Conic Blocking Sets in Desarguesian Projective Planes

Leanne D. Holder

March 11, 2002

Abstract

Define a conic blocking set to be a set of lines in a Desarguesian projective plane such that all conics meet these lines. Conic blocking sets can be used in determining if a collection of planes in projective three-space forms a flock of a quadratic cone. We discuss trivial conic blocking sets and conic blocking sets in planes of small order. We provide a construction for conic blocking sets in planes of non-prime order, and we make additional comments about the structure of these conic blocking sets in certain planes of even order.

Key Words: conic blocking sets, flocks, cones

1 Introduction

Let Q be a quadratic cone in $\mathrm{PG}(3, q)$ with vertex V. Traditionally, a *flock* of Q is a partition of the points of $\mathrm{Q}\backslash\{V\}$ into q conics. Equivalently, we can say that a flock of Q is a set of q planes which intersect the quadratic cone in q disjoint conics. The simplest example of a flock is a *linear flock*, which is a flock consisting of q planes passing through a fixed line skew to the cone.

One of the most interesting features of flocks is that a large variety of other structures are related to flocks. For instance, independently, in 1976 M. Walker [7] and J. A. Thas [2] discovered that to each flock of an irreducible quadric of $\mathrm{PG}(3, q)$ there corresponds a translation plane of order q^2. In 1980, S. E. Payne [5] showed that given a set of q upper triangular 2×2 matrices over $\mathrm{GF}(q)$ of a certain type, known as a q-clan, there exists a generalized quadrangle of order (q^2, q). Then, in 1987 J. A. Thas [6] proved that to a q-clan there corresponds a flock of a quadratic cone of $\mathrm{PG}(3, q)$, and conversely. Hence, with each flock of a quadratic cone of $\mathrm{PG}(3, q)$ there corresponds a generalized quadrangle of order (q^2, q). The following year, Gevaert, Johnson, and Thas [3] showed that flocks of quadratic cones can be used to define translation planes. The strong connection between flocks and other geometrical structures leads us to introduce a new structure in the projective plane that may be used to determine the existence of certain flocks of quadratic cones.

In $\mathrm{PG}(2, q)$, a *conic blocking set* (CBS) is a set $\mathcal{B}$ of lines which meets every conic of $\mathrm{PG}(2, q)$. A CBS $\mathcal{B}$ is called *irreducible*, if for any line of $\mathcal{B}$ there is a conic intersecting $\mathcal{B}$ in just that line. A conic blocking set is a geometrical structure in the plane that is useful in determining if a collection of planes in projective 3-space form a flock of a quadratic cone. For instance, let F be a collection of q planes of $\mathrm{PG}(3, q)$ and V a point not in any plane of F. If the projection from V into any plane of F of the lines of intersection of the planes of F forms a CBS, then there does not exist a quadratic cone with vertex V having F as a flock. On the other hand, if this same projection does not form a CBS, then there exists a quadratic cone with vertex V having F as a flock.

For the remainder of this paper, we make the restriction that all CBSs consist of a set of concurrent lines through a specified point P. Then the *complement* of

a CBS $\mathcal{B}$, denoted $\mathcal{B}^c$, consists of the remaining lines through the point P. In the next section, we give some general results concerning existence of CBSs and CBSs of smallest size (*minimum CBSs*) in PG$(2,2)$ and PG$(2,3)$. In Section 3, we provide a nontrivial CBS construction that relies on results by J. A. Thas [6]. Section 4 identifies an irreducible CBS in PG$(2,2^{2n})$ given by the construction in Section 3. Also, we show that this irreducible CBS is projectively equivalent to a set of concurrent lines in the Baer subplane PG$(2,2^n)$. Finally, we end with open questions and concluding remarks related to the CBS construction given in Section 3.

2 General Results

Observe that in PG$(2,q)$, the $q+1$ lines through any point form an extremely trivial and uninteresting CBS. Furthermore, the set of lines, retained after removing a single line from this CBS, is still a CBS. The following lemma offers an existence of a less trivial CBS of smaller size.

Lemma 2.1 *Any set of $\frac{q+3}{2}$ (resp. $\frac{q+2}{2}$) concurrent lines in PG$(2,q)$ with q odd (resp. q even) form a CBS.*

Proof:

A simple counting argument shows that no conic can exist in $q+1-\frac{q+3}{2}=\frac{q-1}{2}$ concurrent lines. Therefore, any set of $\frac{q+3}{2}$ concurrent lines must be a CBS when q is odd.

A similar argument gives the desired result in PG$(2,q)$, q even.

■

We describe the CBSs in planes of orders 2 and 3, since they are completely classifiable.

Proposition 2.2 *A minimal CBS in PG$(2,2)$ consists of any pair of lines.*

Proof:

Trivial.

■

Proposition 2.3 *Any three concurrent lines form a minimal CBS in PG$(2,3)$.*

Proof:

By Lemma 2.1, any set of three or more concurrent lines form a CBS. If $\mathcal{B}$ is a CBS consisting of only two lines, then $\mathcal{B}^c$ 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 a conic. Since $\mathcal{B}^c$ contains a conic, $\mathcal{B}$ is not a CBS and no pair of lines in PG$(2,3)$ will form a CBS.

■

For p a prime, we let $\mathcal{F}$ denote GF(p), the prime subfield of an extension field $\mathcal{E} = \text{GF}(p^e) = \text{GF}(q)$ with subfield $\mathcal{K} = \text{GF}(p^d)$. In general, $\mathcal{K}$ is assumed to be a proper subfield of $\mathcal{E}$, unless otherwise specified. Let Tr denote the relative trace map $\text{Tr}_{\mathcal{E}/\mathcal{K}}$ from $\mathcal{E}$ onto $\mathcal{K}$ given by $\text{Tr}(t) = t + t^{p^d} + \cdots + t^{(p^d)^{k-1}}$ where $e = dk$ and $t \in \mathcal{E}$.

3 The Trace-Flock Construction

Finding CBSs consists of identifying a set of lines through a point such that all conics in PG$(2,q)$ have at least one secant or tangent in this set. For the CBS construction given in this section, we coordinatize PG$(2,q)$ (from GF(q)) so that $P = (0,1,1)$ is the point of concurrency. Although, $x = 0$ is a line through P, we are able to insure that $x = 0$ is not a line of the CBS. We will determine the slopes, $\bar{m}$, of the lines with equation $y = \bar{m}x + z$ such that every conic in PG$(2,q)$ meets these lines. Since the Kantor-Knuth flocks [6] are a nuisance to the CBS construction given in this section, we discuss some important properties of these flocks that cause the interference.

The q planes of a Kantor-Knuth flock have the equations

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

where m is a fixed nonsquare in $\mathcal{E}$ and σ is a non-identity automorphism of $\mathcal{E}$. The projection of the line of intersection of any two distinct planes, π_s and π_t of the Kantor-Knuth flock, to the plane with equation $w = 0$ is the line with equation $x = m(t - s)^{\sigma-1}z$. We refer to these projections as the KK-lines, and we observe that the number of KK-lines is equal to the size of the image set of $g(t) = t^{p^k-1}$, $1 \le k \le e-1$, $t \neq 0$. The following lemma determines the exact size of a set of KK-lines.

Lemma 3.1 *If $h : \mathcal{E}^* \to \mathcal{E}^*$ is given by $h(t) = t^{p^k-1}$ $1 \le k \le e-1$, then $|Image(h)| = \frac{p^e-1}{p^d-1}$, where $d = \gcd(k, e)$.*

Proof:

For $1 \le k \le e-1$, let $d = \gcd(k, e)$ and define $f_k(t) = t^{p^k}$ so that $h_k(t) = \frac{f_k(t)}{t} = t^{p^k-1}$, for $t \neq 0$. Since f_k is an automorphism of $\mathcal{E}$, f_k has a fixed field $\mathcal{K} = \mathrm{GF}(p^d)$. For $\lambda \neq 0$, it is easily seen that $h_k(t) = h_k(\lambda t)$ if and only if $\lambda \in \mathcal{K}$. That is, if and only if λ is in the fixed field of $f_k(t)$. Since there are $p^e - 1$ nonzero elements in $\mathcal{E}$, for each h_k, $\mathcal{E}^*$ is partitioned into blocks of size $p^d - 1$. Therefore, there are $\frac{p^e-1}{p^d-1}$ distinct values in the Image(h_k).

■

In 1987, J. A. Thas classified those flocks of a quadratic cone all of whose planes contain a common point. We restate his theorems in terminology useful for this paper.

Theorem 3.2 *[6] In $PG(3, 2^e)$, if the 2^e planes of a flock of a quadratic cone contain a common point, then the flock is linear.* ■

Similarly,

Theorem 3.3 *[6] In $PG(3, p^e)$, p an odd prime, if the p^e planes of a flock of a cone contain a common point, then the flock is either a linear or a Kantor-Knuth flock. The latter case occurring only if the common point is an exterior point of the cone.* ■

Lemma 3.4 *If $g : \mathcal{E}^* \to \mathcal{E}$ is given by $g(t) = \frac{Tr_{\mathcal{E}/\mathcal{K}}(t)-t}{t} = \frac{Tr(t)-t}{t}$ for $t \neq 0$, then $|Image(g)| = p^{e-d} + 1$.*

Proof:

To show that the size of Image(g) is $p^{e-d}+1$, we show $\mathcal{E}^*$ is partitioned into $p^{e-d}+1$ blocks: one of size $p^{e-d} - 1$ and p^{e-d} blocks of size $p^d - 1$, such that g is constant on each block.

Observe that $g(t) = g(\lambda t)$ if and only if $\lambda \mathrm{Tr}(t) = \mathrm{Tr}(\lambda t)$. If $\lambda \in \mathcal{K}^*$, then the condition is immediately satisfied. If $\lambda \notin \mathcal{K}^*$, then since the trace function is a homomorphism of $\mathcal{E}$ onto $\mathcal{K}$, the condition can only be satisfied if $\mathrm{Tr}(t) = 0$. Indeed, we have $g(t) = -1$ if and only if $\mathrm{Tr}(t) = 0$.

Since the relative trace function is an additive homomorphism from $\mathcal{E}$ onto $\mathcal{K}$, $|\ker(\mathrm{Tr})| = |\mathcal{E}|/|\mathcal{K}| = p^{e-d}$. Let $T_0 = \ker(\mathrm{Tr}) \setminus \{0\}$, so $|T_0| = p^{e-d} - 1$. We note that g is constant on the block T_0. If $t \notin T_0$, then there are $p^d - 1$ elements s such that $g(t) = g(s)$, namely the elements $s = \lambda t$ with $\lambda \in \mathcal{K}^*$. As $|\mathcal{E}^* \setminus T_0| = p^e - 1 - (p^{e-d} - 1) = p^{e-d}(p^d - 1)$, we see that g is constant on p^{e-d} blocks of size $p^d - 1$. These blocks together with T_0 give the required partition of $\mathcal{E}^*$.

■

We use the function g described in Lemma 3.4 to construct a set of concurrent lines $\{y = g(t)x + z \mid t \in \mathcal{E}^*\}$, which we refer to as the set of trace-flock lines (TF-lines). Lemma 3.4 gives us that there are $p^{e-d} + 1$ lines in a set of TF-lines, and in Lemma 3.1, we determined that there are $\frac{p^e-1}{p^d-1}$ lines in the set of KK-lines. Observe that the number of KK-lines equals the number of TF-lines only when $e = 2d$. In the next lemma, we show that when $e = 2d$, the KK-lines are projectively equivalent to the TF-lines.

Lemma 3.5 *Let q be an odd prime power and $g_f : GF(q^2)^* \to GF(q^2)$ be given by $g_f(t) = \frac{f(t)}{t}$, where f is any nontrivial additive function of $GF(q^2)$ over $GF(q)$. Then the set of lines $\{y = g_f(t)x + z \mid t \in GF(q^2)^*\}$ through $(0, 1, 1)$ is projectively equivalent to the KK-lines, that is, projectively equivalent to the set of lines $\{x = ms^{q-1}z \mid s \in GF(q^2)^*$, m a nonsquare$\}$ through $(0, 1, 0)$.*

Proof:

Any nontrivial additive function of $\mathrm{GF}(q^2)$ has the form $f(t) = \alpha t + \beta t^q$ with α, $\beta \in \mathrm{GF}(q^2)$, $\beta \neq 0$. Let $g_f(t) = \frac{f(t)}{t}$ and $h(t) = t^{q-1}$, $t \neq 0$. Clearly, $\mathrm{Image}(g_f)$ has the same size as $\mathrm{Image}(h)$, which is a cyclic subgroup of $\mathrm{GF}(q^2)$ of order $q + 1$. Let m be a fixed nonsquare in $\mathrm{GF}(q^2)$. It is straightforward to show that the projectivity given by

$$M = \begin{bmatrix} \frac{1}{\beta m} & \frac{\alpha}{\beta m} & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

maps $\{y = g_f(t)x + z \mid t \in \mathrm{GF}(q^2)^*\}$ to $\{x = m(1/t)^{q-1}z \mid m$ a fixed nonsquare$\}$, as required. ■

By setting $\alpha = \beta = 1$, we see from Lemma 3.5 that the set of TF-lines generated by

$g(t) = \frac{\mathrm{Tr}_{\mathrm{GF}(q^2)/\mathrm{GF}(q)}(t)-t}{t} = t^{q-1}$ is projectively equivalent to the set of KK-lines. The significance of this fact is highlighted in the proof of the next theorem and in Remark 3. We now have all the tools necessary to give the CBS construction.

Theorem 3.6 *If $d|e$ and $e > d$, then the set of lines through the origin with slopes in the set $\left\{ \frac{Tr_{\mathcal{E}/\mathcal{K}}(t)-t}{t} \mid t \in \mathcal{E}^* \right\}$ is a CBS of size $p^{e-d}+1$ in $PG(2,p^e)$, unless p is odd and $e = 2d$.*

Proof:

Embed $\mathrm{PG}(2,p^e)$ into $\mathrm{PG}(3,p^e)$ as $w = 0$. Let $f(t) = \mathrm{Tr}_{\mathcal{E}/\mathcal{K}}(t) - t$ and observe that f is an additive function. We have shown that the set of TF-lines given by $\mathcal{B} := \{y = g(t)x + z \mid g(t) = \frac{f(t)}{t}, t \in \mathcal{E}^*\}$ contains $p^{e-d}+1$ lines, and observe that $\mathcal{B}$ is a set of lines in the plane $w = 0$ through the point $(0,1,1,0)$. Consider the $p^e - 1$ planes of the form:

$$\pi_t \ : \ -f(t)x + ty - tz + w = 0,$$

with $t \in \mathcal{E}^*$.

Clearly, the point $(0,0,0,1)$ does not lie on any of these planes, and the point $(0,1,1,0)$ lie on all of these planes. Together with the plane $w = 0$, we have a set of p^e 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 $\mathcal{B}$. If there exists a conic $\mathcal{C}$ that misses $\mathcal{B}$, we can form a cone with vertex $(0,0,0,1)$ and base $\mathcal{C}$. These p^e planes then form a flock of this cone, and the planes of this flock contain the common point $(0,1,1,0)$. We examine this putative flock to show that $\mathcal{B}$ is a CBS. The cases of $p = 2$ and p an odd prime are handled separately.

If $p = 2$, Theorem 3.2 implies this flock is linear, that is $|\mathcal{B}| = 1$. But, $|\mathcal{B}| = 2^{e-d}+1 > 1$, so $\mathcal{C}$ does not exist and $\mathcal{B}$ is a CBS.

If p is an odd prime, we consider the two cases of $(0,1,1,0)$ being a common interior point to the cone and a common exterior point to the cone. If $(0,1,1,0)$ is a common interior point, then Theorem 3.3 implies that this flock is linear and therefore, $|\mathcal{B}| = 1$, contradicting $|\mathcal{B}| = p^{e-d}+1 > 1$. So, $\mathcal{C}$ cannot exist and $\mathcal{B}$ is a CBS. If $(0,1,1,0)$ is a common exterior point, then the same theorem implies that this flock is projectively equivalent to a Kantor-Knuth flock. But, we have shown that any flock

equivalent to a Kantor-Knuth flock produces a set of KK-lines of size $\frac{p^e-1}{p^d-1}$. Observe that $p^{e-d}+1 = \frac{p^e-1}{p^d-1}$ only when $e = 2d$. Hence, when $e \neq 2d$, $\mathcal{C}$ does not exist and again $\mathcal{B}$ is a CBS.

Thus, the trace-flock lines $\{y = [(\mathrm{Tr}_{\mathcal{E}/\mathcal{K}}(t) - t)/t]x + z \mid t \in \mathcal{E}^*\}$ form a CBS of size $p^{e-d}+1$ in $\mathrm{PG}(2, p^e)$, unless p is odd and $e = 2d$. ■

Remark 1. We used the specific function $g(t) = \frac{\mathrm{Tr}_{\mathcal{E}/\mathcal{K}}(t)-t}{t}$ to give the slopes of the lines in the CBS obtained by this trace-flock construction. It should be evident that this function is not unique for this type of CBS construction. When g' is an additive function divided by t, we can imitate the proof in the trace-flock construction by using g' instead of g, to form a CBS, as long as $1 < |\mathrm{Image}(g')| \neq \frac{p^e-1}{p^d-1}$.

Remark 2. The trace-flock construction, and even a generalized construction, such as the one described in Remark 1, does not give CBSs in $\mathrm{PG}(2, p)$, p prime. This can easily be seen by observing that the only additive function, up to scalar multiplication, is the identity. Hence, a generalized construction of the trace-flock construction fails to yield a CBS, since g' generates only one line for the CBS.

Remark 3. We showed in Lemma 3.5 that the trace-flock lines were projectively equivalent to the KK-lines when $\mathcal{E} = \mathrm{GF}(p^{2d})$ and $\mathcal{K} = \mathrm{GF}(p^d)$. Although the CBS construction provided in Theorem 3.6 does yield CBSs in $\mathrm{PG}(2, p^{2d})$, it cannot be used to generate CBSs of size $p^d + 1$ in $\mathrm{PG}(2, p^{2d})$.

Table 1 gives an indication of the sizes of the CBSs obtained by the trace-flock construction described in Theorem 3.6.

q	$p = 2$	p odd
p		
p^2	3	
p^3	5	p^2+1
p^4	5, 9	p^3+1
p^5	17	p^4+1
p^6	9, 17, 33	p^4+1, p^5+1
p^7	65	p^6+1
p^8	17, 65, 129	p^6+1, p^7+1
p^9	65, 257	p^6+1, p^8+1
p^{10}	33, 257, 513	p^8+1, p^9+1

Table 1: Sizes of CBSs given by the Trace-Flock Construction

Finally, we remark that the size of the CBSs produced by the trace-flock construction is an improvement over the size of the trivial CBSs described in Lemma 2.1. For a fixed $q = p^e$, when p is odd, the largest size of a CBS obtained by the trace-flock construction is always smaller than those CBSs constructed in Lemma 2.1. On the other hand, when p is even, the largest size of a CBS obtained by the trace-flock construction is the same as those CBSs constructed in Lemma 2.1. Now, when the exponent, e, on the order of the plane is prime, the trace-flock construction yields exactly one CBS. However, when e is composite, a variety of CBSs are obtained, always yielding an improvement over the sizes of the CBSs obtained by the construction described in Lemma 2.1. To emphasize this improvement, consider CBSs in $\mathrm{PG}(2, 5^3)$. The trace-flock construction gives a CBS of 26 lines whereas the trivial construction requires 64 lines for a CBS in $\mathrm{PG}(2, 5^3)$. Tables 2 and 3 highlight the CBS sizes constructed thus far.

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

Table 2: CBS sizes - q even

q	Trivial	Trace-Flock
p	$(p+3)/2$	
p^2	$(p^2+3)/2$	
p^3	$(p^3+3)/2$	
p^4	$(p^4+3)/2$	p^3+1
p^5	$(p^5+3)/2$	p^4+1
p^6	$(p^6+3)/2$	p^5+1, p^4+1
p^7	$(p^7+3)/2$	p^6+1
p^8	$(p^8+3)/2$	p^7+1, p^6+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

Table 3: CBS sizes - q odd

4 Irreducible CBSs in $\mathbf{PG}(2, 2^{2n})$

In this section, we restrict ourselves to the case where $n \geq 2$ and α is a primitive element of $\mathcal{E} = \mathrm{GF}(2^{2n})$, with $\mathcal{K} = \mathrm{GF}(2^n)$ a proper subfield of $\mathcal{E}$ and $\mathcal{F} = \mathrm{GF}(2)$ is

the prime subfield of $\mathcal{E}$. We show that the trace-flock construction yields an irreducible CBS in $\mathrm{PG}(2, 2^{2n})$, and this CBS is projectively equivalent to the set of lines through a point in the Baer subplane $\mathrm{PG}(2, 2^n)$.

With $n \geq 2$, we have that $|\mathcal{K}| \geq 4$. Hence, there is an element $\beta \in \mathcal{K}$ such that $\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\beta) = 1$, and for $0 \leq i \leq n-1$, $\beta^{2^i} = \beta^{2^{n+i}}$. Now, with $g(t) = \frac{\mathrm{Tr}_{\mathcal{E}/\mathcal{K}}(t)-t}{t} = t^{2^n-1}$, as defined in Lemma 3.4, the Image(g) is a cyclic subgroup of $\mathcal{E}^*$, with any element in Image(g) expressible as $\delta^k = \alpha^{(2^n-1)k}$, $k \in \mathbb{Z}_{2^n+1}$. Using the fact that $\delta^{k(2^n+1)} = 1$, it is simple to prove the following observation, which aids in the proof of Theorem 4.2.

Observation 4.1 *For i a positive integer, we have that $(1+\delta^k)^{-2^i} + (1+\delta^k)^{-2^{n+i}} = 1$.*

■

Using the projectivity given by,

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

it is straightforward to show that the CBS given by the trace-flock construction is projectively equivalent to the CBS, $\mathcal{B}' := \{y = \frac{\mathrm{Tr}_{\mathcal{E}/\mathcal{K}}(t)-t}{t}x \mid t \in \mathcal{E}^*\} = \{y = t^{2^n-1}x \mid t \in \mathcal{E}^*\}$, with point of concurrency $(0, 0, 1)$. We show $\mathcal{B}'$ is irreducible by showing that for every line l in $\mathcal{B}'$ there is a conic, with equation $Ax^2+Bxy+Cy^2+Dxz+Eyz+z^2 = 0$, that meets only l.

Theorem 4.2 *The CBS, $\mathcal{B}' = \{y = t^{2^n-1}x \mid t \in \mathcal{E}^*\} = \{y = \delta^k x \mid 0 \leq k \leq 2^n, \delta = \alpha^{2^n-1}\}$, is irreducible in $PG(2, 2^{2n})$.*

Proof:

Let $\beta \in \mathcal{K}$ such that $\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\beta) = 1$. Consider the quadrics $Q_m(x, y, z)$ with equations:

$$x^2 + \delta^{-m}\beta^{-1/2}xy + \beta^{-1/2}xz + \delta^{-m}\beta^{-1/2}yz + z^2 = 0,$$

where $m \in \mathbb{Z}_{2^n+1}$. The nucleus of Q_m is $\left(\delta^{-m}\beta^{-1/2}, \beta^{-1/2}, \delta^{-m}\right)$ and observe that $Q_m(\delta^{-m}\beta^{-1/2}, \beta^{-1/2}, \delta^{-m}) = \delta^{-2m} \neq 0$. Hence, Q_m is nondegenerate and therefore is a conic. We show that when $k = m$, the line $y = \delta^k x$ is a tangent line to Q_m, and for all $k \in \mathbb{Z}_{2^n+1} \setminus \{m\}$ the line $y = \delta^k x$ is exterior to Q_m. For the line $y = \delta^k x$ of $\mathcal{B}'$ to

meet Q_m, we must have that

$$(1+\delta^{k-m})x^2 + \beta^{-1/2}(1+\delta^{k-m})xz + z^2 \quad = \quad 0 \tag{1}$$

has a solution.

When $k = m$, there is exactly one solution to (1), and the line $y = \delta^m x$ is a tangent line to Q_m.

Let $k - m = j \neq 0$. To show that the line $y = \delta^k x$ does not meet Q_m, we examine the absolute trace of

$$\frac{1+\delta^j}{\left[\beta^{-1/2}(1+\delta^j)\right]^2} = \frac{\beta}{1+\delta^j}.$$

Equation (1) has a solution if and only if this absolute trace is 0. Assume, for the sake of attaining a contradiction, that $\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\frac{\beta}{1+\delta^j}) = 0$. Then

$$\begin{aligned}
\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\beta(1+\delta^j)^{-1}) = 0 \quad \Leftrightarrow \quad & \beta(1+\delta^j)^{-2^0} + \beta^2(1+\delta^j)^{-2^1} + \cdots \\
& + \beta^{2^{n-1}}(1+\delta^j)^{-2^{n-1}} + \beta^{2^n}(1+\delta^j)^{-2^n} + \\
& \beta^{2^{n+1}}(1+\delta^j)^{-2^{n+1}} + \cdots \\
& + \beta^{2^{2n-1}}(1+\delta^j)^{-2^{2n-1}} = 0 \\
\Leftrightarrow \quad & \sum_{i=0}^{2^{n-1}} \beta^{2^i}\left[(1+\delta^j)^{-2^i} + (1+\delta^j)^{-2^{n+i}}\right] = 0 \\
\Leftrightarrow \quad & \sum_{i=0}^{2^{n-1}} \beta^{2^i} = 0 \\
\Leftrightarrow \quad & \mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\beta) = 0.
\end{aligned}$$

However, β was chosen so that $\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\beta) = 1$. Thus, $\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\frac{\beta}{1+\delta^j}) = 1$ and all lines of the form $y = \delta^k x$, $k \neq m$, are exterior to Q_m. Since the removal of any line l from $\mathcal{B}'$ results in $\mathcal{B}'$ no longer being a CBS, $\mathcal{B}'$ is an irreducible CBS in $\mathrm{PG}(2, 2^{2n})$.

■

With the aid of the following lemma, we can show that the CBS $\mathcal{B}' = \{y = \delta^k x \mid k \in \mathbb{Z}_{2^n+1}\}$ is projectively equivalent to the set of lines in the Baer subplane $\mathrm{PG}(2, 2^n)$ of $\mathrm{PG}(2, 2^{2n})$ through the point $(0, 0, 1)$.

Lemma 4.3 *The element*

$$\omega = \frac{(\delta^j + \delta)(1+\delta^2)}{(1+\delta)(\delta^j + \delta^2)} \in \mathcal{E}^*$$

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

Proof:

Observe that $\delta^k = \alpha^{(2^n-1)k}$ where α is a primitive element of $\mathcal{E}$, and so $\left[\delta^k\right]^{2^n} = \delta^{-k}$. Using this observation and a series of algebraic manipulations, it can be shown that $\omega^{2^n-1} = 1$. Hence, $\omega \in \mathcal{K}^*$.

■

Theorem 4.4 *The lines* $\bar{\mathcal{B}} := \{y = mx \mid m \in \mathcal{K}\} \cup \{x = 0\}$ *form an irreducible CBS in* $PG(2, 2^{2n})$.

Proof:

We show that $\bar{\mathcal{B}}$ is an irreducible CBS in $\mathrm{PG}(2, 2^{2n})$ by finding a projectivity in $\mathrm{PGL}(3, 2^{2n})$ that maps the irreducible CBS $\mathcal{B}'$ given in Theorem 4.2 to $\bar{\mathcal{B}}$. Consider the element

$$M = \begin{bmatrix} \frac{1}{1+\delta} & \frac{\delta}{1+\delta} & 0 \\ \frac{1}{1+\delta^2} & \frac{\delta^2}{1+\delta^2} & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

in $\mathrm{PGL}(3, 2^{2n})$. It is straightforward to verify that M fixes $(0, 0, 1)$. It is also simple to verify that M maps the line $y = x$ in $\mathcal{B}'$ to the line $y = x$ in $\bar{\mathcal{B}}$, the line $y = \delta x$ in $\mathcal{B}'$ to the line $y = 0$ in $\bar{\mathcal{B}}$, and the line $y = \delta^2 x$ in $\mathcal{B}'$ to the line $x = 0$ in $\bar{\mathcal{B}}$.

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

$$\begin{bmatrix} \frac{1}{1+\delta} & \frac{\delta}{1+\delta} & 0 \\ \frac{1}{1+\delta^2} & \frac{\delta^2}{1+\delta^2} & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} \delta^j \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{(\delta^j+\delta)(1+\delta^2)}{(1+\delta)(\delta^j+\delta^2)} \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \omega \\ 1 \\ 0 \end{bmatrix}.$$

From Lemma 4.3, $\omega \in \mathcal{K}^*$, therefore ω is of the form $\alpha^{(2^n+1)k}$, $k \neq 0$. Hence, M maps the lines in $\mathcal{B}'$ to distinct lines in $\bar{\mathcal{B}}$, which are the Baer lines through the point $(0, 0, 1)$ in $\mathrm{PG}(2, 2^n)$. Thus, $\bar{\mathcal{B}}$ is projectively equivalent to $\mathcal{B}'$, and we have that $\bar{\mathcal{B}}$ is an irreducible CBS in $\mathrm{PG}(2, 2^{2n})$.

■

By using two projectivities, we have shown that the CBS given by the trace-flock construction is irreducible and projectively equivalent to the set of lines through a point in a Baer subplane of $\mathrm{PG}(2, 2^{2n})$.

5 Concluding Remarks

In this section we elaborate on a few open questions brought to light during this research and highlight some results brought to life during our stint of working with conic blocking sets.

The sizes of the smallest conic blocking sets have been determined for planes up to order 2^7 and 5^3, when q is even and odd respectively. By utilizing optimization techniques, L. D. Holder and G. Kochenberger [4] have also identified CBSs of small size for planes of order less than 199 and 2^{10}, for q odd and even, resp. In a forthcoming paper, we present a CBS construction for planes of order q^{2n}, which gives an upper bound on the size of minimum conic blocking sets. These preliminary results pertaining to conic blocking sets can be found in [4].

In the introduction, we mentioned that CBSs can be used to determine if a collection of planes form a flock of a quadratic cone. In this paper, we explored the structure and construction of a CBS rather than focusing on using CBSs to identify flocks of quadratic cones. W. E. Cherowitzo explores the concept of building a star flock using the function given in Lemma 3.4 in his Flocks of Cones Web Page [1].

In Remark 1, we commented that the trace-flock CBS construction could be generalized to an additive-flock CBS construction. This generalization is made by modifying the function g used in the trace-flock construction to be of the form $f(t)/t$, where f is an additive function of t. A computer search in fields of order $\leq p^e$, for p small and $e \leq 5$ generated all possible image sets of such $f(t)/t$. In all the fields checked, the function $f(t)/t$ used in the trace-flock construction yielded the smallest image set. It seems reasonable to conjecture that the trace-flock construction yields the smallest CBS of all possible additive-flock constructions.

In Remark 3, we discussed the Kantor-Knuth flocks interfering with the trace-flock construction yielding CBSs of size $p^d + 1$ in $\mathrm{PG}(2, p^{2d})$. It is doubtful that generalizing the trace-flock construction in $\mathrm{PG}(2, p^{2d})$ will generate a CBS smaller than $p^d + 1$.

Another matter is the open problem of the irreducibility of the conic blocking sets given by the trace-flock construction. We showed that when $q = 2^{2n}$, then the CBSs in $\mathrm{PG}(2, q)$ formed by the trace-flock construction were irreducible. It remains to be determined if the CBSs, given by the trace-flock construction, in the remaining planes

are irreducible.

Acknowledgments

I am most grateful to Bill Cherowitzo for improving the original proof of Theorem 3.4 and for his comments throughout all phases of this paper. Also, special thanks to Stan Payne for making time to proof read my work.

References

[1] W. E. Cherowitzo. *Flocks of Cones*. World Wide Web, `http://www-math.cudenver.edu/~wcherowi/research/flocks.html`, 1998 - 2001.

[2] J. C. Fisher and J. A. Thas. Flocks in PG(3,q). *Math. Z.*, 169:1 – 11, 1979.

[3] H. Gevaert, N. L. Johnson, and J. A. Thas. Spreads covered by reguli. *Simon Stevin*, 62:51–62, 1988.

[4] L. D. Holder. *On Blocking Sets of Conics*. PhD thesis, Univeristy of Colorado at Denver, 2001.

[5] S. E. Payne. Generalized quadrangles as group coset geometries. *Cong. Numer.*, 29:717–734, 1980.

[6] J. A. Thas. Generalized Quadrangles and Flocks of Cones. *Europ. J. Combinatorics*, 8:441 – 452, 1987.

[7] M. Walker. A class of translation planes. *Geom. Dedicata*, 5:135–146, 1976.

Leanne Holder

The University of Mississippi

Department of Mathematics

University, MS 38677 USA