MINIMAL DEFINING SETS IN A FAMILY OF STEINER TRIPLE SYSTEMS

REBECCA A. H. GOWER

Centre for Combinatorics
Department of Mathematics
The University of Queensland
Qld 4072 Australia

Dedicated to the memory of Alan Rahilly, 1947 – 1992

Abstract

A defining set of a block design is a subset of the blocks of the design which are a subset of no other design with the same parameters. This paper describes and proves the existence of a certain type of set of blocks in the infinite family of Steiner triple systems isomorphic to the points and lines of the projective geometries over GF(2). It is then proven that these sets of blocks are defining sets for the designs and furthermore that they are minimal defining sets.

1. Introduction.

In 1990 Gray [2] introduced the notion of defining sets of block designs. Some work has been done into the study of defining sets for a number of designs with small parameters. Some lower bounds on the minimum size of defining sets have been found and while these can be applied to designs with large parameters, little is known in the way of actual examples of defining sets for designs with large parameters. In this paper a class of minimal defining set for the infinite family of Steiner Triple Systems isomorphic to the points and lines of projective geometries over $GF(2)$ is presented. In some of the small–parameter members of this family the results could be obtained by manual or computer calculation but this work goes well beyond the scope of computer searches.

The first part of this work makes use of the fact that a Steiner Triple System can be characterised by a loop. The operation table of this algebra is a Latin square. There is a relationship between critical sets in the Latin square afforded by the loop and defining sets in the Steiner Triple Systems. A result of Stinson and van Rees [6]

The author would like to thank both Diane Donovan and Sheila Oates–Williams for their help with this paper .

about critical sets is used to help prove a result about defining sets for the infinite family of Steiner Triple Systems described above.

The second part of this work makes use of the structure of the geometry to prove that the defining sets are minimal.

2. Definitions and preliminaries.

Definition 2.1. A *Steiner Triple System* of order v, sometimes denoted by $STS(v)$, is a set V of size v, and a collection $\mathcal{B}$ of subsets of V, each of size 3 such that each pair of elements of V occurs in precisely one of these subsets. A necessary and sufficient condition for the existence of Steiner Triple Systems is that $v \equiv 1$ or 3 (mod 6). STS is often used as an abbreviation for Steiner Triple System and will be used for that purpose from time to time in this paper. (For $n \geq 7$ Steiner Triple Systems are $BIBD(v, b, r, k, \lambda)$ with $k = 3$ and $\lambda = 1$.)

Let $\mathcal{V}$ denote a vector space of dimension $d+1$ over $GF(q)$, the Galois Field of order q.

Definition 2.2. The projective geometry associated with $\mathcal{V}$, denoted by $PG(\mathcal{V})$, has as points the 1–dimensional subspaces of $\mathcal{V}$, as lines the 2–dimensional subspaces and, in general, r–dimensional projective geometric objects are given by the $(r+1)$–dimensional subspaces of $\mathcal{V}$. Incidence is set–theoretic inclusion. The dimension of $PG(\mathcal{V})$ is one less than the dimension of the vector space $\mathcal{V}$; since $\mathcal{V}$ was defined to have dimension $d+1$, $PG(\mathcal{V})$ has dimension d. The geometry $PG(\mathcal{V})$ is sometimes denoted by $PG(d, q)$ and this is the notation which will be used most often in this paper.

In the case of $q = 2$ the projective points are simply the nonzero vectors of $\mathcal{V}$.

Definition 2.3. A subspace of $PG(d, q)$ of dimension $d-1$ is called a *hyperplane.*

This paper is concerned only with those Steiner Triple Systems of order $2^{d+1} - 1$ for $d = 2, 3, 4, \ldots$ which are isomorphic to the point-line designs of $PG(d, 2)$. Here the vertex–set of the Steiner Triple System corresponds to the point–set of the projective geometry and the blocks of the Steiner Triple System correspond to the lines of the projective geometry. This paper will make repeated use of the structure within the geometries.

Definition 2.4. A *loop* is a set S together with a binary operation $\circ$ such that S is closed under the binary operation $\circ$, there is an identity element with respect to $\circ$ and in the equation $x \circ y = z$ the choice of any two of the three elements x, y and z uniquely determines the third element.

A Steiner Triple System with vertex set V can be used to construct a loop. The set S on which the loop is based is the set $V \cup \{e\}$ where e is the identity element and the operation $\circ$ is defined in the following way:

(i) $(\forall v \in V \cup \{e\})(v \circ v = e)$;
(ii) $(\forall v \in V)(v \circ e = v = e \circ v)$;
(iii) $(\forall u, v \in V, u \neq v)(v \circ u = z$ and $u \circ v = z)$ if and only if (u, v, z) is a block of the Steiner Triple System.

This is a loop with some extra properties. It is called a *Steiner loop* or *sloop*.

Conversely, a Steiner loop can be used to construct a Steiner Triple System, (see Ganter and Werner [1]). It is said that the sloop *co–ordinatizes* the STS and vice versa. Hence it can be seen that there is a one–to–one correspondence between sloops and Steiner Triple Systems.

Definition 2.5. A *Latin square* of order n is an $n \times n$ array with entries chosen from a set of size n such that each entry occurs precisely once in each row and column.

The operation table of a loop is a Latin square.

Definition 2.6. A *partial Latin square* P of order n is an $n \times n$ array with entries chosen from a set of size n in such a way that each element occurs at most once in each row and each column. Then P may contain a number of empty cells. So P may be written as $\{(i,j;k)|i,j \in \{1,\ldots,n\}, k \in K\}$, where K is the set of entries of the partial Latin square and $|K| = n$. Then a triple $(i,j;k)$ is in this set if and only if the (i,j) position of the partial Latin square has entry k.

Definition 2.7. A partial Latin square P of order n, $P = \{(i,j;k)|i,j \in \{1,\ldots,n\}, k \in K\}$, where K is the set of entries of the partial Latin square and $|K| = n$, is said to be *uniquely completable* (or P has (UC)) if there is one and only one Latin square of order n which has element k in position (i,j) for each $(i,j;k) \in P$.

Definition 2.8. A *critical set* in a Latin square L is a partial Latin square P, which is uniquely completable to L with the property that no proper subset of P has (UC).

Definition 2.9. A set of blocks which is a subset of a unique $STS(v)$ is said to be a *defining set* of the design.

Definition 2.10. A *minimal defining set* is a defining set, no proper subset of which is a defining set.

Critical sets are to Latin squares as minimal defining sets are to designs.

3. Results about partial Latin squares.

In the last section it was shown how to construct a loop from the blocks of a Steiner Triple System and it was observed that the operation table of the loop is a Latin square. In this manner a Latin square can be obtained from a Steiner Triple System.

Suppose that instead of knowing the complete set of blocks $\mathcal{B}$, of the STS, just the blocks of a subset, D, of $\mathcal{B}$ are known. In this case a partial Latin square can be obtained from D by defining the loop operation only for those pairs of elements from $V \cup \{e\}$ about which there is some information. Let $W = \{w|w \in V$ and $w \in B\}$ where B is a block of D. Define $\circ$ by:

(i) $(\forall v \in W \cup \{e\})(v \circ v = e)$;
(ii) $(\forall v \in W)(v \circ e = v = e \circ v)$;
(iii) $(\forall u, v \in W, u \neq v)(v \circ u = z$ and $u \circ v = z)$ if and only if $(u,v,z) \in D$.

Example 3.1. Consider the Steiner Triple System of order 7 with blocks $(1,2,3)$, $(1,4,5),(1,6,7),(2,4,6),(2,5,7),(3,5,6)$ and $(3,4,7)$. Let $D = \{(1,2,3),(1,4,5),$

$(2,4,6)\}$. (Incidentally, D is a minimal defining set for this STS, [2].) Then $W = \{1,2,3,4,5,6\}$ and the resulting partial Latin square is:

e	1	2	3	4	5	6	$*$
1	e	3	2	5	4	$*$	$*$
2	3	e	1	6	$*$	4	$*$
3	2	1	e	$*$	$*$	$*$	$*$
4	5	6	$*$	e	1	2	$*$
5	4	$*$	$*$	1	e	$*$	$*$
6	$*$	4	$*$	2	$*$	e	$*$
$*$	$*$	$*$	$*$	$*$	$*$	$*$	$*$

The *'s have been used to indicate blank entries in the array and K is fixed to be the set $\{e,1,2,3,4,5,6,7\}$.

Definition 3.2. An element, p of a partial Latin square P is *2–essential* if there is a 2×2 subsquare S of the Latin square L such that $(P \setminus \{p\}) \cap S$ does not have (UC) in S.

A partial Latin square of order 2 needs only one entry to be uniquely completable (for fixed K), so $(P \setminus \{p\}) \cap S$ does not have (UC) if and only if $(P \setminus \{p\}) \cap S = \emptyset$.

Definition 3.3. A partial Latin square P is *2–critical* if it has unique completion to the Latin square L and every element p of P is 2–essential.

For a partial Latin square to be 2–critical is a special case of the partial Latin square being a critical set.

Example 3.1 cont. The partial Latin square shown previously completes uniquely to the following Latin square.

e	1	2	3	4	5	6	7
1	e	3	2	5	4	7	6
2	3	e	1	6	7	4	5
3	2	1	e	7	6	5	4
4	5	6	7	e	1	2	3
5	4	7	6	1	e	3	2
6	7	4	5	2	3	e	1
7	6	5	4	3	2	1	e

Furthermore, removing any entry from the partial Latin square results in a new partial Latin square which has an empty intersection with one of the 2×2 subsquares of the Latin square, so this partial Latin square is 2–critical.

The interest in constructing a partial Latin square from a subset, D, of the set of blocks of a Steiner Triple System is due to the following lemma which transforms information about the partial Latin square into information about D, the subset of blocks.

Lemma 3.4. *Suppose D is a subset of, $\mathcal{B}$, the set of blocks of a Steiner Triple System of order v and that the blocks of D are used to construct a partial Latin square in the manner described earlier in this section. If this partial Latin square has (UC) then the set of blocks, D, is a defining set for the STS.*

Proof. Suppose D is not a defining set, then there are (at least) two different Steiner Triple Systems of order v containing D. Then each of these STS's can be co–ordinatized as a sloop on $v+1$ elements. These sloops must be distinct (or the STS's would not be distinct) and they must contain the partial Latin square constructed from D.

Therefore the partial Latin square constructed from D does not have (UC).

Hence by the contrapositive, D is a defining set for the Steiner Triple System. □

At this point it is convenient to introduce another lemma which is a combination of two results of Stinson and van Rees, but there are a few details to consider first.

Notation 3.5. The abelian group of order 2 is denoted by C_2.

Definition 3.6. Let L be a Latin square of order n with entries $\{0,1,\ldots,n-1\}$ and M be a Latin square of order m with entries $\{0,1,\ldots,m-1\}$. Define L^r to be the array obtained from L by adding rn to each entry of L, for $r = 0,1,\ldots,m-1$. The *direct product* of M with L is the $mn \times mn$ array L^* constructed by replacing the entry r in M by the array L^r.

Example 3.7. The direct product of C_2 with a Latin square L is:

$$L^* = \begin{array}{cc} L^0 & L^1 \\ L^1 & L^0 \end{array}$$

Since the array L^0 is identical to the array L, the superscript is left off in the remainder of this paper.

Lemma 3.8. *(Due to Stinson and van Rees [6].) Given L, a Latin square of order n, and C, a 2–critical set of L, then in the Latin square L^* of order $2n$ which is the direct product of C_2 with L, the partial Latin square C^* is 2–critical, where*

$$C^* = \begin{array}{cc} L & C^1 \\ C^1 & C \end{array}$$

and C^1 is the appropriate image of C in L^1.

Proof. Firstly it is necessary to show that C^* has (UC). Consider the top, right–hand $n \times n$ subarray of C^*. Remember that C^* is being completed to a Latin square so each entry can only occur once in a row. Since each element of the set of entries of L occurs precisely once in the columns 1 to n of each of the rows 1 to n, none of the entries of the Latin square L can occur in columns $n+1$ to $2n$ of these rows. Hence the entries of the top right–hand $n \times n$ subarray can only be elements of the set of entries of L^1. Since C^1 has unique completion to L^1 on that set of entries, the top right–hand $n \times n$ subarray can be completed to L^1 alone.

Similarly, the bottom left–hand $n \times n$ subarray can complete only to L^1.

Now the columns $n+1$ to $2n$ of the rows $n+1$ to $2n$ are forced to contain none of the entries of L^1 because all these entries have already occurred in these rows and in these columns. Therefore they can only contain entries of L but C has unique completion to L on that set of entries, so the bottom right–hand $n \times n$ subarray can complete only to L.

Hence C^* uniquely completes to L^*.

Secondly, it must be shown that for every element c of C^* there is a 2×2 subsquare S of L^* such that $(C^* \setminus \{c\}) \cap S$ does not have (UC) in S. That is to say, each element c is 2–essential.

Recall that C^* has the following form:

$$C^* = \begin{matrix} L & C^1 \\ C^1 & C \end{matrix}$$

Suppose we first consider an element of C^* chosen from one of the $n \times n$ subarrays which is a copy of C^1 or C. Since C^1 is 2–critical in L^1 and C is 2–critical in L, by the definition of 2–critical, any element from one of these subarrays must be 2–essential.

The elements of the top left–hand $n \times n$ subarray, which is a copy of L, must be considered in two parts; those belonging to $L \setminus C$ and those elements of L which are also in C.

Consider an element of the top left–hand $n \times n$ subarray which is one of the elements of $L \setminus C$. Suppose this element is the entry x in position (i,j) of the $2n \times 2n$ array L^*, then there is a subsquare of L^* which makes this element 2–essential. The other elements of this subsquare have as their entries and respective positions, $x+n$ in $(i, j+n)$, $x+n$ in $(i+n, j)$ and x in $(i+n, j+n)$, none of which are in C^* since they belong to $L^1 \setminus C^1$ and $L \setminus C$ respectively.

Now consider an element of the top left–hand $n \times n$ subarray which is one of the elements of C. Suppose this element is the entry x in position (i,j) of C and hence of C^* too. Since C is 2–critical, there must be a 2×2 subsquare of L, called S say, which makes x 2–essential. Suppose S has as elements; the entry x in position (i,j), y in position (i,k), y in position (l,j) and x in position (l,k). These last three elements of L are not elements of C. Consequently, $y+n$ in positions $(i, k+n)$ and $(l+n, j)$ and x in position $(l+n, k+n)$ are not elements of the partial Latin square C^*. These three elements of L^* and the entry x in position (i,j) form a 2×2 subsquare of L^* and so the entry x in position (i,j) is 2-essential in C^*.

Hence every entry of C^* is 2–essential and so C^* is 2–critical. □

4. The defining sets and their geometric structure.

As mentioned earlier, this paper is concerned only with the family of Steiner Triple Systems which are isomorphic to the point–line designs of the projective geometries over $GF(2)$. The main theorem of this paper is about defining sets for this family of designs. The blocks which belong to the defining set are chosen according to the structure of the geometry.

Define a set of type $\mathcal{H}$ to be a set of $d+1$ hyperplanes of $PG(d,2)$, for $d \geq 2$, with the property that there is no point of $PG(d,2)$ incident with all of these $d+1$ hyperplanes.

Theorem 4.1. *Consider the Steiner Triple System of order $2^{d+1}-1$ which is isomorphic to the point–line design of $PG(d,2)$ for $d \geq 2$. The set of blocks of this $STS(2^{d+1}-1)$ which correspond to the lines of the hyperplanes of a set of type $\mathcal{H}$ is a defining set for this design.*

The proof of this theorem will be given later, first it is necessary to introduce some lemmas and definitions.

Lemma 4.2. *A set of type $\mathcal{H}$ exists for each $PG(d,2), d \geq 2$.*

Proof. Consider the set of hyperplanes with equations;

$$\begin{aligned}
1x_d + 0x_{d-1} + 0x_{d-2} + \cdots + 0x_1 + 0x_0 &= 0 \\
0x_d + 1x_{d-1} + 0x_{d-2} + \cdots + 0x_1 + 0x_0 &= 0 \\
&\vdots \\
0x_d + 0x_{d-1} + 0x_{d-2} + \cdots + 1x_1 + 0x_0 &= 0 \\
0x_d + 0x_{d-1} + 0x_{d-2} + \cdots + 0x_1 + 1x_0 &= 0
\end{aligned}$$

where the $x_0, x_1, x_2, \ldots, x_d$ are the co–ordinates of points lying in the hyperplane with respect to a set of $d+1$ basis vectors of the underlying vector space.

This is a set of $d+1$ hyperplanes with no common point. Suppose the point $(x_0, x_1, \ldots, x_d)$ is common to all these hyperplanes then $x_0 = x_1 = \cdots = x_d = 0$ and the zero vector does not correspond to a point of the projective space. □

Of particular use in projective geometry is the Principle of Duality which is explained in Hirschfeld [3, p.31] as follows. To any $\mathcal{S} = PG(d,q)$, there is a *dual space* $\mathcal{S}^*$, whose points and hyperplanes are respectively the hyperplanes and points of $\mathcal{S}$. For any theorem which is true in $\mathcal{S}$, there is an equivalent theorem which is true in $\mathcal{S}^*$. In particular, if T is a theorem in $\mathcal{S}$ stated in terms of points, hyperplanes and incidence, the same theorem is true in $\mathcal{S}^*$ and gives a dual theorem T^* in $\mathcal{S}$ by interchanging 'point' and 'hyperplane' whenever they occur. Hence the dual of an r–space in $PG(d,q)$ is an $(n-r-1)$–space.

Definition 4.3. A *frame* of $PG(d,q)$ is an ordered set of $d+2$ points such that no $d+1$ points chosen from this set are incident with a single hyperplane of the space.

Let $\mathcal{S}$ and $\mathcal{S}'$ be two projective spaces, $PG(d,q)$.

Definition 4.4. A *projectivity* is a bijection $\Phi : \mathcal{S} \to \mathcal{S}'$ given by a non–singular matrix T. (T is the matrix of a linear transformation from the underlying vector space of $\mathcal{S}$ to the underlying vector space of $\mathcal{S}'$.)

Definition 4.5. A *collineation* $\Phi : \mathcal{S} \to \mathcal{S}'$ is a bijection which preserves incidence.

A projectivity is a collineation.

If $\mathcal{S} = \mathcal{S}'$, the set of collineations of $PG(d,q)$ is precisely the set of automorphisms of $PG(d,q)$ and the set of projectivities is a subset of $Aut(PG(d,q))$.

The following lemma is taken from Hirschfeld, [3, p.30] and is stated without proof.

Lemma 4.6. *If $F_1 = \{p_1, p_2, \ldots, p_{d+2}\}$ and $F_2 = \{p'_1, p'_2, \ldots, p'_{d+2}\}$ are two frames of $\mathcal{S} = PG(d,q)$, then there is a unique projectivity Φ mapping F_1 to F_2 such that $p'_i = p_i\Phi$ for all $i \in \{1, 2, \ldots, d+2\}$.*

In the case of $q = 2$, that is, if $\mathcal{S} = PG(d,2)$, it suffices to give the images of p_1, $p_2, \ldots, p_{d+1}$ to determine Φ.

Definition 4.7. The *meet* of two subspaces π_r and π_s of $PG(d,q)$ is the set of points common to both π_r and π_s and is also a subspace of $PG(d,q)$.

Lemma 4.8. *For any two sets of type $\mathcal{H}$ in $PG(d,2)$, there exists an automorphism of the projective space which maps one set to the other.*

Proof. This lemma will be verified by proving the dual lemma. Define the dual of a set of type $\mathcal{H}$ to be a set of type $\mathcal{P}$. Then a set of type $\mathcal{P}$ is a set of $d+1$ points of $PG(d,2)$ with the property that there is no hyperplane of $PG(d,2)$ which is incident with all of these $d+1$ points. The statement of the dual lemma is as follows:

For any two sets of type $\mathcal{P}$ in $PG(d,2)$, there exists an automorphism of the projective space which maps one set to the other.

The $d+1$ points of a set of type $\mathcal{P}$ are a subset of a frame as are the points of any other set of type $\mathcal{P}$ in $PG(d,2)$. So by Lemma 4.6 there is a (unique) projectivity mapping the (ordered) points of one set of type $\mathcal{P}$ to the (ordered) points of the second set of type $\mathcal{P}$.

Hence by duality there is an automorphism mapping the hyperplanes of one set of type $\mathcal{H}$ to any other set of type $\mathcal{H}$. □

Lemma 4.9. *In $PG(d,2), d \geq 2$, for each set of type $\mathcal{H}$ there is exactly one point Π of $PG(d,2)$ which is incident with none of the hyperplanes of the set of type $\mathcal{H}$.*

Proof. The proof of this lemma is in three parts. Firstly it is shown that for all $d \geq 2$, there is one set of type $\mathcal{H}$ in $PG(d,2)$ such that there is *at least one* point of $PG(d,2)$ which is incident with none of the hyperplanes of this set of type $\mathcal{H}$.

Secondly it is shown that for *any* set of type $\mathcal{H}$ in $PG(d,2)$ there is at least one point of the space which is incident with none of the hyperplanes of the set of type $\mathcal{H}$.

Finally it is shown that for any set of type $\mathcal{H}$ there can be *at most one* point of $PG(d,2)$ which is incident with none of the hyperplanes of the set of type $\mathcal{H}$.

In order to verify the first step of the proof, consider the following hyperplanes

which form a set of type $\mathcal{H}$ as discussed in Lemma 4.2;

$$\begin{aligned}
1x_d + 0x_{d-1} + 0x_{d-2} + \cdots + 0x_1 + 0x_0 &= 0 \\
0x_d + 1x_{d-1} + 0x_{d-2} + \cdots + 0x_1 + 0x_0 &= 0 \\
&\vdots \\
0x_d + 0x_{d-1} + 0x_{d-2} + \cdots + 1x_1 + 0x_0 &= 0 \\
0x_d + 0x_{d-1} + 0x_{d-2} + \cdots + 0x_1 + 1x_0 &= 0
\end{aligned}$$

where the $x_0, x_1, x_2, \ldots, x_d$ are the co–ordinates of the points lying in the hyperplane in terms of a set of $d+1$ basis vectors of the underlying vector space. The point $(1,1,\ldots,1,1)$ is not incident with any of these hyperplanes, so for each $PG(d,2)$ there is a set of type $\mathcal{H}$ and a point which is incident with none of the hyperplanes of this set.

Next it is to be shown that for *any* set of type $\mathcal{H}$ of $PG(d,2)$ there exists a point which is incident with none of the hyperplanes of this set of type $\mathcal{H}$.

By Lemma 4.8 there is an automorphism, Φ, mapping the hyperplanes of the above set of type $\mathcal{H}$ to the hyperplanes of any other set of type $\mathcal{H}$. This automorphism preserves incidence so none of the hyperplanes of another set of type $\mathcal{H}$ are incident with $(1,1,\ldots,1,1)\Phi$, the image of the point $(1,1,\ldots,1,1)$ under the appropriate automorphism Φ. So there is at least one point of $PG(d,2)$ incident with none of the hyperplanes of any set of type $\mathcal{H}$.

Now it has been shown that for any set of type $\mathcal{H}$ of $PG(d,2)$ there is at least one point incident with none of the hyperplanes of this set of type $\mathcal{H}$. It remains to be shown that there is at most one such point. This will be shown by proving the dual statement which is: For any set of type $\mathcal{P}$ of $PG(d,2)$ there is at most one hyperplane incident with none of the points of this set of type $\mathcal{P}$.

Suppose there are two hyperplanes which are incident with none of the points of a set of type $\mathcal{P}$. These two hyperplanes meet each other in a $(d-2)$–space, call it S'. There are three hyperplanes incident with S' and between them they contain all the points of $PG(d,2)$, (this is a property of all $(d-2)$–spaces in $PG(d,2)$). Now, two of the three hyperplanes incident with S' are not incident with any of the points of the set of type $\mathcal{P}$, therefore, all the points of the set of type $\mathcal{P}$ must be incident with the third hyperplane which is incident with S'. This is in contradiction with the fact that a set of type $\mathcal{P}$ (defined in Lemma 4.8) is a set of $d+1$ points such that no hyperplane of $PG(d,2)$ is incident with all these points.

Hence there can be at most one hyperplane incident with none of the points of the set of type $\mathcal{P}$. Now the dual statement is proved and it can be concluded that there is at most one point which is not incident with any of the hyperplanes of a set of type $\mathcal{H}$.

Hence there must be precisely one such point Π incident with none of the hyperplanes. □

The following lemma is due to Gray [2] and is stated here without proof.

Lemma 4.10. *Suppose D is a particular defining set of a STS, $\mathcal{S}$, and $\rho \in Aut(\mathcal{S})$, then $\rho(D)$ is also a defining set of $\mathcal{S}$.*

Recall that the $STS(2^{d+1}-1)$ is isomorphic to the point–line design of $PG(d,2)$ which is $PG(\mathcal{V})$ where $\mathcal{V}$ is the $(d+1)$–dimensional vector space over GF(2). So the blocks of the STS are the lines of $PG(d,2)$ and they in turn are the 2–dimensional subspaces of $\mathcal{V}$. That is to say, three points/vertices of the STS are in a block if and only if the corresponding vectors in $\mathcal{V}$ are linearly dependent. Consequently, the sloop operation is derived from the vector addition. Hence the sloop table is both associative and commutative and is actually the elementary abelian group of order 2^{d+1}. The vectors of $\mathcal{V}$ are $(d+1)$–tuples whose entries are zeros and ones. It is possible (and sometimes convenient) to think of these vectors as being the binary representations of the numbers from 0 to $2^{d+1}-1$. Obviously, 0 corresponds to the 'zero vector' which is not a point of $PG(d,2)$, hence the points of $PG(d,2)$ can be represented in a natural fashion by the numbers from 1 to $2^{d+1}-1$.

Proof of Theorem 4.1. This is done as follows, firstly it is shown that for any dimension d, $d \geq 2$, there exists a set of type $\mathcal{H}$ such that the blocks of the $STS(2^{d+1}-1)$ which correspond to the lines incident with the hyperplanes of this set of type $\mathcal{H}$ are a defining set for the STS. Then this will be used to show that any set of type $\mathcal{H}$ will yield a defining set in this way.

Induction will be used to show the existence of a set of type $\mathcal{H}$ yielding a defining set in the $STS(2^{d+1}-1)$ for any $d \geq 2$.

Consider the case $d = 2$, suppose we write the lines of $PG(2,2)$ as $(1,2,3)$, $(1,4,5),(1,6,7),(2,4,6),(2,5,7),(3,5,6)$ and $(3,4,7)$. In this case the hyperplanes of the space are just the lines of the space. Consider the set of hyperplanes, $\{(1,2,3)$, $(1,4,5),(2,4,6)\}$, these are a set of type $\mathcal{H}$ for $PG(2,2)$ and this set of type $\mathcal{H}$ gives us a set of blocks which are a defining set for the STS(7). Furthermore, this defining set gives rise to a 2–critical partial Latin square, (see Example 3.1).

Now let $d = k, k \geq 2$. Let L be the Latin square which is the sloop table of the $STS(2^{k+1}-1)$ corresponding to $PG(k,2)$, with 0 used as the identity element. Assume that there is a set of type $\mathcal{H}$ which yields a defining set in the STS and that the blocks of this defining set give rise to a partial Latin square P which is 2–critical in L. Suppose that the hyperplanes of this set of type $\mathcal{H}$ of $PG(k,2)$ have the equations;

$$\begin{aligned}
a_{1k}x_k + a_{1k-1}x_{k-1} + \cdots + a_{11}x_1 + a_{10}x_0 &= 0\\
a_{2k}x_k + a_{2k-1}x_{k-1} + \cdots + a_{21}x_1 + a_{20}x_0 &= 0\\
&\vdots\\
a_{kk}x_k + a_{kk-1}x_{k-1} + \cdots + a_{k1}x_1 + a_{k0}x_0 &= 0\\
a_{k+1,k}x_k + a_{k+1,k-1}x_{k-1} + \cdots + a_{k+1,1}x_1 + a_{k+1,0}x_0 &= 0
\end{aligned}$$

where the constants a_{ij} are elements of GF(2) and $x_0, x_1, x_2, \ldots, x_k$ are the co–ordinates of points lying in the hyperplane with respect to a set of $k+1$ basis vectors of the underlying vector space. (The equations are written this way around

so that all points/vectors can be represented by the numbers 1 to $2^{k+1}-1$ in their binary form with the co–ordinate x_i representing the contribution of the binary component 2^i.)

Now consider the case $d = k+1$ and the hyperplanes of $PG(k+1,2)$ with equations;

$$\begin{aligned}
0x_{k+1} + a_{1k}x_k + a_{1k-1}x_{k-1} + \cdots + a_{11}x_1 + a_{10}x_0 &= 0 \\
0x_{k+1} + a_{2k}x_k + a_{2k-1}x_{k-1} + \cdots + a_{21}x_1 + a_{20}x_0 &= 0 \\
&\vdots \\
0x_{k+1} + a_{kk}x_k + a_{kk-1}x_{k-1} + \cdots + a_{k1}x_1 + a_{k0}x_0 &= 0 \\
0x_{k+1} + a_{k+1,k}x_k + a_{k+1,k-1}x_{k-1} + \cdots + a_{k+1,1}x_1 + a_{k+1,0}x_0 &= 0 \\
1x_{k+1} + 0x_k + 0x_{k-1} + \cdots + 0x_1 + 0x_0 &= 0
\end{aligned}$$

with the constants a_{ij} identical to those in the equations of the case $d = k$ above and with $x_0, x_1, x_2, \ldots, x_k$ also as in the case $d = k$ and x_{k+1} the co–ordinate in terms of the new basis vector for the underlying vector space. It is claimed that these hyperplanes form a set of type $\mathcal{H}$ in $PG(k+1,2)$. It is also claimed that the blocks of the $STS(2^{k+2}-1)$ which correspond to the lines which are incident with these hyperplanes give rise to a partial Latin square with (UC) and so these blocks are a defining set for the STS (by Lemma 3.4). Hence there is indeed a set of type $\mathcal{H}$ which yields a defining set as required.

Certainly these are a set of $d+1 = k+2$ hyperplanes; in order to prove that they form a set of type $\mathcal{H}$ all that needs to be shown is that no point of $PG(k+1,2)$ is incident with all of these hyperplanes. Suppose there is a point which is incident with all of these hyperplanes, then it must correspond to a vector with a zero–valued co–ordinate in the direction of the new basis vector x_{k+1} or it can not be incident with the last hyperplane in the list. Therefore the point may only belong to the set $\{1,2,\ldots,2^{k+1}-1\}$, but by the inductive assumption, no point from this set is incident with all of the first $k+1$ hyperplanes of the list. Whence, there can be no such point and these hyperplanes form a set of type $\mathcal{H}$.

The blocks of the STS which correspond the the lines of the hyperplanes listed above give rise to a partial Latin square P^* of order 2^{k+2}. It is claimed that P^* has the following form;

$$P^* = \begin{array}{cc} L & P^1 \\ P^1 & P \end{array}$$

where P is the 2–critical partial Latin square of order 2^{k+1} from the inductive assumption pertaining to the case $d = k$ and P^1 is a copy of P with each entry x of P replaced by $x + 2^{k+1}$. By Lemma 3.8, P^* completes uniquely to

$$L^* = \begin{array}{cc} L & L^1 \\ L^1 & L \end{array}$$

Consider the last of the hyperplane equations in the list. This hyperplane is isomorphic to $PG(k,2)$ and the lines incident with this hyperplane correspond to

blocks of a subdesign of the $STS(2^{k+2}-1)$. This subdesign is isomorphic to the $STS(2^{k+1}-1)$ and its blocks give rise to the top left-hand, $2^{k+1} \times 2^{k+1}$ array of the partial Latin square P^*.

Now consider the first $k+1$ equations of the list which correspond to the equations of the hyperplanes in the case $d = k$. Suppose that in the case $d = k$, the block (i,j,l) corresponds to a line of $PG(k,2)$ which is incident with the hyperplane with the m^{th} equation. Then the partial Latin square P would have entry l in the (i,j) position, entry j in the (i,l) position, entry i in the (j,l) position etc. Since the block (i,j,l) corresponds to a line which satisfies the m^{th} equation in the $d = k$ case, this block still corresponds to a line which satisfies the m^{th} equation in the $d = k+1$ case (as the equation is unchanged except for a term with a zero–valued coefficient in the co–ordinate associated with the new basis vector). Further, the blocks $(i, j+2^{k+1}, l+2^{k+1}), (i+2^{k+1}, j, l+2^{k+1})$ and $(i+2^{k+1}, j+2^{k+1}, l)$ also correspond to lines which satisfy the m^{th} equation in the $d = k+1$ case. So in the partial Latin square constructed (in the method of Section 3) from the blocks of the STS which correspond to lines of the projective space which satisfy these equations, the blocks listed above would lead to the entry $l+2^{k+1}$ in the $(i, j+2^{k+1})$ position, the entry $l+2^{k+1}$ in the $(i+2^{k+1}, j)$ position and the entry l in the $(i+2^{k+1}, j+2^{k+1})$ position and so on. These entries all occur in these positions in P^*.

Suppose also that in the case $d = k$, the point i is incident with the m^{th} hyperplane. That is, the binary form of the number i when considered as vector co–ordinates, satisfies the m^{th} hyperplane equation. Then the partial Latin square P has entries; i in the positions $(0,i)$ and $(i,0)$ and an entry of 0 in the position (i,i). Now, in the case $d = k+1$, the block $(i, 2^{k+1}, i+2^{k+1})$ of the STS corresponds to a line which satisfies the m^{th} hyperplane equation. This leads to entries; $i+2^{k+1}$ in $(0, i+2^{k+1})$ and $(i+2^{k+1}, 0)$; and 0 in position $(i+2^{k+1}, i+2^{k+1})$ from the rules (i) and (ii) about constructing a partial Latin square from a subset of the blocks. From the rule (iii) the following entries are obtained; i in position $(2^{k+1}, i+2^{k+1})$ and $(i+2^{k+1}, 2^{k+1})$; 2^{k+1} in positions $(i, i+2^{k+1})$ and $(i+2^{k+1}, i)$ (these form the entries of the diagonals of the top right–hand and bottom left–hand $2^{k+1} \times 2^{k+1}$ arrays); and $i+2^{k+1}$ in the positions $(i, 2^{k+1})$ and $(2^{k+1}, i)$. These entries all occur in these positions in P^*.

Hence by induction it is shown that there is a set of type $\mathcal{H}$ for each d which yields a defining set for the $STS(2^{d+1}-1)$. Now it remains to be shown that any set of type $\mathcal{H}$ will yield a defining set.

By Lemma 4.8, for any two sets of type $\mathcal{H}$ of $PG(d,2)$ there is an automorphism of $PG(d,2)$ which maps the hyperplanes (and the points and lines incident with them) of one set of type $\mathcal{H}$ to the other. By Lemma 4.10, if Φ is an automorphism of the $STS(2^{d+1}-1)$ and D is a defining set for the STS then so is $(D)\Phi$. Since it has been shown that for all $d \geq 2$ there is a set of type $\mathcal{H}$ which yields a defining set and there is an automorphism which maps this set of type $\mathcal{H}$ to any other set of type $\mathcal{H}$ then all sets of type $\mathcal{H}$ yield defining sets. □

From the structure of the partial Latin square P^* described in the last proof, it is apparent that the number of blocks in a defining set arising from a set of type $\mathcal{H}$ in $PG(d,2)$ can be determined as follows. Let $D(d)$ denote such a defining set in

the STS isomorphic to $PG(d,2)$. Then

$$|D(d)| = \text{number of lines of } PG(d-1,2) + \text{ number of points incident with the hyperplanes of a set of type } \mathcal{H} \text{ of } PG(d-1,2) + 3|D(d-1)|$$

The first term comes from the top left–hand $2^d \times 2^d$ array; the entries of this array are due to blocks of the STS which correspond to the lines of a complete hyperplane. The final term comes from the copies of P and P^1, the number of blocks needed to produce these entries is 3 times the number of blocks needed to produce the entries in one of these arrays and that number is the number of blocks from a defining set of this class in the STS isomorphic to $PG(d-1,2)$. The middle term is obtained from the blocks of type $(i, 2^d, i+2^d)$ which were discussed in the last proof, these blocks contribute entries to the main diagonals of the subarrays P and to the head–line and side–line of the subarray P^1 etc. There is one of these blocks for each point incident with a hyperplane of a set of type $\mathcal{H}$ of $PG(d-1,2)$.

Now, the number of lines of $PG(d-1,2)$ is equal to the number of blocks of the $STS(2^d-1)$ and the number of blocks of an $STS(v) = \frac{v(v-1)}{6}$, see Lindner [4]. Also, by Lemma 4.9 the number of points in a set of type $\mathcal{H}$ is one less than the number of points in the geometry which for $PG(d-1,2)$ is 2^d-1. Hence,

$$\begin{aligned}
|D(d)| =& \frac{(2^d-1)((2^d-1)-1)}{6} + ((2^d-1)-1) + 3|D(d-1)| \\
=& (2^d-2)\left(\frac{2^d-1}{6}+1\right) + 3|D(d-1)| \\
=& 2(2^{d-1}-1)(\tfrac{1}{6})((2^d-1)+6) + 3|D(d-1)| \\
=& (\tfrac{1}{3})(2^d+5)(2^{d-1}-1) + 3|D(d-1)| \\
=& \sum_{i=0}^{k}(3^{i-1}(2^{d-i}+5)(2^{d-1-i}-1)) + 3^{k+1}|D(d-1-k)|
\end{aligned}$$

Now, sets of type $\mathcal{H}$ are defined only for $d \geq 2$ so $D(d)$ is only defined for $d \geq 2$. Therefore, in the expression above $d-1-k$ must be greater than or equal to two. Set $d-1-k = 2$, then $k = d-3$ and $k+1 = d-2$, so,

$$|D(d)| = \sum_{i=0}^{d-3}(3^{i-1}(2^{d-i}+5)(2^{d-1-i}-1)) + 3^{d-2}|D(2)|$$

Now $|D(2)| = 3$, therefore,

$$\begin{aligned}
|D(d)| =& \sum_{i=0}^{d-3}(3^{i-1}(2^{d-i}+5)(2^{d-1-i}-1)) + 3^{d-2}.3 \\
=& 3^{d-1} + \sum_{i=0}^{d-3}(3^{i-1}(2^{d-i}+5)(2^{d-1-i}-1))
\end{aligned}$$

It is possible to rewrite this without the summation sign. The first step is to multiply out the factors in the above expression.

$$
\begin{aligned}
|D(d)| =& 3^{d-1} + \sum_{i=0}^{d-3} \left(\frac{3^i 2^d}{3.2^i} + \frac{3^i 5}{3}\right)\left(\frac{2^d}{2^{1+i}} - 1\right) \\
=& 3^{d-1} + \sum_{i=0}^{d-3} \left[\left(\frac{3^i 2^d}{3.2^i}\right)\left(\frac{2^d}{2.2^i}\right) + \left(\frac{3^i 5}{3}\right)\left(\frac{2^d}{2^i.2}\right) - \left(\frac{3^i 2^d}{3.2^i}\right) - 3^i\left(\frac{5}{3}\right)\right] \\
=& 3^{d-1} + \sum_{i=0}^{d-3} \left[\left(\frac{3^i}{2^i 2^i}\right)\left(\frac{2^d 2^d}{3.2}\right) + \left(\frac{3^i}{2^i}\right)\left[\left(\frac{5.2^d}{3.2}\right) - \left(\frac{2^d}{3}\right)\right] - 3^i\left(\frac{5}{3}\right)\right] \\
=& 3^{d-1} + \sum_{i=0}^{d-3} \left[\left(\frac{3}{4}\right)^i \left(\frac{4^d}{6}\right) + \left(\frac{3}{2}\right)^i \left(\frac{2^d}{3}\right)\left(\frac{5}{2} - 1\right) - 3^i\left(\frac{5}{3}\right)\right]
\end{aligned}
$$

Now this can be broken into three separate summations.

$$
|D(d)| = 3^{d-1} + \sum_{i=0}^{d-3} \left(\frac{3}{4}\right)^i \left(\frac{4^d}{6}\right) + \sum_{i=0}^{d-3} \left(\frac{3}{2}\right)^i \left(\frac{2^d}{3}\right)\left(\frac{3}{2}\right) - \sum_{i=0}^{d-3} 3^i \left(\frac{5}{3}\right)
$$

Each of these summations is the sum of the first $d-2$ terms of a geometric series. This is used to rewrite the expression without the summations as follows.

$$
\begin{aligned}
|D(d)| =& 3^{d-1} + \left(\frac{4^d}{6}\right)\left[\frac{1-(\frac{3}{4})^{d-2}}{1-(\frac{3}{4})}\right] + \left(\frac{2^d.3}{3.2}\right)\left[\frac{(\frac{3}{2})^{d-2}-1}{(\frac{3}{2})-1}\right] - \left(\frac{5}{3}\right)\left[\frac{3^{d-2}-1}{3-1}\right] \\
=& 3^{d-1} + \left(\frac{4^d}{3.2}\right)\left[\frac{1-(\frac{3}{4})^{d-2}}{\frac{1}{4}}\right] + \left(\frac{2^d}{2}\right)\left[\frac{(\frac{3}{2})^{d-2}-1}{\frac{1}{2}}\right] - \left(\frac{5}{3}\right)\left[\frac{3^{d-2}-1}{2}\right] \\
=& 3^{d-1} + (\tfrac{2}{3})4^d\left[1 - \left(\frac{3^{d-2}}{4^{d-2}}\right)\right] + (2^d)\left[\left(\frac{3^{d-2}}{2^{d-2}}\right) - 1\right] - (\tfrac{5}{6})[3^{d-2}-1] \\
=& 3^{d-1} + [(\tfrac{2}{3})4^d - (\tfrac{2}{3})(4^2 3^{d-2})] + [(2^2 3^{d-2}) - 2^d] - (\tfrac{5}{6})[3^{d-2}-1] \\
=& (\tfrac{2}{3})4^d + [3 + 2^2 - (\tfrac{2}{3})4^2 - (\tfrac{5}{6})]3^{d-2} - 2^d + (\tfrac{5}{6}) \\
=& (\tfrac{2}{3})4^d - (\tfrac{9}{2})3^{d-2} - 2^d + (\tfrac{5}{6}) \\
=& (\tfrac{2}{3})4^d - (\tfrac{1}{2})3^d - 2^d + (\tfrac{5}{6})
\end{aligned}
$$

5. Minimality of these defining sets.

Not only are the sets of Theorem 4.1 defining sets, they are also minimal defining sets for these STS's. That is the main theorem of this section, but before the theorem is stated and proved some more definitions and lemmas are introduced.

Lemma 5.1. *The* $\binom{d+1}{2}$ *meets of the* $d+1$ *hyperplanes of a set of type* $\mathcal{H}$ *of* $PG(d,2)$ *are all distinct,* $(d \geq 2)$.

Proof. The hyperplanes of a set of type $\mathcal{H}$ all meet each other in $(d-2)$–spaces of $PG(d,2)$ and each $(d-2)$–space of $PG(d,2)$ is incident with three hyperplanes of

the space. Suppose not all the meets are distinct, then there are three hyperplanes of this set of type $\mathcal{H}$ which meet each other in a common $(d-2)$–space. Then between them these three hyperplanes are incident with all the points of $PG(d,2)$ but this contradicts Lemma 4.9 which states that there is precisely one point of the space which is incident with none of the hyperplanes of a set of type $\mathcal{H}$. □

Lemma 5.2. *Consider a set of type $\mathcal{H}$ of $PG(d,2)$ and let π be a hyperplane of $PG(d,2)$ such that π is not one of the hyperplanes of the set of type $\mathcal{H}$. Let $S_1, S_2, \ldots, S_{d+1}$ be the $(d-2)$–spaces in which π meets each of the $d+1$ hyperplanes of the set of type $\mathcal{H}$, then at most one pair of the subspaces $S_1, S_2, \ldots S_{d+1}$ is not distinct. That is to say, either d or $d+1$ of these subspaces are distinct.*

Proof. Suppose that only $d-1$ of the subspaces $S_1, S_2, \ldots, S_{d+1}$ are distinct. Then either three of the hyperplanes of the set of type $\mathcal{H}$ all meet π in a single $(d-2)$–space or there are two pairs of hyperplanes of this set of type $\mathcal{H}$ such that both the hyperplanes of each pair meet π in the same $(d-2)$–space.

By Lemma 5.1, which states that the pair–wise meets of the hyperplanes of a set of type $\mathcal{H}$ are distinct, the former supposition that three hyperplanes of this set of type $\mathcal{H}$ all meet π in a single $(d-2)$–space can not be correct.

So it must be the case that two pairs of hyperplanes of the set of type $\mathcal{H}$ meet each other in common $(d-2)$–spaces of π. That is, there must be hyperplanes H_i, H_j, H_k, H_l in the set of type $\mathcal{H}$ such that H_i and H_j both meet π in S_i and H_k and H_l both meet π in S_k. Now S_i and S_k are both $(d-2)$–spaces of π and therefore meet each other in a $(d-3)$–space of π, call it T^*. So there are four hyperplanes of the set of type $\mathcal{H}$ which are all incident with this $(d-3)$–space, T^*.

Consider one of these four hyperplanes, say H_i then the other d hyperplanes of the set of type $\mathcal{H}$ meet H_i in d $(d-2)$–spaces which are all distinct by Lemma 5.1. That is to say, the $(d-1)$–space, H_i, contains d $(d-2)$–spaces which cannot have a common point (or there would be a point common to all the hyperplanes of the set of type $\mathcal{H}$) so these d $(d-2)$–spaces form a set of type $\mathcal{H}$ in H_i. Now these $(d-2)$–spaces all meet each other in $(d-3)$–spaces of H_i which by Lemma 5.1 must be distinct. However, T^* is a $(d-3)$–space which is incident with H_i and three of the other hyperplanes of the set of type $\mathcal{H}$, so three of these d $(d-2)$–spaces of H_i are also incident with T^*. In other words the $(d-3)$–space T^* is the common intersection of 3 of the d $(d-2)$–spaces of the set of type $\mathcal{H}$ in H_i which is in contradiction to the result of Lemma 5.1.

Therefore the supposition that only $d-1$ of the meets of the hyperplanes of the set of type $\mathcal{H}$ with another hyperplane π are distinct was incorrect. □

Definition 5.3. A set $\{\mathcal{T}_1, \mathcal{T}_2\}$ where $\mathcal{T}_1$ and $\mathcal{T}_2$ are distinct collections of blocks containing precisely the same pairs is called a *trade*.

Consequently, given a STS with block–set $\mathcal{B}$ and a trade $\{\mathcal{T}_1, \mathcal{T}_2\}$ such that $\mathcal{T}_1 \subseteq \mathcal{B}$ then the set $\mathcal{T}_2 \cup \{\mathcal{B} \setminus \mathcal{T}_1\}$ is another STS with the same parameters.

Such collections of blocks are sometimes described as *mutually balanced.*

The following lemma is due to Gray [**2**] and is stated without proof.

Lemma5.4. *If $\{\mathcal{T}_1, \mathcal{T}_2\}$ is a trade and $\mathcal{T}_1 \subseteq \mathcal{B}$ then any defining set of the design with block–set $\mathcal{B}$ must contain at least one block of $\mathcal{T}_1$.*

To show a defining set is minimal it is necessary to show that removing any block from the defining set results in a set of blocks which can belong to more than one design of the given parameters.

Lemma 5.5. *A defining set D of a design with block–set $\mathcal{B}$ is minimal if for each block β of D there exists a subdesign with block–set $\mathcal{B}', (\mathcal{B}' \subset \mathcal{B})$ with $\beta \in \mathcal{B}'$ such that $D \cap \mathcal{B}'$ is a defining set in $\mathcal{B}'$ but $(D \cap \mathcal{B}') \setminus \{\beta\}$ is not a defining set in $\mathcal{B}'$.*

Proof. If $D \cap \mathcal{B}'$ is a defining set in $\mathcal{B}'$ but $(D \cap \mathcal{B}') \setminus \{\beta\}$ is not, then there exists a set of blocks of $\mathcal{B}'$ which has empty intersection with $(D \cap \mathcal{B}') \setminus \{\beta\}$ but non–empty intersection with $D \cap \mathcal{B}'$, which can be substituted for by another set of blocks which also complete the subdesign. That is to say, there is a trade $\{\mathcal{T}_1, \mathcal{T}_2\}$ with $\mathcal{T}_1 \in \mathcal{B}'$ and hence $\mathcal{T}_1 \in \mathcal{B}$ too, such that the only block of $\mathcal{T}_1$ common with D is β. By Lemma 5.4 $D \setminus \{\beta\}$ is not a defining set, therefore β cannot be removed from D.

If this is true for every block, β, in D then D is minimal as no proper subset of D is a defining set. □

Lemma 5.6. *Consider the $STS(15)$ which is isomorphic to $PG(3,2)$. The set of blocks of this STS which correspond to the lines of any set of type $\mathcal{H}$ of $PG(3,2)$ are a minimal defining set for the STS.*

Proof. Consider the set of type $\mathcal{H}$ whose hyperplanes are given by the equations; $x_3 = 0, x_2 = 0, x_1 = 0$ and $x_0 = 0$ where these equations are written in the same notation as described in Section 4. Each of these hyperplanes is isomorphic to the Fano plane. These hyperplanes meet in $(d-2)$–spaces which, since $d = 3$ means that they intersect in lines.

The lines incident with the hyperplane whose equation is $x_3 = 0$ are; $(1,2,3)$, $(1,4,5), (1,6,7), (2,4,6), (2,5,7), (3,4,7)$ and $(3,5,6)$.

The lines incident with the hyperplane whose equation is $x_2 = 0$ are; $(1,2,3)$, $(1,8,9), (1,10,11), (2,8,10), (2,9,11), (3,8,11)$ and $(3,9,10)$.

The lines incident with the hyperplane whose equation is $x_1 = 0$ are; $(1,4,5)$, $(1,8,9), (1,12,13), (4,8,12), (4,9,13), (5,8,13)$ and $(5,9,12)$.

The lines incident with the hyperplane whose equation is $x_0 = 0$ are; $(2,4,6)$, $(2,8,10), (2,12,14), (4,10,14), (4,8,12), (6,8,14)$ and $(6,10,12)$.

It is sufficient to consider only the lines of one of these planes and to show that each of these is needed in the defining set to show that all the lines of these four hyperplanes are needed.

The first hyperplane meets the hyperplane with equation $x_2 = 0$ in the line $(1,2,3)$; the hyperplane with equation $x_1 = 0$ in the line $(1,4,5)$ and the hyperplane with equation $x_0 = 0$ in the line $(2,4,6)$. Suppose the block corresponding to a line which is the meet of two of these planes is removed from the defining set, then the resulting set permits a trade and is not a defining set.

For example, if $(1,2,3)$ is removed from the defining set then the trade $\{\mathcal{T}_1, \mathcal{T}_2\}$ with $\mathcal{T}_1 = \{(1,2,3), (3,13,14), (2,13,15), (1,14,15)\}$ and $\mathcal{T}_2 = \{(1,2,15), (2,3,13),$

$(13,14,15),(1,3,14)\}$ can be made as there is no longer any block of $\mathcal{T}_1$ is in the defining set.

The lines $(1,6,7),(2,5,7)$ and $(3,4,7)$ are each incident with a hyperplane of $PG(3,2)$ which is in turn incident with one of the lines which are the meets of the other three hyperplanes of the set of type $\mathcal{H}$ listed above. The removal of any one of these blocks from the defining set also results in a set which permits a trade.

For example, the line $(1,6,7)$ is incident with the hyperplane whose equation is $x_2+x_1=0$. The lines incident with this hyperplane are $(1,6,7),(1,8,9),(1,14,15)$, $(6,9,15),(6,8,14),(7,8,15)$ and $(7,9,14)$. Now the line $(1,8,9)$ is also incident with the hyperplane whose equation is $x_2=0$ and the hyperplane whose equation is $x_1=0$ so it is the meet of two of the hyperplanes of the set of type $\mathcal{H}$ listed above. Removing the block $(1,6,7)$ from the defining set permits a trade in the subdesign corresponding to this plane. The blocks $\{(1,14,15),(1,6,7),(6,9,15),(7,9,14)\}$ can be traded for $\{(1,6,15),(1,7,14),(6,7,9),(9,14,15)\}$ as no block of the first collection, besides $(1,6,7)$ is in the defining set.

Now, all lines of the plane have been shown to be necessary in the defining set except for the line $(3,5,6)$. The line $(3,5,6)$ is incident with the hyperplane whose equation is $x_2+x_1+x_0=0$ and whose lines are: $(3,5,6),(3,8,11),(3,13,14)$, $(5,11,14),(5,8,13),(6,8,14)$ and $(6,11,13)$. Removing the block $(3,5,6)$ from the defining set leaves a trade in the subdesign corresponding to this plane, namely $\{\mathcal{T}_1,\mathcal{T}_2\}$ where $\mathcal{T}_1=\{(3,5,6),(3,13,14),(5,11,14),(6,11,13)\}$ and $\mathcal{T}_2=\{(3,5,14)$, $(3,6,13),(5,6,11),(11,13,14)\}$. Although there are still three blocks of this subdesign in the defining set, namely, $(3,8,11),(5,8,13)$ and $(6,8,14)$, they are all incident with the point 8 so they are not a defining set for the subdesign. □

Consider a set of type $\mathcal{H}$ of $PG(d,2)$, let ϑ denote the point of $PG(d,2)$ which is incident with none of the hyperplanes of the set of type $\mathcal{H}$. (Such a point exists for each set of type $\mathcal{H}$ by Lemma 4.9.)

Lemma 5.7. *Given a set of type $\mathcal{H}$ of $PG(d,2), d\geq 4$, every line which is incident with one of the hyperplanes of this set is also incident with a hyperplane of the space which contains both the point ϑ and the meet of two of the hyperplanes of the set of type $\mathcal{H}$.*

Proof. Due to Penttila [5]. Firstly consider the set of type $\mathcal{H}$ which has as elements the hyperplanes with equations:

$$\begin{aligned}
1x_d+0x_{d-1}+0x_{d-2}+\cdots+0x_1+0x_0&=0\\
0x_d+1x_{d-1}+0x_{d-2}+\cdots+0x_1+0x_0&=0\\
&\vdots\\
0x_d+0x_{d-1}+0x_{d-2}+\cdots+1x_1+0x_0&=0\\
0x_d+0x_{d-1}+0x_{d-2}+\cdots+0x_1+1x_0&=0
\end{aligned}$$

where the $x_0,x_1,x_2,\ldots,x_d$ are the co–ordinates of the points lying in the hyperplane in terms of a set of $d+1$ basis vectors.

Then ϑ is the point $(1,1,\ldots,1,1)$ and the hyperplanes which contain both a meet of two hyperplanes from the set of type $\mathcal{H}$ and ϑ have equations of the form;

$$a_d x_d + a_{d-1}x_{d-1} + \cdots + a_1 x_1 + a_0 x_0 = 0$$

where precisely two of the constants a_i (chosen from $GF(2)$) have the value 1 and the rest have the value 0. So it is necessary to show that any line incident with a hyperplane of the set of type $\mathcal{H}$ above is incident with a hyperplane of this form.

Now, any line incident with a hyperplane of the set of type $\mathcal{H}$ is the span of two points/vectors $(y_0, y_1, \ldots, y_d)$ and $(z_0, z_1, \ldots, z_d)$ with $y_i = z_i = 0$ if this line is incident with the hyperplane $0x_d + 0x_{d-1} + \cdots + 0x_{i+1} + 1x_i + 0x_{i-1} + \cdots + 0x_0 = 0$ from the set of type $\mathcal{H}$. Suppose such a line is not incident with one of the hyperplanes described above. Consider the pairs (y_j, z_j) for $j \neq i$, none of these pairs can be the pair $(0,0)$ or the line would be incident with the hyperplane with equation $a_d x_d + a_{d-1}x_{d-1} + \cdots + a_1 x_1 + a_0 x_0 = 0$ where $a_i = a_j = 1$ and all the other a_k are 0. Moreover, no two pairs are equal, for if $(y_j, z_j) = (y_k, z_k)$ then the hyperplane with equation $a_d x_d + a_{d-1}x_{d-1} + \cdots + a_1 x_1 + a_0 x_0 = 0$ where $a_j = a_k = 1$ and all the rest are 0 would contain the line. Hence there are three pairs which can occur – namely $(0,1),(1,0)$ and $(1,1)$ – and each occurs at most once. But there are d pairs to consider so $d \leq 3$. Hence for $d \geq 4$ the supposition that a line incident with a hyperplane of the set of type $\mathcal{H}$ is not incident with one of these hyperplanes is incorrect.

By Lemma 4.8 this holds for any set of type $\mathcal{H}$ in $PG(\boldsymbol{d},2), d \geq 4$. □

Theorem 5.8. *The defining sets of Theorem 4.1 are minimal defining sets.*

Proof. Consider the case $d = 2$. The defining set arising from a set of type $\mathcal{H}$ in $PG(2,2)$ is minimal, see Gray [**2**].

The remainder of the proof is by induction. The basis step is the case $d = 3$, the defining set arising from a set of type $\mathcal{H}$ in $PG(3,2)$ is minimal, see Lemma 5.6.

Assume that for $d = k, k \geq 3$ the defining set arising from a set of type $\mathcal{H}$ in $PG(k,2)$ is minimal.

Consider the case, $d = k+1, k \geq 3$ so $d \geq 4$. Each block β of the defining set $D(k+1)$ arising from a set of type $\mathcal{H}$ in $PG(k+1,2)$ corresponds to a projective line, l_β, which is incident with a hyperplane of the set of type $\mathcal{H}$. By Lemma 5.7, each line l which is incident with a hyperplane of the set of type $\mathcal{H}$, is also incident with a hyperplane, π_l, which contains the meet of two hyperplanes of the set of type $\mathcal{H}$. Therefore π_l meets the hyperplanes of the set of type $\mathcal{H}$ in d distinct $(d-2)$–spaces (by Lemma 5.2). There is no point common to these d $(d-2)$–spaces, since, if this was the case there must have been a point common to all the hyperplanes of the set of type $\mathcal{H}$. Hence these d $(d-2)$–spaces of the hyperplanes π_l form a set of type $\mathcal{H}$ in π_l. That is to say the defining set $D(k+1)$ intersects the subdesign of the STS which corresponds to π_l in a defining set $D(k)$, which by the inductive assumption is minimal. Hence, by Lemma 5.5, the defining set $D(k+1)$ is minimal. □

References

1. Bernhard Ganter and Heinrich Werner, *Co-ordinatizing steiner systems*, Ann. Discrete Math. **7** (1980), 3–24.
2. Ken Gray, *On the minimum number of blocks defining a design*, Bull. Austral. Math. Soc. **41** (1990), 97–112.
3. J.W.P. Hirschfeld, *Projective geometries over finite fields*, O.U.P., Oxford, 1979.
4. C.C. Lindner, *Graph decompositions and quasigroup identities*, Le Matematiche **XLV** (1990), 83–118.
5. Tim Penttila, (private communication).
6. D.R. Stinson and G.H.J. van Rees, *Some large critical sets*, Congressus Numerantium **34** (1982), 441–455.

(Received 22/2/93)