NOTE

A NOTE ON GENERALIZED ROOM SQUARES

Ian F. BLAKE*
IBM Thomas J. Watson Research Center, Yorktown Heights, NY 10598, U.S.A.

J.J. STIFFLER
Raytheon Company, Sudbury, MA 01776, U.S.A.

Received 10 August 1976

Using the properties of the Steiner system on 24 points a generalized Room square of degree 4 and order 24 is constructed. Results on a proposed alternative method for constructing generalized Room squares are given which use the notion of a (2, 4, k) array, introduced here.

1. Introduction

A generalized Room square (GRS) \( G(n, k) \) of order \( n \) and degree \( k \) on a set \( S \), \(|S| = n\), is a square array of size \( \binom{n}{k} \) whose cells are either empty or contain an unordered \( k \)-tuple of elements from \( S \) in such a way that each row and each column of \( G \) contains each element of \( S \) exactly once and each unordered \( k \)-tuple of elements from \( S \) appears exactly once in the array. An ordinary Room square is a GRS of degree 2 and they are known to exist for all even orders \( 2s \), \( s \geq 4 \).

Generalized Room squares of degree three were previously investigated by the authors [1, 2]. In this note a \( G(24, 4) \) is constructed using the (unique) Steiner system \( S(5, 8, 24) \). In Section 3 another possible construction method, which has so far proved unfruitful but is nonetheless interesting, is described.

2. A \( G(24, 4) \) from the Steiner system \( S(5, 8, 24) \)

If it is possible to construct two arrays \( A \) and \( A' \) on the set \( S \), \(|S| = n = mk\), with each array containing \( \binom{n}{k} / m = \binom{24}{4} \) rows and each row containing \( m \) \( k \)-tuples of elements of \( S \) such that:

(i) each element of \( S \) appears in exactly one \( k \)-tuple of each row of \( A \) and \( A' \),
(ii) each \( k \)-tuple of \( S \) appears exactly once in each of the arrays \( A \) and \( A' \),
(iii) it two \( k \)-tuples appear in the same row of \( A \) then they appear in different rows of \( A' \),

* On leave from the University of Waterloo, Waterloo, Ont., Canada.
then it is possible to construct a $S(n, k)$. We call two arrays $A$ and $A'$ with these properties, compatible $(k, n)$-arrays $(k \mid n)$. To see the equivalence between compatible $(k, n)$-arrays and GRS’s, form an $s \times s$ cell array $\mathcal{A}$ where each cell will either be empty or contain a $k$-tuple. Label the rows and columns of $\mathcal{A}$ with the integers 1 to $s$ in some fashion. Label the rows of the compatible $(k, n)$-arrays $A$ and $A'$ with the integers 1 to $s$ in some manner. If a $k$-tuple $\sigma$ appears in row $i$ of $A$ and row $j$ of $A'$ place $\sigma$ in cell $(i, j)$ of $\mathcal{A}$. The result is a $S(n, k)$.

Many of the previous constructions of degree 3 GRS’s used compatible $(3, n)$-arrays. A. Rosa (personal communication) and one of the authors constructed a $S(12, 4)$ in this manner. At present the systematic construction of compatible $(k, n)$-arrays seems difficult for arbitrary $k$ and $n$.

In the remainder of this section it is shown how the properties of the Steiner system $S(5, 8, 24)$, as discussed in the interesting paper of Todd [3] can be used to construct compatible $(4, 24)$-arrays and hence a $S(24, 4)$.

Following Todd [3] we refer to the blocks of $S(5, 8, 24)$ as octads, and it contains 759 octads of elements of the set $S = GF(23) \cup \{\infty\}$, GF(23) being the finite field of order 23. The linear fractional group on $S$ is triply transitive and of order 24.23.22. The subgroup $G$ containing those elements with determinant a quadratic residue in GF(23) is of order 24.23.11. The elements

$$
\begin{align*}
  x \rightarrow \frac{x + 1}{-x + 1} \quad \text{and} \quad x \rightarrow \frac{3x - 1}{x - 3}
\end{align*}
$$

generate a group $H$ of order 8 which fixes the octad $e = \{\infty, 0, 1, 3, 12, 15, 21, 22\}$. Elements of the factor group generate $S(5, 8, 24)$ by their action on $e$. From the structure of this group it is also possible to show the Steiner system can be generated by the action of the group of transformations $x \rightarrow rx + a$, $r, a \in GF(23)$, $r$ a quadratic residue, on the disjoint octads

$$
\alpha = \{\infty, 0, 1, 2, 3, 5, 14, 17, \}, \quad \beta = \{4, 13, 16, 22, 6, 7, 19, 21\},
$$

$$
\gamma = \{8, 11, 12, 18, 9, 10, 15, 20\}. \quad (1)
$$

We note for later reference that multiplying the elements of an octad by 5 (the smallest quadratic nonresidue of GF(23)) never yields an octad and this is simply shown by the absence of $5\alpha$, $5\beta$ and $5\gamma$ in the listing of the octads of $S(5, 8, 24)$ in Todd [3]. (This listing is identical to the one whose construction has been described here.)

Each tetrad (unordered 4-tuple) $\sigma$, of elements of $S$ is contained in exactly 5 octads and $\sigma$ and the five complements of $\sigma$ in these octads are disjoint with union $S$. Such a set of tetrads is called a set of mutually complementary tetrads and has the property that the union of any two tetrads in the set is an octad of $S(5, 8, 24)$. Todd [3] shows that the $(\binom{\theta}{4}) = 6.1771$ tetrads fall into 1771 sets of mutually complementary tetrads in a unique way. Call this the array $A$.

To form $A'$ multiply each tetrad of $\mathcal{A}$ by 5, the smallest quadratic nonresidue of GF(23). To show that $A$ and $A'$ are compatible $(4, 24)$ arrays it suffices to show
if \( \sigma \) and \( \eta \) are two tetrads appearing in the same row of \( A \) then they appear in different rows of \( A' \). Assume the contrary and that \( \sigma = 5\sigma' \) and \( \eta = 5\eta' \) appear in the same row of \( A' \), which implies that \( \sigma' \) and \( \eta' \) appear in the same row of \( A \). Since \( \sigma \cup \eta \) and \( \sigma' \cup \eta' \) are both octads of the Steiner system and \( \sigma \cup \eta = 5(x(\sigma' \cup \eta')) \) a contradiction is reached and \( A \) and \( A' \) form compatible \((4,24)\)-arrays implying the existence of \( \mathcal{G}(24,4) \) as claimed.

3. Another possible construction method

Constructing compatible \((k,n)\)-arrays is often difficult and the authors considered the following alternative method as a possibility. Suppose it is possible to construct an array containing \( (\frac{k^2}{2})/(\frac{k}{2}) = \frac{1}{2}(2k-1)(2k-3) = l \) rows, each row containing \( k \) pairs of unordered elements of a set \( S, |S| = 2k \), such that each element of \( S \) appears in exactly one pair in each row. Integrality conditions require that \( k \equiv 0 \) or \( 2 \) (mod 3). We call such an array a \((2,4,k)\) array if by forming all possible unions of pairs of elements in each row, the set of all 4-tuples on 2k elements is generated. To form a \( \mathcal{G}(2k,4) \) from such a \((2,4,k)\) array we assume a Room square \( R \) of order \( k \) (i.e. a \( \mathcal{G}(k,2) \)) exists, (implying only that \( k \) is even and greater than six) on the set \( S' \) with \( |S'| = k \). Associate with each pair in one row of the array an element of \( S' \) and in \( R \) replace each pair of elements of \( S' \) with the corresponding 4-tuple of elements of \( S \). A \((k-1) \times (k-1)\) array containing \( \frac{1}{2}k \) 4-tuples in each row and each column, and each element of \( S \) exactly once in each row and each column, is obtained for each row of the \((2,4,k)\) array. Forming a block diagonal sum of these \( l \) arrays yields a \( \mathcal{G}(2k,4) \). Although the results on this approach are so far negative they are of sufficient interest to comment upon.

We first show that the concept of a \((2,4,k)\) array is non-vexious by the following construction of a \((2,4,3)\) array on \( S = GF(5) \cup \{\infty\} \):

1. \((\infty, 0)\) \((1, 4)\) \((2, 3)\)
2. \((\infty, 1)\) \((0, 2)\) \((3, 4)\)
3. \((\infty, 2)\) \((1, 3)\) \((0, 4)\)
4. \((\infty, 3)\) \((2, 4)\) \((0, 1)\)
5. \((\infty, 4)\) \((0, 3)\) \((1, 2)\)

Each row contributes \( \binom{4}{2} = 6 \) 4-tuples and each of the \( \binom{4}{4} = 15 \) possible 4-tuples appears as a union of two pairs in precisely one row. Each row is obtained by adding one to the row above it.

To attempt a general construction we add some structure to the problem and assume that \( 2k - 1 = p \), a prime, for which \(-1\) is a quadratic residue and such that \( 3 \mid k \). Since \(-1\) is a nonresidue of \( p \) if \( p \) is of the form \( 4k - 1 \), we are assuming \( p \) is of the form \( 12k - 1 \). These assumptions assist in the construction. It is required to find \( (2k - 1)(\frac{3}{4}(2k - 3)) = l \) rows of \( k \) pairs of elements of \( GF(2k - 1) \cup \{\infty\} = S \). We assume that \( m = \frac{1}{2}(2k - 3) \) of the rows are of the form

\[
\sigma_i = (\infty, 0) (r_1, r_1 n_i) (r_2, r_2 n_i) \ldots (r_{k-1}, r_{k-1} n_i), \quad i = 1, \ldots, m,
\]
where $r_1, r_2, \ldots, r_{k-1}$ is the set of residues mod $p$ and $n_i$, $i = 1, \ldots, m$, is a nonresidue. The $(2, 4, k)$ array will then be the set of rows

$$\{\sigma_i + \alpha : i = 1, \ldots, m, \alpha \in \text{GF}(p)\}.$$ 

In order for a set $N = \{n_1, n_2, \ldots, n_m\}$ of nonresidues mod $p$ to yield a $(2, 4, k)$ array in this manner, it is not difficult to show that it is necessary and sufficient that it satisfy the following conditions:

(i) for all 4-tuples containing $\infty$ to be distinct we require that $n_1(1-n_2) \neq 1$ and $n_1 \neq (1-n_2)$ for any pair $n_1, n_2 \in N$.

(ii) for all 4-tuples not containing $\infty$ to be distinct we require that the set $\{(1-n_1), (1+n_1n_2), (n_1+n_2)\}$ not contain all residues or all nonresidues.

These conditions are easily derived by considering all the possibilities of equality among the 4-tuples and recalling that $-1$ was assumed to be a nonresidue.

The first interesting case occurs for $k = 6$ and $S = \text{GF}(11) \cup \{\infty\}$. There are 495 4-tuples on $S$ and we require an array with 33 rows, each row containing 6 pairs and contributing 15 4-tuples. Since $\frac{1}{2}(2k-3) = 3$, we require 3 nonresidues with the above properties and, in this case, these are uniquely determined as $N = \{7, 8, 10\}$ and

$$\sigma_1 = (\infty, 0) (1, 7) (3, 10) (4, 6) (5, 2) (9, 8),$$

$$\sigma_2 = (\infty, 0) (1, 8) (3, 2) (4, 10) (5, 7) (9, 6),$$

$$\sigma_3 = (\infty, 0) (1, 10) (3, 8) (4, 7) (5, 6) (9, 2).$$

The complete array is then given by $\{\sigma_i + \alpha : \alpha \in \text{GF}(11), i = 1, 2, 3\}$.

The next interesting case occurs for $k = 12$ and it is not difficult to show that such an array cannot be constructed by this method i.e., it is impossible to find $\frac{1}{2}(2k-3) = 7$ nonresidues with the required properties.

Unfortunately the authors have been unable to construct the required $(2, 4, k)$ array for any other value of $k$ by the nonresidue or any other method and no GRS has been constructed in this way. The assumptions used in the nonresidue method appear overly restrictive but relaxing any of them quickly introduces other difficulties. It is in doubt whether $(2, 4, k)$ arrays will exist for larger values of $k$. Many other construction methods for these arrays were tried.

4. Comments

It appears that $G(n, 4)$ will exist for many values of $n$ although the only values known by the authors for which they exist are 12 and 24. The method of compatible $(k, n)$-arrays for their construction, as discussed in Section 2, remains the most useful, although all ways known by the authors for $k = 3$ or 4 require some manual checking and trial and error. The method of Section 3 was introduced in an attempt to circumvent these problems but, while interesting in its
own right, may be of little value in such constructions. Some conclusive results on
the existence of \((2, 4, k)\) arrays would nonetheless be of interest.

References

(1975) 159–163.