t-blocking sets and semiovals in the Witt designs

by

Xiaomin Bao

A Thesis
Submitted to the Faculty of Graduate Studies
in Partial Fulfillment of the Requirements
for the Degree of

Doctor of Philosophy

0-612-32874-0

THE UNIVERSITY OF MANITOBA

FACULTY OF GRADUATE STUDIES

*****

COPYRIGHT PERMISSION PAGE

T-BLOCKING SETS AND SEMIOVALS IN THE WITT DESIGNS

BY

XIAOMIN BAO

A Thesis/Practicum submitted to the Faculty of Graduate Studies of The University

of Manitoba in partial fulfillment of the requirements of the degree

of

DOCTOR OF PHILOSOPHY

t-blocking sets and semiovals in the Witt designs

Xiaomin Bao

Department of Mathematics
University of Manitoba
Winnipeg, Manitoba
Canada R3T 2N2

Email: bao@cc.umanitoba.ca

ABSTRACT

We analyze the Witt designs and obtain a number of new results concerning their structures. We characterize all t-blocking sets and semiovals in the Witt designs, and determine the possible sizes of a t-blocking set, classifying them by their frequency vectors. We prove that there are only three types of semiovals in S(3,6,22), one of them has size nine, the other two have size ten; S(5,6,12) and S(4,7,23) each have only one type of semioval; but both S(4,5,11) and S(5,8,24) have no semioval at all.

1991 Mathematics Subject Classification. 05B05; 51E21.
Key words and phrases. t-design, Steiner system, Witt designs, blocking set, t-blocking set, semioval.

Contents

1. INTRODUCTION

First of all we introduce some terminology and notations which will be used in the sequel.

Definition 1.1. A *t-design* $\mathcal{D}$ is a pair $(\mathcal{V}, \mathcal{B})$, where $\mathcal{V}$ is a v-set of elements called points, $\mathcal{B}$ is a family of k-sets of $\mathcal{V}$ called blocks, such that any fixed t-set of $\mathcal{V}$ is contained in exactly λ elements of $\mathcal{B}$. We also say that $\mathcal{D}$ is a t-(v, k, λ) design.

When $\lambda = 1$, the design is called *a Steiner system* and is written $S(t, k, v)$.

A t-design is also a s-design for $s \leq t$ [56, pp. 2].

Let b denote the number of blocks in a t-design. Then for any 2-design we have $v \leq b$ (Fisher's inequality [56, pp. 4]).

A design with $v = b$ is called a *symmetric* design.

Suppose $\mathcal{D}$ is a t-(v, k, λ) design with blocks $B_1, B_2, \cdots, B_b$. The number $|B_i \cap B_j|$, $i \neq j$, is called an *intersection number* of $\mathcal{D}$. Assume that $x_1, x_2, \cdots, x_s$ are the distinct intersection numbers of $\mathcal{D}$. The x_i's and the number s sometimes provide very useful information about the design.

A symmetric 2-design can be characterized by the property that the design has precisely one intersection number [13, pp. 87].

A *quasi-symmetric* design is just a design with at most two intersection numbers x and y $(x < y)$.

Definition 1.2. Let Γ be a finite graph on v vertices. The *degree* or *valency* of a vertex x is the number of edges on x. If each vertex x has the same degree d, then the graph is said to be *regular* of degree d.

Let Γ be a regular graph of degree d, with v vertices. If

1. any two adjacent vertices are simultaneously adjacent to a other vertices,

2. any two non- adjacent vertices are simultaneously adjacent to b other vertices,

then Γ is called a *strongly regular* graph with parameters (v, b, a, d).

Definition 1.3. Let $\mathcal{D}$ be a design, and $\mathcal{V}$ and $\mathcal{B}$ be the point set and block set of $\mathcal{D}$ respectively. Let $x \in \mathcal{V}$. Define:

$$\mathcal{B}_x = \{B - \{x\} : x \in B, B \in \mathcal{B}\}, \ \mathcal{V}_x = \mathcal{V} \bigcap (\bigcup_{X \in \mathcal{B}_x} X).$$

The pair $(\mathcal{V}_x, \mathcal{B}_x)$ is called the contraction of $\mathcal{D}$ at x and we denote it by $\mathcal{D}_x$.

If $\mathcal{D}$ is a t-design, and φ is a $(t-1)$-design such that $\varphi \cong \mathcal{D}_x$, then $\mathcal{D}$ is called an *extension* of φ.

Suppose $\mathcal{D}$ is a design, B is a block of $\mathcal{D}$. Define:

$$\mathcal{D}^B = (\mathcal{V} - B, \mathcal{B} - \{B\}),$$

where $\mathcal{B} - \{B\} := \{A - B \mid A \in \mathcal{B}\}$. $\mathcal{D}^B$ is called the *residual* of $\mathcal{D}$ with respect to the block B. If $\mathcal{D}_1$ is a design, and $\mathcal{D}_1 \cong \mathcal{D}^B$, then $\mathcal{D}_1$ is said to be *embedded* in $\mathcal{D}$.

Suppose $\mathcal{D}$ is a quasi-symmetric design with two intersection numbers x and y $(x < y)$. The *block graph* of $\mathcal{D}$ is the graph whose vertices are the blocks of $\mathcal{D}$: two vertices are adjacent whenever the corresponding blocks intersect in y points.

The following five Steiner systems are called *Witt designs*:

$$S(4,5,11), S(5,6,12), S(3,6,22), S(4,7,23), S(5,8,24).$$

Witt designs are very important in combinatorial design theory. They provide good examples of the extensions of designs, quasi-symmetric designs, and strongly regular graphs.

Example 1. [52, pp. 35] *$S(3,6,22)$ is an extension of $PG(2,4)$. $S(3,6,22)$ is a quasi-symmetric design with $x = 0$, $y = 2$.*

Example 2. [52, pp. 35] *$S(4,7,23)$ is an extension of $S(3,6,22)$, and it is a two fold extension of $PG(2,4)$. It is a quasi-symmetric design with $x = 1$ and $y = 3$.*

By theorem 3.2 in [19] we know that both the block graphs of $S(3,6,22)$ and $S(4,7,23)$ are strongly regular graphs.

Witt designs also provide examples of Steiner systems with $t \geq 4$. Beside the Witt designs, there are only eight known examples of Steiner systems with $t > 4$: $S(5,6,24)$, $S(5,7,28)$, $S(5,6,48)$, $S(5,6,84)$, $S(5,6,72)$, $S(5,6,108)$,$S(5,6,132)$ and $S(5,6,168)$ [22]. Up to now there are no examples of Steiner systems with $t \geq 6$ [13]. From [29, 37, 17] we know that the only non-trivial quasi-symmetric 4-designs are $S(4,7,23)$ and its complement. Shrikhande and Sane [52] conjectured that the only non-trivial quasi-symmetric 3-designs (other than the Hadamard 3-designs) are the 3-designs related to the Witt designs or their complements. Witt designs have close relation with group theory. The automorphism groups of $S(4,5,11)$, $S(5,6,12)$,$S(3,6,22)$, $S(4,7,23)$ and $S(5,8,24)$ are the famous Mathieu groups M_{11}, M_{12}, M_{22}, M_{23} and M_{24} respectively. The five Mathieu groups were the first discovered sporadic simple groups. Historically, statisticians were the first to make a systematic and exhaustive study of block designs, particularly from the point of view of construction. In Shrikhande and Sane's words [52] "From the combinatorialist's point of view, a substantial portion of the research work in design theory centers around various characterizations of the Witt designs by their properties." The attempt to prove the existence and uniqueness of the Witt designs produced many techniques and methods, which also enhanced the theory of combinatorial designs.

The Witt designs were considered to be first constructed by Witt [57] and Carmichael [21].

Witt constructed the five Witt designs from the five Mathieu groups. He proved that M_{11}, M_{12}, M_{22}, M_{23} and M_{24} are the automorphism groups of $S(4,5,11)$, $S(5,6,12)$, $S(3,6,22)$, $S(4,7,23)$ and $S(5,8,24)$ respectively. Witt [58] also proved the uniqueness of these designs.

To construct $S(5,6,12)$, Carmichael considered the linear fractional group G modulo 11 of order $12 \cdot 11 \cdot 5 = 660$. G is a doubly transitive group of degree 12 on $\mathcal{S} = \{\infty, 0, 1, 2, \cdots, 10\}$. Select $B \subseteq \mathcal{S}$, $|B| = 6$, such that B is transformed into itself by just five elements of G. Let

$$\mathcal{B} = \{\, g(B) \mid g \in G \,\},$$

then $|\mathcal{B}| = 132$ and $(\mathcal{S}, \mathcal{B})$ is an $S(5,6,12)$. Let $\mathcal{B}_\infty = \{\, A - \{\infty\} \mid \infty \in A \in \mathcal{B} \,\}$, then $|\mathcal{B}_\infty| = 66$ and $(\mathcal{S} - \{\infty\}, \mathcal{B}_\infty)$ is an $S(4,5,11)$.

Now let G be the linear fractional group modulo 23 of order $24 \cdot 23 \cdot 11 = 6072$ and let $\mathcal{S} = \{\infty, 0, 1, 2, \cdots, 22\}$. G contains a subgroup H of order 8, such that $h(B) = B$ for all $h \in H$, where $B = \{\infty, 0, 1, 12, 15, 21, 22\}$. Let

$$\mathcal{B} = \{\, g(B) \mid g \in G \,\}.$$

Then $(\mathcal{S}, \mathcal{B})$ is an $S(5,8,24)$.

In 1969, Lüneburg [47] constructed the Witt designs by extending known structures. In his proof, Lüneburg considered the geometry of the affine plane over $GF(3)$ (for $S(4,5,11)$ and $S(5,6,12)$) and the geometry of the projective plane over $GF(4)$ (for $S(3,6,22)$, $S(4,7,23)$ and $S(5,8,24)$). Other proofs of the uniqueness of $S(3,6,22)$, $S(4,7,23)$ and $S(5,8,24)$ were given by Jónsson [40] and Iwasaki [39]. Jónsson's proof was based on the geometric aspect of an elementary abelian subgroup of order 16 and a knowledge of the geometries associated with certain subgroups of the alternating group A_8. Iwasaki's proof was based on the fact that any two blocks intersect in 0 or 2 points, in 1 or 3 points or in 0, 2 or 4 points, respectively. From this the blocks can be determined explicitly.

Before Lüneburg, L.J.Paige [50] constructed $S(4,7,23)$ and $S(4,5,11)$. His construction of $S(4,7,23)$ is as follows.

Let $V(23)$ be a vector space of dimension 23 over $GF(2)$, let

$$\mathbf{v}_1 = (0,0,0,0,0,0,1,1,1,1,1,1,1,0,0,0,0,0,0,0,0,0,0),$$

$$\mathbf{v}_2 = (1,1,1,1,1,1,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0),$$

$$\mathbf{v}_3 = (1,1,1,0,0,0,1,1,1,0,0,0,0,1,0,0,0,0,0,0,0,0,0),$$

$$\mathbf{v}_4 = (1,0,0,1,1,0,1,1,0,1,0,0,0,0,1,0,0,0,0,0,0,0,0),$$

$$\mathbf{v}_5 = (0,1,0,1,0,1,1,0,1,1,0,0,0,0,0,1,0,0,0,0,0,0,0),$$

$$\mathbf{v}_6 = (0,0,1,0,1,1,0,1,1,1,0,0,0,0,0,0,1,0,0,0,0,0,0),$$

$$\mathbf{v}_7 = (1,1,0,0,1,0,0,0,1,1,1,0,0,0,0,0,0,0,1,0,0,0,0),$$

$$\mathbf{v}_8 = (1,0,1,0,0,1,1,0,0,1,1,0,0,0,0,0,0,0,0,1,0,0,0),$$

$$\mathbf{v}_9 = (0,1,1,1,0,0,0,1,0,1,1,0,0,0,0,0,0,0,0,0,1,0,0,0),$$

$$\mathbf{v}_{10} = (1,0,0,1,0,1,0,1,1,0,1,0,0,0,0,0,0,0,0,0,1,0,0),$$

$$\mathbf{v}_{11} = (0,1,0,0,1,1,1,1,0,0,1,0,0,0,0,0,0,0,0,0,0,1,0),$$

$$\mathbf{v}_{12} = (0,0,1,1,1,0,1,0,1,0,1,0,0,0,0,0,0,0,0,0,0,0,1),$$

Let $T = < \mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_{12} >$. Then T is a subspace of $V(23)$. For any given vector $\mathbf{v} = (t_1, t_2, \cdots, t_{23}) \in T$, define:

$$H_{\mathbf{v}} = \{i \mid 1 \leq i \leq 23, t_i \neq 0\}.$$

let $\mathcal{B} = \{H_{\mathbf{v}} \mid \mathbf{v} \in T, |H_{\mathbf{v}}| = 7\}$, $\mathcal{V} = \{1, 2, \cdots, 23\}$. Then $(\mathcal{V}, \mathcal{B})$ is an $S(4, 7, 23)$.

$S(4, 5, 11)$ can be constructed similarly by considering $V(11)$ over $GF(3)$.

In order to prove the existence of $S(5, 8, 24)$, Curtis [26] considered the power set $\mathcal{P}(\Omega)$ of a 24-set Ω as a linear space of dimension 24 over $GF(2)$, where the sum of two subsets is defined to be their symmetric difference. Choose a subspace (dimension 12) $\mathcal{C}$ of $\mathcal{P}(\Omega)$, such that the smallest cardinality of the elements in $\mathcal{C}$ is 8 (Curtis called this kind of element an *octad*) and $\mathcal{C}$ contains exactly 759 octads. The set of all octads is the set of blocks of $S(5, 8, 24)$. In his paper Curtis also introduced the so called "Miracle Octad Generator" or **MOG** . The MOG provided a convenient computational device for finding the block containing any five points.

Around 1980, starting from the designs $\mathcal{L}_{11}$ and $\mathcal{L}_{12}$ associated with the Hadamard matrix of order 12, Hughes [34] constructed $S(4, 5, 11)$ and $S(5, 6, 12)$ by an elementary technique. Before long, based on Hughes' ideas, Beth [11] gave a simpler method to construct $S(5, 6, 12)$, he also gave a proof of the uniqueness of $S(5, 6, 12)$. In 1981, Beth and Jungnickel [12] gave another method to construct $S(4, 5, 11)$ and $S(5, 6, 12)$.

Cameron [18], using some of the properties of $S(4, 7, 23)$ and $S(5, 8, 24)$, proved the uniqueness of these two designs.

Cameron and Van Lint [20] discussed the structures of $S(5, 6, 12)$ and $S(5, 8, 24)$.

Using the binary code of $PG(2,4)$, Lander [43] constructed $S(3,6,22)$, then from $S(3,6,22)$, constructed $S(5,8,24)$.

To study a design $\mathcal{D}$ by specifying some of the intersection numbers x_i's or the number s of $\mathcal{D}$ is an interesting research direction in design theory. We already know that if $s = 1$, then $\mathcal{D}$ is a symmetric design; if $s = 2$, then $\mathcal{D}$ is a quasi-symmetric design. Calderbank and Morton [17] classified all quasi-symmetric 3-designs with two intersection numbers x, y and $x = 1$.The only nontrivial examples are $S(4,7,23)$ and its residual, a 3-$(22,7,4)$ design. Ionin and Shrikhande [36] got the following characterizations of $S(4,7,23)$ and $S(5,8,24)$:

1. A $(2s-1)$-design with s intersection numbers is $S(5,8,24)$ if and only if $s \geq 3$ and $\sum_{i=1}^{s} x_i \leq s(s-1)$.
2. A $2s$-design with s intersection numbers is $S(4,7,23)$ if and only if $s \geq 2$ and $\sum_{i=1}^{s} x_i \leq s^2$.

The usual geometric construction of $S(4,7,23)$ starts from $PG(2,4)$. Starting from $PG(3,2)$ Baartmans [1] constructed $S(4,7,23)$.

Let $G = PSL(2,q)$ with $q = 11$ or 13. Iwasaki [38] considered the action of G on a set P, and took all G-images of a subset A in P as blocks. To construct $S(5,6,12)$, he selected $A = Q := \{x^2 \mid x \in GF(11)\}$. To construct $S(5,8,24)$, he selected A as the symmetric difference of the sets Q, $Q+1$ and $Q+4$ in $GF(23)$.

Lenz [45] gives a short uniqueness proof for $S(5,8,24)$, which immediately gives the order of M_{24}.

Let $PSU_6(2^2)$ act on the unitary polar geometry consisting of 693 points, 6237 totally isotropic lines and 891 totally isotropic planes. Jónsson and Mckay [41] proved that M_{22} is a subgroup of $PSU_6(2^2)$ leaving invariant some configuration of

22 planes any two having a point in common, no three having a point in common. $S(3,6,22)$ is obtained from this configuration of 22 planes as a set of 77 other planes called blocks, a block being called incident to one of the 22 planes if the corresponding planes have a line in common.

The monographs [13, 35, 52] all have complete self-contained discussions of Witt designs.

In [42] the action of the Mathieu groups M_n, $n = 22, 23, 24$, on the power sets of the point set of respective Witt designs have been studied. The orbits of all point subsets of $S(3,6,22)$, $S(4,7,23)$ and $S(5,8,24)$ together with the numbers t_i of blocks which meet a point subset in a oribit at i $(0 \leq i \leq 8)$ points in $S(5,8,24)$ and the formulas to calculate these numbers for the orbits in $S(3,6,22)$ and $S(4,7,23)$ have been given. The vectors $(t_0, \cdots, t_k)$, called frequency vectors, for $S(3,6,22)$, $S(4,7,23)$ and $S(5,8,24)$ are listed in appendix A, B and C, respectively.

Witt designs also have relations with other interesting objects, such as Golay codes and the Leech lattice. Just as Hughes and Piper [35] described, they "are a fundamental feature of combinatorics and algebra".

Let F be a finite field.

A *code* C is a subset of F^n, the vectors in C are called *codewords*. If C is a subspace of dimension k, then C is called a *linear* [n, k] *code*.If $F = GF(2)$, then C is called a *binary code*. If $F = GF(3)$, then C is called a *ternary code*. The *(Hamming) weight* of a vector $\mathbf{v}$ in F^n, denoted by $w(\mathbf{v})$, is the number of non-zero coordinates of $\mathbf{v}$. The *(Hamming) distance* $d(\mathbf{x}, \mathbf{y})$ between two codewords $\mathbf{x}$ and $\mathbf{y}$ is the number of coordinate positions in which they differ. Let C be an [n, k] code.

The *(Hamming) distance* d *of the code* C *is*

$$d = \min\{d(\mathbf{x},\mathbf{y}) : \mathbf{x},\mathbf{y} \in \mathsf{C}, \mathbf{x} \neq \mathbf{y}\}.$$

An $[n,k]$ code with distance d will be denoted by $[n,k,d]$. The *support* of a codeword is the set of coordinate positions where its entries are non-zero.

With these definitions we can see that Paige's construction of $S(4,7,23)$ mentioned above is actually to use the supports of the code T to construct the blocks of $S(4,7,23)$.

Let $\mathcal{G}_{24}$ be the code generated by the row vectors of the matrix $[\mathbf{I}_{12}, \mathbf{B}]$ [33], where $\mathbf{I}_{12}$ is the 12 by 12 identity matrix, and

$$\mathbf{B} = \begin{bmatrix} 1&1&0&1&1&1&0&0&0&1&0&1\\ 1&0&1&1&1&0&0&0&1&0&1&1\\ 0&1&1&1&0&0&0&1&0&1&1&1\\ 1&1&1&0&0&0&1&0&1&1&0&1\\ 1&1&0&0&0&1&0&1&1&0&1&1\\ 1&0&0&0&1&0&1&1&0&1&1&1\\ 0&0&0&1&0&1&1&0&1&1&1&1\\ 0&0&1&0&1&1&0&1&1&1&0&1\\ 0&1&0&1&1&0&1&1&1&0&0&1\\ 1&0&1&1&0&1&1&1&0&0&0&1\\ 0&1&1&0&1&1&1&0&0&0&1&1\\ 1&1&1&1&1&1&1&1&1&1&1&0 \end{bmatrix}.$$

Let $\mathcal{G}_{23}$ be the code generated by the row vectors of the matrix $[\mathbf{I}_{12}, \hat{\mathbf{B}}]$, where $\hat{\mathbf{B}}$ is the matrix obtained from $\mathbf{B}$ by deleting the last column of $\mathbf{B}$.

Let $\mathcal{G}_{12}$ be the code generated by the row vectors of the matrix $[\mathbf{I}_6, \mathbf{C}]$ [56], where $\mathbf{I}_6$ is the 6 by 6 identity matrix, and

$$\mathbf{C} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & -1 & -1 & 1 & 1 \\ 1 & 0 & 1 & -1 & -1 & 1 \\ -1 & 1 & 0 & 1 & -1 & 1 \\ -1 & -1 & 1 & 0 & 1 & 1 \\ 1 & -1 & -1 & 1 & 0 & 1 \end{bmatrix}.$$

Let $\mathcal{G}_{11}$ be the code generated by the row vectors of the matrix $[\mathbf{I}_6, \hat{\mathbf{C}}]$, where $\hat{\mathbf{C}}$ is the matrix obtained from $\mathbf{C}$ by deleting the last column of $\mathbf{C}$.

The codes $\mathcal{G}_{24}$ and $\mathcal{G}_{23}$ are binary [24, 12, 8] and [23, 12, 7] codes respectively [33]; the codes $\mathcal{G}_{12}$ and $\mathcal{G}_{11}$ are ternary [12, 6, 6] and [11, 6, 5] codes respectively [56].

The codes $\mathcal{G}_{24}$ and $\mathcal{G}_{12}$ are called *Extended Golay codes*, while $\mathcal{G}_{23}$ and $\mathcal{G}_{11}$ are called *Golay codes*. Golay codes $\mathcal{G}_{23}$ and $\mathcal{G}_{11}$ were discovered by Golay [31]. Golay codes are very important. They have far-reaching implications for sphere packing and simple groups. The extended Golay code $\mathcal{G}_{24}$ was used in the Voyager spacecraft program to transmit the colour pictures of Jupiter and Saturn.

The close relation between Witt designs and Golay codes can be illustrated by the following facts:

- Let $\mathbf{A}$ be an incidence matrix of $S(5, 8, 24)$. Then $\mathbf{A}^T$ is a generating matrix for $\mathcal{G}_{24}$[35, pp. 222-229]. The supports of the codewords of minimum weight (weight 8) of $\mathcal{G}_{24}$ form an $S(5, 8, 24)$[48, pp. 634].

- The supports of the codewords of minimum weight (weight 7) of $\mathcal{G}_{23}$ form an $S(4,7,23)$. $\mathcal{G}_{23}$ may be obtained by deleting any coordinate of $\mathcal{G}_{24}$[48, pp. 634-635]
- The supports of the codewords of minimum weight (weight 6) of $\mathcal{G}_{12}$ form an $S(5,6,12)$[48, pp. 635].
- The supports of the codewords of minimum weight (weight 5) of $\mathcal{G}_{11}$ form an $S(4,5,11)$[48, pp. 635].

The Leech lattice , denoted by Λ_{24} , consists of the vectors [25]

$$\frac{1}{\sqrt{8}}(\mathbf{0} + 2\mathbf{c} + 4\mathbf{x})$$

$$\frac{1}{\sqrt{8}}(\mathbf{1} + 2\mathbf{c} + 4\mathbf{y})$$

where $\mathbf{0} = (\overbrace{0,0,\cdots,0}^{24})$, $\mathbf{1} = (\overbrace{1,1,\cdots,1}^{24})$, $\mathbf{c} \in \mathcal{G}_{24}$ (the components of $\mathbf{c}$ are regarded as real 0's and 1's) and $\mathbf{x}, \mathbf{y} \in \mathbf{Z}^{24}$, satisfy $\sum x_i \equiv 0(mod\, 2)$, $\sum y_i \equiv 1(mod\, 2)$.

The Leech lattice Λ_{24} was discovered by Leech in 1965 [44]. The Leech lattice Λ_{24} has a significant impact in the theory of finite simple groups. Conway [23] constructed three simple groups Co_1, Co_2 and Co_3 by using the Leech lattice. Co_1, Co_2 and Co_3 are all subgroups of Co_0, the group of automorphisms of the Leech lattice Λ_{24}. The Leech lattice also provides a lattice packing in $\mathbf{R}^{24}$, which still stands as the densest known packing in $\mathbf{R}^{24}$ [25].

The purpose of this thesis is to characterize all t-blocking sets (see definition 3.1) and all semiovals (see definition 4.2) in the Witt designs up to the frequency vectors.

In chapter 2 we obtain some results which correct some mistakes in [7, 8]. We also improve the results in [9]. In chapter 3 we thoroughly determine the structure of a Fano set - a fundamental structure used to characterize blocking sets, t-blocking sets and semiovals in $S(3,6,22)$, and obtain a construction method for a Fano set. Then we characterize the t-blocking sets in Witt designs. We determine the possible size of a t-blocking set, classifying them by their frequency vectors. We also analyze the Witt designs and obtain a number of new results. In chapter 4, we characterize all semiovals in the Witt designs. We prove that there are only three types of semiovals in $S(3,6,22)$, one of them has size nine, the other two have size ten, one of them is also a t-blocing set; $S(5,6,12)$ and $S(4,7,23)$ each have only one type of semioval, which are also t-blocking sets; but both $S(4,5,11)$ and $S(5,8,24)$ have no semioval at all.

2. NOTES ON $S(3,6,22)$, $S(4,7,23)$ AND $S(5,8,24)$

2.1. Some definitions and notations.

Definition 2.1. A set of points of a Steiner system is called a *blocking set* if it contains no block, but intersects every block.

Definition 2.2. A blocking set C is said to be of *index t* if C is contained in t blocks, but can not be contained in $t-1$ blocks. The index of C is denoted by $i(C)$.

Definition 2.3. A blocking set C is said to be *irreducible* if for any $x \in C$, the set $C - \{x\}$ is not a blocking set. Otherwise, C is said to be *reducible* .

Definition 2.4. Let X be a set of points of $S(t,k,v)$, let t_i be the number of blocks that are i-secant to X, $i = 0, 1, \cdots, k$. If $\{i_1, \cdots, i_n\}$ is the set of all those i_j's $(0 \le i_j \le k)$ such that $t_{i_j} \ne 0$ and $0 \le i_1 < i_2 < \cdots < i_n$, then we say that X is of *type* $(i_1, i_2, \cdots, i_n)$ and call $(t_0, t_1, \cdots, t_k)$ the *frequency vector* of X, denote it by $FV(X)$.

Definition 2.5. Let X and Y be two point subsets of $S(t,k,v)$. If $|X| = |Y|$ and $FV(X) = FV(Y)$, then we say that X and Y are the same *type*.

In the sequel discussion, $\mathcal{S}$ will be used to denote the point set of $S(t,k,v)$. Given any t points $p_1, \cdots, p_t$ in $\mathcal{S}$, the unique block B which contains $p_1, \cdots, p_t$ is also refered to as *determined* by $p_1, \cdots, p_t$.

Let $r_s (s = 0, 1, \cdots, t)$ be the number of blocks containing a fixed s-set, then

$$r_s = \frac{\binom{v-s}{t-s}}{\binom{k-s}{t-s}}$$

We have the following identities:

$$\sum_{i=s}^{k} \binom{i}{s} t_i = r_s \binom{r}{s}, s = 0, 1, \cdots, t. \tag{1}$$

If $k - t$ of $t_0, \cdots, t_k$ are given, then the rest can be determined by solving the above linear system.

We recall the following:

Result 2.1. [7, result 2.1] Let B and B' be two blocks in $S(3, 6, 22)$. Then either $|B \cap B'| = 0$ or $|B \cap B'| = 2$

Result 2.2. [7, lemma 2.2, lemma 2.7] Let B and B' be two blocks in $S(3, 6, 22)$. If $|B \cap B'| = 2$, then the type of $B \cup B'$ is $(0, 2, 3, 4, 6)$ with

$$t_0 = 4, \ t_2 = 27, \ t_3 = 32, \ t_4 = 12, \ t_6 = 2.$$

If $|B \cap B'| = 0$, then the type of $B \cup B'$ is $(2, 4, 6)$ with

$$t_2 = 30, \ t_4 = 45, \ t_6 = 2.$$

Result 2.3. [7, lemma 5.1] Let B, B' be two blocks of $S(3, 6, 22)$ with $|B \cap B'| = 2$. Denote by a, b two points of $B' - B$. Let $\mathcal{E} = \{E_1, E_2, E_3, E_4\}$ be the set of the four blocks external to $B \cup B'$.

1. There exist two blocks S_1, S_2 which are 2-secant to $B \cup B'$ at a and b.
2. For every $x \in S_1$ (or S_2), with $x \neq a, b$, the two blocks E_i, E_j of $\mathcal{E}$ through x have the other common point y on S_2 (or S_1).
3. One of the two points outside $B \cup B' \cup E_i \cup E_j$ is in S_1 and the other in S_2.

Result 2.4. [8, result 2.1] Every block in $S(4, 7, 23)$ is a 7-set of type $(1, 3, 7)$.

Result 2.5. [8, lemma 2.5] Let B, B' be two blocks of $S(4,7,23)$ with $|B \cap B'| = 3$. Fix $x \in B - B'$ and $y \in B' - B$. There are exactly three blocks D_1, D_2 and D_3 intersecting $B \cup B'$ only at x and y. Moreover $D_1 \cap D_2 \cap D_3 = \{x, y\}$.

Berardi [7, 8] defined the following sets:

1. Use the same notations of result 2.3. Fix $u \in B - B'$ and let z be the only point of S_2 outside $B \cup B' \cup E_1 \cup E_2$. Define

$$N_1 := (B \cup B' - \{a, b, u\}) \cup \{x, z\}.$$

2. Let B, B' and B'' be three blocks in $S(3,6,22)$ with $|B \cap B' \cap B''| = 1$. Fix a point z of $B'' - (B \cup B')$, let y be one of the joint points of the two external blocks to $B \cup B' \cup \{z\}$. Define:

$$N_0 := \left[(B \cup B') - B''\right] \cup \{y, z\}.$$

3. $E_0 := S - (B \triangle B')$, where B and B' are two blocks of $S(4,7,23)$ with $|B \cap B'| = 1$.

4. $E := (B - \{x\}) \cup (B' - \{y\} \cup \{a, b\})$, where B and B' are two blocks of $S(4,7,23)$ with $|B \cap B'| = 3$, $x \in B - B'$, $y \in B' - B$ and

$$\{a, b\} \subset \{x_1, x_2, x_3 | \{x_k\} = D_i \cap D_j - (B \cup B'), \{i, j, k\} = \{1, 2, 3\}\}.$$

   here D_1, D_2 and D_3 are the three blocks intersecting $B \cup B'$ only at x and y.

5. $E_1 := B \cup B' - \{o, w\}$, where B and B' are two blocks of $S(4,7,23)$ with $B \cap B' = \{o\}$ and $w \in B' - B$.

Berardi [7] proved that N_1 and N_0 are the only blocking sets of size nine in $S(3,6,22)$. It is also implied that N_1 and N_0 are different types of blocking sets in $S(3,6,22)$. In [8] Berardi proved that E_0, E and E_1 are blocking sets of size eleven in $S(4,7,23)$. He also claims that E_0, E and E_1 are three different types of blocking sets in $S(4,7,23)$. Here we prove that N_1 and N_0 are the same type of blocking set in $S(3,6,22)$; while E and E_1 are the same type of blocking set in $S(4,7,23)$.

For convenience, we will use $X = Y$ to denote X and Y are the same type.

2.2. The proofs of $N_1 = N_0$ and $E = E_1$.

Lemma 2.1. *There exists a block which is 5-secant to N_0 in $S(3,6,22)$.*

Proof. Let $B = \{o, r, 1, 2, 3, 4\}$, $B' = \{o, r, a, b, c, d\}$, $B'' = \{o, 4, d, z, u, v\}$, $E_1 = \{x, y, m, n, p, q\}$, $E_2 = \{x, y, s, u, v, w\}$; then

$$N_0 = \left[(B \cup B') - B''\right] \cup \{y, z\} = \{r, 1, 2, 3, a, b, c, y, z\}.$$

It is not difficult to prove the following conclusion:

Let $A(i, \alpha)$ be the blocks determined by $\{y, i, \alpha\}$, where $1 \le i \le 3$, $\alpha \in \{a, b, c\}$. If one of $4, d$ is in $A(i, \alpha)$, then the other one is also in $A(i, \alpha)$.

Suppose there is no block which is 5-secant to N_0, then $A(1, \alpha) \ne A(1, \beta)$ if $\alpha \ne \beta$, so each one of $\{o\}$, $\{r\}$ and $\{4, d\}$ is contained in exactly one of $A(1, a)$, $A(1, b)$ and $A(1, c)$. Without loss of generality, we may assume $\{o\} \subset A(1, a)$, $\{r\} \subset A(1, b)$ and $\{4, d\} \subset A(1, c)$. Since $A(2, c) \ne A(1, c) \ne A(3, c)$ and $4, d \notin A(2, c) \cup A(3, c)$, then either $o \in A(2, c)$, $r \in A(3, c)$ or $r \in A(2, c)$, $o \in A(3, c)$. If $o \in A(2, c)$, $r \in A(3, c)$, then since $A(2, b) \ne A(1, a)$, $A(1, b)$, $A(1, c)$, $A(2, c)$, $o, r, a, c, d \notin A(2, b)$, therefore $|A(2, b) \cap B'| = |\{b\}| = 1$, which is a contradiction. If $r \in A(2, c)$ and $o \in A(3, c)$, similarly we can also get a contradiction. □

It is not difficult to prove that a blocking set of size 9 in $S(3,6,22)$ has at most one 5-secant block [7, pp. 39]. By lemma 2.1 and the proof of lemma 5.6 of [7] we can prove

Theorem 2.1. *The set X_0 is the unique blocking set of size nine in $S(3,6,22)$ and $FV(X_0) = (0,18,20,26,12,1,0)$.*

Now we prove

Theorem 2.2. *The blocking sets E and E_1 are the same type of blocking set in $S(4,7,23)$.*

Proof. Let E be defined as in 4 of section 2.1. We only need to prove that there exist two blocks A and A' such that $E = A \cup A' - \{o, w\}$ with $A \cap A' = \{o\}$ and $w \in A' - A$.

Without loss of generality, we may assume $a = x_1$, $b = x_2$ and $c = x_3$; then we have $a, b \in D_3$. Consider the blocks determined by $\{x, a, b, c\}$ and $\{y, a, b, c\}$, respectively. If any one of the blocks meets $B \cap B'$, then it meets $B \cap B'$ at exactly two points. So at most one meets $B \cap B'$. Let A be one which does not meet $B \cap B'$. We may assume that A is determined by $\{x, a, b, c\}$. Since $x, a, b \in D_3$, $x, a, c \in D_2$ and $x, b, c \in D_1$, we have $A - \{x, a, b, c\} \subseteq (B \triangle B') - \{x\}$. By result 2.4, we can obtain that $|(A - \{x, a, b, c\}) \cap (B' - B)| = 1$ or 3.

If $|(A - \{x, a, b, c\}) \cap (B' - B)| = 1$, then $|(A - \{x, a, b, c\}) \cap [B - (B' \cup \{x\})]| = 2$. Let

$$(A - \{x, a, b, c\}) \cap (B' - B) = \{z\},$$

$$(A - \{x, a, b, c\}) \cap [B - (B' \cup \{x\})] = \{u, v\}.$$

By lemma 2.4 in [8], there is a block U through u, z and a such that $U \cap (B \cup B') = \{u, z\}$. Since $U \cap A = \{u, z, a\}$, we have $b, c \notin U$. Therefore, $|U \cap (D_1 - \{x, y, b, c, \})| = 1$ or 3, so $|U \cap D_2| = 2$ or $|U \cap D_3| = 2$, a contradiction.

So $|(A - \{x, a, b, c\}) \cap (B' - B)| = 3$. Therefore $|A \cap E| = 5$, $A \cap B = \{x\}$ and $E = (A \cup B) - \{x, c\}$. □

By remark 2.8 in [8] and theorem 2.2 we know that E_0 and E_1 are the only two different types of blocking sets of size eleven in $S(4, 7, 23)$. So there are four different types of blocking sets in $S(4, 7, 23)$, not six as indicated in [8].

2.3. **Notes on** $S(5,8,24)$. We use the same notations and terminologies as in [9].

Let B, B' be two blocks in $S(5,8,24)$ with $|B \cap B'| = 2$. We have

$$M := B\triangle B';\ M_0 := B\triangle B' - \{a\};\ I := B \cup B' - \{u,v\};\ R := B \cup B' - \{z,a\}$$

where $u \in B - B'$, $v \in B' - B$, $a \in B\triangle B'$, $z \in B \cap B' = \{x,y\}$.

In [9] the following theorem had been proved:

Theorem 2.3. *Let C be a blocking set in $S(5,8,24)$. Then $11 \leq |C| \leq 13$. Moreover,*

1. *$|C| = 11$ implies that $C = M_0$ and $i(M_0) = 2$.*
2. *$|C| = 12$ and C irreducible imply that $C = I$ and $i(I) = 2$.*
3. *$|C| = 12$ and C reducible imply that $C = M_0 \cup \{x\}$, $x \notin M_0$. Moreover, if $i(C) = 2$, then either $C = M$ or $C = R$.*
4. *$|C| = 13$ implies that C is reducible and C is the complement of M_0. Moreover, if $i(C) = 2$, then $C = B \cup B' - \{a\}$, where B, B' are two blocks with $|B \cap B'| = 2$ and $a \in B \cap B'$.*

In this section we prove the following theorem, which has improved the results in the above theorem.

Theorem 2.4. Let C be a blocking set in $S(5,8,24)$. Then $11 \leq |C| \leq 13$ and $i(C) = 2$. Moreover,

1. If $|C| = 11$, then $C = M_0$.
2. If $|C| = 12$ and C is irreducible , then $C = I$.
3. If $|C| = 12$ and C is reducible , then $C = M$ or R.
4. If $|C| = 13$, then $C = S - M_0 = B \cup B' - \{z\}$ is reducible , where B, B' are two blocks with $|B \cap B'| = 2$ and $z \in B \cap B'$.

2.3.1. Some known results on $S(5,8,24)$. In the case of $S(5,8,24)$, if E is a blocking set, then (1) implies:

$$
(2)\qquad
\begin{aligned}
t_1 + t_2 + t_3 + t_4 + t_5 + t_6 + t_7 &= 759\\
t_2 + 2t_3 + 3t_4 + 4t_5 + 5t_6 + 6t_7 &= g_1\\
t_3 + 3t_4 + 6t_5 + 10t_6 + 15t_7 &= g_2\\
t_4 + 4t_5 + 10t_6 + 20t_7 &= g_3\\
t_5 + 5t_6 + 15t_7 &= g_4\\
t_6 + 6t_7 &= g_5
\end{aligned}
$$

where

$$
(3)\qquad
\begin{aligned}
g_1 &= 253c - 759\\
2g_2 &= 77c(c-1) - 2g_1\\
6g_3 &= 21c(c-1)(c-2) - 6g_2\\
24g_4 &= 5c(c-1)(c-2)(c-3) - 24g_3\\
120g_5 &= c(c-1)(c-2)(c-3)(c-4) - 120g_4
\end{aligned}
$$

The following lemmas are quoted from [8, 9].

Lemma 2.2. [9] *Let B, B' be two blocks in $S(5,8,24)$. Then*

1. *The type of B is $(0,2,4,8)$ with*

$$t_0 = 30, t_2 = 448, t_4 = 280, t_8 = 1.$$

2. *If $|B \cap B'| = 4$, then $B \triangle B'$ is a block.*

3. *If* $|B \cap B'| = 2$, *then* $M = B \triangle B'$ *is a set of type* $(2, 4, 6)$ *with*

$$t_2 = t_6 = 132, t_4 = 495.$$

4. *If* $|B \cap B'| = 0$, *then* $B \triangle B' = B \cup B'$ *is a set of type* $(0, 4, 6, 8)$ *with*

$$t_0 = 1, t_4 = 280, t_6 = 448, t_8 = 30.$$

5. *Let* E *be a set. Then* $S - E$ *is a block if and only if* $E = B \cup B'$, $B \cap B' = \emptyset$.

6. *Let* F *be a 4-set,* $F \cap B = \emptyset$; *then there exists a block* B' *such that* $F \subseteq B'$ *and* $B \cap B' = \emptyset$.

By 1, 3 and 4 of lemma 2.2 we get the following corollaries, respectively.

Corollary 2.1. *No blocking set can be contained in one block.*

Corollary 2.2. *The sets* M, M_0 *are blocking sets in* $S(5, 8, 24)$.

Corollary 2.3. *Let* C *be a blocking set. If* $C \subseteq B \cup B'$, *then* $|B \cap B'| = 0$.

Fix a point x in $S(t, k, v)$, the contraction of $S(t, k, v)$ at x is an $S(t-1, k-1, v-1)$. For $S(4, 7, 23)$ we have

Lemma 2.3. [8] *Let* B, B' *be two blocks in* $S(4, 7, 23)$ *with* $B \cap B' = \{x\}$, *then for any* $u \in B - B'$ *and* $v \in B' - B$, *there exists a block* B'' *in* $S(4, 7, 23)$ *such that* $B'' \cap (B \cup B') = \{u, v\}$.

Corollary 2.4. *Let* B, B' *be two blocks in* $S(5, 8, 24)$ *with* $B \cap B' = \{x, y\}$ *and let* $u \in B - B'$, $v \in B' - B$. *Then* $(B \cup B') - \{y, u, v\}$ *is not a blocking set.*

2.3.2. **Proof of the theorem 2.4.** From now on, C will be used to denote a blocking set in $S(5,8,24)$.

Lemma 2.4, proposition 2.1, proposition 2.2 and proposition 2.3 had been proved in [9], we quote them here for our convenience.

Lemma 2.4. $11 \leq |C| \leq 13$.

Proposition 2.1. *If* $|C| = 11$, *then* $C = M_0$ *and* C *has no 7-secant block.*

Proposition 2.2. *I is an irreducible blocking set.*

Proposition 2.3. *R is a reducible blocking set.*

By (2), if $|C| = 12$, then

(4) $$t_1 = t_7, t_2 = t_6 = 132 - 6t_7, t_3 = t_5 = 15t_7, t_4 = 495 - 20t_7.$$

The following proposition plays a crucial role in our proof.

Proposition 2.4. *Let* $|C| = 12$.

1. *If* C *has a 7-secant block, then* $C = R$ *or* I.
2. *If* C *has no 7-secant block, then* $C = M$.

Proof. Let B be a block 7-secant to C, B' be a block containing the five points in $C - B$; then $|B \cap B'| = 2$. Let $B \cap B' = \{x, y\}$. Since $|B \cap C| = 7$, $\{x, y\} \cap C \neq \emptyset$. If $x \in C$, $y \notin C$, then $C = R$. If $x, y \in C$, then $C = I$.

If C has no 7-secant block, then by (4), C is of type $(2,4,6)$. Let B be a block 6-secant to C, let five of the six points in $C - B$ be contained in block B'; then B' contains another point in C. We claim that this point must be the remaining point in $C - B$. Suppose this point is in B; then by lemma 2.2.1, $|B \cap B'| = 2$.

Let $B \cap B' = \{x, y\}$, $x \in C$, $y \notin C$, $u \in B - B'$, $v \in B' - B$, $w \in C - (B \cup B')$. Since C is of type (2.4.6), the set $C - \{w\} = (B \cup B') - \{y, u, v\}$ is a blocking set, a contradiction. So B, B' are blocks 6-secant to C and $C = B \triangle B' = M$. □

Proposition 2.5 and proposition 2.7 are proved in [9], but using proposition 2.4, we can simplify the proofs.

Proposition 2.5. *If $|C| = 12$ and C is irreducible, then $C = I$.*

Proof. Since C is irreducible, $t_7 = t_1 \geq 12$. By proposition 2.4, $C = I$. □

Proposition 2.6. *If $|C| = 12$ and C is reducible, then $C = M$ or R.*

Proof. If C has a 7-secant block, then $C = R$; if C has no 7-secant block, then $C = M$. □

Since M_0 has no 7-secant block, we have

$$FV(M_0) = (0, 22, 110, 165, 330, 66, 66, 0, 0).$$

In theorem 3.17 we will prove that R has eleven 7-secant blocks, so

$$FV(R) = (0, 11, 66, 165, 275, 165, 66, 11, 0).$$

From the fact that I is an irreducible blocking set we know that I has at least twelve 7-secant blocks. Checking the appendix C we know that

$$FV(I) = (0, 12, 60, 180, 255, 180, 60, 12, 0).$$

Lemma 2.2 tells us that $FV(M) = (0, 0, 132, 0, 495, 0, 132, 0, 0)$.

Proposition 2.7. *Let $\mathcal{A}$ be one of the 12-sets I, M and R. Then $\mathcal{S} - \mathcal{A} = \mathcal{A}$.*

Proof. Let $A = M$. Since M is of type $(2,4,6)$, so is $\mathcal{S} - M$. By proposition 2.4, $\mathcal{S} - M = M$.

Let $A = R = B \cup B' - \{z, a\}$, where $|B \cap B'| = 2$, $a \in B \triangle B'$ and $z \in B \cap B'$. Since R has a 7-secant block and $R \cup \{a\}$ is a blocking set, $\mathcal{S} - R$ is reducible and also has a 7-secant block, by proposition 2.6 and proposition 2.4, $\mathcal{S} - R = R$.

Let $A = I$. Suppose $\mathcal{S} - I$ is reducible; then $\mathcal{S} - I = R$, but $\mathcal{S} - (\mathcal{S} - I) = I$, so $I = \mathcal{S} - R = R$, a contradiction. Therefore $\mathcal{S} - I$ is irreducible and $\mathcal{S} - I = I$. $\square$

Proposition 2.8. *If $|C| = 13$, then $C = \mathcal{S} - M_0 = B \cup B' - \{z\}$ is reducible, where B, B' are blocks with $|B \cap B'| = 2$ and $z \in B \cap B'$.*

Proof. Since $|\mathcal{S} - C| = 11$, we have $\mathcal{S} - C = M_0$. But M_0 has no 7-secant block, so C has no 1-secant block. This means that C is reducible .

The fact that M_0 has a 1-secant block means that C has 7-secant blocks. Let B be a 7-secant block to C and let five of the six points in $C - B$ be contained in block B'.

We claim that the remaining one point $w \in C - B$ is still in B'.

Suppose $w \notin B'$; we may assume that $B \cap B' \neq \emptyset$ (If $B \cap B' = \emptyset$, then B' contains three points in $\mathcal{S} - (C \cup B)$. Since there are six blocks that contain five points in $C - B$, any two of these only intersect at four points in $C - B$, and there are only ten points in $\mathcal{S} - (C \cup B)$, so at least one of these blocks will intersect B; we can label this block as B'.). Then $|B \cap B'| = 2$. Let $B \cap B' = \{x, y\}$; since B is 7-secant to C, $\{x, y\} \cap C \neq \emptyset$.

If $x, y \in C$, then $C - \{w\} = I$. But on the other hand, $M_0 \cup \{w\}$ is reducible, so $\mathcal{S} - I = M_0 \cup \{w\} = R$, a contradiction.

If $x \in C$, $y \notin C$, let $v \in B' - (C \cup B)$, $B = \{x, y, a_1, a_2, a_3, a_4, a_5, a_6\}$. By lemma 2.3 we know that there is a block B_i that contains a_i, v, y such that $B_i \cap (C - \{w, a_i\}) = \emptyset$, for $i = 1, 2, 3, 4, 5, 6$. Since C has no 1-secant block, $w \in B_i$, for $i = 1, 2, 3, 4, 5, 6$; let $D_i = B_i - \{v, y, w, a_i\}$; then $|D_i| = 4$, $D_i \subseteq S - (C \cup \{x, y\})$ and $|D_i \cap D_j| = 1$ for $i \neq j$. Since $|S - (C \cup \{v, y\})| = 9$, we have $D_1 \cap D_i \neq D_1 \cap D_j$, if $i \neq j$. Hence $|D_1| \geq 5$, a contradiction.

Now we have proved that $w \in B'$. From $C \subseteq (B \cup B')$ we know that $|B \cap B'| = 2$. Let $B \cap B' = \{x, y\}$; since $|B \cap C| = 7$, this means that $|(B \cap B') \cap C| = 1$, so $C = B \cup B' - \{z\}$ with $z \in B \cap B'$. □

From time to time we apply results of [7, 8, 9] in this thesis. In order to ensure our proofs are not affected by the errors in [7, 8, 9], those we use here have been thoroughly checked.

3. t-BLOCKING SETS IN THE WITT DESIGNS

3.1. Preliminaries.

Definition 3.1. A set C_t ($t \geq 1$) is called a *t-blocking set* if C_t meets every block in at least t points and meets at least one block in exactly t points.

Our definition of t-blocking set is different from that in [14]. Here we require that at least one block meets C_t in exactly t points, while in [14] this is not required.

In recent years, more and more papers dealing with t-blocking sets have been published. Not only is the t-blocking set of theoretic importance by itself (see [3, 16]), it also has applications in other areas . For example, it is known that there is a link between optimal linear codes and t-blocking sets in a projective plane [2]. Batten [5] has pointed out that critical systems are connected with t-blocking sets and Batten [6] has presented a private key cryptosystem which is based on t-blocking sets.

The automorphism groups of the Witt designs $S(4, 5, 11)$, $S(5, 6, 12)$, $S(3, 6, 22)$, $S(4, 7, 23)$ and $S(5, 8, 24)$ are respectively Mathieu's five sporadic simple groups M_{11}, M_{12}, M_{22}, M_{23} and M_{24}; the Mathieu groups M_{11}, M_{12}, M_{23} and M_{24} are the automorphism group of the Golay codes $\mathcal{G}_{11}$, $\mathcal{G}_{12}$, $\mathcal{G}_{23}$ and $\mathcal{G}_{24}$, respectively [56, pp. 111-112]. In [7, 8, 9, 10] Berardi, Eugeni and Ferri characterized the blocking sets in Witt designs. In this chapter we characterize all t-blocking sets in Witt designs.

3.2. t-blocking sets in $S(4, 5, 11)$ and $S(5, 6, 12)$.

3.2.1. t-blocking sets in $S(4, 5, 11)$.

Theorem 3.1. *Let C_t be a t-blocking set in $S(4,5,11)$.*

1. *If $t = 1$, then $5 \le |C_t| \le 7$, and if $|C_t| = 4+i$, $i = 1,2,3$, then we have $C_t = B \cup X$, where B is a block, X is an $(i-1)$-subset of S such that $X \cap B = \emptyset$. When $|C_1| = 5$, $FV(C_1) = (0,15,20,30,0,1)$; when $|C_1| = 6$, $FV(C_1) = (0,5,20,30,10,1)$; when $|C_1| = 7$, $FV(C_1) = (0,1,12,30,20,3)$.*
2. *If $5 \ge t \ge 2$, then $C_t = X$, where X is a $(6-t)$-subset of S, and*

$$FV(C_2) = (0,0,4,24,30,8),\ FV(C_3) = (0,0,0,12,36,18),$$

$$FV(C_4) = (0,0,0,0,30,36),\ FV(C_5) = (0,0,0,0,0,66).$$

Proof. Since the type of the block in $S(4,5,11)$ is $(1,2,3,5)$ and any 4-set is contained in exactly one block, we conclude that $5 \le |C_1| \le 7$.

Because $S(4,5,11)$ does not have any blocking set, C_1 contains a block B. If $|C_1| = 5$, then $C_1 = B$; if $|C_1| = 6$, then $C_1 = B \cup \{x\}$, where $x \notin B$; if $|C_1| = 7$, then $C_1 = B \cup \{x,y\}$, where $x,y \notin B$.

It is easy to prove that if $5 \ge t \ge 2$, then $C_t = X$, where X is a $(6-t)$-subset of S. The frequency vector can be obtained by letting $t_0 = 0$ and solve the linear system (1) □

3.2.2. ***t*-blocking sets in $S(5,6,12)$.**

Theorem 3.2. *Let C_t be a t-blocking set in $S(5,6,12)$.*

1. *If C_t does not contain any block, then $t = 1$, $|C_1| = 6$ and $C_1 = (B-\{a\}) \cup \{x\}$ and $FV(C_1) = (0,6,30,60,30,6,0)$, where B is a block and $a \in B$, $x \notin B$.*

2. *If C_t contains a block, then $C_t = B \cup X_t$, where B is a block and X_t is a t-set such that $X_t \cap B = \emptyset$. The frequency vectors are:*

$$FV(C_1) = (0, 1, 15, 50, 50, 15, 1),\ FV(C_2) = (0, 0, 4, 32, 60, 32, 4),$$

$$FV(C_3) = (0, 0, 0, 12, 54, 54, 12),\ FV(C_4) = (0, 0, 0, 0, 30, 72, 30),$$

$$FV(C_5) = (0, 0, 0, 0, 0, 66, 66),\ FV(C_6) = (0, 0, 0, 0, 0, 0, 132).$$

Proof. The type of a block in $S(5, 6, 12)$ is $(0, 2, 3, 4, 6)$. Noticing the fact that any five points are contained in exactly one block we can easily prove this theorem. ❑

3.3. **Some known results on $S(3, 6, 22)$.** The following results are quoted from [7] for our reference convenience:

Result 3.1. Let B and B' be two blocks in $S(3, 6, 22)$ with $|B \cap B'| = 2$. Let x be a point with $x \notin B \cup B'$. Then the set $B \cup B' \cup \{x\}$ has two external blocks.

Result 3.2. Let B and B' be two blocks in $S(3, 6, 22)$ with $|B \cap B'| = 2$. Denote by W the point set of the complement of $B \cup B'$, and by $\mathfrak{R}$ the set of external blocks of $B \cup B'$. Then the pair $(W, \mathfrak{R})$ is a 1-(12, 6, 2) design.

Result 3.3. Each point in $S(3, 6, 22)$ is on 21 blocks, each pair of points is on 5 blocks.

3.4. **The structure of a Fano set in $S(3, 6, 22)$.**

Definition 3.2. A *Fano set* in $S(3, 6, 22)$ is a 7-set F of type $(1, 3)$.

The frequency vector of a Fano set F is $(0, 42, 0, 35, 0, 0, 0)$. Fano sets played a very important role in Berardi's characterization of the blocking sets in $S(3, 6, 22)$.

We will also use Fano sets in our characterization and calculation of the frequency vectors. So in this section we study the structure of a Fano set thoroughly, and give a construction method for a Fano set. Our main result is theorem 3.3.

Definition 3.3. Let B be a block in $S(3,6,22)$. We define $\Re(B)$ to be the set of blocks which are disjoint from B.

By result 2.2 we can prove

Lemma 3.1. *The pair $(S - B, \Re(B))$ is a 2-(16, 6, 2) design.*

Lemma 3.2. *Let B and $\Re(B)$ be as above, let $B' = \{a, b, c, \bar{a}, \bar{b}, \bar{c}\}$ and $U = \{o, a, b, u, v, w\}$ be two distinct elements of $\Re(B)$. Let $V, W \in \Re(B)$ be the other blocks on $\{o, a\}$ and $\{o, b\}$, respectively. If $V \cap B' = \{a, c\}$, then $W \cap B' = \{b, c\}$.*

Proof. By lemma 3.1 we only need to prove that the block X determined by $\{b, c, o\}$ is in $\Re(B)$.

Suppose $X \notin \Re(B)$; then $|X \cap B| = 2$. Let $B = \{x, y, z, \bar{x}, \bar{y}, \bar{z}\}$ and $X = \{o, b, c, x, \bar{x}, d\}$, let $B_y = \{o, b, \bar{a}, y, \bar{y}, e\}$ be the block determined by $\{o, b, y\}$, let $B_z = \{o, b, \bar{b}, z, \bar{z}, f\}$ be the block determined by $\{o, b, z\}$. Then the block B'' determined by $\{o, b, \bar{c}\}$ would be in $\Re(B)$, so let $B'' = \{o, b, \bar{c}, p, q, r\}$. Because $V \cap U = \{o, a\}$, $V \cap X = \{o, c\}$, so $u, v, w, d \notin V$. As $o \in V \cap B''$, so V contains only one of p, q and r. We may assume that $p \in V$; then $V = \{o, a, c, e, f, p\}$. By lemma 3.1 there exists a block $A \in \Re(B)$ on $\{o, c\}$ such that $A \neq V$. Then $a, b, e, f \notin A$, so $\bar{a}, \bar{b} \in A$ and $|A \cap B''| \geq 3$, a contradiction. □

This lemma guarantees that o is uniquely determined by a, b, c and any two of U, V, W.

Use the notation of lemma 3.2 and let $x \in B$. Let B_1, B_2 and B_3 be the blocks determined by $\{o, a, x\}$, $\{o, b, x\}$ and $\{o, c, x\}$, respectively. Then $B_i \neq B_j$ if $i \neq j$ (otherwise B_i would be one of U, V, W, and $B_i \in \Re(B)$). Let

$$B_1 \cap B - \{x\} = \{\bar{x}\},\ B_2 \cap B - \{x\} = \{\bar{y}\},\ B_3 \cap B - \{x\} = \{\bar{z}\},$$

$$B_1 \cap B' - \{a\} = \{\bar{a}\},\ B_2 \cap B' - \{b\} = \{\bar{b}\},\ B_3 \cap B' - \{c\} = \{\bar{c}\}.$$

These produce partitions of B and B'' into two parts, say $\{x, y, z\}$, $\{\bar{x}, \bar{y}, \bar{z}\}$ and $\{a, b, c\}$, $\{\bar{a}, \bar{b}, \bar{c}\}$.

Lemma 3.3. *The above partition does not depend on the choice of x, that is for any element of B, we get the same partition of B.*

In the same way, the blocks A_1, A_2, A_3 determined by $\{a, b, x\}$, $\{a, c, x\}$, $\{b, c, x\}$, respectively also produce a partition of B. It can be proved that this partition does not depend on x either. The next lemma shows that these are actually the same partition.

Lemma 3.4.

$$\bigcup_{i=1}^{3}(A_i \cap B) - \{x\} = \bigcup_{i=1}^{3}(B_i \cap B) - \{x\}.$$

Proof. It suffices to show $(A_i - \{x\}) \cap \{x, y, z\} = \emptyset$ for $i = 1, 2, 3$.

Let U, V and W be as in lemma 3.2.

Now we prove $(A_1 - \{x\}) \cap \{x, y, z\} = \emptyset$. Suppose $(A_1 - \{x\}) \cap \{x, y, z\} \neq \emptyset$; then $A_1 \cap B = \{x, \alpha\}$, where $\alpha \in \{y, z\}$. Let A be the block determined by $\{o, c, \alpha\}$; then from

$$A \cap V = A \cap W = A \cap B_3 = \{o, c\}$$

and result 3.1 we know that $a, b, x \notin A$ and $|A \cap (U - B')| = 2$. From $a, b \in A_1$ we know that $A_1 \cap (U - B') = \emptyset$. Therefore, $A \cap A_1 = \{\alpha\}$, contradicting result 3.1. Thus, $(A_1 - \{x\}) \cap \{x, y, z\} = \emptyset$.

That $(A_2 - \{x\}) \cap \{x, y, z\} = \emptyset$ and $(A_3 - \{x\}) \cap \{x, y, z\} = \emptyset$ can be proved similarly. □

For the remainder of this section, we assume

$$B = \{x, y, z, \bar{x}, \bar{y}, \bar{z}\}, \; B' = \{a, b, c, \bar{a}, \bar{b}, \bar{c}\}$$

and o is as above.

Lemma 3.5. *Let $D_1, D_2, D_3 \in \mathfrak{R}(B)$ be the blocks on $\{\bar{a}, \bar{b}\}$, $\{\bar{a}, \bar{c}\}$, $\{\bar{b}, \bar{c}\}$, respectively, and $D_i \neq B'$, $i = 1, 2, 3$. Then $o \in D_i$, $i = 1, 2, 3$.*

Proof. If $o \notin D_i$, then D_i would be disjoint from one of U, V, W, say U, and then the union of the two disjoint blocks D_i and U would have an external block B, contradicting result 3.4. □

Lemma 3.6. *Any block determined by three points from $\{\bar{a}, \bar{b}, \bar{c}, \bar{x}, \bar{y}, \bar{z}\}$ contains exactly three points of this set.*

Proof. Suppose there exists a block A containing four points from $\{\bar{a}, \bar{b}, \bar{c}, \bar{x}, \bar{y}, \bar{z}\}$; then A contains two of $\bar{x}, \bar{y}, \bar{z}$, say $\bar{x}, \bar{y}$. Then one of the blocks on $\bar{x}, \bar{y}$ would contain two points $\alpha, \beta \in \{a, b, c\}$; consequently, one of the blocks on $\{\alpha, \beta\}$ would contain two of x, y, z, which is a contradiction. □

Lemma 3.7. *Any block determined by three points from either $\{a, b, c, x, y, z\}$ or $\{\bar{a}, \bar{b}, \bar{c}, \bar{x}, \bar{y}, \bar{z}\}$ does not contain o.*

Proof. Since three points uniquely determine a block, this lemma is just a consequence of lemmas 3.1, 3.2, 3.4 and 3.5. ❐

Lemma 3.8. *Let $X, Y, Z \in \Re(B') - \{B\}$ be three blocks on $\{x, y\}$, $\{x, z\}$ and $\{y, z\}$, respectively, $\bar{X}, \bar{Y}, \bar{Z} \in \Re(B') - \{B\}$ be three blocks on $\{\bar{x}, \bar{y}\}$, $\{\bar{x}, \bar{z}\}$, $\{\bar{y}, \bar{z}\}$, respectively. Then $o \in X \cap Y \cap Z \cap \bar{X} \cap \bar{Y} \cap \bar{Z}$.*

Proof. Since each block meets $B \cup B'$, and there are totally 21 blocks on o, the conclusion is obtained by using the above lemmas to count the blocks which do not contain o. ❐

By summarizing what we have already got, we obtain:

Theorem 3.3. *Let F be a 7-set of the point set S of $S(3, 6, 22)$. Then F is a Fano set if and only if no block determined by three points from F contains more than three points from F.*

The above results give a construction method for a Fano set F:

1. choose $\{a, b, c, x\} \subseteq S$ such that $\{a, b, c, x\}$ is not contained in any block;
2. let B' be the block determined by $\{a, b, c\}$, let $B \in \Re(B')$ be a block on x;
3. let $U, V \in \Re(B) - B'$ be the blocks on $\{a, b\}$ and $\{a, c\}$, respectively; let $o \in (U \cap V) - \{a\}$;
4. let B_1, B_2, B_3 be the blocks determined by $\{a, b, x\}$, $\{a, c, x\}$, $\{b, c, x\}$, respectively, and let

$$\{x, y, z\} = \left[B - \left(\bigcup_{i=1}^{3}(B_i \cap B)\right)\right] \cup \{x\}.$$

Then $F = \{a, b, c, x, y, z, o\}$ is a Fano set.

Example 3. *Let the point set of* $S(3,6,22)$ *be* $\{1,2,\cdots,22\}$*, the blocks be those listed on the next page* [7]. *Let* $a = 10$, $b = 11$, $c = 13$, $x = 4$; *then* $B' = \{10,11,13,16,18,20\}$. *Now we choose* $B = \{4,21,22,5,17,19\}$; *then* $U = \{10,11,9,12,14,3\}$, $V = \{10,13,1,6,8,3\}$, $o = 3$, $B_1 = \{10,11,4,2,5,6\}$, $B_2 = \{10,13,4,7,9,19\}$, $B_3 = \{11,13,4,8,14,17\}$, $\{x,y,z\} = \{4,21,22\}$ *and* $F = \{3,4,10,11,13,21,22\}$ *is a Fano set.*

Note 3.1. In the above mentioned construction, there are six choices of B, but some of them produce the same Fano set. For instance, in the above example, if we choose $B = \{4,3,21,2,8,9\}$; then $U = \{10,11,1,7,17,22\}$, $V = \{10,13,5,14,15,22\}$ and $o = 22$, $\{x,y,z\} = \{4,3,21\}$, and we get the same Fano set as in the above example. It can be proved that there are two different Fano sets which contain $\{a,b,c,x\}$.

Note 3.2. Let F_1 be one of $\{x,y,z\}$, $\{\bar{x},\bar{y},\bar{z}\}$, let F_2 be one of $\{a,b,c\}$, $\{\bar{a},\bar{b},\bar{c}\}$; then $F = F_1 \cup F_2 \cup \{o\}$ is again a Fano set.

Theorem 3.4. *Let F be a Fano set; then there are two disjoint blocks B', B'' and a point $o \notin B \cup B'$ such that F is just the set which consists of three points from each of B', B'' and o.*

Proof. Let $F = \{x,y,z,a,b,c,o\}$; let B, B' be the blocks determined by $\{x,y,z\}$ and $\{a,b,c\}$, respectively. Then $B \cap B' = \emptyset$. ❑

The Fano sets all have frequency vector $(0,42,0,35,0,0,0)$. In appendix A there are two orbits which have the same frequency vector as a Fano set. This means that the Fano sets are divided into two orbits under the action of M_{22}.

The blocks of $S(3,6,22)$.

5 6 7 13 16 17	2 3 4 8 9 21	1 2 3 5 14 17	3 4 5 12 13 18
5 6 8 12 14 21	2 3 6 12 16 20	1 2 4 13 16 22	3 4 6 7 14 22
5 7 11 14 18 19	2 3 7 11 13 15	1 2 6 7 19 21	3 4 10 15 16 17
5 8 9 10 17 18	2 3 10 18 19 22	1 2 8 11 12 18	3 5 6 9 15 19
5 10 13 14 15 22	2 4 5 6 10 11	1 2 9 10 15 20	3 5 7 10 20 21
5 11 12 15 17 20	2 4 7 17 18 20	1 3 4 11 19 20	3 5 8 11 16 22
6 7 8 9 11 20	2 4 12 14 15 19	1 3 6 8 10 13	3 6 11 17 18 21
6 7 10 12 15 18	2 5 7 9 12 22	1 3 7 9 16 18	3 7 8 12 17 19
6 9 10 16 21 22	2 5 8 13 19 20	1 3 12 15 21 22	3 8 14 15 18 20
6 10 14 17 19 20	2 5 15 16 18 21	1 4 5 7 8 15	3 9 10 11 12 14
6 11 12 13 19 22	2 6 8 15 17 22	1 4 6 9 12 17	3 9 13 17 20 22
7 8 13 18 21 22	2 6 9 13 14 18	1 4 10 14 18 21	3 13 14 16 19 21
7 9 14 15 17 21	2 7 8 10 14 16	1 5 6 18 20 22	4 5 9 14 16 20
7 15 16 19 20 22	2 9 11 16 17 19	1 5 9 11 13 21	4 5 17 19 21 22
8 9 12 13 15 16	2 11 14 20 21 22	1 5 10 12 16 19	4 6 8 16 18 19
8 10 11 15 19 21	2 10 12 13 17 21	1 7 10 11 17 22	4 6 13 15 20 21
9 12 18 19 20 21	1 6 11 14 15 16	1 8 9 14 19 22	4 7 9 10 13 19
10 11 13 16 18 20	1 7 12 13 14 20	1 13 15 17 18 19	4 7 11 12 16 21
12 14 16 17 18 22	1 8 16 17 20 21	4 9 11 15 18 22	
4 8 10 12 20 22	4 8 11 13 14 17		

3.5. *t*-blocking sets in $S(3,6,22)$.

3.5.1. 1-blocking sets in $S(3,6,22)$. In this section we characterize the 1-blocking sets in $S(3,6,22)$.

From the definitions of blocking set and t-blocking set we know that a blocking set is a t-blocking set with $t \geq 1$, which contains no block. Hence, when characterizing the t-blocking sets, we can make use of the results in [7]. Let C be a blocking set in $S(3,6,22)$; then the type of C can be determined by checking the results in [7] when $|C| \neq 9, 10, 12, 13$.

In order to determine the types of other blocking sets, we need some more detailed results. We first consider the blocking sets with ten points.

Lemma 3.9. *The blocking set $F \cup \{u, v, w\}$, where F is a Fano set, $x, y, z \notin F$ and the block determined by $\{u, v, w\}$ is 1-secant to F, has three 5-secant blocks. So $FV(F \cup \{u, v, w\}) = (0, 11, 21, 26, 16, 3, 0)$.*

Proof. Let $F = \{x, y, z, a, b, c, o\}$, let B'' be the block determined by $\{u, v, w\}$, and $o \in B''$. On $B'' - \{u, v, w, o\}$ there are four blocks besides B'', so there exists a block B on $B'' - \{u, v, w, o\}$ such that B contains at least two points in $\{x, y, z, a, b, c\}$, say x, y. Since F is a Fano set, we have $|B \cap F| = 3$. Therefore, B contains another point in $\{x, y, z, a, b, c\}$, say z. Let B' be the block determined by $\{a, b, c\}$; then $B' \cap B = \emptyset = B' \cap B''$.

By lemma 3.1, there exist three blocks U, V and W on $\{u, v\}$, $\{v, w\}$ and $\{u, w\}$, respectively, such that $U \neq B''$, $V \neq B''$, $W \neq B''$, U, V and W are disjoint from B'. By lemma 3.2 we know that $|U \cap V \cap W| = 1$. Since $B \cap B' = \emptyset$ and $(U \cup V \cup W) \cap B' = \emptyset$, we have

$$|U \cap B| = |V \cap B| = |W \cap B| = 2.$$

But it is easy to see that $o \notin U \cup V \cup W$, so

$$|U \cap \{x, y, x\}| = |V \cap \{x, y, z\}| = |W \cap \{x, y, z\}| = 1.$$

From $[B'' \cap (B - \{x,y,z\})] \cap (U \cup V \cup W) = \emptyset$, we know that the only point $\bar{x}$ in $(B - \{x,y,z\}) - (B'' \cap B)$ is contained in $U \cap V \cap W$.

Now we consider the blocks A_i $(i = 1,2,3)$ determined by $\{u,v,\alpha\}$, $\{v,w,\beta\}$ and $\{u,w,\theta\}$, respectively, where

$$\alpha \doteq \{x,y,z\} - (U \cap \{x,y,z\}),$$

$$\beta \doteq \{x,y,z\} - (V \cap \{x,y,z\}),$$

$$\theta \doteq \{x,y,z\} - (W \cap \{x,y,z\}).$$

It is easy to see that $A_1 \neq U, B''$; $A_2 \neq V, B''$; $A_3 \neq W, B''$. So $A_1 \cap B' \neq \emptyset$, $A_2 \cap B' \neq \emptyset$, $A_3 \cap B' \neq \emptyset$ and $\bar{x} \notin A_1 \cup A_2 \cup A_3$. Therefore,

$$\{x,y,x\} - (U \cap \{x,y,z\}) \subset A_1,$$

$$\{x,y,z\} - (V \cap \{x,y,z\}) \subset A_2,$$

$$\{x,y,z\} - (W \cap \{x,y,z\}) \subset A_3.$$

Consequently, $|A_i \cap \{a,b,c\}| = 1$, $i = 1,2,3$. Hence $|A_i \cap (F \cup \{u,v,w\})| = 5$, $i = 1,2,3$.

From the above proof we can see that any 5-secant block contains two points in $\{u,v,w\}$ and three points in F, of which one is from $\{a,b,c\}$, two are from $\{x,y,z\}$. So it must be one of A_1, A_2 and A_3.

The fact that $F \cup \{u,v,w\}$ is a blocking set means that $t_0 = t_6 = 0$. So $FV(F \cup \{u,v,w\}) = (0,11,21,26,16,3,0)$. □

The proof of the above lemma actually gives out a method to find the three 5-secant blocks of $F \cup \{u,v,w\}$. Now we consider the blocking sets with eleven points.

Lemma 3.10. *The blocking set $C = D \cup \{w\}$, where $D = (B - \{u\}) \cup (B' - \{v\})$, B and B' are disjoint blocks, $u \in B$, $v \in B'$ and $w \notin B \cup B'$, has six 5-secant blocks, and $FV(C) = (0, 6, 20, 25, 20, 6, 0)$.*

Proof. We can construct a Fano set F based on B and B' such that $u, v, w \in F$. Any 5-secant block of C besides B and B' contains w, meets $B - \{u\}$ and $B' - \{v\}$. So it contains w, one point in $B \cap F - \{u\}$ and one point in $B' \cap F - \{v\}$. But

$$|B \cap F - \{u\}| = 2 = |B' \cap F - \{v\}|,$$

so we have four different blocks of this kind. Hence C has six 5-secant blocks and $FV(C) = (0, 6, 20, 25, 20, 6, 0)$. ◻

Lemma 3.11. *The blocking set $F \cup A - \{u\}$, where F is a Fano set, A is a block, $|A \cap F| = 1$ and $u \in A - F$, has seven 5-secant blocks. So its frequency vector is $(0, 7, 16, 31, 16, 7, 0)$.*

Proof. Let $F = \{x, y, z, a, b, c, o\}$, $A = \{o, u, v, p, q, r, s\}$. We can properly choose two disjoint blocks B and B' such that $|B \cap F| = 3 = |B' \cap F|$, $\{x, y, z\} \subseteq B$, $\{a, b, c\} \subseteq B'$ and $B \cap A = \{u, v\}$. Using the method used in the proof of lemma 3.9 we can prove that on any two points in $\{p, q, r\}$, there exists one 5-secant block to $F \cup A - \{u\}$. Now we consider the blocks A_a, A_b and A_c determined by $\{p, v, a\}$, $\{p, v, b\}$ and $\{p, v, c\}$, respectively. It is obvious that $o, u \notin A_a \cup A_b \cup A_c$. If there exists a $i \in \{a, b, c\}$ such that $|A_i \cap F| = 1$, then A_i contains the unique point in $B - \{x, y, z, u, v\}$. So there exists at most one block of this kind, therefore two of A_a, A_b and A_c, say A_a and A_b, contain one point in $\{x, y, z\}$, respectively. Therefore,

$$|A_a \cap \{a, b, c\}| = 2 = |A_b \cap \{a, b, c\}|.$$

So $A_a = A_b$, and $|A_a \cap (F \cup A - \{u\})| = 5$.

We can similarly prove that there exist a block determined by q, v and a point in $\{a, b, c\}$, a block determined by r, v and a point in $\{a, b, c\}$ such that these two blocks are both 5-secant to $F \cup A - \{u\}$.

Any 5-secant block to $F \cup A - \{u\}$, other than A, meets F at three points, therefore contains two points in A. So it must be one of the above mentioned blocks, and so $FV(F \cup A - \{u\}) = (0, 7, 16, 31, 16, 7, 0)$. ☐

Lemma 3.12. *Let $C = F \cup \{x, y, z, w\}$, where F is a Fano set, $x, y, z, w \notin F$, any block determined by three points in $\{x, y, z, w\}$ is 1-secant to F. If $\{x, y, z, w\}$ is not contained in any block, then C has six 5-secant blocks and the frequency vector of C is $(0, 6, 20, 25, 20, 6, 0)$.*

Proof. It is easy to see that C is a blocking set. Now we only need to prove that C has six 5-secant blocks. But this can be proved by lemma 3.9 and the following fact:

Let u, v be two points not in the union of two disjoint blocks B and B'; then there exists only one block B'' on $\{u, v\}$ such that $|B'' \cap B| = 2 = |B'' \cap B'|$. ☐

In [7] the blocking sets in lemma 3.11 and lemma 3.12 are considered the same type, but are different from the blocking set in lemma 3.10. Here we see that the blocking set in lemma 3.12 and lemma 3.10 are the same type; while the blocking set in lemma 3.11 is a different type.

Let C be a blocking set with ten points; then

$$t_1 = 8 + t_5,\ t_2 = 33 - 4t_5,\ t_3 = 8 + 6t_5,\ t_4 = 28 - 4t_5.$$

Lemma 3.13. *Let C be a blocking set in $S(3, 6, 22)$ with $|C| = 10$. Then $t_5 < 5$.*

Proof. Suppose $t_5 \geq 5$. let B, B' be two 5-secant blocks to C. Then $B \cap B' \neq \emptyset$ (otherwise $t_5 = 2$) and $B \cap B' \subseteq C$(otherwise C would have two external blocks). So $|C - (B \cup B')| = 2$. Let $C - (B \cup B') = \{x, y\}$. by result 3.2 there are two blocks A and A' such that

$$|A \cap (B \cup B' \cup \{x\})| = 0 = |A' \cap (B \cup B' \cup \{x\})|.$$

So $y \in A \cap A'$. Let B_1, B_2 and B_3 be another three 5-secant blocks to C. Then $|B_i \cap [(B \cup B') \cap C]| = 4$, $i = 1, 2, 3$. Hence B_i contains either x or y. So one of x and y, say x, is contained in at least two of B_1, B_2 and B_3, say B_1, B_2. Therefore $|B_1 \cap B_2| \geq 3$, this is a contradiction. □

By lemma 3.9 we know that the type of C is $(1, 2, 3, 4, 5)$; therefore the type of $S - C$ is also $(1, 2, 3, 4, 5)$. This strengthens the result of [7]. The following theorem is a slight improvement of the results of [7].

Theorem 3.5. *If C_1 does not contain any block, then $7 \leq |C_1| \leq 13$, and*

1. *If $|C_1| = 7$, then $C_1 = F$ and $FV(F) = (0, 42, 0, 35, 0, 0, 0)$, where F is a Fano set.*
2. *If $|C_1| = 8$, then $C_1 = F \cup \{x\}$ and $FV(C_1) = (0, 28, 14, 28, 7, 0, 0)$, where F is a Fano set and $x \notin F$.*
3. *If $|C_1| = 9$, then $C_1 = F \cup \{x, y\}$ and $FV(C_1) = (0, 18, 20, 26, 12, 1, 0)$, where F is a Fano set, and $x, y \notin F$.*
4. *If $|C_1| = 10$, then C_1 is one of the following:*
   (a) *$C_1 = D := (B - \{u\}) \cup (B' - \{v\})$ and $FV(D) = (0, 10, 25, 20, 20, 2, 0)$, where B, B' are two blocks with $B \cap B' = \emptyset$, $u \in B$, $v \in B'$.*

(b) $C_1 = F \cup \{x, y, z\}$ and $FV(C_1) = (0, 11, 21, 26, 16, 3, 0)$, *where F is a Fano set, $x, y, z \notin F$ and the block determined by $\{x, y, z\}$ is 1-secant to F.*

5. *If $|C_1| = 11$, then C_1 is one of the following:*

   (a) $C_1 = (F \cup B) - \{x\}$, $FV(C_1) = (0, 11, 0, 55, 0, 11, 0)$, *where F is a Fano set, B is a block and $F \cap B = \{x\}$.*

   (b) $C_1 = D \cup \{w\}$ *and* $FV(C_1) = (0, 6, 20, 25, 20, 6, 0)$, *where D is defined as in 4 and $w \notin B \cup B$.*

   (c) $C_1 = F \cup A - \{u\}$, $FV(C_1) = (0, 7, 16, 31, 16, 7, 0)$, *where F is a Fano set, A is a block and $|A \cap F| = 1$, $u \in A - F$.*

6. *If $|C_1| = 12$, then C_1 is one of the following:*

   (a) $C_1 = \mathcal{S} - (F \cup \{x, y, z\})$ *and* $FV(C_1) = (0, 3, 16, 26, 21, 11, 0)$, *where F is a Fano set, $x, y, z \notin F$, and the block determined by $\{x, y, z\}$ is 1-secant to F.*

   (b) $C_1 = \mathcal{S} - D$ *and* $FV(C_1) = (0, 2, 20, 20, 25, 10, 0)$.

7. *If $|C_1| = 13$, then $C_1 = \mathcal{S} - (F \cup \{x, y\})$, where F is a Fano set, $x, y \notin F$, and* $FV(C_1) = (0, 1, 12, 26, 20, 18, 0)$.

Proof. Let C be a blocking set: then $7 \leq |C| \leq 15$.

1. If $|C| = 7$, then the type of C is $(1, 3)$. Solve the linear system 1 and let $t_0 = t_2 = t_4 = t_5 = t_6 = 0$, we get $t_1 = 42$ and $t_3 = 35$. So we have $FV(C) = (0, 42, 0, 35, 0, 0, 0)$.
2. If $|C| = 8$, then the type of C is $(1, 2, 3, 4)$. $FV(C) = (0, 28, 14, 28, 7, 0, 0)$.
3. If $|C| = 9$, then the type of C is $(1, 2, 3, 4, 5)$. $FV(C) = (0, 18, 20, 26, 12, 1, 0)$.
4. If $|C| = 10$, then the type of C is $(1, 2, 3, 4, 5)$.

5. If $|C| = 11$, then the type of C is $(1,3,5)$ or $(1,2,3,4,5)$.

6. If $|C| = 12$, then the type of C is $(1,2,3,4,5)$.

7. If $|C| = 13$, then the type of C is $(1,2,3,4,5)$.

8. If $|C| = 14$, then the type of C is $(2,3,4,5)$.

9. If $|C| = 15$, then the type of C is $(3,5)$.

Since C_1 does not contain any block, it is a blocking set. By lemmas 3.10, 3.11, 3.12 and theorem 7.4 in [7] the theorem is proved. □

Theorem 3.6. *If C_1 contains at least one block, then $10 \le |C_1| \le 17$, and*

1. *If $|C_1| = 10$, then $C_1 = F \cup \{x, y, z\}$, $FV(C_1) = (0, 12, 18, 28, 18, 0, 1)$, where F is a Fano set, $x, y, z \notin F$, and the block determined by $\{x, y, z\}$ is 3-secant to F.*

2. *If $|C_1| = 11$, then C_1 is one of the following:*

   (a) *$C_1 = B \cup (B' - \{a\})$, where B, B' are two blocks, $B \cap B' = \emptyset$, $a \in B'$; $FV(C_1) = (0, 5, 25, 15, 30, 1, 1)$.*

   (b) *$C_1 = (B \cup B' - \{a\}) \cup \{u, v\}$, $FV(C_1) = (0, 7, 17, 27, 22, 3, 1)$, where B, B' are two blocks, $|B \cap B'| = 2$, $a \in B' - B$, $u \notin B \cup B'$, v is one of the two joint points of the two external blocks of $B \cup B' \cup \{u\}$.*

3. *If $|C_1| = 12$, then C_1 is one of the following:*

   (a) *$C_1 = B \cup B' \cup \{u, v\}$, $FV(C_1) = (0, 4, 14, 24, 29, 4, 2)$, where B and B' are blocks, $|B \cap B'| = 2$, $u \notin B \cup B'$, v is one of the two joint points of the two external blocks of $B \cup B' \cup \{u\}$.*

   (b) *$C_1 = B \cup (B' - \{u\}) \cup \{x\}$, $FV(C_1) = (0, 3, 17, 22, 27, 7, 1)$, where B, B' are disjoint blocks, $u \in B'$ and $x \notin B \cup B'$.*

(c) $C_1 = B \cup (B' \triangle B'' - \{u, v, w\}) \cup \{x\}$. $FV(C_1) = (0, 4, 13, 28, 23, 8, 1)$, *where* B, B' *and* B'' *are blocks*, $B \cap B' = B \cap B'' = \emptyset$, $|B' \cap B''| = 2$, $u, v, w \in B'' - B'$ *and* $x \notin B \cup B' \cup B''$.

(d) $C_1 = F \cup B \cup B' - \{o\}$. $FV(C_1) = (0, 6, 5, 40, 15, 10, 1)$, *where* F *is a Fano set*, B, B' *are blocks*, $|F \cap B \cap B'| = 2$ *and* $o \in B' \cap F - B$.

4. *If* $|C_1| = 13$, *then* C_1 *is one of the following:*

(a) $C_1 = B \cup B' \cup \{u, v, w\}$. $FV(C_1) = (0, 2, 12, 16, 40, 3, 4)$, *where* B, B' *are two blocks*, $|B \cap B'| = 2$ *and* $u, v, w \notin B \cup B'$, *and* v, w *are the joint points of the two external blocks of* $B \cup B' \cup \{u\}$.

(b) $C_1 = B \cup B' \cup \{u, v, w\}$. $FV(C_1) = (0, 2, 10, 24, 28, 11, 2)$, *where* B, B' *are two blocks*, $|B \cap B'| = 2$ *and* $u, v, w \notin B \cup B'$, v *and* w *are contained in the the two external blocks of* $B \cup B' \cup \{u\}$, *but only one of* v, w *is in the join.*

(c) $C_1 = B \cup B' \cup \{u, v, w\}$. $FV(C_1) = (0, 3, 6, 30, 24, 12, 2)$, *where* B, B' *are two blocks*, $|B \cap B'| = 2$ *and* $u, v, w \notin B \cup B'$, *each of the two external blocks of* $B \cup B' \cup \{u\}$ *contains only one of* v *and* w *and* u, v *and* w *are contained in an external block of* $B \cup B'$.

(d) $C_1 = B \cup [(B' \cup B'') - \{a\}]$, $FV(C_1) = (0, 1, 13, 22, 26, 14, 1)$, *where* B, B' *and* B'' *are blocks with* $B \cap B' = \emptyset$, $|B' \cap B''| = |B \cap B''| = 2$ *and* $a \in B' \cap B''$.

5. *If* $|C_1| = 14$, *then* C_1 *is one of the following:*

(a) $C_1 = \mathcal{S} - [(B \cup B') - \{u, v\}]$, *where* B *and* B' *are two blocks*, $|B \cap B'| = 2$, $u \in B - B'$ *and* $v \in B' - B$. $FV(C_1) = (0, 2, 3, 24, 30, 14, 4)$.

(b) $C_1 = \mathcal{S} - [(B \cup B') - \{x, u\}]$, *where* B *and* B' *are two blocks*, $x \in B \cap B'$ *and* $u \in B \triangle B'$; $FV(C_1) = (0, 1, 7, 18, 34, 13, 4)$.

(c) $C_1 = S - [(B \cup B') - \{x, a, b, c\}]$, *where B and B' are two disjoint blocks, $x \in B$ and $a, b, c \in B'$*; $FV(C_1) = (0, 1, 6, 22, 28, 17, 3)$.

6. *If* $|C_1| = 15$, *then* $C_1 = [S - (B \cup \{a, b\})] \cup \{x\}$, *where B is a block, $x \in B$ and $a, b \notin B$*; $FV(C_1) = (0, 1, 2, 17, 32, 19, 6)$.

7. *If* $|C_1| = 16$, *then* $C_1 = [S - (B \cup \{a\})] \cup \{x\}$, *where B is a block, $x \in B$ and $z \notin B$*; $FV(C_1) = (0, 1, 0, 10, 35, 21, 10)$.

8. *If* $|C_1| = 17$, *then* $C_1 = (S - B) \cup \{x\}$, *where B is a block and $x \notin B$*; $FV(C_1) = (0, 1, 0, 0, 40, 20, 16)$.

Proof. Checking the appendix A we obtain that $10 \leq |C_1| \leq 17$.

Let B be a block and $B \subset C_1$.

1. If $|C_1| = 10$, let $C_1 - B = \{a, b, c, o\}$, let B' be the block determined by $\{a, b, c\}$. Since C_1 is a 1-blocking set, we have $B' \cap B = \emptyset$. According to our construction method for a Fano set in section 3.4, we only need to prove that if B_1, B_2 are two blocks on $\{o, a\}$ which are disjoint from B, then $b \in B_1$, $c \in B_2$ or $c \in B_1$, $b \in B_2$.

   Suppose $B' = \{a, b, c, d, e, f\}$. Since on each of $\{d, e\}$, $\{d, f\}$ and $\{e, f\}$ there are two blocks respectively, which are disjoint from B, and B' is one of these, let U, V, W be the other ones on $\{d, e\}$, $\{d, f\}$ and $\{e, f\}$, respectively. Because C_1 is a 1-blocking set, so $o \in U, V, W$; therefore, either $b \in B_1$ and $c \in B_2$ or $c \in B_1$ and $b \in B_2$.

   It is easy to see that C_1 has only one block, and has no 2-secant block. So $FV(C_1) = (0, 12, 18, 28, 18, 0, 1)$.

2. If $|C_1| = 11$, let $C_1 - B = \{a, b, c, d, e\}$.

If $\{a, b, c, d, e\}$ is contained in a block B', then $B' \cap B = \emptyset$ and C_1 has five 1-secant blocks. So $C_1 = B \cup B' - \{x\}$, and $FV(C_1) = (0, 5, 25, 15, 30, 1, 1)$, where $x \in B'$.

If $\{a, b, c, d, e\}$ is not contained in any block, then we claim that there exists a block B' such that B' is determined by three points from $\{a, b, c, d, e\}$ and $|B' \cap B| = 2$.

If there exist four points from $\{a, b, c, d, e\}$, say a, b, c, d, which are contained in a block B'', then $B'' \cap B = \emptyset$. Since there are only two blocks on $\{a, e\}$ which are disjoint from B, one of the blocks determined by $\{a, b, e\}$, $\{a, c, e\}$ and $\{a, d, e\}$, respectively meets B. Let B' be this block.

If no four points from $\{a, b, c, d, e\}$ are contained in any block and suppose the block determined by $\{a, b, c\}$ does not meet B; then one of the blocks determined by $\{a, b, d\}$ and $\{a, b, e\}$, respectively meets B. Let this block be B'.

Without loss of generality we may assume B' is determined by $\{a, b, c\}$. Since $B \cup B' \cup \{d\}$ has two external blocks, e must be in the intersection of the two external blocks.

It not difficult to prove that on each of d and e there exists only one block which is 5-secant to C_1. So C_1 has three 5-secant blocks. Therefore, $FV(C_1) = (0, 7, 17, 27, 22, 3, 1)$.

3. Let $|C_1| = 12$. First we consider the case when C_1 contains another block B'. In this case $|B \cap B'| = 2$. Let $C_1 - (B \cup B') = \{u, v\}$; then v must lie on the intersection of the two external blocks of $B \cup B' \cup \{u\}$ and C_1 has four 5-secant blocks. So $FV(C_1) = (0, 4, 14, 24, 29, 4, 2)$.

Now suppose C_1 contains no block other than B; then C_1 has more than two 5-secant blocks, hence there exists a block A such that A is 5-secant to C_1 and $|B \cap A| = 2$. Let $C_1 - (B \cup A) = \{a, b, c\}$.

If the block A' determined by $\{a, b, c\}$ is not disjoint from $B \cup A$, then there exists a block B' disjoint from B which contains at least two points in $\{a, b, c\}$ and meets A at the two points in $A \cap C_1$.

If $|B' \cap \{a, b, c\}| = 3$, then $C_1 = B \cup (B' - \{u\}) \cup \{x\}$, where $u \in B'$, $x \notin B \cup B'$. It is easy to see that C_1 has three 1-secant blocks. So we have $FV(C_1) = (0, 3, 17, 22, 27, 7, 1)$.

If $|B' \cap \{a, b, c\}| = 2$, then the block $B'' \neq B'$ on $B' - C_1$, which is disjoint from B, contains only one of the two points in $C_1 - (B \cup B')$ (otherwise C_1 would contain at least two blocks), so $C_1 = B \cup (B' \triangle B'' - \{u, v, w\}) \cup \{x\}$, where $u, v, w \in B'' - B'$ and $x \notin B \cup B' \cup B''$.

From the structure of a Fano set we can see that C_1 has four 1-secant blocks, therefore $FV(C_1) = (0, 4, 13, 28, 23, 8, 1)$.

Now suppose A' is disjoint from $B \cup A$. We may even assume that any block disjoint from B on two points in $\{a, b, c\}$ contains the unique point in $A - C_1$ (otherwise, we would have a block which contains four points in C_1 and is disjoint from B). Then the three points in $\{a, b, c\}$ and the point in $A - C_1$ forms a Fano set F with three points in B. The block on two points in $A' - \{a, b, c\}$ which is disjoint from B is a 1-secant block to C_1. There are three of this kind of 1-secant blocks to C_1. For any point $x \in \{a, b, c\}$, we have three different blocks on x and a point in $A' - \{a, b, c\}$ which are disjoint from B. But only one of them is disjoint from A, so it is a 1-secant block to C_1. There are three of this kind of 1-secant blocks to C_1. So C_1 has six 1-secant blocks. $FV(C_1) = (0, 6, 5, 40, 15, 10, 1)$.

4. Let $|C_1| = 13$. If C_1 contains another block B', then $|B \cap B'| = 2$ and $C_1 = B \cup B' \cup \{u, v, w\}$, where $u \notin B \cup B'$ and each of the two external blocks E_1 and E_2 of $B \cup B' \cup \{u\}$ contains at least one of v, w.

   If $v, w \in E_1 \cap E_2$, then the two external blocks E_3 and E_4 of $B \cup B'$ which contain u are the only two 1-secant blocks of C_1. B and B' are two of the four external blocks of $E_3 \cup E_4$; the other two all contain $\{v, w\}$, so they are contained in C_1, thus $FV(C_1) = (0, 2, 12, 16, 40, 3, 4)$.

   If $v \in E_1 \cap E_2$, $w \in E_1 \triangle E_2$, then C_1 has only two 1-secant blocks and contains only two blocks. So $FV(C_1) = (0, 2, 10, 24, 28, 11, 2)$.

   If $v \in E_1 - E_2$, $w \in E_2 - E_1$, we can even assume that u, v and w are contained in another external block of $B \cup B'$ (otherwise, we reduce the case to the above case), then C_1 has only three 1-secant blocks, and contains only two blocks. So $FV(C_1) = (0, 3, 6, 30, 24, 12, 2)$.

   Now suppose C_1 contains only one block B, then there exists a block B' which is 5-secant to C_1. So $B \cap B' = \emptyset$. Let $C_1 - (B \cup B') = \{u, v\}$ and $a \in B' - C_1$; then the block B'' determined by $\{a, u, v\}$ meets B (otherwise, C_1 would contain another block). So $C_1 = B \cup [(B' \cup B'') - \{a\}]$. It is easy to prove that B is the only block contained in C_1; the block which contains $B'' \cap B'$, and is disjoint from B, is the only block which meets C_1 at one point. So $FV(C_1) = (0, 1, 13, 22, 26, 14, 1)$.

5. Here we only prove the case of $|C_1| = 14$; the other cases can be proved similarly.

Since C_1 is a 1-blocking set, there exists a block B such that B is 1-secant to C_1. Let $x \in B \cap C_1$, $S - (C_1 \cup B) = X$, and let B' be the block determined by X. If $B' \cap B \neq \emptyset$, then the four external blocks of $B \cup B'$ are the only blocks contained in C_1. If $x \notin B' \cap B$, then B and B' are the only 1-secant blocks of C_1, so $FV(C_1) = (0, 2, 3, 24, 30, 14, 4)$; if $x \in B' \cap B$, then B is the only 1-secant block of C_1, $FV(C_1) = (0, 1, 7, 18, 34, 13, 4)$. If $B' \cap B = \emptyset$, then $|B' \cap C_1| = 3$. The three blocks which contain two points in $B' \cap C_1$ and are disjoint from B are the only blocks contained in C_1; B is the only 1-secant block of C_1. So $FV(C_1) = (0, 1, 6, 22, 28, 17, 3)$.

□

3.5.2. **2-blocking sets in $S(3, 6, 22)$.**

Lemma 3.14. *Let B be a block in $S(3, 6, 22)$, $x, y \in B$, and A_i, $i = 1, 2, 3, 4$, be another four blocks on $\{x, y\}$. Let $a, b \in A_1 - B$, and let $U_1, U_2 \neq A_1$ be another two blocks on $\{a, b\}$ which meet B. Then U_1 meets one of A_j, $j = 2, 3, 4$, and if $U_1 \cap A_j \neq \emptyset$, then $U_2 \cap A_j \neq \emptyset$ and $(U_1 \cap A_j) \cup (U_2 \cap A_j) = A_j - \{x, y\}$.*

Proof. Because $|U_1 \cap B| = 2$, $|A_1 \cup A_2 \cup A_3 \cup A_4 \cup B| = 22$ and $|U_1| = 6$, so U_1 meets one of A_2, A_3 and A_4. Suppose $U_1 \cap A_2 \neq \emptyset$. Since U_2 also meets one of A_2, A_3 and A_4, if $U_2 \cap A_2 = \emptyset$, and U_2 meets one of A_3, A_4, say A_3, then $|U_2 \cap A_3| = 2$. Let V_1, V_2 be the two blocks on $\{a, b\}$ which do not meet B; then neither V_1 nor V_2 can meet both A_2 and A_3, while both V_1 and V_2 can only meet two of A_2, A_3 and A_4. Suppose $V_1 \cap A_2 \neq \emptyset$, $V_1 \cap A_4 \neq \emptyset$, $V_2 \cap A_3 \neq \emptyset$, $V_2 \cap A_4 \neq \emptyset$; then $(V_1 \cap A_2) \cup (U_1 \cap A_2) = A_2 - B$, $(V_2 \cap A_3) \cup (U_2 \cap A_3) = A_3 - B$ and $(V_1 \cup V_2) \cap A_4 = A_4 - B$. Now consider $A_2 \cup B$. The block V_2 is external to $A_2 \cup B$ and $a \in V_2$. Let W be another external block to $A_2 \cup B$ which contains a;

then W contains at most one point in each of $(V_2 \cap A_3) \cup (V_2 \cap A_4)$, $V_1 \cap A_4$, $U_2 \cap A_3$, respectively, so W meets $A_3 \cup A_4$ in at most three points. Thus, W contains at most five points, which contradicts $|W| = 6$. So $U_2 \cap A_2 \neq \emptyset$. Since $\{a, b\} \subseteq U_1 \cap U_2$ and $U_1 \neq U_2$, we must have $(U_1 \cap A_2) \cup (U_2 \cap A_2) = A_2 - \{x, y\}$. ❐

Lemma 3.15. *Let B, x, y, A_i, $i = 1, 2, 3, 4$, be as in lemma 3.14, let $a, b, c \in A_1 - \{x, y\}$, and let U, V, W be blocks on $\{a, b\}$, $\{a, c\}$ and $\{b, c\}$, respectively, which meet B. Then*

$$\{j \mid 2 \leq j \leq 4,\ A_j \cap (U \cup V \cup W) \neq \emptyset\} = \{2, 3, 4\}.$$

Proof. Suppose $U \cap A_2 \neq \emptyset$, $V \cap A_2 \neq \emptyset$; then by lemma 3.14, a would lie on at least four external blocks of $A_3 \cup A_4$, which contradicts result 3.2. ❐

Lemma 3.16. *Let B and B' be two disjoint blocks, E a 13-subset with $B \subseteq E$ and $|E \cap B'| = 5$; then E is not a 2-blocking set.*

Proof. Let $E - (B \cup B') = \{u, v\}$, $B' = \{a, b, c, d, e, x\}$, where $a, b, c, d, e \in E$ and $x \notin E$; let r be the number of the blocks on any one of $\{x, u\}$, $\{x, v\}$, which are disjoint from B. Then by lemma 3.1 $r \leq 4$. Because the five blocks on $\{x, a\}$, $\{x, b\}$, $\{x, c\}$, $\{x, d\}$ and $\{x, e\}$, respectively, which are disjoint from B and are not equal to B', are all different, so at least one of them contains neither u nor v, and this block is 1-secant to E. Therefore E is not a 2-blocking set. ❐

Similarly we can prove

Lemma 3.17. *If B, B' are two disjoint blocks, E is a 12-subset, $B \subset E$ and $4 \leq |E \cap B'| \leq 5$, then E is not a 2-blocking set.*

Lemma 3.18. *Let C_2 be a 2-blocking set in $S(3,6,22)$. B, U, V be blocks such that $\emptyset \neq U \cap B = V \cap B \neq B$. If $B \subseteq C_2$ and C_2 contains at least five points in each of U and V, then C_2 contains a block B' such that $|B' \cap B| = 2$.*

Proof. This is a consequence of lemmas 3.14 and 3.15. ❑

Theorem 3.7. *Let C_2 be a 2-blocking set in $S(3,6,22)$.*

1. *If C_2 does not contain any block, then $|C_2| = 14$ and $C_2 = S - (F \cup \{x\})$, $FV(C_2) = (0,0,7,28,14,28,0)$, where F is a Fano set and $x \notin F$.*
2. *If C_2 contains a block, then $12 \leq |C_2| \leq 18$.*
   (a) *If $|C_2| = 12$, then $C_2 = B \cup B'$, $FV(C_2) = (0,0,30,0,45,0,2)$, where B, B' are blocks and $B \cap B' = \emptyset$.*
   (b) *If $|C_2| = 13$, then $C_2 = B \cup B' \cup \{x\}$, $FV(C_2) = (0,0,18,12,36,9,2)$, where B and B' are two disjoint blocks and $x \notin B \cup B'$.*
   (c) *If $|C_2| = 14$, then C_2 is one of the following:*
      (i) *$C_2 = B \cup B' \cup B''$, $FV(C_2) = (0,0,14,0,56,0,7)$, where B, B' and B'' are blocks with $|B \cap B' \cap B''| = 2$.*
      (ii) *$C_2 = B \cup B' \cup B''$, $FV(C_2) = (0,0,10,16,32,16,3)$, where B, B' and B'' are blocks, $|B \cap B'| = 2 = |B' \cap B''|$, and $(B \cap B') \cap (B' \cap B'') = \emptyset$.*
      (iii) *$C_2 = B \cup B' \cup (B'' - \{u\}) \cup \{x\}$, $FV(C_2) = (0,0,9,20,26,20,2)$, where B, B' and B'' are blocks with $|B \cap B''| = 2 = |B' \cap B''|$, $(B \cap B') \cap (B' \cap B'') = \emptyset$, $u \in B'' - B'$ and $x \notin B \cup B' \cup B''$.*
   (d) *If $|C_2| = 15$, then C_2 is one of the following:*
      (i) *$C_2 = S - [(B \triangle B') - \{u\}]$, $FV(C_2) = (0,0,7,7,42,14,7)$, where B and B' are blocks, $u \in B \triangle B'$.*

(ii) $C_2 = \mathcal{S} - [(F - \{o\}) \cup \{u\}]$, $FV(C_2) = (0, 0, 4, 19, 24, 26, 4)$, *where* F *is a Fano set,* $o \in F$ *and* $u \notin F$.

(iii) $C_2 = \mathcal{S} - [(F - \{o, x\}) \cup \{u, v\}]$, $FV(C_2) = (0, 0, 5, 15, 30, 22, 5)$, *where* F *is a Fano set* $o, x \in F$, $u, v \notin F$.

(e) *If* $|C_2| = 16$, *then* C_2 *is one of the following:*

(i) $C_2 = \mathcal{S} - (B \triangle B' - \{u, v\})$, $FV(C_2) = (0, 0, 3, 8, 33, 24, 9)$, *where* B *and* B' *are two blocks,* $|B \cap B'| = 2$ *and* $u, v \in B' - B$.

(ii) $C_2 = [\mathcal{S} - (B \cup B' - \{u, v, w, o\})]$, $FV(C_2) = (0, 0, 2, 12, 27, 28, 8)$, *where* B *and* B' *are two blocks,* $|B \cap B'| = 2$, $o \in B \cap B'$, $u, v \in B' - B$ *and* $w \in B - B'$.

(f) *If* $|C_2| = 17$, *then* $C_2 = \mathcal{S} - (B \triangle B' - \{u, v, w\})$, *and* $FV(C_2) = (0, 0, 1, 6, 26, 31, 13)$, *where* B *and* B' *are two blocks with* $|B \cap B'| = 2$ *and* $u, v, w \in B' - B$.

(g) *If* $|C_2| = 18$, *then* $C_2 = \mathcal{S} - (B - \{u, v\})$, $FV(C_2) = (0, 0, 1, 0, 24, 32, 20)$, *where* B *is a block and* $u, v \in B$.

Proof. We prove the theorem case by case:

1. Since C_2 does not contain any block, C_2 actually is a blocking set. By checking the type of the blocking sets we obtain $|C_2| = 14$ and $C_2 = \mathcal{S} - (F \cup \{x\})$, where F is a Fano set, $x \notin F$.

2. Let $B \subset C_2$ be a block. By checking the appendix A, we can obtain that $12 \le |C_2| \le 18$.

   (a) $|C_2| = 12$.

   Since both $B \cup B' \cup \{u, v\}$ and $(B \cup B' - \{x\}) \cup \{u, v, w\}$, where $|B \cap B'| = 2$, $x \in B' - B$, $u, v, w \notin B \cup B'$, are not 2-blocking sets, any block determined by three points in $C_2 - B = \{a, b, c, d, e, f\}$ is disjoint from B. Let B' be the block determined by $\{a, b, c\}$; we claim that $d, e, f \in B'$. Otherwise, by lemma 3.17 $d, e, f \notin B'$ and one of the blocks determined by $\{e, d, f\}$, $\{e, d, a\}$, $\{e, d, b\}$ and $\{e, d, c\}$ would meet B. Thus $C_2 = B \cup B'$ and $B \cap B' = \emptyset$. It is easy to see that C_2 contains only two blocks, so we have $FV(C_2) = (0, 0, 30, 0, 45, 0, 2)$.

(b) $|C_2| = 13$.

If C_2 contains another block B', then $B \cap B' = \emptyset$. Otherwise each of the four external blocks of $B \cup B'$ would contain at least two of the three points in $C_2 - (B \cup B')$; this is not possible since each point outside of $B \cup B'$ lies on exactly two of the four external blocks. So $B \cap B' = \emptyset$. Let $\{x\} = C_2 - (B \cup B')$; then we are done.

Now we prove that C_2 does really contain another block.

Suppose C_2 does not contain another block.

It is not difficult to prove that there exists a block B'' which is 5-secant to C_2. By lemma 3.16 $|B \cap B''| = 2$. Let $B'' - B = \{a, b, c, o\}$, where $a, b, c \in C_2$ and $o \notin C_2$. Let $u, v, x, y \in C_2 - (B \cup B'')$ and let E_1, E_2 be two external blocks of $B \cup B'' \cup \{u\}$. Then each of E_1, E_2 contains at least two of v, x and y; therefore $E_1 \cap E_2$ contains at least one of v, x and y, say v. Since in $\Re(B)$ there are two blocks on $\{x, y\}$, one of them, say U, meets B'' at two of a, b and c, say a and b. Let V be the block determined by $\{u, v, o\}$; then $V \in \Re(B)$ and $|V \cap B''| = 2$. Since by lemma 3.16 there is no block in $\Re(B)$ which is 5-secant to C_2, $\{x, y\}$ is not contained in V. If $V \cap B'' = \{c, o\}$, then $U \cap V$ contains a point $w \notin C_2$. Then the block in $\Re(B)$, which goes through $\{w, o\}$ and is different from V, can not contain

u, v, c and contains at most one of a, b, x, y. So this block contains at most one point in C_2. If $V \cap B'' = \{a, o\}$, let $V' \in \Re(B)$ be the other block on $\{u, v\}$. Then $b, c \in V'$ and therefore by lemma 3.16 $x, y \notin V'$. So there are two points $p, q \in V'$ such that $p, q \notin C_2$, $p \in V' \cap U$ and $q \in V' - U$. The second block in $\Re(B)$ which goes through $\{p, q\}$ can not contain u, v, b, c and contains at most one of x, y, a, so this block contains at most one point in C_2.

(c) $|C_2| = 14$.

We prove that C_2 contains two blocks A, A' such that $|A \cap A'| = 2$. Let T be a block which is 2-secant to C_2, let $C_2 \cap T = \{x, y\}$ and let A_i $(i = 1, 2, 3, 4)$ be the other four blocks on $\{x, y\}$.

If at least two of A_i $(i = 1, 2, 3, 4)$ are contained in C_2, then we are done: if only one of them is contained in C_2, then two of the rest are 5-secant to C_2, and so by lemma 3.18, the conclusion is also true.

If $|T \cap B| = 2$, then we are done.

If $|T \cap B| = 0$ we may even assume that none of A_i $(i = 1, 2, 3, 4)$ is contained in C_2, so A_i $(i = 1, 2, 3, 4)$ are all 5-secant to C_2, and one of A_i $(i = 1, 2, 3, 4)$, say A_1, is disjoint from B. Let a, b and c be the three points contained in $C_2 - (B \cup T \cup A_1)$; let U, V and W be the other three external blocks of $T \cup A_1$, $a \in U \cap V$.

(i) If $U \cap V \subset C_2$, then the block determined by $(W \cap B) \cup \{a\}$ contains $U \cap V$, $T \cap A_1$ and $W \cap B$. Let this block and B be A and A', respectively; then we are done.

(ii) If $U \cap V$ is not contained in C_2, then $b, c \in W$. If $b, c \in U$ or $b, c \in V$, then the block determined by $(B \cap V) \cup \{b\}$ or $(B \cap U) \cup \{b\}$ contains

$U \cap W$ and $T \cap A_1$ or $V \cap W$ and $T \cap A_1$. Let this block and B be A and A', respectively; then we are done. If $b \in U$, $c \in V$, then $U \cap W$ contains a point $u \notin C_2$ and $V \cap W$ contains a point $v \notin C_2$. Now W is a block on $\{u, v\}$ which does not meet A_1. Let B'' be the other block on $\{u, v\}$ which does not meet A_1; then $(U \cap V) \cap B'' = \emptyset$, so B'' contains one point in each of $U \cap B$ and $V \cap B$, and two points in $T - A_1$, and $|B'' \cap B| = 2$. So we are done.

Let A, A' be two blocks contained in C_2 and $|A \cap A'| = 2$; then $|C_2 - (A \cup A')| = 4$. Let $C_2 - (A \cup A') = \{a, b, c, d\}$. Since C_2 is a 2-blocking set, each of the four external blocks of $A \cup A'$ contains exactly two of a, b, c and d. Now we consider the block A'' determined by $\{a, b, c\}$. A'' contains another point outside $A \cup A$. If $d \in A''$, then either $A \cap A' \subseteq A''$ or A'' meets only one of A and A'. If $A \cap A' \subseteq A''$, then $C_2 = A \cup A' \cup A''$ and C_2 contains seven blocks, so $FV(C_2) = (0, 0, 14, 0, 56, 0, 7)$. If A'' meets only one of A and A', say A', then $C_2 = A \cup A' \cup A''$, $A'' \cap A = \emptyset$. In this case C_2 contains only three blocks, so $FV(C_2) = (0, 0, 10, 16, 32, 16, 3)$. If $d \notin A''$, then A'' meets only one of A and A', say A'. In this case C_2 contains only two blocks, so $FV(C_2) = (0, 0, 9, 20, 26, 20, 2)$.

(d) $|C_2| = 15$.

Let B be a block which is 2-secant to C_2, let B' be the block determined by the three points in $S - (C_2 \cup B)$; then either $B' \cap (B \cap C_2) \neq \emptyset$ or $B' \cap B = \emptyset$. If $B' \cap (B \cap C_2) \neq \emptyset$, we may even assume that $B \cap C_2 \subseteq B'$ (otherwise it could reduced to the other case), then C_2 contains seven blocks. So $FV(C_2) = (0, 0, 7, 7, 42, 14, 7)$. If $B' \cap B = \emptyset$, then we choose a point o in C_2 such that $\{o\} \cup (B' - C_2)$ and a point in $B - C_2$ forms a Fano set F. If F contains no point in $B \cap C_2$, then $C_2 = \mathcal{S} - [(F - \{o\}) \cup \{u\}]$, where $u \notin F$. From the structure of a Fano set we know that C_2 contains four blocks. So $FV(C_2) = (0, 0, 4, 19, 24, 26, 4)$. If F contains one point x in $B \cap C_2$, then $C_2 = \mathcal{S} - [(F - \{o, x\}) \cup \{u, v\}]$, where $o, x \in F$. In this case C_2 contains five blocks. So $FV(C_2) = (0, 0, 5, 15, 30, 22, 5)$.

(e) $|C_2| = 16$.

Let B be a block which is 2-secant to C_2, then $|\mathcal{S} - (B \cup C_2)| = 2$. Let B' be a block determined by $\mathcal{S} - (B \cup C_2)$ and one point in $B \cap C_2$. If B' contains the other point in $B \cap C_2$, then $C_2 = \mathcal{S} - (B \triangle B' - \{u, v\})$, where $u, v \in B' - B$. It is easy to see that C_2 contains nine blocks. So $FV(C_2) = (0, 0, 3, 8, 33, 24, 9)$. If B does not contain the other point in $B \cap C_2$, then $C_2 = [\mathcal{S} - (B \cup B' - \{u, v, w, o\})]$, $o \in B \cap B'$, $u, v \in B' - B$ and $w \in B - B'$. It is easy to see that there exist only two 2-secant blocks to C_2. So $FV(C_2) = (0, 0, 2, 12, 27, 28, 8)$.

The cases of $|C_2| = 17$ and $|C_2| = 18$ can be proved similarly.

□

3.5.3. **3-blocking sets in** $S(3, 6, 22)$.

Theorem 3.8. *We have* $15 \leq |C_3| \leq 19$.

1. *If* $|C_3| = 15$, *then* $C_3 = \mathcal{S} - F$, $FV(C_3) = (0, 0, 0, 35, 0, 42, 0)$, *where* F *is a Fano set.*
2. *If* $|C_2| = 16$, *then* $C_3 = (\mathcal{S} - F) \cup \{x\}$, $FV(C_3) = (0, 0, 0, 20, 15, 36, 6)$, *where* F *is a Fano set and* $x \in F$.
3. *If* $|C_3| = 17$, *then* $C_3 = (\mathcal{S} - F)\{x, y\}$, $FV(C_3) = (0, 0, 0, 10, 20, 35, 12)$, *where* F *is a Fano set,* $x, y \in F$.

4. *If* $|C_3| = 18$. *then* $C_3 = (\mathcal{S} - F) \cup \{x, y, z\}$. $FV(C_3) = (0, 0, 0, 4, 18, 36, 19)$. *where* F *is a Fano set*. $x, y, z \in F$.

5. *If* $|C_3| = 19$. *then* $C_3 = (\mathcal{S} - F) \cup \{x, y, z, w\}$. $FV(C_3) = (0, 0, 0, 1, 12, 36, 28)$. *where* F *is a Fano set*. $x, y, z, w \in F$.

Proof. Let $C = (B \cup B' - A) \cup X$. where B. B' are blocks. $|B \cap B'| = 2$. $A \subseteq B' - B$. $0 \leq |A| \leq 1$. $|X| = 4 + |A|$. $X \cap (B \cup B') = \emptyset$. Since $B \cup B'$ has four external blocks. it is not difficult to prove that C is not a 3-blocking set.

Let $C = (B \cup B' - A) \cup X$. where B. B' are two disjoint blocks. $A \subseteq B'$. $0 \leq |A| \leq 3$. $|X| = 2 + |A|$. $X \cap (B \cup B') = \emptyset$. If $|A| = 3$. let $a, b \in A$. let B'' be another block on $\{a, b\}$ which is disjoint from B. If $|B'' \cap X| \geq 3$. then at least one of the four external blocks of $B'' \cup B'$ contains no more than two points from C. so C is not a 3-blocking set. When $|A| = 0, 1$ or 2. we can similarly prove that C is not a 3-blocking set either.

So $15 \leq |C_3|$. It is easy to see that $|C_3| \leq 19$.

Suppose $|C_3| = 15$: then $C_3 = \mathcal{S} - F$. where $F = \{a, b, c, x, y, z, o\}$. Since C_3 is a 3-blocking set. any block determined by three points of F contains exactly three points of F. Let B and B' be the blocks determined by $\{x, y, z\}$ and $\{a, b, c\}$. respectively: then $B \cap B' = \emptyset$ (otherwise two of the blocks determined by $\{x, y, a\}$. $\{x, y, b\}$ and $\{x, y, c\}$ would be the same block. and this block would contain four points from $\{a, b, c, x, y\} \subset F$). So F is a Fano set.

Now suppose $|C_3| = 15 + r$. $1 \leq r \leq 4$: then $C_3 = \mathcal{S} - (\{a, b, c\} \cup A)$. where $|A| = 4 - r$. $A \cap \{a, b, c\} = \emptyset$. Let B' be the block determined by $\{a, b, c\}$. let $B \in \Re(B')$ be a block on A (if $A = \emptyset$: then let $B \in \Re(B')$). let $x \in A$ (if $A = \emptyset$: then choose any point $x \in B$). Denote by B_1, B_2 and B_3 the blocks determined by

$\{a,b,x\}$, $\{a,c,x\}$ and $\{b,c,x\}$, respectively; then $B_i \neq B_j$ if $i \neq j$. Let $\bar{x} \in B_1 \cap B - \{x\}$, $\bar{y} \in B_2 \cap B - \{x\}$, $\bar{z} \in B_3 \cap B - \{x\}$ and $\{x,y,z\} = B - \{\bar{x},\bar{y},\bar{z}\}$; then any block determined by three points from $\{a,b,c,x,y,z\}$ contains exactly three points in $\{a,b,c,x,y,z\}$. By theorem 3.3, there exists a point o such that $F = \{a,b,c,x,y,z,o\}$ is a Fano set. Let $X = F - (\{a,b,c\} \cup A)$; then $|X| = r$ and $C_3 = (\mathcal{S} - F) \cup X$. □

3.5.4. ***t*-blocking sets, $t = 4,5$, in $S(3,6,22)$.** The following theorem is easy to prove, so we omit the proof.

Theorem 3.9. $C_4 = \mathcal{S} - \{x,y\}$, $FV(C_4) = (0,0,0,0,5,32,40)$; $C_5 = \mathcal{S} - \{x\}$, $FV(C_5) = (0,0,0,0,0,21,56)$.

3.6. *t*-blocking sets in $S(4,7,23)$.

3.6.1. **Some known results about $S(4,7,23)$.** We recall the following:

Result 3.4. [40, 5.5] Every block in $S(4,7,23)$ is of type $(1,3,7)$.

Check the appendix B we know that the frequency vector of a block is $(0,112,0,140,0,0,0,1)$.

Result 3.5. (L. Berardi [8] lemma 2.3.) Let B, B' be two blocks in $S(4,7,23)$ with $|B \cap B'| = 3$. Then $FV(B \cup B') = (0,12,48,75,80,36,0,2)$.

Result 3.6. [8, lemma 2.4] Let B, B' be two blocks in $S(4,7,23)$ with $|B \cap B'| = 3$. Fix $x \in B - B'$, $y \in B' - B$ and $u \notin B \cup B'$. Then there exists at least one block through x, y, u intersecting $B \cup B'$ only at x and y.

Result 3.7. [8, lemma 2.5] Let B, B' be two blocks in $S(4,7,23)$ with $|B \cap B'| = 3$. Fix $x \in B - B'$ and $y \in B' - B$. There are exactly three blocks E_1, E_2 and E_3 intersecting $B \cup B'$ only at x and y. Moreover, $E_1 \cap E_2 \cap E_3 = \{x, y\}$.

Result 3.8. [8, lemma 2.7] Let B, B' be two blocks in $S(4,7,23)$ with $|B \cap B'| = 1$. The symmetric difference $B \triangle B'$ is a 12-set of type $(2,4,6)$, so it is a reducible blocking set, $FV(B \triangle B') = (0,0,66,0,165,0,22,0)$.

Result 3.9. [8, lemma 2.10] Let B, B' be two blocks in $S(4,7,23)$ with $|B \cap B'| = 1$. Then $FV(B \cup B') = (0,0,36,30,120,45,20,2)$.

Result 3.10. [8, lemma 2.11] Let B, B' be two blocks in $S(4,7,23)$ with $|B \cap B'| = 1$. Fix $x \in B - B'$ and $y \in B' - B$. There exists exactly one block B'' intersecting $B \cup B'$ at x, y exactly.

Result 3.11. [8, 2.12] Let B, B' be two blocks in $S(4,7,23)$ with $B \cap B' = \{w\}$. Fix $x \in B - \{w\}$, $y \in B' - \{w\}$ and $z \notin B \cup B'$. Then the block B'' that is 2-secant to $B \cup B'$ at x, y contains z iff z is on a block through x, y and 6-secant to $B \cup B'$.

Here we use the same terminology and notations as in [8]. Let B and B' be two blocks. Define:

$E_0 := \mathcal{S} - (B \triangle B')$, where $|B \cap B'| = 1$;

$E_1 := B \cup B' - \{x, u\}$, where $B \cap B' = \{x\}$ and $u \in B' - B$.

By [8] and theorem 2.2 we have

Lemma 3.19. *Let C be a blocking set in $S(4,7,23)$; then $|C| = 11$ or 12 and*

1. *if $|C| = 11$, then $C = E_0$ or E_1;*
2. *if $|C| = 12$, then $C = \mathcal{S} - E_0$ or $\mathcal{S} - E_1$.*

Lemma 3.20. *Let B be a block in $S(4,7,23)$, and $x,1,2,3,4$ five points not in B. Then there is a block B' such that B' contains at least four of $x,1,2,3,4$ and $|B \cap B'| = 1$.*

Proof. If $x,1,2,3,4$ are contained in a block, then we are done; otherwise the five different 4-subsets of $\{x,1,2,3,4\}$ determine five different blocks, and at least four of them meet B at only one point. □

Let B and B' be two blocks in $S(4,7,23)$ with $|B \cap B'| = 1$, and let $B - B' = \{a_1, a_2, a_3, a_4, a_5, a_6\}$, $x \in B' - B$. Denote by U_i the unique block that intersects $B \cup B'$ only at $\{x, a_i\}$, $i = 1, \cdots, 6$.

Lemma 3.21. *The six blocks U_i, $i = 1, \cdots, 6$, satisfy the following conditions:*

1. $|U_i \cap U_j| \geq 3$, *and* $|U_i \cap U_j| = 3$ *iff* $i \neq j$;
2. *Any point in $S - B \cup B'$ lies on exactly three of U_i, $i = 1, \cdots, 6$. Any two points in $S - U \cup B'$ are contained in at least one of U_i, $i = 1, \cdots, 6$.*

Proof. 1. Suppose $|U_1 \cap U_2| < 3$; then $|U_1 \cap U_2| = 1$, hence $|U_3| \leq 6$.

2. If there exists $w \in S - (B \cup B')$ such that $w \in U_1 \cap U_2 \cap U_3 \cap U_4$, then one of U_i, $i = 1, \cdots, 6$, contains at most six points.

If any point in $S - (B \cup B')$ lies on one or two of U_i, $i = 1, \cdots, 6$, then there must exist another point which lies on four or more than four blocks.

Let $a, b \in S - (B \cup B')$. Suppose a lies on U_1, U_2 and U_3. Since $|S - (B \cup B')| = 10$,

$$\left|(S - (B \cup B')) \cap \left(\bigcap_{i=1}^{3} U_i\right)\right| = 1,$$

and a is the only point in $S - B \cup B'$ that lies on $U_1 \cap U_2 \cap U_3$. Since

$$|U_i \cap U_j| = 3, \; i \neq j, \; 1 \leq i, j \leq 3,$$

there are three points in

$$\left(\bigcup_{i=1}^{3} U_i\right) - B \cup B' \cup \{a\},$$

every one of which lies on two of U_i, $i = 1, 2, 3$; each one of the remaining points lies on only one of U_i, $i = 1, 2, 3$. Therefore

$$3 \times 2 + \left|\left(\bigcup_{i=1}^{3} U_i\right) - B \cup B' \cup \{a\}\right| - 3 = 4 \times 3 = 12,$$

so

$$\left|\left(\bigcup_{i=1}^{3} U_i\right) - B \cup B' \cup \{a\}\right| = 9,$$

and b lies on one of U_i, $i = 1, 2, 3$. □

Let B and B' be two blocks in $S(4, 7, 23)$ with $B \cap B' = \{a, b, c\}$.

Lemma 3.22. *There are exactly three blocks T_1, T_2 and T_3 on $\{a, b, c\}$ such that $T_i \cap (B \triangle B') = \emptyset$ for $i = a, b, c$.*

Proof. There are five blocks on $\{a, b, c\}$, B and B' being two of them. So the remaining three can not contain any point in $B \triangle B'$. □

Lemma 3.23. *For $i \in \{a, b, c\}$, there are exactly four blocks T_{ij} $(j = 1, 2, 3, 4)$ such that $T_{ij} \cap (B \cup B') = \{i\}$, $|T_{ij} \cap T_{ik}| = 3$ and each point in $\mathcal{S} - (B \cup B')$ lies on only two of them.*

Proof. There are twelve 1-secant blocks to $B \cup B'$, so each one of them meets $B \cup B'$ at one point in $B \cap B'$. If there is a point $x \in \mathcal{S} - (B \cup B')$ such that x lies on three blocks T_{i1}, T_{i2} and T_{i3}, which meet $B \cup B'$ at i,then one of T_{i1}, T_{i2} and T_{i3} would contain at most six points, a contradiction. So the twelve 1-secant blocks to $B \cup B'$ can be divided into three groups, each group with four blocks, all of which meet $B \cap B'$ at the same point; each point in $\mathcal{S} - (B \cup B')$ lies on exactly two blocks of the group. Let T_{ij} $(j = 1,2,3,4)$ be the four blocks which meet $B \cap B'$ at i, $i \in \{a,b,c\}$. Then $|T_{ij} \cap T_{ik}| = 3$. ☐

Lemma 3.24. *Fix $i \in \{a,b,c\}$. For any $l \in \{a,b,c\}$ we have $|T_{ij} \cap T_l - \{i\}| = 2$ $(j = 1,2,3,4)$ and either*

$$T_{ij} \cap T_l - \{i\} = T_{ik} \cap T_l - \{i\}$$

or

$$(T_{ij} \cap T_l - \{i\}) \cup (T_{ik} \cap T_l - \{i\}) = T_l - \{a,b,c\}.$$

Proof. If $|T_{ij} \cap T_l - \{i\}| \neq 2$, then $|T_{ij} \cap T_l - \{i\}| = 0$ and one of the blocks T_{ik} $(j \neq k \in \{1,2,3,4\})$ would contain at most five points.

If there exist $j,k \in \{1,2,3,4\}$ and $j \neq k$ such that

$$T_{ij} \cap T_l - \{i\} \neq T_{ik} \cap T_l - \{i\}$$

and

$$(T_{ij} \cap T_l - \{i\}) \cup (T_{ik} \cap T_l - \{i\}) \neq T_l - \{a,b,c\},$$

then $|(T_{ij} \cap T_l - \{i\}) \cap (T_{ik} \cap T_l - \{i\})| = 1$. Let $(T_{ij} \cap T_l - \{i\}) \cap (T_{ik} \cap T_l - \{i\}) = \{x\}$ and $T_{ij} \cap T_{ik} - \{i,x\} = \{a\}$, where $a \in T_m$, $m \neq l$. Then the block determined by $(T_{ij} \cup T_{ik}) \cap T_l$ and $T_{ij} \cap T_m - \{a,i\}$ would either not meet at least one of B and B' or meet one of them at two points. ☐

Fix $u \in B - B'$, $v \in B' - B$. Let B'' be the block determined by $\{i,j,u,v\}$, where $i,j \in \{a,b,c\}$.

Lemma 3.25. 1. $|[B'' - (B \cup B')] \cap T_l| = 1$ *for* $l = a,b,c$.

2. *For a fixed* $l \in \{i, j\}$, $|B'' \cap (T_{lk} - \{l\})| = 0$ *or* 2 *for* $k = 1, 2, 3, 4$. *Moreover, there exists only one* $k \in \{1, 2, 3, 4\}$ *such that* $|B'' \cap (T_{lk} - \{l\})| = 0$.

3. *For* $x \in \{a, b, c\} - \{i, j\}$ *we have* $|B'' \cap T_{xj}| = 1$ *or* 3 $(j = 1, 2, 3, 4)$ *and there exists only one* $k \in \{1, 2, 3, 4\}$ *such that* $|B'' \cap T_{xk}| = 3$.

Proof. The results are the consequence of lemma 3.23 and the fact that any two blocks meet either at one point or three points. □

Lemma 3.26. *Let* A_i $(i = 1, 2, 3)$ *be the three blocks which meet* $B \cup B'$ *only at* x *and* v, *where* $x \in B - B'$.

1. *If* $x = u$, *then*

$$|A_i \cap (B'' - B \cup B')| = 1, \quad i = 1, 2, 3,$$

and

$$(A_1 \cup A_2 \cup A_3) \cap (B'' - B \cup B') = B'' - B \cup B'.$$

2. *If* $x \neq u$, *then one of* A_1, A_2 *and* A_3 *does not meet* $B'' - B \cup B'$, *and the remaining two meet* $B'' - B \cup B'$ *at two points.*

Proof. Since $|A_i - (B \cup B')| = 5$, A_i meets one of $T_1 - \{a, b, c\}$, $T_2 - \{a, b, c\}$ and $T_3 - \{a, b, c\}$ at three points, and meets each of the remaining two at one point.

Let

$$T_1 = \{a, b, c, \alpha, \beta, \gamma, \theta\}$$

$$T_2 = \{a, b, c, x, y, z, w\}$$

$$T_3 = \{a, b, c, p, q, s, t\}$$

and $B'' = \{a, b, u, v, \alpha, x, p\}$.

1. If $x = u$, then from $u, v \in A_i \cap B''$ we know that $|A_i \cap (B'' - B \cup B')| = 1$ for $i = 1, 2, 3$.

   In order to prove $(A_1 \cup A_2 \cup A_3) \cap (B'' - B \cup B') = B'' - B \cup B'$, we only need to prove that $A_i \cap (B'' - B \cup B') \neq A_j \cap (B'' - B \cup B')$ if $i \neq j$. Suppose $A_1 \cap (B'' - B \cup B') = A_2 \cap (B'' - B \cup B')$, without loss of generality we assume $A_1 \cap (B'' - B \cup B') = \{\alpha\}$. Then one of A_1 and A_2 meets one of $T_2 - \{a, b, c\}$ and $T_3 - \{a, b, c\}$ at three points, say A_1 meets $T_2 - \{a, b, c\}$ at three points. Then either $x \in A_1$ or $x \in A_2$. So either $|A_1 \cap B''| \geq 4$ or $|A_2 \cap B''| \geq 4$, contradiction.

2. Now suppose $x \neq u$. Then $|A_i \cap (B'' - B \cup B')| = 0$ or 2 for $i = 1, 2, 3$.

   If $|A_1 \cap (B'' - B \cup B')| = 0$, suppose $|A_1 \cap (T_1 - \{a, b, c\})| = 3$, then

$$A_1 \cap (T_1 - \{a, b, c\}) = \{\beta, \gamma, \theta\},$$

so

$$|A_2 \cap (T_1 - \{a, b, c\})| = 1 = |A_3 \cap (T_1 - \{a, b, c\})|.$$

Therefore,

$$|A_2 \cap (T_2 - \{a, b, c\})| = 3 = |A_3 \cap (T_3 - \{a, b, c\})|$$

or

$$|A_2 \cap (T_3 - \{a, b, c\})| = 3 = |A_3 \cap (T_2 - \{a, b, c\})|.$$

Assume $|A_2 \cap (T_2 - \{a, b, c\})| = 3 = |A_3 \cap (T_3 - \{a, b, c\})|$.

   If $A_2 \cap (T_1 - \{a, b, c\}) \not\subset B'' - B \cup B'$ or $A_3 \cap (T_1 - \{a, b, c\}) \not\subset B'' - B \cup B'$, then $A_2 \cap (T_2 - \{a, b, c\})$ or $A_3 \cap (T_3 - \{a, b, c\})$ would contain a point in

$B'' - B \cup B'$. So

$$|A_2 \cap (B'' - B \cup B')| = 2 = |A_3 \cap (B'' - B \cup B')|.$$

If $|A_i \cap (B'' - B \cup B')| = 2$ for $i = 1, 2, 3$, then

$$\bigcup_{i=1}^{3}(A_i - B'') = (A_1 \cup A_2 \cup A_3) - B'' = (T_1 \cup T_2 \cup T_3) - (B'' \cup \{a, b, c\}).$$

$\bigcup_{i=1}^{3}(A_i - B'')$ is a partition of $(T_1 \cup T_2 \cup T_3) - (B'' \cup \{a, b, c\})$. Let T_{ik} be the block in lemma 3.25, which satisfies $|B'' \cap (T_{ik} - \{i\})| = 0$, then

$$T_{ik} - \{i\} \subset (T_1 \cup T_2 \cup T_3) - (B'' - B \cup B').$$

so

$$(T_{ik} - \{i\}) \cap (A_1 \cup A_2 \cup A_3) = T_{ik} - \{i\}$$

and

$$\sum_{j=1}^{3} |(T_{ik} - \{i\}) \cap A_j| = 6.$$

This is impossible since $|(T_{ik} - \{i\}) \cap A_j| = 1$ or 3 for $j = 1, 2, 3$,

$$\sum_{j=1}^{3} |(T_{ik} - \{i\}) \cap A_j| = 3, 5, 7, 9.$$

□

Let B and B' be two blocks in $S(4, 7, 23)$ with $|B \cap B'| = 1$. We know that there are twenty 6-secant blocks to $B \cup B'$. Moreover, we have

Lemma 3.27. *On each point in $S - (B \cup B')$, there are two 6-secant blocks to $B \cup B'$ and these two blocks meet only at this point.*

Proof. We only need to prove the following:

Suppose $x \notin B \cup B'$. If A is a 6-secant block to $B \cup B'$ which contains x, then $\{x\} \cup [B - (A \cap B) \cup (B \cap B')] \cup [B' - (A \cap B') \cup (B \cap B')]$ is a block.

Let A' be the block determined by $\{x\} \cup [B - (A \cap B) \cup (B \cap B')]$. We prove A' contains $B' - [(A \cap B') \cup (B \cap B')]$.

First we prove $|A' \cap B'| = 3$. If $|A' \cap B'| = 1$, then $(A' \cap B') \cap A = \emptyset$. The block determined by x, the point in $A' \cap B'$, a point in $A \cap B'$ and a point in $B' - [(B \cap B') \cup (A \cap B') \cup (A' \cap B')]$ would meet B at two points, a contradiction.

If $|A' \cap B'| = 3$, but $(A' \cap B') \cap A \neq \emptyset$, then $|(A' \cap B') \cap A| = 2$. The block determined by x, the two points in $B' - [(B \cap B') \cup (A \cup A')]$ and a point in $A \cap A' \cap B'$ would also meet B at two points.

So $A' \cap B' = B' - [(A \cap B') \cup (B \cap B')]$. □

3.6.2. **1-blocking sets in $S(4, 7, 23)$.**

Theorem 3.10. *Let C_1 be a 1-blocking set in $S(4, 7, 23)$. Then $7 \leq |C_1| \leq 17$.*

1. *If $|C_1| = 7$, then $C_1 = B$ with $FV(C_1) = (0, 112, 0, 140, 0, 0, 0, 1)$, where B is a block.*
2. *If $|C_1| = 7 + i$, $1 \leq i \leq 3$, then $C_1 = B \cup X$ with frequency vectors $(0, 70, 42, 105, 35, 0, 0, 1)$, $(0, 42, 56, 91, 56, 7, 0, 1)$ and $(0, 24, 54, 85, 70, 18, 1, 1,)$ respectively; where B is a block, $|X| = i$ and $X \cap B = \emptyset$.*
3. *If $|C_1| = 11$, then C_1 is one of the following:*
   (a) *$C_1 = E_0$ with $FV(C_1) = (0, 22, 0, 165, 0, 66, 0, 0)$;*
   (b) *$C_1 = E_1$ with $FV(C_1) = (0, 11, 55, 55, 110, 11, 11, 0)$;*
   (c) *$C_1 = B \cup B'$ with $FV(C_1) = (0, 12, 48, 75, 80, 36, 0, 2)$, where B and B' are blocks with $|B \cap B'| = 3$;*

(d) $C_1 = B \cup B' - \{x, y\}$ with $FV(C_1) = (0, 13, 44, 80, 80, 31, 4, 1)$, where B and B' are blocks with $|B \cap B'| = 1$ and $x, y \in B' - B$.

4. *If* $|C_1| = 12$, *then* C_1 *is one of the following:*

   (a) $C_1 = \mathcal{S} - E_1$ with $FV(C_1) = (0, 11, 11, 110, 55, 55, 11, 0)$;

   (b) $C_1 = B \cup B' \cup \{a\}$ with $FV(C_1) = (0, 6, 34, 70, 85, 50, 6, 2)$, where B and B' are blocks with $|B \cap B'| = 3$ and $a \notin B \cup B'$;

   (c) $C_1 = B \cup B' - \{x\}$ with $FV(C_1) = (0, 6, 35, 65, 95, 40, 11, 1)$, where B and B' are blocks with $|B \cap B'| = 1$ and $x \in B' - B$;

   (d) $C_1 = B \cup B' \cup B'' - \{a, u\}$, $FV(C_1) = (0, 7, 30, 75, 85, 45, 10, 1)$, where B, B' and B'' are blocks with $|B \cap B' \cap B''| = 2$ and $a \in B' \cap B'' - B \cap B' \cap B''$, $u \in B'' - (B \cup B')$.

5. *If* $|C_1| = 13$, *then* C_1 *is one of the following:*

   (a) $C_1 = B \cup B' \cup B'' - \{x, y\}$, $FV(C_1) = (0, 2, 24, 60, 80, 75, 8, 4)$, where B, B' and B'' are blocks with $|B \cap B' \cap B''| = 3$, $x, y \in B'' - (B \cup B')$;

   (b) $C_1 = B \cup B' \cup B'' \cup \{u\} - \{x, y, z\}$, $FV(C_1) = (0, 3, 21, 60, 90, 60, 17, 2)$, where B, B', B'' are blocks, $|B \cap B' \cap B''| = 3$, $x, y, z \in B'' - (B \cup B')$ and $u \notin B \cup B' \cup B''$;

   (c) $C_1 = B \cup B' \cup B'' - \{x\}$, $FV(C_1) = (0, 5, 12, 75, 80, 60, 20, 1)$, where B, B', B'' are blocks, $|B \cap B' \cap B''| = 2$ and $x \in B' \cap B'' - B$.

6. *If* $|C_1| = 14$, *then* C_1 *is one of the following:*

   (a) $C_1 = \mathcal{S} - (B \cup B' - \{a, u\})$, $FV(C_1) = (0, 1, 13, 46, 86, 77, 26, 4)$, where B and B' are blocks with $|B \cap B'| = 3$ and $a \in B \cap B'$, $u \in B \triangle B'$;

   (b) $C_1 = \mathcal{S} - (B \cup B' - \{u, v\})$, $FV(C_1) = (0, 2, 9, 51, 86, 72, 30, 3)$, where B and B' are blocks with $|B \cap B'| = 3$, $u \in B - B'$ and $v \in B' - B$.

7. *If* $|C_1| = 17-n$ $(1 \leq n \leq 3)$, *then* $C_1 = S-(B \cup X-\{a\})$ *with frequency vectors* $(0,1,4,35,80,83,44,6)$, $(0,1,0,20,75,81,66,10)$ *and* $(0,1,0,0,80,60,96,16)$, *respectively, where* B *is a block,* $a \in B$, $|X| = n$ *and* $X \cap B = \emptyset$.

Proof. By lemma 3.19 every blocking set in $S(4,7,23)$ contains at least eleven points, so $|C_1| \geq 7$. By definition there exists at least one block such that C_1 meets this block at only one point, so $|C_1| \leq 23-6 = 17$.

1. If $|C_1| = 7$, let B be a block contained in C_1; then $C_1 = B$.
2. If $|C_1| = 7+i$, $(1 \leq i \leq 3)$, let B be a block contained in C_1; then we have $C_1 = B \cup X$, where $|X| = i$ and $X \cap B = \emptyset$. It is easy to see that when $|C_1| = 8$ or 9, C_1 has no 6-secant block, so $FV(C_1) = (0,70,42,105,35,0,0,1)$ or $(0,42,56,91,56,7,0,1)$; when $|C_1| = 10$, C_1 has only one 6-secant block and so $FV(C_1) = (0,24,54,85,70,18,1,1)$.
3. Let $|C_1| = 11$. If C_1 contains no block, then C_1 is a blocking set, so $C_1 = E_0$ or E_1. If C_1 contains a block B, let B' be the block determined by the four points of $C_1 - B$, then either $|B \cap B'| = 3$ or $|B \cap B'| = 1$. If $|B \cap B'| = 3$, then $C_1 = B \cup B'$ with $FV(C_1) = (0,12,48,75,80,36,0,2)$; if $|B \cap B'| = 1$, then $C_1 = B \cup B' - \{x,y\}$, $FV(C_1) = (0,13,44,80,80,31,4,1)$, where $x,y \in B'-B$.
4. Let $|C_1| = 12$. If C_1 contains no block; then C_1 is a blocking set, so we have $C_1 = S - E_1$, $FV(C_1) = (0,11,11,110,55,55,11,0)$.

   If C_1 contains two blocks B, B', then $|B \cap B'| = 3$, $C_1 = B \cup B' \cup \{a\}$, where $a \notin B \cup B'$. By lemma 3.25 we know that C_1 has six 1-secant blocks. Since $B \cup B'$ has no 6-secant block, C_1 contains only two blocks. So we have $FV(C_1) = (0,6,34,70,85,50,6,2)$.

   Now suppose C_1 contains only one block B.

If there is a block B' which is 6-secant to C_1 and meets B at only one point, then $C_1 = B \cup B' - \{x\}$, where $x \in B' - B$. In this case C_1 has six 1-secant blocks. So $FV(C_1) = (0, 6, 35, 65, 95, 40, 11, 1)$.

If there is no block which is 6-secant to C_1 and meets B at one point, then let B' be a block such that B' is 6-secant to C_1 and $|B' \cap B| = 3$, and let $x, y \in C_1 - (B \cup B')$, $a \in B' - C_1$. Let B'' be the block on $\{x, y, a\}$ such that $|B'' \cap B| = 3$. We claim that $B'' \cap B \not\subset B - B'$. Otherwise, let $B - B' = \{u, v, w, z\}$ and $B'' \cap B = \{u, v, w\}$; then consider the block A on $\{x, y, z\}$ which meets B' at three points. If $A \cap B' \not\subset B' - B$, then there would exist two blocks on $\{x, y, a\}$ or $B'' - (B \cup B')$ which meet B at three points, this is impossible. So $A \cap B' \subset B' - B$. Since there are five blocks on $\{x, y, a\}$, we have $a \notin A$. So $|A \cap B| = 1$, $|A \cap C_1| = 6$, a contradiction. If $|B'' \cap (B \cap B')| = 1$, then $|B'' \cap (B - B')| = 2 = |B'' \cap (B' - B)|$. We consider the block X determined by x, y and the two points in $B' - [B \cup (B'' \cap B')]$. X can not contain $B'' \cap (B' - B) - \{a\}$. If $a \in X$, then X would contain a point in $B - [B' \cup (B'' \cap B)]$. The block determined by x, y, a and a point in $B \cap B' - B''$, would contain $B \cap B' - B''$ and the remaining point in $B - [B' \cup (B'' \cap B)]$. So either there are only four blocks on $\{x, y, a\}$ or the fifth block on $\{x, y, a\}$ would not meet B, contradiction. Therefore, we have $|B'' \cap (B \cap B')| = 2$, and $C_1 = B \cup B' \cup B'' - \{a, u\}$, where $u \in B'' - (B \cup B')$. By lemmas 3.23, 3.24, 3.25 and 3.26 we know that for a point p in $B \cap B'$, there is only one block which meets $B \cup B'$ at p, but does not meet $B'' - (B \cup B')$; for a point q in $B - B'$, there is also only one block which meets $B \cup B'$ at q and a, but does not meet $B'' - (B \cup B' \cup \{u\})$. So C_1 has seven 1-secant blocks and $FV(C_1) = (0, 7, 30, 75, 85, 45, 10, 1)$.

5. Let $|C_1| = 13$.

If C_1 contains two blocks B and B', then $|B \cap B'| = 3$. Let B'' be a block which contains one point in $C_1 - (B \cup B')$ and meets $B \cup B'$ at $B \cap B'$. If B'' contains the other point in $C_1 - (B \cup B')$, then $C_1 = B \cup B' \cup B'' - \{x, y\}$, where $x, y \in B'' - (B \cup B')$. By lemma 3.24, we know that C_1 has two 1-secant blocks, these are two of the blocks which meet $B \cup B'$ only at one point o in $B \cap B'$. The block determined by o, the two points in $B'' - (B \cup B' \cup \{x, y\})$ and a point in $B - B'$ can not contain any point in $S - (B \cup B' \cup B'' - \{x, y\})$. So it is contained in C_1. We have two of this kind of block. Any block contained in C_1 other than B and B' must be one of the two blocks. So C_1 contains four blocks, and $FV(C_1) = (0, 2, 24, 60, 80, 75, 8, 4)$.

If B'' does not contain the other point in $C_1 - (B \cup B')$, then we have $C_1 = B \cup B' \cup B'' \cup \{u\} - \{x, y, y, z\}$, where $x, y, z \in B'' - (B \cup B')$, and $u \notin B \cup B' \cup B''$. By lemma 3.24 we can see that C_1 has three 1-secant blocks and contains only two blocks. So $FV(C_1) = (0, 3, 21, 60, 90, 60, 17, 2)$.

Now we assume C_1 contains only one block B. Let B' be a block which contains three points in $C_1 - B$ and meets B at three points. Let B'' be the block on $C_1 - (B \cup B')$ and meets B at three points. If $B'' \cap B \subset B - B'$, then since C_1 contains only one block B, we have $a \in B''$. Consider the four blocks which meet $B \cup B'$ at a fixed point in $B \cap B'$. By lemma 3.23, one of them contains $C_1 - (B \cup B')$. So there exist three blocks on $C_1 - (B \cup B')$ which meet $B \cup B'$ at one point in $B \cap B'$. Therefore, the fifth block on $C_1 - (B \cup B')$ would contain $B - (B' \cup B'')$ and $B' - (B \cup \{a\})$, so it is contained in C_1, a contradiction. Let $B'' \cap B \not\subset B - B'$. If $B'' \cap (B' - B) = \emptyset$, then $|B'' \cap (B \cap B')| = 1$, so one of the blocks which meet $B \cup B'$ only at

$B \cap B'$ would contain two of the three points in $C_1 - (B \cup B')$. Using the same argument developed in the first paragraph, we obtain that C_1 would contain two blocks, a contradiction. So $B'' \cap (B' - B) \neq \emptyset$, hence $B'' \cap (B' - B) = \{a\}$, and $C_1 = B \cup B' \cup B'' - \{a\}$. By lemmas 3.25 and 3.26 we know that C_1 has five 1-secant blocks. Therefore, $FV(C_1) = (0, 5, 12, 75, 80, 60, 20, 1)$.

6. Let $|C_1| = 14$. Let B be a 1-secant block to C_1; then $|S - (C_1 \cup B)| = 3$. Let B' be the block on $S - (C_1 - B)$ which meets B at three points. If $B \cap C_1 \subset B'$, then $C_1 = S - (B \cup B' - \{a, u\})$, where $a \in B \cap B'$, $u \in B' - B$. By lemma 3.23 we know that there exist four blocks which meet $B \cup B'$ at a. So C_1 contains four blocks. It is easy to see that C_1 has only one 1-secant block to B. Therefore,

$$FV(C_1) = (0, 1, 13, 46, 86, 77, 26, 4).$$

If $B \cap C_1 \not\subset B'$, then $C_1 = S - (B \cup B' - \{u, v\})$, where $u \in B - B'$ and $v \in B' - B$. It is easy to prove that C_1 contains three blocks, and has two 1-secant blocks. So

$$FV(C_1) = (0, 2, 9, 51, 86, 72, 30, 2).$$

The cases of $|C_1| = 15$, 16 and 17 can be proved similarly.

□

3.6.3. 2-blocking sets in $S(4, 7, 23)$.

Theorem 3.11. *Let C_2 be a 2-blocking set in $S(4, 7, 23)$. Then $12 \leq |C_2| \leq 18$, and*

1. *If* $|C_2| = 12$, *then* $C_2 = B \triangle B'$, $FV(C_2) = (0, 0, 66, 0, 165, 0, 22, 0)$, *where* B *and* B' *are blocks with* $|B \cap B'| = 1$.

2. *If* $|C_2| = 13$, *then* $C_2 = B \cup B'$, $FV(C_2) = (0, 0, 36, 30, 120, 45, 20, 2)$, *where* B *and* B' *are blocks with* $|B \cap B'| = 1$.

3. *If* $|C_2| = 14$, *then* C_2 *is one of the following:*

   (a) $C_2 = B \cup B' \cup \{a\}$, $FV(C_2) = (0, 0, 18, 36, 96, 72, 27, 4)$, *where* B *and* B' *are blocks with* $|B \cap B'| = 1$ *and* $a \notin B \cup B'$;

   (b) $C_2 = B \cup B' \cup B'' - \{x, y, z\}$ *and* $FV(C_2) = (0, 0, 14, 56, 56, 112, 7, 8)$, *where* B, B' *and* B'' *are blocks with* $B \cap B' = B \cap B'' = B \cap B' \cap B''$, $B' \cap B'' - B = \{x, y\}$ *and* $z \in B'' - B'$.

4. *If* $|C_2| = 15$, *then* C_2 *is one of the following:*

   (a) $C_2 = S - [(B \cup B') - \{x, y, u\}]$, $FV(C_2) = (0, 0, 7, 35, 70, 98, 35, 8)$, *where* B *and* B' *are blocks with* $|B \cap B'| = 3$, $x, y \in B \cap B'$ *and* $u \in B \triangle B'$;

   (b) $C_2 = S - [(B \cup B') - \{x, u, v\}]$, $FV(C_2) = (0, 0, 8, 30, 80, 88, 40, 7)$, *where* B *and* B' *are blocks with* $|B \cap B'| = 3$, $x \in B \cap B'$, $u \in B - B'$ *and* $v \in B' - B$.

5. *If* $|C_2| = 16$, *then* $C_2 = S - \{a, b, c, d, e, x, y\}$, $FV(C_2) = (0, 0, 3, 20, 65, 96, 57, 12)$, *where* $a, b, c, d, e \in B$ *and* $x, y \notin B$.

6. *If* $|C_2| = 17$, *then* $C_2 = S - \{a, b, c, d, e, x\}$, $FV(C_2) = (0, 0, 1, 10, 50, 95, 77, 20)$, *where* $a, b, c, d, e \in B$ *and* $x \notin B$.

7. *If* $|C_2| = 18$, *then* $C_2 = S - \{a, b, c, d, e\}$, $FV(C_2) = (0, 0, 1, 0, 40, 80, 100, 32)$, *where* $a, b, c, d, e \in B$.

Proof. Since the blocking sets in $S(4, 7, 23)$ all have size greater than or equal to eleven, and the blocking sets of size eleven are all 1-blocking sets, by lemma 3.20, result 3.9 and result 3.10, we know $|C_2| \geq 12$. By definition, C_2 meets a block at two points, so $|C_2| \leq 23 - 5 = 18$.

1. Since $|C_2| = 12$, C_2 contains no block, otherwise C_2 can not be a 2-blocking set by lemma 3.20, result 3.10 and lemma 3.21. So C_2 is a blocking set; therefore $C_2 = B \triangle B'$, $FV(C_2) = (0, 0, 66, 0, 165, 0, 22, 0)$, where B and B' are blocks with $|B \cap B'| = 1$.

2. If $|C_2| = 13$, then since there is no blocking set of size thirteen in $S(4, 7, 23)$, C_2 contains a block B. By lemma 3.20 there exists a block B' such that $|B' \cap (C_2 - B)| = 4, 5$ or 6 and $|B \cap B'| = 1$. If $|B' \cap (C_2 - B)| = 4$ or 5, then C_2 would not be a 2-blocking set, so $|B' \cap (C_2 - B)| = 6$, and $C_2 = B \cup B'$ with $|B \cap B'| = 1$ and $FV(C_2) = (0, 0, 36, 30, 120, 45, 20, 2)$.

3. When $|C_2| = 14$, let B be a block, $B \subseteq C_2$.

   If there exists a block B' which contains six points in $C_2 - B$, then $C_2 = B \cup B' \cup \{a\}$, where $a \notin B \cup B'$ and $|B \cap B'| = 1$. By lemma 3.27, C_2 contains four blocks, so $FV(C_2) = (0, 0, 18, 36, 96, 72, 27, 4)$.

   Suppose no six points in $C_2 - B$ are contained in any block. Since C_2 is a 2-blocking set, no block contains only five points in $C_2 - B$. By lemma 3.20, there exists a block B' such that B' contains only four points in $C_2 - B$ and $|B' \cap B| = 1$. Let $C_2 - (B \cup B') = \{a, b, c\}$, $B' - C_2 = \{x, y\}$. We prove that there exists a block B'' such that

$$a, b, c \in B'', \; B \cap B' \subset B'', \; B'' \cap B' - (B \cap B') = \{x, y\}.$$

   Consider the five blocks on $\{a, b, c\}$. One of them meets B' at three points, let B'' be this block. We prove B'' has the above mentioned properties.

Let $B \cap B' = \{0\}$, $B = \{0,1,2,3,4,5,6\}$. First we prove $0 \in B' \cap B''$. If $0 \notin B' \cap B''$, then $\{x,y\} \subset B'' \cap B'$. Let the other point in $B'' \cap B'$ be u, and let $B'' \cap B = \{6\}$; then the block determined by $\{a,b,u,v\}$, where $v \in B' - (B'' \cup B)$, would contain five points in $C_2 - B$.

So we have proved that $0 \in B'' \cap B'$.

We claim $B'' \cap B' - \{0\} = \{x,y\}$. Otherwise we would have $x \in B'' \cap B'$ and $y \notin B'' \cap B'$ or $x \notin B'' \cap B'$ and $y \in B'' \cap B'$. In each case we would obtain a block which contains five points in $C_2 - B$. Thus $C_2 = B \cup B' \cup B'' - \{x,y,z\}$, where $x,y \in B' \cap B'' - B$ and $z \in B'' - (B \cup B')$.

4. When $|C_2| = 15$, let B be a block with $|B \cap C_2| = 2$, and let $\mathcal{S} - (C_2 \cup B) = \{p,q,r\}$. We consider the block B' on $\{p,q,r\}$ which meets B at three points. It is easy to see that $B' \cap (B \cap C_2) \neq \emptyset$. If $|B' \cap (B \cap C_2)| = 2$, then $C_2 = \mathcal{S} - [(B \cup B') - \{x,y,u\}]$, where $x,y \in B \cap B'$ and $u \in B' - B$. By lemma 3.23 C_2 contains eight blocks. So $FV(C_2) = (0,0,7,35,70,98,35,8)$. If $|B' \cap (B \cap C_2)| = 1$, then $C_2 = \mathcal{S} - [(B \cup B') - \{x,u,v\}]$, where $x \in B \cap B'$, $u \in B - B'$ and $v \in B' - B$. It can be proved that C_2 contains seven blocks. So $FV(C_2) = (0,0,8,30,80,88,40,7)$.

5. If $|C_2| = 16$, then since C_2 meets a block B at two points, we have $C_2 = \mathcal{S} - \{a,b,c,d,e,x,y\}$, where $a,b,c,d,e \in B$ and $x,y \notin B$. By lemma 3.23 there are eight blocks which meet $B \cup B'$ at one point in $B \cap C_2$. It can be proved that on $(B' - B) \cap C_2$ and a point in $B \cap C_2$ there are two blocks which meet $B \cup B'$ only at the three points. So C_2 contains twelve blocks, and $FV(C_2) = (0,0,3,20,65,96,57,12)$.

The set $\mathcal{S} - \{a,b,c,d,e,x,y\}$, where $a,b,c,d,e \in B$, and $x,y \notin B$, is indeed a 2-blocking set, since any block $B'' \neq B$ meets B in at most three points;

in the extreme case, if $x, y \in B''$, B'' still has at least two points in common with $\mathcal{S} - \{a, b, c, d, e, x, y\}$.

6. Similarly we can prove that if $|C_2| = 17$, then $C_2 = \mathcal{S} - \{a, b, c, d, e, x\}$, where a, b, c, d, e are in a block B and $x \notin B$. $FV(C_2) = (0, 0, 1, 10, 50, 95, 77, 20)$.
7. If $|C_2| = 18$, then $C_2 = \mathcal{S} - \{a, b, c, d, e\}$, where a, b, c, d, e are in a block, and $FV(C_2) = (0, 0, 1, 0, 40, 80, 100, 32)$.

□

3.6.4. t-blocking sets, $t \geq 3$, in $S(4, 7, 23)$.

Theorem 3.12. *Let C_3 be a 3-blocking set in $S(4, 7, 23)$; then $15 \leq |C_3| \leq 19$, and*

1. *if $|C_3| = 15$, then $C_3 = \mathcal{S} - (B \triangle B')$, $FV(C_3) = (0, 0, 0, 70, 0, 168, 0, 15)$, where B, B' are blocks with $|B \cap B'| = 3$;*
2. *if $|C_3| = 16$, then $C_3 = \mathcal{S} - (B \triangle B' - \{a\})$, $FV(C_3) = (0, 0, 0, 35, 35, 126, 42, 15)$, where B and B' are blocks with $|B \cap B'| = 3$ and $a \in B' - B$;*
3. *if $|C_3| = 17$, then $C_3 = \mathcal{S} - \{a, b, c, d, e, f\}$, $FV(C_3) = (0, 0, 0, 15, 40, 105, 72, 21)$, where no five points in $\{a, b, c, d, e, f\}$ are contained in any block;*
4. *if $|C_3| = 18$, then $C_3 = \mathcal{S} - \{a, b, c, d, e\}$, $FV(C_3) = (0, 0, 0, 5, 30, 90, 95, 33)$, where $\{a, b, c, d, e\}$ is not contained in any block;*
5. *if $|C_3| = 19$, then $C_3 = \mathcal{S} - \{a, b, c, d\}$ and $FV(C_3) = (0, 0, 0, 1, 16, 72, 112, 52)$.*

Proof. First we prove that $X = \mathcal{S} - [(B \cup B') - \{o, x, y, a, b\}]$ is not a 3-blocking set in $S(4, 7, 23)$, where B and B' are blocks with $B \cap B' = \{o\}$, $a, b \in B - \{o\}$ and $x, y \in B' - \{o\}$.

Let $B - \{o, a, b\} = \{c, d, e, f\}$, $B' - \{o, x, y\} = \{u, v, w, z\}$. We consider the blocks on $\{u, v, w\}$ and $\{u, v, z\}$, respectively, which meet $B - \{o\}$ at three points. One of them contains at most one point in $\{a, b\}$, so it meets X at at most 2 points.

By lemma 3.20 we know that $|C_3| \geq 15$. Obviously $|C_3| \leq 19$.

If $|C_3| = 15$, let B be a block with $B \cap C_3 = \{x, y, z\}$, $\mathcal{S} - (C_3 \cup B) = \{a, b, c, d\}$. Let B' be the block determined by $\{a, b, c, d\}$; then we have $B \cap B' = \{x, y, z\}$, $C_3 = \mathcal{S} - (B \triangle B')$ and $FV(C_3) = (0, 0, 0, 70, 0, 168, 0, 15)$.

If $|C_3| = 16$, let B be a block with $B \cap C_3 = \{x, y, z\}$, let $\mathcal{S} - (C_3 \cup B) = \{a, b, c\}$ and B' the block on $\{a, b, c\}$ and meets B at three points; then $B \cap B'$ can not contain two points in $B - \{x, y, z\}$. Furthermore, we can prove that $B' \cap (B - \{x, y, z\}) = \emptyset$. So $B \cap B' = \{x, y, z\}$ and $C_3 = \mathcal{S} - (B \triangle B' - \{a\})$, where $a \in B' - B$, and $FV(C_3) = (0, 0, 0, 35, 35, 126, 42, 15)$. 3, 4 and 5 can be proved similarly. □

Theorem 3.13. *Let C_4 be a 4-blocking set in $S(4, 7, 23)$; then $|C_4| = 20$ and $C_4 = \mathcal{S} - \{a, b, c\}$ and $FV(C_4) = (0, 0, 0, 0, 5, 48, 120, 80)$.*

Theorem 3.14. *Let C_5 be a 5-blocking set in $S(4, 7, 23)$; then $|C_5| = 21$ and $C_5 = \mathcal{S} - \{a, b\}$ and $FV(C_5) = (0, 0, 0, 0, 0, 21, 112, 120)$.*

Theorem 3.15. *Let C_6 be a 6-blocking set in $S(4, 7, 23)$; then $|C_6| = 22$ and $C_6 = \mathcal{S} - \{a\}$ and $FV(C_6) = (0, 0, 0, 0, 0, 0, 77, 176)$.*

Theorem 3.16. *The 7-blocking set in $S(4, 7, 23)$ is $\mathcal{S}$.*

3.7. t-blocking sets in $S(5, 8, 24)$.

3.7.1. A general result on $S(5, 8, 24)$.

Now we characterize the t-blocking sets in $S(5, 8, 24)$. We use the same terminology and notations as in section 2.3.

First we prove the following

Lemma 3.28. *If C_t contains a block, then $|C_t| > 12$.*

Proof. Let B be a block, $B \subset C_t$, and let $x, y, z, w \notin B$. Then there exists a block B' such that $x, y, z, w \in B'$ and $B \cap B' = \emptyset$. Let B'' be the block such that $B'' \cap (B \cup B') = \emptyset$. If $|C_t| \leq 12$, then $B'' \cap C_t = \emptyset$. ❑

3.7.2. **1-blocking sets in** $S(5, 8, 24)$.

Theorem 3.17. *For the size of a 1-blocking set C_1 we have $11 \leq |C_1| \leq 17$.*

1. *If $|C_1| = 11$, then $C_1 = M_0$ and $FV(M_0) = (0, 22, 110, 165, 330, 66, 66, 0, 0)$.*
2. *If $|C_1| = 12$, then $C_1 = I$ and $FV(I) = (0, 12, 60, 180, 255, 180, 60, 12, 0)$; or*

   $C_1 = R$, $FV(R) = (0, 11, 66, 165, 275, 165, 66, 11, 0)$.
3. *If $|C_1| = 13$, then $C_1 = B \cup B' - \{a\}$, where B and B' are blocks,*

   $|B \cap B'| = 2$ and $FV(C_1) = (0, 5, 37, 135, 245, 220, 95, 21, 1)$ $a \in B \triangle B'$.
4. *If $|C_1| = 17 - r$, $(0 \leq r \leq 3)$, then*

   $C_1 = B \cup B' \cup B'' - \{a, b, c, d, e, f, x_0, x_1, \cdots, x_r\}$,

   where B, B' and B'' are blocks, and

   $B \cap B' = B \cap B'' = B' \cap B'' = \emptyset$, $\{a, b, c, d, e, f, x_0\} \subset B'$, $\{x_1, \cdots, x_r\} \subset B''$.

   The frequency vectors of C_1 are

   $$(0, 2, 19, 96, 215, 250, 138, 36, 3),$$

   $$(0, 1, 7, 63, 175, 259, 189, 58, 7),$$

   $$(0, 1, 0, 35, 140, 231, 252, 85, 15)$$

   and

   $$(0, 1, 0, 0, 140, 140, 336, 112, 30),$$

   respectively.

Proof. If C_1 contains a block, then by lemma 3.28, $|C_1| > 12$; if C_1 does not contain a block, then C_1 is a blocking set, so $|C_1| \geq 11$. Since C_1 is a 1-blocking set, there exists a block B such that $|C_1 \cap B| = 1$; therefore $|C_1| \leq 24 - 5 = 17$.

1. If $|C_1| = 11$, then by lemma 3.28 C_1 is a blocking set. So

   $C_1 = M_0$. It is no difficult to see that there is no 7-secant block to M_0.So $FV(M_0) = (0, 22, 110, 165, 330, 66, 66, 0, 0)$.

2. If $|C_1| = 12$, then C_1 is a blocking set. But in $S(5, 8, 24)$ there are three blocking sets of size twelve: I, R and M, of which M is a 2-blocking set. I and R are 1-blocking sets, so $C_1 = I$ or R.

   Let $R = B \cup B' - \{z, a\}$, where $B \cap B' = \{z, w\}$, $a \in B \triangle B'$. Consider the contraction of $S(5, 8, 24)$ at z. By lemma 3.27 we know that on each point in $S - (B \cup B')$, there exists a block in $S(5, 8, 24)$ which meets $B \triangle B' - \{a\}$ at six points, and meets $B \cap B'$ at z. We have ten of this kind of blocks. By lemma 2.2 we know that $B \cup B'$ contains only two blocks, B and B'. So R has eleven 7-secant blocks, therefore, $FV(R) = (0, 11, 66, 165, 275, 165, 66, 11, 0)$. We already know that $FV(R) = (0, 11, 66, 165, 275, 165, 66, 11, 0)$.

3. If $|C_1| = 13$, then because $M_0 \subset M$, M contains no 7-secant block, so $S - M_0$ is a 2-blocking set. Therefore C_1 contains a block B. Let B' be the block that contains the 5 points of $C_1 - B$. Since C_1 is a 1-blocking set and $B' \cap B \neq \emptyset$, then $|B \cap B'| = 2$. Let $a \in B' - C_1$; then $C_1 = B \cup B' - \{a\}$.

   Now we prove that $B \cup B' - \{a\}$ is a 1-blocking set.

   Since $M \subset B \cup B'$ and the type of M is $(2, 4, 6)$, every block meets the set $B \cup B' - \{a\}$. Let $B' - B = \{a, b, c, d, e, f\}$, and let B'' be a block that contains c, d, e, f and is disjoint from B; then $S - (B \cup B'')$ is a block, and this block meets $B \cup B'$ only at $\{a, b\}$, so is 1-secant to $B \cup B' - \{a\}$. So $FV(C_1) = (0, 5, 37, 135, 245, 220, 95, 21, 1)$.

4. If $|C_1| = 17 - r$, $0 \leq r \leq 3$, then by lemma 3.28, there exists a block B such that $B \subseteq C_1$. Since C_1 is a 1-blocking set, there is a block B' such that $|B' \cap C_1| = 1$. Therefore, $B \cap B' = \emptyset$ and $B'' = \mathcal{S} - B \cup B'$ is a block. Let $B' - C_1 = \{a, b, c, d, e, f, x_0\}$, $B'' - C_1 = \{x_1, \cdots, x_r\}$ (If $r = 0$, then $B'' - C_1 = \emptyset$); then $C_1 = B \cup B' \cup B'' - \{a, b, c, d, e, f, x_0, x_1, \cdots, x_r\}$, and $B \cap B' = B \cap B'' = B' \cap B'' = \emptyset$.

   When $|C_1| = 14$, $r = 3$ and $C_1 = B \cup B' \cup B'' - \{a, b, c, d, e, f, x_0, x_1, x_2, x_3\}$. It can be proved that on $\{x_1, x_2, x_3\}$ there are three blocks which are disjoint from B. So besides B' there is only one 1-secant block to C_1, and there are only two blocks which are contained in C_1. So $FV(C_1) = (0, 2, 19, 96, 215, 250, 138, 36, 3)$. When $|C_1| = 15$, it can be proved that besides B there are six blocks which are contained in C_1. It is easy to see that B' is the only 1-secant block to C_1. So in this case $FV(C_1) = (0, 1, 7, 63, 175, 259, 189, 58, 7)$. While $|C_1| = 16$ and 17, there is only one 1-secant block to C_1, and there is no 2-secant block to C_1. So the frequency vectors of C_1 are $(0, 1, 0, 35, 140, 231, 252, 85, 15)$ and $(0, 1, 0, 0, 140, 140, 336, 112, 30)$, respectively.

□

3.7.3. 2-blocking sets in $S(5, 8, 24)$.

Theorem 3.18. *For the size of the 2-blocking set C_2 we have $12 \leq |C_2| \leq 18$.*

1. *If $|C_2| = 12$, then $C_2 = M$. $FV(M) = (0, 0, 132, 0, 495, 0, 132, 0, 0)$.*
2. *If $|C_2| = 13$, then $C_2 = \mathcal{S} - M_0$, $FV(C_2) = (0, 0, 66, 66, 330, 165, 110, 22, 0)$.*

3. *If* $|C_2| = 14$. *then* $C_2 = B \cup B'$. $FV(C_2) = (0, 0, 30, 72, 240, 240, 135, 40, 2)$. *where* B *and* B' *are blocks*. $|B \cap B'| = 2$.

4. *If* $|C_2| = 15$. *then* $C_2 = B \cup B' \cup \{a\}$. $FV(C_2) = (0, 0, 12, 54, 180, 264, 180, 63, 6)$. *where* B *and* B' *are blocks*. $|B \cap B'| = 2$. $a \notin B \cup B'$.

5. *If* $|C_2| = 18 - r$. $(0 \leq r \leq 2)$. *then* $C_2 = \mathcal{S} - [(B \cup X) - \{a, b\}]$. *where* B *is a block*. $a, b \in B$ *and* $|X| = r$ *with* $X \cap B = \emptyset$. *The frequency vectors of* C_2 *are* $(0, 0, 4, 32, 130, 256, 228, 96, 13)$, $(0, 0, 1, 15, 85, 225, 267, 141, 25)$ *and* $(0, 0, 1, 0, 60, 160, 300, 192, 46)$, *respectively*.

Proof. By the proof of lemma 3.28 we know that if C_2 contains a block, then $|C_2| > 13$. By theorem 3.17, M_0 is a 1-blocking set. Consequently $|C_2| \geq 12$. Since C_2 is a 2-blocking set, there exists a block B' such that $|B' \cap C_2| = 2$, therefore $|C_2| \leq 24 - 6 = 18$.

1. If $|C_2| = 12$, then $C_2 = M$ and $FV(M) = (0, 0, 132, 0, 495, 0, 132, 0, 0)$.
2. If $|C_2| = 13$, then $C_2 = \mathcal{S} - M_0$. $FV(C_2) = (0, 0, 66, 66, 330, 165, 110, 22, 0)$.
3. If $|C_2| = 14$, then since there is no blocking set of size 14, C_2 must contain at least one block. Let B be one of them. Assume $B = \{b_1, b_2, b_3, b_4, b_5, b_6, b_7, b_8\}$, and $C_2 - B = \{a_1, a_2, a_3, a_4, a_5, a_6\}$; let B_i be the unique block determined by $(C_2 - B) - \{a_i\}$, $i = 1, \cdots, 6$. We claim that $B_1 = \cdots = B_6$, as otherwise we would have six different blocks: $B_1, \cdots, B_6$. Since C_2 is a 2-blocking set, $|B \cap B_i| = 2$. But $B_i \neq B_j$ $(i \neq j)$ implies that $(B \cap B_i) \cap (B \cap B_j) = \emptyset$, and therefore B contains at least 12 points. This contradicts the fact $|B| = 8$. Let $B' = B_1 = \cdots = B_6$; then $C_2 = B \cup B'$. Since $B \triangle B'$ is of type $(2, 4, 6)$, C_2 contains only two blocks. So $FV(C_2) = (0, 0, 30, 72, 240, 240, 135, 40, 2)$.

4. If $|C_2| = 15$, let B be a block such that $B \subset C_2$. We claim that there exists at least one block B' such that B' contains six points in $C_2 - B$. Otherwise, let $C_2 - B = \{a_1, a_2, a_3, a_4, a_5, a, b\}$. Consider the six blocks determined by the six 5-subsets of $\{a_1, a_2, a_3, a_4, a_5, a\}$. None of these blocks contains b, while each of these blocks contains only five points in $\{a_1, a_2, a_3, a_4, a_5, a\}$. If at least two of these blocks do not meet B, then each of them would contain three points in $S - C_2$; the other four blocks, each containing at least one point in $S - C_2$, would contain four points in $S - C_2$; the six blocks would contain ten points in $S - C_2$. This is impossible, because $S - C_2$ has only nine points. So among the six blocks, there exists at most one block which does not meet B. Any block which meets B meets B at two points, so five blocks would meet B at ten points, this again is a contradiction. Since C_2 is a 2-blocking set, we have $|B' \cap B| = 2$. So $C_2 = B \cup B' \cup \{a\}$, where $a \notin B \cup B'$.

   $B \cup B' \cup \{a\}$ indeed is a 2-blocking set. In fact, let B'' be a block which contains a and three points in $B' - B$, and is disjoint from B; then $S - (B \cup B'')$ is a block which is 2-secant to $B \cup B' \cup \{a\}$.

5. Let B be a block that meets C_2 at two points, and $X = S - (C_2 \cup B)$; then $|X| = r$ and $C_2 = S - [(B \cup X) - \{a, b\}]$, where $a, b \in B$.

□

3.7.4. ***t*-blocking sets, $t \geq 3$, in $S(5, 8, 24)$.**

Theorem 3.19. *Let C_3 be a 3-blocking set in $S(5, 8, 24)$; then $|C_3| = 18$ or 19.*

1. *If $|C_3| = 18$, then $C_3 = S - \{a, b, c, d, e, f\}$, where $\{a, b, c, d, e, f\}$ is not contained in any block, and $FV(C_3) = (0, 0, 0, 6, 45, 180, 285, 198, 45)$.*

2. *If* $|C_3| = 19$. *then* $C_3 = \mathcal{S} - \{a, b, c, d, e\}$ *and*

$FV(C_3) = (0, 0, 0, 1, 20, 120, 280, 260, 78)$.

Proof. Since C_3 is a 3-blocking set, it meets at least one block at only three points; therefore $|C_3| \leq 24 - 5 = 19$.

If $|C_3| \leq 17$, let $\{a_1, a_2, a_3, a_4, a_5, x, y\} \subseteq \mathcal{S} - C_3$, and let B be the block determined by $\{a_1, a_2, a_3, a_4, a_5\}$. Since C_3 is a 3-blocking set, B contains three points of C_3. Let a_6, a_7, a_8 be the three points. Let B_1, B_2 and B_3 be the blocks determined by $\{x, y, a_1, a_2, a_3\}$, $\{x, y, a_1, a_2, a_4\}$ and $\{x, y, a_1, a_2, a_5\}$, respectively. Since C_3 is a 3-blocking set and B_i has at least 3 points in common with B, $(i = 1, 2, 3)$, so B_i contains one of a_6, a_7, a_8. Assume $a_6 \in B_1$, $a_7 \in B_2$ and $a_8 \in B_3$. The block B_4 determined by $\{x, y, a_3, a_4, a_5\}$ has at least three points a_3, a_4, a_5 in common with B, so it must contain one and only one of a_1, a_2, a_6, a_7, a_8. If $a_6 \in B_4$, let A be the block determined by $\{x, y, a_2, a_3, a_4\}$; then $a_1, a_6, a_7, a_5, a_8 \notin A$. So $|A \cap B'| = 3$, a contradiction. Therefore, $a_6 \notin B_4$. Similarly we can prove that $a_7, a_8 \notin B_4$. So B contains either a_1 or a_2, therefore B_4 contains at most two points of C_3, this contradicts C_3 is a 3-blocking set. So $|C_3| > 17$.

1. If $|C_3| = 18$, then $|\mathcal{S} - C_3| = 6$. Let $\mathcal{S} - C_3 = \{a, b, c, d, e, f\}$; then $\{a, b, c, d, e, f\}$ can not be contained in any block.

2. If $|C_3| = 19$, then $C_3 = \mathcal{S} - \{a, b, c, d, e\}$. ☐

Using the same method as above, we can prove

Theorem 3.20. *Let* C_4 *be a 4-blocking set; then* $|C_4| = 20$, *and* $C_4 = \mathcal{S} - \{a, b, c, d\}$ *and* $FV(C_4) = (0, 0, 0, 5, 64, 240, 320, 130)$.

Theorem 3.21. *Let C_5 be a 5-blocking set; then $|C_5| = 21$, and $C_5 = \mathcal{S} - \{a, b, c\}$, $FV(C_5) = (0, 0, 0, 0, 0, 21, 168, 360, 210)$.*

Theorem 3.22. *Let C_6 be a 6-blocking set; then $|C_6| = 22$, and $C_6 = \mathcal{S} - \{a, b\}$ and $FV(C_6) = (0, 0, 0, 0, 0, 0, 77, 352, 330)$.*

Theorem 3.23. *Let C_7 be a 7-blocking set; then $|C_7| = 23$, and $C_7 = \mathcal{S} - \{a\}$ and $FV(C_7) = (0, 0, 0, 0, 0, 0, 0, 253, 506)$.*

4. SEMIOVALS IN THE WITT DESIGNS

4.1. The definitions.

Definition 4.1. A block B of a t-design $\mathcal{D}$ is called a *tangent* to a set X of points of $\mathcal{D}$ if B contains only one point in X.

If $B \cap X = \{x\}$, we also say that B is a tangent on x to X.

Definition 4.2. A *semioval* O is a set of points such that on every point of O there exists only one tangent to O.

Semiovals have been studied by many authors (see [15, 30, 54]). But much of the previous work was focused on the semiovals of projective planes. In this section we study the semiovals in the Witt designs and characterize all semiovals in the Witt designs up to the frequency vectors.

4.2. Semiovals in $S(4,5,11)$ and $S(5,6,12)$. In $S(4,5,11)$ we have

$$r_0 = 66, r_1 = 30, r_2 = 12, r_3 = 4, r_4 = 1.$$

Lemma 4.1. *The type of a block in $S(4,5,11)$ is $(1,2,3,5)$ with*

$$t_1 = 15, t_2 = 20, t_3 = 30, t_5 = 1.$$

Lemma 4.2. *Let B, B' be two blocks in $S(4,5,11)$ with $|B \cap B'| = 1$. Then the type of $B \cup B'$ is $(3,4,5)$ with $t_3 = 12$, $t_4 = 36$, $t_5 = 18$.*

By lemma 4.1 and lemma 4.2 we can prove the following

Lemma 4.3. *Let B be a block in $S(4,5,11)$, $a \in B$. Let B_1, B_2 and B_3 be three blocks which meet B only at a. Then $|B_i \cap B_j - \{a\}| = 2$ $(i \neq j)$ and $B_1 \cap B_2 \cap B_3 = \{a\}$.*

By the above lemmas we can prove

Lemma 4.4. *Let B be a block in $S(4,5,11)$. Then for every $a \in B$, there exist exactly three blocks which meet B only at a.*

Now we can prove

Theorem 4.1. *There exists no semioval in $S(4,5,11)$.*

Proof. Suppose there exists a semioval O in $S(4,5,11)$. Then since there is no blocking set in $S(4,5,11)$, there must exist a block B such that either $B \subseteq O$ or $B \cap O = \emptyset$.

If $B \subseteq O$, then by lemma 4.4, $O - B \neq \emptyset$. Let $b \in O - B$. By lemma 4.1 any block which contains b meets B. So there is no tangent on b.

If $B \cap O = \emptyset$, then by lemma 4.1, $|O| \neq 6$ and $|O| \geq 5$. So $|O| = 5$. Let $o \notin O \cup B$, let $u, v, w \in O$ and let B' be the block determined by $\{o, u, v, w\}$. Then $|B' \cap B| = 1$. Let $B' \cap B = \{a\}$. By lemma 4.3 there is a block B'' such that $B'' \cap B = \{a\}$ and B'' contains o and one of u, v and w, say u. There are four blocks on $\{a, o, u\}$ and B', B'' are two of them. The other two can not contain any points in $B' \triangle B''$. So both of them are tangents on u, contradiction. □

In $S(5,6,12)$ we have

$$r_0 = 132, r_1 = 66, r_2 = 30, r_3 = 12, r_4 = 4, r_5 = 1.$$

Lemma 4.5. *The type of a block in $S(5,6,12)$ is $(0,2,3,4,6)$ with*

$$t_0 = 1, t_2 = 45, t_3 = 40, t_4 = 45, t_6 = 1.$$

Lemma 4.6. *Let B, B' be two disjoint blocks in $S(5,6,12)$. Then for any two points $a, b \in B$, there exist exactly three blocks B_1, B_2 and B_3 such that*

1. $B_1 \cap B = B_2 \cap B = B_3 \cap B = \{a, b\}$ *and* $|B_1 \cap B'| = |B_2 \cap B'| = |B_3 \cap B'| = 4$;
2. $|B_i \cap B_j \cap B'| = 2$ *and* $B_1 \cap B_2 \cap B_3 \cap B' = \emptyset$.

Lemma 4.7. *Let B, B' be two disjoint blocks in $S(5,6,12)$. Then for any four points $a, b, c, d \in B$, there exist exactly three blocks A_1, A_2 and A_3 such that $A_1 \cap B = A_2 \cap B = A_3 \cap B = \{a, b, c, d\}$ and $(A_1 \cap B') \cup (A_2 \cap B') \cup (A_3 \cap B') = B'$.*

Lemma 4.8. *The blocking set in $S(5,6,12)$ is a semioval.*

Proof. The blocking set C in $S(5,6,12)$ has the structure $C = (B - \{a\}) \cup \{x\}$, where $a \in B$ and $x \notin B$.

Let B' be a block disjoint from B; then $x \in B'$ and B' is a tangent on x to C. By lemma 4.5 the other blocks which contain x meet B in at least two points.

Let $b \in B - \{a\}$. By lemma 4.6 there are exactly three blocks B_1, B_2 and B_3 such that $B_i \cap B = \{a, b\}$ $(i = 1, 2, 3)$, and x is contained in only two of B_1, B_2 and B_3. So one of these blocks is a tangent on b to C. The other blocks which contain b meet B in at least three points. □

Theorem 4.2. *If O is a semioval in $S(5,6,12)$, then O is a blocking set.*

Proof. Suppose O is not a blocking set. If O contains a block A, then any block which contains a point in A contains at least two points in A. So O contains no block; therefore there exists a block B and a point x such that $B \cap O = \emptyset$

and $x \notin B \cup O$. By lemma 4.6 for $a \in O$ there are three tangents on a to O, contradiction. □

4.3. **Semiovals in** $S(3,6,22)$. In the sequel sometimes we will use the results about $S(3,6,22)$ in section 3.3 without explicit reference.

Lemma 4.9. *A semioval in* $S(3,6,22)$ *can not contain a Fano set.*

Lemma 4.10. *A semioval in* $S(3,6,22)$ *contains no block.*

Lemma 4.11. *A semioval in* $S(3,6,22)$ *can not contain* $B \triangle B'$, *where* B *and* B' *are blocks.*

Lemma 4.12. *The set* $D := (B - \{u\}) \cup (B' - \{v\})$, *where* B *and* B' *are disjoint blocks,* $u \in B$ *and* $v \in B'$, *is a semioval.*

Theorem 4.3. *Let* O *be a semioval in* $S(3,6,22)$. *Then* $9 \leq |O| \leq 10$.

Proof. First we prove that O contains at most 10 points.

Let $u, v \in O$, let B and B' be the tangents on u and v respectively.

If $B \cap B' = \emptyset$, then the points not in $B \cup B'$ can not all be contained in O. If there is only one point $x \notin O$, then the nine tangents on the other nine points not in $B \cup B'$ would all contain x and meet both B and B'; on x there are twelve blocks which meet only one of B, B'. None of these mentioned blocks contains all of u, v, x. So there are at least twenty-two blocks on x, a contradiction.

If $B \cap B' \neq \emptyset$, then consider the four external blocks E_1, E_2, E_3 and E_4 of $B \cup B'$. By the proof of lemma 2.2 in [7] we know that $|E_i \cap E_j| = 2$, if $i \neq j$, and $(E_i \cap E_j) \cap (E_k \cap E_h) = \emptyset$ if $\{i,j\} \neq \{k,h\}$. Let $E_1 \cap E_2 = \{x,y\}$, $E_3 \cap E_4 = \{z,w\}$. By lemma 4.10 and lemma 4.11 we only need to prove that the following sets are not semiovals.

a. $X_1 = \{u, v\} \cup E_1 \cup E_2 \cup E_3 \cup E_4 - \{x, z, p\}$, where $p \in E_1 \cap E_3$;

b. $X_2 = \{u, v\} \cup E_1 \cup E_2 \cup E_3 \cup E_4 - \{x, p, q\}$, where $p \in E_1 \cap E_3$, $q \in E_2 \cap E_4$;

c. $X_3 = \{u, v\} \cup E_1 \cup E_2 \cup E_3 \cup E_4 - \{x, p, r\}$, where $p \in E_1 \cap E_3$, $r \in E_1 \cap E_4$.

The set X_1 is not a semioval. Otherwise the tangents on the two points in $E_2 \cap E_4$ would all contain $\{x, z, p\}$.

The set X_2 is not a semioval. Otherwise the tangents on the points in $E_3 \cap E_4$ would all contain $\{x, p, q\}$.

Suppose X_3 is a semioval. Then the tangent on the point in $E_1 \cap E_3 - \{p\}$ contains p, but can not meet $(E_1 \cup E_2 \cup E_3 \cup E_4) - (E_1 \cap E_3)$. So it meets $(B \triangle B') - \{u, v\}$ at four points. Let A_1 be the other block on $E_1 \cap E_3$ which does not meet E_2; then $\{u, v\} \subset A_1$ and $|A_1 \cap (B \triangle B')| = 4$. We can similarly prove that there is a block A_2 on $E_1 \cap E_4$ such that $A_2 \cap E_2 = \emptyset$, $\{u, v\} \subset A_2$ and $|A_2 \cap (B \triangle B')| = 4$. Let A_3 and A_4 be the blocks on $\{u, v\}$ which are disjoint from E_1; then

$$E_3 \cap E_4 \not\subset A_i, E_2 \cap E_3 \not\subset A_i, E_2 \cap E_4 \not\subset A_i \ (i = 3, 4).$$

So

$$|A_i \cap (E_3 \cap E_4)| = |A_i \cap (E_2 \cap E_4)| = |A_i \cap (E_2 \cap E_4)| = 1.$$

Now, the block A_5 determined by $\{u, v, y\}$ would contain x and two points in $(B \triangle B') - \{u, v\}$. The blocks B, B' and A_5 are three external blocks to $E_3 \cup E_4$. Let the forth external block of $E_3 \cup E_4$ be T; then $u, v \notin T$ and $x, y \in T$. So T and E_2 are two tangents on y.

Now we need to show that a semioval contains at least nine points. This can be done by checking the frequency vectors in appendix A. ☐

Let B and B' be two disjoint blocks of $S(3,6,22)$, $x \notin B \cup B'$. Define

$$P := S - (B \cup B' \cup \{x\}).$$

Theorem 4.4. *The set P is a semioval of size 9 and $FV(P) = (2,9,36,12,18,0,0)$.*

Proof. Let $y \in P$. Since on $\{x,y\}$ there are four blocks which are all disjoint from B or B' and there are a total of five blocks on $\{x,y\}$, thus there is a block on $\{x,y\}$ which meets both B and B', so this block is a tangent on y. The other blocks on y all contain at least two points in P. It is easy to see that B and B' are the only two blocks which do not meet P. P contains no block. So we have $FV(P) = (2,9,36,12,18,0,0)$. ☐

Theorem 4.5. *If O is a semioval of size 9, then $O = P$.*

Proof. First we prove that there is no 5-secant block to O.

By solving the linear system (1) we know that the possible values for t_5 are 0 and 4.

If $t_5 = 4$, let B, B' be two blocks which are 5-secant to O; then $B \cap B' \neq \emptyset$. If $B \cap B' \subseteq O$, then $O - (B \cup B')$ has only one point, and on this point there are at least two tangents. If $B \cap B'$ is not contained in O, then $O = B \cup B' - \{x\}$, where $x \in B \cap B'$. By lemma 4.11 this is impossible.

So $t_5 = 0$ and therefore $t_0 = 2$. Let B, B' be the two blocks which do not meet O. We claim that $B \cap B' = \emptyset$. Otherwise, consider $B \cup B' \cup \{x\}$, where $x \notin B \cup B' \cup O$. Then there are two external blocks U and V to $B \cup B' \cup \{x\}$ such that $U \cup V$ contains only 8 points of O. The other point in O would lie on two of the four external blocks of $U \cup V$, a contradiction. Therefore $O = P$. ☐

Let $B = \{x, y, z, \bar{x}, \bar{y}, \bar{z}\}$, $B' = \{a, b, c, \bar{a}, \bar{b}, \bar{c}\}$ be two disjoint blocks, and let o be the point such that

$F = \{a, b, c, x, y, z, o\}$ forms a Fano set. Let U be the block on x, y which does not meet B'. Then $o \in U$. We define

$$M := S - (B \cup B' \cup U - \{a, b, c, o\}).$$

Theorem 4.6. *The set M is a semioval of size 10 with $(1, 10, 15, 40, 5, 6, 0)$ as its frequency vector.*

Proof. We only need to prove that on every point of M, there exists only one tangent.

Let $V, W \neq B$ be the blocks on x, z and y, z respectively which are disjoint from B', let

$$U = \{x, y, o, 1, 2, 3\},\ V = \{x, z, o, 4, 5, 6\},\ W = \{y, z, o, 7, 8, 9\};$$

then $M = \{a, b, c, o, 4, 5, 6, 7, 8, 9\}$.

It is easy to see that U is a tangent on o.

Let $X \neq U$ be a block which contains o. Then $|X \cap F| = 1$ or 3. If $|X \cap F| = 1$, then $|X \cap \{\bar{a}, \bar{b}, \bar{c}\}| = 2$ or $|X \cap \{\bar{x}, \bar{y}, \bar{z}\}| = 2$, so X contains two points in $\{4, 5, 6, 7, 8, 9\}$. Therefore, X is not a tangent to M. If $|X \cap F| = 3$, then

$|X \cap \{a, b, c\}| = |X \cap \{x, y, z\}| = 1$ or $|X \cap \{a, b, c\}| = 2$ and $|X \cap \{x, y, z\}| = 0$ or $|X \cap \{a, b, c\}| = 0$ and $|X \cap \{x, y, z\}| = 2$. In the first two cases, X is not a tangent to M. In the last case, $X = W$, so is not a tangent to M.

Let $u \in \{a, b, c\}$.

Consider the blocks determined by $\{u, 1, 2\}$, $\{u, 1, 3\}$ and $\{u, 2, 3\}$, respectively. None of the three blocks contains any of x, y, z, o. So at most two of them meet V

and W at two points in $\{4,5,6\}$ and two points in $\{7,8,9\}$; therefore at least one of them, say Y, meets $B - \{x,y,z\} = \{\bar{x},\bar{y},\bar{z}\}$ at two points. So Y is a tangent to M.

Let $X \neq Y$ be a block on u. If $|X \cap F'| = 3$, then X is not a tangent; if $|X \cap F'| = 1$, then $|X \cap \{\bar{x},\bar{y},\bar{z}\}| = 2$. Since $X \neq Y$, then $X \cap (Y \cap U) = \emptyset$. Thus $X \cap U = \emptyset$, so X contains two points in $\{4,5,6,7,8,9\}$ and is not a tangent to M.

Let $v \in \{4,5,6\}$.

Consider the blocks determined by $\{v,x,1\}$, $\{v,x,2\}$ and $\{v,x,3\}$ respectively. Since o is not in any of these blocks, none of them contains y or z. So at most two of them can meet either W or $\{a,b,c\}$ at two points; therefore at least one of them, say Z, meets $B' - \{a,b,c\}$. Z is a tangent to M.

Let $X \neq Z$ be a block on v. If $|X \cap F'| = 3$, then X contains o or at least one point in $\{a,b,c\}$. If $|X \cap F'| = 1$, since $X \neq Z$, we have $x \notin X$ (otherwise $y,z,o \notin X$, so $X \cap \{\bar{a},\bar{b},\bar{c}\} \neq \emptyset$ and X has at least three points in common with Z, and so $X = Z$). If $z \in X$, then $y \notin X$, so X contains one point in $\{7,8,9\}$. If $z \notin X$, then X contains one point in $\{o,4,5,6\} - \{v\}$. So in either case X is not a tangent to M.

If $v \in \{7,8,9\}$, we can similarly prove that there is only one tangent on v.

From the structure of a Fano set we can conclude that B is the only block which does not meet M, and M contains no block. So $FV(M) = (1,10,15,40,5,6,0)$. ☐

Theorem 4.7. *Let O be a semioval of size 10. If $O \neq D$, then $O = M$.*

Proof. Checking the appendix B we can see that there is a block B such that $O \cap B = \emptyset$.

Choose a point $o \in O$ and let U be the unique tangent on o. Then using a similar argument as in the third paragraph of the proof of theorem 4.3, we can prove that $U \cap B \neq \emptyset$.

We claim that there exists a block B' which contains three points in O and is disjoint from $B \cup U$.

Let $\mathcal{S} - (B \cup U \cup O) = \{d, e, f\}$. Consider the two external blocks X, Y of $B \cup U \cup \{d\}$. By lemma 4.10 and lemma 4.11, $X \cup Y$ contains eight points in O, and $(X \cap Y) \cap O \neq \emptyset$. If $|(X \cap Y) \cap O| = 1$, then suppose $e \in (X \cap Y) - O$; then f lies on only one of X and Y, say X. In this case, there exist two points on $Y - X$, the tangents of which would all contain $\{d, e, f\}$. This is impossible. So $|(X \cap Y) \cap O| = 2$. The three points d, e and f must all be contained in one of the other two external blocks of $B \cup U$ (otherwise, the tangents on the two points in $X \cap Y$ would all contain d, e and f). Let this block be B', then $|B' \cap O| = 3$ and $B' \cap (B \cup U) = \emptyset$.

Let $B' \cap O = \{a, b, c\}$, let $V, W \in \Re(B)$ with $V \neq B' \neq W$, be the blocks on $\{a, b\}$ and $\{a, c\}$ respectively and let $o' \in (V \cap W) - \{a\}$.

Now we prove $o' = o$.

If $o' \neq o$, then we claim $o' \notin U$. Otherwise, let $U = \{x, y, o, o', u, v\}$, where $\{x, y\} = U \cap B$, let $V = \{a, b, o', u, , 1, 2\}$, $W = \{a, c, o', v, 3, 4\}$. Let $Z \in \Re(B)$, $Z \neq B'$, be the block on $\{b, c\}$. Then $Z = \{b, c, o', o, 5, 6\}$. The tangent T on 5 would contain o', u, v, a contradiction. So $o' \notin U$ and therefore $o' \in O$.

Using the construction method of a Fano set to o', $\{a, b, c\}$ and B (see section 3.4), we can partition B into two parts: B_1 and B_2. Since $o' \notin U$, then x and y cannot be in the same part.

Let X be a block on o'; then $|X \cap (\{a, b, c, o'\} \cup B_1)| = 1$ or 3.

If $|X\cap(\{a,b,c,o'\}\cup B_1)| = 1$, then $|X\cap[B_2\cup(B'-\{a,b,c\})]| = 2$. So X contains at least one point in $O-\{a,b,c,o'\}$; hence $|X\cap O|\geq 2$.

If $|X\cap(\{a,b,c,o'\}\cup B_1)| = 3$, then either $|X\cap\{a,b,c\}|\geq 1$ or $|X\cap B_1| = 2$. If $|X\cap B_1| = 2$, then $|X\cap B'| = 0$, so X contains at least one point in $O-(B\cup B'\cup\{o'\})$.

So we have proved $o' = o$. Therefore $O = M$. □

In the definition of M, there are six choices for U, so there are six semiovals which do not contain B.

4.4. **Semiovals in** $S(4,7,23)$. By checking the frequency vectors in appendix B we can see that the only set that could be a semioval is E_1.

Lemma 4.13. *The set E_1 is a semioval.*

Proof. By lemma 2.11 in [8] we know that on every point in $B-B'$, there exists at least one tangent.

Let $a\in B'-\{o,w\}$. Of the five blocks through $\{o,w,a\}$, only three meet $B-\{o\}$, so there is one which meets $B\cup B'$ only at o, w and a. This block is a tangent on the point a.

Of the five blocks through three fixed points in $B'-\{o,w\}$, four meet $B-\{o\}$, so one meets $B-\{o\}$ at three points. This block is a 6-secant to E_1. There are $\binom{5}{3} = 10$ of these kind of blocks. So there are at least eleven 6-secant blocks to E_1. Let $c = 11$ and solve (2.1) in [8] to get $t_1 = 22 - t_6$. So $t_1 = t_6 = 11$ and there are only eleven tangents to E_1. Hence on every point of E_1 there is only one tangent to E_1, and therefore E_1 is a semioval. □

4.5. **The non-existence of semiovals in** $S(5,8,24)$. In this section we use the same notations and terminology as in [9].

By checking the frequency vectors in appendix C we can see that the only set in $S(5,8,24)$ that could be a semioval is I.

Lemma 4.14. *The set I is not a semioval.*

Proof. Suppose I is a semioval; then since $\mathcal{S} - I$ is the same type of blocking set as I, $\mathcal{S} - I$ is also a semioval. Let $I = (B - \{u\}) \cup (B' - \{v\})$, where B and B' are blocks with $|B \cap B'| = 2$, $u \in B - B'$, $v \in B' - B$ and let U be the tangent on u to $\mathcal{S} - I$; then U is 7-secant to I. So $|U \cap [B - (B' \cup \{u\})]| = 3$ and $|U \cap [B' - (B \cup \{v\})]| = 4$. Now $|U \cap B| = 4$, so by lemma 2.1(b) in [9], $U \triangle B$ is a block. But $(U \triangle B) \cap B'' = 6$, a contradiction. $\square$

So we have

Theorem 4.8. *There exists no semioval in $S(5,8,24)$.*

5. ACKNOWLEDGMENTS

I am very grateful to my advisor - Dr. L. M. Batten, who suggested the topic to me. During the writing of this thesis, Dr. Batten carefully read every version of the manuscript, and made many helpful suggestions. Dr. Batten had also kindly provided me with many papers listed in the references. Also I wish to express my appreciation to professor B. W. Quackenbush, professor J. van Rees and professor W. Martin who have kindly pointed out some errors in my thesis. Dr. Batten and Professor Martin also helped me in the final correction of my thesis.

I would also like to thank the Department of Mathematics and the Faculty of Graduate Studies at the University of Manitoba for the financial support during my Ph.D program.

Appendix

We use n to denote the size of a point subset of $S(t.k.v)$. The number of vectors under each size n is the number of orbits under the action of the Mathieu group [42].

Appendix A. The frequency vectors of the point subsets in $S(3.6.22)$

$n = 0$

(77.0.0.0.0.0.0).

$n = 1$

(56.21.0.0.0.0.0).

$n = 2$

(40.32.5.0.0.0.0).

$n = 3$

(28.36.12.1.0.0.0).

$n = 4$

(20.32.24.0.1.0.0). (19.36.18.4.0.0.0).

$n = 5$

(16.20.40.0.0.1.0). (12.35.20.10.0.0.0). (12.35.20.10.0.0.0). (13.31.26.6.1.0.0).

$n = 6$

(16.0.60.0.0.0.1). (6.36.15.20.0.0.0). (6.36.15.20.0.0.0). (10.21.35.10.0.1.0).

(9.24.33.8.3.0.0). (8.28.27.12.2.0.0).

$n = 7$

(0.42.0.35.0.0.0). (0.42.0.35.0.0.0). (10.6.45.15.0.0.1). (7.14.42.7.7.0.0).

(4.26.24.19.4.0.0). (4.26.24.19.4.0.0). (6.19.32.17.2.1.0). (5.22.30.15.5.0.0).

$n = 8$

(7.0.56.0.14.0.0). (0.28.14.28.7.0.0). (0.28.14.28.7.0.0). (6.8.35.24.3.0.1).

(4.13.34.18.7.1.0). (2.20.26.20.9.0.0). (3.17.28.22.6.1.0). (3.17.28.22.6.1.0).

(4.14.30.24.3.2.0). (3.16.32.16.10.0.0).

$n = 9$

(4.3.40.16.12.2.0). (0.18.20.26.12.1.0). (0.18.20.26.12.1.0). (4.6.29.30.6.1.1).

(3.9.27.28.9.0.1). (2.11.28.24.10.2.0). (1.14.26.22.13.1.0). (2.12.24.30.6.3.0).

(2.12.24.30.6.3.0). (2.9.36.12.18.0.0).

$n = 10$

(4.0.27.32.12.0.2). (0.12.18.28.18.0.1). (2.4.29.24.14.4.0). (0.11.21.26.16.3.0).

(0.11.21.26.16.3.0). (2.6.22.32.12.2.1). (1.8.24.24.19.0.1). (1.8.23.28.13.4.0).

(0.10.25.20.20.2.0). (1.7.27.22.17.3.0). (1.10.15.40.5.6.0). (1.10.15.40.5.6.0).

(2.0.45.0.30.0.0).

$n = 11$

(0.6.20.25.20.6.0). (0.6.20.25.20.6.0). (2.2.18.33.18.2.2). (0.7.17.27.22.3.1).

(1.3.22.27.17.7.0). (0.6.20.25.20.6.0). (0.7.16.31.16.7.0). (0.6.20.25.20.6.0).

(1.4.19.29.19.4.1). (1.5.15.35.15.5.1). (0.7.16.31.16.7.0). (1.5.15.35.15.5.1).

(0.5.25.15.30.1.1). (1.1.30.15.25.5.0). (0.11.0.55.0.11.0). (0.11.0.55.0.11.0).

Appendix B. The frequency vectors of the point subsets in $S(4.7.23)$

$n = 0$

(253.0.0.0.0.0.0.0).

$n = 1$

(176.77.0.0.0.0.0.0).

$n = 2$

(120.112.21.0.0.0.0.0).

$n = 3$

(80, 120, 48, 5, 0, 0, 0, 0).

$n = 4$

(52, 112, 72, 16, 1, 0, 0, 0).

$n = 5$

(32, 100, 80, 40, 0, 1, 0, 0), (33, 95, 90, 30, 5, 0, 0, 0).

$n = 6$

(16, 96, 60, 80, 0, 0, 1, 0), (21, 72, 105, 40, 15, 0, 0, 0), (20, 77, 95, 50, 10, 1, 0, 0).

$n = 7$

(0, 112, 0, 140, 0, 0, 0, 1), (15, 42, 126, 35, 35, 0, 0, 0), (10, 66, 81, 75, 20, 0, 1, 0),

(12, 57, 96, 65, 20, 3, 0, 0).

$n = 8$

(15, 0, 168, 0, 70, 0, 0, 0), (0, 70, 42, 105, 35, 0, 0, 1), (8, 35, 98, 70, 35, 7, 0, 0),

(6, 44, 83, 80, 35, 4, 1, 0), (7, 40, 88, 80, 30, 8, 0, 0).

$n = 9$

(8, 7, 112, 56, 56, 14, 0, 0), (0, 42, 56, 91, 56, 7, 0, 1), (4, 26, 77, 86, 46, 13, 1, 0),

(3, 30, 72, 86, 51, 9, 2, 0), (4, 27, 72, 96, 36, 18, 0, 0).

$n = 10$

(4, 8, 75, 80, 60, 24, 2, 0), (0, 24, 54, 85, 70, 18, 1, 1), (2, 17, 60, 90, 60, 21, 3, 0),

(1, 20, 60, 80, 75, 12, 5, 0), (2, 20, 45, 120, 30, 36, 0, 0).

$n = 11$

(0, 12, 48, 75, 80, 36, 0, 2), (2, 6, 50, 85, 70, 34, 6, 0), (0, 13, 44, 80, 80, 31, 4, 1),

(1, 10, 45, 85, 75, 30, 7, 0), (1, 11, 40, 95, 65, 35, 6, 0), (0, 11, 55, 55, 110, 11, 11, 0),

(0, 22, 0, 165, 0, 66, 0, 0).

APPENDIX C. THE FREQUENCY VECTORS OF THE POINT SUBSETS IN $S(5,8,24)$

$n = 0$

(759, 0, 0, 0, 0, 0, 0, 0, 0).

$n = 1$

(506, 253, 0, 0, 0, 0, 0, 0, 0.

$n = 2$

(330, 352, 77, 0, 0, 0, 0, 0, 0).

$n = 3$

(210, 360, 168, 21, 0, 0, 0, 0, 0).

$n = 4$

(130, 320, 240, 64, 5, 0, 0, 0).

$n = 5$

(78, 260, 280, 120, 20, 1, 0, 0, 0).

$n = 6$

(46, 192, 300, 160, 60, 0, 1, 0, 0), (45, 198, 285, 180, 45, 6, 0, 0, 0).

$n = 7$

(30, 112, 336, 140, 140, 0, 0, 1, 0), (25, 141, 267, 225, 85, 15, 1, 0, 0).

$n = 8$

(30, 0, 448, 0, 280, 0, 0, 0, 1), (15, 85, 252, 231, 140, 35, 0, 1, 0).

(13, 96, 228, 256, 130, 32, 4, 0, 0).

$n = 9$

(15, 15, 280, 168, 210, 70, 0, 0, 1), (7, 58, 189, 259, 175, 63, 7, 1, 0).

(6, 63, 180, 264, 180, 54, 12, 0, 0).

$n = 10$

(7.16.175.224.210.112.14.0.1). (3.36.138.250.215.96.19.2.0).

(2.40.135.240.240.72.30.0.0).

$n = 11$

(3.12.108.219.230.148.36.2.1). (1.21.95.220.245.135.37.5.0).

(0.22.110.165.330.66.66.0.0).

$n = 12$

(3.0.72.192.225.192.72.0.3). (1.8.64.184.245.184.64.8.1).

(0.12.60.180.255.180.60.12.0). (0.11.66.165.275.165.66.11.0).

(0.0.132.0.495.0.132.0.0).

REFERENCES

[1] A. Baartmans, W. Wallis and J. Yucas, *A geometric construction of the Steiner system S(4,7,23)*. Discrete Math. **102** (1992), no.2, 177–186.

[2] S. Ball, *On the size of a triple blocking set in PG(2,q)*. European Journal of Combinatorics **17** (1996), 427–435.

[3] S. Ball, *Multiple blocking sets and arcs in finite planes*, preprint.

[4] S. Ball and A. Blokhuis, *On the size of a double blocking set in PG(2,q)*, preprint.

[5] L. M. Batten, *Determining sets*, preprint.

[6] L. M. Batten, *Protocol for a private key cryptosystem with signature capability based on blocking sets in t-designs*, preprint.

[7] L. Berardi, *Blocking sets in the large Mathieu designs, I: the case S(3,6,22)*, Annals of Discrete Mathematics **37** (1988), 31–42.

[8] L. Berardi, *Blocking sets in the large Mathieu designs, II: the case S(4,7,23)*, J.of Inf. & Opti. Sci. **2** (1988), 263–278.

[9] L. Berardi and F. Eugeni, *Blocking sets in the large Mathieu designs, III: the case S(5,8,24)*, Ars.comb.**29** (1990), 33–41.

[10] L. Berardi, F. Eugeni and O. Ferri, *Sui blocking sets nei sistemi di Steiner*, Boll.Un.Mat.Ital. Sez. D 1(1984),141–164.

[11] Th. Beth, *Some remarks on D.R.Hughes' construction of M_{12} and its associated designs*, finite geometries and designs, LMS lecture notes **49** (1980), 22–30, Cambridge University Press.

[12] Th. Beth and D. Jungnickel, *Mathieu groups, Witt designs, and Golay codes*, Geometries and Groups, Lecture Notes in Mathematics **893** (1981),157–179, Springer-Verlag, Berlin Heidelberg New York.

[13] Th. Beth, D. Jungnickel and H. Lenz, *Design Theory*, Cambridge University Press, 1986.

[14] A. Blokhuis, *Blocking sets in Desarguesian planes*, Bolyai Society Mathematical Studies, Combinatorics, Paul Erdös is eighty Vol. **2**(Hungary) (1993), 1–22.

[15] A. Blokhuis and T. Szönyi, *Note on the structure of semiovals in finite projective planes*, Discrete Math. **106/107** (1992), 61–65.

[16] A. A. Bruen. *Arcs and multiple blocking sets*, Symposia Mathematica **28** Academic Press (1986), 15–29.

[17] A. R. Calderbank and P. Morton. *Quasi-symmetric 3-designs and elliptic curves*. SIAM J. Discrete Math. **3** (1990), no.2, 178–196.

[18] P. J. Cameron. *Parallelisms of Complete Designs*. LMS Lecture Notes Ser **23**. Cambridge University Press. 1976.

[19] P. J. Cameron and J. H. van Lint. *Graph Theory, Coding Theory and Block Designs*. LMS Lecture Notes **19**, Cambridge University Press. 1975.

[20] P. J. Cameron and J. H. van Lint. *Graphs, codes and designs*. LMS Lecture Notes **43**. Cambridge University Press. 1980.

[21] R. D. Carmichael. *Introduction to the theory of groups of finite order*. Ginn and Company. 1937.

[22] C. J. Colbourn and J. H. Dinitz. *The CRC Handbook of Combinatorial Designs*. CRC Press. 1996.

[23] J. H. Conway. *A Group of order* 8,315,553,613,086,720,000. Bull. London Math.Soc., 1 (1969),79-88.

[24] J. H. Conway and N. J. A. Sloane. *Orbit and coset analysis of the Golay and related codes*. IEEE transactions on information theory,Vol.**36**, No.**5**(1990),1038–1050.

[25] J. H. Conway and N. J. A. Sloane. *Sphere Packings, Lattices and Groups*. Springer-Verlag. New York, Berlin, Heidelberg, London, Paris, Tokyo, 1988.

[26] R. T. Curtis. *A new combinatorial approach to* M_{24} . Math. Proc. Cambridge Phil. Soc. **79** (1976), 25–42.

[27] R. H. F. Denniston. *Some new 5-designs*. Bull.London Math.Soc. **8** (1976), 263–267

[28] Jeremy M. Dover. *Semiovals containing large collinear subsets*. preprint.

[29] H. Enomoto, N. Ito and R. Noda. *Tight 4-designs*. Osaka J.Math. **16** (1979), 39–43.

[30] M. de Finis. *On semiovals in projective planes*. Ars. Combin.**24A**(1987), 65–70.

[31] M. J. E. Golay, *Notes on Digital Coding*, Proc.I.R.E(IEEE) **37** (1949), 657.

[32] S. A. Hobart. *On designs related to coherent configurations of type* $\binom{22}{4}$. Discrete Math. **94** (1991), no.2, 103–127.

[33] D. G. Hoffman, D. A. Leonard, C. C. Lindner, K. T. Phelps, C. A. Rodger and J. R. Wall, *Coding Theory*, Marcel Dekker, Inc., 1991.

[34] D. R. Hughes, *A combinatorial construction of the small Mathieu designs and groups*, Ann. Discrete Math. **15** (1982), 259–264.

[35] D. R. Hughes and F. C. Piper, *Design Theory*, Cambridge University Press, Cambridge, 1986.

[36] Y. J. Ionin and M. S. Shrikhande, *(2s − 1)-designs with s intersection numbers*, Geom.Dedicata **48** (1993), no.3, 247–265.

[37] N. Ito, *On tight 4-designs*, Osaka J.Math. **12** (1975), 493–522. (Corrections and Supplements, Osaka J.Math. **15** (1978), 693–697.)

[38] S. Iwasaki, *An elementary and unified approach to the Mathieu-Witt systems*, J. Math. Soc. Japan **40** A(1988), no.3, 393–414.

[39] S. Iwasaki, *An elementary and unified approach to the Mathieu-Witt systems II, the uniqueness of* W_{22}, W_{23}, W_{24}, Hokkaido Math.J. **21** (1992), no.2, 239–250.

[40] W. Jónsson, *On the Mathieu groups* M_{22}, M_{23}, M_{24} *and the uniqueness of the associated Steiner systems*, Math. Z **125** (1972), 193–214.

[41] W. Jónsson and J. Mckay, *More about the Mathieu group* M_{22}, Canad. J. Math. **38** (1976), no.5, 929–937.

[42] E. S. Kramer, S. S. Magliveras and D. M. Mesner, *t-designs from the large Mathieu groups*, Discrete Math. **36** (1981), 171–189.

[43] E. S. Lander, *Symmetric Designs: An Algebraic Approach*, LMS Lecture Notes Ser. **74**, Cambridge University Press, 1983.

[44] J. Leech, *Notes on sphere packings*, Canad.J.Math. **19**(1967),251–267.

[45] H. Lenz, *Variations on the projective plane of order four*, Mitt.Math. Sem.Giessen No. 192(1989), 79–84.

[46] J. H. van Lint, *Codes and combinatorial Designs*, Proceedings of the Marshal Hall conference (1990, University of Vermont), John Wiley & Sons, Inc., 1993, 31–39.

[47] H. Lüneburg, *Transitive Erweiterungen endlicher Permutations Gruppen*, Lecture Notes in Mathematics **84**, Springer-Verlag, NY, 1969.

[48] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland Publishing Company. 1977.

[49] W. H. Mills. *A new 5-design*. Ars Combinaroria **6** (1978). 193–195.

[50] L. J. Paige. *A note on the Mathieu groups*. Canad. J. Math. **9** (1957). 15–18.

[51] A. Pott and M. Shrikhande. *t-designs with few intersection numbers*. Discrete Math. **90** (1991). no.2. 215–217.

[52] M. S. Shrikhande and S. S. Sane. *Quasi-Symmetric Designs*. Cambridge University Press. Cambridge. 1991.

[53] R. G. Stanton. *The Mathieu groups*. Canadian J. Math. **3** (1951). 164–174.

[54] J. A. Thas. *On semiovals and semiovoids*. Geom. Dedicata **3** (1974). 229–231.

[55] J. A. Todd. *A representation of the Mathieu group M_{24} as a collineation group*. Ann. di Mat. Pur ed Appl., **71** (1966). 199–238.

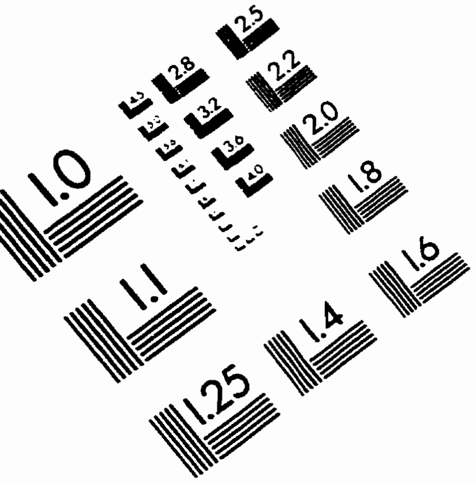
[56] V. D. Tonchev (translated from the Bulgarian by R. A. Melter). *Combinatorial Configurations Designs. Codes. Graphs*. Longman Scientific & Technical. 1988.

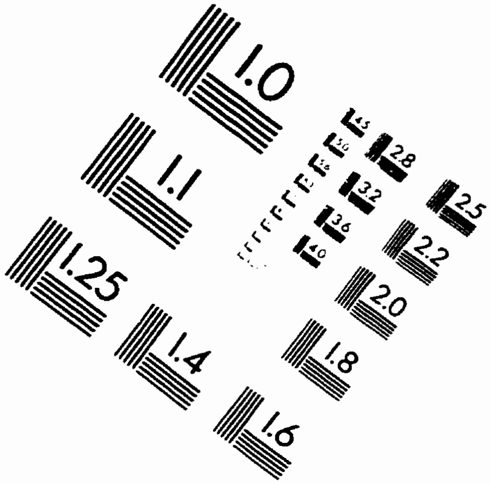
[57] E. Witt. *Die 5-fach transitiven Gruppen von Mathieu*. Abh.Math.Sem.Hamburg **12** (1938). 256–264.

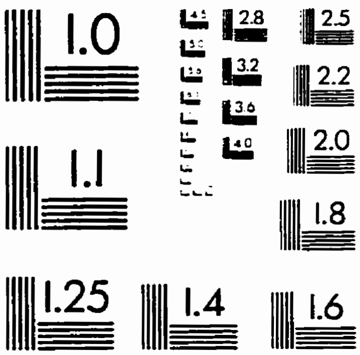
[58] E. Witt. *Über Steinersche Systeme*. Abh.Math.Sem.Hamburg **12** (1938). 265–273.

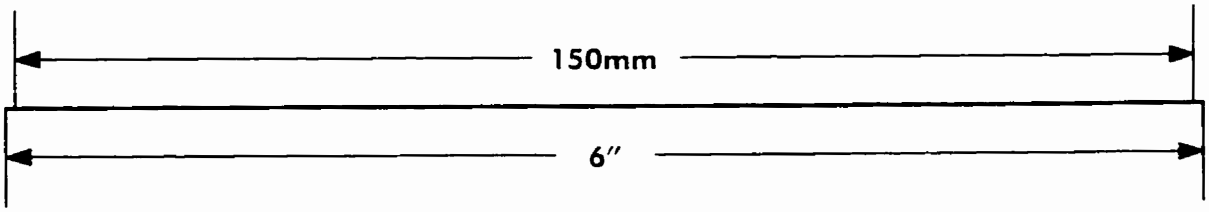
INDEX

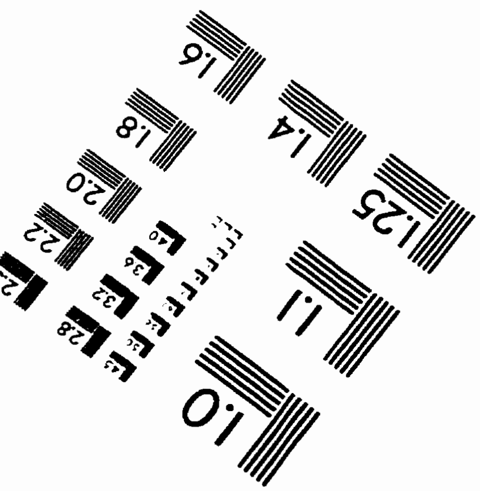
IMAGE EVALUATION TEST TARGET (QA-3)

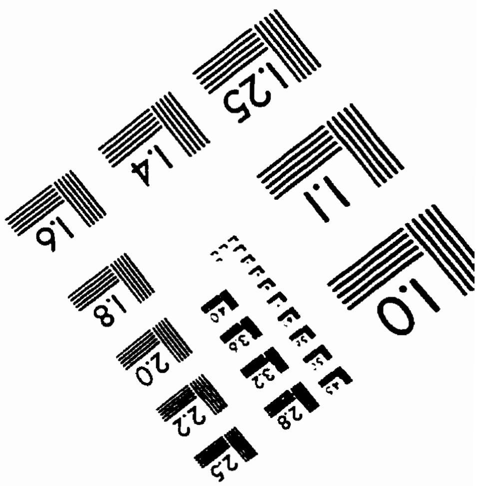












APPLIED IMAGE . Inc
1653 East Main Street
Rochester, NY 14609 USA
Phone: 716/482-0300
Fax: 716/288-5989