CONGRESSUS NUMERANTIUM XXIII

Proceedings of the Tenth Southeastern Conference On Combinatorics, Graph Theory And Computing

Volume I

Florida Atlantic University
Boca Raton
April 2-6, 1979

New Lower Bounds for the Number of Pairwise Orthogonal Symmetric Latin Squares

Jeffrey H. Dinitz

1. Introduction

Two Latin squares R and C on the symbol set $\{1,2,\ldots,r\}$ are said to be orthogonal symmetric Latin squares if:

(i) R and C are both symmetric;

(ii) R and C are both idempotent (i.e. $R(i,i) = C(i,i) = i$) ;

(iii) If R and C have (i,j) entries α and δ respectively, where $i < j$, then there are not numbers k and m for which $k < m$ and R and C have (k,m) entries α and δ respectively, except $k = i$ and $m = j$.

This definition was first given by Gross, Mullin and Wallis [3]. Using their notation we let $\nu(r)$ denote the size of the largest possible set of pairwise orthogonal symmetric Latin squares (POSLS) of side r . In this paper we will prove the following.

Theorem 0. If $q = 2^k t+1$ is a prime power with t odd then $\nu(q) \geq t$.

This will be proved by giving a construction for t POSLS of order q . As an example we have $29 = 4 \cdot 7+1$ and thus, we can construct 7 POSLS of order 29. Earlier constructions have yielded other lower bounds for these prime powers ([3], [4], [5], [1]) , however, the new bounds in this paper are greater than or equal to the previous bounds whenever $t > 1$.

We also point out that the existence of t pairwise orthogonal symmetric Latin squares of order q is equivalent to the existence of t pairwise

PROC. 10TH S-E CONF. COMBINATORICS, GRAPH THEORY, AND COMPUTING, pp. 393-398.

orthogonal one-factorizations of K_{q+1} and also to the existence of a Room t-design of side q . We refer the reader to Gross, Mullin and Wallis [3] or Wallis, Street, Wallis [7] or Horton [4] for discussion and proofs of these equivalences.

2. The Construction

Let G be an abelian group of odd order $r = 2n+1$. A starter in G is defined to be a set $S = \{\{x_1,y_1\},\{x_2,y_2\},\ldots,\{x_n,y_n\}\}$ with the properties that $\{x_1,x_2,\ldots,x_n,y_1,y_2,\ldots,y_n\}$ and $\{\pm(x_1-y_1),\pm(x_2-y_2),\ldots,\pm(x_n-y_n)\}$ consist of all non-zero elements of G taken once. Given a starter there is an associated symmetric Latin square [3].

Two starters S_1 and S_2 are said to be orthogonal if they satisfy the following properties:

(i) S_1 and S_2 have no pair in common

(ii) Given any $\{x_1,y_1\}$ and $\{x_2,y_2\} \in S_1$ with $x_1 \neq x_2$ and any $\{u_1,v_1\}$ and $\{u_2,v_2\} \in S_2$ then $y_i - x_i = v_i - u_i$, $i = 1,2$, implies $x_1 - u_1 \neq x_2 - u_2$.

It is not difficult to show that two starters are orthogonal if and only if their associated symmetric Latin squares are symmetric orthogonal (see [3], or [7]). Thus the following construction of t pairwise orthogonal starters is equivalent to the construction of t pairwise orthogonal symmetric Latin squares.

Theorem 1. There exists t pairwise orthogonal starters in the additive group of GF(q) .

Proof: Let $p^s = q$ be a prime power and write $q = 2^k t+1$ with t a uniquely determined odd number and $k > 0$. Also, let ω be a generator of $GF(q)^*$ and let $\Delta = 2^{k-1}$. Define the cyclotomic classes, C_i , of order t [6] by

$$C_i = \{\omega^{2\Delta s+i} | s = 0,1,\dots,t-1\} \ , \ i = 0,1,\dots,2\Delta-1 \ .$$

The C_i's are pairwise disjoint and their union is $GF(q)^*$. Also, $C_i = -C_{\Delta+i}$ where the subscripts are taken $\bmod 2\Delta$. Observe $C_\Delta = -C_0$ where C_0 is the cyclic subgroup of $GF(q)^*$ of order t.

Call $H \subset GF(q)^*$ a half-set iff $H \cup -H = GF(q)^*$. In particular, $H = C_0 \cup C_1 \cup \dots \cup C_{\Delta-1}$ is a half-set and for all $a \in GF(q)^*$, $a \neq 1$, $H_a = \frac{1}{a-1} H$ is also a half-set. H and H_a also have the properties that $C_\Delta H = -H$ and $C_\Delta H_a = -H_a$.

Claim: $S_a = \{\{x,ax\} | x \in H_a\}$ is a starter for all $a \in C_\Delta$. Furthermore, if $a,b \in C_\Delta$, $a \neq b$, then S_a is orthogonal to S_b.

We see that since $|C_\Delta| = t$ that this claim implies Theorem 1.

Proof (of claim): We must first show that S_a is a starter in $GF(q)^+$. Notice that if $a \in C_\Delta$ then $ax \in C_\Delta H_a = -H_a$. Therefore, $\{\{x,ax\} | x \in H_a\} = GF(q)^*$. Now, the forward differences $x(a-1)$ are all in $H_a(a-1) = H$. The backward differences $x(1-a)$ are all in $-H$. Thus, $\{x(a-1) | x \in H_a\} = H$ and similarly $\{x(1-a) | x \in H_a\} = -H$. So $\{\pm(ax-x) | x \in H_a\} = H \cup -H = GF(q)^*$. Therefore for every $a \in C_\Delta$, S_a is a starter.

Now we must show that if $a \neq b \in C_\Delta$, then S_a is orthogonal to S_b. First, it is clear that S_a and S_b have no pairs in common. Now let

$$\{x,ax\} \ , \ \{y,ay\} \in S_a \qquad x \neq y$$
$$\{z,bz\} \ , \ \{w,bw\} \in S_b$$

such that $x(a-1) = z(b-1)$
and $y(a-1) = w(b-1)$

then $(x-y)(a-1) = (z-w)(b-1)$.

Now since $a-1 \neq b-1$ and $x \neq y$ we have that $x-y \neq z-w$. So $x-z \neq y-w$, which was to be shown.

This proves that S_a is orthogonal to S_b.

3. Example

Let $q = 29 = 4 \cdot 7+1$. We have that 2 is a generator of $GF(29)^*$ and $\Delta = 2$. Also $C_\Delta = \{4,6,9,8,28,13,5,22\}$. We give the 7 orthogonal starters constructed by Theorem 1.

$$S_4 = \begin{array}{l} \{10,11\},\{15,2\},\{8,3\},\{12,19\},\{18,14\},\{27,21\},\{26,17\} \\ \{20,22\},\{1,4\},\{16,6\},\{24,9\},\{7,28\},\{25,13\},\{23,15\} \end{array}$$

$$S_6 = \begin{array}{l} \{6,7\},\{9,25\},\{28,23\},\{13,20\},\{5,1\},\{22,16\},\{4,24\} \\ \{12,14\},\{18,21\},\{27,17\},\{26,11\},\{10,2\},\{15,3\},\{8,19\} \end{array}$$

$$S_9 = \begin{array}{l} \{11,12\},\{2,18\},\{3,27\},\{19,26\},\{14,10\},\{21,15\},\{17,8\} \\ \{22,24\},\{4,7\},\{6,25\},\{9,23\},\{28,20\},\{13,1\},\{5,16\} \end{array}$$

$$S_{28} = \{\{x,-x\} \mid x \in GF(q)^*\}$$

$S_{13} = -S_9$ where $\{x,y\} \in S$ if and only if $\{-x,-y\} \in -S$.

$S_5 = -S_6$

$S_{22} = -S_4$

4. More Starters

For no value of q which was checked did the set of starters given in Theorem 1 prove to be maximal. The size of a maximal set of starters containing those starters defined in Theorem 1 is given in section 5 and constitute greater lower bounds for $\nu(r)$. Listings of these new starters will be given in a later paper. Also, by use of computer, we found new larger maximal sets of orthogonal starters for some small values of n not included in the results of Theorem 1.

5. Known Lower Bounds

We refer the reader to the list of known lower bounds given in Gross, Mullin and Wallis [3].

We amend the list with the following new lower bounds.

r	$\nu(r)$	bound obtained by Thm 0	old bound
13	5*	3	3
25	7*	3	3
29	13	7	4
53	15	13	7
61	21	15	8
73	9	9	3
101	31	25	13

* Also obtained by Gross [2].

Also by computer we have

$$\nu(15) \geq 4$$
$$\nu(17) \geq 4$$
$$\nu(21) \geq 4$$

References

[1] B. C. Chong and K. M. Chan, "On the existance of normalized Room squares",Nanta Math. 7 (1974) , 8-17.

[2] K. B. Gross, "Some new classes of strong starters," Discrete Math. 12 (1975), 225-243.

[3] K. B. Gross, R. C. Mullin and W. D. Wallis, "The number of pairwise orthogonal symmetric Latin squares," Utilitas Mathematica 4 (1973), 239-251.

[4] J. D. Horton, "Room designs and one-factorizations," Aequations Math.

[5] R. C. Mullin and E. Nemeth, "An existence theorem for Room squares," Canad. Math. Bull. 12 (1969), 493-497.

[6] Thomas Storer, Cyclotomy and Difference Sets, Markham, 1967.

[7] W. D. Wallis, Anne Penfold Street and Jennifer Seberry Wallis, Combinatorics: Room Squares, Sum-Free Sets, Hadamard Matrices, Springer-Verlag (1972).