ROOM n-CUBES OF LOW ORDER

JEFFREY H. DINITZ

Abstract

A Room n-cube of side t is an n dimensional array of side t which satisfies the property that each two dimensional projection is a Room square. The existence of a Room n-cube of side t is equivalent to the existence of n pairwise orthogonal symmetric Latin squares (POSLS) of side t. The existence of n pairwise orthogonal starters of order t implies the existence of n POSLS of side t. Denote by $\nu(n)$ the maximum number of POSLS of side t. In this paper, we use Galois fields and computer constructions to construct sets of pairwise orthogonal starters of order $t \leq 101$. The existence of these sets of starters gives improved lower bounds for $\nu(n)$. In particular, we show $\nu(17) \geq 5$, $\nu(21) \geq 5$, $\nu(29) \geq 13$, $\nu(37) \geq 15$ and $\nu(41) \geq 9$, among others.

1980 *Mathematics subject classification (Amer. Math. Soc.)*: 05 B 15.

1. Introduction

A Room n-cube of side r is an n dimensional array of side r which enjoys the property that each two dimensional projection of the array is a Room square of side r. For background information on Room squares and Room n-cubes the reader is referred to [2], [6], [9] and [10]. It is easily shown (see Horton [7]) that the dimension of a Room n-cube of side r must be less than $r - 2$ (that is, $n \leq r - 2$). Let $\nu(r)$ denote the maximum dimension of a Room n-cube of side r. In this paper, we give improved lower bounds for $\nu(r)$ for certain small values of r ($r \leq 101$).

The following is known about $\nu(r)$ (see [2] for a more complete list).

THEOREM 1.1 (Dinitz and Stinson [4]). $v(r) \geqslant 3$ *for all odd $r \geqslant 7$.*

THEOREM 1.2 (Dinitz [1]). $v(q) \geqslant t$, *if $q = 2^k t + 1$ is a prime power with t odd.*

THEOREM 1.3 (Gross, Mullin and Wallis [6]). $v(r) \to \infty$ *as $r \to \infty$.*

In order to construct Room n-cubes, we define the notion of orthogonal starters. A *starter* of order g in an additive abelian group G, $|G| = g$, is a set of pairs $A = \{\{s_i, t_i\}, 1 \leqslant i \leqslant \frac{1}{2}(g-1)\}$ satisfying the properties:
  (i) $\{s_i\} \cup \{t_i\} = G \backslash \{0\}$,
  (ii) $\{\pm(s_i - t_i)\} = G \backslash \{0\}$.
The starter $P = \{\{x, -x\} \mid x \in G\}$ is termed the *patterned* starter. A starter $A = \{\{s_i, t_i\}\}$ is a *strong starter* if $s_i + t_i \neq s_j + t_j$ for all $i \neq j$.

Let $A = \{\{s_i, t_i\}\}$ and $B = \{\{u_i, v_i\}\}$ be two starters in G. We may assume that $t_i - s_i = v_i - u_i$ for all $1 \leqslant i \leqslant \frac{1}{2}(g-1)$. A and B are *orthogonal starters* if $u_i - s_i \neq u_j - s_j$ for all $i \neq j$, and if $u_i \neq s_i$ for all i. It is easily shown that if A is a strong starter, then A and $-A = \{\{-s_i, t_i\}\}$ and P are 3 pairwise orthogonal starters. All starters constructed in this paper will be strong starters. The connection between orthogonal starters and Room n-cubes is given in the following theorem.

THEOREM 1.4 (Horton [7]). *If there exist n pairwise orthogonal starters of order r, then there is a Room n-cube of side r, and thus $v(r) \geqslant n$.*

In view of the above theorem, to find lower bounds for $v(r)$ it is convenient to search for large sets of pairwise orthogonal starters of order r. The proof of Theorem 1.2 above introduces a construction for t pairwise orthogonal starters in $GF(q)^+$, where $q = 2^k t + 1$ is a prime power with t odd. In Section 2 we show that the starters found in Theorem 1.2 are in some sense unique. In Section 3 we will add on some starters to those given in Theorem 1.2 to obtain larger sets of pairwise orthogonal starters. These new starters will be termed two-quotient starters and will be defined presently.

In Section 4 we give 4 pairwise orthogonal starters of order 15 and 5 pairwise orthogonal starters of orders 17, 21, 33, 35, 39. These starters were obtained by use of a computer.

2. One quotient starters

For this section and the next we assume $q = 2^k t + 1$ is a prime power with t odd. For the sake of clarity we indicate the proof of Theorem 1.2.

Let $G = GF(q)^*$ be the multiplicative group of the Galois field $GF(q)$ and let $C_0 \subseteq G$ be the subgroup of G or order t. Let $\Delta = 2^{k-1}$ and let $C_0, C_1, \ldots, C_{2\Delta-1}$ be the multiplicative cosets of C_0. Note that $C_i = -C_{\Delta+i}$ where the subscripts are taken mod $2\Delta = 2^k$. In particular, $-1 \in C_\Delta = -C_0$.

Call $H \subseteq G$ a *half-set* if $H \cup -H = G$. Thus $H = C_0 \cup C_1 \cup \cdots \cup C_{\Delta-1}$ is a half-set, and for all $a \in G$, $a \neq 1$, $H_a \doteq (1/(a-1)) H$ is also a half-set. H and H_a also have the properties that $C_\Delta H = -H$ and $C_\Delta H_a = -H_a$. For each $a \in C_\Delta$ define $S_a = \{\{x, ax\} \mid x \in H_a\}$.

Theorem 1.2 asserts that for each $a \in C_\Delta$, S_a is a starter, and for $a \neq b \in C_\Delta$ that S_a is orthogonal to S_b. The proof is straightforward and we omit it here. Note that $|C_\Delta| = t$ and thus we have constructed t pairwise orthogonal starters of order $q = 2^k t + 1$. Therefore $\nu(q) \geq t$.

Every starter defined above and the original Mullin-Nemeth starters [8] which these starters generalize, have the property that the quotient of the elements in any pair is a constant. To be more precise, define $S = \{\{x_i, y_i\}\}$ to be a *one quotient starter* in $GF(q)^+$ if there exists some $a \in GF(q)^*$ such that $x_i/y_i = a$ or $y_i/x_i = a$ for all i. Then we see that each starter S_a is a one quotient starter with quotient $a \in C_\Delta$.

The following theorem determines the possible quotients of one quotient starters.

THEOREM 2.1. *If S is a one quotient starter in $GF(q)^+$ with quotient a, then $a \in C_\Delta$.*

PROOF. Let $S = \{\{s_i, t_i\}\}$ be a starter in $GF(q)^+$ and without loss of generality let $t_i/s_i = a$ for all i. If $\{x, ax\} \in S$, then so must be $\{a^2x, a^3x\}$, $\{a^4x, a^5x\}, \ldots$ and $\{a^{s-2}x, a^{s-1}x\}$ where s is the order of a in $GF(q)^*$. The differences between the elements in these pairs are $\pm x(a-1)$, $\pm a^2x(a-1)$, $\pm a^4x(a-1), \ldots$ and $\pm a^{s-2}x(a-1)$, respectively. Since S is a starter these differences are all distinct. However, if $4 \mid s$, then $s/2 = 2n$ is even. Since $a^{s/2} = -1$, then $x(a-1) = -a^{s/2}x(a-1) = a^{2n}x(a-1)$, which implies that the differences above are not all distinct, a contradiction. Thus $4 \nmid s$.

With $C_0, C_1, \ldots, C_\Delta, \ldots, C_{2\Delta-1}$ as defined above, it is clear that if s is the order of a and if $4 \nmid s$, then $a \in C_0 \cup C_\Delta$.

Assume $a \in C_0$. Then it must be possible to write $C_0 = \cup_j \{x_j, ax_j\}$ where $\{x_j, ax_j\} \in S$ for all j. But $|C_0| = t$ is odd. Thus C_0 is not the disjoint union of pairs of elements. Therefore $a \neq C_0$, and thus the result.

REMARK. Note that according to Theorem 2.1, those starters S_a defined above comprise the largest possible set of orthogonal one quotient starters.

3. Two quotient starters

In this section we will find new starters which are pairwise orthogonal to each other and also orthogonal to each of the starters determined by Theorem 1.2. In view of the remark following Theorem 2.1 it is impossible for these new starters to be one quotient starters. So as a generalization of one quotient starters we define $S = \{\{s_i, t_i\}\}$ to be a k *quotient starter* in $GF(q)^+$ if there exist $Q = \{a_0, a_1, \ldots, a_{k-1}\} \subseteq GF(q)^*$ such that $t_i/s_i \in Q$ or $s_i/t_i \in Q$ for each i. Note that if $a_1 = a_2 = \cdots = a_k$, then S is also a one quotient starter. We will concentrate on two quotient starters.

Let $q = 4t + 1$ be a prime power with t odd. As in the previous section let $C_0 \subseteq GF(q)^* = G$ be the subgroup of order t (so C_0 has index 4). Again let C_0, C_1, C_2, C_3 be the multiplicative cosets of C_0. Define the set $S(a_0, a_1) \doteq \{\{x, a_0, x\}, \{y, a_1 y\} \mid x \in C_0^{a_0}, y \in C_1^{a_1}\}$ where $C_i^{a_i} = (1/(a_i - 1))C_i$ for $i = 0, 1$. Notice that if $S(a_0, a_1)$ is a starter, then it is a two quotient starter. Also, if $a_0 = a_1 = a \in C_2$, then $S(a_0, a_1) = S_a$ defined in Section 2 (since $H_a = C_0^a \cup C_1^a$). The following gives necessary and sufficient conditions for $S(a_0, a_1)$ to be a starter.

LEMMA 3.1. $S(a_0, a_1)$ *is a starter in* $GF(q)^+$ *if and only if the following conditions are satisfied*:

(a) $a_0 \notin C_0, a_1 \notin C_0,$

(b) $\dfrac{a_1 - 1}{a_0 - 1} \notin C_1,$

(c) $\dfrac{a_1 - 1}{a_1(a_0 - 1)} \notin C_1,$

(d) $\dfrac{(a_1 - 1)a_0}{a_1 - 1} \notin C_1,$

(e) $\dfrac{(a_1 - 1)a_0}{(a_0 - 1)a_1} \notin C_1.$

PROOF. To prove that $S(a_0, a_1)$ is a starter in $GF(q)^+$ it must be shown that every non-zero element is contained in exactly one pair in $S(a_0, a_1)$, and that every non-zero element is a difference of one of the pairs in $S(a_0, a_1)$.

Using the conditions of the lemma it can be checked that $(1/(a_0 - 1))C_0$, $(a_0/(a_0 - 1))C_0$, $(1/(a_1 - 1))C_1$, $(a_1/(a_1 - 1))C_1$ are all different cosets. Thus, every element in G is in exactly one pair in $S(a_0, a_1)$. The differences occurring in a pair of the form $\{x, a_0, x\}$ are $\pm a_0 x - x = \pm(a_0 - 1)x$ and occur in the cosets $\neq (a_0 - 1) \cdot (1/(a_0 - 1))C_0 = C_0 \cup C_2$. Those differences obtained from the other type of pairs, $\{y, a_1, y\}$ with $y \in C_1^{a_1}$, can similarly be shown to be the elements of the cosets $C_1 \cup C_3$. Thus, every element in G is a difference for exactly one pair in $S(a_0, a_1)$.

The proof of necessity is similar.

If $a_0 = a_1 = a$, then in order for $S(a, a)$ to be a starter, the conditions of the above lemma imply that $a \in C_2$. Thus, $S(a, a)$ is one of the starters given by Theorem 1.2, in particular, $S(a, a) = S_a$.

We now give conditions for orthogonality.

LEMMA 3.2. *Let $S(a_0, a_1)$ and $S(b_0, b_1)$ be two quotient starters. Then $S(a_0, a_1)$ and $S(b_0, b_1)$ are orthogonal if and only if*

$$\frac{b_0 - a_0}{b_1 - a_1} \cdot \frac{a_1 - 1}{a_0 - 1} \cdot \frac{b_1 - 1}{b_0 - 1} \notin C_1, \qquad a_0 \neq b_0 \quad and \quad a_1 \neq b_1.$$

PROOF. Assume $S(a_0, a_1)$ and $S(b_0, b_1)$ are orthogonal two quotient starters. Then there exist pairs $\{x, a_0 x\}$ and $\{y, a_1 y\} \in S(a_0, a_1)$ such that $a_0 x - x = 1$ and $a_1 y - y = g_1$ for some given $g_1 \in C_1$. This follows since $a_0 x - x = 1$ implies $x = 1(a_0 - 1)$ and $1/(a_0 - 1) \in C_0^{a_0}$. Similarly $y = g_1/(a_1 - 1) \in C_1^{a_1}$. Also, there exist pairs $\{z, b_0 z\}$ and $\{w, b_1 w\} \in S(b_0, b_1)$ with $b_0 z - z = 1$ and $b_1 w - w = g_1$. This implies $z = 1/(b_0 - 1) \in C_0^{b_0}$ and $w = g_1/(b_1 - 1) \in C_1^{g_1}$.

Now, since $S(a_0, a_1)$ and $S(b_0, b_1)$ are orthogonal we must have that $x - z \neq y - w$. Therefore $1/(a_0 - 1) - 1/(b_0 - 1) \neq g_1/(a_1 - 1) - g_1/(b_1 - 1)$. So $(b_0 - a_0)/(a_0 - 1)(b_0 - 1) \neq g_1(b_1 - a_1)/(a_1 - 1)(b_1 - 1)$ and thus $((b_0 - a_0)/(b_1 - a_1)) \cdot ((a_1 - 1)/(a_0 - 1)) \cdot ((b_1 - 1)/(b_0 - 1)) \neq g_1$ for any $g_1 \in C_1$. Thus $((b_0 - a_0)/(b_1 - a_1)) \cdot ((a_1 - 1)/(a_0 - 1)) \cdot ((b_1 - 1)/(b_0 - 1)) \notin C_1$. Also it is clear that if $a_0 = b_0$ or $a_1 = b_1$, then the two starters would have a pair in common contradicting the assumption of orthogonality. Thus the conclusion.

Now assume $S(a_0, a_1)$ and $S(b_0, b_1)$ are not orthogonal. Then there are two distinct pairs $\{x, a_i x\}$, $\{y, a_j y\} \in S(a_0, a_1)$ and two distinct pairs $\{z, b_i z\}$,

$\{w, b_j w\} \in S(b_0, b_1)$, with $x(a_i - 1) = z(b_i - 1)$, $y(a_j - 1) = w(b_j - 1)$ and $x - z = y - w$. If $a_i = a_j$ or $b_i = b_j$, then both $a_i = a_j$ and $b_i = b_j$. This follows by assuming (without loss of generality) that $a_i = a_j = a_0$, with $b_i = b_0$ and $b_j = b_1$. Then $y(a_0 - 1) \in C_0$ while $w(b_1 - 1) \in C_1$ but $y(a_0 - 1) = w(b_1 - 1)$, a contradiction. Thus assume $a_i = a_j$ and $b_i = b_j$. Then we have that $(x - y)(a_i - 1) = (z - w)(b_i - 1)$. Since $x \neq y$ and $z \neq w$, then $a_i - 1 = b_i - 1$ and so $a_i = b_i$, again a contradiction.

If $a_i \neq a_j$, then without loss of generality assume $a_i = a_0$ and $a_j = a_1$, and so $b_i = b_0$ and $b_j = b_1$. Now let $x = (1/(a_0 - 1)) \cdot x_0$ where $x_0 \in C_0$ and $w = (1/(b_1 - 1))w_1$ where $w_1 \in C_1$. Then $y = ((b_1 - 1)/(a_1 - 1))(1/b_1 - 1)w_1 = w_1/(a_1 - 1)$ and $z = ((a_0 - 1)/(b_0 - 1)) \cdot (1/(a_0 - 1))x_0 = x_0/(b_0 - 1)$. So $x - y = z - w$ implies

$$\frac{x_0}{a_0 - 1} - \frac{w_1}{a_1 - 1} = \frac{x_0}{b_0 - 1} - \frac{w_1}{b_1 - 1},$$

$$x_0\left(\frac{1}{a_0 - 1} - \frac{1}{b_0 - 1}\right) = w_1\left(\frac{1}{a_1 - 1} - \frac{1}{b_1 - 1}\right),$$

$$x_0\left(\frac{b_0 - a_0}{(a_0 - 1)(b_0 - 1)}\right) = w_1\left(\frac{b_1 - a_1}{(a_1 - 1)(b_1 - 1)}\right).$$

Thus

$$\frac{b_0 - a_0}{b_1 - a_1} \cdot \frac{a_1 - 1}{a_0 - 1} \cdot \frac{b_1 - 1}{a_1 - 1} = \frac{w_1}{x_0} \in C_1.$$

So we have that if $S(a_0, a_1)$ and $s(b_0, b_1)$ are not orthogonal, then $a_0 = b_0$ or $a_1 = b_1$ or $((b_0 - a_0)/(b_1 - a_1)) \cdot ((a_1 - 1)/(a_0 - 1)) \cdot ((b_1 - 1)/(b_0 - 1)) \in C_1$. So if $a_0 \neq b_0$ and $a_1 \neq b_1$ and $((b_0 - a_0)/(b_1 - a_1)) \cdot ((a_1 - 1)/(a_0 - 1)) \cdot ((b_1 - 1)/(b_0 - 1)) \notin C_1$, then $S(a_0, a_1)$ and $S(b_0, b_1)$ are orthogonal.

Again we note that if $a_0 = a_1 = a \in C_2$ and $b_0 = b_1 = b \in C_2$ with $a \neq b$, then the starters $S_a = S(a_0, a_1)$ and $S_b = S(b_0, b_1)$ are orthogonal. This is now easy to show, since in this case

$$\frac{b_0 - a_0}{b_1 - a_1} \cdot \frac{a_1 - 1}{a_0 - 1} \cdot \frac{b_1 - 1}{b_0 - 1} = \frac{b - a}{b - a} \cdot \frac{a - 1}{a - 1} \cdot \frac{b - 1}{b - 1} = 1 \notin C_1.$$

Often when considering a starter $s = \{\{s_i, t_i\}\}$, we wish to investigate the negative starter $-S = \{\{-s_i, -t_j\}\}$. In the case of two quotient starters $S(a_0, a_1)$ this negative starter has a nice form.

LEMMA 3.3. *If $S(a_0, a_1)$ is a two quotient starter, then $-S(a_0, a_1) = S(1/a_0, 1/a_1)$.*

PROOF. $S(1/a_0, 1/a_1) = \{\{z, (1/a_1)z\}, \{w, (1/a_1)w\} \mid z \in C_0^{1/a_0}, \ w \in C_1^{1/a_1}\}$.
Now $z \in C_0^{1/a_0} = (1/(1/a_0 - 1))C_0 = (a_0/(1 - a_0))C_0$. Thus $-z \in (a_0/(a_0 - 1))C_0$. Let $x = -(1/a_0)z$, then $x \in (1/(a_0 - 1))C_0 = C_0^{a_0}$. Similarly, it can be shown that if $y = -(1/a_1)w$, then $y \in C_1^{a_1}$. We now have that $S(1/a_0, 1/a_1) = \{\{-a_0 x, -x\}, \{-a_1 y, -y\} \mid x \in C_0^{a_0}, \ y \in C_1^{a_1}\}$. This is just $-S(a_0, a_1)$.

As an application of the two previous lemmata we give the following theorem.

THEOREM 3.4. *Let* $S(a_0, a_1) = \{\{s_i, t_i\}\}$ *be a quotient starter; then the following are equivalent.*
(a) $S(a_0, a_1)$ *is orthogonal to* $-S(a_0, a_1)$.
(b) $S(a_0, a_1)$ *is a strong starter (that is, $s_i + t_i \neq s_j + t_j$ if $i \neq j$),*
(c)

$$\frac{a_1 - 1}{a_0 - 1} \cdot \frac{1 + a_0}{1 + a_1} \notin C_1.$$

PROOF. (a $\Leftrightarrow$ b). See [10].
(a $\Leftrightarrow$ c). Use Lemma 3.3 to write $-S(a_0, a_1) = S(1/a_0, 1/a_1)$. Then use Lemma 3.2. The following are equivalent.

$$S(a_0, a_1) \text{ is orthogonal to } -S(a_0, a_1)$$

$$\Leftrightarrow S(a_0, a_1) \text{ is orthogonal to } S\left(\frac{1}{a_0}, \frac{1}{a_1}\right)$$

$$\Leftrightarrow \frac{1/a_0 - a_0}{1/a_1 - a_1} \cdot \frac{a_1 - 1}{a_0 - 1} \cdot \frac{1/a_1 - 1}{1/a_0 - 1} \notin C_1$$

$$\Leftrightarrow \frac{(1 + a_0)(a_1 - 1)}{(1 + a_1)(a_0 - 1)} \notin C_1.$$

The original motivation for investigating two quotient starters was to find more starters orthogonal to the set of starters $S_a = \{\{x, ax\} \mid x \in H_a\}$ for $a \in C_2$. With this in mind we assume $a_0 \notin C_2$ and $a_1 \notin C_2$. Since if either $a_0 \in C_2$ or $a_1 \in C_2$, then $S(a_0, a_1)$ would have some pairs in common with S_b where $b = a_0$ or a_1. The following lemma gives conditions for a two quotient starter to be orthogonal to the original set of starters S_a for $a \in C_2$.

LEMMA 3.5. *Suppose* $\{a_0, a_1\} \subseteq G$ *such that* $S(a_0, a_1)$ *is a starter and*
(a) $a_0 \in C_1, a_1 \in C_3$ *and* $((a_0 - b)/(a_1 - b)) \notin C_3$ *for all* $b \in C_2$, *or*
(b) $a_0 \in C_1, a_1 \in C_1$ *and* $((a_0 - b)/(a_1 - b)) \notin C_2$ *for all* $b \in C_2$, *or*
(c) $a_0 \in C_3, a_1 \in C_1$ *and* $((a_0 - b)/(a_1 - b)) \notin C_1$ *for all* $b \in C_2$, *or*

(d) $a_0 \in C_3$, $a_1 \in C_3$ and $((a_0 - b)/(a_1 - b)) \notin C_2$ for all $b \in C_2$, then $S(a_0, a_1)$ is orthogonal to S_b for all $b \in C_2$, and thus $-S(a_0, a_1)$ is orthogonal to S_b for all $b \in C_2$. Also, $S(a_0, a_1)$ is orthogonal to $-S(a_0, a_1)$.

PROOF. (a) Using Lemma 3.1 it is seen that since $S(a_0, a_1)$ is a starter then $((a - 1)/(a_0 - 1)) \in C_2$. By Lemma 3.2 $S(a_0, a_0)$ is orthogonal to S_b for all $b \in C_2$ if $x = ((a_0 - b)(a_1 - b)) \cdot ((a_1 - 1)/(a_0 - 1)) \cdot ((b - 1)/(b - 1)) \notin C_1$. But by assumption $((a_0 - b)/(a_1 - b)) \notin C_3$ for all $b \in C_2$. Thus $x \notin C_1$. The other cases are similar.

If $S(a_0, a_1)$ is orthogonal to S_b for all $b \in C_2$, then $-S(a_0, a_1)$ is orthogonal to $-S_b$ for all $b \in C_2$. But $-S_b = S_{1/b}$ and if $b \in C_2$, then $1/b \in C_2$. Thus $-S(a_0, a_1)$ is also orthogonal to S_b for all $b \in C_2$.

Noting that $-1 \in C_2$, the assumption that $((a_0 - b)/(a_1 - b)) \notin C_3$ for all $b \in C_2$ implies $((a_0 + 1)/(a_1 + 1)) \notin C_3$. For each of the cases it is easily shown that $((a_0 + 1)/(a_1 + 1)) \cdot ((a_1 - 1)/(a_0 - 1)) \notin C_1$. Thus by Theorem 3.4, $S(a_0, a_1)$ is orthogonal to $-S(a_0, a_1)$. This completes the proof.

The following theorem improves upon the result of Theorem 1.2.

THEOREM 3.6. (a) *There are 5 pairwise orthogonal starters in* $\mathbf{Z}_{13}$, *thus* $\nu(13) \geqslant 5$.
(b) *There are 15 pairwise orthogonal starters in* $\mathbf{Z}_{37}$, *thus* $\nu(37) \geqslant 15$.

PROOF. (a) Let $q = 13$ with 3 a generator for $GF(13)^*$. Consider the two quotient starter $S(2, 11)$. The conditions of Lemma 3.1 are easily checked. We check the conditions of Theorem 3.5. In this case $C_2 = \{4, 12, 10\}$. First of all $a_0 = 2 \in C_1$ while $a_1 = 11 \in C_3$, thus we are in case (a) in the above lemma. For $b = 4$ we have $\frac{2-4}{11-4} \equiv \frac{11}{7} \equiv 9 \in C_0$. If $b = 12$, then $\frac{2-12}{11-12} \equiv \frac{3}{12} \equiv 10 \in C_2$. Finally, if $b = 10$, then $\frac{2-10}{11-10} \equiv \frac{5}{1} \equiv 5 \in C_1$. Thus by Theorem 3.5 $S(2, 11)$ and $-S(2, 11) = S(7, 6)$ are orthogonal to S_4, S_{12}, and S_{10} and to each other. Thus since S_4, S_{12} and S_{10} are pairwise orthogonal by Theorem 1.2, the results follows.

(b) Let $q = 37$ with 2 a generator for $GF(37)^*$. Using Lemmata 3.1, 3.2 and Theorem 3.5 the following starters can be shown to be pairwise orthogonal and orthogonal to all of the starters S_b for $b \in C_2$. These starters are $\pm S(35, 2)$, $\pm S(15, 6)$ and $\pm S(23, 14)$. Thus we have $6 + 9 = 15$ pairwise orthogonal starters in $GF(37)^+$. So $\nu(37) \geqslant 15$.

We note that the same 5 starters were found by Gross [5]. His construction also made use of the multiplicative cosets of order 3 in $GF(13)^*$.

The following lemma proves that if $S(a_0, a_1)$ and $S(b_0, b_2)$ are two quotient starters with $a_1/a_0 = b_1/b_0$, then they are orthogonal.

LEMMA 3.7. *Suppose* $\{a_0, a_1\} \subseteq G$ *such that* $S(a_0, a_1)$ *is a two quotient starter. Also suppose there is a set* $T = \{1 = t_0, t_1, t_2, \ldots, t_v\} \subseteq C_0 \cup C_0$ *and that the following properties hold*:

(a) $a_0 \in C_1$, $a_1 \in C_3$,

(b) $t_i \neq t_j$ *if* $i \neq j$,

(c) $\dfrac{t_i a_1 - 1}{t_i a_0 - 1} \in C_2$ *for all* $t_i \in T \cap C_0$,

(d) $\dfrac{t_i a_1 - 1}{t_i a_0 - 1} \in C_0$ *for all* $t_i \in T \cap C_2$,

(e) $\dfrac{t_i t_j a_0^2 - 1}{t_i t_j a_1^2 - 1} \notin C_1$ *if* $\{t_i, t_j\} \subseteq C_0$ *or* $\{t_i, t_j\} \subseteq C_2$,

(f) $\dfrac{t_i t_j a_0^2 - 1}{t_i t_j a_1^2 - 1} \notin C_3$ *if* $t_i \in C_0$ *and* $t_j \in C_2$.

Then $S(t_i a_0, t_i a_1)$ *is a starter for each* $t_i \in T$. *Also* $S(t_i a_0, t_i a_1)$ *is orthogonal to* $\pm S(t_j a_0, t_j a_1)$ *for* $t_i \neq t_j$.

PROOF. We must first show that $S(t_i a_0, t_i a_1)$ is a starter. Since $a_0 \in C_1$ and $a_1 \in C_3$, by the proof of Lemma 3.5 we have $(a_1 - 1)/(a_0 - 1) \in C_2$. Now, in order to show that $S(t_i a_0, t_i a_1)$ is a starter, we show that the conditions of Lemma 3.1 are satisfied. Consider the case when $t_i \in C_0$. By assumption $(t_i a_1 - 1)/(t_i a_0 - 1) \in C_2$. So $(t_i a_1 - 1)/(t_i a_1)(t_i a_0 - 1) \in C_3$, $(t_i a_1 - 1)t_i a_0/(t_i a_1 - 1) \in C_3$ and $((t_i a_1 - 1)/(t_i a_0 - 1)) \cdot (t_i a_0/t_i a_1) \in C_0$. Thus by Lemma 3.1, $S(t_i a_0, t_i a_1)$ is a starter for all $t_i \in C_0$. The case $t_i \in C_2$ is similar.

To show that if $i \neq j$, then $S(t_i a_0, t_i a_1)$ and $S(t_j a_0, t_j a_1)$ are orthogonal we use Lemma 3.2. Consider $x = ((t_j a_0 - t_i a_0)/(t_j a_1 - t_i a_1)) \cdot ((t_i a_1 - 1)/(t_i a_0 - 1)) \cdot ((t_j a_1 - 1)/(t_j a_0 - 1))$. The starters are orthogonal if $x \notin C_1$. Simplifying yields $x = (a_0/a_1) \cdot ((t_i a_1 - 1)/(t_i a_0 - 1)) \cdot ((t_j a_1 - 1)/(t_j a_0 - 1))$. Now $a_0/a_1 \in C_2$, $(t_i a_1 - 1)/(t_i a_0 - 1) \in C_0 \cup C_2$ and $(t_j a_1 - 1)/(t_{j0} - 1) \in C_0 \cup C_2$, thus $x \notin C_1$, and therefore the starters are orthogonal.

Finally, it need only be shown that $S(t_i a_0, t_i a_1)$ is orthogonal to $-S(t_j a_0, t_j a_1)$. By Lemma 3.2, the two starters are orthogonal if

$$x = \frac{1/t_j a_0 - t_i a_0}{1/t_j a_0 - t_i a_1} \cdot \frac{t_i a_1 - 1}{t_i a_0 - 1} \cdot \frac{1/t_j a_1 - 1}{1/t_j a_0 - 1} \notin C_1.$$

Reducing gives

$$x = \frac{1 - t_i t_j a_0^2}{1 - t_i t_j a_1^2} \cdot \frac{t_j a_1}{t_j a_0} \cdot \frac{t_i a_1 - 1}{t_i a_0 - 1} \cdot \frac{1 - t_j a_1}{1 - t_j a_0} \cdot \frac{t_j a_0}{t_j a_1}$$

$$= \frac{t_i t_j a_0^2 - 1}{t_i t_j a_1^2 - 1} \cdot \frac{t_i a_1 - 1}{t_i a_0 - 1} \cdot \frac{t_j a_1 - 1}{t_j a_0 - 1}.$$

If t_i and t_j are both in C_0 or both in C_2, then conditions (c), (d), and (e) above imply $x \notin C_1$. If t_i and t_j are in different cosets, then conditions (c), (d), and (f) imply $x \notin C_1$. Thus the result.

Lemma 3.5 can be combined with Lemma 3.7 to obtain the following theorem which yields large sets of pairwise orthogonal starters.

THEOREM 3.8. *Suppose* $\{a_0, a_1\} \subseteq G$ *such that* $S(a_0, a_1)$ *is a two quotient starter. Also suppose there is a set* $T = \{1 = t_0, t_1, t_2, \ldots, t_v\} \subseteq C_0 \cup C_2$ *and that the following properties hold*:

(a) $a \in C_1, \qquad a_1 \in C_3,$

(b) $\dfrac{a_0 - b}{a_1 - b} \notin C_3 \quad$ *for all* $b \in C_2,$

(c) $t_i \neq t_j \quad$ *if* $i \neq j,$

(d) $\dfrac{t_i a_1 - 1}{t_i a_0 - 1} \in C_2 \quad$ *for all* $t_i \in T \cap C_0,$

(e) $\dfrac{t_i a_1 - 1}{t_i a_0 - 1} \in C_0 \quad$ *for all* $t_i \in T \cap C_2,$

(f) $\dfrac{t_i t_j a_0^2 - 1}{t_i t_j a_1^2 - 1} \notin C_1 \quad$ *if* $\{t_i, t_j\} \subseteq C_0$ *or* $\{t_i, t_j\} \subseteq C_2,$

(g) $\dfrac{t_i t_j a_0^2 - 1}{t_i t_j a_1^2 - 1} \notin C_3 \quad$ *if* $t_i \in C_0$ *and* $t_j \in C_2.$

Then $\pm S(t_i a_0, t_i a_1)$ *and* S_b *are pairwise orthogonal starters for all* $t_i \in T$ *and* $b \in C_2$.

PROOF. This is immediate from Lemmata 3.5a and 3.7 and Theorem 3.1.

We now apply the above theorem to $q = 29, 61,$ and 101.

THEOREM 3.9. (a) *There exist* 13 *pairwise orthogonal starters of order* 29, *and thus* $\nu(29) \geqslant 13$.

(b) *There exist* 21 *pairwise orthogonal starters of order* 61, *and thus* $\nu(61) \geqslant 21$.

(c) *There exist* 31 *pairwise orthogonal starters of order* 101, *and thus* $\nu(101) \geqslant 31$.

PROOF. (a) Let $a_0 = 3 \in C_1$, $a_1 = 27 \in C_3$, $t_0 = 1$, $t_1 = 28$ and $t_2 = 23$. Then the conditions in Theorem 3.8 can be shown to be satisfied.

(b) Let $a_0 = 32$, $a_1 = 31$, $t_0 = 1$, $t_1 = 22$ and $t_2 = 56$. Again the conditions in Theorem 3.8 are satisfied.

(c) Let $a_0 = 67$, $a_1 = 90$, $t_0 = 1$, $t_1 = 5$, and $t_2 = 58$. Then once again the conditions in Theorem 3.8 are satisfied.

In all previous cases, we have searched for large sets of pairwise orthogonal two quotient starters which are also orthogonal to the original one quotient starters S_a given in Section 2. We now give a technique for finding large sets of exclusively two quotient starters.

If $S = \{\{s_i, t_i\}\}$ is a starter in $GF(q)^+$, then certainly for any $\alpha \in GF(q)^*$, $\alpha \cdot S = \{\{\alpha s_i, \alpha t_i\}\}$ is also a starter in $GF(q)^+$. Call T a *conjugate* of S if $T = \alpha S$ for some $\alpha \in GF(q)^*$. The following lemma holds for two quotient starters. The proof is straightforward and is omitted.

LEMMA 3.10. *Let* $S(a_0, a_1)$ *be a two quotient starter in* $GF(q)^+$, $q = 4t + 1$. *Then*

$$\alpha S(a_0, a_1) = S(a_0, a_1) \quad \text{if } \alpha \in C_0,$$

$$= S\left(\frac{1}{a_1}, a_0\right) \quad \text{if } \alpha \in C_1,$$

$$= S\left(\frac{1}{a_0}, \frac{1}{a_1}\right) \quad \text{if } \alpha \in C_2,$$

$$= S\left(a_1, \frac{1}{a_0}\right) \quad \text{if } \alpha \in C_3.$$

PROPOSITION 3.11. *If* $S(a_0, a_1)$ *is a two quotient starter and if* $S(a_0, a_1)$ *is orthogonal to* $S(a_1, 1/a_0)$, *then it is orthogonal to* $S(1/a_1, a_0)$.

PROOF. Using Lemma 3.2, if $S(a_0, a_1)$ is orthogonal to $S(a, 1/a_0)$, then $((a_0 - a_1)/(a_1 - 1/a_0)) \cdot ((a_1 - 1)/(a_0 - 1)) \cdot ((1/a_0 - 1)/(a_1 - 1)) \notin C_1$. Thus by simplification $(a_0 - a_1)/(1 - a_0 a_1) \notin C_1$. Now again using Lemma 3.2, it is seen that $S(a_0, a_1)$ is orthogonal to $S(1/a_1, a_0)$ if $((a_0 - 1/a_1)/(a_1 - a_0)) \cdot$

$((a_1 - 1)/(a_0 - 1)) \cdot ((a_0 - 1)/(1/a_1 - 1)) \notin C_1$. This simplifies to $(a_0 - a_0)/(1 - a_0a_1) \notin C_1$. Hence the result.

Define a two quotient starter $S(a_0, a_1)$ to be *super strong* if it is not only strong (orthogonal to $-S(a_0, a_1)$) but also orthogonal to its conjugate $\alpha S(a_0, a_1)$ for $\alpha \in C_1 \cup C_3$. That is, a two quotient starter $S(a_0, a_1)$ is super strong if it is orthogonal to $\alpha S(a_0, a_1)$ for $\alpha \notin C_0$. It is easy to see that if $S(a_0, a_1)$ is orthogonal to all $\alpha S(a_0, a_1)$ for $\alpha \notin C$, then $\alpha S(a_0, a_1)$ is orthogonal to all $\beta S(a_0, a_1)$ for all β, $\beta/\alpha \notin C_0$. Thus, in view of Proposition 3.11, if it is shown that $S(a_0, a_1)$ is strong and orthogonal to $S(a_1, 1/a_0) = \alpha S(a_0, a_1)$, $\alpha \in C_1$, then the conjugate starters to $S(a_0, a_1)$ form a set of 4 pairwise orthogonal starters. We also have the following proposition which is trivial to prove.

PROPOSITION 3.12. *Suppose $S(a_0, a_1)$ and $S(b_0, b_1)$ are super strong two quotient starters. If $S(a_0, a_1)$ is orthogonal to $\beta S(b_0, b_1)$ for all $\beta \in GF(q)^*$, then $\alpha S(a_0, a_1)$ is orthogonal to $\beta S(b_0, b_1)$ for all α, $\beta \in GF(q)^*$. Thus there is a set of 9 pairwise orthogonal starters in $GF(q)^+$. (The 8 two quotient starters and the patterned starter $P = (\{x, -x\} \mid x \neq 0))$.*

We use this proposition to get

THEOREM 3.13. *There are 17 pairwise orthogonal starters in $GF(53)^+$, thus $\nu(53) \geqslant 17$.*

PROOF. We give 4 super strong starters with the property that each is pairwise orthogonal to all of the conjugates of the others. Thus by Proposition 3.12, there are 17 pairwise orthogonal starters. The starters are $S(2, 18)$, $S(22, 12)$, $S(51, 5)$ and $S(34, 19)$.

For the more general case of prime powers $q = 2^k t + 1$ define

$$S = S(a_0, a_1, \ldots, a_{2^{k-1}-1}) = \left\{ \{x_i, a_i x_i\} \mid x_i \in C_i^{a_i}, 0 \leqslant i \leqslant 2^{k-1} - 1 \right\}$$

where C_i is the ith coset of C_0 (the subgroup of order t), and $C_i^{a_i} = (1/(a_i - 1))C_i$. Then under certain conditions analogous to those in Lemma 3.1, S will be a starter (a 2^{k-1} quotient starter). Four quotient starter are used in the following theorem to construct pairwise orthogonal starters.

THEOREM 3.14. (a) *There are 7 pairwise orthogonal starters of order 25, thus $\nu(25) \geqslant 7$.*

(b) *There are 9 pairwise orthogonal starters of order 41, thus $\nu(41) \geqslant 9$.*

PROOF. (a) In $GF(5)$ let w be a root of the irreducible polynomial $x^2 - 4x - 3$. Then $GF(25) = \{aw + b \mid a, b \in GF(5)\}$. Denote the element $aw + b$ by ab. The 7 starters are:

$$S_{32} = S(32, 32, 32, 32) = \{\{23, 24\}, \{01, 32\}, \{31, 04\}, \{11, 21\}, \{10, 44\},$$
$$\{34, 40\}, \{03, 41\}, \{43, 02\}, \{14, 12\}, \{30, 22\},$$
$$\{42, 20\}, \{33, 13\}\};$$

$$S(11, 20, 11, 40) = \{\{22, 23\}, \{20, 01\}, \{13, 31\}, \{44, 04\}, \{40, 24\},$$
$$\{21, 32\}, \{10, 03\}, \{34, 43\}, \{11, 14\}, \{41, 33\},$$
$$\{02, 30\}, \{12, 42\}\};$$

$$S(21, 21, 21, 13) = \{\{11, 12\}, \{10, 41,\} \{34, 02\}, \{03, 13\}, \{43, 22\},$$
$$\{14, 20\}, \{30, 23\}, \{42, 01\}, \{33, 31\}, \{40, 32\},$$
$$\{21, 04\}, \{44, 24\}\};$$

$$P = S(04, 04, 04, 04) = \{\{x, x\} \mid x \in GF(25)^*\};$$

$$-S_{32}; -S(11, 20, 11, 40) \quad \text{and} \quad -S(21, 21, 21, 13).$$

It can be checked that the above starters are pairwise orthogonal. In [5] Gross also finds 7 pairwise orthogonal starters of order 25; however, they are not the same ones given here.

(b) For $41 = 8 \cdot 5 + 1$, it can be checked that the following 9 starters are pairwise orthogonal: $\pm S_{25}, \pm S_4, P = S_{40}, \pm S(20, 35, 2, 35)$, and $\pm(22, 27, 27, 19)$.

4. Further results

For all orders $n \leqslant 133$ not a power of a prime, the best lower bound for $\nu(n)$ is $\nu(n) \geqslant 3$. In this section we have employed computer techniques to improve upon this bound for the orders 15, 17, 21, 33, 35 and 39. By use of a simple backtracking algorithm we have

THEOREM 4.1. *There are 4 pairwise orthogonal starters of order 15, and thus* $\nu(15) > 4$.

PROOF. We give the orthogonal starters in $\mathbf{Z}_{15}$:

$$S_1 = \{\{13, 14\}, \{10, 12\}, \{4, 7\}, \{5, 9\}, \{1, 6\}, \{2, 8\}, \{11, 3\}\},$$
$$S_2 = \{\{11, 12\}, \{6, 8\}, \{1, 4\}, \{14, 3\}, \{5, 10\}, \{7, 13\}, \{2, 9\}\},$$
$$S_3 = \{\{10, 11\}, \{14, 1\}, \{2, 5\}, \{4, 8\}, \{7, 12\}, \{3, 9\}, \{6, 13\}\},$$
$$S_4 = \{\{1, 2\}, \{7, 9\}, \{11, 14\}, \{6, 10\}, \{3, 8\}, \{13, 4\}, \{5, 12\}\}.$$

By means of a slight modification of the algorithm for finding strong starters described in [3], we have found 5 pairwise orthogonal starters of several orders.

THEOREM 4.2. *There are 5 pairwise orthogonal starters of orders* $n = 17, 21, 33, 35$ *and 39, and thus for each of these* n, $\nu(n) \geqslant 5$.

PROOF. For each of these orders n we have found two strong starters A, B which have the property that A is orthogonal to B and $-B$. It then follows that $-A$ is orthogonal to both B and $-B$ and thus the starters A, $-A$, B, $-B$ and $P = \{\{x, -x\} \mid x \in \mathbf{Z}_n\}$ form a set of 5 pairwise orthogonal starters in $\mathbf{Z}_n$. For each n we give the starters A and B.

$$n = 17$$
$$A = \{\{2,3\}, \{11,13\}, \{5,8\}, \{14,1\}, \{7,12\}, \{4,10\}, \{9,16\}, \{15,6\}\},$$
$$B = \{\{1,2\}, \{14,16\}, \{10,13\}, \{5,9\}, \{3,8\}, \{6,12\}, \{4,11\}, \{7,15\}\}.$$

$$n = 21$$
$$A = \{\{19,20\}, \{12,14\}, \{13,16\}, \{4,8\}, \{1,6\}, \{5,11\}, \{3,10\}, \{15,2\},$$
$$\{9,18\}, \{7,17\}\},$$
$$B = \{\{3,4\}, \{10,12\}, \{16,19\}, \{14,18\}, \{2,7\}, \{9,15\}, \{20,6\}, \{5,13\},$$
$$\{8,17\}, \{1,11\}\}.$$

$$n = 33$$
$$A = \{\{20,21\}, \{6,8\}, \{28,31\}, \{12,16\}, \{25,30\}, \{7,13\}, \{29,3\}, \{15,23\},$$
$$\{2,11\}, \{17,27\}, \{32,10\}, \{14,26\}, \{9,22\}, \{24,5\}, \{4,19\}, \{18,1\}\},$$
$$B = \{\{29,30\}, \{3,5\}, \{21,24\}, \{6,10\}, \{7,12\}, \{14,20\}, \{18,25\}, \{26,1\},$$
$$\{23,32\}, \{9,19\}, \{2,13\}, \{15,27\}, \{4,17\}, \{8,22\}, \{16,31\}, \{28,11\}\}.$$

$$n = 35$$
$$A = \{\{10,11\}, \{16,18\} \{26,29\}, \{32,1\}, \{17,22\}, \{33,4\}, \{5,12\}, \{20,28\},$$
$$\{25,34\}, \{9,19\}, \{30,6\}, \{2,14\}, \{8,21\}, \{13,27\}, \{23,3\}, \{15,31\},$$
$$\{7,24\}\},$$
$$B = \{\{30,31\}, \{19,21\}, \{23,26\}, \{12,16\}, \{34,4\}, \{3,9\}, \{11,18\}, \{32,5\},$$
$$\{6,15\}, \{17,27\}, \{14,25\}, \{33,10\}, \{29,7\}, \{22,1\}, \{13,28\}, \{8,24\},$$
$$\{20,2\}\}.$$

$$n = 39$$

$A = \{\{17,18\},\{27,29\},\{23,26\},\{36,1\},\{28,33\},\{16,22\},\{6,13\},\{11,19\},$
$\quad \{37,7\},\{5,15\},\{31,3\},\{35,8\},\{38,12\},\{20,34\},\{9,24\},\{25,2\},$
$\quad \{4,21\},\{14,32\},\{30,10\}\},$

$B = \{\{37,38\},\{4,6\},\{16,19\},\{31,35\},\{29,34\},\{3,9\},\{23,30\},\{5,13\},$
$\quad \{1,10\},\{15,25\},\{17,28\},\{20,32\},\{14,27\},\{12,26\},\{7,22\},\{8,24\},$
$\quad \{33,11\},\{18,36\},\{2,21\}\}.$

A few comments are in order concerning the search for orthogonal starters. First of all, the above set of starters in Z_{15} constitute a maximal set. Secondly, an exhaustive search for orthogonal starters of orders 11 and 13 was possible with the result that there are *not* 6 pairwise orthogonal starters of orders 11 and 13. Furthermore, the only set of 5 pairwise orthogonal starters of order 11 is the set given in Section 2. Also, there are only two sets of 5 pairwise orthogonal starters of order 13 and both can be obtained by the method of two-quotient starters. Finally, we have found that the maximal set of pairwise orthogonal starters of orders 15, one of which is P, the patterned starter, is 3. Thus the method used to find 5 orthogonal starters in Theorem 4.2 can not be used for $n = 15$.

5. Conclusion

We have found improved lower bounds for $\nu(n)$ for many small values of n ($n = 13, 15, 17, 21, 25, 29, 33, 35, 37, 39, 41, 53, 61,$ and 101). The bounds for prime-powers were determined by difference methods in cyclotomic fields while the other values were determined by computer techniques.

We have not investigated upper bounds for $\nu(n)$. It has been conjectured [6] that $\nu(n) \leqslant (n-1)/2$ for all $n \geqslant 7$. This conjectured upper bound is attained when n is a prime-power, $n \equiv 3 \pmod{4}$. In no other instance has this bound been achieved. Most of the lower bounds presented in this paper vary a good deal from the conjectured upper bound. However, there are several cases where this difference is only 1; we have $\nu(9) \geqslant 3$ [2], $\nu(13) \geqslant 5$ and $\nu(29) \geqslant 13$.

Possible further research into the behavior of $\nu(n)$ could be directed at a proof that $\nu(n) \leqslant (n-1)/2$. Also, it would be of interest to show that if $p = 2^k t + 1$ is a prime-power with t odd, then $\nu(p) > t$. This result is suggested by the small examples presented in this paper.

References

[1] J. H. Dinitz, 'New lower bounds for the number of pairwise orthogonal symmetric Latin squares,' *Proc. 10th S-E Conf. on Combinatorics, Graph Theory and Computing*, Boca Raton, Florida, (1979), 393–398.

[2] J. H. Dinitz, 'Pairwise orthogonal symmetric Latin squares,' *Congressus Numerantium* **32** (1981), 261–265.

[3] J. H. Dinitz and D. R. Stinson, 'A fast algorithm for finding strong starters,' *SIAM J. Algebraic and Discrete Methods* **2** (1981), 50–56.

[4] J. H. Dinitz and D. R. Stinson, 'The spectrum of Room cubes,' *European J. Combinatorics* **2** (1981), 221–230.

[5] K. B. Gross, 'Some new classes of strong starters,' *Discrete Math.* **12** (1975), 225–243.

[6] K. B. Gross, R. C. Mullin, and W. D. Wallis, 'The number of pairwise orthogonal symmetric Latin squares,' *Utilitas Math.* **4** (1973), 239–251.

[7] J. D. Horton, 'Room designs and one-factorizations,' *Aequationes Math.*, to appear.

[8] R. C. Mullin and E. Nemeth, 'An existence theorem for Room squares,' *Canad. Math. Bull.* **12** (1969), 493–497.

[9] R. C. Mullin and W. D. Wallis, 'The existence of Room squares,' *Aequationes Math.* **13** (1975), 1–7.

[10] W. D. Wallis, A. P. Street and J. S. Wallis, *Combinatorics: Room squares, sum-free sets, Hadamard matrices* (Springer-Verlag, 1972).

Department of Mathematics
University of Vermont
Burlington, Vermont 05405
U.S.A.