Construction Methods for Row-Complete Latin Squares

by

Jeffrey T. Higham

A thesis
presented to the University of Waterloo
in fulfilment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Combinatorics and Optimization

Waterloo, Ontario, Canada, 1996

0-612-21356-0

The University of Waterloo requires the signatures of all persons using or photocopying this thesis. Please sign below, and give address and date.

Abstract

A latin square L of order n is said to be *row-complete*, and is denoted by $RCLS(n)$, if the ordered pairs $(L_{ij}, L_{i,j+1})$ are all distinct for $1 \leq i \leq n$ and $1 \leq j \leq n-1$. Row-complete latin squares are also called *roman squares* , and are used in statistics in the design of sequential experiments. In the language of statistics, an $RCLS(n)$ is a *balanced repeated measurements* (n, n, n) *design* .

In 1949, Williams provided a simple construction for an $RCLS(2m)$ for every m, but the situation for odd orders has proven to be much more difficult. In the last 30 years or so, various authors have given constructions of $RCLS$ for certain odd orders, but the state of knowledge has nevertheless remained somewhat sparse.

In this thesis, two new methods of construction for $RCLS$ are given. The first, a product construction, yields infinitely many new orders for which $RCLS$ are known to exist. The second construction, which is the highlight of this thesis, is a direct construction of an $RCLS$ for any odd composite order other than 9. Since $RCLS$ of order 9 and of even order have previously been constructed, this proves that $RCLS$ of every composite order exist.

In addition, a new result is given on the related concept of *quasi-complete* latin squares ($QCLS$). Specifically, it is shown that complete sets of mutually orthogonal $QCLS(p)$ exist for every prime p. Such sets were previously known to exist only for primes $p \leq 13$.

Acknowledgements

I would like to thank my supervisor, Ron Mullin, for his guidance and advice.

To my parents, Verna G. Higham and the late Stephen G. Higham

Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 *RCLS* - Applications and History

A *latin square* L of order n is an $n \times n$ array of n symbols (usually the numbers 1 to n or 0 to $n-1$) such that each symbol occurs exactly once in each row and in each column. L is said to be *row-complete* (or is sometimes called a *roman* square), and is denoted by $RCLS(n)$, if the ordered pairs $(L_{ij}, L_{i,j+1})$ are all distinct for $1 \leq i \leq n$ and $1 \leq j \leq n-1$. In the language of statistics, an $RCLS(n)$ is a *balanced repeated measurements* (n, n, n) *design* (see e.g. [13]). In connection to graph theory, an $RCLS(n)$ gives rise to a decomposition of the complete directed graph on n vertices into n edge-disjoint Hamiltonian paths [17].

Row-complete latin squares are used in statistics in the design of sequential experiments (see [4, 19] or [7, Section 2.3]). For example, suppose adjacent plots of land in a square array are to receive different treatments in an agricultural experiment to determine the relative effectiveness of the treatments. The entries of a latin square may correspond to the treatments applied to the plots of land, but treatments applied to adjacent plots of land might interact, and so the latin square should be row-complete in order to balance out these interactions.

Another example is in the field of psychology. Suppose n subjects are each taking part in a series of n psychological tests. The performance of a subject on a given test might be influenced by both the number of tests the subject has already taken (e.g. fatigue may set in) and the immediately preceding test. The first of these influences can be compensated for by letting the i^{th} subject take the tests in the order given by the i^{th} row of a latin square, and the second, by ensuring the latin square is row-complete.

In 1949, Williams [19] provided a simple construction for an $RCLS(2m)$ for every m, but the situation for odd orders has proven to be much more difficult. An $RCLS(1)$ exists trivially, and it is known that there are no $RCLS$ of orders 3, 5 or 7. In 1968, Mendelsohn [17] found an $RCLS(21)$, the first non-trivial $RCLS$ of odd order ever constructed. Over the next 15 years, various authors gave constructions for $RCLS$ of orders 9, 15, 25, 27, 33, 39, 55 and 57 (see [2, 8, 13, 16, 18]).

It is known that an $RCLS(n)$ exists whenever there exists a *sequenceable* group of order n, that is, a group with identity e whose elements can be ordered as $g_1 = e, g_2, ..., g_n$, so that the partial products $g_1 g_2 \cdots g_i$ are all distinct for $1 \leq i \leq n$ (the ordering is then said to be a *sequencing* of the group) [12]. Sequencings for the two non-abelian groups of order 27 are known (see [1, 16]), and the non-abelian groups of order pq, where $p < q$ are odd primes with $p \mid q - 1$, were sequenced by Keedwell [15] in 1981 whenever p has 2 as a primitive root. This latter result gave the first infinite class of odd order $RCLS$ (e.g. take $p = 3$ and note that there are infinitely many primes congruent to 1 (mod 3)).

Two latin squares A and B of order n are *orthogonal* if the ordered pairs

(A_{ij}, B_{ij}) are all distinct for $1 \leq i, j \leq n$, and the latin squares $A_1, A_2, ..., A_t$ are called *mutually orthogonal* if each pair of them is orthogonal. Heinrich [14] proved in 1979 that if there exist k mutually orthogonal $RCLS(n)$ and if there exists an $RCLS(k)$, then an $RCLS(nk)$ also exists. In 1991, Dénes and Keedwell [8] generalized results of Heinrich [14] to show that if there exists a non-abelian sequenceable group of order n and p is the smallest prime factor of n, then there exist $p-1$ mutually orthogonal $RCLS(n)$. This result, along with the results of Heinrich and Keedwell above, gave more orders for which $RCLS$ can be constructed, the smallest being $11 \cdot 23 \cdot 9 = 2277$ (obtained by taking $p = 11$, $q = 23$, $n = pq$ and $k = 9$).

All of the orders of known $RCLS$ prior to this thesis have come from the abovementioned results.

1.2 New Results in This Thesis

In Chapter 2 it is proved that if an $RCLS(m)$ and a sequencing of a group of order n both exist, then so does an $RCLS(mn)$. This product construction provides infinitely many new orders for which $RCLS$ can be constructed, the smallest of which is $9 \cdot 21 = 189$ (obtained by taking $m = 9$ and $n = 21 = 3 \cdot 7$).

The main result of this thesis, a direct construction for an $RCLS$ of any odd composite order other than 9, is presented in Chapter 3. Since $RCLS$ of order 9 and of even order have previously been constructed, this proves that $RCLS$ of every composite order exist.

The related concept of *quasi-complete* latin squares ($QCLS$) is discussed in Chapter 4, where it is shown that complete sets of mutually orthogonal $QCLS(p)$ exist for every prime p. Such sets were previously known only for primes $p \leq 13$.

Chapter 2

A Product Construction

In this chapter, a construction of an $RCLS(mn)$ is given using an $RCLS(m)$ and a sequencing of a group of order n, where m and n are assumed to be odd (since, as noted in Section 1.1, even order $RCLS$ have already been constructed). This yields infinitely many new orders for which row-complete latin squares can be constructed.

2.1 Sequenceable Groups and Property P

Two latin squares A and B of the same order and defined on the same set of symbols will be said to have *property P* if whenever $A_{ij} = B_{kj}$ then $A_{kj} = B_{ij}$.

The results of Heinrich in [14] provide the following theorem.

Theorem 2.1 ([8, Theorem 1.4]) *Let $a_1, a_2, ..., a_n$ be a sequencing of a group G of order n, and let $b_1 = a_1, b_2 = a_1a_2, ..., b_n = a_1a_2 \cdots a_n$ be the corresponding partial products. If $h_1, h_2, ..., h_n$ and $k_1, k_2, ..., k_n$ are orderings of the elements of G such that $h_1k_1^{-1}, h_2k_2^{-1}, ..., h_nk_n^{-1}$ is also an ordering of the elements of G, then the arrays H and K defined by $H_{ij} = h_ib_j$ and $K_{ij} = k_ib_j$ are orthogonal $RCLS(n)$.*

In particular, if n is odd, then the following holds.

Theorem 2.2 *If there exists a sequenceable group of odd order n, then there exist two orthogonal $RCLS(n)$ having property P.*

Proof Setting $k_i = h_i^{-1}$ for $1 \leq i \leq n$ satisfies the conditions of Theorem 2.1. This is because the mapping $g \mapsto g^r$ is a permutation of G whenever r is relatively prime to n, since if $g_1^r = g_2^r$, then $g_1 = g_1^{rs} = (g_1^r)^s = (g_2^r)^s = g_2^{rs} = g_2$, where $rs \equiv 1 \ (mod\ n)$. Furthermore, H and K then have property P, since if $H_{ij} = K_{kj}$, then $h_i b_j = h_k^{-1} b_j$, hence $h_i = h_k^{-1}$ and so $h_k = h_i^{-1}$, giving $H_{kj} = h_k b_j = h_i^{-1} b_j = K_{ij}$. ∎

This theorem will be used in the next section, where the main ”mesh” construction is presented.

2.2 The Mesh Construction

If A and B are m by m arrays (not necessarily defined on the same set of symbols), define A *mesh* B, written $A \circ B$, to be the m by m array defined by

$$(A \circ B)_{ij} = \begin{cases} A_{ij} & \text{if } j \text{ is odd} \\ B_{ij} & \text{if } j \text{ is even,} \end{cases}$$

for $1 \leq i, j \leq m$. Note that in general, $A \circ B \neq B \circ A$.

Also, if C is an m by m array of symbols, define the *reverse* of C, written C^R, to be the m by m array formed by reversing the columns of C, that is,

$$C_{ij}^R = C_{i,m+1-j},$$

for $1 \leq i, j \leq m$.

Theorem 2.2 will be used to prove the following main theorem.

Theorem 2.3 *If an $RCLS(m)$ and a sequenceable group of order n both exist, then an $RCLS(mn)$ also exists.*

Proof As mentioned above, m and n can be assumed to be odd. So by Theorem 2.2, there exist two orthogonal $RCLS(n)$ H and K defined on the symbols $1, 2, ..., n$ having property P. Let A be an $RCLS(m)$ defined, say, on the symbols $1, 2, ..., m$, and let $A^{(1)}, A^{(2)}, ..., A^{(n)}$ be n isomorphic copies of A on disjoint sets of symbols, namely

$$A_{ij}^{(k)} = (A_{ij}, k),$$

for $1 \leq i, j \leq m$ and $1 \leq k \leq n$.

Let L be the mn by mn array, defined on the set $S = \{(x, y) : 1 \leq x \leq m, 1 \leq y \leq n\}$ of mn symbols, whose $(i, j)^{th}$ "block" is

$$\begin{cases} A^{(H_{ij})} \circ A^{(K_{ij})} & \text{if } j \text{ is odd} \\ (A^{(H_{ij})} \circ A^{(K_{ij})})^R & \text{if } j \text{ is even,} \end{cases}$$

for $1 \leq i, j \leq n$, that is,

$$L_{(i-1)m+u,(j-1)m+v} = \begin{cases} (A^{(H_{ij})} \circ A^{(K_{ij})})_{uv} & \text{if } j \text{ is odd} \\ ((A^{(H_{ij})} \circ A^{(K_{ij})})^R)_{uv} & \text{if } j \text{ is even,} \end{cases}$$

for $1 \leq i, j \leq n$ and $1 \leq u, v \leq m$. Then L is an $RCLS(mn)$.

To see this, first it is necessary to show that L is a latin square. To prove this, it suffices to show that the array B, where

$$B_{(i-1)m+u,(j-1)m+v} = (A^{(H_{ij})} \circ A^{(K_{ij})})_{uv},$$

for $1 \leq i, j \leq n, 1 \leq u, v \leq m$, is a latin square, since B is obtained from L by permuting its columns.

Let (x, y) be any symbol in S, and consider any row $r = (i-1)m + u$ of B, where $1 \leq i \leq n$ and $1 \leq u \leq m$. Since A is a latin square, there exists j_1 with $1 \leq j_1 \leq m$, such that $A_{uj_1} = x$, and so $A^{(y)}_{uj_1} = (x, y)$. Since H and K are latin squares, there exist j_2 and j_3 with $1 \leq j_2, j_3 \leq n$, such that $H_{ij_2} = K_{ij_3} = y$.

If j_1 is odd, then

$$\begin{aligned} B_{(i-1)m+u,(j_2-1)m+j_1} &= (A^{(H_{ij_2})} \circ A^{(K_{ij_2})})_{uj_1} \\ &= A^{(H_{ij_2})}_{uj_1} = A^{(y)}_{uj_1} = (x, y), \end{aligned}$$

while if j_1 is even, then

$$\begin{aligned} B_{(i-1)m+u,(j_3-1)m+j_1} &= (A^{(H_{ij_3})} \circ A^{(K_{ij_3})})_{uj_1} \\ &= A^{(K_{ij_3})}_{uj_1} = A^{(y)}_{uj_1} = (x, y). \end{aligned}$$

Thus each symbol in S occurs in each row of B.

Now consider any column $c = (j-1)m + v$ of B, where $1 \leq j \leq n$ and $1 \leq v \leq m$. Since A is a latin square, there exists i_1 with $1 \leq i_1 \leq m$, such that $A_{i_1v} = x$, and so $A^{(y)}_{i_1v} = (x, y)$. Since H and K are latin squares, there exist i_2 and i_3 with $1 \leq i_2, i_3 \leq n$, such that $H_{i_2j} = K_{i_3j} = y$.

If v is odd, then

$$\begin{aligned} B_{(i_2-1)m+i_1,(j-1)m+v} &= (A^{(H_{i_2j})} \circ A^{(K_{i_2j})})_{i_1v} \\ &= A^{(H_{i_2j})}_{i_1v} = A^{(y)}_{i_1v} = (x, y), \end{aligned}$$

while if v is even, then

$$\begin{aligned} B_{(i_3-1)m+i_1,(j-1)m+v} &= (A^{(H_{i_3j})} \circ A^{(K_{i_3j})})_{i_1v} \\ &= A^{(K_{i_3j})}_{i_1v} = A^{(y)}_{i_1v} = (x, y). \end{aligned}$$

Thus each symbol in S also occurs in each column of B, and so B is a latin square, hence so is L.

It remains to show that L is row-complete. To this end, let $((x,y),(z,w))$ be any ordered pair of symbols of S, where $1 \leq x, z \leq m$ and $1 \leq y, w \leq n$. There are two cases.

Case 1: Suppose $x \neq z$.

Since A is row-complete, there exist i_1, j_1, i_2 and j_2 with $1 \leq i_1, i_2 \leq m$ and $1 \leq j_1, j_2 \leq m-1$, such that $(A_{i_1 j_1}, A_{i_1,j_1+1}) = (x,z)$ and $(A_{i_2,j_2}, A_{i_2,j_2+1}) = (z,x)$. Then $(A^{(y)}_{i_1 j_1}, A^{(w)}_{i_1,j_1+1}) = (A^{(y)}_{i_2 j_2+1}, A^{(w)}_{i_2,j_2}) = ((x,y),(z,w))$. Since H and K are orthogonal, there exist s and t with $1 \leq s, t \leq n$, such that $(H_{st}, K_{st}) = (y,w)$, and so since H and K have property P, there exists r with $1 \leq r \leq n$, such that $(H_{rt}, K_{rt}) = (w,y)$.

If t is odd and j_1 is odd, then

$$\begin{aligned} L_{(s-1)m+i_1,(t-1)m+j_1} &= (A^{(H_{st})} \circ A^{(K_{st})})_{i_1 j_1} \\ &= A^{(H_{st})}_{i_1 j_1} = A^{(y)}_{i_1 j_1} = (x,y), \end{aligned}$$

and

$$\begin{aligned} L_{(s-1)m+i_1,(t-1)m+(j_1+1)} &= (A^{(H_{st})} \circ A^{(K_{st})})_{i_1,j_1+1} \\ &= A^{(K_{st})}_{i_1,j_1+1} = A^{(w)}_{i_1,j_1+1} = (z,w). \end{aligned}$$

If t is odd and j_1 is even, then

$$\begin{aligned} L_{(r-1)m+i_1,(t-1)m+j_1} &= (A^{(H_{rt})} \circ A^{(K_{rt})})_{i_1 j_1} \\ &= A^{(K_{rt})}_{i_1 j_1} = A^{(y)}_{i_1 j_1} = (x,y), \end{aligned}$$

and

$$\begin{aligned} L_{(r-1)m+i_1,(t-1)m+(j_1+1)} &= (A^{(H_{rt})} \circ A^{(K_{rt})})_{i_1,j_1+1} \\ &= A^{(H_{rt})}_{i_1,j_1+1} = A^{(w)}_{i_1,j_1+1} = (z,w). \end{aligned}$$

If t is even and j_2 is odd, then

$$\begin{aligned} L_{(r-1)m+i_2,(t-1)m+(m-j_2)} &= ((A^{(H_{rt})} \circ A^{(K_{rt})})^R)_{i_2,m-j_2} \\ &= (A^{(H_{rt})} \circ A^{(K_{rt})})_{i_2,j_2+1} \\ &= A^{(K_{rt})}_{i_2,j_2+1} = A^{(y)}_{i_2,j_2+1} = (x,y), \end{aligned}$$

and

$$\begin{aligned} L_{(r-1)m+i_2,(t-1)m+(m+1-j_2)} &= ((A^{(H_{rt})} \circ A^{(K_{rt})})^R)_{i_2,m+1-j_2} \\ &= (A^{(H_{rt})} \circ A^{(K_{rt})})_{i_2,j_2} \\ &= A^{(H_{rt})}_{i_2,j_2} = A^{(w)}_{i_2,j_2} = (z,w). \end{aligned}$$

Finally, if t is even and j_2 is even, then

$$\begin{aligned} L_{(s-1)m+i_2,(t-1)m+(m-j_2)} &= ((A^{(H_{st})} \circ A^{(K_{st})})^R)_{i_2,m-j_2} \\ &= (A^{(H_{st})} \circ A^{(K_{st})})_{i_2,j_2+1} \\ &= A^{(H_{st})}_{i_2,j_2+1} = A^{(y)}_{i_2,j_2+1} = (x,y), \end{aligned}$$

and

$$\begin{aligned} L_{(s-1)m+i_2,(t-1)m+(m+1-j_2)} &= ((A^{(H_{st})} \circ A^{(K_{st})})^R)_{i_2,m+1-j_2} \\ &= (A^{(H_{st})} \circ A^{(K_{st})})_{i_2,j_2} \\ &= A^{(K_{st})}_{i_2,j_2} = A^{(w)}_{i_2,j_2} = (z,w). \end{aligned}$$

This completes Case 1.

Case 2: Suppose $x = z$.

Since H is row-complete, there exist i, j with $1 \leq i \leq n$ and $1 \leq j \leq n-1$, such that $(H_{ij}, H_{i,j+1}) = (y, w)$. Since A is a latin square, there exist u_1 and u_2 with $1 \leq u_1, u_2 \leq m$, such that $A_{u_1 m} = A_{u_2 1} = x$, so that $A^{(y)}_{u_1 m} = A^{(y)}_{u_2 1} = (x, y)$ and $A^{(w)}_{u_1 m} = A^{(w)}_{u_2 1} = (x, w) = (z, w)$.

If j is odd, then

$$\begin{aligned} L_{(i-1)m+u_1,(j-1)m+m} &= (A^{(H_{ij})} \circ A^{(K_{ij})})_{u_1 m} \\ &= A^{(H_{ij})}_{u_1 m} = A^{(y)}_{u_1 m} = (x,y), \end{aligned}$$

and

$$\begin{aligned} L_{(i-1)m+u_1,jm+1} &= ((A^{(H_{i,j+1})} \circ A^{(K_{i,j+1})})^R)_{u_1 1} \\ &= (A^{(H_{i,j+1})} \circ A^{(K_{i,j+1})})_{u_1 m} \\ &= A^{(H_{i,j+1})}_{u_1 m} = A^{(w)}_{u_1 m} = (z,w), \end{aligned}$$

while if j is even, then

$$\begin{aligned} L_{(i-1)m+u_2,(j-1)m+m} &= ((A^{(H_{ij})} \circ A^{(K_{ij})})^R)_{u_2 m} \\ &= (A^{(H_{ij})} \circ A^{(K_{ij})})_{u_2 1} \\ &= A^{(H_{ij})}_{u_2 1} = A^{(y)}_{u_2 1} = (x,y), \end{aligned}$$

and

$$\begin{aligned} L_{(i-1)m+u_2,jm+1} &= (A^{(H_{i,j+1})} \circ A^{(K_{i,j+1})})_{u_2 1} \\ &= A^{(H_{i,j+1})}_{u_2 1} = A^{(w)}_{u_2 1} = (z,w). \end{aligned}$$

This completes Case 2.

So L is row-complete, hence L is an $RCLS(mn)$, proving Theorem 2.3. ∎

Note that in the above proof, the fact that K is row-complete is never used. K merely needs to be a latin square which is orthogonal to the $RCLS(n)$ H such that H and K have property P.

The following are some useful corollaries of Theorem 2.3.

Corollary 2.4 *If there exists an $RCLS(m)$ and if there exist sequenceable groups of each of the orders $n_1, n_2, ..., n_k$ (where $n_1, n_2, ..., n_k$ are not necessarily distinct), then there exists an $RCLS(mn_1n_2 \cdots n_k)$.*

Proof Apply Theorem 2.3 repeatedly. ∎

Corollary 2.5 *If m is of the form $m = r \cdot 27^s(p_1q_1)^{t_1}(p_2q_2)^{t_2} \cdots (p_kq_k)^{t_k}$, where $r \in \{1, 9, 15, 25, 33\}$, $p_i < q_i$ are odd primes such that $p_i \mid q_i - 1$ and p_i has 2 as a* *primitive root* $(1 \leq i \leq k)$*, and* $k, s, t_1, t_2, ..., t_k$ *are non-negative integers, then an* $RCLS(m)$ *exists.*

Proof As mentioned in Section 1.1, groups of order 27 and p_iq_i (where p_i and q_i satisfy the stated conditions) have been sequenced, and $RCLS$ of orders 1, 9, 15, 25 and 33 have been found. Applying Corollary 2.4 then gives the result. ▮

It is interesting to note that setting $k = 0$ and $r = 1$ or 9 in Corollary 2.5, and letting s range over all the non-negative integers, gives an $RCLS(3^j)$ for each non-negative integer $j \equiv 0$ or 2 $(mod\ 3)$. $RCLS$ of these orders were not previously known to exist for $j > 3$.

Corollary 2.5 gives infinitely many new orders for which $RCLS$ can be constructed. Table 2.1 lists these new orders (indicated by an asterisk *) as well as the previously known odd orders, under 3000.

Table 2.1

Odd Orders of *RCLS* Known Prior to This Thesis

Plus New Orders Obtained via the Mesh Construction (up to 3000)

(* indicates new orders via the mesh construction)

1	9	15	21	25	27	33	39
55	57	93	111	129	155	183	189*
201	205	219	237	243*	253	291	305
309	315*	327	351*	355	381	405*	417
441*	453	471	489	495*	505	513*	525*
543	567*	579	585*	597	633	655	669
675*	687	689	693*	723	729*	737	755
813	819*	825*	831	837*	849	855*	891*
905	921	939	955	975*	979	993	999*
1011	1027	1047	1053*	1055	1101	1119	1137
1155*	1161*	1191	1197*	1205	1227	1255	1263
1287*	1299	1317	1355	1371	1375*	1389	1395*
1405	1425*	1461	1485*	1497	1521*	1539*	1555
1569	1623	1641	1647*	1655	1665*	1703	1711
1713	1731	1803	1809*	1815*	1821	1839	1845*
1857	1881*	1893	1929	1935*	1953*	1971*	1983
2005	2019	2041	2073	2105	2127	2133*	2145*
2155	2181	2189	2199	2217	2223*	2253	2271
2277	2305	2307	2325*	2331*	2361	2433	2455
2469	2487	2511*	2559	2577	2605	2619*	2631
2649	2705	2709*	2721	2745*	2757	2775*	2781*
2811	2855	2901	2943*	2973	2991	2997*	

Chapter 3

A Composite Order Direct Construction

3.1 Introduction

The highlight of this thesis is presented in this chapter, namely, a construction of a row-complete latin square of order n, where n is any odd composite number other than 9. Since row-complete latin squares of order 9 and of even order have previously been constructed, this proves that row-complete latin squares of every composite order exist.

The construction is presented in Sections 3.2 through 3.5. An example of the construction when the order is 35 (the smallest odd composite order for which an *RCLS* was not previously known to exist) is given in Section 3.6.

3.2 Generating Arrays

Throughout this chapter, let $q = p^\alpha$ be a power of an odd prime p with $q \neq 3$ (p can equal 3, but then $\alpha \geq 2$), and let m be an odd number with $m \geq 3$. Also, denote by F_q the finite field of order q and by Z_m the set of integers modulo m.

Define a *generating array* (see [2]) to be a $q \times mq$ array A defined on the symbol set $\mathsf{F}_q \times \mathsf{Z}_m$ such that, writing $A_{ij} = (x_{ij}, y_{ij})$ for $1 \leq i \leq q$ and $1 \leq j \leq mq$, the following conditions hold:

(G1) each symbol appears once in each row of A;

(G2) if $x_{i_1 j} = x_{i_2 j}$, then $i_1 = i_2$;

(G3) if $y_{i_1, j_1+1} - y_{i_1 j_1} = y_{i_2, j_2+1} - y_{i_2 j_2}$ and $(x_{i_1 j_1}, x_{i_1, j_1+1}) = (x_{i_2 j_2}, x_{i_2, j_2+1})$, then $(i_1, j_1) = (i_2, j_2)$.

Suppose A is a $q \times mq$ generating array (with $A_{ij} = (x_{ij}, y_{ij})$). Define L to be the $mq \times mq$ array on symbol set $\mathsf{F}_q \times \mathsf{Z}_m$ with

$$L_{kq+i,j} = (x_{ij}, y_{ij} + k)$$

for $1 \leq i \leq q, 1 \leq j \leq mq$ and $0 \leq k \leq m-1$ (and of course computations involving the first and second coordinates are carried out in F_q and Z_m respectively). As in [2], the following holds.

Theorem 3.1 *The array L defined above is an $RCLS(mq)$.*

Proof Suppose $L_{kq+i,j_1} = L_{kq+i,j_2}$. Then $x_{ij_1} = x_{ij_2}$ and $y_{ij_1} + k = y_{ij_2} + k$, so that $A_{ij_1} = A_{ij_2}$. By condition (G1), $j_1 = j_2$. So no symbol occurs more than once in any row of L.

Suppose $L_{k_1q+i_1,j} = L_{k_2q+i_2,j}$. Then $x_{i_1j} = x_{i_2j}$ and $y_{i_1j} + k_1 = y_{i_2j} + k_2$. Since $x_{i_1j} = x_{i_2j}$, it follows from condition (G2) that $i_1 = i_2$. But then $y_{i_1j} = y_{i_2j}$, and so $k_1 = k_2$. So no symbol occurs more than once in any column of L.

Therefore L is a latin square.

To show that L is row-complete, suppose

$$(L_{k_1q+i_1,j_1}, L_{k_1q+i_1,j_1+1}) = (L_{k_2q+i_2,j_2}, L_{k_2q+i_2,j_2+1}).$$

Then

$$(x_{i_1j_1}, y_{i_1j_1} + k_1) = (x_{i_2j_2}, y_{i_2j_2} + k_2)$$

and

$$(x_{i_1,j_1+1}, y_{i_1,j_1+1} + k_1) = (x_{i_2,j_2+1}, y_{i_2,j_2+1} + k_2).$$

Hence

$$(x_{i_1j_1}, x_{i_1,j_1+1}) = (x_{i_2j_2}, x_{i_2,j_2+1}),$$

and

$$\begin{aligned} y_{i_1,j_1+1} - y_{i_1,j_1} &= (y_{i_1,j_1+1} + k_1) - (y_{i_1,j_1} + k_1) \\ &= (y_{i_2,j_2+1} + k_2) - (y_{i_2,j_2} + k_2) \\ &= y_{i_2,j_2+1} - y_{i_2,j_2}, \end{aligned}$$

so by condition (G3), $(i_1, j_1) = (i_2, j_2)$.

Therefore L is row-complete, and so L is an $RCLS(mq)$. ■

So to construct an $RCLS(mq)$, it suffices to construct a $q \times mq$ generating array A (with $A_{ij} = (x_{ij}, y_{ij})$), which is what will now be discussed.

3.3 Choosing The y_{ij}'s - R-Sequenceability

In Sections 3.3 and 3.4, assume $m = 4r + 1$, where $r \geq 1$. The case $m = 4r + 3$ (with $r \geq 0$) is similar, and is dealt with in Section 3.5.

Set y to be constant along columns of A, that is, set

$$y_{ij} = s_j$$

for $1 \leq i \leq q$ and $1 \leq j \leq mq$, where the sequence s is to be determined.

Writing

$$d_j = s_{j+1} - s_j$$

for $1 \leq j \leq mq - 1$, condition (G3) then states that for each fixed $z \in \mathbb{Z}_m$, the ordered pairs $(x_{ij}, x_{i,j+1})$ for which $d_j = z$ must all be different. Since there are at most q^2 such ordered pairs, and since i is free to range from 1 to q, at most q of the d_j's can take on a fixed value z. Furthermore, if $z = 0$, then $y_{i,j+1} = s_{j+1} = s_j = y_{ij}$, hence by condition (G1), $x_{i,j+1} \neq x_{ij}$, and so by a similar argument as above, at most $q - 1$ of the d_j's can take on the value 0. A simple counting argument then shows that these upper bounds must be met, that is, exactly $q - 1$ of the d_j's must equal 0, and for fixed $z \neq 0$, exactly q of the d_j's must equal z.

So to summarize, the following are *necessary* conditions which the above sequence s must satisfy if A is to be a generating array:

(S1) each $z \in \mathbb{Z}_m$ appears q times in s;

(S2) each nonzero $z \in \mathbb{Z}_m$ appears q times as a difference $s_{j+1} - s_j$;

(S3) 0 appears $q - 1$ times as a difference $s_{j+1} - s_j$.

An additive group of order m is called *R-sequenceable* if there is an ordering $g_1 = 0, g_2, ..., g_m$ of its elements so that the partial sums $g_1 + g_2 + \ldots + g_i$ are all distinct for $1 \leq i \leq m-1$ (exactly one element does not occur among these partial sums). The ordering is then said to be an *R-sequencing* of the group.

The concept of R-sequenceability will be used to construct a sequence s satisfying conditions (S1), (S2) and (S3).

The following is the sequence of partial sums of the R-sequencing of Z_m (where $m = 4r+1$) given in [8]: $0, 4r, 1, 4r-1, ..., r-2, 3r+2, r-1, 3r+1, r, 3r-1, r+1, 3r-2, ..., 2r-2, 2r+1, 2r-1, 2r, 0$. By the definition of R-sequenceability, all of the numbers in the above sequence, except for the last, are distinct. Furthermore, each nonzero element of Z_m occurs once as a difference of consecutive terms in the sequence (and 0 occurs zero times as a difference). Deleting the last term 0 then gives a sequence z of length $m-1$, all of whose terms are distinct, and such that each nonzero element of Z_m occurs once as a difference of *cyclically* consecutive terms. In fact, the same properties will hold for any sequence which is obtained from z by cyclically shifting z and then adding a constant element of Z_m to each term of the resulting sequence.

In particular, these properties hold for the following sequence w obtained by adding $r+1$ to each term of z and then cyclically shifting the resulting sequence $2r$ places forward: $2r+1, 4r, 2r+2, 4r-1, ..., 3r-1, 3r+2, 3r, 3r+1, r+1, r, r+2, r-1, ..., 2r-1, 2, 2r, 1$.

Define the *reverse* of the sequence w, written $rev\, w$, to be the sequence obtained by reversing the order of the elements of w, and choose s to be the sequence which begins with $q-1$ 0's, followed by $q-1$ sequences w, followed by one sequence $rev\, w$, and then ends with a single 0.

Theorem 3.2 *The sequence s, chosen as above, satisfies conditions (S1), (S2) and (S3).*

Proof Condition (S1) clearly holds since, as mentioned above, each nonzero element of $\mathbb{Z}_m$ appears exactly once (and 0 does not appear at all) in w, and hence also in $rev\, w$. Also by the discussion above, the differences $s_{j+1} - s_j$ appearing in s are: $q-2$ 0's, followed by a single $2r+1$, followed by $q-1$ of each nonzero element of $\mathbb{Z}_m$ except $q-2$ of $(2r+1)-1 = 2r$, followed by a single 0, followed by one of each nonzero element of $\mathbb{Z}_m$ except $1-(2r+1) = 2r+1$, followed finally by a single $0-(2r+1) = 2r$. From this it is clear that conditions (S2) and (S3) hold. ∎

3.4 Choosing the x_{ij}'s - Component Squares

Let σ be a primitive element of $\mathbb{F}_q$ (i.e. a generator of the multiplicative group of nonzero elements of $\mathbb{F}_q$), and write $\mathbb{F}_q = \{f_1, f_2, ..., f_q\}$. To define the x_{ij}'s, latin squares of side q on symbol set $\mathbb{F}_q$ will be used. These latin squares will henceforth be called *component squares* . For $0 \le k \le m-1$, define the k^{th} component square $C^{(k)}$ by

$$C_{ij}^{(k)} = \begin{cases} a_k f_i + b_k \sigma^j + c_k & \text{if } 1 \le j \le q-1 \\ a_k f_i + c_k & \text{if } j = q \end{cases}$$

for $1 \le i, j \le q$, where a_k, b_k and c_k are constants in $\mathbb{F}_q$ to be determined later, and

$$a_k, b_k \ne 0 \quad (0 \le k \le m-1). \tag{3.1}$$

Since a_k and b_k are nonzero, and since σ is a primitive element, $C^{(k)}$ is a latin square.

For $1 \le j \le mq$, suppose symbol s_j occurs for the t_j^{th} time at position j of the sequence s (i.e. $t_j = |\{j' : s_{j'} = s_j, 1 \le j' \le j\}|$). So specifically, t is the sequence which begins with $1, 2, ..., q-1$, followed by $m-1$ 1's, $m-1$ 2's,..., $m-1$ q's, and which ends with a single q.

Set the j^{th} column of x's in A to be the t_j^{th} column of the s_j^{th} component square, that is,

$$x_{ij} = C^{(s_j)}_{i,t_j}$$

for $1 \leq i \leq q$ and $1 \leq j \leq mq$.

Clearly the ordered pairs (s_j, t_j) are all distinct. Therefore condition (G1) is now satisfied, since if $A_{ij_1} = A_{ij_2}$, then $s_{j_1} = y_{ij_1} = y_{ij_2} = s_{j_2}$ and also $C^{(s_{j_1})}_{i,t_{j_1}} = x_{ij_1} = x_{ij_2} = C^{(s_{j_2})}_{i,t_{j_2}} = C^{(s_{j_1})}_{i,t_{j_2}}$, so that $t_{j_1} = t_{j_2}$ (since the $C^{(k)}$'s are latin squares), and hence $j_1 = j_2$.

Furthermore, A satisfies condition (G2), since if $x_{i_1 j} = x_{i_2 j}$, then $C^{(s_j)}_{i_1,t_j} = C^{(s_j)}_{i_2,t_j}$, and so since the $C^{(k)}$'s are latin squares, $i_1 = i_2$.

The rest of this section deals with finding values of the a_k's, b_k's and c_k's for which A satisfies condition (G3) (and hence is a generating array).

Condition (G3) requires that, for each fixed $d \in \mathbb{Z}_m$, all of the ordered pairs

$$(C^{(s_j)}_{i,t_j}, C^{(s_{j+1})}_{i,t_{j+1}}),$$

where $1 \leq i \leq q$, $1 \leq j \leq mq$ and $s_{j+1} - s_j = d$, be distinct.

There are seven cases.

Case 1: $d = 0$.

The relevant ordered pairs are $(C^{(0)}_{iv}, C^{(0)}_{i,v+1})$ and $(C^{(1)}_{i,q-1}, C^{(1)}_{i,q})$ for $1 \leq i \leq q$ and $1 \leq v \leq q-2$, that is (using $\sigma^{q-1} = 1$),

$$(a_0 f_i + b_0\sigma^v + c_0, a_0 f_i + b_0\sigma^{v+1} + c_0)$$

and

$$(a_1 f_i + b_1 + c_1, a_1 f_i + c_1).$$

Since $a_0 f_i + b_0\sigma^v + c_0$ and $a_1 f_i + b_1 + c_1$ both range over all of the elements of F_q as i ranges from 1 to q and v is fixed, these are precisely the ordered pairs

$$(u, u + b_0\sigma^v(\sigma - 1))$$

and

$$(u, u - b_1),$$

where $u \in \mathsf{F}_q$ and $1 \leq v \leq q-2$. Now for fixed u, the values $u + b_0\sigma^v(\sigma - 1)$ are all distinct as v varies from 1 to $q-2$, (since $b_0 \neq 0$ and since σ is a primitive element of F_q). The ordered pair $(u, u + b_0(\sigma - 1))$ is missing, and so $b_0(\sigma - 1)$ should be set to $-b_1$. Thus the only additional condition arising from this case is

$$b_1 = (1 - \sigma)b_0. \tag{3.2}$$

The next four cases are similar to each other.

Case 2: $d = 2h - 1$ for $1 \leq h \leq r$.

The relevant ordered pairs are $(C_{iv}^{(3r-h+1)}, C_{iv}^{(3r+h)})$ and $(C_{iq}^{(r-h+1)}, C_{iq}^{(r+h)})$ for $1 \leq i \leq q$ and $1 \leq v \leq q-1$, that is

$$(a_{3r-h+1} f_i + b_{3r-h+1}\sigma^v + c_{3r-h+1}, a_{3r+h} f_i + b_{3r+h}\sigma^v + c_{3r+h})$$

and

$$(a_{r-h+1} f_i + c_{r-h+1}, a_{r+h} f_i + c_{r+h}).$$

Since $a_{3r-h+1} f_i + b_{3r-h+1}\sigma^v + c_{3r-h+1}$ and $a_{r-h+1} f_i + c_{r-h+1}$ both range over all of the elements of F_q as i ranges from 1 to q and v is fixed, these are precisely the ordered pairs

$$\left(u, \frac{a_{3r+h}}{a_{3r-h+1}}u + (b_{3r+h} - \frac{a_{3r+h}}{a_{3r-h+1}}b_{3r-h+1})\sigma^v + c_{3r+h} - \frac{a_{3r+h}}{a_{3r-h+1}}c_{3r-h+1}\right)$$

and

$$\left(u, \frac{a_{r+h}}{a_{r-h+1}}u + c_{r+h} - \frac{a_{r+h}}{a_{r-h+1}}c_{r-h+1}\right),$$

where $u \in \mathsf{F}_q$ and $1 \leq v \leq q-1$.

Setting

$$\frac{a_{3r+h}}{a_{3r-h+1}} = \frac{a_{r+h}}{a_{r-h+1}} \quad (1 \leq h \leq r), \tag{3.3}$$

$$b_{3r+h} - \frac{a_{3r+h}}{a_{3r-h+1}}b_{3r-h+1} \neq 0,$$

that is

$$\frac{b_{3r+h}}{b_{3r-h+1}} \neq \frac{a_{3r+h}}{a_{3r-h+1}} \quad (1 \leq h \leq r), \tag{3.4}$$

and

$$c_{3r+h} - \frac{a_{3r+h}}{a_{3r-h+1}}c_{3r-h+1} = c_{r+h} - \frac{a_{r+h}}{a_{r-h+1}}c_{r-h+1},$$

that is

$$c_{3r+h} - c_{r+h} = \frac{a_{r+h}}{a_{r-h+1}}(c_{3r-h+1} - c_{r-h+1}) \quad (1 \leq h \leq r), \tag{3.5}$$

it is evident by an analysis similar to that in Case 1 that all the ordered pairs in this case will then be distinct.

Case 3: $d = 2r + 2h - 1$ for $2 \leq h \leq r$.

The relevant ordered pairs here are $(C_{iv}^{(4r-h+2)}, C_{iv}^{(2r+h)})$ and $(C_{iq}^{(2r-h+2)}, C_{iq}^{(h)})$ for $1 \leq i \leq q$ and $1 \leq v \leq q-1$.

By an analogous argument to that given in Case 2, setting

$$\frac{a_{2r+h}}{a_{4r-h+2}} = \frac{a_h}{a_{2r-h+2}} \quad (2 \leq h \leq r), \tag{3.6}$$

$$\frac{b_{2r+h}}{b_{4r-h+2}} \neq \frac{a_{2r+h}}{a_{4r-h+2}} \quad (2 \leq h \leq r), \tag{3.7}$$

and

$$c_{2r+h} - c_h = \frac{a_h}{a_{2r-h+2}}(c_{4r-h+2} - c_{2r-h+2}) \quad (2 \leq h \leq r), \tag{3.8}$$

forces all of the ordered pairs in this case to be distinct.

Case 4: $d = 2r - 2h + 2$ for $2 \leq h \leq r$.

The relevant ordered pairs are $(C_{iv}^{(h)}, C_{iv}^{(2r-h+2)})$ and $(C_{iq}^{(2r+h)}, C_{iq}^{(4r-h+2)})$ for $1 \leq i \leq q$ and $1 \leq v \leq q-1$.

By an analogous argument to that given in Case 2, setting

$$\frac{a_{2r-h+2}}{a_h} = \frac{a_{4r-h+2}}{a_{2r+h}} \quad (2 \leq h \leq r), \tag{3.9}$$

$$\frac{b_{2r-h+2}}{b_h} \neq \frac{a_{2r-h+2}}{a_h} \quad (2 \leq h \leq r), \tag{3.10}$$

and

$$c_{2r-h+2} - c_{4r-h+2} = \frac{a_{4r-h+2}}{a_{2r+h}}(c_h - c_{2r+h}) \quad (2 \leq h \leq r), \tag{3.11}$$

forces all of the ordered pairs in this case to be distinct.

Case 5: $d = 4r - 2h + 2$ for $1 \leq h \leq r$.

The relevant ordered pairs here are $(C_{iv}^{(r+h)}, C_{iv}^{(r-h+1)})$ and $(C_{iq}^{(3r+h)}, C_{iq}^{(3r-h+1)})$ for $1 \leq i \leq q$ and $1 \leq v \leq q-1$.

By an analogous argument to that given in Case 2, setting

$$\frac{a_{r-h+1}}{a_{r+h}} = \frac{a_{3r-h+1}}{a_{3r+h}} \quad (1 \leq h \leq r), \tag{3.12}$$

$$\frac{b_{r-h+1}}{b_{r+h}} \neq \frac{a_{r-h+1}}{a_{r+h}} \quad (1 \leq h \leq r), \tag{3.13}$$

and

$$c_{r-h+1} - c_{3r-h+1} = \frac{a_{3r-h+1}}{a_{3r+h}}(c_{r+h} - c_{3r+h}) \quad (1 \leq h \leq r), \tag{3.14}$$

forces all of the ordered pairs in this case to be distinct.

The last two cases are somewhat different.

Case 6: $d = 2r$.

The ordered pairs under consideration here are $(C_{iv}^{(1)}, C_{i,v+1}^{(2r+1)})$, $(C_{iq}^{(r+1)}, C_{iq}^{(3r+1)})$ and $(C_{iq}^{(2r+1)}, C_{iq}^{(0)})$ for $1 \leq i \leq q$ and $1 \leq v \leq q-2$, that is

$$(a_1 f_i + b_1\sigma^v + c_1, a_{2r+1}f_i + b_{2r+1}\sigma^{v+1} + c_{2r+1}),$$

$$(a_{r+1}f_i + c_{r+1}, a_{3r+1}f_i + c_{3r+1}),$$

and

$$(a_{2r+1}f_i + c_{2r+1}, a_0 f_i + c_0).$$

Since $a_1 f_i + b_1\sigma^v + c_1$, $a_{r+1}f_i + c_{r+1}$ and $a_{2r+1}f_i + c_{2r+1}$ all range over all of the elements of F_q as i ranges from 1 to q and v is fixed, these are precisely the ordered pairs

$$\left(u, \frac{a_{2r+1}}{a_1}u + (b_{2r+1}\sigma - \frac{a_{2r+1}}{a_1}b_1)\sigma^v + c_{2r+1} - \frac{a_{2r+1}}{a_1}c_1\right),$$
$$\left(u, \frac{a_{3r+1}}{a_{r+1}}u + c_{3r+1} - \frac{a_{3r+1}}{a_{r+1}}c_{r+1}\right),$$

and

$$\left(u, \frac{a_0}{a_{2r+1}}u + c_0 - \frac{a_0}{a_{2r+1}}c_{2r+1}\right),$$

where $u \in \mathsf{F}_q$ and $1 \leq v \leq q-2$.

Setting

$$\frac{a_{2r+1}}{a_1} = \frac{a_{3r+1}}{a_{r+1}} = \frac{a_0}{a_{2r+1}}, \tag{3.15}$$

$$b_{2r+1}\sigma - \frac{a_{2r+1}}{a_1}b_1 \neq 0,$$

that is,

$$\frac{b_1}{b_{2r+1}} \neq \sigma\frac{a_1}{a_{2r+1}}, \tag{3.16}$$

$$b_{2r+1}\sigma - \frac{a_{2r+1}}{a_1}b_1 + c_{2r+1} - \frac{a_{2r+1}}{a_1}c_1 = c_0 - \frac{a_0}{a_{2r+1}}c_{2r+1}, \tag{3.17}$$

and

$$c_{2r+1} - \frac{a_{2r+1}}{a_1}c_1 = c_{3r+1} - \frac{a_{3r+1}}{a_{r+1}}c_{r+1}, \tag{3.18}$$

it follows by an analysis similar to that in Case 1 that all the ordered pairs in this case will then be distinct.

Case 7: $d = 2r + 1$.

The relevant ordered pairs are $(C_{i,q-1}^{(0)}, C_{i1}^{(2r+1)})$ and $(C_{iv}^{(3r+1)}, C_{iv}^{(r+1)})$ for $1 \leq i \leq q$ and $1 \leq v \leq q-1$, that is

$$(a_0 f_i + b_0 + c_0, a_{2r+1} f_i + b_{2r+1}\sigma + c_{2r+1})$$

and

$$(a_{3r+1} f_i + b_{3r+1}\sigma^v + c_{3r+1}, a_{r+1} f_i + b_{r+1}\sigma^v + c_{r+1}).$$

Since $a_0 f_i + b_0 + c_0$ and $a_{3r+1} f_i + b_{3r+1}\sigma^v + c_{3r+1}$ both range over all of the elements of F_q as i ranges from 1 to q and v is fixed, these are precisely the ordered pairs

$$\left(u, \frac{a_{2r+1}}{a_0}u + b_{2r+1}\sigma + c_{2r+1} - \frac{a_{2r+1}}{a_0}b_0 - \frac{a_{2r+1}}{a_0}c_0\right)$$

and

$$\left(u, \frac{a_{r+1}}{a_{3r+1}}u + (b_{r+1} - \frac{a_{r+1}}{a_{3r+1}}b_{3r+1})\sigma^v + c_{r+1} - \frac{a_{r+1}}{a_{3r+1}}c_{3r+1}\right),$$

where $u \in \mathsf{F}_q$ and $1 \leq v \leq q-1$.

Setting

$$\frac{a_{2r+1}}{a_0} = \frac{a_{r+1}}{a_{3r+1}}, \tag{3.19}$$

$$b_{r+1} - \frac{a_{r+1}}{a_{3r+1}}b_{3r+1} \neq 0,$$

that is

$$\frac{b_{r+1}}{b_{3r+1}} \neq \frac{a_{r+1}}{a_{3r+1}}, \tag{3.20}$$

and

$$c_{r+1} - \frac{a_{r+1}}{a_{3r+1}} c_{3r+1} = b_{2r+1}\sigma + c_{2r+1} - \frac{a_{2r+1}}{a_0} b_0 - \frac{a_{2r+1}}{a_0} c_0, \qquad (3.21)$$

it follows by an analysis similar to that in Case 1 that all the ordered pairs in this case will then be distinct.

This completes the seven cases.

So whenever the a_k's, b_k's and c_k's satisfy conditions (3.1) through (3.21) above (some of which are actually redundant, e.g. (3.9) follows from (3.1) and (3.6)), then condition (G3) is satisfied and A is a $q \times mq$ generating array (and so an $RCLS(mq)$ exists by Theorem 3.1).

Theorem 3.3 *Suppose $\sigma \neq 2$, and set $a_0 = ... = a_{2r} = 1, a_{2r+1} = ... = a_{4r} = -1, b_0 = 1, b_1 = 1 - \sigma, b_2 = ...b_r = 1, b_{r+1} = ... = b_{2r} = -1, b_{2r+1} = ... = b_{3r} = \frac{1}{2} - \frac{1}{\sigma}, b_{3r+1} = ... = b_{4r} = \frac{1}{2}, c_0 = -\frac{\sigma}{2}$ and $c_1 = ... = c_{4r} = 0$. Then the a_k's, b_k's and c_k's satisfy conditions (3.1) through (3.21).*

Proof Condition (3.1) holds since $\sigma \neq 2$, and condition (3.2) clearly also holds. Both the left and right-hand sides of (3.3), (3.6), (3.9) and (3.12) equal 1, so these conditions hold. Both the left and right-hand sides of (3.5), (3.8), (3.11), (3.14) and (3.18) equal 0, so these conditions also hold. (3.4) holds since the left-hand side is $\frac{\sigma}{\sigma-2}$ (recall $\sigma \neq 2$), which is unequal to the right-hand side value of 1. (3.7) holds since the left-hand side is $\frac{\sigma-2}{\sigma}$, which is unequal to the right-hand side value of 1. (3.10) holds since the left-hand side is -1, which is unequal to the right-hand side value of 1. (3.13) holds since, for $1 \leq h \leq r - 1$, the left-hand side value of -1 is unequal to the right-hand side value of 1, and for $h = r$, the left-hand side value of $\sigma - 1$ is unequal to the right-hand side value of 1 (since $\sigma \neq 2$). Condition (3.15) holds since all three expressions equal -1. (3.16) holds since the left-hand side is $\frac{-\sigma(2\sigma-2)}{\sigma-2}$ (recall $\sigma \neq 2$), which is unequal to the right-hand side value of $-\sigma$. (3.17) holds since both the left and right-hand sides equal $-\frac{\sigma}{2}$. (3.19) holds since both the left and right-hand sides equal -1. (3.20) holds since the left-hand side is -2, which is unequal to the right-hand side value of -1. Finally, condition (3.21) holds since both the left and right-hand sides equal 0. ∎

Now it is well-known that there are $\phi(q-1)$ primitive elements in F_q. Also, $\phi(q-1) \geq 2$ since $q \geq 5$. So F_q has a primitive element $\sigma \neq 2$, completing the proof of the following theorem.

Theorem 3.4 *There exists an $RCLS(mq)$ whenever $m \equiv 1$ (mod 4), $m \geq 5$, and q is an odd prime power, $q \neq 3$.*

Once again, the reader is referred to Section 3.6, in which the construction is illustrated with an example.

3.5 The Case $m = 4r + 3$

In this section, the case $m = 4r + 3$, where $r \geq 0$, is dealt with. The analysis is similar to the $m = 4r + 1$ case, with only minor modifications, and so the details will be kept to a minimum. Also, the same notation will be used here.

The following is the sequence of partial sums of the R-sequencing of $\mathbb{Z}_m$ (where $m = 4r + 3$) given in [8]: $0, 4r + 2, 1, 4r + 1, ..., r - 2, 3r + 4, r - 1, 3r + 3, r, 3r + 1, r + 1, 3r, r + 2, 3r - 1, ..., 2r - 1, 2r + 2, 2r, 2r + 1, 0$. Deleting the last term 0 gives the sequence z. Adding $r + 1$ to each term of z, taking the reverse of the resulting sequence (note that this was not necessary in the $m = 4r + 1$ case), and then cyclically shifting that sequence $2r + 1$ places forward gives the sequence w, which is: $2r+1, 1, 2r, 2, ..., r+3, r-1, r+2, r, r+1, 3r+2, 3r+1, 3r+3, 3r, 3r+4, ..., 4r, 2r+3, 4r+1, 2r+2, 4r+2$. Again s is the sequence which begins with $q-1$ 0's, followed by $q-1$ sequences w, followed by one sequence *rev* w, and then ends with a single 0.

As in the $m = 4r+1$ case, set

$$a_k, b_k \neq 0 \quad (0 \leq k \leq m-1), \tag{3.22}$$

so that the $C^{(k)}$'s will be latin squares.

There are once again seven cases to consider, depending on the value of $d = s_{j+1} - s_j$. Just the relevant ordered pairs and the resulting conditions will be listed, as their derivation is similar to the $m = 4r+1$ case.

Case 1: $d = 0$.

The relevant ordered pairs are $(C^{(0)}_{iv}, C^{(0)}_{i,v+1})$ and $(C^{(4r+2)}_{i,q-1}, C^{(4r+2)}_{i,q})$ for $1 \leq i \leq q$ and $1 \leq v \leq q-2$, and the only condition arising from this case is

$$b_{4r+2} = (1-\sigma)b_0. \tag{3.23}$$

Case 2: $d = 2h-1$ for $1 \leq h \leq r$.

The relevant ordered pairs here are $(C^{(r-h+1)}_{iv}, C^{(r+h)}_{iv})$ and $(C^{(3r-h+2)}_{iq}, C^{(3r+h+1)}_{iq})$ for $1 \leq i \leq q$ and $1 \leq v \leq q-1$, and the conditions are

$$\frac{a_{r+h}}{a_{r-h+1}} = \frac{a_{3r+h+1}}{a_{3r-h+2}} \quad (1 \leq h \leq r), \tag{3.24}$$

$$\frac{b_{r+h}}{b_{r-h+1}} \neq \frac{a_{r+h}}{a_{r-h+1}} \quad (1 \leq h \leq r), \tag{3.25}$$

and

$$c_{r+h} - c_{3r+h+1} = \frac{a_{3r+h+1}}{a_{3r-h+2}}(c_{r-h+1} - c_{3r-h+2}) \quad (1 \leq h \leq r). \tag{3.26}$$

Case 3: $d = 2r + 2h + 1$ for $1 \leq h \leq r$.

The relevant ordered pairs here are $(C_{iv}^{(2r-h+2)}, C_{iv}^{(h)})$ and $(C_{iq}^{(4r-h+3)}, C_{iq}^{(2r+h+1)})$ for $1 \leq i \leq q$ and $1 \leq v \leq q-1$, and the conditions are

$$\frac{a_h}{a_{2r-h+2}} = \frac{a_{2r+h+1}}{a_{4r-h+3}} \quad (1 \leq h \leq r), \tag{3.27}$$

$$\frac{b_h}{b_{2r-h+2}} \neq \frac{a_h}{a_{2r-h+2}} \quad (1 \leq h \leq r), \tag{3.28}$$

and

$$c_h - c_{2r+h+1} = \frac{a_{2r+h+1}}{a_{4r-h+3}}(c_{2r-h+2} - c_{4r-h+3}) \quad (1 \leq h \leq r). \tag{3.29}$$

Case 4: $d = 2r - 2h + 2$ for $1 \leq h \leq r$.

The ordered pairs under consideration in this case are $(C_{iv}^{(2r+h+1)}, C_{iv}^{(4r-h+3)})$ and $(C_{iq}^{(h)}, C_{iq}^{(2r-h+2)})$ for $1 \leq i \leq q$ and $1 \leq v \leq q-1$, and the conditions are

$$\frac{a_{4r-h+3}}{a_{2r+h+1}} = \frac{a_{2r-h+2}}{a_h} \quad (1 \leq h \leq r), \tag{3.30}$$

$$\frac{b_{4r-h+3}}{b_{2r+h+1}} \neq \frac{a_{4r-h+3}}{a_{2r+h+1}} \quad (1 \leq h \leq r), \tag{3.31}$$

and

$$c_{4r-h+3} - c_{2r-h+2} = \frac{a_{2r-h+2}}{a_h}(c_{2r+h+1} - c_h) \quad (1 \leq h \leq r). \tag{3.32}$$

Case 5: $d = 4r - 2h + 4$ for $1 \leq h \leq r$.

The ordered pairs under consideration in this case are $(C_{iv}^{(3r+h+1)}, C_{iv}^{(3r-h+2)})$ and $(C_{iq}^{(r+h)}, C_{iq}^{(r-h+1)})$ for $1 \leq i \leq q$ and $1 \leq v \leq q-1$, and the conditions are

$$\frac{a_{3r-h+2}}{a_{3r+h+1}} = \frac{a_{r-h+1}}{a_{r+h}} \quad (1 \leq h \leq r), \tag{3.33}$$

$$\frac{b_{3r-h+2}}{b_{3r+h+1}} \neq \frac{a_{3r-h+2}}{a_{3r+h+1}} \quad (1 \leq h \leq r), \tag{3.34}$$

and

$$c_{3r-h+2} - c_{r-h+1} = \frac{a_{r-h+1}}{a_{r+h}}(c_{3r+h+1} - c_{r+h}) \quad (1 \leq h \leq r). \tag{3.35}$$

<u>Case 6</u>: $d = 2r + 2$.

The ordered pairs under consideration are $(C_{iv}^{(4r+2)}, C_{i,v+1}^{(2r+1)})$, $(C_{iq}^{(3r+2)}, C_{iq}^{(r+1)})$ and $(C_{iq}^{(2r+1)}, C_{iq}^{(0)})$ for $1 \leq i \leq q$ and $1 \leq v \leq q-2$, and the conditions are

$$\frac{a_{2r+1}}{a_{4r+2}} = \frac{a_{r+1}}{a_{3r+2}} = \frac{a_0}{a_{2r+1}}, \tag{3.36}$$

$$\frac{b_{4r+2}}{b_{2r+1}} \neq \sigma\frac{a_{4r+2}}{a_{2r+1}}, \tag{3.37}$$

$$b_{2r+1}\sigma - \frac{a_{2r+1}}{a_{4r+2}}b_{4r+2} + c_{2r+1} - \frac{a_{2r+1}}{a_{4r+2}}c_{4r+2} = c_0 - \frac{a_0}{a_{2r+1}}c_{2r+1}, \tag{3.38}$$

and

$$c_{2r+1} - \frac{a_{2r+1}}{a_{4r+2}}c_{4r+2} = c_{r+1} - \frac{a_{r+1}}{a_{3r+2}}c_{3r+2}. \tag{3.39}$$

<u>Case 7</u>: $d = 2r + 1$.

The relevant ordered pairs are $(C_{i,q-1}^{(0)}, C_{i1}^{(2r+1)})$ and $(C_{iv}^{(r+1)}, C_{iv}^{(3r+2)})$ for $1 \leq i \leq q$ and $1 \leq v \leq q-1$, and the conditions are

$$\frac{a_{2r+1}}{a_0} = \frac{a_{3r+2}}{a_{r+1}}, \tag{3.40}$$

$$\frac{b_{3r+2}}{b_{r+1}} \neq \frac{a_{3r+2}}{a_{r+1}}, \tag{3.41}$$

and

$$c_{3r+2} - \frac{a_{3r+2}}{a_{r+1}}c_{r+1} = b_{2r+1}\sigma + c_{2r+1} - \frac{a_{2r+1}}{a_0}b_0 - \frac{a_{2r+1}}{a_0}c_0. \tag{3.42}$$

This completes the seven cases.

So whenever the a_k's, b_k's and c_k's satisfy conditions (3.22) through (3.42) above (some of which are actually redundant, e.g. (3.30) follows from (3.22) and (3.27)), then condition (G3) is satisfied and A is a $q \times mq$ generating array (and so an $RCLS(mq)$ exists by Theorem 3.1).

Theorem 3.5 *Suppose $\sigma \neq 2$ and $3\sigma \neq 2$, and set $a_0 = \ldots = a_{2r} = 1, a_{2r+1} = \ldots = a_{4r+1} = -1, a_{4r+2} = 1, b_0 = \ldots = b_r = 1, b_{r+1} = \ldots = b_{2r} = -1, b_{2r+1} = \frac{1}{2} - \frac{1}{\sigma}, b_{2r+2} = \ldots = b_{3r+1} = 1, b_{3r+2} = \ldots = b_{4r+1} = -1, b_{4r+2} = 1 - \sigma, c_0 = -\frac{\sigma}{2}$ and $c_1 = \ldots = c_{4r+2} = 0$. Then the a_k's, b_k's and c_k's satisfy conditions (3.22) through (3.42).*

Proof Condition (3.22) holds since $\sigma \neq 2$, and condition (3.23) clearly also holds. Both the left and right-hand sides of (3.24) and (3.33) equal 1, so these conditions hold. Both the left and right-hand sides of (3.27) and (3.30) equal -1 when $h = 1$ and 1 when $2 \leq h \leq r$, so these conditions hold. Both the left and right-hand sides of (3.26), (3.29), (3.32), (3.35) and (3.39) equal 0, so these conditions also hold. (3.25) holds since the left-hand side is -1, which is unequal to the right-hand side value of 1. (3.28) holds since, when $h = 1$, the left-hand side value of $\frac{2\sigma}{\sigma-2}$ (recall $\sigma \neq 2$) is unequal to the right-hand side value of -1 (since $3\sigma \neq 2$), and when $2 \leq h \leq r$, the left-hand side value of -1 is unequal to the right-hand side value of 1. (3.31) holds since, when $h = 1$, the left-hand side value of $1 - \sigma$ is unequal to the right-hand side value of -1 (since $\sigma \neq 2$), and when $2 \leq h \leq r$, the left-hand side value of -1 is unequal to the right-hand side value of 1. (3.34) holds since the left-hand side equals -1, which is unequal to the right-hand side value of 1. Condition (3.36) holds since all three expressions equal -1. (3.37) holds since the left-hand side equals $\frac{-\sigma(2\sigma-2)}{\sigma-2}$ (recall $\sigma \neq 2$), which is unequal to the right-hand side value of $-\sigma$. (3.38) holds since both the left and right-hand sides equal $-\frac{\sigma}{2}$. (3.40) holds since both the left and right-hand sides equal -1. (3.41) holds since the left-hand side is 1, which is unequal to the right-hand side value of -1. Finally, condition (3.42) holds since both the left and right-hand sides equal 0. ∎

Observe that 3 and 5 are primitive elements of $\mathbb{F}_5$ and $\mathbb{F}_7$ respectively, which satisfy both of the conditions imposed on σ in Theorem 3.5. Also, since there are $\phi(q-1)$ primitive elements in F_q, and since $\phi(q-1) \geq 3$ when $q \geq 9$, it follows that F_q also has a primitive element σ satisfying $\sigma \neq 2$ and $3\sigma \neq 2$ when $q \geq 9$ (note that at most one $\sigma \in \mathsf{F}_q$ satisfies $3\sigma = 2$), completing the proof of the following theorem.

Theorem 3.6 *There exists an $RCLS(mq)$ whenever $m \equiv 3$ $(mod\ 4)$, $m \geq 3$, and q is an odd prime power, $q \neq 3$.*

Theorems 3.4 and 3.6, combined with the facts (mentioned in Section 1.1) that *RCLS* of order 9 and of every even order have been constructed, give the following main theorem, the most important result in this thesis.

Theorem 3.7 *There exists an $RCLS(n)$ whenever n is composite.*

Proof By the remarks above, it suffices to consider the case when n is odd and not equal to 9. Clearly such an n has an odd prime power factor q with $q \neq 3$ and $q < n$. But then $n = mq$ for some odd number $m \geq 3$. Invoking Theorems 3.4 and 3.6 when $m \equiv 1$ or 3 $(mod\ 4)$, respectively, completes the proof. ∎

The question as to whether there exist *RCLS* of odd prime order remains open. Currently, the only known result relating to this question is that there do not exist *RCLS* of orders 3, 5 or 7. Also, as an aside, several authors have studied the question of whether or not a given row-complete latin square can be made to be *column-complete* (i.e. to have a row-complete transpose) by suitably reordering its rows. It turns out that this is not always the case (see e.g. [2] or [6]).

3.6 An Example

In this section, an $RCLS(35)$ is constructed to illustrate the method described above. Note that 35 is the smallest composite order n for which an $RCLS(n)$ was previously not known to exist.

Take $m = 5$ and $q = 7$ (one could also take $m = 7$ and $q = 5$). Then $m = 4r + 1$ where $r = 1$, and so w is the sequence $3, 4, 2, 1$. Therefore, s is the sequence

$$0\,0\,0\,0\,0\,0\,3\,4\,2\,1\,3\,4\,2\,1\,3\,4\,2\,1\,3\,4\,2\,1\,3\,4\,2\,1\,3\,4\,2\,1\,1\,2\,4\,3\,0.$$

As in Theorem 3.3, set $\sigma = 3$, a primitive element of F_7 not equal to 2, and set $a_0 = a_1 = a_2 = 1, a_3 = a_4 = -1, b_0 = 1, b_1 = 1 - \sigma = -2, b_2 = -1, b_3 = \frac{1}{2} - \frac{1}{\sigma} = 4 - 5 = -1, b_4 = \frac{1}{2} = 4, c_0 = -\frac{\sigma}{2} = -3 \cdot 4 = 2$, and $c_1 = c_2 = c_3 = c_4 = 0$. Write $f_i = i$ for $1 \leq i \leq 7$. Then $C^{(0)}, C^{(1)}, C^{(2)}, C^{(3)}$ and $C^{(4)}$ (in that order) are the following component squares.

```
6 5 2 0 1 4 3   2 4 3 0 5 6 1   5 6 2 4 3 0 1   3 4 0 2 1 5 6   4 0 2 1 5 3 6
0 6 3 1 2 5 4   3 5 4 1 6 0 2   6 0 3 5 4 1 2   2 3 6 1 0 4 5   3 6 1 0 4 2 5
1 0 4 2 3 6 5   4 6 5 2 0 1 3   0 1 4 6 5 2 3   1 2 5 0 6 3 4   2 5 0 6 3 1 4
2 1 5 3 4 0 6   5 0 6 3 1 2 4   1 2 5 0 6 3 4   0 1 4 6 5 2 3   1 4 6 5 2 0 3
3 2 6 4 5 1 0   6 1 0 4 2 3 5   2 3 6 1 0 4 5   6 0 3 5 4 1 2   0 3 5 4 1 6 2
4 3 0 5 6 2 1   0 2 1 5 3 4 6   3 4 0 2 1 5 6   5 6 2 4 3 0 1   6 2 4 3 0 5 1
5 4 1 6 0 3 2   1 3 2 6 4 5 0   4 5 1 3 2 6 0   4 5 1 3 2 6 0   5 1 3 2 6 4 0
```

Writing $x + 7y + 1$ for $(x, y) \in \mathsf{F}_7 \times \mathsf{Z}_5$, then A is the following 7×35 generating array.

```
7 6 3 1 2 5 25 33 20 10 26 29 21 12 22 31 17 11 24 30 19  8 23 34 18 13 27 32 15 14  9 16 35 28 4
1 7 4 2 3 6 24 32 21 11 25 35 15 13 28 30 18 12 23 29 20  9 22 33 19 14 26 31 16  8 10 17 34 27 5
2 1 5 3 4 7 23 31 15 12 24 34 16 14 27 29 19 13 22 35 21 10 28 32 20  8 25 30 17  9 11 18 33 26 6
3 2 6 4 5 1 22 30 16 13 23 33 17  8 26 35 20 14 28 34 15 11 27 31 21  9 24 29 18 10 12 19 32 25 7
4 3 7 5 6 2 28 29 17 14 22 32 18  9 25 34 21  8 27 33 16 12 26 30 15 10 23 35 19 11 13 20 31 24 1
5 4 1 6 7 3 27 35 18  8 28 31 19 10 24 33 15  9 26 32 17 13 25 29 16 11 22 34 20 12 14 21 30 23 2
6 5 2 7 1 4 26 34 19  9 27 30 20 11 23 32 16 10 25 31 18 14 24 35 17 12 28 33 21 13  8 15 29 22 3
```

Finally, the $RCLS(35)$ L is shown in Figure 3.1.

Figure 3.1
An $RCLS(35)$

7	6	3	1	2	5	25	33	20	10	26	29	21	12	22	31	17	11	24	30	19	8	23	34	18	13	27	32	15	14	9	16	35	28	4
1	7	4	2	3	6	24	32	21	11	25	35	15	13	28	30	18	12	23	29	20	9	22	33	19	14	26	31	16	8	10	17	34	27	5
2	1	5	3	4	7	23	31	15	12	24	34	16	14	27	29	19	13	22	35	21	10	28	32	20	8	25	30	17	9	11	18	33	26	6
3	2	6	4	5	1	22	30	16	13	23	33	17	8	26	35	20	14	28	34	15	11	27	31	21	9	24	29	18	10	12	19	32	25	7
4	3	7	5	6	2	28	29	17	14	22	32	18	9	25	34	21	8	27	33	16	12	26	30	15	10	23	35	19	11	13	20	31	24	1
5	4	1	6	7	3	27	35	18	8	28	31	19	10	24	33	15	9	26	32	17	13	25	29	16	11	22	34	20	12	14	21	30	23	2
6	5	2	7	1	4	26	34	19	9	27	30	20	11	23	32	16	10	25	31	18	14	24	35	17	12	28	33	21	13	8	15	29	22	3
14	13	10	8	9	12	32	5	27	17	33	1	28	19	29	3	24	18	31	2	26	15	30	6	25	20	34	4	22	21	16	23	7	35	11
8	14	11	9	10	13	31	4	28	18	32	7	22	20	35	2	25	19	30	1	27	16	29	5	26	21	33	3	23	15	17	24	6	34	12
9	8	12	10	11	14	30	3	22	19	31	6	23	21	34	1	26	20	29	7	28	17	35	4	27	15	32	2	24	16	18	25	5	33	13
10	9	13	11	12	8	29	2	23	20	30	5	24	15	33	7	27	21	35	6	22	18	34	3	28	16	31	1	25	17	19	26	4	32	14
11	10	14	12	13	9	35	1	24	21	29	4	25	16	32	6	28	15	34	5	23	19	33	2	22	17	30	7	26	18	20	27	3	31	8
12	11	8	13	14	10	34	7	25	15	35	3	26	17	31	5	22	16	33	4	24	20	32	1	23	18	29	6	27	19	21	28	2	30	9
13	12	9	14	8	11	33	6	26	16	34	2	27	18	30	4	23	17	32	3	25	21	31	7	24	19	35	5	28	20	15	22	1	29	10
21	20	17	15	16	19	4	12	34	24	5	8	35	26	1	10	31	25	3	9	33	22	2	13	32	27	6	11	29	28	23	30	14	7	18
15	21	18	16	17	20	3	11	35	25	4	14	29	27	7	9	32	26	2	8	34	23	1	12	33	28	5	10	30	22	24	31	13	6	19
16	15	19	17	18	21	2	10	29	26	3	13	30	28	6	8	33	27	1	14	35	24	7	11	34	22	4	9	31	23	25	32	12	5	20
17	16	20	18	19	15	1	9	30	27	2	12	31	22	5	14	34	28	7	13	29	25	6	10	35	23	3	8	32	24	26	33	11	4	21
18	17	21	19	20	16	7	8	31	28	1	11	32	23	4	13	35	22	6	12	30	26	5	9	29	24	2	14	33	25	27	34	10	3	15
19	18	15	20	21	17	6	14	32	22	7	10	33	24	3	12	29	23	5	11	31	27	4	8	30	25	1	13	34	26	28	35	9	2	16
20	19	16	21	15	18	5	13	33	23	6	9	34	25	2	11	30	24	4	10	32	28	3	14	31	26	7	12	35	27	22	29	8	1	17
28	27	24	22	23	26	11	19	6	31	12	15	7	33	8	17	3	32	10	16	5	29	9	20	4	34	13	18	1	35	30	2	21	14	25
22	28	25	23	24	27	10	18	7	32	11	21	1	34	14	16	4	33	9	15	6	30	8	19	5	35	12	17	2	29	31	3	20	13	26
23	22	26	24	25	28	9	17	1	33	10	20	2	35	13	15	5	34	8	21	7	31	14	18	6	29	11	16	3	30	32	4	19	12	27
24	23	27	25	26	22	8	16	2	34	9	19	3	29	12	21	6	35	14	20	1	32	13	17	7	30	10	15	4	31	33	5	18	11	28
25	24	28	26	27	23	14	15	3	35	8	18	4	30	11	20	7	29	13	19	2	33	12	16	1	31	9	21	5	32	34	6	17	10	22
26	25	22	27	28	24	13	21	4	29	14	17	5	31	10	19	1	30	12	18	3	34	11	15	2	32	8	20	6	33	35	7	16	9	23
27	26	23	28	22	25	12	20	5	30	13	16	6	32	9	18	2	31	11	17	4	35	10	21	3	33	14	19	7	34	29	1	15	8	24
35	34	31	29	30	33	18	26	13	3	19	22	14	5	15	24	10	4	17	23	12	1	16	27	11	6	20	25	8	7	2	9	28	21	32
29	35	32	30	31	34	17	25	14	4	18	28	8	6	21	23	11	5	16	22	13	2	15	26	12	7	19	24	9	1	3	10	27	20	33
30	29	33	31	32	35	16	24	8	5	17	27	9	7	20	22	12	6	15	28	14	3	21	25	13	1	18	23	10	2	4	11	26	19	34
31	30	34	32	33	29	15	23	9	6	16	26	10	1	19	28	13	7	21	27	8	4	20	24	14	2	17	22	11	3	5	12	25	18	35
32	31	35	33	34	30	21	22	10	7	15	25	11	2	18	27	14	1	20	26	9	5	19	23	8	3	16	28	12	4	6	13	24	17	29
33	32	29	34	35	31	20	28	11	1	21	24	12	3	17	26	8	2	19	25	10	6	18	22	9	4	15	27	13	5	7	14	23	16	30
34	33	30	35	29	32	19	27	12	2	20	23	13	4	16	25	9	3	18	24	11	7	17	28	10	5	21	26	14	6	1	8	22	15	31

Chapter 4

Quasi-Complete Latin Squares

In this chapter, the related concept of quasi-complete latin squares ($QCLS$) is introduced, and a proof that complete sets of mutually orthogonal $QCLS$ of order p exist for every prime p. Such sets were previously only known to exist for primes $p \leq 13$.

4.1 Complete Sets of Mutually Orthogonal $QCLS$

An $n \times n$ latin square L is *quasi-row-complete* if each *unordered* pair of symbols occurs exactly twice among the unordered pairs $\{L_{ij}, L_{i,j+1}\}$, where $1 \leq i \leq n$, $1 \leq j \leq n-1$. L is *quasi-column-complete* if its transpose is quasi-row-complete, and L is *quasi-complete* if it is both quasi-row-complete and quasi-column-complete. A quasi-complete latin square of order n will be denoted by $QCLS(n)$. Finally, a *complete set* of mutually orthogonal latin squares of order n is a set of $n-1$ such squares. (It is well-known and easy to show that no more than $n-1$ such squares can exist.)

Freeman [9, 10] suggested that a $QCLS(n)$ be used in the design of certain types of experiments for values of n for which no $RCLS(n)$ is known to exist, and in [10] he constructed a $QCLS(n)$ for every n. He then went on to prove that complete sets of mutually orthogonal $QCLS(5)$ and $QCLS(7)$ exist [11].

In [5], Campbell and Geller also proved the existence of a $QCLS(n)$ for every n (but used the term *balanced* latin square instead of $QCLS$), and they also showed that complete sets of mutually orthogonal $QCLS(n)$ also exist for $n = 7$, 11 and 13.

Now it will be shown that complete sets of mutually orthogonal $QCLS(p)$ exist for *every* prime p. The proof is quite straightforward, and makes use of terraces.

A *terrace* (see [3]) of a group G of order n is an ordering $b_1, b_2, \ldots, b_n$ of the elements of G, such that each x in G with $x^2 = e$ occurs once among the elements $b_1^{-1}b_2, b_2^{-1}b_3, \ldots, b_{n-1}^{-1}b_n$, and for every other x in G, x and x^{-1} together occur a total of two times among these elements (so either x occurs twice and x^{-1} does not occur, or x^{-1} occurs twice and x does not occur, or both x and x^{-1} occur once).

Clearly whenever $a_1, a_2, ..., a_n$ is a terrace of G, so is $ca_1, ca_2, ..., ca_n$ for any c in G. Also, if G is abelian, then whenever $a_1, a_2, ..., a_n$ is a terrace of G, so is $a_1^{-1}, a_2^{-2}, ..., a_n^{-1}$ (see e.g. [8, pg. 62]). The following theorem was proven by Bailey in 1984.

Theorem 4.1 **([3, Theorem 1])** *The $n \times n$ array L with $L_{ij} = a_i b_j$ $(1 \le i, j \le n)$ is a $QCLS(n)$ if and only if $a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1}$ and $b_1, b_2, \ldots, b_n$ are both terraces of G.*

Now $0, n-1, 1, n-2, 2, n-3, ...$ is easily seen to be a terrace of $(\mathbb{Z}_n, +)$ (see e.g. [8, Theorem 2.3]). This fact, along with Theorem 4.1, will be used in the proof of the following theorem.

Theorem 4.2 *There exists a complete set of mutually orthogonal $QCLS(p)$ for every prime p.*

Proof Let $a_1, a_2, ..., a_p$ denote the terrace of $\mathbb{Z}_p$ mentioned above. Define the $p-1$ arrays $L^{(1)}, L^{(2)}, ..., L^{(p-1)}$ of size $p \times p$ by

$$L_{ij}^{(k)} = a_i + ka_j,$$

for $1 \le i, j \le p$ and $1 \le k \le p-1$. Then $ka_1, ka_2, ..., ka_p$ is a terrace of $\mathbb{Z}_p$, and since $\mathbb{Z}_p$ is abelian, $-a_1, -a_2, ..., -a_p$ is also a terrace of $\mathbb{Z}_p$. So by Theorem 4.1, $L^{(k)}$ is a $QCLS(p)$ for $1 \le k \le p-1$.

Suppose $(L_{ij}^{(k_1)}, L_{ij}^{(k_2)}) = (L_{uv}^{(k_1)}, L_{uv}^{(k_2)})$ for some $k_1 \neq k_2$ with $1 \le i, j \le p$ and $1 \le k_1, k_2 \le p-1$. Then

$$a_i + k_1 a_j = a_u + k_1 a_v,$$

and

$$a_i + k_2 a_j = a_u + k_2 a_v.$$

Subtracting these equations and rearranging gives

$$(k_1 - k_2)(a_j - a_v) = 0,$$

and so since $k_1 \neq k_2$, $a_j = a_v$, that is, $j = v$, and hence also $a_i = a_u$, that is, $i = u$. This shows that $L^{(k_1)}$ and $L^{(k_2)}$ are orthogonal for any $k_1 \neq k_2$, thereby completing the proof of the theorem. ∎

Bibliography

[1] B. A. Anderson, *A fast method for sequencing low order non-abelian groups,* Ann. Discrete Math. **34** (1987), 27-42.

[2] D. S. Archdeacon, J. H. Dinitz, D. R. Stinson and T. W. Tillson, *Some new row-complete latin squares,* J. Combin. Theory Ser. A **29** (1980), 395-398.

[3] R. A. Bailey, *Quasi-complete latin squares: construction and randomization,* J. Roy. Statist. Soc. Ser. B **46** (1984), 323-334.

[4] B. R. Bugelski, *A note on Grant's discussion of the latin square principle in the design of experiments,* Psychological Bulletin **46** (1949), 49-50.

[5] G. Campbell and S. Geller, *Balanced latin squares,* Univ. of Purdue preprint, Dept. of Statist., Mimeoseries No. 80-26 (1980).

[6] D. Cohen and T. Etzion, *Row-complete latin squares which are not column-complete,* Ars Combinatoria **32** (1991), 193-201.

[7] J. Dénes and A. D. Keedwell, *Latin squares and their applications,* Academic Press, New York/London, 1974.

[8] J. Dénes and A. D. Keedwell, "Sequenceable and R-sequenceable groups: row-complete latin squares," *Latin squares: new developments in the theory and*

applications, J. Dénes and A. D. Keedwell (Editors), North-Holland, Amsterdam, 1991, pp. 43-100.

[9] G. H. Freeman, *Some two-dimensional designs balanced for nearest neighbours,* J. Roy. Statist. Soc. Ser. B **41** (1979), 88-95.

[10] G. H. Freeman, *Complete latin squares and related experimental designs,* J. Roy. Statist. Soc. Ser. B **41** (1979), 253-262.

[11] G. H. Freeman, *Further results on quasi-complete latin squares,* J. Roy. Statist. Soc. Ser. B **43** (1981), 314-320.

[12] B. Gordon, *Sequences in groups with distinct partial products,* Pacific J. Math. **11** (1961), 1309-1313.

[13] A. Hedayat and K. Afsarinejad, *Repeated measurements designs, II,* Ann. Statist. **6** (1978), 619-628.

[14] K. Heinrich, *Pairwise orthogonal row-complete latin squares,* Congr. Numer. **24** (1979), 501-510.

[15] A. D. Keedwell, *On the sequenceability of non-abelian groups of order pq,* Discrete Math. **37** (1981), 203-216.

[16] A. D. Keedwell, "Some problems concerning complete latin squares," *Combinatorics (Proc. British Combin. Conf., Aberystwyth, 1973),* T. P. McDonough and V. C. Mavron (Editors), Cambridge Univ. Press, London, 1974, pp. 89-96.

[17] N. S. Mendelsohn, "Hamiltonian decomposition of the complete directed n-graph," *Theory of Graphs (Proc. Colloq., Tihany, 1966),* P. Erdős and J. Catona (Editors), Academic Press, New York, 1968, pp. 237-241.

[18] L. L. Wang, *A test for the sequencing of a class of finite groups with two generators,* Notices Amer. Math. Soc. **20** (1973), 73T-A275.

[19] E. J. Williams, *Experimental designs balanced for the estimation of residual effects of treatments,* Austral. J. Sci. Res. Ser. A **2** (1949), 149-168.