

BLOCKING SETS OF CONICS

by

Leanne D. Holder

B.S., University of Southern Mississippi, 1994

M.S., University of Colorado at Denver, 1997

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

2001

This thesis for the Doctor of Philosophy

degree by

Leanne D. Holder

has been approved

by

---

William E. Cherowitzo

---

Sylvia Lu

---

J. Richard Lundgren

---

Stanley E. Payne

---

Laurel A. Rogers

---

Date

Holder, Leanne D. (Ph.D., Applied Mathematics)

Blocking Sets of Conics

Thesis directed by Professor William E. Cherowitzo

### ABSTRACT

Traditionally, the study of *blocking sets* has been devoted to studying sets of points in a projective plane with the property that every line of the plane contains at least one point in that set. In this classical situation, we refer to a blocking set as a line blocking set. A line blocking set is said to be irreducible if no proper subset is a line blocking set. Although the study of line blocking sets takes its origins in game theory, many of the results pertaining to blocking sets of lines are due to finite geometers. Using basic properties of the plane, it is simple to show that such sets exist. Most of the research pertaining to line blocking sets consists of examining existence, structure, and obtaining bounds on the sizes of irreducible blocking sets.

Just as there are sets of points that block lines, there are sets of lines that block conics. We define a *conic blocking set* (CBS) to be a set of lines in a Desarguesian projective plane such that all conics meet these lines. This dissertation presents a study of conic blocking sets restricted to sets of concurrent lines and is divided into two parts: CBSs in planes of even characteristic, and CBSs in planes of odd characteristic. In both settings, there is a trivial proof that guarantees the existence of CBSs. There are non-trivial constructions of CBSs that rely heav-

ily on results by J. A. Thas relating to the theory of flocks of quadratic cones. An efficient algorithm is developed for finding the minimum size of CBSs. This algorithm requires working with the dualized projective plane and incorporates optimization techniques. Along with the results of the computer searches, bounds on the minimum size of CBSs are discussed.

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

Signed \_\_\_\_\_  
William E. Cherowitzo

## ACKNOWLEDGMENT

My great thanks and appreciation go to the following people. This is but a brief list of those who stuck by me and made obtaining this degree a reality. In their own special way, they have given me a different perspective on various aspects of life. I hope I can do the same for someone else one day.

*Bill Cherowitzo* - for his encouragement, guidance, and generosity, for the years of racquetball. I can't believe you survived six years of my pestering; *Allen Holder* - for being my best friend, for being my husband, for being my spine, for believing in me when I wouldn't. You are still the best thing that ever happened to me; *Tim Penttila* - for sharing your sabbatical and your dinners with me, for sitting in the car eight hours while I drive you around southern Colorado, but mostly, for the help you gave me with the work presented in this dissertation. Without it, I'd still be in school; *Dianne Daniel* - for being my mom, which pretty much covers anything else that might need to be said; *Donnie Daniel* - for being my dad, whose advice and lectures after all these years are finally making sense. Now, you can quit bugging me to finish so that I can get a job; *Caroline Heberton* - for celery, peppers, black olives, sushi, sleepless nights, artificial hi-ways, and peeing dogs. Without you, the start of my evolution may not ever have occurred; *Kathy, Alex, & Maggie Martinez* - for racquetball, for opening up their home to me, for racquetball, for the hot tub, for racquetball; *Art & Holly Carlson* - for Sunday night pizzas and X-Files. I couldn't have adopted better surrogate parents than the two of you; *Renata Heberton* - for letting me lose to her in cards; *Alyssa Heberton* - for being an Alyssa and for loaning me clothes on the two occasions in which I had to dress up; *Brendan Heberton* - for cooking breakfast with me in the morning. By the way, you still can't knock me down; *Harvey Greenberg* - for being my Jewish mother, for letting me cry on your shoulder, and for all the advice that you offered, even if I never asked for it; *Mark & Andrea Miller* - for being Mark & Andrea Miller; *Stan Payne* - for answering my Questions of the Day

and for the insightful comments and insight with various parts of my research; *John Wilson* - for letting me bug him when I didn't want to work, for helping with my programming, and lately, for the style file that he wrote for this dissertation; *Lexie Taylor* and *Dave Krutsinger* - for Sunday dinners and the X-Files, for being the best dog sitters ever, for Mara, for future Thanksgivings, for being my fashion coordinator, and most importantly, for not being math geeks; *Renee Wisniewski* - for our weekly lunches and walks downtown; *Mr. Warren Bateman* - for the establishment of the Lynn Bateman Teaching award, which enabled me to attend Combinatorics '98 so that I could obtain exposure to my future mathematical community; *Debbie Wangerin* - for looking out for us; *Zenas Hartvigson* - for supporting me in teaching (in more ways than you can remember); and *Chris Linden* - for getting me out of the house and for making these last two years more enjoyable than they could have been. "Never Surrender - Never Give Up!"

Leanne Holder

2001 May

## CONTENTS

Figures . . . . .	x
Tables . . . . .	xii
<u>Chapter</u>	
1. Projective Geometry Applications . . . . .	1
1.1 Applications of Geometry to a Communication System . . . . .	1
1.2 Applications of Geometry to Coding Theory . . . . .	4
1.3 Applications of Geometry in Cryptography . . . . .	6
1.3.1 Secret Sharing Schemes . . . . .	8
1.4 Conclusion . . . . .	10
2. Introduction and Review . . . . .	11
2.1 Finite Fields . . . . .	11
2.1.1 Polynomials over Finite Fields . . . . .	13
2.1.2 Quadratic Equations . . . . .	16
2.2 Projective Geometry . . . . .	18
2.2.1 The Projective Line . . . . .	22
2.2.2 The Projective Plane . . . . .	23
2.2.2.1 Planes of Even Order . . . . .	31
2.2.2.2 Planes of Odd Order . . . . .	38
2.2.3 Projective Three-Space . . . . .	43
2.3 Blocking Sets of Lines . . . . .	45
2.3.1 Definitions and Examples . . . . .	46

2.3.2	Bounds on the Size of Irreducible Blocking Sets . . . . .	48
2.3.3	Rédei Blocking Sets . . . . .	49
2.4	Blocking Sets of Conics . . . . .	51
3.	CBSs in Planes of Even Order . . . . .	54
3.1	Introduction . . . . .	54
3.2	The Trace-Flock Construction . . . . .	55
3.3	Irreducible CBSs in $\text{PG}(2, 2^h)$ , $h$ even . . . . .	60
3.4	Searching for Minimum CBSs . . . . .	68
3.5	Bounds on the Sizes of Minimum Conic Blocking Sets . . . . .	76
3.6	Chapter Summary . . . . .	80
4.	CBSs in Planes of Odd Order . . . . .	83
4.1	Introduction . . . . .	83
4.2	The Trace-Flock Construction . . . . .	84
4.3	Searching for Minimum CBSs . . . . .	94
4.3.1	Restricted Quadratic Form Model . . . . .	95
4.3.1.1	Review of Linear Algebra and Quadratic Forms . . . . .	95
4.3.1.2	Restricting Nondegenerate Quadrics to a Line . . . . .	99
4.3.1.3	Classifying Points in the Dual Setting . . . . .	101
4.3.1.4	The Restricted-Dual Model Summary . . . . .	104
4.3.1.5	Finding the CBSs in the Set Covering Setting . . . . .	105
4.3.2	Secant-Tangent Mapping Model . . . . .	108
4.4	Small Conic Blocking Sets in $\text{PG}(2, q^2)$ . . . . .	112
4.5	Bounds on the Sizes of Minimum Conic Blocking Sets . . . . .	128
4.6	Chapter Summary . . . . .	139

5. Conic Blocking Sets and Flocks . . . . .	141
5.1 General Terminology and Background Material . . . . .	141
5.2 The Dual Setting and Star Flocks . . . . .	145
6. Avenues of Further Research . . . . .	156
<u>Appendix</u>	
A. CBS Parameters for $q$ Even . . . . .	158
B. CBS Parameters for $q$ Odd . . . . .	160
C. The Branch and Bound Algorithm . . . . .	163
<u>References</u> . . . . .	171

## FIGURES

Figure

1.1	A Communication System with Seven Users and Switches . . . . .	3
1.2	Atmospheric Noise . . . . .	5
1.3	A Simple Cryptosystem . . . . .	7
2.1	The Fano Plane . . . . .	24
2.2	Desargues' Configuration . . . . .	26
2.3	$X$ and $Y$ Not on a Common Tangent Line . . . . .	37
2.4	$X$ and $Y$ on a Common Tangent Line . . . . .	37
2.5	Constructing the Polar of a Point with Respect to a Conic . . . . .	41
2.6	Flock of a Cone . . . . .	44
2.7	The Complement of a CBS . . . . .	52
3.1	A partitioning of $\mathcal{E}$ . . . . .	57
4.1	A partitioning of $\mathcal{E}$ . . . . .	86
4.2	A Collection of Values $Q((\lambda + k)n)$ . . . . .	124
4.3	The Union of 3-Cycles . . . . .	126
4.4	The 3-Cycles for $Q(x) = x^2 + \alpha^{10}x + 1$ . . . . .	128
5.1	An Arbitrary Cone . . . . .	141
5.2	Linear Flock . . . . .	142
5.3	Primary and Secondary Baselines . . . . .	144
5.4	Dual Flock Setting . . . . .	146
5.5	Dual Baseline Setting . . . . .	147

5.6	Dual Proper Star Flock in $PG(3, q)$ . . . . .	150
C.1	A Tree . . . . .	166

## TABLES

Table

3.1 CBS Sizes Given by the Trace-Flock Construction . . . . .	59
3.5 Minimum CBS Sizes . . . . .	76
3.6 Construction Sizes . . . . .	81
3.7 CBS Bounds and Sizes . . . . .	82
4.1 CBS Sizes Given by the Trace-Flock Construction . . . . .	93
4.5 Array $B$ to Array $A$ Conversion in $\text{PG}(2, 3)$ . . . . .	107
4.6 Values for Minimum CBSs . . . . .	112
4.14 Squarity Subtraction Tables . . . . .	129
4.16 Construction Sizes . . . . .	139
4.17 Minimum Values and Bounds on Minimum Values . . . . .	140
4.18 Bounds on Minimum Values . . . . .	140
A.1 CBSs in Planes of Even Order . . . . .	158
B.1 Minimum CBSs in Planes of Prime Order . . . . .	160
B.2 Minimum CBSs in Planes of Nonprime Order . . . . .	161
B.3 Smallest Known CBSs for $q$ an Odd Prime . . . . .	162
B.4 Smallest Known CBSs for $q$ an Odd Nonprime . . . . .	162

## 1. Projective Geometry Applications

Projective geometry has applications in modern information and communication science, more specifically, in coding theory and cryptography. The aim of coding theory is to develop methods that enable the recipient of a message to detect or even correct errors that occur while transmitting data. Many problems of coding theory can be directly translated into geometric problems. As to cryptography, one of its tasks is to keep information secret by enciphering it. Another task is to protect data against alteration. Surprisingly, cryptosystems based on geometry have excellent properties: in contrast to most systems used in practice they offer provable security of arbitrarily high level.

### 1.1 Applications of Geometry to a Communication System

To illustrate how projective geometry can be applied to a communication problem, we will examine one that is developed in [8]. Consider a scenario where there is a collection of users who wish to communicate with each other. To make this scenario more interesting, several conditions are imposed on the participants and on the communications network.

For the participants of the scenario, two constraints are imposed. First, it is impossible for any participant to get in direct contact with another participant. Secondly, each participant must use the communications network which will consist of switches. For the communications network, three conditions are imposed. First, each switch is responsible for a certain number of users. Second, each switch can connect any two of the users. Third, any connection between two users needs

at least one switch. Finally, for economic reasons, the condition that the number of switches should be as small as possible is imposed.

Now, we examine the requirements for this communication system. The first requirement is

- any two users can be connected using just one switch.

Since any switch should have some use, the second requirement is

- each switch connects at least two users.

If all users were connected by only one switch then there would be a substantial amount of mutual interference; therefore the third requirement is that

- there are at least two switches.

Finally, since it should be possible to produce switches cheaply, the final requirement is

- all switches look ‘alike’.

We will expound further on this last requirement.

Now that we have formulated the requirements for the communication system, we translate this into geometrical language using linear spaces.

**Definition 1.1** *A linear space is a geometry  $\mathbf{L}$  consisting of points and lines such that following three axioms hold.*

**(L1)** *Any two distinct points of  $\mathbf{L}$  are incident with precisely one line.*

**(L2)** *On any line of  $\mathbf{L}$  there are at least two points.*

**(L3)**  $L$  has at least two lines.

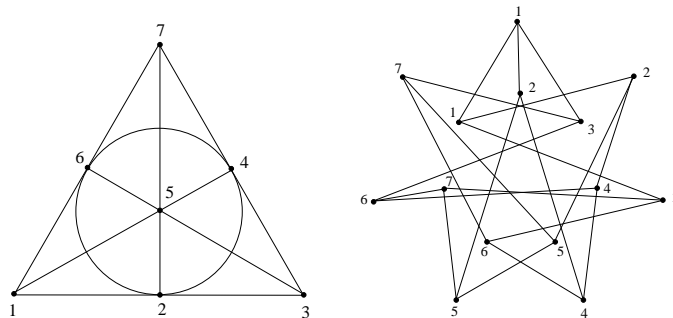
In order to do this translation, the users are called points and the switches are called lines. Now, the first three requirements of the system translate into the axioms of a linear space. That is, in order to obtain a good communications system we have to find a linear space

- that has a number of lines that is as small as possible, and
- in which all lines look ‘alike’.

Although the phrase ‘looking alike’ has not been precisely defined, this phrase can be taken to mean that any line has the same number of points, or in terms of the switches, each switch connects the same number of users.

The following example will further clarify this communication network description.

**Example 1.**



**Figure 1.1:** A Communication System with Seven Users and Switches

Consider the communications network system that has seven users, 1, 2, 3, 4, 5, 6, 7, and seven switches such that each switch handles three users. Then the switches would be 123, 145, 167, 246, 257, 347, 356.

By designating the ‘outer’ points to represent switches (lines) and the ‘inner’ points to represent users (points), we see that the picture on the right-hand side of Figure 1.1 is a communication system. For further information about this communications system, see [8, 72]. ■

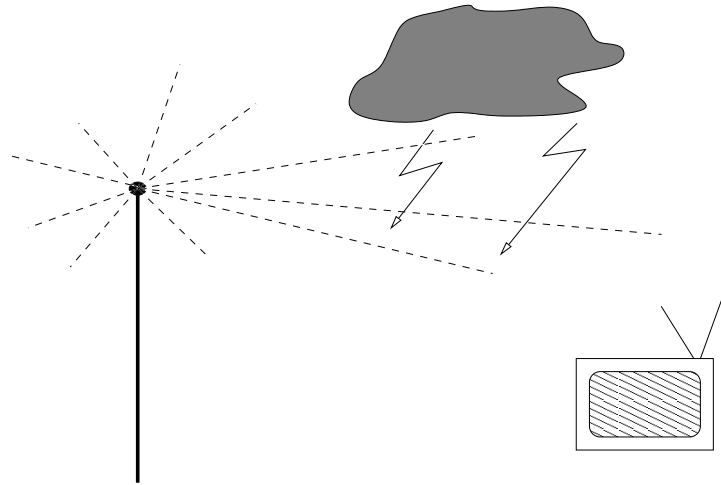
Most importantly, it can be shown that communication systems with the least number of switches are obtained from projective planes [8].

## 1.2 Applications of Geometry to Coding Theory

Coding theory originated with the arrival of computers. Early computers were huge and their reliability was low compared to the computers of today. These computers consisted of banks of mechanical relays, and if a single relay failed to close an entire calculation was in error. The engineers of the time devoted much energy to finding ways to detect faulty relays so that they could be replaced. While R. W. Hamming was working for Bell Labs [33], he began to work on the problem of having the machine not only detect when an error occurred, but correct the error as well. Hamming devised a way of encoding information so that if an error was detected it could also be corrected. Based in part on this work, Claude Shannon [64] developed the theoretical framework for the science of coding theory.

In this section, we briefly examine the error-correcting aspect of coding theory. The problem that can be answered using projective geometry deals with the difficulties inherent with the transmission of messages. More particularly, suppose that we wished to transmit a message and knew that in the process of transmission there would be some sort of “noise” causing the message to be altered. This noise could be due to weak signals, sporadic electrical bursts, and other naturally occurring noise that creeps into the transmission medium. The problem is to in-

sure that the intended message is obtainable from whatever is actually received. One simple approach to this problem is to code the message so that the original content is easily obtainable, even if the coded message received is full of errors.



**Figure 1.2:** Atmospheric Noise

A basic error-correcting code consists of transmitting redundant information together with the message that is to be communicated. That is, the message is extended so that the sequence of symbols, in the message, is a longer sequence and this extension is done in a systematic manner. This particular coding method has many economical drawbacks. There are other error-correcting codes, and some are more economical.

There are many codes for encoding and decoding transmitted data that are related to projective geometry. For instance, projective geometry has ties to Hamming codes, linear codes, cyclic codes, MDS codes, and Reed-Muller codes. The Reed-Muller code is one of the most studied codes and has been used by NASA for transmission of data.

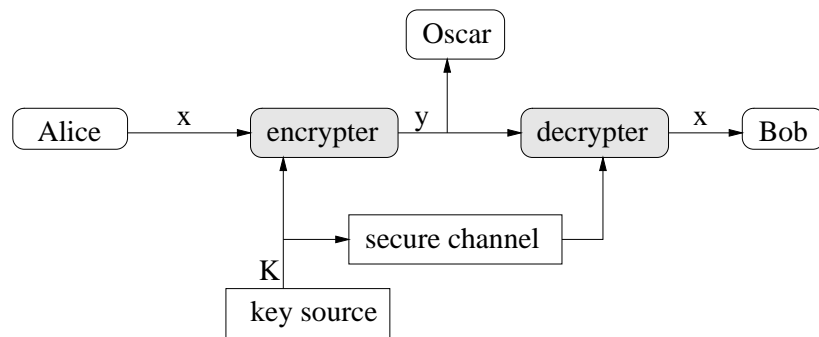
To examine one of the applications of codes, consider NASA's Mariner 9 mission in 1971. Mariner 9 was a space probe whose mission was to fly over Mars, photograph the surface, and then transmit the pictures back to Earth. The black and white camera aboard the Mariner 9 took the pictures, and a fine grid was then placed over the picture and for each square of the grid the degree of blackness is measured on a scale from 0 to 63. These numbers, expressed in binary, are the data that is transmitted to Earth. By the time the data arrived back at Earth, the signal was weak and needed to be amplified. Noise from space modified the signal and thermal noise from the amplifier had the effect that occasionally a signal transmitted as a 1 was interpreted by the receiver as a 0 and vice versa. Thus, there was clearly a need to code this information with an error correcting code. The Reed-Muller code was chosen for this task of transmitting pictures. For more information about the Mariner 9 mission and the coding theory used in that project, see [71, 56]. For more information on the Reed-Muller codes as an application of projective geometry, see [16, 2].

### **1.3 Applications of Geometry in Cryptography**

As mentioned at the beginning of this chapter, cryptography has two main purposes. The first is to provide a method that guarantees the privacy of information. The second is to provide methods that allow the receiver of the message to determine if the message has been altered and verify that the message came from the claimed sender. Such systems are often based on secret keys; therefore the secure distribution and storing of secret keys is a central area of cryptography.

The following illustration of a simple cryptosystem is found in [68]. A simple cryptosystem usually enables two people, referred to Alice and Bob, to communi-

cate over an insecure channel in such a way that an opponent, referred to as Oscar, cannot understand what is being communicated. The channel could be anything from a telephone line or a CB radio to a computer network. The *plaintext* information that Alice sends to Bob is encrypted by Alice using a predetermined key. This *ciphertext* is then sent over the channel where Oscar, whose is eavesdropping, cannot determine what the plaintext was, but Bob who has the encryption key can decrypt the ciphertext to reconstruct the plaintext.



**Figure 1.3:** A Simple Cryptosystem

For this illustration, Alice and Bob use the following protocol for their cryptosystem. First, in a secure setting, Alice and Bob chose a random key  $K$ . When Alice wants to communicate with Bob, she encrypts the plaintext  $x$  using the key  $K$  into the ciphertext  $y$  which is sent over the communication channel. When Bob receives the ciphertext  $y$ , he decrypts it using the key.

It is often the case that the authenticity of the plaintext is more important than the confidentiality of the plaintext. A message is said to be *authentic* if the recipient is sure that

1. he receives exactly the data the sender has sent (data integrity) and

2. the data really originated from the claimed sender (data authenticity).

We see that there are two types of attacks available to disrupt the authenticity of a message. One is when an attacker tries to insert a message claiming that he is the real sender and the other is when an attacker tries to modify the sent message. As protection against the attacks described, *authentication systems* have been invented [65].

In 1974, Gilbert, MacWilliams, and Sloane [30] showed that if  $\kappa$  is the number of possible keys to an authentication system, then an attacker could deceive with probability at least  $1/\sqrt{\kappa}$ . A authentication system with  $\kappa$  keys is called *perfect*, if the probability that an attacker will be able to insert or substitute a message is only  $1/\sqrt{\kappa}$ . Perfect authentication systems exist and can be constructed using mathematical structures such as projective geometry.

Another aspect of cryptography that can involve projective geometry is the problem of storing and retrieving secret data. This problem can be solved in an optimal way by using a *secret sharing scheme* [63, 66].

### 1.3.1 Secret Sharing Schemes

In a secret sharing scheme, a dealer has a secret and would like to distribute to 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 [68, 12]. 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.

To better illustrate this concept, consider a generic secret sharing scheme involving the employees of a bank [38].

**Example 2.** 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 [68]. 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 alone can open the vault while allowing any vice president in cooperation with a pair of senior tellers the ability to open the vault [67]. 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.

A model for both Design A and Design B can be developed by using various relationships between certain points, lines, and planes of a projective four-space to represent the secret and the shares. ■

## **1.4 Conclusion**

For all of the applications presented in this chapter, the basic properties had to be worked out before projective geometry could be applied to solve such problems. In this thesis, we are working out the basic properties of a new concept in projective geometry.

## 2. Introduction and Review

This introductory chapter contains a survey of some basic algebraic and geometric concepts that will be employed throughout this dissertation. We begin with a discussion of finite fields and functions over finite fields, since both are instrumental to the development of projective geometries. After that, we provide a detailed overview of projective geometries.

### 2.1 Finite Fields

**Definition 2.1** *A field is a set  $K$  closed under two operations  $+$ ,  $\times$  such that*

1.  $(K, +)$  is an abelian group with identity  $0$ ;
2.  $(K^*, \cdot)$  is an abelian group with identity  $1$ , where  $K^* = K \setminus \{0\}$ ;
3.  $x(y + z) = xy + xz$ ,  $(x + y)z = xz + yz$ , for all  $x, y, z$  in  $K$ ;

Below, we list definitions and properties that are useful to the development of the results given in this paper. These are taken from [35, Ch.1], and the reader is referred to [48] for an in-depth look at finite fields or to [26] for an introduction to finite fields.

1. A *finite field* is a field with only a finite number of elements.
2. The *characteristic* of a finite field  $K$  is the smallest positive integer (which must be a prime)  $p$  such that  $px = 0$  for all  $x$  in  $K$ .
3.  $\text{GF}(p)$ ,  $p$  prime, consists of the residue classes of the integers modulo  $p$  under the natural addition and multiplication and is a finite field of  $p$  elements.

4. A finite field  $K$  of characteristic  $p$  has a subfield isomorphic to  $\text{GF}(p)$  and has  $p^h$  elements for some  $h$  in  $\mathbb{N}$ .
5. If  $f(t)$  is an irreducible polynomial of degree  $h$  over  $\text{GF}(p)$ , then

$$\begin{aligned}\text{GF}(p^h) &= \text{GF}(p)[t]/(f) \\ &= \{a_0 + a_1t + \dots + a_{h-1}t^{h-1} \mid a_i \in \text{GF}(p), f(t) = 0\}.\end{aligned}$$

6. The elements  $x$  of  $\text{GF}(q)$ ,  $q = p^h$ , satisfy

$$x^q - x = 0,$$

and there exists  $s$  in  $\text{GF}(q)$  such that

$$\text{GF}(q) = \{0, 1, s, \dots, s^{q-2} \mid s^{q-1} = 1\};$$

such an  $s$  is called a *primitive element of  $\text{GF}(q)$*  or *generator of  $\text{GF}(q)^*$* .

7. Any field of  $q$  elements,  $q = p^h$  is isomorphic to  $\text{GF}(q)$ , which is called the *Galois field of order  $q$* .

By Property 6, we have that every element in  $\mathcal{E} = \text{GF}(2^n)$  satisfies  $x^{2^n} = x$ , so that  $x$  is the square of the element  $x^{2^{n-1}}$ . We also remark that every element in  $\mathcal{E}$  has exactly one square root, since  $-1 = 1$  in  $\mathcal{E}$ .

Unlike the situation in  $\text{GF}(2^n)$ , if  $\mathcal{E} = \text{GF}(p^n)$  with  $p$  an odd prime, then not every element in  $\mathcal{E}$  is a square. Those that are not squares are called *nonsquares*. If  $\lambda$  is a primitive element of  $\mathcal{E}$ , so that  $\lambda^{p^n-1} = 1$  and  $\lambda^{(p^n-1)/2} = -1$ , the even powers of  $\lambda$  are squares; while the odd powers are nonsquares. The element 0 is not considered a square or a nonsquare. Hence, there are  $\frac{p^n-1}{2}$  squares and the

same number of nonsquares. Furthermore, it is easy to see that the product or quotient of two squares or nonsquares is a square; but the product or quotient of a square and nonsquare is a nonsquare. We often denote a square element with the symbol  $\square$  and a nonsquare element with the symbol  $\not\square$ . The following theorem will prove to be useful when we obtain counts of various sums in  $\mathcal{E}$ .

**Theorem 2.2** [24, Thm.67] *If  $S$  denotes the number of squares  $\sigma^2$  in  $\mathcal{E}$  for which  $\sigma^2 + 1 = \square$  and  $N$  denotes the number of squares  $\tau^2$  for which  $\tau^2 + 1 = \not\square$ , we have*

$$S = \frac{1}{4}(p^n - 5), N = \frac{1}{4}(p^n - 1), \text{ if } -1 = \square;$$

$$S = \frac{1}{4}(p^n - 3), N = \frac{1}{4}(p^n + 1), \text{ if } -1 = \not\square.$$

■

### 2.1.1 Polynomials over Finite Fields

Polynomials for which the associated polynomial functions are permutations of a given finite field  $\text{GF}(q)$  are called *permutation polynomials*. These polynomials exist over any  $\text{GF}(q)$  since every mapping of  $\text{GF}(q)$  into itself can be expressed by a polynomial function. We remind the reader of the obvious, that if the function  $f$  is a permutation polynomial of  $\text{GF}(q)$ , then  $f$  is one-to-one and onto. Other criteria and properties of permutation polynomials can be found in [48, ch.7].

**Definition 2.3** [48] *Let  $\text{GF}(q^m)$  be an extension of  $\text{GF}(q)$  and let  $\alpha \in \text{GF}(q^m)$ . Then the elements  $\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{m-1}}$  are called the conjugates of  $\alpha$  with respect to  $\text{GF}(q)$ .*

Let  $\mathcal{E} = \text{GF}(q^m)$  be an extension of  $\mathcal{K} = \text{GF}(q^d)$ , where  $d$  is any divisor of  $m$ . An *automorphism*  $\sigma$  of  $\mathcal{E}$  over  $\mathcal{K}$  is a mapping of  $\mathcal{E}$  onto itself that fixes the

elements of  $\mathcal{K}$  point-wise. Thus,  $\sigma$  is required to be a one-to-one mapping from  $\mathcal{E}$  onto itself with  $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$  and  $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$  for all  $\alpha, \beta \in \mathcal{E}$  and  $\sigma(a) = a$  for all  $a \in \mathcal{K}$ . The relationship between conjugate elements and certain automorphisms of a finite field is explained in the following theorem.

**Theorem 2.4** [48] *The distinct automorphisms of  $\mathcal{E} = \text{GF}(q^m)$  over  $\mathcal{K} = \text{GF}(q)$  are exactly the mappings  $\sigma_0, \sigma_1, \dots, \sigma_{m-1}$ , defined by  $\sigma_i(t) = t^{q^i}$  for  $t \in F$  and  $0 \leq i \leq m - 1$ . ■*

For example, the automorphisms of  $\text{GF}(2^4)$  are

$$\begin{aligned}\sigma_0(t) &= t, \\ \sigma_1(t) &= t^2, \\ \sigma_2(t) &= t^4, \\ \sigma_3(t) &= t^8.\end{aligned}$$

It is clear, from the previous theorem, that the conjugates of  $\alpha \in \mathcal{E}$  with respect to  $\mathcal{K}$  are obtained by applying all automorphisms of  $\mathcal{E}$  over  $\mathcal{K}$  to the element  $\alpha$ . The next map we examine is a linear map from  $\mathcal{E}$  to  $\mathcal{K}$ , and it is important in the construction of conic blocking sets.

**Definition 2.5** [48] *For  $\alpha \in \mathcal{E}$ , the trace  $Tr_{\mathcal{E}/\mathcal{K}}(\alpha)$  of  $\alpha$  is an additive homomorphism of  $\mathcal{E}$  into  $\mathcal{K}$  is defined by*

$$Tr_{\mathcal{E}/\mathcal{K}}(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \dots + \alpha^{q^{m-1}}.$$

*If  $\mathcal{K}$  is the prime subfield of  $\mathcal{E}$ , then  $Tr_{\mathcal{E}/\mathcal{K}}(\alpha)$  is called the absolute trace of  $\alpha$ . Otherwise,  $Tr_{\mathcal{E}/\mathcal{K}}(\alpha)$  is called a relative trace of  $\alpha$  over  $\mathcal{K}$ .*

We see that the trace of  $\alpha$  over  $\mathcal{K}$  is the sum of the conjugates of  $\alpha$  with respect to  $\mathcal{K}$ . For example,

$$\mathrm{Tr}_{\mathrm{GF}(16)/\mathrm{GF}(2)}(t) = t + t^2 + t^4 + t^8,$$

and

$$\mathrm{Tr}_{\mathrm{GF}(16)/\mathrm{GF}(4)}(t) = t + t^4.$$

Moreover,  $\mathrm{Tr}_{\mathcal{E}/\mathcal{K}}(\alpha)$  is always an element of  $\mathcal{K}$ .

The following theorem gives several useful properties of the trace function, most notably that the trace function is linear.

**Theorem 2.6** [48] *Let  $\mathcal{E} = \mathrm{GF}(q^m)$  and  $\mathcal{K} = \mathrm{GF}(q)$ . Then the trace function  $\mathrm{Tr}_{\mathcal{E}/\mathcal{K}}$  satisfies the following properties:*

1.  $\mathrm{Tr}_{\mathcal{E}/\mathcal{K}}(\alpha + \beta) = \mathrm{Tr}_{\mathcal{E}/\mathcal{K}}(\alpha) + \mathrm{Tr}_{\mathcal{E}/\mathcal{K}}(\beta)$  for all  $\alpha, \beta \in \mathcal{E}$ ;
2.  $\mathrm{Tr}_{\mathcal{E}/\mathcal{K}}(c\alpha) = c\mathrm{Tr}_{\mathcal{E}/\mathcal{K}}(\alpha)$  for all  $c \in \mathcal{K}, \alpha \in \mathcal{E}$ ;
3.  $\mathrm{Tr}_{\mathcal{E}/\mathcal{K}}$  is a linear transformation from  $\mathcal{E}$  onto  $\mathcal{K}$ , where both  $\mathcal{E}$  and  $\mathcal{K}$  are viewed as vector spaces over  $\mathcal{K}$ ;
4.  $\mathrm{Tr}_{\mathcal{E}/\mathcal{K}}(a) = ma$  for all  $a \in \mathcal{K}$ ;
5.  $\mathrm{Tr}_{\mathcal{E}/\mathcal{K}}(\alpha^q) = \mathrm{Tr}_{\mathcal{E}/\mathcal{K}}(\alpha)$  for all  $\alpha \in \mathcal{E}$ .

■

Often it is more convenient for us to denote  $\mathrm{Tr}_{\mathcal{E}/\mathcal{K}}$  by  $\mathrm{tr}$  or  $\mathrm{Tr}$  when the fields in question are understood. Other properties of the trace function can be found

in the first chapter of [35]. When  $q$  is even, we may express  $\mathcal{E} = \Upsilon_0 \cup \Upsilon_1$  where  $\Upsilon_0$  is the set of elements of absolute trace 0, and  $\Upsilon_1$  is the set of elements of absolute trace 1. Then, we have the additional properties:

- (a)  $0 \in \Upsilon_0$ ;
- (b)  $q = 2^{2m} \iff 1 \in \Upsilon_0$ ;
- (c)  $q = 2^{2m+1} \iff 1 \in \Upsilon_1$ ;
- (d)  $t \in \Upsilon_i \iff \sigma(t) \in \Upsilon_i$  for all automorphisms  $\sigma$ ;
- (e)  $s \in \Upsilon_i, t \in \Upsilon_j \implies \begin{cases} s + t \in \Upsilon_0 & \text{if } i = j, \\ s + t \in \Upsilon_1 & \text{if } i \neq j. \end{cases}$
- (f)  $|\Upsilon_0| = |\Upsilon_1| = q/2$ .

It is easy to show that  $\text{Tr}(t^2) + \text{Tr}(t) = 0$  for all  $t \in \mathcal{E}$ . From this it can be shown that any element that can be expressed as the sum of another element and its square has trace 0.

In Chapters 3 and 4, the trace function will be used to construct conic blocking sets. In the next section, we use the trace function to determine the number of solutions of a quadratic equation in a finite field. This will be useful in later chapters for determining the relationship between a line of the projective plane and a quadratic form in the plane.

### 2.1.2 Quadratic Equations

We are interested in determining the number of solutions to quadratic equations in a finite field of order  $q$ . We can determine the number of irreducible

factors of a quadratic equation,

$$ax^2 + bx + c = 0, \quad a \neq 0, \quad (2.1)$$

over a field of odd characteristic by examining the discriminant of the quadratic equation. However, in fields of characteristic two, the discriminant proves insufficient to determine the number of irreducible factors. In this case, the number of irreducible factors can be determined by using the absolute trace function. We describe the cases of odd and even characteristic separately.

If the characteristic of the field is not two, the *discriminant* of the quadratic equation (2.1) is

$$\Delta = b^2 - 4ac.$$

There are three cases:

1. if  $\Delta = 0$ , then (2.1) has the unique solution  $x = -b/(2a)$ ;
2. if  $\Delta$  is a nonsquare in  $\text{GF}(q)$ , then (2.1) has no solutions in  $\text{GF}(q)$ ;
3. if  $\Delta$  is a square in  $\text{GF}(q)$ , then (2.1) has two solutions  $x = (-b \pm \sqrt{\Delta})/(2a)$ .

For characteristic two, let  $\text{Tr}(t)$  denote the absolute trace of  $t$  over  $\text{GF}(2)$ . Instead of using the discriminant as our invariant, we use a different invariant called  $\delta$ .

(a) First, if  $b = 0$ , then (2.1) becomes  $ax^2 + c = 0$ , and the unique solution to (2.1) is given by  $x = \sqrt{c/a}$ .

(b) If  $b \neq 0$ , we can multiply (2.1) by  $a/b^2$  to obtain the equation  $\frac{a^2x^2}{b^2} + \frac{ax}{b} + \frac{ac}{b^2} = 0$ . Let  $y = ax/b$  and  $\delta = ac/b^2$ , so that (2.1) becomes

$$y^2 + y + \delta = 0. \quad (2.2)$$

Then,  $\delta$  is the invariant of equation (2.1) and also of (2.2).

As mentioned in the previous section,  $\text{Tr}$  is a homomorphism into  $\mathcal{K} = \text{GF}(2)$ , i.e.,  $\text{Tr}(\delta) = 0$  or  $1$ .

1. If  $\text{Tr}(\delta) = 1$ , then (2.2) and so (2.1) have no solutions.
2. If  $\text{Tr}(\delta) = 0$ , then (2.2) and so (2.1) have two solutions. If  $y = s$  is one solution of (2.2), then  $y = s + 1$  is the other.

## 2.2 Projective Geometry

The material presented in the upcoming sections is meant to serve as a cursory review of some of the basic ideas from finite projective geometry specifically related to finite projective lines, planes, and solids. A natural place to begin is the construction of a projective geometry. A commonly used construction for obtaining a projective geometry starts with a vector space. For reasons that will soon be clear, we will use the word ‘rank’ in lieu of ‘dimension’ when referring to vector spaces. Let  $V = V(n + 1, q)$  be an  $(n + 1)$ -rank vector space over the field  $\text{GF}(q)$  with zero element  $0$ . We view the elements of  $V(n + 1, q)$  as the  $(n + 1)$ -tuples of the form  $(x_0, x_1, \dots, x_n)$  where the  $x_i$  are in  $\text{GF}(q)$ . Consider the equivalence relation on the elements of  $V \setminus \{0\}$  whose equivalence classes are the rank one subspaces of  $V$  with the zero deleted. So, if  $X, Y \in V \setminus \{0\}$ , then  $X$  is equivalent to  $Y$  if  $Y = tX$  for some  $t \in \text{GF}(q)^* = \text{GF}(q) \setminus \{0\}$ . With this equivalence relation in mind, we can form the *n-dimensional projective space over GF(q)*, denoted  $PG(n, q)$ , in the following manner: The *points, lines, planes, and solids* of  $PG(n, q)$  are defined as the subspaces of rank 1, 2, 3, and 4, respectively. In keeping with classical geometric terminology, we say that these objects have

(projective) *dimension* 0, 1, 2, and 3, respectively. In general, for  $0 < k \leq n$ , a rank  $k$  subspace of  $V$  is said to have projective dimension  $k - 1$ . A rank  $n$  subspace of  $V$  (i.e. an  $n - 1$  dimensional object in  $\text{PG}(n, q)$ ) is often called a *hyperplane*.

Lines in this setting are regarded as certain sets of points; planes can also be regarded as certain sets of points. If a point lies on a line or in a plane, the point is said to be *incident* with the line or plane. This is equivalent to the notion of a rank one subspace being contained in a rank two or rank three subspace.

A well known result from linear algebra states that if  $S$  and  $T$  are vector spaces,

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

where  $\text{rk}$  denotes the algebraic dimension (rank) of a vector space. This is called the *rank formula*. For clarity, consider the following example.

**Example 3.**

Let  $\Omega = \text{PG}(4, q)$  be derived from a rank 5 vector space. The rank formula is used to determine all possible incidences of lines and planes in  $\Omega$ .

First, the relationship between two distinct planes,  $\pi_1$  and  $\pi_2$ , in  $\Omega$  is examined. If  $\pi_1$  and  $\pi_2$  lie in a common 3-dimensional subspace of  $\Omega$  (that is, rank four vector space), then by the rank formula these two planes intersect in a line (a rank two vector subspace). But, if  $\pi_1$  and  $\pi_2$  do not lie in a common 3-dimensional subspace of  $\Omega$ ,  $\pi_1$  and  $\pi_2$  must intersect in a point, because their union (span) would have rank four. Let  $P$ ,  $Q$ , and  $R$  be three noncollinear points in  $\Omega$ . Since each point has rank one, and two points determine a line, using two of these two lines, according to the rank formula, the smallest subspace containing these three points is a rank three subspace of  $\Omega$ , which is a projective plane.

Second consider the incidence relationship between a line  $l$  and a plane  $\pi$ , both in  $\Omega$ . If  $l$  meets  $\pi$ ,  $l$  either meets  $\pi$  in a point or is entirely contained within  $\pi$ . Suppose two points of  $l$  are in  $\pi$ . Then since  $\pi$  is a vector subspace, the span of any two points that lie in  $\pi$  also lies in  $\pi$ . In this case, it must be that  $l$  is entirely contained in  $\pi$ . ■

If  $\Pi_1$  and  $\Pi_2$  are two spaces  $\text{PG}(n, q)$  with  $n \geq 2$ , then a *collineation*  $\Gamma : \Pi_1 \rightarrow \Pi_2$  is a bijection which preserves incidence; that is if  $\Pi_r \subset \Pi_s$ , then  $\Pi_r\Gamma \subset \Pi_s\Gamma$ , where  $\Pi_r$  and  $\Pi_s$  are subspaces of  $\Pi_1$ . For instance,  $\Gamma$  maps collinear points to collinear points and concurrent lines to concurrent lines. If  $S$  is a set of points in  $\text{PG}(2, q)$  with the property that no three are collinear,  $\Gamma$  maps  $S$  to another set of points with the same property. A *projectivity* is a collineation that is induced by the action of a nonsingular matrix on the underlying vector space.

The Fundamental Theorem of Projective Geometry is vital to the work in Chapters 3 and 4. Below is the statement as given in [35].

**Theorem 2.7** [35, 2.1.2 (b)] *Suppose  $\{P_0, \dots, P_{n+1}\}$  and  $\{P'_0, \dots, P'_{n+1}\}$  are both ordered subsets of  $\text{PG}(n, q)$  of cardinality  $n + 2$  such that no  $n + 1$  points chosen from the same set lie in a hyperplane. Then, there exists a unique projectivity  $\mathcal{T}$  such that  $P'_i = P_i\mathcal{T}$ , for  $0 \leq i \leq n + 1$ . ■*

For a projective plane where  $n = 2$ , the previous theorem essentially states that the group of projectivities of the plane,  $\text{PGL}(3, q)$ , acts sharply transitively on four points (no three collinear) of  $\text{PG}(2, q)$  [9].

Any projective space  $\text{PG}(n, q)$ , has a dual space  $\text{PG}(n, q)^*$ , whose points and hyperplanes are respectively the hyperplanes and points of  $\text{PG}(n, q)$ . For any theorem true in  $\text{PG}(n, q)$ , there is an equivalent theorem true in  $\text{PG}(n, q)^*$ . That is,

if  $T$  is a theorem in  $\text{PG}(n, q)$  stated in terms of points, hyperplanes and incidence, the same theorem is true in  $\text{PG}(n, q)^*$  and gives a dual theorem  $T^*$  by substituting ‘hyperplane’ for point and ‘point’ for ‘hyperplane’. So, we have that the dual of an  $r$ -space in  $\text{PG}(n, q)$  is an  $(n - r - 1)$ -space. The fact that we can make such a replacement is known as “the principle of duality”, and this principle carries over into any projective geometry.

For instance, in the plane  $\text{PG}(2, q)$ , every statement about points and lines can be replaced by a *dual* statement about lines and points. In  $\text{PG}(3, q)$ , a point and plane are dual, whereas the dual of a line is a line. In order to simplify calculations it is often necessary to work in the dual setting.

A *quadric* in  $\text{PG}(n, q)$  is a set of points in  $\text{PG}(n, q)$  whose coordinates satisfy a homogeneous equation of degree two. If  $Q$  is a quadratic form, that is,

$$\begin{aligned} Q &= \sum_{\substack{i, j = 0 \\ i \leq j}}^n a_{ij} X_i X_j \\ &= a_{00} X_0^2 + a_{01} X_0 X_1 + \cdots, \end{aligned}$$

then the set of points satisfying  $Q = 0$  is a *quadric* in  $\text{PG}(n, q)$ . For instance, a quadric in  $\text{PG}(2, q)$  is the set of points whose coordinates  $(X_0, X_1, X_2)$  satisfy the homogeneous quadratic equation  $a_{00} X_0^2 + a_{01} X_0 X_1 + a_{11} X_1^2 + a_{02} X_0 X_2 + a_{12} X_1 X_2 + a_{22} X_2^2 = 0$ .

In Sections 2.2.1 and 2.2.3, we further examine the projective line and projective 3-space. Since the bulk of the results pertain to projective planes, emphasis is placed on background material in Section 2.2.2.

### 2.2.1 The Projective Line

The projective line,  $PG(1, q)$ , is important for the results developed in Chapters 3 and 4. There are  $q + 1$  points of  $PG(1, q)$  and they are  $\{(1, 0)\} \cup \{(x, 1) \mid x \in GF(q)\}$ . Each point  $(x, 1)$  of  $PG(1, q)$  can be represented by the nonhomogeneous coordinate  $x$  in  $GF(q)$  and the coordinate for  $(1, 0)$  is  $\infty$ . In the remainder of this dissertation, these points of  $PG(1, q)$  are often referred to in terms of the parameters  $t \in GF(q) \cup \{\infty\}$ .

A projectivity  $\mathcal{T}$  of  $PG(1, q)$  is given by  $Y = XT$ , where  $X = (x_0, x_1)$ ,  $Y = (y_0, y_1)$  and  $T = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ ,  $T \in PGL(2, q)$ . The Fundamental Theorem of Projective Geometry states that any three points of  $PG(1, q)$  can be mapped to any other three points by a projectivity. Since this property is used in the upcoming chapters, a small example of how a projectivity of the line maps points to points is presented below.

#### Example 4.

There are six points on the line  $PG(1, 5)$  which have coordinates  $(0, 1)$ ,  $(1, 1)$ ,  $(2, 1)$ ,  $(3, 1)$ ,  $(4, 1)$ , and  $(1, 0)$ . The projectivity  $T = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$  maps these points of  $PG(1, q)$  to the points  $(1, 1)$ ,  $(4, 1)$ ,  $(0, 1)$ ,  $(3, 1)$ ,  $(1, 0)$ , and  $(2, 1)$ , respectively. ■

Let  $Q(1, q)$  be the set of quadrics of  $PG(1, q)$  and  $\mathcal{S}_{a,b,c} = \{(x, y) \in PG(1, q) \mid ax^2 + bxy + cy^2 = 0 \text{ for } a, b, c \in GF(q)\}$ . Then,

$$Q(1, q) = \{\mathcal{S}_{a,b,c} \mid a, b, c \in GF(q)\}.$$

There are  $q^2 + q + 1$  quadrics in  $Q(1, q)$ , and each quadric is classifiable by examining the discriminant of the quadratic form. Quadrics of the projective line will resurface again in the development of constructions of conic blocking sets in planes of odd order.

### 2.2.2 The Projective Plane

Since the majority of results presented in this dissertation deal with the projective plane, a more detailed review is offered. There are a variety of ways to define or construct a projective plane. One such way is the vector space construction given in Section 2.2. We begin this section by giving an axiomatic definition of a projective plane. This is followed by definitions, theorems, and properties of the projective plane that are relevant to the results given in this dissertation.

**Definition 2.8** *A projective plane is a set of points and a set of lines together with an incidence relation between them satisfying the following three axioms.*

**(P1)** *Any two points are incident with a unique common line.*

**(P2)** *Any two lines are incident with a unique common point.*

**(P3)** *There are at least four points, no three of which are incident with a common line.*

It can be shown that any finite projective plane must satisfy the following theorem.

**Theorem 2.9** [1] *Let  $\pi$  be a finite projective plane. Then there is an integer  $q$  such that*

1. *Every point of  $\pi$  is incident with exactly  $q + 1$  lines;*
2. *Every line of  $\pi$  is incident with exactly  $q + 1$  points;*

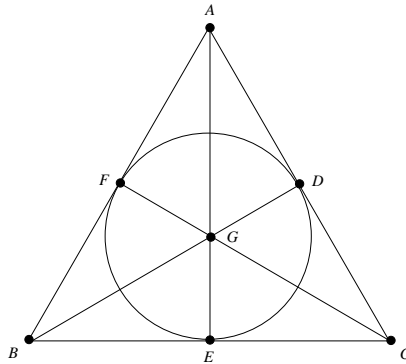
3.  $\pi$  contains exactly  $q^2 + q + 1$  points;

4.  $\pi$  contains exactly  $q^2 + q + 1$  lines.

■

In some treatments the conclusion of Theorem 2.9 is taken as the definition of a finite projective plane. That is, a finite projective plane can be defined as a set of  $q^2 + q + 1$  points and a set of lines in which each line is incident with  $q + 1$  points in such a way that any two points are incident with a unique line. For an example of this approach, see [16]. Of course, this combinatorial definition can be shown to be equivalent to the previous axiomatic definition.

**Example 5.** The simplest finite projective plane is the one with  $q = 2$ . It consists of seven points and seven lines with three points on every line and three lines through every point. This projective plane is called the *Fano plane* and may be illustrated as shown in Figure 2.1. The points are  $A, B, C, D, E, F,$  and  $G$  and the lines are  $ADC, AGE, AFB, CGF, CEB, DGB,$  and  $DEF$ . ■



**Figure 2.1:** The Fano Plane

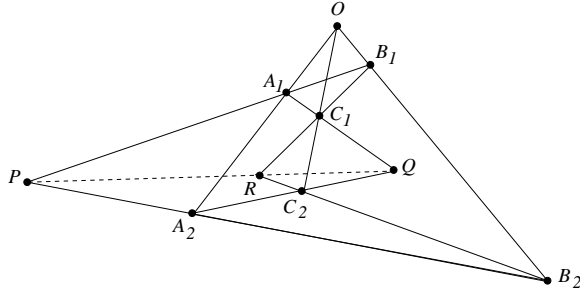
The number  $q$  is called the *order* of the projective plane, and in all known examples  $q$  is prime or a prime power. It is a fact that for any given prime power, there exists at least one projective plane of that order. It is not known whether planes of nonprime power order exist, although it is commonly believed that any finite projective plane must have prime power order. The following theorem, due to Bruck and Ryser [13], gives some restrictions on the possible existence of nonprime power order finite projective planes.

**Theorem 2.10** *If  $q$  is congruent to 1 or 2 mod 4, then there cannot be a projective plane of order  $q$  unless  $q = a^2 + b^2$  for some integers  $a$  and  $b$ . ■*

All of the projective planes with which we will be working satisfy a property that is based on a relationship between triangles. Two triangles  $ABC$  and  $XYZ$  are said to be *perspective from a point  $P$*  provided the lines  $AX$ ,  $BY$ , and  $CZ$  meet at  $P$ . The triangles are said to be *perspective from a line  $l$*  provided that the points  $AB \cap XY$ ,  $AC \cap XZ$ , and  $BC \cap XZ$  all lie on the line  $l$ . The planes that satisfy the following theorem of the real projective plane, due to Desargues, are called Desarguesian and those that do not are called non-Desarguesian.

**Theorem 2.11** *If two triangles are perspective from a point, they are perspective from a line. ■*

The theorem is illustrated in Figure 2.2; the intersections of corresponding lines,  $P$ ,  $Q$ , and  $R$ , are collinear. There are various equivalent statements of the Theorem of Desargues, most notably a finite plane is Desarguesian if and only if it can be coordinatized by a finite field. For the remainder of this dissertation, we restrict ourselves to the Desarguesian planes defined over the Galois Field  $\text{GF}(p^h)$



**Figure 2.2:** Desargues' Configuration

and coordinatized in the standard way. Such a plane is denoted  $\text{PG}(2, q)$ . This is consistent with earlier notation since projective geometries of dimension two constructed from vector spaces over finite fields are Desarguesian.

Some of the most popular objects to study in projective planes are quadrics and the results given in this dissertation deal heavily with nondegenerate quadrics. To begin our overview of quadrics in the projective plane, we examine the definition of a quadratic form over a vector space. Let  $\mathcal{E} = \text{GF}(q)$  and  $V = \mathcal{E}^3$ , viewed as a vector space.

**Definition 2.12** *A map  $Q : V \rightarrow \mathcal{E}$  is called a quadratic form of  $V$  provided*

(i)  $Q(cw) = c^2Q(w)$  for all  $c \in \mathcal{E}$ ,  $w \in V$ , and

(ii) for every  $u, v \in V$  the function  $f$  defined by  $f(u, v) = Q(u+v) - Q(u) - Q(v)$  is a symmetric, bilinear form called the polar form of  $Q$ .

**Definition 2.13** *The quadratic form  $Q$  of  $V$  with polar form  $f$  is said to be nondegenerate if the following is true: if  $Q(w) = 0$  and  $f(u, w) = 0$  for all  $u \in V$  then  $w = 0$ .*

If  $Q$  is a quadratic form of  $V$ , then  $Q(v) = 0$  implies that  $Q(cv) = 0$  for all  $c \in \mathcal{E}$ . This is the basis of the next definition.

**Definition 2.14** *Let  $Q$  be a quadratic form of the vector space  $V$ . The quadric of the projective plane  $PG(2, q)$  corresponding to  $Q$  is the set of all points  $\langle v \rangle$  of  $PG(2, q)$  with  $Q(v) = 0$ . A quadric is nondegenerate if its corresponding quadratic form is nondegenerate.*

**Definition 2.15** *A conic is a nonempty, nondegenerate quadric in the projective plane.*

For the results in this dissertation, we work with a quadratic form of  $V$  in the following context. If

$$A = \begin{bmatrix} \bar{a} & \bar{b} & \bar{d} \\ 0 & \bar{c} & \bar{e} \\ 0 & 0 & \bar{f} \end{bmatrix}$$

is a given upper triangular matrix, then  $B = A + A^T$  is symmetric. A quadratic form is given by  $Q(X) = XAX^T$ . The quadratic form  $Q$  is nonsingular and its polar form  $f(u, v)$  is nondegenerate provided  $(\bar{e}, \bar{d}, \bar{b})^T \in \text{Null}(B)$  and not on  $Q$ , in other words,  $4\bar{a}\bar{c}\bar{f} - \bar{a}\bar{e}^2 - \bar{b}^2\bar{f} + \bar{b}\bar{e}\bar{d} - \bar{c}\bar{d}^2 \neq 0$ . A quadric is

$$\{X \in PG(2, q) \mid Q(X) = XAX^T = 0\}$$

or equivalently,

$$\{(x, y, z) \in PG(2, q) \mid \bar{a}x^2 + \bar{b}xy + \bar{c}y^2 + \bar{d}xz + \bar{e}yz + \bar{f}z^2 = 0\}.$$

Moreover, the quadric is a conic provided  $4\bar{a}\bar{c}\bar{f} - \bar{a}\bar{e}^2 - \bar{b}^2\bar{f} + \bar{b}\bar{e}\bar{d} - \bar{c}\bar{d}^2 \neq 0$ .

Now, an *oval* is a set of  $q + 1$  points in the projective plane such that no three are collinear. We point out that a conic is an “algebraic” concept and an oval is

a “geometric” concept. It can be shown that every conic is an oval, that is every conic contains  $q + 1$  points, no three collinear. In 1954, Segre [60] proved the following theorem. (For an English version of this result, see [61].)

**Theorem 2.16** *Any oval in a finite Desarguesian projective plane of odd order is a conic.* ■

This result does not extend to projective planes of even order, and in Example 7 of Section 2.2.2.1, we give an example of an oval that is not a conic.

**Observation 2.17** *The image of a quadric under any projectivity in  $PGL(3, q)$  is a quadric.*

**Proof:** Let  $Q(X) = XAX^T$  be a quadric and let  $B \in PGL(3, q)$ . Observe that

$$\begin{aligned} Q(X) = XAX^T &= X(BB^{-1}AB^{-T}B^T)X^T \\ &= (XB)(B^{-1}AB^{-T})(XB)^T \\ &= Y(B^{-1}AB^{-T})Y^T \\ &= Q'(Y), \end{aligned}$$

where  $Y = XB$ . Then  $Q'(X) = (XB)(B^{-1}AB^{-T})(XB)^T$  is also a quadric. Hence, the image of a quadric under  $PGL(3, q)$  is also a quadric. ■

**Theorem 2.18** [35, Thm. 7.4]  *$PGL(3, q)$  acts transitively on the set of conics of  $PG(2, q)$ .* ■

We now examine the subgroup of  $\text{PGL}(3, q)$  leaving a nonsingular quadric in the plane invariant, denoted by  $\text{PGO}(3, q)$ , which can be represented by,

$$\text{PGO}(3, q) = \left\{ A = \begin{pmatrix} a^2 & ab & b^2 \\ 2ac & ad + bc & 2bd \\ c^2 & cd & d^2 \end{pmatrix} : ad \neq bc \text{ and } a, b, c, d \in \text{GF}(q) \right\}.$$

**Lemma 2.19** *PGO(3, q) acts sharply triply transitively on the points of a conic in the plane PG(2, q).*

**Proof:** By Theorem 2.18, we may map any conic in  $\text{PG}(2, q)$  to the conic  $\mathcal{C}$  with equation  $y^2 = xz$ . That is,  $\mathcal{C} = \{(t^2, t, 1) \mid t \in \text{GF}(q)\} \cup \{(1, 0, 0)\}$ . We show  $\text{PGO}(3, q)$  is sharply triply transitive on the points of  $\mathcal{C}$  by first showing that  $\text{PGO}(3, q)$  acts transitively on the points of  $\mathcal{C}$ , and then examining one and two point stabilizers. We follow this by arguing that only the identity element of  $\text{PGO}(3, q)$  fixes three points of  $\mathcal{C}$ .

Let  $H_1 = \left\{ \begin{pmatrix} a^2 & ab & b^2 \\ 0 & ad + bc & 0 \\ c^2 & cd & d^2 \end{pmatrix} : a, b, c, d \in \text{GF}(q) \right\} \in \text{PGO}(3, q)$ . For  $A \in H_1$ , observe that  $(1, 0, 0) \cdot A = (a^2, ab, b^2)$  is a conic point. Moreover, the orbit of  $(1, 0, 0)$  under  $H_1$  contains every point of the conic, since  $a$  and  $b$  cannot both be simultaneously 0. So,  $\text{PGO}(3, q)$  is transitive on the points of  $\mathcal{C}$ .

Let  $H_2 = \left\{ \begin{pmatrix} a^2 & ab & b^2 \\ 0 & ad & 0 \\ 0 & 0 & d^2 \end{pmatrix} : a, b, c, d \in \text{GF}(q) \right\} \in \text{PGO}(3, q)$  where  $a, d \neq 0$ . For  $B \in H_2$ , observe that  $(0, 0, 1) \cdot B = (0, 0, 1)$  and so  $B$  fixes the conic point  $(0, 0, 1)$ . Now,  $(1, 0, 0) \cdot B = (a^2, ab, b^2)$  is a conic point. Moreover, the orbit of  $(1, 0, 0)$  under  $H_2$  contains every point of the conic except for  $(0, 0, 1)$ , since  $a \neq 0$ . Thus,  $\text{PGO}(3, q)$  is doubly transitive on the points of  $\mathcal{C}$ .

Let  $H_3 = \left\{ \begin{pmatrix} a^2 & 0 & 0 \\ 0 & ad & 0 \\ 0 & 0 & d^2 \end{pmatrix} : a, b, c, d \in \text{GF}(q) \right\} \in \text{PGO}(3, q)$  where  $a, d \neq 0$ . For  $C \in H_3$  observe that  $(0, 0, 1) \cdot C = (0, 0, 1)$  and  $(1, 0, 0) \cdot C = (1, 0, 0)$ , and we have that  $C$  fixes both  $(0, 0, 1)$  and  $(1, 0, 0)$ . Now,  $(1, 1, 1) \cdot C = (a^2, ad, d^2)$  which is a point of the conic. Moreover, the orbit of  $(1, 1, 1)$  under  $H_3$  contains every point of the conic except for the two points  $(0, 0, 1)$  and  $(1, 0, 0)$ , since  $a, d \neq 0$ . Thus,  $\text{PGO}(3, q)$  is triply transitive on the points of  $\mathcal{C}$ .

To show  $\text{PGO}(3, q)$  is sharply triply transitive, we need to show that the only element in  $\text{PGO}(3, q)$  that fixes three points of the conic is the identity element. We have already shown that  $\text{PGO}(3, q)$  is triply transitive on  $\mathcal{C}$ , so suppose

$$M = \begin{pmatrix} a^2 & ab & b^2 \\ 2ac & ad + bc & 2bd \\ c^2 & cd & d^2 \end{pmatrix} \in \text{PGO}(3, q)$$

fixes the three points  $(1, 0, 0)$ ,  $(0, 0, 1)$ , and  $(1, 1, 1)$  of  $\mathcal{C}$ . Now,  $(1, 0, 0) \cdot M = (a^2, ab, b^2) = (1, 0, 0)$  implies that  $b = 0$  and  $(0, 0, 1) \cdot M = (c^2, cd, d^2) = (0, 0, 1)$  implies that  $c = 0$ , so that

$$M = \begin{pmatrix} a^2 & 0 & 0 \\ 0 & ad & 0 \\ 0 & 0 & d^2 \end{pmatrix}.$$

Now,  $(1, 1, 1) \cdot M = (a^2, ad, d^2) = (1, 1, 1)$ , and we have that  $a = d$ . Hence,

$$M = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

which is the identity element in  $\text{PGO}(3, q)$ . Thus, there is a unique collineation that fixes three points of the conic, and so  $\text{PGO}(3, q)$  is sharply triply transitive on the points of the conic in  $\text{PG}(2, q)$ . ■

Because of the significant variations between the properties of conics in planes of even order with the properties of conics in planes of odd order, we will discuss these situations separately.

### 2.2.2.1 Planes of Even Order

Since the conic blocking set material revolves around points and lines of the plane and their relationships with conics, it is necessary to discuss these relationships in detail. We begin with the classification of lines and points of the plane with respect to a conic from a geometric viewpoint, and then offer an algebraic method for classifying points and line with respect to conics. We include relevant counts pertaining to points, lines, and conics; although, an explanation of how to derive these counts is not offered.

Since no three points of a conic, denoted  $\mathcal{C}$ , are collinear, any line  $l$  in  $\pi$  can intersect  $\mathcal{C}$  in at most two points. Hence,  $l$  is geometrically classified in the following way:

- $l$  is a *tangent line* to  $\mathcal{C}$  provided  $|l \cap \mathcal{C}| = 1$ ,
- $l$  is a *secant line* to  $\mathcal{C}$  provided  $|l \cap \mathcal{C}| = 2$ ,
- $l$  is an *exterior line* to  $\mathcal{C}$  provided  $|l \cap \mathcal{C}| = 0$ .

There are  $q + 1$  tangent lines,  $\frac{q(q+1)}{2}$  secant lines, and  $\frac{q(q-1)}{2}$  exterior lines with respect to  $\mathcal{C}$ .

Similarly, the points of the plane are geometrically classified with respect to a conic. If  $P$  is a point in a plane of even order, then  $P$  is classified in three ways with respect to  $\mathcal{C}$ :

- if  $P$  is on  $\mathcal{C}$ ,  $P$  is called a *conic point*,
- if  $P$  is the unique point not on  $\mathcal{C}$ , that lies on all the tangent lines to  $\mathcal{C}$ ,  $P$  is called the *nucleus*, and
- if  $P$  is not on  $\mathcal{C}$  and not the nucleus, then  $P$  is often referred to as a *regular point*.

Any conic point has one tangent and  $q$  secants through it. While the nucleus has  $q + 1$  tangents through it, the remaining points have exactly one tangent,  $\frac{q}{2}$  secant and  $\frac{q}{2}$  exterior lines through them.

In order to describe algebraically the relationship between points and lines with respect to conics, we need to recall from Section 2.1, the method for determining the number of solutions to a quadratic equation. Although there are no new concepts developed here for determining the relationship between lines in the plane with a conic, we are grateful to S. E. Payne [55] for his help with this review. Given any quadratic equation over a field  $\mathcal{E}$  of even characteristic of the form

$$ax^2 + bx + c = 0 \text{ with } a \neq 0, \tag{2.3}$$

the number of solutions to this equation is determined by computing the absolute trace of  $ac/b^2$ , if  $b \neq 0$ . That is,

1. if  $\text{Tr}(ac/b^2) = 1$ , then there are no solutions, and
2. if  $\text{Tr}(ac/b^2) = 0$ , then there are two solutions.

Let  $\Pi$  be a projective plane of even order and  $C'$  some conic in  $\Pi$  with nucleus  $N'$ . The Fundamental Theorem allows us to select any three points of  $C'$

and the nucleus,  $\{P'_0, P'_1, P'_2, N'\}$ , and map this ordered set to the ordered set  $\{(1, 0, 0), (0, 0, 1), (1, 1, 1), (0, 1, 0)\}$ . There is a unique conic satisfying the given conditions, and it has equation  $y^2 + xz = 0$ . Note that this is due to the fact that three points and the nucleus determine a conic in planes of even characteristic.

Since any conic in the plane can be mapped to  $y^2 + xz = 0$ , we can use this particular conic to illustrate the algebraic method for determining how a line meets a conic in a plane of even order. Each line  $l$  in the plane has an equation of the form  $mx + ny + pz = 0$ . Every tangent line to  $C$  must contain the nucleus and, therefore,  $n = 0$  for all tangent lines to  $C$ .

$$(0, 1, 0) \cdot \begin{bmatrix} m \\ n \\ p \end{bmatrix} = 0 \Rightarrow n = 0.$$

Thus, the tangent lines to this conic are easily detected.

To classify the remaining lines in the plane with respect to  $C$ , assume that  $n \neq 0$ , so that without loss of generality  $n = 1$ . Any non-tangential line in the plane to  $C$  has an equation of the form  $mx + y + pz = 0$ , and a typical point on this line is given by  $T = (x, mx + pz, z)$ . The line with equation  $mx + y + pz = 0$  is either an exterior or a secant line to  $C$ , and we must determine how the line meets  $C$ . If  $T$ , on the line, is also on the conic, then necessarily  $(mx + pz)^2 + xz = 0$ , or rather

$$m^2x^2 + xz + p^2z^2 = 0. \tag{2.4}$$

If  $x = 0$ , then  $p = 0$  or  $z = 0$ . In the case that  $z = 0$ , we have  $T = (0, 0, 0)$ , and this cannot occur. On the other-hand, if  $p = 0$ , the line has equation  $mx + y = 0$ , and the point  $(0, 0, 1)$  of the conic also lies on this line. The line  $y = mx$  is not

a tangent line, so there must be another point of the conic on this line; namely, a point with coordinates of the form  $(x, mx, m^2x)$ . But, when  $x = 0$ , this form gives  $(0, 0, 0)$ , so  $x \neq 0$ . If  $p = 0$ , but  $x \neq 0$ ,  $l$  is a secant line as the points  $(0, 0, 1)$  and  $(1, m, m^2)$  lie on both  $l$  and  $C$ . Assume now that  $x \neq 0$  and  $p \neq 0$ . We divide both sides of (2.4) by  $x^2$  to obtain

$$m^2 + \left(\frac{z}{x}\right) + p^2 \left(\frac{z}{x}\right)^2 = 0$$

or, rather

$$p^2 \left(\frac{z}{x}\right)^2 + 1 \left(\frac{z}{x}\right) + m^2 = 0. \quad (2.5)$$

If we let  $\frac{z}{x} = \frac{t}{p^2}$  and  $\delta = m^2p^2$ , (2.5) becomes

$$t^2 + t + \delta = 0. \quad (2.6)$$

From the previous section, we can determine how many solutions there are to (2.6) and so (2.5). If  $\text{Tr}(\delta) = 1$ , (2.6) and so (2.5) have no solutions, and therefore  $l$  is an exterior line to  $C$ . If  $\text{Tr}(\delta) = 0$ , (2.6) and so (2.5) have two solutions, and therefore  $l$  is a secant line to  $C$ .

In conclusion, even though the quadratic formula cannot be used to determine if a line is a secant or exterior line to a conic, the absolute trace function can be used to make this distinction. For the quadratic equation given in (2.3), we have that, when  $b \neq 0$ , if

$$\text{Tr}\left(\frac{ac}{b^2}\right) = \begin{cases} 1, & \text{there are no solutions, and the line is exterior} \\ 0, & \text{there are two solutions, and the line is secant.} \end{cases} \quad (2.7)$$

If  $b = 0$ , there is one solution and the line is tangent.

**Example 6.**

Consider the conic with equation  $\mathcal{C} : xy+xz+z^2 = 0$  and nucleus  $N = (0, 1, 1)$ . The point  $(0,0,1)$  is not on  $\mathcal{C}$  and the  $q + 1$  lines through  $(0,0,1)$  are  $x = 0$  and  $mx + y = 0$ ,  $m \in \text{GF}(q)$ . Using the methods previously discussed, the relationship between the lines through  $(0,0,1)$  and the conic  $\mathcal{C}$  is easily identifiable. The line with equation  $mx + y = 0$  is a secant line when  $\text{Tr}(m) = 0$ , and the line  $x = 0$  is a tangent line to  $\mathcal{C}$ . ■

Classifying points in the plane with respect to a fixed conic is a much simpler task than classifying lines. Let  $Q(x, y, z)$  be the quadratic form of the conic described by the equation

$$\mathbf{A}x^2 + \mathbf{B}xy + \mathbf{C}y^2 + \mathbf{D}xz + \mathbf{E}yz + \mathbf{F}z^2 = 0. \quad (2.8)$$

If  $P = (\bar{x}, \bar{y}, \bar{z})$  satisfies  $Q(P) = 0$ ,  $P$  is a conic point. If  $P = (\mathbf{E}, \mathbf{D}, \mathbf{B})$ , then from [35, Cor. 7.12],  $P$  is the nucleus of the conic. Otherwise, it must be that if  $Q(\bar{x}, \bar{y}, \bar{z}) \neq 0$  and  $P \neq (\mathbf{E}, \mathbf{D}, \mathbf{B})$ ,  $P$  is neither on the conic nor the nucleus of the conic.

The nucleus of the quadric is special in the sense that knowing the nucleus allows us to determine if the quadric is singular. In fact, Hirschfeld [35, Thm. 7.16] shows that if  $Q(\mathbf{E}, \mathbf{D}, \mathbf{B}) = 0$ , the quadric is singular and therefore is not a conic.

In planes of even order, there are examples of ovals which are not conics. In [35], we find that for  $q = 2$  and  $4$  every oval is a conic. In the planes of order  $\geq 8$ , there are ovals which are not conics. The following example illustrates the situation.

**Example 7.**

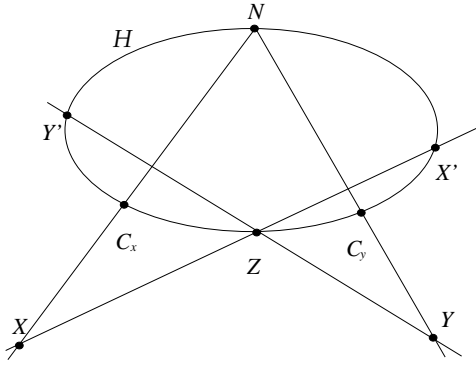
Let  $\mathcal{C}$  be a conic in the projective plane  $\text{PG}(2, q)$ ,  $q \geq 8$  and even, and let  $\mathcal{N}$  be the nucleus of  $\mathcal{C}$ . Let  $\mathcal{H}$  denote the *hyperoval* which consists of the  $q + 1$  points of  $\mathcal{C}$  and the nucleus of  $\mathcal{C}$ . So,  $\mathcal{H}$  is a set of  $q + 2$  points with the property that no three are collinear. And by construction, there are no tangent lines to  $\mathcal{H}$ . Any line in the plane must be either a secant line or an exterior line. Let  $\mathcal{O}$  be the oval which consists of  $\mathcal{N}$  and any  $q$  points of  $\mathcal{C}$ . Recall that five points, no three collinear, determine a unique conic.  $\mathcal{C}$  and  $\mathcal{O}$  have  $q$  points in common and these  $q$  points satisfy a quadratic equation. But, the point  $\mathcal{N}$  of  $\mathcal{O}$  does not satisfy this quadratic equation. Hence, there is no quadratic equation which every point of  $\mathcal{O}$  satisfies, so  $\mathcal{O}$  is not a conic. ■

Before we develop similar concepts for planes of odd order, we examine the orbits of points of the plane under the action of a group of collineations which stabilizes a conic (that is, leaves the set of points of the conic invariant). This information proves useful in a model used for finding conic blocking sets in Chapter 3.

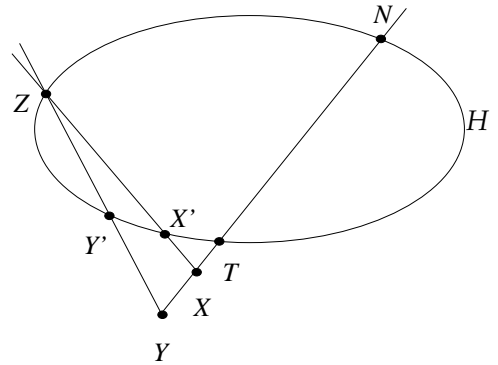
**Lemma 2.20** *The group of collineations which stabilize a conic has three orbits of the points of a plane.*

**Proof:** Let  $\mathcal{C}$  be a conic,  $N$  be the nucleus of this conic, and  $\mathcal{H} = \mathcal{C} \cup \{N\}$  be the corresponding hyperoval. Any collineation that stabilizes the conic will also stabilize its nucleus, since every conic has a unique nucleus. We consider two cases, one where two distinct points off of  $\mathcal{C}$  do not lie on a common tangent line and the other where these two points do lie on a common tangent line.

Let  $X$  and  $Y$  be two points off of  $\mathcal{H}$ . If the tangent line joining  $X$  to  $N$  is distinct from the tangent line joining  $Y$  to  $N$ , let  $C_x$  and  $C_y$  be the corresponding conic points on these tangent lines. Let  $Z$  be an arbitrary conic point not  $N$ ,  $C_x$ , or  $C_y$ . Let  $XZ \cap \mathcal{C} = X'$  and  $YZ \cap \mathcal{C} = Y'$ . Since  $\text{PGO}(3, q)$  is sharply triply transitive, there is a unique collineation,  $\Gamma$ , such that  $Z\Gamma = Z$ ,  $C_x\Gamma = C_y$ , and  $X'\Gamma = Y'$ . And so,  $X\Gamma = (NC_x \cap X'Z)\Gamma = (NC_y \cap Y'Z) = Y$ , and when  $X$  and  $Y$  do not lie on a common tangent line, we have that they are in the same orbit.



**Figure 2.3:**  $X$  and  $Y$  Not on a Common Tangent Line



**Figure 2.4:**  $X$  and  $Y$  on a Common Tangent Line

If  $X$  and  $Y$  are on the same tangent line, then let  $T$  be the point of the conic on this tangent line. Let  $Z$  be an arbitrary conic point other than  $T$  and not  $N$ . Let  $X' = XZ \cap \mathcal{C}$  and  $Y' = YZ \cap \mathcal{C}$ . Since  $\text{PGO}(3, q)$  is sharply triply transitive, there is a unique collineation,  $\Gamma$ , such that  $Z\Gamma = Z$ ,  $T\Gamma = T$ , and  $X'\Gamma = Y'$ . Thus,  $X\Gamma = (NT \cap X'Z)\Gamma = (NT \cap Y'Z) = Y$ .

Combining these two cases, we have that there exists a collineation that stabilizes the conic, fixes the nucleus, and maps  $X$  to  $Y$  for any points  $X$  and  $Y$  off of  $\mathcal{C}$  and not the nucleus of  $\mathcal{C}$ . ■

### 2.2.2.2 Planes of Odd Order

In planes of odd order, every oval is a conic. That is, the geometric object we call an oval can be described algebraically as a conic. This was first proved by Segre in [60]. For a proof that every conic is an oval in English, the reader is directed to [61]. This fact is occasionally used for conic blocking sets results. As every conic is an oval and an oval has  $q + 1$  points on it, every conic consists of  $q + 1$  points that satisfy some nondegenerate quadratic equation.

Since the conic blocking set material revolves around points and lines of the plane and their relationships with conics, it is necessary to discuss these relationships in detail. We begin with the classification of lines and points of the plane with respect to a conic from a geometric viewpoint, and then offer the algebraic method for classifying points and line with respect to conics. We summarize relevant counts pertaining to points, lines, and conics.

Since no three points of a conic  $\mathcal{C}$  are collinear, any line  $l$  in  $\pi$  can intersect  $\mathcal{C}$  in at most two points. Hence,  $l$  is geometrically classified in the following way:

- $l$  is a *tangent line* to  $\mathcal{C}$  provided  $|l \cap \mathcal{C}| = 1$ ,
- $l$  is a *secant line* to  $\mathcal{C}$  provided  $|l \cap \mathcal{C}| = 2$ ,
- $l$  is an *exterior line* to  $\mathcal{C}$  provided  $|l \cap \mathcal{C}| = 0$ .

There are  $q + 1$  tangent lines,  $\frac{q(q+1)}{2}$  secant lines, and  $\frac{q(q-1)}{2}$  exterior lines with respect to  $\mathcal{C}$ .

Similar to geometrically classifying the lines in the plane with respect to a conic, we geometrically classify the points of the plane with respect to a conic. If  $P$  is a point in the plane then  $P$  is classified in three ways with respect to  $\mathcal{C}$ :

- if  $P$  is on  $\mathcal{C}$ ,  $P$  is called a *conic point*,
- if  $P$  is not on  $\mathcal{C}$ , but on a tangent line to  $\mathcal{C}$ ,  $P$  is called an *exterior point*,  
and
- if  $P$  is neither on  $\mathcal{C}$  nor on a tangent line to  $\mathcal{C}$ ,  $P$  is called an *interior point*.

Any conic point has one tangent and  $q$  secants through it. While an interior point has  $\frac{q+1}{2}$  secants and  $\frac{q+1}{2}$  exterior lines through it, an exterior point has exactly two tangents,  $\frac{q-1}{2}$  secant and  $\frac{q-1}{2}$  exterior lines through it.

Algebraically, classifying the lines of the plane with respect to a conic is similar to the classification method in the Euclidean plane.

Let  $ax - by + cz = 0$  be the equation of a line in the plane. Since not all of the coefficients of the line are zero, suppose that  $b \neq 0$  and then solve for  $y$ . The line now has equation

$$y = a'x + c'z, \tag{2.9}$$

where  $a' = a/b$  and  $c' = c/b$ . Substitute (2.9) into (2.3) to obtain the quadratic equation

$$A'x^2 + B'xz + C'z^2 = 0 \tag{2.10}$$

where  $A' = \mathbf{A} + \mathbf{B}a' + \mathbf{C}a'^2$ ,  $B' = \mathbf{B}c' + 2\mathbf{C}a'c' + \mathbf{E}a' + \mathbf{D}$ , and  $C' = c'^2 + \mathbf{E}c' + \mathbf{F}$ . If  $z = 0$ , there is one solution to (2.10) provided  $A' \neq 0$ , and  $y = a'x + c'z$  is a

tangent line. If  $z \neq 0$ , we may divide (2.10) through by  $z^2$  to obtain a quadratic equation in one variable,

$$A'x'^2 + B'x' + C' = 0. \quad (2.11)$$

If  $A' = 0$  and  $B' = 0$ , then necessarily  $C' = 0$  implying that  $\mathcal{C}$  is degenerate, a contradiction. If  $A' = 0$  and  $B' \neq 0$ , there is clearly one solution to (2.11), and the line is a tangent line. Else, if  $A' \neq 0$ , we can use the discriminant of the quadratic equation to determine how many solutions there are to (2.11) and thereby determine the type of line with which we are dealing. If  $B'^2 - 4A'C' = 0$ , the line given in (2.9) is a tangent line. If the discriminant is a square, then the line is a secant line. If the discriminant is a nonsquare, the line is exterior to the conic.

Algebraically, classifying points with respect to a conic is not as intuitive as classifying lines with respect to a conic. We defer introducing the algebraic method for classifying points as introduced to us by S.E. Payne in [54], until Section 4.3.1.1.

The proof of the following theorem, given in [35, Thm. 7.16], states that if the symmetric  $3 \times 3$  matrix representing the quadratic form is nonsingular, then the zeros of the quadratic form a conic.

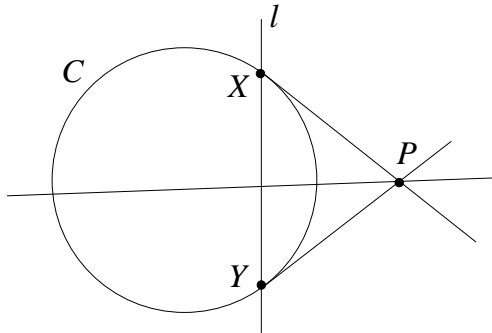
**Theorem 2.21** *If  $\mathcal{F} = \sum_{i \leq j} a_{ij}X_iX_j$ , then  $\mathcal{F}$  is singular if and only if  $\delta = 0$ , where*

$$\delta = 4a_{00}a_{11}a_{22} + a_{01}a_{02}a_{12} - a_{00}a_{12}^2 - a_{11}a_{02}^2 - a_{22}a_{01}^2.$$

■

**Definition 2.22** [43] *Let  $\mathcal{C}$  be a conic and  $l$  a secant line to  $\mathcal{C}$  through the points  $X$  and  $Y$  of  $\mathcal{C}$ . The tangent lines to  $\mathcal{C}$  through both  $X$  and  $Y$  will intersect at a*

point  $P \notin \mathcal{C}$ . We call  $l$  the polar of  $P$  and  $P$  the pole of  $l$ . The polars of  $X$  and  $Y$  are the tangent lines to  $X$  and  $Y$  respectively.



**Figure 2.5:** Constructing the Polar of a Point with Respect to a Conic

The assignment of pole to polar and polar to pole with respect to a conic, is an example of a polarity. A *polarity* is a one-to-one correspondence between points and lines of a projective plane that preserves the relation of incidence and is of order two. That is, it sends points into lines, lines into points, ranges into pencils, pencils into ranges, quadrangles into quadrilaterals, and so forth. One of the nice properties of polarities is that if a polarity sends  $A$  to its polar  $a$ , then it sends  $a$  to its pole  $A$ . [21]

We examine the orbits of the points of the plane under the group of collineations which stabilize a conic. This information proves useful in a model used for finding conic blocking sets in Chapter 4. Let  $G(Q)$  be the subgroup of  $\text{PGL}(3, q)$  stabilizing the conic  $Q$ . Let

$$\begin{aligned} \mathcal{O}_1 &= \text{points on } Q, \\ \mathcal{O}_2 &= \text{points off } Q, \end{aligned}$$

$$\begin{aligned}
\mathcal{O}_3 &= \text{tangents to } \mathbb{Q}, \\
\mathcal{O}_4 &= \text{secants of } \mathbb{Q}, \\
\mathcal{O}_5 &= \text{external lines of } \mathbb{Q}.
\end{aligned}$$

Since  $\text{PGO}(3, q)$  is sharply triply transitive on conics,  $G(\mathbb{Q})$  acts triply transitively on  $\mathcal{O}_1$  and  $\mathcal{O}_3$ . For  $q$  odd, we have that

$$\mathcal{O}_2 = \mathcal{O}_2^+ \cap \mathcal{O}_2^-,$$

where

$$\mathcal{O}_2^+ = \{\text{external points of } \mathbb{Q}\}, \quad \mathcal{O}_2^- = \{\text{internal points of } \mathbb{Q}\}.$$

**Lemma 2.23** [36]

- (i)  $G(\mathbb{Q})$  act transitively on  $\mathcal{O}_4$  and  $\mathcal{O}_5$ ;
- (ii)  $G(\mathbb{Q})$  has two orbits on  $\mathcal{O}_2$ , namely  $\mathcal{O}_2^+$  and  $\mathcal{O}_2^-$ .

**Proof:**

Let  $\mathbb{Q}$  be the set of points that satisfy  $x^2 + yz = 0$ . Consider the action of  $G(\mathbb{Q})$  on  $\mathcal{O}_2$ , the points off  $\mathbb{Q}$ . Since each point of  $\mathcal{O}_2^+$  is the intersection of two tangents,  $\mathbb{Q}$  is transitive on  $\mathcal{O}_2^+$ , the external points, and by the polarity on  $\mathcal{O}_4$ , the secants.

Any external line contains an external point. So, to show the transitivity of  $G(\mathbb{Q})$  on  $\mathcal{O}_5$ , and by polarity on  $\mathcal{O}_2^-$ , it suffices to show the transitivity on the external lines through a particular external point. Let  $U_0 = (1, 0, 0)$  be this point. Then the line  $l_t$  given by the equation  $y + tz = 0$  is a secant or external line if  $t$  is a nonzero square or nonsquare respectively. The projectivity  $\Gamma_c$ ,  $c \neq 0$ ,

given by  $(x, y, z)\Gamma_c = (cx, y, c^2z)$  fixes  $Q$  and transforms  $l_t$  to  $l_{\frac{t}{c^2}}$ . So, we can pass from any secant through  $U_0$  to any other secant through  $U_0$  and any external line through  $U_0$  to any other external line through  $U_0$ . So,  $G(Q)$  is transitive on  $\mathcal{O}_5$ , the external lines, and by the polarity on  $\mathcal{O}_2^-$ , the internal points. ■

Due to Lemma 2.23, we have that the stabilizer of a conic in a plane of odd order has these three orbits:

1. the conic,
2. the set of external points of the conic, and
3. the set of internal points of the conic.

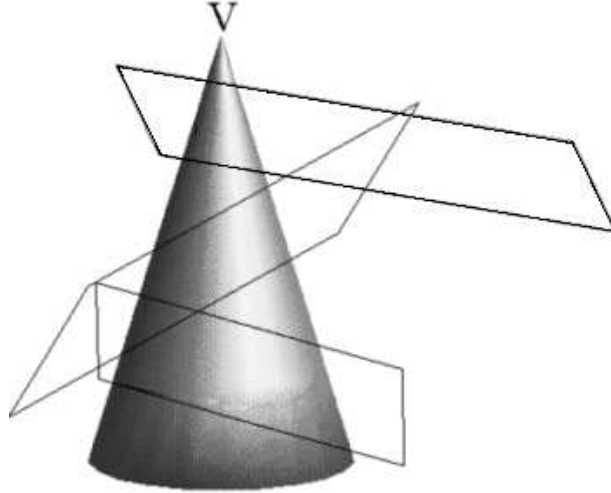
### 2.2.3 Projective Three-Space

As in the previous sections, the material presented in this section is meant to serve as a cursory review of some of the basic ideas from finite projective three-space that is relevant to the work presented in Chapters 3 and 4. We forego an in-depth examination of an analogous axiomatic definition, as given in the previous section, as well as the vector space construction described in Section 2.2, of projective three-space.

A plethora of geometrical objects exist in projective three-space; such as ovoids, generalized quadrangles,  $k$ -caps, spreads, and flocks. Of these, we are most interested in flocks.

Assume  $\text{PG}(2, q)$  is a subspace of  $\text{PG}(3, q)$ , and let  $\mathcal{C}$  be a conic in  $\text{PG}(2, q)$  with  $V$  (the vertex) a point in  $\text{PG}(3, q) \setminus \text{PG}(2, q)$ . A *quadratic cone*  $K$  is the union of the points on the lines joining  $V$  to the  $q + 1$  points of  $\mathcal{C}$ . A *flock* of a

cone  $K$  is a set of  $q$  planes in  $\text{PG}(3, q)$  which do not contain  $V$  such that no two planes of the flock meet at a point of  $K$ . This definition of flock differs from that



**Figure 2.6:** Flock of a Cone

found in the majority of papers dealing with flocks. The more common definition of a flock refers to the conics that partition the cone instead of the planes whose sections partition the cone. However, the difference is only a matter of viewpoint. If the  $q$  planes of the flock contain a common line, the flock is said to be *linear*.

Consider the flock  $F$  whose planes have equations

$$xt + f(t)y + g(t)z + w = 0,$$

where  $f, g \in \text{GF}(q)[x]$  with  $f(0) = g(0) = 0$ . If  $f$  and  $g$  are additive, we say  $F$  is a *semifield flock*. When  $q$  is even, Johnson [42] has shown that all semifield flocks are linear. In [29], Gevaert and Johnson have shown that the flock  $F$  is a semifield flock if and only if  $f$  and  $g$  are additive.

The *Knuth-Kantor semifield flock* [44] is one of the three classes of nonlinear semifield flocks known. For  $q$  odd and  $t \in \text{GF}(q)$ , the planes  $\pi_t$  are defined to be:

$$\pi_t : tx - mt^\sigma y + w = 0,$$

where  $m$  is a fixed nonsquare and  $\sigma$  is an automorphism of the field. These planes define a semifield flock of the cone  $K$ . This flock is linear if and only if  $\sigma = 1$ .

**Theorem 2.24** [69, 70] *In  $PG(3, p^2)$ , for any prime  $p$ , the semifield flocks are linear or else they are Knuth-Kantor semifield flocks. ■*

More will be said about the Knuth-Kantor flocks in Chapter 4.

In the past few years, W. Cherowitzo has made significant strides in generalizing the theory of flocks of cones by removing the restriction that the flock is a flock of a cone with a quadratic base. That is, by slightly revising some basic definitions, it is possible to consider flocks of cones whose base may range over anything from the empty set, a line, or even a random collection of points in the carrier plane. To examine his most recent advances in generalizing the theory of flocks, see [18]. In Chapter 5, we give a conic blocking set application for this general theory of flocks.

It is worth noting here that it is often more convenient to work with flocks in the dual setting which we will develop in Chapter 5.

### 2.3 Blocking Sets of Lines

Line blocking sets originate from game theoretical problems. Richardson [58] defines a *finite projective game*, in the plane, by taking as players the points of the projective plane and specifying the lines of the plane as minimal winning coalitions. A *blocking coalition* is a set of points containing no line but intersecting

every line. A *minimum blocking coalition* is a blocking coalition of smallest cardinality. Isbell [40] also examines these games, but not from a geometric viewpoint. In [25], DiPaola examines minimal blocking coalitions in planes of order  $\leq 9$  and makes the note that the blocking coalition concepts provide working material for game theorists who work with *simple games*. In recent years, researchers have made huge strides in studying blocking coalitions. We give a brief introduction to the results obtained and direct the reader to [35] for more details and references.

### 2.3.1 Definitions and Examples

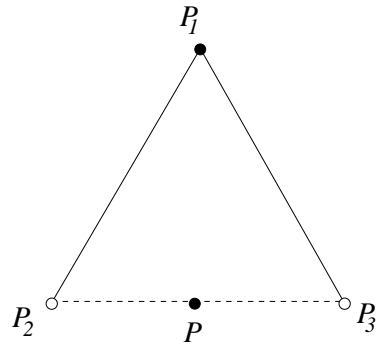
A *blocking set*  $\mathcal{B}$  in  $\Pi = \text{PG}(2, q)$  is a subset of points of  $\Pi$  which meets every line but contains no line completely; that is,  $1 \leq |\mathcal{B} \cap l| \leq q$  for every line  $l$  in  $\Pi$ . If  $|\mathcal{B}| = k$ ,  $\mathcal{B}$  is called a *blocking  $k$ -set*. It follows immediately from the definition that the complement of a blocking set,  $\Pi \setminus \mathcal{B}$ , is also a blocking set.

A blocking set is *irreducible* if  $\mathcal{B} \setminus \{P\}$  is not a blocking set for any  $P \in \mathcal{B}$ . A blocking set of *Rédei type* in  $\text{PG}(2, q)$  is a blocking set of size  $q + m$  for which there is some line  $l \in \Pi$  for which  $|l \cap \mathcal{B}| = m$ .

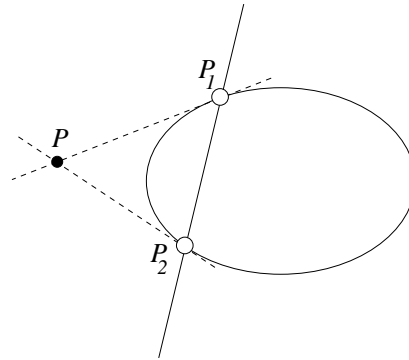
**Lemma 2.25** *A blocking set  $\mathcal{B}$  exists in  $\Pi$  if and only if  $q > 2$ . ■*

**Lemma 2.26** *The following are irreducible blocking sets in  $\Pi = \text{PG}(2, q)$ , when  $q > 2$ :*

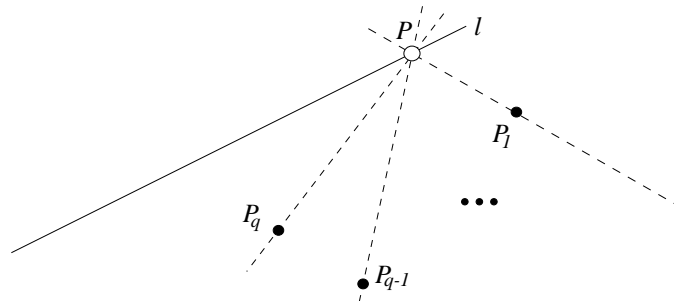
- (i) *the set  $\mathcal{B}_1 = \{P_1P_2 \cup P_1P_3 \cup P\} \setminus \{P_2, P_3\}$  of  $2q$  points consisting of the points on two sides of a triangle with vertices  $\{P_1, P_2, P_3\}$  and a point  $P$  on  $P_2P_3$ , minus the two vertices  $\{P_2, P_3\}$  of the triangle;*



(ii) the set  $\mathcal{B}_3 = (C \cup l \cup \{P\}) \setminus \{P_1, P_2\}$  of  $2q - 1$  points, where  $C$  is the set of points of a conic,  $l$  is a secant meeting  $C$  in  $P_1$  and  $P_2$ , and  $P$  is the intersection of the tangents to  $C$  at  $P_1$  and  $P_2$ ;



(iii) the set  $\mathcal{B}_2 = (l \setminus \{P\}) \cup \{P_1, \dots, P_q\}$  of  $2q$  points consisting of a line  $l$  minus a point  $P$  plus a set  $P_1, \dots, P_q$  of  $q$  points, one on each of the  $q$  lines through  $P$  other than  $l$ , but with  $P_1, \dots, P_q$  not all collinear;



(iv) a Baer subplane  $PG(2, \sqrt{q})$  of  $PG(2, q)$  consisting of  $q + \sqrt{q} + 1$  points, when  $q$  is a square;

(v) the set of  $q\sqrt{q} + 1$  points of a unital in  $PG(2, q^2)$ . ■

Of the irreducible blocking sets listed in Lemma 2.26, all are Rédei type blocking sets except for (v).

### 2.3.2 Bounds on the Size of Irreducible Blocking Sets

In this section, the upper and lower bounds on the sizes of blocking sets and irreducible blocking sets are given. As seen in Lemma 2.26, when  $q$  is a square, the points of a Baer subplane form a blocking set.

**Lemma 2.27** [14]

(i) If  $\mathcal{B}$  is a blocking  $k$ -set in  $PG(2, q)$ , then

$$q + \sqrt{q} + 1 \leq k \leq q^2 - \sqrt{q}.$$

(ii) A blocking  $k$ -set in  $PG(2, q)$  with  $k = q^2 - \sqrt{q}$  is the complement of a subgeometry  $PG(2, \sqrt{q})$ . ■

The next result is due to Bruen and Thas [15].

**Theorem 2.28**

(i) If  $\mathcal{B}$  is an irreducible blocking  $k$ -set in  $PG(2, q)$ , then  $k \leq q\sqrt{q} + 1$ .

(ii) Equality holds in (i) if and only if  $\mathcal{B}$  is a Hermitian arc (unital) and  $q$  is a square. ■

### 2.3.3 Rédei Blocking Sets

From Section 2.3.1,  $\mathcal{B}$  is a blocking set of Rédei type if  $\mathcal{B}$  is a blocking set with  $q + m$  points containing an  $m$ -secant. For any function  $f : \text{GF}(q) \rightarrow \text{GF}(q)$ , let

$$\mathcal{D}_f = \left\{ \frac{f(x) - f(y)}{x - y} \mid x, y \in \text{GF}(q); x \neq y \right\},$$

be the set of directions determined by  $f$ .

**Lemma 2.29** [35] *A blocking set of Rédei type can be constructed in  $PG(2, q)$  from any function  $f : \text{GF}(q) \rightarrow \text{GF}(q)$  unless  $f$  is linear or determines every direction.*

**Proof:** Take  $\mathcal{B}$  to be the  $k$ -set consisting of  $\{(t, f(t), 1) \mid t \in \text{GF}(q)\} \cup \{(1, d, 0) \mid d \in \mathcal{D}_f\}$ . Consider the lines through a point  $P$  on the the line  $z = 0$ . Either  $P$  is a point of the form  $(1, d_1, 0)$  for some  $d_1 \in \mathcal{D}_f$  or all the lines through  $P$  meet exactly one of the points of the form  $(t, f(t), 1)$ . The set  $\mathcal{B}$  contains a line if  $f$  determines every direction, in which case  $\mathcal{B}$  contains the line  $z = 0$ , or  $f$  is linear, in which case  $\mathcal{B}$  contains the line with equation  $tx + f(t)y + z = 0$ . Hence, the line  $z = 0$  is a  $|\mathcal{D}_f|$ -secant and so  $\mathcal{B}$  is a blocking set of Rédei type.  $\blacksquare$

Irreducible blocking sets can be constructed using Lemma 2.29.

**Lemma 2.30** [10] *The following are irreducible blocking sets  $\mathcal{B}$  in  $PG(2, q)$ , where  $\mathcal{B}$  is constructed as in Lemma 2.29.*

1. *If  $q$  is odd, let  $f(x) = x^{(q+1)/2}$ ; then  $f$  determines  $\frac{1}{2}(q + 3)$  directions and  $\mathcal{B}$  is an irreducible blocking set of size  $\frac{3}{2}(q + 1)$ .*
2. *Let  $f$  be the trace function from  $GF(q)$  to a subfield  $GF(q')$ ; then  $f$  determines  $q/q' + 1$  directions, and hence  $\mathcal{B}$  is a blocking set of size  $q + q/q' + 1$ .*

3. If  $q' \mid q$ , let  $f(x) = x^{q'}$ ; then  $f$  determines  $(q-1)/(q'-1)$  directions, and hence  $\mathcal{B}$  is a blocking set of size  $q + (q-1)/(q'-1)$ . ■

Choosing the  $m$ -secant to be the line at infinity  $l_\infty$ , we consider the set of directions determined by the set  $S = \mathcal{B} \setminus l_\infty$  of size  $q$ . Let  $S$  be a set of  $q$  points in  $\text{AG}(2, q) = \text{PG}(2, q) \setminus l_\infty$  and, with  $u = (u_1, u_2)$ ,  $v = (v_1, v_2)$ , let

$$\mathcal{D} = \left\{ \frac{u_2 - v_2}{u_1 - v_1} \mid u \neq v'u, v \in S \right\} \subset \text{GF}(q) \cup \{\infty\}$$

be the set of directions determined by the set  $S$ . As a converse to the examples of Lemma 2.30, the following result holds.

**Theorem 2.31** [5] *Let  $A \subset \text{AG}(2, q)$  be a point set of size  $q = p^h$ , let  $\mathcal{D}$  be the set of slopes of secants of  $S$ , and put  $m = |\mathcal{D}|$ . Let  $e$ , with  $0 \leq e \leq h$ , be the largest integer such that each line with slope in  $\mathcal{D}$  meets  $S$  in a multiple of  $p^e$  points. Then one of the following holds:*

1.  $e = 0$  and  $(q+3)/2 \leq m \leq q+1$ ;
2.  $e = 1$ ,  $p = 2$ , and  $(q+5)/3 \leq m \leq q-1$ ;
3.  $p^e > 2$ , where  $e$  divides  $h$ , and  $q/p^e + 1 \leq m \leq (q-1)/(p^e-1)$ ;
4.  $e = h$  and  $m = 1$ . ■

For more results on blocking sets of Rédei type, see [50], [5], and [11]. We will show in Chapter 5 that Theorem 2.31 has application to flocks of a cone.

For a more detailed introduction to blocking sets, see Chapter 13 of [35], which also contains an extensive list of references for results dealing with blocking sets from the past 30 years.

## 2.4 Blocking Sets of Conics

Recall, from Section 2.2.3, a *flock* of a quadratic cone with vertex  $V$  in  $\text{PG}(3, q)$  is a set of  $q$  planes not through  $V$  which do not intersect on the cone. There is a considerable amount of interest in flocks due to their connections with  $q$ -clans, spreads, translation planes, and generalized quadrangles. One interesting question about flocks that deserves further research is, if given a set of  $q$  planes in  $\text{PG}(3, q)$  and a point  $V$  not on any of the planes, does there exist a quadratic cone with vertex  $V$  having these planes as a flock? Using the conic blocking set results that are developed in this dissertation, we can start on an answer to this question.

A *conic blocking set* (CBS),  $\mathcal{B}$ , is a set of lines in a projective plane  $\pi$  which meets every conic in  $\pi$ . If every conic in  $\pi$  has at least one secant or tangent line in  $\mathcal{B}$ , then  $\mathcal{B}$  is a CBS. A CBS is *irreducible* if no proper subset of  $\mathcal{B}$  is a CBS. In other words,  $\mathcal{B}$  is irreducible if  $\mathcal{B} \setminus \{l\}$  is not a CBS for every line  $l$  in  $\mathcal{B}$ . A CBS of smallest cardinality is said to be *minimum*. Clearly, a minimum CBS is irreducible.

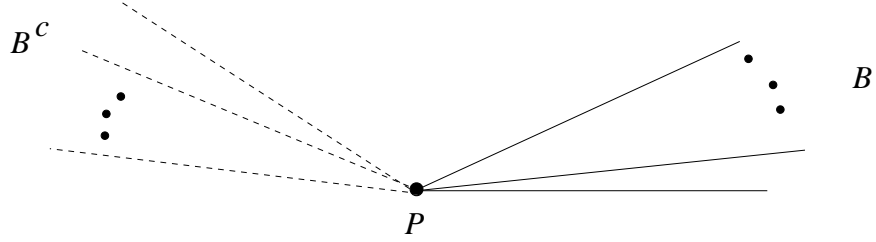
**Lemma 2.32** *If  $\pi$  is a projective plane, then  $\pi$  contains a CBS.*

**Proof:** Let  $\mathcal{B}$  consist of the  $q + 1$  lines through any point  $P$  in  $\pi$ . Clearly,  $\mathcal{B}$  contains all the points in  $\pi$ . Since every conic in  $\pi$  is contained in  $\mathcal{B}$ , every conic meets  $\mathcal{B}$  and  $\mathcal{B}$  is a conic blocking set. ■

Since the removal of any single line from the conic blocking set described in Corollary 2.32 is still a CBS, that CBS is neither minimum nor irreducible.

In the next two chapters, conic blocking sets in projective planes are closely examined. For the remainder of this dissertation, we make the restriction that all conic blocking sets consist of a set of concurrent lines through a specified

point,  $P$ . The *complement* of a CBS,  $\mathcal{B}^c$ , consists of the remaining lines through the point  $P$ . We say a CBS  $\mathcal{B}$  is *projectively equivalent* to another CBS  $\mathcal{B}'$  if



**Figure 2.7:** The Complement of a CBS

there exist an element  $A$  in  $\text{PGL}(3, q)$  such that  $A$  maps all the lines in  $\mathcal{B}$  to the lines in  $\mathcal{B}'$ . For instance, suppose  $\mathcal{B}$  is a CBS consisting of a subset of the lines  $\{y = mx + z \mid m \in \text{GF}(q)\}$  through  $(0, 1, 1)$ . Consider the element

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -1 & 1 \end{bmatrix}$$

in  $\text{PGL}(3, q)$ . Observe that  $(0, 1, 1) \cdot A = (0, 0, 1)$  and

$$A \cdot \begin{bmatrix} m \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} m \\ 1 \\ 0 \end{bmatrix}.$$

The set of lines of the form  $y = mx + z$  through the point  $(0, 1, 1)$  are projectively equivalent to the set of lines of the form  $y = mx$  through the point  $(0, 0, 1)$ . So, a CBS consisting of the subset of lines of the form  $y = mx + z$  is projectively equivalent to a CBS consisting of the lines of the form  $y = mx$ , since the projectivity maps conics to conics.

Non-trivial constructions for finding conic blocking sets and upper and lower bounds on minimum CBSs are discussed below. The theoretical and computer

models used to generate minimum CBSs in projective planes are also described. As planes with even characteristic vary from those of odd characteristic, we discuss CBSs in these planes separately.

### 3. CBSs in Planes of Even Order

In this chapter, we focus on CBSs in planes of even order. Properties of certain flocks are used to prove that our constructions give CBSs in  $\text{PG}(2, 2^h)$ . When  $h$  is even, we derive irreducible CBSs and also show how Baer lines form CBSs. Theoretical lower and upper bounds on the sizes of minimum CBSs are given. A model which allows the search for minimum CBSs to become more efficient is developed. Examples of minimum CBSs are located in Appendix A.

#### 3.1 Introduction

To set notation, let  $\mathcal{E} = \text{GF}(2^h) = \text{GF}(q)$ ,  $\mathcal{K} = \text{GF}(2^d)$ ,  $\mathcal{F} = \text{GF}(2)$ , and  $\pi = \text{PG}(2, q)$ , where  $h > 1$  and  $d|h$  such that  $d \neq h$ . Certainly,  $\mathcal{K} = \mathcal{F}$  if  $d = 1$ . Let  $\text{tr}(t)$  denote the relative trace function,  $\text{Tr}_{\mathcal{E}/\mathcal{K}}(t) = t + t^{2^d} + \cdots + t^{2^{d(h-1)}}$ .

In Chapter 2, we showed that all projective planes have conic blocking sets. The next theorem sharpens that result by showing that just over half the lines through a point are enough to form a CBS.

**Lemma 3.1** *Any set of  $\frac{q}{2} + 1$  concurrent lines in  $\text{PG}(2, q)$  form a CBS.*

**Proof:** For the sake of obtaining a contradiction, assume that there is a conic  $\mathcal{C}$  contained in the  $\frac{q}{2}$  lines of  $\mathcal{B}^c$ . Since each line of  $\mathcal{B}^c$  contains at most two points of  $\mathcal{C}$ , we account for at most  $2 \cdot \left(\frac{q}{2}\right) = q$  points of  $\mathcal{C}$ . But, as  $\mathcal{C}$  contains  $q + 1$  points,  $\mathcal{C}$  cannot be contained in  $\mathcal{B}^c$  and thus,  $\mathcal{B}$  is a CBS. ■

We consider CBSs in  $\text{PG}(2, 2)$  now, so that the remainder of the chapter can be devoted to finding small CBSs in  $\text{PG}(2, 2^h)$ , with  $h > 1$ , using more sophisticated techniques than those of Lemma 3.1.

**Theorem 3.2** *A CBS in  $PG(2, 2)$  contains at least two lines.*

**Proof:** In  $PG(2, 2)$ , any point  $P$  lies on three lines. In Lemma 3.1, we established that any  $2 = \frac{q}{2} + 1$  lines (which must be concurrent) form a CBS in  $PG(2, 2)$ . We need now only show that one line is not a CBS.

Suppose  $\mathcal{B}$  is a CBS consisting of the single line  $l$ . A conic  $C$  in  $PG(2, 2)$  consists of three points and of the seven lines of the plane, three are secants, three are tangents, and one is an exterior line with respect to  $C$ . By the Fundamental Theorem of Projective Geometry, any conic can be mapped to a conic that has  $l$  as an exterior line. Hence, there is some conic in  $PG(2, 2)$  not blocked by  $l$ , and one line is not enough to form a CBS. ■

### 3.2 The Trace-Flock Construction

Finding CBSs consists of identifying a set of lines through a point such that all conics in  $\pi$  have at least one secant or tangent line in this set. For the CBS construction given in this section,  $\pi$  is coordinatized so that  $P = (0, 1, 1)$  is the point of concurrency. Note that the lines through  $P$  are  $x = 0$  and  $y = mx + z$  for  $m \in GF(q)$ . We are able to insure that  $x = 0$  is not a line of the CBS, so an equivalent problem statement is to identify the slopes of the lines of the form  $y = mx + z$  such that every conic in  $\pi$  meets these lines. We begin by examining the size of the range of a specific function in  $GF(q)$ ; for this function will determine the slopes of the CBS lines.

**Lemma 3.3** *If  $g : \mathcal{E}^* \rightarrow \mathcal{E}$  is given by  $g(t) = \frac{tr(t)+t}{t}$  for  $t \neq 0$ , then  $|Range(g)| = 2^{h-d} + 1$ .*

**Proof:** To show that the size of the range of  $g$  is  $2^{h-d} + 1$ , we show that  $\mathcal{E}$

can be partitioned into  $2^{h-d} + 1$  blocks: one of size  $2^{h-d}$  and  $2^{h-d}$  blocks of size  $2^d - 1$ .

Let  $t \in \mathcal{E}^*$ , then

$$\begin{aligned} g(t) = 1 &\Leftrightarrow \frac{\text{tr}(t) + t}{t} = 1 \\ &\Leftrightarrow \text{tr}(t) + t = t \\ &\Leftrightarrow \text{tr}(t) = 0. \end{aligned}$$

Since the trace function is an additive homomorphism from  $\mathcal{E}$  onto  $\mathcal{K}$ ,  $\ker(\text{tr})$  is a normal subgroup of  $\mathcal{E}$ . We have that  $|\ker(\text{tr})| = |\mathcal{E}|/|\mathcal{K}| = \frac{2^h}{2^d} = 2^{h-d}$ . So,  $g(t) = 1 \Leftrightarrow t$  is one of the  $2^{h-d} - 1$  nonzero elements in  $\mathcal{E}$  with trace 0. Hence, there is one block of  $\mathcal{E}$  that contains the  $2^{h-d}$  elements with trace 0.

Now, we show that the remaining elements in  $\mathcal{E}$  are partitioned into blocks of size  $2^d - 1$ , giving  $2^{h-d}$  blocks. To do this, we first determine when  $g(t) = g(\lambda t)$  for  $\lambda \in \mathcal{E} \setminus \mathcal{K}$ .

$$\begin{aligned} g(t) = g(\lambda t) &\Leftrightarrow \frac{\text{tr}(t) + t}{t} = \frac{\text{tr}(\lambda t) + \lambda t}{\lambda t} \\ &\Leftrightarrow \lambda \text{tr}(t) + \lambda t = \text{tr}(\lambda t) + \lambda t \\ &\Leftrightarrow \lambda \text{tr}(t) = \text{tr}(\lambda t). \end{aligned}$$

As  $\text{tr} : \mathcal{E} \rightarrow \mathcal{K}$ , we have that  $\text{tr}(\lambda t), \text{tr}(t) \in \mathcal{K}$ . But, since  $\lambda \in \mathcal{E} \setminus \mathcal{K}$ ,  $\lambda \text{tr}(t) \in \mathcal{K} \Leftrightarrow \text{tr}(t) = 0$ . We see that  $g(t) = g(\lambda t)$  for some  $\lambda \in \mathcal{E} \setminus \mathcal{K}$  iff  $t$  is a nonzero element with trace 0. That is,  $t \in \ker(\text{tr})$ .

Observe that  $g(t) = g(\lambda t)$  for  $t \notin \ker(\text{tr})$  for any  $\lambda \in \mathcal{K}^*$ . Let  $T_0 = \{x \in \mathcal{E}^* \mid \text{tr}(x) = 0\}$ . Then  $t \in T_0 \Leftrightarrow g(t) = 1$ . Now,  $|\mathcal{E} \setminus T_0| = 2^h - 2^{h-d} = 2^{h-d}(2^d - 1)$  and we see that  $g$  partitions  $\mathcal{E}$  into  $2^{h-d} + 1$  blocks. There is one

block containing  $2^{h-d}$  elements with trace 0, and the remaining elements of  $\mathcal{E}$  are split into  $2^{h-d}$  blocks of size  $2^d - 1$  one for each value of  $g$  that is not equal to 1. Thus,  $|\text{Range}(g)| = 2^{h-d} + 1$ . ■

					$\mathcal{E}$
$2^d - 1$	$2^d - 1$	$2^d - 1$	$2^d - 1$	$2^d - 1$	
$2^d - 1$	$2^d - 1$	$2^d - 1$	$2^d - 1$	$2^d - 1$	
$2^d - 1$	$2^d - 1$	$2^d - 1$	$2^d - 1$	$2^d - 1$	
$2^d - 1$	$2^d - 1$	$2^d - 1$	$2^d - 1$	$2^d - 1$	
$2^d - 1$	$2^d - 1$	$2^d - 1$	$2^{h-d}$		$\mathcal{K}$
$2^d - 1$	$2^d - 1$	$2^d - 1$			

**Figure 3.1:** A partitioning of  $\mathcal{E}$

If  $h$  is prime, then  $\text{tr}(t)$  is the absolute trace of  $t$  and  $|\text{Range}(g)| = 2^{h-1} + 1$ . If  $h$  is composite, then there exists a  $g$ , as in Lemma 3.3, such that  $|\text{Range}(g)| < 2^{h-1} + 1$ . In other words, when  $h$  is composite,  $g$  can be defined using a relative trace, which allows for a smaller range than the one obtained by using the absolute trace.

In Section 2.2.3, we defined a *flock* of a cone  $K$  with vertex  $V$  to be a set of  $q$  planes not through  $V$  which do not intersect on the cone. For the results given in this section, the base of the cone is contained in the plane  $w = 0$ . The following theorem due to Thas is instrumental in the proof of Theorem 3.5.

**Theorem 3.4** [69] *In  $PG(3, 2^h)$ , if the planes  $\pi_1, \pi_2, \dots, \pi_q$ , of a flock of a quadratic cone contain a common point, then  $F$  is linear.* ■

We now prove the main result of this section.

**Theorem 3.5** *In  $PG(2, 2^h)$  with  $h \geq 2$ , if  $d \mid h$  then there is a CBS of size  $2^{h-d} + 1$ .*

**Proof:**

Consider the additive function  $f(t) = \text{Tr}_{\mathcal{E}/\mathcal{K}}(t) + t = \text{tr}(t) + t$ , which we use to form the function  $g(t) = \frac{f(t)}{t} = \frac{\text{tr}(t)+t}{t}$ ,  $t \neq 0$ . As shown in Lemma 3.3,  $|\text{Range}(g)| = 2^{h-d} + 1$  and is larger than one.

Let  $\mathcal{B} = \{y = g(t)x + z \mid t \neq 0\}$  be the set of lines in the plane  $w = 0$  through  $(0, 1, 1, 0)$  with slope in the  $\text{Range}(g)$ . Consider the planes of the form:

$$\pi_t : f(t)x + ty + tz + w = 0 \text{ with } t \in \mathcal{E}^*.$$

There are  $2^h - 1$  planes of this type since  $t \in \mathcal{E}^*$ . Clearly, the point  $(0, 0, 0, 1)$  does not lie on these planes and the point  $(0, 1, 1, 0)$  lies on all these planes. Any two distinct planes  $\pi_s$  and  $\pi_t$  ( $s \neq t$ ) meet in a line which projects from  $(0, 0, 0, 1)$  to the line  $y = \frac{f(s-t)}{s-t}x + z = g(s-t)x + z$  in the plane  $w = 0$ . This line is in the set  $\mathcal{B}$ . With the plane  $w = 0$ , we have a set of  $2^h$  planes all passing through  $(0, 1, 1, 0)$  such that every pair of these planes meet in a line which projects to a line of  $\mathcal{B}$ . Suppose there exists a conic  $\mathcal{C}$  that misses  $\mathcal{B}$ . Form a cone,  $K$ , with vertex  $(0, 0, 0, 1)$  and base  $\mathcal{C}$ . These  $2^h$  planes form a flock of  $K$ , and the planes all contain the common point  $(0, 1, 1, 0)$ . Theorem 3.4 implies this flock is linear; in other words,  $|\mathcal{B}| = 1$ . But  $|\mathcal{B}| = 2^{h-d} + 1 > 1$ , so  $\mathcal{C}$  does not exist and  $\mathcal{B}$  is a CBS. ■

In the trace-flock construction, the specific function  $g(t) = \frac{\text{tr}(t)+t}{t}$  was used to give the slopes of the lines in the CBS. Since  $g$  is an additive function divided by

$t$  and the size of its image set is known, we used  $g$  to form a CBS of size  $2^{h-d} + 1$ . Any function of this form can be used to produce a CBS, as long as the image has more than one element in it. The trace-flock construction does not give CBSs when  $q = 2$ , since the only additive function, up to scalar multiplication, is the identity. This is the reason for handling  $\text{PG}(2, 2)$  at the beginning of this chapter.

Table 3.1 lists the sizes of CBSs guaranteed by the trace-flock construction described in Theorem 3.5, for small  $q$ .

$q$	Guaranteed CBS Sizes
$2^2$	3
$2^3$	5
$2^4$	9, 5
$2^5$	17
$2^6$	33, 17, 9
$2^7$	65
$2^8$	129, 65, 17
$2^9$	257, 65
$2^{10}$	513, 257, 33

**Table 3.1:** CBS Sizes Given by the Trace-Flock Construction

For a fixed  $q$ , the largest size of a CBS guaranteed by the trace-flock construction is the same size as those CBSs constructed in Lemma 3.1. When  $h$  is prime, the trace-flock construction yields exactly one CBS. When  $h$  is composite, a variety of CBSs are obtained and there is always a CBS smaller than the one given in Lemma 3.1. To emphasize the significance of this fact, the trace-flock

construction gives a CBS of size 33 that blocks the (over  $1.12 \times 10^{15}$ ) conics in the plane  $\text{PG}(2, 2^{10})$ , whereas by Lemma 3.1, 513 lines were needed to form a CBS.

### 3.3 Irreducible CBSs in $\text{PG}(2, 2^h)$ , $h$ even

In this section, we focus on proving that the CBSs given by the trace-flock construction are irreducible. Recall from Chapter 2, a CBS  $\mathcal{B}$  is *equivalent* to another CBS  $\mathcal{B}'$  if there exists an element  $A$  in  $\text{PGL}(3, q)$  such that  $A$  maps all the lines in  $\mathcal{B}$  to the lines in  $\mathcal{B}'$ . We showed that a CBS consisting of the subset of lines of the form  $y = mx + z$  is projectively equivalent to a CBS consisting of the lines of the form  $y = mx$ . We use this fact to prove that the conic blocking set given by the trace-flock construction, for  $h$  even, is irreducible.

Throughout the remainder of this section, let  $h = 2n$ ,  $n \geq 2$ ,  $d = n$ , so that  $\mathcal{E} = \text{GF}(2^{2n})$ ,  $\mathcal{K} = \text{GF}(2^n)$ , and  $\mathcal{F} = \text{GF}(2)$ . Then  $g(t) = \frac{\text{Tr}_{\mathcal{E}/\mathcal{K}}(t)+t}{t} = \frac{t+t^{2^n}+t}{t} = t^{2^n-1}$ . Let  $\alpha$  be a generator of  $\mathcal{E}$ . Then  $\text{Range}(g) = \{1, \alpha^{2^n-1}, \alpha^{2(2^n-1)}, \dots, \alpha^{2^n(2^n-1)}\}$  is a cyclic subgroup of  $\mathcal{E}^*$  of order  $2^n + 1$ . Observe that any element in  $\text{Range}(g)$  is expressible as  $\alpha^{(2^n-1)k}$  where  $k \in \mathbb{Z}_{2^n+1}$ .

In Section 3.2, we showed that the set of lines  $\{y = g(t)x + z\}$  formed a CBS, and this set of lines is projectively equivalent to the set  $\mathcal{B} = \{y = g(t)x\}$ . So, we have that  $\mathcal{B}$  is a CBS. It remains to show that  $\mathcal{B}$  is an irreducible CBS. As an illustration, we show  $\mathcal{B}$  is irreducible in  $\text{PG}(2, 16)$  and then present a formal proof of irreducibility for all  $q = 2^{2n}$ .

#### Example 8.

Let  $h = 4$ ,  $n = 2$ , and  $\alpha$  be a generator of  $\mathcal{E}$ . Observe that  $\text{Range}(g) = \{t^3 | t \in \mathcal{E}^*\} = \{1, \alpha^3, \alpha^6, \alpha^9, \alpha^{12}\} = \{\alpha^{3k} | k \in \mathbb{Z}_5\}$ . To show that the CBS

$\mathcal{B} = \{y = \alpha^{3k} \mid k \in \mathbb{Z}_5\}$  is irreducible, we show that for every line in  $\mathcal{B}$ , there is a conic that meets the line but does not meet any other line of  $\mathcal{B}$ .

Consider the quadric  $Q_m : \{(x, y, z) \mid x^2 + \alpha^{-3m}yz + z^2 = 0\}$  where  $m \in \mathbb{Z}_5$ . Since the nucleus,  $(\alpha^{-3m}, 0, 0)$ , does not lie on  $Q_m$ , this quadric is nondegenerate. We show that  $\mathcal{B}$  is irreducible by showing that the line  $y = \alpha^{3m}x$  is a secant line to  $Q_m$  while all other lines,  $y = \alpha^{3k}x$  with  $k \neq m$ , are exterior to  $Q_m$ .

To determine how the line  $y = \alpha^{3k}x$  meets  $Q_m$ , we examine

$$\begin{aligned} x^2 + \alpha^{-3m}\alpha^{3k}xz + z^2 &= 0 \\ \Leftrightarrow x^2 + \alpha^{3(k-m)}xz + z^2 &= 0. \end{aligned}$$

This equation has two solutions if  $\text{Tr}\left(\frac{ac}{b^2}\right) = \text{Tr}\left(\frac{1 \cdot 1}{\alpha^{6(k-m)}}\right) = \text{Tr}(\alpha^{9(k-m)}) = 0$ . Let  $k - m = j$ . Then

$$\begin{aligned} \text{Tr}(\alpha^{9(k-m)}) &= \text{Tr}(\alpha^{9j}) = \alpha^{9j} + (\alpha^{9j})^2 + (\alpha^{9j})^4 + (\alpha^{9j})^8 \\ &= \alpha^{9j} + \alpha^{18j} + \alpha^{36j} + \alpha^{72j} \\ &= \alpha^{9j} + \alpha^{3j} + \alpha^{6j} + \alpha^{12j}. \end{aligned}$$

If  $j = 0$ , then  $k = m$  and  $\text{Tr}(\alpha^{9j}) = \text{Tr}(1) = 0$  in  $\text{GF}(16)$ . Therefore, when  $k = m$ , the line  $y = \alpha^m x$  is secant to  $Q_m$ . When  $j$  is a fixed element in  $Z_5^*$ ,  $\alpha^{9j}$ ,  $\alpha^{3j}$ ,  $\alpha^{6j}$ ,  $\alpha^{12j}$  are distinct. More importantly,  $\alpha^{9j}$ ,  $\alpha^{3j}$ ,  $\alpha^{6j}$ ,  $\alpha^{12j}$  are four of the five 5<sup>th</sup> roots of unity over  $\mathcal{E}^*$ , with 1 the remaining 5<sup>th</sup> root of unity. Thus,  $\alpha^{9j} + \alpha^{3j} + \alpha^{6j} + \alpha^{12j} = 1$  and  $\text{Tr}(\alpha^{9j}) = \text{Tr}(\alpha^{9(k-m)}) = 1$ . Since the absolute trace is 1, there are no solutions to this quadratic equation. Therefore, when  $k \neq m$ , the line  $y = \alpha^{3k}x$  is exterior to  $Q_m$ .

Since the removal of any line  $l$  from  $\mathcal{B}$  results in  $\mathcal{B} \setminus \{l\}$  no longer being a CBS,  $\mathcal{B}$  is irreducible. ■

Since  $(0, 0, 1)$  is on all lines of the CBS, we only need to block conics with equations  $Ax^2 + Bxy + Cy^2 + Dxz + Eyz + Fz^2 = 0$  which do not pass through the point  $(0, 0, 1)$ . For these,  $F \neq 0$  and without loss of generality we may assume that  $F = 1$ . The set  $\mathcal{B} = \{y = t^{2^n-1}x \mid t \neq 0\}$  blocks all of these conics in the plane  $\text{PG}(2, 2^{2n})$ . We can show that  $\mathcal{B}$  is irreducible by showing that for every line in  $\mathcal{B}$ , there is a conic that only meets that line. We now provide two lemmas that aid in proving this result in Theorem 3.8.

When  $n \geq 2$ ,  $|\mathcal{K}| \geq 4$ , and there is an element  $\beta$  in  $\mathcal{K}$  with  $\text{Tr}_{\mathcal{K}/\mathcal{F}}(\beta) = 1$ . Since  $\beta \in \mathcal{K} \subset \mathcal{E}$ ,  $\beta = \beta^{2^n}$ . This implies that for  $0 \leq i \leq n-1$ ,

$$\beta^{2^i} = (\beta^{2^n})^{2^i} = \beta^{2^{n+i}}. \quad (3.1)$$

This observation is useful in the proof of Theorem 3.8. Lemmas 3.6 and 3.7 are used to simplify calculations for Theorem 3.8.

**Lemma 3.6** *Let  $j$  be a positive integer. Then  $\alpha^{(2^n-1)j+2^n(2^n-1)j} = 1$ .*

**Proof:**

$$\alpha^{(2^n-1)j+2^n(2^n-1)j} = [\alpha^{(2^n+1)(2^n-1)j}] = [\alpha^{q^2-1}]^j = 1, \quad \forall \alpha \in \mathcal{E}^*.$$

■

**Lemma 3.7** *Let  $j$  be a positive integer. Then  $\frac{1}{(\alpha^{(2^n-1)j})^{2^i}} + \frac{1}{(\alpha^{(2^n-1)j})^{2^{n+i}}} = 1$ .*

**Proof:** Let  $s = (2^n - 1)j$ . Recall from Lemma 3.6,  $\alpha^{s2^i+s2^{n+i}} = 1$ . Then

$$\frac{1}{(1 + \alpha^s)^{2^i}} + \frac{1}{(1 + \alpha^s)^{2^{n+i}}} = \frac{(1 + \alpha^s)^{2^{n+i}} + (1 + \alpha^s)^{2^i}}{(1 + \alpha^s)^{2^i}(1 + \alpha^s)^{2^{n+i}}}$$

$$\begin{aligned}
&= \frac{(1 + \alpha^s)^{2^{n+i}} + (1 + \alpha^s)^{2^i}}{(1 + \alpha^{s^{2^i}})(1 + \alpha^{s^{2^{n+i}}})} \\
&= \frac{1 + \alpha^{s^{2^{n+i}}} + 1 + \alpha^{s^{2^i}}}{1 + \alpha^{s^{2^{n+i}}} + \alpha^{s^{2^i}} + \alpha^{s^{2^i+s^{2^{n+i}}}}} \\
&= \frac{\alpha^{s^{2^{n+i}}} + \alpha^{s^{2^i}}}{1 + \alpha^{s^{2^{n+i}}} + \alpha^{s^{2^i}} + 1} \\
&= \frac{\alpha^{s^{2^{n+i}}} + \alpha^{s^{2^i}}}{\alpha^{s^{2^{n+i}}} + \alpha^{s^{2^i}}} \\
&= 1.
\end{aligned}$$

■

**Theorem 3.8** *The CBS,  $\mathcal{B} = \{y = t^{2^n-1}x \mid t \neq 0\}$ , is irreducible in  $PG(2, 2^{2^n})$ .*

**Proof:** Let  $\beta \in \mathcal{K}$  such that  $\text{Tr}_{\varepsilon/\mathcal{K}}(\beta) = 1$ . Consider the conics  $Q_m$  with equations:

$$Q_m(x, y, z) = x^2 + \alpha^{(1-2^n)m}xy + \frac{1}{\beta^{1/2}}xz + \frac{\alpha^{(1-2^n)m}}{\beta^{1/2}}yz + z^2 = 0,$$

where  $m \in \mathbb{Z}_{2^n+1}$ . The nucleus of  $Q_m$  is  $(\frac{\alpha^{(1-2^n)m}}{\beta^{1/2}}, \frac{1}{\beta^{1/2}}, \alpha^{(1-2^n)m})$  and observe that  $Q_m(\frac{\alpha^{(1-2^n)m}}{\beta^{1/2}}, \frac{1}{\beta^{1/2}}, \alpha^{(1-2^n)m}) = \alpha^{(1-2^n)2m} \neq 0$ , hence  $Q_m$  is nondegenerate. Express  $\mathcal{B}$  as the set of lines of the form  $\{y = \alpha^{(2^n-1)k}x \mid k \in \mathbb{Z}_{2^n+1}\}$ . We show that when  $k = m$ , the line  $y = \alpha^{(2^n-1)m}x$  is a tangent line to  $Q_m$ , and when  $k \neq m$ , the line  $y = \alpha^{(2^n-1)k}x$  is exterior to  $Q_m$ , for all  $k \in \mathbb{Z}_{2^n+1}^*$ .

For a line in  $\mathcal{B}$  to meet  $Q_m$ , we must have that

$$x^2 + \alpha^{(1-2^n)m+(2^n-1)k}x^2 + \frac{1}{\beta^{1/2}}xz + \frac{\alpha^{(1-2^n)m+(2^n-1)k}}{\beta^{1/2}}xz + z^2 = 0,$$

has a solution. This can be rewritten as

$$(1 + \alpha^{(2^n-1)(k-m)})x^2 + \left(\frac{1}{\beta^{1/2}} + \frac{\alpha^{(1-2^n)m+(2^n-1)k}}{\beta^{1/2}}\right)xz + z^2 = 0. \quad (3.2)$$

When  $k = m$ , (3.2) becomes  $z^2 = 0$ . Since there is only one solution to this equation, the line  $y = \alpha^{(2^n-1)m}x$  is a tangent line to  $Q_m$ .

Let  $k - m = j \neq 0$ . To show that the line  $y = \alpha^{(2^n-1)k}x$  does not meet  $Q_m$ , examine the absolute trace of

$$\begin{aligned} \frac{(1 + \alpha^{(2^n-1)j})}{\left(\frac{1}{\beta^{1/2}} + \frac{1 + \alpha^{(2^n-1)2j}}{\beta^{1/2}}\right)^2} &= \frac{(1 + \alpha^{(2^n-1)j})}{\frac{1}{\beta} + \frac{1 + \alpha^{(2^n-1)2j}}{\beta}} \\ &= \frac{(1 + \alpha^{(2^n-1)j})}{\frac{1}{\beta}(1 + \alpha^{(2^n-1)2j})} \\ &= \frac{(1 + \alpha^{(2^n-1)j})}{\frac{1}{\beta}(1 + \alpha^{(2^n-1)j})^2} \\ &= \frac{\beta}{(1 + \alpha^{(2^n-1)j})}. \end{aligned}$$

As we now show, these lines are exterior to  $Q_m$ . Assume, for the sake of attaining a contradiction, that  $\text{Tr}\left(\frac{\beta}{(1 + \alpha^{(2^n-1)j})}\right) = 0$ . Then,

$$\begin{aligned} &\text{Tr}\left(\frac{\beta}{(1 + \alpha^{(2^n-1)j})}\right) = 0 \\ \Rightarrow &\frac{\beta}{(1 + \alpha^{(2^n-1)j})} + \frac{\beta^2}{(1 + \alpha^{(2^n-1)j})^2} + \frac{\beta^4}{(1 + \alpha^{(2^n-1)j})^4} + \cdots \\ &+ \frac{\beta^{2^n-1}}{(1 + \alpha^{(2^n-1)j})^{2^n-1}} + \frac{\beta^{2^n}}{(1 + \alpha^{(2^n-1)j})^{2^n}} + \frac{\beta^{2^{n+1}}}{(1 + \alpha^{(2^n-1)j})^{2^{n+1}}} + \cdots \\ &+ \frac{\beta^{2^{2n}-1}}{(1 + \alpha^{(2^n-1)j})^{2^{2n}-1}} = 0 \\ \Rightarrow &\beta \left[ \frac{1}{(1 + \alpha^{(2^n-1)j})} + \frac{1}{(1 + \alpha^{(2^n-1)j})^{2^n}} \right] + \beta^2 \left[ \frac{1}{(1 + \alpha^{(2^n-1)j})^2} + \frac{1}{(1 + \alpha^{(2^n-1)j})^{2^{n+1}}} \right] + \cdots \end{aligned}$$

$$+\beta^{2^n-1} \left[ \frac{1}{(1+\alpha^{(2^n-1)j})^{2^n-1}} + \frac{1}{(1+\alpha^{(2^n-1)j})^{2^{2^n-1}}} \right] = 0 \quad (\text{by equation 3.1})$$

$$\Rightarrow \beta + \beta^2 + \beta^4 + \dots + \beta^{2^n-2} + \beta^{2^n-1} = 0 \quad (\text{by Lemma 3.7})$$

$$\Rightarrow \text{Tr}_{\kappa/\mathcal{F}}(\beta) = 0.$$

However,  $\beta$  was chosen such that  $\text{Tr}_{\kappa/\mathcal{F}}(\beta) = 1$ . Thus,  $\text{Tr}\left(\frac{\beta}{(1+\alpha^{(2^n-1)j})}\right) = 1$  and all lines of the form  $y = \alpha^{(2^n-1)k}x$ ,  $k \neq m$ , are exterior to  $Q_m$ .

For every line in  $\mathcal{B}$ , there is a conic that meets only that line. The removal of any line  $l$  from  $\mathcal{B}$  results in  $\mathcal{B} \setminus \{l\}$  no longer being a CBS. Thus,  $\mathcal{B}$  is irreducible. ■

Observe that  $|\mathcal{B}| = |\{y = t^{2^n-1}x \mid t \neq 0\}| = 2^n + 1$  which is the number of lines of a Baer subplane through a point in a Baer subplane of  $\text{PG}(2, 2^{2^n})$ . A natural question to ask is whether the lines through a point in a Baer subplane (*Baer lines*) are projectively equivalent to the irreducible CBS given in Theorem 3.8? We now show that the answer to that question is yes.

**Lemma 3.9** *Let  $\beta = \alpha^{2^n-1}$ . The element*

$$X = \frac{(\beta^j + \beta)(1 + \beta^2)}{(1 + \beta)(\beta^j + \beta^2)} \in \mathcal{E}^*,$$

*with  $j \neq 1, 2$ , lies in the subfield  $\mathcal{K}^*$ .*

**Proof:**

We show that  $X$  lies in  $\mathcal{K}$  by showing that  $X^{2^n-1} = 1$ . First, observe that with  $\beta = \alpha^{2^n-1}$ ,

$$[\beta^k]^{2^n} = \frac{1}{\beta^k},$$

for any  $k$ . Now,

$$\begin{aligned}
X^{2^n-1} &= \left[ \frac{(\beta^j + \beta)(1 + \beta^2)}{(1 + \beta)(\beta^j + \beta^2)} \right]^{2^n-1} \\
&= \frac{(\beta^j + \beta)^{2^n} (1 + \beta^2)^{2^n}}{(1 + \beta)^{2^n} (\beta^j + \beta^2)^{2^n}} \cdot \frac{(1 + \beta)(\beta^j + \beta^2)}{(\beta^j + \beta)(1 + \beta^2)} \\
&= \frac{(\beta^j + \beta)^{2^n} (\beta^j + \beta^2)}{(\beta^j + \beta^2)^{2^n} (\beta^j + \beta)} \cdot \frac{(1 + \beta^2)^{2^n} (1 + \beta)}{(1 + \beta)^{2^n} (1 + \beta^2)} \\
&= \frac{([\beta^j]^{2^n} + \beta^{2^n})(\beta^j + \beta^2)}{([\beta^j]^{2^n} + [\beta^2]^{2^n})(\beta^j + \beta)} \cdot \frac{(1 + [\beta^2]^{2^n})(1 + \beta)}{(1 + [\beta]^{2^n})(1 + \beta^2)} \\
&= \frac{\left(\frac{1}{\beta^j} + \frac{1}{\beta}\right)(\beta^j + \beta^2)}{\left(\frac{1}{\beta^j} + \frac{1}{\beta^2}\right)(\beta^j + \beta)} \cdot \frac{\left(1 + \frac{1}{\beta^2}\right)(1 + \beta)}{\left(1 + \frac{1}{\beta}\right)(1 + \beta^2)} \\
&= \frac{\frac{1}{\beta^j+1}(\beta + \beta^j)(\beta^j + \beta^2)}{\frac{1}{\beta^j+2}(\beta^j + \beta^2)(\beta + \beta^j)} \cdot \frac{\frac{1}{\beta^2}(\beta^2 + 1)(1 + \beta)}{\frac{1}{\beta}(1 + \beta)(\beta^2 + 1)} \\
&= \beta \cdot \frac{1}{\beta} = 1.
\end{aligned}$$

Since  $X^{2^n-1} = 1$  and  $X \neq 0$ ,  $X$  lies in  $\mathcal{K}^*$ . ■

**Theorem 3.10** *The lines  $\mathcal{B}' = \{y = mx \mid m \in \mathcal{K}\} \cup \{x = 0\}$  form an irreducible CBS in  $PG(2, 2^{2n})$ .*

**Proof:**

We show that  $\mathcal{B}'$  is an irreducible CBS in  $PG(2, 2^{2n})$  by finding a projectivity in  $PGL(3, 2^{2n})$  that maps the irreducible CBS  $\mathcal{B}$  given in Theorem 3.8 to  $\mathcal{B}'$ . Let

$\beta$  be as defined in Lemma 3.9. Consider the element

$$A = \begin{bmatrix} \frac{1}{1+\beta} & \frac{\beta}{1+\beta} & 0 \\ \frac{1}{1+\beta^2} & \frac{\beta^2}{1+\beta^2} & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

in  $\text{PGL}(3, 2^{2n})$ . It is a simple argument to show that  $A$  is nondegenerate and that  $A$  leaves  $(0, 0, 1)$  fixed. Next, we show that  $A$  maps the lines  $\mathcal{B} = \{y = t^{2^n-1}x \mid t \neq 0\}$  into the lines in  $\mathcal{B}' = \{y = mx \mid m \in \mathcal{K}\} \cup \{x = 0\}$ .

It is easy to verify that  $A$  sends the line  $y = x$  in  $\mathcal{B}$  to the line  $y = x$  in  $\mathcal{B}'$ , the line  $y = \beta x$  in  $\mathcal{B}$  to the line  $y = 0$  in  $\mathcal{B}'$ , and the line  $y = \beta^2 x$  in  $\mathcal{B}$  to the line  $x = 0$  in  $\mathcal{B}'$ . We show now that the remaining lines in  $\mathcal{B}$  are mapped to the remaining lines in  $\mathcal{B}'$ .

For  $j \neq 0, 1, 2$ , we denote the remaining lines in  $\mathcal{B}'$  by  $\begin{bmatrix} \beta^j \\ 1 \\ 0 \end{bmatrix}$ . Now,

$$\begin{bmatrix} \frac{1}{1+\beta} & \frac{\beta}{1+\beta} & 0 \\ \frac{1}{1+\beta^2} & \frac{\beta^2}{1+\beta^2} & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} \beta^j \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{(\beta^j+\beta)(1+\beta^2)}{(1+\beta)(\beta^j+\beta^2)} \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} X \\ 1 \\ 0 \end{bmatrix}.$$

From Lemma 3.9,  $X$  lies in  $\mathcal{K}^*$ , therefore  $X$  is of the form  $\alpha^{(2^n+1)k}$ ,  $k \neq 0$ .  $A$  maps the lines in  $\mathcal{B}$  to distinct lines in  $\mathcal{B}'$ , which are the Baer lines through the point  $(0, 0, 1)$  in  $\text{PG}(2, 2^n)$ . Thus,  $\mathcal{B}'$  is projectively equivalent to  $\mathcal{B}$ , and  $\mathcal{B}'$  is an irreducible CBS in  $\text{PG}(2, 2^{2n})$ . ■

### 3.4 Searching for Minimum CBSs

Having established that CBSs exist and having provided a construction of CBSs, we devote this section to finding minimum CBSs and obtaining upper and lower bounds on the sizes of these CBSs. We develop a model that efficiently and effectively searches for minimum CBSs using optimization software. The results of the search are given at the end of this chapter.

Due to the combinatorial explosion inherent in exhaustive searches, we develop a more sophisticated technique to find an efficient algorithm for locating minimum CBSs. Reducing the size of the problem is vital to the algorithm. For this reason, we review definitions and properties introduced in Chapter 2 that are relevant to the algorithm.

A *collineation* from a projective plane to another one is a bijection of the points and of the lines which preserves incidence. The set of all collineations of  $\text{PG}(2, q)$  form a group where the group operation is the composition of maps. A *projectivity* is a collineation which can be represented by a  $3 \times 3$  nonsingular matrix. Projectivities of the line  $\text{PG}(1, q)$  can be represented by  $2 \times 2$  nonsingular matrices. The group of projectivities of the plane is denoted by  $PGL(3, q)$ , and the group of projectivities of the line is denoted by  $PGL(2, q)$ . [35]

$PGL(3, q)$  is transitive on the points and lines of  $\text{PG}(2, q)$ , just as  $PGL(2, q)$  is transitive on the points of  $\text{PG}(1, q)$ . Any map in  $PGL(3, q)$  preserves incidences between points and lines and is also transitive on conics of  $\text{PG}(2, q)$ . So, any map in  $PGL(3, q)$  will map conics to conics. Every conic has a unique nucleus, hence,

any map that sends a conic,  $\overline{C}$ , to itself will fix the nucleus. Since  $\overline{C}$  is stabilized and the nucleus is fixed, the remaining points in the plane are mapped to each other. In Chapter 2.2.2.1, we showed the stabilizer of  $\overline{C}$  has three orbits in the plane:

1. the points of  $\overline{C}$ ;
2. the nucleus of  $\overline{C}$ ;
3. the rest of the points in the plane.

Since the stabilizer of a conic has three orbits in the plane, the stabilizer of a conic  $\overline{C}$  is transitive on the set of points that are neither on the conic nor equal to the nucleus.

Denote the lines through a point  $P$  with nonhomogeneous coordinates  $[t]$ , if the line is non-vertical, and  $[\infty]$ , for the vertical line through  $P$ , and denote the lines through a point  $Q$  with nonhomogeneous coordinates  $[u]$ , if the line is non-vertical, and  $[\infty]$ , for the vertical line through  $Q$ . Now, if an element  $g \in \text{PGL}(3, q)$  maps the point  $P$  to the point  $Q$ , then there is an element

$$h = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{PGL}(2, q)$$

with the property that for any line  $l$  through  $P$  with coordinate  $[t]$  or  $[\infty]$ , the coordinate of the image of  $l$  under  $g$  is given by

$$u = \frac{at+c}{bt+d}, \quad \text{if } bt + d \neq 0$$

$$\infty, \quad \text{otherwise.}$$

The following example illustrates this concept.

**Example 9.** [55]

Let  $P = (0, 0, 1)$  and  $Q = (0, 1, 0)$ . The line  $[t]$  through  $P$  (and not  $Q$ ) containing the points  $(1, t, z)$  for all  $z \in \text{GF}(q)$  is  $[t] = \begin{bmatrix} t \\ 1 \\ 0 \end{bmatrix}$  and the line  $[u]$  through  $Q$  (and not  $P$ ) containing  $(1, y, u)$  for all  $y \in \text{GF}(q)$  is  $[u] = \begin{bmatrix} u \\ 0 \\ 1 \end{bmatrix}$ . We wish to send  $P$  to  $Q$ , fix the line  $\overline{PQ}$ , and send the remaining lines through  $P$  to the remaining lines through  $Q$ . Let  $A \in \text{PGL}(3, q)$  be given by

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ 0 & a_{22} & a_{23} \\ 0 & 1 & 0 \end{bmatrix}.$$

Since  $A \in \text{PGL}(3, q)$ ,  $\det(A) \neq 0$  implying that both  $a_{11}$  and  $a_{23}$  are nonzero. Observe that  $\overline{PQ}$  is stabilized by  $A$ , but, more importantly,  $P$  is mapped to  $Q$ . A line  $[t]$  through  $P$  consists of the points  $\{(1, t, z) \mid z \in \text{GF}(q)\} \cup \{P\}$ , and a line  $[u]$  through  $Q$  consists of the points  $\{(1, y, u) \mid y \in \text{GF}(q)\} \cup \{Q\}$ . Because  $A$  maps  $P$  to  $Q$ , if  $A$  maps the set  $\{(1, t, z) \mid z \in \text{GF}(q)\}$  to  $\{(1, y, u) \mid y \in \text{GF}(q)\}$ , then  $A$  maps the lines  $[t]$  through  $P$  to the lines  $[u]$  through  $Q$ . This implies that

$$(1, t, z) \cdot A = (a_{11} + 0t, a_{12} + a_{22}t + z, a_{13} + a_{23}t).$$

Now,

$$\begin{aligned} (1, t, z) \cdot A &= (a_{11}, a_{12} + a_{22}t + z, a_{13} + a_{23}t) \\ &= \left(1, \frac{a_{12} + a_{22}t + z}{a_{11}}, \frac{a_{13} + a_{23}t}{a_{11}}\right) \\ &= \left(1, *, \frac{a_{23}t + a_{13}}{0t + a_{11}}\right) = (1, *, u). \end{aligned}$$

In this situation, the element  $h \in \text{PGL}(2, q)$  is given by

$$\begin{bmatrix} a_{23} & a_{13} \\ 0 & a_{11} \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{PGL}(2, q).$$

■

Given a point  $P$  and a conic  $\mathcal{C}$  such that  $P \notin \mathcal{C}$  and  $P$  is not the nucleus of  $\mathcal{C}$ , the absolute trace function is used to classify the lines through  $P$  with respect to  $\mathcal{C}$  as secant, tangent, or exterior lines. Recall that the stabilizer of  $P$  in  $\text{PGL}(3, q)$  is transitive on conics that  $P$  is not on and for which  $P$  is not the nucleus. If  $\mathcal{C}$  is mapped to another conic  $\mathcal{C}_1$ , the tangent and secant lines of  $\mathcal{C}$  are mapped respectively to tangent and secant lines of  $\mathcal{C}_1$ . Thus, for each element in  $\text{PGL}(3, q)$  that maps  $\mathcal{C}$  to  $\mathcal{C}_1$ , there is an element in  $\text{PGL}(2, q)$  that sends the tangent and secant lines of  $\mathcal{C}$  through  $P$  to the tangent and secant lines of  $\mathcal{C}_1$  through  $P$ .

Consider the conic  $\mathcal{C}$  with equation  $xy + xz + z^2 = 0$  and nucleus  $N = (0, 1, 1)$ . The point  $(0, 0, 1)$  is not on  $\mathcal{C}$  and the  $q + 1$  lines through  $(0, 0, 1)$  are  $x = 0$  and  $mx + y = 0$ ,  $m \in \text{GF}(q)$ . Using the methods discussed in Chapter 2, the tangent and secant lines of  $\mathcal{C}$  through  $(0, 0, 1)$  are easily identified. The line  $mx + y = 0$  is a secant line to  $\mathcal{C}$  when  $\text{Tr}(m) = 0$  and the line  $x = 0$  is a tangent line to  $\mathcal{C}$ .

We identify the lines through  $(0, 0, 1)$  with the elements of  $\text{GF}(q) \cup \{\infty\}$  by

$$\begin{aligned} mx + y = 0 &\rightarrow (m), \\ x = 0 &\rightarrow (\infty). \end{aligned}$$

Let  $S_P = \{(m) \mid \text{Tr}(m) = 0\} \cup \{(\infty)\}$  denote the set of tangent and secant lines of  $\mathcal{C}$  through  $(0, 0, 1)$ . Using the standard duality, we dualize so that all the lines through  $(0, 0, 1)$  become points on the line  $z = 0$  with homogeneous coordinates.

That is,

$$(m) : mx + y = 0 \mapsto (m, 1, 0),$$

$$(\infty) : x = 0 \mapsto (0, 0, 1).$$

Note, the set  $S_P = \{(m) \mid \text{Tr}(m) = 0\} \cup \{(\infty)\}$  can still be used to identify the points in the dual plane that correspond to tangent and secant lines in the original plane.

Let  $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{PGL}(2, q)$  and consider the following calculations:

$$(m, 1) \begin{bmatrix} a & b \\ c & d \end{bmatrix} = (am + c, bm + d) = \begin{cases} \left(\frac{am+c}{bm+d}, 1\right), & \text{if } bm + d \neq 0 \\ (1, 0), & \text{if } bm + d = 0, \end{cases}$$

$$(1, 0) \begin{bmatrix} a & b \\ c & d \end{bmatrix} = (a, b) = \begin{cases} \left(\frac{a}{b}, 1\right), & \text{if } b \neq 0 \\ (1, 0), & \text{if } b = 0. \end{cases}$$

The image of  $S_P$  under  $\text{PGL}(2, q)$  is  $\left\{ \left\{ \frac{ax+c}{bx+d} \mid \text{Tr}(x) = 0 \right\} \cup \left\{ \frac{a}{b} \right\} \right\}$  where it is understood that if  $bx + d = 0$ , then  $\frac{ax+c}{bx+d} = \infty$ , and if  $b = 0$ , then  $\frac{a}{b} = \infty$ .

To summarize the procedure, find a conic  $\mathcal{C}$  and fix a point  $P \notin \mathcal{C}$  such that  $P$  is not the nucleus of  $\mathcal{C}$ . Identify the tangent line and secant lines through  $P$  with respect to  $\mathcal{C}$ . Then dualize and parameterize to obtain a set of parameters for the points in the dual plane that correspond to tangent and secant lines of the conic in the original plane. Using collineations of the line  $\text{PG}(1, q)$ , map this set of parameters to another set of parameters representing tangent and secant lines of another conic in  $\text{PG}(2, q)$ . Once all possible parameter sets corresponding to tangent and secant lines have been generated, a CBS can be found by selecting a representative from each of these image parameter sets. A minimum CBS is found by selecting a representative from each of these parameter sets in such a way as to get the smallest number of distinct representatives.

**Example 10.**

Consider this situation in  $\text{PG}(2, 4)$  with  $\text{GF}(4) = \{0, 1, \alpha, \alpha^2\}$  such that  $\alpha^2 = \alpha + 1$ . Observe that  $S_P = \{0, 1, \infty\}$  and the distinct images sets of  $S_P$  under  $\text{PGL}(2, q)$  are  $\{0, 1, \infty\}$ ,  $\{0, \alpha, \alpha^2\}$ ,  $\{0, \alpha, \infty\}$ ,  $\{0, 1, \alpha^2\}$ ,  $\{0, \alpha^2, \infty\}$ ,  $\{0, 1, \alpha\}$ ,  $\{\alpha, \alpha^2, \infty\}$ ,  $\{1, \alpha, \infty\}$ ,  $\{1, \alpha^2, \infty\}$ , and  $\{1, \alpha, \alpha^2\}$ .

Scanning this list of image sets shows that at least one of the elements  $0, 1, \infty$  appears in each of the image sets. When this information is translated back to the original plane, we find that the lines  $y = 0$ ,  $y = x$ , and  $x = 0$  form a conic blocking set in  $\text{PG}(2, 4)$ . As shown earlier, in  $\text{PG}(2, 4)$  any set of three concurrent lines will form a CBS. The 10 image sets listed above give all possible parameter choices for three concurrent lines through the point  $(0, 0, 1)$ . In fact, any one of the 10 image sets is a conic blocking set which is not difficult to verify by hand. This example is unique, since each one of these parameter sets represents a CBS and this is the only projective plane of even characteristic with this property. ■

As the order of the plane increases, it is no longer feasible to do a hand search for minimum CBSs. For this reason, the computer is used to find the minimum CBSs. This is what we now discuss.

We start with the set of points  $S_P = \{(m) \mid \text{Tr}(m) = 0\} \cup \{(\infty)\}$  which represents a set of concurrent tangent and secant lines of a specific conic. And, we use the collineations in  $\text{PGL}(2, q)$  to generate the image sets of  $S_P$ . We put these sets in an array,  $A$ , such that

- the columns of  $A$  are the points of the line  $z = 0$ ,
- the rows of  $A$  are the images of the set  $S_P$ ,

- the entries are given by standard incidence, that is, a 1 is stored if the point is in the image set and a 0 is stored otherwise.

To find a CBS, a collection of columns must be obtained such that each row of  $A$  has a 1 in at least one of the columns in this collection. This set of columns corresponds to a set of points in the dual plane, which corresponds to a set of lines in the original plane that form a CBS. To find a minimum CBS, the smallest set of columns must be found such that each row of  $A$  has a 1 in the corresponding column set. Hence, the problem of finding a CBS can now be viewed as a set covering problem which is easily turned into an optimization problem.

For this particular optimization problem, in the dual plane, the objective is to minimize the number of points on the line  $z = 0$ , subject to the constraint that every row of the array  $A$  has a representative in the collection of points. Let  $\vec{x}$  be a binary vector of length  $q + 1$ . The vector  $\vec{x}$  is used to keep track of which columns (points) are selected for the CBS. For instance, if  $x(i) = 1$ , then the point represented by column  $i$  has been selected to be in the CBS. If  $x(j) = 0$ , the point represented by column  $j$  has not been selected to be in the CBS. We write the integer programming problem as

$$\min \sum_{i=1}^{q+1} x(i)$$

such that

$$\sum_{i=1}^{q+1} A(k, i)x(i) \geq 1.$$

It is not difficult to visualize how stating the problem like this leads to a solution. If any row of  $A$  is picked and multiplied by  $\vec{x}$ , a nonnegative integer is obtained, for we are only multiplying 0's and 1's. If for some row of  $A$ , a 0 is

obtained by multiplying by  $\vec{x}$ , then there is not a representative in that image set. Hence,  $\vec{x}$  cannot represent a CBS.

Since the action of  $\text{PGL}(3, q)$  on the points a projective plane is 3-transitive, it is possible to make the problem of finding minimum CBSs more efficient. By the Fundamental Theorem, we are free to select any three points to always be in the CBS. Any image set that has a 1 in the column corresponding to one of these three chosen points, automatically has a representative in the set. Therefore, there is no need to store this image set in the array  $A$ . It is only necessary to keep track of the image sets with 0's in the columns of the three chosen points. Since the remaining image sets have 0's in the columns of the three chosen points, there is no need to store these columns in  $A$ . Hence, the optimization problem can be restated so that  $\vec{x}$  is a binary vector of length  $q + 1 - 3 = q - 2$ . Then the IP-problem is

$$\min \sum_{i=1}^{q-2} x(i)$$

such that

$$\sum_{i=1}^{q-2} A(k, i)x(i) \geq 1.$$

The optimization software package called Cplex [39] is used to search for the optimal solution. Cplex uses a *branch and bound* algorithm to find the optimal solution. The branch and bound algorithm first solves the integer programming problem as a linear programming problem by relaxing the integrality conditions. That is, it allows for fractional solutions. If the resultant solution is integer, the problem is solved. Otherwise a tree search is performed which guarantees optimality. The branch and bound algorithm is an efficient algorithm that guarantees, in our setting, finding a minimum conic blocking set. For a simple explanation of

the branch and bound process, see Appendix C. For full details of the branch and bound algorithm, see [73].

Table 3.5 lists the size of a minimum CBS and the minimum CBSs as found by Cplex are found in Appendix A.

$q$	Minimum CBS Sizes
$2^2$	3
$2^3$	5
$2^4$	5
$2^5$	8
$2^6$	9
$2^7$	9

**Table 3.5:** Minimum CBS Sizes

A complete search for minimum CBSs by Cplex in  $\text{PG}(2, 2^h)$ ,  $h \geq 8$ , was not feasible. As  $h$  increases, the size of the array surpasses the built-in limitations on the number of rows in the array. Also, as  $h$  increases, a substantial amount of time is required for Cplex to check all nodes of the tree. For instance, in  $\text{PG}(2, 2^8)$ , Cplex located a CBS of size 13, and after nearly two months of searching the tree, it had not located a smaller CBS. The program had to be terminated, due to overwhelming memory usage on the machine, before it could verify that 13 was the size of the minimum CBS in  $\text{PG}(2, 2^8)$ .

### 3.5 Bounds on the Sizes of Minimum Conic Blocking Sets

In this section, upper and lower bounds are obtained for the size of a minimum conic blocking set.

For the purposes of obtaining a lower bound, let  $q = 2^h$ ,  $\text{tr}(x)$  denote the absolute trace of an element  $x \in \mathcal{E} = \text{GF}(q)$ , and let  $V = \text{AG}(h, 2)$  be the vector space over  $\text{GF}(2)$  represented by  $\mathcal{E}$  under addition. For  $0 \neq a \in \mathcal{E}$ , let  $f_a : \mathcal{E} \rightarrow \text{GF}(2)$  be given by  $x \mapsto \text{tr}(ax)$ . Let  $\mathcal{H}_a = \ker(f_a)$ . Clearly,  $f_a$  is additive. This implies that  $f_a$  is a group homomorphism from  $\mathcal{E}$  to  $\text{GF}(2)$ . Hence,  $\ker(f_a)$  is a normal subgroup. Since  $\ker(f_a)$  is a subgroup of  $\mathcal{E}$ , it is a subspace of  $V$ . The rank of the image space of  $f_a$  is 1. Hence, the rank of the overlying vector space minus 1 equals the rank of the kernel of  $f_a$ , that is,

$$\text{rank}(V) - 1 = \text{rank}(\ker(f_a)).$$

Hence,  $\mathcal{H}_a = \ker(f_a)$  is a hyperplane in  $\text{AG}(h, 2)$ .

**Lemma 3.11** [55] *There are precisely  $q - 1$  subgroups of  $\text{AG}(h, 2) = \mathcal{E}(+)$  of index 2. They are the  $\mathcal{H}_a$ , for  $a \neq 0 \in \mathcal{E}$ .*

**Proof:** Suppose  $\mathcal{H}_a = \mathcal{H}_b$  with  $a, b \neq 0$ . This implies that  $\text{tr}(ax) = 0 \Leftrightarrow \text{tr}(bx) = 0 \forall x \in \mathcal{E}$

$$\Leftrightarrow \text{tr}(ax) = \text{tr}(bx) \quad \forall x \in \mathcal{E}$$

$$\Leftrightarrow \text{tr}(ax - bx) = 0 \quad \forall x \in \mathcal{E}$$

$$\Leftrightarrow \text{tr}((a - b)x) = 0 \quad \forall x \in \mathcal{E}.$$

This is a contradiction, since  $x$  ranges over  $\mathcal{E}$ ,  $(a - b)x$  is a linear function and therefore, there is some  $x$  for which  $\text{tr}((a - b)x) = 1$ . Hence, all the  $\mathcal{H}_a$  are distinct.

From the paragraph preceding Lemma 3.11,  $\mathcal{H}_a$  is a hyperplane in  $\text{AG}(h, 2)$ . As there are  $q - 1$  choices for nonzero  $a$ , there are  $q - 1$  subgroups  $\mathcal{H}_a$ . The number of points of  $\text{PG}(h - 1, 2)$  is the number of nonzero vectors in  $V$ . By duality, the number of points in  $\text{PG}(h - 1, 2)$  equals the number of hyperplanes in  $\text{PG}(h - 1, 2)$ .

So, there are  $\frac{2^h-1}{2-1} = 2^h - 1 = q - 1$  hyperplanes in  $\text{AG}(h, 2)$ . Hence, the  $\mathcal{H}_a$  are all the hyperplanes of  $\text{AG}(h, 2)$ . ■

**Observation 3.12** Consider the conic  $y^2 = \frac{1}{a}xz$ ,  $a \neq 0$ , with nucleus  $(0, 1, 0)$ . This conic can also be written as  $\{(a, t, t^2) \mid t \in \text{GF}(q)\} \cup \{(0, 0, 1)\}$ . Let  $l$  be the line  $x = 0$  and  $P$  the point  $(0, 1, 1)$ . The remaining lines through  $P$  have equations  $y = bx + z$  for  $b \in \text{GF}(q)$ . The line  $y = bx + z$  is external to the conic if and only if  $\text{Tr}\left(\frac{b^2}{a^2}\right) = 1 \Leftrightarrow \text{Tr}(ab) = 1$ . So, for fixed nonzero  $a$ , the external lines through  $P$  to this conic are those with slope  $b$  such that  $\text{Tr}(ab) = 1$ . ■

**Observation 3.13** Consider the conic  $y^2 + \frac{c^2}{2}x^2 + \frac{1}{a}xz = 0$ , with nucleus  $(0, 1, 0)$ , where  $c$  is fixed such that  $\text{Tr}(c) = 1$ , and  $a \neq 0 \in \text{GF}(q)$ . This conic can also be written as  $\{(a, t + c, t^2) \mid t \in \text{GF}(q)\} \cup \{(0, 0, 1)\}$ . Let  $l$  be the line  $x = 0$  and let  $P$  be the point  $(0, 1, 1)$ . The remaining lines through  $P$  have equations  $y = bx + z$  for  $b \in \text{GF}(q)$ . The line  $y = bx + z$  is external to the conic if and only if

$$\begin{aligned} \text{Tr}\left[\frac{b^2 + \frac{c^2}{a^2}}{\frac{1}{a^2}}\right] = 1 &\Leftrightarrow \text{Tr}(b^2 a^2 + c^2) = 1 \\ &\Leftrightarrow \text{Tr}(ba) + \text{Tr}(c) = 1 \\ &\Leftrightarrow \text{Tr}(ba) = 0. \end{aligned}$$

So, for fixed nonzero  $a$ , the external lines through  $P$  to this conic are those with slope  $b$  such that  $\text{Tr}(ab) = 0$ . ■

**Theorem 3.14** If  $\mathcal{B}$  is a minimum CBS in  $\text{PG}(2, 2^h)$ , then  $|\mathcal{B}| \geq h$ .

**Proof:**

Let  $\mathcal{B}$  be a CBS which consists of a set of concurrent lines through the point  $P$  in  $\text{PG}(2, q)$ . There exists a line  $l$  through  $P$  and not in  $\mathcal{B}$ , else  $|\mathcal{B}| = q + 1$

and we are done. We may choose coordinates in such a way that  $l$  is assigned the nonhomogeneous parameter  $\infty$ . The other lines through  $P$  are assigned distinct elements of  $\text{GF}(q)$ . Since  $\mathcal{B}$  is a CBS, it must block all conics tangent to  $l$ .

In the preceding two observations, we showed that the external lines through  $P$  to such a conic have parameter sets of the form  $\{b \mid \text{Tr}(ab) = 0\}$  or  $\{b \mid \text{Tr}(ab) = 1\}$ , for any nonzero  $a$ . Moreover, by varying the conic, all such parameter sets arise. Hence,  $\mathcal{B}$  lies in no set of this form. (If the parameter set for  $\mathcal{B}$  was contained in one of these sets, then a conic would exist outside of the conic blocking set.)

Consider the vector space  $V$  over  $\text{GF}(2)$  represented by  $\text{GF}(q)$  under addition. By Lemma 3.11, these parameter sets are all the hyperplanes of the corresponding affine space  $\text{AG}(h, 2)$ . As  $\mathcal{B}$  is contained in no hyperplane of  $\text{AG}(h, 2)$ ,  $\mathcal{B}$  contains a linearly independent set of vectors whose span is  $\text{AG}(h, 2)$ . (A set of vectors not contained in any hyperplane must generate the whole space.) A linearly independent set of vectors whose span is  $\text{AG}(h, 2)$  contains  $h$  vectors. So,  $|\mathcal{B}| \geq h$ . ■

**Theorem 3.15** *If  $\mathcal{B}$  is a minimum CBS in  $\text{PG}(2, 2^h)$ , then  $|\mathcal{B}| \leq 2h + 1$ .*

**Proof:**

As shown in Section 3.4, the sets for which we have to find a set of representatives are the images of  $S_P = \{m \mid \text{Tr}(m) = 0\} \cup \{\infty\}$  under  $\text{PGL}(2, q)$ . Consider the function  $\tau_b : x \mapsto x + b$  where  $\text{Tr}(b) = 0$ . It is clear that  $\tau_b$  maps the set  $S_P$  to itself. Since there are  $q/2$  elements of trace 0 in  $\mathcal{E}$ , the size of the stabilizer of  $S_P$ ,  $|\text{PGL}(2, q)_{S_P}|$ , is at least  $q/2$ . By the Orbit-Stabilizer theorem,

$$\begin{aligned}
|\text{orbit of } S_P| &= |\text{PGL}(2, q) : \text{PGL}(2, q)_{S_P}| \\
&\leq q(q^2 - 1)/(q/2) = 2(q^2 - 1).
\end{aligned}$$

There are at most  $2(q^2 - 1)$  distinct image sets of  $S_P$  of size  $(q+2)/2$ . These image sets give rise to at most  $2(q^2 - 1)$  complementary sets of size  $q+1 - (q+2)/2 = q/2$ . So there are  $2(q^2 - 1)\binom{q/2}{n}$  subsets of size  $n$  that miss some conic, and there are  $\binom{q+1}{n}$  subsets of size  $n$ . If

$$\binom{q+1}{n} \geq 2(q^2 - 1)\binom{q/2}{n},$$

then there is a CBS of size  $n$ . Now, suppose  $n - 1 > 2 \log_2(q)$ , then we have that

$$\begin{aligned}
n - 1 &> \log_2(q^2) \\
\Rightarrow 2^{n-1} &> q^2 \\
\Rightarrow 2^{n-3} &> \frac{q^2 - 6q + 8}{4}, \text{ since } q \geq 2 \\
\Rightarrow 2^{n-3}(q+1)q(q-1) &> 2(q+1)(q-1)\left(\frac{q}{2}\right)\left(\frac{q-2}{2}\right)\left(\frac{q-4}{2}\right) \\
\Rightarrow (q+1)q(q-1)(q-2)\cdots(q+1-(n-1)) &> 2(q^2-1)\left(\frac{q}{2}\right)\left(\frac{q-2}{2}\right)\cdots\left(\frac{q-2(n-1)}{2}\right) \\
\Rightarrow \binom{q+1}{n} &\geq 2(q^2-1)\binom{q/2}{n}.
\end{aligned}$$

So  $\binom{q+1}{n} \geq 2(q^2 - 1)\binom{q/2}{n}$  when  $n > 2 \log_2(q) + 1 = 2h + 1$ . Thus,  $|\mathcal{B}| \leq 2h + 1$ . ■

Thus, we have shown that if  $\mathcal{B}$  is a minimum CBS in  $\text{PG}(2, 2^h)$ , then  $h \leq |\mathcal{B}| \leq 2h + 1$ .

### 3.6 Chapter Summary

We have produced CBSs using the trace function and the method used to generate these CBSs can be mimicked using any additive function. In  $\text{PG}(2, 2^h)$ ,

where  $h$  is even, these CBSs are irreducible and projectively equivalent to a set of lines through the origin in a Baer subplane. Table 3.6 illustrates the sizes of the CBSs found by methods presented in this chapter.

$q$	Trivial Sizes	Trace-Flock Sizes	Baer Lines Sizes
2	2		
4	3	3	3
8	5	5	
16	9	9, 5	5
32	17	17	
64	33	33, 17, 9	9
128	65	65	
256	129	129, 65, 17	17
512	257	257, 65	
1024	513	513, 257, 33	33

**Table 3.6:** Construction Sizes

We developed a model to aid in the search for minimum CBSs. Due to computer and software limitations, we were only able to perform a complete search for minimum CBSs for  $q < 256$ . To obtain small CBSs for  $256 < q \leq 1024$ , we used either an ad-hoc method of selecting potential CBSs and checking, or we employed a greedy-based algorithm to search for small CBSs. It is believed that with more sophisticated programming techniques, finding minimum CBSs in  $\text{PG}(2, 256)$  and  $\text{PG}(2, 512)$  using commercial optimization software should be feasible. Finally, we gave upper and lower bounds on the sizes of minimum CBSs in  $\text{PG}(2, q)$ .

Table 3.7 illustrates the minimum CBSs found and the corresponding bounds. Let  $q$  denote the order of the plane, U.B. denote the upper bound, L.B. denote the lower bound, and S.S.F. denote the size of the smallest set found by one of the following methods: the branch-and-bound algorithm contained in Cplex; a surrogate-based heuristic algorithm, written by G. Kochenberger [47], based on a greedy algorithm; or an ad-hoc method of selecting points and checking if these points form a CBS. A \* indicates that the smallest CBS found is not a minimum CBS.

$q$	L.B.	S.S.F.	U.B.
$2^2$	2	3	5
$2^3$	3	5	7
$2^4$	4	5	9
$2^5$	5	8	11
$2^6$	6	9	13
$2^7$	7	9	15
$2^8$	8	13*	17
$2^9$	9	15*	19
$2^{10}$	10	23*	21

**Table 3.7:** CBS Bounds and Sizes

Appendix A contains a listing of the parameters for CBSs with sizes in Table 3.7.

## 4. CBSs in Planes of Odd Order

In this chapter, we focus on CBSs in planes of odd order. Properties of semi-field flocks are used to prove that our constructions give CBSs in  $\text{PG}(2, p^h)$ . We give theoretical lower and upper bounds on the sizes of minimum CBSs. Two models are developed which allow efficient searching for minimum CBSs. Examples of minimum CBSs are located in Appendix B.

### 4.1 Introduction

Throughout this chapter, let  $\mathcal{E} = \text{GF}(p^h) = \text{GF}(q)$ ,  $\mathcal{K} = \text{GF}(p^d)$ ,  $\mathcal{F} = \text{GF}(p)$ , and  $\pi = \text{PG}(2, q)$ , where  $p$  is an odd prime,  $h \geq 1$  and  $d|h$  such that  $d \neq h$ . Clearly,  $\mathcal{K} = \mathcal{F}$  if  $d = 1$ . Let  $\text{tr}(t)$  denote the relative trace function,  $\text{Tr}_{\mathcal{E}/\mathcal{K}}(t) = t + t^{p^d} + \dots + t^{p^{d(h-1)}}$ .

In Chapter 2, we saw that all projective planes have conic blocking sets. The next theorem sharpens that result by showing that just over half the lines through a point are enough to form a CBS.

**Lemma 4.1** *Any set of  $\frac{q+1}{2} + 1$  concurrent lines in  $\text{PG}(2, q)$  form a CBS.*

**Proof:** Let  $\mathcal{B}$  be a set of  $\frac{q+1}{2} + 1$  concurrent lines. For the sake of obtaining a contradiction, assume that there is a conic  $\mathcal{C}$  contained in the  $\frac{q-1}{2}$  lines of  $\mathcal{B}^c$ . Since each line of  $\mathcal{B}^c$  contains at most two points of  $\mathcal{C}$ , we account for at most  $2 \cdot \left(\frac{q-1}{2}\right) = q-1$  points of  $\mathcal{C}$ . But, as  $\mathcal{C}$  contains  $q+1$  points,  $\mathcal{C}$  cannot be contained in  $\mathcal{B}^c$  and thus,  $\mathcal{B}$  is a CBS. ■

We now consider CBSs in  $\text{PG}(2, 3)$ , so that the remainder of the chapter can

be devoted to finding small CBSs in  $\text{PG}(2, p^h)$ ,  $p^h > 3$ , using more sophisticated techniques than that of Lemma 4.1.

**Theorem 4.2** *A CBS in  $\text{PG}(2, 3)$  contains at least three lines.*

**Proof:** By Lemma 4.1, any set of three concurrent lines form a CBS, so that any set of concurrent lines with more than three lines in it will also be a CBS. It remains to show that any pair of concurrent lines do not form a CBS.

Suppose  $\mathcal{C}$  is a CBS consisting of two concurrent lines. The complement of  $\mathcal{C}$  also consists of two lines for which we can pick four points, two on each of the complement lines, no three collinear. These four points form an oval which is therefore a conic. Since the complement of  $\mathcal{C}$  contains a conic,  $\mathcal{C}$  is not a CBS and no pair of lines in  $\text{PG}(2, 3)$  can be a CBS. ■

## 4.2 The Trace-Flock Construction

The process of finding a CBS consists of identifying a set of lines through a point such that all conics in  $\pi$  have at least one secant or tangent line in this set. For the CBS construction given in this section,  $\pi$  is coordinatized so that  $P = (0, 1, 1)$  is the point of concurrency. Note that the lines through  $P$  are  $x = 0$  and  $y = mx + z$  where  $m \in \text{GF}(q)$ . Since we will insist that  $x = 0$  is not a line of the CBS, an equivalent problem statement is to identify the slopes of the lines of the form  $y = mx + z$  such that every conic in  $\pi$  meets these lines. We begin by examining the size of the range of a specific function in  $\text{GF}(q)$ .

**Lemma 4.3** *If  $g : \mathcal{E}^* \rightarrow \mathcal{E}$  is given by  $g(t) = \frac{\text{tr}(t)-t}{t}$  for  $t \neq 0$ , then  $|\text{Range}(g)| = p^{h-d} + 1$ .*

**Proof:** To show that the size of the range of  $g$  is  $p^{h-d} + 1$ , we show that  $\mathcal{E}$  can be partitioned into  $p^{h-d} + 1$  blocks: one of size  $p^{h-d}$  and  $p^{h-d}$  blocks of size  $p^d - 1$ .

Let  $t \in \mathcal{E}^*$ , then

$$\begin{aligned} h(t) = -1 &\Leftrightarrow \frac{\text{tr}(t) - t}{t} = -1 \\ &\Leftrightarrow \text{tr}(t) - t = -t \\ &\Leftrightarrow \text{tr}(t) = 0. \end{aligned}$$

Since the trace function is an additive homomorphism from  $\mathcal{E}$  onto  $\mathcal{K}$ ,  $\ker(\text{tr})$  is a normal subgroup of  $\mathcal{E}$ . We have that  $|\ker(\text{tr})| = |\mathcal{E}|/|\mathcal{K}| = \frac{p^h}{p^d} = p^{h-d}$ . So,  $g(t) = -1 \Leftrightarrow t$  is one of the  $p^{h-d} - 1$  nonzero elements in  $\mathcal{E}$  with trace 0. Hence, there is one block of  $\mathcal{E}$  that contains the  $p^{h-d}$  elements with trace 0.

Now, we show that the remaining elements in  $\mathcal{E}$  are partitioned into blocks of size  $p^d - 1$ , giving  $p^{h-d}$  blocks. To do this, we first determine when  $g(t) = g(\lambda t)$  for  $\lambda \in \mathcal{E} \setminus \mathcal{K}$ .

$$\begin{aligned} g(t) = g(\lambda t) &\Leftrightarrow \frac{\text{tr}(t) - t}{t} = \frac{\text{tr}(\lambda t) - \lambda t}{\lambda t} \\ &\Leftrightarrow \lambda \text{tr}(t) - \lambda t = \text{tr}(\lambda t) - \lambda t \\ &\Leftrightarrow \lambda \text{tr}(t) = \text{tr}(\lambda t). \end{aligned}$$

As  $\text{tr} : \mathcal{E} \rightarrow \mathcal{K}$ , we have that  $\text{tr}(\lambda t)$ ,  $\text{tr}(t) \in \mathcal{K}$ . But, since  $\lambda \in \mathcal{E} \setminus \mathcal{K}$ ,  $\lambda \text{tr}(t) \in \mathcal{K} \Leftrightarrow \text{tr}(t) = 0$ . We see that  $g(t) = g(\lambda t)$  for some  $\lambda \in \mathcal{E} \setminus \mathcal{K}$  iff  $t$  is a nonzero element with trace 0. That is,  $t \in \ker(\text{tr})$ .

Observe that  $g(t) = g(\lambda t)$  for  $t \notin \ker(\text{tr})$  for any  $\lambda \in \mathcal{K}^*$ . Let  $T_0 = \{x \in \mathcal{E}^* \mid \text{tr}(x) = 0\}$ . Then  $t \in T_0 \Leftrightarrow g(t) = -1$ . Now,  $|\mathcal{E} \setminus T_0| = p^h - p^{h-d} = p^{h-d}(p^d - 1)$

and we see that  $g$  partitions  $\mathcal{E}$  into  $p^{h-d} + 1$  blocks. There is one block containing  $p^{h-d}$  elements with trace 0, and the remaining elements of  $\mathcal{E}$  are split into  $p^{h-d}$  blocks of size  $p^d - 1$ , one for each value of  $g \neq -1$ . Thus,  $|\text{Range}(g)| = p^{h-d} + 1$ .

					$\mathcal{E}$
$p^d - 1$	$p^d - 1$	$p^d - 1$	$p^d - 1$	$p^d - 1$	
$p^d - 1$	$p^d - 1$	$p^d - 1$	$p^d - 1$	$p^d - 1$	
$p^d - 1$	$p^d - 1$	$p^d - 1$	$p^d - 1$	$p^d - 1$	
$p^d - 1$	$p^d - 1$	$p^d - 1$	$p^d - 1$	$p^d - 1$	
$p^d - 1$	$p^d - 1$	$p^d - 1$	$p^{h-d}$		$\mathbb{K}$
$p^d - 1$	$p^d - 1$	$p^d - 1$	$p^{h-d}$		

**Figure 4.1:** A partitioning of  $\mathcal{E}$

■

If  $h$  is prime, then  $\text{tr}(t)$  is the absolute trace of  $t$  and  $|\text{Range}(g)| = p^{h-1} + 1$ . If  $h$  is composite, then there exist a  $g$  such that  $|\text{Range}(g)| < p^{h-1} + 1$ . In other words, when  $h$  is composite,  $g$  can be defined using a relative trace with respect to some subfield, which allows for a smaller range than the one obtained by using the absolute trace.

In Section 2.2.3, we defined a *flock* of a cone  $K$  with vertex  $V$  to be a set of  $q$  planes in  $\text{PG}(3, q)$  not through  $V$  which do not intersect on the cone. For the results given in this section, we may assume that the base of the cone is contained in the plane  $w = 0$ .

The  $q$  planes of a *Knuth-Kantor flock* (for which we use the abbreviation KK-flock) have the form

$$\pi_t : xt - mt^\sigma z + w = 0,$$

where  $m$  is a fixed  $\varnothing \in \mathcal{E}$  and  $\sigma$  a non-identity automorphism of  $\mathcal{E}$ . Any two distinct planes of the KK-flock,  $\pi_s$  and  $\pi_t$ , meet in a line, and when this line is projected to the plane  $w = 0$ , the line has equation

$$x = m(t - s)^{\sigma-1}z.$$

The size of the set of KK-lines,  $\{x = m(t - s)^{\sigma-1}z\}$ , is determined by the automorphism minus one,  $\sigma - 1$ . Multiplying by a nonzero constant will not affect the size of the set of KK-lines. By Theorem 2.4, we have that any non-identity automorphism in  $\mathcal{E}$  has the form  $t \rightarrow t^{p^k}$ , where  $1 \leq k \leq h - 1$ . Any image set of a function of the form  $t^{p^{k-1}}$  has the same size as the set of slopes of the KK-lines, since these image sets are generated by the same type of function, that is, a variable raised to an automorphism minus one. So, we can say that any set of slopes generated from functions of the form  $t^{p^{k-1}}$ , where  $1 \leq k \leq h - 1$ , has the potential to be projectively equivalent to the slopes corresponding to KK-lines.

**Lemma 4.4** *In  $\mathcal{E}$ , the size of the image set of  $g(t) = t^{p^k-1}$ ,  $1 \leq k \leq h - 1$ , is  $\frac{p^h-1}{p^d-1}$ , where  $d = \gcd(k, h)$ .*

**Proof:** For  $1 \leq k \leq h - 1$ , define  $f_\kappa(t) = t^{p^k}$  and  $g_\kappa(t) = \frac{f_\kappa(t)}{t} = t^{p^k-1}$ , for  $t \neq 0$ . Let  $d = \gcd(k, h)$ . Since  $f_\kappa$  is an automorphism of  $\mathcal{E}$ ,  $f_\kappa$  has a fixed field

$\mathcal{K} = \text{GF}(p^d)$ . For  $\lambda \neq 0$ ,

$$\begin{aligned} g_{\mathcal{K}}(t) = g_{\mathcal{K}}(\lambda t) &\Leftrightarrow t^{p^k-1} = \lambda^{p^k-1} t^{p^k-1} \\ &\Leftrightarrow 1 = \lambda^{p^k-1} \\ &\Leftrightarrow \lambda = \lambda^{p^k} \\ &\Leftrightarrow \lambda \in \mathcal{K}. \end{aligned}$$

So,  $g_{\mathcal{K}}(t) = g_{\mathcal{K}}(\lambda t) \Leftrightarrow \lambda$  is in the fixed field of  $f_{\mathcal{K}}(t)$ . Since there are  $p^h - 1$  nonzero elements in  $\mathcal{E}$ , for each  $g_{\mathcal{K}}$ ,  $\mathcal{E}$  is partitioned into blocks of size  $p^d - 1$ . Therefore, there are  $\frac{p^h-1}{p^d-1}$  different values in the image of  $g_{\mathcal{K}}$ .  $\blacksquare$

The previous lemma states that the set of slopes corresponding to nonlinear KK-flocks have size  $\frac{p^h-1}{p^d-1}$  where  $d \mid h$  and  $d < h$ . We determine when the size of the slopes of the KK-lines,  $|\text{KK}|$ , of a nonlinear KK-flock are the same as the  $|\text{Range}(g_{\mathcal{K}})|$  for the  $g_{\mathcal{K}}$  that were defined previously. The case of  $g_{\mathcal{K}}$  being defined by the absolute trace function is examined first. That is, we determine when  $\frac{p^h-1}{p^d-1} = p^{h-1} + 1$  for  $h \geq 3$ . After that, the necessary conditions for  $\frac{p^h-1}{p^d-1} = p^{h-d} + 1$  are determined.

**Lemma 4.5** *If  $h \geq 3$  and  $p$  is an odd prime,  $\frac{p^h-1}{p^d-1} \neq p^{h-1} + 1$ .*

**Proof:** Assume  $\frac{p^h-1}{p^d-1} = p^{h-1} + 1$ . Since the RHS is an integer, the LHS must also be an integer and  $d$  must divide  $h$ . We first obtain bounds on the size of  $d$ . As  $d \mid h$ , clearly  $d \leq h$ . If  $d = h$ , then  $\frac{p^h-1}{p^d-1} = 1 \neq p^{h-1} + 1$  since  $p$  is an odd prime. So,  $d \neq h$ . If  $d = 1$ ,  $\frac{p^h-1}{p^d-1} = \sum_{i=0}^{h-1} p^i \neq p^{h-1} + 1$  unless  $h = 2$ . But, as  $h \geq 3$ ,  $d \neq 1$ . Now,  $d \neq h - 1$  as this would imply that  $(h - 1) \mid h$ , which can only be true if  $h < 3$ .

So, assume that  $1 < d < h - 1$ . Then,

$$\begin{aligned}
\frac{p^h - 1}{p^d - 1} = p^{h-1} + 1 &\Leftrightarrow p^h - 1 = (p^d - 1)(p^{h-1} + 1) \\
&\Leftrightarrow p^h = p^{d+h-1} + p^d - p^{h-1} \\
&\Leftrightarrow p^h + p^{h-1} = p^{d+h-1} + p^d \\
&\Leftrightarrow p^{h-d} + p^{h-d-1} - p^{h-1} = 1.
\end{aligned}$$

Since  $d \leq h - 2$ ,  $p \mid$  LHS which implies that  $p \mid 1$ , a contradiction. Thus, for  $1 \leq d \leq h - 1$ ,  $\frac{p^h - 1}{p^d - 1} \neq p^{h-1} + 1$ . ■

**Lemma 4.6** *Let  $\mathcal{E} = GF(p^h)$ ,  $h$  composite and  $d$  such that  $1 < d < h$  with  $d \mid h$ . Then  $\frac{p^h - 1}{p^d - 1} = p^{h-d} + 1$  if and only if  $d = \frac{h}{2}$ .*

**Proof:**

( $\Leftarrow$ ) Trivial.

( $\Rightarrow$ )

$$\begin{aligned}
\frac{p^h - 1}{p^d - 1} = p^{h-d} + 1 &\Leftrightarrow p^h - 1 = (p^d - 1)(p^{h-d} + 1) \\
&\Leftrightarrow p^h = p^{d+h-d} + p^d - p^{h-d} \\
&\Leftrightarrow p^{h-d} = p^d \\
&\Leftrightarrow h - d = d \\
&\Leftrightarrow d = \frac{h}{2}.
\end{aligned}$$

■

If  $\mathcal{K} = GF(p^d)$  is any subfield of  $\mathcal{E} = GF(p^h)$ , define  $\text{tr}(t) = \text{Tr}_{\mathcal{E}/\mathcal{K}}(t)$  and  $g(t) = \frac{\text{tr}(t) - t}{t}$ , for  $t \neq 0$ . Now, if  $d \neq 1, h$ , or  $\frac{h}{2}$ , we can construct a function  $g$  such that  $|\text{Range}(g)| = \frac{p^h - 1}{p^d - 1}$ . As stated above, this value is smaller than  $p^{h-1} + 1$ .

So, when  $h$  is composite, a function with smaller size range than  $p^{h-1} + 1$  can always be found unless  $d$  is prime and  $h = 2d$ .

The following theorems, due to Thas, are instrumental in the construction of the CBS.

**Theorem 4.7** [69] *If the planes  $\pi_1, \pi_2, \dots, \pi_q$ , of a flock  $F$  of cone  $K$  contain a common interior point  $P$  of  $K$ , then  $F$  is a linear flock.* ■

**Theorem 4.8** [69] *If the planes  $\pi_1, \pi_2, \dots, \pi_q$ , of a flock  $F$  of cone  $K$  contain a common exterior point of  $K$ , then  $F$  is either a linear or a Knuth-Kantor Flock.* ■

We have all the tools necessary to prove the main result of this section.

**Theorem 4.9** *In  $PG(2, p^h)$ , with  $h \geq 3$ , if  $d \neq \frac{h}{2}$  and  $d \mid h$ , then there is a CBS of size  $p^{h-d} + 1$ .*

**Proof:** Consider the additive function  $f(t) = \text{Tr}_{\mathcal{E}/\mathcal{K}}(t) - t = \text{tr}(t) - t$ , which we use to form the function  $g(t) = \frac{f(t)}{t} = \frac{\text{tr}(t)-t}{t}$ , for  $t \neq 0$ . As shown in Lemma 4.3,  $|\text{Range}(g)| = p^{h-d} + 1$  and by Lemmas 4.4 and 4.5, this size does not correspond to the size of a set of KK-lines.

Let  $\mathcal{B} = \{y = g(t)x + z \mid t \neq 0\}$  be the set of lines in the plane  $w = 0$  through  $(0, 1, 1, 0)$  with slope in  $\text{Range}(g)$ . Consider the planes of the form:

$$\pi_t : -f(t)x + ty - tz + w = 0 \text{ with } t \in \mathcal{E}^*.$$

There are  $p^h - 1$  planes of this type, since  $t \in \mathcal{E}^*$ . Clearly, the point  $(0, 0, 0, 1)$  does not lie on these planes and the point  $(0, 1, 1, 0)$  lies on all these planes. Any

two distinct planes,  $\pi_s$  and  $\pi_t$ , ( $s \neq t$ ) meet in a line which projects from  $(0, 0, 0, 1)$  to the line  $y = \frac{f(s-t)}{s-t}x + z = g(s-t)x + z$  in the plane  $w = 0$ . This line is in the set  $\mathcal{B}$ . Together with the plane  $w = 0$ , we have a set of  $q = p^h$  planes all passing through  $(0, 1, 1, 0)$  such that every pair of these planes meet in a line which projects to a line of  $\mathcal{B}$ . Suppose there exists a conic  $\mathcal{C}$  that misses  $\mathcal{B}$ . Form a cone,  $K$ , with vertex  $(0, 0, 0, 1)$  and base  $\mathcal{C}$ . These  $p^h$  planes form a flock of  $K$  and the planes all contain the common point  $(0, 1, 1, 0)$ . To show that  $\mathcal{B}$  is a CBS, the two cases, where  $(0, 1, 1, 0)$  is an interior point and  $(0, 1, 1, 0)$  is an exterior point, are handled separately.

If  $(0, 1, 1, 0)$  is an interior point to  $\mathcal{C}$ , then Theorem 4.7 implies that this flock is linear, contradicting  $|\text{Range}(g)| = p^{h-d} + 1$ . Thus, this conic does not exist and  $\mathcal{B}$  blocks all conics with  $(0, 1, 1, 0)$  as an interior point.

If  $(0, 1, 1, 0)$  is an exterior point to  $\mathcal{C}$ , then Theorem 4.8 implies this flock is projectively equivalent to a KK-flock. But, any flock equivalent to a KK-flock in a plane of order  $p^h$  has size one (linear) or size  $\frac{p^h-1}{p^d-1}$  (nonlinear). Since  $p^{h-d} + 1 \neq 1$  or  $\frac{p^h-1}{p^d-1}$  for any  $d$  such that  $d \mid h$ ,  $\mathcal{C}$  does not exist and  $\mathcal{B}$  blocks all conics with  $(0, 1, 1, 0)$  as an exterior point.

Thus, the set of lines  $\{y = \frac{\text{tr}(t)-t}{t}x + z \mid t \neq 0\}$  form a CBS of size  $p^{h-d} + 1$  in the plane  $\text{PG}(2, p^h)$ , when  $h \neq 2d$  and  $h > 3$ . ■

In the trace-flock construction, the specific function  $g(t) = \frac{\text{tr}(t)-t}{t}$  was used to give the slopes of the lines in the CBS. Since  $g$  is an additive function divided by  $t$  and the size of its image set is known, we used  $g$  to form a CBS of size  $p^{h-d} + 1$ . Any function of this form can be used to construct a CBS, as long as the image contains more than one element.

The trace-flock construction does not give CBSs when  $q$  is prime, since the only additive function, up to scalar multiplication, is the identity.

As  $t$  and  $t^q$  are the only two automorphisms in  $\text{GF}(q^2)$  over  $\text{GF}(q)$ , any additive function in  $\text{GF}(q^2)$  has the form  $\alpha t + \beta t^q$ , where  $\alpha, \beta \in \text{GF}(q^2)$ ,  $\beta \neq 0$ . The image set of the function  $\frac{\alpha t + \beta t^q}{t} = \alpha + \beta t^{q-1}$  is the same size as the set of KK-lines.

Using the projectivity

$$\begin{bmatrix} \frac{-1}{\beta} & \frac{\alpha}{\beta} & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \in \text{PGL}(3, q^2),$$

we find that the set of lines  $\{y = (\alpha + \beta t^{q-1})x + z\}$  is projectively equivalent to the set of lines  $\{y = g(t)x + z \mid t \in \text{GF}(q^2)^*\} = \{y = t^{q-1}x + z \mid t \in \text{GF}(q^2)^*\}$ .

When  $g(t) = t^{q-1}$  and  $\alpha$  is a generator of  $\text{GF}(q^2)$ , we have that  $\text{Range}(g) = \{1, \alpha^{q-1}, \alpha^{2(q-1)}, \dots, \alpha^{q(q-1)}\}$  which is a cyclic subgroup of  $\text{GF}(q^2)$  of order  $q + 1$ .

Moreover, we have that when  $x \in \text{Range}(g)$ , then  $x^{-1} \in \text{Range}(g)$ .

In Section 2.4, we showed that the set of lines  $\{y = g(t)x + z \mid t \in \text{GF}(q^2)^*\} = \{y = t^{q-1}x + z \mid t \in \text{GF}(q^2)^*\}$  through  $(0, 1, 1)$  was projectively equivalent to the set of lines

$$T = \left\{ \left[ \begin{array}{c} -t^{q-1} \\ 1 \\ 0 \end{array} \right] \mid t \in \text{GF}(q^2) \right\}$$

through  $(0, 0, 1)$ . The KK-lines through  $(0, 1, 0)$  are given by

$$S = \left\{ \left[ \begin{array}{c} 1 \\ 0 \\ -mt^{q-1} \end{array} \right] \mid m = \text{fixed } \neq 0, t \in \text{GF}(q^2) \right\}.$$

Consider the projectivity

$$M = \begin{bmatrix} \frac{1}{m} & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \in \text{PGL}(3, q^2).$$

Observe that  $(0, 0, 1) \cdot M = (0, 1, 0)$  and

$$\begin{bmatrix} \frac{1}{m} & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} -t^{q-1} \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} -\frac{1}{m}t^{q-1} \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ -m\frac{1}{t^{q-1}} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ -ms^{q-1} \end{bmatrix} \in S.$$

Hence,  $T$  is projectively equivalent to the KK-lines in  $\text{PG}(2, q^2)$ . So, the set of lines through  $(0, 1, 1)$  generated by functions of the form  $\alpha + \beta t^{q-1}$ ,  $\beta \neq 0$  is projectively equivalent to the lines through  $(0, 1, 0)$  corresponding to KK-lines. Therefore, the trace-flock construction does not yield a CBS in  $\text{PG}(2, q^2)$ .

Table 4.1 lists the sizes of CBSs obtained by the trace-flock construction described in Theorem 4.9.

$q$	Guaranteed CBS Sizes
$p^3$	$p^2 + 1$
$p^4$	$p^3 + 1$
$p^5$	$p^4 + 1$
$p^6$	$p^5 + 1, p^4 + 1$
$p^7$	$p^6 + 1$
$p^8$	$p^7 + 1, p^6 + 1$
$p^9$	$p^8 + 1, p^6 + 1$
$p^{10}$	$p^9 + 1, p^8 + 1$

**Table 4.1:** CBS Sizes Given by the Trace-Flock Construction

For a fixed  $q$ , even the largest size of a CBS obtained by this construction is always smaller than those CBSs constructed in Lemma 4.1. When  $h$  is prime, the trace-flock construction yields exactly one CBS. When  $h$  is composite, a variety of CBSs are obtained. To emphasize the significance of this fact, the trace-flock construction gives a CBS of size 26 that blocks the (over  $3.05 \times 10^{10}$ ) conics in the plane  $\text{PG}(2, 125)$ , whereas by Lemma 4.1, 64 lines were needed to form a CBS.

### 4.3 Searching for Minimum CBSs

Having established that CBSs exist and having provided a construction of CBSs, we now focus on finding minimum CBSs and obtaining bounds on the sizes of these CBSs. Two different models that permit efficient computer searches for minimum CBSs are developed. The first model developed is later used in finding CBSs in  $\text{PG}(2, q^2)$ . The second model is similar to the one developed in Chapter 3. Both models are developed in the dual plane. The results of the searches are located at the end of this chapter.

Currently, finding a CBS consists of finding a set of concurrent lines such that the lines in this set have certain properties with respect to all conics in the plane. Namely, every conic in the plane must have at least one secant or tangent in that set. Dualizing, this set of concurrent lines becomes a set of points on a line, and these points all have special properties with respect to the dual conics. When we dualize by using the standard polarity, we transform each point (or line) into the line (or point) with the same coordinates. The conics in  $\pi$  are the zeros of nondegenerate quadratic forms. After dualizing, these line conics are associated with the same nondegenerate quadratic forms, which can be represented by  $3 \times 3$  nonsingular matrices. Since we are free to coordinatize  $\pi$  in any manner, we can

insure that the point of concurrency in the plane  $\pi$  for the two models below will be the point  $(0, 0, 1)$ . This point becomes the line  $z = 0$  in the dual plane  $\pi^*$ . In  $\pi$ , the lines through  $(0, 0, 1)$  have equations  $x = 0$  and  $mx + y = 0$ ,  $m \in \text{GF}(q)$ . After dualizing, these lines become the points  $(1, 0, 0)$  and  $(m, 1, 0)$ ,  $m \in \text{GF}(q)$ , on the line  $z = 0$  in  $\pi^*$ . In  $\pi$ , a CBS consists of a set of concurrent lines through the point  $(0, 0, 1)$  that satisfy a certain property. In  $\pi^*$ , a CBS consists of a set of points on the line  $z = 0$  that also satisfy some property. In these models, we identify the property that the points on the line  $z = 0$  must satisfy in order to be a CBS. For notational simplicity, we make the identification between the points of  $z = 0$  in  $\pi^*$ , and hence, the lines through  $(0, 0, 1)$  in  $\pi$ , and the elements of  $\text{GF}(q) \cup \{\infty\}$  by

$$\begin{aligned} mx + y = 0 &\leftrightarrow (m), \\ x = 0 &\leftrightarrow (\infty). \end{aligned}$$

This allows us to refer to the points of the CBS in terms of the parameters.

### 4.3.1 Restricted Quadratic Form Model

Before this model is developed, a review of linear algebra and quadratic forms is provided.

#### 4.3.1.1 Review of Linear Algebra and Quadratic Forms

The material presented in this section is found in greater detail in [54]. Throughout this section and model development, we work over the Galois field  $\mathcal{E} = \text{GF}(q)$ ,  $q = p^h$ ,  $p$  an odd prime. Let  $V = \mathcal{E}^3$  be the vector space over which we are working.

**Definition 4.10** *A function  $Q : V \mapsto \mathcal{E}$  is a quadratic form on  $V$  provided*

1.  $Q(cw) = c^2Q(w)$  for all  $c \in \mathcal{E}$ ,  $w \in V$ , and

2. for every  $u, v \in V$  the function  $f$  defined by  $f(u, v) = Q(u+v) - Q(u) - Q(v)$  is a symmetric, bilinear form called the polar form of  $Q$ .

If  $A$  is a given upper triangular matrix, then  $B = A + A^T$  is symmetric. A quadratic form is given by  $Q(X) = XAX^T$ . Two distinct points,  $X = \langle v \rangle$  and  $Y = \langle w \rangle$ , are orthogonal (or perpendicular) if and only if  $XBY^T = 0$ , which is equivalent to  $f(v, w) = Q(v + w) - Q(v) - Q(w) = 0$ . The polar of  $X$  is the line  $BX^T$ . The quadratic form  $Q$  is nonsingular and its polar form  $f$  is nondegenerate provided  $|B| = \det(B) \neq 0$ . The discriminant of  $Q$  (or of  $f$  or of  $B$ ) is defined to be  $\text{disc}(B) = |B|$  modulo the group of squares in  $\mathcal{E}^* = \mathcal{E} \setminus \{0\}$ .

As above, let  $Q : V \mapsto \mathcal{E}$  be a nonsingular quadratic form on  $V$  with polar form  $f$ . Since  $Q(v) = 0$  if and only if  $Q(cv) = c^2Q(v) = 0$  for all  $c \in \mathcal{E}^*$ , the quadric  $Q(n-1, q) = \{v \in P(V) : Q(v) = 0\}$  is a well-defined set of points of the projective space  $P(V)$  associated with  $V$ . If  $W$  is a subspace of  $V$ , define  $W^\perp = \{v \in V : f(v, w) = 0 \text{ for all } w \in W\}$ . If  $W \cap W^\perp = \{0\}$ , it is possible to show that  $V = W \oplus W^\perp$ . Moreover, if  $\mathcal{B}_1$  is a basis of  $W$  and  $\mathcal{B}_2$  is a basis of  $W^\perp$ , then  $\mathcal{B}_1 \cup \mathcal{B}_2$  is a basis of  $V$ , and the matrix  $B$  that is the Gram matrix of  $Q$  with respect to the basis  $\mathcal{B}_1 \cup \mathcal{B}_2$  is the direct sum of the matrices of  $B_1, B_2$  that are the Gram matrices of  $Q$  restricted to  $W, W^\perp$ , respectively. Hence,

$$\text{disc}(Q) = \text{disc}(Q|_W) \cdot \text{disc}(Q|_{W^\perp}).$$

Now suppose  $W = \langle x, y \rangle$  is a line, that is, a rank two subspace of  $V$ . Put  $f(x, x) = a, f(x, y) = f(y, x) = b, f(y, y) = c$ . Then  $\text{disc}(Q|_W) = \begin{vmatrix} a & b \\ b & c \end{vmatrix} = ac - b^2$ . So  $Q(dx + ey) = 0$  if and only if  $0 = f(dx + ey, dx + ey) = d^2a + 2deb + e^2c$  has no solutions  $(d, e) \neq (0, 0)$  if and only if  $4b^2 - 4ac = -4(b^2 - ac) \equiv -\text{disc}(Q|_W) = \not\equiv \in \mathcal{E}$ . This proves the following theorem.

**Theorem 4.11** *The line  $W$  is anisotropic (or elliptic), that is, contains no nonzero vector  $v$  with  $Q(v) = 0$ , if and only if  $-\text{disc}(Q|_W) = \emptyset$ . ■*

This result may be used to develop a formula to classify a point with respect to a conic  $C$  given by the quadratic form  $Q$  as being either interior or exterior. If  $W$  is a subspace for which  $W \cap W^\perp = 0$ , then  $\text{disc}(Q) = \text{disc}(Q|_W) \cdot \text{disc}(Q|_{W^\perp})$ . If  $P$  is a point, then  $P^\perp$  is a line. Put  $W = P^\perp$ , so  $W^\perp = P$ . Then  $P$  is an internal point of the quadric given by  $Q$  if and only if  $W = P^\perp$  is anisotropic, that is, if and only if  $-\text{disc}(Q|_W) = \emptyset$ . Hence,  $P$  is an internal point if and only if

$$\text{disc}(Q) = \text{disc}(Q|_W) \cdot \text{disc}(Q|_{W^\perp})$$

$$\text{disc}(Q) = -\emptyset \cdot \text{disc}(Q|_{W^\perp})$$

$$\text{disc}(Q) = -\emptyset \cdot f(P, P)$$

$$\text{disc}(Q) = -\emptyset \cdot 2Q(P)$$

$$\emptyset \text{disc}(Q) = -2Q(P)$$

$$\emptyset(\text{disc}(Q))^2 = -2Q(P)\text{disc}(Q)$$

$$\emptyset = -2Q(P)\text{disc}(Q).$$

Thus,  $P$  is an internal point of  $C$  if and only if  $-2Q(P)\text{disc}(Q) = \emptyset$  and  $P$  is an external point of  $C$  if and only if  $-2Q(P)\text{disc}(Q) = \square$ .

**Example 11.** In this example, the points on the line  $z = 0$  are classified with respect to the conic  $C$  given by the quadratic form  $Q : x^2 + y^2 - xz + z^2$  in  $\text{PG}(2, 5)$ .

The points of  $C$  are  $\{(1, 2, 0), (1, 3, 0), (0, 2, 1), (0, 3, 1), (1, 2, 1), (1, 3, 1)\}$ , and the points of  $z = 0$  are  $\{(1, 0, 0), (0, 1, 0), (1, 1, 0), (1, 2, 0), (1, 3, 0), (1, 4, 0)\}$ . The tangent lines, along with the points contained in them, are listed below.

$$\begin{aligned}
y = 3x + z & : \{(1, 3, 0), (0, 1, 1), (1, 4, 1), (2, 2, 1), (3, 0, 1), (4, 3, 1)\} \\
y = x + z & : \{(1, 1, 0), (0, 1, 1), (1, 2, 1), (2, 3, 1), (3, 4, 1), (4, 0, 1)\} \\
y = 4x + 2z & : \{(1, 4, 0), (0, 2, 1), (1, 1, 1), (2, 0, 1), (3, 4, 1), (4, 3, 1)\} \\
y = x + 3z & : \{(1, 1, 0), (0, 3, 1), (1, 4, 1), (2, 0, 1), (3, 1, 1), (4, 2, 1)\} \\
y = 4x + 4z & : \{(1, 4, 0), (0, 4, 1), (1, 3, 1), (2, 2, 1), (3, 1, 1), (4, 0, 1)\} \\
y = 2x + 4z & : \{(1, 2, 0), (0, 4, 1), (1, 1, 1), (2, 3, 1), (3, 0, 1), (4, 2, 1)\}
\end{aligned}$$

Clearly, the points  $(1, 1, 0)$  and  $(1, 4, 0)$  are exterior points because these points lie on two tangents. The points  $(0, 1, 0)$  and  $(1, 0, 0)$  do not lie on any tangent lines and therefore must be interior points. Finally, the points  $(1, 1, 0)$  and  $(1, 3, 0)$  are conic points.

The  $\text{disc}(Q) = \square$  which implies that  $-2\text{disc}(Q)Q(P) = \emptyset$ . The following chart shows the classification of each point on  $z = 0$ , using the formula provided in this section.

$P$	$Q(P)$	$-2\text{disc}(Q)Q(P)$	Classification
$(1, 0, 0)$	$1 = \square$	$\emptyset \square \square = \emptyset$	internal
$(0, 1, 0)$	$1 = \square$	$\emptyset \square \square = \emptyset$	internal
$(1, 1, 0)$	$2 = \emptyset$	$\emptyset \square \emptyset = \square$	external
$(1, 2, 0)$	$0$	$\emptyset \square 0 = 0$	on
$(1, 3, 0)$	$0$	$\emptyset \square 0 = 0$	on
$(1, 4, 0)$	$2 = \emptyset$	$\emptyset \square \emptyset = \square$	external

■

### 4.3.1.2 Restricting Nondegenerate Quadrics to a Line

$W = \langle (1, 0, 0), (0, 1, 0) \rangle$  is a line, namely, the line  $z = 0$ . Consider the conic given by the nondegenerate quadratic form  $Q(X) = XAX^T$  on  $\mathcal{E}^3 = \text{GF}(q)^3$  where

$$A = \begin{bmatrix} a & b & d \\ 0 & c & e \\ 0 & 0 & f \end{bmatrix}$$

and

$$B = A + A^T = \begin{bmatrix} 2a & b & d \\ b & 2c & e \\ d & e & 2f \end{bmatrix}.$$

It is not difficult to show that the pole of  $z = 0$  is the point  $\left( \frac{be-2cd}{\det(B)}, \frac{bd-2ae}{\det(B)}, \frac{4ac-b^2}{\det(B)} \right)$  or equivalently  $(be - 2cd, bd - 2ae, 4ac - b^2)$ . If  $4ac = b^2$ , then the pole of  $z = 0$  lies on  $z = 0$  and  $W \cap W^\perp \neq \{0\}$ . If  $4ac \neq b^2$ , then the pole of  $z = 0$  does not lie on  $z = 0$  and  $W \cap W^\perp = \{0\}$ . Thus, if  $W \cap W^\perp = \{0\}$  then  $4ac \neq b^2$ , and if  $W \cap W^\perp \neq \{0\}$  then  $4ac = b^2$ ; as these statements are the contrapositives of the previous statements.

The structure of  $Q|_W$  is now reviewed. Assume that  $4ac \neq b^2$ ,  $W = \langle (1, 0, 0), (0, 1, 0) \rangle = \langle \bar{x}, \bar{y} \rangle$  and  $W^\perp = \langle (j, k, 1) \rangle = \langle \bar{z} \rangle$ . Clearly,  $W \cap W^\perp = \{0\}$ . Write  $V = W \oplus W^\perp$  and compute the Gram matrix for the quadratic form  $Q$  given by  $Q(X) = XAX^T = ax^2 + bxy + cy^2 + dxz + eyz + fz^2$  where  $A$  and  $B$  are given above. Now,

$$f(\bar{x}, \bar{x}) = 2Q(\bar{x}) = 2a$$

$$\begin{aligned}
f(\bar{x}, \bar{y}) &= a + b + c - a - c = b \\
f(\bar{y}, \bar{x}) &= f(\bar{x}, \bar{y}) \\
f(\bar{y}, \bar{y}) &= 2Q(\bar{y}) = 2c \\
f(\bar{z}, \bar{z}) &= 2Q(\bar{z}).
\end{aligned}$$

The Gram matrix of  $f$  is given by

$$\left[ \begin{array}{cc|c} 2a & b & 0 \\ b & 2c & 0 \\ \hline 0 & 0 & 2Q(\bar{z}) \end{array} \right] = \left[ \begin{array}{c|c} B_1 & \vec{0} \\ \hline \vec{0} & B_2 \end{array} \right].$$

Recall that in Section 4.3.1.1, it was shown that  $0 \neq \det(B) = \det(B_1) \cdot \det(B_2)$ , and we have that  $\det(B_1) = 4ac - b^2 \neq 0$  and  $\det(B_2) = 2Q(\bar{z})$ . Now,  $Q|_W$  is given by  $\tilde{X}A'\tilde{X}^T = ax^2 + bxy + cy^2$  where

$$A' = \begin{bmatrix} 2a & b \\ b & 2c \end{bmatrix}.$$

Let  $\bar{P}$  denote  $P|_W$ , that is, if  $P = (m, n, 0)$ , then  $\bar{P} = (m, n)$ . For any point  $\bar{P} \in W$ , we have that  $Q|_W(\bar{P}) = am^2 + bmn + cn^2 = Q(P)$ .

Under the specified conditions, this restriction of the quadratic form to the line  $z = 0$  is what enables the model for finding small CBSs to be efficient. Effectively, the problem drops from six variables (the coefficients in the quadratic form) to three variables (the coefficients in the quadratic form restricted to the line  $z = 0$ ).

As mentioned earlier, the point  $(0, 0, 1)$  becomes the line  $z = 0$  in the dual plane. In  $\pi$ , a quadric is a set of points satisfying a quadratic equation. In  $\pi^*$ , the dual line quadric is the set of lines whose line coordinates satisfy the same quadratic equation. If the pole of  $z = 0$  is a point on the line  $z = 0$ , then this

implies that  $z = 0$  is a line of the line quadric. Thus in  $\pi$ , the point  $(0, 0, 1)$  is on the quadric and therefore, this quadric is blocked. To clarify this idea, we offer the following example.

**Example 12.**

Let  $\mathcal{E} = \text{GF}(5)$  and consider the conic with equation  $y^2 - xz = 0$  in  $\text{PG}(2, 5)$ . This conic is given by the quadratic form  $Q(X) = XAX^T$  where

$$A = \begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

and

$$B = A + A^T = \begin{bmatrix} 0 & 0 & -1 \\ 0 & 2 & 0 \\ -1 & 0 & 0 \end{bmatrix}.$$

Now,  $\det(B) = 3$  so that  $\text{disc}(Q) = \emptyset$ . In  $\pi$ , the points on the conic are  $\{(0, 0, 1), (1, 0, 0), (1, 1, 1), (1, 4, 1), (4, 2, 1), (4, 3, 1)\}$ , and clearly, the line  $z = 0$  is a tangent line to  $C$ . The pole of  $z = 0$  with respect to this conic is the point  $(1, 0, 0)$  which, coincidentally, is also a point of the conic. If  $W = \langle(1, 0, 0), (0, 1, 0)\rangle$  then  $W^\perp = \langle(1, 0, 0)\rangle$  and  $W \cap W^\perp \neq \{0\}$ , so  $V$  cannot be written as  $W \oplus W^\perp$ . Notice that the point  $(0, 0, 1)$  is on the conic and this conic will be blocked in  $\pi$  by any non-empty set of lines through  $(0, 0, 1)$ . ■

**4.3.1.3 Classifying Points in the Dual Setting**

In Section 4.3.1.1, an explanation of how to classify a point with respect to a conic as being interior or exterior was given. To summarize, let  $P$  be a point in the plane and  $C$  a conic given by the quadratic form  $Q$ . If

$$-2Q(P)\text{disc}(Q) = \begin{cases} \emptyset \\ \square \\ 0 \end{cases} \text{ then } P \text{ is } \begin{cases} \text{internal to} \\ \text{external to} \\ \text{on} \end{cases}$$

the conic. We have shown that if  $W = \langle(1, 0, 0), (0, 1, 0)\rangle$  and  $W \cap W^\perp = \{0\}$ , then for all  $P \in W$ , we have  $Q(P) = Q|_W(P)$ . This implies that if

$$-2Q(P)\text{disc}(Q) = -2Q|_W(P)\text{disc}(Q) = \begin{cases} \not\sqsupset \\ \square \\ 0 \end{cases} \text{ then } P \text{ is } \begin{cases} \text{internal to} \\ \text{external to} \\ \text{on} \end{cases}$$

the conic. Since we are dealing with quadratic forms restricted to the line, we cannot say for certain whether  $\text{disc}(Q|_W)$  is a  $\square$  or a  $\not\sqsupset$ , as is illustrated by the following example.

**Example 13.** Let  $\mathcal{E} = \text{GF}(5)$  and consider the conic with equation  $x^2 + xy + y^2 + fz^2 = 0$ ,  $f \neq 0$ , in  $\text{PG}(2, 5)$ . This conic is given by the quadratic form  $Q(X) = XAX^T$  where

$$A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & f \end{bmatrix}$$

and

$$B = A + A^T = \begin{bmatrix} 2 & 1 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 2f \end{bmatrix}.$$

We have shown that  $Q|_W = x^2 + xy + y^2$ , where  $W = \langle(1, 0, 0), (0, 1, 0)\rangle = \langle\bar{x}, \bar{y}\rangle$ .

The polar of  $(0, 0, 1)$  is  $W$ , since

$$\begin{bmatrix} 2 & 1 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 2f \end{bmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}.$$

So,  $W^\perp = \langle(0, 0, 1)\rangle = \langle\bar{z}\rangle$  and  $W \cap W^\perp = \{0\}$ . Also,  $\det(B) = f$ .

Assume  $f = 1$ , so that  $\text{disc}(Q) = \square$ . We now classify the points in  $W$  with respect to  $Q$ .

$P$	$-2\text{disc}(Q)Q(P)$	Classification
$(1, 0, 0)$	$\not\equiv$	internal
$(0, 1, 0)$	$\not\equiv$	internal
$(1, 1, 0)$	$\square$	external
$(2, 1, 0)$	$0$	on
$(3, 1, 0)$	$0$	on
$(4, 1, 0)$	$\square$	external

Assume  $f = 2$ , so that  $\text{disc}(Q) = \not\equiv$ . We now classify the points in  $W$  with respect to  $Q$ .

$P$	$-2\text{disc}(Q)Q(P)$	Classification
$(1, 0, 0)$	$\square$	external
$(0, 1, 0)$	$\square$	external
$(1, 1, 0)$	$\not\equiv$	internal
$(2, 1, 0)$	$0$	on
$(3, 1, 0)$	$0$	on
$(4, 1, 0)$	$\not\equiv$	internal

■

This example shows that when the quadratic form is restricted to the line  $z = 0$ , the information about the discriminant of  $Q$  is lost.

Since  $\text{disc}(Q) = \text{disc}(Q|_W) \cdot (2f \pmod{\square})$ , by varying the choices of  $f$ ,  $\text{disc}(Q)$  varies. Therefore the external points to the dual conic on the line  $z = 0$  are either

$$\{(x, y, 0) \mid Q(x, y, 0) = Q|_W(x, y) = \square\}$$

or

$$\{(x, y, 0) \mid Q(x, y, 0) = Q|_W(x, y) = \emptyset\}.$$

Now, as there are conics in the original plane for which the external points on  $z = 0$  to the dual conic are  $\{(x, y, 0) \mid Q(x, y, 0) = Q|_W(x, y) = \square\}$  and there are conics in the original plane for which the external points on  $z = 0$  are  $\{(x, y, 0) \mid Q(x, y, 0) = Q|_W(x, y) = \emptyset\}$ , both these situations must be taken into account in the model development.

#### 4.3.1.4 The Restricted-Dual Model Summary

By dualizing, the problem is transformed from finding a set of concurrent lines that satisfy a certain property to finding a set of collinear points that satisfy some property. Define the subspace  $W$  of  $V$  to be  $\langle(1, 0, 0), (0, 1, 0)\rangle$ . If  $W \cap W^\perp = \{0\}$ , then we may write  $V = W \oplus W^\perp$  and  $Q|_W$  is nondegenerate. Let  $\mathcal{B}$  be the set of points on  $z = 0$  corresponding to a specific set of concurrent lines in the original plane. In order for  $\mathcal{B}$  to be a CBS, one of the following must be satisfied.

1. There exists a point  $u \in \mathcal{B}$  such that  $Q|_W(u) = 0$ . ( $u$  corresponds to a tangent line in the original plane.)
2. There exists at least two distinct points  $u$  and  $v$  in  $\mathcal{B}$  such that  $Q|_W(u) = \square$  and  $Q|_W(v) = \emptyset$ . ( $Q|_W(u) \neq 0$  and  $Q|_W(v) \neq 0$ .) ( $u$  and  $v$  correspond to one secant line and one exterior line in the original plane.)

Now, if  $W \cap W^\perp \neq \{0\}$ , then we may not write  $V = W \oplus W^\perp$ . This will not affect the CBS problem. When  $W \cap W^\perp \neq \{0\}$  with respect to some quadratic form  $Q$ , then  $Q$  is already blocked in  $\pi$ .

#### 4.3.1.5 Finding the CBSs in the Set Covering Setting

We now discuss how the computer is used in the search for minimum CBSs.

We examine each of the conics of the form  $ax^2 + bxy + cy^2 = 0$  and store the classification of the points of  $z = 0$  in an array  $B$ , such that:

- the columns of  $B$  are the points of the line  $z = 0$ ,
- the rows of  $B$  are the dual conics,
- the entries are the classification of a point with respect to a conic, that is, 1 is stored if the point is exterior (secant line),  $-1$  is stored if the point is interior (exterior line), and 0 is stored if the point is on the conic (tangent line).

To obtain a CBS, we find a set of columns such that each row of  $B$  has a 0 or 1 in at least one column of this set. This set of columns corresponds to a set of points in  $\pi^*$  which, in turn, corresponds to a set of lines in  $\pi$ . To find a minimum CBS, we want to obtain the smallest such set of columns. This is a set covering problem which can be efficiently solved using a commercial solver such as Cplex.

We create a new array  $A$  from  $B$  by the mapping

$$a_{ij} = \begin{cases} 1 & \text{if } b_{ij} = 0, \\ 1 & \text{if } b_{ij} = 1, \\ 0 & \text{if } b_{ij} = -1. \end{cases}$$

Let  $\vec{x}$  be a binary vector of length  $q + 1$ . The vector  $\vec{x}$  is used to keep track of which columns (points) are selected for the CBS. For instance, if  $x(i) = 1$ , then

the point represented by column  $i$  has been selected to be in the CBS. If  $x(j) = 0$ , then the point represented by column  $j$  has not been selected to be in the CBS. Then the optimization problem is to find an  $\vec{x}$  with

$$\min \sum_{i=1}^{q+1} x(i)$$

such that for all rows,  $k$  of the array  $A$

$$\sum_{i=1}^{q+1} A(k, i)x(i) \geq 1.$$

If any row of  $A$  is picked and multiplied by  $\vec{x}$ , a nonnegative integer is obtained, for we are only multiplying 0's and 1's. If for some row of  $A$ , a 0 is obtained by multiplying by  $\vec{x}$ , then there is not a representative in that image set. Hence,  $\vec{x}$  cannot represent a CBS.

**Example 14.**

There are nine conics given by the quadratic forms, up to scalar multiplication, of the type  $ax^2 + bxy + cy^2$  in  $\text{PG}(2, 3)$ . They are  $xy$ ,  $xy + y^2$ ,  $2xy + y^2$ ,  $x^2 + xy$ ,  $x^2 + 2xy$ ,  $x^2 + y^2$ ,  $x^2 + 2y^2$ ,  $x^2 + xy + y^2$ , and  $x^2 + 2xy + 2y^2$ . The array  $B$  with the point classification and the corresponding array  $A$  are given in Table 4.5.

$$\begin{array}{ccc}
B = & & A = \\
\left[ \begin{array}{cccc}
0 & -1 & 1 & 0 \\
0 & 1 & -1 & 0 \\
0 & 1 & 0 & -1 \\
0 & -1 & 0 & 1 \\
0 & 0 & 1 & -1 \\
0 & 0 & -1 & 1 \\
-1 & 1 & 0 & 0 \\
1 & -1 & 0 & 0 \\
-1 & 0 & 1 & 0 \\
1 & 0 & -1 & 0 \\
1 & -1 & -1 & 1 \\
-1 & 1 & 1 & -1 \\
-1 & 0 & 0 & 1 \\
1 & 0 & 0 & -1 \\
1 & 1 & -1 & -1 \\
-1 & -1 & 1 & 1 \\
1 & -1 & 1 & -1 \\
-1 & 1 & -1 & 1
\end{array} \right] & \longleftrightarrow & \left[ \begin{array}{cccc}
1 & 0 & 1 & 1 \\
1 & 1 & 0 & 1 \\
1 & 1 & 1 & 0 \\
1 & 0 & 1 & 1 \\
1 & 1 & 1 & 0 \\
1 & 1 & 0 & 1 \\
0 & 1 & 1 & 1 \\
1 & 0 & 1 & 1 \\
0 & 1 & 1 & 1 \\
1 & 1 & 0 & 1 \\
1 & 0 & 0 & 1 \\
0 & 1 & 1 & 0 \\
0 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 \\
1 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 \\
1 & 0 & 1 & 0 \\
0 & 1 & 0 & 1
\end{array} \right]
\end{array}$$

**Table 4.5:** Array  $B$  to Array  $A$  Conversion in  $\text{PG}(2,3)$

It is not difficult to see that the selection of any two columns is not sufficient to form a CBS, but the selection of any three columns (points) is sufficient to form a CBS. This is consistent with the results of Theorem 4.2. ■

### 4.3.2 Secant-Tangent Mapping Model

The restricted-dual model allowed us to efficiently find a minimum CBS for planes of small order. These CBSs can be found in parameter form in Appendix B. We now make minor modifications to the model developed in Chapter 3, to obtain a similar model for finding minimum CBSs when  $q$  is odd. Since most of the details for this model are provided in Chapter 3, only the changes that are necessary to make the corresponding model work in odd characteristic are mentioned.

When the characteristic of the plane is even, every conic has a unique nucleus. When the characteristic of the plane is odd, there is no nucleus of a conic and so the orbits of a stabilizer of a conic in a plane of odd characteristic will not be the same as a conic in a plane of even characteristic. As shown in Chapter 2, in a plane of odd characteristic, the stabilizer of a conic has the three orbits:

1. the points of the conic;
2. the external points with respect to the conic;
3. the internal points with respect to the conic.

That is, the stabilizer of a conic is transitive on the set of internal points of a conic and is transitive on the set of external points of a conic.

Since  $\text{PGL}(3, q)$  acts transitively on the set of conics of  $\text{PG}(2, q)$ , and the stabilizer of a conic acts transitively on the set of internal points and the set of external points, for any point  $P$ , the stabilizer of  $P \in \text{PGL}(3, q)$  acts transitively

on the sets of conics for which  $P$  is an internal or external point. This implies that when  $P$  is stabilized and  $\mathcal{C}$  is mapped to another conic  $\mathcal{C}_1$ , the secant and tangent lines of  $\mathcal{C}$  are mapped to secant and tangent lines of  $\mathcal{C}_1$ . Just as in the model developed in Chapter 3, denote the lines through a point  $P$  with nonhomogeneous coordinates  $[t]$ , if the line is non-vertical, and  $[\infty]$ , for the vertical line through  $P$ , and denote the lines through a point  $Q$  with nonhomogeneous coordinates  $[u]$ , if the line is non-vertical, and  $[\infty]$ , for the vertical line through  $Q$ . Now, if an element  $g \in \text{PGL}(3, q)$  maps the point  $P$  to the point  $Q$ , then there is an element  $h = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{PGL}(2, q)$  with the property that for any line  $l$  through  $P$  with coordinate  $[t]$  or  $[\infty]$ , the coordinate of the image of  $l$  under  $g$  is given by

$$u = \frac{at+c}{bt+d}, \text{ if } bt + d \neq 0$$

$$\infty, \quad \text{otherwise.}$$

Thus, for each element in  $\text{PGL}(3, q)$  that maps  $\mathcal{C}$  to  $\mathcal{C}_1$ , there is an element in  $\text{PGL}(2, q)$  that sends the secant and tangent lines of  $\mathcal{C}$  through  $P$  to the secant and tangent lines of  $\mathcal{C}_1$  through  $P$ .

When the order of the plane was even, one conic was used to generate an initial set of tangent and secant lines. Since the order of the plane is odd, the cases of  $P$  being an internal and external point must be dealt with separately when generating the sets of initial secant and tangent lines. The first case handled is when  $P$  is an internal point.

Consider the conic  $Q$  whose points satisfy  $-xy + y^2 + 2yz + z^2 = 0$ . The lines  $x = 0$  and  $y = 0$  are tangent lines to  $Q$ . Since  $(0, 0, 1)$  lies on both of these tangent lines,  $(0, 0, 1)$  is an external point with respect to  $Q$ . The lines through  $(0, 0, 1)$  are  $x = 0$  and  $y = mx$ , for  $m \in \mathcal{E}$ . It is not difficult to show that  $y = mx$  is a secant

line when  $m = \square \neq 0$ . For this conic, the set of parameters  $\{m \mid m = \square\} \cup \{\infty\}$ , represent the secant and tangent lines of  $Q$ .

Now, consider the conic  $Q$ , whose points satisfy  $ny^2 + xz + z^2 = 0$ , where  $n$  is a fixed  $\not\square$ . In order for a line with equation  $y = mx$  to be a tangent line to  $Q$ , we must have that  $\frac{1}{4n} = m^2$ , which cannot occur. Thus, there are no lines through  $(0, 0, 1)$  that are tangent to  $Q$ , and  $(0, 0, 1)$  is an internal point to  $Q$ . The line  $y = mx$  is a secant line to  $Q$  provided that  $m$  is such that  $1 - 4nm^2 = \square$ . If  $-1 = \square$ , then  $x = 0$  is an exterior line to  $Q$ . If  $-1 = \not\square$ , then  $x = 0$  is a secant line to  $Q$ . When  $q \equiv 1 \pmod{4}$ , the set of parameters for the secant lines of  $Q$  through  $(0, 0, 1)$  is  $\{m \mid 1 - 4nm^2 = \square\} \cup \{\infty\}$ . When  $q \equiv 3 \pmod{4}$ , the set of parameters for the secant lines of  $Q$  through  $(0, 0, 1)$  is  $\{m \mid 1 - 4nm^2 = \square\}$ .

Once these sets of secant and tangent lines are identified, the development of the model is nearly identical to the even characteristic model. Using the standard duality, we dualize so that all the lines through  $(0, 0, 1)$  become points on the line  $z = 0$  with homogeneous coordinates  $(m, 1, 0)$ ,  $m \in \text{GF}(q)$  and  $(0, 0, 1)$ . Note that we can still use the specified parameter sets to identify the points in the dual plane that correspond to tangent and secant lines in the original plane.

Let  $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{PGL}(2, q)$  and consider the following calculations:

$$(x, 1) \begin{bmatrix} a & b \\ c & d \end{bmatrix} = (ax + c, bx + d) = \begin{cases} \left(\frac{ax+c}{bx+d}, 1\right), & \text{if } bx + d \neq 0 \\ (1, 0), & \text{if } bx + d = 0, \end{cases}$$

$$(1, 0) \begin{bmatrix} a & b \\ c & d \end{bmatrix} = (a, b) = \begin{cases} \left(\frac{a}{b}, 1\right), & \text{if } b \neq 0 \\ (1, 0), & \text{if } b = 0. \end{cases}$$

For  $q \equiv 1 \pmod{4}$ , the image sets of  $\{m \mid m = \square, 0\} \cup \{\infty\}$  and  $\{m \mid 1 - 4nm^2 = \square\} \cup \{\infty\}$  are

$$\left\{ \frac{am+c}{bm+d} \mid m = \square, 0 \right\} \cup \left\{ \frac{a}{b} \right\} \quad \text{and} \quad \left\{ \frac{am+c}{bm+d} \mid 1 - 4m^2n = \square \right\} \cup \left\{ \frac{a}{b} \right\},$$

respectively. For  $q \equiv 3 \pmod{4}$ , the image sets of  $\{m \mid m = \square, 0\} \cup \{\infty\}$  and  $\{m \mid 1 - 4nm^2 = \square\}$  are

$$\left\{ \frac{am+c}{bm+d} \mid m = \square, 0 \right\} \cup \left\{ \frac{a}{b} \right\} \quad \text{and} \quad \left\{ \frac{am+c}{bm+d} \mid 1 - 4m^2n = \square \right\},$$

respectively. It is understood that if  $bm+d=0$ ,  $\frac{am+c}{bm+d} = \infty$ , and if  $b=0$ ,  $\frac{a}{b} = \infty$ .

To summarize the procedure, we find two conics  $\mathcal{C}_1$  and  $\mathcal{C}_2$ , and then we fix a point  $P \notin \mathcal{C}_1$  or  $\mathcal{C}_2$ , such that  $P$  is external to  $\mathcal{C}_1$  and internal to  $\mathcal{C}_2$ . After identifying the secant and tangent lines through  $P$  to the respective conics, we obtain two parameter sets of points in the dual plane that correspond to tangent and secant lines of these conics in the original plane. Using collineations of the line  $\text{PG}(1, q)$ , these sets of parameters are mapped to two more sets of parameters representing tangent and secant lines of another conic in  $\text{PG}(2, q)$ . Once all possible parameter sets corresponding to tangent and secant lines have been generated, a minimum CBS can be found by selecting a representative from each of these sets in such a way as to get the smallest number of distinct representatives.

Since the resulting computer and optimization model are nearly identical to the models developed above and in Chapter 3, we do not develop them again. Listed in Table 4.6 are the sizes of the minimum CBSs found. The points that comprise the minimum conic blocking set found by either model are located in Appendix B.

$m =$  size of minimum CBS in  $\text{PG}(2, q)$

$q$	$m$	$q$	$m$	$q$	$m$	$q$	$m$	$q$	$m$
3	3	19	6	41	8	67	9	97	10
5	4	23	7	43	8	71	9	101	10
7	4	25	8	47	8	73	9	103	10
9	5	27	8	49	9	79	8	107	10
11	6	29	8	53	9	81	10	109	10
13	6	31	8	59	9	83	10	113	10
17	6	37	8	61	9	89	10	125	11

**Table 4.6:** Values for Minimum CBSs

A complete search for minimum CBSs by Cplex in  $\text{PG}(2, 121)$  and  $\text{PG}(2, 169)$  was not feasible. Although a CBS of size 11 in  $\text{PG}(2, 121)$  and a CBS of size 12 in  $\text{PG}(2, 169)$  were located, due to memory constraints, Cplex was unable to verify that these CBSs are of minimum size.

#### 4.4 Small Conic Blocking Sets in $\text{PG}(2, q^2)$

The trace-flock construction is a method which produces CBSs in  $\text{PG}(2, p^h)$ ,  $h > 2$ . In this section, we present a construction derived from a model involving restricting quadratic forms to the line  $z = 0$ , which gives CBSs of size  $2q - 1$  in  $\text{PG}(2, q^2)$ . Let  $\mathcal{E} = \text{GF}(q^2)$ ,  $\mathcal{K} = \text{GF}(q)$ , and  $\mathcal{F} = \text{GF}(p)$  for  $p$  an odd prime,  $q = p^h$ . Let  $\text{tr}(x) = x + x^q$  denote the relative trace of an element  $x$  of  $\mathcal{E}$  into  $\mathcal{K}$ .

While working with the model described in Section 4.3.1, we were working with conics in the restricted dual setting. A CBS is identified with a set of points

on the line  $z = 0$ . A conic given by the quadratic form  $Q$ , in this setting, is blocked by a set of points (CBS) if

1.  $\exists P \in \text{CBS} \ni Q(P) = 0$ , or
2.  $\exists P, R \in \text{CBS}, P \neq R \ni Q(P) = \square$  and  $Q(R) = \square$ .

The line  $z = 0$  consists of the points  $\{(1, n, 0) \mid n \in \mathcal{E}\} \cup \{(0, 1, 0)\}$ . For simplicity's sake, we drop the third coordinate, which is always 0, and denote the points on  $z = 0$  by  $\{(1, n) \mid n \in \mathcal{E}\} \cup \{(0, 1)\}$ . The conics that are to be blocked have the quadratic form  $Q(x, y) = Ax^2 + Dxy + By^2$  with the additional property that  $D^2 - 4AB \neq 0$ . Because of the equivalence of points written in homogeneous coordinates, for  $n \neq 0$  the point  $(1, n)$  may be written as  $(m, 1)$  for some nonzero  $m \in \mathcal{E}$ . These points are rewritten in order to simplify the notation that is used in the proofs of Lemma 4.15 and Theorem 4.23. Next, we assign to each of the points on  $z = 0$  a parameter in  $\mathcal{E} \cup \{\infty\}$ . We make the assignments of the points on  $z = 0$  with the elements of  $\mathcal{E} \cup \{\infty\}$  as follows: assign to the point  $(0, 1)$  the parameter  $\infty$ , assign to the point  $(1, 0)$  the parameter 0, and to the remaining points  $(1, n)$ , or equivalently  $(m, 1)$ , assign the parameter  $m$  for all  $m \in \mathcal{E}^*$ .

By transitivity of  $\text{PGL}(2, q)$  on the points of  $\text{PG}(1, q)$ , we can assume the point given by the parameter 0 is in the CBS. Now,  $Q(1, 0) = A$ . This implies that if  $A = 0$ , the conic is blocked. Hence, we may assume  $A$  is nonzero and divide through by  $A$  to obtain the quadratic form  $Q'(x, y) = x^2 + dxy + ay^2$ . Since the remaining points to be chosen for the CBS are of the form  $(x, 1)$ , throughout the rest of this section we will work with the quadratic form  $Q$  given by

$$Q'(x, 1) = Q(x) = x^2 + dx + a, \tag{4.1}$$

and we identify the points of  $z = 0$  with their assigned parameters in  $\mathcal{E}$ .

Observe that for any point  $m$  chosen for the CBS,

$$Q(m) = m^2 + dm + a. \quad (4.2)$$

We also have that

$$Q'(1, 0) = 1. \quad (4.3)$$

For  $Q$  not to be blocked by a set  $S$ , the “squarity” (being a square or a nonsquare) of (4.2) has to be the same as (4.3), for all  $x \in S$ . Now, as  $1 = \square$ , the only conics that are not blocked by 0 are those for which  $Q(x) = \square$  for all points  $x \in S$ .

Before the main result of this section is given, several algebraic observations will be made.

**Lemma 4.12**  *$\mathcal{E}$  is partitioned into cosets of  $\ker(\text{tr})$  and each coset has size  $q$ .*

**Proof:** The relative trace function is a homomorphism from  $\mathcal{E}$  onto  $\mathcal{K}$ . Now,  $\text{tr}(x) = x + x^q = 0$  if and only if  $x = 0$  or  $1 + x^{q-1} = 0$ . Define  $f(x) = x^{q-1}$  for all  $x \in \mathcal{E}$ . We show that  $f(x) = -1$  has  $q - 1$  solutions. Let  $\alpha$  be a primitive element of  $\mathcal{E}$ . Then  $x = \alpha^{(q+1)/2}$  satisfies  $x^{q-1} = -1$ . So,  $-1$  is in the image of  $f$ . Now,  $f$  is a multiplicative homomorphism and  $q - 1$  divides the order  $q^2 - 1$  of the multiplicative (cyclic) group,  $\mathcal{E}^*$ . Thus, since  $-1$  is in the image of  $f$ , there are exactly  $q - 1$  solutions. This shows that the kernel of  $\text{tr}$  has size  $q$ . Hence, the image of  $\text{tr}$  has size  $q^2/q = q$ . Finally, the domain of a homomorphism is partitioned into cosets of the kernel, so  $\mathcal{E}$  is partitioned into cosets of the kernel of  $\text{tr}$ . ■

The previous lemma tells us that there are  $q$  elements in  $\mathcal{E}$  of relative trace  $k$  for any  $k \in \mathcal{K}$ . This fact is used in the proof of Theorem 4.23, as well as several of the observations preceding Theorem 4.23.

**Lemma 4.13** *There are exactly  $\frac{q-1}{2}$  squares of  $\mathcal{E}$  in every proper coset of  $\mathcal{K}$  in  $\mathcal{E}$ .*

**Proof:** There are  $\frac{q^2-1}{2}$  squares in  $\mathcal{E}^*$  and  $q-1$  squares in  $\mathcal{K}^*$ . So, we have  $\frac{q^2-1}{2} - (q-1) = (q-1)\left(\frac{q-1}{2}\right)$  squares in  $\mathcal{E} \setminus \mathcal{K}$ . We show that there are  $q-1$  additive cosets of  $\mathcal{K}$ , and each coset contains exactly  $\frac{q-1}{2}$  squares in  $\mathcal{E} \setminus \mathcal{K}$ .

Since  $\mathcal{E}$  is a quadratic extension over  $\mathcal{K}$  ( $|\mathcal{E} : \mathcal{K}| = 2$ ), every element  $\eta \in \mathcal{E}$  can be uniquely expressed as an element of the form  $\eta = a\lambda + b$  where  $a, b \in \mathcal{K}$  and  $\lambda$  is a primitive element of  $\mathcal{E}$  over  $\mathcal{K}$ . Consider the additive cosets of  $\mathcal{K}$  distinct from  $\mathcal{K}$ . These cosets are expressible as  $\eta + \mathcal{K}$ . But, as  $\eta = a\lambda + b$ , we have that  $\eta + \mathcal{K}$  is equivalent to the coset  $a\lambda + \mathcal{K}$ , for any  $a \in \mathcal{K}^*$ .

Assume the coset  $\lambda + \mathcal{K}$  has exactly  $x$  squares of  $\mathcal{E} \setminus \mathcal{K}$  in it. When  $a \neq 0$ , each of the cosets  $a(\lambda + \mathcal{K}) \equiv a\lambda + \mathcal{K}$  also contains exactly  $x$  squares of  $\mathcal{E} \setminus \mathcal{K}$ , since  $a$  is a square in  $\mathcal{E}$ . There are  $q-1$  nonzero choices for  $a$ , so we have  $q-1$  cosets of  $\mathcal{K}$ . Now, these  $q-1$  cosets must contain the same number of squares of  $\mathcal{E} \setminus \mathcal{K}$ , therefore,  $x = \frac{q-1}{2}$ . ■

**Observation 4.14** *Let  $Q(x) = x^2 + dx + a$  where  $a, d \in \mathcal{E}$ . If  $Q(x) = Q(y)$  with  $x \neq y$ , then  $x = -d - y$ .*

**Proof:** Suppose  $Q(x) = Q(y)$ . Then  $x^2 + dx + a = y^2 + dy + a \Rightarrow (x^2 - y^2) + d(x - y) = 0$ , and so,  $x = -d - y$ . ■

**Lemma 4.15**  $Q(x) = x^2 + dx + a = \square \in \mathcal{E}^*$  for all  $x \in \mathcal{K}$ , where  $a \neq d^2/4$ , if and only if  $a, d \in \mathcal{K}$ .

**Proof:** Clearly, if  $a$  and  $d$  are in  $\mathcal{K}$ ,  $x^2 + dx + a = \square$  for all valid choices of  $a$  and  $d$ .

Assume  $d \in \mathcal{K}$ . In Observation 4.14, we showed that  $Q(x) = Q(-d - x)$ , so each value  $Q(x)$  appears twice, except for  $Q(\frac{-d}{2})$  which appears only once. This implies that  $Q$  takes on exactly  $\frac{q-1}{2} + 1 = \frac{q+1}{2}$  distinct values. If for some  $x \in \mathcal{K}$ ,  $Q(x) \in \mathcal{K}$ , there exists an  $s \in \mathcal{E}$  such that  $x^2 + dx + a = s^2 \in \mathcal{K}$ . This implies that  $a = s^2 - x^2 - dx \in \mathcal{K}$ , and we are done. Thus, we may assume that none of the values  $Q(x)$  are in  $\mathcal{K}$ .

Observe that  $Q(x_i) - Q(x_j) \in \mathcal{K} \forall i, j$ , since  $(x_i^2 - x_j^2) + d(x_i - x_j) \in \mathcal{K}$ . So, the set of  $Q(x_i)$  is contained in one coset of  $\mathcal{K}$ , that is,  $a + \mathcal{K}$ . By Lemma 4.13, there are only  $\frac{q-1}{2}$  squares in each coset of  $\mathcal{K}$ . Therefore, there are not enough squares in a coset of  $\mathcal{K}$ , for all  $x \in \mathcal{K}$  to yield a square. This contradiction implies that we need only consider the case where  $d \notin \mathcal{K}$ .

Suppose  $a = 0$ . Then,  $Q(0) = 0$  which is not a square in  $\mathcal{E}^*$ . Therefore, for the remainder of the proof, we assume  $a \neq 0$ .

Since  $\mathcal{E}$  is a quadratic extension over  $\mathcal{K}$ , there exists a primitive irreducible polynomial

$$f(x) = x^2 + ex + b$$

with  $e, b \in \mathcal{K}$ , both nonzero, and let  $\lambda$  be a root of this polynomial. That is,  $\lambda$  is a primitive element of  $\mathcal{E}$  over  $\mathcal{K}$ . Then,

$$\begin{aligned} f(\lambda) &= \lambda^2 + e\lambda + b = 0 \\ \Rightarrow \lambda^2 &= -e\lambda - b. \end{aligned}$$

We also have that every element of  $\mathcal{E}$  can be expressed uniquely in the form

$$\omega\lambda + \rho$$

where  $\omega, \rho \in \mathcal{K}$ . Let  $d = \delta\lambda + \beta$ , with  $\delta, \beta \in \mathcal{K}$  and, by assumption,  $\delta \neq 0$ .

Now,  $Q(x) = x^2 + dx + a = (\mu_x\lambda + \nu_x)^2 = (-\mu_x\lambda - \nu_x)^2$  with  $\mu_x, \nu_x \in \mathcal{K}$  and  $\mu_x \neq 0$ . By associating either  $\mu_x$  or  $-\mu_x$  with each  $x \in \mathcal{K}$  we can define a function  $\beta_1 : \mathcal{K} \mapsto \mathcal{K}$ .  $Q$  and  $\beta_1$  implicitly define  $\beta_2 : \mathcal{K} \mapsto \mathcal{K}$ , so that  $Q(x) = x^2 + dx + a = (\beta_1(x)\lambda + \beta_2(x))^2$ . We then have:

$$\begin{aligned} Q(x) = x^2 + dx + a &= x^2 + (\delta\lambda + \beta)x + a \\ &= (\delta x)\lambda + (x^2 + \beta x + a) \\ &= (\beta_1(x)\lambda + \beta_2(x))^2 \\ &= \beta_1^2(x)\lambda^2 + 2\beta_1(x)\beta_2(x)\lambda + \beta_2^2(x) \\ &= \beta_1^2(x)[-e\lambda - b] + 2\beta_1(x)\beta_2(x)\lambda + \beta_2^2(x) \\ &= [2\beta_1(x)\beta_2(x) - e\beta_1^2(x)]\lambda + [\beta_2^2(x) - b\beta_1^2(x)]. \end{aligned}$$

Thus,

$$\delta x = 2\beta_1(x)\beta_2(x) - e\beta_1^2(x) \tag{4.4}$$

and

$$x^2 + \beta x + a = \beta_2^2(x) - b\beta_1^2(x). \tag{4.5}$$

Since every function over a finite field, more specifically  $\mathcal{K}$ , can be represented as a polynomial of degree  $\leq q - 1$ , we can view the functions  $\beta_i(x)$  as polynomials of  $x$ . Moreover, if need be,  $\beta_1(x)$  can be chosen so that  $\deg(\beta_1(x))$  is as small as possible.

Assume that in (4.4)  $\deg(\text{RHS}) \leq q-1$ . This implies that  $\delta x = \beta_1(x)[2\beta_2(x) - e\beta_1(x)]$  in  $\mathcal{K}[x]$ . Now assume that  $\beta_1(x)$  has degree less than or equal to one. If  $\beta_1(x)$  is not constant, then  $2\beta_2(x) - e\beta_1(x)$  must be constant. Thus, since  $\beta_1(x)$  is linear, we see that  $\beta_2(x)$  must also be linear. Let  $\beta_1(x) = Ax + B$  and  $\beta_2(x) = Cx + D$ , with  $A \neq 0$ , so that  $2\beta_2(x) - e\beta_1(x) = k$ , for some constant  $k$ .

$$\begin{aligned} 2(Cx + D) - e(Ax + B) &= k \\ \Rightarrow (2C - eA)x + (2D - eB) &= k \\ \Rightarrow 2C - eA &= 0 \\ \Rightarrow C &= \frac{eA}{2}. \end{aligned}$$

We now have

$$\begin{aligned} x^2 + \beta x + a &= \left(\frac{Ae}{2}x + D\right)^2 - b(Ax + B)^2 \\ &= \left(\frac{A^2e^2}{4} - A^2b\right)x^2 + (ADe - 2ABb)x + (D^2 - bB^2), \end{aligned}$$

implying that

$$\frac{A^2e^2}{4} - A^2b = 1, \beta = ADe - 2ABb, a = D^2 - bB^2.$$

Now,  $\frac{A^2e^2}{4} - A^2b = 1$  implies that

$$\begin{aligned} A^2e^2 - 4A^2b &= 4 \\ \Rightarrow A^2(e^2 - 4b) &= 4 \\ \Rightarrow e^2 - 4b &= \frac{4}{A^2} \\ \Rightarrow e^2 - 4b &= \square. \end{aligned}$$

But,  $f(x) = x^2 + ex + b$  is a monic irreducible polynomial of degree two over  $\mathcal{K}[x]$ . If  $e^2 - 4b = \square$ , then  $f(x)$  factors, a contradiction. Thus,  $\beta_1(x)$  and  $\beta_2(x)$  cannot both be linear functions.

Still under the assumption that  $\deg(\text{RHS}) \leq q - 1$ , if  $\beta_1(x)$  is constant, we see that  $\beta_2(x)$  must be linear. Let  $\beta_1(x) = B$  and  $\beta_2(x) = Cx + D$ . Then

$$\begin{aligned}\delta x &= 2B(Cx + D) - eB^2 \\ &= 2BCx + (2BD - eB^2)\end{aligned}$$

implying that

$$\delta = 2BC. \tag{4.6}$$

Similarly,

$$\begin{aligned}x^2 + \beta x + a &= (Cx + D)^2 - bB^2 \\ &= C^2x^2 + 2CDx + (D^2 - bB^2)\end{aligned}$$

implying that

$$1 = C^2 \tag{4.7}$$

$$\beta = 2CD \tag{4.8}$$

$$a = D^2 - bB^2. \tag{4.9}$$

Now, (4.7)  $\Rightarrow C = \pm 1$ . With  $C = 1$ , (4.6) implies that  $\delta = 2B \Rightarrow B = \frac{\delta}{2}$ . Also, (4.8) implies that  $D = \frac{\beta}{2}$ . Using these relations,

$$\beta_1(x) = B = \frac{\delta}{2} \text{ and } \beta_2(x) = \left(x + \frac{\beta}{2}\right).$$

Thus,

$$\begin{aligned}
x^2 + dx + a &= (\beta_1(x)\lambda + \beta_2(x))^2 \\
&= \left(\frac{\delta}{2}\lambda + \left(\frac{\beta}{2} + x\right)\right)^2 \\
&= \left(\frac{\delta\lambda + \beta}{2} + x\right)^2 \\
&= \left(x + \frac{d}{2}\right)^2 \\
\Rightarrow a &= \frac{d^2}{4}. \rightarrow\leftarrow
\end{aligned}$$

In other words, the conic is degenerate. The same contradiction is obtained when  $C = -1$ . So,  $\beta_1(x)$  cannot be constant.

Assume that  $\deg(\beta_1(x)) \geq 2$ . Since  $\delta x = \beta_1(x)[2\beta_2(x) - e\beta_1(x)]$ , with  $\deg(\beta_1(x)) \geq 2$ , we must have  $[2\beta_2(x) - e\beta_1(x)] = 0$ . But, if  $[2\beta_2(x) - e\beta_1(x)] = 0$ , then necessarily  $\delta = 0$ .  $\rightarrow\leftarrow$

We are now left to consider that (4.4) is an equality in  $\mathcal{K}[x]$  with

$$\delta x^q = \beta_1(x)[(2\beta_2(x) - e\beta_1(x))].$$

This implies that  $\beta_1(x) \mid x^q$ , more precisely  $\beta_1(x) = x^j$  for some  $j \leq q - 1$  and  $x^{q-j} = \frac{1}{\delta}(2\beta_2(x) - e\beta_1(x))$ . Solving explicitly for  $\beta_2(x)$ , we find that  $\beta_2(x) = \frac{\delta x^{q-j} + ex^j}{2}$ . Then from (4.5),

$$\begin{aligned}
x^2 + \beta x + a &= [\beta_2^2(x) - b\beta_1^2(x)] \\
&= \frac{\delta^2}{4}x^{2q-2j} + \frac{e\delta}{2}x^q + \frac{e^2 - 4b}{4}x^{2j}.
\end{aligned}$$

This cannot occur since when  $x = 0$ , this implies  $a = 0$ .  $\rightarrow\leftarrow$  Thus, when  $\delta \neq 0$ , there does not exist a polynomial  $\beta_1(x)$ . Hence,  $\delta = 0$ , that is, the case  $d \notin \mathcal{K}$  does not arise. ■

This lemma also aids in showing that, unlike the situation in planes of even order, the set of lines through a point in a Baer subplane do not form a CBS. The following observations aid in the proof of Theorem 4.23.

**Observation 4.16** *Let  $\alpha$  be a generator of  $\mathcal{E}^*$ . The  $q$  trace 0 elements of  $\mathcal{E}$  are  $\mathcal{N} = \{ \lambda \alpha^{\frac{q+1}{2}} \mid \lambda \in \mathcal{K} \}$ .*

**Proof:** Since  $\lambda \in \mathcal{K}$ ,  $\lambda^q = \lambda$ . Recall that  $\alpha^{(\frac{q+1}{2})q} = \alpha^{\frac{q^2+q}{2}} = \alpha^{\frac{q^2-1+1+q}{2}} = \alpha^{\frac{q^2-1}{2} + \frac{q+1}{2}} = \left( \alpha^{\frac{q^2-1}{2}} \right) \left( \alpha^{\frac{q+1}{2}} \right) = -1 \alpha^{\frac{q+1}{2}}$ , since  $\alpha^{\frac{q^2-1}{2}} = -1$ . Now,  $\text{tr}(\lambda \alpha^{\frac{q+1}{2}}) = \lambda \alpha^{\frac{q+1}{2}} + \lambda^q \alpha^{\frac{q+1}{2}q} = \lambda \alpha^{\frac{q+1}{2}} - \lambda \alpha^{\frac{q+1}{2}} = 0$ . For any  $\lambda \in \mathcal{K}$ , we have that  $\text{tr}(\lambda \alpha^{\frac{q+1}{2}}) = 0$ , and so there are  $q$  elements in  $\mathcal{E}$  of trace 0. By Lemma 4.12, this accounts for all of the trace 0 elements of  $\mathcal{E}$ . ■

**Observation 4.17** *For all  $n \in \mathcal{N}^* = \mathcal{N} \setminus \{0\}$ ,  $n^2$  is a nonsquare within  $\mathcal{K}$ .*

**Proof:** Since  $n \in \mathcal{N}^*$ ,  $n = \lambda \alpha^{\frac{q+1}{2}}$ , for some  $\lambda \in \mathcal{K}^*$ . With  $\lambda \in \mathcal{K}^*$  and  $\alpha$  a generator of  $\mathcal{E}^*$ , we may express  $\lambda$  as  $\alpha^{k(q+1)}$ , for some  $k$ . Now,  $n = \alpha^{k(q+1)} \alpha^{\frac{q+1}{2}} = \alpha^{(2k+1)(q+1)/2}$ , and since  $\alpha^{q+1}$  is a primitive element of  $\mathcal{K}$ , we have that  $n^2 = (\alpha^{q+1})^{2k+1} = \not\in \mathcal{K}$  within  $\mathcal{K}$ . ■

**Observation 4.18** *For all  $n \in \mathcal{N}$ ,  $\lambda, d \in \mathcal{K}$ , and  $k \in \mathcal{F}$ , we have that  $\text{tr}(\lambda n + \frac{d+kn}{2}) = d$ .*

**Proof:** Since  $\frac{d}{2} \in \mathcal{K}$ ,  $(\frac{d}{2})^q = \frac{d}{2}$  and  $\text{tr}(\frac{d}{2}) = \frac{d}{2} + (\frac{d}{2})^q = d$ . Also, as  $\text{tr}(sn) = \text{str}(n) \forall s \in \mathcal{K}$ , we have that  $\text{tr}(\lambda n) = \lambda \text{tr}(n) = 0$  and  $\text{tr}(\frac{kn}{2}) = \frac{k}{2} \text{tr}(n) = 0$ . Hence,  $\text{tr}(\lambda n + \frac{d+kn}{2}) = \text{tr}(\lambda n) + \text{tr}(\frac{d}{2}) + \text{tr}(\frac{kn}{2}) = \text{tr}(\frac{d}{2}) = d$ . ■

**Observation 4.19** For  $q \equiv 1 \pmod{4}$ , all nonzero trace 0 elements are nonsquares in  $\mathcal{E}$ . For  $q \equiv 3 \pmod{4}$ , all nonzero trace 0 elements are squares in  $\mathcal{E}$ .

**Proof:** If  $q = 4m + 1$ , then  $\frac{q+1}{2} = 2m + 1$ , which is odd. Since  $\lambda \in \mathcal{K}^*$ ,  $\lambda$  is a square in  $\mathcal{E}$ . The product of a square ( $\lambda$ ) and a nonsquare ( $\alpha^{\frac{q+1}{2}}$ ) is a nonsquare. Hence, when  $q \equiv 1 \pmod{4}$ , all nonzero trace 0 elements in  $\mathcal{E}$  are nonsquares.

A similar argument gives the desired result for  $q \equiv 3 \pmod{4}$ . ■

**Observation 4.20** For  $q \equiv 1 \pmod{4}$ , there are  $\frac{q+1}{2}$  square elements in  $\mathcal{E}$  of trace  $d$ . For  $q \equiv 3 \pmod{4}$ , there are  $\frac{q-1}{2}$  square elements in  $\mathcal{E}$  of trace  $d$ .

**Proof:** Let  $x$  denote the number of square trace 1 elements in  $\mathcal{E}$ . Then, there are  $x$  square elements in  $\mathcal{E}$  with trace  $k$ ,  $k \in \mathcal{K}^*$ . So, there are  $x(q-1)$  square elements with nonzero trace. Because there are  $\frac{q^2-1}{2}$  nonzero squares in  $\mathcal{E}$ , we have that ( $\#$  of square nonzero trace 0 elements)  $+x(q-1) = \frac{q^2-1}{2}$ .

By Observation 4.19, when  $q \equiv 1 \pmod{4}$ , there are no nonzero square trace 0 elements in  $\mathcal{E}$ , so  $x = \frac{q+1}{2}$ ; and when  $q \equiv 3 \pmod{4}$ , all nonzero trace 0 elements in  $\mathcal{E}$  are squares, giving  $x = \frac{q-1}{2}$ . ■

**Observation 4.21** Let  $\lambda, \lambda', d \in \mathcal{K}$ ,  $k \in \mathcal{F}$ , and  $n \in \mathcal{N}^*$ . Then,  $\lambda n + \frac{d+kn}{2} = \lambda' n + \frac{d-kn}{2}$  only when  $\lambda' = \lambda + k$ .

**Proof:**

$$\begin{aligned} \lambda n + \frac{d+kn}{2} &= \lambda' n + \frac{d-kn}{2} \\ \Leftrightarrow \lambda n + kn &= \lambda' n \\ \Leftrightarrow \lambda + k &= \lambda'. \end{aligned}$$

■

**Observation 4.22** For  $p$  an odd prime,  $p \nmid \frac{p^{m+1}}{2}$  and  $p \nmid \frac{p^m-1}{2}$ ,  $m \geq 1$ .

**Proof:** Trivial. ■

**Theorem 4.23** In  $PG(2, q^2)$ ,  $q = p^h$  an odd prime power, the  $2q - 1$  points on the line  $z = 0$  with parameters that either have trace 0 or are in the subfield  $\mathcal{K}$  form a CBS.

**Proof:**

By Lemma 4.15, the conics that are not blocked by the points with parameters in the subfield are those with coefficients in the subfield. So, assume that  $d, a \in \mathcal{K}$ , with  $a \neq 0$ , and let  $Q(x) = x^2 + dx + a$ .

If  $d^2 - 4a = \square$  within  $\mathcal{K}$ ,  $Q(x)$  factors. That is, if  $d^2 - 4a = s^2$ ,  $s \in \mathcal{K}$ , then  $Q(x) = (x + \frac{d+s}{2})(x + \frac{d-s}{2})$ . Clearly,  $Q$  has roots in  $\mathcal{K}$ , therefore,  $Q$  is blocked by  $\mathcal{K}$ .

If  $d^2 - 4a = 0$ ,  $Q$  is degenerate.

Since the conics with square or zero discriminant are blocked, we need only examine the case where the discriminant is a nonsquare within  $\mathcal{K}$ . Assume  $d^2 - 4a = \not\square$  within  $\mathcal{K}$ . Then, by Observation 4.17, there is some  $n \in N^*$  such that  $n^2 = d^2 - 4a$  and  $Q(x) = (x + \frac{d+n}{2})(x + \frac{d-n}{2})$ .

Define the graph  $G$  by

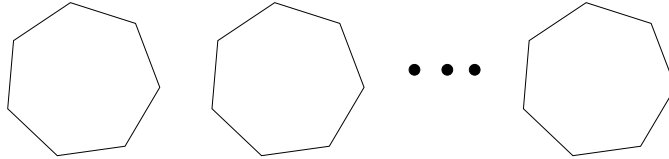
$$V(G) = \{(\lambda, m) \mid \lambda \in \mathcal{K}, m \in \mathcal{F}\},$$

where two vertices  $(\lambda, m)$  and  $(\lambda', m')$  are adjacent if  $\lambda = \lambda'$  and  $\exists k \in \mathcal{F}$  such that  $Q((\lambda + k)) = (\lambda n + \frac{d+mn}{2})(\lambda n + \frac{d-m'n}{2})$ . By Observation 4.21, exactly two values of  $Q$  share a common factor. So,  $G$  must be a regular graph of degree two, and hence, a union of cycles.

Let  $\lambda \in \mathcal{K}$  and  $\lambda n \in \mathcal{N}$ , where  $n$  is fixed in  $\mathcal{N}^*$ . Observe that

$$\begin{aligned} Q((\lambda + 1)n) &= \left(\lambda n + \frac{d+3n}{2}\right) \left(\lambda n + \frac{d+n}{2}\right) \\ Q(\lambda n) &= \left(\lambda n + \frac{d+n}{2}\right) \left(\lambda n + \frac{d-n}{2}\right) \\ Q((\lambda - 1)n) &= \left(\lambda n + \frac{d-n}{2}\right) \left(\lambda n + \frac{d-3n}{2}\right). \end{aligned}$$

More generally, for any  $k$  in the prime subfield  $\mathcal{F} = \text{GF}(p)$ , we have that the value of  $Q((\lambda + k)n)$  is  $\left(\lambda n + \frac{d+(2k+1)n}{2}\right) \left(\lambda n + \frac{d+(2k-1)n}{2}\right)$ . For fixed  $\lambda \in \mathcal{K}$ , we obtain a collection of  $p$  distinct values  $Q((\lambda + k)n)$  such that, by Observation 4.21, exactly two of the values in this collection share a common factor of this form. Moreover, if  $\lambda' \neq \lambda + k$  for some  $\lambda, \lambda' \in \mathcal{K}$  and all  $k \in \mathcal{F}$ , the two values  $Q((\lambda + k)n)$  and  $Q(\lambda'n)$  do not share a common factor. So,  $G$  is a union of  $p^{h-1}$   $p$ -cycles such that every value  $Q(\lambda n)$  for all  $\lambda \in \mathcal{K}$  appears as an edge in some  $p$ -cycle. Figure 4.2 illustrates this idea. Combining Observation 4.18 and



**Figure 4.2:** A Collection of Values  $Q((\lambda + k)n)$

Observation 4.20, we have that all the factors of  $Q$  have the same trace, and we know exactly how many of these factors are squares and nonsquares.

When  $q \equiv 1 \pmod{4}$  (resp.  $3 \pmod{4}$ ),  $\frac{q+1}{2}$  (resp.  $\frac{q-1}{2}$ ) of the factors must be squares in  $\mathcal{E}$ . But, by Observation 4.22, these  $\frac{q+1}{2}$  (resp.  $\frac{q-1}{2}$ ) square factors cannot be distributed over the  $p$ -cycles in such a way that the  $p$ -cycles consist only of squares or nonsquares. Hence, there must exist a  $p$ -cycle in which adjacent vertices

have different squarity, so there exists a value  $Q(\lambda n)$  that is a nonsquare, and  $Q$  is blocked.

Thus, we have that the  $q$  points with parameters in the subfield  $\mathcal{K}$  and the  $q - 1$  points in the set of nonzero trace 0 elements  $\mathcal{N}^*$  form a CBS of size  $2q - 1$  in  $\text{PG}(2, q^2)$ . ■

To illustrate the proof of Theorem 4.23, consider the following example.

**Example 15.**

Let  $q^2 = 81$ , so that  $q = 9$  and  $p = 3$ . For the results given in this example, we will be using the primitive polynomial  $f(x) = x^4 - x^2 - x - 1$  for  $\mathcal{E} = \text{GF}(81)$ . Now,  $\mathcal{K}^* = \{\alpha^{10k} \mid 0 \leq k \leq 8\}$  and  $\mathcal{N} = \{\lambda\alpha^5 \mid \lambda \in \mathcal{K}\}$ . It can be shown that

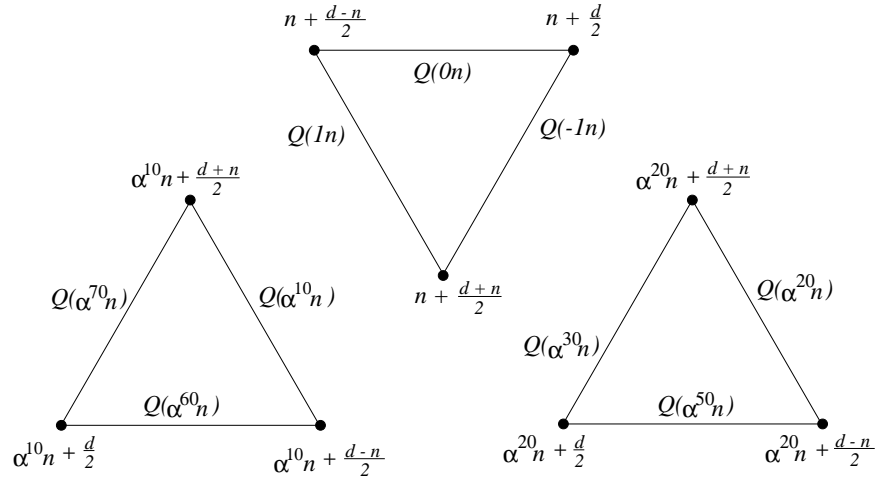
$1 + 1 = -1$	$\alpha^{30} + 1 = \alpha^{50}$	$\alpha^{60} + 1 = \alpha^{10}$
$\alpha^{10} + 1 = \alpha^{70}$	$-1 + 1 = 0$	$\alpha^{70} + 1 = \alpha^{60}$
$\alpha^{20} + 1 = \alpha^{30}$	$\alpha^{50} + 1 = \alpha^{20}$	$0 + 1 = 1$

We illustrate how the conics not blocked by points with subfield parameters are blocked by points with parameters that have relative trace 0. The conics that remain to be blocked by points with parameters that have relative trace 0 are those of the form  $Q(x) = x^2 + dx + a$  where  $d, a \in \mathcal{K}$  and  $d^2 - 4a = n^2$  for some  $n \in \mathcal{N}^*$ . Observe that  $Q((\lambda + k)n) = \left(\lambda n + \frac{d+(2k+1)n}{2}\right) \left(\lambda n + \frac{d+(2k-1)n}{2}\right)$  for any  $\lambda \in \mathcal{K}$  and  $k \in \mathcal{F}$ . We examine the values of  $Q$ .

$$\begin{aligned}
 Q(\alpha^{70}n) &= Q((\alpha^{10} + 1)n) = \left(\alpha^{10}n + \frac{d}{2}\right) \left(\alpha^{10}n + \frac{d+n}{2}\right) \\
 Q(\alpha^{10}n) &= Q((\alpha^{10}n + 0)) = \left(\alpha^{10}n + \frac{d+n}{2}\right) \left(\alpha^{10}n + \frac{d-n}{2}\right) \\
 Q(\alpha^{60}n) &= Q((\alpha^{10} - 1)n) = \left(\alpha^{10}n + \frac{d-n}{2}\right) \left(\alpha^{10}n + \frac{d}{2}\right)
 \end{aligned}$$

$$\begin{aligned}
Q(\alpha^{30}n) &= Q((\alpha^{20} + 1)n) = (\alpha^{20}n + \frac{d}{2})(\alpha^{20}n + \frac{d+n}{2}) \\
Q(\alpha^{20}n) &= Q((\alpha^{20}n + 0)) = (\alpha^{20}n + \frac{d+n}{2})(\alpha^{20}n + \frac{d-n}{2}) \\
Q(\alpha^{50}n) &= Q((\alpha^{20} - 1)n) = (\alpha^{20}n + \frac{d-n}{2})(\alpha^{20}n + \frac{d}{2}) \\
Q(-n) &= Q((1 + 1)n) = (1n + \frac{d}{2})(1n + \frac{d+n}{2}) \\
Q(n) &= Q((1 + 0)n) = (1n + \frac{d+n}{2})(1n + \frac{d-n}{2}) \\
Q(0n) &= Q((1 - 1)n) = (1n + \frac{d-n}{2})(1n + \frac{d}{2}).
\end{aligned}$$

It is easy to see that any given factor appears in exactly two values of  $Q$ . The following union of 3-cycles represents the distribution of the factors of  $Q(\lambda n)$ , as  $\lambda$  varies through  $\mathcal{K}$ .



**Figure 4.3:** The Union of 3-Cycles

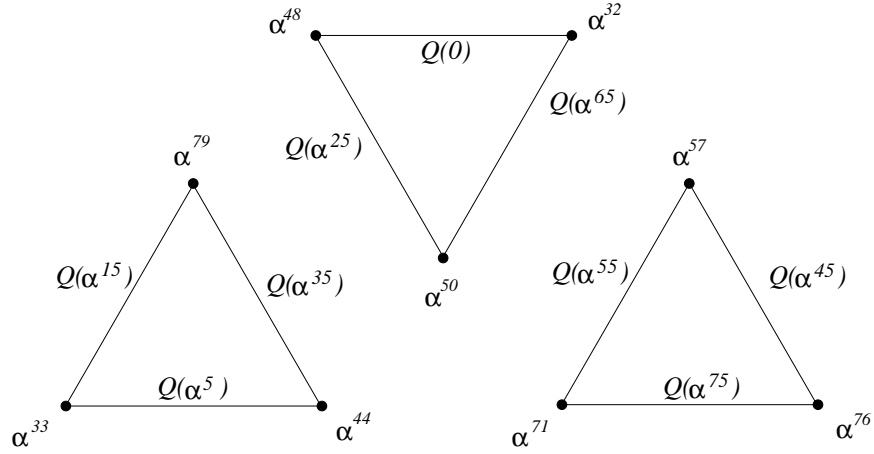
Since  $9 \equiv 1 \pmod{4}$ , five of the factors given as the vertex labels in Figure 4.3 must be squares and the remaining factors must be nonsquares. This implies that there must exist a 3-cycle that contains both squares and nonsquares. So,

there is a  $\lambda \in \mathcal{K}$  such that  $Q(\lambda n) = \square$ , and we have that these conics, which are not blocked by points with subfield parameters, are blocked by points with trace 0 parameters.

For instance, consider the specific conic  $Q(x) = x^2 + \alpha^{10}x + 1$  whose discriminant,  $\alpha^{20} - 1 = \alpha^{50} = (\alpha^{25})^2$ , is a nonsquare with  $\mathcal{K}$  and is an element of  $\mathcal{N}$ . With  $n = \alpha^{25}$ , we can factor  $Q$  so that  $Q(x) = \left(x + \frac{\alpha^{10} + \alpha^{25}}{2}\right) \left(x + \frac{\alpha^{10} - \alpha^{25}}{2}\right) = (x + \alpha^{48})(x + \alpha^{32})$ . We have that the values of  $Q$  are

$$\begin{aligned}
Q(\alpha^{70}\alpha^{25}) = Q(\alpha^{15}) &= (\alpha^{15} + \alpha^{48})(\alpha^{15} + \alpha^{32}) = \alpha^{33} * \alpha^{79} = \alpha^{32} = \square \\
Q(\alpha^{10}\alpha^{25}) = Q(\alpha^{35}) &= (\alpha^{35} + \alpha^{48})(\alpha^{35} + \alpha^{32}) = \alpha^{79} * \alpha^{44} = \alpha^{43} = \square \\
Q(\alpha^{60}\alpha^{25}) = Q(\alpha^5) &= (\alpha^5 + \alpha^{48})(\alpha^5 + \alpha^{32}) = \alpha^{44} * \alpha^{33} = \alpha^{77} = \square \\
Q(\alpha^{30}\alpha^{25}) = Q(\alpha^{55}) &= (\alpha^{55} + \alpha^{48})(\alpha^{55} + \alpha^{32}) = \alpha^{71} * \alpha^{57} = \alpha^{48} = \square \\
Q(\alpha^{20}\alpha^{25}) = Q(\alpha^{45}) &= (\alpha^{45} + \alpha^{48})(\alpha^{45} + \alpha^{32}) = \alpha^{57} * \alpha^{76} = \alpha^{53} = \square \\
Q(\alpha^{50}\alpha^{25}) = Q(\alpha^{75}) &= (\alpha^{75} + \alpha^{48})(\alpha^{75} + \alpha^{32}) = \alpha^{76} * \alpha^{71} = \alpha^{67} = \square \\
Q(\alpha^{40}\alpha^{25}) = Q(\alpha^{65}) &= (\alpha^{65} + \alpha^{48})(\alpha^{65} + \alpha^{32}) = \alpha^{32} * \alpha^{50} = \alpha^2 = \square \\
Q(\alpha^0\alpha^{25}) = Q(\alpha^{25}) &= (\alpha^{25} + \alpha^{48})(\alpha^{25} + \alpha^{32}) = \alpha^{50} * \alpha^{48} = \alpha^{18} = \square \\
Q(0) = Q(0) &= (\alpha^{48})(\alpha^{32}) = \alpha^{48} * \alpha^{32} = 1 = \square.
\end{aligned}$$

Figure 4.4 represents the graph of the factors of  $Q$  over  $\mathcal{N}$ .



**Figure 4.4:** The 3-Cycles for  $Q(x) = x^2 + \alpha^{10}x + 1$

For this choice of conic, we see that there are two 3-cycles that hold a combination of squares and nonsquares. More importantly, we see that  $Q(\alpha^{35})$ ,  $Q(\alpha^5)$ ,  $Q(\alpha^{45})$ , and  $Q(\alpha^{75})$  are all nonsquares. This conic is clearly blocked by four elements of  $\mathcal{N}$ . ■

#### 4.5 Bounds on the Sizes of Minimum Conic Blocking Sets

In this section, bounds are given for the size of a minimum conic blocking set in  $\text{PG}(2, q)$ . For the purposes of obtaining these bounds, we use the restricted-dual model developed in Section 4.3.1. We also assume that the points identified with parameters 0, 1, and  $\infty$  are in the CBS. We begin by examining the upper bound for minimum CBSs.

Based on [24, Thm.67], the following table gives the counts on the number of nonsquares (nonzero squares) in a finite field, which when subtracted from the

$q \equiv 3 \pmod{4}$		$q \equiv 1 \pmod{4}$	
$1 - \not\equiv$		$1 - \square$	
$\frac{q-3}{4}$	$\frac{q-3}{4}$	$\frac{q-1}{4}$	$\frac{q-5}{4}$
$\frac{q+1}{4}$	$\frac{q-3}{4}$	$\frac{q-1}{4}$	$\frac{q-1}{4}$
$\square$		$\square$	
$\not\equiv$		$\not\equiv$	

**Table 4.14:** Squarity Subtraction Tables

element 1 give a square (nonzero) or nonsquare.

**Lemma 4.24** *There are  $\left(\frac{q-3}{2}\right)^2$  nondegenerate quadrics of the form  $Q(x) = x^2 + dx + a$  with the properties*

1.  $Q(0) = a = \square \neq 0$ , and
2.  $Q(1) = 1 + d + a = \square \neq 0$ .

*Of these,  $\frac{(q-3)(q-5)}{8}$  are reducible and  $\frac{(q-3)(q-1)}{8}$  are irreducible.*

**Proof:** There are  $\frac{q-1}{2}$  nonzero choices for  $a$ . For a fixed  $a$ , as  $d$  varies through the field,  $d + a$  also varies. So, there are  $\frac{q-1}{2}$   $(d + a)$ 's that are  $\square$ 's such that  $1 + d + a = \square \neq 0$ . When  $d = \pm 2\sqrt{a}$ , we have that  $1 + d + a = (1 \pm \sqrt{a})^2$ , and when  $a = 1$  and  $d = -2$ , we have  $(1 - \sqrt{1})^2 = 0$ . Although the choices of  $d = \pm 2\sqrt{a}$  satisfy  $1 + d + a = \square \neq 0$  for  $a \neq 1$ , these choices of  $d$  yield a degenerate quadric. Thus, these choices are removed from the count of the eligible ones. This leaves  $\frac{q-1}{2} - 2 = \frac{q-5}{2}$  possible choices for  $d$  for each  $a$ . When  $a = 1$  and  $d = -2$ ,  $Q$  is a degenerate quadric and  $1 + d + a = 0$ . This choice of  $a$  and  $d$  was subtracted twice, and hence, we must add one back in. There are  $\frac{q-1}{2}$  choices for  $a$  and  $\frac{q-5}{2}$

choices for  $d$ , and so there are

$$\left(\frac{q-1}{2}\right)\left(\frac{q-5}{2}\right)+1=\left(\frac{q-3}{2}\right)^2$$

quadratic forms with the specified properties.

If  $x^2 + dx + a$  is reducible, then we may write this quadric as

$$\begin{aligned}x^2 + dx + a &= (x - \beta)(x - \alpha) \\ &= x^2 - (\alpha + \beta)x + \alpha\beta,\end{aligned}$$

for some  $\alpha, \beta \in \mathcal{E}$ , with  $\alpha \neq \beta$ . To count the number of reducible quadrics, we determine how many  $\alpha$ 's and  $\beta$ 's satisfy  $\alpha\beta = \square$ ,  $1 - (\alpha + \beta) + \alpha\beta = \square$ , and  $(\alpha - \beta)^2 \neq 0$ . As we want to count the number of quadrics such that  $Q(1) = (1 - \alpha)(1 - \beta) = \square$ , we must consider two cases. The first case is when  $(1 - \alpha)$  and  $(1 - \beta)$  are both squares and the second case is when  $(1 - \alpha)$  and  $(1 - \beta)$  are both nonsquares. To complete this count, consider the cases of  $q \equiv \pm 1 \pmod{4}$  separately.

#### Case $q \equiv 3 \pmod{4}$

Suppose  $\alpha = \square$ . Then by Table 4.14, there are  $\frac{q-3}{4}$  choices for  $\alpha$  such that  $1 - \alpha = \square \neq 0$ , and so, there are  $\frac{q-3}{4} - 1 = \frac{q-7}{4}$  choices for  $\beta$  such that  $1 - \beta = \square \neq 0$ . Similarly, there are  $\frac{q-3}{4}$  choices for  $\alpha$  such that  $1 - \alpha = \not\square$ , and so, there are  $\frac{q-3}{4} - 1 = \frac{q-7}{4}$  choices for  $\beta$  such that  $1 - \beta = \not\square$ .

Now, suppose  $\alpha = \not\square$ . Then by Table 4.14, there are  $\frac{q-3}{4}$  choices for  $\alpha$  such that  $1 - \alpha = \square \neq 0$ , and so, there are  $\frac{q-3}{4} - 1 = \frac{q-7}{4}$  choices for  $\beta$  such that  $1 - \beta = \square \neq 0$ . Similarly, there are  $\frac{q+1}{4}$  choices for  $\alpha$  such that  $1 - \alpha = \not\square$ , and so, there are  $\frac{q+1}{4} - 1 = \frac{q-3}{4}$  choices for  $\beta$  such that  $1 - \beta = \not\square$ .

So, when  $q \equiv 3 \pmod{4}$ , we have  $\frac{1}{2} \left[ 3 \binom{q-3}{4} \binom{q-7}{4} + \binom{q+1}{4} \binom{q-3}{4} \right] = \frac{(q-3)(q-5)}{8}$  and there are  $\frac{(q-3)(q-5)}{8}$  reducible quadrics.

**Case  $q \equiv 1 \pmod{4}$**

Suppose  $\alpha = \square$ . Then by Table 4.14, there are  $\frac{q-5}{4}$  choices for  $\alpha$  such that  $1-\alpha = \square \neq 0$ , and so, there are  $\frac{q-5}{4}-1 = \frac{q-9}{4}$  choices for  $\beta$  such that  $1-\beta = \square \neq 0$ . Similarly, there are  $\frac{q-1}{4}$  choices for  $\alpha$  such that  $1-\alpha = \emptyset$ , and so, there are  $\frac{q-1}{4}-1 = \frac{q-5}{4}$  choices for  $\beta$  such that  $1-\beta = \emptyset$ .

Suppose  $\alpha = \emptyset$ . Then by Table 4.14, there are  $\frac{q-1}{4}$  choices for  $\alpha$  such that  $1-\alpha = \square \neq 0$ , and so, there are  $\frac{q-1}{4}-1 = \frac{q-5}{4}$  choices for  $\beta$  such that  $1-\beta = \square \neq 0$ . Similarly, there are  $\frac{q-1}{4}$  choices for  $\alpha$  such that  $1-\alpha = \emptyset$ , and so, there are  $\frac{q-1}{4}-1 = \frac{q-5}{4}$  choices for  $\beta$  such that  $1-\beta = \emptyset$ .

So, when  $q \equiv 1 \pmod{4}$ , we have  $\frac{1}{2} \left[ 3 \binom{q-1}{4} \binom{q-5}{4} + \binom{q-5}{4} \binom{q-9}{4} \right] = \frac{(q-3)(q-5)}{8}$ , and so, there are  $\frac{(q-3)(q-5)}{8}$  reducible quadrics.

Hence, the number of reducible quadrics with the specified properties is  $\frac{(q-3)(q-5)}{8}$ . Subtracting this from the total number of quadrics with the specified properties gives  $\frac{(q-3)(q-1)}{8}$  irreducible quadrics. ■

**Theorem 4.25** *If  $\mathcal{B}$  is a minimum CBS in  $PG(2, q)$ ,  $q$  odd, then  $|\mathcal{B}| \leq 2 \log_2(q-5) + 1$ .*

**Proof:** We obtain an upper bound for the size of a minimum CBS by comparing the total number of  $k$ -sets in a pencil with the appropriate number of quadrics, of the form described in Lemma 4.24.

Let  $Q(x) = x^2 + dx + a$  and note that  $Q(s) = Q(-d - s)$ . Now,  $Q(\frac{-d}{2}) = (-1)^{\frac{1}{4}}(d^2 - 4a) = \square$  when  $-1 = \not\square$  and  $d^2 - 4a = \not\square$ , and also when  $-1 = \square$  and  $d^2 - 4a = \square$ . So, every value  $Q(x)$  appears twice, with the exception of  $Q(\frac{-d}{2})$  which appears only once.

For  $q \equiv 3 \pmod{4}$ ,  $Q(\frac{-d}{2}) = \square$  when  $Q$  is irreducible. Thus, the irreducible quadrics will always yield an odd number of squares. Since  $\frac{q-1}{2}$  is odd, there will be  $\frac{q-1}{2}$  squares for the irreducible quadrics and  $\frac{q+1}{2}$  squares for the reducible quadrics.

For  $q \equiv 1 \pmod{4}$ ,  $Q(\frac{-d}{2}) = \square$  when  $Q$  is reducible. Thus, the reducible quadrics will always yield an odd number of squares. Since  $\frac{q+1}{2}$  is odd, there will be  $\frac{q+1}{2}$  squares for the reducibles and  $\frac{q-1}{2}$  squares for the irreducibles.

If  $Q$  is irreducible, then there are  $\frac{q-1}{2}$  elements  $x \in \text{GF}(q)$  that give a square value for  $Q(x)$ . Since these  $\frac{q-1}{2}$  elements include 0 and 1, we have  $\frac{q-1}{2} - 2 = \frac{q-5}{2}$  elements in  $\text{GF}(q) \setminus \{0, 1\}$  such that  $Q(x) = \square$ .

If  $Q$  is reducible, then there are  $\frac{q+1}{2}$  elements  $x \in \text{GF}(q)$  that give a square value for  $Q(x)$ . Since these  $\frac{q+1}{2}$  elements include 0, 1, and the two roots of  $Q$ , we have  $\frac{q+1}{2} - 4 = \frac{q-7}{2}$  elements in  $\text{GF}(q) \setminus \{0, 1, \frac{-d \pm \sqrt{d^2 - 4a}}{2a}\}$  such that  $Q(x) = \square$ .

There are  $\binom{q-2}{k}$  sets of size  $k$  of elements of  $\text{GF}(q)$  that do not include 0 and 1. As there are  $\frac{(q-3)(q-1)}{8}$  irreducible quadrics and  $\frac{(q-3)(q-5)}{8}$  reducible quadrics, we have that there are  $\binom{\frac{q-1}{2}-2}{k} \frac{(q-3)(q-1)}{8} + \binom{\frac{q+1}{2}-4}{k} \frac{(q-3)(q-5)}{8}$   $k$ -sets of points contained in nondegenerate quadrics which give only squares in the image of the quadrics. That is, for which  $Q(x) = \square$  for all  $x$  in the set of  $k$  points. As long as,

$$\binom{q-2}{k} > \binom{\frac{q-5}{2}}{k} \frac{(q-3)(q-1)}{8} + \binom{\frac{q-7}{2}}{k} \frac{(q-3)(q-5)}{8},$$

there must be a CBS of size  $k+3$  (which includes  $0, 1, \infty$ ). In other words, if there are more sets on the left, then some set of size  $k+3$  cannot give all squares for any of the conics and therefore is a CBS. Now, suppose  $k+3 > 2\log_2(q-5) + 1$ , then we have that

$$\begin{aligned} k+2 &> 2\log_2(q-5) \\ \Rightarrow 2^{k+2} &> (q-5)^2 \\ \Rightarrow 2^k &> \frac{1}{2^2}(q-3)(q-5). \end{aligned}$$

Since  $q-k > \frac{q-(2k+3)}{2}$  for all  $k > 0$ , (or equivalently  $2(q-k) > q-(2k+3)$  for all  $k > 0$ ), we have

$$\begin{aligned} 2^k(q-2)(q-3)\cdots((q-2)-(k-1)) &> \binom{q-3}{2} \binom{q-5}{2} (q-7)\cdots \\ &\quad (q-3-2k)(q-3-k) \\ \Rightarrow (q-2)(q-3)\cdots((q-2)-(k-1)) &> \binom{q-3}{2} \binom{q-5}{2} \binom{q-7}{2} \cdots \\ &\quad \binom{q-3-2k}{2} \binom{q-3-k}{2} \\ \Rightarrow \binom{q-2}{k} &> \binom{q-3}{4} (q-3-k) \binom{q-5}{k} \\ &= \binom{q-5}{k} \frac{(q-3)(q-1)}{8} \\ &\quad + \binom{q-7}{k} \frac{(q-3)(q-5)}{8}. \end{aligned}$$

So,  $\binom{q-2}{k} > \binom{q-5}{k} \frac{(q-3)(q-1)}{8} + \binom{q-7}{k} \frac{(q-3)(q-5)}{8}$  when  $k+3 > 2\log_2(q-5) + 1$ .

Thus,  $|\mathcal{B}| \leq 2\log_2(q-5) + 1$ . ■

The following theorem is obtained from Theorem 2.2.

**Theorem 4.26** *If  $S$  denotes the number of nonsquares  $n$  in  $\mathcal{E}$  for which  $n+1 = \square$*

and  $N$  denotes the number of nonsquares  $m$  for which  $m + 1 = \square$ , we have

$$S = \frac{1}{4}(p^n - 1), N = \frac{1}{4}(p^n - 5), \text{ if } -1 = \square;$$

$$S = \frac{1}{4}(p^n + 1), N = \frac{1}{4}(p^n - 3), \text{ if } -1 = \not\square.$$

**Theorem 4.27** *If  $\mathcal{B}$  is a minimum CBS in  $PG(2, q)$ ,  $q \geq 9$ , then  $|\mathcal{B}| \geq 5$ .*

**Proof:** Let  $Q(x) = x^2 + dx + a$  be defined as in Lemma 4.24. Since  $0, 1$ , and  $\infty$  are already in the CBS, we have that  $a = \square \neq 0$  and  $1 + d + a = \square \neq 0$ . Suppose that  $\mathcal{B} = \{0, 1, \infty, t\}$  is a CBS in  $PG(2, q)$ .

Let  $d = -t$  so that  $Q_t(x) = x^2 - tx + a$ . Now,

$$Q_t(0) = a$$

$$Q_t(1) = 1 - t + a$$

$$Q_t(t) = t^2 - t^2 + a = a.$$

For every fixed  $t \neq 0, 1$ , we exhibit an  $a$  such that  $Q_t(1) = \square$ . Then, for this value of  $t$ , we find a nondegenerate quadric that is not blocked by  $\mathcal{B}$ .

Assume  $q \equiv 3 \pmod{4}$ .

Suppose  $t$  is such that  $1 - t = \square$ . By Theorem 2.2, there are  $\frac{q-3}{4}$  nonzero square values  $\sigma^2$  for which  $\sigma^2 + 1 = \square$ . Let  $a = \frac{1-t}{\sigma^2}$  so that  $\sigma^2 = \frac{1-t}{a}$ . Then,  $1 + \sigma^2 = 1 + \frac{1-t}{a} = \square$  implying that  $Q_t(1) = \square$ .

Suppose  $t$  is such that  $1 - t = \not\square$ . By Theorem 4.26, there are  $\frac{q+1}{4}$  nonsquare values  $n$  for which  $n + 1 = \square$ . Let  $a = \frac{1-t}{n}$  so that  $n = \frac{1-t}{a}$ . Then,  $1 + n = 1 + \frac{1-t}{a} = \square$  implying that  $Q_t(1) = \square$ .

Assume  $q \equiv 1 \pmod{4}$ .

Suppose  $t$  is such that  $1 - t = \square$ . By Theorem 2.2, there are  $\frac{q-5}{4}$  nonzero square values  $\sigma^2$  for which  $\sigma^2 + 1 = \square$ . Let  $a = \frac{1-t}{\sigma^2}$  so that  $\sigma^2 = \frac{1-t}{a}$ . Then,

$1 + \sigma^2 = 1 + \frac{1-t}{a} = \square$  implying that  $Q_t(1) = \square$ .

Suppose  $t$  is such that  $1 - t = \not\square$ . By Theorem 4.26, there are  $\frac{q-1}{4}$  nonsquare values  $n$  for which  $n + 1 = \square$ . Let  $a = \frac{1-t}{n}$  so that  $n = \frac{1-t}{a}$ . Then,  $1 + n = 1 + \frac{1-t}{a} = \square$  implying that  $Q_t(1) = \square$ .

So, for every choice of  $t \in \text{GF}(q) \setminus \{0, 1\}$ , there exists a nondegenerate quadric that is not blocked by the set  $\mathcal{B}$ . Hence, for  $q \geq 9$  any CBS in  $\text{PG}(2, q)$  of minimum size must consist of at least five points.  $\blacksquare$

Note that in the previous theorem, the case of  $q = 7$  was excluded. If  $q = 7$ ,  $q \equiv 3 \pmod{4}$  and  $\frac{7-3}{4} = 1$ . In  $\text{GF}(7)$ , 1 is the only square such that  $1 + 1 = \square$ . Then,  $a = 1 - t$  must be a square, and the only choices for  $t$  that satisfy this condition are  $t = 2, 4, 6$ . These choices for  $t$  give rise to the following quadrics:  $x^2 - 2x + 1$ ,  $x^2 - 4x + 4$ ,  $x^2 - 6x + 2$ ; all of which are degenerate. Hence, when  $q \equiv 3 \pmod{4}$ ,  $q$  must be greater than 7 in order for there to exist a nondegenerate conic that is not blocked by  $\mathcal{B}$ .

This bound, although it is low, is in fact, an improvement over several variations of the bound given by counting intersections of lines with conics in the plane. We give one of these variations now.

Let  $\pi$  be a projective plane of order  $q$ . Let  $S$  be a set of concurrent lines, at the point  $\mathcal{O}$ , with the property that all conics in  $\pi$  meet  $S$ . Assume  $|S| = q - \lambda$  and  $\lambda \geq 0$ .

Let  $x_i$ ,  $1 \leq i \leq q - \lambda$ , denote the number of conics of  $\pi$  meeting  $S$  in exactly  $i$  lines. For these counts, we will not include conics that contain the point  $\mathcal{O}$ . Then

$$\sum_{i=1}^{q-\lambda} x_i = q^5 - q^4. \quad (4.10)$$

Next, we count incidences of a line in  $S$  with the conics and then with pairs of lines in  $S$ .

- $|\{(Q, l) \mid l \in S, Q \cap l \neq \emptyset\}|$ 
  - For a (fixed) line  $l \in S$ ,  $l$  has  $\frac{q^5 - q^3}{2}$  conics on it and there are  $q - \lambda$  lines in  $S$ .
  - For a conic  $Q$ ,  $Q$  meets  $x_i$  lines. There are  $i$  ways to pick one of these lines. Summing gives

$$\sum_{i=1}^{q-\lambda} i x_i = (q - \lambda) \left[ \frac{q^5 - q^3}{2} \right]. \quad (4.11)$$

- $|\{(l_1, l_2, Q) \mid l_1, l_2 \in S, l_1 \neq l_2, Q \cap l_1 \neq \emptyset, Q \cap l_2 \neq \emptyset\}|$ 
  - For a pair of lines in  $S$ , there are  $\frac{q^5 + q^3 - 2q^2}{4}$  conics that meet both lines of this pair. There are  $\binom{q-\lambda}{2}$  ways of picking two lines of  $S$  to meet  $Q$ .
  - For a given conic  $Q$ , it lies on  $i$  lines of  $S$ . There are  $\binom{i}{2}$  ways of picking two lines of  $S$ . Summing gives

$$\sum_{i=1}^{q-\lambda} i(i-1)x_i = (q - \lambda)(q - \lambda - 1) \left[ \frac{q^5 + q^3 - 2q^2}{4} \right]. \quad (4.12)$$

Consider the sum

$$(\lambda - q) \cdot (4.10) + (q - \lambda) \cdot (4.11) - (4.12).$$

Then we have that

$$\begin{aligned} \sum_{i=1}^{q-\lambda} (q - \lambda - i)(i - 1)x_i &= (\lambda - q)(q^5 - q^4) \frac{q^5 + q^3 - 2q^2}{4} + (q - \lambda)^2 \frac{q^5 - q^3}{2} \\ &\quad - (q - \lambda)(q - 1 - \lambda) \frac{q^5 + q^3 - 2q^2}{4}. \end{aligned} \quad (4.13)$$

Since the LHS is non-negative, the RHS must also be non-negative. This implies that

$$(\lambda - q) \left( \lambda - \frac{q^2 - q - 2}{q + 2} \right) \geq 0.$$

Hence,  $\lambda < q$  and  $\lambda \leq \frac{q^2 - q - 2}{q + 2}$ . This implies that  $|S| \geq q - \frac{q^2 - q - 2}{q + 2} = \frac{3q + 2}{q + 2}$ . That is,  $|S| \geq 3$ .

This approach gives a lower bound of three on the size of a minimum CBS for all  $q$ . By modifying  $|S|$ , the overall argument is the same, as well as the result. This same type of counting technique was applied to the dual model, which also gave a bound of three. It is possible that by adding additional constraints to the count, a bound better than three can be obtained.

Since the problem of finding minimum CBSs tends to be naturally related to set covering problems (SCPs), we tried several approaches from an optimization viewpoint. Working with the array  $A$ , given in Sections 4.3 and 3.4, containing the set covering information, we explored finding a bound by using a lazy greedy set covering approach. That is, we determined the maximum number of rows covered by the selection of a column and calculated the minimum number of columns necessary to cover all rows. This approach did not yield results any better than those given in the previous counting argument.

During this process of exploring a greedy approach to finding a minimum, we observed that often a greedy covering would give the minimum CBS sizes (as found by Cplex). For combinatorial optimization, a matroid is a problem structure where the greedy algorithm gives an optimal answer [32]. But, NP-hard problems, like the set covering problem, cannot have matroidal structure. So, this approach to finding a lower bound will not produce a result.

The SCP is notoriously hard to solve and is, in fact, NP-complete ([46], [49], [41], [27], [19]). Because the SCP is NP-hard, much research has been devoted to developing good heuristic algorithms that give close approximation to the optimum. In [19], Chvátal found the tight worst case bound of the greedy heuristic commonly considered in the set covering literature. The worst case behavior of the greedy heuristic for the (unweighted) SCP was shown by Johnson [41] and Lovász [49] to be given by the relation

$$\frac{z_G}{z_F} \leq H(d) \quad (< 1 + \ln d), \quad (4.14)$$

where  $z_G$  is the value of a greedy cover,  $z_F$  is the value of a fractional cover,  $d$  is the largest column sum of the 0-1 matrix  $A$ , and  $H(d) = \sum_{j=1}^d 1/j$ . Chvátal [19] has shown that the worst case bound given by (4.14) is also valid for the greedy heuristic when applied to the weighted SCP with arbitrary, but positive, cost coefficients. Ho [37] has shown that the bound on the ratio  $\frac{Z_h}{Z_o}$ , where  $Z_h$  and  $Z_o$  are the values of the heuristic and optimal solutions respectively, is also  $H(d)$  for a more general setting of SCP's. In terms of the minimum CBS problem,  $d$  is the largest number of conics blocked by a line. Since the number of conics blocked by a line is  $\frac{q^5+2q^4-q^3-2q^2}{2}$ , this ratio gives

$$|\mathcal{B}| > \frac{z_G}{1 + \ln \left( \frac{q^5+2q^4-q^3-2q^2}{2} \right)},$$

where  $z_G$  is the solution to the problem given by the greedy algorithm. This bound is not practical for us, since it relies on finding a greedy solution before we can calculate the bound.

## 4.6 Chapter Summary

As in Chapter 3, we have produced CBSs using the trace function and the method used to generate these CBSs can be applied to any additive function in place of the trace function. Since nonlinear Knuth-Kantor flocks exist when the characteristic is odd, the trace-flock construction did not yield CBSs in  $\text{PG}(2, q^2)$ . To compensate for the KK-flocks, a CBS for  $\text{PG}(2, q^2)$  was developed from one of the models used to search for minimum CBSs. Table 4.16 illustrates the sizes of the CBSs obtained from the constructions described in this chapter.

$q$	Trivial	Trace-Flock	Subfield-Trace 0
$p$	$(p + 3)/2$		
$p^2$	$(p^2 + 3)/2$		$2p - 1$
$p^3$	$(p^3 + 3)/2$	$p^2 + 1$	
$p^4$	$(p^4 + 3)/2$	$p^3 + 1$	$2p^2 - 1$
$p^5$	$(p^5 + 3)/2$	$p^4 + 1$	
$p^6$	$(p^6 + 3)/2$	$p^5 + 1, p^4 + 1$	$2p^3 - 1$
$p^7$	$(p^7 + 3)/2$	$p^6 + 1$	
$p^8$	$(p^8 + 3)/2$	$p^7 + 1, p^6 + 1$	$2p^4 - 1$
$p^9$	$(p^9 + 3)/2$	$p^8 + 1, p^6 + 1$	
$p^{10}$	$(p^{10} + 3)/2$	$p^9 + 1, p^8 + 1$	$2p^5 - 1$

**Table 4.16:** Construction Sizes

We developed two models to aid in the search for minimum CBSs. One of these models is directly related to the model developed for planes of even order.

Due to computer, software, and time limitations, we were only able to perform a complete search for minimum CBSs for  $q \leq 113$  and  $q = 125$ . Table 4.17 illustrates the orders of the planes and the sizes ( $m$ ) of the minimum CBSs in those planes.

$m =$  size of minimum CBS in  $\text{PG}(2, q)$

$q$	$m$	$q$	$m$	$q$	$m$	$q$	$m$	$q$	$m$	$q$	$m$	$q$	$m$
3	3	13	6	27	8	43	8	61	9	81	10	103	10
5	4	17	6	29	8	47	8	67	9	83	10	107	10
7	4	19	6	31	8	49	9	71	9	89	10	109	10
9	5	23	7	37	8	53	9	73	9	97	10	113	10
11	6	25	8	41	8	59	9	79	8	101	10	125	11

**Table 4.17:** Minimum Values and Bounds on Minimum Values

To obtain small CBSs for  $q > 113$ , we used either an ad-hoc method of selecting potential CBSs and checking or we employed a greedy-based algorithm to search for small CBSs. Table 4.18 contains the sizes of the smallest CBSs found by one of these methods.

$s =$  size of the smallest CBS found in  $\text{PG}(2, q)$

$q$	$s$	$q$	$s$	$q$	$s$	$q$	$s$	$q$	$s$	$q$	$s$
121	11	137	12	151	12	167	12	179	12	193	12
127	11	139	11	157	12	169	12	181	12	197	12
131	11	149	12	163	12	173	12	191	12	199	12

**Table 4.18:** Bounds on Minimum Values

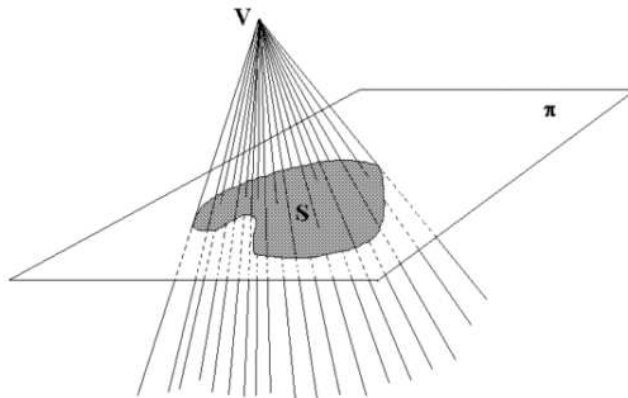
## 5. Conic Blocking Sets and Flocks

All work presented in this chapter as an application of conic blocking sets is found in [18] unless otherwise denoted.

### 5.1 General Terminology and Background Material

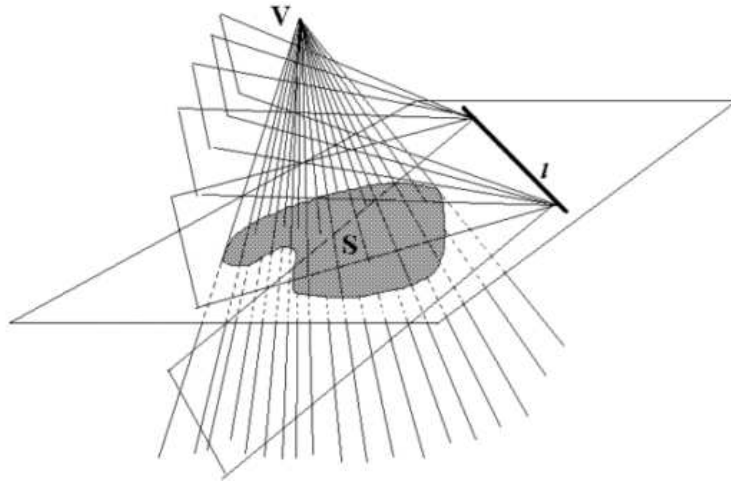
In Section 2.2.3, flocks of quadratic cones were introduced. We begin this section by defining a flock in terms of an arbitrary cone. The definition of flock for the results presented in this chapter is consistent with that given in Section 2.2.3, but we define the cone of the flock in a more general setting.

Let  $\pi$  be a projective plane which is embedded in  $\text{PG}(3, q)$ . Let  $S$  be an arbitrary set of points in  $\pi$  and  $V$  be a point of  $\text{PG}(3, q) \setminus \pi$ . The *cone*, denoted  $C = C(V, S)$ , with *vertex*  $V$  and *carrier*  $S$  is the union of the points on the lines joining  $V$  to the points of  $S$ . We call  $\pi$  the *carrier plane* of the cone  $C$ , and the lines joining  $V$  to  $S$  the *generator lines* of the cone.



**Figure 5.1:** An Arbitrary Cone

A *flock*  $F$  of a cone  $C$  is a set of  $q$  planes which do not contain  $V$  such that no two planes of  $F$  meet at a point of  $C$ . The intersections of the planes of the flock with the cone partition the points of the cone except for the vertex  $V$ . Given a cone  $C(V, S)$  and line  $l$  of  $\text{PG}(3, q)$  which does not intersect  $C(V, S)$ , the  $q$  planes which pass through  $l$  and do not contain the point  $V$  form a *linear flock* of  $C(V, S)$ . Note that both of these definitions are consistent with those given in Section 2.2.3.



**Figure 5.2:** Linear Flock

There are cones which admit only linear flocks. For example,

**Proposition 5.1** [18] *A flock of any cone in  $\text{PG}(3, 2)$  which has a flock, is linear.*

**Proof:** A flock of a cone in  $\text{PG}(3, 2)$  consists of just two planes. As these two planes must meet in a line which does not intersect the cone, the flock is a linear flock. ■

Flocks that are not linear are called *nonlinear flocks*, and the results given in this chapter are concentrated on nonlinear flocks. We introduce coordinates and certain normalizations in order to simplify notation in the following sections.

Let  $C = C(V, S)$  be a cone in  $\text{PG}(3, q)$  with a flock  $F$ . We will assume that one of the planes of  $F$ , denoted  $\pi_0$ , is chosen as the carrier plane of the cone. In other words,  $S$  is contained in  $\pi_0$ . We can introduce projective coordinates,  $(x, y, z, w)$ , in  $\text{PG}(3, q)$  so that  $V$  has coordinates  $(0, 0, 0, 1)$  and the plane  $\pi_0$  has equation  $W = 0$ . Furthermore, if the points of  $S$  are not all collinear, then we can, without loss of generality, assume that  $S$  contains the points  $A = (1, 0, 0, 0)$ ,  $B = (0, 1, 0, 0)$ , and  $C = (0, 0, 1, 0)$ . For our purposes,  $S$  will always contain at least three points.

To each plane of the flock  $F$ , we associate a unique element of the field  $\text{GF}(q)$ , subject only to the restriction that 0 is associated to the plane  $\pi_0$ . With this indexing of the planes of  $F$ , and since the planes do not pass through  $V$ , there exist functions  $f, g$ , and  $h : \text{GF}(q) \rightarrow \text{GF}(q)$ , so that the planes  $\pi_t$ , with  $t$  running through  $\text{GF}(q)$ , have equations:

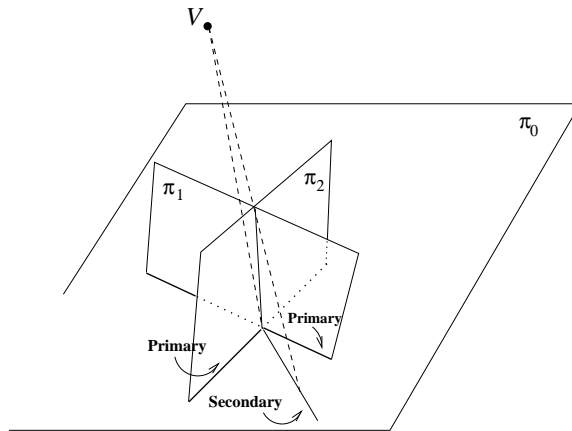
$$\pi_t : f(t)X + g(t)Y + h(t)Z + W = 0.$$

We call these three functions the *coordinate functions* of the flock. Since  $\pi_0$  is the plane with equation  $W = 0$ , we have that the coordinate functions must satisfy  $f(0) = g(0) = h(0) = 0$ . We will use the notation  $F = F(f, g, h)$  to denote the flock  $F$  with coordinate functions  $f, g$ , and  $h$ .

Many of the results in this chapter are centered around arbitrary cones, therefore, it is convenient to classify cones based on their carrier sets. We begin with the trivial cones.

The cone  $C(V, S)$  is said to be a *flat* cone if either it is the empty cone ( $S = \emptyset$ ) or the points of  $S$  are collinear.  $C(V, S)$  is a *thin* cone if the points of  $S$  are contained in some set of fewer than  $\lfloor \frac{q+2}{2} \rfloor$  concurrent lines. So, we see that every flat cone is a thin cone. A non-thin cone is referred to as a *wide* cone, that is, the points of  $S$  are not contained in any set of fewer than  $\lfloor \frac{q+2}{2} \rfloor$  concurrent lines. Finally, a wide cone whose carrier contains at least  $q + 1$  points is a *thick* cone.

Let  $S \in \pi_0$  be the carrier of cone with vertex  $V$  and  $F$  be a flock with cone  $C(V, S)$ . The lines of  $\pi_0$  which are the projections from  $V$  of the lines of intersection of pairs of planes of  $F$  into  $\pi_0$  are called the *baselines* of  $F$  (in  $\pi_0$ ). We distinguish two types of baselines. Those which are the intersections of  $\pi_0$  with the other planes of  $F$  are called the *primary* baselines, while the others are called the *secondary* baselines.



**Figure 5.3:** Primary and Secondary Baselines

Given a set  $F$  of  $q$  planes, if  $S'$  is the complement of the union of the baselines of  $F$ , then the cone  $C(V, S')$  is called the *critical cone* of  $F$ . Any subset of  $S'$  is

the carrier of a cone that has  $F$  as a flock. Proposition 5.2 introduces limitations on possible baseline configurations for a flock.

**Proposition 5.2** [18] *At the intersection of two distinct primary baselines there is a secondary baseline which cannot coincide with either of these primary baselines.*

**Proof:** Let  $\pi_1$  and  $\pi_2$  be two planes which intersect the carrier plane  $\pi$  in distinct primary baselines. Let  $P$  be the point of intersection of these baselines. Now, the intersection of  $\pi_1$  and  $\pi_2$  is a line  $l$  which does not lie in  $\pi_0$  (otherwise the baselines would not be distinct). The projection of  $l$  from  $V$  into  $\pi_0$  is a secondary baseline which passes through  $P$ . Suppose, without loss of generality, that this secondary baseline coincided with the primary baseline of  $\pi_1$ . The plane containing the primary baseline and  $l$  is clearly  $\pi_1$ , but because  $l$  projects to the baseline,  $V$  must also be in this plane. This contradiction shows that the secondary baseline must be distinct from both primary baselines. ■

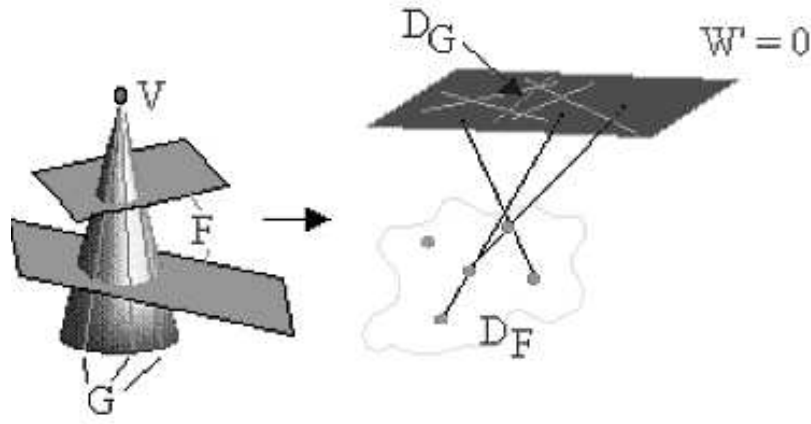
## 5.2 The Dual Setting and Star Flocks

Viewing flocks in the dual setting has been an effective technique in the classical quadratic cone situation. For instance in [22], DeClerk and Herssens used the dual setting to aid in the search used to find and classify flocks of quadratic cones for small values of  $q$ . It is also convenient for us to use the dual setting to illustrate the application of conic blocking sets to finding flocks.

Let  $F$  be a flock of the cone  $C(V, S)$  in  $\text{PG}(3, q)$ . By passing to the dual space,  $F$  becomes a set of  $q$  points in  $\text{PG}(3, q)$  and the cone is the set of all planes

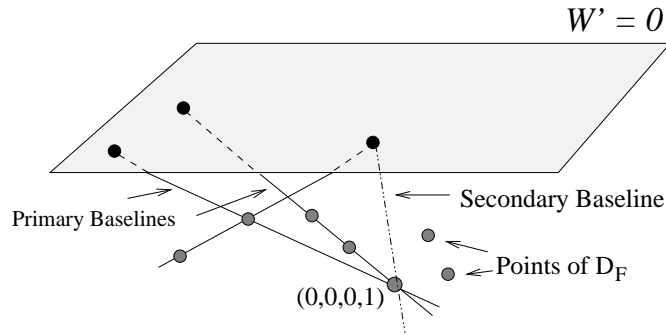
passing through a set of lines in the plane corresponding to  $V$  with the property that no line determined by a pair of the  $q$  points lies in any of these planes.

We set up some notation for the dual setting. Let  $F$  be a flock of the cone  $C(V, S)$  with  $V = (0, 0, 0, 1)$  where the planes of  $F$  are given by  $f(t)X + g(t)Y + h(t)Z + W = 0$ . Using the standard duality, the flock becomes a set of points  $D_F = \{(f(t), g(t), h(t), 1) \mid t \in \text{GF}(q)\}$ . The vertex  $V$  becomes a plane with equation  $W' = 0$ . The points on a generator of the cone  $C(V, S)$  become the set of all planes passing through a line in  $W' = 0$ . The set of all lines in the plane  $W' = 0$ , corresponding to generators of  $C(V, S)$  will be denoted by  $D_G$ , and the set of all planes passing through the lines of  $D_G$  will be denoted by  $D_C$ . The carrier  $S$  becomes the set of planes, denoted by  $D_S$ , passing through the point  $(0, 0, 0, 1)$  which intersect  $W' = 0$  in a line of  $D_G$ . The condition that the lines formed by pairs of points of  $D_F$  do not lie in the planes of  $D_C$  is equivalent to the condition that these lines do not intersect the lines of  $D_G$ .



**Figure 5.4:** Dual Flock Setting

Next we consider how primary and secondary baselines are represented in the dual setting. A primary baseline is the intersection of the plane  $W = 0$  with one of the other planes of the flock, so in the dual setting this is a line joining the point  $(0, 0, 0, 1)$  with one of the other points of  $D_F$ . A secondary baseline is the projection into  $W = 0$  of the line of intersection of two flock planes (which does not lie in  $W = 0$ ) from the vertex  $V$ . Thus, it is the intersection of the plane determined by  $V$  and the intersection line, with  $W = 0$ . This plane in the dual setting is a point in  $W' = 0$  which is on a line determined by two points of  $D_F$  which does not pass through  $(0, 0, 0, 1)$ , and the secondary baseline is therefore the line joining this point with  $(0, 0, 0, 1)$ .



**Figure 5.5:** Dual Baseline Setting

A *star flock* is a flock of a cone whose planes share a common point and a *proper star flock* is one for which this common point is unique. Linear flocks are clearly star flocks, but not proper star flocks. If  $F$  is a star flock, then the corresponding  $q$  points in the dual are coplanar. Moreover, if the points of  $D_F$  are collinear, then the planes of  $F$  must intersect in a common line. So the star flock is linear and therefore is not a proper star flock.

By examining baseline configurations, we can show that

**Proposition 5.3** [18] *The flocks of all non-flat cones in  $PG(3, 3)$  that have flocks are linear.*

**Proof:** There are only two planes other than the carrier plane in a flock of  $PG(3, 3)$ . Thus, there are only two primary baselines. These may coincide, in which case the flock is linear, or not, in which case their point of intersection is in all three planes and the flock is a proper star flock. Thus, any flock of any cone admitting a flock is a star flock.

Now, suppose that the two primary baselines are distinct (that is, the flock is a proper star flock). By Proposition 5.2 there is a secondary baseline through the point of intersection. These three baselines form the entire baseline configuration. The complement of the union of the baselines thus consists of the points on the remaining line through this point of intersection (not including that point). Thus, the critical cone is flat. So, a non-flat cone in  $PG(3, 3)$  cannot admit a proper star flock. ■

In great detail, we examine the dual of a proper star flock of a non-empty cone. Let  $F$  be a star flock of a non-empty cone, we can coordinatize  $F$  so that the flock has the form  $F(t, g(t), 0)$ . Let the vertex of the cone be given by  $V = (0, 0, 0, 1)$ , and observe that the point  $R = (0, 0, 1, 0)$  is in all the planes of  $F$ . We build the dual star flock model piece-by-piece.

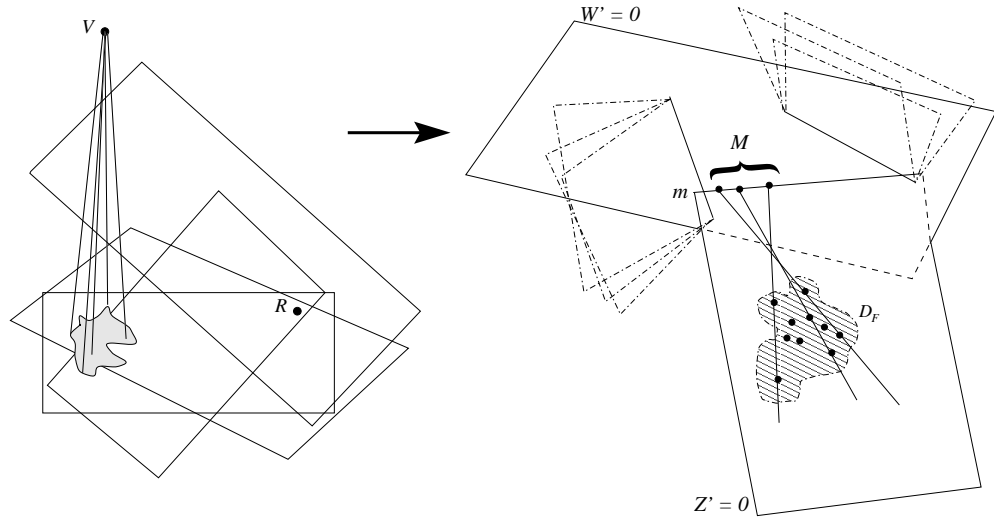
As mentioned earlier, the dual of the vertex  $V$  becomes the plane  $W' = 0$ . The dual of the common point  $R$  becomes the plane  $Z' = 0$ . Since  $R$  and  $V$  are distinct points in the original plane, we have that in the dual, the planes  $W' = 0$

and  $Z' = 0$  intersect in a line,  $m$ . Observe that any point on  $m$  has coordinates  $(x, y, 0, 0)$ .

Since every plane of the flock  $F(t, g(t), 0)$  contains the point  $R$ , the dual flock,  $D_F$  is a set of  $q$  points  $(t, g(t), 0, 1)$  all contained in the plane  $Z' = 0$ . Note that none of the points of  $D_F$  lie on the line  $m$ , for if a point of  $D_F$  were on the line  $m$ , then this point is in the plane  $W' = 0$ , implying that one of the planes of the flock would contain the vertex, which cannot happen. So, the  $q$  dual flock points all lie in the plane  $Z' = 0$ , and none of these points lie on the line  $m$  which is the intersection of  $W' = 0$  and  $Z' = 0$ . Take  $m$  as the line at infinity of the plane  $Z' = 0$  and use affine coordinates in the affine plane obtained by removing  $m$  from  $Z' = 0$ . The point in this affine plane with coordinates  $(x, y)$  is the point  $(x, y, 0, 1)$  of (the plane  $Z' = 0$  in)  $\text{PG}(3, q)$ . Hence, the  $q$  points of  $D_F$  in this affine plane have coordinates  $(t, g(t))$  for  $t \in \text{GF}(q)$ .

The points comprising a generator line  $g$  of the flock  $F$  become a set of planes, in the dual setting, that intersect in a common line. This line of intersection must lie in the plane  $W' = 0$ , since  $g$  contains  $V$ . Let  $D_G$  denote the set of dual generator lines in the plane  $W' = 0$ . We get one  $D_G$  line for every point in the carrier set, and each of the lines of  $D_G$  must meet  $m$  in a point. We remark that it is possible for two dual generator lines to meet at the same point on  $m$ . But, if the carrier set for the flock is a conic, only two lines of  $D_G$  can meet at the same point on  $m$ .

The line joining any two points of  $D_F$  must meet  $m$  in a point, say  $X$ . If a line of  $D_G$  also met  $m$  at the point  $X$ , we would have two planes of the flock meeting on the cone. So, this situation cannot arise.



**Figure 5.6:** Dual Proper Star Flock in  $\text{PG}(3, q)$

Let  $M$  be the set of all “slopes” determined by pairs of the points of  $D_F$ . That is,

$$M = \left\{ \frac{g(t) - g(s)}{t - s} \mid t \neq s \text{ and } t, s \in \text{GF}(q) \right\}$$

and let  $|M| = N$ . Each slope in  $M$  corresponds to a point of  $m$  through which passes at least one line of  $Z' = 0$  containing at least two points of  $D_F$ . In fact,  $M$  is the collection of slopes of the dual baselines in the plane  $Z' = 0$ . Consider the set of *free points* on the line  $m$ . These are the points on  $m$  that do not have slope in  $M$ . Now, to satisfy the flock condition, no line of  $D_G$  can pass through a point on  $m$  that is also on a line that contains at least two points of  $D_F$ . Thus, in order for  $F$  to be a proper star flock of a wide cone, we must have that  $N \leq q + 1 - \lfloor (q + 2)/2 \rfloor = \lfloor (q + 1)/2 \rfloor$ .

The problem of determining the number of slopes determined by  $q$  points in an affine plane has been well studied due to a connection with blocking sets (of lines)

of Rédei type. Recall from Chapter 2, a blocking set of *Rédei type* in  $\text{PG}(2, q)$  is a blocking set of size  $q + k$  for which there is some line  $l \in \Pi$  for which  $|l \cap \mathcal{B}| = k$ . Determining the number of slopes of a set of points with the specified property is almost completely settled. We restate Theorem 2.31 by Ball, Blokhuis, Brouwer, Storme, and Szönyi, using our terminology.

**Theorem 5.4** [5] *If  $q = p^n$  for some prime  $p$ , let  $e$  be the largest integer so that any line of the affine plane containing at least two points of  $D_F$  contains a multiple of  $p^e$  points of  $D_F$ . Then we have one of the following:*

- (i)  $e = 0$  and  $(q + 3)/2 \leq N \leq q + 1$ ,
- (ii)  $p = 2$  and  $e = 1$ , and  $(q + 5)/3 \leq N \leq q - 1$ ,
- (iii)  $p^e > 2$ ,  $e \mid n$ , and  $p^{n-e} + 1 \leq N \leq (q - 1)/(p^e - 1)$ ,
- (iv)  $e = n$  and  $N = 1$ .

Moreover, if  $p^e > 3$  or ( $p^e = 3$  and  $N = q/3 + 1$ ), then  $g$  is a  $p^e$ -linearized polynomial. ■

**Definition 5.5** *A  $p^e$ -linearized polynomial is one of the form:*

$$g(t) = \sum_{i=0}^{k-1} \alpha_i t^{p^{ie}},$$

where  $\alpha_i \in GF(p^n)$  and  $n = ke$ .

All bounds given for  $N$  are sharp, in the sense that there are examples with equality, except for the lower bound in case (ii). In case (ii), there is no known example with  $N < q/2 + 1$ . It is conjectured that in this case,  $N = \frac{q}{2} + 1$ , and this is true for  $q \leq 16$ .

We will discover that if we have a set of  $q$  points, not all collinear, in a plane that is embedded in projective 3-space, then after dualizing, this set of  $q$  points form a proper star flock of a cone. If  $q$  points in a plane produce a set  $M$  of size  $N$  of slopes, then we are able to determine the size of the free set. The free set consists of the points of  $m$  that do not lie on a line of  $Z' = 0$  that also contains at least two of the  $q$  points. These points of  $m$  in the free set are free to have dual generator lines through them. These dual generator lines lie in  $W' = 0$ , but meet the plane  $Z' = 0$  at the line  $m$ . The more free points, the more dual generator lines can be created, and so the larger the critical carrier set will be in the original space. With this large critical set, we can construct a cone that has those  $q$  points as a dual star flock.

The next theorems and corollary illustrate the consequences of Theorem 5.4 as related to star flocks of cones.

**Theorem 5.6** [18] *If  $q = p^n$  with  $p > 3$  a prime, then a proper star flock of any wide cone is given by  $F(t, g(t), 0)$  if and only if  $g$  is a nonlinear  $p^e$ -linearized polynomial for some  $e \mid n$  with  $e < n$ .*

**Proof:** For a star flock to be a flock of a wide cone, we must have that  $N \leq \lfloor \frac{q+1}{2} \rfloor$  and so, we may rule out Case (i) in Theorem 5.4. Also, for a star flock to be proper, we must have  $N > 1$  and so, we may rule out Case (iv) in the same theorem. Since  $p$  is a prime greater than 3, we may rule out Case (ii). Thus, all except Case (iii) of Theorem 5.4 is eliminated, and we have that  $g$  is a  $p^e$ -linearized polynomial.

Suppose  $g$  is a  $p^e$ -linearized polynomial for some  $e \mid n$  with  $e < n$ . Such functions are additive, so to calculate  $N$  we need only to calculate the number of

distinct values of  $\frac{g(t)}{t}$ , for  $t \neq 0$ . Let  $\mathcal{K} = \text{GF}(p^e)$  be a proper subfield of  $\text{GF}(p^n)$ . For each  $c \in \mathcal{K}$  we have  $g(ct) = cg(t)$ . Thus, for  $c \in \mathcal{K}^*$ ,  $\frac{g(ct)}{t} = \frac{g(t)}{t}$  and the number of distinct nonzero values of  $\frac{g(t)}{t}$  is at most  $|\text{GF}(p^n)^*|/|\text{GF}(p^e)^*| = \frac{q-1}{p^e-1}$ . Therefore,  $N \leq \frac{q-1}{p^e-1} + 1 < \frac{q+1}{2}$  since  $p^e > 3$ . ■

**Corollary 5.7** [18] *If  $q$  is prime, then all star flocks of wide cones are linear.*

**Proof:** The cases of  $q = 2$  (Proposition 5.1) and  $q = 3$  (Proposition 5.3) have already been dealt with. So, we may assume that  $q > 3$  is prime. Since a prime field has no proper subfields, there are no  $p^e$ -linearized polynomials other than the linear ones, so by Theorem 5.4 there are no proper star flocks. ■

As a restatement of the open cases in the classification given by Theorem 5.4, we have the following theorem.

**Theorem 5.8** [18] *If  $q = p^n$ , with  $p = 2$  or  $3$ , then a proper star flock of a wide cone is given by  $F(t, g(t), 0)$  where  $g$  is a  $p^e$ -linearized polynomial for some  $e \mid n$  with  $e < n$ , or every line of  $Z' = 0$  which contains at least two points of the dual flock  $D_F$  contains a multiple of  $p$ , but not a multiple of  $p^2$  points of  $D_F$  and, in characteristic 3,  $N > \frac{q}{3} + 1$ . ■*

For flocks of quadratic cones, we have two classes of examples which correspond to the extreme values of  $N$ . Example 16 illustrates how we can construct the Knuth-Kantor flock described in Section 2.2.3.

**Example 16.** Let  $\mathcal{E} = \text{GF}(p^n)$  with a subfield  $\mathcal{K} = \text{GF}(p^e)$ . The function  $g(t) = t^{p^e}$  gives  $N = \frac{q-1}{p^e-1}$  (Lemma 4.4). For  $p^e > 2$ , we have  $N \leq \lfloor \frac{q+1}{2} \rfloor$ , and so, we can construct a star flock of a wide cone, more specifically, a proper star flock

of a quadratic cone. This particular construction leads to the Knuth-Kantor flock that was described in Section 2.2.3.

Example 17 illustrates how we can construct a proper star flock using the relative trace function.

**Example 17.** Let  $\mathcal{E} = \text{GF}(p^n)$  with a subfield  $\mathcal{K} = \text{GF}(p^e)$ . Consider the function  $g(t) = \text{Tr}_{\mathcal{E}/\mathcal{K}}(t)$ , the relative trace function from  $\mathcal{E}$  onto  $\mathcal{K}$ . Similar to the proofs given in Lemmas 4.3 and 3.3, we find that  $N = p^{n-e} + 1$ . If  $p^e > 3$ , then  $N < \lfloor \frac{q+1}{2} \rfloor$ , and so, we can construct a proper star flock of a wide (quadratic) cone.

In the case where the wide cone is a quadratic cone, we can restate the theorems of Thas (3.4, 4.7, 4.8) in star flock terminology.

**Theorem 5.9** [69] *In even characteristic, all star flocks of quadratic cones are linear.* ■

**Theorem 5.10** [69] *In odd characteristic, a star flock of a quadratic cone is either linear or a Knuth-Kantor flock.* ■

Suppose  $F$  is a proper star flock of a cone  $C(V, S)$  and the carrier set  $S'$  of the critical cone  $C(V, S')$  contains a conic. Then by Theorems 5.9 and 5.10,  $F$  is either linear or Knuth-Kantor. Since  $F$  is a proper star flock,  $F$  cannot be linear. If  $N \neq (q-1)/(p^e-1)$ , then  $F$  is not Knuth-Kantor. Since  $F$  is a proper star flock that cannot be linear or Knuth-Kantor, the critical carrier set of  $F$  cannot contain a conic. Hence, the baselines of the flock form a conic blocking set in  $W = 0$ . In other words, all proper star flocks of cones give conic blocking sets, except for the Knuth-Kantor flock described in Example 16.

These theorems prove that the baselines of a proper star flock of a wide cone, which is not of Knuth-Kantor type, form a conic blocking set. In this setting, since  $N < \lfloor \frac{q+1}{2} \rfloor$ , the conic blocking sets which arise have the property that no conic is completely contained in the set of lines.

## 6. Avenues of Further Research

In this thesis we examined constructions for finding conic blocking sets and we studied bounds on the size of minimum conic blocking sets. In this chapter, we mention open problems and questions that have not been solved. These remain to be studied further.

In planes of odd characteristic every conic is an oval. The concept of an *oval blocking set* is no different than that of a conic blocking set. In planes of even characteristic, these two concepts do not coincide as there are examples of ovals that are not conics. A computer search by W. Cherowitzo has shown that the conic blocking set,  $\{y = t^3x + z \mid t \neq 0\}$ , does not block the Subiaco ovals [17]. Similar to the work presented in this dissertation, there is research to be done with oval blocking sets.

All of the material on CBSs given here is centered around CBSs consisting of concurrent lines. A natural direction to pursue is to examine conic blocking sets of nonconcurrent lines. S. Ball, A. Blokhuis, and M. Lavrauw [6] have preliminary results about semifield flocks that can be used to find conic blocking sets of nonconcurrent lines for planes of odd order.

We were able to use the structure of the image set of an additive function to obtain many of the CBSs presented in this dissertation. Since planes of prime order lack interesting additive functions, no CBS constructions were found for these planes. Finding CBS constructions for planes of prime order remains an open problem.

For  $q$  odd, preliminary computer computations show that there are several construction ideas worth further examination. For  $q = p^2$ , the set of lines through the point  $(0, 0, 1)$  with absolute trace 1 or absolute trace 0 slope seem to form a conic blocking set of size  $2p$  in  $\text{PG}(2, p^2)$ . Also, there is preliminary work showing that we can add relatively few lines to the set of lines that correspond to the KK-lines and form a CBS in  $\text{PG}(2, p^h)$ ,  $h$  even and  $p$  odd.

In Section 4.4, we exhibited a CBS construction for  $\text{PG}(2, q^2)$  using points with parameters in  $\text{GF}(q)$  and with parameters with relative trace 0. This CBS should be examined to determine if it is irreducible.

There is work to be done with oval blocking sets in non-Desarguesian projective planes.

The minimum sizes of CBSs in planes of odd order exhibited a mostly monotonic behavior as the size of the plane increased. There are two examples where this behavior was not monotonic;  $q = 79$  and  $q = 137$  or  $139$ . There is further work to be done in explaining the dip in sizes at these values of  $q$ .

For  $q$  even, computer computations show that in  $\text{PG}(2, 2^h)$ ,  $h$  an odd prime, the set of lines with slope in a nontrivial cyclotomic coset along with the three lines  $x = 0$ ,  $y = 0$ , and  $y = x$  through the point  $(0, 0, 1)$  form a CBS of size  $h + 3$ .

There is more work to be done in strengthening the lower bounds on the sizes of minimum CBSs.

### A. CBS Parameters for $q$ Even

This appendix contains the parameters for the minimum conic blocking sets and the smallest conic blocking sets found in  $\text{PG}(2, q)$ ,  $q$  even. We indicate the minimum CBS found with an M and the smallest CBS found with an S in the size column. The Method column denotes which method was used to find the CBS. An ST denotes the model developed in Section 3.4 was used, an SBH denotes that the modified greedy algorithm (surrogate-based heuristic) developed by Gary Kochenberger [47] was used, and finally an AH denotes that an ad-hoc method of searching for CBSs was used. The fourth column contains the primitive polynomial used to generate  $\text{GF}(q)$ . The last column contains the parameters for the points (in the dual setting) that form a CBS.

$q$	Size	Method	Primitive Polynomials	Parameters
$2^2$	M	ST	$x^2 = x + 1$	$0, 1, \infty$
$2^3$	M	ST	$x^3 = x^2 + 1$	$0, 1, \infty, \alpha, \alpha^2$
$2^4$	M	ST	$x^4 = x + 1$	$0, 1, \infty, \alpha^5, \alpha^{10}$
$2^5$	M	ST	$x^5 = x^2 + 1$	$0, 1, \infty, \alpha^6, \alpha^8, \alpha^{23}, \alpha^{24}, \alpha^{25}$
$2^6$	M	ST	$x^6 = x + 1$	$0, 1, \infty, \alpha, \alpha^5, \alpha^6, \alpha^{37}, \alpha^{44}, \alpha^{62}$
$2^7$	M	ST	$x^7 = x + 1$	$0, 1, \infty, \alpha, \alpha^2, \alpha^{29}, \alpha^{49}, \alpha^{80}, \alpha^{100}$

**Table A.1:** CBSs in Planes of Even Order

$q$	Size	Method	Primitive Polynomials	Parameters
$2^8$	S	SBH	$x^8 = x^5 + x^4 + x^3 + 1$	$0, 1, \infty, \alpha, \alpha^2, \alpha^3, \alpha^6, \alpha^{17}, \alpha^{52}, \alpha^{54}, \alpha^{60}, \alpha^{119}, \alpha^{168}$
$2^9$	S	SBH	$x^9 = x^4 + 1$	$0, 1, \infty, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^{25}, \alpha^{59}, \alpha^{80}, \alpha^{147}, \alpha^{269}, \alpha^{283}, \alpha^{385}, \alpha^{433}$
$2^{10}$	S	AH & ST	$x^{10} = x^3 + 1$	$0, 1, \infty, \alpha^1, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \alpha^{32}, \alpha^{64}, \alpha^{128}, \alpha^{256}, \alpha^{512}, \alpha^{93}, \alpha^{186}, \alpha^{279}, \alpha^{372}, \alpha^{465}, \alpha^{558}, \alpha^{651}, \alpha^{744}, \alpha^{837}, \alpha^{930}$

**Table A.1:** (Cont.)

## B. CBS Parameters for $q$ Odd

This appendix contains the parameters for the minimum conic blocking sets in  $\text{PG}(2, q)$ ,  $q$  odd. Although there were two models developed for finding minimum CBSs, we used the restricted-dual model (RD) for our searches. The modified greedy algorithm (surrogate-based heuristic) developed by Gary Kochenberger [47] is denoted SBH. Tables B.1 and B.2 contains the parameter sets of minimum conic blocking sets in planes of prime and nonprime order, respectively. Tables B.3 and B.4 contains the parameter sets for the smallest conic blocking set found, but not verified as a CBS of minimum size, in planes of prime and nonprime order.

Order	Model	Parameters
3	RD	0, 1, $\infty$
5	RD	0, 1, $\infty$ , 3
7	RD	0, 1, $\infty$ , 5
11	RD	0, 1, $\infty$ , 5, 7, 9
13	RD	0, 1, $\infty$ , 5, 6, 10
17	RD	0, 1, $\infty$ , 4, 6, 14
19	RD	0, 1, $\infty$ , 4, 8, 13
23	RD	0, 1, $\infty$ , 12, 13, 15, 17
29	RD	0, 1, $\infty$ , 3, 8, 19, 23, 26
31	RD	0, 1, $\infty$ , 4, 5, 11, 13, 26
37	RD	0, 1, $\infty$ , 13, 23, 24, 25, 29
41	RD	0, 1, $\infty$ , 4, 10, 21, 32, 37
43	RD	0, 1, $\infty$ , 8, 18, 23, 27, 41
47	RD	0, 1, $\infty$ , 2, 4, 6, 34, 43
53	RD	0, 1, $\infty$ , 13, 31, 37, 44, 47, 52

**Table B.1:** Minimum CBSs in Planes of Prime Order

Order	Model	Parameters
59	RD	0, 1, $\infty$ , 12, 40, 41, 43, 48, 57
61	RD	0, 1, $\infty$ , 7, 9, 14, 21, 45, 60
67	RD	0, 1, $\infty$ , 17, 34, 35, 45, 50, 53
71	RD	0, 1, $\infty$ , 10, 23, 24, 30, 64, 69
73	RD	0, 1, $\infty$ , 9, 12, 25, 36, 51, 60
79	RD	0, 1, $\infty$ , 12, 24, 40, 52, 61
83	RD	0, 1, $\infty$ , 15, 21, 24, 28, 42, 53, 73
89	RD	0, 1, $\infty$ , 9, 22, 30, 31, 45, 73, 85
97	RD	0, 1, $\infty$ , 27, 44, 47, 49, 65, 70, 93
101	RD	0, 1, $\infty$ , 20, 32, 34, 51, 76, 85, 90
103	RD	0, 1, $\infty$ , 5, 39, 52, 62, 65, 69, 91
107	RD	0, 1, $\infty$ , 17, 31, 32, 54, 58, 62, 93
109	RD	0, 1, $\infty$ , 9, 15, 19, 39, 55, 73, 85
113	RD	0, 1, $\infty$ , 11, 13, 31, 38, 54, 57, 65, 84

**Table B.1:** (Cont.)

Order	Model	Primitive Polynomials	Parameters
9	RD	$x^2 = x + 1$	0, 1, $\infty$ , $\alpha^2$ , $\alpha^3$
25	RD	$x^2 = x + 3$	0, 1, $\infty$ , $\alpha$ , $\alpha^2$ , $\alpha^{10}$ , $\alpha^{16}$ , $\alpha^{17}$
27	RD	$x^3 = x + 2$	0, 1, $\infty$ , $\alpha^2$ , $\alpha^3$ , $\alpha^9$ , $\alpha^{21}$ , $\alpha^{25}$
49	RD	$x^2 = x + 4$	0, 1, $\infty$ , $\alpha$ , $\alpha^6$ , $\alpha^{25}$ , $\alpha^{30}$ , $\alpha^{34}$ , $\alpha^{42}$
81	RD	$x^4 = x + 1$	0, 1, $\infty$ , $\alpha^3$ , $\alpha^9$ , $\alpha^{14}$ , $\alpha^{33}$ , $\alpha^{38}$ , $\alpha^{64}$ , $\alpha^{68}$
125	RD	$x^3 = x + 2$	0, 1, $\infty$ , $\alpha^8$ , $\alpha^{11}$ , $\alpha^{25}$ , $\alpha^{33}$ , $\alpha^{52}$ , $\alpha^{121}$ , $\alpha^{122}$ , $\alpha^{123}$

**Table B.2:** Minimum CBSs in Planes of Nonprime Order

Order	Model	Parameters
127	SBH	0, 1, $\infty$ , 2, 3, 7, 24, 53, 65, 115, 118
131	SBH	0, 1, $\infty$ , 2, 18, 50, 78, 88, 111, 127, 128
137	SBH	0, 1, $\infty$ , 2, 3, 4, 8, 35, 90, 103, 130, 132
139	SBH	0, 1, $\infty$ , 10, 12, 35, 41, 42, 44, 62, 79
149	SBH	0, 1, $\infty$ , 2, 5, 9, 18, 45, 49, 70, 106, 109
151	SBH	0, 1, $\infty$ , 3, 5, 11, 13, 15, 31, 33, 49, 79
157	SBH	0, 1, $\infty$ , 2, 7, 10, 15, 16, 24, 89, 93, 102
163	SBH	0, 1, $\infty$ , 2, 8, 22, 25, 29, 34, 53, 63, 103
167	SBH	0, 1, $\infty$ , 5, 6, 14, 20, 36, 37, 114, 118, 159
173	SBH	0, 1, $\infty$ , 2, 11, 13, 14, 15, 45, 72, 81, 94
179	SBH	0, 1, $\infty$ , 2, 10, 32, 36, 53, 74, 113, 141, 167
181	SBH	0, 1, $\infty$ , 2, 9, 11, 39, 69, 114, 129, 132, 150
191	SBH	0, 1, $\infty$ , 5, 7, 15, 32, 33, 43, 49, 83, 117
193	SBH	0, 1, $\infty$ , 5, 11, 12, 49, 68, 72, 79, 106, 118
197	SBH	0, 1, $\infty$ , 2, 6, 14, 55, 57, 62, 110, 116, 193
199	SBH	0, 1, $\infty$ , 3, 13, 17, 71, 139, 147, 157, 164, 173

**Table B.3:** Smallest Known CBSs for  $q$  an Odd Prime

Order	Model	Primitive Polynomials	Parameters
121	RD	$x^2 = 10x + 4$	0, 1, $\infty$ , $\alpha^9$ , $\alpha^{21}$ , $\alpha^{30}$ , $\alpha^{38}$ , $\alpha^{78}$ , $\alpha^{113}$ , $\alpha^{118}$ , $\alpha^{119}$
169	RD	$x^2 = 12x + 11$	0, 1, $\infty$ , $\alpha^{18}$ , $\alpha^{32}$ , $\alpha^{47}$ , $\alpha^{59}$ , $\alpha^{61}$ , $\alpha^{67}$ , $\alpha^{124}$ , $\alpha^{163}$ , $\alpha^{167}$

**Table B.4:** Smallest Known CBSs for  $q$  an Odd Nonprime

### C. The Branch and Bound Algorithm

As shown in Chapters 3 and 4, the problem of finding minimum conic blocking sets is directly related to the set covering problem. In this appendix, we introduce the set covering problem (SCP) as an optimization problem and briefly discuss several aspects of the solvers used.

Let  $S$  be a set of objects which are numbered  $\{1, 2, \dots, m\}$  and  $\mathcal{F}$  be a collection of subsets of  $S$ . Furthermore, assume that each of the elements of  $S$  has a cost associated with it. The SCP is to ‘cover’ all members of  $\mathcal{F}$  at minimum cost using elements of  $S$ . That is, to find a subset  $\mathcal{P}$  of  $S$  such that  $\mathcal{P} \cap C_i \neq \emptyset$  for all  $C_i \in \mathcal{F}$  at a minimum cost.

For example, suppose  $S = \{1, 2, 3, 4\}$  and  $\mathcal{F} = \{C_1 = \{1, 2\}, C_2 = \{2, 3\}, C_3 = \{1, 4\}\}$ . One cover for  $S$  would be  $\mathcal{P}_1 = \{1, 3\}$ , since  $\mathcal{P}_1 \cap C_1 = \{1\}$ ,  $\mathcal{P}_1 \cap C_2 = \{3\}$ , and  $\mathcal{P}_1 \cap C_3 = \{1\}$ . Another cover would be  $\mathcal{P}_2 = \{1, 2, 4\}$ , as  $\mathcal{P}_2 \cap C_1 = \{1\}$ ,  $\mathcal{P}_2 \cap C_2 = \{2\}$ , and  $\mathcal{P}_2 \cap C_3 = \{1, 4\}$ . Suppose that the element 1 has a cost of 10, the elements 2 and 3 both have a cost of 2, and the element 4 has a cost of 1. Then the cost of the covering  $\mathcal{P}_1$  is 12 and the cost of the covering  $\mathcal{P}_2$  is 13. A minimum cover for this problem is  $\mathcal{P} = \{2, 4\}$ , which has an associated cost of 3.

One method for finding a minimum cover is to build a 0-1 pure integer programming (PIP) model. Constraints are introduced to ensure that each member (set) of  $\mathcal{F}$  is covered. If the objective is to minimize the cost of a cover of  $\mathcal{F}$ , the

resultant model is,

$$\begin{array}{ll}
 \text{Minimize} & 10x_1 + 2x_2 + 2x_3 + 1x_4 \\
 \text{subject to} & x_1 + x_2 \geq 1, \\
 & x_2 + x_3 \geq 1, \\
 & x_1 + x_4 \geq 1,
 \end{array}$$

or

$$\begin{array}{ll}
 \min & c^T x \\
 \text{subject to} & Ax \geq b \\
 & x \in \{0, 1\},
 \end{array}$$

where

$$A = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}, b = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \text{ and } c^T = \begin{bmatrix} 10 & 2 & 2 & 1 \end{bmatrix}.$$

There are many applications for the SCP other than searching for minimum CBSs. A comprehensive list of applications is found in [3] by Balas and Padberg. There are also many algorithms that exist for integer problems. Two standard algorithms are the branch and bound algorithm and the cutting-plane algorithm, which are described in Chapter 4 of Garfinkle and Nemhauser [28]. We provide a brief explanation of the branch and bound algorithm shortly. The difficulty of solving set covering problems usually arises not from their structure, but from their size. This fact became more apparent to us as the order of the projective plane increased.

SCP's are comparatively easy to solve with the branch and bound algorithm, and this algorithm guarantees an optimal solution. So, for our problems, we are guaranteed that the conic blocking set found by the branch and bound algorithm is indeed a minimum conic blocking set.

The branch and bound (B&B) algorithm is an optimization technique that enumerates a tree to find an optimal solution. By calculating upper and lower bounds on the objective function, the B&B algorithm accelerates the fathoming process and thereby shortens the enumeration. A node is *fathomed* if it is determined that no completion from this point could produce a better solution than one already obtained. This could happen by bounding the objective, or it can happen by determining there is no feasible solution with the partial specifications corresponding to the node.

Commercial solvers invoke a heuristic before starting the fathoming process to obtain an initial “good” solution. Thus, the process begins with a feasible solution, but there is no guarantee of optimality. Enumerative algorithms invariably benefit from starting with a good feasible solution. And so, by beginning the tree search with a feasible solution, a lower bound on the optimal objective function is provided. This bound is used for fathoming in the algorithm, resulting in a pruning of the enumeration tree.

The following typical integer linear program (ILP)

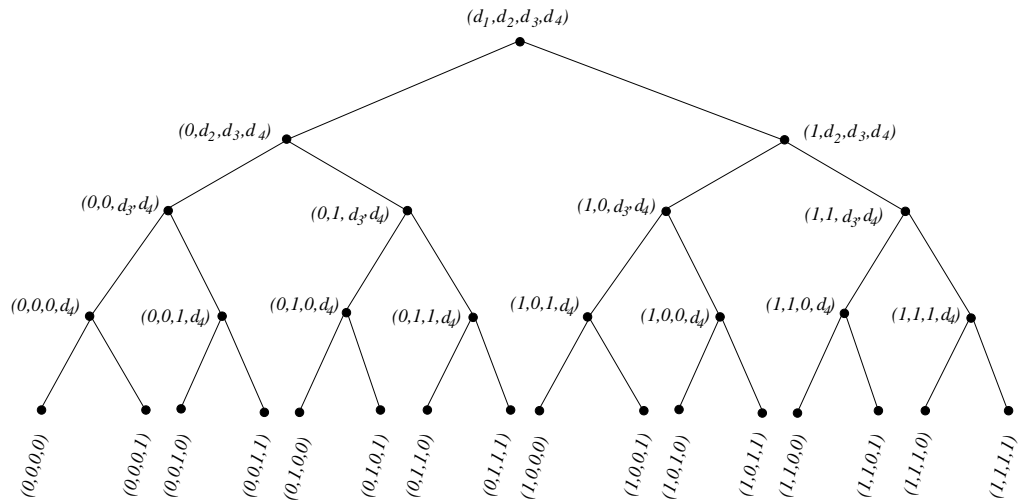
$$\begin{array}{ll}
 \min & c^T x \\
 \text{subject to} & Ax \geq b \\
 & x \in \{0, 1\}
 \end{array}$$

has the corresponding LP relaxation (RLP)

$$\begin{aligned} \min \quad & c^T x \\ \text{subject to} \quad & Ax \geq b \\ & 0 \leq x \leq 1, \end{aligned}$$

where  $c^T x$  is the objective function, the components of  $c$  are the cost coefficients,  $A$  is called the coefficient matrix,  $b$  is the right-hand side, and  $x$  is a vector of decision variables. Notice that in the LP relaxation there are no more integrality constraints, but rather the decision variables are restricted to the interval  $[0, 1]$ .

To explain the B&B process, we focus on the set covering problem given earlier. Since the decision variable is binary, we use the tree given in Figure C.1 to help illustrate the algorithm.



**Figure C.1:** A Tree

Suppose the heuristic algorithm obtains the feasible solution  $z_0 = c^T x = 14$  at vertex  $(1, 1, 1, 0)$ . The B&B algorithm begins the process of fathoming

(investigating) the enumeration tree. If the algorithm tested vertex  $(1, 1, 1, 1)$ , it would find that the cost  $c^T x = 15 > z_0$ , so this vertex is pruned. Continuing with its branching process, the algorithm examines the RLP at the vertex  $(1, 1, 0, d_4)$ . The RLP is given by

$$\begin{aligned} \min & 12 + d_4 \\ \text{s.t.} & 2 + d_4 \geq 1 \\ & 1 + d_4 \geq 1 \\ & 0 \leq d_4 \leq 1. \end{aligned}$$

The optimal solution to this relaxation is  $12 < 14$ , so further exploration below vertex  $(1, 1, 0, d_4)$  is warranted. At vertex  $(1, 1, 0, 0)$ , we obtain an update for the objective value since  $z_1 = c^T x = 12$ . The vertex  $(1, 1, 0, 1)$  yields a feasible solution of 13, but is no longer a candidate for an optimal solution, since we have a feasible solution with an objective value of  $z_1 = 12$ .

Having completed a search from vertex  $(1, 1, d_3, d_4)$ , the algorithm now considers the RLP at vertex  $(1, 0, d_3, d_4)$ .

$$\begin{aligned} \min & 10 + 2d_3 + d_4 \\ \text{s.t.} & 1 + d_3 \geq 1 \\ & 1 + d_4 \geq 1 \\ & 0 \leq d_i \leq 1, i = 3, 4. \end{aligned}$$

In this RLP, the optimal solution is  $10 < 12 = z_1$ , so no decision can be made at this vertex. The RLP is examined at vertex  $(1, 0, 0, d_4)$  and we discover that no feasible solution can be obtained, since one of the constraints becomes  $0 \geq 1$ . Hence, the branch from vertex  $(1, 0, 0, d_4)$  is pruned. No decision by the RLP is made at vertex  $(1, 0, 1, d_4)$ , so we explore further down the branch. Vertex

$(1, 0, 1, 0)$  yields an alternative optimal solution of 12. Since vertex  $(1, 0, 1, 1)$  does not yield a better optimal solution, this vertex is pruned.

At this point, the algorithm has (nearly) exhaustively searched the branch beginning with vertex  $(1, d_2, d_3, d_4)$  and examines the branch beginning with  $(0, d_2, d_3, d_4)$ . Notice that there is no feasible solution to the RLP at vertex  $(0, 0, d_3, d_4)$ , and the tree may be pruned at this vertex. Solving the RLP at the vertex  $(0, 1, d_3, d_4)$ ,

$$\begin{aligned} \min \quad & 2 + 2d_3 + d_4 \\ \text{s.t.} \quad & 1 + d_3 + d_4 \geq 1 \\ & d_4 \geq 1 \\ & 0 \leq d_i \leq 1, i = 3, 4, \end{aligned}$$

gives a minimum value of 3, and further exploration is warranted. Exploring the rest of the tree, from vertex  $(0, 1, 0, d_4)$ , using this LP relaxation leads to the new optimal solution  $z_2 = c^T x = 3$  at vertex  $(0, 1, 0, 1)$ . At vertex  $(0, 1, 1, d_4)$ , the cost value is at least  $4 > 3 = z_2$ , so this vertex is pruned. Hence, when the B&B algorithm terminates, we have an optimal solution of 3 given by  $x = \begin{bmatrix} 0, 1, 0, 1, \end{bmatrix}^T$ .

Observe that if the heuristic had found an initial feasible solution in the tree that branches from vertex  $(0, d_2, d_3, d_4)$ , then after branching through this tree we would have obtained the optimal solution. Then, the entire subtree that branches from vertex  $(1, d_2, d_3, d_4)$  would have been pruned since any feasible solution will have a cost of at least 10, which is greater than any cost given from the other tree. This observation illustrates the benefits of using a good heuristic to find an initial feasible solution.

This simple example illustrates how the B&B algorithm essentially performs an intelligent exhaustive search that guarantees optimality. For a formal proof that the algorithm finds an optimal solution see [28] or [52].

For the problem of finding minimum conic blocking sets, we chose to use the General Algebraic Modeling System (GAMS) which is a modeling system for mathematical programming problems [20]. GAMS lets the user concentrate on modeling. GAMS eliminates the need of the user to think about purely technical machine-specific problems, and instead allows the user to focus on conceptualizing and running the model, and then analyzing the results. After GAMS builds the model from a simple language, it then sends the model to a solver. We chose the solver Cplex [39], which touts itself as being the “World’s Leading Mathematical Programming Optimizers”. Cplex is a good solver and is used to solve a wide range of models in the corporate community. To illustrate the simplicity of using this modeler and solver to find a solution to the set covering problem, we give a sample of the code used to model this problem.

```

[h]
sets i/1*4/;
sets k/1*3/;
table a(k,i)
      1 2 3 4
      1 1 1 0 0
      2 0 1 1 0
      3 1 0 0 1
;
binary variable x(i);
variable z;
parameter c(i);
      /1 10
      2 2
      3 2
      4 1 /;
equations obj, cover(k);
obj .. z =e= sum(i,c(i)*x(i));
cover(k)..sum(i,a(k,i)*x(i)) =g= 1;
model Sample /all/;
solve Sample using mip minimizing z;

```

The code for the conic blocking set problem is similar to this set covering code. In the CBS problem, all cost coefficients of the objective function are 1 and so in the GAMS code for the CBS problem, there is no parameter  $c(i)$ .

## References

- [1] A. Albert and R. Sandler. *An Introduction to Finite Projective Planes*. Holt, Rinehart, and Winston, Inc., 1968.
- [2] E. F. Assmus and T. D. Key. *Designs and their Codes*, volume 103 of *Cambridge Tracts in Math*. Cambridge University Press, 1992.
- [3] E. Balas and W. Padberg. On the set covering problem II. *Ops Res.*, 23:74 – 90, 1975.
- [4] E. Balas and W. Padberg. Set Partitioning: A Survey. *SIAM Review*, 18:710 – 760, 1976.
- [5] S. Ball, A. Blokhuis, A. Brouwer, L. Storme, and T. Szőnyi. On the number of slopes of the graph of a function defined on a finite field. *J. C. T.*, 86(A):187 – 196, 1999.
- [6] S. Ball, A. Blokhuis, and M Lavrauw. Private communications, 2000.
- [7] Elwyn R. Berlekamp. *Algebraic Coding Theory*. McGraw-Hill Inc., 1968.
- [8] Albrecht Beutelspacher and Ute Rosenbaum. *Projective Geometry*. Cambridge University Press, 1998.
- [9] Norman Biggs. *Permutation Groups and Combinatorial Structures*. Cambridge Univeristy Press, 1979.
- [10] A. Blokhuis. Polynomials in finite geometries and combinatorics. In *Surveys in Combinatorics*, volume 187 of *London Math. Soc. Lecture Note Series*, pages 35 – 52, Cambridge, 1993. Cambridge University Press.
- [11] A. Blokhuis, A. E. Brouwer, and T. Szőnyi. The Number of Directions Determined by a Function  $f$  on a Finite Field. *Jounral of Combinatorial Theory*, 70:349 – 353, 1995.
- [12] Ernest F. Brickell. Some Ideal Secret Sharing Schemes. In J.J. Quizquater and J. Vandewalle, editors, *Lecture Notes in Computer Science, Advances in Cryptology- EUROCRYPTO '89*, volume 434, pages 468–490. Springer-Verlag, April 1989.
- [13] R. H. Bruck and H. J. Ryser. The non-existence of certain finite projective planes. *Canadian Journal of Mathematics*, 1:88 – 93, 1949.

- [14] A. A. Bruen. Blocking sets in finite projective planes. *SIAM J. Appl. Math.*, 21:380 – 392, 1971.
- [15] A. A. Bruen and J. A. Thas. Partial spreads, packings and hermitian manifolds in  $PG(3,q)$ . *Math Z.*, 151:207 – 214, 1976.
- [16] P. J. Cameron and J. H. Van Lint. *Designs, Graphs, Codes, and their Links*. Cambridge University Press, 1991.
- [17] W. Cherowitzo, T. Penttila, I. Pinneri, and G. F. Royle. Flocks and Ovals. *Geometriae Dedicata*, 60:17 – 37, 1996.
- [18] W. E. Cherowitzo. *Flocks of Cones*. World Wide Web, <http://www-math.cudenver.edu/~wcherowi/research/flocks.html>, 1998 - 2001.
- [19] V. Chvátal. A greedy heuristic for the set covering problem. *Mathematics of Operations Research*, 4:233 – 235, 1979.
- [20] GAMS Development Corporation. *Gams*. World Wide Web, <http://www.gams.com>, 1987 - 1999.
- [21] H. S. M. Coxeter. *Projective Geometry*. Blaisdell Publishing Company, 1964.
- [22] F. DeClerck and C. Herssens. *Flocks of the quadratic cone in  $PG(3,q)$ , for  $q$  small*, volume 8, pages 1 – 75. Ghent University, 1993.
- [23] Peter Dembowski. *Finite Geometries*. Springer-Verlag, 1968.
- [24] Leonard Eugene Dickson. *Linear Groups with an Exposition of the Galois Field Theory*. Dover Publications Inc., 1958.
- [25] Jane W. DiPaola. On Minimum Blocking Coalitions in Small Projective Plane Games. *SIAM J. Appl. Math.*, 17(2):378 – 392, March 1969.
- [26] Joseph A. Gallian. *Contemporary Abstract Algebra*. Houghton Mifflin Company, 1998.
- [27] M. R. Garey and D. S. Johnson. *Computers and Intractability: A Guide to the Theory of NP-Completeness*. W.H. Freeman, New York, NY, 1979.
- [28] R. Garfinkle and G. Nemhauser. *Integer Programming*. John Wiley & Sons, 1972.
- [29] H. Gevaert and N. L. Johnson. Flocks of quadratic cones, generalized quadrangles and translation planes. *Geom. Ded.*, 27:301 – 317, Dec. 1988.

- [30] E. N. Gilbert, F. J. MacWilliams, and N. J. A. Sloane. Codes which detect deception. *Bell System Tech. J.*, 53:405 – 425, 1974.
- [31] H. Greenberg. *Mathematical Programming Glossary*. World Wide Web, <http://www-math.cudenver.edu/~hgreenbe/glossary/glossary.html>, 1996 - 1998.
- [32] H. Greenberg. *Mixed Integer Programming and Combinatorial Optimization*. World Wide Web, [http://www-math.cudenver.edu/~hgreenbe/courses/mip/7594\\_S01.html](http://www-math.cudenver.edu/~hgreenbe/courses/mip/7594_S01.html), 2001.
- [33] R. W. Hamming. Error detecting and error correcting codes. *Bell System Tech. J.*, 29:147 – 160, 1950.
- [34] J. W. P. Hirschfeld. *Finite Projective Spaces of Three Dimensions*. Oxford University Press, 1985.
- [35] J. W. P. Hirschfeld. *Projective Geometries over Finite Fields*. Oxford University Press, 1998.
- [36] J. W. P. Hirschfeld and J. A. Thas. *General Galois Geometries*. Oxford University Press, 1991.
- [37] A. Ho. Worst Case Analysis of a Class of Set Covering Heuristics. *Math. Programming*, 23:170 – 181, 1982.
- [38] L. D. Holder. The Construction of Geometric Threshold Schemes with Projective Geometry. Master's thesis, Univeristy of Colorado at Denver, 1997.
- [39] ILOG. *Cplex*. World Wide Web, <http://www.ilog.com/products/cplex/>, 2000.
- [40] J. R. Isbell. A Class of Simple Games. *Duke Mathematical Journal*, 25:425 – 436, 1958.
- [41] D. S. Johnson. Approximation Algorithms for Combinatorial Problems. *Journal of Computer and System Sciences*, 9:256 – 278, 1974.
- [42] N. L. Johnson. Semifield flocks of quadratic cones. *Simon Steven*, 61:313 – 326, 1987.
- [43] Lars Kadison and Matthias T. Kromann. *Projective Geometry and Modern Algebra*. Birkäuser, 1996.

- [44] W. M. Kantor. Some generalized quadrangles with parameters  $(q^2, q)$ . *Math. Z.*, 192:45 – 50, 1986.
- [45] Irving Kaplansky. *Linear Algebra and Geometry*. Chelsea Publishing Company, 1974.
- [46] R. M. Karp. Reducibility among Combinatorial Problems. In R. E. Miller and J. W. Thatcher, editors, *Complexity of Computer Computations*, pages 85 – 103. Plenum Press, New York, NY, 1972.
- [47] Gary Kochenberger. Private communications, 2001.
- [48] Rudolf Lidl and Harald Niederreiter. *Finite Fields*. Cambridge University Press, 1997.
- [49] L. Lovász. On the Ratio of Optimal Integral and Fractional Covers. *Discrete Mathematics*, 13:383 – 390, 1975.
- [50] L. Lovász and A. Schrijver. Remarks on a Theorem of Rédei. *Studia Scientiarum mathematicarum Hungarica*, 16:449 – 454, 1981.
- [51] James A. Murtha and Earl R. Willard. *Linear Algebra and Geometry*. Holt, Rinehart, and Winston Inc., 1969.
- [52] G. Nemhauser and L. Wolsey. *Integer and Combinatorial Optimization*. John Wiley & Sons, 1988.
- [53] Ben Noble and James W. Daniel. *Applied Linear Algebra*. Prentice-Hall, 1988.
- [54] S. E. Payne. Quadratic Forms, BLT-Sets and  $q$ -Clans. 1998.
- [55] S. E. Payne. Private communications, 2000.
- [56] E. C. Posner. Combinatorial Structures in Planetary Reconnaissance. In H. B. Mann, editor, *Error Correcting Codes*. Wiley, New York, 1968.
- [57] L. Rédei. *Lacunary polynomials over finite fields*. American Elsevier Publishing Co., Inc., New York, N.Y., 1973.
- [58] Moses Richardson. On Finite Projective Games. *Proceedings Amer. Math. Society*, 7:458 – 465, June 1956.
- [59] Pierre Samuel. *Projective Geometry*. Springer-Verlag, 1988.

- [60] B. Segre. Sulle ovali nei piani lineari finite. *Rend. Accad. Naz. Lincei*, 17:141 – 142, 1954.
- [61] B. Segre. Ovals in a finite projective plane. *Canad. J. Math.*, 7:414 – 416, 1955.
- [62] B. Segre and U. Bartocci. Ovali ed altre curve nei piani di galois di caratteristica due. *Acta Arith.*, 8:423 – 449, 1971.
- [63] A. Shamir. How to share a secret. *Commun. ACM*, 22:612 – 613, 1979.
- [64] C. E. Shannon. A mathematical theory of communication. *Bell System Tech. J.*, 27:379 – 423, 623 – 656, 1948.
- [65] G. J. Simmons. A game theoretical model of digital message authentication. *Congressus Numerantium*, 34:413 – 424, 1982.
- [66] G. J. Simmons. An introduction to shared secret/shared control schemes. In G. J. Simmons, editor, *Contemporary Cryptology*, pages 441 – 497. IEEE Press, New York, 1992.
- [67] Gustavus Simmons. Sharply Focused Sets of Lines on a Conic in  $PG(2,q)$ . In *Congressus Numerantium*, volume 73, pages 181–204, January 1990.
- [68] D. R. Stinson. *Cryptography, Theory and Practice*. CRC Press, 1995.
- [69] J. A. Thas. Generalized Quadrangles and Flocks of Cones. *Europ. J. Combinatorics*, 8:441 – 452, 1987.
- [70] J. A. Thas. Generalized quadrangles of order  $(s, s^2)$ . *J. Comb. Theory (A)*, 79:223 – 254, 1997.
- [71] J. H. Van Lint. Coding, decoding, and combinatorics. In R. J. Wilson, editor, *Applications of Combinatorics*. Shiva, 1982.
- [72] W. D. Wallis. *Combinatorial Designs*. Marcel Dekker, Inc., 1988.
- [73] H. P. Williams. *Model Solving in Mathematical Programming*. Wiley, Chichester, 1993.