

CRYPTOGRAPHY BASED ON DETERMINING SETS

Christine Exley

submitted in partial fulfillment of the requirements for Honors in
Mathematics at the University of Mary Washington

Fredericksburg, Virginia

May 2009

This thesis by **Christine Exley** is accepted in its present form as satisfying the thesis requirement for Honors in Mathematics.

DATE

APPROVED

Keith E. Mellinger, Ph.D.
thesis advisor

Jeffrey Edmunds, Ph.D.
committee member

Suzanne Sumner, Ph.D.
committee member

Contents

1	Introduction and preliminaries	1
1.1	Finite projective planes	1
1.2	Blocking sets	2
1.3	How do we create a cryptosystem?	4
1.4	Determining sets	6
2	Constructions of determining sets with one conic and two lines	6
2.1	Case One: $\mathcal{S}_{TT\mathcal{E}}$	8
2.2	Case Two \mathcal{S}_{SSE}	12
2.3	Case Three: \mathcal{S}_{SSC}	13
2.4	Case Four: $\mathcal{S}_{SS\mathcal{L}}$	15
2.5	Remaining cases	16
2.6	Summary of all cases	19
3	Construction of a determining set with $3q - 4$ points	20
3.1	The set \mathcal{ME}	20
3.2	Are the three conditions of the candidates for X' necessary?	24
3.3	Proof that there is always at least one Candidate for X'	25
3.4	Proof that \mathcal{ME} is a determining set for all lines	28
4	Constructions of determining sets with two conics and two lines	29
5	Conclusions	34
5.1	Why some determining sets can not have fewer than $3q - 3$ points	35
5.2	New ideas	35
	References	37

List of Figures

1	Triangle	3
2	Vertex-less triangle	4
3	\mathcal{S}_{TTE}	9
4	Secant lines through \mathcal{S}_{TTE}	9
5	\mathcal{S}_{SSE}	12
6	\mathcal{S}_{SSC}	14
7	\mathcal{S}_{SSI}	15
8	$\mathcal{S}_{\kappa\kappa\epsilon}$	17
9	\mathcal{S}_{TSE}	18
10	\mathcal{S}_{TSC}	18
11	\mathcal{S}_{TKE}	19
12	\mathcal{S}_{SKE}	20
13	Important points to the set \mathcal{ME}	22
14	Possible location of X'	22
15	The set \mathcal{ME} with possible X'	23
16	\mathcal{S}_{TSC1}	26
17	Two conics and two lines	31
18	The set \mathcal{T}	33

List of Tables

1	Some possible constructions of determining sets with one conic and two lines	8
2	\mathcal{S}_{TTE} incidence results	11
3	Possible constructions of determining sets with one conic and two lines . . .	21
4	Set \mathcal{ME} incidence results	29
5	The set \mathcal{T} incidence results	34

Acknowledgment

With just a few months until graduation, reflection on the past four years is inevitable. I am extremely grateful to all of my professors, especially a few who have quite literally been there from the start. In fact, everyone on my mathematics honors thesis committee was not only instrumental during my time at the University of Mary Washington, for they were also instrumental to me choosing to attend UMW. It is for both of these reasons that I would like to extend my sincere gratitude and take a moment to highlight them.

I first met Dr. Sumner as a nervous high school student being interviewed for the Washington Scholarship. While I am not convinced that it was my eloquent interview that led to the scholarship being awarded, I am grateful for the faith she had in me and that I chose to accept it. The Washington Scholarship not only prompted one of my best decisions (i.e., to attend UMW), for it also has opened the doors to graduate school. Perhaps just as noteworthy, Dr. Sumner successfully got me through my *only* history class during college, the history of math. Since then, I have enjoyed returning to history of math as a presentation grader and our several get-togethers as part of Pi Mu Epsilon. I am also very appreciative for the time she took to read through this very long thesis, and, as a result, the many grammatical errors that no longer exist.

I still remember sitting at my dining room table when Dr. Edmunds called to convince me that I would enjoy UMW much more than the other colleges on my list. As a high school senior, I was floored that someone with a doctorate actually called to talk to me! And, as perhaps the leading question asker throughout all of my classes with Dr. Edmunds, I certainly made him live up to his promise that UMW would be my best choice. My freshman year, I discovered a new level of love for math during his multivariable calculus class. Later, I learned to respect math as I survived two semesters of his real analysis class. In fact, the former convinced me to become a math major, and the latter confirmed that I acutally would graduate as a math major. As my professor for several classes and my math advisor, Dr. Edmunds has spent countless hours helping me navigate through math problems, scheduling and perhaps most importantly—my plan for the future. I know that I truly miss the “throne” in Dr. Edmunds office, where so many of us have sat as we waited for Dr. Edmunds to explain our question of the moment.

I sat in on one crazy day in Dr. Mellinger’s abstract algebra class as a high school senior. Despite the fact that I understood little to nothing about the math they were discussing, the lively (and rather funny) atmosphere as well as the obviously close relationship between the students and Dr. Mellinger sold me on my choice to attend UMW. Although scheduling then prevented me from being in any of his traditional classes, I was fortunate enough to have two independent studies with him. My first independent study led by Dr. Mellinger sparked my interest in cryptography, which then opened the doors to a competitive internship with

a leading agency in this field. My second independent study with Dr. Mellinger yielded this thesis. As my math thesis advisor, Dr. Mellinger took the time to teach me finite geometry and then proposed his idea for my thesis. Since I immediately loved the idea, we began working at it. While we had many exciting discoveries along the way, it was the discovery of the determining set \mathcal{ME} that stands above the rest. It all started over Christmas break when I was putting (what I thought were) the final edits on my thesis. I could not figure out why I could not remove an additional point from the set \mathcal{S}_{STC} , so I made a note to ask Dr. Mellinger when I returned to UMW in January. To my surprise, Dr. Mellinger too could not see why we could not remove an additional point from the set \mathcal{S}_{TSC} . Then, with a huge diagram of the set \mathcal{S}_{STC} on Dr. Mellinger's whiteboard and on my bedroom door for the next few weeks, we scrutinized this set. Many times, we almost proved that we could remove an additional point only to discover some new constraint. But, eventually, a great day arose when we both were convinced that we could remove an additional point from the set \mathcal{S}_{STC} . The resulting set \mathcal{ME} is the most exciting breakthrough of this paper! By now, you may be wondering why this discovery was so amazing. Well, read on and then you too will be able to understand.

Abstract

Using the protocol developed by Lynn Batten, this paper explores the construction of *determining sets* in finite projective planes that form the basis for secure cryptosystems. In short, if \mathcal{D} is a determining set in π , then every line in π has a different intersection pattern with \mathcal{D} and thus can be uniquely identified. In other words, if we let the lines in a finite projective plane represent different characters of the cryptosystem, we can recover these characters when encrypted by identifying their different intersection patterns with \mathcal{D} .

We construct several determining sets with two lines and one conic and one determining set with two lines and two conics. While many of these determining sets contain fewer points than the vertex-less triangle (i.e., $3q - 3$ points, which we use as the threshold for an interesting determining set), such a reduction in size normally prevents the set from being a determining set for *all* lines in $PG(2, q)$. On the other hand, most determining sets for all lines in $PG(2, q)$ can not be reduced to a size of fewer than $3q - 3$ points. Thus, our most interesting discovery is a determining set for all lines in $PG(2, q)$ that only requires $3q - 4$ points. This determining set is named \mathcal{ME} .

1 Introduction and preliminaries

This thesis researches relationships between finite geometry and cryptography. In particular, we study a cryptographic protocol that was discovered by Lynn Batten in 2000 and was patented shortly thereafter (the patent can be viewed freely on the Internet¹).

1.1 Finite projective planes

Our work relies on the structure of an object in discrete mathematics called a finite projective plane. More details about finite planes can be found in the foundational book by Hughes and Piper [3]. A more thorough treatment of finite planes appears in the more comprehensive book by Hirschfeld [2]. We provide some brief background information that is relevant to our discussion.

Definition 1.1. *A **finite projective plane** is a finite set of points along with a set of subsets of these points, known as lines, satisfying the following three axioms.*

1. *Every two distinct points determine a unique line.*
2. *Every two distinct lines determine a unique point.*
3. *There exist four points, no three of which are collinear.*

For this project, we work with a certain class of finite projective planes that are constructed from finite fields. A *finite field* contains a finite and prime power number of elements, which is often referred to as the order of the finite field. Note that a finite field of order q is denoted $GF(q)$. Also, all algebraic operations in $GF(q)$ are carried out modulo p where $q = p^k$ for some integer k .

We now describe how to obtain a finite projective plane from a finite field. Let V be a 3-dimensional vector space whose coordinates are taken from $GF(q)$. We define points to be the 1-dimensional subspaces of V , and lines to be the 2-dimensional subspaces of V . One can easily check that the axioms above are satisfied. We use the symbol π to represent $PG(2, q)$ (the finite projective geometry of dimension 2 and order q), which is the finite projective plane obtained from this construction. One can use elementary counting techniques to prove the statements in Proposition 1.2.

Proposition 1.2. *Let π be the finite projective plane of order q . Then,*

1. *Every line in π contains $q + 1$ points.*
2. *Every point in π has $q + 1$ lines through it.*

¹<http://www.patentstorm.us/patents/6075864/description.html>

3. The total number of lines and the total number of points in π is $q^2 + q + 1$.

In order to study objects in π , we will need to find a way to represent points and lines using coordinates. Just as we use ordered pairs and linear equations to represent points and lines of \mathbb{R}^2 , we need a representation for points and lines of π . First of all, we represent points as (a, b, c) . Since points are defined to be 1-dimensional subspaces, we have a uniqueness of representation problem. For instance, the 1-dimensional subspace spanned by $(1, 0, 1)$ is the same as the 1-dimensional subspace spanned by $(2, 0, 2)$. Thus, we only use **normalized vectors**.

Definition 1.3. A *normalized vector* is a non-zero vector whose first (from the left) non-zero coordinate is equal to 1. The set of all normalized vectors provide a unique representation for the points of a projective space.

Thus, in the case of points in π , there are only three possible forms of all points, which are listed below:

- $(0, 0, 1)$
- $(0, 1, a)$ where $a \in GF(q)$
- $(1, a, b)$ where $a, b \in GF(q)$

Note that any point not already in normalized form can be *normalized* by multiplying all of its coordinates by some factor k in $GF(q)$ so that the first (from the left) non-zero coordinate is equal to 1.

Now, just as points can be represented with normalized vectors, so too can lines. That is, any line is represented by a 2-dimensional subspace. We use the orthogonal complement of such a space to represent it. So, normalized vectors can be used to represent both points and lines. In π , we use the notation $[x, y, z]$ for a line. In other words, parentheses are used for points, and square brackets are used for lines. It immediately follows that the point (a, b, c) is on the line $[x, y, z]$ if and only if $(a, b, c) \cdot [x, y, z] = 0$, that is, $ax + by + cz = 0$.

1.2 Blocking sets

For this paper, it is also important to understand how a set of points in π can create a **blocking set**, which is defined as follows.

Definition 1.4. An *n-fold blocking set* in π is a subset of its points, denoted \mathcal{B} , such that every line in π intersects \mathcal{B} in at least n points. In general, note that a blocking set is defined as a 1-fold (or greater) blocking set.

We will now construct examples of blocking sets.

Example of a 2-fold blocking set: In π , a triangle is a 2-fold blocking set. Consider the triangle composed of three lines, l_1 , l_2 and l_3 , that intersect at points P , Q and R as shown below in Figure 1. We know that any two lines determine a unique point (i.e. intersect). Thus, if some line m (not equal to l_1 , l_2 or l_3) does not intersect with points P , Q or R , then m intersects with \mathcal{B} in three distinct points, that is, one point on l_1 , l_2 and l_3 . However, if m does intersect with point P (as illustrated in Figure 1 with a dotted line), then it must intersect with l_1 in a point not equal to P . A similar result is true if m intersects with Q or R . In short, in these cases, m intersects with \mathcal{B} in two distinct points. Thus, all lines in π intersect \mathcal{B} in at least two points, proving that \mathcal{B} is a 2-fold blocking set.

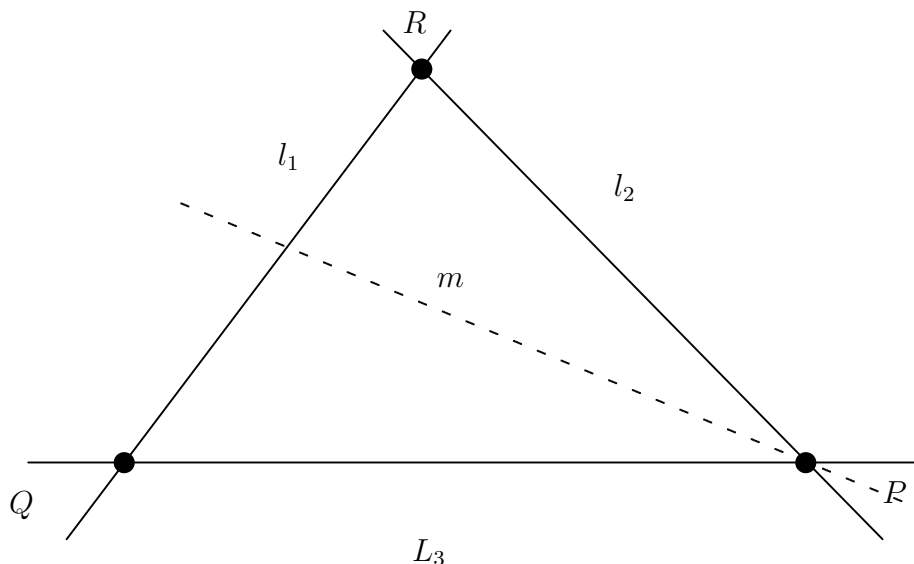


Figure 1: Triangle

Example of a semioval blocking set: Before I explain such an example, we first need to define a semioval.

Definition 1.5. A non-empty set of points \mathcal{S} of π is said to be a **semioval** if for every point P in \mathcal{S} , there exists a unique line l in π such that $l \cap \mathcal{S} = P$. That is, every point in a semioval has a unique tangent line (i.e., a line that only intersects the semioval in that point).

For our purpose, finding a set that is both a blocking set and a semioval would be valuable, for such a set can form the basis of an interesting and secure cryptosystem (through a protocol explained later). An example of a semioval blocking set is the *vertex-less triangle*. That is,

consider three non-concurrent lines, l_1, l_2 and l_3 , and remove each of the three intersection points, P, Q and R . If a line in π does not intersect any of the vertices, then it has three points of intersection with the vertex-less triangle. However, now consider lines in π that do intersect one of the vertices. It is clear that these lines intersect the vertex-less triangle in exactly one unique point; as shown in the Figure 2, all lines through P, Q or R intersect the vertex-less triangle in different points on l_1, l_2 or l_3 , respectively. It follows that every point in the vertex-less triangle has a unique tangent through it. So, the vertex-less triangle forms a semioval, and by the previous example, is a blocking set.

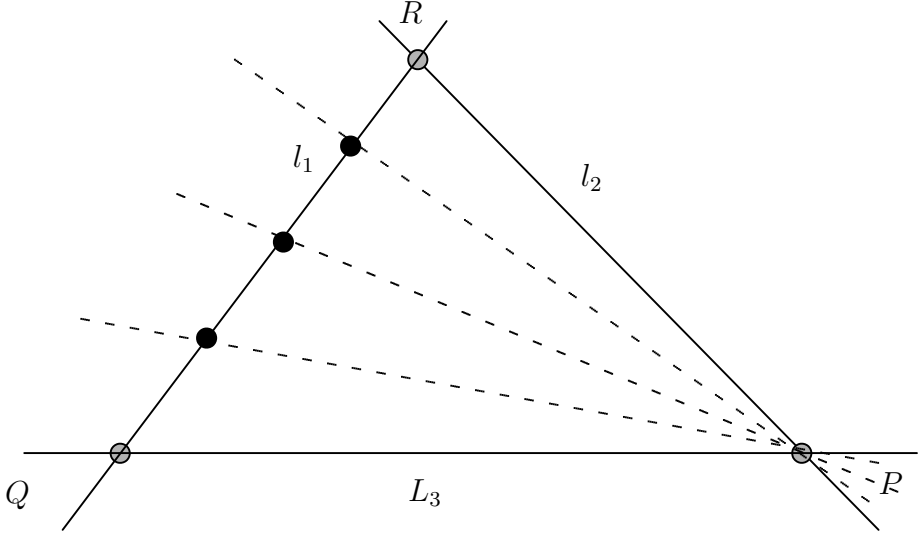


Figure 2: Vertex-less triangle

1.3 How do we create a cryptosystem?

Since the basis for the constructions of our cryptosystem comes from Lynn Batten’s work that was mentioned in Section 1, we first discuss her cryptosystem. Although her cryptosystem can hold for any d -blocking set where $d \geq 2$, we will only discuss her cryptosystem that calls for a two-fold blocking set in π , called \mathcal{B} . However, before we explain this cryptosystem, note that the following notations will be used.

- \mathcal{L} is the finite set of plaintexts where each needed character to form the plaintext corresponds to some line l in π .
- \mathcal{C} is the finite set of ciphertexts.
- \mathcal{P} is the finite set of points in π .

Using these notations, form the **incidence matrix**, M , with the rows labeled with the lines $l_1, l_2, \dots, l_{q^2+q+1}$, and the columns labeled with the points $p_1, p_2, \dots, p_{q^2+q+1}$. Recall from Proposition 1.2 that there are $q^2 + q + 1$ lines and points in π , so this incidence matrix is a square matrix of size $(q^2 + q + 1) \times (q^2 + q + 1)$. Let $M_{i,j}$ represent the $(i, j)^{th}$ entry in M . If the line l_i contains the point p_j , then we put a 1 in position (i, j) . Else, we put a 0 in this position. Hence, M is a (0,1)-matrix. We will not be performing operations on the entries of this matrix. Hence, the symbols we use are really arbitrary.

We can effectively think of M as the union of two disjoint incidence matrices, M_B and $M_{\pi \setminus B}$. Let M_B be the incidence matrix defined by only the points P_i that are in the blocking set \mathcal{B} , together with all of the lines on the space. Then, by Definition 1.4, we know that each row, l_i contains at least two 1s that correspond to the intersection points of the line l_i with the blocking set \mathcal{B} . And, by Definition 1.1, we know that these two points uniquely determine the line (or row), l_i . Let $M_{\pi \setminus B}$ be the incidence matrix of all the other points P_i that are not in \mathcal{B} and all of the lines.

Now, we form a cryptosystem as follows. Alice wants to send her message, m' , to Bob, using the plaintext in set \mathcal{L} . We first require a set of keys $(\mathcal{B}, \rho, \sigma)$ where

- \mathcal{B} is the blocking set in π ,
- ρ is a cipher on the columns of M_B , and
- σ is a cipher on the columns of $M_{\pi \setminus B}$.

To have a secure cryptosystem, make the following information available as follows.

- M is made available to the public.
- \mathcal{B} and ρ are known to both Alice and Bob.
- σ is known only to Alice (i.e. σ is private).

Let us first assume that Alice, the transmitter, wants to send a one character message, m' , that corresponds to l . To do so, Alice applies ρ to the entries in l corresponding to the points in \mathcal{B} and σ to the entries in l corresponding to the points of $\pi \setminus B$. Alice sends the corresponding encrypted message, c , to Bob. After Bob receives c , he then applies ρ^{-1} to all the entries in the received vector (since Bob, does not know which line Alice sent) that are in the positions of M_B . Note that Bob can do this since ρ and \mathcal{B} are known to Bob, as well. Subsequently, Bob now knows all of the decrypted values for all of the entries in the vector in the positions of M_B . Since \mathcal{B} is a 2-fold block set, there are two points of incidence in M_B . Thus, Bob can use these two points that uniquely determine a line and the public M to determine to which line the message corresponds. Bob then can recover m' . However, the

public, who does not know \mathcal{B} nor ρ cannot recover m' without a brute force search through all lines. For large values of q , this becomes computationally infeasible.

Alice can send a message with multiple characters by sending a stream of one character messages (i.e. vectors). Similarly, Bob can decrypt this string to uncover the original message in the same manner as explained above.

Expanding from Batten's above cryptosystem, the goal of this paper is to form cryptosystems based off of determining sets formed from lines and conics in a finite projective plane. In particular, a cryptosystem will be defined by how lines in π intersect with certain sets of points.

1.4 Determining sets

The geometric idea used in the cryptographic protocol described above is that of a 2-fold blocking set. However, we observe that this geometric idea has a nice generalization. As long as each line of the plane can be uniquely recovered, the protocol will still be effective. This leads us to the definition of a *determining set* which was first studied in [1].

Definition 1.6. *Let \mathcal{D} be a subset of π . Then \mathcal{D} is called a **determining set** of π if for any two distinct lines l_i and l_j of π , $\mathcal{D} \cap l_i \neq \mathcal{D} \cap l_j$.*

In return, note that if \mathcal{D} is a **determining set** in π , then every line in π has a different intersection pattern with \mathcal{D} (note that this definition differs slightly from the one given in [1]). Thus, we can allow these different intersections to identify the lines. A simple example of a cryptosystem would then be to allow each specific line to represent a given character. Then, since the intersection of each line with points in \mathcal{D} would be different, we could use the incidence matrix of all lines and all points in π to recover the characters as explained in Section 1.3.

The remainder of this thesis is about the construction of previously unknown determining sets that can, in return, be used to create new cryptosystems. Note that the following sections do not explain how these determining sets are used to create new cryptosystems since the above protocol can be used for all constructions. Our tools will involve the geometry of lines and conics in the finite projective plane π .

2 Constructions of determining sets with one conic and two lines

Let \mathcal{C} be the conic of π defined by the quadratic form $y^2 = xz$. Before we construct new examples of determining sets, we consider how lines intersect a conic. This will create three

classes of lines that will be useful in our constructions.

Definition 2.1. A *skew line*, a *tangent line* and a *secant line* intersect \mathcal{C} in no points, exactly one point or exactly two points, respectively.

Note that \mathcal{K} , \mathcal{T} and \mathcal{S} represent the set of all skew, tangent and secant lines, respectively. Also \mathcal{L} represents the set of all lines. Using elementary counting techniques and Proposition 1.2, we also know that the number of types of lines in π is as follows.

1. $|\mathcal{K}| = \frac{q(q-1)}{2}$
2. $|\mathcal{T}| = q + 1$
3. $|\mathcal{S}| = \frac{q(q+1)}{2}$
4. $|\mathcal{L}| = q^2 + q + 1$

The points of π can similarly be characterized relative to the conic, \mathcal{C} . One can easily count the number of non-conic points that lie on tangent lines and this amounts to a total of $\frac{q(q+1)}{2}$ points. Hence, not all points of π lie on a tangent line. The points that do lie on a tangent line are called *external points*, and those that do not lie on a tangent line are called *internal points*. Let \mathcal{E} and \mathcal{I} represent the sets of external and internal points, respectively. It then follows that

1. $|\mathcal{E}| = \frac{q(q+1)}{2}$
2. $|\mathcal{C}| = q + 1$
3. $|\mathcal{I}| = \frac{q(q-1)}{2}$

All of the constructions in this section will involve one conic, \mathcal{C} , and two lines, l_1 and l_2 . The intersection point of l_1 and l_2 will be referred to as point P . As point P shows to be critical to the construction of these sets, there is one last important counting note about point P . In particular, we want to consider the skew lines to \mathcal{C} that intersect P .

1. If $P \in \mathcal{C}$ (i.e., on \mathcal{C}), there are no skew lines to \mathcal{C} that intersect P .
2. If $P \in E$ (i.e., external to \mathcal{C}), there are exactly $\frac{q-1}{2}$ skew lines to \mathcal{C} that intersect P .
3. If $P \in I$ (i.e., internal to \mathcal{C}), there are exactly $\frac{q+1}{2}$ skew lines to \mathcal{C} that intersect P .

While case (1) is obvious since P is on \mathcal{C} and thus no lines through P can be skew to \mathcal{C} , case (2) and case (3) require a short discussion. For case (2), we assume that P is external to \mathcal{C} . It can easily be shown that there exist two distinct lines through P that are tangent to \mathcal{C} ,

say at points Y_1 and Y_2 . Then, of the remaining $q - 1$ points on \mathcal{C} , there exist secant lines to \mathcal{C} through P that hit a unique pair of points on \mathcal{C} . That is, there are $\frac{q-1}{2}$ secant lines to \mathcal{C} through P . Since there are a total of $q + 1$ lines through P , the number of skew lines to \mathcal{C} through P then must be $\frac{q-1}{2}$. For case (3), we assume the P is internal to \mathcal{C} . Then, by definition there can be no tangent lines to \mathcal{C} through P . For the same reasons explained above, there would then be $\frac{q+1}{2}$ secant lines to \mathcal{C} through P . Thus, there must be $\frac{q+1}{2}$ skew lines to \mathcal{C} through P .

All possibilities of how the sets can be constructed and corresponding locations of P are shown in Table 1. Note that the subscript of \mathcal{S} correlates with the construction of the set.

Case	$l_1 \cap \mathcal{C}$	$l_2 \cap \mathcal{C}$	location of P
$\mathcal{S}_{\mathcal{T}\mathcal{T}\mathcal{E}}$	tangent	tangent	external
$\mathcal{S}_{\mathcal{S}\mathcal{S}\mathcal{E}}$	secant	secant	external
$\mathcal{S}_{\mathcal{S}\mathcal{S}\mathcal{C}}$	secant	secant	on \mathcal{C}
$\mathcal{S}_{\mathcal{S}\mathcal{S}\mathcal{I}}$	secant	secant	internal
$\mathcal{S}_{\mathcal{K}\mathcal{K}\mathcal{E}}$	skew	skew	external
$\mathcal{S}_{\mathcal{T}\mathcal{S}\mathcal{E}}$	tangent	secant	external
$\mathcal{S}_{\mathcal{T}\mathcal{S}\mathcal{C}}$	tangent	secant	on \mathcal{C}
$\mathcal{S}_{\mathcal{T}\mathcal{K}\mathcal{E}}$	tangent	skew	external
$\mathcal{S}_{\mathcal{S}\mathcal{K}\mathcal{E}}$	secant	skew	external

Table 1: Some possible constructions of determining sets with one conic and two lines

In the following subsections, we will construct one previously unknown determining set for each of the constructions detailed in Table 1. In each determining set construction, we will look to minimize the number of points in the determining set (i.e., to the extent where, if any other point is removed from the set, it will no longer be a determining set). However, note that one can always add more points to the determining set without losing the properties associated with determining sets.

In terms of the number of points in a determining set, we will use the vertex-less triangle with $3q - 3$ points as our rough point of reference. That is, if we can construct a determining set with less than $3q - 3$ points, we will find it of particular interest.

2.1 Case One: $\mathcal{S}_{\mathcal{T}\mathcal{T}\mathcal{E}}$

Suppose that the intersection of l_1 and l_2 occurs at P , a point external to \mathcal{C} , and that both l_1 and l_2 are tangent to \mathcal{C} at points R and Q , respectively. Define $\mathcal{S}_{\mathcal{T}\mathcal{T}\mathcal{E}}$ as the set of points covered by \mathcal{C} and two lines with the following points removed:

- the points of intersection of the tangent lines to \mathcal{C} through P (i.e., points Q and R), and
- one point from each of the sets $l \cap \mathcal{C}$ where l is a line through P that is secant to \mathcal{C} . (Note that this equates to $\frac{q-1}{2}$ points being removed.)

Figure 3 illustrates \mathcal{S}_{TTE} where gray dots correspond to the removed points. Figure 4 illustrates how the secant lines still intersect \mathcal{S}_{TTE} in one point after the designated points of \mathcal{C} are removed.

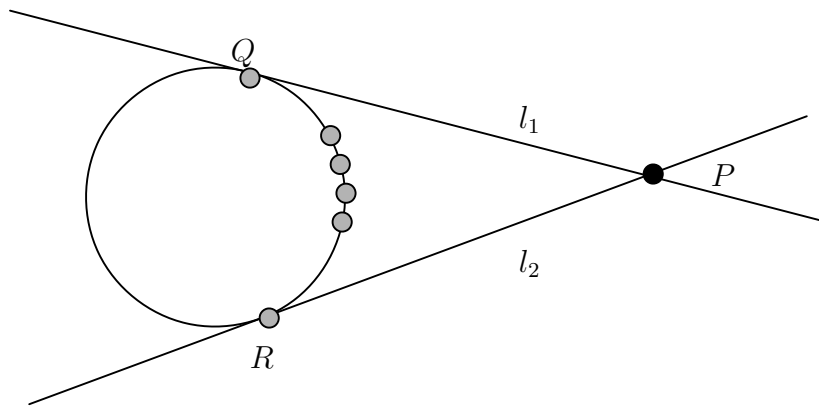


Figure 3: \mathcal{S}_{TTE}

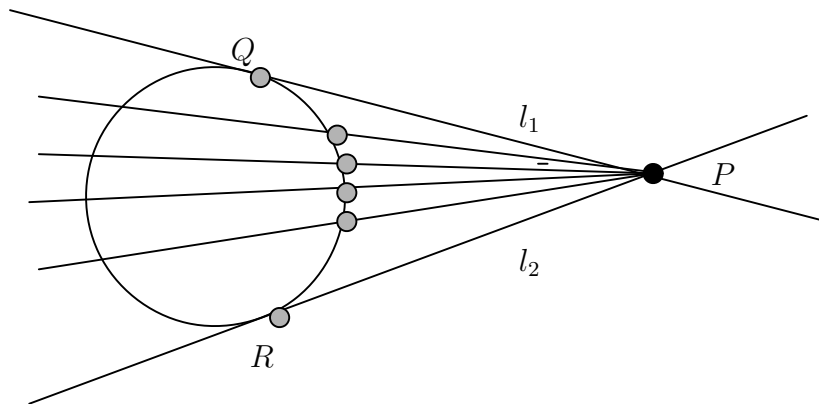


Figure 4: Secant lines through \mathcal{S}_{TTE}

Now, let us consider the number of points in \mathcal{S}_{TTE} ,

- $|l_1 \cap \mathcal{S}_{TTE}| = q + 1 - 1 = q$ since Q was removed from \mathcal{S}_{TTE} and thus the number of points in \mathcal{S}_{TTE} on l_1 is one fewer than the total number of points on l_1 (i.e., $q + 1$).

- $|l_2 \cap \mathcal{S}_{\mathcal{T}\mathcal{T}\mathcal{E}}| = q + 1 - 1 = q$ since R was removed from $\mathcal{S}_{\mathcal{T}\mathcal{T}\mathcal{E}}$ and thus the number of points in $\mathcal{S}_{\mathcal{T}\mathcal{T}\mathcal{E}}$ on l_2 is one fewer than the total number of points on l_2 .
- $|\mathcal{C} \cap \mathcal{S}_{\mathcal{T}\mathcal{T}\mathcal{E}}| = q + 1 - 2 - \frac{q-1}{2} = \frac{q-1}{2}$ since Q , R and $\frac{q-1}{2}$ other points were removed from $\mathcal{S}_{\mathcal{T}\mathcal{T}\mathcal{E}}$ and thus the number of points in $\mathcal{S}_{\mathcal{T}\mathcal{T}\mathcal{E}}$ on \mathcal{C} is $2 + \frac{q-1}{2}$ fewer than the total number of points on \mathcal{C} .

Now observe that l_1 and l_2 share the points P . Thus, by inclusion/exclusion, the total number of points in $\mathcal{S}_{\mathcal{T}\mathcal{T}\mathcal{E}}$ is

$$\begin{aligned} |\mathcal{S}_{\mathcal{T}\mathcal{T}\mathcal{E}}| &= q + (q - 1) + \frac{q - 1}{2} \\ &= \frac{5q - 3}{2} \end{aligned}$$

Note that $\frac{5q-3}{2}$ is less than $3q-3$ (the number of points in the vertex-less triangle) whenever $q > 3$.

Theorem 2.2. *The set $\mathcal{S}_{\mathcal{T}\mathcal{T}\mathcal{E}}$ is a **determining set** of size $\frac{5q-3}{2}$ for all lines in π except for the $\frac{q-1}{2}$ skew lines through P .*

Proof. First recall that there are $\frac{q-1}{2}$ skew lines through P , as described in the beginning of Section 2.

Now, call \mathcal{L}' the set of all lines in π except for these $\frac{q-1}{2}$ skew lines through P . Then, by Definition 1.6, $\mathcal{S}_{\mathcal{T}\mathcal{T}\mathcal{E}}$ is a determining set for \mathcal{L}' if and only if any pair of lines in \mathcal{L}' has a different intersection pattern with $\mathcal{S}_{\mathcal{T}\mathcal{T}\mathcal{E}}$. We will consider the intersections of lines in \mathcal{L}' with $\mathcal{S}_{\mathcal{T}\mathcal{T}\mathcal{E}}$, as follows.

Table 2 represents all possible intersections of lines in \mathcal{L}' with $\mathcal{S}_{\mathcal{T}\mathcal{T}\mathcal{E}}$ sorted by their intersection size with \mathcal{C} . Each row in Table 2 represents a possible subset of lines in \mathcal{L}' and what point(s) it shares with $\mathcal{S}_{\mathcal{T}\mathcal{T}\mathcal{E}}$. Table 2 also shows in how many ways each line of a given type intersects with \mathcal{C} , l_1 and l_2 .

Let X_i represent one of the $\frac{q-1}{2}$ points of \mathcal{C} not in $\mathcal{S}_{\mathcal{T}\mathcal{T}\mathcal{E}}$ and not equal to Q nor R . Also, let Y_i represent a point of \mathcal{C} and in $\mathcal{S}_{\mathcal{T}\mathcal{T}\mathcal{E}}$.

It is clear that any row with at most one zero indicates that lines of that type have at least two points of intersection with $\mathcal{S}_{\mathcal{T}\mathcal{T}\mathcal{E}}$. By Definition 1.1, we know that two points determine a unique line, and thus all such lines have different intersections with $\mathcal{S}_{\mathcal{T}\mathcal{T}\mathcal{E}}$. Now, we only need to prove that lines with two or more zeros in Table 2 also have different intersections with $\mathcal{S}_{\mathcal{T}\mathcal{T}\mathcal{E}}$.

There are only three types of lines that have two or more zeros in Table 2. In particular, (1) the secant line QR , (2) the secant lines QX_i and (3) the secant lines RX_i . We consider these cases.

type	Intersects with	C	l_1	l_2
tangent	Q	0	1	q
tangent	R	0	q	1
tangent	X_i	0	1	1
tangent	Y_i	1	1	1
secant	QR	0	0	0
secant	QX_i	0	1	0
secant	QY_i	1	1	0
secant	RX_i	0	0	1
secant	RY_i	1	0	1
secant	X_iX_j	0	1	1
secant	Y_iY_j	2	1	1
secant	X_iY_j	1	1	1
skew	P	0	1	1
skew	not P	0	1	1

Table 2: \mathcal{S}_{TTE} incidence results

1. Note that there is only one line of this type, and this is the only line that does not intersect \mathcal{S}_{TTE} at any points. Thus, its lack of intersection with \mathcal{S}_{TTE} uniquely defines it.
2. There are precisely the $\frac{q-1}{2}$ lines that intersect \mathcal{S}_{TTE} with a point on l_1 but not with a point on l_2 . Thus, if a line intersects \mathcal{S}_{TTE} with a point on l_1 but not with a point on l_2 , we know that this line actually goes through R on l_2 and its other defined point on l_1 . Then, since two points uniquely define a line, each line in (2) is uniquely defined.
3. There are precisely the $\frac{q-1}{2}$ lines that intersect \mathcal{S}_{TTE} with a point on l_2 but not with a point on l_1 . Thus, if a line intersects \mathcal{S}_{TTE} with a point on l_2 but not with a point on l_1 , we know that this line actually goes through the removed point Q on l_1 and its other defined point on l_2 . Then, since two points uniquely define a line, each line in (3) is uniquely defined.

Thus, we have proven that any pair of lines in \mathcal{L}' have a different intersection with \mathcal{S}_{TTE} . In other words, \mathcal{S}_{TTE} is a determining set for all lines in π except the $\frac{q-1}{2}$ skew lines through P .

□

2.2 Case Two $\mathcal{S}_{SS\mathcal{E}}$

Now, suppose that the intersection of l_1 and l_2 occurs at P , a point external to \mathcal{C} , and that both l_1 and l_2 are secant to \mathcal{C} at points Q and S , and R and T , respectively. Define $\mathcal{S}_{SS\mathcal{E}}$ as the above conic and two lines with the following points removed:

- point P , and
- one point from each of the sets $l \cap \mathcal{C}$ where l is a line through P that is secant to \mathcal{C} . (Note that this equates to $\frac{q-1}{2}$ points being removed. and that this removes points S and T .)

Figure 5 illustrates the set $\mathcal{S}_{SS\mathcal{E}}$ where the gray dots represent points that have been removed. Note that not all removed points are represented (i.e., the number of removed points is a function of q).

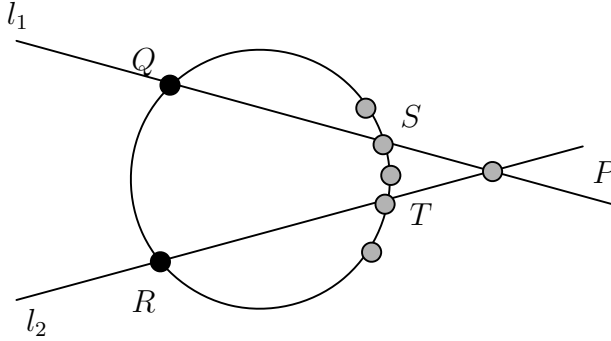


Figure 5: $\mathcal{S}_{SS\mathcal{E}}$

Now, let us consider the number of points in $\mathcal{S}_{SS\mathcal{E}}$.

- $|l_1 \cap \mathcal{S}_{SS\mathcal{E}}| = q + 1 - 2 = q - 1$ since S and P were removed from $\mathcal{S}_{SS\mathcal{E}}$ and thus the number of points in $\mathcal{S}_{SS\mathcal{E}}$ on l_1 is two fewer than the total number of points on l_1 .
- $|l_2 \cap \mathcal{S}_{SS\mathcal{E}}| = q + 1 - 2 = q - 1$ since T and P were removed from $\mathcal{S}_{SS\mathcal{E}}$ and thus the number of points in $\mathcal{S}_{SS\mathcal{E}}$ on l_2 is two fewer than the total number of points on l_2 .
- $|\mathcal{C} \cap \mathcal{S}_{SS\mathcal{E}}| = q + 1 - \frac{q-1}{2} = \frac{q+3}{2}$ since $\frac{q-1}{2}$ other points were removed from $\mathcal{S}_{SS\mathcal{E}}$ and thus the number of points in $\mathcal{S}_{SS\mathcal{E}}$ on \mathcal{C} is $\frac{q-1}{2}$ fewer than the total number of points on \mathcal{C} .

Thus, by inclusion/exclusion, the total number of points is:

$$\begin{aligned} |\mathcal{S}_{SS\mathcal{E}}| &= (q - 1) + (q - 1) + \left(\frac{q + 3}{2}\right) \\ &= \frac{5q - 1}{2} \end{aligned}$$

Note that $\frac{5q-1}{2}$ is less than $3q - 3$ whenever $q > 5$.

Theorem 2.3. *The set \mathcal{S}_{SSE} is a **determining set** for all lines in π except for the $\frac{q-1}{2}$ skew lines through P .*

Proof. Recall from the beginning of Section 2 that there are exactly $\frac{q-1}{2}$ skew lines through P .

Now, call the set of all lines through P in π that are not skew lines the set \mathcal{L}' . Then, we can prove that \mathcal{S}_{SSE} is a determining set for all lines \mathcal{L}' by using the same methodology as the case by case analysis depicted in Table 2 in the proof of Theorem 2.2. However, for the sake of simplicity, this methodology will not be detailed again. Instead, we will provide an abbreviated but sufficient proof as follows.

First, note that lines l_1 and l_2 are identified by $q - 1$ points. Then all other lines not through P , S , or T will intersect l_1 and l_2 in two distinct points, and thus can be uniquely identified.

Now, consider the lines through P . We do not include any skew lines through P in our set \mathcal{L}' . Then, any line through P can be identified by its intersection with \mathcal{S}_{SSE} , for they are the only lines that intersect this set at a point on \mathcal{C} and not at a point on l_1 nor l_2 .

Now, consider the lines through S and/or T . The line through S and T is the only such line that does not intersect \mathcal{S}_{SSE} at any points on l_1 , l_2 nor \mathcal{C} and thus can be uniquely identified by its lack of intersection. As for the lines through S and not T , they are the only lines that intersect \mathcal{S}_{SSE} at a point on l_2 but not at a point on l_1 . Thus, if a line intersects \mathcal{S}_{SSE} at a point on l_2 but not on l_1 , this line can be identified by actually going through the removed point S on l_1 and its other defined point on l_2 . A similar argument holds true for those lines through T but not S .

Thus, we have proven that any pair of lines in \mathcal{L}' has a different intersection with \mathcal{S}_{SSE} . Or, in other words, \mathcal{S}_{SSE} is a determining set for all lines in π except the $\frac{q-1}{2}$ skew lines through P .

□

2.3 Case Three: \mathcal{S}_{SSC}

Now suppose that the intersection of l_1 and l_2 occurs at P , a point on \mathcal{C} , and that both l_1 and l_2 are secant to \mathcal{C} at points Q and R , respectively. Define the \mathcal{S}_{SSC} as the above conic and two lines with the points Q and R removed.

Figure 6 illustrates the set \mathcal{S}_{SSC} where the gray dots represent points that have been removed.

Now, let us consider the number of points in \mathcal{S}_{SSC} .

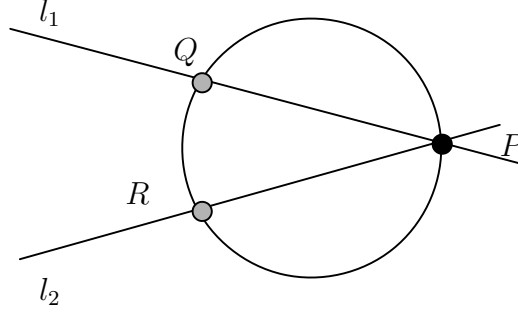


Figure 6: \mathcal{S}_{SSC}

- $|l_1 \cap \mathcal{S}_{SSC}| = q + 1 - 1 = q$ since Q was removed from \mathcal{S}_{SSC} and thus number of points on l_1 in \mathcal{S}_{SSC} is one fewer than the total number of points on l_1 .
- $|l_2 \cap \mathcal{S}_{SSC}| = q + 1 - 1 = q$ since since R was removed from \mathcal{S}_{SSC} and thus the number of points on l_2 in \mathcal{S}_{SSC} is one fewer than the total number of points on l_2 .
- $|C \cap \mathcal{S}_{SSC}| = q + 1 - 2 = q - 1$ since Q and R were removed from \mathcal{S}_{SSC} and thus the number of points on C in \mathcal{S}_{SSC} is two fewer than the total number of points on C .

Thus, by inclusion/exclusion, the total number of points is:

$$\begin{aligned} |\mathcal{S}_{SSC}| &= q + (q - 1) + (q - 2) \\ &= 3q - 3 \end{aligned}$$

Theorem 2.4. *The set \mathcal{S}_{SSC} is a **determining set** for all lines in π .*

Proof. We can prove that \mathcal{S}_{SSC} is a determining set for all lines π by using the same methodology as in the previous proof. First, note that lines l_1 and l_2 are identified by q points. Then all other lines not through P , Q , or R will intersect \mathcal{S}_{SSC} in two distinct points on l_1 and l_2 , and thus can be uniquely identified.

Now, consider the lines through P . By construction, there are no skew lines through P . There is only one tangent line through P , which can be identified only intersecting \mathcal{S}_{SSC} at the point P . Also, any secant lines through P can be identified by intersecting \mathcal{S}_{SSC} at both P and some other point on with C .

Now, consider the lines through Q and/or R . The line through Q and R is the only such line that does not intersect \mathcal{S}_{SSC} at any point and thus can be uniquely identified by its lack of intersection. As for the lines through Q and not R , they are the only lines that intersect \mathcal{S}_{SSC} at a point on l_2 but not at a point on l_1 . Thus, if a line intersects \mathcal{S}_{SSC} at a point on l_2 but not at a point on l_1 , this line can be identified by actually going through the removed

point Q on l_1 and its other defined point on l_2 . A similar argument holds true for those lines through R but not Q .

Thus, we have proven that any pair of lines in π has a different unique intersection with \mathcal{S}_{SSC} . Or, in other words, \mathcal{S}_{SSC} is a determining set for all lines in π . □

2.4 Case Four: $\mathcal{S}_{SS\mathcal{I}}$

Now suppose that the intersection of l_1 and l_2 occurs at P , a point internal to \mathcal{C} and that both l_1 and l_2 are secant to \mathcal{C} at points Q and T , and R and S , respectively. Define $\mathcal{S}_{SS\mathcal{I}}$ as the above conic and two lines with the following points removed:

- point P , and
- one point from each of the sets $l \cap \mathcal{C}$ where l is a line through P that is secant to \mathcal{C} . (Note that includes points Q and R , and this equates to $\frac{q+1}{2}$ points being removed.)

Figure 7 illustrates the set $\mathcal{S}_{SS\mathcal{I}}$ where the gray dots represent points that have been removed. Note that not all removed points are represented (i.e., the number of removed points is a function of q).

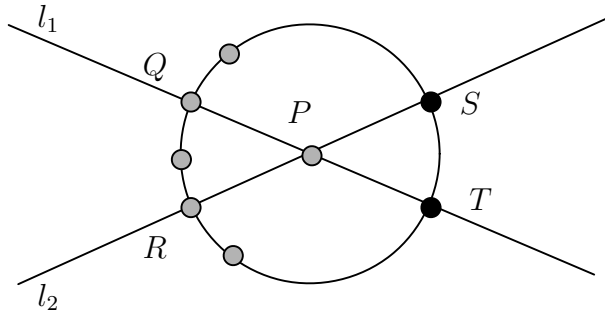


Figure 7: $\mathcal{S}_{SS\mathcal{I}}$

Now, let us consider the number of points in $\mathcal{S}_{SS\mathcal{I}}$.

- $|l_1 \cap \mathcal{S}_{SS\mathcal{I}}| = q + 1 - 2 = q - 1$ since Q and P were removed from $\mathcal{S}_{SS\mathcal{I}}$ and thus the number of points in $\mathcal{S}_{SS\mathcal{I}}$ on l_1 is two fewer than the total number of points on l_1 .
- $|l_2 \cap \mathcal{S}_{SS\mathcal{I}}| = q + 1 - 2 = q - 1$ since R and P were removed from $\mathcal{S}_{SS\mathcal{I}}$ and thus the number of points in $\mathcal{S}_{SS\mathcal{I}}$ on l_2 is two fewer than the total number of points on l_2 .
- $|\mathcal{C} \cap \mathcal{S}_{SS\mathcal{I}}| = q + 1 - \frac{q+1}{2} = \frac{q+1}{2}$ since $\frac{q+1}{2}$ other points were removed from $\mathcal{S}_{SS\mathcal{I}}$ and thus the total number of points in $\mathcal{S}_{SS\mathcal{I}}$ on \mathcal{C} is $\frac{q+1}{2}$ fewer than the total number of points on \mathcal{C} .

Thus, by inclusion/exclusion, the total number of points is:

$$\begin{aligned} |\mathcal{S}_{SS\mathcal{I}}| &= (q-1) + (q-1) + \binom{q+1}{2} \\ &= \frac{5q-3}{2} \end{aligned}$$

Note that $\frac{5q-3}{2}$ is less than $3q-3$ whenever $q > 3$.

Theorem 2.5. *The set $\mathcal{S}_{SS\mathcal{I}}$ is a **determining set** for all lines in π except for the $\frac{q+1}{2}$ skew lines through P .*

Proof. Recall again from the beginning of Section 2 that there are exactly $\frac{q+1}{2}$ skew lines through P .

Now, call the set of all lines through P in π that are not skew lines the set \mathcal{L}' . Then, we can prove that $\mathcal{S}_{SS\mathcal{I}}$ is a determining set for all lines \mathcal{L}' by repeating our techniques

First, note that lines l_1 and l_2 are identified by intersecting $\mathcal{S}_{SS\mathcal{I}}$ at $q-1$ points. Then all other lines not through P , Q , or R will intersect $\mathcal{S}_{SS\mathcal{I}}$ at two distinct points on l_1 and l_2 , and thus can be uniquely identified.

Now, consider the lines through P . By construction, we are not considering the skew lines through P . Then, any other line through P can be identified by intersecting $\mathcal{S}_{SS\mathcal{I}}$ at a point on \mathcal{C} but not at a point on l_1 nor l_2 .

Now, consider the lines through Q and/or R . The line through Q and R is the only such line that does not intersect $\mathcal{S}_{SS\mathcal{I}}$ at any point and thus can be uniquely identified by its lack of intersection. As for the lines through Q and not R , they are the only lines that intersect $\mathcal{S}_{SS\mathcal{I}}$ at a point on l_2 but not at a point on l_1 . Thus, if a line intersects $\mathcal{S}_{SS\mathcal{I}}$ at a point on l_2 but not at a point on l_1 , this line can be identified by actually going through the removed point Q on l_1 and its other defined point on l_2 . A similar argument holds true for those lines through R but not Q .

Thus, we have proven that any pair of lines in \mathcal{L}' has a different intersection with $\mathcal{S}_{SS\mathcal{I}}$. Or, in other words, $\mathcal{S}_{SS\mathcal{I}}$ is a determining set for all lines in π except for the $\frac{q+1}{2}$ skew lines through P .

□

2.5 Remaining cases

There are five remaining possible constructions involving two lines and one conic. An example of a determining set of each type is depicted below, labeled as **Case Five - Case Nine**.

Case Five: $\mathcal{S}_{\mathcal{K}\mathcal{K}\mathcal{E}}$: Suppose that the intersection of l_1 and l_2 occurs at P , a point external of \mathcal{C} , and that both l_1 and l_2 are skew to \mathcal{C} . Define $\mathcal{S}_{\mathcal{K}\mathcal{K}\mathcal{E}}$ as the above conic and two lines with the following points removed:

- the point P ,
- the point Q where the line through Q and P is tangent to \mathcal{C} , and
- one point from each of the sets $l \cap \mathcal{C}$ where l is a line through P that is secant to \mathcal{C} .
(Note that this equates to $\frac{q-1}{2}$ points being removed.)

Then, $\mathcal{S}_{\mathcal{K}\mathcal{K}\mathcal{E}}$ is a **determining set** for all lines in π except for the $\frac{q-1}{2}$ skew lines through P . The set $\mathcal{S}_{\mathcal{K}\mathcal{K}\mathcal{E}}$ is displayed in Figure 8.

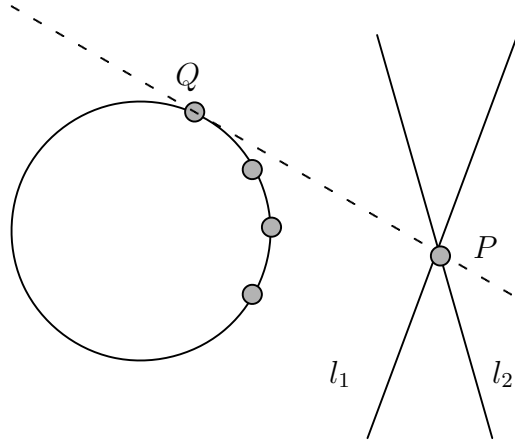


Figure 8: $\mathcal{S}_{\mathcal{K}\mathcal{K}\mathcal{E}}$

Case Six: $\mathcal{S}_{\mathcal{T}\mathcal{S}\mathcal{E}}$: Suppose that the intersection of l_1 and l_2 occurs at P , a point external of \mathcal{C} , and that l_1 and l_2 are tangent and secant to \mathcal{C} , respectively. Define $\mathcal{S}_{\mathcal{T}\mathcal{S}\mathcal{E}}$ as the above conic and two lines with the following points removed:

- the point P ,
- the point Q where the line through Q and P is tangent to \mathcal{C} , and
- one point from each of the sets $l \cap \mathcal{C}$ where l is a line through P that is secant to \mathcal{C} .
(Note that includes this equates to $\frac{q-1}{2}$ points being removed.)

Then, $\mathcal{S}_{\mathcal{T}\mathcal{S}\mathcal{E}}$ is a **determining set** for all lines in π except for the $\frac{q-1}{2}$ skew lines through P . The set $\mathcal{S}_{\mathcal{T}\mathcal{S}\mathcal{E}}$ is displayed in Figure 9.

Case Seven: $\mathcal{S}_{\mathcal{T}\mathcal{S}\mathcal{C}}$: Suppose that the intersection of l_1 and l_2 occurs at P , a point on \mathcal{C} , and that l_1 and l_2 are tangent and secant to \mathcal{C} , respectively. Define $\mathcal{S}_{\mathcal{T}\mathcal{S}\mathcal{C}}$ as the above conic and two lines with the following points removed:

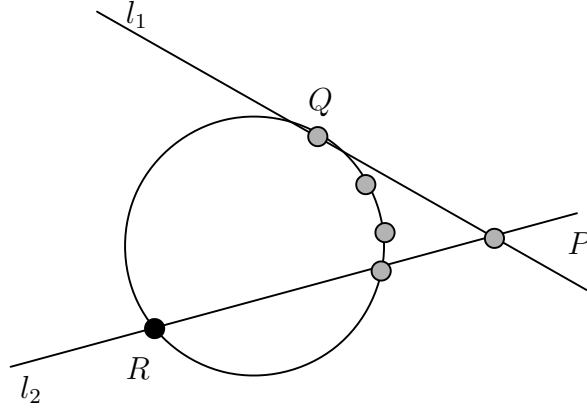


Figure 9: \mathcal{S}_{TSE}

- the point P ,
- the point R that is on l_2 and on \mathcal{C} (but not equal to P), and
- the point Q that is on \mathcal{C} and not equal to R nor P .

Then, \mathcal{S}_{TSC} is a **determining set** for all lines in π . The set \mathcal{S}_{TSC} is displayed in Figure 10.

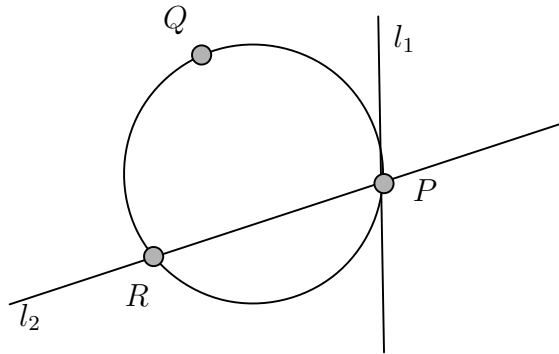


Figure 10: \mathcal{S}_{TSC}

Case Eight: $\mathcal{S}_{TK\mathcal{E}}$: Suppose that the intersection of l_1 and l_2 occurs at P , a point external to \mathcal{C} and that l_1 and l_2 are tangent and skew to \mathcal{C} , respectively. Define $\mathcal{S}_{TK\mathcal{E}}$ as the above conic and two lines with the following points removed:

- the point P ,
- the point Q where Q is on l_1 and tangent to \mathcal{C} ,

- the point R where R is on \mathcal{C} , and the line through R and P is tangent to \mathcal{C} , and
- one point from each of the sets $l \cap \mathcal{C}$ where l is a line through P that is secant to \mathcal{C} .
Note that this removes points Q and R , and this equates to $\frac{q-1}{2}$ points being removed.

Then, $\mathcal{S}_{\mathcal{TK}\mathcal{E}}$ is a **determining set** for all lines in π except for the $\frac{q-1}{2}$ skew lines through P . The set $\mathcal{S}_{\mathcal{TK}\mathcal{E}}$ is displayed in Figure 11.

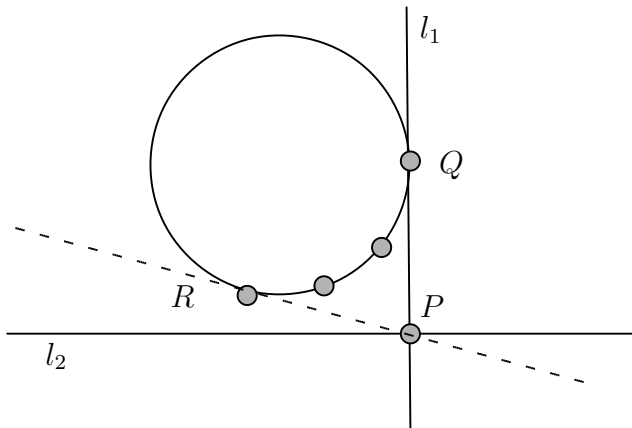


Figure 11: $\mathcal{S}_{\mathcal{TK}\mathcal{E}}$

Case Nine: $\mathcal{S}_{\mathcal{SK}\mathcal{E}}$: Suppose that the intersection of l_1 and l_2 occurs at P , a point external to \mathcal{C} , and that l_1 and l_2 are secant and skew to \mathcal{C} , respectively. Define $\mathcal{S}_{\mathcal{SK}\mathcal{E}}$ as the above conic and two lines with the following points removed:

- the point P ,
- the point S where S is on \mathcal{C} and the line through S and P is tangent to \mathcal{C} , and
- one point from each of the sets $l \cap \mathcal{C}$ where l is a line through P that is secant to \mathcal{C} .
Note that this equates to $\frac{q-1}{2}$ points being removed.

Then, $\mathcal{S}_{\mathcal{SK}\mathcal{E}}$ is a **determining set** for all lines in π except for the $\frac{q-1}{2}$ skew lines through P . The set $\mathcal{S}_{\mathcal{SK}\mathcal{E}}$ is displayed in Figure 12.

2.6 Summary of all cases

All of the above constructed determining sets are summarized in Table 3. In particular, this table depicts how many points are contained in each determining set and how many (if any) lines must be excluded. Note that the results for cases five through nine can be calculated similarly to those of the first four cases, as explained in Sections 2.1 - 2.4.

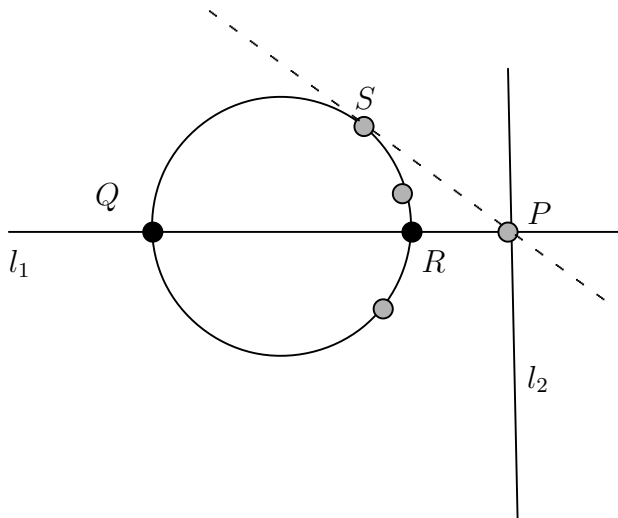


Figure 12: $\mathcal{S}_{SK\mathcal{E}}$

Note that the determining sets $\mathcal{S}_{TT\mathcal{E}}$, $\mathcal{S}_{SS\mathcal{I}}$ and $\mathcal{S}_{TK\mathcal{E}}$ have fewer points than the vertex-less triangle (i.e., $3q - 3$ points) if $q > 3$, while $\mathcal{S}_{SS\mathcal{E}}$, $\mathcal{S}_{KK\mathcal{E}}$, $\mathcal{S}_{TS\mathcal{E}}$ and $\mathcal{S}_{SK\mathcal{E}}$ have fewer points than the vertex-less triangle if $q > 5$. However, note that these sets are not determining sets for all lines in π (i.e., some lines had to be removed). On the other hand, $\mathcal{S}_{SS\mathcal{C}}$ and $\mathcal{S}_{TS\mathcal{C}}$ are determining sets for all lines in π although they have the same number of points as the vertex-less triangle. Lastly, it is important to note that the next section discusses how, under certain conditions, it is possible to form a new determining set from $\mathcal{S}_{TS\mathcal{C}}$ that has $3q - 4$ points.

3 Construction of a determining set with $3q - 4$ points

In this section, we will construct a new determining set by removing one point, X' , that meets particular conditions, from the determining set $\mathcal{S}_{TS\mathcal{C}}$. Note that this new determining set, referred to as the set $\mathcal{M}\mathcal{E}$, would thus only have $3q - 4$ points, which is less than the vertex-less triangle. Moreover, unlike our other determining sets with fewer points than the vertex-less triangle, the set $\mathcal{M}\mathcal{E}$ is a determining set for *all* lines in π .

3.1 The set $\mathcal{M}\mathcal{E}$

Suppose that the intersection of l_1 and l_2 occurs at P , a point on \mathcal{C} , and that l_1 and l_2 are tangent and secant to \mathcal{C} , respectively. Before we explain the conditions that the point X' must satisfy, it is helpful to define the following points in the set $\mathcal{M}\mathcal{E}$. Note that the locations of these points are shown in Figure 13.

Case	$l_1 \cap \mathcal{C}$	$l_2 \cap \mathcal{C}$	location of P	size of set	number of lines removed
\mathcal{S}_{TTE}	tangent	tangent	external	$\frac{5q-3}{2}$	$\frac{q-1}{2}$
\mathcal{S}_{SSE}	secant	secant	external	$\frac{5q-1}{2}$	$\frac{q-1}{2}$
\mathcal{S}_{SSC}	secant	secant	on \mathcal{C}	$3q - 3$	None
\mathcal{S}_{SSI}	secant	secant	internal	$\frac{5q-3}{2}$	$\frac{q+1}{2}$
\mathcal{S}_{KKE}	skew	skew	external	$\frac{5q-1}{2}$	$\frac{q-1}{2}$
\mathcal{S}_{TSE}	tangent	secant	external	$\frac{5q-1}{2}$	$\frac{q-1}{2}$
\mathcal{S}_{TSC}	tangent	secant	on \mathcal{C}	$3q - 3$	None
\mathcal{S}_{TKE}	tangent	skew	external	$\frac{5q-3}{2}$	$\frac{q-1}{2}$
\mathcal{S}_{SKE}	secant	skew	external	$\frac{5q-1}{2}$	$\frac{q-1}{2}$

Table 3: Possible constructions of determining sets with one conic and two lines

- R is on l_2 and is the other secant point on \mathcal{C} (i.e., not equal to P).
- Q is on \mathcal{C} and not equal to R nor P .
- A is the intersection point on l_1 with the tangent line to \mathcal{C} through R .
- B is the intersection point on l_1 with the tangent line to \mathcal{C} through Q .
- F is the intersection point on l_2 with the tangent line to \mathcal{C} through Q .
- G is the intersection point on l_1 with the secant line to \mathcal{C} through RQ .
- H is the intersection point on l_2 with the tangent line to \mathcal{C} through G .

In a given construction of \mathcal{ME} , X' could be any point that meets the following three conditions. While we will call the set of all points that satisfy these conditions *candidates for X'* , note that one and only one point can be designated X' .

1. X' is on l_2 .
2. X' is on a secant line to \mathcal{C} through A .
3. X' is not on a skew line to \mathcal{C} through G .

Figure 14 shows a possible location of X' . The dashed lines through X' indicate that X' intersects those lines, while the dotted lines not through X' indicate that X' can not intersect those lines.

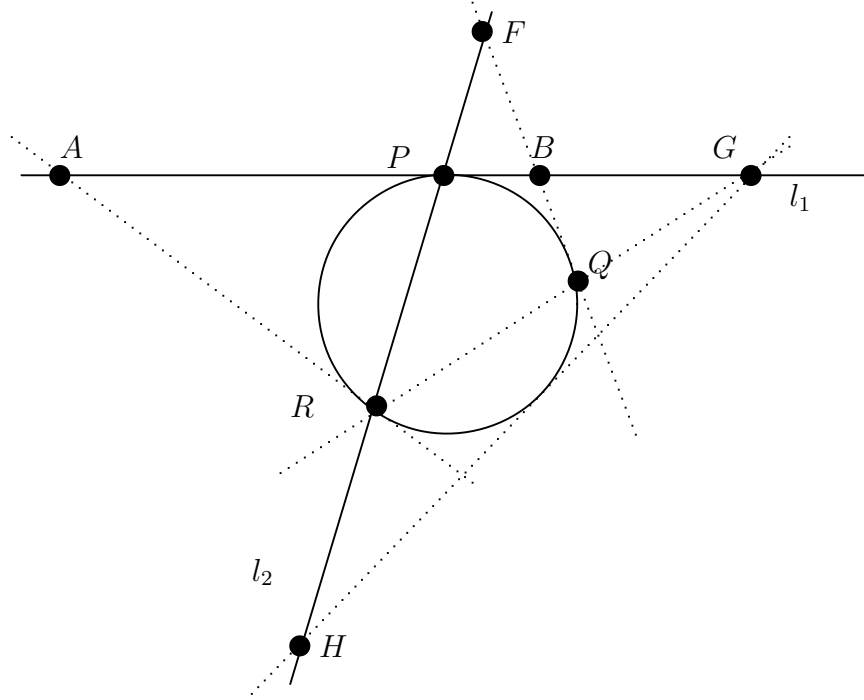


Figure 13: Important points to the set \mathcal{ME}

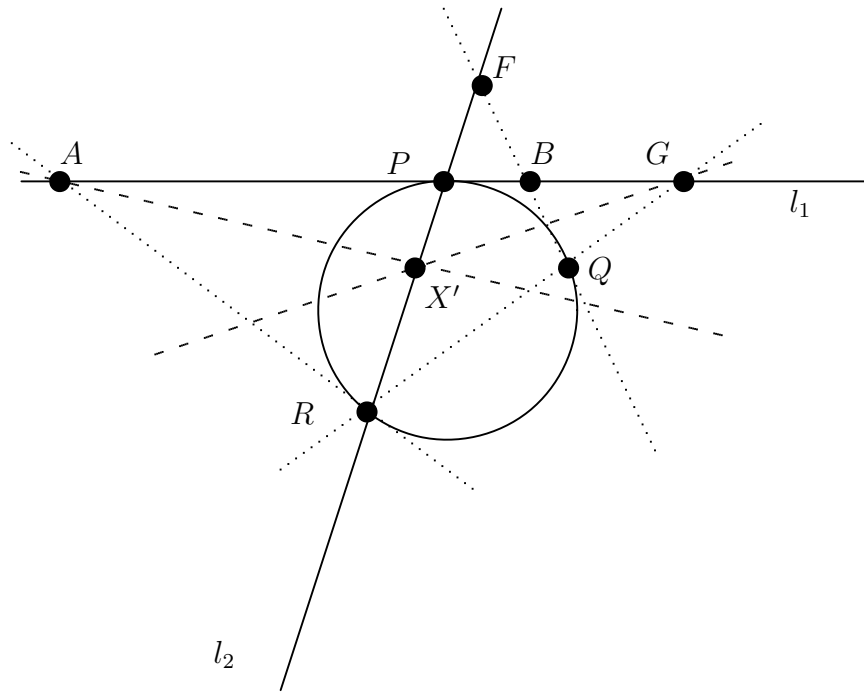


Figure 14: Possible location of X'

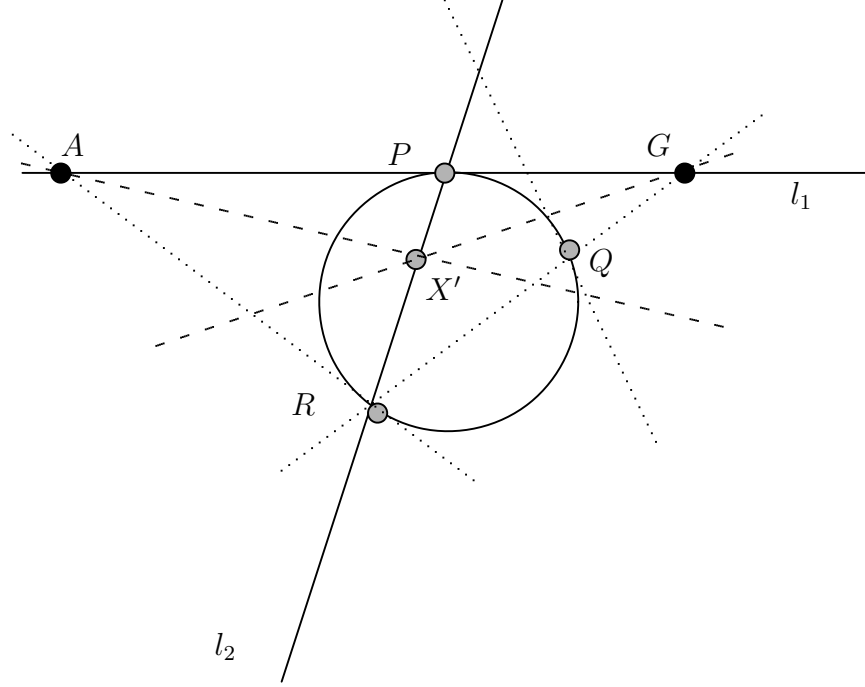


Figure 15: The set \mathcal{ME} with possible X'

Define the set \mathcal{ME} as the points covered by the conic \mathcal{C} and two lines, l_1 and l_2 , with the points P , Q , R and X' removed. That is, \mathcal{ME} is the same as the set \mathcal{S}_{TSC} with the additional point X' removed. Figure 15 illustrates the set \mathcal{ME} with the gray points representing points not in \mathcal{ME} .

Now, let us consider the number of points in \mathcal{ME} .

- $|l_1 \cap \mathcal{ME}| = q + 1 - 1 = q$ since P was removed from \mathcal{ME} and thus the number of points in \mathcal{ME} on l_1 is one fewer than the total number of points on l_1 .
- $|l_2 \cap \mathcal{ME}| = q + 1 - 3 = q - 2$ since P , X' and R were removed from \mathcal{ME} and thus the number of points in \mathcal{ME} on l_2 is three fewer than the total number of points on l_2 .
- $|\mathcal{C} \cap \mathcal{ME}| = q + 1 - 3 = q - 2$ since P , Q and R were removed from \mathcal{ME} and thus the total number of points in \mathcal{ME} on \mathcal{C} is three fewer than the total number of points on \mathcal{C} .

Thus, by inclusion/exclusion, the total number of points is:

$$\begin{aligned} |\mathcal{ME}| &= q + (q - 2) + (q - 2) \\ &= 3q - 4 \end{aligned}$$

3.2 Are the three conditions of the candidates for X' necessary?

While we will prove that the three conditions of *candidates for X'* are sufficient to guarantee that \mathcal{ME} is a determining set in Section 3.4, are all of these conditions necessary? In short, yes. In particular, the following explanations demonstrate how \mathcal{ME} *cannot* be a determining set if any of the conditions for the *candidates for X'* are not met.

Let us first consider condition (1), X' is on l_2 . Recall that the set \mathcal{ME} was formed by removing one point, X' , from the set $\mathcal{S}_{\mathcal{TC}}$. Thus, this condition can easily be explained by showing that removing a point in $\mathcal{S}_{\mathcal{TC}}$ from \mathcal{C} or from l_1 to form \mathcal{ME} prevents \mathcal{ME} from being a determining set. First, assume that \mathcal{ME} is formed by removing an additional point, X , from \mathcal{C} . Then, the line through X and P will have no intersection with the set \mathcal{ME} . However, the line through P and Q also has no intersection with the set \mathcal{ME} . Hence, it is not the case that all lines in the plane have different intersection patterns with \mathcal{ME} , and so \mathcal{ME} is not a determining set. Similarly, assume that \mathcal{ME} is formed by removing an additional point, Y , from l_1 . Let Z represent the point where the line through R and Y intersects the conic \mathcal{C} . Then, the line through R and Y will have the same intersection pattern with \mathcal{ME} as line through P and Z ; that is, both lines only intersect \mathcal{ME} at point Z . Thus, for the same reasons above, \mathcal{ME} could not be a determining set. In other words, it is clear that for \mathcal{ME} to be a determining set, X' cannot be on l_1 nor \mathcal{C} , and then the only remaining *possibility* is for X' to be on l_2 .

Now we will consider condition (2), X' is on a secant line to \mathcal{C} through A . For the sake of contradiction, assume X' is not on a secant line through A —that is, X' is on a tangent or skew line through A . The tangent lines to \mathcal{C} through A are l_1 and the line AR , which intersect \mathcal{C} at P and R , respectively. Since X' must be on l_2 , and P and R are not elements of \mathcal{ME} , X' cannot be on a tangent line to \mathcal{C} through A . Then, X' must be on a skew line through A . Also, note that any skew line through A and X' would only intersect the set \mathcal{ME} at point A . However, the line AR also only intersects the set \mathcal{ME} at point A , which then implies that \mathcal{ME} cannot be a determining set. Thus, X' must be on a secant line through A .

Lastly, we will consider condition (3), X' is not on a skew line to \mathcal{C} through G . For the sake of contradiction, assume that X' is on a skew line to \mathcal{C} through G . Then, this line would intersect \mathcal{ME} only at point G . However, the secant through QR also only intersects \mathcal{C} through G , which then implies that \mathcal{ME} cannot be a determining set. Thus, X' cannot be on a skew line to \mathcal{C} through G .

Thus, we have now shown that the three conditions of the *candidates for X'* are necessary. However, before we prove that these conditions are sufficient to guarantee that \mathcal{ME} is a determining set (see Section 3.4), we need to address one last assumption. That is, given $\mathcal{S}_{\mathcal{TC}}$, does at least one *candidate for X'* exist?

3.3 Proof that there is always at least one Candidate for X'

Recall that the set \mathcal{ME} is formed by removing X' from $\mathcal{S}_{\mathcal{TS}\mathcal{C}}$. All points that are candidates for X' are obviously in $\mathcal{S}_{\mathcal{TS}\mathcal{C}}$ (i.e. Condition (1) states that X' is on l_2). However, if there is no point in the set of candidates for X' , then there is no possible X' to remove from $\mathcal{S}_{\mathcal{TS}\mathcal{C}}$. Thus, in this section, we will prove that the set of *candidates for X'* always contains at least one point and subsequently that the construction of \mathcal{ME} is always possible.

First, we will assume a specific construction of $\mathcal{S}_{\mathcal{TS}\mathcal{C}}$ and determine which points are candidates for X' . From this, we will determine the number of points that are candidates for X' depending on the value chosen for q . By proving that this number is always one or greater, we will show that \mathcal{ME} can always be constructed. Finally, we will use a group theoretic argument to prove that the same results apply regardless of how we construct $\mathcal{S}_{\mathcal{TS}\mathcal{C}}$.

Recall that we construct the set $\mathcal{S}_{\mathcal{TS}\mathcal{C}}$ from one conic, \mathcal{C} , and two lines, l_1 and l_2 , with certain points removed. In particular, let the intersection of l_1 and l_2 occur at P , a point on \mathcal{C} , and let l_1 and l_2 be tangent and secant lines to \mathcal{C} , respectively. Then, $\mathcal{S}_{\mathcal{TS}\mathcal{C}}$ is the above conic and two lines with the following points removed:

- the point P ,
- the point R that is on l_2 and on \mathcal{C} (but not equal to P), and
- the point Q that is on \mathcal{C} and not equal to R nor P .

Thus, to define a specific construction of $\mathcal{S}_{\mathcal{TS}\mathcal{C}}$, we must define \mathcal{C} , P , Q and R . In particular, let us call the first possible construction of $\mathcal{S}_{\mathcal{TS}\mathcal{C}}$ the set $\mathcal{S}_{\mathcal{TS}\mathcal{C}1}$ where \mathcal{C} is defined by the quadratic form $y^2 = xz$, and P , Q and R are the points $(1,0,0)$, $(1,1,1)$ and $(0,0,1)$, respectively. Note that it can easily be shown that these points lie on \mathcal{C} since they satisfy the given quadratic form.

Recall that the point (a, b, c) is on the line $[x, y, z]$ if and only if $(a, b, c) \cdot [x, y, z] = 0$, that is, $ax + by + cz = 0$. By manipulating this definition, we can easily prove that $l_1 = [0, 0, 1]$ and $l_2 = [0, 1, 0]$. We can verify that the lines are tangent and secant to \mathcal{C} as desired. It is also clear that l_1 contains P while l_2 contains P and Q . Figure 16 illustrates $\mathcal{S}_{\mathcal{TS}\mathcal{C}1}$.

Now that we have constructed $\mathcal{S}_{\mathcal{TS}\mathcal{C}1}$, we will prove the following theorem as to which points are candidates for X' .

Theorem 3.1. *Let $d \in GF(q)$ where $\frac{d}{4}$ and $\frac{d}{4} + 1$ are both squares, and $d \neq 0$. Then, given the construction of $\mathcal{S}_{\mathcal{TS}\mathcal{C}1}$, the candidates for X' are points of the form $(1, 0, d)$. Moreover, there are $\lceil \frac{q-3}{4} \rceil$ choices for d .*

Proof. To prove that all points of the form $(1, 0, d)$ are candidates for X' , we must show that all points of this form satisfy the needed three conditions.

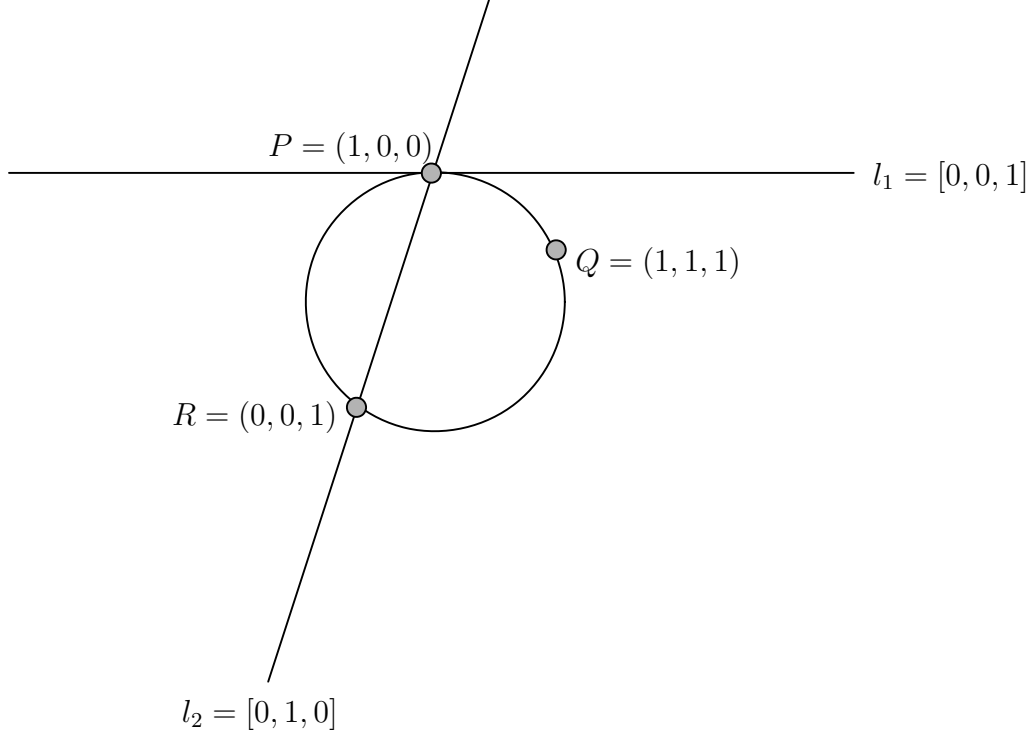


Figure 16: \mathcal{S}_{TSC1}

Let us first consider condition (1), X' is on l_2 . Since $l_2 = [0, 1, 0]$ and it is always the case that $[0, 1, 0] \cdot (1, 0, d) = 0$, it is clear that all points of the form $(1, 0, d)$ are on l_2 .

Now we will consider condition (2), X' is on a secant line to \mathcal{C} through A . Recall that A is the point where the tangent line through R intersects l_2 . It can easily be verified that the tangent line through R is $[1, 0, 0]$. Similarly, it is not difficult to show that $(0, 1, 0)$ lies on both $[1, 0, 0]$ and $l_2 = [0, 0, 1]$, and thus the point $A = (0, 1, 0)$.

Now, we must prove that all points of the form $(1, 0, d)$ are on secant lines to \mathcal{C} through A . First, note that all lines through $A = (0, 1, 0)$ and any point $(1, 0, d)$ must be of the form $[1, 0, -\frac{1}{d}]$. To determine at how many points $[1, 0, -\frac{1}{d}]$ intersects \mathcal{C} , we must do the following calculations.

$$\begin{aligned} \left[1, 0, -\frac{1}{d}\right] \cdot (1, x, x^2) &= 0 \\ -\frac{1}{d}x^2 + 1 &= 0 \\ x^2 &= d \end{aligned}$$

Since 4 is always a square and $\frac{d}{4}$ is a square, it follows that $4 \times \frac{d}{4} = d$ is also a square. Thus,

there are two possible solutions for x , which then implies that the line $[1, 0, -\frac{1}{d}]$ intersects \mathcal{C} at two points. That is, $(1, 0, d)$ is on the line $[1, 0, -\frac{1}{d}]$, which is a secant line to \mathcal{C} through A .

Lastly, we will consider condition (3), X' is not on a skew line to \mathcal{C} through G . Recall that G is the intersection point on l_1 with the secant line through RQ . Since $R = (0, 0, 1)$ and $Q = (1, 1, 1)$, it can easily be verified that this secant line is $[1, -1, 0]$. It is also not difficult to show that $(1, 1, 0)$ is on both $[1, -1, 0]$ and $l_1 = [0, 0, 1]$, and thus the point $G = (1, 1, 0)$.

Now, we must prove that all points of the form $(1, 0, d)$ are not on skew lines to \mathcal{C} through G . That is, $(1, 0, d)$ is always on a tangent or secant line to \mathcal{C} through G . Note that all lines through $G = (1, 1, 0)$ and any point $(1, 0, d)$ must be of the form $[1, -1, -\frac{1}{d}]$. To determine for how many points $[1, -1, -\frac{1}{d}]$ intersect with \mathcal{C} , we must do the following calculations.

$$\begin{aligned} \left[1, -1, -\frac{1}{d}\right] \cdot (1, x, x^2) &= 0 \\ -\frac{1}{d}x^2 - x + 1 &= 0 \\ x^2 + dx - d &= 0 \end{aligned}$$

Thus, the number of possible solutions to x depends on the discriminant, which equals $d^2 + 4d = d(d + 4)$. Since 4 , $\frac{d}{4}$ and $\frac{d}{4} + 1$ are squares, it follows that $4 \times \frac{d}{4} = d$ and $4 \times (\frac{d}{4} + 1) = d + 4$ are squares. That is, the discriminant, $d(d + 4) = d^2 + 4d$, is a square. Since $d \neq 0$ (i.e., $(1, 0, 0)$ is P), x has one solution if $d = -4$ or two possible solutions if $d \neq -4$. Thus, if $d = -4$ (which only happens for certain values of q that we identify later), the line $[1, -1, -\frac{1}{d}]$ intersects \mathcal{C} at one point. That is, $(1, 0, d)$ is on the line $[1, -1, -\frac{1}{d}]$, which is a tangent line (i.e., not on a skew line) to \mathcal{C} through G . On the other hand, if $d \neq -4$, the line $[1, -1, -\frac{1}{d}]$ intersects \mathcal{C} at two points. That is, $(1, 0, d)$ is on the line $[1, -1, -\frac{1}{d}]$, which is a secant line (i.e., not on a skew line) to \mathcal{C} through G . It is thus clear that in all possible cases, $(1, 0, d)$ is not on a skew line to \mathcal{C} through G .

With respect to $\mathcal{S}_{\mathcal{I}SC1}$, we now have proven that if $\frac{d}{4}$ and $\frac{d}{4} + 1$ are squares, then all points of the form $(1, 0, d)$ satisfy the needed three conditions to be candidates for X' . Moreover, we know that there are $q - 1$ points on l_2 that could be candidates for X' . It is well-known and easily verified that half of the non-zero elements in a finite field of odd characteristic are squares. Hence, there are $\frac{q-1}{2}$ choices for d that are squares. Some result on cyclotomy, which can be found in the book by Storer [4] for instance, argue that roughly half (i.e., about $\frac{q-1}{4}$) of these squares satisfy the condition that $\frac{d}{4} + 1$ is also square. One of these choices for d is $d = 0$, which clearly is unavailable since this gives us the point P . It follows that there are exactly $\lceil \frac{q-3}{4} \rceil$ candidates for X' of the form $(1, 0, d)$. For $q > 3$, this number is clearly non-zero. \square

Expanding from the results of Theorem 3.1, Corollary 3.2 presents a helpful result that allows X' to be easily found if q satisfies certain conditions.

Corollary 3.2. *Recall that H is the intersection point with l_2 of the tangent through G . Then, given the construction of S_{TSC1} , if $q \equiv 1 \pmod{4}$, $H = (1, 0, -4)$ is a candidate for X' .*

Proof. Recall from the proof of Theorem 3.1, we already know that the intersection with l_2 of the tangent line through G is $(1, 0, d)$ where $d = -4$. That is, $H = (1, 0, -4)$. We only need to show that -4 is a square.

We know that 4 is always a square, but is -1 a square? Let α be a primitive element for $GF(q)$ so that $\alpha^{q-1} = 1$, which then implies that $\alpha^{\frac{q-1}{2}} = -1$. Since $q \equiv 1 \pmod{4}$, it follows that $\frac{q-1}{4} = k$ for some integer k . Thus, there exists a y in $GF(q)$ such that $y = \alpha^{\frac{q-1}{4}}$. Then, note that $y^2 = \alpha^{\frac{q-1}{4}} \times \alpha^{\frac{q-1}{4}} = \alpha^{\frac{q-1}{2}} = -1$. That is, -1 is a square. Thus, since 4 and -1 are squares it is clear that $-4 = (-1)4$ is also a square. \square

We note that we can generalize both Theorem 3.1 and Corollary 3.2 so that the results hold regardless of how \mathcal{S}_{TSC} is constructed. Recall that we chose specific coordinates for P , Q and R on the conic \mathcal{C} defined by $y^2 = xz$ to construct \mathcal{S}_{TSC1} . However, the group $PG(2, q)$ acts 3-transitively on the conic \mathcal{C} , which implies that these three points on \mathcal{C} can be moved to any other three points. Thus, regardless of which points we select for the construction of \mathcal{S}_{TSC} , we know that there is always some candidate for X' as long as $q > 3$.

3.4 Proof that \mathcal{ME} is a determining set for all lines

Now that we know that the construction of the set \mathcal{ME} is always possible, all we need to do is show that \mathcal{ME} is a determining set for all lines in π . To do this, we will consider all of the intersection patterns of lines in π with the set \mathcal{ME} , which is shown in Table 4. Note that we let Y_i be any point on \mathcal{C} and in \mathcal{ME} . Also, recall that Figure 14 indicates the locations of important points in \mathcal{ME} while Figure 15 displays the set \mathcal{ME} .

As shown in Table 4, all possible lines are defined by at least two points and thus can be uniquely identified except for the following cases. However, it is shown that even in these cases, the lines can be uniquely identified.

1. The secant lines through PY_i only intersect \mathcal{ME} in one point on \mathcal{C} . However, these are the only lines that intersect \mathcal{C} in one point and no other points in \mathcal{ME} . Thus, they still have different intersection patterns from all other lines' intersections patterns with \mathcal{ME} .

type	Intersects with	\mathcal{C}	l_1	l_2
tangent	P	0	q	0
tangent	Q	0	B	1 or 0 if X' is on this line
tangent	R	0	A	0
tangent	Y_i	1	1	1 or 0 if X' is on the line
secant	QR	0	G	0
secant	QY_i	1	1	1 or 0 if X' is on the line
secant	RP	0	0	$q - 1$
secant	RY_i	1	1	0
secant	Y_iY_j	2	1	1 or 0 if X' is on the line
secant	PY_i	1	0	0
skew	X'	0	1	0
skew	not X'	0	1	1

Table 4: Set \mathcal{ME} incidence results

2. The tangent line through R and the secant line through QR only intersect \mathcal{ME} in points A and G on l_1 , respectively. While the skew line through X' only intersect \mathcal{ME} in one point on l_1 , X' is on a secant line through A and not on a skew line through G . That is, the skew lines through X' cannot intersect l_1 at A nor at G and thus the tangent line through R and the secant line through QR can be uniquely identified by their different intersection patterns with \mathcal{ME} .
3. The only remaining possible conflict is with the tangent line through Q if X' lies on it, for then this line only intersects \mathcal{ME} at B . However, if this is the case, then there clearly cannot be a skew line through X' and B . Then, there is no other line that only intersects \mathcal{ME} at B .

It is thus clear that any pair of lines in π has a different intersection pattern with \mathcal{ME} . Or, in other words, \mathcal{ME} is a determining set with $3q - 4$ points for all lines in π .

4 Constructions of determining sets with two conics and two lines

While in the previous sections we constructed determining sets from one conic and two lines, we will now consider the construction of determining sets from two conics and two lines. In particular, we will examine such a construction involving about half of the points from each of the two conics.

Let \mathcal{C}_1 be the conic defined by $y^2 = xz$, and let l_1 and l_2 be the tangent lines to \mathcal{C}_1 through $(0, 0, 1)$ and $(1, 0, 0)$, respectively. Also, let P be the intersection point of l_1 and l_2 .

Theorem 4.1. *The homogeneous coordinates for l_1 and l_2 are $l_1 = [1, 0, 0]$ and $l_2 = [0, 0, 1]$, and P is $(0, 1, 0)$.*

Proof. Let l have the homogeneous coordinate $[1, 0, 0]$. Then, we know that all points on l dotted with $[1, 0, 0]$ must equal zero. It is thus clear that all points on l must be of the form $(0, a, b)$. Now, any intersection point of l with \mathcal{C}_1 must satisfy the equation for \mathcal{C}_1 , $y^2 = xz$. That is, $a^2 = 0(b)$ or $a = 0$.

Hence, there is only one point on l that intersects \mathcal{C}_1 and that point is $(0, 0, b)$, which, when normalized, is equivalent to $(0, 0, 1)$. Thus, l is tangent to \mathcal{C}_1 at $(0, 0, 1)$, and so $l = l_1 = [1, 0, 0]$.

Similarly, it can be proven that all points on $[0, 0, 1]$ must be of the form $(d, e, 0)$ and l_2 is then tangent to \mathcal{C}_1 at $(1, 0, 0)$, as desired.

Now consider the intersection of l_1 and l_2 . It must be of the form $(0, a, b)$ and $(d, e, 0)$. The only possibility when normalized is $(0, 1, 0)$. Hence, the intersection point is $P = (0, 1, 0)$. \square

There are certain conditions that are vital to the eventual construction of the determining set involving l_1, l_2, \mathcal{C}_1 and another conic \mathcal{C}_2 . In particular, we do not want there to exist any lines through P that are skew to both conics, for there would be no way to distinguish the intersections of these skew lines through P . The following Theorem 4.4 is thus vital.

Theorem 4.2. *Let \mathcal{C}_1, l_1, l_2 be defined as above and let \mathcal{C}_2 be defined by $x^2 + y^2 + z^2 - 2xy + ezx - 2yz$ where $2 - e$ is a square. Then,*

1. l_1 and l_2 are tangent to \mathcal{C}_2 at the points $(1, 1, 0)$ and $(0, 1, 1)$,
2. all secant lines to \mathcal{C}_1 that contain P are skew to \mathcal{C}_2 , and
3. all secant lines to \mathcal{C}_2 that contain P are skew to \mathcal{C}_1 .

Moreover, the converse of this theorem holds true. That is, if the above three conditions are met, then $2 - e$ is a square. Note that Figure 17 displays this construction.

Proof. We first will prove statement (1). From the proof of Theorem 4.1, we know that points on l_1 are of the form $(0, a, b)$. Hence, if l_1 intersects with \mathcal{C}_2 , it will be at a point of the form $(0, a, b)$. That is, $x^2 + y^2 + z^2 - 2xy + ezx - 2yz = 0$ when $x = 0, y = a$ and $z = b$.

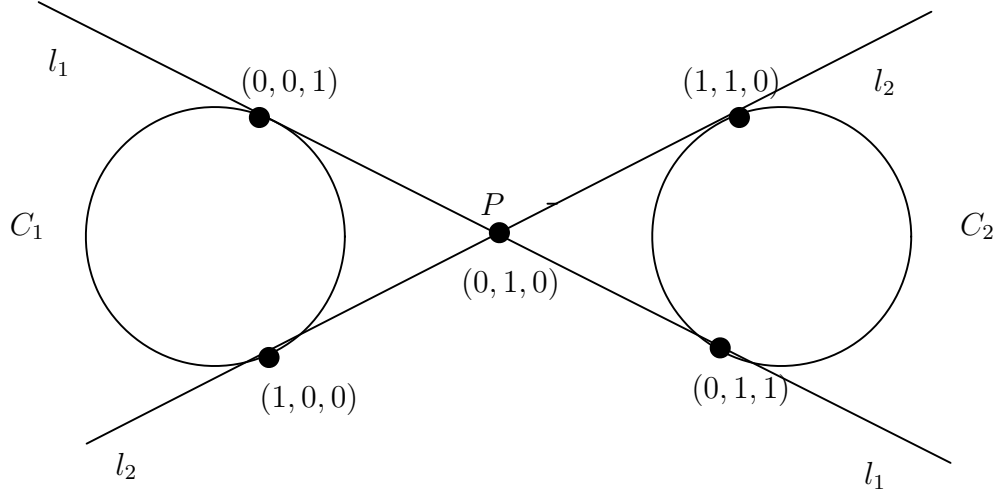


Figure 17: Two conics and two lines

We then obtain:

$$\begin{aligned}
 (0)^2 + a^2 + b^2 - 2(0)(a) + e(0)(b) - 2ab &= 0 \\
 a^2 + b^2 - 2ab &= 0 \\
 (a - b)^2 &= 0 \\
 (a - b) &= 0 \\
 a &= b.
 \end{aligned}$$

Hence, the points on l_1 that lie on \mathcal{C}_2 are of the form $(0, a, a)$, which when normalized is equal to $(0, 1, 1)$. Thus, l_1 is tangent to \mathcal{C}_2 at $(0, 1, 1)$. We can similarly prove that l_2 is tangent to \mathcal{C}_2 at the point $(1, 1, 0)$.

Now, it is clear that all lines through the point $P = (0, 1, 0)$ are of the form $[1, 0, z]$. Points on a line of the form $[1, 0, z]$ must be of the form either $(0, 1, 0)$ or $(1, b, \frac{-1}{z})$ for $z \neq 0$. In particular, we want to consider the lines through P that are secant to \mathcal{C}_1 . Such lines would have two points of the form $(1, b, \frac{-1}{z})$ as solutions to the quadratic form for $\mathcal{C}_1 : y^2 = xz$. That is, $b^2 = \frac{-1}{z}$. Hence lines of the form $[1, 0, z]$ (and thus contain P) are secant to \mathcal{C}_1 if and only if $\frac{-1}{z}$ is a square.

Now, assuming that $\frac{-1}{z}$ is a square (and hence the line $[1, 0, z]$ contains P and is secant to \mathcal{C}_1), can the line $[1, 0, z]$ also be secant to \mathcal{C}_2 ? To answer this question, we substitute the points on the line $[1, 0, z]$ into \mathcal{C}_2 to see if two solutions are possible. That is, we substitute

in $(1, b, \frac{-1}{z})$ into C_2 , as shown below.

$$1 + b^2 + \frac{1}{z^2} - 2b - \frac{e}{z} + \frac{2b}{z} = 0$$

$$b^2 + b \left(-2 + \frac{2}{z} \right) + \left(1 + \frac{1}{z^2} - \frac{e}{z} \right) = 0$$

The above only has two solutions for b if the discriminant is a nonzero square. That is,

$$\left(-2 + \frac{2}{z} \right)^2 - 4(1) \left(1 + \frac{1}{z^2} - \frac{e}{z} \right) = 0$$

$$4 - \frac{8}{z} + \frac{4}{z^2} - 4 - \frac{4}{z^2} + \frac{4e}{z} = 0$$

$$-\frac{8-4e}{z} = 0$$

$$4 \left(\frac{-1}{z} \right) (2-e) = 0$$

We know that 4 is a square and recall that we assumed that $\frac{-1}{z}$ is a square. Hence, there are only two solutions (and in fact any solutions) to the above if $2-e$ is a square. In other words, if $2-e$ is not a square, then the lines through P and secant to C_1 are skew to C_2 .

Statement (3) of Theorem 4.2 can be proven in the same manner as statement (2) was proven. Also note that the converse of this theorem can be proven by reversing the steps above. \square

Definition 4.3. Define the set \mathcal{T} in π as the set containing the points of C_1 , C_2 , l_1 and l_2 , but with the following points removed:

- the point P , the intersection of l_1 and l_2 ;
- the points $(0, 0, 1)$ and $(1, 0, 0)$, the points of tangency to the conics;
- one point from each of the sets $l \cap (C_1 \cup C_2)$ where l is a line through P that is secant to either C_1 or C_2 .

Figure 18 illustrates the set of points in \mathcal{T} .

Counting the numbers of points on the conics, and then on the lines, the total number of points in \mathcal{T} is:

$$|\mathcal{T}| = \frac{2q-2}{2} + 2q - 2$$

$$= 3q - 3$$

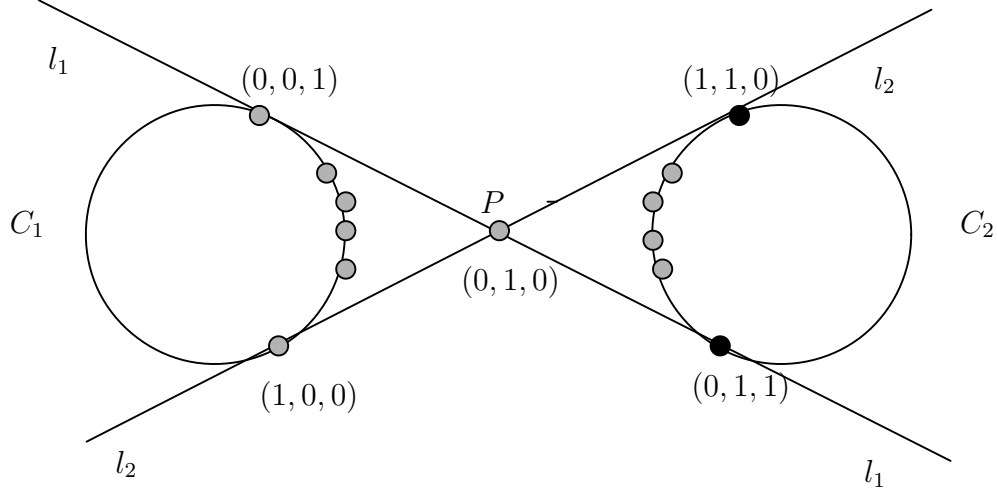


Figure 18: The set \mathcal{T}

Theorem 4.4. *The set \mathcal{T} is a determining set for all lines in π with $3q - 3$ points.*

Proof. Let W_i represent the $\frac{q-1}{2}$ points of \mathcal{C}_1 not in \mathcal{T} , and not equal to $(0, 0, 1)$ nor $(1, 0, 0)$. Let X_i represent all points of \mathcal{C}_1 and in \mathcal{T} . Also, let Y_i represent all $\frac{q-1}{2}$ points of \mathcal{C}_2 not in \mathcal{T} , and Z_i represent all points of \mathcal{C}_2 in \mathcal{T} and not equal to $(1, 1, 0)$ and $(0, 1, 1)$. Table 5 shows how lines in π meet our set \mathcal{T} .

First note that there are no skew lines through P , and hence the entry of NA, which stands for Not Applicable. The reason there are no skew lines through P can be shown through the following simple calculation. We know that P has exactly $q + 1$ lines through it. Two of those lines are the tangent lines l_1 and l_2 . Also, since we have established that there are $\frac{q-1}{2}$ secant lines to \mathcal{C}_1 through P that are skew to \mathcal{C}_2 (and $\frac{q-1}{2}$ secant lines to \mathcal{C}_2 through P that are skew to \mathcal{C}_1), there are a total of $\frac{q-1}{2} + \frac{q-1}{2} = q - 1$ such lines through P . Then, the number of tangent lines plus the number of secant lines equals $q + 1$ lines. Thus, it is not possible to have any skew lines through P .

Also, note that there is only one line that does not intersect \mathcal{T} and hence is uniquely identified. As for the two situations where lines intersect with P , such lines can be uniquely identified by intersecting \mathcal{T} at one point on either \mathcal{C}_1 or \mathcal{C}_2 and at no points on l_1 nor l_2 . All other possible lines intersect \mathcal{T} at two distinct points on l_1 and l_2 and thus can be uniquely identified.

Thus, we have shown that all lines in π have a different intersection with \mathcal{T} , and hence \mathcal{T} is a determining set for all lines in π . □

type	Intersects with	C_1	C_2	l_1	l_2
tangent to C_1 and C_2	$(0, 0, 1), (0, 1, 1)$	1	1	q	0
tangent to C_1 and C_2	$(1, 0, 0), (1, 1, 0)$	1	1	0	q
tangent to C_1	W_i	0	0	1	1
tangent to C_1	X_i	1	0	1	1
tangent to C_2	Y_i	0	0	1	1
tangent to C_2	Z_i	0	1	1	1
secant to C_1	$(0, 0, 1), (1, 0, 0)$	0	0	0	0
secant to C_1	$W_i W_j$	0	0	1	1
secant to C_1	$W_i X_j$ and not P	1	0	1	1
secant to C_1	$W_i X_j$ and P	1	0	0	0
secant to C_2	$X_i X_j$	2	0	1	1
secant to C_2	$Y_i Y_j$	0	0	1	1
secant to C_2	$Y_i Z_j$ and not P	0	1	1	1
secant to C_2	$Y_i Z_j$ and P	0	1	0	0
skew to C_1 and C_2	P	NA	NA	NA	NA
skew to C_1 and C_2	not P	0	0	1	1

Table 5: The set \mathcal{T} incidence results

5 Conclusions

By using Batten's idea of determining sets as explained in [1], we were able to construct eleven previously unknown determining sets, all of which can form the basis of a cryptosystem. While many of these determining sets contained fewer points than the vertex-less triangle, certain restrictions had to be in place (i.e., they were not determining sets for all lines in π). Also, some determining sets could not possess fewer points than the vertex-less triangle for reasons explained in Section 5.1.

In fact, the only determining set for *all* lines in π that contained fewer points than the vertex-less triangle was \mathcal{ME} . For this reason, \mathcal{ME} is certainly the most important result of this paper. While \mathcal{ME} is the only such determining set that we know of, we suspect other such determining sets may exist. In particular, we believe that the fundamental approach of this paper can be applied to find more determining sets, and thus allow for secure and previously unknown ways to construct cryptosystems. Other possible ways to construct new determining sets are touched upon in Section 5.2.

5.1 Why some determining sets can not have fewer than $3q - 3$ points

The determining sets \mathcal{S}_{SSC} , \mathcal{S}_{STC} and \mathcal{T} have $3q - 3$ points. The reason additional points cannot be removed from determining sets of these forms is as follows.

Although \mathcal{S}_{TSC} only has $3q - 3$ points, recall that we were able to use this set to create set \mathcal{ME} , which has $3q - 4$ points.

Now, let us consider the case of \mathcal{S}_{SSC} . Assume an additional point, X , is removed from the conic, \mathcal{C} . Then, the line through X and P will only intersect the set \mathcal{S}_{SSC} in the point P . However, the tangent line through P only intersects the set \mathcal{S}_{SSC} in the point P as well. Hence, it is not the case that all lines in the plane have different intersection patterns with our set, and so \mathcal{S}_{SSC} is not a determining set. Similarly, assume that an additional point Y is removed from one of the lines. Then the line through Y and Q (or R depending as to which line Y is on) will have no intersection with the set \mathcal{S}_{SSC} . However, the line through Q and R has no intersection with the set \mathcal{S}_{SSC} as well. Hence, for the same reason as above, \mathcal{S}_{SSC} can not be a determining set.

Lastly, let us consider the case with two conics, the set \mathcal{T} . If any additional point, X , is removed from \mathcal{C}_1 or \mathcal{C}_2 , then the line through P and X will not intersect \mathcal{T} . However, the line through $(0, 0, 1)$ and $(1, 0, 0)$ also does not intersect \mathcal{T} and thus can not be a determining set. Now, assume that a point Y is removed from l_1 and that the line through Y and $(1, 0, 0)$ intersects \mathcal{C}_1 at point Z . Then, the line through Y and $(1, 0, 0)$ only intersect the set \mathcal{T} at point Z . However, the line through P and Z also only intersects the set \mathcal{T} at point Z and thus \mathcal{T} can not be a determining set. Lastly, assume that an additional point W is removed from l_2 and that the line through W and $(0, 0, 1)$ intersects \mathcal{C}_1 at point V . Then, using the same logic as with removing X from l_1 , the line through W and $(0, 0, 1)$ and the line through P and W only intersect \mathcal{T} in the point V . Thus, the set \mathcal{T} cannot be a determining set.

5.2 New ideas

One obvious way to expand this paper's constructions of determining sets would be to explore other possible constructions involving two conics and two lines. In particular, one may explore lines that are secant and/or skew to one or both of the conics.

Similarly, more interesting determining sets may arise from constructions involving only one line and two conics. With the exception of \mathcal{ME} , we have shown that our determining sets either can not have less than $3q - 3$ points or must possess certain restrictions (i.e., cannot be a determining set for all lines in π). However, perhaps if different points were removed from the conic or lines, this would not be the case.

Lastly, there is no reason to limit our search for determining sets in π to two lines and

one or two conics. Since the possibilities are certainly not limited, we believe that more explorations of determining sets in finite projective planes will yield more interesting and new cryptosystems. Even more so, we believe it may be possible to uncover a methodology that will help to construct such interesting determining sets.

References

- [1] Lynn Margaret Batten, *Determining sets*, Australas. J. Combin. **22** (2000), 167–176. MR MR1795333 (2001i:05048)
- [2] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, second ed., Oxford Mathematical Monographs, The Clarendon Press Oxford University Press, New York, 1998. MR MR1612570 (99b:51006)
- [3] Daniel R. Hughes and Fred C. Piper, *Projective planes*, Springer-Verlag, New York, 1973, Graduate Texts in Mathematics, Vol. 6. MR MR0333959 (48 #12278)
- [4] Thomas Storer, *Cyclotomy and difference sets*, Lectures in Advanced Mathematics, No. 2, Markham Publishing Co., Chicago, Ill., 1967. MR MR0217033 (36 #128)