Combinatorial designs and their automorphism groups

Thesis

Combinatorial designs and their automorphism groups

Graham John Lovegrove, M.A., MSc.

Thesis submitted for the degree of Doctor of Philosophy

Department of Mathematics and Statistics,

The Open University,

Walton Hall,

Milton Keynes, MK7 6AA,

United Kingdom.

November 2008.

ABSTRACT

This thesis concerns the automorphism groups of Steiner triple systems and of cycle systems. Although most Steiner triple systems have trivial automorphism groups [2], it is widely known that for every abstract group, there exists a Steiner triple system whose automorphism is isomorphic to that group [16].

The well-known Bose construction [4] for Steiner triple systems, which has a number of variants, has a particularly nice structure, which makes it possible to say much about the automorphism group, and in the case of the construction based on an Abelian group, to derive the full automorphism group. The thesis contains a full analysis of these matters. Some of these results have been published by the author in [14]. The thesis also proves new results concerning the automorphism group for Steiner triple systems constructed using the tripling construction.

An m-cycle system is a decomposition of a complete graph into cycles of length m. A Steiner triple system is thus a 3-cycle system. The thesis proves the result that for all $m > 3$, and for each abstract finite group, there exists an m-cycle system whose automorphism group is isomorphic to that group.

In addition, the thesis contains a collection of new results concerning the conjecture by Füredi that every Steiner triple system is decomposable into triangles. Although this conjecture is expected to remain open for some time, it is possible to prove it for a number of standard constructions. It is further shown that for sufficiently large v, the number of Steiner triple systems of order v that are decomposable into triangles is at least $v^{v^2(\frac{1}{54}-o(1))}$.

ACKNOWLEDGMENTS

I would like to thank the following people and organisations:

- My supervisors, Professors T.S. Griggs and M.J.Grannell, for their encouragement, interest, and enormous patience.
- My wife for her understanding and support.
- My sometime employers Thales UK for their sponsorship during part of this time.

Contents

Chapter 1

Introduction

This thesis is primarily concerned with the automorphism groups of two types of combinatorial design, namely Steiner triple systems, and cycle systems.

A Steiner triple system of order v, $D = STS(v)$, is an ordered pair $(V, \mathcal{B})$ where V is a set of *elements* or *points*, of cardinality v, and $\mathcal{B}$ is a collection of 3-element subsets of V, called *blocks* or *triples* which collectively have the property that every 2-element subset of V is contained in exactly one block. It is well-known that such systems exist if and only if $v \equiv 1, 3 \pmod 6$, a fact first proved by Kirkman in 1847 [13].

An *m-cycle system of order n*, $m > 2$ is a decomposition of the complete graph on n vertices into cycles of length m. Thus a 3-cycle system is a Steiner triple system. A necessary condition for the existence of an m-cycle system of order n is that n is odd and m divides $n(n-1)/2$. Such a value of n is called *m-admissible*. The question of cycle-system existence has been settled for all m-admissible n when $m \leq 50$ or a prime power, for all even m with $n \equiv 1 \pmod{2m}$, and all odd m with $n \equiv m \pmod{2m}$ ([7], page 266).

L. Babai [2] has proved that almost all Steiner triple systems have trivial

automorphism group, a result which is widely believed to be true for m-cycle systems in general, although no similar results for $m > 3$ have been reported to date. On the other hand, E. Mendelsohn [16] has shown that for every abstract finite group there exists a Steiner triple system whose full automorphism group is isomorphic to that group.

Chapters 2 to 4 of this thesis concern some constructions for Steiner triple systems for which the automorphism group can be directly evaluated.

Chapter 2 concerns the automorphism group of a Steiner triple system generated by the so-called Bose construction. Chapter 3 applies the results to specific cases of the construction. Parts of both these chapters have been published in [14]. In Chapter 4, a number of results are derived concerning the standard tripling construction for Steiner triple systems. Both these constructions are defined in detail in the relevant chapters.

In Chapters 5 and 6, the results of Mendelsohn are extended to m-cycle systems. In Chapter 5 it is proved that for every abstract finite group there exists a $2m$-cycle system whose automorphism group is isomorphic to that group. Chapter 6 proves the corresponding result for odd cycle systems.

The final chapter of the thesis concerns a different aspect of Steiner triple systems. A *triangle* is a set of three blocks of the form

$$\{a, b, c\},\ \{c, d, e\},\ \{e, f, a\}.$$

There is a conjecture [12] that it is possible to decompose every Steiner triple system into triangles, with possibly one or two remainder blocks. Although this conjecture remains unproved, it is known [17] that there exists an STS(v) that is decomposable into triangles for every $v \equiv 1, 3 \pmod 6$. In this chapter we firstly

present a number of new triangle decompositions for well-known constructions of Steiner triple systems. In the second part of this chapter we prove a lower bound on the number of STS(v) which are decomposable into triangles, namely that for sufficently large v, the number of STS(v) is at least of order $v^{v^2(\frac{1}{54}-o(1))}$. The best result previously reported in this area is that for $v \equiv 1, 19 \pmod{72}$, the number of decomposable STS(v)s tends towards infinity with v [12].

Chapter 2

Bose construction

2.1 Bose construction

In 1939, Bose [4] gave a particularly elegant construction for STS(v) in the case where $v = 6s + 3$. Bose's original construction was based on an Abelian group of odd order. In this chapter however, we shall consider a more general formulation of the construction, which is based on a symmetric idempotent Latin square.

A Latin square $L = \{L(i, j) : 1 \leq i \leq n,\ 1 \leq j \leq n\}$ is an $n \times n$ array in which each cell contains a single element from an n-set X, such that each element occurs exactly once in each row and column [7], page 97. In this definition, the indexing sets of the rows and columns can be different from each other and different from X. We shall in this work assume for the most part that the rows and columns of a Latin square are indexed by the same n-set X as the cells. Where it is necessary to consider indexing sets different from X this will be stated.

A Latin square is symmetric if for all $i, j \in X$, $L(i, j) = L(j, i)$, and is idempotent if for all $i \in X$, $L(i, i) = i$.

We shall henceforth abbreviate the term symmetric idempotent Latin square

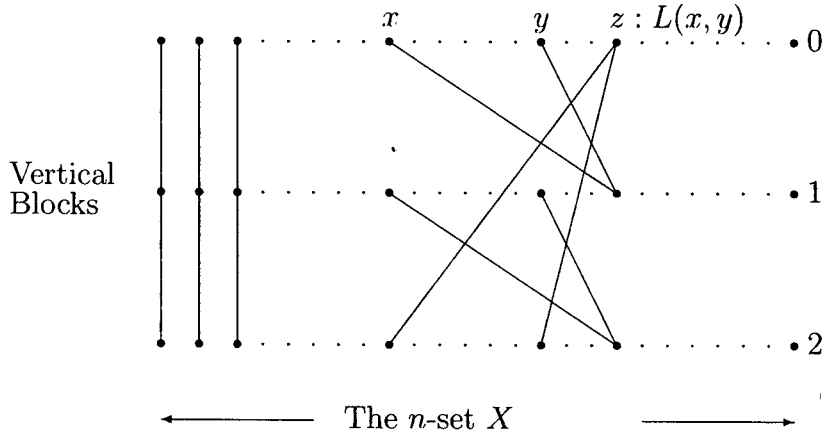
to SILS. It is easy to see that SILSs only exist for odd values of n. This is because by reason of idempotency, each element occurs in $n-1$ off-diagonal cells and so, by reason of symmetry, occurs $\frac{1}{2}(n-1)$ times in the multiset $\{L(i,j) : i,j \in X, i < j\}$. Hence n is odd.

It will be convenient to assume that $n > 1$.

We now give the Bose construction. Take $V = X \times Z_3$, where Z_3 denotes the group of integers modulo 3, and let $\mathcal{B}$ be the collection of blocks:

$$\{(x,0),(x,1),(x,2)\} : x \in X,$$
$$\{(x,0),(y,0),(z,1)\} : x,y,z \in X, x \neq y, z = L(x,y),$$
$$\{(x,1),(y,1),(z,2)\} : x,y,z \in X, x \neq y, z = L(x,y),$$
$$\{(x,2),(y,2),(z,0)\} : x,y,z \in X, x \neq y, z = L(x,y).$$

Diagramatically the Bose construction can be represented as follows.



A Steiner triple system constructed in this way will be called a *Bose design.*

The purpose of this chapter is to examine the full automorphism group of a Steiner triple system, D, constructed by this method, in terms of the properties of the SILS L.

An automorphism of the SILS L is a permutation of X that preserves the SILS structure, i.e. if ϕ is an automorphism of L and $x, y \in X$ then $L(\phi(x), \phi(y)) = \phi(L(x, y))$. The set of automorphisms of L, denoted here by $Aut(L)$ naturally forms a group by the composition: $(\phi.\psi)(x) = \phi(\psi(x))$ for $\phi,\ \psi\ \in Aut(L),\ x\ \in X$.

An automorphism of a Steiner triple system $D = (V, \mathcal{B})$ is a permutation of the point set V that preserves blocks. This definition ensures that the mapping is a permutation of blocks, because if ϕ is such an automorphism, and $\{u, v, w\}, \{u', v', w'\}\ \in\ \mathcal{B}$ and $\{\phi(u), \phi(v), \phi(w)\} = \{\phi(u'), \phi(v'), \phi(w')\}$, then $\{u, v, w\} = \{u', v', w'\}$, perhaps with some re-ordering, since the order of points in a block is unimportant. We denote the group of all automorphisms of D as $Aut(D)$.

It is clear from the definition of the Bose design D that, if $B \in \mathcal{B}$, where $B = \{(x, i), (y, j), (z, k)\}$, then $\{(x, s+i), (y, s+j), (z, s+k)\} \in \mathcal{B}$ for any $s \in Z_3$; also, that for any $\beta \in Aut(L)$,

$$\beta(B) = \{(\beta(x), i), (\beta(y), j), (\beta(z), k)\} \in \mathcal{B}$$

Thus the bijection $[\beta, s]$ on V defined by

$$[\beta, s](x, i) = (\beta(x), s + i)$$

clearly defines an automorphism of D.

Before proceeding, some further terminology and definitions are appropriate. In the Bose construction, there is a natural distinction between two types of block, those of the form $\{(x,0),(x,1),(x,2)\}$ and the remainder. We will need to use this distinction in several parts of this thesis, and therefore, in analogy with the usual diagrammatic representation of the Bose construction as given for example in [18], page 114, the former will be referred to as *vertical* blocks, and the remainder as *non-vertical.* Also of importance will be the *signature* of a block. Defining the *label* of an element to be the Z_3 component, the *signature* of a block is the sum of the values of the *labels* of the block modulo 3. Observe that the signature of a vertical block is zero, the signature of a non-vertical block is 1, and that no block has signature 2.

2.2 Block signatures and automorphism type

In this section we use the concept of block signature to begin to classify the types of automorphism which can exist in a Bose design $D = (V, \mathcal{B})$ on a SILS L, and show that two particular types of automorphism exist only in the unique $STS(9)$, the Bose design on Z_3.

Lemma 2.2.1. *If E is a 3×3 array of points of D such that the rows and columns are all distinct blocks of D, then:*

(a) all the rows of E have the same signature,

(b) all the columns of E have the same signature,

(c) *if all the rows (columns) of E have signature 0, then all the columns (rows) have signature 1.*

Proof. Suppose that one row has signature 0, i.e. it is a *vertical* block. Then since all rows and columns of E are distinct blocks of D, all the columns of E must be *non-vertical.* This is because two vertical blocks having a common point must be the same block, and so a row and a column each consisting of a vertical block cannot be distinct. Hence the sum of the signatures of the columns is 0 modulo 3, and so the sum of the row signatures must be the same, and the other rows have signature 0.

Similarly, if one column has signature 0, then all rows are *non-vertical*, and every column has signature 0.

The third possibility is that all rows and columns have signature 1, and so represent non-vertical blocks. □

The next two lemmas use this result to classify the automorphisms of D by their actions on the vertical blocks of D.

Lemma 2.2.2. *A member of $Aut(D)$ maps the vertical blocks of D either all to vertical blocks or all to non-vertical blocks.*

Proof. Let ϕ be a member of $Aut(D)$, and $x, y,\ x \neq y$ any two elements of X. Apply Lemma 2.2.1 to the image under ϕ of the array:

$$\begin{array}{ccc} (x,0) & (x,1) & (x,2) \\ (y,0) & (y,1) & (y,2) \\ (L(x,y),1) & (L(x,y),2) & (L(x,y),0) \end{array}$$

We first note that since $x \neq y$, the first two rows of this array are distinct. Further, $L(x, y) \neq x$, since the x^{th} row of L has only one entry equal to x, namely $L(x, x)$. Similarly $L(x, y) \neq y$, and we deduce that all rows of the array are distinct.

Suppose that under ϕ, the top row is mapped to a vertical (non-vertical) block. Then by Lemma 2.2.1, the other rows are mapped similarly. Since the choice of y is arbitrary, this shows that all vertical blocks are mapped in the same way by ϕ. □

The above lemma allows the classification of automorphisms into the types *vertical* and *non-vertical*, according to whether it maps all vertical blocks to vertical blocks or non-vertical blocks.

We shall say that a vertical block is mapped evenly/oddly by an automorphism if it is mapped to a vertical block, and the labels Z_3 are permuted evenly/oddly.

Lemma 2.2.3. *A vertical automorphism of D maps the vertical blocks of D either all even-vertically or all odd-vertically.*

Proof. Let ϕ be a vertical automorphism of D, and consider the image under ϕ of the array of Lemma 2.2.2. Suppose that some row is mapped even-vertically, and another odd-vertically. We shall consider only the values of the labels of the individual elements, as defined above, so we can write the values for these two rows as:

$$\begin{array}{ccc} j & j+1 & j+2 \\ i & i+2 & i+1 \end{array}$$

Since by Lemma 2.2.1 all the columns of the image array have signature 1, the third row must have label values which are all $1 - i - j$, which is not valid for a block of D. □

Lemmas 2.2.2 and 2.2.3 enable us to classify an automorphism of D as *even-vertical*, *odd-vertical*, or *non-vertical* according to whether it maps the vertical blocks of D even-vertically, odd-vertically, or non-vertically.

The final result of this section shows that all the automorphisms of all but just one Bose design are even-vertical, but first we need the following simple lemma:

Lemma 2.2.4. *If for the SILS L on the n-set X, there exists a map $\alpha : X \to \{0, 1, 2\}$ such that for all $x, y \in X$ with $x \neq y$,*

$$\alpha(x) + \alpha(y) + \alpha(L(x, y)) \equiv 1 \pmod 3,$$

then $n = 3$.

Proof. Let the numbers of elements of X which map to 0, 1, and 2 under α be m_0, m_1, and m_2 respectively. Since L is idempotent, $L(x, x) = x$ for all $x \in X$, so $\alpha(L(x, x)) = \alpha(x)$ for all $x \in X$.

Suppose that there exists $x \in X$, such that $\alpha(x) = 0$, i.e. $m_0 \geq 1$. In the x^{th} row of L there are precisely m_1 values of $L(x, y)$ with $\alpha(L(x, y)) = 1$. These can only correspond to values of y with $\alpha(y) = 0$, except $y = x$. Therefore $m_1 = m_0 - 1$.

By similar reasoning, we also obtain $m_2 = m_1 - 1$, and $m_0 = m_2 - 1$, if $m_1 \geq 1$ and $m_2 \geq 1$ respectively. This implies $m_0 = m_0 - 3$, so not all of the assumptions

can be true. Hence $(m_0, m_1, m_2) = (0, 1, 2)$ or $(1, 0, 2)$, or $(2, 1, 0)$, i.e. $n = 3$. $\square$

This lemma now enables us to prove the following result:

Theorem 2.2.1. *If any element ϕ of $Aut(D)$ is either odd-vertical, or non-vertical, then $n = 3$, and D is the unique $STS(9)$.*

Proof. In both cases, the proof relies on constructing a suitable map $\alpha : X \to \{0, 1, 2\}$, and invoking Lemma 2.2.4. We prove the result for odd-vertical automorphisms first. Suppose $n > 3$, and that an automorphism ϕ acts oddly on all vertical blocks. It is evident that for any vertical block $\{(x, 0),\ (x, 1),\ (x, 2)\}$, the odd-vertical automorphism ϕ will leave one label unchanged, e.g. if

$$\phi : \{(x, 0),\ (x, 1),\ (x, 2)\} \to \{(y, 0),\ (y, 2),\ (y, 1)\}$$

for some $y \in X$, then 0 is fixed in this case.

Of course, the label fixed by ϕ will not necessarily be the same for every vertical block. Suppose now that for the vertical block $\{(x, 0),\ (x, 1),\ (x, 2)\}$, the label i is fixed by ϕ. Then it is easily checked that the labels of the images of $(x, 0),\ (x, 1),\ (x, 2)$ are $2i,\ 2i + 2,\ 2i + 1$ respectively. We shall now set $\alpha(x) = i$. Then α is defined on X, and $\alpha : X \to Z_3$.

It remains to prove that for any $x, y \in X$, $x \neq y$, $\alpha(x) + \alpha(y) + \alpha(L(x, y)) \equiv 1 \pmod 3$ and invoke Lemma 2.2.4.

Put $z = L(x, y)$, $\alpha(x) = i$, $\alpha(y) = j$, $\alpha(z) = k$, then the labels of the image under ϕ of the array:

$$\begin{array}{ccc} (x,0) & (x,1) & (x,2) \\ (y,0) & (y,1) & (y,2) \\ (z,1) & (z,2) & (z,0) \end{array}$$

are:

$$\begin{array}{ccc} 2i & 2i+2 & 2i+1 \\ 2j & 2j+2 & 2j+1 \\ 2k+2 & 2k+1 & 2k, \end{array}$$

and since the columns represent non-vertical blocks, we conclude that $2i + 2j + 2k + 2 \equiv 1 \pmod 3$, so

$$i + j + k = \quad \alpha(x) + \alpha(y) + \alpha(L(x,y)) \equiv 1 \pmod 3,$$

as required.

We will now prove the non-vertical case. If ϕ is non-vertical, then the image under ϕ of each vertical block is a non-vertical block. Also, since ϕ is an automorphism, each vertical block is the image of a non-vertical block, so exactly n non-vertical blocks are mapped to vertical blocks by ϕ, and the remaining non-vertical blocks are mapped to non-vertical blocks.

To prove the required result, we are again going to construct a suitable map α that satisfies the conditions of Lemma 2.2.4. We shall only be concerned with the labels in the images of vertical blocks under ϕ in each case.

Consider any vertical block $\{(x,0),\ (x,1),\ (x,2)\}$. The label multiset of its image under ϕ is $\{i, i, i+1\}$ for some $i \in Z_3$. We shall choose for our map α the label in the pre-image that maps to the non-repeated label in the image of ϕ. In other words, if the label j is mapped to the non-repeated label $i + 1$, then set

$\alpha(x) = j$. Now in order for α to satisfy the conditions of the lemma, we must show that for any $x, y \in X$, $x \neq y$, $\alpha(x) + \alpha(y) + \alpha(L(x,y)) \equiv 1 \pmod 3$.

We shall again examine the labels of the image under ϕ of the array:

$$\begin{array}{ccc} (x,0) & (x,1) & (x,2) \\ (y,0) & (y,1) & (y,2) \\ (z,1) & (z,2) & (z,0), \end{array}$$

where again $z = L(x,y)$. The image of this array will have non-vertical blocks as rows, but its columns may be either all vertical blocks or all non-vertical blocks, by Lemma 2.2.1.

In the vertical case, the labels of the columns will sum to zero, and in the non-vertical case, the labels of the columns will sum to 1.

There are three cases to consider. The first is that the mapping is of the form:

$$\begin{array}{ccc} (x,0) & (x,1) & (x,2) \\ (y,0) & (y,1) & (y,2) \\ (z,1) & (z,2) & (z,0) \end{array} \rightarrow \begin{array}{ccc} i & i & i+1 \\ j & j & j+1 \\ k & k & k+1, \end{array}$$

or any permutation of the columns of the array of labels on the right.

The second case is of the form:

$$\begin{array}{ccc} (x,0) & (x,1) & (x,2) \\ (y,0) & (y,1) & (y,2) \\ (z,1) & (z,2) & (z,0) \end{array} \rightarrow \begin{array}{ccc} i+1 & i & i \\ j & j+1 & j \\ k & k & k+1, \end{array}$$

or any permutation of the columns on the right.

The third case is of the form:

$$\begin{array}{ccc} (x,0) & (x,1) & (x,2) \\ (y,0) & (y,1) & (y,2) \\ (z,1) & (z,2) & (z,0) \end{array} \rightarrow \begin{array}{ccc} i+1 & i & i \\ j+1 & j & j \\ k & k+1 & k, \end{array}$$

or any permutation of the rows and columns on the right.

Since the image array must have columns which are either all vertical blocks or all non-vertical blocks, the the sums of the labels in the columns must be either all 0 or all 1 (mod 3).

In the first of these cases, the sum of each column is $i+j+k$ modulo 3, and so each column is vertical if $i+j+k \equiv 0 \pmod 3$, and non-vertical if $i+j+k \equiv 1 \pmod 3$.

In the second case, the sum of each column is $i+j+k+1$ modulo 3, so each column is vertical if $i+j+k = 2$ modulo 3, and non-vertical if $i+j+k \equiv 1 \pmod 3$.

However in the final case, the column sums are different, and so this arrangement of labels cannot occur.

We now calculate α for the two valid cases. In the first case, we have:

$$\begin{aligned} \alpha(x) &= 2+\lambda \\ \alpha(y) &= 2+\lambda \\ \alpha(z) &= 0+\lambda \end{aligned}$$

where choice of $\lambda \in \{0,1,2\}$ serves to permute the columns of the label array. So

we can write:

$$\alpha(x) + \alpha(y) + \alpha(L(x,y)) = \alpha(x) + \alpha(y) + \alpha(z) = 4 + 3\lambda \equiv 1 \pmod 3,$$

and the first case is proved.

In the second case, we have the six possibilities given by the columns below:

$$\begin{aligned} \alpha(x) &= 0,\ 1,\ 1,\ 2,\ 2,\ 0 \\ \alpha(y) &= 1,\ 0,\ 2,\ 1,\ 0,\ 2 \\ \alpha(z) &= 0,\ 0,\ 1,\ 1,\ 2,\ 2. \end{aligned}$$

In each case,

$$\alpha(x) + \alpha(y) + \alpha(L(x,y)) = \alpha(x) + \alpha(y) + \alpha(z) \equiv 1 \pmod 3,$$

and so the result is proved. □

Corollary 2.2.1. *The full automorphism group $Aut(D)$ is the group of even-vertical automorphisms of D, unless D is the unique STS(9).*

2.3 Standard automorphisms

We shall call an automorphism of D *standard* if it is even-vertical and subjects the labels of every vertical block to the same even permutation (which can equally well be represented as a translation by an element of Z_3). A group of automorphisms is standard if all of its members are standard. An automorphism/group of automorphisms is *non-standard* if it is not standard. The distinction is important, because for most Bose designs D, the full automorphism group is standard.

Of course the automorphisms of L induce automorphisms of the Bose design on L, as noted in Section 2.1.

Lemma 2.3.1. *The (sub)group of standard automorphisms of Aut(D) is isomorphic to* $Aut(L) \times Z_3$.

Proof. The labels of every vertical block are permuted in the same way. We represent the standard automorphism Φ by:

$$\Phi : \{(x,0)\ (x,1)\ (x,2)\} \rightarrow \{(\psi(x),k)\ (\psi(x),1+k)\ (\psi(x),2+k)\}$$

for some $k \in Z_3$, and permutation ψ of X. If $x, y \in X$, $x \neq y$, and $z = L(x,y)$, then

$$\Phi : \begin{array}{ccc} \{(x,0) & (x,1) & (x,2)\} \\ \{(y,0) & (y,1) & (y,2)\} \\ \{(z,1) & (z,2) & (2,0)\} \end{array} \rightarrow \begin{array}{ccc} \{(\psi(x),k) & (\psi(x),1+k) & (\psi(x),2+k)\} \\ \{(\psi(y),k) & (\psi(y),1+k) & (\psi(y),2+k)\} \\ \{(\psi(z),1+k) & (\psi(z),2+k) & (\psi(z),k)\} \end{array}$$

Also, $\psi(L(x,x)) = \psi(x) = L(\psi(x),\psi(x))$. Hence we have

$$\psi(L(x,y)) = \psi(z) = L(\psi(x),\psi(y)),$$

and so ψ is an automorphism of L. Hence any standard automorphism of D is a member of $Aut(L) \times Z_3$. Clearly any element of $Aut(L) \times Z_3$ is a standard automorphism, and so the result follows. □

2.4 Example

We illustrate the results of the previous sections with the simplest example, the unique STS(9), which is isomorphic to the Bose construction on the SILS

$$\begin{array}{ccc} 0 & 2 & 1 \\ 2 & 1 & 0 \\ 1 & 0 & 2, \end{array}$$

and has the 12 blocks:

$$\{(0,0)(0,1)(0,2)\}, \{(1,0)(1,1)(1,2)\}, \{(2,0)(2,1)(2,2)\}$$

$$\{(0,0)(1,0)(2,1)\}, \{(0,1)(1,1)(2,2)\}, \{(0,2)(1,2)(2,0)\}$$

$$\{(1,0)(2,0)(0,1)\}, \{(1,1)(2,1)(0,2)\}, \{(1,2)(2,2)(0,0)\}$$

$$\{(2,0)(0,0)(1,1)\}, \{(2,1)(0,1)(1,2)\}, \{(2,2)(0,2)(1,0)\}$$

which can be more compactly represented as the rows, columns, and all diagonals of the array:

$$\begin{array}{ccc} (0,0) & (1,0) & (2,1) \\ (0,1) & (1,1) & (2,2) \\ (0,2) & (1,2) & (2,0), \end{array}$$

where the columns are the vertical blocks. The automorphisms of the STS(9) provide examples of all the automorphism types identified for the Bose construction:

i even-vertical and standard,

ii even-vertical and non-standard,

iii odd-vertical,

iv non-vertical.

i The automorphism:

$$\begin{array}{ccc} (0,0) & (1,0) & (2,1) \\ (0,1) & (1,1) & (2,2) \\ (0,2) & (1,2) & (2,0) \end{array} \rightarrow \begin{array}{ccc} (0,1) & (1,1) & (2,2) \\ (0,2) & (1,2) & (2,0) \\ (0,0) & (1,0) & (2,1), \end{array}$$

is even-vertical and standard because the labels of the vertical blocks are all permuted in the same way.

ii The automorphism:

$$\begin{array}{ccc} (0,0) & (1,0) & (2,1) \\ (0,1) & (1,1) & (2,2) \\ (0,2) & (1,2) & (2,0) \end{array} \rightarrow \begin{array}{ccc} (0,0) & (1,1) & (2,0) \\ (0,1) & (1,2) & (2,1) \\ (0,2) & (1,0) & (2,2), \end{array}$$

is even-vertical and non-standard because the labels are not permuted in the same way for all vertical blocks.

iii The automorphism:

$$\begin{array}{ccc} (0,0) & (1,0) & (2,1) \\ (0,1) & (1,1) & (2,2) \\ (0,2) & (1,2) & (2,0) \end{array} \rightarrow \begin{array}{ccc} (0,0) & (1,0) & (2,1) \\ (0,2) & (1,2) & (2,0) \\ (0,1) & (1,1) & (2,2), \end{array}$$

is odd-vertical because the permutation of the labels is odd,

iv The automorphism:

$$\begin{array}{ccc} (0,0) & (1,0) & (2,1) \\ (0,1) & (1,1) & (2,2) \\ (0,2) & (1,2) & (2,0) \end{array} \rightarrow \begin{array}{ccc} (0,0) & (0,1) & (0,2) \\ (1,0) & (1,1) & (1,2) \\ (2,1) & (2,2) & (2,0), \end{array}$$

is non-vertical since vertical blocks are not mapped to vertical blocks.

As has been proved in Section 2.2, the STS(9) is the only Bose design which admits odd or non-vertical automorphisms.

We shall derive the full automorphism group of this design as part of a more general result in the next chapter.

2.5 Full automorphism group

In Section 2.2 we proved that, except in the case of the STS(9), all automorphisms of designs made with the Bose construction are even-vertical. In this section we shall find a characterisation of this automorphism group in the most general terms.

We first of all note that by Corollary 2.2.1, we need only to characterise the group of even vertical automorphisms of D.

An even vertical automorphism ϕ of D will not necessarily permute the labels of all vertical blocks in the same way. Accordingly, we must represent ϕ as a pair (ψ, κ), where ψ is a permutation of X, and $\kappa : X \rightarrow Z_3$, and the operation of ϕ is such that if (x, a) is a point of D, $x \in X$, $a \in Z_3$, then $\phi(x, a) = (\psi(x), a + \kappa(x))$.

The next few results establish conditions on κ and ψ.

Lemma 2.5.1. *If $\phi = (\psi, \kappa)$ is an even vertical automorphism of D, then for $x,\ y\ \in X$,*

$$\kappa(x) + \kappa(y) + \kappa(L(x, y)) = 0,$$

in Z_3.

Proof. The result holds trivially if $x = y$, since L is idempotent. Now assume that $x \neq y$. Since ϕ is even vertical, it maps vertical blocks to vertical blocks and non-vertical blocks to non-vertical blocks.

Hence the image of $\{(x, 0)\ (y, 0)\ (L(x, y), 1)\}$ is non-vertical and therefore has signature 1. The image of this block under ϕ is:

$$\{(\psi(x), \kappa(x))\ (\psi(y), \kappa(y))\ (\psi(L(x, y)), 1 + \kappa(L(x, y)))\}.$$

so

$$\kappa(x) + \kappa(y) + 1 + \kappa(L(x, y)) = 1,$$

and the result follows □

If κ is constant on X, then the automorphism ϕ is standard, and we know from Lemma 2.3.1 that ψ is an automorphism of L. If κ is not constant on X, then ϕ is non-standard.

Lemma 2.5.2. *If $\phi = (\psi, \kappa)$ is a non-standard automorphism of D, then the set of values $\{\kappa(x) : x \in X)\}$ partitions X into 3 equal parts.*

Proof. Observe first that if $\kappa(x_0) \neq \kappa(y_0)$, then $\kappa(L(x_0, y_0)) \neq \kappa(x_0)$, and $\kappa(L(x_0, y_0)) \neq \kappa(y_0)$ by Lemma 2.5.1, so κ takes all values of Z_3.

Put $z_0 = L(x_0, y_0)$, and let y vary through $\{y : \kappa(y) = \kappa(y_0)\}$. Then since $\kappa(x_0) + \kappa(y) + \kappa(L(x_0, y)) = 0$ in Z_3, we have $\kappa(L(x_0, y)) = \kappa(z_0)$. Therefore the number of $z = L(x_0, y)$ for which $\kappa(z) = \kappa(z_0)$ must be at least as large as the number of y for which $\kappa(y) = \kappa(y_0)$.

Also, since $\kappa(x_0) + \kappa(y_0) + \kappa(z_0) = 0$ in Z_3, we have $\kappa(y_0) = \kappa(L(x_0, z_0))$, so we may exchange y_0 and z_0 in the above argument to show that there are at least as many y for which $\kappa(y) = \kappa(y_0)$ as z for which $\kappa(z) = \kappa(z_0)$. Therefore $|\{y : \kappa(y) = \kappa(y_0)\}| = |\{z : \kappa(z) = \kappa(z_0)\}|$, and similarly both are equal to $|\{z : \kappa(z) = \kappa(z_0)\}|$. □

This partitioning of X by κ consequently causes a partitioning of L into subarrays. Let $X_i = \{x \in X : \kappa(x) = i\}$, $i = 0, 1, 2$.

Lemma 2.5.3. *If $\phi = (\psi, \kappa)$ is a non-standard automorphism of D, then for each $i, j \in Z_3$, L restricted to rows indexed by X_i and columns indexed by X_j is a Latin sub-square of L with rows indexed by X_i, columns indexed by X_j, and cell values in X_{2i+2j}. It is a sub SILS of L if $i = j$.*

Proof. If $x, y \in X$, $\kappa(x) = i$ and $\kappa(y) = j$, then since $\kappa(x)+\kappa(y)+\kappa(L(x, y)) = 0$, $\kappa(L(x, y)) = 2i + 2j$. Since L is a Latin square, we know that no row or column of this restricted array contains any value more than once, but since every entry $z = L(x, y)$ satisfies $\kappa(z) = 2i + 2j$, each value must occur exactly once, which proves that the restricted array is a Latin square. If $i = j$, the restricted array also inherits the symmetry and idempotency properties of L, and so is therefore also a SILS. This is illustrated in the figure below. □

	X_0	X_1	X_2
X_0	X_0	X_2	X_1
X_1	X_2	X_1	X_0
X_2	X_1	X_0	X_2

We now look at the relationship between ψ and κ for a non-standard automorphism $\phi = (\psi, \kappa)$. Suppose $\kappa(x) = 0$ and $\kappa(y) = 1$ for some $x, y \in X$. Put $z = L(x, y)$. Then $\kappa(z) = 2$ by Lemma 2.5.1, and ϕ maps the non-vertical block $\{(x,0)\ (y,0)\ (z,1)\}$ to

$$\{(\psi(x),0)\ (\psi(y),1)\ (\psi(z),0)\},$$

and so we conclude that $\psi(y) = L(\psi(x), \psi(z))$. Thus we can state the following characterisation of even-vertical automorphisms:

Theorem 2.5.1. *The mapping $\phi = (\psi, \kappa) : (x, i) \to (\psi(x), i + \kappa(x))$ of points of D with ψ a permutation of X and $\kappa : X \to Z_3$, is an even-vertical automorphism of D if and only if for every $x, y \in X$ the following conditions are both satisfied:*

i) $\kappa(x) + \kappa(y) + \kappa(L(x, y)) = 0.$

ii) For $z = L(x, y)$:

(a) if $\kappa(x) = \kappa(y)$ then $\psi(z) = L(\psi(x), \psi(y))$, and

(b) if $\kappa(x) = \kappa(y) + 1$ then $\psi(x) = L(\psi(y), \psi(z))$.

Proof. First the necessity. If ϕ is an even-vertical automorphism then i) is true by Lemma 2.5.1. Also, if ϕ is standard then $\kappa(x) = \kappa(y)$ for all $x, y \in X$, and iia) is true. If ϕ is non-standard then for all $x, y \in X$ where $\kappa(x) = \kappa(y)$, iia) is true, and if $\kappa(x) \neq \kappa(y)$, then either $\kappa(x) = \kappa(y) + 1$ or $\kappa(x) = \kappa(y) + 1$ and iib) is true by the argument above.

Secondly, sufficiency. We have to show that if these conditions are satisfied, then ϕ is an automorphism of D.

1. For a vertical block $\{(x,0)\ (x,1)\ (x,2)\}$, ϕ maps this to the vertical block $\{(\psi(x), 0+\kappa(x))\ (\psi(x), 1+\kappa(x))\ (\psi(x), 2+\kappa(x))\}$, which is again a vertical block.

2. If $\{(x,i)\ (y,i)\ (z,i+1)\}$, with $z = L(x,y)$, is a non-vertical block and $\kappa(x) = \kappa(y)$, then condition i) gives us that $\kappa(z) = \kappa(y)$ also. Hence ϕ maps the block to $\{(\psi(x), i+\kappa(y))\ (\psi(y), i+\kappa(y))\ (\psi(z), i+1+\kappa(y))\}$, which is again a non-vertical block since $\psi(z) = L(\psi(x), \psi(y))$ by condition iia).

3. If $\{(x,i)\ (y,i)\ (z,i+1)\}$, with $z = L(x,y)$, is a non-vertical block and $\kappa(x) = \kappa(y) + 1$, then condition i) gives us that $\kappa(z) = \kappa(y) + 2$. Hence ϕ maps the block to $\{(\psi(x), i+1+\kappa(y))\ (\psi(y), i+\kappa(y))\ (\psi(z), i+\kappa(y))\}$. Condition iib) gives us $\psi(x) = L(\psi(y), \psi(z))$, and so the image is also a non-vertical block of D.

□

If ϕ is a non-standard automorphism of D, then Theorem 2.5.1 shows that L has special properties. The next chapter will deal with special types of Latin

square that will in some cases possess such properties. However, here we shall deal with the topic in a general way.

Firstly however, we need a further definition concerning Latin squares. Let M be a $m \times m$ Latin square with symbols on the m-set X_2, with rows indexed by the m-set X_0, and columns indexed by the m-set X_1. Let $\mathcal{T} = \{(x_0, x_1, x_2) : M(x_0, x_1) = x_2\}$. Let (a, b, c) be any permutation of $(0, 1, 2)$. The *(a,b,c)-conjugate* of M, $M_{(a,b,c)}$ has rows indexed by X_a, columns indexed by X_b, and symbols by X_c, and is defined by $M_{(a,b,c)}(x_a, x_b) = x_c$ for each $(x_0, x_1, x_2) \in \mathcal{T}$, [7], page 97.

In particular, $M_{(0,1,2)} = M$, and $M_{(1,0,2)}$ is the transpose of M.

The following construction provides an example of a design with a non-standard automorphism.

Let $n = 3m$, and $X = X_0 \cup X_1 \cup X_2$, with $X_a = \{x_{a,1}, x_{a,2}, \ldots, x_{a,m}\}$ for $a = 0, 1, 2$. Let L_0, L_1, L_2 each be a $m \times m$ SILS, where L_a has rows, columns and symbols indexed by X_a. Let M be an $m \times m$ Latin square with rows indexed by X_0, columns indexed by X_1, and symbols by X_2. We define the $3m \times 3m$ SILS L by the figure below:

	X_0	X_1	X_2
X_0	L_0	$M_{(0,1,2)}$	$M_{(0,2,1)}$
X_1	$M_{(1,0,2)}$	L_1	$M_{(1,2,0)}$
X_2	$M_{(2,0,1)}$	$M_{(2,1,0)}$	L_2

This is symmetric because the L_a, $a = 0, 1, 2$, are symmetric, and because,

for any permutation (a, b, c) of $(0, 1, 2)$:

$$L(x_{a,i}, x_{b,j}) = M_{(a,b,c)}(x_{a,j}, x_{b,i}) = M_{(b,a,c)}(x_{b,j}, x_{a,i}) = L(x_{b,j}, x_{a,i}).$$

Also, L is idempotent because the L_a are.

Moreover L possesses the property that for any permutation (a, b, c) of $(0, 1, 2)$, if $x_{c,k} = L(x_{a,i}, x_{b,j})$, then $x_{a,i} = L(x_{b,j}, x_{c,k})$ and $x_{b,j} = L(x_{a,i}, x_{c,k})$, since

$$L(x_{b,j}, x_{c,k}) = M_{(b,c,a)}(x_{b,j}, x_{c,k}) = x_{a,i}$$

and

$$L(x_{c,k}, x_{a,i}) = M_{(c,a,b)}(x_{c,k}, x_{a,i}) = x_{b,j}.$$

We shall refer to this as Property (*).

Now let τ be any function $\{0, 1, 2\} \to Z_3$ such that $\tau(0) + \tau(1) + \tau(2) = 0$, then the mapping on D defined by

$$\phi_\tau(x_{a,i},\ s) = (x_{a,i},\ s + \tau(a))$$

is an even-vertical automorphism of D by Theorem 2.5.1. If τ is constant, then the ϕ_τ is standard, otherwise it is non-standard. Now the group of possible τ is isomorphic to $Z_3 \times Z_3$ since the value of τ on any two elements of Z_3 can be chosen independently. Therefore the group of even-vertical automorphisms generated by all ϕ_τ is also isomorphic to $Z_3 \times Z_3$. This is not necessarily the full automorphism group of D, since L may have further automorphisms.

Chapter 3

Bose designs from special Latin squares

This chapter deals with the automorphism groups of Bose designs based on two types of Latin square: firstly where the SILS is provided by another Steiner triple system, and secondly where the SILS is derived from an Abelian group. The previous chapter has provided an analysis of the automorphism groups at the most general level. This chapter will focus mainly on the conditions for the automorphism group to have non-standard automorphisms.

3.1 Bose designs on Steiner triple systems

A Steiner triple system $T = (U, \mathcal{A})$ with point set U and block set $\mathcal{A}$ can be interpreted as a special type of SILS, with the extra property that, if $\{x, y, z\}$ is in $\mathcal{A}$, then $L(x, y) = z$, $L(y, z) = x$, and $L(x, z) = y$, since every pair of points occurs in exactly one block. This is similar to the Property (*) mentioned in Section 2.5. For a Steiner triple system $T = (U, \mathcal{A})$, the Bose design based on T,

$D = (V, \mathcal{B})$, has as point set:

$$V = \{(x, i) : x \in U, i \in Z_3\},$$

and block set:

$$\mathcal{B} = \{\ \{(x,0)\ (x,1)\ (x,2)\} : x \in U\} \cup$$

$$\{\ \{(x,i)\ (y,i)\ (z,i+1)\},$$

$$\{(x,i)\ (z,i)\ (y,i+1)\},$$

$$\{(y,i)\ (z,i)\ (x,i+1)\} :\ \{x,y,z\} \in\ \mathcal{A},\ i \in Z_3\ \}.$$

We can immediately cite Lemma 2.3.1 to give:

Lemma 3.1.1. *The group of standard automorphisms of the Bose design $D = (V, \mathcal{B})$ obtained from the Steiner triple system T is isomorphic to $Aut(T) \times Z_3$ where $Aut(T)$ is the automorphism group of T.*

A major point of interest is to determine which designs give rise to non-standard automorphisms.

Referring to Theorem 2.5.1, we see that if ψ is any automorphism of T, and κ is any mapping $\kappa : U \rightarrow Z_3$ satisfying $\kappa(x) + \kappa(y) + \kappa(z) = 0$ for every block $\{x, y, z\}$ in $\mathcal{A}$, then $\phi = (\psi, \kappa)$ is an even-vertical automorphism of D, which is non-standard if κ is not constant on U.

Existence of a non-standard automorphism of D therefore implies via Lemma 2.5.2 that $|U|$ is divisible by 3, with $U = W_0 \cup W_1 \cup W_2$, $|W_q| = \frac{|U|}{3}$. From Lemma 2.5.3 we have that the blocks of T are of 4 types:

i) $\mathcal{C}_0 = \{\ \{x, y, z\} :\ x, y, z \in W_0\}$,

ii) $\mathcal{C}_1 = \{\ \{x,y,z\} :\ x,y,z \in W_1\}$,

iii) $\mathcal{C}_2 = \{\ \{x,y,z\} :\ x,y,z \in W_2\}$,

iv) $\mathcal{C}_{0,1,2} = \{\ \{x,y,z\} :\ x \in W_0,\ y \in W_1,\ z \in W_2\}$.

Further, each pair $S_q = (W_q, \mathcal{C}_q)$ is a Steiner triple subsystem of T, and Lemma 2.5.3 shows that the blocks $\mathcal{C}_{0,1,2}$ form a Latin square. It also follows that $|U| \equiv 3$ or $9 \pmod{18}$. We can therefore state the following:

Theorem 3.1.1. *The Bose Steiner triple system D constructed on the Steiner triple system $T = (U, \mathcal{A})$ has a non-standard automorphism if and only if $|U| = 3m$ with $m \equiv 1$ or $3 \pmod 6$; $U = W_0 \cup W_1 \cup W_2$, $|W_q| = m$ for $q = 0,1,2$, and there exist Steiner triple systems $S_q = (W_q, \mathcal{C}_q)$, $q = 0,1,2$ and an $m \times m$ Latin square M with rows indexed by W_0, columns indexed by W_1, and symbols indexed by W_2 such that:*

$$\mathcal{A} = \mathcal{C}_0 \cup \mathcal{C}_1 \cup \mathcal{C}_2 \cup \{\ \{x,y,z\} : x \in W_0, y \in W_1, z \in W_2, z = M(x,y)\ \}$$

Proof. The necessity part of the proof is furnished by the argument above.

The sufficiency is provided by the mapping ϕ which is defined on U by $\phi(x,i) = (x, i+\kappa(x))$, where $\kappa(x) = q$ if $x \in W_q$. The map ϕ is clearly one-to-one. To show that it is an automorphism of D, we must prove it maps blocks of D to blocks of D. For a vertical block $\{(w_q,0)\ (w_q,1)\ (w_q,2)\}$, with $w_q \in W_q$, the image under ϕ is $\{(w_q,q)\ (w_q,1+q)\ (w_q,2+q)\}$, which is the same vertical block. Now consider non-vertical blocks, which are of two types:

a) Firstly blocks of the form $\{(x_q,i)\ (y_q,i)\ (z_q,i+1)\}$, derived from a block $\{x_q,y_q,z_q\}$ of the subsystem S_q of T. This is mapped by ϕ to $\{(x_q,q+i)\ (y_q,q+i)\ (z_q,q+i+1)\}$, which is again a non-vertical block.

b) Secondly blocks derived from blocks of T of the form $\{x_0, y_1, z_2\}$, where $x_0 \in W_0$, $y_1 \in W_1$, $z_2 \in W_2$, and $z_2 = M(x_0, y_1)$. For each such block and each $i \in Z_3$ there are three blocks of D, namely: $\{(x_0, i)\ (y_1, i)\ (z_2, i+1)\}$, $\{(x_0, i+1)\ (y_1, i)\ (z_2, i)\}$, and $\{(x_0, i)\ (y_1, i+1)\ (z_2, i)\}$. The map ϕ takes these blocks to: $\{(x_0, i)\ (y_1, i+1)\ (z_2, i)\}$, $\{(x_0, i+1)\ (y_1, i+1)\ (z_2, i+2)\}$, and $\{(x_0, i)\ (y_1, i+2)\ (z_2, i+2)\}$ respectively. These are again non-vertical blocks.

The automorphism ϕ is non-standard, because κ is not constant on U. □

A special case of the construction in Theorem 3.1.1 is the *tripling construction.* In the language of Theorem 3.1.1, the tripling construction sets all of S_0, S_1, S_2 isomorphic to the same Steiner triple system $S = (W, \mathcal{C})$ of order m, with M being the SILS which is derived from the same system. We represent the point set of T as $U = \{(x, q) : x \in W, q \in Z_3\}$. The block set is:

$$\begin{aligned}\mathcal{A} = \{&\{(x,0)\ (y,0)\ (z,0)\},\\ &\{(x,1)\ (y,1)\ (z,1)\},\ \{(x,2)\ (y,2)\ (z,2)\},\\ &\{(x,0)\ (y,1)\ (z,2)\},\ \{(x,1)\ (y,2)\ (z,0)\},\\ &\{(x,2)\ (y,0)\ (z,1)\},\ \{(x,0)\ (y,2)\ (z,1)\},\\ &\quad \{(x,2)\ (y,1)\ (z,0)\},\ \{(x,1)\ (y,0)\ (z,2),\ \} : \{x,y,z\} \in \mathcal{C}\} \cup\\ &\{\{(x,0)\ (x,1)\ (x,2)\ \} : x \in W\}.\end{aligned}$$

This may be more succinctly represented as:

$$\begin{aligned}\mathcal{A} = \{&\{(x,i)\ (y,i+j)\ (z,i+2j)\} : \{x,y,z\} \in \mathcal{C},\ i,j \in Z_3\} \cup\\ &\{\{(x,0)\ (x,1)\ (x,2)\ \} : x \in W\}.\end{aligned}$$

If ψ is an automorphism of the STS T obtained from S by the tripling con-

struction, we assert that the maps $\phi_{r,s}$, for any $r, s \in Z_3$, defined by

$$\phi_{r,s} : ((x,i),k) \rightarrow (\psi(x,i), k + r + is),$$

for $x \in W$, $i, k \in Z_3$, are automorphisms of the Bose design $D = (V, \mathcal{B})$ on T.

Firstly, $\phi_{r,s}$ is one-to-one on V because if

$$(\psi(x,i), k + r + is) = (\psi(y,j), k' + r + js),$$

then $x = y$ and $i = j$ because ψ is one-to-one on U, and so $k = k'$ also.

Secondly, $\phi_{r,s}$ maps blocks to blocks. Considering the vertical block:

$\phi_{r,s} : \{((x,i),0),\ ((x,i),1),\ ((x,i),2)\} \rightarrow$

$\{(\psi(x,i), r + is),\ (\psi(x,i), 1 + r + is),\ (\psi(x,i), 2 + r + is)\}$,

which is again a vertical block.

Now consider non-vertical blocks:

$\phi_{r,s} : \{((x,i),k),\ ((y,i+j),k),\ ((z,i+2j),k+1)\} \rightarrow$

$\{(\psi(x,i), k+r+is),\ (\psi(y,i+j), k+r+is+js),\ (\psi(z,i+2j), k+1+r+is+2js)\}$,

which is a non-vertical block because it has signature 1, and:

$\phi_{r,s} : \{((x,0),k),\ ((x,1),k),\ ((x,2),k+1)\} \rightarrow$

$\{(\psi(x,0), k + r),\ (\psi(x,1), k + r + s),\ (\psi(x,2), k + 1 + r + 2s)\}$, also a non-vertical block.

The $\phi_{r,s}$ are distinct because $r + is = r' + is'$ for all $i \in Z_3$ if and only if $r = r'$ and $s = s'$.

We have therefore shown that the Steiner triple system $D = (V, \mathcal{B})$ constructed on the tripled design $T = (U, \mathcal{A})$ using the Bose construction has a group Γ of even-vertical automorphisms that is isomorphic to $Aut(T) \times Z_3 \times Z_3$, where $Aut(T)$

is the automorphism group of T. The group Γ contains both standard and non-standard automorphisms, but is not necessarily the full automorphism group of the Bose design.

3.2 Bose designs on Abelian groups

If G is an Abelian group of odd order with the group operation written additively, then for $x, y \in G$,

$$L(x, y) = (x + y)/2$$

defines a SILS on the elements of G.

In this section, we shall deduce the full automorphism group of the Bose design D constructed from this special type of SILS in terms of the group G and its automorphisms, building on the results of the previous chapter.

3.2.1 Conditions for $Aut(D)$ to be non-standard.

We shall say that an even-vertical automorphism ϕ of D *acts standardly* on $x \in G$ if ϕ permutes the labels of the vertical block on x in the same way as it permutes the labels of the vertical block on the zero element of G. We shall say that ϕ of D *acts non-standardly* on x if it does not act standardly.

Theorem 3.2.1. *If $Aut(D)$ is non-standard, then all elements of G are of order either 3 or 9, and so G is isomorphic to a direct sum of copies of Z_3 and/or Z_9.*

Proof. We assume that $|G| \geq 3$. Suppose that ϕ is an automorphism of D, which

acts non-standardly on $x \in G$. Consider the array

$$\begin{array}{ccc} (0,0) & (0,1) & (0,2) \\ (x,2) & (x,0) & (x,1) \\ (-x,2) & (-x,0) & (-x,1) \end{array}$$

Since the composition of ϕ with a translation $\tau : (x,i) \to (x,i+k)$ for some $k \in Z_3$ still acts non-standardly on x, we may assume that the top row maps to $(u,0),\ (u,1),\ (u,2)$ for some $u \in G$. Then the next row maps to either $(v,0),\ (v,1),\ (v,2)$ or $(v,1),\ (v,2),\ (v,0)$ for some $v \in G$, in which case the third row maps to either $(w,1),\ (w,2),\ (w,0)$ or $(w,0),\ (w,1),\ (w,2)$ respectively for some $w \in G$. There is no loss of generality, because x can be renamed $-x$ or vice-versa, in assuming the former in each case. So the above array maps to

$$\begin{array}{ccc} (u,0) & (u,1) & (u,2) \\ (v,0) & (v,1) & (v,2) \\ (w,1) & (w,2) & (w,0) \end{array}$$

Hence $u + v = 2w$.

Suppose $3x \neq 0$. Then, by considering the blocks $\{(3x,1),\ (-x,1),\ (x,2)\}$ and $\{(-3x,0),\ (x,0),\ (-x,1)\}$, it follows that $(3x,1)$ maps to $((v+w)/2,1)$, and $(-3x,0)$ maps to $(2v-w,0)$. Now from the block $\{(9x,0),\ (-3x,0),\ (3x,1)\}$ it is deduced that $(9x,0)$ maps to $(2w-v,0) = (u,0)$. Hence $9x = 0$, i.e. all elements of G on which ϕ acts non-standardly have order either 3 or 9.

We have yet to show that *all* non-zero elements of G have order 3 or 9. Observe

that for $x, y, z \in G$, and $x + y = 2z$, and any even-vertical automorphism ϕ of $AutD$, ϕ either applies the same permutation of the labels to the vertical blocks on all three of x, y, z, or different permutations to each. This is because ϕ preserves signatures, and so ϕ either shifts all the labels of any non-vertical block containing x, y and z by the same value, or all by different values.

Suppose that ϕ acts non-standardly on x and standardly on $y \neq 0$, that is, the permutations applied to the labels on the vertical blocks on x and y are different. Consider the block $\{(x, 0), (y, 0), (\frac{x+y}{2}, 1)\}$. Then the permutation applied to the vertical block on $\frac{x+y}{2}$ is different to both of them. So ϕ also acts non-standardly on $\frac{x+y}{2}$. Thus $9(\frac{x+y}{2}) = 0$, giving $9y = 0$, i.e. all elements, other than the identity, have order either 3 or 9. □

3.2.2 Group of standard automorphisms.

The full automorphism group of every Bose design except for those designs constructed from copies of Z_3 and/or Z_9 is therefore standard. The remaining automorphism groups possess standard subgroups. The result proved in this section provides the structure for all standard automorphism groups. First of all however, it is necessary to visit a group construct.

A *semidirect product* $K \times_\theta H$ is formed from two groups K, H, and a homomorphism $\theta : H \to Aut(K)$, with the binary operation

$$* : (k_1, h_1) * (k_2, h_2) = (\ k_1\theta(h_1)(k_2), h_1h_2\ ).$$

A prime example of a semidirect product is the product NH of a normal subgroup N and another subgroup H of some containing group Γ, such that $N \cap H = \{1\}$. The set NH is a subgroup of Γ because: $n_1h_1n_2h_2 = n_1(h_1n_2h_1^{-1})h_1h_2$.

Since N is normal in Γ, the element $h_1 n_2 h_1^{-1}$ is an element of N, so $n_1(h_1 n_2 h_1^{-1}) \in N$, and of course $h_1 h_2 \in H$, so $n_1 h_1 n_2 h_2 \in NH$. Also, if $n_1 h_1 = n_2 h_2$, then $n_2^{-1} n_1 = h_2 h_1^{-1} \in N \cap H = \{1\}$, so $n_1 = n_2$ and $h_1 = h_2$, and every element of NH has a unique expression in terms of N and H.

The map $\phi_h : n \to hnh^{-1}$ is an automorphism of N (an *inner automorphism*), and the map $\theta : h \to \phi_h$ is a homomorphism $\theta : H \to Aut(N)$.

If $H \cong Aut(K)$, with θ the identity, then the semidirect product is called the *Holomorph* of K, denoted by $Hol(K)$ (see [15] page 461).

Theorem 3.2.2. *The group of standard automorphisms of D is isomorphic to $Hol(G) \times Z_3$, and so is of order $3|G||Aut(G)|$.*

Proof. If $g \in G$, $\alpha \in Aut(G)$, and s is an element of Z_3, then consider the map $[g, \alpha, s]$ of elements of D defined by $[g, \alpha, s] : (x, i) \to (g + \alpha(x), i + s)$. The map $[g, \alpha, s]$ is clearly a permutation of the points of D. It maps vertical blocks to vertical blocks, and also non-vertical blocks to non-vertical blocks, because if $x, y, z \in G$, and $x + y = 2z$, then

$$(g + \alpha(x)) + (g + \alpha(y)) = 2g + \alpha(x + y) = 2(g + \alpha(z)),$$

and because even permutations of the labels preserve blocks. So $[g, \alpha, s]$ is an element of $Aut(D)$, and is standard. Moreover the mapping $(g, \alpha, s) \mapsto [g, \alpha, s]$ is a one-to-one map of the set $G \times Aut(G) \times Z_3$ into $Aut(D)$. This is because if $(g_1 + \alpha_1(x), i + s_1) = (g_2 + \alpha_2(x), i + s_2)$ for all $x \in G$, then $s_1 = s_2$, and $g_1 + \alpha_1(0) = g_2 + \alpha_2(0)$. Thus since $\alpha_1(0) = \alpha_2(0) = 0$, $g_1 = g_1$ and $\alpha_1(x) = \alpha_2(x)$ for all $x \in G$, so $\alpha_1 = \alpha_2$ also.

The mapping is also a group homomorphism $Hol(G) \times Z_3 \to Aut(D)$ because

for any element (x, i) of D,

$$\begin{aligned}
[g_1, \alpha_1, s_1][g_2, \alpha_2, s_2](x, i) &= [g_1, \alpha_1, s_1](g_2 + \alpha_2(x), i + s_2) \\
&= (g_1 + \alpha_1(g_2) + \alpha_1\alpha_2(x), i + s_1 + s_2) \\
&= [g_1 + \alpha_1(g_2), \alpha_1\alpha_2, s_1 + s_2](x, i)
\end{aligned}$$

We show that this is a mapping onto to the subgroup comprising the standard automorphisms of D by constructing a corresponding triple (g, α, s) for any given standard automorphism.

Suppose ϕ is a standard automorphism of D. We can represent ϕ as $\phi : (x, i) \rightarrow (\phi_G(x), i + s)$ for a fixed $s \in Z_3$ and a permutation ϕ_G of G.

We assert that the required triple is $[\phi_G(0), \Phi, s]$ where the map $\Phi : G \rightarrow G$ is given by $\Phi(x) = \phi_G(x) - \phi_G(0)$.

That the map $\Phi : x \mapsto \phi_G(x) - \phi_G(0)$ is an automorphism of G follows from the identity

$$\phi(\{(x, 0),\ (y, 0),\ (z, 1)\}) = \{(\phi_G(x), s),\ (\phi_G(y), s),\ (\phi_G(z), 1 + s)\}$$

for mapping of non-vertical blocks, applied to the blocks

$$\begin{aligned}
\{(x, 0),&\ (-x, 0),&\ (0, 1)\} \\
\{(y, 0),&\ (0, 0),&\ (\tfrac{1}{2}y, 1)\} \\
\{(x + y, 0),&\ (-x, 0),&\ (\tfrac{1}{2}y, 1)\}
\end{aligned}$$

which implies the identities

$$\begin{aligned}\phi_G(x) + \phi_G(-x) &= 2\phi_G(0)\\ \phi_G(y) + \phi_G(0) &= 2\phi_G(\frac{1}{2}y)\\ \phi_G(x+y) + \phi_G(-x) &= 2\phi_G(\frac{1}{2}y)\end{aligned}$$

which implies

$$\phi_G(x+y) = \phi_G(x) + \phi_G(y) - \phi_G(0).$$

Therefore $\Phi(x+y) = \Phi(x) + \Phi(y)$, and Φ is an automorphism of G. Clearly $[\phi_G(0), \Phi, s] = \phi$, and we have the required isomorphism. □

3.2.3 Non-standard automorphisms

As has been proved Section 3.2.1, non-standard automorphisms are only possessed by Bose designs constructed from groups G is of the form $Z_3^n \oplus Z_9^m$, $n + m \neq 0$. The non-standard and standard automorphisms of a Bose design together also form an automorphism group, which is the whole automorphism group unless $G = Z_3$. We now derive the structure for this group.

Lemma 3.2.1. *If $x, y \in Z_3$, then*

$$(-2)^x + (-2)^y \equiv (-2)^{x+y} + 1 \pmod 9$$

Proof. There are only nine cases to check, seven of which are trivial. □

We can represent any even-vertical automorphism ϕ of D as a pair of maps (ψ, κ), $\psi : G \to G$, $\kappa : G \to Z_3$, where ψ is a permutation of G, and if (x, i) is

any point of D,

$$\phi : (x, i) \mapsto (\psi(x), i + \kappa(x))$$

The next lemma characterises κ as a map of groups, and proves identities necessary for the characterisation of the automorphism group.

Lemma 3.2.2. *If G is of the form $Z_3^n \oplus Z_9^m$, and $\phi = (\psi, \kappa)$ is any even-vertical automorphism of D, then the following are true:*

(a) If $x, y, z \in G$, and if $x + y = 2z$, then $\kappa(x) + \kappa(y) + \kappa(z) \equiv 0 \pmod 3$,

(b) The map $G \to Z_3$ defined by $x \mapsto \kappa(x) - \kappa(0)$ is a homomorphism,

(c) If $x, y, z \in G$, and $x + y = 2z$, then

$$(-2)^{\kappa(x)}\psi(x) + (-2)^{\kappa(y)}\psi(y) + (-2)^{1+\kappa(z)}\psi(z) = 0$$

(d) If $x, y, z \in G$, and $x + y = 2z$, then

$$(-2)^{\kappa(x)} + (-2)^{\kappa(y)} + (-2)^{1+\kappa(z)} \equiv 0 \pmod 9$$

Proof. (a) This was established for any SILS in Lemma 2.5.1.

(b) We have to show that $\kappa(x + y) - \kappa(0) = \kappa(x) - \kappa(0) + \kappa(y) - \kappa(0)$ for any $x, y \in G$, i.e. $\kappa(x + y) + \kappa(0) = \kappa(x) + \kappa(y)$. But, putting $x + y = 2z$, we have from (a) by writing $x + y = 2z = (x + y) + 0$,

$$\kappa(x) + \kappa(y) + \kappa(z) = 0 = \kappa(x + y) + \kappa(0) + \kappa(z)$$

and the result follows.

(c) Observe from (a) that $\kappa(x), \kappa(y), \kappa(z)$ are either all the same or all different. Consider the mapping of the block $\{(x,i),\ (y,i),\ (z,i+1)\}$ by (ψ,κ) to the block $\{\psi(x), i+\kappa(x)),\ (\psi(y), i+\kappa(y)),\ (\psi(z), i+1+\kappa(z))\}$. If $\kappa(x), \kappa(y), \kappa(z)$ are all the same, then $\psi(x)+\psi(y) = 2\psi(z)$, and hence $\psi(x)+\psi(y)+(-2)\psi(z) = 0$. If they are all different, then suppose without loss of generality that $\kappa(x) = 1+\kappa(z)$, and $\kappa(y) = 2+\kappa(z)$, then the image of $\{(x,i),\ (y,i),\ (z,i+1)\}$ is

$$\{(\psi(x), i+1+\kappa(z)),\ (\psi(y), i+2+\kappa(z)),\ (\psi(z), i+1+\kappa(z))\}$$

and so $\psi(x)+\psi(z) = 2\psi(y)$, or $\psi(x)+(-2)\psi(y)+\psi(z) = 0$, so

$$(-2)^{1+\kappa(z)}\psi(x) + (-2)^{2+\kappa(z)}\psi(y) + (-2)^{1+\kappa(z)}\psi(z) = 0$$

and the required result follows.

(d) It is only necessary to use (a), and to check the three cases where $\kappa(x)$, $\kappa(y)$, $\kappa(z)$ are: all the same, an even permutation of $(0,1,2)$, and an odd permutation of the same.

□

The previous two lemmas provide the material to identify the group of all even-vertical automorphisms of D. In the following theorem we denote the group of homomorphisms from G to Z_3 by $Hom(G, Z_3)$, where for $\alpha_1, \alpha_2 \in Hom(G, Z_3)$, we define $\alpha_1 + \alpha_2$ by $(\alpha_1+\alpha_2)(g) = \alpha_1(g) + \alpha_2(g)$ for all $g \in G$.

Theorem 3.2.3. *If $\phi = (\psi, \kappa)$ is an even-vertical automorphism of D, then the map $x \mapsto (-2)^{\kappa(x)}(\psi(x) - \psi(0))$ is an automorphism of G. The group of even-*

vertical automorphisms of D is isomorphic to a group on
$Z_3 \times G \times Hom(G, Z_3) \times Aut(G)$, *by the map*

$$(\psi, \kappa)(x) \mapsto (\kappa(0), \psi(0), \kappa(x) - \kappa(0), (-2)^{\kappa(x)}(\psi(x) - \psi(0)))$$

so that all even-vertical automorphisms $\phi = (\psi, \kappa)$ of D can be expressed in the form

$$\kappa(x) = s + h(x), \quad \psi(x) = g + (-2)^{-\kappa(x)}\alpha(x);$$

$$s \in Z_3, \ h \in Hom(G, Z_3), \ g \in G, \ \alpha \in Aut(G).$$

Proof. That the map $x \mapsto (-2)^{\kappa(x)}(\psi(x) - \psi(0))$ is a group homomorphism uses Lemma 3.2.2 parts (c) and (d). Writing $\alpha(x) = (-2)^{\kappa(x)}(\psi(x) - \psi(0))$, (c) and (d) imply that if $x + y = 2z$ (including $x = y = z$), then

$$\begin{aligned}\alpha(x) + \alpha(y) - 2\alpha(z) = {} & (-2)^{\kappa(x)}\psi(x) + (-2)^{\kappa(y)}\psi(y) + (-2)^{1+\kappa(z)}\psi(z) \\ & - \psi(0)((-2)^{\kappa(x)} + (-2)^{\kappa(y)} + (-2)^{1+\kappa(z)}) \\ = {} & 0.\end{aligned}$$

So, in the same way as for Lemma 3.2.2, we can write:

$$\begin{aligned} \alpha(2x) + \alpha(2y) &= 2\alpha(x+y) \\ 2\alpha(x) &= \alpha(2x) + \alpha(0) \\ 2\alpha(y) &= \alpha(2y) + \alpha(0) \end{aligned}$$

Since $\alpha(0) = 0$, the sum of these three equations yields $\alpha(x) + \alpha(y) = \alpha(x + y)$ for all $x, y \in G$, and so α is a group homomorphism on G. To show that α is one-to-one it is sufficient to show that $\alpha(x) = 0$ iff $x = 0$, since α is a group

homomorphism. However from its definition, $\alpha(x) = 0$ iff $\psi(x) = \psi(0)$, so $x = 0$ since ψ is one-to-one on G.

The above establishes the mapping from $Aut(D)$ to the Cartesian product $Z_3 \times G \times Hom(G, Z_3) \times Aut(G)$. The map is one-to-one because the first three components of the image determine $\psi(0)$ and κ, whilst these and the fourth component are sufficient to determine ψ.

We next show that the map is onto. We shall show that if $s \in Z_3$, $h \in Hom(G, Z_3)$, $\alpha \in Aut(G)$, and $g \in G$, then (ψ, κ), where $\psi : G \mapsto G$ is defined as $\psi(x) = g + (-2)^{-\kappa(x)}\alpha(x)$, and $\kappa : G \mapsto Z_3$ is defined as $\kappa(x) = s + h(x)$, is an automorphism of D. Firstly we assert that (ψ, κ) maps blocks to blocks. Clearly it maps vertical blocks to vertical blocks, so in the following we have only to consider non-vertical blocks.

Observe that if $x, y, z \in G$ such that $x + y = 2z$, then

$$\kappa(x) + \kappa(y) + \kappa(z) = 0$$

since the left-hand side is equal to

$$3s + h(x) + h(y) + h(z) = h(x + y) - 2h(z) = h(x + y - 2z) = 0,$$

since $h \in Hom(G, Z_3)$. Also,

$$(-2)^{\kappa(x)}\psi(x) + (-2)^{\kappa(y)}\psi(y) + (-2)^{1+\kappa(z)}\psi(z) = 0$$

since the left-hand side is equal to

$$\begin{aligned}
&\alpha(x)+\alpha(y)-2\alpha(z)+((-2)^{\kappa(x)}+(-2)^{\kappa(y)}+(-2)^{1+\kappa(z)})g \\
&= 0+((-2)^{\kappa(x)}+(-2)^{\kappa(y)}+(-2)^{1+\kappa(z)})g, \quad \text{since } \alpha \in Aut(G) \\
&= (1+(-2)^{\kappa(x)+\kappa(y)}+(-2)^{1+\kappa(z)})g, \qquad \text{by Lemma 3.2.1} \\
&= (2+(-2)^{\kappa(x)+\kappa(y)+1+\kappa(z)})g, \qquad \text{again by Lemma 3.2.1,} \\
&= (2+(-2)^{3s+3h(z)+1})g \\
&= 0.
\end{aligned}$$

The first of these relationships once again shows that $\kappa(x), \kappa(y), \kappa(z)$ are either all the same or all different. If they are all the same, the second relationship gives $\psi(x)+\psi(y)=2\psi(z)$, and so (ψ, κ) maps the block $\{(x,i),(y,i),(z,i+1)\}$ to the block

$$\{(\psi(x), i+\kappa(x)), (\psi(y), i+\kappa(x)), (\psi(z), 1+i+\kappa(x))\}.$$

If $\kappa(x), \kappa(y), \kappa(z)$ are all different, then $1+\kappa(z)$ is equal either to $\kappa(x)$ or to $\kappa(y)$. Without loss of generality suppose the former. Then $\kappa(y) = 1+\kappa(x)$, and the second of the relationships proved above implies

$$(-2)^{\kappa(x)}\psi(x)+(-2)^{1+\kappa(x)}\psi(y)+(-2)^{\kappa(x)}\psi(z)=0.$$

Hence $\psi(x)+\psi(z)+(-2)\psi(y)=0$ since $(-2)^{\kappa(x)} \neq 0$, so $\psi(x)+\psi(z)=2\psi(y)$, and (ψ, κ) maps the block $\{(x,i),(y,i),(z,i+1)\}$ to the block

$$\{(\psi(x), i+\kappa(x)), (\psi(z), i+\kappa(x)), (\psi(y), 1+i+\kappa(x))\}.$$

Therefore (ψ, κ) maps blocks to blocks.

Secondly we show that (ψ, κ) is one-to-one. This follows because if $(\psi, \kappa)(x, i) = (\psi, \kappa)(y, j)$, then $\psi(x) = \psi(y)$, i.e.

$$(-2)^{-\kappa(x)}\alpha(x) + g = (-2)^{-\kappa(y)}\alpha(y) + g.$$

Since (-2) factors commute with α, we have $\alpha((-2)^{-\kappa(x)}x) = \alpha((-2)^{-\kappa(y)}y)$, so $(-2)^{-\kappa(x)}x = (-2)^{-\kappa(y)}y$ since α is one-to-one. Thus

$$(-2)^{-\kappa(x)+\kappa(y)}x - y = (-2)^{-h(x-y)}x - y = 0.$$

However $h((-2)^z x) = (-2)^z h(x) = h(x)$ for any $z \in Z_3$, since (-2) is the identity on Z_3, so

$$h(x - y) = h((-2)^{-h(x-y)}x - y) = h(0) = 0,$$

and so $x = y$. Also, since $i+\kappa(x) = j+\kappa(y)$, $i = j$. Therefore (ψ, κ) is one-to-one. Thus (ψ, κ) is an automorphism of D. □

The group $Hom(G, Z_3)$ is of order 3^{n+m}, since for any such homomorphism each generator of $G = {Z_3}^n \oplus {Z_9}^m$ maps to one of 0, 1, or 2. The group of even-vertical automorphisms $Z_3 \times G \times Hom(G, Z_3) \times Aut(G)$ is therefore of order $3^{2n+3m+1}|AutG|$ for $G = Z_3^n \oplus Z_9^m$, and is the full automorphism group except for the special case $G = Z_3$, due to the extra symmetry between G and the label set Z_3.

3.2.4 Affine geometries, $AG(n,3)$.

The STS(9) has a special automorphism group in the series of group-based Bose constructions because it is also in another series of Steiner triple systems, the affine geometries, $AG(n,3)$. These have as their point set the groups Z_3^n, and for blocks the triples $\{(g_1,g_2,g_3) : g_1 \neq g_2, g_1+g_2+g_3 = 0\}$. This works because the equation ensures that exactly one block contains each pair, and no block contains repeated points because if $g_1 = g_2$, then $g_3 = -g_1 - g_2 = -2g_1 = g_1$.

The full automorphism group for these systems is readily found.

Theorem 3.2.4. *The full automorphism group of the STS $D = AG(n,3)$ is isomorphic to $Hol(Z_3^n)$.*

Proof. The proof is very similar to that of Theorem 3.2.2. Let H be the set of all maps $[g,\alpha]$, $g \in Z_3^n$, $\alpha \in Aut(Z_3^n)$ defined by $[g,\alpha](x) = g + \alpha(x)$. We shall show that:

i The $[g,\alpha]$ are distinct.

ii Each $[g,\alpha]$ is an automorphism of D.

iii Every automorphism of D is a $[g,\alpha]$ for some g and α.

iv H is a group isomorphic to $Hol(Z_3^n)$.

i If $[g_1,\alpha_1] = [g_2,\alpha_2]$, then $g_1+\alpha_1(x) = g_2+\alpha_2(x)$ for all $x \in Z_3^n$. This implies that $g_1-g_2 = \alpha_1(x)-\alpha_2(x)$ for all $x \in Z_3^n$. Hence $g_1-g_2 = \alpha_1(0)-\alpha_2(0) = 0$, since α_1, α_2 are group automorphisms. So $g_1 = g_2$ and $\alpha_1(x) = \alpha_2(x)$ for all $x \in Z_3^n$, so $\alpha_1 = \alpha_2$. Hence the $[g,\alpha]$ are distinct.

ii Each $[g, \alpha]$ is clearly one-to-one because α is one-to-one, and maps blocks to blocks because if $x, y, z \in Z_3^n$ and $x + y + z = 0$, then

$$\begin{aligned} [g,\alpha](x) + [g,\alpha](y) + [g,\alpha](z) &= 3g + \alpha(x) + \alpha(y) + \alpha(z) \\ &= 0 + \alpha(x+y+z) \\ &= \alpha(0) \\ &= 0. \end{aligned}$$

Therefore $[g, \alpha]$ is an automorphism of D.

iii If ϕ is an automorphism of D, set $\Phi(x) = \phi(x) - \phi(0)$. We assert that Φ is a group automorphism of Z_3^n, and that $[\phi(0), \Phi] = \phi$. The map Φ is clearly one-to-one because ϕ is. We have to show that for $x, y \in Z_3^n$, $\Phi(x) + \Phi(y) = \Phi(x + y)$. Firstly we show that $\Phi(-x) = -\Phi(x)$. Since $\{-x, x, 0\}$ is a block, and $\Phi(0) = 0$, we have $\Phi(-x) + \Phi(x) = 0$. Then, since $\{x, y, -(x + y)\}$ is a block, we have $\Phi(x) + \Phi(y) + \Phi(-(x + y)) = 0$, so $\Phi(x) + \Phi(y) = \Phi(x + y)$.

iv H has the same underlying set $Z_3^n \times Aut(Z_3^n)$ as $Hol(Z_3^n)$. We have to show that H is a group with the same composition rule as $Hol(Z_3^n)$. For $x \in Z_3^n$,

$$[g_1, \alpha_1][g_2, \alpha_2](x) = [g_1, \alpha_1](g_2, \alpha_2(x)) = g_1 + \alpha_1(g_2) + \alpha_1\alpha_2(x) = [g_1 + \alpha_1(g_2), \alpha_1\alpha_2](x),$$

which is the composition rule for $Hol(Z_3^n)$. The inverse of $[g, \alpha]$ is $[-\alpha^{-1}(g), \alpha^{-1}]$, since

$$[g, \alpha][-\alpha^{-1}(g), \alpha^{-1}](x) = [g - \alpha\alpha^{-1}(g), \alpha^{-1}\alpha](x) = x,$$

and

$$[-\alpha^{-1}(g), \alpha^{-1}][g, \alpha](x) = [-\alpha^{-1}(g) + \alpha^{-1}(g), \alpha^{-1}\alpha](x) = x.$$

Hence H is isomorphic to $Hol(Z_3^n)$.

□

3.2.5 Some examples

As an illustration of the results of this chapter, we will consider four STS(81)s, and calculate the orders of their automorphism groups.

Let

$$G_1 = Z_{27},$$

$$G_2 = Z_3 \times Z_3 \times Z_3,$$

$$G_3 = Z_3 \times Z_9,$$

and

$$G_4 = Z_3 \times Z_3 \times Z_3 \times Z_3.$$

Then the Bose constructions on G_1, G_2, and G_3 are all of order 81, as is the affine geometry on G_4.

Before we can calculate the orders of the Bose designs we need to know $|Aut(G)|$ for $G = Z_3^n$, and $G = Z_3 \times Z_9$. For the former, the result is well-known, see for example [6] page 128, as the order of $GL(n, Z_3)$:

$$|Aut(Z_3^n)| = \prod_{i=0}^{i=n-1} (3^n - 3^i)$$

For $G_3 = Z_3 \times Z_9$, $Aut(G)$ is readily seen to be the group of all 2×2 matrices of form:

$$\begin{pmatrix} a & c \\ 3b & d \end{pmatrix}$$

where $a, b, c \in \{0, 1, 2\}$, and $d \in \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$, and the determinant is non-zero modulo 3. The order of this group is 108.

Consider first the Bose design on G_1. By Theorem 3.2.1, the automorphism group of this design is standard, since the group has an element of order 27. The order of the automorphism group of the design is then

$$3|Z_{27}||Aut(Z_{27})| = 3 \cdot 27 \cdot 18 = 1458.$$

The design on G_2 has an non-standard automorphism group of order

$$3^7|Aut(G_2)| = 3^7(3^3 - 1)(3^3 - 3)(3^3 - 9) = 2187 \cdot 26 \cdot 24 \cdot 18 = 24,564,384.$$

The design on G_3 also has an non-standard automorphism group of order

$$3^6|Aut(G_3)| = 3^6 \cdot 108 = 78,732.$$

Finally, the design on G_4, being the affine geometry $AG(4, 3)$, has by Theorem 3.2.4 the automorphism group $Hol(G_4)$, which has order

$$|G_4| \cdot |Aut(G_4)| = 3^4 \cdot (3^4 - 1) \cdot (3^4 - 3) \cdot (3^4 - 3^2) \cdot (3^4 - 3^3) = 1,965,150,720.$$

Chapter 4

Tripling construction

4.1 Introduction

In Chapter 3, we introduced the following STS tripling construction which starts with an STS $S = (W, \mathcal{C})$ of order v, and produces the STS $T = (U, \mathcal{A})$ on the $3v$ points $\{(x, i) : x \in W, i \in Z_3\}$ with block set:

$$\mathcal{A} = \{ \{(x,i),(y,i+j),(z,i+2j)\} : \{x,y,z\} \in \mathcal{C} : i,j \in Z_3\} \cup$$

$$\{ \{(x,0),(x,1),(x,2)\} : x \in U\}.$$

The object of this chapter is to discover as much as possible about the automorphisms of STS formed with this construction.

First of all we shall define some terminology. In common with Chapter 2, we shall call the Z_3 component of any point of T the *label*. We now give names to the various types of block. If x is a point of S, then a block of the form $\{(x,0),(x,1),(x,2)\}$ is called a *vertical block*. If $\{x,y,z\}$ is a block of S, then a

block of T of the form $\{(x,i),(y,i),(z,i)\}$ is called a *horizontal block*, and a block of the form $\{(x,i),(y,j),(z,k)\}$, where i,j,k are all different is called a *diagonal block*. We shall refer to the STS T as the *tripling* of S if it obtained from the STS S by the tripling construction.

Theorem 4.1.1. *Let S be any Steiner triple system with automorphism group Aut(S), and T be the STS obtained by tripling S. Then T has an automorphism group isomorphic to $Aut(S) \times S_3$ (where S_3 stands as usual for the symmetric group on 3 points).*

Proof. Let ψ be any automorphism of S, σ any permutation of $\{0,1,2\}$, $x \in W$, $\{x,y,z\} \in \mathcal{C}$, and $i \in Z_3$. The map $(\psi,\sigma) : W \times Z_3 \to W \times Z_3$ is one-one on points of T because ψ and σ are one-one, and therefore (ψ,σ) is one-one on blocks. To complete the proof that (ψ,σ) is an automorphism of T, we have to show that the image of any block under (ψ,σ) is also a block. Taking each type of block in turn:

a) Vertical blocks:

$$(\psi,\sigma) : \{(x,0),\ (x,1),\ (x,2)\} \to \{(\psi(x),\sigma(0)),\ (\psi(x),\sigma(1)),\ (\psi(x),\sigma(2))\},$$

which is again a vertical block of T.

b) Horizontal blocks:

$$(\psi,\sigma) : \{(x,i),\ (y,i),\ (z,i)\} \to \{(\psi(x),\sigma(i)),\ (\psi(y),\sigma(i)),\ (\psi(z),\sigma(i))\},$$

which is again a horizontal block of T.

c) Diagonal blocks:

$$(\psi, \sigma) : \{(x, 0),\ (y, 1),\ (z, 2)\} \to \{(\psi(x), \sigma(0)),\ (\psi(y), \sigma(1)),\ (\psi(z), \sigma(2))\},$$

which is again a diagonal block of T.

□

Note that for any given automorphism in the last theorem the label of each point of U is permuted in the same way as every other point. We shall call automorphisms of T of this form *standard* automorphisms, in analogy with automorphisms of the same name in Chapter 2. Note that this is an extension of the previous usage, because in that case, only even vertical automorphisms were included. Of more interest is for what STS S this is not the full automorphism group of the tripled system T.

4.2 The full automorphism group

We shall consider 3×3 matrices of points:

$$\begin{array}{ccc} (a, i_0) & (b, j_0) & (c, k_0) \\ (d, i_1) & (e, j_1) & (f, k_1) \\ (r, i_2) & (s, j_2) & (t, k_2), \end{array}$$

where all columns, rows, and diagonals are distinct blocks of T, twelve in all. We shall call this a *complete matrix of blocks*. If $\{a, b, c\}$ is a block of S, then

$$\begin{array}{lll} (a,0) & (a,1) & (a,2) \\ (b,0) & (b,1) & (b,2) \\ (c,0) & (c,1) & (c,2) \end{array}$$

is a prime example of this. We shall repeatedly make use of the fact that the image of any complete matrix of blocks of T under an automorphism of T is again a complete matrix of blocks.

Lemma 4.2.1. *The rows (resp. columns) of a complete matrix of blocks of T are either all vertical blocks, or all horizontal blocks, or all diagonal blocks.*

Proof. We need only deal with rows. The argument for columns is identical. Firstly, suppose the first row is a vertical block $\{(u,0),(u,1),(u,2)\}$ in some order. Then we have:

$$\begin{array}{lll} (u,i) & (u,j) & (u,k) \\ \bullet & (y,m) & \bullet \\ (x,n) & \bullet & (z,p), \end{array}$$

for some points $x, y, z \in W$, $m, n, p \in Z_3$. Then $\{(u,i),(y,m),(z,p)\}$ and $\{(u,k),(y,m),(x,n)\}$ are blocks of T which are derived from blocks $\{u,y,z\}$ and $\{u,y,x\}$ of S. Since any pair of points of W occurs in exactly one block of S, we deduce that $x = z$. Moreover, the bottom line of the matrix must be a vertical block of T, since only vertical blocks of T contain repeated points of S. A similar argument shows that the middle row is also a vertical block.

Next let the first row of this complete matrix of blocks be a horizontal block $\{(u,i)\ (v,i)\ (w,i)\}$ for some $i \in Z_3$. Again represent the middle element by

(y, m). Then the full matrix must be of form:

$$\begin{array}{lll} (u,i) & (v,i) & (w,i) \\ (x,m) & (y,m) & (z,m) \\ (r, 2i+2m) & (s, 2i+2m) & (t, 2i+2m), \end{array}$$

for some $x, z, r, s, t \in W$, because the labels must sum to zero modulo 3 in each row, column and diagonal. Thus each row is a horizontal block, because all the labels are the same.

Finally if the first row of this complete matrix of blocks is a diagonal block, then all are diagonal blocks, since by the previous arguments, if one row is a vertical (resp. horizontal) block then all are vertical (resp. horizontal) blocks. □

An automorphism of T maps all vertical blocks to either all vertical blocks, all horizontal blocks, or all diagonal blocks. This is because, for any pair of distinct vertical blocks $\{(a,0),\ (a,1),\ (a,2)\}$ and $\{(b,0),\ (b,1),\ (b,2)\}$, if c is the unique point of W such that $\{a, b, c\}$ is a block of S, then

$$\begin{array}{lll} (a,0), & (a,1), & (a,2) \\ (b,\check{0}), & (b,1), & (b,2) \\ (c,0), & (c,1), & (c,2) \end{array}$$

is a complete matrix of blocks. Since the image of this matrix is also a complete matrix of blocks, the blocks forming the rows of the image are all of the same type by Lemma 4.2.1. Since the first two vertical blocks were chosen arbitrarily, the automorphism maps all vertical blocks either all to vertical blocks, or all to horizontal blocks, or all to diagonal blocks.

We shall name automorphisms that map vertical blocks to vertical blocks

vertical automorphisms, automorphisms that map vertical blocks to horizontal blocks *horizontal automorphisms*, and automorphisms that map vertical blocks to diagonal blocks *diagonal automorphisms*. Also, we shall collectively call the latter two *non-vertical* automorphisms.

The standard automorphisms that we met in the last section are a particular type of vertical automorphism: those for which the permutation of the labels is the same for every block. We shall call any vertical automorphism that is not standard *non-standard*. The next question we shall tackle is whether non-standard automorphisms of T exist. First of all we need the following lemma:

Lemma 4.2.2. *If the rows of a complete matrix of blocks of T are all vertical blocks, then the labels of the points in each row are either all even permutations of $\{0,1,2\}$, or all odd permutations of the same. Moreover, either the labels of all rows are the same permutation, or the permutations are all different.*

Proof. We need only be concerned with the labels of each point. Suppose the labels of the first row are the even permutation $i\ i+1\ i+2$ of $\{0,1,2\}$, and the second row the odd permutation $j\ j+2\ j+1$. Then since each column is a block, the labels of each column must sum to zero modulo 3, the complete matrix of labels must be:

$$\begin{array}{lll} i & i+1 & i+2 \\ j & j+2 & j+1 \\ 2i+2j & 2i+2j & 2i+2j. \end{array}$$

But the labels of the third row are not the labels of a vertical block, so this cannot occur. Therefore the permutations of the rows must be of the same type,

i.e either:

$$\begin{array}{lll} i & i+1 & i+2 \\ j & j+1 & j+2 \\ 2i+2j & 2i+2j+1 & 2i+2j+2, \end{array}$$

or

$$\begin{array}{lll} i & i+2 & i+1 \\ j & j+2 & j+1 \\ 2i+2j & 2i+2j+2 & 2i+2j+1. \end{array}$$

If $i = j$, then all the row permutations are the same in both cases, otherwise they are all different. □

Suppose ϕ is a vertical automorphism of T. Then by Lemma 4.2.2, for any block $\{a, b, c\}$ of S, ϕ maps the complete matrix of blocks:

$$\begin{array}{lll} (a,0) & (a,1) & (a,2) \\ (b,0) & (b,1) & (b,2) \\ (c,0) & (c,1) & (c,2) \end{array}$$

to another complete matrix of blocks, either:

$$\begin{array}{lll} (u,i) & (u,i+1) & (u,i+2) \\ (v,j) & (v,j+1) & (v,j+2) \\ (w,2i+2j) & (w,2i+2j+1) & (w,2i+2j+2), \end{array}$$

or

$$\begin{array}{lll} (u,i) & (u,i+2) & (u,i+1) \\ (v,j) & (v,j+2) & (v,j+1) \\ (w,2i+2j) & (w,2i+2j+2) & (w,2i+2j+1), \end{array}$$

for some block $\{u, v, w\}$ of S, and $i, j \in Z_3$. The first form occurs where the labels of the vertical blocks are always permuted evenly, and the second where they are permuted oddly.

If $i = j$ for every pair a, b, then ϕ is a standard automorphism.

We can represent any vertical automorphism of T, ϕ as a pair of maps (ψ, τ); $\psi : W \to W$, $\tau : W \times Z_3 \to Z_3$ with some properties yet to be discovered. From the three diagrams above we see that we can represent τ as $\tau = \sigma + \kappa$, where σ is a fixed permutation of $\{0, 1, 2\}$, and $\kappa : W \to Z_3$. If ϕ is standard, then κ is constant on all of W. Furthermore, even if κ is not constant on W, from these diagrams we also deduce:

Lemma 4.2.3. *If T has a non-standard vertical automorphism, then there exists a non-constant map $\kappa : W \to Z_3$ such that for $\{a, b, c\}$ any block of S, $\kappa(a) + \kappa(b) + \kappa(c) = 0$.*

This relation allows us to show that if T has non-standard vertical automorphisms, then S can itself be constructed from subsystems, in the same way as in Theorem 3.1.1 we showed that the Bose design constructed from a Steiner triple system has non-standard automorphisms only if the STS is itself constructable from three subsystems that have equal orders, but are not necessarily isomorphic. It is in fact the same construction. We shall prove:

Theorem 4.2.1. *Let $S = (W, \mathcal{C})$ be a Steiner triple system of order v, and let $T = (U, \mathcal{A})$ be the Steiner triple system of order $3v$ that is obtained from S by the tripling construction. Then T has a non-standard vertical automorphism if and only there exist disjoint subsets X_i; $i = 0, 1, 2$ of W with $W = X_0 \cup X_1 \cup X_2$, and $|X_0| = |X_1| = |X_2|$, such that each X_i forms a subsystem of S, and a Latin square L, with rows, columns and entries indexed by X_0, X_1, and X_2 respectively. The*

blocks of S consist of: a) the blocks of each X_i, and b) the triples $\{x_0, x_1, x_2\}$, with $x_i \in X_i$; $i = 0, 1, 2$ such that $x_2 = L(x_0, x_1)$.

Proof. We shall prove the necessity first. If T has a non-standard vertical automorphism then according to Lemma 4.2.3, there exists a function $\kappa : W \to Z_3$ such that, for $\{a, b, c\}$ any block of S, $\kappa(a) + \kappa(b) + \kappa(c) = 0$ and κ is not constant on W. We choose the elements of X_i to be the elements a of W such that $\kappa(a) = i$. The X_i are all non-empty because κ is not constant on W.

The X_i are of equal size. To show this, choose any point $x_0 \in X_0$, and let x_1 run through all points of X_1. For each such pair x_0, x_1 there is a unique block $\{x_0\ x_1\ x_2\}$ of S, with $x_2 \in X_2$ because of the condition satisfied by κ. So $|X_1| \leq |X_2|$, and interchanging X_1 and X_2 yields $|X_2| \leq |X_1|$. So $|X_1| = |X_2|$, and similarly we deduce $|X_0| = |X_1|$ also.

The points of each X_i form a subsystem of S because, if $x, y \in X_i$, then if $z \in W$ is the unique point such that $\{x,\ y,\ z\}$ is a block of S, then since $\kappa(x) = \kappa(y) = i$, and since $\kappa(x) + \kappa(y) + \kappa(z) = 0 \pmod 3$, we have $\kappa(z) = i$ also, so $z \in X_i$ also.

The blocks $\{x_0, x_1, x_2\}$ of S with $x_i \in X_i$, $i = 0, 1, 2$ define a Latin square, because for each $x_0 \in X_0$ and $x_2 \in X_2$, there is exactly one block $\{x_0, x_1, x_2\}$, with $x_1 \in X_1$, so each $x_2 \in X_2$ occurs exactly once in each row, and similarly each $x_2 \in X_2$ occurs exactly once in each column.

This concludes the necessity argument. To show sufficiency, if S is any Steiner triple system constructed in this way, then we define the function κ by $\kappa(a) = i$ if $a \in X_i$, and the automorphism ϕ as $\phi(a, j) = (a, j + \kappa(a))$. The automorphism ϕ of T is a non-standard vertical automorphism of T because κ is not constant on W. □

Next, we examine the conditions necessary for T to have horizontal automorphisms. We shall prove:

Theorem 4.2.2. *Let $S = (W, \mathcal{C})$ be a Steiner triple system of order v, and let $T = (U, \mathcal{A})$ be the Steiner triple system of order $3v$ that is obtained from S by the tripling construction. If T has horizontal automorphisms, then S is itself obtained from a Steiner triple system by the tripling construction.*

Proof. Suppose ϕ is a horizontal automorphism of T. Let the sets X_i; $i = 0, 1, 2$ be defined as $a \in X_i$ if the vertical block on a maps to a block with labels i.

Suppose first that X_0 is not empty, and $a \in X_0$, and let $\phi : \{(a,0)\ (a,1)\ (a,2)\} \rightarrow \{(x,0)\ (y,0)\ (z,0)\}$. We extend this mapping to construct the following diagram:

$$\begin{array}{lll} (a,0) & (a,1) & (a,2) \\ (a',j) & (a',j+1) & (a',j+2) \\ (a'',2j) & (a'',2j+1) & (a'',2j+2) \end{array} \xrightarrow{\phi} \begin{array}{lll} (x,0) & (y,0) & (z,0) \\ (x,1) & (y,1) & (z,1) \\ (x,2) & (y,2) & (z,2), \end{array}$$

for some $a', a'' \in W$ with $\{a, a', a''\} \in C$ and $j \in Z_3$ by adding extra rows on the right-hand side to make three columns, each of which is a vertical block, then applying the inverse of ϕ to produce second and third rows on the left also. Observe that the right-hand side is a complete matrix of blocks, so the left-hand side matrix is therefore one also, and that all of its rows are vertical because the first was chosen to be, and so the other rows are vertical by Lemma 4.2.1.

This diagram establishes one-one mappings between the X_i since to every $a \in X_0$ it associates a unique $a' \in X_1$ and $a'' \in X_2$ (unique because ϕ is one-one). We denote the mapping from X_0 to X_1 by ξ_1, and the mapping from X_0 to X_2 by ξ_2. We clearly could have started with a in any other X_i and achieved the same

result.

The X_i are therefore all of size $v/3$. We assert that the X_i are isomorphic subsystems of S, and that S is isomorphic to the tripling construction on X_0.

To prove that the X_i are subsystems of S, we show that if $a,\ b \in X_i$, and if $\{a, b, c\}$ is the unique block of S containing a, b, then $c \in X_i$ also. Suppose $c \in X_j$. The diagram:

$$\begin{array}{ccccc} (a,0) & (a,1) & (a,2) & & (x,i) & (y,i) & (z,i) \\ (b,0) & (b,1) & (b,2) & \xrightarrow{\phi} & (u,i) & (v,i) & (w,i) \\ (c,0) & (c,1) & (c,2) & & (r,j) & (s,j) & (t,j), \end{array}$$

is constructed as usual by taking the images of the vertical blocks on a, b, and c under ϕ, which are horizontal blocks for some $x, y, z, u, v, w, r, s, t \in W$. Since the left hand side is a complete matrix of blocks, so is the right hand side. Since the columns of the right-hand side are blocks, the labels of each column must sum to zero modulo 3. Therefore $j = i$, and $c \in X_i$ also.

To show that S is isomorphic to the STS obtained by applying the tripling construction to the subsystem on X_0, we have to show that the subsystems on X_1 and X_2 are isomorphic to that on X_0, and that for any block $\{a, b, c\}$ of X_0, the triples:

$$\begin{array}{lll} \{a, b, c\} & \{\xi_1(a), \xi_1(b), \xi_1(c)\} & \{\xi_2(a), \xi_2(b), \xi_2(c)\} \\ \{a, \xi_1(b), \xi_2(c)\} & \{\xi_2(a), b, \xi_1(c)\} & \{\xi_1(a), \xi_2(b), c\} \\ \{a, \xi_2(b), \xi_1(c)\} & \{\xi_1(a), b, \xi_2(c)\} & \{\xi_2(a), \xi_1(b), c\} \end{array}$$

are all blocks of S. This will be proved if we can show that

$$\begin{array}{ccc} a & b & c \\ \xi_1(a) & \xi_1(b) & \xi_1(c) \\ \xi_2(a) & \xi_2(b) & \xi_2(c) \end{array}$$

is a complete matrix of blocks, because firstly it would show that the subsystems on the X_i are isomorphic because it implies that if $\{a, b, c\}$ is a block of the subsystem on X_0, then $\{\xi_1(a), \xi_1(b), \xi_1(c)\}$ and $\{\xi_2(a), \xi_2(b), \xi_2(c)\}$ are blocks of the subsystems on X_1 and X_2 respectively. Secondly, each triple we require to be a block of S is either a row, column, or diagonal of this matrix. In order to show this, if $\{a, b, c\}$ is a block of the subsystem of S on X_0, we have a mapping of the form

$$(a,0) \quad (b,0) \quad (c,0) \quad \xrightarrow{\phi} \quad (u,0) \quad (v,0) \quad (w,0)$$

for some $u, v, w \in W$. We can extend each column on the right-hand side and map back using the inverse of ϕ to give:

$$\begin{array}{ccccc} (a,0) & (b,0) & (c,0) & & (u,0) \quad (v,0) \quad (w,0) \\ (\xi_1(a),j) & (\xi_1(b),j) & (\xi_1(c),j) & \xrightarrow{\phi} & (u,1) \quad (v,1) \quad (w,1) \\ (\xi_2(a),2j) & (\xi_2(b),2j) & (\xi_2(c),2j) & & (u,2) \quad (v,2) \quad (w,2), \end{array}$$

for some $j \in Z_3$. The left hand side is again a complete matrix of blocks because the matrix on the right is one. In particular, each column, row and diagonal on the left-hand side is a block of T. Since a, b, c are distinct, the points of S given by the S-components of the points on the left-hand side are distinct and form a complete matrix of blocks as required, because the S-components of any block of T are either a single point or a block of S. Thus S is isomorphic

to the STS obtained by applying the tripling construction to the subsystem on X_0. □

Results for the case where T has diagonal automorphisms are not so neat. Suppose $\phi : \{(a,0)\ (a,1)\ (a,2)\} \to \{(x,i)\ (y,i+j)\ (z,i+2j)\}$ for some block $\{x,y,z\}$ of S and $i,j \in Z_3$, $j \neq 0$ (the case $j = 0$ corresponds to a horizontal automorphism). By extending each column on the right-hand side to a vertical block and mapping back via the inverse of ϕ, we obtain a diagram of the form

$$\begin{array}{ccc} (a,0) & (a,1) & (a,2) \\ (a',k) & (a',k+1) & (a',k+2) \\ (a'',2k) & (a'',2k+1) & (a'',2k+2) \end{array} \xrightarrow{\phi} \begin{array}{ccc} (x,i) & (y,i+j) & (z,i+2j) \\ (x,i+1) & (y,1+i+j) & (z,1+i+2j) \\ (x,i+2) & (y,2+i+j) & (z,2+i+2j), \end{array}$$

for some $a', a'' \in W$, where $\{a, a', a''\}$ is also a block of S, and $k \in Z_3$. We can reduce the number of cases to consider by composing ϕ with simple permutations of the labels. Firstly, we eliminate i by adding $2i$ to all labels in the image of ϕ. Secondly, we can use pre-composition with an automorphism that exchanges the labels 1 and 2 and permutation of columns on both sides to reduce the cases to be considered to $j = 1, k = 0$, $j = 2, k = 0$, $j = 1, k = 1$, and $j = 2, k = 1$, i.e.

$$\begin{array}{ccc} (a,0) & (a,1) & (a,2) \\ (a',0) & (a',1) & (a',2) \\ (a'',0) & (a'',1) & (a'',2) \end{array} \xrightarrow{\phi} \begin{array}{ccc} (x,0) & (y,1) & (z,2) \\ (x,1) & (y,2) & (z,0) \\ (x,2) & (y,0) & (z,1), \end{array}$$

and

$$\begin{array}{ccc} (a,0) & (a,1) & (a,2) \\ (a',1) & (a',2) & (a',0) \\ (a'',2) & (a'',0) & (a'',1) \end{array} \xrightarrow{\phi} \begin{array}{ccc} (x,0) & (y,1) & (z,2) \\ (x,1) & (y,2) & (z,0) \\ (x,2) & (y,0) & (z,1). \end{array}$$

In the cases where $k = 0$, the inverse of ϕ is observed to be a horizontal automorphism, and so by Theorem 4.2.2, S is itself isomorphic to a tripled STS. We shall not be concerned any further with these cases.

In the other cases, for S to be isomorphic to a tripled STS, we need a non-constant map κ from the points of S to Z_3 such that for any block $\{a, b, c\}$ of S, $\kappa(a) + \kappa(b) + \kappa(c) = 0$. However, no such natural mapping is apparent, and so we cannot assert that S is isomorphic to a tripled STS. On the other hand, if we take any STS $(\mathcal{B}, V)$ and apply the tripling construction twice, it is apparent that this does have diagonal automorphisms. If $a \in V$, $i, j \in Z_3$, then the mapping $(a, i, j) \mapsto (a, i - j, j)$ is a diagonal automorphism. This can be seen from the diagram

$$\begin{array}{ccc} (a,0,0) & (a,0,1) & (a,0,2) \\ (a,1,1) & (a,1,2) & (a,1,0) \\ (a,2,2) & (a,2,0) & (a,2,1) \end{array} \xrightarrow{\phi} \begin{array}{ccc} (a,0,0) & (a,2,1) & (a,1,2) \\ (a,0,1) & (a,2,2) & (a,1,0) \\ (a,0,2) & (a,2,0) & (a,1,1). \end{array}$$

However, returning to the general case, we can observe that the diagram

$$\begin{array}{ccc} (a,0) & (a,1) & (a,2) \\ (a',1) & (a',2) & (a',0) \\ (a'',2) & (a'',0) & (a'',1) \end{array} \xrightarrow{\phi} \begin{array}{ccc} (x,0) & (y,1) & (z,2) \\ (x,1) & (y,2) & (z,0) \\ (x,2) & (y,0) & (z,1). \end{array}$$

defines a parallel class of S, because, starting with any $a \in W$, we can obtain a unique block $\{a, a', a''\}$ by using the diagram. We then expand the partial parallel class by the same method using at each stage any point not yet included in the class, until all the points are used up. The blocks obtained are pairwise disjoint because otherwise any two non-disjoint blocks would correspond to the

same vertical blocks on the right-hand side of the diagram. Therefore, $|W| \equiv 3 \pmod 6$.

Furthermore, the automorphism defines a natural Steiner triple system having as its points the blocks of the parallel class. If $a, b \in W$ are in different blocks of the parallel class, and $\phi(a,0) = (u,0)$, $\phi(b,0) = (v,0)$, then the blocks of the parallel class containing a and b respectively are $\{a, a', a''\}$ and $\{b, b', b''\}$ where a', a'' are defined by $(a',1) = \phi^{-1}(u,1)$, $(a'',2) = \phi^{-1}(u,2)$, and b', b'' are defined by $(b',1) = \phi^{-1}(v,1)$, $(b',2) = \phi^{-1}(v,2)$. If $w \in W$ is the unique point such that $\{u, v, w\}$ is a block of S, then we define a third block of the parallel class by $\{c, c', c''\}$, where $(c,0) = \phi^{-1}(w,0)$, $(c',0) = \phi^{-1}(w,1)$ and $(c'',0) = \phi^{-1}(w,2)$. Thus every pair of distinct blocks of the parallel class occurs in a unique triple of blocks defined in this way. In particular, $\frac{|W|}{3} \equiv 1$ or $3 \pmod 6$, i.e. $|W| \equiv 3$ or $9 \pmod{18}$. Since the right-hand side of the diagram

$$\begin{array}{ccc} (a,0) & (b,0) & (c,0) \\ (a',1) & (b',1) & (c',1) \\ (a'',2) & (b'',2) & (c'',2) \end{array} \quad \stackrel{\phi}{\rightarrow} \quad \begin{array}{ccc} (u,0) & (v,0) & (w,0) \\ (u,1) & (v,1) & (w,1) \\ (u,2) & (v,2) & (w,2). \end{array}$$

is a complete matrix of blocks then so is the left-hand side also, and so the array

$$\begin{array}{ccc} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{array}$$

of points of S is also a complete matrix of blocks.

This analysis enables us to state the final result.

Corollary 4.2.1. *If the Steiner triple system T is constructed from the Steiner*

triple system S by the tripling construction, and if S is of order 1, 7, 13, or 15 (mod 18), then all automorphisms of T are standard, and $Aut(T) \equiv Aut(S) \times S_3$.

Proof. If S has order not equal to 3 or 9 (mod 18), then by Theorems 4.2.1 and 4.2.2 and the above reasoning, T can have neither non-standard vertical, nor horizontal, nor diagonal automorphisms, and its automorphisms are all standard. □

Finally, we provide an example of an STS S which itself is not obtained by tripling, but whose tripling T does possess a diagonal automorphism. Let $(\mathcal{B}, V)$ be any STS, and choose $\{x, y, z\} \in \mathcal{B}$. We define S by modifying the STS obtained from the tripling of $(\mathcal{B}, V)$, replacing the complete matrix of blocks

$$\begin{matrix} (x,0) & (y,0) & (z,0) \\ (x,1) & (y,1) & (z,1) \\ (x,2) & (y,2) & (z,2) \end{matrix}$$

by the matrix

$$\begin{matrix} (x,2) & (y,0) & (z,0) \\ (x,0) & (y,1) & (z,1) \\ (x,1) & (y,2) & (z,2), \end{matrix}$$

i.e. $\{(x, i-1), (y, i+k), (z, i+2k)\}$, $i, k \in Z_3$ plus the vertical blocks. We define the mapping ϕ on T, the tripling of S, by $(x, i, j) \to (x, i-j, j)$, for $x \in V$, $i, j \in Z_3$. We show this is an automorphism of T. For any $u \in V$,

$$\begin{matrix} (u,0,0) & (u,0,1) & (u,0,2) \\ (u,1,0) & (u,1,1) & (u,1,2) \\ (u,2,0) & (u,2,1) & (u,2,2) \end{matrix} \xrightarrow{\phi} \begin{matrix} (u,0,0) & (u,2,1) & (u,1,2) \\ (u,1,0) & (u,0,1) & (u,2,2) \\ (u,2,0) & (u,1,1) & (u,0,2). \end{matrix}$$

For any block $\{u, v, w\} \neq \{x, y, z\} \in \mathcal{B}$,

$$\begin{array}{ccc} (u,0,0) & (v,0,1) & (w,0,2) \\ (u,1,0) & (v,1,1) & (w,1,2) \\ (u,2,0) & (v,2,1) & (w,2,2) \end{array} \xrightarrow{\phi} \begin{array}{ccc} (u,0,0) & (v,2,1) & (w,1,2) \\ (u,1,0) & (v,0,1) & (w,2,2) \\ (u,2,0) & (v,1,1) & (w,0,2) \end{array}$$

for each $j \in Z_3$. For the block $\{x, y, z\}$, for each $i, j, k \in Z_3$,

$$\begin{array}{ccc} (x,2,0) & (y,0,1) & (z,0,2) \\ (x,0,0) & (y,1,1) & (z,1,2) \\ (x,1,0) & (y,2,1) & (z,2,2) \end{array} \xrightarrow{\phi} \begin{array}{ccc} (x,2,0) & (y,2,1) & (z,1,2) \\ (x,0,0) & (y,0,1) & (z,2,2) \\ (x,1,0) & (y,1,1) & (z,0,2). \end{array}$$

In each case, inspection shows that on both sides, each row, column, and diagonal is a block of T. The mapping ϕ therefore preserves blocks, and since it is one-to-one, it is an automorphism of T. Moreover, the first diagram shows that ϕ is a diagonal automorphism of T when it is viewed as the tripling of S.

Chapter 5

4-cycle and even-cycle systems

5.1 Introduction

An m-cycle system of order n is a decomposition of the complete graph on n vertices, K_n, into cycles of length m. The order n is *admissible* if n is odd and $\frac{1}{2}n(n-1)$ is divisible by m. Existence has been proved for ([7], page 266):

i) all admissible n for $m \leq 50$,

i) all admissible n for m a prime power,

iii) all $n \equiv 1 \pmod{2m}$ for all m,

iv) $n \equiv m \pmod{2m}$ for all odd m.

In this chapter we shall be almost exclusively interested in cycles of even length $2k$. We shall denote such a system by $2k\text{CS}(n)$, or sometimes simply $2k\text{CS}$.

For $2k$-cycle systems there is an elegant construction, given $2k$-cycle systems of order $4kr+1$ and $4kr'+1$ respectively, for constructing a system of order $4k(r+r')+1$. We identify one point in each system to be a common point, and

take as the cycles of the enlarged system the cycles of the original systems together with the cycles of any decomposition of the complete bipartite graph $K_{4kr,4kr'}$ into $2k$-cycles. We shall use this construction several times in this chapter.

5.2 4-cycle systems with given automorphism group

In 1978, E. Mendelsohn [16] proved that for any finite abstract group Γ there exists a Steiner triple system with full automorphism group isomorphic to Γ. If $|\Gamma| = \gamma$ and a minimal generator set of Γ has size ν, then the order of the STS in Mendelsohn's construction is at least $2^{2\gamma\nu}$. In this chapter, it is proved that for any given abstract group, Γ, there exists a 4-cycle system whose full automorphism group is Γ, and moreover our construction yields a 4CS of sub-exponential order. The result extends immediately to $2k$-cycle systems if some existence criteria are met. We shall prove in the final sections that these existence criteria are indeed met, and thus that the corresponding result for $2k$-cycle systems is true.

Following Mendelsohn, we shall use the result [9] of Frucht that for any given abstract group Γ there exists a ğraph whose full automorphism group is Γ.

We first give the construction. Recall that the necessary and sufficient conditions for the existence of a 4-cycle system of order v is that $v \equiv 1 \pmod 8$. For the construction we shall need the following building blocks:

a) an automorphism-free 4-CS(9) on the points $\{\infty\} \cup \{1, 2, \ldots, 8\}$, which we shall call T.

b) two different symmetric decompositions of $K_{8,8}$. The chosen decompositions must be symmetric in the sense that if the 4-cycle $ab'cd'$ is in the decompo-

sition, where the unprimed letters are vertices of one part and the primed letters are vertices of the other part, then the 4-cycle $a'bc'd$ is also in the decomposition. Such decompositions obviously exist, e.g. for the first we could choose:

$$(a,a',b,b')\ (a,c',b,d')\ (a,e',b,f')\ (a,g',b,h')$$
$$(c,a',d,b')\ (c,c',d,d')\ (c,e',d,f')\ (c,g',d,h')$$
$$(e,a',f,b')\ (e,c',f,d')\ (e,e',f,f')\ (e,g',f,h')$$
$$(g,a',h,b')\ (g,c',h,d')\ (g,e',h,f')\ (g,g',h,h').$$

We require the two decompositions to be different only in the sense that there is a pair of edges that belong to the same cycle in one decomposition but not in the other, e.g. exchanging b with c and b' with c' is sufficient. We shall call one decomposition the *edge* decomposition, and the other the *non-edge* decomposition.

Construction 1

Take any graph $G = (V, E)$ for which $Aut(G) = \Gamma$. We construct a 4-cycle system $S(G)$ of order $8|V| + 1$ on the set $\{\infty\} \cup \{(v,i), v \in V, i \in \{1,2,\ldots,8\}\}$. We can consider the edges of the complete graph on this set as all the edges in the complete graphs on $\{\infty\} \cup \{(v,i), i \in \{1,2,\ldots,8\}\}$ for $v \in V$, and all the edges of the complete bipartite graphs on the parts $\{(u,i), i \in \{1,2,\ldots,8\}\}$ and $\{(v,i), i \in \{1,2,\ldots,8\}\}$ for all distinct $u, v \in V$.

For each $v \in V$, decompose the complete graph on $\{\infty\} \cup \{(v,i), i \in \{1,2,\ldots,8\}\}$ with a copy of T. For each distinct $u, v \in V$, if $(u,v) \in E$, decompose the complete bipartite graph on $\{(u,i), i \in \{1,2,\ldots,8\}\} \cup \{(v,i), i \in \{1,2,\ldots,8\}\}$, with a copy of the edge decomposition. Since the decompositions are symmetric, it does not matter which way the parts are allocated. If $(u,v) \notin E$, use the non-edge

decomposition instead. Every edge is therefore in a unique 4-cycle, and $S(G)$ is a 4CS$(8|V|+1)$.

In order to complete the construction, we have to show that automorphism-free 4CS(9)s exist.

Lemma 5.2.1. *If the intersection of two subsystems of a 4CS has size greater than one, then it is also a subsystem.*

Proof. If a and b are points in the intersection, then the unique cycle (a, b, c, d) containing the edge (a, b), must be a cycle of both subsystems. Therefore the points of the intersection form a 4-cycle system. □

Lemma 5.2.2. *If the set of fixed points of any automorphism of a 4CS has size greater than one, then it forms a subsystem.*

Proof. If a and b are fixed points then the unique cycle containing the edge (a, b) is fixed, so the other points in this cycle are also fixed. Thus the complete graph on the fixed points is decomposed into 4-cycles. □

Lemma 5.2.3. *If an automorphism of a 4CS(9) fixes more than one point, then it is the identity.*

Proof. By the previous Lemma, the set of fixed points is either a subsystem or of order one. However a 4CS(9) has no proper subsystems, since otherwise, if the subsystem has order n, then n is odd, $n(n-1) \equiv 0 \pmod 8$, and $n < 9$, for which the only solution is $n = 1$. □

Lemma 5.2.4. *The 4CS(9) on the points $\{\infty, a, b, c, d, e, f, g, h\}$ with the following cycles:*

$$(\infty, a, g, b), (\infty, c, a, d), (\infty, e, b, f), (\infty, g, e, h), (a, b, c, f),$$

$$(f, h, a, e), (g, h, b, d), (c, d, f, g), (c, e, d, h)$$

is automorphism-free.

Proof. Assume that there is a non-trivial automorphism. Then by Lemma 5.2.3, it has no more than one fixed point. We note the cycles:

$$(c, e, d, h), (\infty, c, a, d), (f, h, a, e),$$

which we shall denote by A, B, C respectively. These cycles are the only ones in this 4CS(9) where any alternate pairs of points, namely c, d and e, h are repeated. Consequently any non-trivial automorphism must either swap c with d and e with h or swap c, d with e, h. Thus the cycle A is fixed and either B and C are fixed or they are swapped. If B and C are fixed, then the automorphism must exchange e with h, c with d, ∞ with a and a with f. However, the last two exchanges are inconsistent, and so the automorphism is trivial.

If B and C are exchanged, then a is fixed and ∞ and f are also exchanged. Considering also the cycles (c, d, f, g) and (∞, g, e, h) we see that g is also fixed, and so the automorphism is again trivial. □

Before the giving the main theorem, we first define some terminology for the above construction. We shall call the 4CS on the inflated vertices the *vertex subsystems.* A cycle (i.e. 4-cycle) of a $K_{8,8}$ representing an edge (resp. non-edge) of G shall be called an *edge* (resp. *non-edge*) *cycle.*

Theorem 5.2.1. *The 4-cycle system S obtained from an abstract group Γ by Construction 1 has full automorphism group Γ. Moreover, if $|\Gamma| = \gamma$, then S has no more than $16\gamma log_2\gamma + 1$ vertices if Γ is non-cyclic and $24\gamma + 1$ vertices otherwise.*

Proof. Firstly we show that the only 4CS(9) subsystems of S are the vertex subsystems. Every point of S except the infinity point is in exactly one vertex subsystem, and the infinity point is in all vertex subsystems. Suppose S contains a 4CS(9), P, that is not a vertex subsystem. Then P intersects more than one vertex subsystem. It cannot intersect any vertex subsystem in more than one point, since otherwise by Lemma 5.2.1, it would be the whole vertex subsystem because a 4CS(9) has no proper subsystems. Therefore any two points of P must be in difference vertex subsystems. Therefore any edge of P is either in an edge cycle or a non-edge cycle. However every edge cycle and every non-edge cycle contains two points of the same vertex subsystem, contradicting our previous assumption. Therefore the only 4CS(9) subsystems of S are vertex subsystems.

This implies that any automorphism of S maps one vertex subsystem onto another. Moreover for any automorphism ϕ of S, if the image of the point (v,i) is (u,j), $u,v \in V$, $\{i,j \in \{1,2,\ldots,8\}\}$, then $i=j$ because the 4CS(9) T of which each vertex subsystem is a copy has no automorphisms other than the identity. Thus we can put $\phi((v,i)) = (\psi(v),i)$ where ψ is a 1-1 mapping $V \rightarrow V$. Now we show that ψ is an automorphism of G. For any pair $u,v \in V$, the edges of S of form $((u,i),(v,j))$, $i,j \in \{1,2,\ldots,8\}$ are either all in edge cycles or all in non-edge cycles by construction, according as (u,v) is an edge of G or not. Moreover since the edge decomposition and the non-edge decomposition differ in at least one cycle, we can tell whether (u,v) is an edge of G by examining the cycles containing these edges of S. If (u,v) is an edge of G, then the edges $((u,i),(v,j))$, $i,j \in \{1,2,\ldots,8\}$ of S are in edge cycles, therefore the edges $(\phi((u,i)),\phi((v,j))) = ((\psi(u),i),(\psi(v),j))$, $i,j \in \{1,2,\ldots,8\}$ of S are also in edge cycles of S, and so $(\psi(u),\psi(v))$ is an edge of G. Similarly if (u,v) is not an

edge of G, then neither is $(\psi(u), \psi(v))$. Thus ψ is an automorphism of G.

Conversely, for any automorphism ψ of G we can define an automorphism ϕ of S by $\phi((v,i)) = (\psi(v), i)$. We show that it is an automorphism of S. The mapping ϕ is clearly 1-1 on S, and maps any vertex subsystem to another. We have further to show that ϕ maps edge decompositions to edge decompositions and non-edge decompositions to non-edge decompositions. That the edges $((u,i),(v,j))$, $i,j \in \{1,2,\ldots,8\}$ of S are in edge cycles of S implies (u,v) is an edge of G. But (u,v) is an edge of G implies $(\psi(u),\psi(v))$ is an edge of G, and $(\psi(u),\psi(v))$ is an edge of G implies the edges $(\phi((u,i)),\phi((v,j))) = ((\psi(u),i)),(\psi(v),j))$, $i,j \in \{1,2,\ldots,8\}$ are in edge cycles of S. Similarly for non-edge cycles. Thus ϕ is an automorphism of S.

We have therefore a 1-1 correspondence between automorphisms of S and automorphisms of G. In order to show that we have an isomorphism of automorphism groups, we need to show that the composition of two automorphisms of G gives rise to the composition of the corresponding automorphisms of S. If ψ_1 and ψ_2 are automorphisms of G, and $\phi_1((v,i)) = (\psi_1(v),i)$, $\phi_2((v,i)) = (\psi_2(v),i)$ for all $v \in V$, $i \in \{1,2,\ldots,8\}$, then $\phi_2\phi_1((v,i)) = \phi_2((\psi_1(v),i)) = (\psi_2\psi_1(v),i)$ for all $v \in V$, $i \in \{1,2,\ldots,8\}$. Thus, since the identity on G maps to the identity on S, we shown that our correspondence is an isomorphism of automorphism groups.

Further results of Frucht [9], [10] have shown that if $|\Gamma| = \gamma$ and a minimal generator set for Γ is of size ν, then we may take the graph G to have $2\gamma\nu$ vertices if Γ is non-cyclic and 3γ otherwise. Since the group $(Z_2)^\nu$ is the smallest group with ν generators, $\nu \leq log_2\gamma$ for any group. Thus it follows that 4CS S has no more than $16\gamma log_2\gamma + 1$ vertices if Γ is non-cyclic and $24\gamma + 1$ otherwise. □

Babai and Goodman [1] [3], among others, have proved results concerning

the minimum order and numbers of edges for graphs with given automorphism group, which may allow further reduction of the order of 4-cycle systems with given automporphism group.

5.3 Even-cycle systems

In this section we seek to generalise Theorem 5.2.1. Reviewing Construction 1, and the proof of Theorem 5.2.1, we can extend the construction and the result to all $2k$-cycle systems if we have two different symmetric decompositions of $K_{4k,4k}$ into $2k$-cycles, and a $2k\text{CS}(4k+1)$ that is automorphism-free and has no subsystems. Theorems 5.3.2 and 5.3.1 provide the required existence results.

Theorem 5.3.1. *For every $k \geq 2$, there exists a $2k$CS$(4k+1)$ having trivial automorphism group and with no proper subsystems.*

Theorem 5.3.2. *For each $k \geq 2$ there exists at least two different decompositions of $K_{4k,4k}$ into $2k$-cycles which are symmetric in the sense that if the vertex sets of the parts of the $K_{4k,4k}$ are $\{0,1,\ldots,(4k-1)\}$ and $\{0',1',\ldots,(4k-1)'\}$ respectively, then if the $2k$-cycle $(i_0,i'_1,\ldots,i_{2k-2},i'_{2k-1})$ is in the decomposition, then so is also the cycle $(i'_0,i_1,\ldots,i'_{2k-2},i_{2k-1})$.*

We shall prove these results in the following subsections. We can therefore state our generalisation of Theorem 5.2.1:

Theorem 5.3.3. *For every $k \geq 2$, and for any abstract group Γ of order γ, there exists a $2k$-cycle system S having full automorphism group isomorphic to Γ. Moreover S has no more than $8k\gamma log_2\gamma + 1$ vertices if Γ is non-cyclic and $12k\gamma + 1$ vertices otherwise.*

5.3.1 Proof of Theorem 5.3.1

We give the next four lemmas for more general m-cycle systems before specialising to even-cycle systems. Lemmas 5.3.1 and 5.3.2 trivially extend Lemmas 5.2.1 and 5.2.2.

Lemma 5.3.1. *If two subsystems of a mCS(n) intersect in more than one point, then their intersection is also a subsystem.*

Lemma 5.3.2. *If the set of fixed points of any automorphism of a mCS(n) has size greater than one, then it forms a subsystem.*

Lemma 5.3.3. *A cyclic mCS($2m+1$) has no proper subsystems if $m > 3$.*

Proof. A cyclic mCS($2m+1$) has just one orbit, since there are just $2m+1$ cycles. Suppose there is a cyclic mCS($2m+1$) S with a proper subsystem. Let T be a minimal subsystem of S of order t. Then $m \leq t < 2m+1$ since T must contain at least one cycle.

Since there is only one orbit, every cycle of S is a translate of every other cycle, and so every cycle of S is in a translate of T. Since T is minimal, T does not share any cycles with any of its translates, since otherwise, by Lemma 5.3.1 the intersection of two translates of T would be a smaller subsystem than T.

Every point of T is in precisely m cycles of S, and is in precisely $(t-1)/2$ cycles of T and of each translate in which it occurs. Each point of T is in the same number of translates of T. Let this number be r. Then $m = r(t-1)/2$. Putting $t = 2q+1$, since $t \geq m \geq 3$, we have $2q+1 \geq qr \geq 3$, so either $r = 1$, $r = 2$, or $q = 1$ and $r = 3$.

If $r = 1$, then T is the whole of S. If $q = 1$ and $r = 3$, then $m = 3$, and the mCS($2m+1$) is the unique STS(7), and every 3-cycle is a proper subsystem.

If $r = 2$, then $t = m + 1$, but then m must be even since t must be odd to be admissible. But t cannot be admissible because then m must divide $\frac{1}{2}(m+1)m$. Therefore for $m > 3$ a cyclic $m\text{CS}(2m+1)$ has no proper subsystems.

□

We have already proved Theorem 5.3.1 for the case $k = 2$. To prove this for $k > 2$, we shall modify a suitable construction for cyclic m-cycle systems. The following, given by Buratti and Del Fra, [5], will suffice:

Lemma 5.3.4. *Let $B = (b_1, b_2, \ldots, b_m)$ be the m-cycle defined by:*

$$\begin{aligned} b_i &= i(-1)^{i+1} \quad for \quad i < \tfrac{m}{2} \\ &= i(-1)^i \quad for \quad i \geq \tfrac{m}{2}. \end{aligned}$$

The translates of B (mod $2m+1$) generate a cyclic mCS$(2m+1)$.

We shall find it convenient in these constructions to number the positions in the cycle from 1 to m, but the cycles themselves from 0 to $2m$. Cycle B has label 0. As an example, the following is the 6CS(13) constructed by this method:

$$\begin{array}{lll} (1,-2,-3,4,-5,6) & , & (2,-1,-2,5,-4,-6) \\ (3,0,-1,6,-3,-5) & , & (4,1,0,-6,-2,-4) \\ (5,2,1,-5,-1,-3) & , & (6,3,2,-4,0,-2) \\ (-6,4,3,-3,1,-1) & , & (-5,5,4,-2,2,0) \\ (-4,6,5,-1,3,1) & , & (-3,-6,6,0,4,2) \\ (-2,-5,-6,1,5,3) & , & (-1,-4,-5,2,6,4) \\ (0,-3,-4,3,-6,5) & & \end{array}$$

Observe that for sufficently large m, and $1 \leq i < \frac{m}{2} - 2$, and for $\frac{m}{2} \leq i \leq m - 2$,

the difference between the i^{th} and $i + 2^{th}$ entries of B is ± 2. Consequently, considering alternate positions in a cycle, the same pair of points occurs several times in the system, for instance in the 6CS(13) example above, the points -3 and -5 occur in the third and fifth positions in the zeroth cycle, and in the sixth and fourth positions in the fourth cycle. We can exploit this to produce a different mCS$(2m+1)$ by exchanging the intervening points, i.e. in our example exchanging the 4 in cycle 0 with the -1 in cycle 4. Each edge still occurs exactly once in the new system, but the new system is no longer cyclic. We formalise this in the following for the case of even cycles. Constructions for the cases $k = 3, 4$ are provided separately.

Construction 2

For any $k > 4$, take the $2k$CS$(4k+1)$ constructed by Lemma 5.3.4. Put $k = 2t$ for k even and $k = 2t+1$ for k odd. We shall call this cyclic $2k$CS$(4k+1)$ system S, and will construct a new system which we shall call S'.

In the case of $k = 2t$ we exchange the $2t + 2^{th}$ point of the 0^{th} cycle with the $4t - 3^{th}$ point of the $2t + 2^{th}$ cycle. In the case of $k = 2t + 1$ we exchange the $2t + 4^{th}$ point of the 0^{th} cycle with the $(4t - 1)^{th}$ point of the $2t + 2^{th}$ cycle.

Lemma 5.3.5. *Construction 2 produces a $2k$CS$(4k+1)$.*

Proof. In order to show that S' is a $2k$CS$(4k+1)$ we must show that it is a decomposition of $K_{4k+1,4k+1}$ into $2k$-cycles. Since S' differs from the $2k$CS$(4k+1)$ S in only two cycles we merely have to show that the two new cycles contain the same edges as the originals, and that the points in each cycle are distinct.

We shall deal first with the case where k is even, $k = 2t$, $t > 2$. The $2t + 1^{th}$, $2t + 2^{th}$, and $2t + 3^{th}$ points of the 0^{th} cycle of the original system S are $-(2t+1)$, $2t + 2$, and $-(2t + 3)$ respectively, by reference to the expression for the points

of the cycle B given in Lemma 5.3.4.

The $4t-4^{th}$, $4t-3^{th}$, and $4t-2^{th}$ points of the $2t+2^{th}$ cycle of S are obtained by adding $2t+2$ to the corresponding points of of the 0^{th} cycle, and so these are, (mod $8t+1$):

$$\begin{aligned}
(4t-4)+2t+2 &= 6t-2 &&= -(2t+3), \\
-(4t-3)+2t+2 & &&= -(2t-5), \text{ and} \\
4t-2+2t+2 &= 6t &&= -(2t+1)
\end{aligned}$$

respectively. Noting from this that the $2t+1^{th}$ point of the 0^{th} cycle of S is equal to the $4t-2^{th}$ point of the $2t+2^{th}$ cycle, and that the $2t+3^{th}$ point of the 0^{th} cycle of S is equal to the $4t-4^{th}$ point of the $2t+2^{th}$ cycle, we conclude that if the $2t+2^{th}$ of the 0^{th} cycle is exchanged with the $4t-3^{th}$ point of the $2t+2^{th}$ cycle, the new cycles contain the same edges as before.

We must also be sure that the 0^{th} cycle of S does not contain the point $-(2t-5)$, and that the $2t+2^{th}$ cycle does not contain the point $2t+2$. In the first case this is because if $-(2t-5)$ were in the 0^{th} cycle, it would be the $2t-5^{th}$ point. But referring to Lemma 5.3.4, the $2t-5^{th}$ point of the cycle is $2t-5$. In the second case, we observe that the $2t+2^{th}$ cycle of S contains the point $2t+2$ only if the 0^{th} cycle contains the point 0. But this is not the case. Hence for the case $k=2t$, S' is a $2k\text{CS}(4k+1)$.

Now we prove the case for k odd, $k=2t+1$, $t\geq 2$. We shall proceed as in the even case. The $2t+3^{th}$, $2t+4^{th}$, and $2t+5^{th}$ points of the 0^{th} cycle of the original system S are $-(2t+3)$, $2t+4$, and $-(2t+5)$ respectively, by reference to the expression for the points of the cycle B given in Lemma 5.3.4.

The $4t-2^{th}$, $4t-1^{th}$, and $4t^{th}$ points of the $2t+2^{th}$ cycle of S are obtained

by adding $2t+2$ to the corresponding points of of the 0^{th} cycle, and so these are, (mod $8t+5$):

$$\begin{aligned} 4t-2+2t+2 &= 6t &&= -(2t+5), \\ -(4t-1)+2t+2 & &&= -(2t-3), \text{ and} \\ 4t+2t+2 &= 6t+2 &&= -(2t+3) \end{aligned}$$

respectively. Noting from this that the $2t+3^{th}$ point of the 0^{th} cycle of S is equal to the $4t^{th}$ point of the $2t+2^{th}$ cycle, and that the $2t+5^{th}$ point of the 0^{th} cycle of S is equal to the $4t-2^{th}$ point of the $2t+2^{th}$ cycle, we conclude that if the $2t+2^{th}$ point of the 0^{th} cycle is exchanged with the $4t+1^{th}$ point of the $2t+2^{th}$ cycle, the new cycles contain the same edges.

We must show that the 0^{th} cycle of S does not already contain the point $-(2t-3)$, and that the $2t+2^{th}$ cycle does not contain the point $2t+4$. In the first case this is because if $-(2t-3)$ were in the 0^{th} cycle, it would be the $2t-3^{th}$ point. But referring to Lemma 5.3.4, the $2t-3^{th}$ point of the cycle is $2t-3$. Also, we observe that the $2t+2^{th}$ cycle of S contains the point $2t+4$ only if the 0^{th} cycle contains the point $(2t+4)-(2t+2)=2$. But this is not the case. Hence S' is also a $2k\text{CS}(4k+1)$ for $k=2t+1$, $t \geq 2$. □

Lemma 5.3.6. *For $k>4$, the $2k\text{CS}(4k+1)$, S' that is produced by Construction 2 has no proper subsystems.*

Proof. Again, we put $k=2t$, for k even and $k=2t+1$ for k odd. We shall deal with the case $k=2t$ first. Any subsystem of S' must contain either the 0^{th} cycle or the $2t+2^{th}$ cycle, since otherwise the same subsystem would be present in the orginal cyclic system S, which has no proper subsystems by Lemma 5.3.3. But if the subsystem contains either of these cycles it must contain both, since

the cycles have two points in common, namely the neighbours of the exchanged points, as seen in Lemma 5.3.5. But if a proper subsystem of S' contains both cycles, then by restoring the exchanged points to their original places, we could produce a proper subsystem of S, contradicting Lemma 5.3.3. Therefore S' has no proper subsystems.

The proof for $k = 2t + 1$ proceeds in exactly the same way. □

We shall call a pair of alternate points in a cycle an *alternate pair*. For the sake of clarity we show alternate pairs in square brackets, e.g. $[a, b]$. In order to prove the $2k\text{CS}(4k + 1)$ S' has trivial automorphism group, we examine the frequency of each possible alternate pair in S'. We shall find it convenient to do this first for the cyclic system S. We need only look at the 0^{th} cycle of S. We shall take the cases $k = 2t$ and $k = 2t + 1$ separately.

Firstly, we take $k = 2t$. The 0^{th} cycle of S is:

$$(1, -2, 3, \ldots, -(2t-2), 2t-1, 2t, -(2t+1), 2t+2, -(2t+3) \ldots, -(4t-1), 4t),$$

where all points are (mod $8t + 1$). Except for the alternate pairs $[-(2t-2), 2t]$, $[2t-1, -(2t+1)]$, $[-(4t-1), 1]$, and $[4t, -2]$, the absolute difference between alternate pairs is 2. In a single cycle of S, there are therefore $4t - 4$ alternate pairs with difference 2, two with difference $4t$, and one each with differences $4t-2$ and $4t + 2$ respectively. The frequency of any alternate pair in S is equal to the frequency of pairs with the same difference in a single cycle, so for instance the alternate pair $[1, 3]$ occurs $4t - 4$ times in S.

Now we consider S'. The only cycles of S' that are different from S are the 0^{th} and $2t + 2^{th}$ cycles, and these are:

$$(1, -2, 3, \ldots, 2t, -(2t+1), -(\mathbf{2t-5}), -(2t+3), 2t+4, \ldots, 4t), \text{ and}$$
$$(2t+3, 2t, \ldots, -(2t-7), -(2t+3), \mathbf{2t+2}, -(2t+1), -(2t-3), -(2t-1)\ ),$$

where the exchanged points are show in bold. This has the effect of replacing the alternate pairs $[2t, 2t+2]$ and $[2t+2, 2t+4]$ in the 0^{th} cycle by $[2t, -(2t-5)]$ and $[-(2t-5), 2t+4]$, and the pairs $[-(2t-7), -(2t-5)]$ and $[-(2t-5), -(2t-3)]$ in the $2t+2^{th}$ cycle by $[-(2t-7), 2t+2]$ and $[2t+2, -(2t-3)]$. Thus alternate pairs with differences 2 are replaced with cycles with differences $4t-5$, $4t-1$, $4t-5$, and $4t-1$. In particular we note that in S' the alternate pairs $[2t, 2t+2]$, $[2t+2, 2t+4]$, $[-(2t-7), -(2t-5)]$ and $[-(2t-5), -(2t-3)]$ each occur with frequency $4t-5 \geq 7$, whereas every other alternate pair with difference 2 occurs with frequency $4t-4$, and no other alternate pair occurs with frequency more than two.

Secondly we consider $k = 2t+1$, $t \geq 2$. The 0^{th} cycle of S is:

$(1, -2, 3, \ldots, 2t-1, -2t, -(2t+1), 2t+2, -(2t+3), 2t+4, -(2t+5), 2t+6,$

$\ldots, -(4t+1), 4t+2),$

where all points are (mod $8t+5$). Except for the alternate pairs $[2t-1, -(2t+1)]$, $[-2t, 2t+2]$, $[-(4t+1), 1]$, and $[4t+2, -2]$, the absolute difference between alternate pairs is 2. In a single cycle of S, there are therefore $4t-2$ alternate pairs with difference 2, two pairs with difference $4t+2$, and one each with difference $4t$ and $4t+4$ respectively. All alternate pairs with these differences occur with these frequencies in S.

Considering S', the only cycles of S' that are different from S are the 0^{th} and $2t+2^{th}$ cycles, and these are:

$$(1, -2, 3, \ldots, 2t+2, -(2t+3), \mathbf{-(2t-3)}, -(2t+5), 2t+6, \ldots, 4t+2), \quad \text{and}$$

$$(2t+3, 2t, \ldots, -(2t-5), -(2t+5), \mathbf{2t+4}, -(2t+3), -(2t-1), -(2t+1)\ ),$$

This has the effect of replacing the alternate pairs $[2t+2, 2t+4]$ and $[2t+4, 2t+6]$ in the 0^{th} cycle by the pairs $[2t+2, -(2t-3)]$ and $[-(2t-3), 2t+6]$, and the

pairs $[-(2t-5),-(2t-3)]$ and $[-(2t-3),-(2t-1)]$ in the $2t+2^{th}$ cycle by $[-(2t-5),2t+4]$ and $[2t+4,-(2t-1)]$. Thus alternate pairs with difference 2 are replaced with cycles with differences $4t-1$, $4t+3$, $4t-1$, and $4t+3$. In particular we note that in S' the alternate pairs $[2t+2,2t+4]$, $[2t+4,2t+6]$, $[-(2t-5),-(2t-3)]$ and $[-(2t-3),-(2t-1)]$ each occur with frequency $4t-3 \geq 5$, whereas every other alternate pair with difference 2 occurs with frequency $4t-2$, and no other alternate pair occurs with frequency more than two.

Lemma 5.3.7. *For $k > 4$ the automorphism group of the $2kCS(4k+1)$ S' is trivial.*

Proof. Since by Lemma 5.3.2 the fixed points of any automorphism of S' form a subsystem, and since by Lemma 5.3.6 S' has no proper subsystems, no non-trivial automorphism has more than one fixed point. We consider the case $k = 2t$ first. We know from the above analysis that the four alternate pairs $[2t, 2t+2]$, $[2t+2, 2t+4]$, $[-(2t-7),-(2t-5)]$ and $[-(2t-5),-(2t-3)]$ occur with unique frequency $4t-5$. Any automorphism of S' must either permute or stabilise these pairs. Since the point $2t+2$ is common to two pairs, and $-(2t-5)$ is common to the other two, any automorphism either fixes both points or transposes them. Supposing them to be transposed, either $2t$ must be transposed with $-(2t-7)$ and $2t+4$ with $-(2t-3)$ or $2t$ with $-(2t-3)$ and $2t+4$ with $-(2t-7)$.

The 3^{rd} cycle contains the sequence $-(2t-7), 2t, -(2t-5), 2t+2, \ldots$, starting at the $2t-4^{th}$ position. The cycle does not contain either of the points $2t+4$ or $-(2t-3)$ because otherwise the 0^{th} cycle would contain $2t+1$ or $-2t$. Since this is the unique cycle containing the edge $-(2t-5), 2t+2$, the automorphism preserves the cycle and reverses it. But then $-(2t-7)$ and $2t$ cannot be mapped to $2t+4$ and $-(2t-3)$. Therefore the automorphism is the identity.

The case $k = 2t + 1$, $t \geq 2$ is proved in a similar way. Suppose there exists a non-trivial automorphism of S'. The alternate pairs $[2t+2, 2t+4]$, $[2t+4, 2t+6]$, $[-(2t-5), -(2t-3)]$ and $[-(2t-3), -(2t-1)]$ are the only ones that occur with frequency $4t-3$ in S'. Therefore a non-trivial automorphism transposes $2t+4$ and $-(2t-3)$, and either exchanges $2t+2$ with $-(2t-5)$ and $2t+6$ with $-(2t-1)$ or exchanges $2t+2$ with $-(2t-1)$ and $2t+6$ with $-(2t-5)$.

However the $6t+7^{th}$ cycle contains the sequence $2t+2, 2t+6, 2t+4, -(2t-3), -2t, -(2t-5)$ starting at the $4t^{th}$ position. The cycle does not contain the point $-(2t-1)$, because otherwise the 0^{th} cycle would contain -1. Since this is the unique cycle containing the edge $(2t+4, -(2t-3))$, the automorphism preserves it and reverses it about this edge. But then $2t+6$ would map to $-2t$, not $-(2t-1)$. Thus the automorphism is the identity. □

Lemma 5.3.8. *There exists a 6CS(13) with trivial automorphism group and no proper subsystems.*

Proof. We modify the construction of Lemma 5.3.4 for $m = 6$ exchanging 4 at position 4 in the 0^{th} cycle with -1 at position 5 in the 4^{th} cycle.

(1,	−2,	−3,	−1,	−5,	6)	,	(2,	−1,	−2,	5,	−4,	−6)
(3,	0,	−1,	6,	−3,	−5)	,	(4,	1,	0,	−6,	−2,	−4)
(5,	2,	1,	−5,	4,	−3)	,	(6,	3,	2,	−4,	0,	−2)
(−6,	4,	3,	−3,	1,	−1)	,	(−5,	5,	4,	−2,	2,	0)
(−4,	6,	5,	−1,	3,	1)	,	(−3,	−6,	6,	0,	4,	2)
(−2,	−5,	−6,	1,	5,	3)	,	(−1,	−4,	−5,	2,	6,	4)
(0,	−3,	−4,	3,	−6,	5)							

This 6CS(13) is proved to have no proper subsystems using the same method as

for Lemma 5.3.6. The differences between alternate pairs in ordinary cycles, i.e. cycles with no exchange, are $4, 6, 2, 2, 6, 5$. In the 0^{th} cycle the corresponding differences are $4, 1, 2, 6, 6, 5$, and in the 4^{th} cycle they are $4, 6, 3, 2, 1, 5$. In particular, we see that the alternate pair $[6, -1]$ occurs three times in S', in the 0^{th}, 8^{th}, and 11^{th} cycles respectively, whereas no other alternate pair occurs with frequency greater than two. Consequently, the points 6 and -1 are either both fixed or swapped by any automorphism of S'. If they are fixed then the automorphism is trivial by Lemma 5.3.2. Otherwise, considering the triples of consecutive points $-1, -5, 6$ in the 0^{th} cycle, $6, 5, -1$ in the 8^{th} cycle, and $6, 4, -1$ in the 11^{th} cycle, -5 must either be fixed or mapped to either 5 or 4. But considering the 2^{nd} cycle, which contains the edge $(-1, 6)$ and also -5, if 6 and -1 are swapped, then -5 must be swapped with 3. Hence 6 and -1 must be fixed, and any automorphism of S' is trivial. □

Lemma 5.3.9. *There exists an $8CS(17)$ with trivial automorphism group and no proper subsystems.*

Proof. We modify the construction of Lemma 5.3.4 for $m = 8$ exchanging 6 at

position 6 in the 0^{th} cycle with -3 at position 7 in the 4^{th} cycle.

$$
\begin{array}{ll}
(1,-2,3,4,-5,-3,-7,8) & , \ (2,-1,4,5,-4,7,-6,-8) \\
(3,0,5,6,-3,8,-5,-7) & , \ (4,1,6,7,-2,-8,-4,-6) \\
(5,2,7,8,-1,-7,6,-5) & , \ (6,3,8,-8,0,-6,-2,-4) \\
(7,4,-8,-7,1-5,-1,-3) & , \ (8,5,-7,-6,2,-4,0,-2) \\
(-8,6,-6,-5,3,-3,1,-1) & , \ (-7,7,-5,-4,4,-2,2,0) \\
(-6,8,-4,-3,5,-1,3,1) & , \ (-5,-8,-3,-2,6,0,4,2) \\
(-4,-7,-2,-1,7,1,5,3) & , \ (-3,-6,-1,0,8,2,6,4) \\
(-2,-5,0,1,-8,3,7,5) & , \ (-1,-4,1,2,-7,4,8,6) \\
(0,-3,2,3,-6,5,-8,7) &
\end{array}
$$

Again, the system has no proper subsystems, which can be shown by the same method as in Lemma 5.3.6. For cycles other than the 0^{th} and the 4^{th}, the sequence of alternate differences is $2,6,8,2,2,2,8,7$. For the 0^{th} cycle it is $2,6,8,7,2,6,8,7$, and for the 4^{th} cycle it is $2,6,8,2,7,2,1,7$. From these differences we see that, except for the alternate pairs $[4,6]$, $[6,8]$ and $[-1,-3]$, each alternate pair with difference 2 occurs four times in the system, whereas these pairs each occur only three times each. No other alternate pair occurs three times. Therefore an automorphism can only permute these pairs, and the point 6 is common to two of them it is fixed by all automorphisms. By Lemma 5.3.2, an automorphism that fixes more than one point is the identity, so a non-trivial automorphism transposes 4 with 8 and -1 with -3. In particular, cycle 6 uniquely contains the edge $-1,-3$, and so it is preserved. However, this cycle contains 4 but not 8, so the only automorphism is the identity.

Therefore, by Lemma the only automorphism is the identity. □

5.3.2 Proof of Theorem 5.3.2

We require two different symmetric decompositions of $K_{4k,4k}$ into $2k$-cycles. We first of all show that there is at least one such decomposition.

Theorem 5.3.4. *For each $k \geq 2$ there exists a symmetric decomposition of $K_{4k,4k}$ into $2k$-cycles.*

Proof. As already remarked, the case $k = 2$ has been covered in Section 5.2. For $k > 2$ we present a separate construction for each residue class (mod 4).

I) For $k \equiv 0 \pmod 4$, we put $k = 4s$, and partition the $2k - 2$ differences (mod $4k$), excluding 0, k and $2k$, into sequences, each of length $k - 1$. For $k \geq 12$ these sequences are:

$-3, 5, -7, \ldots, -(k-1), -(k-2), (k-4), -(k-6), \ldots, -2, k+1,$

and

$1, -(k+3), (k+5), -(k+7), \ldots, -(2k-1), -(2k-2), (2k-4),$

$-(2k-6), (2k-8), \ldots, -(k+2),$

where in the first sequence the central, $2s^{th}$ value is $-(k-2)$, and in the second sequence the central value is $-(2k-1)$. For $k = 4$ the sequences are $-3, -2, 5$ and $1, -7, -6$ respectively, and for $k = 8$ they are:

$-3, 5, -7, -6, 4, -2, 9$ and $1, -11, 13, -15, -14, 12, -10$.

The first sequence sums to zero and the second to k. This can be seen for instance in the first sequence by pairing -3 with $-(k-2)$, 5 with $(k-4)$ etc, which sum alternately to $\pm(k+1)$, giving

$$-s(k+1) + (s-1)(k+1) + (k+1) = 0.$$

For the second sequence, pairing $-(k+3)$ with $-(2k-2)$ etc., we obtain similarly

$$1 - s(3k+1) + (s-1)(3k+1) = -3k \equiv k \pmod{4k}.$$

Develop these into sequences of k points starting with 0 by successive addition:

a) $0, -3, 2, -5, 4, -7, \ldots, -(2s+1), -(6s-1), -(2s+3), -(6s-3),$
$-(2s+5), \ldots, -(k-1), -(k+1), 0,$ and

b) $0, 1, -(k+2), 3, -(k+4), \ldots, -(6s-2), (2s-1), -6s, (2s+2),$
$-(6s+2), (2s+4), -(6s+4), \ldots, (k-2), -(2k-2), k.$

From sequence a) we shall construct $4k$ cycles that additionally contain the edges with difference k, and from sequence b) we shall construct $2k$ cycles that additionally contain the edges with difference zero and $2k$ cycles that additionally contain the edges with difference $2k$.

From sequence a), take the four sequences obtained by adding 0, k, $2k$ and $3k$ respectively:

i) $0, -3, \ldots - (k+1), 0,$

ii) $k, (k-3), \ldots, -1, k,$

iii) $2k, (2k-3), \ldots (k-1), 2k,$

iv) $3k, (3k-3), \ldots, (2k-1), 3k.$

Now concatenate i) with ii) and iii) with iv), then join the ends and label alternately to obtain the cycles:

$(0', -3, \ldots - (k+1)', 0, k', (k-3), \ldots, -1', k)$, and

$(2k', (2k-3), \ldots (k-1)', 2k, 3k', (3k-3), \ldots, (2k-1)', 3k)$.

Labelling the points in the opposite way and pairing i) with iv) and ii) with iii) we obtain:

$(0, -3', \ldots - (k+1), 0', 3k, (3k-3)', \ldots, (2k-1), 3k')$, and

$(k, (k-3)', \ldots, -1, k', 2k, (2k-3)', \ldots (k-1), 2k')$.

We develop each of these cycles cyclicly by adding $0, 1, \ldots, (k-1)$ respectively to each point to obtain a total of $4k$ cycles that in particular contain all the edges with difference k.

We construct the cycles containing the edges with differences zero and $2k$ from sequence b). Take the four sequences obtained by adding 0, k, $2k$ and $3k$ respectively:

i) $0, 1, \ldots, -(2k-2), k$,

ii) $k, k+1, \ldots, -(k-2), 2k$,

iii) $2k, 2k+1, \ldots 2, 3k$,

iv) $3k, 3k+1, \ldots, k+2, 0$.

To construct the cycles with difference zero, we concatenate two copies of sequence i), one reversed, and label alternately, joining the ends to obtain a cycle, and do the same also with sequence iii). This yields the cycles:

$(0, 1', \ldots, -(2k-2), k', k, -(2k-2), \ldots, 1, 0')$, and

$(2k, (2k+1)', \ldots, 2, 3k', 3k, 2', \ldots, (2k+1), 2k')$.

Develop these cyclicly by adding $0, 1, \ldots, (k-1)$ respectively to each point to obtain a total of $2k$ cycles.

To construct the cycles with difference $2k$, concatenate sequence ii) with

sequence iv) reversed, join the ends and label in both ways to obtain the cycles:

$(k, (k+1)', \ldots, -(k-2), 2k', 0, (k+2)', \ldots, (3k+1), 3k')$, and

$(k', (k+1), \ldots, -(k-2)', 2k, 0', (k+2), \ldots, (3k+1)', 3k)$.

Develop these cyclicly by adding $0, 1, \ldots, (k-1)$ respectively to each point to obtain a further $2k$ cycles.

This completes the symmetric decomposition for $k \equiv 0 \pmod 4$.

II) For $k \equiv 1 \pmod 4$, we put $k = 4s+1$, and partition the $2k-2$ differences (mod $4k$), excluding 0, k and $2k$ into two sequences each of length $k-1$. For $k \geq 9$ these are:

$-1, 2, -3, \ldots, -(2s-1), (2s+1), -(2s+2), (2s+3), \ldots, -(k-1), (6s+1)$,

and

$-2s, (k+1), -(k+2), (k+3), \ldots, -(6s-1), 6s, -(6s+2)$,

$(6s+3), \ldots, -(2k-2), (2k-1)$,

and for $k = 5$ the sequences are $-1, 3, -4, 7$ and $-2, 6, -8, 9$. As a further example, the sequences for $k = 9$ are

$-1, 2, -3, 5, -6, 7, -8, 13$ and $-4, 10, -11, 12, -14, 15, -16, 17$. Each sequence sums to k. This can be seen for instance with the first sequence by pairing -1 with $-(k-1)$, 2 with $(k-2)$ etc, which sum alternately to $\pm k$, giving $-ks + k(s-1) + (2s+1) + (6s+1) = k$. Similarly with the second sequence, pairing $(k+1)$ with $(2k-1)$ etc., we have $-2s + 3ks - (6s+2) - 3k(s-1) = k$. Develop each of these into sequences of k points starting with 0 by successive addition:

a) $0, -1, 1, -2, 2, \ldots, -(s-1), (s-1), -s, (s+1), -(s+1), (s+2)$,
$-(s+2), \ldots, 2s, -2s, k$, and

b) $0, -2s, (2s+2), -(2s+1), (2s+3), -(2s+2), (2s+5), \ldots, -(3s-1),$
$(3s+1), -(3s+1), (3s+2), -(3s+2), \ldots, (k-1), -(k-1), k.$

From sequence a) we shall construct $4k$ cycles that additionally contain the edges with difference k, and from sequence b) we shall construct $2k$ cycles that additionally contain the edges with difference zero and $2k$ cycles that additionally contain the edges with difference $2k$.

From sequence a) construct a cycle by concatenating two copies, labelling alternate points, and joining the ends, i.e.
$(0', -1, 1', \ldots, -2s, k', 0, -1', 1, \ldots, -2s', k)$. This cycle has two new edges with difference k. Develop cyclicly (mod $4k$) to obtain $4k$ cycles.

We now construct the cycles containing the edges with differences zero and $2k$ from sequence b). Take the four sequences obtained by adding 0, k, $2k$ and $3k$ respectively:

i) $0, -2s, \ldots, -(k-1), k,$

ii) $k, (k-2s), \ldots, 1, 2k,$

iii) $2k, (2k-2s), \ldots, k+1, 3k,$

iv) $3k, (3k-2s), \ldots, 2k+1, 0.$

To construct the cycles with difference zero, we concatenate two copies of sequence i), one reversed, and label alternately, joining the ends to obtain a cycle, and do the same also with sequence iii). This yields the cycles:
$(0, -2s', \ldots, -(k-1), k', k, -(k-1)', \ldots, -2s, 0')$, and
$(2k, (2k-2s)', \ldots, (k+1), 3k', 3k, (k+1)', \ldots, (2k-2s), 2k')$.
Develop these cyclicly by adding $0, 1, \ldots, (k-1)$ respectively to each point to obtain a total of $2k$ cycles.

To construct the cycles with difference $2k$, concatenate sequence ii) with sequence iv) reversed, join the ends and label in both ways to obtain the cycles:

$(k, (k-2s)', \ldots, 1, 2k', 0, (2k+1)', \ldots, (3k-2s), 3k')$, and

$(k', (k-2s), \ldots, 1', 2k, 0', (2k+1), \ldots, (3k-2s)', 3k)$.

Develop these cyclicly by adding $0, 1, \ldots, (k-1)$ respectively to each point to obtain a further $2k$ cycles.

This completes the symmetric decomposition for $k \equiv 1 \pmod 4$.

III) For $k \equiv 2 \pmod 4$, we put $k = 4s+2$. In this case we shall decompose $K_{2k,2k}$ into $2k$-cycles. We can expand this to a decomposition of $K_{4k,4k}$ by partitioning $K_{4k,4k}$ into four copies of $K_{2k,2k}$, then decomposing each of those into $2k$-cycles.

Firstly we arrange the $k-1$ differences (mod $2k$), excluding k and 0, into the sequence $1, -2, 3, -4, \ldots, (k-1)$. This has sum $\frac{k}{2}$, which we can see by pairing consecutive terms, giving $-\frac{(k-2)}{2} + (k-1) = \frac{k}{2}$. Develop this into a sequence of k points starting with 0 by successive addition to obtain $0, 1, -1, 2, -2 \ldots, 2s, -2s, (2s+1) = \frac{k}{2}$.

Take the four sequences obtained by adding 0, $\frac{k}{2}$, k and $\frac{3k}{2}$ respectively to each point:

a) $0, 1, -1, 2, -2, \ldots, \frac{k-2}{2}, -\frac{k-2}{2}, \frac{k}{2}$,

b) $\frac{k}{2}, \frac{k+2}{2}, \frac{k-2}{2}, \ldots, k-1, 1, k$,

c) $k, k+1, k-1, \ldots, \frac{k+2}{2}, \frac{3k}{2}$,

d) $\frac{3k}{2}, \frac{3k+2}{2}, \frac{3k-2}{2}, \ldots, k+1, 0$.

Now concatenate two copies of a), one reversed, label alternately, and join the ends to obtain the $2k$-cycle

$$(0', 1, -1', \ldots, -\tfrac{k-2}{2}', \tfrac{k}{2}, \tfrac{k}{2}', -\tfrac{k-2}{2}, \ldots, 1', 0).$$

We do the same with sequence c) to obtain the cycle

$$(k', k+1, k-1', \ldots, \tfrac{k+2}{2}', \tfrac{3k}{2}, \tfrac{3k}{2}', \tfrac{k+2}{2}, \ldots, k-1, k+1', k)$$

These cycles each contain two new edges with difference zero. Develop each of these cyclicly (mod $2k$) for $\frac{k}{2}$ repetitions only to obtain k cycles. Finally, concatenate b) with d) reversed, join the ends and label in both possible ways to obtain the two cycles

$$(\tfrac{k}{2}', \tfrac{k+2}{2}, \tfrac{k-2}{2}', \ldots, 1', k, 0', k+1, \ldots, \tfrac{3k+2}{2}', \tfrac{3k}{2}), \text{ and}$$
$$(\tfrac{k}{2}, \tfrac{k+2}{2}', \tfrac{k-2}{2}, \ldots, 1, k', 0, k+1', \ldots, \tfrac{3k+2}{2}, \tfrac{3k}{2}').$$

These cycles each contain two new edges with difference k. Develop each of these cyclicly (mod $2k$) for $\frac{k}{2}$ repetitions to obtain k further cycles. This completes the symmetric decomposition for $k \equiv 2 \pmod 4$.

IV) For $k \equiv 3 \pmod 4$, we put $k = 4s + 3$. As for the previous case, we shall decompose $K_{2k,2k}$ into $2k$-cycles, and expand this to a decomposition of $K_{4k,4k}$.

Firstly, we arrange the $k-1$ differences (mod $2k$), excluding k, into the sequence

$$-1, 3, -5, \ldots, (k-4), -(k-2), (k+1), -(k+3), (k+5), -(k+7),$$
$$\ldots, -(2k-4), (2k-2) = -2.$$

The sequence sums to k, which we can see by pairing -1 with $(k+1)$, and 3 with $-(k+3)$ etc., giving $k(s+1)-ks=k$. Develop this into a sequence of points starting with 0 by successive addition:

$0,-1,2,-3,\ldots,-\frac{k-1}{2},\frac{k+3}{2},-\frac{k+3}{2},\ldots,k-2,-(k-2),k.$

Concatenate two copies of this, one reversed, label alternately, and join the ends to obtain the $2k$-cycle

$(0',-1,2',\ldots,-(k-2),k',k,-(k-2)',\ldots,-1',0).$

This cycle contains two new edges, each with difference 0. Develop this cyclicly (mod $2k$) for k repetitions to give k cycles. Now add k to each point of the original sequence of points to obtain

$k,(k-1),(k+2),\ldots,2,0$, and concatenate two copies of this sequence end to end, label alternately, and join the ends to obtain

$(k',(k-1),(k+2)',\ldots,2,0',k,(k-1)',(k+2),\ldots,2',0).$

This cycle contains two new edges, each with difference k. Finally develop this (mod $2k$) for k repetitions to complete the symmetric decomposition for the case $k\equiv 3 \pmod 4$.

This completes the proof of Theorem 5.3.4. □

Recall that we have already provided a second different decomposition of $K_{8,8}$ into 4-cycles in Section 5.2. For $k>2$, given one decomposition we can easily produce a second different one by the following method. Denote the vertices of the two parts of $K_{4k,4k}$ by $0,1,\ldots,(4k-1)$ and $0',1',\ldots,(4k-1)'$ respectively. Note that for the cases $k\equiv 0,1,3 \pmod 4$ in Theorem 5.3.4, the decomposition contains a cycle that contains the edges $(0,0')$ and (k,k') but not the edge $(1,1')$. Also, for the case $k\equiv 2 \pmod 4$ the decomposition contains the edges $(0,0')$ and $(\frac{k}{2},\frac{k'}{2})$ but again not the edge $(1,1')$. If we now re-label the decomposition by

exchanging the label 1 with 0, and the label $1'$ with $0'$ in all cycles, we obtain a new, though isomorphic decomposition, but which in the cases $k \equiv 0, 1, 3 \pmod 4$ the cycle that contains the edge (k, k') also contains the edge $(1, 1')$ but not the edge $(0, 0')$, and in the case $k \equiv 2 \pmod 4$ the cycle that contains the edge $(\frac{k}{2}, \frac{k'}{2})$ also contains the edge $(1, 1')$ but not $(0, 0')$. In each case the second decomposition is different to the original in the sense required.

This completes the proof of Theorem 5.3.2.

Chapter 6

Odd cycle systems

6.1 Introduction

In this chapter we shall prove that for every group Γ and every odd $m > 3$, there is an mCS(n) system for some n, which has full automorphism Γ. Mendelsohn, [16], has already proved this for $m = 3$. The proof of this result requires a different fundamental construction from that used for the even-cycles case of Chapter 5, but we will also use some of the basic results proved there.

In common with the even-cycles case, the approach is to show that for any graph $G = (V, E)$, there is an mCS(n) system with the same automorphism group. The result of Frucht [9] is then used to provide a graph with the required automorphism group.

To construct an mCS system with the same automorphism group as a given graph, we define a recursive construction analogous to a $|V|$-dimensional cube, where V is the vertex set of the graph. Subsystems on selected 2-faces of this cube are modified to give a new system with the required automorphism group.

Section 6.2 describes the recursive construction and derives some important

properties. Section 6.3 details the modified construction, and proves that the modified system has the required automorphism group. Section 6.4 gives constructions which provide the basic building blocks required. Section 6.5 draws these elements together to prove the main result.

6.2 Basic construction

Given an $m\mathrm{CS}(n)$, S, $(m, n \geq 3)$, and a non-zero positive integer v, we define an $m\mathrm{CS}(n^v)$ on the n^v points $(x_1, x_2, \ldots, x_v)$, $x_i \in \{0, 1, \ldots, n-1\}$, which we denote by S^v. Before proceeding we define some notation. If $X = (x_1, x_2, \ldots, x_v)$ is any point of S^v we denote the value of the i^{th} coordinate of X by $(X)_i$, i.e. $(X)_i = x_i$. We denote the set $\{0, 1, \ldots, n-1\}$ by the symbol $[n]$.

We now define the cycles of S^v. The sequence $(X_1, X_2, \ldots, X_m)$, $X_j \in S^v$, $j = 1, 2, \ldots, m$ is a cycle of S^v if

i) for at least one $i \in \{1, 2, \ldots, v\}$, the sequence

$$((X_1)_i, (X_2)_i, \ldots, (X_m)_i) \quad \text{is a cycle of } S, \text{ and}$$

ii) if $((X_1)_i, (X_2)_i, \ldots, (X_m)_i)$ is not a cycle of S, then

$$(X_1)_i = (X_2)_i = \ldots = (X_m)_i.$$

The cycles of S^v define an $m\mathrm{CS}(n^v)$, because if X_1, X_2 are distinct points of S^v, the edge (X_1, X_2) is in a unique cycle of S^v because for each $i \in \{1, 2, \ldots, v\}$ if $(X_1)_i \neq (X_2)_i$ the edge $((X_1)_i, (X_2)_i)$ is in a cycle of S, which is unique by definition.

The construction just given is valid for all such S. However, from this point on we shall assume that S is has trivial automorphism group, and also that it has no proper subsystems.

The system S^v has many subsystems of order n^k for all $1 \leq k \leq v$. We are particularly interested in the case $k = 1$, as we shall use these to derive the automorphism group for S^v. We characterise the subsystems of order n in the following lemma.

Lemma 6.2.1. *If S has trivial automorphism group and has no proper subsystems, then every mCS(n) subsystem of S^v consists of the points in which the values of $k \geq 1$ distinct coordinates $i_1 < i_2 < \cdots < i_k$ are equal, and take all the values in $[n]$, and the remainder of the coordinates are constant.*

Proof. Let T be any mCS(n) subsystem of S^v, and let $(X_1, X_2, \ldots, X_m)$ be any cycle in T. For any $i \in \{1, 2, \ldots, v\}$, either $(X_1)_i = (X_2)_i = \ldots = (X_m)_i$ or $((X_1)_i, (X_2)_i, \ldots, (X_m)_i)$ is a cycle of S. If two points of T differ in the i^{th} coordinate, with values x and y, then there is at least one edge of T whose endpoints have i^{th} coordinate values x and y. So if the i^{th} coordinate is not constant for every cycle of T, the cycles of S obtained by taking the i^{th} coordinate in each point for each cycle of T form a subsystem of S. However this must be the whole of S, since S has no proper subsystems. Therefore, if the i^{th} coordinate is not constant in T, it takes all values $0, 1, \ldots, n-1$.

If there are two distinct coordinates i, and j, whose values are both not constant for all points of T, then they both take all values $0, 1, \ldots, n-1$, and since T is of order n, each value of the i^{th} coordinate occurs with only one value of the j^{th} coordinate. Since S has trivial automorphism group, these must be equal for all points of T, otherwise the correspondence would define a non-trivial

automorphism of S.

□

Thus for any $A \subset \{1, 2, \ldots, v\}$, each n-set of points $(x_1, x_2, \ldots, x_v)$ in S^v with x_j held fixed for $j \notin A$, and for $j \in A$, taking the same value which ranges across all values $0, 1, \ldots, n-1$, is an $m\mathrm{CS}(n)$ subsystem of S^v isomorphic to S. For any A there are therefore $n^{v-|A|}$ such $m\mathrm{CS}(n)$, one for each choice of the fixed values. We shall say that any two subsystems corresponding to the same set A are mutually *parallel.*

Lemma 6.2.2. *For each automorphism ϕ of S^v there is a permutation, σ, of $1, \ldots, v$ such that $\phi(x_1, \ldots, x_v) = (x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(v)})$, for every $x_1, \ldots, x_v \in [n]$. In other words, each automorphism of S^v corresponds to a permutation of the coordinates.*

Proof. We prove that for each $1 \leq i \leq v$, there is a $1 \leq j \leq v$ such that for any values $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_v \in [n]$, there are values $\alpha_1, \ldots, \alpha_{j-1}, \alpha_{j+1}, \ldots, \alpha_v \in [n]$ with

$$\phi(a_1, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_v) = (\alpha_1, \ldots, \alpha_{j-1}, x, \alpha_{j+1}, \ldots, \alpha_v)$$

for each $x \in [n]$.

For any choice of i and of values $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_v$, the set of points $\{X(x) : (X(x))_r = a_r, r \neq i, (X(x))_i = x, x \in [n]\}$ forms an $m\mathrm{CS}(n)$ subsystem of S^v, and therefore so does the image of these points in ϕ. By Lemma 6.2.1 there is a non-empty set of values $A_i = \{j_1, j_2, \ldots j_k\} \subset \{1, 2, \ldots, v\}$, and a set of values $\{\alpha_r : \alpha_r \in [n], r \in \{1, 2, \ldots, v\} \setminus A_i\}$ such that for each $X(x)$, $x \in [n]$ there is a $y \in [n]$ with $(\phi(X(x)))_r = y$ for $r \in A_i$ and $(\phi(X(x)))_r = \alpha_r$ otherwise.

Observe that for any $r \in A_i$, the mapping $x \mapsto X(x) \mapsto (\phi(X(x)))_r = y$ provides an automorphism of S, from which we conclude that $y = x$, since S has trivial automorphism group.

We now show that the images under ϕ of the $mCS(n)$ subsystems obtained by varying the $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_v$ are mutually parallel.

In order to show this it is only necessary show to that A_i remains the same if we change any one a_t, $t \neq i$ at a time. So choose $t \neq i$, $1 \leq t \leq v$, and substitute any value $a'_t \neq a_t$ for a_t. Then there is a set $A'_i \subset \{1, 2, \ldots, v\}$, and values α'_r, $r \in \{1, 2, \ldots, v\} \setminus A'_i$ such that ϕ maps each point
$X'(x) = (a_1, \ldots, a_{t-1}, a'_t, a_{t+1}, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_v)$ to the point $\phi(X'(x))$, where $(\phi(X'(x)))_r = x$ if $x \in A'_i$, and $(\phi(X'(x)))_r = \alpha'_r$ otherwise.

For each fixed $x \in [n]$, the points $X(x)$ and $X'(x)$ are both members of the mCS(n) subsystem consisting of the points
$(a_1, \ldots, a_{t-1}, y, a_{t+1}, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_v)$, $y \in [n]$. We shall call this a *crossing subsystem.* Thus $\phi(X(x))$ and $\phi(X'(x))$ are also members of a crossing subsystem.

Suppose $r \in A_i \setminus A'_i$. Then $(\phi(X(x)))_r = x$ and $(\phi(X'(x)))_r = \alpha_r$ for each $x \in [n]$. But for any given value of x, as members of the same crossing subsystem, either $(\phi(X(x)))_r = (\phi(X'(x)))_r$ or $(\phi(X(x)))_r = a_t$ and $(\phi(X'(x)))_r = a'_t$, by Lemma 6.2.1 and the trivial automorphism group of S.

But if $n > 2$, we can find values of x that contradict this, so we must conclude that $A_i \subset A'_i$. Reversing the roles of $X(x)$ and $X'(x)$, we can show $A_i \subset A'_i$. So $A_i = A'_i$, and A_i is independent of the choice of the values a_r, $r \neq i$.

We next show that $|A_i| = 1$. Denote the mCS(n) subsystem $\{(x_1, \ldots, x_v) : x_j = a_j, j \neq i, x_i \in [n]\}$ by $P_i(a_1, \ldots, a_v)$, and set

$$\mathcal{P}_i = \{P_i(a_1, \ldots, a_v) : a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_v \in [n]\}.$$

Also denote the $m\mathrm{CS}(n)$ subsystem

$$\{(x_1, \ldots, x_v) : x_j = \alpha_j, j \notin A_i, x_j = x, j \in A_i, x \in [n]\}$$

by $Q_i(\alpha_1, \ldots, \alpha_v)$, and set

$$\mathcal{Q}_i = \{Q(\alpha_1, \ldots, \alpha_v) : \alpha_1, \ldots, \alpha_v \in [n]\}.$$

The members of $\mathcal{P}_i$ are pairwise disjoint, as are those of $\mathcal{Q}_i$, and ϕ maps each member of $\mathcal{P}_i$ to a member of $\mathcal{Q}_i$. But there are n^{v-1} members of $\mathcal{P}_i$ and $n^{v-|A_i|}$ members of $\mathcal{Q}_i$, so $|A_i| = 1$.

We have proved that for any $1 \leq i \leq v$, there is a $1 \leq j \leq v$ such that for any values $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_v$ in $[n]$, there are values $\alpha_1, \ldots, \alpha_{j-1}, \alpha_{j+1}, \ldots, \alpha_v$ in $[n]$ such that ϕ maps the point $(a_1, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_v)$ of S^v to the point $(\alpha_1, \ldots, \alpha_{j-1}, x, \alpha_{j+1}, \ldots, \alpha_v)$ for each $x \in [n]$. Set $\sigma(i) = j$. The map $i \mapsto \sigma(i)$ is 1-1 because $\sigma(i) = \sigma(i')$ implies that for every $X \in S^v$, $(X)_i = (X)_{i'}$, so $i = i'$. Thus since v is finite, σ is a permutation of $1, 2, \ldots, v$, and the result is proved.

□

6.3 Main construction

We now construct an $m\mathrm{CS}$ with automorphism group isomorphic to that of an arbitrary graph G. If κ is a permutation of $[n]$, then we denote by $\kappa(S)$ the $mCS(n)$ with cycles $(\kappa(x_1), \kappa(x_2), \ldots, \kappa(x_m))$, where each $(x_1, x_2, \ldots, x_m)$ is a cycle of S.

Construction

Given a graph $G = (V, E)$, where $|V| = v$ and $V = \{1, 2, \ldots, v\}$, an $m\mathrm{CS}(n)$ system S, defined on $[n]$, with trivial automorphism group and no proper subsystems, and a non-trivial permutation, κ of $[n]$, define the $m\mathrm{CS}(n^v)$ $U(G, S, \kappa)$ from S^v by, for each edge (i, j) of G, replacing the $m\mathrm{CS}(n)$ subsystem of S^v defined by the set of points $\{X \in S^v : (X)_p = 0, p \neq i, j, (X)_i = (X)_j \in [n]\}$ by the subsystem on the same points which has cycles $(X_1, \ldots, X_m)$ where each cycle $((X_1)_i, (X_2)_i, \ldots, (X_m)_i) = ((X_1)_j, (X_2)_j, \ldots, (X_m)_j)$ is a cycle of $\kappa(S)$.

For any edge (i, j) of G, we shall call a cycle $(X_1, \ldots, X_m)$ with $(X_p)_t = 0$ for $t \neq i, j$ and $(X_p)_i = (X_p)_j$ for all p, an *edge cycle* of $U(G, S, \kappa)$, and all other cycles of $U(G, S, \kappa)$ *non-edge cycles.* We shall call the $m\mathrm{CS}(n)$ system comprising the (i, j) edge cycles for the edge (i, j) of G, the (i, j) *edge subsystem* of $U(G, S, \kappa)$.

It is worth noting that, rather than replacing copies of S by $\kappa(S)$, we could instead have replaced them with an $m\mathrm{CS}(n)$ non-isomorphic to S. This would have the advantage that the corresponding version of Lemma 6.3.3 has a simpler proof, but the disadvantage of needing to find two non-isomorphic $m\mathrm{CS}(n)$, both with trivial automorphism group and without proper subsystems for each m.

We now prove the analogue of Lemma 6.2.1 for $U(G, S, \kappa)$.

Lemma 6.3.1. *Every $mCS(n)$ subsystem of $U(G, S, \kappa)$ consists of the points in which the values of k distinct coordinates $i_1 < i_2 < \cdots < i_k$ are equal for some $1 \leq k \leq v$, and the remainder of the coordinates are constant.*

Proof. Let T be any $mCS(n)$ subsystem of $U(G, S, \kappa)$. If T contains no edge cycles, then the argument of Lemma 6.2.1 can be applied. Otherwise, T contains edge cycles, so T is an edge subsystem of $U(G, S, \kappa)$, because each edge subsystem is isomorphic to S, and so has no proper subsystems. In either case, T is of the

stated form. □

Lemma 6.3.2. *If σ is an automorphism of G, then the map*
$\phi : (x_1, x_2, \ldots, x_v) \mapsto (x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, \ldots, x_{\sigma^{-1}(v)})$ *is an automorphism of* $U(G, S, \kappa)$.

Proof. The map ϕ is one-to-one on $U(G, S, \kappa)$, so it only remains to show that ϕ is a map of cycles of $U(G, S, \kappa)$.

If $(X_1, \ldots, X_m)$ is an (i, j) edge cycle of $U(G, S, \kappa)$, then for each $t \neq i, j$, $(X_r)_t = 0$ for all $r \in \{1, \ldots, m\}$, $(X_r)_i = (X_r)_j$ for all r, and $((X_1)_i, (X_2)_i, \ldots, (X_m)_i) = ((X_1)_j, (X_2)_j, \ldots, (X_m)_j)$ is a cycle of $\kappa(S)$. But since σ is an automorphism of G, $(\sigma(i), \sigma(j))$ is an edge of G, and so $(\phi(X_1), \phi(X_2), \ldots, \phi(X_m))$ is an $(\sigma(i), \sigma(j))$ edge cycle of $U(G, S, \kappa)$ because for each $t \neq i, j$, $(\phi(X_r))_{\sigma(t)} = (X_r)_t = 0$ for all r, and $((\phi(X_1))_{\sigma(i)}, (\phi(X_2))_{\sigma(i)}, \ldots, (\phi(X_m))_{\sigma(i)}) = ((X_1)_i, (X_2)_i, \ldots, (X_m)_i)$ $= ((X_1)_j, (X_2)_j, \ldots, (X_m)_j) = ((\phi(X_1))_{\sigma(j)}, (\phi(X_2))_{\sigma(j)}, \ldots, (\phi(X_m))_{\sigma(j)})$ is a cycle of $\kappa(S)$.

If $(X_1, \ldots, X_m)$ is a non-edge cycle of $U(G, S, \kappa)$, then for each $t \in \{1, \ldots, v\}$, either $(X_r)_t$ is constant for all $r \in \{1, \ldots, m\}$, or $((X_1)_t, (X_2)_t, \ldots, (X_m)_t)$ is a cycle of S. The sequence $(\phi(X_1), \phi(X_2), \ldots, \phi(X_m))$ is then a non-edge cycle of $U(G, S, \kappa)$ because $(\phi(X_r))_{\sigma(t)} = (X_r)_t$, and so $(\phi(X_r))_{\sigma(t)}$ is the same for all $r \in \{1, \ldots, m\}$ if $(X_r)_t$ is the same for all r, and $((\phi(X_1))_{\sigma(t)}, (\phi(X_2))_{\sigma(t)}, \ldots, (\phi(X_m))_{\sigma(t)})$ is a cycle of S if $((X_1)_t, (X_2)_t, \ldots, (X_m)_t)$ is a cycle of S. □

Lemma 6.3.3. *Any automorphism of $U(G, S, \kappa)$ is of the form*

$$(x_1, x_2, \ldots, x_v) \rightarrow (x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, \ldots, x_{\sigma^{-1}(v)})$$

for some permutation σ of $\{1, 2, \ldots, v\}$.

Proof. We use the proof of Lemma 6.2.2 as the basis of the proof.

We again prove that for any $1 \leq i \leq v$, there is a $1 \leq j \leq v$ such that for any values $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_v \in [n]$, there are values

$$\alpha_1, \ldots, \alpha_{j-1}, \alpha_{j+1}, \ldots, \alpha_v \in [n]$$

with

$$\phi(a_1, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_v) = (\alpha_1, \ldots, \alpha_{j-1}, x, \alpha_{j+1}, \ldots, \alpha_v)$$

for each $x \in [n]$.

For any choice of i and of values $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_v$, we shall again compare the mapping of the $m\mathrm{CS}(n)$ subsystem

$$\{X(x) : \ (X(x))_s = a_s, s \neq i, \ (X(x))_i = x, \ x \in [n]\}$$

with the mapping of the subsystem $\{X'(x) : x \in [n]\}$ obtained by changing any one of the values a_t, $t \neq i$, to any different value a'_t, to show that the images of these subsystems are also mutually parallel.

We again denote the set of coordinates whose values are not constant in $\{\phi(X(x)) : x \in [n]\}$ by A_i, and the corresponding set for $\{\phi(X'(x)) : x \in [n]\}$ by A'_i.

There are several extra cases to consider. Using the same terms as in the proof of Lemma 6.2.2, we have to additionally consider the possibility that either of the $m\mathrm{CS}(n)$ subsystems $\{X(x) : x \in [n]\}$ and $\{X'(x) : x \in [n]\}$ may be mapped to edge subsystems of $U(G, S, \kappa)$ by the automorphism ϕ.

If $\{\phi(X(x)) : x \in [n]\}$ is the edge subsystem for an edge (e, e') of G, then $\phi(X(x)) = Y(y)$ where $(Y(y))_s = 0$, $s \neq e, e'$ and $(Y(y))_e = (Y(y))_{e'} = y$.

Then $y = \kappa(x)$ for all x, since the mapping $x \mapsto X(x) \mapsto \phi(X(x)) \mapsto y$ is an isomorphism from S to $\kappa(S)$, which must be κ since S, and therefore also $\kappa(S)$, has trivial automorphism group.

If $r \in A_i \setminus A_i'$. Then $(\phi(X(x)))_r$ takes a different value for each value of x, and $(\phi(X'(x)))_r$ is constant. Also, for any given value of x, $X(x)$ and $X'(x)$ are in the same crossing subsystem, and accordingly, either $(\phi(X(x)))_r = (\phi(X'(x)))_r$ or $(\phi(X(x)))_r = a_t$ and $(\phi(X'(x)))_r = a_t'$ if the crossing subsystem is a non-edge subsystem, and $(\phi(X(x)))_r = \kappa(a_t)$ and $(\phi(X'(x)))_r = \kappa(a_t')$ if the crossing subsystem is an edge subsystem. But since $n > 2$, we can find values of x to contradict this, so $A_i \subset A_i'$. By exchanging $X(x)$ and $X'(x)$ in the argument we also show that $A_i' \subset A_i$, so $A_i = A_i'$.

The same argument as was used in Lemma 6.2.2 then shows that $|A_i| = 1$, and that, if $A_i = \{j\}$, then the mapping $\sigma(i) = j$ provides the required permutation.

□

Lemma 6.3.4. *If ϕ is an automorphism of $U(G, S, \kappa)$, then it is of the form $\phi : (x_1, x_2, \ldots, x_v) \mapsto (x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, \ldots, x_{\sigma^{-1}(v)})$, where σ is an automorphism of G.*

Proof. By Lemma 6.3.3 there exists a permutation σ of V such that $\phi(x_1, x_2, \ldots, x_v) = (x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, \ldots, x_{\sigma^{-1}(v)})$ for every point $(x_1, \ldots, x_v)$ in $U(G, S, \kappa)$. We show that σ is an automorphism of G.

Let (i, j) be any edge of G. We have to prove that $(\sigma(i), \sigma(j))$ is also an edge of G. As an mCS(n) subsystem of $U(G, S, \kappa)$ has no proper subsystems, no two such subsystems share a cycle. Since S has trivial automorphism group, there is a cycle $(x_1, x_2, \ldots, x_m)$ of $\kappa(S)$ that is not a cycle of S. Define the (i, j) edge cycle $(X_1, X_2, \ldots, X_m)$ of U by $(X_r)_s = 0$, $s \neq i, j$, and $(X_r)_i = (X_r)_j = x_r$

for $r = 1, 2, \ldots, m$. Then the image $(\phi(X_1), \phi(X_2), \ldots, \phi(X_m))$ in ϕ is a cycle of U, and $(\phi(X_r))_s = 0$, $s \neq \sigma(i), \sigma(j)$, and $(\phi(X_r))_{\sigma(i)} = (\phi(X_r))_{\sigma(j)} = x_r$ for $r = 1, 2, \ldots, m$.

But since $(x_1, x_2, \ldots, x_m)$ is a cycle of $\kappa(S)$ but not of S, $(\phi(X_1), \phi(X_2), \ldots, \phi(X_m))$ is an edge cycle of U, so $(\sigma(i), \sigma(j))$ is an edge of G. □

Theorem 6.3.1. *The automorphism group of $U(G, S, \kappa)$ is isomorphic to the automorphism group of G.*

Proof. Lemmas 6.3.2, 6.3.3 and 6.3.4 have established a one-to-one correspondence between the automorphisms of $U(G, S, \kappa)$ and the automorphisms of G. We have to show that this correspondence is a group isomorphism. Let σ_1, σ_2 be automorphisms of G, and let ϕ_1, ϕ_2 be the corresponding automorphisms of $U(G, S, \kappa)$, i.e. for all $X \in U(G, S, \kappa)$, $(\phi_1(X))_j = (X)_{\sigma_1^{-1}(j)}$ and $(\phi_2(X))_j = (X)_{\sigma_2^{-1}(j)}$ for $j = 1, 2 \ldots, v$.

Then $(\phi_1(\phi_2(X)))_j = (\phi_2(X))_{\sigma_1^{-1}(j)} = (X)_{\sigma_2^{-1}(\sigma_1^{-1}(j))} = (X)_{(\sigma_1\sigma_2)^{-1}(j)}$ for all $X \in U(G, S, \kappa)$, $j = 1, 2 \ldots, v$.

Hence, since the identity on G corresponds to the identity on $U(G, S, \kappa)$, our correspondence is an isomorphism of groups. □

6.4 Construction of mCS with trivial automorphism group and no proper subsystems

In this section we address constructions for the the mCS(n) systems S needed to construct $U(G, S, \kappa)$. It is clearly desirable for our purpose of constructing mCS with given automorphism group, that we should build $U(G, S, \kappa)$ of minimal order

n^v for any given m by selecting n as small as possible. For odd $m \geq 9$, we could almost certainly choose $n = m$. However, in this thesis, it has been decided to present a construction for $mCS(2m+1)$ with the requisite properties. For the case $m = 9$, a $9CS(9)$ example has also been included.

6.4.1 An mCS$(2m+1)$ with trivial automorphism group for $m \geq 9$

We again utilise Lemma 5.3.4 and prove the counterpart of Construction 2 in Chapter 5 for cycles of odd length. Recall that the basic cycle B, which is developed (mod $2m+1$), is defined by $B = (b_1, b_2, \ldots, b_m)$

$$\begin{aligned} b_i &= i(-1)^{i+1} \quad for \quad i < \tfrac{m}{2} \\ &= i(-1)^i \quad for \quad i \geq \tfrac{m}{2}. \end{aligned}$$

We shall again use the convention that positions in cycles are labelled 1 to m, but cycles labelled 0 to $2m$. Cycle B is referred to as cycle 0. We refer to this unmodified system as S.

Construction 2′

We consider the cases $m = 4t+1$, and $4t+3$, $t \geq 2$ separately.

For $m = 4t+1$, the point at position $2t+2$ in cycle 0 is exchanged with the point at position $4t-1$ in cycle $2t+2$.

For $m = 4t+3$, the point at position $2t+4$ is exchanged with the point at position $4t+1$ in cycle $2t+2$.

We shall refer to the modified system as S'.

Lemma 6.4.1. *The modified system S' is an $mCS(2m+1)$.*

Proof. We consider the case $m = 4t + 1$ first. Arithmetic is modulo $8t + 3$. Cycle 0 of S is:

$$(1, -2, 3, \ldots, (2t-1), -2t, -(2t+1), (2t+2), -(2t+3), 2t+4, -(2t+1), \ldots, 4t, -(4t+1))$$

with the point $(2t + 2)$ at position $2t + 2$). Cycle $2t + 2$ is therefore:

$$(2t + 3, 2t, \ldots, -(2t - 5), -(2t + 3), -(2t - 3), -(2t + 1), -(2t - 1))$$

with the point $-(2t - 3)$ at position $4t - 1$. Since the points to be exchanged both have the same neighbours, no edges are added or destroyed. We check that no point is duplicated in a cycle by the exchange. Point $-(2t - 3)$ is not already in cycle zero, because $(2t - 3)$ is. The point $2t + 2$ cannot be present in cycle $2t + 2$ because otherwise cycle 0 would contain 0. Thus there is no duplication of points, and S' is an $mCS(2m + 1)$.

We next consider the case $m = 4t + 3$. Arithmetic is modulo $8t + 7$. Cycle 0 of S is:

$$(1, -2, 3, \ldots, -2t, (2t+1), (2t+2), -(2t+3), (2t + 4), -(2t+5), 2t+6, \ldots, -(4t+3))$$

where the point $(2t + 4)$ is at position $2t + 4$. So cycle $2t + 2$ is

$$(2t + 3, 2t, \ldots, -(2t - 3), -(2t + 5), -(2t - 1), -(2t + 3), -(2t + 1))$$

with the point $-(2t - 1)$ at position $4t + 1$. The points which are to be exchanged have the same neighbours, so no edges are added or deleted. The point $-(2t - 1)$ is not already present in the 0^{th} cycle because $2t - 1$ occupies position $2t - 1$

in that cycle. The point $2t+4$ is not already present in cycle $2t+2$ because otherwise cycle zero would contain 2. Therefore S' is an $mCS(2m+1)$. □

Lemma 6.4.2. *The $mCS(2m+1)$ S' given by Construction 2' has no proper subsystems.*

Proof. This proceeds in exactly the same way as Lemma 5.3.6. □

Recall that we call a pair of alternate points in a cycle an *alternate pair*, and that we show alternate pairs in square brackets, viz. $[a,b]$. In preparation for examining the automorphism group, we calculate the frequency of occurrence of each alternate pair as in Chapter 5.

Firstly, we take $m = 4t+1$ and $t \geq 2$. The 0^{th} cycle of S is:
$(1,-2,3,\ldots,(2t-1),-2t,-(2t+1),(2t+2),-(2t+3),2t+4,\ldots,-(4t-1),$
$4t,-(4t+1))$.
Cycle $2t+2$ is
$(2t+3,2t,\ldots,4t+1,2,1,-(4t-1),\ldots,-(2t-5),-(2t+3),-(2t-3),$
$-(2t+1),-(2t-1))$,
where all points are (mod $8t+3$).

Apart from the alternate pairs $[4t,1]$, $[-(4t+1),-2]$, $[(2t-1),-(2t+1)]$, $[-2t,(2t+2)]$, all alternate pairs have difference 2. So in a single cycle of S, there are $4t-3$ alternate pairs with difference 2, two with difference $4t-1$, one with difference $4t$ and one with difference $4t+2$. Each pair with difference 2 has frequency $4t-3$.

We now examine the alternate pairs in S'.

i) In cycle 0, the pair $[-2t,2t+2]$ is replaced with $[-2t,-(2t-3)]$, and the pair $[2t+2,2t+4]$ is replaced with $[-(2t-3),2t+4]$. The replacement pairs have difference of 3 and $4t+1$.

ii) In cycle $2t+2$, the pair $[-(2t-5), -(2t-3)]$ is replaced with $[-(2t-5), 2t+2]$, and the pair $[-(2t-3), -(2t-1))]$ is replaced with $[2t+2, -(2t-1))]$. The replacement pairs have differences $4t-3$ and $4t+1$.

Therefore, in S', the pairs $[2t+2, 2t+4]$, $[-(2t-5), -(2t-3)]$, and $[-(2t-3), -(2t-1))]$ have frequency $4t-4 > 3$. All other pairs with difference 2 have frequency $4t-3$, and no other pair has frequency greater than two.

We do the same for the case $m = 4t+3$, $t \geq 2$. Cycle 0 of S is:

$(1, -2, 3, \ldots, -2t, 2t+1, 2t+2, -(2t+3), 2t+4, -(2t+5), 2t+6, \ldots,$

$-(4t+1), 4t+2, -(4t+3))$

where the point to be exchanged, $2t+4$ is at position $2t+4$.

Cycle $2t+2$ is

$(2t+3, 2t, \ldots, 4t+1, 2, 4t+3, -(4t+3), -1, \ldots, -(2t-3), -(2t+5), -(2t-1),$

$-(2t+3), -(2t+1)),$

where the point $-(2t-1)$ at position $4t+1$ is to be exchanged with the point $2t+4$ in cycle 0. Arithmetic is modulo $8t+7$.

The alternate pairs in cycle 0 with difference other than 2 are $[-2t, 2t+2]$, $[2t+1, -(2t+3)]$, $[4t+2, 1]$, and $[-(4t+3)), -2]$. A single cycle of S contains $4t-1$ pairs with difference 2, one pair with difference $4t+2$, two with difference $4t+1$, and one with difference $4t+3$ in S.

In S', the frequencies are modified in the following way.

i) For cycle 0, the pair $[2t+2, 2t+4]$ is replaced by $[2t+2, -(2t-1)]$ and $[2t+4, 2t+6]$ by $[-(2t-1), 2t+6]$.

ii) In cycle $2t+2$, $[-(2t-3), -(2t-1)]$ is replaced by $[-(2t-3), 2t+4]$ and $[-(2t-1), -(2t+1)]$ by $[2t+4, -(2t+1)]$.

Of the replacement pairs, two have difference $4t+1$ and two have difference $4t+2$. In S' the pairs $[2t+2, 2t+4]$, $[2t+4, 2t+6]$, $[-(2t-3), -(2t-1)]$ and $[-(2t-1), -(2t+1)]$ therefore occur with frequency $4t-2 \geq 6$. Other pairs with difference 2 have frequency $4t-1$, and no other pair has frequency greater than 4.

We now have the means to prove the triviality of the automorphism group of S'.

Lemma 6.4.3. *The $mCS(2m+1)$ S' obtained by Construction 2' has trivial automorphism group.*

Proof. We know by Lemma 5.2.2 that the fixed points of any automorphism of S' form a subsystem, and since by Lemma 6.4.2 S' has no proper subsystems, no automorphism other than the identity has more than one fixed point.

In the case $m = 4t+1$, $t \geq 2$, the alternate pairs with unique frequency of occurrence in S' are $[2t+2, 2t+4]$, $[-(2t-5), -(2t-3)]$ and $[-(2t-3), -(2t-1)]$. An automorphism of S' must either preserve or permute these pairs of points. Two pairs share the point $-(2t-3)$, so this is fixed by any automorphism, and if it is not the identity, it must exchange $2t+2$ with $2t+4$ and $-(2t-5)$ with $-(2t-1)$.

Cycle $2t+4$ contains the sequence $-(2t-5), -(2t-1), -(2t-3), 2t+5, 2t+2$, starting at the $4t-1^{th}$ position. This cycle does not contain the point $2t+4$ because otherwise the 0^{th} cycle would contain 0. This is the unique cycle containing the edge $-(2t-5), -(2t-1)$, so the cycle is preserved by any automorphism, and a non-trivial automorphism must exchange them, reversing the cycle. But then $-(2t-3)$ would not be fixed. Thus the only automorphism of S' is the identity.

For the case $m = 4t+3$, the pairs that occur a unique number of times in S'

are $[2t+2, 2t+4]$, $[2t+4, 2t+6]$, $[-(2t-3), -(2t-1)]$ and $[-(2t-1), -(2t+1)]$. Therefore any automorphism must either preserve of permute these pairs. Since two share the point $2t+4$ and the others share the point $-(2t-1)$, any automorphism that is not the identity exchanges these points, and either exchanges $2t+2$ with $-(2t-3)$ and $2t+6$ with $-(2t+1)$, or exchanges $2t+2$ with $-(2t+1)$ and $2t+6$ with $-(2t-3)$.

The $6t+7^{th}$ cycle contains the sequence

$$2t+6, 2t+2, 2t+4, -(2t-1), -(2t+2), -(2t-3),$$

starting at the $4t+1^{th}$ position. The cycle does not contain the point $-(2t+1)$, because otherwise cycle zero would contain -1. Since this is the unique cycle containing the edge $(2t+4, -(2t-1))$, a non-trivial automorphism preserves the cycle and transposes this edge. But then $2t+2$ would be exchanged with $-(2t+2)$, contrary to the previous deduction. Therefore the only automorphism is the identity.

□

6.4.2 An mCS(n) with trivial automorphism group for $m = 5, 7$

This section deals with the remaining cases.

A 5CS(11)with trivial automorphism group and no proper subsystems

The following system

$$\begin{array}{lll} (1,-2,-3,4,-4) & (2,-1,-2,5,-4) & (3,0,-1,-5,-3) \\ (4,1,0,-4,-2) & (5,2,1,-3,-1) & (-5,3,2,-2,0) \\ (-5,4,3,-1,1) & (-3,5,4,0,2) & (-2,-5,5,1,3) \\ (-1,-4,-5,2,4) & (0,-3,-4,3,5) & \end{array}$$

is obtained from the construction Lemma 5.3.4 by exchanging the -5 at position 5 in cycle zero with the -4 at position 1 in the 6^{th} cycle. Arithmetic is modulo 11. It is a valid 5CS system because the points exchanged have the same neighbours, i.e. 4 and 1, and also because, after the exchange, neither cycle contains any point more than once.

The new system has no proper subsystems by invoking Lemma 5.3.3, using the same proof as for Lemma 5.3.6 and Lemma 6.4.2, because the new system was obtained from a cyclic system.

We now examine the frequencies of alternate pairs in the system. The alternate pairs in a single cycle of the original system have frequencies $1, 1, 1, 2, 2$, corresponding to 2^{nd} differences $4, 5, 2, 3, 3$. In the new system, the pairs $[-3, -5]$ and $[-5, -2]$ in cycle zero and $[-4, 3]$ and $[-1, -4]$ in cycle 6 are replaced by pairs $[-3, -4]$,$[-4, -2]$,$[-5, 3]$ and $[-1, -5]$. The pair $[-5, -2]$ also occurs in cycle 5. The pair $[-2, -4]$ appears also in cycle 1. The pair $[-5, 3]$ occurs also in cycles 2 and 8, and $[-1, -5]$ occurs as well in cycle 9. Thus the frequencies of occurrence

of alternate pairs in the new system are

$$\begin{array}{lll} 1,2,1,2,2; & 1,1,2,2,2; & 1,1,1,3,2; \\ 1,1,1,2,2; & 1,1,1,2,2; & 1,1,1,1,2; \\ 3,1,1,2,2; & 1,1,1,2,2; & 1,1,1,2,3; \\ 2,1,1,2,2; & 1,1,1,2,2. & \end{array}$$

Only cycles that have the same frequency pattern (allowing for cyclic permutation and reversal) can be mapped to each other by an automorphism of the new system. Cycle six has a unique pattern, and therefore can only be mapped to itself. Further, since the pair $[-5,3]$ has unique frequency in this cycle, an automorphism must either fix or exchange these points. If the points are fixed, then since the system has no proper subsystems, all points are fixed, by Lemma 5.2.2. If the points -5 and 3 are exchanged, then 4 is fixed and 1 and -1 are also exchanged. But cycle 5 is the unique cycle containing the edge $(-5,3)$, so if -5 and 3 are exchanged, the automorphism reverses the cycle, fixing the point -2. Thus at least two points are fixed, and so all points are fixed.

A 7CS(15) with trivial automorphism group and no proper subsystems

We prove that the following system has the required properties.

$$\begin{array}{lll} (1,-2,3,4,-5,-1,-7) & (2,-1,4,5,-4,7,-6) & (3,0,5,6,-3,-7,-5) \\ (4,1,6,7,-2,-6,-4) & (5,2,7,-7,6,-5,-3) & (6,3,-7,-6,0,-4,-2) \\ (7,4,-6,-5,1,-3,-1) & (-7,5,-5,-4,2,-2,0) & (-6,6,-4,-3,3,-1,1) \\ (-5,7,-3,-2,4,0,2) & (-4,-7,-2,-1,5,1,3) & (-3,-6,-1,0,6,2,4) \\ (-2,-5,0,1,7,3,5) & (-1,-4,1,2,-7,4,6) & (0,-3,2,3,-6,5,7). \end{array}$$

This was obtained from a cyclic system by switching the 6 in cycle zero with the -1 in cycle four. It is a 7CS because the points exchanged have the same neighbours, -5 and -7. The system is shown to have no proper subsystems again by the same proof as for Lemma 5.3.6 and Lemma 6.4.2.

Now we show that it has trivial automorphism group. Before the switch, each cycle has the same pattern of frequencies of occurrence, which is $3, 1, 1, 3, 3, 2, 2$, corresponding to 2^{nd} differences $2, 6, 7, 2, 2, 5, 5$. The switch of points causes the alternate pairs $[4, 6]$, $[6, 1]$ to be destroyed in cycle zero, and pairs $[7, -1]$ and $[-1, 3]$ destroyed in cycle four, to be replaced by the pairs and the pairs $[4, -1]$, $[-1, 1]$, $[7, 6]$ and$[6, -3]$. Of the altered pairs:

i) $[4, 6]$ is also in cycles 3 and 11,

ii) $[6, 1]$ is also in cycle 8,

iii) $[-1, -3]$ is also in cycles 8 and 11,

iv) $[4, -1]$ is also in cycles 6 and 13,

v) $[1, -1]$ is also in cycles 6,10, and 13,

vi) $[6, -3]$ is also in cycle 8.

Pairs $[7, -1]$ and $[7, 6]$ are in no other cycles. This results in the new frequency patterns:

$3, 1, 1, 3, 3, 4, 2$	$3, 1, 1, 3, 3, 2, 2$	$3, 1, 1, 3, 3, 2, 2$
$2, 1, 1, 3, 3, 2, 2$	$3, 1, 1, 3, 2, 2, 2$	$3, 1, 1, 3, 3, 2, 2$
$3, 1, 1, 3, 4, 2, 3$	$3, 1, 1, 3, 3, 2, 2$	$3, 2, 1, 2, 3, 2, 1$
$3, 1, 1, 3, 3, 2, 2$	$3, 1, 1, 4, 3, 2, 2$	$2, 1, 1, 3, 2, 2, 2$
$3, 1, 1, 3, 3, 2, 2$	$4, 1, 1, 3, 3, 3, 2$	$3, 1, 1, 3, 3, 2, 2.$

We note that the frequency pattern for cycle zero is unique in the sense that no cyclic permutation the pattern nor its reverse matches any of the other patterns. Therefore, any automorphism of the system must map this cycle to itself. Also, this pattern does not match any cyclic permutation of itself or its reverse, so in fact any automorphism fixes all points in this cycle. Therefore, since more than one point is fixed, we deduce by Lemma 5.2.2 that the system has trivial automorphism group.

6.4.3 A 9CS(9) with trivial automorphism group

The previous constructions have concerned $m\mathrm{CS}(2m+1)$. This example is provided to illustrate that $m\mathrm{CS}(m)$ with the right properties certainly exist for $m \geq 9$. We start by constructing $9CS(9)$ from the basic cycle $(0, 1, -1, 2, -2, 3, -3, 4, \infty)$ The differences between consecutive numerical points cover all the differences (mod 8) except 4 twice, and the latter difference once. When developed cyclicly (mod 8), leaving the infinity point fixed, this gives a $9CS(9)$ with an automorphism group of order 8.

$$(0,1,-1,2,-2,3,-3,4,\infty) \qquad (1,2,0,3,-1,4,-2,-3,\infty)$$
$$(2,3,1,4,0,-3,-1,-2,\infty) \qquad (3,4,2,-3,1,-2,0,-1,\infty).$$

The following 9CS(9)

$$(-1,1,0,-2,2,3,-3,4,\infty) \qquad (1,2,0,3,-1,4,-2,-3,\infty)$$
$$(-2,3,1,4,0,-3,-1,2,\infty) \qquad (3,4,2,-3,1,-2,-1,0,\infty).$$

is obtained from the first system by the transpositions $(0,-1)$ and $(2,-2)$ in cycle zero, $(2,-2)$ in cycle two, and $(-1,0)$ in cycle three. The first two transpositions

cause the loss of edges $(0,\infty)$, $(-1,2)$ and $(-2,3)$ and the gain of edges $(-1,\infty)$, $(0,-2)$ and $(2,3)$ in cycle zero. In cycle two, the transposition causes the loss of edges $((-1,-2)$ and $(2,3)$, and the gain of edges $(-1,2)$ and $(-2,3)$. In cycle three, the transposition $(-1,0)$ results in the loss of edges $(-1,\infty)$ and $(-2,0)$ and the gain of edges $(0,\infty)$ and $(-2,-1)$. Since every edge lost in one cycle is gain gained back in another cycle, the new set of cycles is also a 9CS(9). We now prove that this new system has no automorphisms other than the identity. The alternate pairs $[-1,0]$, $[3,4]$, and $[-3,4]$ all occur with frequency 3, whereas all others have frequency 2 or less. By Lemma 5.2.2 the fixed points of an automorphism form a subsystem, and since a 9CS(9) can have no proper subsystems, a non-trivial automorphism can fix no more than one point. Since 4 occurs in two of these pairs, it must be fixed by every automorphism, and 3 and -3 must be switched by a non-trivial automorphism. The sequence $3,-3,4,\ldots$ in cycle zero must be mapped to $-3,3,4,\ldots$. Since this sequence does not occur in any cycle, the system has trivial automorphism group.

6.5 Main result

Theorem 6.5.1. *If Γ is any abstract group, $|\Gamma| = \gamma$, then for any odd $m \geq 3$, there exists an mCS with full automorphism group isomporphic to Γ. For $m \geq 5$, the order of this mCS is of order no greater than $(2m+1)^{2\gamma log_2 \gamma}$ if Γ is non-cyclic, and $(2m+1)^{3\gamma}$ otherwise.*

Proof. for $m = 3$ this is covered by Mendelsohn's result [16]. In Theorem 6.3.1 it was shown that for any graph $G = (V, E)$, and given an mCS(n), m odd, with suitable properties, there exists a mCS($n^{|V|}$) that has full automorphism group isomorphic to that of G. Frucht, in [9] and [10] has shown that if a minimal

generator set for Γ is of size ν, then there is a graph G with full automorphism group isomorphic to Γ which has $2\gamma\nu$ vertices if Γ is non-cyclic and 3γ otherwise. We know that $\nu \leq log_2\gamma$ for any group, since the group $(Z_2)^\nu$ is the smallest group with ν generators. Finally, the results of Section 6.4 have shown that for $m \geq 5$ we may assume $n = 2m + 1$. These individual results establish what was to be proved.

□

The author is sure that for $m \geq 9$ we can substitute we $n = m$ in the above result, although the construction necessary to prove this has not been completed.

Chapter 7

Decompositions of Steiner triple systems into triangles

7.1 Introduction

This chapter is concerned with the decomposition of the sets of triples of a Steiner triple system into configurations. A *configuration* is simply a partial triple system, but the terminology is generally used for partial triple systems having a fixed small number of triples. A fundamental question then is, given a configuration C, whether the blocks of an STS(v) can be decomposed into copies of C. Strictly speaking this implies that if C is a configuration containing n triples, then n divides b, the number of blocks of the STS(v). However it is usual to extend the definition to include the situation where the decomposition includes all but a remainder of fewer than n blocks. This extended definition is the one used here. There are two 2-block and five 3-block configurations which can occur in a Steiner triple system. Complete or nearly complete results for the decomposition of both 2-block configurations and three of the 3-block configurations are known

[12]. But the 3-block configuration of greatest interest is the triangle (three triples isomorphic to $\{a, z, b\}, \{b, x, c\}, \{c, y, a\}$). It was Füredi who first asked whether, if the number of triples in a Steiner triple system is divisible by three, the blocks can be decomposed into triangles. The problem is very much an open one. The best that is known is an existential result:

Theorem 7.1.1. *[17] For every $v \equiv 1$ or 3 (mod 6) there exists an STS(v) decomposable into triangles.*

Apart from this the only other results that appear to be known are that every STS(v), $v \leq 15$ is decomposable into triangles, and that when $v \equiv 1$ or 19 (mod 72), the number of STS(v) decomposable into triangles tends to infinity with v [12]. Information about decomposition of Steiner triple systems into configurations can also be found in chapter 13 of [8], and in [11].

We first present four general results on decomposition into triangles. We shall prove:

Theorem 7.1.2. *The STS which is obtained by the Bose construction on any Abelian group of odd order is decomposable into triangles.*

Theorem 7.1.3. *The STS(3v) which is obtained by the Bose construction on any STS(v) is decomposable into triangles.*

Theorem 7.1.4. *If any STS(v) has a decomposition into triangles, then so does the STS(2v + 1) formed from it by applying the doubling construction.*

Theorem 7.1.5. *The STS(3v) which is constructed from any STS(v) by the tripling construction is decomposable into triangles.*

The first and third of these results together solve three quarters of the existence problem directly, leaving only the case $v \equiv 1$ (mod 12).

As noted above, a result of [12] is the closest approach to an enumeration of STS(v) that are decomposable into triangles. The number of STS(v) is known to be $v^{v^2(\frac{1}{6}-o(1))}$ [2]. In the final section of this chapter we shall prove:

Theorem 7.1.6. *The number of STS(v) that are decomposable into triangles is at least* $v^{v^2(\frac{1}{54}-o(1))}$.

We prove these results in the following sections.

7.2 Bose construction on Abelian groups of odd order

In this section we prove Theorem 7.1.2. The notation for the Bose construction from Chapters 2 and 3 will be used. We shall first prove the theorem for cyclic groups, then extend it to all odd-order Abelian groups.

We first state the following decomposition of the non-vertical blocks, which is applicable for any Abelian group of odd order. We define an *inverse-free set*, Δ, for G to be a subset of $G \setminus \{0\}$ containing exactly one of $\pm x$ for each $x \in G \setminus \{0\}$. We define the *difference* for the non-vertical block $\{(x,i),(y,i),(z,i+1)\}$, where $x, y \in G$, $z = (x+y)/2$, $i \in Z_3$, to be whichever of $x-y$ or $y-x$ is in Δ.

The set of triangles:

$$\begin{aligned} &\{(g+\delta,1), \quad (g+2\delta,0), \quad (g,0)\} \\ &\{(g,0), \quad (g+\delta,2), \quad (g-\delta,2)\} \\ &\{(g-\delta,2), \quad (g-3\delta,1), \quad (g+\delta,1)\}, \end{aligned}$$

$\forall g \in G$, $\delta \in \Delta$, contains each non-vertical block of the STS once. Observe that two of the blocks in each triangle have the same difference. That difference

is 2δ, and the third block has a difference 4δ. This partitions the non-vertical blocks because multiplication by two is always an isomorphism in an Abelian group of odd order. We shall use the notation $T(\delta, g)$ to refer to triangles of the above form. This is the basis for all the decompositions into triangles in this section. Our approach will be to select one triangle $T(\delta, g)$ for each vertical block, replacing one block of each triangle by a vertical block in such a way that the displaced blocks can themselves be made into triangles.

7.2.1 Cyclic group case

Lemma 7.2.1. *The Bose STS on a cyclic group of odd order can be decomposed into triangles.*

Proof. Take the cyclic group G to be Z_n for odd n. We set $q = \lfloor n/3 \rfloor$.

Assuming an inverse-free set, Δ for G, we use the above mentioned decomposition of the non-vertical blocks. It remains to incorporate the vertical blocks,$\{(g,0),(g,1),(g,2)\}$, for all $g \in G$ into triangles. We note that the in the triangle $T(\delta, g)$, the last block may be replaced by the vertical block on $(g+\delta)$ to make a different triangle. Our method will be to find parameters δ_1, δ_2, δ_3, g_1, g_2 which define three disjoint series of triangles: $T(\delta_1, g)$, $T(\delta_2, g+g_1)$, $T(\delta_3, g+g_2)$; $g = 0, 1, \ldots, q-1$, such that the sets of three blocks displaced by the incorporation of a vertical block into each triangle will themselves form new triangles.

We shall deal first with the case where n is not divisible by three. For fixed

g, conditions for the three displaced blocks:

$$\begin{array}{ccc} \{(g-\delta_1,2), & (g-3\delta_1,1), & (g+\delta_1,1)\} \\ \{(g+g_1-\delta_2,2), & (g+g_1-3\delta_2,1), & (g+g_1+\delta_2,1)\} \\ \{(g+g_2-\delta_3,2), & (g+g_2-3\delta_3,1), & (g+g_2+\delta_3,1)\} \end{array}$$

to form a triangle are:

$$\begin{aligned} g_1-\delta_2 &= -\delta_1 \\ g_2-3\delta_3 &= -3\delta_1 \\ g_2+\delta_3 &= g_1-3\delta_2, \end{aligned}$$

where arithmetic is modulo n. Further, we set conditions modulo n to make the three series of vertical blocks incorporated into the triangles contiguous and non-overlapping:

$$\begin{aligned} g_1+\delta_2 &= q+\delta_1 \\ g_2+\delta_3 &= 2q+\delta_1 \end{aligned}$$

The above five equations have the solution:

$$\delta_1 = -\tfrac{3q}{4}, \quad \delta_2 = \delta_3 = -\tfrac{q}{4}, \quad g_1 = \tfrac{q}{2}, \quad g_2 = \tfrac{3q}{2}$$

These values are well-defined and non-zero because n is not divisible by 2 or 3. Note that although $\delta_2 = \delta_3$, the two series of triangles $T(\delta_2, g+g_1)$, $T(\delta_3, g+g_2)$; $g = 0, 1 \ldots, q-1$ are disjoint because $g_2 - g_1 = q$.

Therefore, if we choose an inverse-free set Δ which contains the values $-\frac{3q}{4}$ and

$-\frac{q}{4}$, the above process decomposes the Bose STS on G into triangles, except for the vertical block on $\delta_1 + 3q = \frac{9q}{4}$ in the case that $n \equiv 1 \pmod 6$, and the vertical blocks on $\frac{9q}{4}$ and $\frac{9q}{4}+1$ respectively in the case that $n \equiv 5 \pmod 6$. The two series of triangles $T(-\frac{3q}{4}, g)$, $g = 0, 1, \ldots, q-1$, and $T(-\frac{q}{4}, g)$, $g = \frac{q}{2}, \frac{q}{2}+1, \ldots, \frac{5q}{2}-1$ are re-arranged in the decomposition.

In the case that n is divisible by 3, say $n = 6t+3$, we use as inverse-free set $1, 2, \ldots, 3t+1$. Now take the $6t+3$ triangles $T(2t+1, g)$:

$$\begin{aligned} &\{(g+2t+1,1), \quad (g+4t+2,0), \quad (g,0)\} \\ &\{(g,0), \quad (g+2t+1,2), \quad (g+4t+2,2)\} \\ &\{(g+4t+2,2), \quad (g,1), \quad (g+2t+1,1)\}, \end{aligned}$$

$g = 0, 1, \ldots, 6t+2$, and the $6t+3$ vertical blocks, and reassemble them into the $8t+4$ triangles:

$$\begin{aligned} &\{(g+2t+1,1), \quad (g+4t+2,0), \quad (g,0)\} \\ &\{(g,0), \quad (g+2t+1,2), \quad (g+4t+2,2)\} \\ &\{(g+2t+1,0), \quad (g+2t+1,1), \quad (g+2t+1,2)\}, \end{aligned}$$

$g = 0, 1, \ldots, 6t+2$, and

$$\begin{aligned} &\{(g+4t+2,2), \quad (g+2t+1,1), \quad (g,1)\} \\ &\{(g,2), \quad (g+4t+2,1), \quad (g+2t+1,1)\} \\ &\{(g+2t+1,2), \quad (g,1), \quad (g+4t+2,1)\}, \end{aligned}$$

$g = 0, 1, \ldots, 2t$. There are in this case no remainder blocks. This concludes the proof for the case where G is a cyclic group. $\square$

7.2.2 Proof of the main theorem

In order to prove the theorem for all Abelian groups we need some intermediate cases, firstly that in which the group is a product of two factors. There is a complication when the orders of the factors both have residue 5 (mod 6), because the factors each have a decomposition into triangles with two remainder blocks, whereas we require a decomposition into triangles of the product with only one remainder block. This requires a little extra rearrangement of triangles, and is dealt with in Lemma 7.2.3. But first, we prove the simpler case.

Lemma 7.2.2. *If H and K are Abelian groups of odd order such that the Bose STS on each has a decomposition into triangles, and in the case of H the remainder blocks are vertical blocks, then the Bose construction on $H \times K$ has a decomposition into triangles if at least one of $|H|$, $|K|$ has residue not equal to* 5 (mod 6).

Proof. Let $G = H \times K$, where H, K, are Abelian groups of odd order. Assume that $|H| \neq 5 \pmod 6$. Let Δ_H, Δ_K be inverse-free sets for H, K respectively. Then the set:

$$\Delta = \{(\delta, k); \delta \in \Delta_H, k \in K\} \cup \{(0, \delta'); \delta' \in \Delta_K\}$$

is an inverse-free set for G. We can write the set of blocks for the Bose design on

G as the disjoint union $\mathcal{B}_G = \mathcal{B}_1 \cup \mathcal{B}_2 \cup \mathcal{B}_3$, where

$$\begin{aligned}\mathcal{B}_1 = \{\ &\{((h,k),0),\ ((h+\delta,k),2),\ ((h-\delta,k),2)\},\\ &\{((h,k),1),\ ((h+\delta,k),0),\ ((h-\delta,k),0)\},\\ &\{((h,k),2),\ ((h+\delta,k),1),\ ((h-\delta,k),1)\},\\ &\{((h,k),0),\quad ((h,k),1),\quad ((h,k),2)\};\\ &\qquad h\in H,\quad k\in K,\quad \delta\in\Delta_H\ \}\end{aligned}$$

$$\begin{aligned}\mathcal{B}_2 = \{\ &\{((h,k),0),\ ((h+\delta,k+k'),2),\ ((h-\delta,k-k'),2)\},\\ &\{((h,k),1),\ ((h+\delta,k+k'),0),\ ((h-\delta,k-k'),0)\},\\ &\{((h,k),2),\ ((h+\delta,k+k'),1),\ ((h-\delta,k-k'),1)\};\\ &\qquad h\in H,\quad k\in K,\quad \delta\in\Delta_H,\quad k'\in K\setminus\{0\}\ \}\end{aligned}$$

$$\begin{aligned}\mathcal{B}_3 = \{\ &\{((h,k),0),\ ((h,k+\delta'),2),\ ((h,k-\delta'),2)\},\\ &\{((h,k),1),\ ((h,k+\delta'),0),\ ((h,k-\delta'),0)\},\\ &\{((h,k),2),\ ((h,k+\delta'),1),\ ((h,k-\delta'),1)\};\\ &\qquad h\in H,\quad k\in K,\quad \delta'\in\Delta_K\ \}\end{aligned}$$

The set $\mathcal{B}_1$ contains all the blocks where the difference has a zero second coordinate, plus all the vertical blocks. The set $\mathcal{B}_2$ contains all the blocks where the difference is non-zero in both coordinates, and the set $\mathcal{B}_3$ contains all the blocks where the difference is zero in the first coordinate. Now $\mathcal{B}_2$ can be completely decomposed into triangles with no remainder blocks:

$$\begin{aligned}&\{((h,k),0),\quad ((h+\delta,k+k'),2),\quad ((h-\delta,k-k'),2)\},\\ &\{((h+\delta,k+k'),1),\quad ((h+2\delta,k+2k'),0),\quad ((h,k),0)\},\\ &\{((h-\delta,k-k'),2),\quad ((h-3\delta,k-3k'),1),\quad ((h+\delta,k+k'),1)\},\end{aligned}$$

where $h \in H, k \in K, \delta \in \Delta_H, k' \in K \setminus \{0\}$. Also $\mathcal{B}_3$ can be completely decomposed into triangles with no remainder blocks since it is the disjoint union of $|H|$ copies of the non-vertical blocks of the Bose STS on K:

$$\begin{aligned}
\{((h,k),0), \quad ((h,k+\delta'),2), \quad ((h,k-\delta'),2)\},\\
\{((h,k+\delta'),1), \quad ((h,k+2\delta'),0), \quad ((h,k),0)\},\\
\{((h,k-\delta'),2), \quad ((h,k-3\delta'),1), \quad ((h,k+\delta'),1)\},
\end{aligned}$$

where $h \in H, k \in K, \delta' \in \Delta_K$.

Now observe that $\mathcal{B}_1$ is the disjoint union of $|K|$ copies of the Bose STS on H, each of which we can decompose into triangles, such that:

1. if $|H| \equiv 3 \pmod 6$, there are no remainder blocks,

2. if $|H| \equiv 1 \pmod 6$, the set of remainder blocks is of the form

$$\{\ \{((h_1,k),0),\ ((h_1,k),1),\ ((h_1,k),2)\};\ k \in K\ \},$$

for some $h_1 \in H$, corresponding to the one remainder block of the Bose STS on H.

In case 1, the proof is complete. In case 2, the remainder blocks:

$$\{\ \{((h_1,k),0),\ ((h_1,k),1),\ ((h_1,k),2)\}; k \in K\ \},$$

together with the subset:

$$\begin{aligned}
\{((h_1,k),0), \quad ((h_1,k+\delta),2), \quad ((h_1,k-\delta),2)\},\\
\{((h_1,k+\delta),1), \quad ((h_1,k+2\delta),0), \quad ((h_1,k),0)\},\\
\{((h_1,k-\delta),2), \quad ((h_1,k-3\delta),1), \quad ((h_1,k+\delta),1)\},
\end{aligned}$$

$k \in K$, $\delta \in \Delta_K$ of $\mathcal{B}_3$ is a copy of the Bose STS on K, and may be decomposed into triangles, leaving one or two remainder blocks respectively according as $|K| \equiv 1, 5 \pmod 6$.

Finally assume that $|H| \equiv 5 \pmod 6$. Then from the theorem, $|K| \neq 5 \pmod 6$, and we reverse the roles of H and K in the above. This completes the proof. □

The method would leave a remainder of 4 vertical blocks in the case that both $|H|$ and $|K|$ have residue 5 (mod 6). To deal with this case we need an extra device which is provided by the next result, which is for cyclic groups only.

Lemma 7.2.3. *The Bose STS on the product of two cyclic groups each with order congruent to* 5 (mod 6) *can be decomposed into triangles.*

Proof. We repeat and extend the proof of Lemma 7.2.2, using the construction of Lemma 7.2.1, in the case $|H|, |K| \equiv 5 \pmod 6$. The blocks of the Bose STS on $H \times K$ are divided into three subsets $\mathcal{B}_1$, $\mathcal{B}_2$, and $\mathcal{B}_3$ as before. The set of blocks $\mathcal{B}_2$ can be decomposed into a set of triangles which we shall call $\mathcal{T}_2$. We shall postpone specifying the difference set to be used. The set of blocks $\mathcal{B}_3$ can also be decomposed into a set of triangles we shall call $\mathcal{T}_3$. We shall choose that the difference set of $\{0\} \times K$ for that decomposition contains the differences $(0, -\frac{q_K}{4})$ and $(0, -\frac{3q_K}{4})$, where $q_K = \lfloor |K|/3 \rfloor$.

The set $\mathcal{B}_1$ is equivalent to $|K|$ copies of the Bose STS on H. We choose an inverse-free difference set for $H \times \{0\}$ which includes the differences $(-\frac{3q_H}{4}, 0)$ and $(-\frac{q_H}{4}, 0)$, where $q_H = \lfloor |H|/3 \rfloor$, and decompose the non-vertical blocks of each copy of the Bose STS on H into triangles in the standard way. We shall call the resulting set of triangles $\mathcal{T}_1$. We incorporate $3q_H|K|$ vertical blocks into triangles by rearranging the $q_H|K|$ triangles $T((-\frac{3q_H}{4}, 0), (h, k))$, $h = 0, 1, \ldots, q_H - 1$,

$k \in K$, and the $2q_H|K|$ triangles $T((-\frac{q_H}{4}, 0), (h, k))$, $h = \frac{q_H}{2}, \frac{q_H}{2}+1, \ldots, \frac{5q_H}{2}-1$, $k \in K$. This leaves $2|K|$ remainder blocks, which are the vertical blocks on $\{(h_1, k);\ k \in K\}$ and $\{(h_2, k);\ k \in K\}$, where h_1 and h_2 are $\frac{9q_H}{4}$ and $1+\frac{9q_H}{4}$ in some order. We can combine each of these sets with the subsets of $\mathcal{T}_3$ corresponding to h_1, respectively h_2. The two sets of vertical blocks are incorporated by rearranging the $2q_K$ triangles $T((0, -\frac{3q_K}{4}), (h_1, k))$, $T((0, -\frac{3q_K}{4}), (h_2, k))$, $k = 0, 1, \ldots, q_K - 1$, and $4q_K$ triangles $T((0, -\frac{q_K}{4}), (h_1, k))$, $T((0, -\frac{q_K}{4}), (h_2, k))$, $k = \frac{q_K}{2}, \frac{q_K}{2}+1, \ldots, \frac{5q_K}{2}-1$. This leaves four remainder blocks, namely the vertical blocks on (h_1, k_1), (h_2, k_1), (h_1, k_2) and (h_2, k_2), where k_1 and k_2 are $\frac{9q_K}{4}$ and $1+\frac{9q_K}{4}$ in some order. To complete the proof, it remains to incorporate three of these into triangles.

In common with earlier proofs we shall find three triangles from the existing partial decomposition which we shall combine with three of the four above remainder blocks to produce four new triangles and leave just one remainder block. Using the notation of Lemma 7.2.1, a triangle $T(\delta, g)$, where δ and g are elements of $H \times K$, can be combined with the vertical block $\{(g+\delta, 0),\ (g+\delta, 1),\ (g+\delta, 2)\}$, discarding the block $\{(g-\delta, 2),\ (g-3\delta, 1),\ (g+\delta, 1)\}$. We suppose the three starting triangles to be $T(\delta_1, g_1)$, $T(\delta_2, g_2)$, $T(\delta_3, g_3)$, and require them to be combined with the three remainder blocks:

$$\{((h_2, k_2), 0),\ ((h_2, k_2), 1),\ ((h_2, k_2), 2)\},$$
$$\{((h_1, k_1), 0),\ ((h_1, k_1), 1),\ ((h_1, k_1), 2)\},$$
$$\{((h_2, k_1), 0),\ ((h_2, k_1), 1),\ ((h_2, k_1), 2)\}.$$

We may therefore set:

$$\begin{aligned} g_1 + \delta_1 &= (h_2, k_2) \\ g_2 + \delta_2 &= (h_1, k_1) \\ g_3 + \delta_3 &= (h_2, k_1), \end{aligned}$$

and derive conditions for the discarded blocks:

$$\begin{aligned} &\{(g_1 - \delta_1, 2),\ (g_1 - 3\delta_1, 1),\ (g_1 + \delta_1, 1)\} \\ &\{(g_2 - \delta_2, 2),\ (g_2 - 3\delta_2, 1),\ (g_2 + \delta_2, 1)\} \\ &\{(g_3 - \delta_3, 2),\ (g_3 - 3\delta_3, 1),\ (g_3 + \delta_3, 1)\} \end{aligned}$$

to form a triangle. There are several choices. Selecting:

$$\begin{aligned} g_1 - \delta_1 &= g_2 - \delta_2 \\ g_3 - 3\delta_3 &= g_1 + \delta_1 \\ g_3 + \delta_3 &= g_2 - 3\delta_2 \end{aligned}$$

defines the triangle:

$$\begin{aligned} &\{(((h_1 + h_2)/2, k_1), 2),\ ((h_1, 2k_1 - k_2), 1),\ ((h_2, k_2), 1)\} \\ &\{(((h_1 + h_2)/2, k_1), 2),\ ((h_2, k_1), 1),\ ((h_1, k_1), 1)\} \\ &\{((h_2, (k_1 + k_2)/2), 2),\ ((h_2, k_2), 1),\ (h_2, k_1), 1)\}. \end{aligned}$$

This triangle corresponds to the values:

$$\begin{aligned}
\delta_1 &= ((h_2 - h_1)/4, (k_2 - k_1)/2), & g_1 &= ((3h_2 + h_1)/4, (k_2 + k_1)/2) \\
\delta_2 &= ((h_1 - h_2)/4, 0), & g_2 &= ((h_2 + 3h_1)/4, k_1) \\
\delta_3 &= (0, (k_1 - k_2)/4), & g_3 &= (h_2, (k_2 + 3k_1)/4)
\end{aligned}$$

If $(h_1 - h_2)/4 \in \Delta_H$, then $T(\delta_2, g_2)$ is in $\mathcal{T}_1$, but if this not the case then we can merely exchange h_1 and h_2 in our defining equations. Similarly we can ensure that $T(\delta_3, g_3)$ is in $\mathcal{T}_3$ by exchanging k_1 and k_2 if necessary. We can ensure that $T(\delta_1, g_1)$ is in $\mathcal{T}_2$, because, we have not so far used re-used any triangles from $\mathcal{T}_2$, and can we choose any inverse-free set for the blocks $\mathcal{T}_2$ which includes δ_1.

Thus it is possible to ensure that the three triangles are in $\mathcal{T}_2$, $\mathcal{T}_1$ and $\mathcal{T}_3$ respectively. However it is still necessary to check that $T(\delta_2, g_2)$ was not among the $q_H|K|$ triangles $T((-\frac{3q_H}{4}, 0), (h, k))$, $h = 0, 1, \ldots, q_H - 1$, $k \in K$, or the $2q_H|K|$ triangles $T((-\frac{q_H}{4}, 0), (h, k))$, $h = \frac{q_H}{2}, \frac{q_H}{2} + 1, \ldots, \frac{5q_H}{2} - 1$, $k \in K$ which were rearranged earlier in the decomposition of $\mathcal{B}_1$, and that $T(\delta_3, g_3)$ was not among the $2q_K$ triangles $T((0, -\frac{3q_K}{4}), (h_1, k))$,
$T((0, -\frac{3q_K}{4}), (h_2, k))$, $k = 0, 1, \ldots, q_K - 1$, and $4q_K$ triangles
$T((0, -\frac{q_K}{4}), (h_1, k))$, $T((0, -\frac{q_K}{4}), (h_2, k))$, $k = \frac{q_K}{2}, \frac{q_K}{2} + 1, \ldots, \frac{5q_K}{2} - 1$ of $\mathcal{T}_3$ which were also rearranged.

The two cases are similar. Taking $h_1, h_2 = \frac{9q_H}{4}, \frac{9q_H}{4} + 1$ in some order, we have that δ_2 is $(\pm 1/4, 0)$. If $|H| = 6t + 5$, then $-\frac{3q_H}{4} = 1/2$ can never equal either value, as $|H|$ is not divisible by 3. The condition for $-\frac{q_H}{4}$ to equal δ_2 is $\pm 1/4 = t + 1 \pmod{6t + 5}$, which only occurs when $t = 0$, i.e. $|H| = 5$. Similarly, δ_3 is never equal to $(0, -\frac{3q_K}{4})$, but $\delta_3 = (0, -\frac{q_K}{4})$ if $|K| = 5$. We have therefore to check the cases $|H| = 5$ and $|K| = 5$ further.

If $|H|| = 5$, then $-\frac{3q_H}{4} = 3$, and $-\frac{q_H}{4} = 1$, and we have to choose $h_1 = 9/4 = 1$ and $h_2 = 9/4 + 1 = 2$. So $\delta_2 = (1, 0)$ and $g_2 = (0, k_1)$. The rearranged triangles of $\mathcal{T}_1$ of interest are $T((3, 0), (0, k))$, $T((1, 0), (3, k))$ and $T((1, 0), (4, k))$, $k \in K$. Thus $T(\delta_2, g_2)$ is $T((1, 0), (0, k_1))$, which is not one of the rearranged triangles. Similarly, if $|K| = 5$, $T(\delta_3, g_3)$ has not previously been rearranged. This concludes the proof.

□

Lemmas 7.2.2 and 7.2.3 are now readily be combined to produce the general result:

Proof of Theorem 7.1.2. The group can be expressed as a product of cyclic factors. We are at liberty to choose the order of the factors, and choose to group all the factors with order residue 5 (mod 6) together, and further group them into pairs, with possibly one unpaired factor of order residue 5 (mod 6). Considering each pair as a single factor, the whole group is now written as a product where all but possibly one of the factors has order 1 or 3 (mod 6), and for each of which we have demonstrated a decomposition into triangles for the corresponding Bose STS, by Lemmas 7.2.1 and 7.2.3. Furthermore each of these decompositions satisfies the additional condition for Lemma 7.2.2, that any remainder blocks should be vertical blocks, and so by Lemma 7.2.2 and induction on the number of factors there is a decomposition into triangles for the Bose STS on the whole group. □

7.3 Bose construction on Steiner triple systems

The *Bose construction on Steiner triple systems* produces a new STS on $3v$ points from any STS on v points. Assume $(V, \mathcal{B})$ is the original STS, and $(V', \mathcal{B}')$ is the

new STS, then

$V' = \{(a,0),(a,1),(a,2); a \in V\}$, and

$\mathcal{B}' = \{\ \{(a,0),(a,1),(a,2)\};\ a \in V\} \cup$

$\{\ \{(a,i),(b,i),(c,i+1)\},\ \{(b,i),(c,i),(a,i+1)\},\ \{(c,i),(a,i),(b,i+1)\};$

$\{a,b,c\} \in \mathcal{B};\ i \in Z_3\}$.

It is conventional to refer to the first part of $\mathcal{B}'$ as the *vertical blocks* of $\mathcal{B}'$, and the second as the *non-vertical blocks.* Recall that in this and subsequent sections triangles are written in rows.

Proof of Theorem 7.1.3. Firstly decompose the non-vertical blocks of $\mathcal{B}'$ into triangles as:

$$\begin{array}{lll}
\{(a,1),(b,0),(c,0)\} & \{(b,0),(c,2),(a,2)\} & \{(c,2),(a,1),(b,1)\}, \\
\{(b,1),(c,0).(a,0)\} & \{(c,0),(a,2),(b,2)\} & \{(a,2),(b,1),(c,1)\}, \\
\{(c,1),(a,0),(b,0)\} & \{(a,0),(b,2),(c,2)\} & \{(b,2),(c,1),(a,1)\},
\end{array}$$

for each block $\{a,b,c\} \in \mathcal{B}$. The vertical blocks of $(V',\mathcal{B}')$ must be incorporated into triangles by modification of some of the above. A *partial parallel class* of $\mathcal{B}$ is a subset of $\mathcal{B}$ which contains no point of V more than once. Select any maximal partial parallel class of the STS(v), and divide the points of the STS(v) into those which are covered by the partial parallel class and those which are not. For each block, $\{a,b,c\}$ of that class, we take the three corresponding triangles from the non-vertical blocks, together with the three corresponding vertical blocks: $\{(a,0),(a,1),(a,2)\}$, $\{(b,0),(b,1),(b,2)\}$, $\{(c,0),(c,1),(c,2)\}$, and

rearrange them into the four triangles:

$$\begin{array}{lll}
\{(a,0),(a,1),(a,2)\} & \{(b,0),(c,2),(a,2)\} & \{(c,2),(a,1),(b,1)\}, \\
\{(b,1),(c,0),(a,0)\} & \{(c,0),(c,1),(c,2)\} & \{(a,2),(b,1),(c,1)\}, \\
\{(c,1),(a,0),(b,0)\} & \{(a,0),(b,2),(c,2)\} & \{(b,0),(b,1),(b,2)\}, \\
\{(a,1),(b,0),(c,0)\} & \{(c,0),(a,2),(b,2)\} & \{(b,2),(c,1),(a,1)\}
\end{array}$$

If the starting STS, $(V, \mathcal{B})$, has either a complete parallel class or one which includes all but one point, the tripled STS, $(V', \mathcal{B}')$, is completely decomposed into triangles with a maximum of one remainder block, and we are finished. If there is more than one point not covered by the partial parallel class, then there are at least 3 points not covered, because $v \equiv 1$ or 3 (mod 6). Take any three such points a, b, c, and select the three blocks $\{a,b,d\}$, $\{c,a,e\}$, $\{b,c,f\}$ of the original STS(v). None of these blocks is in the partial parallel class, and so for each of these blocks all 3 triangles in the tripled system as constructed above are intact. We take one triangle from each set:

$$\begin{array}{lll}
\{(d,1),(a,0),(b,0)\} & \{(b,2),(d,1),(a,1)\} & \{(a,0),(b,2),(d,2)\}, \\
\{(e,1),(a,0),(c,0)\} & \{(a,2),(c,1),(e,1)\} & \{(c,0),(e,2),(a,2)\}, \\
\{(f,1),(b,0),(c,0)\} & \{(c,2),(f,1),(b,1)\} & \{(b,0),(c,2),(f,2)\},
\end{array}$$

and merge them with the three vertical blocks $\{(a,0),(a,1),(a,2)\}$,

$\{(b,0),(b,1),(b,2)\}$, $\{(c,0),(c,1),(c,2)\}$ to form the four triangles:

$$\begin{array}{lll}
\{(a,0),(a,1),(a,2)\} & \{(b,2),(d,1),(a,1)\} & \{(a,0),(b,2),(d,2)\}, \\
\{(c,0),(c,1),(c,2)\} & \{(a,2),(c,1),(e,1)\} & \{(c,0),(e,2),(a,2)\}, \\
\{(b,0),(b,1),(b,2)\} & \{(c,2),(f,1),(b,1)\} & \{(b,0),(c,2),(f,2)\}, \\
\{(d,1),(a,0),(b,0)\} & \{(e,1),(a,0),(c,0)\} & \{(f,1),(b,0),(c,0)\},
\end{array}$$

We may clearly proceed in this way until all the points but possibly one are used up. All but possibly one (vertical) block of the tripled system is therefore included in triangles, and the proof is complete. □

7.4 Doubling construction

The *doubling construction* produces a new STS on $2v+1$ points from any STS on v points. If $(V,\mathcal{B})$ is the original STS, and $(V',\mathcal{B}')$ is the new STS, then

$V' = \{\infty\} \cup \{(a,0),(a,1); a \in V\}$, and

$\mathcal{B}' = \{\ \{\infty,(a,0),(a,1)\};\ a \in V\} \cup$

$\{\ \{(a,i),(b,j),(c,k)\}; \{a,b,c\} \in \mathcal{B};\ i,j,k \in Z_2, i+j+k=0\}.$

Proof of Theorem 7.1.4. We denote the STS(v) by $(V,\mathcal{B})$, and the doubled STS(2v+1) by $(V',\mathcal{B}')$, and divide the blocks of $(V',\mathcal{B}')$ into three parts:

i) $\{\ \{(a,0),(b,0),(c,0)\}; \{a,b,c\} \in \mathcal{B}\}$,

ii) $\{\ \{(a,1),(b,1),(c,0)\},\ \{(a,1),(b,0),(c,1)\},\ \{(a,0),(b,1),(c,1)\};$
$\{a,b,c\} \in \mathcal{B}\}$,

iii) $\{\ \{\infty,(a,0),(a,1)\}; a \in V\}$.

The blocks ii) as stated are already decomposed into triangles with no remainder. The blocks i), being isomorphic to the original STS(v), have a decomposition into triangles by assumption, with possibly one or two blocks remaining. There remain the blocks iii) and the remainder from i) to be incorporated into triangles.

Firstly, for each remainder block, $\{a, b, c\}$ from i), we form a triangle with two blocks, $\{\infty, (a, 0), (a, 1)\}$, $\{\infty, (b, 0), (b, 1)\}$ from iii). If there are two remainder blocks it is easy to do this for both even if the remainder blocks have a point in common.

Next, divide the remaining blocks of iii) arbitrarily into threes, with zero, one or two blocks remaining. If a triple of blocks $\{\infty, (a, 0), (a, 1)\}$, $\{\infty, (b, 0), (b, 1)\}$, $\{\infty, (c, 0), (c, 1)\}$, corresponds to a block $\{a, b, c\}$ of $\mathcal{B}$, then there is a triangle $\{(a, 1), (b, 1), (c, 0)\}$, $\{(a, 1), (b, 0), (c, 1)\}$, $\{(a, 0), (b, 1), (c, 1)\}$ of ii). These six blocks can be rearranged into two new triangles:

$$\begin{array}{lll} \{(a,1),(b,1),(c,0)\} & \{(a,1),(b,0),(c,1)\} & \{\infty,(c,0),(c,1)\}, \\ \{\infty,(a,0),(a,1)\} & \{\infty,(b,0),(b,1)\} & \{(a,0),(b,1),(c,1)\} \end{array}$$

If a triple of blocks $\{\infty, (a, 0), (a, 1)\}$, $\{\infty, (b, 0), (b, 1)\}$, $\{\infty, (c, 0), (c, 1)\}$, does not correspond to a block of $\mathcal{B}$, then there are three distinct blocks of $\mathcal{B}$, $\{a, b, d\}$,$\{b, c, e\}$,$\{c, a, f\}$, and we take the corresponding triangles of ii):

$$\begin{array}{lll} \{(a,1),(b,1),(d,0)\} & \{(a,1),(b,0),(d,1)\} & \{(a,0),(b,1),(d,1)\}, \\ \{(b,1),(c,1),(e,0)\} & \{(b,1),(c,0),(e,1)\} & \{(b,0),(c,1),(e,1)\}, \\ \{(c,1),(a,1),(f,0)\} & \{(c,1),(a,0),(f,1)\} & \{(c,0),(a,1),(f,1)\}, \end{array}$$

and the three blocks from iii), and rearrange to form the four triangles:

$$\begin{array}{lll}
\{(a,1),(b,1),(d,0)\} & \{(b,1),(c,1),(e,0)\} & \{(c,1),(a,1),(f,0)\}, \\
\{\infty,(a,0),(a,1)\} & \{(a,1),(b,0),(d,1)\} & \{(a,0),(b,1),(d,1)\}, \\
\{\infty,(b,0),(b,1)\} & \{(b,1),(c,0),(e,1)\} & \{(b,0),(c,1),(e,1)\}, \\
\{\infty,(c,0),(c,1)\} & \{(c,1),(a,0),(f,1)\} & \{(c,0),(a,1),(f,1)\}.
\end{array}$$

All blocks of $\mathcal{B}'$ can be incorporated into triangles in this way, and so the proof is complete. □

Corollary 7.4.1. *Every projective Steiner triple system is decomposable into triangles.*

Proof. Starting with the trivial STS on three points, apply Theorem 7.1.4 repeatedly. Since the initial STS is decomposable, so are all the resulting STS. □

7.5 Tripling construction

The *standard tripling construction* produces a new STS on $3v$ points from any STS on v points. Assume $(V,\mathcal{B})$ is the original STS, and $(V',\mathcal{B}')$ is the new STS, then

$V' = \{(a,0),(a,1),(a,2); a \in V\}$, and

$\mathcal{B}' = \{\{(a,i),(b,j),(c,k)\}; \{a,b,c\} \in \mathcal{B};\ i,j,k \in Z_3,\ i+j+k=0\} \cup$

$\{\{(a,0),(a,1),(a,2)\};\ a \in V\}$.

We shall refer to the first part of $\mathcal{B}'$ as the *mixed blocks* of $\mathcal{B}'$. The second part of $\mathcal{B}'$ will be referred to as the *vertical blocks* of $\mathcal{B}'$.

Proof of Theorem 7.1.5. Firstly decompose the mixed blocks of $\mathcal{B}'$ as:

$$\begin{array}{lll}
\{(a,1),(b,2),(c,0)\} & \{(a,1),(b,0),(c,2)\} & \{(a,0),(b,0),(c,0)\}, \\
\{(a,2),(b,0),(c,1)\} & \{(a,2),(b,1),(c,0)\} & \{(a,1),(b,1),(c,1)\}, \\
\{(a,0),(b,1),(c,2)\} & \{(a,0),(b,2),(c,1)\} & \{(a,2),(b,2),(c,2)\},
\end{array}$$

for each block $\{a,b,c\} \in \mathcal{B}$. The vertical blocks of the tripled system must be incorporated into triangles by modification of some of the above. Select any maximal partial parallel class, and divide the points of the original STS(v) into those which are covered by the partial parallel class and those which are not. For each block, $\{a,b,c\}$ of the partial parallel class, we take the three corresponding triangles from the mixed blocks, together with the three corresponding vertical blocks: $\{(a,0),(a,1),(a,2)\}$, $\{(b,0),(b,1),(b,2)\}$,$\{(c,0),(c,1),(c,2)\}$, and rearrange them into the four triangles:

$$\begin{array}{lll}
\{(a,0),(a,1),(a,2)\} & \{(a,1),(b,0),(c,2)\} & \{(a,0),(b,0),(c,0)\} \\
\{(a,2),(b,0),(c,1)\} & \{(b,0),(b,1),(b,2)\} & \{(a,1),(b,1),(c,1)\} \\
\{(a,0),(b,1),(c,2)\} & \{(a,0),(b,2),(c,1)\} & \{(c,0),(c,1),(c,2)\} \\
\{(a,1),(b,2),(c,0)\} & \{(a,2),(b,1),(c,0)\} & \{(a,2),(b,2),(c,2)\}
\end{array}$$

If the starting STS, $(V,\mathcal{B})$, has either a complete parallel class or one which includes all but one point, the tripled STS, $(V',\mathcal{B}')$, is completely decomposed into triangles with a maximum of one remainder block, and we are finished. If there is more than one point not covered by the partial parallel class, then there are at least 3 points not covered, because $v \equiv 1$ or 3 (mod 6). Take any three such points a, b, c, and select the three blocks $\{a,b,d\}$, $\{c,a,e\}$, $\{b,c,f\}$ of the original STS(v). None of these blocks is in the partial parallel class, and so for

each of these blocks all 3 triangles in the tripled system as constructed above are intact. We take one triangle from each set:

$$\begin{array}{lll}
\{(a,1),(b,2),(d,0)\} & \{(a,1),(b,0),(d,2)\} & \{(a,0),(b,0),(d,0)\}, \\
\{(c,1),(a,2),(e,0)\} & \{(c,1),(a,0),(e,2)\} & \{(c,0),(a,0),(e,0)\}, \\
\{(b,1),(c,2),(f,0)\} & \{(b,1),(c,0),(f,2)\} & \{(b,0),(c,0),(f,0)\},
\end{array}$$

and merge them with the three vertical blocks $\{(a,0),(a,1),(a,2)\}$, $\{(b,0),(b,1),(b,2)\}$, $\{(c,0),(c,1),(c,2)\}$ to form the four triangles:

$$\begin{array}{lll}
\{(a,1),(b,2),(d,0)\} & \{(a,1),(b,0),(d,2)\} & \{(b,0),(b,1),(b,2)\}, \\
\{(c,1),(a,2),(e,0)\} & \{(c,1),(a,0),(e,2)\} & \{(a,0),(a,1),(a,2)\}, \\
\{(b,1),(c,2),(f,0)\} & \{(b,1),(c,0),(f,2)\} & \{(c,0),(c,1),(c,2)\}, \\
\{(a,0),(b,0),(d,0)\} & \{(c,0),(a,0),(e,0)\} & \{(b,0),(c,0),(f,0)\}.
\end{array}$$

We may clearly proceed in this way until all the points but possibly one are used up. All but possibly one (vertical) block of the tripled system is therefore included in triangles, and the proof is complete. □

Since the Affine Geometries are obtainable from the trivial STS(3) by repeated application of the standard tripling construction,we have immediately:

Corollary 7.5.1. *The Affine Geometries, $AG(n,3)$, $n \geq 1$ are decomposable into triangles.*

7.6 Enumeration of decomposable STS

We prove that the number of STS(v) that are decomposable into triangles is at least $v^{v^2(\frac{1}{54}-o(1))}$ by proving the result for each admissible v (mod 18). We deal

first with the easy case:

Theorem 7.6.1. *Theorem 7.1.6 is true for* $v \equiv 3, 9 \pmod{18}$.

Proof. For $v = 18s+3$ and $v = 18s+9$, $v/3$ is also admissible. Further, by Theorem 7.1.3, the STS(v) constructed from any STS($v/3$) by the Bose construction is decomposable into triangles. But by [2], there are $(v/3)^{v/3^2(\frac{1}{6}-o(1))} = v^{v^2(\frac{1}{54}-o(1))}$ differently labelled STS($v/3$), so there are at least that number of differently labelled STS(v) that are decomposable into triangles. However, an STS(v) has an automorphism group of order no more than $v!$, so the number of non-isomorphic STS(v) that are decomposable into triangles is at least $\frac{v^{v^2(\frac{1}{54}-o(1))}}{v!} = v^{v^2(\frac{1}{54}-o(1))}$, which proves the result. □

In the following we make extensive use of 3-GDDs, a type of group divisible design. A 3-GDD is a triple $(\mathcal{V}, \mathcal{B}, \mathcal{G})$, where $\mathcal{V}$ is a set of points of cardinality v, $\mathcal{G}$ is a partition of $\mathcal{V}$ into parts (groups), and $\mathcal{B}$ is a family of blocks which satisfy the following properties:

1. If $B \in \mathcal{B}$, then $|B| = 3$.
2. Every pair of elements of $\mathcal{V}$ occurs either in exactly one block, or one group, but not both.
3. $|\mathcal{G}| > 1$.

A 3-GDD is said to be of type $g_1^{a_1} g_2^{a_2} \ldots g_s^{a_s}$ if $v = a_1 g_1 + a_2 g_2 \ldots + a_s g_s$, and $\mathcal{G}$ contains a_i groups of size g_i for $i = 1, 2 \ldots s$.

To prove the result for $v \equiv 1, 7, 13, 15 \pmod{18}$, we use a construction that requires:

a) One each of STS(7), STS(9), STS(13), STS(15) and STS(19) that are decomposable into triangles.

b) A decomposition of the tripartite complete graph $K_{3,3,3}$ into triangles. This of course a Latin square of side 3.

c) For all s greater than some lower bound, 3-GDDs of types 6^s, 6^s2^1, and 6^s4^1.

d) For all s greater than some lower bound, a 3-GDD of type $3^{2s}5^1$.

For the decomposable triple systems required in a), those of order $9, 15$ exist by Theorem 7.1.3, and those of order $7, 19$ exist by Theorem 7.1.4. For the STS(13), we decompose the cyclic STS on the base blocks $\{0,1,4\}$ and $\{0,2,7\}$ into the eight triangles:

$\{0,1,4\},\{3,4,7\},\{12,0,3\}$; $\{1,2,5\},\{5,6,9\},\{12,1,6\}$;

$\{0,2,7\},\{6,8,0\},\{6,7,11\}$; $\{1,3,8\},\{7,9,1\},\{7,8,12\}$;

$\{2,4,9\},\{8,10,2\},\{8,9,0\}$; $\{3,5,10\},\{9,11,3\},\{9,10,1\}$;

$\{4,6,11\},\{10,12,4\},\{10,11,2\}$; $\{5,7,12\},\{11,0,5\},\{11,12,3\}$,

and the two remainder blocks $\{2,3,6\}$ and $\{4,5,8\}$.

For c), we first state the general conditions for the existence of 3-GDDs of the relevant types, which are taken from [7], page 189-190. A 3-GDD of type t^u exists iff:

- t =1,5 (mod 6); $u = 1,3$ (mod 6), $u \geq 3$
- $t = 2,4$ (mod 6); u =0,1 (mod 3), $u \geq 3$
- t =3 (mod 6); u =1 (mod 2), $u \geq 3$
- t =0 (mod 6); $u \geq 3$.

A 3-GDD of type $g^t u^1$ exists if all the following conditions are satisfied:

(1) if $g > 0$ and either $t \geq 3$, or $t = 2$ and $u = g$, or $t = 1$ and $u = 0$, or $t = 0$

(2) $u \leq g(t-1)$ or $gt = 0$

(3) $g(t-1) + u \equiv 0 \pmod 2$ or $gt = 0$

(4) $gt \equiv 0 \pmod 2$, or $u = 0$

(5) $\frac{1}{2}g^2 t(t-1) + gtu \equiv 0 \pmod 3$.

From these conditions we see that the 3-GDDs of types 6^s, $6^s 2^1$, and $6^s 4^1$ exist for all $s \geq 3$, and 3-GDDs of type $3^{2s}5^1$ exist for all $s \geq 2$.

We therefore have all the requirements. We now give the construction.

Construction

For $v = 1, 7, 13, 15$ we construct a STS($18s + v$) that is decomposable into triangles.

- For $v = 1$, take a 3-GDD of type 6^s and an extra point, which we will call the infinity point. Replace each point of each group by three points, and replace each block by a copy of $K_{3,3,3}$, where each part is a tripled-up point. Thus we now have a 3-GDD of type 18^s which is decomposable into copies of $K_{3,3,3}$, and the infinity point. We now fit a copy of the decomposable STS(19) across each group and the infinity point. This structure is an STS($18s + 1$) because each pair between groups is in a unique block of the GDD, each pair within a group is in one block of a copy of the STS(19), and each pair containing the infinity point is in one block of a STS(19) copy. The STS($18s + 1$) is decomposable into triangles because the GDD of type 18^s is decomposable into copies of $K_{3,3,3}$, each of which is decomposable

into triangles with no remainder, and each STS(19) is also decomposable into triangles with no remainder blocks.

- For $v = 7$, take a 3-GDD of type 6^s2^1 and an extra infinity point. Again replace each point of each group by three points, and replace each block by a copy of $K_{3,3,3}$, where each part is a tripled-up point. Thus we now have a 3-GDD of type 18^s6^1 which is decomposable into copies of $K_{3,3,3}$, and the infinity point. We now fit a copy of the decomposable STS(19) on each group of size 18 and the infinity point. We also fit a copy of the decomposable STS(7) on the points of the group of size 6 and the infinity point. This structure is an STS($18s + 7$) because each pair between groups is in a unique block of the GDD, each pair within a group of size 18 is in one block of a copy of the STS(19), each pair in the group of size 6 is in one block of the STS(7), and each pair containing the infinity point is either in one block of a STS(19) copy or in one block of the STS(7). It is decomposable into triangles with one remainder block because the GDD of type 18^s6^1 is decomposable into copies of $K_{3,3,3}$, each of which is decomposable into triangles with no remainder, each STS(19) is also decomposable into triangles with no remainder blocks, and the STS(7) is decomposable into triangles with one remainder block.

- For $v = 13$, take a 3-GDD of type 6^s4^1 and an extra infinity point. Again replace each point of each group by three points, and replace each block by a copy of $K_{3,3,3}$, where each part is a tripled-up point. Thus we now have a 3-GDD of type 18^s12^1 which is decomposable into copies of $K_{3,3,3}$, and the infinity point. We now fit a copy of the decomposable STS(19) across each group of size 18 and the infinity point. We also fit a copy of

the decomposable STS(13) on the group of size 12 and the infinity point. This structure is an STS($18s + 13$) because each pair between groups is in a unique block of the GDD, each pair within a group of size 18 is in one block of a copy of the STS(19), each pair within a group of size 12 is in one block of a copy of the STS(13), and each pair containing the infinity point is either in one block of a STS(19) copy or in one block of the STS(13). The STS($18s + 13$) is decomposable into triangles with two remainder blocks because the GDD of type 18^s12^1 is decomposable into copies of $K_{3,3,3}$, each of which is decomposable into triangles with no remainder, each STS(19) is decomposable into triangles with no remainder blocks, and the STS(13) is decomposable into triangles with two remainder blocks.

- For $v = 15$, take a 3-GDD of type $3^{2s}5^1$. Again replace each point of each group by three points, and replace each block by a copy of $K_{3,3,3}$, where each part is a tripled-up point. Thus we now have a 3-GDD of type $9^{2s}15^1$ which is decomposable into copies of $K_{3,3,3}$. We now fit a copy of the decomposable STS(9) across each group of size 9. We also fit a copy of the decomposable STS(15) on the group of size 15. This structure is an STS($18s + 15$) because each pair between groups is in a unique block of the GDD, each pair within a group of size 9 is in one block of a copy of the STS(9), and each pair within the group of size 15 is in one block of the STS(15). The STS($18s + 15$) is decomposable into triangles with two remainder blocks because the GDD of type 18^s15^1 is decomposable into copies of $K_{3,3,3}$, each of which is decomposable into triangles with no remainder, each STS(9) is decomposable into triangles with no remainder blocks, and the STS(15) is decomposable into triangles with two remainder

blocks.

We now prove the remaining four cases of Theorem 7.1.6 by finding a lower bound on the number of 3-GDDs of the required type for large s in the construction above. We shall make extensive use of the fact that, if $L(n)$ is the number of latin squares of order n, then $ln(L(n)) \geq n^2(ln(n) - 2)$. This result is proved for instance in [6], page 95. Each case will be approached in the same way. For each GDD with parameter s we construct a GDD with parameter $3s$, using a Latin square, which can be viewed as a GDD with three groups. With additional infinity points, this construction can be extended to parameters $3s+1$ and $3s+2$. The construction then enables us to write an inequality which can be used to construct a lower bound on the number of 3-GDDs with parameter s for sufficiently large s, which in turn, via Construction, leads to a lower bound on the number of decomposable STS.

7.6.1 The case $v = 1$.

The recursive construction needs the extra condition that each 3-GDD has a fixed subsystem of type 6^5. The existence of the designs with this extra condition is proved first, although the motivation will not be apparent until we give the construction itself.

Existence

Take a 3-GDD of type 6^s30^1. This exists for all $s \geq 6$ by the conditions quoted above. Replace the group of size 30 by a 3-GDD of type 6^5, and the result is a 3-GDD of type 6^{s+5} with the required subsystem, so the systems of the required type exist for all $s \geq 11$.

Recursive construction

Starting from 3-GDDs of type 6^s we construct 3-GDDs of types 6^{3s}, 6^{3s+1}, and 6^{3s+5}.

For 6^{3s} we take a latin square of order $6s$, written as a 3-GDD of type $(6s)^3$. Across each group fit a 3-GDD of type 6^s each having the required subsystem of type 6^5. Each of these 3-GDDs can be different. To construct this 3-GDD, only one of the GDDs of type 6^s actually needs the given fixed subsystem, however for our lower bound we specify that all of them do. This yields a 3-GDD of type 6^{3s}. If $D(s)$ denotes the number of differently-labelled 3-GDDs of type 6^s each with the required subsystem of type 6^5, and $L(n)$ denotes the number of differently-labelled latin squares of order n, then we have $D(3s) \geq L(6s)D(s)^3$ for $s \geq 11$.

For 6^{3s+1} we take a latin square of order $6s$ as before, plus 6 infinity points, which we group together. Across each group and the group of infinity points we fit a 6^{s+1}, each having the required subsystem. Each of these 3-GDDs can be different. This yields a 3-GDD of type 6^{3s+1}. Thus we have $D(3s+1) \geq L(6s)D(s+1)^3$ for $s \geq 10$.

For 6^{3s+5} we take a we take a latin square of order $6s$, plus 30 infinity points. On the infinity points we place a copy of our chosen system of type 6^5, Across each group and the infinity points we fit a system of type 6^{s+5} containing the required subsystem, identifying that subsystem with the one on the infinity points. Each of these 3-GDDs can be different. This yields a 3-GDD of type 6^{3s+5}. Thus we have $D(3s+5) \geq L(6s)D(s+5)^3$ for $s \geq 6$.

To summarise these results, we have that for all $s \geq 11$,
$D(3s) \geq L(6s)D(s)^3$, $D(3s-2) \geq L(6(s-1))D(s)^3$, and $D(3s-10) \geq L(6(s-$

$5))D(s)^3$.

Lower bound for $D(s)$.

Before we can use these to produce the lower bound on the numbers of 3-GDDs of the given type, we need a facilitating lemma.

Lemma 7.6.1. $(t-5)^2 ln(t-5) > (t+\frac{1}{18})^2 ln(t+\frac{1}{18}) - (t+8)^2$ *for* $t \geq 9$.

Proof. let $f(t) = (t-5)^2 ln(t-5) - (t+\frac{1}{18})^2 ln(t+\frac{1}{18}) + (t+8)^2$. Then $f(9) \approx 130.5 > 0$ Also $f'(t) = 2(t-5)ln(t-5) - 2(t+\frac{1}{18})ln(t+\frac{1}{18}) + 2t + 10\frac{17}{18}$, so $f'(9) \approx 0.13 > 0$, and $f''(t) = 2ln\left(\frac{t-5}{t+\frac{1}{18}}\right) + 2$, which is monotonic increasing, and $f''(9) \approx 0.37 > 0$. Therefore, $f'(t)$ is increasing for $t \geq 9$, and therefore so is $f(t)$. □

Lemma 7.6.2. *For* $t \geq 11$ *and* $u = t + \frac{1}{18}$, $ln(D(t)) \geq 6u^2(ln(u) - ln(54\frac{1}{18}))$, *i.e.* $D(t) \geq (ku)^{6u^2}$ *for* $k = \frac{1}{54\frac{1}{18}}$.

Proof. We have shown above that $D(t) \geq 1$ for $t \geq 11$. The result is therefore true for all $11 \leq t \leq 54$. Also, since $ln(L(n)) \geq n^2(ln(n)-2)$, and this function is monotonic increasing, we have that $ln((D(3t))$, $ln(D(3t-2))$, $ln(D(3t-10))$ are all greater than or equal to $g(t)$ for $t \geq 11$, where $g(t) = 36(t-5)^2(ln(6(t-5)) - 2) + 3ln(D(t))$. We assume inductively that $ln(D(t)) \geq 6u^2(ln(u) - ln(54\frac{1}{18})$, where $u = t + \frac{1}{18}$.

To complete the proof, it suffices to show that
$g(t) \geq 6(3t+\frac{1}{18})^2(ln(3t+\frac{1}{18}) - ln(54\frac{1}{18}))$ for $t \geq 17$.
Consider $h(t) = g(t) - 6(3t+\frac{1}{18})^2(ln(3t+\frac{1}{18}) - ln(54\frac{1}{18}))$. We show that $h(t) \geq 0$ for $t \geq 15$. By Lemma 7.6.1 we have, for $t \geq 9$,
$h(t) \geq 36u^2 ln(u) - 36(t+8)^2 + 36(t-5)^2 ln(6) - 72(t-5)^2 + 18u^2 ln(u)$

$$
\begin{aligned}
&- 18u^2 ln(54\tfrac{1}{18}) - 6(3t+\tfrac{1}{18})^2 ln(3t+\tfrac{1}{18}) + 6(3t+\tfrac{1}{18})^2 ln(54\tfrac{1}{18}) \\
&= 54u^2 ln(u) - 36(t+8)^2 + 36(t-5)^2 ln(6) - 72(t-5)^2 - 18u^2 ln(54\tfrac{1}{18}) \\
&\quad - 6(3t+\tfrac{1}{18})^2 ln(3t+\tfrac{1}{18}) + 6(3t+\tfrac{1}{18})^2 ln(54\tfrac{1}{18}) \\
&\geq 54u^2 ln(u) - 36(t+8)^2 + 36(t-5)^2 ln(6) - 72(t-5)^2 - 18u^2 ln(54\tfrac{1}{18}) - \\
&6(3u)^2 ln(3u) + 6(3t)^2 ln(54\tfrac{1}{18}) \\
&= 54t^2 ln(54\tfrac{1}{18}) - 18u^2 ln(54\tfrac{1}{18}) - 36(t+8)^2 + 36(t-5)^2 ln(6) \\
&\quad - 72(t-5)^2 - 54u^2 ln(3) \\
&= t^2(36 ln(54\tfrac{1}{18}) - 36 + 36 ln(6) - 72 - 54 ln(3)) \\
&\quad - t(576 + 360 ln(6) - 720 + 2 ln(54\tfrac{1}{18}) + 6 ln(3)) \\
&\quad - (2304 - 900 ln(6) + 1800 + \tfrac{1}{18} ln(54\tfrac{1}{18}) + \tfrac{1}{6} ln(3)) \\
&\approx 40.82t^2 - 515.61t - 2491.82 > 539 > 0 \text{ for } t \geq 17, \text{ and so the lemma is}
\end{aligned}
$$

proved. □

Lower bound for numbers of STS(v)

Lemma 7.6.3. *If $v = 18s + 1$, and $s \geq 11$, then the number of non-isomorphic STS(v) that are decomposable into triangles is at least $\frac{1}{v!}\left(\frac{v}{973}\right)^{\frac{v^2}{54}} = v^{v^2(c-o(1))}$ as $v \to \infty$, where $c = \frac{1}{54}$.*

Proof. As in Construction above, take a 3-GDD of type 6^{3s} and an infinity point. Inflate the GDD by a factor of 3, placing a $K_{3,3,3}$ across each inflated block, and STS(19)s across the inflated groups and infinity point. The resulting construct is a STS($18s+1$). Since all the ingredients are decomposable into triangles, so is the STS($18s+1$). By Lemma 7.6.2, the number of differently labelled decomposable STS($18s+1$) is therefore at least $D(s) \geq \left(\frac{s+\frac{1}{18}}{54\frac{1}{18}}\right)^{6(s+\frac{1}{18})^2}$ for $s \geq 11$. This gives $D(s) \geq \left(\frac{v}{973}\right)^{\frac{v^2}{54}}$. The largest possible size of automorphism group for an STS(v) is $v!$, so the number of non-isomorphic decomposable STS($18s+1$) is therefore

at least $\frac{1}{v!}\left(\frac{v}{973}\right)^{\frac{v^2}{54}}$ when $v = 18s + 1$, $s \geq 11$.

□

7.6.2 The case $v = 7$.

To facilitate the construction we set the additional condition that the 3-GDDs all coincide on particular fixed 3-GDDs of types $6^4 2^1$ and $6^8 2^1$.

Existence

The proof is in three parts.

a) We construct a system of type $6^{3r}2^1$. By [7], page 189 there exist 3-GDDs of types $6^2 4^3$ and 2^3. Replace each group of size 6 in the first by a system of type 2^3, which yields one of type $2^6 4^3$. Inflate each group by a factor of 12 and place systems of type 12^3 on each inflated block. This give a system of type $24^6 48^3$. Now take a system of type $18^t 288^1$, which exists for $t \geq 17$. Replace the group of size 288 by the system of type $24^6 48^3$, to give a system of type $18^t 24^6 48^3$. Now introduce 2 infinity points and on the infinity points and each group of size 18 place a system of type $6^3 2^1$. On the infinity points and each group of size 24 place a system of type $6^4 2^1$. On the infinity points and each group of size 48 place a system of type $6^8 2^1$. Thus we have a system of type $6^{3t+48}2^1$ with the required subsystems. So we have a system of type $6^{3r}2^1$ for all $r \geq 33$.

b) We construct a system of type $6^{3r+1}2^1$. By [7], page 189, there exists a 3-GDD of type $8^3 4^1$. Inflate each group by a factor of 6 and place systems of type 6^3 on each inflated block. This give a system of type $48^3 24^1$. Now

take a system of type 18^t168^1, which exists for $t \geq 11$. Replace the group of size 168 by the system of type 48^324^1, to give a system of type $18^t48^324^1$. Now introduce 2 infinity points and on the infinity points and each group of size 18 place a system of type 6^32^1. On the infinity points and each group of size 24 place a system of type 6^42^1. On the infinity points and each group of size 48 place a system of type 6^82^1. Thus we have a system of type $6^{3t+28}2^1$ with the required subsystems. So we have a system of type $6^{3r+1}2^1$ for all $r \geq 20$.

c) We construct a system of type $6^{3r+2}2^1$. By [7], page 189, there exists a 3-GDD of type 8^14^3. Inflate each group by a factor of 6 and place systems of type 6^3 on each inflated block. This give a system of type 48^124^3. Now take a system of type 18^t120^1, which exists for $t \geq 8$. Replace the group of size 120 by the system of type 48^124^3, to give a system of type $18^t48^124^3$. Now introduce 2 infinity points and on the infinity points and each group of size 18 place a system of type 6^32^1. On the infinity points and each group of size 24 place a system of type 6^42^1. On the infinity points and each group of size 48 place a system of type 6^82^1. Thus we have a system of type $6^{3t+20}2^1$ with the required subsystems. So we have a system of type $6^{3r+2}2^1$ for all $r \geq 14$.

Thus 3-GDDs of type 6^s2^1 with the necessary fixed subsystems exist for all $s \geq 99$.

Recursive construction

From 3-GDDs of type 6^s2^1 with the required fixed subsystems we construct 3-GDD of types $6^{3s}2^1$, $6^{3s+4}2^1$, and $6^{3s+8}2^1$, each again with the required fixed subsystems. There are separate arguments for these cases.

Firstly we take a latin square of order $6s$, written as a 3-GDD of type $(6s)^3$, plus an additional 2 infinity points. Across each group and the infinity points, fit a 3-GDD of type 6^s2^1, having the required fixed subsystems of types 6^42^1 and 6^82^1. The 3-GDDs can be different, providing they have the same fixed subsystems previously mentioned. This yields a $6^{3s}2^1$. To construct the 3-GDD of type $6^{3s}2^1$, only one of the GDDs of type 6^s2^1 actually needs the given fixed subsystems, however for the purpose of producing a lower bound we specify that all of them do. If $D(s)$ denotes the number of differently-labelled 3-GDDs of type 6^s2^1 with the given fixed subsystems, and $L(n)$ denotes the number of latin squares of order n, then we have $D(3s) \geq L(6s)D(s)^3$ for $s \geq 99$.

Secondly, for $6^{3s+4}2^1$, we take a latin square of order $6s$ as before, plus 26 infinity points. On the infinity points we place a copy of the chosen system of type 6^42^1, Across each group and the common infinity points we fit a possibly different 3-GDD of type $6^{s+4}2^1$ with the fixed subsystems, identifying the subsystem of type 6^42^1 with the one on the infinity points. This yields a 3-GDD of type $6^{3s+4}2^1$ with the required subsystems. Thus we have $D(3s+4) \geq L(6s)D(s+4)^3$ for $s \geq 95$.

Finally, for $6^{3s+8}2^1$ we take a latin square of order $6s$ plus 50 infinity points. On the infinity points we place a copy of our chosen system of type 6^82^1. Across each group and the common infinity points we fit a $6^{s+8}2^1$ which has the fixed subsystems of types 6^42^1 and 6^82^1, identifying the subsystem of type 6^82^1 with the one on the infinity points. This yields a 3-GDD of type $6^{3s+8}2^1$ with the required subsystems. Thus we have $D(3s+8) \geq L(6s)D(s+8)^3$ for $s \geq 91$. Hence, to summarise these results, we have that for all $s \geq 99$, $D(3s) \geq L(6s)D(s)^3$, $D(3s-8) \geq L(6(s-4))D(s)^3$, and $D(3s-16) \geq L(6(s-8))D(s)^3$.

Lower bound for $D(s)$.

Lemma 7.6.4. $(t-8)^2 ln(t-8) > (t+\frac{7}{18})^2 ln(t+\frac{7}{18}) - (t+8)^2$ *for* $t \geq 50$.

Proof. let $f(t) = (t-8)^2 ln(t-8) - (t+\frac{7}{18})^2 ln(t+\frac{7}{18}) + (t+8)^2$. Then $f(50) \approx 4.8 > 0$ Also $f'(t) = 2(t-8)ln(t-8) - 2(t+\frac{7}{18})ln(t+\frac{7}{18}) + 2t + 7\frac{11}{18}$, so $f'(50) \approx 26.55 > 0$, and $f''(t) = 2ln\left(\frac{t-8}{t+\frac{7}{18}}\right) + 2$, which is monotonic increasing, and $f''(50) \approx 1.64$. Therefore, $f'(t)$ is increasing for $t \geq 50$, and therefore so is $f(t)$. □

Lemma 7.6.5. *For* $t \geq 99$ *and* $u = t + \frac{7}{18}$, $ln(D(u)) \geq 6u^2(ln(u) - ln(297\frac{7}{18}))$, *i.e.* $D(t) \geq (ku)^{6u^2}$ *for* $k = \frac{1}{297\frac{7}{18}}$.

Proof. We have shown above that $D(t) \geq 1$ for $t \geq 99$. The result is therefore true for all $99 \leq t \leq 297$. Also, since $ln(L(n)) \geq n^2(ln(n) - 2)$, and this function is monotonic increasing, we have that $ln((D(3t))$, $ln(D(3t-8))$, $ln(D(3t-16))$ are all greater than or equal to $g(t)$ for $t \geq 99$, where $g(t) = 36(t-8)^2(ln(6(t-8)) - 2) + 3ln(D(t))$. We assume inductively that $ln(D(t)) \geq 6u^2(ln(u) - ln(297\frac{7}{18}))$, where $u = t + \frac{7}{18}$.

To complete the proof, it suffices to show that

$g(t) \geq 6(3t + \frac{7}{18})^2(ln(3t + \frac{7}{18}) - ln(297\frac{7}{18}))$ for $t \geq 99$.

Consider $h(t) = g(t) - 6(3t+\frac{7}{18})^2(ln(3t+\frac{7}{18}) - ln(297\frac{7}{18}))$. We show that $h(t) \geq 0$ for $t \geq 50$. By Lemma 7.6.4 we have, for $t \geq 50$,

$$\begin{aligned}
h(t) &\geq 36u^2 ln(u) - 36(t+8)^2 + 36(t-8)^2 ln(6) - 72(t-8)^2 + 18u^2 ln(u) \\
&\quad - 18u^2 ln(297\tfrac{7}{18}) - 6(3t + \tfrac{7}{18})^2 ln(3t + \tfrac{7}{18}) + 6(3t + \tfrac{7}{18})^2 ln(297\tfrac{7}{18}) \\
&= 54u^2 ln(u) - 36(t+8)^2 + 36(t-8)^2 ln(6) - 72(t-8)^2 - 18u^2 ln(297\tfrac{7}{18}) \\
&\quad - 6(3t + \tfrac{7}{18})^2 ln(3t + \tfrac{7}{18}) + 6(3t + \tfrac{7}{18})^2 ln(297\tfrac{7}{18}) \\
&\geq 54u^2 ln(u) - 36(t+8)^2 + 36(t-8)^2 ln(6) - 72(t-8)^2 - 18u^2 ln(297\tfrac{7}{18}) \\
&\quad - 6(3u)^2 ln(3u) + 6(3t)^2 ln(297\tfrac{7}{18})
\end{aligned}$$

$$= 54t^2 ln(297\tfrac{7}{18}) - 18u^2 ln(297\tfrac{7}{18}) - 36(t+8)^2 + 36(t-8)^2 ln(6)$$
$$- 72(t-8)^2 - 54u^2 ln(3)$$
$$= t^2(36ln(297\tfrac{7}{18}) - 36 + 36ln(6) - 72 - 54ln(3))$$
$$- t(576 + 576ln(6) - 1152 + 14ln(297\tfrac{7}{18}) + 42ln(3))$$
$$- (2304 - 2304ln(6) + 4608 + \tfrac{49}{18}ln(297\tfrac{7}{18}) + \tfrac{49}{6}ln(3))$$
$\approx 102.2t^2 - 581.9t - 2808.3 > 232 > 0$ for $t \geq 9$, so $h(t) > 0$ for $t \geq 50$, and the lemma is proved. □

Lower bound for numbers of STS(v)

Lemma 7.6.6. *If $v = 18s + 7$, and $s \geq 99$, then the number of non-isomorphic STS(v) that are decomposable into triangles is at least $\frac{1}{v!}\left(\frac{v}{5353}\right)^{\frac{v^2}{54}} = v^{v^2(c-o(1))}$ as $v \to \infty$, where $c = \frac{1}{54}$.*

Proof. As in Construction above, take a 3-GDD of type $6^s 2^1$ and an infinity point. Inflate the GDD by a factor of 3, placing a $K_{3,3,3}$ across each inflated block. Also place a decomposable STS(19) across each inflated group of size 6 and the infinity point, and a decomposable STS(7) across the inflated group of size 2 and the infinity point. The resulting construct is a STS($18s + 7$). Since all the ingredients are decomposable into triangles, so is the STS($18s + 7$). By Lemma 7.6.5, the number of differently-labelled decomposable STS($18s + 7$) is therefore at least $D(s) \geq \left(\frac{s+\frac{7}{18}}{297\frac{7}{18}}\right)^{6(s+\frac{7}{18})^2}$ for $s \geq 99$. This gives $D(s) \geq \left(\frac{v}{5353}\right)^{\frac{v^2}{54}}$. As the largest possible size of automorphism group for an STS(v) is $v!$, the number of distinct decomposable STS($18s + 7$) is at least $\frac{1}{v!}\left(\frac{v}{5353}\right)^{\frac{v^2}{54}} = v^{v^2(\frac{1}{54}-o(1))}$ when $v = 18s + 7$, $s \geq 99$.

□

7.6.3 The case $v = 13$.

The 3-GDDs of type 6^s are required to contain fixed subsystems of types $6^4 4^1$ and $6^8 4^1$.

Existence

We use the same method as for the case $v = 7$. For that case we showed that there are 3-GDDs of types: $18^t 24^6 48^3$ for $t \geq 17$, $18^t 48^3 24^1$ for $t \geq 11$, and $18^t 48^1 24^3$ for $t \geq 8$. We shall use these as a basis for this construction.

a) Take a 3-GDD of type $18^t 24^6 48^3$ and 4 infinity points, and on the infinity points and each group of size 18 place a system of type $6^3 4^1$. On the infinity points and each group of size 24 place a system of type $6^4 4^1$. On the infinity points and each group of size 48 place a system of type $6^8 4^1$. Thus we have a system of type $6^{3t+48} 4^1$ with the required subsystems. So we have a system of type $6^{3r} 4^1$ for all $r \geq 33$.

b) Take a 3-GDD of type $18^t 48^3 24^1$ and 4 infinity points, and on the infinity points and each group of size 18 place a system of type $6^3 4^1$. On the infinity points and the group of size 24 place a system of type $6^4 4^1$. On the infinity points and each group of size 48 place a system of type $6^8 4^1$. Thus we have a system of type $6^{3t+28} 4^1$ with the required subsystems. So we have a system of type $6^{3r+1} 4^1$ for all $r \geq 20$.

c) Take a 3-GDD of type $18^t 48^1 24^3$ and 4 infinity points, and on the infinity points and each group of size 18 place a system of type $6^3 4^1$. On the infinity points and each group of size 24 place a system of type $6^4 4^1$. On the infinity points and the group of size 48 place a system of type $6^8 4^1$. Thus we have a

system of type $6^{3t+20}4^1$ with the required subsystems. So we have a system of type $6^{3r+2}4^1$ for all $r \geq 14$.

Thus 3-GDDs of type 6^s4^1 with the necessary fixed subsystems exist for all $s \geq 99$.

Recursive construction

From 3-GDDs of type 6^s4^1 with the required subsystems we construct 3-GDDs of types $6^{3s}4^1$, $6^{3s+4}4^1$, and $6^{3s+8}4^1$, each again with the required fixed subsystems. There are separate arguments for each case.

For GDDs of type $6^{3s}4^1$ we take a latin square of order $6s$, written as a 3-GDD of type $(6s)^3$, plus an additional 4 infinity points, which are grouped together. Across each group and the infinity points, fit a 3-GDD of type 6^s4^1, having the required subsystems. The 3-GDDs can be different, providing they have the same fixed subsystems previously mentioned. This yields a $6^{3s}4^1$. To construct this 3-GDD, only one of the GDDs of type 6^s4^1 actually needs the given fixed subsystems, however for our lower bound we specify that all of them do.

For GDDs of type $6^{3s+4}4^1$ we take a latin square of order $6s$ as before, plus 28 infinity points. On the infinity points we place a copy of our system of type 6^44^1. Across each group and the common infinity points we fit a $6^{s+4}4^1$ with the appropriate subsystems, identifying the subsystem of type 6^44^1 with the one on the infinity points. This yields a 3-GDD of type $6^{3s+4}4^1$ with the required subsystem.

For GDDs of type $6^{3s+8}4^1$ we take a latin square of order $6s$ plus 52 infinity points. On the infinity points we place a copy of the chosen system of type 6^84^1. Across each group and the common infinity points we fit a $6^{s+8}4^1$ with the required subsystems, identifying the one of type 6^84^1 with the one on the infinity

points. This yields a 3-GDD of type $6^{3s+8}4^1$ with the required subsystems.

Therefore, if $D(s)$ represents the number of differently-labelled 3-GDD of type 6^s4^1 with the required subsystems, then for all $s \geq 99$,
$D(3s) \geq L(6s)D(s)^3$, $D(3s-8) \geq L(6(s-4))D(s)^3$, and $D(3s-16) \geq L(6(s-8))D(s)^3$.

Lower bound for $D(s)$.

Lemma 7.6.7. $(t-8)^2 ln(t-8) > (t+\frac{13}{18})^2 ln(t+\frac{13}{18}) - (t+8)^2$ *for* $t \geq 56$.

Proof. let $f(t) = (t-8)^2 ln(t-8) - (t+\frac{13}{18})^2 ln(t+\frac{13}{18}) + (t+8)^2$. Then $f(56) \approx 22.8 > 0$ Also $f'(t) = 2(t-8)ln(t-8) - 2(t+\frac{13}{18})ln(t+\frac{13}{18}) + 2t + 7\frac{5}{18}$, so $f'(56) \approx 32.8 > 0$, and $f''(t) = 2ln\left(\frac{t-8}{t+\frac{13}{18}}\right) + 2$, which is monotonic increasing, and $f''(56) \approx 1.67$. Therefore, $f'(t)$ is increasing for $t \geq 56$, and therefore so is $f(t)$. □

Lemma 7.6.8. *For* $t \geq 99$ *and* $u = t + \frac{13}{18}$, $ln(D(u)) \geq 6u^2(ln(u) - ln(297\frac{13}{18}))$, *i.e.* $D(t) \geq (ku)^{6u^2}$ *for* $k = \frac{1}{297\frac{13}{18}}$.

Proof. We have shown above that $D(t) \geq 1$ for $t \geq 99$. The result is therefore true for all $99 \leq t \leq 297$. Also, since $ln(L(n)) \geq n^2(ln(n) - 2)$, and this function is monotonic increasing, we have that $ln((D(3t))$, $ln(D(3t-8))$, $ln(D(3t-16))$ are all greater than or equal to $g(t)$ for $t \geq 99$, where $g(t) = 36(t-8)^2(ln(6(t-8)) - 2) + 3ln(D(t))$. We assume inductively that $ln(D(t)) \geq 6u^2(ln(u) - ln(297\frac{13}{18}))$, where $u = t + \frac{13}{18}$.

To complete the proof, it suffices to show that
$g(t) \geq 6(3t+\frac{13}{18})^2(ln(3t+\frac{13}{18}) - ln(297\frac{13}{18}))$ for $t \geq 99$.
Consider $h(t) = g(t) - 6(3t+\frac{13}{18})^2(ln(3t+\frac{13}{18}) - ln(297\frac{13}{18}))$. We show that $h(t) \geq 0$ for $t \geq 56$. By Lemma 7.6.7 we have, for $t \geq 56$,

$$
\begin{aligned}
h(t) &\geq 36u^2ln(u) - 36(t+8)^2 + 36(t-8)^2ln(6) - 72(t-8)^2 + 18u^2ln(u) \\
&\quad - 18u^2ln(297\tfrac{13}{18}) - 6(3t+\tfrac{13}{18})^2ln(3t+\tfrac{13}{18}) + 6(3t+\tfrac{13}{18})^2ln(297\tfrac{13}{18}) \\
&= 54u^2ln(u) - 36(t+8)^2 + 36(t-8)^2ln(6) - 72(t-8)^2 - 18u^2ln(297\tfrac{13}{18}) \\
&\quad - 6(3t+\tfrac{13}{18})^2ln(3t+\tfrac{13}{18}) + 6(3t+\tfrac{13}{18})^2ln(297\tfrac{13}{18}) \\
&\geq 54u^2ln(u) - 36(t+8)^2 + 36(t-8)^2ln(6) - 72(t-8)^2 - 18u^2ln(297\tfrac{13}{18}) \\
&\quad - 6(3u)^2ln(3u) + 6(3t)^2ln(297\tfrac{13}{18}) \\
&= 54t^2ln(297\tfrac{13}{18}) - 18u^2ln(297\tfrac{13}{18}) - 36(t+8)^2 + 36(t-8)^2ln(6) \\
&\quad - 72(t-8)^2 - 54u^2ln(3) \\
&= t^2(36ln(297\tfrac{13}{18}) - 36 + 36ln(6) - 72 - 54ln(3)) \\
&\quad - t(576 + 576ln(6) - 1152 + 26ln(297\tfrac{13}{18}) + 78ln(3)) \\
&\quad - (2304 - 2304ln(6) + 4608 + \tfrac{169}{18}ln(297\tfrac{13}{18}) + \tfrac{169}{6}ln(3)) \\
&\approx 102.24t^2 - 689.84t - 2868.2 > 457 > 0 \text{ for } t \geq 10, \text{ so } h(t) > 0 \text{ for } t \geq 99,
\end{aligned}
$$

and so the lemma is proved. □

Lower bound for numbers of STS(v)

Lemma 7.6.9. *If $v = 18s + 13$, and $s \geq 99$, then the number of non-isomorphic STS(v) that are decomposable into triangles is at least $\frac{1}{v!}\left(\frac{v}{5359}\right)^{\frac{v^2}{54}} = v^{v^2(c-o(1))}$ as $v \to \infty$, where $c = \frac{1}{54}$.*

Proof. As in Construction above, take a 3-GDD of type 6^s4^1 and an infinity point. Inflate the GDD by a factor of 3, placing a $K_{3,3,3}$ across each inflated block, and STS(19)s and a decomposable STS(13) across the inflated groups and infinity point. The resulting construct is a STS($18s + 13$). Since all the ingredients are decomposable into triangles, so is the STS($18s + 13$). By Lemma 7.6.8, the number of differently-labelled decomposable STS($18s + 13$) is therefore at least $D(s) \geq \left(\frac{s+\frac{13}{18}}{297\frac{13}{18}}\right)^{6(s+\frac{13}{18})^2}$ for $s \geq 99$. This gives $D(s) \geq \left(\frac{v}{5359}\right)^{\frac{v^2}{54}}$. The largest

possible size of automorphism group for an STS(v) is $v!$, so the number of distinct decomposable STS($18s+13$) is therefore at least $\frac{1}{v!}\left(\frac{v}{5359}\right)^{\frac{v^2}{54}}$ when $v = 18s+13$, $s \geq 99$. □

7.6.4 The case $v = 15$.

Our enumeration of decomposable STS($18s+15$) uses a construction of 3-GDDs of type $3^{2s}5^1$. The construction needs the additional condition that the 3-GDDs all coincide on particular fixed 3-GDDs of type 3^85^1 and 3^45^1.

Existence

We prove the existence for the separate cases $s \equiv 0, 1 \pmod 2$. For $s \equiv 0 \pmod 2$, we start with a 3-GDD of type 12^t24^1, which exists for $t \geq 3$. Add 5 new points and join these and the 24-group with a system of type 3^85^1. Also join each 12-group and the 5 new points by a system of type 3^45^1. This gives a system of type $3^{4t+8}5^1$. Thus the required system exists for even s if $s \geq 10$.

For $s \equiv 1 \pmod 2$, we first take a 3-GDD of type $8^16^14^3$, which exists by [7], page 189. Inflate each point by a factor of 3, and replace each tripled-up block by a system of type 3^3. This yields a system of type $24^118^112^3$. Now take a 3-GDD of type 12^t78^1, which exists for $t \geq 8$. Replace the 78-group by a system of type $24^118^112^3$, giving a system of type $12^{t+3}24^118^1$. Add 5 new points and join these and the 24-group with a system of type 3^85^1, the 18-group with a system of type 3^65^1, and the 12-groups with systems of type 3^45^1. This gives a system of type $3^{4t+26}5^1$. Thus such systems with odd s exist for $s \geq 29$, and so 3-GDDs of type $3^{2s}5^1$ with the required subsystems exist for $s \geq 28$.

Recursive construction

Starting from 3-GDDs of type $3^{2s}5^1$ with the required subsystems, 3-GDDs of types $3^{6s}5^1$, $3^{6s+8}5^1$, and $3^{6s+4}5^1$ are constructed, each again with the required fixed subsystems. There are separate arguments for each case.

For GDDs of type $3^{6s}5^1$, we take a latin square of order $6s$, written as a 3-GDD of type $(6s)^3$, plus an additional 5 infinity points. Across each group and the infinity points, fit a 3-GDD of type $3^{2s}5^1$, having the required subsystems. These 3-GDDs can be different, providing they have the same fixed subsystems previously mentioned. This yields a $3^{6s}5^1$. To construct the 3-GDD of type $3^{6s}5^1$, only one of the GDDs of type $3^{2s}5^1$ actually needs the given subsystems, however for our lower bound we specify that all of them do. If $D(s)$ denotes the number of differently-labelled 3-GDDs of type $3^{2s}5^1$ with given fixed subsystems of type 3^85^1 and 3^45^1, and $L(n)$ denotes the number of latin squares of order n, then we have $D(3s) \geq L(6s)D(s)^3$ for $s \geq 28$.

For GDDs of type $3^{6s+4}5^1$, we take a we take a latin square of order $6s$, plus 17 infinity points. On the infinity points we place a copy of our chosen system of type 3^45^1. Across each group and the common infinity points we fit a possibly different 3-GDD of type $3^{2s+4}5^1$ with the appropriate subsystems, identifying the subsystem of type 3^45^1 with the one on the infinity points. This yields a 3-GDD of type $3^{6s+4}5^1$. Thus we have $D(3s+2) \geq L(6s)D(s+2)^3$ for $s \geq 26$.

For GDDs of type $3^{6s+8}5^1$, we take a latin square of order $6s$ as before, plus 29 infinity points. On the infinity points we place a copy of the chosen system of type 3^85^1. Across each group and the common infinity points we fit a possibly different 3-GDD of type $3^{2s+8}5^1$ with the appropriate subsystems, identifying the subsystem of type 3^85^1 with the one on the infinity points. This yields a 3-

GDD of type $3^{6s+8}5^1$ with the required subsystems. Thus we have $D(3s+4) \geq L(6s)D(s+4)^3$ for $s \geq 24$.

To summarise these results, we have that for all $s \geq 28$,
$D(3s) \geq L(6s)D(s)^3$, $D(3s-4) \geq L(6(s-2))D(s)^3$, and $D(3s-8) \geq L(6(s-4))D(s)^3$.

Lower bound for $D(s)$.

Lemma 7.6.10. $(t-4)^2 ln(t-4) > (t+\frac{5}{6})^2 ln(t+\frac{5}{6}) - (t+6)^2$ *for* $t \geq 13$.

Proof. Let $f(t) = (t-4)^2 ln(t-4) - (t+\frac{5}{6})^2 ln(t+\frac{5}{6}) + (t+6)^2$. Then $f(13) \approx 36.3 > 0$ Also $f'(t) = 2(t-4)ln(t-4) - 2(t+\frac{5}{6})ln(t+\frac{5}{6}) + 2t + 7\frac{1}{6}$, so $f'(13) \approx 0.034 > 0$, and $f''(t) = 2ln\left(\frac{t-4}{t+\frac{5}{6}}\right) + 2$, which is monotonic increasing, and $f''(13) \approx 1.14 \geq 0$. Therefore, $f'(t)$ is increasing for $t \geq 13$, and therefore so is $f(t)$. □

Lemma 7.6.11. *For* $t \geq 28$ *and* $u = t + \frac{5}{6}$, $ln(D(t)) \geq 6u^2(ln(u) - ln(84\frac{5}{6}))$, *i.e.* $D(t) \geq (ku)^{6u^2}$ *for* $k = \frac{1}{84\frac{5}{6}}$.

Proof. We have shown above that $D(t) \geq 1$ for $t \geq 28$. The result is therefore true for all $28 \leq t \leq 84$. Also, since $ln(L(n)) \geq n^2(ln(n) - 2)$, and this function is monotonic increasing, we have that $ln((D(3t))$, $ln(D(3t-4))$, $ln(D(3t-8))$ are all greater than or equal to $g(t)$ for $t \geq 28$, where $g(t) = 36(t-4)^2(ln(6(t-4)) - 2) + 3ln(D(t))$. We assume inductively that $ln(D(t)) \geq 6u^2(ln(u) - ln(84\frac{5}{6}))$, where $u = t + \frac{5}{6}$.

To complete the proof, it suffices to show that
$g(t) \geq 6(3t+\frac{5}{6})^2(ln(3t+\frac{5}{6}) - ln(84\frac{5}{6}))$ for $t \geq 28$.
Consider $h(t) = g(t) - 6(3t+\frac{5}{6})^2(ln(3t+\frac{5}{6}) - ln(84\frac{5}{6}))$. We show that $h(t) \geq 0$ for $t \geq 28$. By Lemma 7.6.10 we have
$h(t) \geq 36u^2 ln(u) - 36(t+6)^2 + 36(t-4)^2 ln(6) - 72(t-4)^2 + 18u^2 ln(u)$

$$
\begin{aligned}
&- 18u^2 ln(84\tfrac{5}{6}) - 6(3t+\tfrac{5}{6})^2 ln(3t+\tfrac{5}{6}) + 6(3t+\tfrac{5}{6})^2 ln(84\tfrac{5}{6}) \\
&= 54u^2 ln(u) - 36(t+6)^2 + 36(t-4)^2 ln(6) - 72(t-4)^2 - 18u^2 ln(84\tfrac{5}{6}) \\
&\quad - 6(3t+\tfrac{5}{6})^2 ln(3t+\tfrac{5}{6}) + 6(3t+\tfrac{5}{6})^2 ln(84\tfrac{5}{6}) \\
&\geq 54u^2 ln(u) - 36(t+6)^2 + 36(t-4)^2 ln(6) - 72(t-4)^2 - 18u^2 ln(84\tfrac{5}{6}) \\
&\quad - 6(3u)^2 ln(3u) + 6(3t)^2 ln(84\tfrac{5}{6}) \\
&= 54t^2 ln(84\tfrac{5}{6}) - 18u^2 ln(84\tfrac{5}{6}) - 36(t+6)^2 + 36(t-4)^2 ln(6) \\
&\quad - 72(t-4)^2 - 54u^2 ln(3) \\
&= t^2(36 ln(84\tfrac{5}{6}) - 36 + 36 ln(6) - 72 - 54 ln(3)) \\
&\quad - t(432 + 288 ln(6) - 576 + 30 ln(84\tfrac{5}{6}) + 90 ln(3)) \\
&\quad - (1296 - 576 ln(6) + 1152 + 12.5 ln(84\tfrac{5}{6}) + 37.5 ln(3)).
\end{aligned}
$$

$\approx 57t^2 - 604t - 1512.7 > 6083 > 0$ for $t \geq 18$, and so the lemma is proved. □

Lower bound for numbers of STS(v)

Lemma 7.6.12. *If $v = 18s+15$, and $s \geq 28$, then the number of non-isomorphic STS(v) that are decomposable into triangles is at least $\frac{1}{v!}\left(\frac{v}{1527}\right)^{\frac{v^2}{54}} = v^{v^2(c-o(1))}$ as $v \to \infty$, where $c = \frac{1}{54}$.*

Proof. As in Construction above, take a 3-GDD of type $3^{2s}5^1$. Inflate by a factor of 3, placing a $K_{3,3,3}$ across each inflated block, and STS(9)s and a decomposable STS(15) across the inflated groups. The resulting construct is a STS($18s+15$). Since all the ingredients are decomposable into triangles, so is the STS($18s+15$). The number of differently-labelled decomposable STS($18s+15$) is therefore at least $D(s) \geq \left(\frac{s+\frac{5}{6}}{84\frac{5}{6}}\right)^{6(s+\frac{5}{6})^2}$ for $s \geq 28$. This gives $D(s) \geq \left(\frac{v}{1527}\right)^{\frac{v^2}{54}}$. The largest possible size of automorphism group for an STS(v) is $v!$, so the number of distinct decomposable STS($18s+15$) is therefore at least $\frac{1}{v!}\left(\frac{v}{1527}\right)^{\frac{v^2}{54}}$ when $v = 18s+15$, $s \geq 28$.

□

This completes the proof of Theorem 7.1.6.

Bibliography

[1] L. Babai, *On the minimum order of graphs with given group*, Canad. Math. Bull. **17** (1974), 467-470.

[2] L. Babai, *Almost all Steiner triple systems are assymetric*, Annals of Discrete Mathematics **7** (1980), 37-39.

[3] L. Babai, A.J. Goodman, *Subdirectly Reducible Groups and Edge-Minimal Graphs with Given Automorphism Group*, J. London Math. Soc. **47** (1993), 417-432.

[4] R.C. Bose, *On the construction of balanced incomplete block designs*, Ann. Eugenics, **9** (1939), 353-399.

[5] M. Buratti, A. Del Fra, *Discrete Mathematics* **261** (2003), 113-125.

[6] P.J. Cameron, *Combinatorics*, Cambridge University Press, Cambridge, England 1994.

[7] C.J. Colbourn and J.H. Dinitz (eds), *The CRC Handbook of Combinatorial Designs*, 1st Ed., CRC Press 1996.

[8] C.J. Colbourn and A. Rosa, *Triple Systems*, Oxford University Press, New York 1999.

[9] R. Frucht, *Herstellung von Graphen mit Vorgegebener abstrakter Gruppe*, Compositio Math. **6** (1938), 239-250.

[10] R. Frucht, *Graphs of Degree Three with a Given Abstract Group*, Canadian Journal of Math. **1** (1949), 365-378.

[11] M.J. Grannell and T.S. Griggs, *Configurations*, in Chapman and Hall/CRC Research Notes in Math., (ed. F.C.Holroyd, K.A.S. Quinn, C. Rowley and B.S. Webb), **403** (1999), 103-126.

[12] P. Horák, A. Rosa, *Decomposing of Steiner triple systems into small configurations*, Ars. Combin. **26** (1988), 91-105.

[13] T.P. Kirkman, *On a problem in combinations*, Cambridge and Dublin Math. Journal **2** (1847), 191-204.

[14] G.J. Lovegrove, *The automorphism groups of Steiner triple systems obtained by the Bose construction*, Journal of Algebraic Combinatorics, **18** (2003), 159-170.

[15] S. MacLane and G. Birkhoff, *Algebra*, MacMillan, London 1967.

[16] E. Mendelsohn, *On Groups of Automorphisms of Steiner Triple and Quadruple Systems*, Journal Of Combinatorial Theory, Series A, **25** (1978), 97-104.

[17] R.C. Mullin, A.L. Poplove and L. Zhu, *Decomposition of Steiner triple systems into triangles*, J. Comb. Math. Comb. Comput. **1** (1987), 149-174.

[18] A.P. Street and D.J Street, *Combinatorics of Experimental Design*, Clarendon Press, Oxford, 1987.