AN EXISTENCE THEOREM FOR ROOM SQUARES*

R. C. Mullin and E. Nemeth

(received April 11, 1969)

It is shown that if \( v \) is an odd prime power, other than a prime of the form \( 2^n + 1 \), then there exists a Room square of order \( v + 1 \).

1. Introduction. A room square of order \( 2n \), where \( n \) is a positive integer, is an arrangement of \( 2n \) objects in a square array of side \( 2n - 1 \), such that each of the \( (2n - 1)^2 \) cells of the array is either empty or contains exactly two distinct objects; each of the \( 2n \) objects appears exactly once in each row and column; and each (unordered) pair of objects occurs in exactly one cell.

Room squares are known to exist for all even orders \( v \leq 48 \) (except 4 and 6)[3], for \( v = 2^{2n} + 1 \) [1] and for \( v + 1 \) where \( v = p^n \equiv 1 \text{ mod } 6 \) [2].

2. Previous Results. We now cite some results of [2] which will be used in this construction. Let \( G \) be a finite Abelian group of odd order \( 2n + 1 \).

By a starter in \( G \) we mean a set \( X = \{(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)\} \) of unordered pairs of elements of \( G \) such that

(i) the elements \( x_1, y_1, x_2, y_2, \ldots, x_n, y_n \) comprise all the non-zero elements of \( G \), and

(ii) the differences \( \pm (x_i - y_i) \) \( i = 1, 2, \ldots, n \) comprise all the non-zero elements of \( G \) (generating each precisely once).

* Work supported in part by NRC Grant No. A-3071.


493
By an adder for the starter $X$ we mean a set $A(X)$ of $n$ distinct non-zero elements $a_1, a_2, \cdots, a_n$ from $G$ such that the elements $\{x_i + a, y_i + a\} \quad i = 1, 2, \cdots, n$ are all distinct and comprise all the non-zero elements of $G$.

Then by [2, Theorem 1], if an Abelian group $G$ of odd order $v = 2n + 1$ admits a starter $X$ and an adder $A(X)$, then there exists a Room square of order $v + 1$; by Corollary 1 to Theorem 2, if an Abelian group $G$ of order $2n + 1$ admits a starter $X = \{(x_i, y_i): i = 1, 2, \cdots, n\}$ such that all sums of corresponding pairs are distinct and non-zero then the set of elements $-(x_i + y_i)$ forms an adder for $X$. In view of these results, letting $G = GF(p^n)$ we need only construct a starter with the additional property that the sums of corresponding pairs of elements are all distinct and non-zero to guarantee the existence of a Room square of order $p^n + 1$.

3. The Construction. The construction of this section produces a starter with the required additional property, for the additive group of $GF(p^n)$ where $p^n = 2^k t + 1$, $t$ odd and exceeding 1. Let us call such a starter strong. The form of the starter depends on the exponent $k$. We begin with a lemma for the specific case of $k = 1$ which indicates the general method used.

**Lemma 1.** If $p^n \equiv 1 \mod 2$ but $p^n \not\equiv 1 \mod 4$, then there exists a strong starter for $G = GF(p^n)$ for $p^n \neq 3$.

**Proof.** Let $x$ be primitive in $GF(p^n)$ where $p^n = 2t + 1$, $t$ odd; then the set $X = \{ (x^0, x^1), (x^2, x^3), \cdots, (x^{2t-2}, x^{2t-1}) \}$ is a starter for $G$ and further the sums of respective pairs are all distinct and non-zero, that is, $X$ is a strong starter.

Since $x$ is primitive in $GF(p^n)$ it generates $G - \{0\}$ and the elements $x^0, x^1, x^2, \cdots, x^{2t-1}$ are all distinct and non-zero. Further the differences of corresponding pairs in the set $X$ are $+ x(1-x), x(1-x), \cdots, x^{2t-2}(1-x)$ respectively. $(1-x)$ is a non-zero field element so it is evident that the only possible duplication would occur if $x^i(1-x) = - x^j(1-x)$ for $0 \leq i, j \leq t-1$, but then $x^i + x^j = 0$. If $i = j$ the field $GF(p^n)$ would have characteristic 2, an impossibility since $p^n$ is odd. If $i \neq j$, say $i < j$ then $x^i(1 + x^{2j-2i}) = 0$ and it follows that $x^{2j-2i} = -1$. But since $x$ is
primitive in $\text{GF}(2^t + 1)$, $x^t = -1$ and $0 < 2j - 2i \leq 2t - 2 < p^n - 1$
is a residue mod $p^n$ and hence must be equal to $t$, a contradiction occurs since $2j - 2i$ is even and $t$ is odd. The sums of corresponding pairs of elements of $X$ are $x^0 (1 + x)$, $x^2 (1 + x)$, $\cdots$ $x^{2t-2} (1 + x)$.

Indeed, suppose that $x^{2i} (1 + x) = x^{2j} (1 + x)$, then if $x \neq -1$, (i.e. if $p^n > 3$), $(1 + x)^{-1}$ exists and we would have $x^{2i} = x^{2j}$ for $0 < 2i, 2j < p^n - 1$ which can only happen if $i = j$, and the lemma follows.

**THEOREM 1.** There exists a strong starter for $G = \text{GF}(p^n)$, where $p^n = 2^k t + 1$ for $k$ a positive integer and $t$ an odd integer $> 1$.

**Proof.** Let $2^{k-1} = \Delta$, and $x$ be a primitive element in $\text{GF}(2^k t + 1)$. Then the set

$$X = \begin{cases}
(x^0, x) & (x^{2\Delta}, x^{3\Delta}) & \cdots & (x^{(2t-2)\Delta}, x^{(2t-1)\Delta}); \\
(x^1, x^{\Delta+1}) & (x^{2\Delta+1}, x^{3\Delta+1}) & \cdots & (x^{(2t-2)\Delta+1}, x^{(2t-1)\Delta+1}); \\
\vdots & \vdots & \ddots & \vdots \\
(x^{\Delta-1}, x^{2\Delta-1}) & (x^{3\Delta-1}, x^{4\Delta-1}) & \cdots & (x^{(2t-1)\Delta-1}, x^{2t\Delta-1})
\end{cases},$$

is a strong starter for $\text{GF}(p^n)$. The set $X$, if considered as an array and read vertically lists the elements $x^0, x^1, x^2, \ldots, x^{2t\Delta-1} = x^{2^{k-1} - 1} = x^{p^n - 2}$ in natural order and thus comprises $G - \{0\}$. The differences between pairs in the starter are

$$x^0 (1 - x^\Delta), \; x^{2\Delta} (1 - x^\Delta), \; \ldots, \; x^{(2t-2)\Delta} (1 - x^\Delta);$$

$$x^1 (1 - x^\Delta), \; x^{2\Delta+1} (1 - x^\Delta), \; \ldots, \; x^{(2t-2)\Delta+1} (1 - x^\Delta);$$

$$\vdots \quad \vdots \quad \vdots \quad \vdots \\
\vdots \quad \vdots \quad \vdots \quad \vdots \\
\vdots \quad \vdots \quad \vdots \quad \vdots \\
(x^{\Delta-1} (1 - x^\Delta), \; x^{3\Delta-1} (1 - x^\Delta), \; \ldots, \; x^{(2t-1)\Delta-1} (1 - x^\Delta).$$

$(1 - x^\Delta)$ is a non zero element of $G$ since the order of the element $x$ is by hypothesis $2t\Delta > \Delta$. Suppose $x^{2i\Delta + j} (1 - x^\Delta) = x^{2i'\Delta + j'} (1 - x^\Delta)$ for $0 \leq i, i' \leq t - 1$, and $0 \leq j, j' \leq \Delta - 1$, then $x^{2i\Delta + j} + x^{2i'\Delta + j'} = 0.$
Since $p$ is an odd prime, $2i\Delta + j \neq 2i'\Delta + j'$. Assuming that 
$2i\Delta + j < 2i'\Delta + j'$ we write $x^{2i\Delta+j} (1 + x^{2i'\Delta + j' - 2i\Delta + j}) = 0$.
As before, this implies $2i'\Delta + j' - 2i\Delta - j = (2i' - 2i)\Delta + (j' - j) = \Delta t$.
Since $j' - j$ lies in the range $-\Delta + 1$ to $\Delta - 1$ and is a multiple of $\Delta$, it must be 0. Hence $2i' - 2i = t$ which contradicts the fact that $t$ is odd.

The fact that the starter $X$ is strong can be seen by noting that the sums of respective pairs are the same form as the differences with the factor $(1 + x^{\Delta})$ rather than $(1 - x^{\Delta})$. But $(1 + x^{\Delta})$ is non-zero if $x$ is not of order $2\Delta$, that is, if $t > 1$. As above, this hypothesis guarantees that the starter is strong, and the theorem follows.

We note that in the case $p = 2^{k} + 1$, the set

$$X = \{(x^0, x^\Delta), (x^1, x^{\Delta+1}), \ldots, (x^{\Delta-1}, x^{2\Delta-1})\}$$

is a starter, but the sums of pairs of respective elements are $x^0(1 + x^\Delta)$, $x(1 + x^{\Delta})$, $\ldots$, $x^{\Delta-1}(1 + x^\Delta)$; however, $1 + x^\Delta = 0$ and so these sums are all equal to zero. However, it is still possible to obtain further results in this case. It is trivial to show that if $p$ is a prime of the form $2^{k} + 1$, then $p^3$ does not have this form, that is, if $p^3$ has the form $2^{k} + 1$, $p$ does not. However, Stanton [4] has shown that if there exist squares of sides $m$ and $n$, then there exists a square of side $mn$. So in any event, there exists a Room square of side $p^3$ for all odd primes $p$. A similar argument shows that there exists a Room square of side $p^2$ for all odd primes $p \neq 3$. However, a square of side 9 is known to exist [3]. Since any prime power $p^m$ ($m > 1$) may be written as $(2^a)(p^\beta)$, for non-negative integers $a$, $\beta$, there exists a Room square of side $p^m$ for all odd primes $p$ and all integers $m > 1$. Hence the only prime power exceptions are some of the primes themselves. Moreover it is an elementary exercise in number theory to show that $2^{k+1}$ cannot be prime unless $k$ is a power of 2; that is, the only exceptional primes are the famous Fermat primes, namely 3, 5, 17, 257, 65,537 and any other Fermat primes which may exist. (A Room square of side 17 is known to exist, cf. [3].)

The authors wish to thank Professor R. G. Stanton for his valuable comments and suggestions.
REFERENCES


2. R.C. Mullin and E. Nemeth, On furnishing Room squares. (to appear)


4. R.G. Stanton, A multiplication theorem for Room squares. (to appear)

University of Waterloo
Waterloo, Ontario

Florida Atlantic University
Boca Raton, Florida 33432