

THE CONSTRUCTION OF GEOMETRIC
THRESHOLD SCHEMES WITH PROJECTIVE
GEOMETRY

by

Leanne D. Holder

B.S., University of Southern Mississippi, 1994

A thesis submitted to the
University of Colorado at Denver
in partial fulfillment
of the requirements for the degree of
Master of Science
Applied Mathematics

1997

This thesis for the Master of Science

degree by

Leanne D. Holder

has been approved

by

William E. Cherowitzo

Stanley E. Payne

J. Richard Lundgren

Date _____

Holder, Leanne D. (M.S., Applied Mathematics)

The Construction of Geometric Threshold Schemes With Projective Geometry

Thesis directed by Associate Professor William E. Cherowitzo

ABSTRACT

In a secret sharing scheme, a dealer has a secret and distributes shares of the secret to the participants. The shares are distributed in such a way that only certain subsets of the participants can combine their shares to recover the secret. We use projective geometry to construct a secret sharing scheme for which the shares are represented by points in a projective 4-space. A sharply focused set is a set of k points, no three collinear, in a finite projective plane in which the $\binom{k}{2}$ distinct secants formed by this set intersect a given line in exactly k points. We use sharply focused sets to design a scheme so that certain subsets of participants can pool their shares to calculate the secret. Several examples show how sharply focused sets can be used for differing sizes of the subsets of the participants that are allowed to calculate the secret. We provide a proof that sharply focused sets obtained from a certain construction correspond to cosets of a group. This implies that the possible sizes of these sharply focused sets are divisors of the group order. Finally, we provide a new construction that uses subplanes in planes of prime power order. The previous construction method works only on planes of odd order, but the subplane construction method works in planes of both even and odd order.

This abstract accurately represents the content of the candidate's thesis. I recommend its publication.

Signed _____
William E. Cherowitzo

ACKNOWLEDGMENT

There are many people who deserve more than just an acknowledgment on this page. The following people deserve many hugs.

My advisor, *Bill Cherowitzo*, for the many geometric lessons on and off the racketball court. May his seemingly bottomless well of patience not run dry until long after I am finished with my studies.

My best friend, *Allen Holder*, for his love, encouragement, and patience over the past five years. I consider myself extremely blessed to have him as my husband.

My mom, *Dianne M. Daniel*, for teaching me how to “play the game” so well. Bring on the goldfish.

My dad, *Donnie L. Daniel*, for his profound and more often than not, practical words of wisdom.

CONTENTS

<u>Chapter</u>		
1	Secret Sharing Schemes	1
1.1	A Generic Secret Sharing Scheme Involving the Employees of a Bank	1
1.2	An Introduction to Projective Geometry	2
1.3	Using Projective Geometry to Construct A Secret Sharing Scheme for a Bank	6
2	Sharply Focused Sets of lines in $PG(2,q)$	11
2.1	The Relationship Between Sharply Focused Sets and Secret Sharing Schemes for a Bank	11
2.2	Coordinate Representation of Points and Lines in $PG(2,q)$	13
2.3	Construction of Sharply Focused Sets in $PG(2,q)$	14
2.4	Two Examples with $q = 11$	16
2.5	Two Examples with $q = 13$	21
2.6	Structure of the Incidence Tables	23
2.7	General Method	25
3	Proving the Divisibility Argument	27
3.1	A Relationship Between Points of Ω and Points of l	27
3.2	Sharply Focused Sets Correspond to Cosets of a Group	30
4	Another Construction of Sharply Focused Sets	33

4.1	Even Characteristic Preamble	34
4.2	Existence and Construction of Sharply Focused Sets in Planes of Prime Power Order	34
4.3	Super Sharply Focused Sets in Planes of Even Order . .	36
4.4	A Sharply Focused and Super Sharply Focused Set in $PG(2,16)$	37
4.5	Advantages and Disadvantages of Each Construction of Sharply Focused Sets	38
5	Further Studies	39
	<u>References</u>	40

FIGURES

Figure

1.1	A Geometric Representation	7
1.2	Another Geometric Representation	9
2.1	Structure of the Incidence Tables	23
4.1	Subplane of a Projective Plane	33

TABLES

Table

2.1	The Incidence Table for $q = 11$ and l an Exterior Line . . .	16
2.2	The Incidence Table for $q = 11$ and l a Secant Line	20
2.3	The Incidence Table for $q = 13$ and l an Exterior Line . . .	21
2.4	The Incidence Table for $q = 13$ and l a Secant Line	22

1. Secret Sharing Schemes

In a secret sharing scheme, a dealer has a secret and would like to give every participant of this scheme a share of the secret. The shares should be distributed secretly, so that no participant knows the share of another participant. Also, some time later a subset of the participants could pool their shares in an attempt to compute the secret. In some situations the dealer may want some of the subsets of participants to be able to compute the secret while other subsets of the participants to be unable to compute the secret [2, 7]. If the dealer is faced with this type of situation, then it is necessary to identify the appropriate subsets of participants before the shares are distributed.

1.1 A Generic Secret Sharing Scheme Involving the Employees of a Bank

In a bank, there is a vault that must be opened every day. The president of the bank employs a number of senior tellers and vice presidents but does not trust any individual with the combination to the vault. So, a system needs to be designed in which certain combinations of these employees can open the vault.

One plan is to design a system, call it Design A, whereby any three senior tellers can open the vault or any two vice presidents can open the vault. Although this appears as a practical solution in theory, this system might not

work in reality if only two senior tellers and one vice president show up for work [7]. A more practical design, Design B, is obtained by adding to Design A the ability for two tellers and one vice president to open the vault. One must insure that no pair of senior tellers can open the vault while allowing any vice president in cooperation with a pair of senior tellers the ability to open the vault [6]. If we can do this, we will have obtained a secret sharing scheme in which the dealer is the president of the bank, the participants are the vice presidents and senior tellers, and the secret is the combination to the vault.

1.2 An Introduction to Projective Geometry

People who have studied only Euclidean geometry regard it as an obvious fact that two coplanar lines with a common perpendicular are *parallel*, in the sense that, however far we extend them, they will remain the same distance apart. By stretching our imagination we can conceive the possibility that this is merely a first approximation: that if we could extend them for millions or billions of miles we might find the lines getting closer together or farther apart. When we look along a straight railroad we get the impression that the two parallel rails meet on the horizon. Anyhow, by assuming that two coplanar lines always meet, we obtain a system of propositions which is just as logically consistent as Euclid's system [3].

Definition: [8] A *finite projective plane* consists of a finite set \mathcal{P} of points and a set of subsets of \mathcal{P} called lines, which satisfies the axioms (A1), (A2), and (A3):

- (A1) Given two points, there is exactly one line that contains both;
- (A2) Given two lines, there is exactly one point that lies on both;
- (A3) There are four points, of which no three are collinear.

In this setting, if a point lies on a line then the point is said to be *incident* with the line. Similarly, the line is also said to be *incident* with the

point. The axioms in the definition of a finite projective plane are the keys to the proofs of the following lemmas dealing with the incidence of points and lines in a finite projective plane, Π .

Lemma 1.3.1. [1] If l_1 and l_2 are any two distinct lines of Π , then there is a point P in Π not incident with l_1 and l_2 . ■

Lemma 1.3.2. [1] Any two lines of Π are incident with the same number of points. ■

Lemma 1.3.3. [1] Any two points of Π are incident with the same number of lines. ■

In a finite projective plane, there are a finite number of points on a line, a finite number of lines through a point, and a finite number of points and lines in the plane. The previous three lemmas can be combined with some results not mentioned here to obtain the following important theorem on the exact numbers for the above incidences.

Theorem 1.3.4. [1] *Let Π be a finite projective plane. Then there is an integer q such that*

- (1) *Every point of Π is incident with exactly $q + 1$ lines;*
- (2) *Every line of Π is incident with exactly $q + 1$ points;*
- (3) *Π contains exactly $q^2 + q + 1$ points;*
- (4) *Π contains exactly $q^2 + q + 1$ lines.* ■

One commonly used construction for obtaining a projective geometry, denoted by $\text{PG}(n, q)$, starts with a vector space. Let $V(n+1, q)$ be a vector space of rank $n + 1$ over a finite field $\text{GF}(q)$ where q is a prime power. The elements of $V(n+1, q)$ are the $(n+1)$ -tuples of the form (x_0, x_1, \dots, x_n) where

the x_i are in $\text{GF}(q)$. The points, lines, and planes of $\text{PG}(n,q)$ are the rank 1, 2, and 3 vector subspaces in V , where rank is the algebraic dimension of a vector subspace. The geometric dimension of objects in $\text{PG}(n,q)$ refers to the geometric concept where lines are 1-dimensional, planes are 2-dimensional and so forth. The rank and dimension always differ by one, i.e., a rank 2 subspace corresponds to a line which is referred to as having geometric dimension 1.

In this construction, incidence is defined by subspace containment. In the projective geometry setting, lines are regarded as certain sets of points and similarly planes can also be regarded as certain sets of points. If a point lies on a line or in a plane, then the point is said to be *incident* with the line or plane. This is equivalent to the notion of a rank 1 subspace being contained in a rank 2 or rank 3 subspace.

When $n = 2$, the vector space construction of a projective geometry gives a finite projective plane that we examined earlier. Every plane arising from this construction satisfies the axioms given in the formal definition of a finite projective plane.

A well known result from Linear Algebra states that if S and T are vector spaces then

$$\text{rk}(S) + \text{rk}(T) = \text{rk}(S \cap T) + \text{rk}(S \cup T).$$

Let $\Gamma = \text{PG}(4,q)$ be derived from a rank 5 vector space. Then we can use the rank formula to determine the possible incidences of lines and planes in Γ .

First, we examine the relationship between two distinct planes, π_1 and π_2 , in Γ . If π_1 and π_2 lie in a common 3-dimensional subspace of Γ , (i.e., rank 4 vector space) then the rank formula tells us that these two planes

intersect in a line (a rank 2 vector subspace). But, if π_1 and π_2 do not lie in a common 3-dimensional subspace of Γ , by the rank formula, π_1 and π_2 must intersect in a point, since their union would have rank 4. Let P , Q , and R are be three non-collinear points in Γ . Since each point has rank 1 and two points determine a line, the rank formula tells us that the smallest subspace containing these 3 points is a rank 3 subspace of Γ , which is a projective plane.

Next, we examine the incidence relationship between a line, l and a plane π , both in Γ . If l meets π , then l either meets π in a point or is entirely contained within π . Suppose two points of l are in π . Then since π is a vector subspace, the span of any two points that lie in π , also lies in π . In this case, it must be that l is entirely contained in π .

We will consider a special type of object called an oval in the projective plane, $\pi = \text{PG}(2, q)$. Similar to an oval in Euclidean geometry, an *oval*, denoted Ω , in π is set of $q + 1$ points in π such that no three of the points are collinear. Since no three points on Ω are collinear, if l is a line in π , then l can intersect Ω in at most two points and we can classify l in the following way:

- l is a *tangent line* to Ω provided $|l \cap \Omega| = 1$,
- l is a *secant line* to Ω provided $|l \cap \Omega| = 2$,
- l is an *exterior line* to Ω provided $|l \cap \Omega| = 0$.

Let P be a point in π . Then P can be classified in three ways with respect to Ω :

- if P is on Ω then P is called an *oval-point*,
- if P is not on Ω but on a tangent line to Ω then P is called an *exterior point*, and

- if P is neither on Ω nor on a tangent line to Ω then P is called an *interior point*.

For q odd, we have that any exterior point to Ω has exactly two tangents through it. When q is even, there are no interior points, since every point is on a tangent line and all tangents with respect to Ω intersect at a unique point in the plane, called the *nucleus* (or knot) of Ω .

We can use some of the incidence relationships between l , π and a point P in Γ to construct a secret sharing scheme that satisfies the requirements of Design A and Design B. This is accomplished by assigning, as the shares each participant receives in the scheme, a special point in Γ . The points of π and l will represent the shares distributed to the senior tellers and vice presidents and a point P will represent the secret. We will describe a method for distributing the shares in a projective 4-space so that only certain predetermined subsets of participants can calculate the secret.

1.3 Using Projective Geometry to Construct A Secret Sharing Scheme for a Bank

We are now ready to examine the relationship between the bank situation and some planes and lines in a projective 4-space. In both Design A and Design B, we would like the secret to be represented by a special point, P , in a finite projective plane, V_d in Γ . The only information available about P to the senior tellers and vice presidents is that P is represented by a point in V_d . V_d is often referred to as the domain variety and is generally public knowledge. The shares belonging to the senior tellers and the vice presidents

can be represented by specially selected points in Γ . By carefully selecting the points that we pick to represent shares, we can alter the relationships between l and V_d as well as l , π and V_d to create a geometric interpretation of the secret sharing schemes associated with the bank problem.

In Design A, the secret sharing scheme that we seek to develop is sometimes referred to as a two-level concurrence scheme. A two-level concurrence scheme requires concurrence of the participants in at least one of the two levels before a controlled action can take place. In this instance, the controlled action is the pooling of the shares to calculate the combination to the bank vault. One concurrence level consists of the bank vice presidents and the other concurrence level consists of the senior tellers. Any two points representing the shares of the vice presidents will define a line $l \in \Gamma$ that intersects V_d in only point P . Any three points representing the shares of the senior tellers should define a plane $\pi \in \Gamma$ that intersects V_d in only point P . In order to have this property in the latter case we must insure that no three of these points are collinear. For, if those points were collinear, they would only define a line and not the desired plane π that we require them to form.

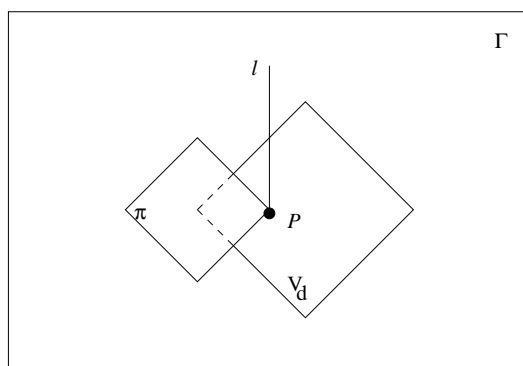


Figure 1.1. A Geometric Representation

Suppose the line l formed by two shares belonging to vice presidents intersects the plane π formed by the three shares belonging to senior tellers in exactly one point. Also, suppose that π and l both intersect V_d at the point P . Then necessarily, the intersection of π and l is P . This is the situation as described in Design A. One point is not enough information to generate a line and two points are not enough information to generate a plane. So, if l is not contained in π and only one vice president and two senior tellers come to work, then there will not be enough information among the three participants to calculate the secret.

To avoid this situation in Design A, we created a new design, Design B, having a stronger relationship between l and π other than their intersection being only P . If l and π intersect at more than one point, then l must lie in the plane π . Just as in Design A, l and π both need to intersect V_d in the point P . Since P is a point that represents the secret, the coordinates that represent P are unknown to the senior tellers and vice presidents. Just one vice president alone does not have enough information to generate a line that intersects V_d at P , since two points are required to generate a line. Similarly, any two senior tellers do not have enough information to generate a plane that intersects V_d at the point P , since three points are required to generate a plane. Furthermore, for this to be a perfect design, i.e., one in which no set of shares other than the pre-determined ones can be combined to obtain the secret, no pair of the points in π belonging to the senior tellers can be collinear with P .

For three senior tellers to be able to pool their shares and calculate the secret, it is necessary for the points representing the shares belonging to

the senior tellers to have the property that they are not collinear and all lie in the same plane, π . Thus, these points are constrained to lie on an oval.

The points representing the shares of the vice presidents must lie on a line that intersects V_d at P . Since we are adding the new restriction that a vice president and any two senior tellers have the ability to pool their shares and calculate the secret, we need the points representing the shares belonging to the vice presidents to also lie in π . In order for any vice president to be able to calculate the secret with only two senior tellers, any pair of points in π given to senior tellers may not be collinear with any point on l belonging to any of the vice presidents. With these restrictions, we can be assured that one vice president and any pair of senior tellers can calculate the secret while at the same time insuring that no pair of senior tellers can calculate the secret alone. Figure 1.2 illustrates this concept.

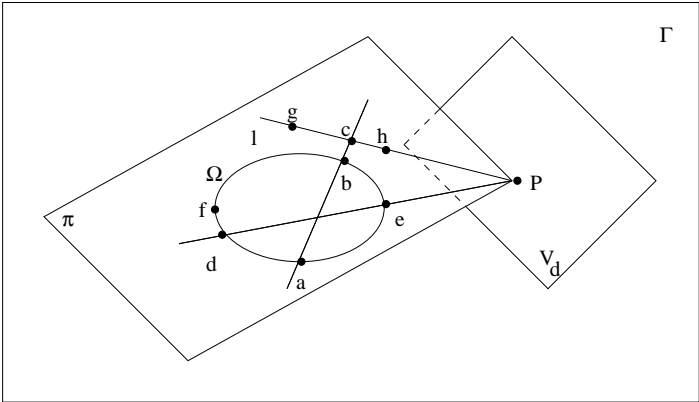


Figure 1.2. Another Geometric Representation

In Figure 1.2, we have a geometric representation of a possible way to distribute the shares. Suppose that a and b are used as shares, then a third

share, say c , collinear with a and b , could not be used in conjunction with a and b . If this happened, then these three shares would generate a line instead of the desired plane necessary to recover P . Any three shares distributed to the senior tellers should not be collinear, since these points could not determine a plane. It is for this reason that we require that the shares belonging to the senior tellers lie on an oval of π .

An example of a geometric perfect secret sharing scheme for Design B would be to let the shares belonging to the vice presidents be represented by the points g and h and the shares belonging to the senior tellers be represented by the points a , d , and f . Thus, the two vice presidents could calculate a line intersecting V_d at P , and the three senior tellers could calculate the plane π intersecting V_d at P , while any vice president and two senior tellers could also calculate this plane intersecting V_d at P .

2. Sharply Focused Sets of lines in $PG(2,q)$

2.1 The Relationship Between Sharply Focused Sets and Secret Sharing Schemes for a Bank

In the previous bank illustration, the president of a bank does not trust any individual with the combination to the vault. A system was designed that would allow certain subsets of the employees to open the vault, while other subsets were not able to open the vault. For instance, one vice president and two senior tellers could open the vault, but one vice president and one senior teller could not. The system that was designed in Chapter 1 to accommodate the president's wishes had strict restrictions on what type of points could represent the shares belonging to the senior tellers and vice presidents. What happens to our design of a perfect secret sharing scheme, when the president adds more employees? We are interested in maximizing the number of shares that can be distributed in π , so that an efficient design can be constructed for any number of employees, such that:

- any two vice presidents can combine their shares to calculate the secret,
- any three senior tellers can combine their shares to calculate the secret, and
- any one vice president and any two of the senior tellers can combine their shares to calculate the secret.

Since any line in π has $q + 1$ points, there are at most q points available to use as shares for the vice presidents, since one point of the line must be used to represent the secret. In a projective plane of odd order, there are at most $q + 1$ points with the property that no three of the points are collinear and these $q + 1$ points form an oval, Ω . Points of Ω are ideal choices to represent the shares belonging to the senior tellers. In the bank illustration, it was necessary that no pair of points in π belonging to the senior tellers be collinear with P . Also, for any vice president and any two senior tellers to be able to pool their shares to calculate the secret, it was necessary for the two shares belonging to the senior tellers not be collinear with the share belonging to the vice president. Out of the $q + 1$ points on l and the $q + 1$ points on the oval, how many can be used as shares so that the incidences mentioned above are avoided?

Any two shares given to the senior tellers determine a secant line of Ω that intersects l in a point. We would like to determine the subsets of the $q + 1$ points of Ω whose secants intersect l in the smallest number of points. Such subsets will provide the greatest number of points for use as shares for the vice presidents. Let K be a subset of Ω with k points. There are $\binom{k}{2}$ distinct secants formed by points of K . Let x represent the number of points at which these secants intersect l . Observe that, for a fixed point on l , there are at most $\lfloor \frac{k}{2} \rfloor$ secants of K that contain this point. Clearly, $x \lfloor \frac{k}{2} \rfloor \geq \binom{k}{2}$. If $k = 2m + 1$, for some m , the minimum value of x consistent with this inequality is k , but if $k = 2m$, $k - 1$ is the minimum number of shares that may not be distributed to the vice presidents. The lower bound of $k - 1$ can only be achieved under

special circumstances, which leads us to the following definition. A set, \mathcal{K} , of k points no three collinear in a finite projective plane $\pi = \text{PG}(2, q)$ is said to be *sharply focused* on a line l if the $\binom{k}{2}$ distinct lines defined by pairs of the points of \mathcal{K} intersect l in only k distinct points [6]. By having the shares belonging to the senior tellers be focused on as few points as possible on l , more shares can be distributed. That is, the remaining points on l (other than P) are then eligible to be used as shares for vice presidents.

2.2 Coordinate Representation of Points and Lines in $\text{PG}(2, q)$

Before we develop a construction for finding sharply focused sets and present examples, we need a coordinate representation of points and lines in a projective plane. Let $\mathcal{F} = \text{GF}(p^n)$ be a finite field of order p^n , p a prime and define π to be the projective plane, $\text{PG}(2, p^n)$. Then the points of π can be represented by ordered triples of elements from \mathcal{F} , with not all of the coordinates being zero. For instance, a point $P \in \pi$ can be represented by (x_1, x_2, x_3) where $x_i \in \mathcal{F}$ and at least one $x_i \neq 0$. Two points (x_1, x_2, x_3) and (y_1, y_2, y_3) are said to be equivalent if there is a scalar $\alpha \in \mathcal{F}$, $\alpha \neq 0$, such that $x_i = \alpha y_i$ for $i = 1, 2, 3$. So that any point in π can be represented in the form $(x_1, x_2, 1)$, $(1, x_2, 0)$, or $(0, 1, 0)$ where 1 is the identity of \mathcal{F} [1].

The lines in π are defined in the same manner as the points but instead of using ordinary parenthesis, we use square brackets. So that if l is a line of π , $l = [x_1, x_2, x_3]$ with not all $x_i = 0$. Two lines, $[x_1, x_2, x_3]$ and $[y_1, y_2, y_3]$ are equivalent if there is some scalar $\alpha \in \pi$, $\alpha \neq 0$, such that $x_i = \alpha y_i$ for $i = 1, 2, 3$. A point, (a, b, c) , and a line, $[x, y, z]$, are incident

if and only $ax + by + cz = 0$. For $m, x, y, k \in \mathcal{F}$ we can represent lines in our projective plane as equations of lines used in the Euclidean Plane. The line $y = mx + b$ can be written as $[m, -1, b]$ and consists of all points of the form $(x, mx + b, 1)$ as well as the point $(1, m, 0)$. The line $x = k$ has the form $[-1, 0, k]$ and consists of all points represented by $(k, y, 1)$ and $(0, 1, 0)$. The line $[0, 0, 1]$, also referred to as *the line at infinity*, contains all points represented by $(1, x, 0)$ [1].

2.3 Construction of Sharply Focused Sets in $\text{PG}(2, q)$

We now develop the construction used in [6] to create sharply focused sets in $\text{PG}(2, q)$ with q odd.

Let Ω be an arbitrary conic in $\pi = \text{PG}(2, q)$, q odd and l either an exterior line or a secant line of Ω . A *conjugate pair* of points on Ω with respect to the line l are two points A and B , such that the tangent lines to Ω at A and B both intersect l in the same point. If l is an exterior line to Ω , then these conjugate pairs are determined by first computing the tangent line equation for each point on Ω . These $q + 1$ tangent lines intersect l in exterior points and will lie two at a time on each exterior point of l . If l is a secant line to Ω , then l and Ω share two points. Disregarding these two points, the remaining $q - 1$ points of Ω can be classified into conjugate pairs by the same method used when l was an exterior line. In the process of identifying conjugate pairs of points on Ω , we identify all the exterior points on l , so that the remaining points on l must be interior points.

The secant/tangent incidence table is the main tool used to identify sharply focused sets corresponding to l . This is a square table whose rows and columns are indexed by points on Ω , not on l , and whose entries are indexed by points on l , not on Ω . More specifically, let i and j be two points on $\Omega \setminus l$. If $i \neq j$, then these two points determine a secant line that intersects l at the point in the (i, j) position of the table. Similarly, if $i = j$, then this point has a tangent line that intersects l at the point in the (i, i) position of the table. For the ease of finding sharply focused sets, points of Ω will be listed by conjugate pairs in the table.

To look at specific examples, we will make several choices for the oval as well as the line on which this oval is to be sharply focused. First we choose for our arbitrary oval the specific conic,

$$\Omega = \{(j, j^2, 1) \mid j \in \text{GF}(q)\} \cup \{(0, 1, 0)\}.$$

The exterior and secant lines that we will be dealing with in the examples consist of the set of points in π that satisfy the equation $y = c$, $c \in \text{GF}(q)$ along with the point $(1, 0, 0)$. This line, l , will be referred to as “ $y = c$ ”. If c is a square in $\text{GF}(q)$, then this will be a secant line to Ω , since l and Ω will have two points in common. If c is not a square, then this will be an exterior line to Ω . For simplicity, we will use a compact notation to represent points of Ω as well as points of l . The point $(0, 1, 0) \in \Omega$ will be represented by \bar{a} and the number \bar{j} will indicate the point $(j, j^2, 1) \in \Omega$. Similarly, the point $(1, 0, 0) \in l$ will be represented with a and the number i will indicate the point $(j, c, 1)$ of l .

2.4 Two Examples with $q = 11$

The following two examples for $q = 11$ help to clarify the procedure and also show how the secant/tangent incidence tables are used to obtain sharply focused sets.

Example 2.4.1 Let $q = 11$ and, since 2 is not a square in $\text{GF}(11)$, let l be the exterior line to Ω are given by $y = 2$. Then the six exterior points of l with respect to Ω , $a, 6, 5, 0, 4, 7$, correspond to the following conjugate pairs of points on Ω : $\{\bar{a}, \bar{0}\}$, $\{\bar{5}, \bar{7}\}$, $\{\bar{6}, \bar{4}\}$, $\{\bar{3}, \bar{8}\}$, $\{\bar{9}, \bar{10}\}$, and $\{\bar{1}, \bar{2}\}$.

	\bar{a}	$\bar{0}$	$\bar{5}$	$\bar{7}$	$\bar{6}$	$\bar{4}$	$\bar{3}$	$\bar{8}$	$\bar{9}$	$\bar{10}$	$\bar{1}$	$\bar{2}$
\bar{a}	a	0	5	7	6	4	3	8	9	10	1	2
$\bar{0}$	0	a	7	5	4	6	8	3	10	9	2	1
$\bar{5}$	5	7	6	4	a	0	9	10	1	2	3	8
$\bar{7}$	7	5	4	6	0	a	10	9	2	1	8	3
$\bar{6}$	6	4	a	0	5	7	1	2	3	8	9	10
$\bar{4}$	4	6	0	a	7	5	2	1	8	3	10	9
$\bar{3}$	3	8	9	10	1	2	0	a	7	5	4	6
$\bar{8}$	8	3	10	9	2	1	a	0	5	7	6	4
$\bar{9}$	9	10	1	2	3	8	7	5	4	6	0	a
$\bar{10}$	10	9	2	1	8	3	5	7	6	4	a	0
$\bar{1}$	1	2	3	8	9	10	4	6	0	a	7	5
$\bar{2}$	2	1	8	3	10	9	6	4	a	0	5	7

Table 2.1. The Incidence Table for $q = 11$ and l an Exterior Line

Notice that every 2×2 block in Table 2.1 contains either exterior points of l or interior points of l , but not both. Also, observe that this table can be partitioned into four 6×6 blocks, where the two 6×6 blocks that constitute the main diagonal contain only exterior points and the two 6×6 blocks that constitute the off diagonal contain only interior points of l .

We are searching for a set of k points on Ω whose secant and tangent

lines intersect l in exactly k points. We start the search for sharply focused sets by taking a closer look at the two 6×6 blocks that lie on the main diagonal of the table. The block that appears in the upper right corner of the table contains only the six exterior points of l and is created from the secant and tangent lines generated by three distinct conjugate pairs of elements in Ω , namely $\{\bar{a}, \bar{0}\}$, $\{\bar{5}, \bar{7}\}$, and $\{\bar{6}, \bar{4}\}$. Similarly, the block that appears in the lower right corner of the table also contains only the six exterior points of l . This block is created from the secant and tangent lines generated by the three other distinct conjugate pairs of elements in Ω , $\{\bar{3}, \bar{8}\}$, $\{\bar{9}, \bar{10}\}$, and $\{\bar{1}, \bar{2}\}$. We see that the two sets $\mathcal{K}_1 = \{\bar{a}, \bar{0}, \bar{5}, \bar{7}, \bar{6}, \bar{4}\}$ and $\mathcal{K}_2 = \{\bar{3}, \bar{8}, \bar{9}, \bar{10}, \bar{1}, \bar{2}\}$ are both sharply focused on the six exterior points of l .

We can use certain elements from the three conjugate pairs that generate each 6×6 block on the diagonal of the table to create sharply focused sets of size three. Let \mathcal{K}_1 and \mathcal{K}_2 be the two sets of points on Ω whose elements are the first elements in each conjugate pair and the second elements in each conjugate pair, respectively. Then we have that $\mathcal{K}_1 = \{\bar{a}, \bar{5}, \bar{6}\}$ and $\mathcal{K}_2 = \{\bar{0}, \bar{7}, \bar{4}\}$. The secant and tangent lines created from \mathcal{K}_1 intersect the points on l that lie in the $(1, 1)$ -position of each 2×2 subblock. Since there are only 3 points of l in each corner of the 2×2 subblocks, \mathcal{K}_1 is sharply focused on the points a , 5, and 6 of l . A similar inspection with \mathcal{K}_2 , shows that this set is sharply focused on the points 0, 7, and 4 of l .

Two more sharply focused sets of size six can be created in a similar fashion to the sharply focused sets of size three that were created. Let $\mathcal{K}_1 = \{\bar{a}, \bar{5}, \bar{6}, \bar{3}, \bar{9}, \bar{1}\}$ and $\mathcal{K}_2 = \{\bar{0}, \bar{7}, \bar{4}, \bar{8}, \bar{10}, \bar{2}\}$ be sets constructed from extracting

either the first or second elements in each conjugate pair listed across the top row of the table. Then, by examining the $(1, 1)$ -position of each 2×2 subblock of the table, we can see that \mathcal{K}_1 is sharply focused on the points $a, 5, 6, 3, 9$, and 1 of l . Similarly, by examining the $(2, 2)$ -entry of each 2×2 subblock of the table, we see that \mathcal{K}_2 is sharply focused on the points $0, 7, 4, 8, 10$, and 2 .

For the final search for sharply focused sets, we will examine corresponding 2×2 subblocks in each of the four 6×6 blocks. More specifically, for $i = 1, 2, 3$, we want to examine the blocks of size four created from the i^{th} conjugate pair and the $(3 + i)^{\text{th}}$ conjugate pair of points on Ω listed across the top of the table.

The secant and tangent lines generated by the conjugate pairs, $\{\bar{a}, \bar{0}\}$ and $\{\bar{3}, \bar{8}\}$ intersect l in points that lie in the four 2×2 subblocks located in the upper left corner of each of the 6×6 blocks. Since these four 2×2 subblocks contain only four points of l , these two conjugate pairs form a sharply focused set of four points.

Similarly, the two conjugate pairs, $\{\bar{5}, \bar{7}\}$, and $\{\bar{9}, \bar{10}\}$ generate secant and tangent lines whose intersections with l are the points located in the 2×2 subblocks located in the center of each 6×6 block. Since these four 2×2 subblocks contain only four points of l , the two conjugate pairs of points on Ω form a sharply focused set of size four.

A final sharply focused set of size four can be created from the remaining two conjugate pairs of the table. The pairs, $\{\bar{6}, \bar{4}\}$ and $\{\bar{1}, \bar{2}\}$ have secant and tangent lines that intersect l in exactly four points. The points of intersection are in the 2×2 subblocks that are located in the bottom right

corner of each 6×6 block. Thus, these two conjugate pairs also form a sharply focused set of size four.

Thus, by inspecting the table, we have found sharply focused sets of sizes 6, 4, and 3. The sets of six points $\{\bar{a}, \bar{0}, \bar{5}, \bar{7}, \bar{6}, \bar{4}\}$ and $\{\bar{3}, \bar{8}, \bar{9}, \bar{10}, \bar{1}, \bar{2}\}$ of Ω are both sharply focused on the points $a, 0, 5, 7, 6,$ and 4 of l . The sets $\{\bar{a}, \bar{5}, \bar{6}, \bar{3}, \bar{9}, \bar{1}\}$ and $\{\bar{0}, \bar{7}, \bar{4}, \bar{8}, \bar{10}, \bar{2}\}$ are sharply focused on $a, 5, 6, 3, 9,$ and 1 of l and $0, 7, 4, 8, 10,$ and 2 of l respectively. The sets of four points $\{\bar{a}, \bar{0}, \bar{3}, \bar{8}\}, \{\bar{5}, \bar{7}, \bar{9}, \bar{10}\},$ and $\{\bar{6}, \bar{4}, \bar{1}, \bar{2}\}$ of Ω are sharply focused on the points $a, 0, 3, 8,$ the points $6, 4, 1, 2,$ and the points $5, 7, 9, 10$ of l , respectively. The sets of three points $\{\bar{a}, \bar{5}, \bar{6}\}$ and $\{\bar{0}, \bar{7}, \bar{4}\}$ of Ω are sharply focused on the points $a, 5,$ and 6 of l , while the sets of points $\{\bar{3}, \bar{9}, \bar{1}\}$ and $\{\bar{8}, \bar{10}, \bar{2}\}$ are sharply focused on the points $0, 7,$ and 4 of l .

Example 2.4.2 Again, let $q = 11$ but instead of using the exterior line $y = 2$ to Ω , we use a secant line in the search for sharply focused sets. Since 5 is a square in $\text{GF}(11)$, let l be the secant line given by $y = 5$. Since l is a secant line to Ω , the two points that lie on both l and Ω will be omitted from the table. The five exterior points of l with respect to Ω , $a, 3, 6, 5, 8,$ have the corresponding conjugate pairs of points on Ω : $\{\bar{a}, \bar{0}\}, \{\bar{5}, \bar{1}\}, \{\bar{3}, \bar{9}\}, \{\bar{8}, \bar{2}\},$ and $\{\bar{6}, \bar{10}\}.$

Since we have an odd number of conjugate pairs, this table cannot be divided into four subblocks as was done for the previous example. Notice that every 2×2 block in this table contains exterior points of l on the diagonal and interior points of l on the off diagonal.

We can find sharply focused sets of size five by conducting a search

	\bar{a}	$\bar{0}$	$\bar{5}$	$\bar{1}$	$\bar{3}$	$\bar{9}$	$\bar{8}$	$\bar{2}$	$\bar{6}$	$\bar{10}$
\bar{a}	a	0	5	1	3	9	8	2	6	10
$\bar{0}$	0	a	1	5	9	3	2	8	10	6
$\bar{5}$	5	1	3	9	8	2	6	10	a	0
$\bar{1}$	1	5	9	3	2	8	10	6	0	a
$\bar{3}$	3	9	8	2	6	10	a	0	5	1
$\bar{9}$	9	3	2	8	10	6	0	a	1	5
$\bar{8}$	8	2	6	10	a	0	5	1	3	9
$\bar{2}$	2	8	10	6	0	a	1	5	9	3
$\bar{6}$	6	10	a	0	5	1	3	9	8	2
$\bar{10}$	10	6	0	a	1	5	9	3	2	8

Table 2.2. The Incidence Table for $q = 11$ and l a Secant Line

similar to that in the previous example. Let $\mathcal{K}_1 = \{\bar{a}, \bar{5}, \bar{3}, \bar{8}, \bar{6}\}$ and $\mathcal{K}_2 = \{\bar{0}, \bar{1}, \bar{4}, \bar{2}, \bar{10}\}$ be sets constructed from extracting either the first or second elements in each conjugate pair listed across the top row of the table. Then, by examining the $(1, 1)$ -entry of each 2×2 subblock of the table, we can see that \mathcal{K}_1 is sharply focused on the points $a, 5, 3, 8,$ and 6 of l . Similarly, by examining the $(2, 2)$ -entry of each 2×2 subblock of the table, we see that \mathcal{K}_2 is also sharply focused on the points $a, 5, 3, 8,$ and 6 of l .

By inspecting the table, it can be seen that sharply focused sets of size 5 exist and can be obtained by creating a set that contains exactly one point from each conjugate pair of Ω . The sets $\{\bar{a}, \bar{5}, \bar{3}, \bar{8}, \bar{6}\}$ and $\{\bar{0}, \bar{1}, \bar{9}, \bar{2}, \bar{10}\}$ of points on Ω are both sharply focused on the five points $a, 5, 3, 8,$ and 6 of l .

Thus, for $q = 11$, there exist sharply focused sets of sizes 3, 4, 5, and 6.

2.5 Two Examples with $q = 13$

Next, we examine the various secant/tangent incidence tables for $q = 13$ when l is an exterior line and a secant line.

Example 2.5.1

Let $q = 13$ and since 2 is not a square in $\text{GF}(13)$, let l be the exterior line to Ω given by $y = 2$. Then the seven exterior points $\{a, 3, 6, 11, 1, 4, 8\}$ of l with respect to Ω have the corresponding conjugate pairs of points on Ω : $\{\bar{a}, \bar{0}\}$, $\{\bar{1}, \bar{2}\}$, $\{\bar{3}, \bar{5}\}$, $\{\bar{4}, \bar{7}\}$, $\{\bar{6}, \bar{9}\}$, $\{\bar{8}, \bar{10}\}$, and $\{\bar{11}, \bar{12}\}$.

	\bar{a}	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{5}$	$\bar{4}$	$\bar{7}$	$\bar{6}$	$\bar{9}$	$\bar{8}$	$\bar{10}$	$\bar{11}$	$\bar{12}$
\bar{a}	a	0	1	2	3	5	4	7	6	9	8	10	11	12
$\bar{0}$	0	a	2	1	5	3	7	4	9	6	10	8	12	11
$\bar{1}$	1	2	3	5	4	7	6	9	8	10	11	12	a	0
$\bar{2}$	2	1	5	3	7	4	9	6	10	8	12	11	0	a
$\bar{3}$	3	5	4	7	6	9	8	10	11	12	a	0	1	2
$\bar{5}$	5	3	7	4	9	6	10	8	12	11	0	a	2	1
$\bar{4}$	4	7	6	9	8	10	11	12	a	0	1	2	3	5
$\bar{7}$	7	4	9	6	10	8	12	11	0	a	2	1	5	3
$\bar{6}$	6	9	8	10	11	12	a	0	1	2	3	5	4	7
$\bar{9}$	9	6	10	8	12	11	0	a	2	1	5	3	7	4
$\bar{8}$	8	10	11	12	a	0	1	2	3	5	4	7	6	9
$\bar{10}$	10	8	12	11	0	a	2	1	5	3	7	4	9	6
$\bar{11}$	11	12	a	0	1	2	3	5	4	7	6	9	8	10
$\bar{12}$	12	11	0	a	2	1	5	3	7	4	9	6	10	8

Table 2.3. The Incidence Table for $q = 13$ and l an Exterior Line

This table is similar to the table in Example 2.2, since the seven exterior points of l lie on the main diagonal of each 2×2 subblock of the incidence table and the seven interior points of l lie on the off diagonal of each 2×2 subblock of the table. By inspecting the table and conducting our search in a similar fashion to the search in Example 2.2, it can be seen that two

sharply focused sets of size 7 exist. Namely, the sets $\{\bar{a}, \bar{1}, \bar{3}, \bar{4}, \bar{6}, \bar{11}, \bar{8}\}$ and $\{\bar{0}, \bar{2}, \bar{5}, \bar{7}, \bar{9}, \bar{10}, \bar{12}\}$ of points from Ω are both sharply focused on the points $a, 1, 3, 4, 6, 8,$ and 11 of l .

Example 2.5.2

Again, let $q = 13$ but instead of using the exterior line $y = 2$ to Ω , we use a secant line to aid in the search for sharply focused sets. Since 3 is a square in $\text{GF}(13)$, let l be the secant line given by $y = 3$. Then, the six exterior points $a, 8, 5, 0, 2, 11$ of l with respect to Ω have the corresponding points as conjugate pairs: $\{\bar{a}, \bar{0}\}, \{\bar{5}, \bar{10}\}, \{\bar{8}, \bar{2}\}, \{\bar{6}, \bar{7}\}, \{\bar{3}, \bar{1}\},$ and $\{\bar{12}, \bar{10}\}$.

	\bar{a}	$\bar{0}$	$\bar{5}$	$\bar{11}$	$\bar{8}$	$\bar{2}$	$\bar{6}$	$\bar{7}$	$\bar{3}$	$\bar{1}$	$\bar{12}$	$\bar{10}$
\bar{a}	a	0	5	11	8	2	6	7	3	1	12	10
$\bar{0}$	0	a	11	5	2	8	7	6	1	3	10	12
$\bar{5}$	5	11	8	2	a	0	3	1	12	10	6	7
$\bar{11}$	11	5	2	8	0	a	1	3	10	12	7	6
$\bar{8}$	8	2	a	0	5	11	12	10	6	7	3	1
$\bar{2}$	2	8	0	a	11	5	10	12	7	6	1	3
$\bar{6}$	6	7	3	1	12	10	0	a	11	5	2	8
$\bar{7}$	7	6	1	3	10	12	a	0	5	11	8	2
$\bar{3}$	3	1	12	10	6	7	11	5	2	8	0	a
$\bar{1}$	1	3	10	12	7	6	5	11	8	2	a	0
$\bar{12}$	12	10	6	7	3	1	2	8	0	a	11	5
$\bar{10}$	10	12	7	6	1	3	8	2	a	0	5	11

Table 2.4. The Incidence Table for $q = 13$ and l a Secant Line

Observe that we can partition this table into four 9×9 blocks. Also, notice that in this table pairs of the exterior points lie in the 2×2 blocks on the main diagonal, and pairs of the interior points lie in the 2×2 blocks on the off diagonal. This table has a similar structure to the table in Example 2.1 and the search for sharply focused sets can be conducted in a similar fashion.

By inspecting the table, it can be seen that there are sharply focused sets of size 6, 4, and 3. The sets $\{\bar{a}, \bar{5}, \bar{8}, \bar{6}, \bar{3}, \bar{12}\}$ and $\{\bar{0}, \bar{11}, \bar{2}, \bar{7}, \bar{1}, \bar{10}\}$ of points on Ω are both sharply focused on the points $a, 5, 8, 6, 3,$ and 12 of l . The sets $\{\bar{a}, \bar{5}, \bar{8}, \bar{6}, \bar{3}, \bar{12}\}$ and $\{\bar{0}, \bar{11}, \bar{2}, \bar{7}, \bar{1}, \bar{10}\}$ are both sharply focused on the points $a, 5, 8, 6, 3,$ and 12 of l . The sets $\{\bar{a}, \bar{0}, \bar{6}, \bar{7}\}, \{\bar{5}, \bar{11}, \bar{3}, \bar{1}\},$ and $\{\bar{8}, \bar{2}, \bar{12}, \bar{10}\}$ of points of Ω are sharply focused on the points $a, 0, 6, 7,$ the points $8, 2, 12, 10,$ and the points $5, 11, 3,$ and 1 of l respectively. The two sets $\{\bar{a}, \bar{5}, \bar{8}\}$ and $\{\bar{0}, \bar{11}, \bar{2}\}$ of points on Ω are both sharply focused on the points $a, 5,$ and 8 of l . Similarly, the two sets $\{\bar{6}, \bar{3}, \bar{12}\}$ and $\{\bar{7}, \bar{1}, \bar{10}\}$ are both sharply focused on the points $0, 11,$ and 2 of l . Thus, for $q = 13,$ there exists sharply focused sets of size: 3, 4, 6, and 7.

2.6 Structure of the Incidence Tables

The structure of the incidence tables in Examples 2.1-2.4 can be somewhat explained. The 2×2 blocks of each incidence table are always of the form

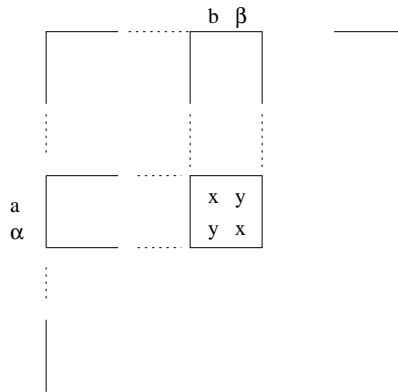


Figure 2.1. Structure of the Incidence Tables

where the nature of x and y (with respect to Ω) are determined by whether $q \equiv \pm 1 \pmod{4}$. The points b, β and a, α on Ω are conjugate pairs with respect to some line l . That is, the tangents through both a and α intersect l at the same point. The same is true for b and β . If a secant through a and b intersects l at x then so does the secant through α and β . Similarly, if a secant through a and β intersects l at y then so does the secant through α and b [6].

The secant/tangent incidence tables will be one of two basic designs, depending on whether $q \equiv \pm 1 \pmod{4}$ and whether l is a secant line or an exterior line to Ω .

- If $q \equiv 1 \pmod{4}$ and l is an exterior line to Ω , then there will be an odd number of conjugate pairs in Ω . Each 2×2 block of the incidence table will have the exterior points of l on the diagonal and interior points of l lie on the off diagonal. The same structure occurs for $q \equiv -1 \pmod{4}$ and l a secant line to Ω .
- If $q \equiv -1 \pmod{4}$ and l is an exterior line, then there will be an even number, n , of conjugate pairs in Ω with respect to l . The table can be partitioned into four sub-blocks each of size $n \times n$. If the conjugate pairs of Ω are arranged appropriately, then the two sub-blocks that lie on the main diagonal of the table consist of 2×2 blocks of exterior points of l and the two sub-blocks on the off diagonal consist of 2×2 blocks of interior points of l . The same structure also occurs for $q \equiv 1 \pmod{4}$ and l a secant line to Ω .

2.7 General Method

After creating the secant/tangent table, it is a matter of examining this table to determine the sharply focused sets. For small values of q , we can obtain subsets of Ω that are sharply focused on a line l by using the following methods:

Suppose $q \equiv 1 \pmod{4}$ and l is an exterior line or $q \equiv -1 \pmod{4}$ and l is a secant line. Then depending on the congruence of q , we can construct sharply focused sets of size either $\frac{n+1}{2}$ or $\frac{n-1}{2}$, where n is the odd number of conjugate pairs. To construct two sharply focused sets of the above size, we take either all the first elements of each conjugate pair listed in the incidence table or all the second elements of each conjugate pair listed in the table.

If $q \equiv 1 \pmod{4}$ and l is a secant line or $q \equiv -1 \pmod{4}$ and l is an exterior line, then there are several ways to create sharply focused sets of various sizes. Let n be the even number of conjugate pairs created in the construction of the table. To create two sharply focused sets of size $\frac{n}{2}$ we use the first $\frac{n}{2}$ conjugate pairs in the incidence table to construct one set and the remaining $\frac{n}{2}$ conjugate pairs in the incidence table to construct another set. This creates two sets of $\frac{n}{2}$ elements of Ω that are sharply focused on all the exterior points of l . To create sharply focused sets of size 4, we use only two conjugate pairs. For $1 \leq k \leq \frac{n}{2}$, the k^{th} conjugate pair in the incidence table and the $(\frac{n}{2} + k)$ conjugate pair in the incidence table will produce a sharply focused set of size 4.

In $\text{PG}(2, q)$, q odd, there exists sharply focused sets of size k , where k is 3, 4 or a proper divisor of $q + 1$ and $q - 1$ other than 2. Simmons [6] offers no

proof that these are the only possible sizes of sharply focused sets, in the next chapter we provide a proof that this is always the case for this construction.

3. Proving the Divisibility Argument

The restrictions imposed on the length of Simmons' paper [6] did not allow him to provide proofs for statements concerning the secant/tangent incidence tables and the division property that sizes of sharply focused sets must divide either $q + 1$ or $q - 1$. We shall provide the proofs that the size of a sharply focused set constructed by his method must divide $q + 1$ or $q - 1$.

3.1 A Relationship Between Points of Ω and Points of l

Let $\mathcal{F} = \text{GF}(q)$, where q is an odd prime power, be a field and let a be a symbol not in \mathcal{F} . The construction used to create sharply focused sets in $\text{PG}(2, q)$ used the specific conic $\Omega = \{(j, j^2, 1) | j \in \text{GF}(q)\} \cup \{(0, 1, 0)\}$, where the points of Ω are denoted by \bar{j} and \bar{a} . When c is not a square in $\text{GF}(q)$, l is the exterior line $y = c$ whose points $\{(j, c, 1) | j \in \text{GF}(q)\} \cup \{(1, 0, 0)\}$ are denoted by j and a . The points of Ω are identified with the elements of $\mathcal{F} \cup \{a\}$ by $\bar{x} \leftrightarrow x$ and the points of l are identified by $x \leftrightarrow x$. By means of these identifications, the secant/tangent incidence table defines a binary operation on $\mathcal{F} \cup \{a\}$, which is given by:

$$i \oplus j = \begin{cases} \frac{c+ij}{i+j} & \text{if } i \neq -j \\ a & \text{if } i = -j \\ i & \text{if } j = a \\ j & \text{if } i = a. \end{cases}$$

Proof: Let $\bar{i} = (i, i^2, 1)$ and $\bar{j} = (j, j^2, 1)$ be two points of Ω . The line through \bar{i} and \bar{j} is given by $y = (i + j)x - ij$. Note: if $i = j$ then this is a tangent line. The point of intersection of this line and l is the point whose y -coordinate is c . Setting this line equal to c and solving for x , we find that the point of intersection has first coordinate $\frac{c+ij}{i+j}$, provided $i \neq -j$. If \bar{i} is the same point as $\overline{-j}$, then the line through these points is the horizontal line given by $y = i^2$ which intersects $y = c$ at the point a .

The points \bar{i} and \bar{a} form the secant line $x = i$. The line $x = i$ intersects the line $y = c$ at the point with x -coordinate i . Similarly, the points \bar{a} and \bar{j} form the secant line $x = j$, which intersects $y = c$ at the point with x -coordinate j . ■

Thus, we have a way of relating the points of Ω to those of l by examining the relationship between the elements of $\mathcal{F} \cup \{a\}$ under the operation of \oplus . Let $\mathcal{F}^* = \mathcal{F} \cup \{a\}$. The following theorem proves that \mathcal{F}^* is a group under \oplus .

Theorem 3.1.1. $\mathcal{F}^* = \mathcal{F} \cup \{a\}$ is a group under the binary operation \oplus .

Proof: To show that \mathcal{F}^* is a group under \oplus , we need to show that the following three properties are satisfied.

- associativity: $i \oplus (j \oplus k) = (i \oplus j) \oplus k \forall i, j, k \in \mathcal{F}^*$
- identity: there exists $e \in \mathcal{F}^*$ such that $i \oplus e = e \oplus i = i \forall i \in \mathcal{F}^*$
- inverse: for all $i \in \mathcal{F}^*$ there is a $j \in \mathcal{F}^*$ such that $i \oplus j = j \oplus i = e$.

a. (Associativity)

Case 1. Suppose $i, j, k \neq a$. Then

$$\begin{aligned}
i \oplus (j \oplus k) &= (i \oplus j) \oplus k \\
&= i \oplus \frac{c+jk}{j+k} \\
&= \frac{c + i \left(\frac{c+jk}{j+k} \right)}{i + \left(\frac{c+jk}{j+k} \right)} \\
&= \frac{c + k \left(\frac{c+ij}{i+j} \right)}{k + \left(\frac{c+ij}{i+j} \right)} \\
&= \left(\frac{c+ij}{i+j} \right) \oplus k \\
&= (i \oplus j) \oplus k.
\end{aligned}$$

Case 2. Suppose $i = a$. Then

$$\begin{aligned}
a \oplus (j \oplus k) &= j \oplus k \\
&= (a \oplus j) \oplus k.
\end{aligned}$$

The other cases involving element a are similar.

Case 3. Suppose $k = -j$. Then

$$\begin{aligned}
i \oplus (j \oplus -j) &= i \oplus a \\
&= i \\
&= i \frac{(c-j^2)}{c-j^2} \\
&= \frac{c+ij}{i+j} \oplus -j \\
&= (i \oplus j) \oplus -j.
\end{aligned}$$

Again, the remaining cases of this type are similar.

So, for any choice of $i, j, k \in \mathcal{F}^*$, associativity holds.

b. (Identity) Since $a \oplus j = j = j \oplus a$, the identity of \mathcal{F}^* is a .

c. (Inverse) Since $i \oplus -i = a = -i \oplus i$, for all $i \in \mathcal{F}^*$, the inverse of i is $-i$. ■

For c a square in $\text{GF}(q)$, the secant line l given by $y = c$ intersects Ω in the points \bar{x} and \bar{y} . Notice that in this case $\bar{x} = x$ and $\bar{y} = y$. Let \bar{i} and \bar{j} be two distinct points of Ω other than \bar{x} and \bar{y} . If the secant line through \bar{i} and \bar{j} intersects l at, say x , then since \bar{x} is also on Ω , we have three points, \bar{i} , \bar{j} , and \bar{x} that are collinear. But, since Ω is an oval, no three points are collinear and this can never happen. Now, observe that \bar{a} and a are not in the intersection of Ω and l . Since $\bar{a} = (0, 1, 0)$ of Ω is not the same as the point $a = (1, 0, 0)$ of l . Thus, \bar{a} and a will never be in the set $\Omega \cap l = \{\bar{x}, \bar{y}\}$. So, the secant/tangent incidence table is closed since the two points removed from both Ω and l do not appear anywhere in the table. We find that the set $\mathcal{F}^* \setminus \{\bar{x}, \bar{y}\}$ is closed and possesses inverses for each element as well as an identity. Thus, $\mathcal{F}^* \setminus \{\bar{x}, \bar{y}\}$ is a group under the same binary operation \oplus defined above. The proof when l a secant line is essentially the same as the proof when l is an exterior line. ■

Thus, regardless of whether l is an exterior line or a secant line, the secant/tangent incidence table of the points of Ω and l is isomorphic to the multiplication table of a group.

3.2 Sharply Focused Sets Correspond to Cosets of a Group

The next thing that we show is that sharply focused sets correspond to the cosets of \mathcal{F}^* .

Theorem 3.2.1. *Sharply focused sets constructed in this way have sizes that are divisors of $q + 1$ or $q - 1$, other than 2. Furthermore, these sharply focused sets correspond to cosets in \mathcal{F}^* .*

Proof: Let $H = \{b_1, b_2, \dots, b_k\}$ be a sharply focused set of Ω such that $|H| = k$. We want to examine the subarray whose rows and columns are indexed by the elements in H . Let c_{ij} denote the (i, j) -entry of this subarray. Since H is a sharply focused set the c_{ij} are all elements of a size k subset of \mathcal{F}^* .

Suppose $c_{rj} = c_{sj} = c$ for some r and s . This implies that the secant line determined by b_r and b_j intersects l in the same point as the secant line determined by b_s and b_j . Since c and b_j determine a unique line, this implies that b_r, b_s, b_j are all collinear. This is impossible since they are all points of an oval. Thus, no element appears twice in a column.

A similar argument shows that no element appears twice in the same row.

This implies that the subarray indexed by H under \oplus is a Latin square, a $k \times k$ array whose entries all come from a set, S , of size k , with the property that each element of S appears exactly once in each row and column of the array.

Examine

$$\begin{aligned} H \oplus -b_1 &= \{b_1 \oplus -b_1, b_2 \oplus -b_1, \dots, b_k \oplus -b_1\} \\ &= \{a, b_2 \oplus -b_1, \dots, b_k \oplus -b_1\}. \end{aligned}$$

Let the entries indexed by $H \oplus -b_1$ be d_{ij} , where

$$\begin{aligned} d_{ij} &= (b_i \oplus -b_1) \oplus (b_j \oplus -b_1) \\ &= (b_i \oplus b_j) \oplus -2b_1 \\ &= c_{ij} \oplus -2b_1. \end{aligned}$$

By adding the same constant to each of the c_{ij} 's, we obtain a set of d_{ij} 's which come from a set of k elements. The addition of a constant to all entries does not affect the property of the array of being a Latin square. Notice that

$$\begin{aligned} d_{1j} &= (b_1 \oplus -b_1) \oplus (b_j \oplus -b_1) \\ &= a \oplus (b_j \oplus -b_1) \\ &= b_j \oplus -b_1 \in H \oplus -b_1. \end{aligned}$$

Thus, each entry of the subarray indexed by $H \oplus -b_1$ is an element of $H \oplus -b_1$ since this is a Latin square. This implies that $H \oplus -b_1$ is closed under \oplus . Since Ω is finite and $H \oplus -b_1$ is closed under the operation of \oplus , $H \oplus -b_1$ is a subgroup, and so, H is a coset. Since the order of a coset is the same as the order of a subgroup, Lagrange's theorem tells us that the sizes of sharply focused sets must divide $q + 1$ or $q - 1$. ■

Although the proofs for the claims in [6] concerning the structure of the secant/tangent incidence tables can be explicitly given using the previous two theorems and some number theoretical arguments, the proofs will not be provided here.

4. Another Construction of Sharply Focused Sets

Sets

Chapter 2 was devoted to using Simmon's [6] method to construct sharply focused sets in planes of order q . We will show that there is a method of constructing sharply focused sets in planes of any prime power order, by using subplanes in $\text{PG}(2, q)$. Let Π be a projective plane and let π' be a projective plane whose points form a subset of the points of Π and which is such that every line \mathcal{L}' of π' is the intersection of π' and a line \mathcal{L} of Π . Then π' is called a *subplane* of Π [1].

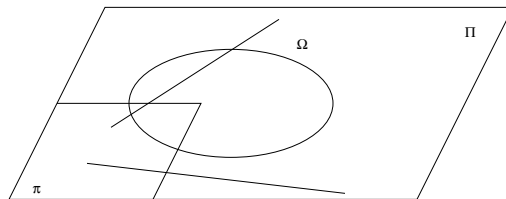


Figure 4.1. Subplane of a Projective Plane

Since we are dealing with projective planes that are constructed over finite fields we have the following useful theorem pertaining to subfields of finite fields.

Theorem. [5] *For each divisor m of n , $GF(p^n)$ has a unique subfield of order p^m . Moreover, these are the only subfields of $GF(p^n)$.* ■

4.1 Even Characteristic Preamble

One of the properties fundamental to the previous construction, with q odd, is the existence of conjugate pairs of points on an oval with respect to some line l . Recall that a conjugate pair consists of two points on an oval whose tangents intersected a given line at the same point. When p is even all tangents to the oval intersect at the same point in the plane, known as the *nucleus*. Therefore, conjugate pairs in planes of even order do not exist. If sharply focused sets are to be found in planes of even order, an alternate construction to the one provided by [6] that does not rely on conjugate pairs will need to be developed.

4.2 Existence and Construction of Sharply Focused Sets in Planes of Prime Power Order

The following theorem provides us with a new construction of sharply focused sets when q is a prime power.

Theorem 4.3.1. *In $PG(2, p^e)$, p a prime, there exists sharply focused sets of sizes $p^m + 1$, p^m , and $p^m - 1$ where m is a divisor of e .*

Proof: Let m be any divisor of e . Then $\pi = PG(2, p^m)$ is a subplane of $PG(2, p^e)$. $\mathcal{K} = \{(x, x^2, 1) \mid x \in GF(p^m)\} \cup \{(0, 1, 0)\}$ is a set of $p^m + 1$ points in π , with the property that no three are collinear. Then \mathcal{K} is sharply focused on any exterior line l of K in π . Since π is a subplane of $PG(2, p^e)$, l can be extended to a unique line l' in $PG(2, p^e)$. \mathcal{K} being sharply focused on l and l' being the extension of l in $PG(2, p^e)$ implies that \mathcal{K} is sharply focused on l' in $PG(2, p^e)$.

Now, suppose that l is a tangent line to the oval K in π at a point P , and define $S = K \setminus \{P\}$, so $|S| = p^m$. Then l is an exterior line to S and by the preceding paragraph, S is sharply focused on $l \setminus \{P\}$.

Finally, suppose that l is a secant line to the oval \mathcal{K} in π at the points P and Q , and define $\mathcal{M} = \mathcal{K} \setminus \{P, Q\}$, so that $|\mathcal{M}| = p^m - 1$. Then l is an exterior line to \mathcal{M} and by the first paragraph of the proof, \mathcal{M} is sharply focused on $l \setminus \{P, Q\}$.

Thus, in $\text{PG}(2, p^e)$ there exist sharply focused sets of sizes $p^m + 1$, p^m , and $p^m - 1$ when m is a divisor of e . ■

This theorem can be used to construct sharply focused sets in projective planes of both even and odd prime power orders. If π' is a subplane in a projective plane Π , we use the $p^m + 1$ points of a conic in Π that lie in π' to form the desired sharply focused set, \mathcal{K} , \mathcal{M} , or S , of points. Since \mathcal{K} is sharply focused on any exterior line in π' , S is sharply focused on the appropriate tangent line in π' , and \mathcal{M} is sharply focused on the appropriate secant line, we can construct sharply focused sets of sizes p^m , $p^m + 1$, and $p^m - 1$.

According to the construction method used for q , an odd prime power, in $\text{PG}(2, 25)$ we should find sharply focused sets of sizes 3, 4, 6, 8, 12, and 13. Since $\text{PG}(2, 5)$ is a subplane of $\text{PG}(2, 25)$, we can use the previous theorem to construct another sharply focused set, a set of size 5.

Define Ω to be a conic in $\text{PG}(2, 5)$ and l a tangent line to Ω at a point P . Let $S = \Omega \setminus \{P\}$ and observe that l is an exterior line to S . By Theorem 4.3.1, S is a set of 5 points sharply focused on l and therefore S is a sharply focused set of 5 points in $\text{PG}(2, 25)$.

4.3 Super Sharply Focused Sets in Planes of Even Order

All of the constructions encountered so far have focused on finding a set of k points in a projective plane and a line l so that the $\binom{k}{2}$ distinct lines defined by pairs of the points in \mathcal{K} intersect l in only k distinct points. If we restrict our focus to projective planes of only even order, then it is possible for us to construct super sharply focused sets. A *super sharply focused set* is a set of m points, no three collinear, that are sharply focused on $m - 1$ points of a line.

Let π be a plane of order 2^m with a subplane of order 2^n . Let Ω be a hyperoval, an oval together with its nucleus N , in $\text{PG}(2, 2^n)$. Ω contains $2^n + 2$ points. Let l be the secant line to Ω through any point P on Ω and N . Let $\mathcal{K} = \Omega \setminus \{P, N\}$. Then the 2^n points in \mathcal{K} generate $\binom{2^n}{2}$ distinct lines that intersect l in $2^n - 1$ points. Namely, the 2^n points of \mathcal{K} generate lines that intersect l at every point except for P and N . Thus, in projective planes of even order we can create super sharply focused sets.

There is one possible advantage for having super sharply focused sets as opposed to sharply focused sets in the creation of this particular type of secret sharing scheme. For instance, suppose the president of the bank hires temporary tellers during the holidays to help with the seasonal increase in banking transactions. Then with the addition of several new tellers, he would like to incorporate them into the current design rather than produce a new design to redistribute the shares of the combinations to the current employees as well as the new ones. In this light, it makes sense to have access to spare shares that can be distributed when new employees are hired. By using super

sharply focused sets instead sharply focused sets, we can increase the number of shares given out to the participants of the scheme by one. In this manner, super sharply focused sets are more practical than sharply focused sets.

4.4 A Sharply Focused and Super Sharply Focused Set in $\text{PG}(2,16)$

Let $\Omega = \{(i, i^2, 1) \mid i \in \text{GF}(16)\} \cup (0, 1, 0)$ be a conic in $\text{PG}(2,16)$ and α a generator of $\text{GF}(16) \setminus \{0\}$. Then $(\alpha^5)^2 = \alpha^{10}$ and $(\alpha^5)^3 = \alpha^{15} = 1$ implies that $\text{GF}(4) = \{\alpha^5, \alpha^{10}, 1, 0\} \subset \text{GF}(16)$.

Then we have that the points of $\Omega \in \text{PG}(2, 16)$ that lie in $\text{PG}(2,4)$ are $(\alpha^5, \alpha^{10}, 1)$, $(\alpha^{10}, \alpha^5, 1)$, $(0, 1, 0)$, $(1, 1, 1)$, $(0, 0, 1)$. These five points generate 10 secants and 5 tangents which intersect each other at the following points: $(0, 1, 1)$, $(0, \alpha^{10}, 1)$, $(0, \alpha^5, 1)$, $(1, 1, 0)$, $(1, 0, 1)$, $(1, \alpha^{10}, 0)$, $(\alpha^{10}, 0, 1)$, $(\alpha^{10}, \alpha^{10}, 1)$, $(\alpha^5, \alpha^5, 1)$, $(1, \alpha^5, 1)$, $(1, \alpha^{10}, 1)$, $(\alpha^5, 0, 1)$, $(1, \alpha^5, 0)$, $(\alpha^{10}, 1, 1)$, $(\alpha^5, 1, 1)$. These points are sharply focused on the lines $y = x + \alpha^5$, $y = x + \alpha^{10}$, $y = \alpha^5 x + 1$, $y = \alpha^5 x + \alpha^5$, $y = \alpha^{10} x + 1$, and $y = \alpha^{10} x + \alpha^{10}$ in $\text{PG}(2,4)$, which are exterior lines in $\text{PG}(2,4)$ and secant lines in π . So,

$$\mathcal{K} = \{(\alpha^5, \alpha^{10}, 1), (\alpha^{10}, \alpha^5, 1), (0, 1, 0), (1, 1, 1), (0, 0, 1)\}$$

is a set of five points in $\text{PG}(2,16)$ that is sharply focused on a line.

We can also obtain a sharply focused set of size 4 by following the construction given in Theorem 4.3.1. Let $\Omega = \mathcal{K}$ be defined as above and let l be a tangent line to Ω at P in $\text{PG}(2,4)$. Then $S = \Omega \setminus \{P\}$ is a sharply focused set of size 4 with respect to the tangent line l .

To obtain a super sharply focused set in $\text{PG}(2,16)$, we let Ω be the hyperoval given by $\{(\alpha^5, \alpha^{10}, 1), (\alpha^{10}, \alpha^5, 1), (0, 1, 0), (1, 1, 1), (0, 0, 1), (1, 0, 0)\}$

where $N = (1, 0, 0)$ is the nucleus. Then let l be a secant line through any of the first five points listed for Ω and N and let S be a set that contains the points of $\Omega \notin l$. Then by Theorem 4.3.1, S is sharply focused on l .

So, in $\text{PG}(2,16)$, by using the results from Theorem 4.3.1, we can construct sharply focused sets of sizes 5 and 4, as well as a super sharply focused set of size 4.

4.5 Advantages and Disadvantages of Each Construction of Sharply Focused Sets

A limiting factor to the use of subplanes for constructing sharply focused sets is the number of subplanes that can be generated to obtain a sharply focused set. For instance, in $\text{PG}(2, p^e)$, where e is a prime, then the only divisors of e are 1 and itself. In this case, the generated subplanes are the p -subplane and the whole space. In the situation where we deal with the p -subplane, we can obtain sharply focused sets of sizes $p - 1$, p , and $p + 1$. In the situation where we are only dealing with the whole space, this method does not produce any non-trivial sharply focused sets.

The construction method provided in [6] relies on the ability to find conjugate pairs of an oval with respect to either an exterior line or a secant line in the plane. This method does not work in planes of even order, since conjugate pairs no longer exist. However, in projective planes of even order, we can always produce super sharply focused sets that do not exist in planes of odd order.

5. Further Studies

In this thesis we have examined two types of constructions for finding sharply focused sets for use in secret sharing schemes. In this chapter, we would like to mention a few problems and questions that have not been solved. These remain to be studied further.

- This paper offers two different constructions for finding sharply focused sets. Whether or not there exist other constructions of sharply focused sets still needs to be addressed.
- The construction provided by Simmons [6] requires the use of conics but the subplane construction does not. It still remains to be determined whether or not sharply focused sets based on other types of arcs in planes of even order greater than 16 exist. An exhaustive search using the Lunelli-Sce oval in $\text{PG}(2,16)$ did not find any non-trivial sharply focused sets.
- $\text{PG}(2,8)$ is the smallest case in which the subplane construction does not give a sharply focused set. An exhaustive search found no sharply focused sets in this plane, other than the trivial super-sharply focused quadrangles. Is this always the case for $\text{PG}(2,2^p)$, p a prime?

REFERENCES

- [1] A. ALBERT AND R. SANDLER, **An Introduction to Finite Projective Planes**, Holt, Rinehart, and Winston, Inc., 1968.
- [2] E. F. BRICKELL, **Some Ideal Secret Sharing Schemes**, in Lecture Notes in Computer Science, Advances in Cryptology- EUROCRYPTO '89, J. Quizquater and J. Vandewalle, eds., vol. 434, Springer-Verlag, April 1989, pp. 468–490.
- [3] H. COXETER, **Projective Geometry**, Springer-Verlag, 1987.
- [4] P. DEMBOWSKI, **Finite Geometries**, Springer-Verlag, 1968.
- [5] J. A. GALLIAN, **Contemporary Abstract Algebra**, D.C. Heath and Company, 1990.
- [6] G. SIMMONS, **Sharply Focused Sets of Lines on a Conic in $PG(2, q)$** , in *Congressus Numerantium*, vol. 73, January 1990, pp. 181–204.
- [7] D. R. STINSON, **Cryptography, Theory and Practice**, CRC Press, 1995.
- [8] W. WALLIS, **Combinatorial Designs**, Marcel Dekker Inc., 1988.