even, also n/s is even, i.e., $n/(2s)$ is an integer. Value of $m = 2$ is suitable for any evenly even n . \square

The necessity condition states that there is no m -circulant PCS matrix of oddly even order.

As before, mutually prime values of m , $m-1$, $m+1$, and n cause no repetition in columns or extended diagonals of an m -circulant matrix of order n and this any such matrix is PCS. For other cases, we have to establish existence of a permutation defining an m -circulant PCS matrix.

LEMMA 4. For an integer $n \geq 4$, odd or a multiple of 4, there exists an integer m , $1 < m < n-1$, such that any permutation p chosen in accordance with Lemma 2 defines an m -circulant PCS matrix.

Proof. If n is prime then for any m and any p the PCS property holds. Otherwise, a choice of p in accordance with Lemma 2 guarantees a constant sum in columns of ${}^m C_p$. If additionally $\gcd(m^2-1, n)$

divides $n(n-1)/2$ then the necessary condition for the constant sum of diagonals is satisfied. If $\gcd(m^2-1, n) = 1$ then there is no repetition of the elements on the broken diagonals. The number of repetitions in the columns is $\gcd(m, n)$, and in the diagonal directions $\gcd(m-1, n)$ and $\gcd(m+1, n)$, respectively. If at least two of these values are greater than 1 and differ from each other then the existence of a permutation p with the divisibility properties discussed in Lemma 2 holding for both of these values simultaneously is not certain. On the other hand, for any n in question there exists an m for which only one of the \gcd 's is greater than 1. Namely, for odd n such an m equals the smallest divisor of n , and for even n , the largest divisor, i.e., $n/2$. Then an appropriate permutation p (cf. Lemma 2) ensures the PCS property. \square

We are now in a position to state a theorem indicating how to construct pandiagonal magic squares of a given feasible order.

THEOREM 2. (Construction) For an integer $n \geq 4$, odd or a multiple of 4, there exist an integer m and a permutation p such that the m -circulant matrix ${}^m C_p$ of order n together with its transpose determine a pandiagonal magic square $A = n {}^m C_p + m {}^m C_p^T$.

Proof. In view of Theorem 1 we need only prove that ${}^m C_p$ is self-orthogonal. Lemma 3 assures existence of a value m such that $\gcd(m^3-m, n) = 1$ which together with a permutation p chosen accordingly to Lemma 2 gives the PCS property. We will show that for two pairs of indices, $\langle k_1, \ell_1 \rangle \neq \langle k_2, \ell_2 \rangle$, ${}^m C_p[k_1, \ell_1] = {}^m C_p[k_2, \ell_2]$ implies ${}^m C_p[\ell_1, k_1] = {}^m C_p[\ell_2, k_2]$, which asserts selforthogonality of ${}^m C_p$. Using the expression for a general entry of a circulant matrix, ${}^m C_p[i, j] = p[(im+j) \bmod n]$ and defining $k = k_1 - k_2$, $\ell = \ell_1 - \ell_2$, a violation of the above implication would give $(k \pm \ell)(m \pm 1) = 0 \pmod{n}$ which can be true only if ${}^m C_p[k_1, \ell_1] = {}^m C_p[k_2, \ell_2]$ are on the same diagonal. This contradicts our assumption that there are no repetitions of entries on diagonals of ${}^m C_p$. Thus ${}^m C_p$ is selforthogonal and defines a pandiagonal magic square A . \square

Below we give examples of pandiagonal magic squares of order 8 and 9 obtained by the method suggested in Theorem 2 for the permutations defined in Examples 1 and 2, respectively.

Example 3. $n = 8, m = 4, p = \langle 0 \ 1 \ 2 \ 3 \ 7 \ 6 \ 5 \ 4 \rangle$.

$$m_p^C = \begin{pmatrix} 0 & 1 & 2 & 3 & 7 & 6 & 5 & 4 \\ 7 & 6 & 5 & 4 & 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 & 7 & 6 & 5 & 4 \\ 7 & 6 & 5 & 4 & 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 & 7 & 6 & 5 & 4 \\ 7 & 6 & 5 & 4 & 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 & 7 & 6 & 5 & 4 \\ 7 & 6 & 5 & 4 & 0 & 1 & 2 & 3 \end{pmatrix}$$

$$m_p^{C^T} = \begin{pmatrix} 0 & 7 & 0 & 7 & 0 & 7 & 0 & 7 \\ 1 & 6 & 1 & 6 & 1 & 6 & 1 & 6 \\ 2 & 5 & 2 & 5 & 2 & 5 & 2 & 5 \\ 3 & 4 & 3 & 4 & 3 & 4 & 3 & 4 \\ 7 & 0 & 7 & 0 & 7 & 0 & 7 & 0 \\ 6 & 1 & 6 & 1 & 6 & 1 & 6 & 1 \\ 5 & 2 & 5 & 2 & 5 & 2 & 5 & 2 \\ 4 & 3 & 4 & 3 & 4 & 3 & 4 & 3 \end{pmatrix}$$

$$A = \begin{pmatrix} 0 & 15 & 16 & 31 & 56 & 55 & 40 & 39 \\ 57 & 54 & 41 & 38 & 1 & 14 & 17 & 30 \\ 2 & 13 & 18 & 29 & 58 & 50 & 42 & 37 \\ 59 & 52 & 43 & 36 & 3 & 12 & 19 & 28 \\ 7 & 8 & 23 & 24 & 63 & 48 & 47 & 32 \\ 62 & 49 & 46 & 33 & 6 & 9 & 22 & 25 \\ 5 & 10 & 21 & 26 & 61 & 50 & 45 & 34 \\ 60 & 51 & 44 & 35 & 4 & 11 & 20 & 27 \end{pmatrix}$$

Example 4. $n = 9, m = 3, p = \langle 2 \ 0 \ 1 \ 3 \ 4 \ 5 \ 7 \ 8 \ 6 \rangle$.

$$m_p^C = \begin{pmatrix} 2 & 0 & 1 & 3 & 4 & 5 & 7 & 8 & 6 \\ 3 & 4 & 5 & 7 & 8 & 6 & 2 & 0 & 1 \\ 7 & 8 & 6 & 2 & 0 & 1 & 3 & 4 & 5 \\ 2 & 0 & 1 & 3 & 4 & 5 & 7 & 8 & 6 \\ 3 & 4 & 5 & 7 & 8 & 6 & 2 & 0 & 1 \\ 7 & 8 & 6 & 2 & 0 & 1 & 3 & 4 & 5 \\ 2 & 0 & 1 & 3 & 4 & 5 & 7 & 8 & 6 \\ 3 & 4 & 5 & 7 & 8 & 6 & 2 & 0 & 1 \\ 7 & 8 & 6 & 2 & 0 & 1 & 3 & 4 & 5 \end{pmatrix}$$

$$m_p^{C^T} = \begin{pmatrix} 2 & 3 & 7 & 2 & 2 & 3 & 7 & 2 & 3 & 7 \\ 0 & 4 & 8 & 0 & 4 & 8 & 0 & 4 & 8 \\ 1 & 5 & 6 & 1 & 5 & 6 & 1 & 5 & 6 \\ 3 & 7 & 2 & 3 & 7 & 2 & 3 & 7 & 2 \\ 4 & 8 & 0 & 4 & 8 & 0 & 4 & 8 & 0 \\ 5 & 6 & 1 & 5 & 6 & 1 & 5 & 6 & 1 \\ 7 & 2 & 3 & 7 & 2 & 3 & 7 & 2 & 3 \\ 8 & 0 & 4 & 8 & 0 & 4 & 8 & 0 & 4 \\ 6 & 1 & 5 & 6 & 1 & 5 & 6 & 1 & 5 \end{pmatrix}$$

$$A = \begin{pmatrix} 20 & 3 & 16 & 29 & 39 & 52 & 65 & 75 & 61 \\ 27 & 40 & 53 & 63 & 76 & 62 & 18 & 4 & 17 \\ 64 & 77 & 60 & 19 & 5 & 15 & 28 & 41 & 51 \\ 21 & 7 & 11 & 30 & 43 & 47 & 66 & 79 & 56 \\ 31 & 44 & 45 & 67 & 80 & 54 & 22 & 8 & 9 \\ 68 & 78 & 55 & 23 & 6 & 10 & 32 & 42 & 46 \\ 25 & 2 & 12 & 34 & 38 & 48 & 70 & 74 & 57 \\ 35 & 36 & 49 & 71 & 72 & 58 & 26 & 0 & 13 \\ 69 & 73 & 59 & 24 & 1 & 14 & 33 & 37 & 50 \end{pmatrix}$$

3. Concluding remarks.

In order to classify pandiagonal magic squares we introduce the notion of similarity. Let us consider the following set of transformations of two-dimensional arrays: rotation, transposition, and cyclic translation (shift of rows and columns). Two arrays, A and A' , are *similar* iff there exist a finite composition T of the above transformations such that $A' = T(A)$. Note that the properties of pandiagonal magic square mapped onto the surface of a torus are invariant under these transformations. The PCS property of circulant matrices is also preserved under T . For instance, an m -circulant matrix C of order n is similar to an $(m-n)$ -circulant C' with the same first row. Thus, whenever $A = nC + C^T$ is a pandiagonal magic square, so is $A' = nT(C) + T(C^T)$. This fact should simplify classification of pandiagonal magic squares according to Theorem 2.

For example, there are only 6 distinct pandiagonal magic squares of order 5 based on 2-circulant matrices. (The values $m = 2$ and $m = 3$ are the only feasible shift values for $n = 5$, and the corresponding circulant matrices are similar.) The matrices are given by the following permutations: $\langle 0 \ 1 \ 2 \ 3 \ 4 \rangle$; $\langle 0 \ 1 \ 2 \ 4 \ 3 \rangle$; $\langle 0 \ 1 \ 3 \ 2 \ 4 \rangle$; $\langle 0 \ 1 \ 3 \ 4 \ 2 \rangle$; $\langle 0 \ 1 \ 4 \ 2 \ 3 \rangle$; $\langle 0 \ 1 \ 4 \ 3 \ 2 \rangle$.

Nothing has yet been said about the existence of pandiagonal magic squares other than those satisfying the assumptions of Theorem 2. In Figure 1 we give as an example two PCS matrices representing the only two equivalence classes of PCS matrices of order 4 under similarity. Only the second one is circulant.

$$\begin{bmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 3 & 2 \\ 3 & 2 & 0 & 1 \\ 0 & 1 & 3 & 2 \\ 3 & 2 & 0 & 1 \end{bmatrix}$$

Figure 1. Two PCS matrices of order 4.

The notion of PCS square matrices can be generalized to cubes. In a cube, in addition to the three coordinate directions and six diagonal directions there are also four directions of "space diagonals".

If a cube is continued periodically into the space, we define an extended diagonal as any sequence of n consecutive elements in a diagonal direction. Construction of pandiagonal magic cubes from selforthogonal, circulant, pandiagonal latin cubes was considered in [2].

References

- [1] J. Denes and A.D. Keedwell, *Latin Squares and their Applications*, Academic Press 1974.
- [2] W. Proskurowski, *Construction of pandiagonal magic squares and cubes of prime order*, TRITA-NA Report 76.22, Royal Institute of Technology, Stockholm 1976.

Department of Mathematics
University of Southern California
Los Angeles, CA 90080 - 1113
U.S.A.

Department of Computer & Info. Sci.
University of Oregon
Eugene, OR 97403 - 1202
U.S.A.