The Existence of Resolvable Steiner Quadruple Systems

ALAN HARTMAN

IBM - Israel Scientific Centre, Technion City, Haifa 32000, Israel

Communicated by Haim Hanani
Received June 26, 1986

A Steiner quadruple system of order \( v \) is a set \( X \) of cardinality \( v \), and a set \( Q \), of 4-subsets of \( X \), called blocks, with the property that every 3-subset of \( X \) is contained in a unique block. A Steiner quadruple system is resolvable if \( Q \) can be partitioned into parallel classes (partitions of \( X \)). A necessary condition for the existence of a resolvable Steiner quadruple system is that \( v \equiv 4 \) or \( 8 \) (mod 12). In this paper we show that this condition is also sufficient for all values of \( v \), with 24 possible exceptions.

1.0. INTRODUCTION

A Steiner quadruple system of order \( v \), denoted \( \text{SQS}(v) \), is an ordered pair \((X, Q)\), where \( X \) is a non-empty set of cardinality \( v \), and \( Q \) is a set of 4-subsets of \( X \), called blocks, such that every 3-subset of \( X \) is contained in a unique block.

In 1960 Hanani [7] proved that an \( \text{SQS}(v) \) exists if and only if \( v \equiv 2 \) or 4 (mod 6) or \( v \equiv 1 \).

Let \( r(v) = \frac{(v - 1)(v - 2)}{6} \) be the number of blocks in an \( \text{SQS}(v) \) which contain a fixed point of \( X \). An \( \text{SQS}(v) \) is resolvable, denoted \( \text{RSQS}(v) \), if there exists a partition \( \hat{P}_i = \{ P_i : i \in I \} \) of the block set \( Q \), indexed by a set \( I \) of cardinality \( r(v) \), with the property that each \( P_i \) is a partition of the point set \( X \) into parts of size four. If \( Q \) is non-empty it follows that \( v \equiv 0 \) (mod 4) and hence a necessary condition for the existence of an \( \text{RSQS}(v) \) is that \( v \equiv 4 \) or \( 8 \) (mod 12) or \( v = 1 \) or 2. A positive integer satisfying this condition will be called admissible. In this paper, we show that this condition is also sufficient with the possible exception of twenty-four values of \( v \) which are listed in the Appendix.

The history of the existence problem for resolvable combinatorial designs begins with Kirkman's famous "schoolgirl problem" [14], posed in 1847. The general problem is to determine necessary and sufficient conditions on \( v \) for the existence of resolvable \( t-(v, k, \lambda) \) designs. The problem has been solved for very few values of the block size \( k \) and index \( \lambda \) parameters.
These solutions may be found in \([6] (k, \lambda) = (3, 1), (4, 1), [8] (k, \lambda) = (3, 2), \) and \([1] (k, \lambda) = (4, 3), (6, 10). (Note that the references given are not necessarily the first proofs of these results.) All of these papers deal with combinatorial designs of dimension \((t)\) two. Ray-Chaudhuri and Wilson \([17]\) and Lu \([16]\) have also shown the existence of a constant \(c(k, \lambda)\) such that the trivial necessary conditions for the existence of resolvable \(2-(v, k, 1)\) designs are sufficient for all \(v \geq c(k, \lambda)\). This paper constitutes the first effective determination of necessary and sufficient conditions for the existence of a family of resolvable designs of dimension three.

Since the nineteenth century it has been known that the planes of the affine geometry of dimension \(n\) over \(GF(2)\) form the block set of an SQS\((2^n)\). The natural parallelism forms a partition of the planes which is a resolution. This motivates the use of the term parallel class for the parts \(P_i\) of the resolution partition \(\hat{P}_i\). In 1978 Booth, Greenwell, and Lindner \([2, 5]\) constructed an RSQS\((20)\) and an RSQS\((28)\), thus providing the first examples with \(v\) not a power of two. Knowledge of the existence of RSQS\((v)\) for small values of \(v\) was expanded by the author's papers \([9, 10]\). The main recursive construction for RSQS used in this paper was first given in \([11]\). To state this result precisely we need the following definition.

Let \((X, Q, \hat{P}_j)\) be an RSQS\((V)\) and let \((x, q, \hat{p}_j)\) be an RSQS\((v)\) such that \(x \in X, q \in Q, J \subseteq I, \) and \(p_j \subseteq P_j\) for all \(j \in J.\) Then \((X, Q, \hat{P}_j)\) is an RSQS\((V)\) with a resolvable subsystem of order \(v\), and will be denoted by RSQS\((V[v])\). For all \(V \geq 4\) an RSQS\((V)\) is also an RSQS\((V[v])\), where \(v \in \{1, 2, 4\}\). Using the substitution property for subdesigns, the reader can easily verify that if there exists an RSQS\((V[v])\) and an RSQS\((v[s])\), then there exists an RSQS\((V[v])\).

The main result of this paper is proved using the following theorem.

**Theorem 1.1** (Hartman \([11]\)). *If there exists an RSQS\((V[v])\) and \(V \equiv 2v \pmod{12}\) then there exists an RSQS\((3V - 2v[V])\).*

As a corollary we obtain

**Theorem 1.2** (Hartman \([12]\)). *If there exists a constant \(k\), such that for all admissible \(V\) in the range \(k \leq V < 3k\) there exists an RSQS\((V[64])\) then for all admissible \(V > k\) there exists an RSQS\((V[64])\).*

**Proof.** We first note that the existence of an RSQS\((V[2^n])\) implies the existence of an RSQS\((V[2^m])\) for all \(m \leq n\), since the affine geometry of dimension \(n\) contains subsystems of dimension \(m\), and the parallelism respects these subsystems. We proceed by induction, if \(V \geq 3k\) is admissible then write \(V = 3v - 2m\), where \(m = 6, 1, 2, 5, 4, 3\) when \(V = 4, 8, 16, 20, 28, 32 \pmod{36}\), respectively. It is a simple matter to check that \(k \leq v < V,\)
$v$ is admissible, and $v \equiv 2.2^m \pmod{12}$, so we may apply the induction hypothesis, Theorem 1.1, and the substitution property to give the result.

In the remainder of this paper we prove the existence of the constant $k$ hypothesized in Theorem 1.2. In fact we show that $128 \leq k \leq 6364$.

In Section 2 we show that the author's tripling construction [13] can be adapted to preserve resolvability in some cases. Specifically we prove

**THEOREM 2.1.** If there exists an RSQS($V[v]$) with $V \equiv v \pmod{12}$ and $14v \geq 5V$ then there exists an RSQS($3V - 2v[v]$).

In Section 3 we describe the methods used to construct RSQS($V[v]$) for some small values of $V$. The basic techniques are described in more detail in [9, 10, and 11]. In this paper we discuss the hill-climbing strategy used by the computer algorithms which generated the designs given in the Appendix. We also discuss the computer program used to calculate the upper bound on the constant $k$ of Theorem 1.2.

2.0. A RESOLUTION PRESERVING TRIPLING CONSTRUCTION

In [13] a tripling construction for SQS is given which has the following form. If there exists an SQS($v$) with a subdesign of order $s \equiv v \pmod{6}$ then there exists an SQS($3v - 2s$) with a subdesign of order $v$. In this section we show that if the input system is resolvable, and if the subsystem is large enough, then the output system has a resolution. The exact statement of this result is given below. In [11] a similar construction with the restriction that $2s \equiv v \pmod{6}$ was shown to preserve resolvability in all cases. Concise accounts of both the constructions of [11 and 13] may be found in [15].

**THEOREM 2.1.** If there exists an RSQS($v[s]$) with $v \equiv s \pmod{12}$ and $14s \geq 5v$ then there exists an RSQS($3v - 2s[v]$).

The theorem is trivially true when $s = 1$ or 2 so henceforth we assume $s \equiv 4$ or 8 $\pmod{12}$. It is almost certain that the truth of the theorem would be unaffected by omitting the condition $14s \geq 5v$, however the construction would undoubtedly be considerably more complicated. Before giving the proof of the theorem we need the following definitions and notation. Define $I_m = \{0, 1, \ldots, m - 1\}$. Let $Z_m$ denote the cyclic group on $I_m$ under addition modulo $m$. For $x \in Z_m$ we define $|x|$ by

$$|x| = \begin{cases} x & \text{if } 0 \leq x < m/2, \\ -x & \text{otherwise.} \end{cases}$$
Let $m \geq 2$ be an integer and let $L$ be a non-empty subset of \{1, 2, ..., \ceil{m/2}\}, where \ceil{x} is the greatest integer $\leq x$.

The cyclic graph $G(m, L)$ is defined to be the graph with vertex set $\mathbb{Z}_m$ and edge set $E$ defined by $\{x, y\} \in E$ if and only if $|y - x| \in L$. The following result is due to Stern and Lenz [18].

**Theorem 2.2.** A cyclic graph $G(m, L)$ has a 1-factorization if and only if $m$ is even and $m/\gcd(i, m)$ is even for some $i \in L$.

We now proceed with the proof of Theorem 2.1. Let $s \equiv 4$ or 8 (mod 12), and let $v = 12n + s$, where $14s \geq 5v$. Now let $(X, Q, \tilde{P}_1)$ be an RSQS($v[3]$), with resolvable subsystem $(Y, S, \tilde{R}_1)$. For definiteness we take $Y = \{\infty_0, \infty_1, \ldots, \infty_{s-1}\}$, $X = Y \cup Z_{12n}$, $I = I_{r(v)}$, and $J = I_{r(s)}$.

We now construct an RSQS($3v - 2s[3]$) $(X', Q', \tilde{P}'_k)$ as follows. Let

$$X' = Y \cup (Z_{12n} \times Z_3).$$

We define the block set $Q'$ implicitly by constructing the resolution $\tilde{P}'_k$, and letting $Q'$ be the union of all the parallel classes. In order to construct the resolution we need the following definitions.

For each $i \in Z_3$ we define the embedding $\lambda_i : X \to X'$ by

$$\lambda_i(x) = \begin{cases} x & \text{if } x \in Y, \\ (x, i) & \text{if } x \in Z_{12n}. \end{cases}$$

In the sequel we shall write $x_i$ for the ordered pair $(x, i) \in Z_{12n} \times Z_3$.

Another major ingredient in the construction of $\tilde{P}'_k$ is the set $H$ of pairs of members of $Z_{12n}$ defined below. Let $h = (12n - s)/2$. Since $s$ is divisible by 4, and $14s \geq 5v = 5(12n + s)$, we deduce that $h$ is even and $h \leq 8n/3$. Now consider

$$H^*_1 = \{9n - i, 9n - 3 + i]: 2 \leq i \leq 3n + 1, i \not\equiv 0 \pmod{3}\}$$

$$H^*_2 = \{3n - i, 3n + i]: 1 \leq i \leq 3n - 2, i \not\equiv 0 \pmod{3}\}.$$

Note that $|H^*_1| = 2n$ and $|H^*_2| = 2n - 1$. Let $H_i$ be any subset of $H^*_i$ of cardinality $h/2$ ($i = 1, 2$), and let $H = H_1 \cup H_2$.

The set $H$ has been chosen to have the following properties:

1. $|H| = h = (12n - s)/2 \leq 8n/3$.
2. The pairs in $H$ are disjoint, so if $VH = \bigcup H$ then $|VH| = 2h$.
3. The distances between members of $H$ are distinct, so if $LH = \{|y - x|: \{x, y\} \in H\}$ then $|LH| = h$.
4. The distances between members of $H_1$ are odd.
5. For all $\{x, y\} \in H$ we have $\{x, y\} \equiv \{1, 2\} \pmod{3}$.
Since $6n \notin LH$ and $|H| = h$ the graph $G(12n, \{1, 2, ..., 6n\} - LH)$ has a one factorization $F_1, F_2, ..., F_{12n-2h-1}$ by Theorem 2.2.

We now begin the construction of $P'_K$. The first $r(s)$ parallel classes are defined by

$$P'_j = \{ \{\lambda_i(x), \lambda_i(y), \lambda_i(z), \lambda_i(t)\}: i \in Z_3, \{x, y, z, t\} \in P_j \}, \quad j \in I_{r(s)}, \quad (A)$$

The next $3(r(v) - r(s))$ parallel classes $P'_{ij}, i \in Z_3$ and $j \in I_{r(v)} - I_{r(s)}$, are defined to contain the set of $v/4$ blocks

$$\{ \{\lambda_i(x), \lambda_i(y), \lambda_i(z), \lambda_i(t)\}: \{x, y, z, t\} \in P_j \}, \quad (A)$$

and $6n$ additional blocks of the form $\{x_{i+1}, y_{i+1}, z_{i+2}, t_{i+2}\}$ constructed as follows. Let $I_{m,k}$ be a latin square of side $6n$ over the symbol set $\{1, 2, ..., 6n\}$. The set of blocks

$$\{x_{i+1}, y_{i+1}, z_{i+2}, t_{i+2}\}:
$$

$$\{x, y\} \text{ is the } m\text{th member of } F_{u}, \{z, t\} \text{ is the } l_{m,k}\text{th member of } F_{u}, m = 1, 2, ..., 6n \}
$$

is a partition of $(12n \times \{i + 1, i + 2\}$). Allowing $u$ to range over $1, 2, ..., 12n - 2h - 1$, and $k$ to range over $1, 2, ..., 6n$, gives us completions of the parallel classes $P'_{ij}$ for $j = r(s), r(s) + 1, ..., r(s) + 6n(12n - 2h - 1) - 1$. Now $r(v) - r(s) = 6n(12n - 2h - 1) + 4nh$. The remaining $4nh$ parallel classes $P'_{ij}$ with $i$ fixed are completed by the set of $6n$ blocks

$$\{(a + x)_{i+1}, (a + y)_{i+1}, (a + 3e - x)_{i+2}, (a + 3e - y)_{i+2}\}:
$$

$$a \in Z_{12n}, a \equiv \delta \text{ (mod 2)} \}. \quad (x_2)$$

Allowing $\delta$ to range over $Z_2$, $e$ to range over $Z_{4n}$, and $\{x, y\}$ to range over $H_1$, gives $4nh$ distinct completions. We use the fact that differences between members of $H_1$ are odd to show that the above set of blocks is indeed a partition of $Z_{12n} \times \{i + 1, i + 2\}$.

The number of parallel classes remaining to be constructed is $r(3v - 2s) - 3r(v) + 2r(s) = 12n.4n.3$, accordingly we label the remaining parallel classes as $P'_{a,e,i}$ with $a \in Z_{12n}, i \in Z_{4n}$, and $i \in Z_3$. The following set of $h$ blocks are in $P'_{a,e,i}$:

$$\{(a + 3d)_{i+1}, (a + 3e - 3d)_{i+1}, (x - 2a - 3e)_{i+2}, (y - 2a - 3e)_{i+2}\}:
$$

$$d \in I_h, \{x, y\} \text{ is the } d\text{th member of } H \}. \quad (x_1)$$

The following set of $h/2$ blocks are in $P'_{a,e,i}$:

$$\{(a + x)_{i+1}, (a + y)_{i+1}, (a + 3e - x)_{i+1}, (a + 3e - y)_{i+1}\}: \{x, y\} \in H_2 \}. \quad (x_2)$$
The remaining $s$ blocks in $P_{a,s,i}'$ are a set of the form
\[ \{ (a + g(i, k), (a + 3s - g(i, k)), (f(k) - 2a - 3s), i+1, a+1) : k \in I_s \}. \] (A)

The function $f(k)$ is an arbitrary fixed bijection from $I_s$ to $Z_{12n} - VH$. This guarantees that every point of $Z_{12n} \times \{ i + 2 \}$ is contained in a block of $P_{a,s,i}'$. Similarly the functions $g(i, k)$ (with $i$ fixed) must be constructed to be bijections from $I_s$ to $Z_{12n} - \{ 3d: d \in I_h \} \cup VH_2$. There is, however, another restriction on the values of $g(i, k)$. The blocks of the form (A) are required to cover all triples of the form $x_0, y_1, z_2$ where $x + y + z \equiv f(k)$ (mod $12n$). The case analysis given below shows that this requires $g(i, k)$ to take three distinct values modulo 3 whenever $f(k) \equiv 0$ (mod 3). When $f(k) \not\equiv 0$ (mod 3), we use two methods for assigning values to $g(i, k)$:

\[ g(0, k) \equiv g(1, k) \equiv g(2, k) \pmod{3} \] (A)

\[ g(0, k) = f(k), \quad g(1, k) \equiv 0, \quad g(2, k) \equiv -f(k) \pmod{3}. \] (B)

We use the following schemes to define $g(i, k)$:

(S0) Let $f(k_0), f(k_1), f(k_2)$ be three distinct values all congruent to 0 (mod 3), and let $b_i \equiv i$ (mod 3), $i \in Z_3$ be three members of the range of $g(i, k)$. Define $g(i, k_j) = b_i + j$, i.e.,

\[ g(0, k_0) = b_0, \quad g(1, k_0) = b_1, \quad g(2, k_0) = b_2, \]

\[ g(0, k_1) = b_1, \quad g(1, k_1) = b_2, \quad g(2, k_1) = b_0, \]

\[ g(0, k_2) = b_2, \quad g(1, k_2) = b_0, \quad g(2, k_2) = b_1. \]

(S1) Let $f(k_0), f(k_1)$ be two distinct values both congruent to 0 (mod 3), and let $f(k_2)$ be congruent to 1 or 2 (mod 3). Let $b_i$ be defined as in (S0). Define $g(i, k_j)$ by

\[ g(0, k_0) = b_{-f(k_2)}, \quad g(1, k_0) = b_{f(k_2)}, \quad g(2, k_0) = b_0 \]

\[ g(0, k_1) = b_0, \quad g(1, k_1) = b_{-f(k_2)}, \quad g(2, k_1) = b_{f(k_2)} \]

\[ g(0, k_2) = b_{f(k_2)}, \quad g(1, k_2) = b_0, \quad g(2, k_2) = b_{-f(k_2)} \]

cf. (B) above, with subscripts taken modulo 3 throughout.

(S2) Let $f(k) \not\equiv 0$ (mod 3), and let $b$ be in the range of $g(i, \cdot)$. Define $g(i, k) = b$ for all $i \in Z_3$, cf. (A).

To show that we can meet all the requirements on $g(i, k)$ we note that, the range of $f(k)$ contains $4n$ numbers congruent to 0 (mod 3), $4n - h$ numbers congruent to 1 (mod 3), and $4n - h$ numbers congruent to 2 (mod 3). The range of $g(i, k)$ contains $4n - h$ numbers congruent to 0 (mod 3),
4n - h/2 numbers congruent to 1 (mod 3), and 4n - h/2 numbers congruent to 2 (mod 3). Now, to construct the functions g(i, k), first partition the 4n members of the range of f which are zero mod 3 into parts of size 3, and 0, 1, or 2 parts of size 2 (according as n ≡ 0, 2, or 1 (mod 3)). The number of parts in this partition is \(\lceil (4n + 2)/3 \rceil\). Since h ≤ 8n/3, we can choose \(\lceil (4n + 2)/3 \rceil\) disjoint triples \(b_0, b_1, b_2\) from the range of g and apply schemes (S0) and (S1) to the parts of size 3 and 2, respectively. Having defined g(i, k) for all k such that f(k) ≡ 0 (mod 3), and at most 2 values such that f(k) ≢ 0 (mod 3), it is possible to extend the definition for all other values of k, using scheme (S2), so that each g(i, ·) is a bijection. We give two examples.

**Example 2.1.** n = 1, s = 8, h = 2, \(H_1 = \{7, 8\}\), \(H_2 = \{2, 4\}\).

<table>
<thead>
<tr>
<th>k</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>(-I_8)</th>
</tr>
</thead>
<tbody>
<tr>
<td>f(k)</td>
<td>0</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>9</td>
<td>5</td>
<td>10</td>
<td>11</td>
<td>(Z_{12} - {2, 4, 7, 8})</td>
</tr>
<tr>
<td>g(0, k)</td>
<td>5</td>
<td>6</td>
<td>1</td>
<td>7</td>
<td>9</td>
<td>8</td>
<td>10</td>
<td>11</td>
<td>(Z_{12} - {0, 2, 3, 4})</td>
</tr>
<tr>
<td>g(1, k)</td>
<td>1</td>
<td>5</td>
<td>6</td>
<td>8</td>
<td>7</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>(Z_{12} - {0, 2, 3, 4})</td>
</tr>
<tr>
<td>g(2, k)</td>
<td>6</td>
<td>1</td>
<td>5</td>
<td>9</td>
<td>8</td>
<td>7</td>
<td>10</td>
<td>11</td>
<td>(Z_{12} - {0, 2, 3, 4})</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>S1</th>
<th>S1</th>
<th>S2</th>
<th>S2</th>
</tr>
</thead>
</table>

**Example 2.2.** n = 2, s = 20, h = 2, \(H_1 = \{16, 17\}\), \(H_2 = \{5, 7\}\).

\(\text{ran}(f) = Z_{24} - \{5, 7, 16, 17\}\) \(\text{ran}(g(i, \cdot)) = Z_{24} - \{0, 3, 5, 7\}\).

| k  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| f(k) | 0 | 3 | 6 | 9 | 12 | 15 | 18 | 21 | 1 | 2 | 4 | 8 | 10 | 11 | 13 | 14 | 19 | 20 | 22 | 23 |
| g(0, k) | 6 | 1 | 2 | 9 | 4 | 8 | 11 | 12 | 10 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| g(1, k) | 1 | 2 | 6 | 4 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| g(2, k) | 2 | 6 | 1 | 8 | 9 | 4 | 12 | 10 | 11 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |

<table>
<thead>
<tr>
<th></th>
<th>S0</th>
<th>S0</th>
<th>S1</th>
<th>S1</th>
<th>S2</th>
<th>S2</th>
<th>S2</th>
<th>S2</th>
<th>S2</th>
<th>S2</th>
<th>S2</th>
<th>S2</th>
<th>S2</th>
<th>S2</th>
</tr>
</thead>
</table>

To complete the proof of Theorem 2.1, it remains to show that every 3-subset of \(X\) is contained in some block defined above. To facilitate this discussion we classify the 3-subsets into the four mutually exclusive classes T1, T2, T3, and T4 defined below.

T1 consists of all 3-subsets in the image of \(X\) under \(\lambda_i\) for some \(i\). This class includes all 3-subsets of the forms \(\{\infty_j, \infty_k, \infty_m\}\), \(\{\infty_j, \infty_k, x_i\}\), \(\{\infty_j, x_i, y_i\}\), and \(\{x_i, y_i, z_i\}\). Each T1-triple is contained in a unique block defined in the equations marked (A).

T2 triples have the form \(\{\infty_k, x_i, y_{i+1}\}\). Each T2-triple is contained in a unique block defined by Eq. (A) as follows. If \(f(k) \equiv 0 \pmod{3}\) then by
the construction of $g$ there exists a unique $j$ such that $g(j, k) \equiv y - x \pmod{3}$. If $i = j$ then Eqs. (2.1) have a unique solution for $a \in \mathbb{Z}_{12n}$ and $\varepsilon \in \mathbb{Z}_{4n}$:

$$x = a + g(j, k),$$
$$y = a + 3\varepsilon - g(j, k).$$

(2.1)

If $i = j + 1$ then Eqs. (2.2) have a unique solution for $a \in \mathbb{Z}_{12n}$ and $\varepsilon \in \mathbb{Z}_{4n}$:

$$x = a + 3\varepsilon - g(j, k),$$
$$y = f(k) - 2a - 3\varepsilon.$$

(2.2)

If $i = j + 2$ then Eqs. (2.3) have a unique solution for $a \in \mathbb{Z}_{12n}$ and $\varepsilon \in \mathbb{Z}_{4n}$:

$$x = f(k) - 2a - 3\varepsilon,$$
$$y = a + g(j, k).$$

(2.3)

If $f(k) \not\equiv 0 \pmod{3}$ and $g(j, k)$ has been constructed by scheme (A), i.e., $g(0, k) \equiv g(1, k) \equiv g(2, k) \pmod{3}$, then Eqs. (2.1) have a unique solution when $y - x \equiv g(j, k) \pmod{3}$, Eqs. (2.2) have a unique solution when $y - x \equiv g(j, k) + f(k) \pmod{3}$, and Eqs. (2.3) have a unique solution when $y - x \equiv g(j, k) - f(k) \pmod{3}$.

If $f(k) \not\equiv 0 \pmod{3}$ and $g(j, k)$ has been constructed by scheme (B), i.e., $g(0, k) \equiv f(k)$, $g(1, k) \equiv 0$, $g(2, k) \equiv -f(k) \pmod{3}$ then Eqs. (2.1) with $j = i$ have a unique solution when

$$y - x \equiv f(k) \pmod{3} \quad {\text{and}} \quad i = 0,$$
$$y - x \equiv 0 \pmod{3} \quad {\text{and}} \quad i = 1,$$
$$y - x \equiv -f(k) \pmod{3} \quad {\text{and}} \quad i = 2;$$

Eqs. (2.2) with $j + 1 = i$ have a unique solution when

$$y - x \equiv 0 \pmod{3} \quad {\text{and}} \quad i = 0,$$
$$y - x \equiv -f(k) \pmod{3} \quad {\text{and}} \quad i = 1,$$
$$y - x \equiv f(k) \pmod{3} \quad {\text{and}} \quad i = 2;$$

Eqs. (2.3) with $j + 2 = i$ have a unique solution when

$$y - x \equiv -f(k) \pmod{3} \quad {\text{and}} \quad i = 0,$$
$$y - x \equiv f(k) \pmod{3} \quad {\text{and}} \quad i = 1,$$
$$y - x \equiv 0 \pmod{3} \quad {\text{and}} \quad i = 2.
T3 triples have the form \( \{x_i, y_i, z_{i\pm 1}\} \) and are contained in a unique block defined by Eq. (\( \Phi \)) when \( |y - x| \notin LH \), by the properties of the 1-factorization \( F_1, F_2, \ldots \) and the latin square \( l_{m,k} \). When \( |y - x| \in LH \), and \( x + y + z \equiv 0 \pmod{3} \) then the triple \( \{x_i, y_i, z_{i\pm 1}\} \) is contained in a unique block defined by Eq. (\( \chi_1 \)), since the pair \( \{b, c\} \in H \) and its ordinal \( d \) are uniquely determined by the equation \( y - x = c - b \). (Here we use the fact that distances between members of \( H \) are distinct.) Now the following equations have a unique solution for \( a \in \mathbb{Z}_{2n} \) and \( \varepsilon \in \mathbb{Z}_{4n} \):

\[
\begin{align*}
x &= b - 2a - 3\varepsilon \\
y &= c - 2a - 3\varepsilon \\
z &= a + 3d \quad \text{(for } z_{i+1} \text{)} \\
z &= a + 3\varepsilon - 3d \quad \text{(for } z_{i-1} \text{)}.
\end{align*}
\]

When \( |y - x| \in LH \), and \( x + y + z \not\equiv 0 \pmod{3} \) then the triple \( \{x_i, y_i, z_{i\pm 1}\} \) is contained in a unique block defined by the equations (\( \chi_2 \)) since the pair \( \{b, c\} \in H \) is uniquely determined by the equation \( y - x = c - b \). Here we use the property that \( \{b, c\} \equiv \{1, 2\} \pmod{3} \). When \( x + y + z \equiv b \pmod{3} \) and the subscript of \( z \) is \( i + 1 \) then the following equations can be uniquely solved for \( a \) and \( \varepsilon \):

\[
\begin{align*}
x &= a + b \\
y &= a + c \\
z &= a + 3\varepsilon - c.
\end{align*}
\]

The three other cases (\( x + y + z \equiv b \) and \( z_{i-1} \)), (\( x + y + z \equiv c \) and \( z_{i+1} \)), and (\( x + y + z \equiv c \) and \( z_{i-1} \)) are similar.

T4 triples have the form \( \{x_0, y_1, z_2\} \) and are contained in a unique block defined by Eq. (\( A \)) when \( x + y + z \notin VH \), since the definition of \( f(k) \) guarantees a unique solution for \( k \) of the equation \( f(k) = x + y + z \). The block containing \( \{x_0, y_1, z_2\} \) is then found by the algorithm given above for the block containing \( \{\infty_k, x_0, y_1\} \). If however, \( x + y + z = b \in VH \) then the triple is contained in a unique block defined by Eq. (\( \chi_1 \)). Here again we use the fact that \( b \not\equiv 0 \pmod{3} \), which implies that precisely two of \( x, y, \) and \( z \) are congruent modulo 3. If \( x \equiv y \pmod{3} \) then the equations

\[
\begin{align*}
x &= a + 3d \\
y &= a + 3\varepsilon - 3d \\
z &= b - 2a - 3\varepsilon.
\end{align*}
\]
have a unique solution for \( a \) and \( \varepsilon \). (Note that \( d \) is uniquely determined by the value of \( b \).) The other two cases \( y \equiv z \) and \( z \equiv x \) are similar.

This completes the proof that \((X', Q', \hat{P}_k')\) where

\[
K = I_{r(s)} \cup (Z_3 \times (I_{r(v)} - I_{r(s)}) \cup (Z_{12n} \times Z_{4n} \times Z_3)
\]

is an RSQS\((3v - 2s)\). It remains to show that the system contains a resolvable subsystem of order \( v \). From the construction of the blocks \((A)\) it is clear that \((\lambda_0(X), \lambda_0(Q), \lambda_0(\hat{P}_1), K_0)\) is a resolvable subsystem of order \( v \) with resolution indexed by \( K_0 = I_{r(s)} \cup (\{0\} \times (I_{r(v)} - I_{r(s)})\).

An immediate application of Theorem 2.1 to the existence problem for RSQS is the construction of an RSQS\((92)\) by applying the theorem twice to the RSQS\((20[8])\) constructed in [11]. Prior to this paper the order 92 was the smallest order \( v \) for which the existence of an RSQS\((v)\) was in doubt.

3.0. The Basis for the Induction

In this section we discuss the computations involved in determining an upper bound on the constant \( k \) with the property that for all admissible \( v \in [k, 3k) \), there exists an RSQS\((v[64])\). A necessary condition for the existence of an SQS\((v)\) with a subsystem of order \( s \) is that \( v \geq 2s \) or \( v = s \), which implies the lower bound \( k \geq 128 \).

The first step in the computation of an upper bound is the determination of some small orders \( v \) and \( s \) for which an RSQS\((v[s])\) exists. The next step is to apply the full power of the three recursive constructions given in Theorems 1.1, 2.1, and 3.1 (see below) to all the initial designs and their descendants. The list of resolvable subdesigns is updated using the replacement property for subdesigns mentioned in Section 1. The third recursive construction is a variant of the standard doubling construction for Steiner quadruple systems and is slightly stronger than a similar result of Greenwell and Lindner [5].

**Theorem 3.1** (Hartman [11]). If there exists an RSQS\((v[s])\) then there exists an RSQS\((2v[2s])\) and an RSQS\((2v[v])\).

The basic data structure for the computations is a \( 4m \times m \) array, \( rsqs(v, s) \) of bits, initialized with the values

\[
rsqs(v, s) = \begin{cases} 
1 & \text{if an RSQS}(v[s]) \text{ exists} \\
0 & \text{otherwise} 
\end{cases}
\]
The algorithm for computing the output of the recursive constructions given an initial list \( L \) of pairs \((v, s)\) such that an \( \text{RSQS}(v[s]) \) is known to exist is given in Fig. 1.

A certain amount of care is necessary in implementing the algorithm to avoid attempts to set bits outside the domain of the array \( \text{rsqs} \). The main difficulty in implementation, however, arises due to the large size of \( \text{rsqs} \). To compute the upper bound for \( k \) we needed to run the program with \( m \sim 5000 \) thus requiring \( 2 \times 10^8 \) bits of storage in a simple minded realization of the array. An efficient data structure is achieved by allocating space only for admissible pairs \((v, s)\) (i.e., \( v \equiv 4 \text{ or } 8 \mod 12 \) \( s \equiv 4 \text{ or } 8 \mod 12 \) or \( s = 2 \) and \( s \leq v/2 \)) in the range \( 4 \leq v \leq 2m \), and only one bit

\[
(* \text{initialize} *)
\]
BEGIN
\text{rsqs}(\cdot, \cdot) := 0
FOR \((u, s)\) in \( L \) DO \text{rsqs}(u, s) := 1
(* apply the recursive constructions *)
FOR \( v := 4 \) TO \( 2m \) DO
BEGIN
IF \text{rsqs}(v, 2) THEN
(* apply Theorem 3.1 *)
BEGIN
\text{rsqs}(2u, u) := 1
replace \((2u, u)\)
FOR \( s := 2 \) TO \( u/2 \) DO IF \text{rsqs}(v, s) THEN \text{rsqs}(2v, 2s) := 1
END
FOR \( s := 2 \) TO \( u/2 \) DO IF \text{rsqs}(v, s) \& \( v \equiv 2s \mod 12 \) THEN
(* apply Theorem 1.1 *)
BEGIN
\text{rsqs}(3v - 2s, u) := 1
replace \((3v - 2s, u)\)
END
FOR \( s := 5v/14 \) TO \( u/2 \) DO IF \text{rsqs}(v, s) \& \( v \equiv s \mod 12 \) THEN
(* apply Theorem 2.1 *)
BEGIN
\text{rsqs}(3v - 2s, v) := 1
replace \((3v - 2s, v)\)
END
END
\]
PROCEDURE replace \((v, s)\)
(* replacement of subdesigns *)
BEGIN
FOR \( t := 2 \) TO \( s/2 \) DO IF \text{rsqs}(s, t) THEN \text{rsqs}(v, t) := 1
END

Fig. 1. Algorithm for computing an upper bound on \( k \).
representing \( rsqs(v, 64) \) in the range \( 2m < v \leq 4m \). More space saving is possible by noting that the contents of the row \( rsqs(v, 1) \) may be output after the row has been used for the recursive constructions, and the space reused for rows of the array with index greater than \( 3v \).

The program was run with an input list comprising the 40 pairs \((v, s)\) described below and \( m = 4800 \), and produced the following results. For all admissible \( 4 \leq v \leq 6364 \), with the 24 exceptions listed in the Appendix, there exists an RSQS\((v)\). For all admissible \( 6364 < v < 19092 \) there exists an RSQS\((v[64])\). Hence Theorem 1.2 implies

**Theorem 3.2.** For all \( v \equiv 4 \) or \( 8 \pmod{12} \) with 24 possible exceptions there exists an RSQS\((v)\).

The list of 40 pairs \((v, s)\) such that an RSQS\((v[s])\) is known to exist is broken up into 3 classes:

- \( L_1 = \{(4,2), (20,2), (20,4), (20,8), (28,2), (28,4), (28,8), (52,16)\} \)
- \( L_2 = \{(v,2), (v,4) : v = 164, 344, 524, 740, 812, 860, 920\} \)
- \( L_3 = \{(v,2), (v,4) : v = 76, 172, 508, 596, 892, 1084, 4252\} \cup \{(76,8)\}. \)

The design on 4 points is trivial; the designs on 20 and 28 points are constructed in [2, 5, and 11]; the designs on 164 and 344 points are constructed in [9]. The remaining designs for pairs in \( L_2 \) are constructed as follows.

**The \( q+1 \) Construction** (Hartman [9]). Let \( q \) be a prime power with \( q \equiv 7 \pmod{12} \), and let \( g \) be the unique cube root of unity in \( GF(q) \) such that \( g - 1 \) is a nonzero quadratic residue. Carmichael [3] has shown that the PSL\((2, q)\) orbit of the quadruple \( \{\infty, 0, 1, g+1\} \) is the block set of an SQS\((q+1)\) with point set \( GF(q) \cup \{\infty\} \).

Let \( \omega \) be a generator of the multiplicative subgroup of \( GF(q) \), then the stabilizer of \( \infty \) in PSL\((2, q)\) is the group \( \Gamma \) of transformations

\[
\Gamma = \{ \gamma(x) = \omega^{2k}x + c : 0 \leq k < (q-1)/2, \ c \in GF(q) \}. \]

For \( 0 \leq j < e = (q-1)/3 \) define the cyclotomic classes \( C_j \) by

\[
C_j = \{\omega^j, \omega^{j+e}, \omega^{j+2e}\}. \]

Note that \( C_0 = \{1, g, g^2\} \).

It has been shown [9] that the block set of any QS\((q+1)\) which contains \( \Gamma \) in its automorphism group consists of \( (q-7)/12 \) \( \Gamma \)-orbits of length \( q(q-1)/2 \) and two orbits of length \( q(q-1)/6 \). One of the short orbits con-
tains all the blocks of the form \( C_{2j} \cup \{ \infty \} \), and the other contains all blocks of the form \( C_{2j+1} \cup \{ 0 \} \) where \( 0 \leq j < (q-1)/6 \).

A resolution of such a quadruple system can be constructed as follows. We define a \( \rho(q, 2j, 2k+1) \)-set to be a set of distinct representatives of the long \( \Gamma \)-orbits \( B_1, B_2, \ldots, B_{(q-7)/12} \) with the property that \( \{ \omega^{2j}, \omega^{2k+1} \} \cup \bigcup_{i=1}^{(q-7)/12} B_i \) is a set of distinct representatives of the cyclotomic classes \( C_n \), \( 0 \leq n < \varepsilon \). Then the set of blocks

\[
P = \{ R_i, gR_i, g^2R_i : 1 \leq i \leq (q-7)/12 \} \cup \{ C_{2j} \cup \{ \infty \}, C_{2k+1} \cup \{ 0 \} \}
\]

is a parallel class, and the set of \( q(q-1)/3 \) distinct \( \Gamma \)-images of \( P \) forms a resolution of the system. In the Appendix we list \( \rho(q, 2j, 2k+1) \)-sets from the Carmichael system of order \( q+1 \) for \( q \in \{ 523, 739, 811, 859, 919 \} \). This completes the construction of the designs for \( L_2 \).

An exhaustive search of all SDR's of the long block orbits is clearly out of the question so we adopted the following hill-climbing strategy. Construct a partial SDR of the long orbits which is also a partial SDR of the cyclotomic classes by the greedy algorithm. (This phase typically took 4-5 minutes of CPU time.) From each orbit not yet represented, choose a block which conflicts with fewest members of the partial SDR, and exhaustively test the conflicting orbits for a representative consistent with the new block and the other members of the partial SDR. If no appropriate SDR was found after 6 h of CPU time, the algorithm was restarted with the long orbits in a different random order, giving rise to a different greedy starter. The restart was necessary only for \( q > 859 \), the smaller values all completed on the first start. The computations were performed on an IBM 4381 computer. No success has yet been achieved with \( q = 1171 \), which would decrease the number of exceptions in Theorem 3.2 by one.

The remaining designs for pairs in \( L_1 \) are constructed as follows.

**The 4p Construction (Hartman [10])**. Let \( (X, Q) \) be an SQS(v), and let \( E \) be the set of edges of the complete graph with vertex set \( X \). If there exists a partition \( \tilde{P} \) of \( Q \cup E \) into \( r(v) + v - 1 \) parts, each of which is a partition of \( X \) into parts of sizes 4 and 2, then \( (X, Q, \tilde{P}) \) is said to be an augmented resolvable quadruple system of order \( v \). A result in [11] states that if there exists an augmented resolvable quadruple system of order \( v \) then there exists an RSQS(2v). In this section we shall show how to construct an augmented resolvable quadruple system of order \( 2p \) for some primes \( p \equiv 7 \pmod{12} \), and hence an RSQS(4p).

Let \( \omega, g, e, \) and \( C_j \) be defined as in the previous construction. Let \( X = \text{GF}(p) \times Z_2 \) and consider the following group of permutations of \( X \):

\[
\Gamma_2 = \{ \gamma(x) = (\omega^kx + c)_+ : 0 \leq k < p-1, \ c \in \text{GF}(p) \}.
\]
Note that \( I_2 \) contains the transformation \( \gamma(x_i) = -x_i + 1 \), since 
\(-1 = \omega^{(p-1)/2}\).

Following [10] we define the block set \( Q \) of an SQS(2p) by taking the \( I_2 \)-images of 

1. blocks in the Carmichael QS(p + 1) which do not contain \( \infty \)
2. the blocks \( \{(1/(g-1))_0, (g/(g-1))_0, (2k+1)_1, (2k+2)_1 \} \) 
   \( 0 \leq k < (p-1)/2 \)
3. the block \( \{0_1, 1_0, g_0, (g^2)_0\} \).

If there exists a \( p(p, 2j, 2k+1) \)-set \( \{B_i: 1 \leq i \leq (p-7)/12\} \) then we construct a parallel class containing the following \( (p-3)/2 \) blocks

\[
B_i \times \{0\}, \ gB_i \times \{0\}, \ g^2B_i \times \{0\}, \\
-B_i \times \{1\}, \ -gB_i \times \{1\}, \ -g^2B_i \times \{1\}, \\
(C_{2k+1} \cup \{0\}) \times \{0\}, \ (-C_{2k+1} \cup \{0\}) \times \{1\},
\]

and the following three edges

\[
\{(\omega^{2j})_0, (\omega^{2j}+\varepsilon)_0\}, \ \{(\omega^{2j})_1, (\omega^{2j}+\varepsilon)_1\}, \ \{(\omega^{2j+2\varepsilon})_0, (\omega^{2j+2\varepsilon})_1\}.
\]

We now form \( p(p-1)/6 \) parallel classes from the images of the above class under the action of the permutations \( \gamma(x_i) = (\omega^{2m}x + c)_i \) with 
\( 0 \leq 2m < \varepsilon \) and \( c \in GF(p) \). This accounts for all the blocks in 1 and 
\( (p-1)/6 \) pure(0), pure(1), and mixed differences from the edge set. Note that the mixed differences all have the same quadratic character as \(-2\).

The next base parallel class contains the following \( (p-1)/2 \) blocks

\[
\left\{ \left( \frac{1}{g-1} + 2i \right)_0, \left( \frac{g}{g-1} + 2i \right)_0, (4i+1)_1, (4i+2)_1 \right\} \\
0 \leq i \leq (p-3)/4
\]

\[
\left\{ \left( \frac{1}{g-1} + 2i + 1 \right)_0, \left( \frac{g}{g-1} + 2i + 1 \right)_0, (4i+2)_1, (4i+3)_1 \right\} \\
(p+1)/4 \leq i \leq (p-1)/2
\]

and the edge

\[
\left\{ \left( \frac{g+1}{2(g-1)} \right)_0, 0_1 \right\}.
\]

Now form \( p(p-1)/2 \) parallel classes from the images of the above class under the action of the permutations \( \gamma(x_i) = (\omega^{2m}x + c)_i \) with
0 \leq 2m < p - 1$ and $c \in \text{GF}(p)$. This accounts for all the blocks in 2, since it was shown in [10] that the $I_2$-orbits of these blocks are covered by these transformations. This group of parallel classes also covers $(p - 1)/2$ mixed differences with the same quadratic character as 2 (since $g + 1 = -g^2$ is a quadratic nonresidue). Hence these edges did not appear in the first group of parallel classes.

The blocks in 3 are now included in parallel classes by the following strategy. Let $n$ be a quadratic nonresidue in $\text{GF}(p)$, and let $d \in \text{GF}(p)$ have the properties that $nd \omega^{2m}, (d + 1) \omega^{2m}, (d + g) \omega^{2m}, (d + g^2) \omega^{2m}, 0 \leq 2m < e$ are 4($p - 1$)/6 distinct members of $\text{GF}(p)$ and, $nd \omega^{2m}, n(d + 1) \omega^{2m}, n(d + g) \omega^{2m}, n(d + g^2) \omega^{2m}, 0 \leq 2m < e$ are also 4($p - 1$)/6 distinct members of $\text{GF}(p)$. Then the blocks

$$\{(d\omega^{2m}), (d + 1)\omega^{2m}, (d + g)\omega^{2m}, (d + g^2)\omega^{2m}\}$$

$$\{(nd\omega^{2m}), (n(d + 1)\omega^{2m}), (n(d + g)\omega^{2m}), (n(d + g^2)\omega^{2m})\}$$

$0 \leq 2m < e$, form a partial parallel class which can be completed by a 1-factor of the remaining points in $X$ using edges whose differences have not appeared in any of the previous parallel classes. This parallel class is used to generate $p$ further parallel classes by the transformations $\gamma(x_i) = (x + c), c \in \text{GF}(p)$.

Finding the constants $n$ and $d$ and a 1-factor with the appropriate properties was done by hand in the case $p = 43$. In the cases where $p \in \{127, 199, 223, 271, 1063\}$, $\text{GF}(p)$ has the property that 2 is a quadratic residue. In this case we can take $n = -1$ and $d = 1$ and the 1-factor can be explicitly constructed as the edges

$$\{(2g\omega^{2m}), (2g^2\omega^{2m})\}$$

$$\{(-2g\omega^{2m}), (-2g^2\omega^{2m})\}$$

$$\{0, 0\}, \quad 0 \leq 2m < e.$$

To match this set of parallel classes we note that there is a unique quadratic residue $\omega^{2r}$ with the property that $|\omega^{2r} + e - \omega^{2t}| = |2(g^2 - 1)|$. Now constructing the first set of parallel classes using a $\rho(p, 2r, 2k + 1)$-set guarantees that the pure differences used are all distinct. In the Appendix we give examples of such sets.

The remaining parallel classes in the augmented resolvable quadruple system are a 1-factorization of the graph with edge set consisting of all edges whose differences have not appeared so far. If this graph contains $m$ mixed differences, $u$ pure($0$) and $u$ pure($1$) differences where $m \geq u$, then the graph consists of $m - u$ edge disjoint one-factors and $u$ edge disjoint
THE EXISTENCE OF RESOLVABLE STEINER

generalized Petersen graphs, each of which has a 1-factorization by a result of Castagna and Prins [4].

We now give an example of the $4p$ construction with $p = 19$, in order to clarify the details of the construction and to prove the existence of an RSQS$(76 \{8\})$. The existence of this design was first proved in the thesis [12], but has not appeared in print elsewhere.

Using the primitive root $\omega = 2$ of GF(19) we first construct the $\rho(19, 4, 1)$ set which contains the single block $\{1, 4, 8, 13\}$. This gives us the following base parallel class:

$\{1_0, 4_0, 8_0, 13_0\} \{7_0, 9_0, 18_0, 15_0\} \{11_0, 6_0, 12_0, 10_0\}$

$\{18_1, 15_1, 11_1, 6_1\} \{12_1, 10_1, 1, 4_1\} \{8_1, 13_1, 7_1, 9_1\}$

$\{16_0, 17_0\} \{3_1, 2_1\} \{5_0, 14_1\}$.

Taking the images of this parallel class under the action of the permutations $\gamma(x_i) = (mx + c)$, with $m = 1, 4, 16$ and $c \in$ GF(19) gives 3.19 parallel classes covering all the blocks in 1, and edges with pure differences 1, 4, 3 and mixed differences 9, 17, 11.

The second base parallel class is as follows:

$\{16_0, 17_0, 1_1, 2_1\} \{8_0, 9_0, 3_1, 4_1\}$

$\{18_0, 0_0, 5_1, 6_1\} \{10_0, 11_0, 7_1, 8_1\}$

$\{1_0, 2_0, 9_1, 10_1\} \{12_0, 13_0, 11_1, 12_1\}$

$\{3_0, 4_0, 13_1, 14_1\} \{14_0, 15_0, 15_1, 16_1\}$

$\{5_0, 6_0, 17_1, 18_1\} \{7_0, 0_1\}$.

Taking the images of this parallel class under the action of the permutations $\gamma(x_i) = (mx + c)$, with $m = 1, 4, 16, 7, 9, 17, 11, 6, 5$ (i.e., $m$ a quadratic residue) and $c \in$ GF(19) gives 9.19 parallel classes covering all the blocks in 2, and edges with mixed differences 12, 10, 2, 8, 13, 14, 18, 15, 3 (the non-residues). We now form the third base parallel class as described above with $n = 1$ and $d = 5$. The edges were constructed by hand:

$\{5_1, 6_0, 12_0, 16_0\} \{1_1, 5_0, 10_0, 7_0\} \{4_1, 1_0, 2_0, 9_0\}$

$\{14_0, 13_1, 7_1, 3_1\} \{18_0, 14_1, 9_1, 12_1\} \{15_0, 18_1, 17_1, 10_1\}$

$\{4_0, 17_0\} \{8_0, 13_0\} \{2_1, 8_1\} \{11_1, 16_1\}$

$\{0_0, 6_1\} \{3_0, 0_1\} \{11_0, 15_1\}$.

Taking the images of this parallel class under the action of the permutations $\gamma(x_i) = (x + c)$, with $c \in$ GF(19) gives 19 parallel classes covering all the blocks in 3, and edges with pure differences 5, 6 and mixed differences 6, 16, 4. The remaining edges with pure differences 2, 7, 8, 9 and mixed
differences 0, 1, 5, 7 form four edge disjoint generalized Petersen graphs and thus can be divided into 12 further parallel classes.

To demonstrate the existence of an RSQS(76[8]) it is sufficient (by Corollary 6.2 of [11]) to construct an augmented resolvable system of order 38 with an augmented resolvable subsystem of order 4. Note that the image of the second base parallel class under the action of \(\gamma(x_i) = 7x_i\) contains the block \(\{30, 100, 101, 171\}\). To complete the subsystem on these points we reserve the pure differences 2, 7, the mixed differences 0, 7, and we break up the image of the second base parallel class under \(\gamma(x_i) = (17x_i + 17)\) (shown below) which contains the edge \(\{30, 171\}\),

\[
\begin{align*}
\{40, 20, 151, 131\}, & \{10, 180, 111, 91\}, \{00, 170, 71, 51\}, \\
\{60, 80\}, & \{100, 120\}, \{140, 160\}, \{50, 70\}, \{90, 110\}, \{130, 150\}, \\
\{170, 01\}, & \{21, 41\}, \{61, 81\}, \{101, 121\}, \{141, 161\}, \{181, 111\}, \\
\{30, 31\}
\end{align*}
\]

These blocks and edges can be redistributed into the seven parallel classes shown below:

\[
P_1 = \{(14i + 3)0, (14i + 10)0\}, \{(14i + 10)1, (14i + 17)1\}: 0 \leq i \leq 8 \cup \{150, 31\}
\]

\[
P_2 = \{(7i + 3)0, (7i + 10)1\}: 0 \leq i \leq 16 \cup \{80, 150\}, \{151, 31\}
\]

\[
P_3 = \{(14i + 5)0, (14i + 12)0\}, \{(14i + 12)1, (14i)1\}: 0 \leq i \leq 6 \cup \{30, 171\}, \{100, 101\}, \{80, 151\}, \{150, 170\}, \{31, 51\}
\]

\[
P_4 = \{i0, i1\}: i \neq 3, 5, 10, 17 \cup \{30, 50\}, \{100, 170\}, \{31, 101\}, \{51, 171\}
\]

\[
P_5 = \begin{pmatrix}
\{40, 20, 151, 131\}, & \{10, 180, 111, 91\}, \{00, 170, 71, 51\}, \\
\{60, 80\}, & \{100, 120\}, \{140, 160\}, \{50, 70\}, \{90, 110\}, \{130, 150\}, \\
\{170, 01\}, & \{21, 41\}, \{61, 81\}, \{101, 121\}, \{141, 161\}, \{181, 111\}, \\
\{30, 31\}
\end{pmatrix}
\]

\[
P_6 = \begin{pmatrix}
\{160, 140, 31, 11\}, & \{120, 100, 141, 121\}, \{80, 60, 61, 41\}, \\
\{170, 00\}, & \{20, 40\}, \{180, 10\}, \{70, 90\}, \{110, 130\}, \{30, 150\}, \\
\{81, 101\}, & \{161, 181\}, \{71, 91\}, \{111, 131\}, \{151, 171\}, \{01, 21\}, \\
\{50, 51\}
\end{pmatrix}
\]

\[
P_7 = \begin{pmatrix}
\{150, 130, 181, 161\}, & \{110, 90, 101, 81\}, \{70, 50, 21, 01\}, \\
\{00, 20\}, & \{40, 60\}, \{80, 100\}, \{120, 140\}, \{160, 180\}, \{10, 30\}, \\
\{41, 61\}, & \{121, 141\}, \{11, 31\}, \{51, 71\}, \{91, 111\}, \{131, 151\}, \\
\{170, 171\}
\end{pmatrix}
\]
Observe that \( P_1 \) contains the edges \( \{3_0, 10_0\} \) and \( \{10_1, 17_1\} \), \( P_2 \) contains the edges \( \{3_0, 10_1\} \), and \( \{10_0, 17_1\} \), and \( P_3 \) contains the edges \( \{3_0, 17_1\} \) and \( \{10_0, 10_1\} \). This completes the construction.

To complete the basis for the induction it remains to construct an RSQS(52[16]). This is done using a variant of the construction given in \([11]\) to prove Theorem 1.1.

**A Special Construction.** Let \((X, Q, \hat{P}_j)\) be an RSQS(20[8]), where \( X = \{\infty_0, \infty_1, \infty_2, \infty_3\} \cup Z_{16} \) and such that the block \( \{\infty_0, \infty_1, \infty_2, \infty_3\} \) is contained in \( P_0 \). Further let the resolvable subsystem of order 8 have point set \( E = \{0, 2, 4, 6, 8, 10, 12, 14\} \) and let its blocks be included in the parallel classes \( P_0, P_1, \ldots, P_6 \). Any RSQS(20[8]) can be labelled in this manner.

Let \( X' = \{\infty_0, \infty_1, \infty_2, \infty_3\} \cup (Z_{16} \times Z_3) \) and define the embeddings \( \lambda_j : X \to X' \) as in the Section 2. We shall construct an RSQS(52[16]) \((X', Q', \hat{P}_j')\), where the resolvable subsystem has point set \( E \times \{0, 1\} \). We use the 1-factorization of \( G(16, \{2, 4, 6, 8\}) \) and the latin square \( l_{m,k} \) of side 8 with a subsquare of side 4 given below.

\[
\begin{align*}
F_1 &= \{\{0, 2\}, \{4, 6\}, \{8, 10\}, \{12, 14\}, \{1, 3\}, \{5, 7\}, \{9, 11\}, \{13, 15\}\} \\
F_2 &= \{\{0, 4\}, \{2, 6\}, \{8, 12\}, \{10, 14\}, \{1, 5\}, \{3, 7\}, \{9, 13\}, \{11, 15\}\} \\
F_3 &= \{\{0, 6\}, \{2, 4\}, \{8, 14\}, \{10, 12\}, \{1, 7\}, \{3, 5\}, \{9, 15\}, \{11, 13\}\} \\
F_4 &= \{\{0, 8\}, \{2, 10\}, \{4, 12\}, \{6, 14\}, \{1, 9\}, \{3, 11\}, \{5, 13\}, \{7, 15\}\} \\
F_5 &= \{\{0, 10\}, \{2, 8\}, \{4, 14\}, \{6, 12\}, \{1, 11\}, \{3, 9\}, \{5, 15\}, \{7, 13\}\} \\
F_6 &= \{\{0, 12\}, \{2, 14\}, \{4, 8\}, \{6, 10\}, \{1, 13\}, \{3, 15\}, \{5, 9\}, \{7, 11\}\} \\
F_7 &= \{\{0, 14\}, \{2, 12\}, \{4, 10\}, \{6, 8\}, \{1, 15\}, \{3, 13\}, \{5, 11\}, \{7, 9\}\}
\end{align*}
\]

<p>| | | | | | | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1 2 3 4</td>
<td>5 6 7 8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 1 4 3</td>
<td>6 5 8 7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 4 1 2</td>
<td>7 8 5 6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4 3 2 1</td>
<td>8 7 6 5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

We now define the parallel classes in \( \hat{P}_j \), and thus implicitly defining the blocks in \( Q' \). Let

\[
P'_0 = \lambda_0(P_0) \cup \lambda_1(P_0) \cup \lambda_2(P_0).
\]
For \( i \in \mathbb{Z}_3 \) and \( j = 1, 2, \ldots, 56 \) we initially define \( P'_i \) to contain the 5 blocks in \( \lambda_i(P_j) \) and 8 blocks of the form \( \{x_{i+1}, y_{i+1}, z_{i+2}, t_{i+2}\} \). Let \( B_{i,m,n,k} \) be the block \( \{x_{i+1}, y_{i+1}, z_{i+2}, t_{i+2}\} \), where \( \{x, y\} \) is the \( k \)th member of \( F_n \) and \( \{z, t\} \) is the \( l_{m,n,k} \)th member of \( F_n \) (\( 1 \leq m, k \leq 8 \) and \( 1 \leq n \leq 7 \)). Further let \( B_{i,m,n} = \{B_{i,m,n,k} : 1 \leq k \leq 8\} \). Now any one of the 56 sets \( B_{i,m,n} \) with \( 1 \leq m \leq 8 \) and \( 1 \leq n \leq 7 \) can be used to complete the parallel class \( P'_i \). Note that of the 35 parallel classes needed in the resolvable subsystem of order 16 we already have one contained in \( P'_0 \) and 28 contained in the sets \( B_{2,m,n} \), where \( 1 \leq m \leq 4 \) and \( 1 \leq n \leq 7 \). The remaining 6 parallel classes are constructed by performing the following permutation with \( 1 \leq j \leq 6 \). Remove the two blocks with points \( E \times \{i\} \) from \( P'_i \) for \( i = 1, 2 \). Place these four blocks in \( B_{0,1,j} \) and remove the four blocks \( B_{0,1,j,k} \) with \( 1 \leq k \leq 4 \). Adding \( B_{0,1,j} \) to the parallel classes \( P'_i \) completes the subsystem. We now have to relocate the four removed blocks and complete the parallel classes \( P'_j \) and \( P'_i \). First remove blocks \( B_{1,5,j,3} \) and \( B_{1,5,j,4} \) from \( B_{1,5,j} \) and add the four blocks \( B_{0,1,j,3} \) and \( B_{0,1,j,4} \) from \( B_{0,1,j} \). Next remove the four blocks \( B_{2,7,j,3} \) and \( B_{2,7,j,4} \) from \( B_{2,7,j} \) and add the four blocks \( B_{0,1,j,3} \) and \( B_{0,1,j,4} \) from \( B_{0,1,j} \). Complete the parallel classes \( P'_j \) with the new \( B_{2,7,j} \).

We illustrate the construction below in the case \( j = 1 \):

\[
\begin{align*}
\text{Before} & \quad \{0,2,1,0,2,2\}, \{4,6,4,2,6,2\}, \{8,1,10,8,2,10,2\}, \{12,14,12,2,14,2\} \in P'_{0,1} \\
\text{After} & \quad \{0,2,1,4,6,1\}, \{8,1,10,12,14,1\}, \{8,2,10,9,0,11,0\}, \{12,2,14,2,13,0,15,0\} \in P'_{1,1} \\
& \quad \{0,2,2,4,6,2\}, \{8,2,10,12,14,2\}, \{9,0,11,0,2,1\}, \{13,0,15,0,4,6,1\} \in P'_{2,1} \\
& \quad \{0,2,1,4,6,1\}, \{8,1,10,12,14,1\}, \{0,2,2,4,6,2\}, \{8,2,10,12,14,2\} \in P'_{0,1} \\
& \quad \{8,1,10,8,2,10,2\}, \{12,1,14,12,2,14,2\}, \{9,0,11,0,2,1\}, \{13,0,15,0,4,6,1\} \in P'_{1,1} \\
& \quad \{0,2,1,0,2,2\}, \{4,6,4,2,6,2\}, \{8,2,10,9,0,11,0\}, \{12,2,14,2,13,0,15,0\} \in P'_{2,1}.
\end{align*}
\]

The number of parallel classes remaining to be constructed is \( 16^2 \) and accordingly we denote them by \( P'_{a,b,c} \), where \( a, b, c \in \mathbb{Z}_{16} \) and \( a + b + c \equiv 0 \) (mod 16). The parallel class \( P'_{a,b,c} \) contains the following 10 blocks:

\[
\begin{align*}
\{\infty_0(a+5)(b+13)(c+8)\} & \{\infty_1(a+10)(b+7)c\} \\
\{\infty_2(a+9)(b+3)(c+1)\} & \{\infty_3(a+15)(b+8)(c+9)\} \\
\{(a+7)(a+14)(b+1)(c+15)\} & \{(a+8)(a+13)(b+2)(c+4)\} \\
\{(a+9)(b+4)(b+11)(c+7)\} & \{(a+12)(b+6)(b+9)(c+4)\} \\
\{a_0b_1(c+2)(c+3)\} & \{(a+4)(b+12)(c+5)(c+12)\}.
\end{align*}
\]

The last three blocks in \( P'_{a,b,c} \) are dependent on the parities of \( a, b, \) and \( c. \) If \( a \equiv b \equiv c \equiv 0 \) (mod 2) then add the blocks
\{(a+1)_0(a+2)_0(b+5)_1(b+10)_1\}
\{(b+14)_1(b+15)_1(c+6)_2(c+11)_2\}
\{(c+10)_2(c+13)_2(a+3)_0(a+6)_0\}.

If \(a \equiv 0, b \equiv c \equiv 1 \pmod{2}\) then add the blocks
\{(a+3)_0(a+6)_0(b+14)_1(b+15)_1\}
\{(b+5)_1(b+10)_1(c+6)_2(c+11)_2\}
\{(c+10)_2(c+13)_2(a+1)_0(a+2)_0\}.

If \(b \equiv 0, a \equiv c \equiv 1 \pmod{2}\) then add the blocks
\{(a+3)_0(a+6)_0(b+14)_1(b+15)_1\}
\{(b+5)_1(b+10)_1(c+10)_2(c+13)_2\}
\{(c+6)_2(c+11)_2(a+1)_0(a+2)_0\}.

If \(c \equiv 0, a \equiv b \equiv 1 \pmod{2}\) then add the blocks
\{(a+1)_0(a+2)_0(b+5)_1(b+10)_1\}
\{(b+14)_1(b+15)_1(c+10)_2(c+13)_2\}
\{(c+6)_2(c+11)_2(a+3)_0(a+6)_0\}.

By a case analysis similar to that of Section 2 and that given in [11], it can be verified that \((X', Q', \mathcal{P}_0')\) is indeed an RSQS(52[16], with a subsystem of order 16 embedded as described above.

APPENDIX

A.1. The orders for which the existence problem for RSQS remains open

| 220 | 236 | 292 | 364 | 460 | 596 | 676 |
| 724 | 1076 | 1100 | 1172 | 1252 | 1316 | 1820 |
| 2236 | 2308 | 2324 | 2380 | 2540 | 2740 | 2812 |
| 3620 | 3820 | 6356 |

A.2. The initial designs

A.2.1. The \(q + 1\) construction

\(q = 163\) · see [9]
\(q = 343\) · see [9]
\(q = 523\) \(\omega = 2\)
\(\rho(523, 72, 11)\)
\{1, 2, 3, 391\} \{5, 6, 8, 477\} \{16, 32, 80, 77\} \{48, 64, 128, 284\} \{256, 512, 223, 487\}
\{245, 501, 468, 86\} \{435, 347, 254, 388\} \{171, 87, 461, 344\} \{363, 484, 4, 156\} \{294, 65, 161, 145\}
\{422, 321, 54, 260\} \{119, 238, 335, 211\} \{414, 504, 375, 28\} \{282, 476, 307, 202\}
THE EXISTENCE OF RESOLVABLE STEINER

\{53, 306, 689, 70\} \{378, 756, 557, 592\} \{190, 380, 506, 833\} \{86, 608, 244, 517\} \{818, 803, 702, 594\}

\{463, 67, 822, 778\} \{460, 690, 347, 132\} \{366, 732, 836, 376\} \{41, 266, 349, 136\}

\{536, 213, 377, 595\} \{251, 621, 104, 262\} \{268, 324, 550, 456\} \{427, 488, 529, 418\}

\{564, 752, 729, 148\} \{574, 555, 396, 612\} \{234, 683, 520, 829\} \{467, 269, 703, 587\}

\{757, 465, 845, 698\} \{841, 779, 513, 713\} \{30, 539, 602, 635\} \{189, 810, 345, 71\}

\{498, 130, 502, 609\} \{469, 751, 725, 217\} \{351, 491, 289, 558\} \{541, 766, 173, 250\}

\{12, 296, 247, 659\} \{828, 383, 797, 125\} \{269, 538, 590, 320\} \{332, 250, 291, 408\}

\{646, 309, 293, 134\}

\(q = 919 \omega = 7\)

\(p = 199 \omega = 3\)

\(p(127, 72, 37)\)

\{106, 49, 119, 70\} \{97, 91, 79, 47\} \{73, 19, 111, 7\} \{13, 83, 52, 95\} \{12, 16, 44, 105\}

\{75, 100, 46, 18\} \{82, 86, 126, 62\} \{68, 72, 116, 55\} \{41, 125, 31, 3\} \{115, 10, 5, 80\}

\(p = 199 \omega = 3\)

\(p(127, 72, 37)\)

\{106, 49, 119, 70\} \{97, 91, 79, 47\} \{73, 19, 111, 7\} \{13, 83, 52, 95\} \{12, 16, 44, 105\}

\{75, 100, 46, 18\} \{82, 86, 126, 62\} \{68, 72, 116, 55\} \{41, 125, 31, 3\} \{115, 10, 5, 80\}

A.2.2. The 4p construction

\(p = 19 - \text{including construction of an } RSQ\{6\}\{4.19(3)\}\text{ see Section 3.}\n
\(p = 43 \omega = 3\)

\(p(43, 10, 3)\)

\(n = 3, d = 9\)

One factor

\{1, 2, 3, 15\} \{30, 7, 14, 30\} \{11, 70, 4, 19\}

\(n = 3, d = 9\)

One factor

\{1, 2, 3, 15\} \{5, 9, 25\} \{16, 19, 29\} \{24, 25, 37\} \{26, 41, 53\} \{34, 42, 59\} \{1, 3, 11\} \{5, 14, 23\}

\(m = 14 \geq u = 7\)

\(p = 127 \omega = 3\)

\(p(127, 72, 37)\)

\{106, 49, 119, 70\} \{97, 91, 79, 47\} \{73, 19, 111, 7\} \{13, 83, 52, 95\} \{12, 16, 44, 105\}

\{75, 100, 46, 18\} \{82, 86, 126, 62\} \{68, 72, 116, 55\} \{41, 125, 31, 3\} \{115, 10, 5, 80\}

\(p = 199 \omega = 3\)

\(p(199, 106, 65)\)

\{125, 7, 88, 27\} \{14, 95, 58, 143\} \{37, 182, 20, 167\} \{63, 195, 59, 180\} \{131, 114, 12, 87\}

\{187, 181, 139, 15\} \{151, 127, 134, 92\} \{128, 138, 29, 67\} \{176, 102, 158, 83\} \{39, 18, 185, 5\}

\{169, 163, 79, 170\} \{77, 123, 17, 57\} \{53, 38, 196, 69\} \{177, 160, 19, 152\} \{107, 33, 99, 126\}

\{84, 60, 40, 124\}
A.2.3. Miscellaneous constructions

\text{RSQS}(4) \text{ - trivial.}
\text{RSQS}(20[8]) \text{ - see [11]}
\text{RSQS}(28[8]) \text{ - see [11]}
\text{RSQS}(52[16]) \text{ - see Section 3.
After approximately 1200 hours of computer time, the following construction for an RSQS(1172) was found. This reduces the number of orders for which the existence question remains open to 23.

\[ q = 1171, \omega = 2 \]

\[
\begin{align*}
(1, 2, 11, 855) & \quad (4, 8, 48, 249) & \quad (16, 32, 208, 823) & \quad (64, 128, 586, 662) & \quad (104, 62, 645, 423) \\
(1024, 877, 1014, 966) & \quad (583, 1166, 1126, 962) & \quad (1161, 1151, 971, 544) & \quad (504, 246, 28, 1083) \\
(80, 96, 416, 667) & \quad (1131, 1091, 251, 821) & \quad (1011, 851, 684, 317) & \quad (192, 226, 621, 647) \\
(231, 1052, 285, 112) & \quad (953, 733, 922, 1128) & \quad (225, 324, 200, 69) & \quad (299, 598, 1072, 572) \\
(400, 800, 1090, 1053) & \quad (75, 100, 875, 158) & \quad (545, 974, 650, 123) & \quad (921, 671, 618, 70) \\
(464, 1009, 803, 305) & \quad (523, 1046, 615, 988) & \quad (171, 342, 643, 716) & \quad (449, 988, 1117, 408) \\
(847, 221, 943, 734) & \quad (1032, 343, 473, 196) & \quad (704, 158, 804, 744) & \quad (632, 93, 522, 478) \\
(725, 186, 75, 472) & \quad (634, 97, 717, 78) & \quad (5, 6, 57, 101) & \quad (776, 381, 919, 168) \\
(194, 388, 325, 850) & \quad (844, 204, 134, 280) & \quad (749, 597, 282, 872) & \quad (437, 874, 21, 149) \\
(201, 887, 861, 61) & \quad (679, 733, 757, 1064) & \quad (1069, 1035, 1133, 1057) & \quad (320, 384, 1116, 1158) \\
(316, 474, 1153, 54) & \quad (372, 558, 84, 371) & \quad (954, 737, 856, 715) & \quad (1020, 189, 267, 904) \\
(206, 412, 1051, 1169) & \quad (321, 642, 560, 754) & \quad (351, 1112, 631, 704) & \quad (466, 932, 728, 777) \\
(796, 421, 584, 824) & \quad (430, 860, 917, 624) & \quad (678, 791, 648, 85) & \quad (1026, 851, 277, 816) \\
(340, 425, 218, 836) & \quad (518, 1081, 655, 533) & \quad (579, 90, 179, 210) & \quad (909, 41, 1066, 910) \\
(925, 24, 651, 437) & \quad (706, 140, 291, 367) & \quad (1023, 1039, 457, 785) & \quad (442, 663, 979, 297) \\
(88, 176, 109, 254) & \quad (380, 760, 1071, 180) & \quad (627, 491, 920, 711) & \quad (486, 349, 378, 288) \\
(629, 58, 772, 1038) & \quad (234, 602, 799, 981) & \quad (699, 227, 685, 907) & \quad (22, 44, 672, 795) \\
(755, 339, 726, 177) & \quad (1034, 707, 596, 377) & \quad (225, 450, 287, 1001) & \quad (1129, 1122, 79, 600) \\
(693, 1139, 787, 595) & \quad (825, 479, 422, 913) & \quad (575, 1150, 1111, 972) & \quad (1019, 867, 181, 1102) \\
(736, 591, 866, 239) & \quad (641, 996, 1106, 1120) & \quad (1022, 354, 1113, 1152) & \quad (293, 63, 402, 1095) \\
(1119, 630, 590, 413) & \quad (270, 983, 387, 690) & \quad (811, 451, 187, 441) & \quad (443, 268, 301, 18) \\
(1145, 502, 608, 113) & \quad (468, 73, 43, 91) & \quad (190, 1092, 243, 902) & \quad (138, 161, 184, 1144) \\
(808, 590, 154, 403) & \quad (1135, 114, 564, 383) & \quad (36, 230, 1006, 47) & \quad (141, 327, 86, 692) \\
(571, 404, 573, 743) & \quad (89, 931, 970, 846) & \quad (294, 493, 914, 1028) & \\
\end{align*}
\]

REFERENCES