The Annals of Mathematical Statistics
1970, Vol. 41, No. 3, 1122–1125

ON STANTON AND MULLIN'S CONSTRUCTION OF ROOM SQUARES[1]

BY KARL BYLEEN

University of Nebraska

1. Introduction. A *Room square* is a $(2n+1)\times(2n+1)$ array in which each cell is either empty or contains an (unordered) pair of the $2n+2$ symbols $0, 1, \cdots, 2n, \infty$. Moreover, each of the symbols appears exactly once in each row and in each column of the array, and each (unordered) pair appears exactly once in the entire array. A *cyclic Room square* (CRS) is a Room square in which the entries a_{ij}, $i, j = 0, 1, \cdots, 2n$, satisfy $a_{ij} = (x, y)$ if and only if $a_{i-1, j-1} = (x-1, y-1)$ (where addition is reduced modulo $2n+1$ and $\infty + a = a + \infty = \infty$ for $a = 0, 1, \cdots, 2n$). A *patterned Room square* (PRS) is a CRS in which the first row (the entries a_{0i}, $i = 0, 1, \cdots, 2n$) contains the (unordered) pairs $(\infty, 0)$, $(1, 2n)$, $(2, 2n-1), \cdots$, $(n, n+1)$, not necessarily in this order. Stanton and Mullin [3] gave a computer construction for PRS of (odd) side 7 through 49, with the exception of 9, for which a PRS does not exist. This note extends that result by showing that PRS of side p always exist, where p is a prime not of the form 2^s+1.

Mullin and Nemeth [1] give the following definitions for a starter and adder for a general finite Abelian group G of order $2n+1$: A *starter* in G is a set $X = \{(x_1, y_1), (x_2, y_2), \cdots, (x_n, y_n)\}$ of unordered pairs of elements of G such that (i) the elements $x_1, y_1, x_2, y_2, \cdots, x_n, y_n$, comprise all nonzero elements of G, and (ii) the differences $\pm(x_i - y_i)$, $i = 1, 2, \cdots, n$ comprise all nonzero elements of G (generating each exactly once). An *adder for* X is a set $A(X)$ of n distinct nonzero elements $a_1, a_2, \cdots, a_n$ from G such that the elements $\{x_i + a_i, y_i + a_i\}$, $i = 1, 2, \cdots, n$ are all distinct and comprise all the nonzero elements of G.

As shown in [3] and in greater detail in [1], the existence of a starter and adder for a cyclic group of order $2n+1$ implies the existence of a CRS of side $2n+1$. The proof of this fact uses the following procedure for constructing a CRS from a starter X and adder $A(X)$: the entries a_{0i} of the first row of a $(2n+1)\times(2n+1)$ array are specified by (i) $a_{00} = (\infty, 0)$, and (ii) $a_{0, -a_i} = (x_i, y_i)$, $i = 1, 2, \cdots, n$, and then the array is completed by imposing the condition that the array must satisfy the cyclic property. The result is a CRS. A PRS is thus determined by an adder which corresponds to a starter consisting of the pairs $(1, 2n)$, $(2, 2n-1), \cdots, (n, n+1)$. In the next section, an adder is given for such a starter.

Other references to the literature of Room squares will be found in [1].

Received October 3, 1969.

[1] The research for this paper was supported by NSF Undergraduate Research Participation grant GY5718, under the supervision of Professor Donald W. Crowe, at the University of Wisconsin.

2. An adder for the construction of patterned Room squares.

THEOREM. *Let* $p = 1+2^s m$, *where* $m > 1$ *is odd, let* $\Delta = 2^{s-1}$, *and let* x *be a primitive element in* $GF(p)$. *Then*

$$A(X) = \left\{(-1)^{[k/\Delta]}\frac{x^\Delta+1}{x^\Delta-1}x^k: k = 0, 1, \ldots, m\Delta-1\right\}$$

is an adder for the starter $X = \{(x^k, x^{k+m\Delta}): k = 0, 1, \cdots, m\Delta-1\}$. (*As usual,* $[t]$ *denotes the greatest integer less than or equal to* t.)

PROOF. It suffices to show (a) the elements of $A(X)$ are distinct and nonzero, and (b) in the set

$$X+A(X) = \left\{\left(x^k+(-1)^{[k/\Delta]}\frac{x^\Delta+1}{x^\Delta-1}x^k,\right.\right.$$
$$\left.\left. x^{k+m\Delta}+(-1)^{[k/\Delta]}\frac{x^\Delta+1}{x^\Delta-1}x^k\right): k = 0, 1, \ldots, m\Delta-1\right\}$$

each nonzero element of $GF(p)$ appears exactly once as a first or second component.

(a) Since $m > 1$ is odd, $x^\Delta \neq \pm 1$, so the elements of $A(X)$ are nonzero. Furthermore,

$$(-1)^{[k/\Delta]}\frac{x^\Delta+1}{x^\Delta-1}x^k = (-1)^{[j/\Delta]}\frac{x^\Delta+1}{x^\Delta-1}x^j$$

implies $x^k = \pm x^j$. Since $k, j = 0, 1, \cdots, m\Delta-1$, we must have $x^k = x^j$, as required.

(b) Noting that $X+A(X)$ contains $m\Delta$ pairs, and hence $2m\Delta = p-1$ components, it suffices to show that in $X+A(X)$, (i) no two first components are equal, (ii) no two second components are equal, and (iii) no first component equals some second component. We consider first the implications of the equality

$$x^k(\pm(x^\Delta-1)\pm(x^\Delta+1)) = x^j(\pm(x^\Delta-1)\pm(x^\Delta+1))$$

in the 16 possible choices of the $+$ and $-$ signs. *Case* 1. $++++$, $----$, $+-+-$, $-+-+$. Each of these choices implies $x^k = x^j$, so $k = j$. *Case* 2. $+-++$, $+++-$, $-+--$, $---+$. Each implies either $-x^k = x^{j+\Delta}$ or $-x^j = x^{k+\Delta}$. Thus either $k+m\Delta = j+\Delta$ or $j+m\Delta = k+\Delta$, so $[j/\Delta]$ and $[k/\Delta]$ have the same parity. *Case* 3. $++-+$, $+---$, $--+-$, $-+++$. Proceeding as in Case 2, we find that $[j/\Delta]$ and $[k/\Delta]$ have different parity. *Case* 4. $++--$, $+--+$, $--++$, $-++-$. Each implies $x^k = -x^j$, so $k = j+m\Delta$. We now establish (b) by showing (i), (ii), and (iii).

(i) Suppose two first components are equal. Then there exist $j, k = 0, 1, \cdots, m\Delta-1$ such that

$$x^k+(-1)^{[k/\Delta]}\frac{x^\Delta+1}{x^\Delta-1}x^k = x^j+(-1)^{[j/\Delta]}\frac{x^\Delta+1}{x^\Delta-1}x^j,$$

which implies $x^k((x^\Delta-1)+(-1)^{[k/\Delta]}(x^\Delta+1)) = x^j((x^\Delta-1)+(-1)^{[j/\Delta]}(x^\Delta+1))$. If $[k/\Delta]$ and $[j/\Delta]$ have the same parity, then Case 1 applies (and $k = j$). If $[k/\Delta]$

and $[j/\Delta]$ have different parity, then Case 2 applies (a contradiction). Thus the only possibility is $k = j$, which shows that no two first components are equal.

(ii) Suppose two second components are equal. Proceeding as in (i) we find again that the only possibility is $k = j$, as required.

(iii) Suppose some first component equals some second component. Then there exist $j, k = 0, 1, \cdots, m\Delta - 1$ such that

$$x^k + (-1)^{[k/\Delta]} \frac{x^\Delta + 1}{x^\Delta - 1} x^k = -x^j + (-1)^{[j/\Delta]} \frac{x^\Delta + 1}{x^\Delta - 1} x^j,$$

which implies $x^k((x^\Delta - 1) + (-1)^{[k/\Delta]}(x^\Delta + 1)) = x^j(-(x^\Delta - 1) + (-1)^{[j/\Delta]}(x^\Delta + 1))$. If $[k/\Delta]$ and $[j/\Delta]$ have the same parity, then Case 3 applies (a contradiction). If $[k/\Delta]$ and $[j/\Delta]$ have different parity, then Case 4 applies (again a contradiction since $k = j + m\Delta$ is impossible). Thus no first component equals some second component, completing the proof of (b), and of the main result.

From the remarks made in the introduction, it follows that PRS of side p exist, where p is a prime not of the form $2^s + 1$.

3. Patterned Room squares from strong starters. In [2], Mullin and Nemeth defined a *strong starter* $X = \{(x_i, y_i): i = 1, 2, \cdots, n\}$ to be a starter with the additional property that the elements of the set $\{x_i + y_i: i = 1, 2, \cdots, n\}$ are distinct and nonzero. In [1] it was shown that for a strong starter the set $\{-(x_i + y_i): i = 1, 2, \cdots, n\}$ is an adder, say $A(X)$. Thus the set $X + A(X) = \{(-y_i, -x_i): i = 1, 2, \cdots, n\}$ is also a strong starter. The following similar result shows how a patterned Room square may be obtained from a strong starter.

PROPOSITION. *If $X = \{(x_i, y_i): i = 1, 2, \cdots, n\}$ is a strong starter, then the set $A = \{-(x_i + y_i)/2: i = 1, 2, \cdots, n\}$ is an adder for X.*

PROOF. It suffices to show that the elements of each of the two sets A and $B = \{x_i - (x_i + y_i)/2,\ y_i - (x_i + y_i)/2:\ i = 1, 2, \cdots, n\} = \{(x_i - y_i)/2,\ (y_i - x_i)/2:\ i = 1, 2, \cdots, n\}$ are distinct and nonzero. Since X is a strong starter the elements of each of the sets $C = \{x_i + y_i: i = 1, 2, \cdots, n\}$ and $D = \{x_i - y_i, y_i - x_i: i = 1, 2, \cdots, n\}$ are distinct and nonzero. Hence the elements of A (compare to set C) are distinct and nonzero, as are the elements of B (compare to set D), thus completing the proof.

Therefore A is an adder for X, say $A(X)$, and furthermore the pairs in $X + A(X) = \{((x_i - y_i)/2, (y_i - x_i)/2): i = 1, 2, \cdots, n\}$ are in the form $(a, -a)$. Thus the first column of the CRS obtained from the strong starter X and the adder $A(X)$ in a cyclic group contains the pairs $(\infty, 0)$, $(1, 2n)$, $(2, 2n-1)$, $\cdots$, $(n, n+1)$, so the array is a PRS (we consider the rows as columns and columns as rows to strictly satisfy the definition given for PRS).

The existence of a strong starter in $GF(p^n)$ where p^n is not of the form $2^s + 1$ (exhibited in [2]), thus also shows the existence of PRS of side p where p is not of the form $2^s + 1$.

The theorem also holds for $GF(p^n)$, $n > 1$, although in this case the Room square constructed from the starter and adder (as in [1]) will not be cyclic, and thus not a

PRS. Mullin has noted that by generalizing the definition of PRS to a Room square (not necessarily cyclic) in which the first row consists of inverse elements, then the theorem (as well as the strong starter result) implies the existence of the generalized PRS of side q, where q is a prime power not of the form 2^s+1.

REFERENCES

[1] MULLIN R. C. and NEMETH, E. (1969). On furnishing Room squares. *J. Combinatorial Theory* **7** 266–272.

[2] MULLIN, R. C., and NEMETH, E. (1969). An existence theorem for Room squares. *Canad. Math. Bull.* **12** 493–497.

[3] STANTON, R. G. and MULLIN, R. C. (1968). Construction of Room squares. *Ann. Math. Statist.* **39** 1540–1548.