New Lower Bounds on the Maximum Number of Mutually Orthogonal Steiner Triple Systems

J. H. Dinitz and P. Dukes

February 25, 2002

Abstract

Two Steiner triple systems (STS) are orthogonal if their sets of triples are disjoint, and two disjoint pairs of points defining intersecting triples in one system fail to do so in the other. We define the quantity $\sigma(n)$ as the size of a maximum collection of pairwise orthogonal STS of order n. Special starters in the finite fields are used to improve the best known lower bounds on $\sigma(n)$ for prime-powers $n \equiv 1 \pmod 6$, $n < 500$. Additionally, hill-climbing and isomorphisms are used together to show $\sigma(n) \geq 3$ or 4 for certain other small n, including some orders $n \equiv 3 \pmod 6$. Asymptotic existence for three mutually orthogonal STS is a consequence.

1 Introduction

A *Steiner triple system* (STS) of order n is a pair $(V, \mathcal{B})$, where V is an n-set of elements and $\mathcal{B}$ is a collection of 3-subsets (triples) of V such that every pair of elements in V is contained in a unique triple of $\mathcal{B}$. The necessary numerical condition $n \equiv 1$ or $3 \pmod 6$ is well-known to be sufficient [13].

Two STS, $(V, \mathcal{B}_1)$ and $(V, \mathcal{B}_2)$, are *orthogonal* if
(i) $\mathcal{B}_1 \cap \mathcal{B}_2 = \emptyset$, and
(ii) for u, v, x, y distinct, $\{u, v, a\}, \{x, y, a\} \in \mathcal{B}_1$ and $\{u, v, w\}, \{x, y, z\} \in \mathcal{B}_2$ implies $w \neq z$.

Every STS defines a *third element function* $\Theta : \binom{V}{2} \to V$ given by $\Theta(\{u, v\}) = w$ if and only if $\{u, v, w\}$ is a triple. Two STS $(V, \mathcal{B}_1)$ and $(V, \mathcal{B}_2)$ with third element functions Θ_1 and Θ_2,

respectively, are orthogonal if and only if for each $c \in V$, the list $(\Theta_2(\{u,v\})|\Theta_1(\{u,v\}) = c)$ consists of distinct elements none of which equal c. This verification is called the *orthogonality certificate*.

It can be checked by hand that there exists a pair of orthogonal STS of order 7 but that there does not exist such a pair for orders 3 or 9. The reader is referred to [1] for a discussion of the history of orthogonal Steiner triple systems. We note here that they were first introduced by O'Shaughnessey [11] in 1968 as a means to finding Room squares. After much work the spectrum problem for orthogonal STS was completely solved [1] in 1994. The paper [7] gives a description of the algorithms used to find many small orders. We build upon these algorithms in this present work. Let $\sigma(n)$ denote the size of a maximum collection of mutually orthogonal Steiner triple systems of order n. We record the result in [1] for later reference.

Theorem 1.1 [1] $\sigma(n) \geq 2$ *for all* $n \equiv 1, 3 \pmod 6$, $n \neq 3, 9$.

Several other results concerning $\sigma(n)$ are known. These are summarized in the following three theorems.

Theorem 1.2 [14] $\sigma(n) \geq 3$ *for* $n = 2^{6k \pm 1} - 1$ *and* $\sigma(127) = 6$.

Theorem 1.3 [8] $\sigma(31) \geq 6$, $\sigma(43) \geq 4$, $\sigma(61) \geq 3$, $\sigma(67) \geq 6$, $\sigma(103) \geq 5$, $\sigma(109) \geq 3$, $\sigma(139) \geq 8$, $\sigma(151) \geq 12$, $\sigma(157) \geq 8$, *and* $\sigma(163) \geq 6$.

The results of this paper will improve upon many of the bounds in Theorem 1.3.

Theorem 1.4 [8] $\lim_{m \to \infty} \sigma(6m+1) = \infty$.

An interesting question is to consider upper bounds on $\sigma(n)$. ¿From the condition of disjoint block sets alone, there can be no more than $\binom{n}{3}/|\mathcal{B}_i| = n - 2$ pairwise orthogonal STS $(V, \mathcal{B}_i)$ of order n. But also the existence of k mutually orthogonal STS of order n implies k mutually orthogonal symmetric Latin squares of order n. Hence $\sigma(n) \leq (n-1)/2$ may be a better conjectured bound. More discussion on this upper bound can be found in [4].

In the next section, we merge the algebraic methods of Dinitz [2] and Gross [8] to improve the best known bounds on $\sigma(n)$ for $n \equiv 1 \pmod 6$ a prime-power less than 500. Later,

hill-climbing is used to handle some small values (in particular, we will show that $\sigma(19) \geq 3$) and we will also exhibit the first known collections of three pairwise orthogonal STS of 3 (mod 6) order. We are quite pleased with these results as it was originally conjectured in [11] that there would never be orthogonal Steiner triple systems for any order congruent to 3 modulo 6.

2 Starters over Finite Fields

2.1 One parameter systems

In what follows, the sum (product) of two sets is defined to be the set of all sums (products) of elements by taking one from each set. Similarly, the sum (product) of an element with a set is the set of all sums (products) of that element with every member of the set. The following construction is essentially that of Gross [8].

Let K be a finite field of order $q = 6t + 1$, t odd (so $q \equiv 7 \pmod{12}$). Let $U \subset Q$ be subgroups of K^* of index 6 and 3, respectively. Choose $a \in K^* \setminus Q$ such that $a(a+1) \in Q$. Now $U\{\{0, a, a+1\}\}$ is a set of triples whose $6t$ total differences exhaust K^*. So, $(K, K + U\{\{0, a, a+1\}\})$ is a Steiner triple system of order q developed under K. This STS will be denoted as S_a.

Example: Let K be the field of order 19 (with generator 2). Then $U = \{1, 7, 11\}$ and $Q = U \cup \{8, 18, 12\}$. Then $a = 3$ satisfies the criterion above. The triples forming the base blocks of S_3 (an STS(19)) are thus $U\{\{0, 3, 4\}\} = \{\{0, 3, 4\}, 7\{0, 3, 4\}, 11\{0, 3, 4\}\} = \{\{0, 3, 4\}, \{0, 2, 9\}, \{0, 14, 6\}\}$.

Now consider two STS, say from S_a and S_b. A result in [8] states that these STS are orthogonal if ab^{-1} and $(a+1)(b+1)^{-1}$ are both in U. At this time, we note a generalization of this which, though not as elegant, offers a check of orthogonality easily implementable on a computer.

Lemma 2.1 *S_a and S_b are orthogonal if and only if x, y, z are in distinct cosets of U in K^*, where $x = a - b$,*

$$y = \begin{cases} ab^{-1} - 1, & \text{if } ab^{-1} \in U, \\ 1 - a - ab^{-1}, & \text{if } ab^{-1} \in -U, \\ (a+1)(b+1)b^{-1} - a, & \text{if } (a+1)b^{-1} \in U, \\ 1 - (a+1)(b+1)b^{-1}, & \text{if } (a+1)b^{-1} \in -U, \end{cases}$$

$$\text{and} \quad z = \begin{cases} 1-(a+1)(b+1)^{-1}, & \text{if } (a+1)(b+1)^{-1} \in U, \\ 1-(a+1)b(b+1)^{-1}, & \text{if } (a+1)(b+1)^{-1} \in -U, \\ ab(b+1)^{-1}-a-1, & \text{if } a(b+1)^{-1} \in U, \\ -ab(b+1)^{-1}-1, & \text{if } a(b+1)^{-1} \in -U. \end{cases}$$

Proof. First note that it is straightforward to show that y and z given above are indeed well defined. Let Θ_a and Θ_b be the third element functions for the two STS. Clearly, since $\{0, b, b+1\} \in S_b$,

$$\Theta_b(\{a, a+1\}) = a - b = x.$$

Suppose $ab^{-1}, (a+1)(b+1)^{-1} \in U$. A straightforward computation gives

$$\Theta_b(\{-1, -1-a\}) = \Theta_b(\{0, -a\}) - 1 = ab^{-1}\Theta_b(\{0, -b\}) - 1 = ab^{-1} - 1 = y,$$

$$\Theta_b(\{1, -a\}) = 1 + (a+1)(b+1)^{-1}\Theta_b(\{0, -(b+1)\}) = 1 - (a+1)(b+1)^{-1} = z.$$

The other 15 cases are similar. So the list $(\Theta_b(\{u, v\}) | \Theta_a(\{u, v\}) = 0)$ consists of distinct elements if and only if x, y, z are in distinct cosets of U in K^*. By construction, these STS are invariant under additive shifts, so it is sufficient to merely check one such list. □

Remarks: If $ab^{-1}, (a+1)(b+1)^{-1} \in U$, it is clear that x, y, z as in the lemma are always in distinct cosets of U in K^*, hence the result in [8]. However, this lemma is more general. For example, in the field of order 79, S_3 and S_{49} are orthogonal by Lemma 2.1, but not by the test in [8].

When $(q-1)/6$ is even, there are similar conditions for orthogonality (but with more cases). This will be treated in Section 2.2.

The following approach is now used to build sets of mutually orthogonal STS of order q.

(1) Determine the set of all $a \in K^* \setminus Q$ such that $a(a+1) \in Q$.
(2) Use Lemma 2.1 to check orthogonality of each pair of resulting STS.
(3) Create a graph G of orthogonality between these systems and find a large clique.

Our results are summarized in Table 2.2 below. The column "primitive" lists the primitive polynomials used, (in the prime case $x - g$, where g is a generator of K^*). The next four columns list the number of systems considered, the total number of orthogonal pairs, the size of a largest clique in the orthogonality graph G (giving a lower bound for $\sigma(q)$), and the values of a forming this clique. We have listed only those orders $q \equiv 7 \pmod{12}$, $q < 500$, for which an improvement on the best known bound for $\sigma(q)$ is obtained. A table with bounds on $\sigma(n)$ for other n will be given in the conclusion.

Table 2.2 *New bounds on* $\sigma(q)$ *for some* $q \equiv 7 \pmod{12}$*, with* q *a prime power and* $q < 500$.

q	primitive	systems	edges	$\sigma(G) \geq$	clique
67	$x-2$	14	70	8	$38, 36, 37, 28, 12, 29, 54, 30$
79	$x-3$	14	34	4	$3, 49, 59, 30$
103	$x-5$	26	199	8	$57, 86, 58, 56, 15, 46, 6, 47$
151	$x-6$	38	484	14	$88, 22, 47, 128, 32, 95, 55, 11, 62, 118, 105, 45, 103, 139$
163	$x-2$	42	594	9	$2, 32, 151, 72, 87, 11, 113, 75, 107$
199	$x-3$	42	495	9	$3, 46, 71, 14, 162, 72, 169, 53, 70$
211	$x-2$	50	811	14	$180, 201, 204, 173, 189, 49, 196, 9, 154, 47, 14, 163, 176, 21$
223	$x-3$	56	979	12	$85, 96, 185, 211, 152, 204, 92, 160, 78, 80, 19, 21$
271	$x-6$	54	774	9	$36, 142, 204, 77, 108, 133, 179, 182, 21$
283	$x-3$	56	1033	11	$185, 179, 22, 159, 248, 238, 165, 236, 11, 44, 193$
307	$x-5$	72	1578	10	$25, 284, 286, 222, 293, 126, 276, 169, 65, 133$
331	$x-3$	74	1774	11	$3, 81, 195, 109, 295, 255, 112, 222, 288, 169, 197$
343	x^3+3x+2	72	1431	9	$2x^2+6x+1, 2x^2+2x+6, x^2+3x+1, 5x^2+3x+3, 5x^2+6x+5, x^2+4x+3, 6x^2+5x+5, 4x^2+5x, 6x^2$
367	$x-6$	74	1666	11	$282, 42, 139, 223, 284, 153, 283, 165, 70, 83, 65$
379	$x-2$	78	1881	11	$2, 46, 291, 278, 358, 17, 230, 31, 89, 152, 74$
439	$x-15$	104	3514	14	$180, 169, 106, 160, 338, 212, 267, 38, 204, 325, 171, 409, 45, 334$
463	$x-3$	98	3100	15	$3, 335, 217, 310, 263, 16, 258, 21, 195, 142, 369, 166, 441, 354, 372$
487	$x-3$	114	4215	16	$3, 9, 239, 372, 350, 252, 109, 180, 155, 52, 68, 153, 466, 88, 192, 326$
499	$x-7$	104	3616	17	$57, 397, 170, 43, 317, 455, 139, 407, 328, 178, 84, 320, 359, 34, 441, 91, 464$

2.2 Higher parameter systems

Here a richer collection of Steiner triple systems is introduced analogous to the 2^s quotient starters in [2]. Let K be a finite field of order $q = 3 \cdot 2^{s+1}t + 1$ with t odd and $s \geq 1$. As before, let $U \subset Q$ be subgroups of K^* of index $3 \cdot 2^{s+1}$ and 3, respectively. Suppose g is a generator for K^* and let $h = g^3$. Let $T = \{1, h, h^2, \ldots, h^{2^s-1}\}U$. Then T is a transversal of ± 1 (or half-set) in Q; in other words, T and $-T$ partition Q. The same conditions on an element a as before, namely that $a \in K^* \setminus Q$ and $a(a+1) \in Q$, guarantee $T\{\{0, a, a+1\}\}$ is a difference family over K generating an STS.

Now consider 2^s (not neccessarily distinct) elements $a_i \in K^* \setminus Q$, $0 \le i < 2^s$, and suppose the set $\cup_i \pm h^i\{1, a_i, a_i + 1\}$ exhausts a set of coset representatives for U in K^*. Then $U\{h^i\{0, a_i, a_i + 1\} | 0 \le i < 2^s\}$ is also a difference family over K^* generating an STS. For $\mathbf{a} = (a_0, a_1, \ldots)$ we will write $S_{\mathbf{a}} = (K, K + U\{h^i\{0, a_i, a_i + 1\} | 0 \le i < 2^s\}$. The third element function for this STS will be denoted by $\Theta_{\mathbf{a}}$.

Example: Let K be the field of order 61 (with generator $g = 2$). Note $s = 1$ since $61 = 6 \cdot 2^1 \cdot 5 + 1$, and $h = 8$. Then $U = \langle h^4 \rangle = \{1, 9, 20, 58, 34\}$, $T = \{1, 8\}U$, and $Q = \pm T$. The field elements 5 and 6 belong to the coset $2Q$, while 35 and 36 belong to $4Q$. Furthermore, $\pm U\{5, 6\}$ and $\pm 8U\{35, 36\}$ exhaust the respective cosets of Q in K^* (with no repetition). So $\mathbf{a} = (a_0, a_1) = (5, 35)$ generates an STS. The 10 base blocks for $S_{\mathbf{a}}$ are

$$\{1, 9, 20, 58, 34\} \cdot \{\{0, 5, 6\}, 8\{0, 35, 36\}\}.$$

In practice, it is sometimes the case that s is too large for a full consideration of 2^s parameters. Computations are simplified here by taking $|\{a_i : 0 \le i < 2^s\}| = 1, 2$, or 4, with the a_i periodic in i. The resulting STS will be called a one, two, or four parameter system, respectively. For a fixed order, many more systems may result from considering two or four parameters than from just considering one parameter systems. However, the orthogonality test generalizing Lemma 2.1 is more stringent when $s > 0$.

Theorem 2.3 *Let K be a field of order $q = 3 \cdot 2^{s+1}t + 1$ with t odd. For K^*, suppose g is a generator, $h = g^3$, and U is a subgroup of order t. Assume* $\mathbf{a}$ *and* $\mathbf{b}$ *generate the STS $S_{\mathbf{a}}$ and $S_{\mathbf{b}}$ in K^*. Define $\beta_j, \beta'_j \in \pm\{b_j, b_j + 1\}$, $f(i), f'(i) \in \{0, 1, \ldots, 2^s - 1\}$, and $u_i, u'_i \in U$ according to*

$$-a_i h^i = u_i h^{f(i)} \beta_{f(i)} \text{ and } -(a_i + 1)h^i = u'_i h^{f'(i)} \beta'_{f'(i)}.$$

For each $i \in \{0, \ldots, 2^s - 1\}$, let

$$x_i = h^i(a_i - b_i),\ y_i = -h^i + u_i h^{f(i)} \theta(\beta_{f(i)}),\ \text{and } z_i = h^i + u'_i h^{f'(i)} \theta(\beta'_{f'(i)}),$$

where $\theta(b_j) = b_j + 1$, $\theta(b_j + 1) = b_j$, $\theta(-b_j) = 1$, and $\theta(-b_j - 1) = -1$. Then $S_{\mathbf{a}}$ and $S_{\mathbf{b}}$ are orthogonal if and only if the $3 \cdot 2^s$ elements x_i, y_i, z_i are in distinct cosets of U in K^*.

Proof: Observe first that the notation introduced is well-defined because the base blocks of $S_{\mathbf{b}}$ form a difference family. Since the systems $S_{\mathbf{a}}$ and $S_{\mathbf{b}}$ are invariant under additive translation, they are orthogonal if and only if $(\Theta_{\mathbf{b}}(\{u, v\}) | \Theta_{\mathbf{a}}(\{u, v\}) = 0)$ consists of distinct elements of K^*; that is, if

$$\Theta_{\mathbf{b}}(\{a_i h^i, (a_i + 1)h^i\}),\ \Theta_{\mathbf{b}}(\{-(a_i + 1)h^i, -h^i\}),\ \Theta_{\mathbf{b}}(\{-a_i h^i, h^i\}),\quad 0 \le i < 2^s$$

are all in distinct cosets of U in K^*. Using the notation in the statement of the theorem, these may be computed:

$$\begin{aligned}\Theta_{\mathbf{b}}(\{a_i h^i, (a_i+1)h^i\}) &= a_i h^i + \Theta_{\mathbf{b}}(\{0, h^i\}) \;=\; a_i h^i - b_i h^i \;=\; x_i,\\ \Theta_{\mathbf{b}}(\{-(a_i+1)h^i, -h^i\}) &= -h^i + \Theta_{\mathbf{b}}(\{0, -a_i h^i\}) \;=\; -h^i + u_i \Theta_{\mathbf{b}}(\{0, h^{f(i)}\beta_{f(i)}\})\\ &= -h^i + u_i h^{f(i)}\theta(\beta_{f(i)}) \;=\; y_i,\end{aligned}$$

and similarly $\Theta_{\mathbf{b}}(\{-a_i h^i, h^i\}) = z_i$. □

Luckily, there is not total chaos among the elements x_i, y_i, z_i. Suppose that the parameter period is p, so that $a_i = a_{i+p}$ and similarly for the b_i, where the indices are mod 2^s. Then clearly $x_{i+p} = h^p x_i$ for all i. Now if for some i it turns out that $f(i) < 2^s - p$, then

$$u_{i+p} h^{f(i+p)}\beta_{f(i+p)} = -a_{i+p}h^{i+p} = h^p(-a_i h^i) = h^p(u_i h^{f(i)}\beta_{f(i)}) = u_i h^{f(i)+p}\beta_{f(i)}.$$

Thus $h^{f(i+p)}\beta_{f(i+p)}$ and $h^{f(i)+p}\beta_{f(i)}$ are in the same cosets of U in K^*. By periodicity of the b_j and the difference family condition, it must be that $f(i+p) = f(i)+p$ and $\beta_{f(i+p)} = \beta_{f(i)}$, which in turn implies that $u_{i+p} = u_i$. So $y_{i+p} = h^p y_i$, and similarly for the z_i. Note that when $f(i) \geq 2^s - p$, there is a small issue with β_i and β_i' switching sign. To summarize, the distinct coset test of the theorem is less stringent for larger periods p.

Example: For $q = 97 = 6 \cdot 2^4 + 1$, we generated all one, two, and four parameter STS $S_{\mathbf{a}}$ and automated Theorem 2.3 to build an orthogonality graph. The number of vertices, edges, and edge density of these graphs are presented in below. In each case, the maximum clique size found was 3. (In Lemma 3.6 we show $\sigma(97) \geq 4$.)

period	vertices	edges	density
1	26	47	1.45×10^{-1}
2	111	106	1.74×10^{-2}
4	1786	359	2.25×10^{-4}

Under the rough estimation that both the number of B parameter systems and edge density of the B parameter orthogonality graph are proportional to the Bth power of those quantities for one parameter systems, it seems reasonable to expect little improvement when considering higher parameter systems. After all, the expected clique size of a random graph with N vertices and edge probability p is $\log_{1/p} N$. However, it is certainly the case that individual orders may turn out to admit larger collections of mutually orthogonal STS when more parameters are considered.

Two or four parameters were attempted for all 1 (mod 12) prime power orders less than 500. For some of these orders, however, a largest clique was found simply among one parameter systems. Some small orders belong to this class but still larger mutually orthogonal collections are presented later. The results for the remaining orders in this class are presented in the following table. Field element a in the column "clique" represents that $S_{\mathbf{a}}$, where $a_i = a$ for all $i = 0, 1, \ldots, 2^s - 1$, is among the systems present in the maximum clique.

Table 2.4 *New bounds on $\sigma(q)$ using one parameter systems for some $q \equiv 1 \pmod{12}$, with q a prime power and $q < 500$.*

q	s	primitive	systems	edges	$\sigma(G) \geq$	clique
49	3	$x^2 + x + 3$	14	23	4	$2, 4, 5x + 5, 2x + 1$
61	1	$x - 2$	14	29	5	$4, 12, 47, 13, 46$
121	2	$x^2 + x + 7$	32	127	5	$x, 8x + 7, 4x + 7, 7x + 3, 3x + 10$
169	2	$x^2 + x + 2$	38	159	4	$12x + 11, 4x, 5x + 12, 6x + 5$
193	5	$x - 5$	38	69	3	$46, 47, 84$
241	3	$x - 7$	50	214	4	$12, 19, 221, 228$
289	4	$x^2 + x + 3$	72	299	3	$x, 13x + 4, 11x + 4$
313	2	$x - 10$	62	445	5	$119, 76, 101, 214, 62$
337	3	$x - 10$	74	403	4	$227, 128, 109, 208$
361	2	$x^2 + x + 2$	78	711	5	$7x + 10, 3x + 5, 2x + 16, 7x + 12, 3x + 17$
409	2	$x - 21$	98	1044	6	$206, 164, 96, 355, 17, 141$
433	3	$x - 5$	96	675	4	$25, 22, 49, 95$
457	2	$x - 13$	104	1220	6	$361, 323, 98, 133, 358, 149$

In the next table, we give improved bounds on $\sigma(q)$ when two parameters are considered. In all these cases $s = 1$. The column "clique" gives vectors $\mathbf{a}$ generating pairwise orthogonal STS. A singleton entry a in this column means $a_i = a$ for $i = 0, 1$.

Table 2.5 *New bounds on $\sigma(q)$ using two parameter systems for some $q \equiv 1 \pmod{12}$, with q a prime power and $q < 500$.*

q	primitive	systems	edges	$\sigma(G) \geq$	clique
109	$x-6$	120	1433	6	$79,(30,6),(20,88),(58,39),(14,94),(84,24)$
181	$x-2$	359	13968	7	$57,(148,119),(147,43),(165,15),(20,164),$ $(80,37),(17,163)$
229	$x-6$	616	42981	7	$6,182,134,69,166,(94,99),(133,110)$
277	$x-5$	616	44659	8	$116,160,(78,71),(100,55),(10,219),$ $(248,85),(209,115),(136,35)$
349	$x-2$	1233	187283	9	$122,226,(141,12),(189,188),(93,191),$ $(23,243),(164,2),(50,219),(55,325)$
397	$x-5$	1776	359971	10	$307,202,339,57,194,74,89,322,$ $(338,58),(308,88)$
421	$x-2$	1827	391517	10	$400,277,20,192,(300,134),(191,239),$ $(382,38),(326,280),(398,380),(237,57)$

One surprisingly nice construction using four parameter systems is now given.

Proposition 2.6 *There exist four mutually orthogonal STS of order 25.*

Proof: Let $K = \mathbf{Z}_5[x]/(x^2+x+2)$, with generator $g = x$ and $h = g^3 = 4x+2$. Note $s = 2$ for $q = 25$. The four systems with parameter lists $(4x+4, x, x, x)$, $(2x+3, 2x+3, 3x+1, 3x+1)$, $(3x, 3x, 3x, 3x)$ and $(2x+2, 2x+2, 2x+2, 2x+2)$ are claimed to be pairwise orthogonal. The four sets of base blocks are given below.

$$\begin{aligned}
\text{I}: &\quad \{\{0, 4x+4, 4x\}\} \cup \{h, h^2, h^3\}\{\{0, x, x+1\}\},\\
\text{II}: &\quad \{1, h\}\{\{0, 2x+3, 2x+4\}\} \cup \{h^2, h^3\}\{\{0, 3x+1, 3x+2\}\},\\
\text{III}: &\quad \{1, h, h^2, h^3\}\{\{0, 3x, 3x+1\}\}, \text{ and}\\
\text{IV}: &\quad \{1, h, h^2, h^3\}\{\{0, 2x+2, 2x+3\}\}.
\end{aligned}$$

We will check that the first two sets of starter blocks $S_{\mathbf{a}}$ and $S_{\mathbf{b}}$ (I and II above) form a difference family over K and that the resulting STS are orthogonal. The pairs occurring with 0 in $S_{\mathbf{a}}$, their third elements in $S_{\mathbf{b}}$, and the corresponding pairs occurring with 0 in $S_{\mathbf{b}}$ are given in the table below. Note the left and right columns exhaust K^* (the difference family condition) and the middle column consists of distinct elements of K^* (the orthogonality condition). Analysis of the other pairs of systems is similar. □

$\{u,v\} \in \Theta_{\mathbf{a}}^{-1}(0)$	$\Theta_{\mathbf{b}}(\{u,v\})$	$w + \{u,v\} \in \Theta_{\mathbf{b}}^{-1}(0)$
$4x+4, 4x$	$2x+1$	$2x+3, 2x+4$
$1, x+1$	$2x+2$	$3x+4, 4x+4$
$4x+1, 3x+4$	$4x+3$	$3, 4x+1$
$3x+2, 2x+4$	2	$3x, 2x+2$
$3x+1, x+3$	$3x+2$	$4, 3x+1$
$x, 4$	$4x+4$	$2x+1, x$
$2x, 2x+2$	$x+3$	$x+2, x+4$
$3x+3, 3$	$2x$	$x+3, 3x+3$
$4x+2, 2x+3$	$4x+1$	$1, 3x+2$
$x+4, 4x+3$	3	$x+1, 4x$
$x+2, 2x+1$	$3x+4$	$4x+3, 2$
$2, 3x$	x	$4x+2, 2x$

Remark: The first two STS can be described more compactly as

$$\{1, h^5, h^6, h^7\}\{\{0, 4x+4, 4x\}\}, \text{ and } \{1, h, h^5, h^6\}\{\{0, 2x+3, 2x+4\}\}.$$

In this alternative description, the a_i and b_i are constant (period one), but the transversals used deviate from the usual $\{1, h, h^2, h^3\}$.

Skew-orthogonal STS

It was shown in [11] that pairs of orthogonal STS correspond to Room squares. For this Room square to be skew, [5], the following additional condition must hold.

(iii) $\{u,v,a\}, \{x,y,w\} \in \mathcal{B}_1$ and $\{u,v,z\}, \{x,y,a\} \in \mathcal{B}_2$ implies $w \neq z$.
(Note $u = x$ is possible).

Two orthogonal STS $(V, \mathcal{B}_1)$ and $(V, \mathcal{B}_2)$ satisfying (iii) are *skew-orthogonal*. The algebraic methods introduced so far can be easily modified to handle this stronger relationship. It is an easy consequence of the definitions that two abelian group generated STS with third element functions Θ_1 and Θ_2 are skew-orthogonal if and only if the set $(\pm\Theta_2(\{u,v\})|\Theta_1(\{u,v\}) = 0)$ exhausts the nonzero group elements. In other words, the orthogonality certificate must form a *half-set* in the group. Theorem 2.3 (and similarly Lemma 2.1) may be modified for skew-orthogonality by stipulating that all the elements $\pm x_i, \pm y_i, \pm z_i$ lie in distinct cosets of U. Of course, it is equally easy to automate this test on computer and find cliques in the resulting skew-orthogonal subgraphs of the original graphs. It is not our intention to conduct a thorough analysis here. However, it should be reported that we often found

cliques of size at least three. It is known that skew-orthogonal pairs of STS arise from Mullin-Nemeth starters in the finite fields. In the table below, a few lower bounds for the maximum number of pairwise skew-orthogonal STS of order q, denoted $\sigma'(q)$, which improve upon this are noted.

q	31	43	61	67	79	103	109	127	139	151	157	163
$\sigma'(q) \geq$	3	3	3	4	3	5	3	4	4	5	3	6

3 Automorphisms and Hill-climbing

In this section we will describe the use of hill-climbing techniques to find sets of orthogonal Steiner triple systems.

3.1 Small 3 (mod 6) orders

An *automorphism* of an STS $(V, \mathcal{B})$ is a function $f : V \to V$ such that $f\mathcal{B} = \mathcal{B}$. If such an f (viewed as a permutation) consists of three cycles of equal length $n/3$, the STS is called *3-cyclic*. Such a system is determined completely by $(n-1)/2$ *base triples*, or orbit representatives for f. See [1] or [7] for more on automorphisms of triple systems. We now outline a construction for 3 mutually orthogonal 3-cyclic STS of order $n \equiv 3 \pmod 6$. Take the pointset $V = \mathbf{Z}_{n/3} \times \mathbf{Z}_3$, with generating automorphism $x_i \mapsto (x+1)_i$ and define the map $\alpha : x_i \mapsto x_{i+1}$. As usual, subscripts represent the second coordinate in the product. A standard hill-climb (like the algorithm in [7]) is used to construct a set of $(n-1)/2$ base triples, which when developed form a set $\mathcal{B}$ of blocks so that $(V, \mathcal{B})$ is orthogonal to $(V, \alpha\mathcal{B})$. A randomly chosen base block $B = \{x, y, z\}$ either augments a partial STS or replaces a block already covering one of the pairs in B, provided the new system causes no conflict with either orthogonality condition (i) or (ii). Call the third element relation in the partial design Θ. Condition (i) simply amounts to checking $\alpha^{\pm 1}x \neq \Theta(\{\alpha^{\pm 1}y, \alpha^{\pm 1}z\})$. Verifying (ii) is where the majority of the computing time lies, since it involves a loop over all points c and the tests (when Θ is defined)

$$\Theta(\alpha x, \alpha y) \neq \Theta\left(\alpha c, \alpha\Theta(c, z)\right),$$

as well as for α^{-1} and the other rearrangements of x, y, z.

Orthogonality of two STS is clearly invariant under a common map. So these base triples actually produce three pairwise orthogonal STS: $(V, \mathcal{B})$, $(V, \alpha\mathcal{B})$, and $(V, \alpha^2\mathcal{B})$. We have

had success with this method for $27 \leq n \leq 81$, with computation times ranging between seconds and many days. The time before finding a solution depends partly on a threshold parameter which restarts the hill-climb after repeated failure to augment the partial design. This parameter was set roughly proportional to the total number of base blocks possible for the given order. Computing time also varies according to the optimization in compiling and the platform used. An exhaustive search of all 3-cyclic STS of order 21 revealed no design with the desired condition.

Lemma 3.1 *$\sigma(n) \geq 3$ for $n \in \{27, 33, 39, 45, 51, 57, 63, 69, 75, 81\}$.*

Proof: Three pairwise orthogonal STS of order n are presented below by specifying the $(n-1)/2$ base triples for one system. The other systems are obtained by shifting indices. □

$n = 27$: $\{0_0, 2_1, 8_2\}$, $\{0_1, 1_0, 2_0\}$, $\{0_0, 2_2, 7_2\}$, $\{0_0, 3_1, 4_2\}$, $\{0_2, 6_1, 7_1\}$, $\{0_1, 0_0, 4_0\}$, $\{0_1, 3_1, 5_1\}$, $\{0_2, 6_0, 8_0\}$, $\{0_0, 0_2, 6_2\}$, $\{0_0, 6_1, 5_2\}$, $\{0_1, 4_2, 5_2\}$, $\{0_1, 5_0, 8_0\}$, $\{0_1, 0_2, 7_2\}$

$n = 33$: $\{0_0, 10_1, 7_2\}$, $\{0_1, 4_0, 8_0\}$, $\{0_2, 3_0, 9_0\}$, $\{0_1, 9_2, 10_2\}$, $\{0_1, 0_0, 2_0\}$, $\{5_1, 8_1, 9_1\}$, $\{0_0, 8_1, 10_2\}$, $\{0_0, 2_1, 4_1\}$, $\{0_2, 0_0, 8_0\}$, $\{0_1, 5_0, 6_0\}$, $\{0_0, 1_1, 6_2\}$, $\{0_2, 0_1, 5_1\}$, $\{0_1, 4_2, 7_2\}$, $\{0_0, 4_2, 9_2\}$, $\{0_1, 1_2, 3_2\}$, $\{0_0, 1_2, 5_2\}$

$n = 39$: $\{0_0, 0_2, 4_2\}$, $\{0_0, 3_1, 11_1\}$, $\{0_2, 3_0, 10_0\}$, $\{0_2, 5_0, 8_0\}$, $\{0_1, 7_0, 11_0\}$, $\{0_2, 0_1, 2_1\}$, $\{0_2, 1_1, 4_1\}$, $\{0_0, 10_1, 12_2\}$, $\{5_2, 10_2, 11_2\}$, $\{0_1, 3_2, 6_2\}$, $\{0_0, 0_1, 9_1\}$, $\{0_0, 12_1, 7_2\}$, $\{0_2, 7_0, 12_0\}$, $\{0_1, 8_0, 9_0\}$, $\{0_0, 7_1, 8_1\}$, $\{0_0, 1_1, 2_2\}$, $\{0_1, 5_2, 7_2\}$, $\{0_2, 2_0, 4_0\}$, $\{0_2, 3_1, 9_1\}$

$n = 45$: $\{0_2, 0_1, 4_1\}$, $\{0_0, 4_2, 14_2\}$, $\{0_0, 2_2, 3_2\}$, $\{0_0, 2_1, 9_1\}$, $\{0_0, 6_1, 12_1\}$, $\{0_2, 11_1, 13_1\}$, $\{0_0, 7_1, 8_2\}$, $\{0_0, 3_1, 4_1\}$, $\{0_2, 5_1, 8_1\}$, $\{0_2, 2_0, 3_0\}$, $\{0_2, 0_0, 10_0\}$, $\{0_0, 13_1, 11_2\}$, $\{0_1, 1_0, 4_0\}$, $\{0_0, 6_2, 10_2\}$, $\{0_0, 1_1, 7_2\}$, $\{0_0, 4_0, 13_0\}$, $\{0_1, 9_2, 12_2\}$, $\{0_0, 5_1, 10_1\}$, $\{0_1, 0_0, 7_0\}$, $\{0_1, 8_2, 14_2\}$, $\{0_0, 1_2, 9_2\}$, $\{0_1, 3_2, 5_2\}$

$n = 51$: $\{0_0, 14_1, 3_2\}$, $\{0_0, 6_1, 12_1\}$, $\{0_0, 2_1, 1_2\}$, $\{0_2, 2_1, 10_1\}$, $\{0_1, 1_0, 8_0\}$, $\{1_0, 4_0, 12_0\}$, $\{0_1, 11_2, 13_2\}$, $\{0_2, 3_1, 8_1\}$, $\{0_0, 10_1, 12_2\}$, $\{0_0, 7_2, 15_2\}$, $\{0_0, 0_1, 15_1\}$, $\{0_1, 4_0, 16_0\}$, $\{0_0, 0_2, 4_2\}$, $\{0_0, 5_1, 8_1\}$, $\{0_1, 13_0, 14_0\}$, $\{0_2, 4_0, 8_0\}$, $\{0_2, 9_1, 13_1\}$, $\{0_0, 11_1, 16_2\}$, $\{0_0, 5_2, 10_2\}$, $\{0_0, 7_1, 2_2\}$, $\{0_2, 0_1, 16_1\}$, $\{3_2, 4_2, 10_2\}$, $\{0_2, 9_0, 11_0\}$, $\{0_0, 11_2, 14_2\}$, $\{0_2, 7_1, 14_1\}$

$n = 57$: $\{2_2, 5_2, 12_2\}$, $\{0_1, 5_0, 10_0\}$, $\{0_0, 1_1, 2_2\}$, $\{0_1, 0_0, 16_0\}$, $\{0_1, 4_0, 11_0\}$, $\{0_2, 13_0, 15_0\}$, $\{0_0, 4_1, 16_2\}$, $\{0_2, 15_1, 17_1\}$, $\{0_0, 11_2, 15_2\}$, $\{10_1, 11_1, 17_1\}$, $\{0_1, 5_2, 18_2\}$, $\{2_1, 6_1, 11_1\}$, $\{0_0, 2_1, 18_1\}$, $\{0_0, 10_1, 7_2\}$, $\{0_1, 6_2, 14_2\}$, $\{0_1, 15_2, 17_2\}$, $\{0_1, 2_0, 13_0\}$, $\{0_0, 7_1, 17_2\}$, $\{0_0, 16_1, 10_2\}$, $\{0_2, 10_0, 11_0\}$, $\{8_0, 12_0, 18_0\}$, $\{0_0, 13_1, 3_2\}$, $\{0_0, 12_1, 1_2\}$, $\{0_0, 0_2, 14_2\}$, $\{0_0, 12_2, 13_2\}$, $\{0_0, 11_1, 18_2\}$, $\{0_0, 5_1, 5_2\}$, $\{0_2, 8_1, 16_1\}$

$n = 63$: $\{0_1, 4_1, 9_1\}$, $\{0_0, 1_2, 3_2\}$, $\{0_0, 10_1, 13_2\}$, $\{0_0, 1_1, 12_1\}$, $\{0_0, 17_1, 10_2\}$, $\{0_0, 19_1, 20_1\}$, $\{0_2, 1_1, 14_1\}$, $\{0_0, 7_2, 8_2\}$, $\{0_1, 8_0, 14_0\}$, $\{0_0, 11_2, 20_2\}$, $\{0_2, 0_0, 17_0\}$, $\{0_0, 15_1, 17_2\}$, $\{0_0, 14_1, 15_2\}$, $\{0_2, 0_1, 2_1\}$, $\{0_0, 2_0, 14_0\}$, $\{0_0, 11_1, 5_2\}$, $\{0_0, 6_2, 16_2\}$, $\{0_2, 9_0, 12_0\}$, $\{0_0, 9_1, 14_2\}$, $\{0_1, 11_2, 16_2\}$, $\{0_0, 2_1, 19_2\}$, $\{0_1, 10_2, 13_2\}$, $\{0_1, 5_0, 18_0\}$, $\{0_1, 16_0, 17_0\}$, $\{0_2, 3_0, 19_0\}$, $\{0_2, 12_1, 15_1\}$, $\{0_1, 8_2, 12_2\}$, $\{0_2, 3_1, 17_1\}$, $\{0_0, 0_1, 6_1\}$, $\{0_2, 7_2, 13_2\}$, $\{0_1, 3_0, 13_0\}$

$n = 69$: $\{0_1, 11_2, 18_2\}$, $\{3_0, 9_0, 11_0\}$, $\{0_0, 2_1, 16_1\}$, $\{0_0, 19_1, 20_1\}$, $\{0_0, 4_2, 10_2\}$, $\{0_0, 1_1, 22_2\}$, $\{0_0, 12_2, 21_2\}$, $\{0_0, 18_1, 14_2\}$, $\{0_1, 2_0, 15_0\}$, $\{0_0, 13_1, 20_2\}$, $\{0_1, 6_0, 17_0\}$, $\{0_2, 6_0, 7_0\}$, $\{0_2, 0_1, 21_1\}$, $\{0_0, 5_1, 6_2\}$, $\{0_2, 5_0, 10_0\}$, $\{0_0, 9_1, 22_1\}$, $\{0_0, 4_1, 10_1\}$, $\{0_2, 3_1, 7_1\}$, $\{0_2, 10_1, 17_1\}$, $\{0_1, 8_2, 9_2\}$, $\{0_0, 11_1, 14_1\}$, $\{1_2, 9_2, 13_2\}$, $\{0_0, 2_2, 7_2\}$, $\{0_2, 0_0, 20_0\}$, $\{0_2, 13_1, 18_1\}$, $\{0_2, 8_1, 19_1\}$, $\{0_2, 4_0, 18_0\}$, $\{0_1, 16_0, 20_0\}$, $\{0_0, 9_2, 11_2\}$, $\{0_1, 14_2, 17_2\}$, $\{0_1, 12_2, 22_2\}$, $\{0_0, 12_1, 15_2\}$, $\{0_0, 0_1, 15_1\}$, $\{0_2, 15_0, 22_0\}$

$n = 75$: $\{0_0, 20_1, 24_2\}$, $\{2_0, 9_0, 14_0\}$, $\{0_2, 19_1, 23_1\}$, $\{0_2, 9_1, 20_1\}$, $\{0_0, 23_1, 9_2\}$, $\{0_2, 11_0, 14_0\}$, $\{0_0, 8_2, 18_2\}$, $\{0_1, 1_0, 20_0\}$, $\{0_1, 4_0, 19_0\}$, $\{0_0, 9_1, 15_1\}$, $\{0_0, 7_1, 2_2\}$, $\{0_0, 6_2, 20_2\}$, $\{0_1, 12_0, 14_0\}$, $\{0_1, 13_0, 17_0\}$, $\{0_1, 6_0, 7_0\}$, $\{0_1, 14_2, 19_2\}$, $\{0_1, 0_0, 9_0\}$, $\{0_1, 10_2, 22_2\}$, $\{6_1, 21_1, 23_1\}$, $\{0_0, 1_2, 23_2\}$, $\{0_0, 4_1, 22_1\}$, $\{0_2, 0_0, 8_0\}$, $\{0_0, 17_1, 15_2\}$, $\{0_0, 7_2, 13_2\}$, $\{0_0, 3_2, 5_2\}$, $\{0_2, 4_0, 15_0\}$, $\{0_0, 2_1, 3_1\}$, $\{0_0, 14_1, 22_2\}$, $\{0_2, 1_1, 10_1\}$, $\{0_0, 12_2, 16_2\}$, $\{0_0, 1_1, 4_2\}$, $\{0_1, 1_2, 17_2\}$, $\{0_2, 4_1, 7_1\}$, $\{0_2, 0_1, 12_1\}$, $\{0_0, 10_1, 19_2\}$, $\{0_2, 13_1, 18_1\}$, $\{5_2, 22_2, 23_2\}$

$n = 81$: $\{0_1, 4_2, 20_2\}$, $\{0_0, 4_1, 23_1\}$, $\{0_0, 22_1, 24_2\}$, $\{0_2, 12_0, 26_0\}$, $\{0_0, 19_2, 20_2\}$, $\{0_2, 2_1, 22_1\}$, $\{0_0, 5_1, 10_1\}$, $\{0_2, 14_1, 24_1\}$, $\{0_0, 18_1, 19_1\}$, $\{0_0, 4_2, 6_2\}$, $\{0_0, 3_1, 10_2\}$, $\{0_2, 1_0, 9_0\}$, $\{0_0, 2_2, 25_2\}$, $\{0_2, 0_0, 18_0\}$, $\{0_0, 1_1, 17_2\}$, $\{0_1, 8_2, 11_2\}$, $\{0_2, 8_2, 15_2\}$, $\{0_2, 4_0, 15_0\}$, $\{0_0, 13_1, 15_1\}$, $\{0_0, 12_1, 24_1\}$, $\{0_0, 8_1, 21_1\}$, $\{0_1, 0_0, 20_0\}$, $\{0_0, 1_0, 3_0\}$, $\{0_0, 9_1, 25_1\}$, $\{0_0, 12_0, 17_0\}$, $\{0_1, 9_2, 19_2\}$, $\{0_2, 9_1, 13_1\}$, $\{0_0, 16_1, 13_2\}$, $\{0_2, 16_0, 20_0\}$, $\{0_0, 6_1, 5_2\}$, $\{0_2, 17_1, 26_1\}$, $\{0_0, 3_2, 21_2\}$, $\{0_1, 10_0, 16_0\}$, $\{0_0, 14_1, 14_2\}$, $\{0_1, 15_2, 21_2\}$, $\{0_0, 8_2, 22_2\}$, $\{0_0, 2_1, 26_1\}$, $\{0_0, 20_1, 16_2\}$, $\{0_1, 17_2, 22_2\}$, $\{0_2, 15_1, 21_1\}$

Note that the examples above are the first for values of $n \equiv 3 \pmod 6$ where $\sigma(n) \geq 3$. One easy consequence of Theorem 1.4, Lemma 3.1, and the PBD-closure of the existence of k mutually orthogonal STS is now given.

Theorem 3.2 *There exists N such that $\sigma(n) \geq 3$ for all $n \equiv 1, 3 \pmod 6, n \geq N$.*

A construction of arbitrarily large sets of mutually orthogonal STS of order 3 (mod 6) is not known at this time. However, the following seems very reasonable.

Conjecture 3.3 *For $n \equiv 3 \pmod 6$, $\lim_{n\to\infty} \sigma(n) = \infty$.*

3.2 Multiplicative images of cyclic STS

An STS of order n with an automorphism consisting of a single cycle of length n is called *cyclic*. When $n \equiv 1 \pmod 6$, the design is determined by $(n-1)/6$ base triples. The cyclic group $V = \mathbf{Z}_n$ with generating automorphism $x \mapsto x+1$ will be used for the points of a cyclic STS here. The base triples can then be chosen as *zero-sum* triples, by an appropriate additive shift. Let $\mu : V \to V$ be multiplication by $m \in \mathbf{Z}_n^*$, and define μ to act on each block of $\mathcal{B}$ elementwise. Suppose the multiplicative order of m in $\mathbf{Z}_n^*$ is t. It is of interest when $\mu^i\mathcal{B}$, $0 \le i < t$, form block sets for t pairwise orthogonal STS of order n. The case when $m = -1$ (and thus $t = 2$) was studied by Schrieber in [12]. The resulting objects are called *opposite orthogonal* STS. There is a simple characterization of when a cyclic STS $(V, \mathcal{B})$ is orthogonal to $(V, -\mathcal{B})$.

Proposition 3.4 [12] *A cyclic STS $(V, \mathcal{B})$ is opposite orthogonal if and only if the zero-sum triples of $\mathcal{B}$ have among them no repeated elements of $V \setminus \{0\}$.*

This fact can be exploited in the search for several pairwise orthogonal STS in many ways. The most fruitful method we found was to first hill-climb to an opposite orthogonal STS $(V, \mathcal{B})$, and then backtrack or hill-climb to another cyclic STS subject to it being orthogonal to both $(V, \mathcal{B})$ and $(V, -\mathcal{B})$. This produces a set of three pairwise orthogonal STS. We have had success at this method for $31 \le n \le 205$. The small examples were found in seconds, but the largest ones took a few days on a parallel computer. In general, when the number of base triples is similar, this algorithm appears to be comparable in efficiency to the algorithm for 3 (mod 6) orders presented earlier.

Lemma 3.5 *$\sigma(n) \ge 3$ for all $n \in \{37, 55, 91, 115, 133, 145, 175\}$.*

Proof: The three systems are given for each order by specifying the $(n-1)/6$ zero-sum base triples for an opposite orthogonal STS, followed by $(n-1)/6$ base triples for a cyclic STS orthogonal to both the first system and its negative. Note in each case the first collection of triples are disjoint. □

$n = 37$: $\{13,26,35\}, \{10,12,15\}, \{2,14,21\}, \{18,24,32\}, \{4,8,25\}, \{33,34,7\}$;
$\{8,12,17\}, \{2,10,25\}, \{23,25,26\}, \{2,8,27\}, \{14,25,35\}, \{11,28,35\}$

$n = 55$: $\{29,11,15\}$, $\{39,9,7\}$, $\{12,22,21\}$, $\{33,36,41\}$, $\{49,34,27\}$, $\{44,16,50\}$, $\{52,23,35\}$,
$\{54,38,18\}$, $\{30,19,6\}$;

$\{20,18,17\}$, $\{38,16,1\}$, $\{40,13,2\}$, $\{43,36,31\}$, $\{46,37,27\}$, $\{46,42,22\}$, $\{48,35,27\}$, $\{52,36,22\}$, $\{54,31,25\}$

$n = 91$: $\{11,15,65\}$, $\{8,22,61\}$, $\{64,67,51\}$, $\{72,7,12\}$, $\{66,5,20\}$, $\{3,50,38\}$, $\{41,1,49\}$, $\{87,81,14\}$, $\{73,63,46\}$, $\{19,78,85\}$, $\{10,52,29\}$, $\{23,44,24\}$, $\{30,2,59\}$, $\{35,90,57\}$, $\{28,37,26\}$;
$\{1,18,30\}$, $\{8,24,79\}$, $\{83,85,41\}$, $\{6,82,17\}$, $\{21,3,49\}$, $\{90,30,67\}$, $\{67,58,62\}$, $\{27,17,41\}$, $\{25,26,18\}$, $\{50,69,11\}$, $\{48,18,21\}$, $\{55,89,23\}$, $\{7,45,85\}$, $\{5,26,74\}$, $\{68,18,12\}$

$n = 115$: $\{2,64,49\}$, $\{100,21,109\}$, $\{93,86,51\}$, $\{16,40,59\}$, $\{72,75,83\}$, $\{10,99,6\}$, $\{31,52,32\}$, $\{50,107,73\}$, $\{42,17,56\}$, $\{45,62,8\}$, $\{112,81,37\}$, $\{102,92,36\}$, $\{103,29,98\}$, $\{96,68,66\}$, $\{87,5,23\}$, $\{63,34,18\}$, $\{79,12,24\}$, $\{13,76,26\}$, $\{53,15,47\}$;
$\{41,29,18\}$, $\{2,57,89\}$, $\{108,34,113\}$, $\{13,28,19\}$, $\{4,54,58\}$, $\{75,99,18\}$, $\{60,39,105\}$, $\{109,110,2\}$, $\{91,14,62\}$, $\{30,93,50\}$, $\{93,63,90\}$, $\{16,2,58\}$, $\{50,89,67\}$, $\{66,13,26\}$, $\{9,78,60\}$, $\{55,39,29\}$, $\{13,32,57\}$, $\{21,101,103\}$, $\{64,101,33\}$

$n = 133$ $\{116,109,41\}$, $\{92,79,95\}$, $\{114,89,63\}$, $\{74,112,80\}$, $\{24,19,90\}$, $\{77,3,53\}$, $\{98,10,25\}$, $\{33,111,122\}$, $\{17,103,13\}$, $\{47,75,11\}$, $\{14,35,84\}$, $\{91,45,130\}$, $\{76,105,85\}$, $\{121,81,64\}$, $\{88,78,100\}$, $\{55,22,56\}$, $\{38,129,99\}$, $\{118,65,83\}$, $\{120,18,128\}$, $\{127,31,108\}$, $\{72,70,124\}$, $\{26,67,40\}$;
$\{20,108,114\}$, $\{9,62,110\}$, $\{50,26,91\}$, $\{24,120,15\}$, $\{103,69,83\}$, $\{87,95,43\}$, $\{108,103,85\}$, $\{88,109,2\}$, $\{19,34,30\}$, $\{129,80,55\}$, $\{46,122,92\}$, $\{95,31,66\}$, $\{54,116,16\}$, $\{24,87,8\}$, $\{120,59,69\}$, $\{76,18,54\}$, $\{84,126,6\}$, $\{50,69,38\}$, $\{55,98,105\}$, $\{72,75,73\}$, $\{17,94,34\}$, $\{107,80,14\}$

$n = 145$: $\{115,44,131\}$, $\{59,94,137\}$, $\{23,18,104\}$, $\{144,129,17\}$, $\{11,61,73\}$, $\{47,60,38\}$, $\{134,15,141\}$, $\{2,16,127\}$, $\{53,50,42\}$, $\{32,126,132\}$, $\{138,31,121\}$, $\{13,43,89\}$, $\{83,4,58\}$, $\{1,54,90\}$, $\{66,110,114\}$, $\{88,67,135\}$, $\{68,8,69\}$, $\{20,77,48\}$, $\{102,37,6\}$, $\{140,116,34\}$, $\{124,84,82\}$, $\{139,64,87\}$, $\{81,91,118\}$, $\{107,3,35\}$;
$\{137,38,45\}$, $\{91,127,17\}$, $\{86,143,58\}$, $\{126,44,65\}$, $\{62,76,50\}$, $\{115,53,40\}$, $\{124,106,87\}$, $\{5,46,84\}$, $\{67,125,36\}$, $\{48,3,19\}$, $\{97,38,93\}$, $\{8,105,14\}$, $\{122,26,137\}$, $\{46,111,122\}$, $\{126,3,53\}$, $\{57,24,125\}$, $\{74,113,49\}$, $\{41,81,14\}$, $\{30,25,28\}$, $\{81,72,82\}$, $\{4,12,36\}$, $\{66,117,14\}$, $\{132,34,4\}$, $\{140,120,97\}$

$n = 175$: $\{116,150,84\}$, $\{90,159,101\}$, $\{169,88,93\}$, $\{72,113,165\}$, $\{148,58,144\}$, $\{89,132,129\}$, $\{85,55,35\}$, $\{76,59,40\}$, $\{57,173,120\}$, $\{168,161,21\}$, $\{125,17,33\}$, $\{138,171,41\}$, $\{3,64,108\}$, $\{94,100,156\}$, $\{152,4,19\}$, $\{149,139,62\}$, $\{63,75,37\}$, $\{114,7,54\}$, $\{31,122,22\}$, $\{141,117,92\}$, $\{124,45,6\}$, $\{109,95,146\}$, $\{155,11,9\}$, $\{56,136,158\}$, $\{47,68,60\}$, $\{172,52,126\}$, $\{153,43,154\}$, $\{50,98,27\}$, $\{163,42,145\}$;
$\{76,97,14\}$, $\{147,74,161\}$, $\{90,132,5\}$, $\{70,111,104\}$, $\{23,62,173\}$, $\{88,78,66\}$, $\{35,130,48\}$, $\{110,148,156\}$, $\{125,44,101\}$, $\{149,34,79\}$, $\{79,56,85\}$, $\{137,163,107\}$, $\{132,25,121\}$, $\{168,2,101\}$, $\{43,149,39\}$, $\{87,115,26\}$, $\{124,73,174\}$, $\{117,74,42\}$,

$\{107,70,125\}$, $\{87,35,34\}$, $\{171,80,113\}$, $\{30,77,108\}$, $\{76,56,92\}$, $\{126,107,161\}$,
$\{38,104,87\}$, $\{4,139,67\}$, $\{24,68,83\}$, $\{114,111,109\}$, $\{85,58,162\}$

Another method for finding three pairwise orthogonal STS is available when $3|\phi(n)$. In this case, there is a primitive third root of unity $m \in \mathbf{Z}_n$. Hill-climbing on a cyclic STS subject to orthogonality to its m and m^2 multiplicative shifts has worked for small n as well.

Using a square root of -1 and hill-climbing to find four orthogonal STS in two opposite orthogonal pairs has also worked, but produced only minor improvements to our earlier work. The examples below each took on the order of a few hours due to the large number of restarts needed.

Lemma 3.6 *$\sigma(n) \geq 4$ for $n \in \{73, 85, 97\}$.*

Proof: For each of these orders, we give a subgroup H of order 4 in $\mathbf{Z}_n^*$, followed by a list of $(n-1)/6$ base triples for which the cyclic systems generated under multiplication by H are pairwise orthogonal. Note in each case the collection of triples is disjoint. □

$n = 73$: $H = \{\pm 1, \pm 27\}$
$\{9,68,69\}$, $\{33,41,72\}$, $\{17,63,66\}$, $\{14,20,39\}$, $\{18,25,30\}$, $\{21,54,71\}$, $\{36,45,65\}$,
$\{12,23,38\}$, $\{22,57,67\}$, $\{5,26,42\}$, $\{40,44,62\}$, $\{28,58,60\}$

$n = 85$: $H = \{\pm 1, \pm 13\}$
$\{14,15,56\}$, $\{43,49,78\}$, $\{11,76,83\}$, $\{32,68,70\}$, $\{18,22,45\}$, $\{33,58,79\}$, $\{36,50,84\}$,
$\{7,31,47\}$, $\{19,29,37\}$, $\{41,60,69\}$, $\{3,25,57\}$, $\{16,27,42\}$, $\{9,12,64\}$, $\{21,26,38\}$

$n = 97$: $H = \{\pm 1, \pm 22\}$
$\{3,31,63\}$, $\{13,87,94\}$, $\{41,76,77\}$, $\{9,29,59\}$, $\{1,25,71\}$, $\{12,20,65\}$, $\{47,69,78\}$,
$\{7,24,66\}$, $\{21,36,40\}$, $\{57,67,70\}$, $\{10,89,95\}$, $\{5,39,53\}$, $\{22,27,48\}$, $\{2,35,60\}$,
$\{23,80,91\}$, $\{28,82,84\}$

3.3 Rotational automorphisms for orders 19 and 21

An STS of order $n = kt + 1$ with an automorphism consisting of a fixed point and t cycles of equal length on the remaining points is called *t-rotational*. The pointset $(\mathbf{Z}_k \times \mathbf{Z}_t) \cup \{\infty\}$ is typically used, with the second coordinate in the product represented with subscripts. The automorphism is then $(\infty)\prod_{0 \leq i < t}(0_i\ 1_i\ \ldots\ (k-1)_i)$. As with cyclic STS, a set of

base blocks is enough to specify the design, and it is often relatively fast to hill-climb to a t-rotational STS that is orthogonal to some orbit shift of itself. For $n = 19$ and 21, these orders fail to admit sets of more than two pairwise orthogonal STS by the earlier methods. So a range of techniques were attempted using 6-rotational and 4-rotational STS, respectively. We were successful in showing $\sigma(19) \geq 3$ by first hill-climbing to a 6-rotational STS that is orthogonal to a shift of its orbits, and then hill-climbing again to an orthogonal mate of both. This worked surprisingly fast but several different initial pairs had to be tried before a mate to both was found.

Proposition 3.7 *There exist three pairwise orthogonal STS of order 19.*

Proof: Below are the 19 base blocks for a 6-rotational STS orthogonal to its orbit shift defined by $x_i \mapsto x_{i+3}$, followed by base blocks for another 6-rotational STS orthogonal to each of these. Label the resulting designs IA, IB, and II. The orthogonality certificates follow in a table according to this labeling. □

$$\{0_5, 1_2, 2_1\}, \{\infty, 0_1, 2_0\}, \{0_2, 1_2, 1_0\}, \{\infty, 0_4, 2_2\}, \{0_0, 1_0, 0_5\}, \{0_4, 0_2, 2_1\}, \{0_1, 1_1, 0_5\},$$
$$\{0_5, 2_3, 2_0\}, \{0_4, 1_4, 2_0\}, \{0_4, 0_1, 0_0\}, \{0_5, 1_3, 2_2\}, \{0_5, 2_4, 0_2\}, \{\infty, 0_5, 0_3\},$$
$$\{0_3, 1_3, 2_4\}, \{0_3, 2_2, 2_1\}, \{0_4, 0_3, 1_1\}, \{0_3, 0_2, 2_0\}, \{0_3, 0_1, 1_0\}, \{0_5, 1_5, 1_4\}$$

$$\{0_5, 1_2, 1_1\}, \{0_5, 0_4, 2_2\}, \{0_5, 0_3, 1_0\}, \{0_3, 0_2, 1_1\}, \{0_2, 1_2, 2_0\}, \{0_1, 1_1, 1_5\}, \{\infty, 0_5, 0_2\},$$
$$\{0_5, 1_5, 2_3\}, \{0_3, 1_2, 0_1\}, \{0_3, 2_2, 2_0\}, \{0_4, 1_4, 1_2\}, \{0_4, 2_1, 1_0\}, \{0_5, 1_4, 0_0\},$$
$$\{0_4, 2_3, 1_1\}, \{\infty, 0_4, 0_1\}, \{0_5, 2_4, 2_0\}, \{0_0, 1_0, 0_1\}, \{\infty, 0_3, 0_0\}, \{0_3, 1_3, 0_4\}$$

c	$\Theta_{IB}\Theta_{IA}^{-1}(c)$	$\Theta_{IA}\Theta_{II}^{-1}(c)$	$\Theta_{IB}\Theta_{II}^{-1}(c)$
0_0	$1_3, 0_5, 0_3, 1_0, 2_3, 2_4, 0_1, 0_4, 1_2$	$\infty, 2_0, 0_1, 2_2, 1_5, 1_2, 0_3, 2_4, 0_5$	$1_5, 2_1, 0_3, 1_0, 2_2, 1_1, 2_0, 0_4, 1_4$
0_1	$2_2, 0_0, 2_4, 1_3, 0_3, 2_1, 1_5, 1_4, \infty$	$1_1, 1_0, 2_1, 1_2, 2_5, 0_4, 0_3, 2_2, 0_5$	$1_0, 0_3, 0_4, 0_2, 0_0, 1_5, \infty, 2_3, 2_1$
0_2	$0_3, 2_2, 2_5, 0_1, 2_1, 2_4, 1_5, 2_0, \infty$	$2_1, 0_5, 0_4, 2_2, 2_3, 0_3, 0_0, 1_2, 1_0$	$\infty, 2_0, 2_1, 0_5, 1_3, 1_1, 2_4, 0_4, 2_2$
0_3	$1_1, 0_4, 2_2, 1_2, 1_5, 2_3, 2_0, 1_0, \infty$	$0_0, 2_5, 2_4, 1_4, 1_2, 1_3, 1_1, 2_3, 0_1$	$0_4, 1_2, 2_3, 1_5, \infty, 2_5, 0_2, 0_0, 2_1$
0_4	$2_0, 0_5, 1_4, 0_1, 2_1, 1_5, 1_1, 1_2, 0_3$	$1_3, 0_1, 0_5, \infty, 0_0, 1_2, 2_0, 0_3, 2_4$	$1_4, 2_4, 1_5, 0_0, 1_3, 0_1, 2_5, 2_2, 0_2$
0_5	$1_4, 2_2, 1_0, 0_2, 1_5, 2_1, 2_3, 2_0, 1_2$	$2_3, \infty, 0_1, 2_5, 1_4, 0_2, 1_0, 2_4, 2_1$	$0_2, 2_4, 1_5, 1_3, 0_0, 2_5, 2_0, 0_1, 0_3$
∞	$0_0, 1_0, 2_0, 0_4, 1_4, 2_4, 0_5, 1_5, 2_5$	$0_0, 1_0, 2_0, 0_4, 1_4, 2_4, 0_5, 1_5, 2_5$	$0_3, 1_3, 2_3, 0_1, 1_1, 2_1, 0_2, 1_2, 2_2$

For $n = 21$, no success resulted from this same method using 4-rotational STS and an order two map on the orbits generating two of the three systems. Hill-climbing to a single STS orthogonal to each of its images under an order three shift of its orbits ((1)(234), say) has also produced no results. The frequency of partial designs encountered missing one base block seems to indicate no triple of pairwise orthogonal STS of order 21 exists having these additional properties.

4 Conclusion

In the first part of this paper we used finite fields to construct a rich collection of Steiner triple systems and then tested these for pairwise orthogonality. Using this method we found new lower bounds for $\sigma(q)$ for many prime powers $q < 500$. In the second part we employed several different variants of the hill-climbing algorithm for Steiner triple systems to get sets of orthogonal triple systems (in general) for non-prime power orders.

It is certainly the case that computing limitations, rather than nonexistence results, are the main obstacle in finding larger sets of mutually orthogonal STS. Without a doubt, higher quotient starters and hill-climbing can find still better bounds; however, there are memory constraints in storing orthogonailty graphs, and time constraints for probabilistic searching.

We conclude with a table of the best known lower bounds on $\sigma(n)$ for $n < 500$, with references (theorems, lemmas or tables in this paper or the original source). Entries in bold are exact. In the first two columns, all orders less than 90 are given. In the third column, only orders 1 (mod 6) are given. In the fourth and fifth columns, only prime-powers are listed.

n	$\sigma \geq$	Ref.	n	$\sigma \geq$	Ref.	n	$\sigma \geq$	Ref.	n	$\sigma \geq$	Ref.	n	$\sigma \geq$	Ref.
1	∞	$--$	45	3	3.1	91	3	3.5	181	7	2.5	343	9	2.2
3	**1**	$--$	49	4	2.4	97	4	3.6	193	3	2.4	349	9	2.5
7	**2**	$--$	51	3	3.1	103	8	2.2	199	9	2.2	361	5	2.4
9	**1**	[10]	55	3	3.5	109	6	2.5	211	14	2.2	367	11	2.2
13	**2**	[6]	57	3	3.1	115	3	3.5	223	12	2.2	373	9	2.5
15	**2**	[6]	61	5	2.4	121	5	2.4	229	7	2.5	379	11	2.2
19	3	3.7	63	3	3.1	127	6	[14]	241	4	2.4	397	10	2.5
21	2	[7]	67	8	2.2	133	3	3.5	271	9	2.2	409	6	2.4
25	4	2.6	69	3	3.1	139	8	[8]	277	8	2.5	421	10	2.5
27	3	3.1	73	4	3.6	145	3	3.5	283	11	2.2	433	4	2.4
31	6	[8]	75	3	3.1	151	14	2.2	289	3	2.4	439	14	2.2
33	3	3.1	79	4	2.2	157	8	[8]	307	10	2.2	457	6	2.4
37	3	3.5	81	3	3.1	163	9	2.2	313	5	2.4	463	15	2.2
39	3	3.1	85	4	3.6	169	4	2.4	331	11	2.2	487	16	2.2
43	4	[8]	87	2	[7]	175	3	3.5	337	4	2.4	499	17	2.2

Acknowledgments

The second author is grateful for the support of his NSERC PGS B award. The longer hill-climb searches were carried out on machines at the Center for Advanced Computing Research at the California Institute of Technology.

References

[1] C. J. Colbourn, P. B. Gibbons, R. Mathon, R. C. Mullin, and A. Rosa, *The spectrum of orthogonal Steiner triple systems*, Canad. J. Math. **46(2)** (1994), 239–252.

[2] J. H. Dinitz, *Room n-cubes of low order,* J. Austral. Math. Soc. (A) **36** (1984), 237–252.

[3] J. H. Dinitz, "Starters" in *The CRC Handbook of Combinatorial Designs*, (C. J. Colbourn and J. H. Dinitz, eds.) CRC Press, Inc., 1996, 467–473.

[4] J. H. Dinitz and D. R. Stinson, "Room squares and related designs," in *Contemporary Design Theory: A Collection of Surveys* (J. H. Dinitz and D. R. Stinson, eds) John Wiley & Sons, New York, 1992, 137–204.

[5] P. Dukes and E. Mendelsohn, *Skew-orthogonal Steiner triple systems,* J. Combin. Des. **7** (1999), 431-440.

[6] P. B. Gibbons, *A census of orthogonal Steiner triple systems of order 15*, Ann. Discrete Math. **26** (1985), 165–182.

[7] P. B. Gibbons and R. A. Mathon, *The use of hill-climbing to construct orthogonal Steiner triple systems*, J. Combin. Des. **1** (1993), 27–50.

[8] K. B. Gross, *On the maximal number of pairwise orthogonal Steiner triple systems,* J. Combin. Theory (A) **19** (1975), 256–263.

[9] R. C. Mullin and E. Nemeth, *On furnishing Room squares,* J. Combin. Theory **7** (1969), 266–272.

[10] R. C. Mullin and E. Nemeth, *On the nonexistence of orthogonal Steiner triple systems of order 9,* Canad. Math. Bull. **13** (1970), 131–134.

[11] C. D. O'Shaughnessey, *A Room design of order 14*, Canad. Math. Bull. **11** (1968), 191–194.

[12] S. Schreiber, *Cyclical Steiner triple systems orthogonal to their opposites,* Discrete Math. **77** (1989), 281–284.

[13] W. D. Wallis, *Combinatorial Designs*, Dekker **118**, New York, 1988.

[14] L. Zhu, *A construction for orthogonal Steiner triple systems,* Ars Combin. **9** (1980), 253–262.