UNIVERZA NA PRIMORSKEM
FAKULTETA ZA MATEMATIKO, NARAVOSLOVJE IN
INFORMACIJSKE TEHNOLOGIJE

Master's thesis
(Magistrsko delo)

Secret sharing schemes arising from finite geometry

(Sheme delitve skrivnosti, ki izhajajo iz končne geometrije)

Ime in priimek: *Jelena Ilić*
Študijski program: *Matematične znanosti, 2. stopnja*
Mentor: *izr. prof. dr. György Kiss*

Koper, september 2022

Ključna dokumentacijska informacija

Ime in PRIIMEK: Jelena ILIĆ
Naslov magistrskega dela: Sheme delitve skrivnosti, ki izhajajo iz končne geometrije

Kraj: Koper
Leto: 2022

Število listov: 70 Število slik: 10
Število prilog: 1 Število strani prilog: 3
Število referenc: 32
Mentor: izr. prof. dr. György Kiss

UDK: 514.14(043.2)
Ključne besede: Sheme delitve skrivnosti, Projektivna geometrija, Afina geometrija, Sheme pragov, Sheme predelkov, Večnivojske sheme, Afino pravilni poligoni, Projektivni k-loki
Math. Subj. Class. (2020): 94A62, 05B25, 51E21
Izvleček:
Magistrsko delo se osredotoča na to, kako je sheme delitve skrivnosti mogoče videti skozi končno geometrijo z uporabo lastnosti afine in projektivne geometrije. Začnemo z uvedbo nekaterih temeljnih in dobro znanih pojmov in zasnov iz projektivne in afine geometrije, teorije grup in končnih polj. Poleg tega definiramo sheme delitve skrivnosti skozi štirifazni cikel, pojme skrbnikov, udeležencev, delnic in strukture dostopa. Nato opišemo najpomembnejše sheme skupne rabe skrivnosti, sheme pragov, predelkov in večnivojskih shem ter dokažemo, da je vsaka od teh shem popolna, tj. nobena ustrezna podmnožica skupnih rab ne izda nobenih informacij o skrivnosti. Nadaljujemo z določeno vrsto večnivojske sheme, $(2, s)$-nivojske sheme. Zaradi tega, ker obstajata dve skupini, katerih množice udeležencev označujemo s $\mathbf{S}$ in $\mathbf{T}$, razpravljamo o nekaterih mejah teh množic. Na ta način uvedemo afino pravilne poligone in projektivne k-loke, omenimo nekatere njihove lastnosti in rezultate ter na svoj način podamo več dokazov. Na koncu opišemo konstrukcije hierarhičnih množic $\mathbf{S}$ in $\mathbf{T}$ večnivojskih shem z uporabo dobljenih rezultatov.

Key document information

Name and SURNAME: Jelena ILIĆ
Title of the thesis: Secret sharing schemes arising from finite geometry

Place: Koper
Year: 2022

Number of pages: 70 Number of figures: 10
Number of appendices: 1 Number of appendix pages: 3
Number of references: 32
Mentor: Assoc. Prof. György Kiss, PhD

UDC: 514.14(043.2)
Keywords: Secret sharing schemes, Projective geometry, Affine geometry, Threshold schemes, Compartment Schemes, Multilevel Schemes, Affinely regular polygons, Projective k-arcs
Math. Subj. Class. (2020): 94A62, 05B25, 51E21
Abstract:
The master's thesis focuses on how secret sharing schemes can be seen through finite geometry, using the properties of affine and projective geometry. We start by introducing some fundamental and well-known notions and concepts from projective and affine geometry, group theory, and finite fields. Furthermore, we define the secret sharing schemes throughout the four-phase cycle, the notions of the dealer, participants, shares/shadows, and the access structure. Then, we describe the most important secret sharing schemes, Threshold, Compartment, and Multilevel schemes, and prove that each of these schemes is perfect, i.e., no proper subset of shares releases any information about the secret. We continue with the specified type of the multilevel scheme, $(2, s)$-level schemes. As there are two levels, whose sets of participants we denote by $\mathbf{S}$ and $\mathbf{T}$, we discuss some bounds on these sets. In that manner, we introduce the affinely regular polygons and projective k-arcs, mention some of their properties and results, and provide several proofs in our way. Finally, we describe constructions of the hierarchical sets $\mathbf{S}$ and $\mathbf{T}$ of multilevel schemes using the obtained results.

List of Contents

List of Figures

List of Appendices

List of Abbreviations

i.e.	that is
e.g.	for example
wrt	with respect to
$\forall$	for all
$\exists$	there exists

Acknowledgments

First, I would like to express my deepest thanks to my supervisor, Prof. György Kiss. His patience, support, constructive feedback, and wide knowledge were key motivations throughout my project. It was my pleasure to research this topic and expand my knowledge. I express my gratitude to FAMNIT for the scholarship during my studies.

Posebno se želim zahvaliti mojoj porodici i prijateljima na razumijevanju tokom pisanja završnog kao i na pružanju bezuslovne podrške u svim trenucima!

1 INTRODUCTION

To begin, I would like to quote my professor and mentor, who introduced me to this topic by telling the following story: "Imagine two shopkeepers who share a stand or a commodity store. Each has a key, and it is possible to open the store and sell goods only if both keys are present. They created some form of security sharing scheme." And such a simple example motivated me to choose this topic to research for my thesis.

As we can see, the notion of secret sharing schemes has always been present. It is now primarily linked to the process of data protection. What has become important today is to protect significant and sensitive data often exposed to attacks. Data is kept in databases and on servers, and it is frequently accessed, making it vulnerable to threats. Thus, many new methods to secure data and increase its security are still being developed. Secrecy sharing methods are just one way to protect data by sharing it. So, we can see a secret sharing scheme as a method of distributing a secret among a group of participants, where each of the participants is assigned a portion of the secret. A secret is reconstructed once a sufficient number of secret portions have been obtained. Secret sharing schemes mostly rely on cryptography, coding theory, and finite geometry. In this project, we will mainly consider and investigate their construction from the aspect of finite geometry. Given this, we need to establish plenty of new terms that we will use throughout the project to help us understand and comprehend what is ahead. To clarify the notion of a secret sharing scheme, let us consider the following example. Suppose that you want to construct a secret X, n-bit string and split it into partial secrets, called shares so that it can only be reconstructed if at least two shares are known. We use a projective plane $\mathrm{PG}(2, q)$ to build such a secret sharing method. To describe what $\mathrm{PG}(2, q)$ is, we actually need to define a projective plane.

1.1 PROJECTIVE GEOMETRY

Let us briefly go through the notation we are going to use. We use upper and lower case Latin letters to represent the points and the lines, respectively. Moreover, if the line l contains a point P, or a point P is incident with the line l, we simply say that P is on l or $P \in l$. A line passing through specific two points, say P and Q, will be denoted by PQ. On the other hand, the point intersecting two lines, say p and q, is some point X such that $X = p \cap q$.

In layman's terms, we can see a *projective plane* as the Euclidean plane extended with additional points at infinity where a class of parallel lines intersects and the line at infinity consisting of all the points at infinity. More precisely, we refer to the projective plane if the incidence geometry $\Pi = (\mathcal{P}, \mathcal{E}, I)$ satisfies the following axioms:

- **P1** : For any two different elements in $\mathcal{P}$, there is exactly one element in $\mathcal{E}$ such that it is in I relation to both elements in $\mathcal{P}$. In other words, we say there exists a unique line through any two different points.
- **P2** : For any two different elements in $\mathcal{E}$, there is exactly one element in $\mathcal{P}$ such that it is in I relation to both elements in $\mathcal{E}$. In other words, two lines intersect in a unique point.
- **P3** : Each element of $\mathcal{E}$ has at least three different elements of $\mathcal{P}$ related by the I relation.
- **P4** : Each element of $\mathcal{P}$ has at least three different elements of $\mathcal{E}$ related by the I relation.

The classical projective plane meets the axioms of abstract projective planes. There exist finite structures, too. In the following figure, we represent an example of the projective plane, named the *Fano plane*. One can easily check that it satisfies all the axioms.

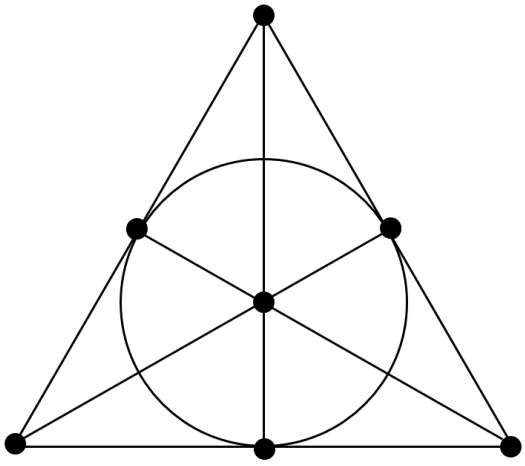

Figure 1: Fano plane.

One can show that $\mathrm{PG}(2, \mathbb{F})$ is a projective plane by applying the Dimension Theorem from linear algebra. Let us also recall what this theorem states.

Theorem 1.1 (Dimension Formula)**.** *If V is a finite-dimensional vector space, with its subspaces U and W, then*

$$\dim(U \cup W) = \dim(U) + \dim(W) - \dim(U \cap W).$$

It is also useful to mention some of the projective planes' characteristics. We say that the order of the projective plane is n if it has a line that is incident to $n+1$ points. Furthermore, if there is such a line, then:

- every line of such a plane contains $n + 1$ points,
- every point of such a plane lies on $n + 1$ lines,
- this plane contains the same number of points and lines, i.e., $n^2 + n + 1$.

Once we have projective planes, we could also extend our definition to the 3-dimensional *projective space*. Intuitively, it contains all the points, lines, and planes as the Euclidean space with additional points, called points at infinity, the additional lines, called lines at infinity, and the additional plane called the plane at infinity. The parallel classes of lines correspond to the points at infinity, and the parallel classes of planes correspond to the lines at infinity. Finally, the plane at infinity contains only the points and lines at infinity. For the classical projective spaces, we have the following incidence properties:

- Two different points determine a unique line.
- Every three non-collinear points lie on a unique plane.
- Every line lies on a plane or intersects it in a unique point, i.e., if we denote a point by P, a line by l and a plane by π, then $l \in \pi$ or $l \cap \pi = P$.
- Two distinct planes intersect in a line.
- Two distinct lines can either intersect in a unique point, or we have the skew lines.

There are higher dimensional projective spaces, too. If n is the dimension of the finite projective space, then

- the subspaces of dimension 0 are points,
- the subspaces of dimension 1 are lines,
- the subspaces of dimension 2 are planes,
- the subspaces of dimension $n - 1$ are hyperplanes.

Now, we are ready to define the notion of PG(n, q). Consider the vector space of dimension $n+1$, say V_{n+1}, over the finite field $GF(q)$. Then, the n-dimensional projective space PG(n, q) is the geometry whose d-dimensional subspaces are the $(d+1)$-dimensional subspaces of V_{n+1} for $d \in \{0, 1, ..., n\}$. Moreover, the number of d-dimensional subspaces of PG(n, q) is $\begin{bmatrix} n+1 \\ d+1 \end{bmatrix}_q$, where

$$\begin{bmatrix} n \\ d \end{bmatrix}_q = \frac{(q^n-1)(q^n-q)\cdots(q^n-q^{d-1})}{(q^d-1)(q^d-q)\cdots(q^d-q^{d-1})},$$

is known as *Gaussian binomial* or *q-nomial coefficients*.

As the Euclidean space has its own Cartesian coordinates, projective space also has its coordinates, known as *homogeneous coordinates*. Let P be an arbitrary point with a representative vector $\mathbf{x} = (x_0, x_1, x_2, \ldots, x_n)$. Then, the homogeneous coordinates corresponding to P are $(x_0 : x_1 : \cdots : x_n)$. If $\mathbf{x} = (x_0, x_1, \ldots, x_n)$ and $\mathbf{y} = (y_0, y_1, \ldots, y_n)$ are two vectors such that $x_i = \lambda y_i$, $0 \neq \lambda \in GF(q)$ for every $i = 0, 1, \ldots, n$, we say that $\mathbf{x}$ is in a relation with $\mathbf{y}$, and since this is an equivalence relation, we denote by $[\mathbf{x}]$ the equivalence classes of vector $\mathbf{x}$.
Additionally, suppose that $\mathbf{u}^T = (u_0, u_1, \ldots, u_n)$ defines a hyperplane Σ. Then, the homogeneous coordinates corresponding to Σ are $[u_0 : u_1 : \cdots : u_n]$. Similarly as in the case of representative vector of point, if we have $\mathbf{u}^T = (u_0, u_1, \ldots, u_n)$ and $\mathbf{v}^T = (v_0, v_1, \ldots, v_n)$ such that $\mathbf{u}^T = \lambda \mathbf{v}^T$, $0 \neq \lambda \in GF(q)$, for every $i = 0, 1, \ldots, n$, then they define the same hyperplane.

Let us go back to the planar case. The concept of homogeneous coordinates aids in the formulation of quadratic curves. The set of points with coordinates satisfying an equation $F(X_0, X_1, X_2) = 0$, where F is a homogeneous quadratic polynomial, is called the *quadratic curve*.
If $F(X_0, X_1, X_2) = \sum_{i,j=0}^{2} c_{i,j} X_i X_j$ and q is odd, we can also define quadratic curves as a set of points satisfying the equation $XAX^T = 0$, where A is the matrix of the curve such that:

$$a_{i,j} = \begin{cases} c_{i,i}, & \text{if } i = j, \\ \frac{1}{2}(c_{i,j} + c_{j,i}), & \text{if } i \neq j. \end{cases}.$$

Moreover, the notions of degenerate and non-degenerate quadratic curves chould also be mentioned. Since their definitions include some new terms, let us also explain those. Suppose that the curve $\mathcal{Q}$ is given by a matrix A. If $\mathbf{p}A\mathbf{q}^T = 0$, then we say that P and Q are *conjugate* with respect to $\mathcal{Q}$. Furthermore, we say that the point is *self-conjugate* if it is conjugate with itself. Let P be a point, $\mathcal{Q}$ be a quadratic curve, and $\mathcal{P}$ be a set of points conjugate to P wrt $\mathcal{Q}$.

We distinguish two types of points depending on $\mathcal{P}$. If it is a line, we call P an *ordinary point*, and if it is the whole plane, we call it a *singular point*. Now, the curve $\mathcal{Q}$ containing no singular points is *non-degenerate* and *degenerate* if it contains at least one singular point. In terms of the curve given by the matrix A, the curve is said to be degenerate iff $\det(A) = 0$. Furthermore, a non-degenerate quadratic curve in $\mathrm{PG}(2, q)$ containing at least one point in the plane represents a conic.

Going a step further, it will be nice to introduce some combinatorially defined sets of points in the projective planes. They play an important role in mathematical branches, such as coding theory, cryptography, and graph theory.

The first one which is worth mentioning is an arc. The *arc* is a set of points in a finite projective plane such that no three are collinear. Moreover, the arc consisting of precisely k points is called the *k-arc*. When it is not contained in any $(k+1)$-arc, we say that it is *complete*. In a projective plane, every line intersects with the arc in at most 2 points. Regarding the number of points at which the line l intersects some arc κ, we have the following three cases:

- if $|l \cap \kappa| = 2$, then l is called a *secant* to κ,
- if $|l \cap \kappa| = 1$, then l is called a *tangent* to κ,
- if $|l \cap \kappa| = 0$, then l is called an *external line* to κ.

There is a very nice feature concerning the secants, and it says that the secants to a complete k-arc in a finite plane cover all the points in that plane. Moreover, Lunelli and Sce [13] found that for the complete k-arc in a finite projective plane of order n, we have the following bound:

$$n < \frac{k(k-1)}{2} \iff \sqrt{2n} < k.$$

A parity of n also plays a role, as

$$k \leq \begin{cases} n+1, & \text{if } n \text{ is odd} \\ n+2, & \text{if } n \text{ is even} \end{cases}.$$

When k reaches the above bounds, we are talking about special k-arcs known as ovals and hyperovals. More precisely, in a plane of order n, we call

- $(n+1)$-arc an *oval*,
- $(n+2)$-arc a *hyperoval*.

Hence, oval exists in the projective planes $\mathrm{PG}(2,q)$ for all q, while hyperoval exists only if q is even.

A definition of k-arcs can now be extended to that of (k,n)-arcs. In a plane of order q, a set of points κ is called a (k,n)-*arc* if $|\kappa| = n$, each line intersects κ in at most n points and there is a line intersecting κ in precisely n points. In such a plane, the following bound is also established:

$$k \leq nq - q + n = 1 + (n-1)(q+1).$$

We say that κ is maximal, when equality occurs. For more on this, we refer the reader to [13].

All of the mentioned concepts are essential in the study of non-linear geometric objects in finite geometry, as well as in practical application. What will be our main interest is their application in secret sharing schemes. Before the secret sharing scheme introduction, let us also define and list some properties of the affine geometry.

1.2 AFFINE GEOMETRY

Previuosly, we have discussed the notion of the projective plane. If we remove a line from the projective plane $(\mathcal{P}, \mathcal{E}, I)$ together with all of its points, what is left over is a structure $(\mathcal{P}', \mathcal{E}', I')$, where I' is the restriction of I onto $\mathcal{P}' \times \mathcal{E}'$. We call it an *affine plane* if it satisfies the following axioms:

- **A1** : For any two different elements in $\mathcal{P}'$, there is exactly one element in $\mathcal{E}'$ such that it is in I' relation to both elements in $\mathcal{P}'$. In other words, we say there exists a unique line through any two different points.
- **A2** : If a point $P \in \mathcal{P}'$ is not in I' relation with $e \in \mathcal{E}'$, then there exists an element of $\mathcal{E}'$ that is in relation I' with P but it is not in I' relation with any element from $\mathcal{P}'$ being in relation I' with e. In other words, if we have a point and a line that does not contain that point, there exists a unique line containing the given point and is parallel to the given line.
- **A3** : Each element of $\mathcal{E}'$ has at least two different elements of $\mathcal{P}'$.
- **A4** : Each element of $\mathcal{P}'$ has at least three different elements of $\mathcal{E}'$ related by the I' relation.

Reprahsing the stated axioms, we could also define $\mathcal{S} = (\mathcal{P}, \mathcal{L}, I)$ as an affine plane if the following axioms are satisfied:

- **A1** : For any two different points, there is a unique line containing them.
- **A2** : For any non-incident point-line pair (P, l), there exists a unique line m such that $P\ I\ l$ and $l \cap m = \emptyset$.
- **A3** : There exist three non-collinear points.

The axiom of parallelism is a common name for the second axiom. In terms of affine geometry, if lines l and m do not have a common point, we can say they are parallel. Moreover, the set of all lines in an affine plane may be partitioned into parallel classes. It is important to mention that our definition of the affine plane makes no assumptions about the concept of angle, distance, or any other metric property. So, when we ignore the metric concepts of distance and angle, the remaining geometry is considered an affine geometry. In affine geometry, properties are preserved by parallel projection from one plane to another. One of the characteristics of parallels discovered by Pappus of Alexandria, known also as Pappus' law, has been adopted as a principle in affine geometry. Assume that P, Q, and R are on one line and P', Q' and R' are on another one. If the lines PQ' and $P'Q$ are parallel, as well as the lines QR' and $Q'R$, then the lines RP' and $R'P$ are also parallel.

In the following figure, we represent an example of the affine plane $\mathrm{AG}(2, 3)$. One can easily check that it satisfies all the axioms.

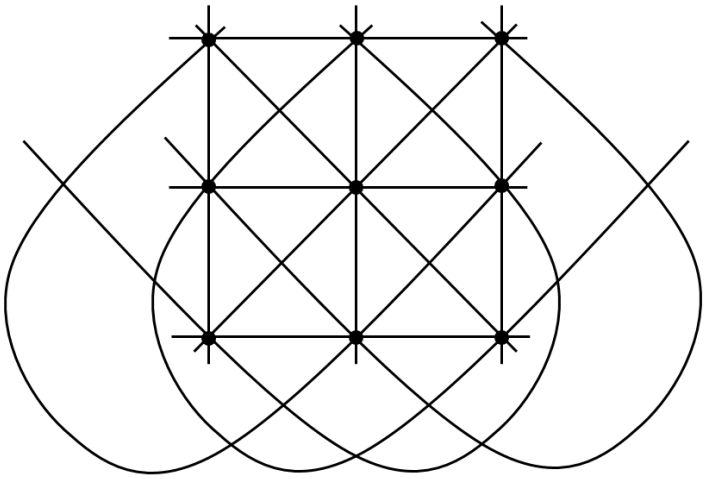

Figure 2: $\mathrm{AG}(2, 3)$.

As in the case of projective plane, let us list some combinatorial properties of an affine plane. If $\mathcal{A}$ is an affine plane having a line incident with n points, then

- every line in $\mathcal{A}$ is incident with n points,
- every point in $\mathcal{A}$ is incident with $n+1$ lines,
- $\mathcal{A}$ consists of n^2 points and n^2+n lines.

Moreover, n is called the order of the affine plane $\mathcal{A}$.

Affine planes and projective planes are closely related. For each class of parallel lines in the affine plane $\mathcal{A}$, add an ideal point (also known as the point at infinity). Then, add this point to every line in that parallel class. Finally, make a line through the ideal points or points at infinity to obtain the line at infinity, l_∞. The projective closure also known as the projective completion of the affine plane $\mathcal{A}$ is the name given to the resulting structure. Similar to this, if $\mathcal{P}$ is any projective plane, and l is any line, then removing the line l and all of its points from $\mathcal{P}$ will result in an affine plane $\mathcal{P}\backslash l$. Parallelism is an equivalence relation. Reflexivity and symmetry follow trivially, while transitivity arises from the second axiom.

1.3 GROUP THEORY

We will briefly mention a few necessary concepts from group theory. Let G be a nonempty set together with a binary operation. Then G is called a group under this operation, if the following conditions hold (the operation is the multiplication):

- *Closure*: $\forall a, b \in G \Rightarrow ab \in G$,
- *Identity*: There exists an element, usually denoted by e, such that $\forall a \in G$, $ea = ae = a$,
- *Inverses*: $\forall a \in G, \exists a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = e$,
- *Associativity*: The operation is associative, i.e., $\forall a, b, c \in G$, we have that $(ab)c = a(bc)$.

A group G is called cyclic if there is an element $a \in G$ such that $G = \langle a \rangle = \{a^n |\ n \in \mathbb{Z}\}$. We call an element a a generator of G. The order of the group corresponds to its size. If G is a group of order n, i.e., $|G| = n$, then $a^n = 1$, $\forall a \in G$ with 1 being the identity element and $a^i = a^{i \pmod n}$, $\forall a \in G$ and $\forall i \in \mathbb{Z}$.

The central theorem of group theory and abstract algebra is Lagrange theorem. It states that for any finite group say G with $H \leq G$, the order of H divides the order of G, i.e., $|H| \mid |G|$.

Let G be a group, $H \subset G$ and $g \in G$ and let

$$gH = \{gh : h \in H\}.$$

Sometimes the operation is denoted by ,,+" (for example the additive group of a field) and in this case

$$g + H = \{g + h : h \in H\}.$$

When $H \leq G$, the sets of the form $g + H$ or gH are called the left cosets of H in G. In a similar way, the right cosets are defined. Furthermore, two left (right) cosets are either disjoint or equal and they have the same cardinality.
Moreover, as we will need the following notion in the fourth chapter, let us also define the addition of two cosets. If $H \subset (GF(q), +)$, and G_1 is a coset of H, then

$$\begin{aligned} G_1 + G_1 &= \{g_i + g_j : g_i \in G_1, g_j \in G_1\} \\ &= \{(g + h_1) + (g + h_2) : h_1, h_2 \in H\} \\ &= \{2g + h_3 : h_3 \in H\}. \end{aligned}$$

1.4 FINITE FIELDS

Let us go through a few fundamental concepts relating to finite fields. First of all, the order of every finite field is a power of a prime. Moreover, for any prime power q, there exists a unique field (up to isomoprhism) containg q elements. We denote this field by $GF(q)$. The multiplicative group $GF(q)\backslash\{0\}$ of $GF(q)$ is cyclic. It means that there exists some element, say g, such that every other member of the group can be expressed as a power of g. We name such an element a generator. The additive group of $GF(q)$, with $q = p^r$, is an elementary Abelian p-group. It means that any element of $GF(q)$ will result in 0 if added to itself p times, and the field has characteristic p. Thus, Binomial Theorem implies that $(a + b)^p = a^p + b^p$ for any $a, b \in GF(q)$. Hence, the mapping $x \to x^p$ is a field automorphism of $GF(q)$.
When q is odd, exactly half of the nonzero elements are squares and the other half are nonsquares. The quadratic equation $aX^2 + bX + c = 0$, with $a, b, c \in GF(q)$ and $a \neq 0$ for odd q is irreducible if and only if the discriminant $b^2 - 4ac = 0$ is a nonsquare in $GF(q)$. In the third chapter, at some point, we will redefine q so the field in question is $GF(q^2)$. The automorphism $\phi : x \to x^q$ is also called conjugation, as it is equivalent to complex conjugation on the field of complex numbers with the real numbers as the fixed field.

Let $G(q) = \{a + ib, a, b \in GF(q)\}$, where $q = p^r$ and p is an odd prime. Let $i^2 = m$, where m is a non-square. We can choose $i^2 = -1$ if and only if $q \equiv 3 \pmod 4$. The set $G(q)$ is the set of Gaussian integers over $GF(q)$. If we denote by $\otimes$ the Cartesian product, then the set $G(q)$ with the operations

- $\oplus$: $G(q) \oplus G(q) \to G(q)$,
  $(a_1 + ib_1, a_2 + ib_2) \to (a_1 + ib_1) \oplus (a_2 + ib_2) = (a_1 + a_2) + i(b_1 + b_2)$, and
- $*$: $G(q) \otimes G(q) \to G(q)$,
  $(a_1 + ib_1, a_2 + ib_2) \to (a_1 + ib_1) \otimes (a_2 + ib_2) = (a_1a_2 + mb_1b_2) + i(a_1b_2 + a_2b_1)$.

is the field, i.e., $\langle G(q), \oplus, * \rangle$ is a field and it is isomorphic to $GF(q^2)$.

1.5 SUMMARY OF THE THESIS

Let us now briefly explain the summary of the thesis.

In the first chapter, i.e., in the introduction, we provided the basic notions and properties of the affine and projective planes and spaces, group theory and finite fields. We introduced the secret sharing schemes and the schemes we'll be dealing with. We include a summary of each chapter.

In the second chapter, we will define the secret sharing schemes throughout the four-phase cycle, the notions of the dealer, participants, shares/shadows, and the access structure. Furthermore, we will describe each of the schemes mentioned in the introduction, i.e., Threshold, Compartment, and Multilevel schemes, provide some basic examples, and prove that each of these schemes is perfect, i.e., no proper subset of shares releases any information about the secret. We will also include some results we come up with.

In the third chapter, we will continue with the specified type of the multilevel scheme, $(2, s)$-level schemes. As there are two levels, whose sets of participants we denote by $\mathbf{S}$ and $\mathbf{T}$, we will discuss some bounds on these sets. In that manner, we will introduce the affinely regular polygons and projective k-arcs, using some of their properties and results and providing some of the proofs in our way.

In the fourth chapter, we will discuss some specific constructions of sets $\mathbf{S}$ and $\mathbf{T}$ satisfying the predefined conditions. These constructions mostly come from article [3]. We will provide detailed proofs and explanations for all of them.

In the last chapter, we will summarize the important results we mentioned and found throughout the project. Even though most of the things throughout the thesis are well-known and proven, we give some other insight into these results and how they can be applied.

2 SECRET SHARING SCHEMES

As already mentioned, secrecy sharing methods are just one way to protect data by sharing it. Throughout the project, we will deal with the construction and application of secret sharing schemes, their qualifications, and properties. In cryptography, the method of *secret sharing schemes* refers to any method for sharing a secret or data among a group of people so that each person owns a piece of it. *Cryptography* is a scientific discipline that deals with the study of methods for sending messages in such a form that only those for whom they are intended can read them. We would say that it serves two main purposes:

- *Enciphering* - the process of transforming a message or a piece of information into a code or cipher that ensures data privacy.
- *Authentication* - the process of confirming a user's identification and detecting data modifications.

As cryptographic systems are based on secret keys, key management is one of the most difficult and essential issues that cryptographic system users face. The goal of its concepts and processes is to provide a secure way to distribute keys among a group of participants in a cryptographic scheme. According to Beutelspacher and Rosenbaum [2], there are the following aspects of the key management: generation, distribution, storage and deletion of secret data. In that manner, we will consider the problem of storing secret data, or, to be more specific, the conflict between data secrecy and availability, which is efficiently solved by secret sharing methods. We have seen earlier that a secret sharing scheme is a method of restricting access to a secret to only previously determined subsets of a group of authorized participants. As suggested in the article [21], thinking of the participants as the points and the access group as the blocks, we could model such a scheme using finite geometry. It is finite as we have a finite number of participants. The reason for taking the geometry is that, as Beutelspacher and Rosenbaum [2] pointed out, an issue given in an application could be translated into a geometrical problem, commonly only considering the incidence structure. The applications focus on projective and affine spaces over finite fields because of their calculation efficiency. A scheme that is built on geometry preserves all of the underlying geometric structure. Furthermore, geometries' complex structures are used to create efficient models for hierarchical structures and systems.

Unlike some algorithms, the security of crypto-systems derived from geometry can be verified as they rely on proven assumptions. A secret sharing scheme consists of a person who holds a secret, called a *dealer*, and participants called *users* to whom the dealer distributes the parts of the secrets, also known as *shares*. We denote the set of participants by $\mathcal{P}$. Once we have a set of participants $\mathcal{P}$, we can define the access structure $\mathcal{A}$ that specifies subsets of $\mathcal{P}$ authorized to reconstruct the secret. We will stick with the definition given in [18].

Definition 2.1. A set of subsets $\mathcal{A} \subseteq 2^{\mathcal{P}}$ is considered *access structure* if it is monotone, i.e., if $A \in \mathcal{A}$ and $A \subset B$, then also $B \in \mathcal{A}$.

Since we will consider only the perfect secret sharing schemes, we should also define the meaning of perfect in that sense.

Definition 2.2. A secret sharing scheme is *perfect* if the probability of revealing the secret is the same for all non-legal combinations of participants.

We can also define the secret sharing schemes using the notion of random variables and it is given in [18].

Definition 2.3. A *perfect secret sharing scheme*, having an access structure $\mathcal{A}$ and a set of participants $\mathcal{P}$, is a set of random variables X_i, $\forall i \in \mathcal{P}$ and a secret X, with:

- Reconstruction: If $A \in \mathcal{A}$, then the set $\{X_i : i \in A\}$ determines the secret X.
- Perfectness: If $B \notin \mathcal{A}$, then the set $\{X_i : i \in B\}$ is independent of the secret X.

Let us now go through the four-phase cycle of the secret sharing scheme as Beutelspacher and Rosenbaum did in their book [2]. They categorized the following phases:

1. The definition phase,
2. The mathematical phase,
3. Generation of the secret,
4. The application phase.

Let us briefly explain the meaning of each of them.

1. *The definition phase:* As its name says, we should define something, i.e., we should determine who would be able to reconstruct the secret as suggested by the Definition 2.3. The process of reconstruction involves the access structure predefined by the service provider. The second thing the service provider pays attention to is the probability of deception.

It is not possible to create a 100% secure system, but in a geometric secret sharing scheme, we could lower the attacker's probability of success as much as we wanted. In general, the probability of $p = 10^{-20}$ is chosen as the tolerance for an illegal reconstruction.

2. *The mathematical phase:* The goal is to provide structures that mathematicians will analyze. The underlying algebra of projective geometry has appeared to be quite useful in the construction of secret sharing schemes. More on this will be given later on.

3. *Generation of the secret:* Once the dealer (the service provider) specifies the secret, its portions called shares are determined by the method mathematicians established and then distributed to the users (participants). The secret, as well as shares, are entirely the dealer's responsibility. It is unaffected by the requirements that have been specified or the mathematical framework that has been adopted.

4. *The application phase:* The final phase entails reconstructing the secret from the legal share constellations.

    - The first, referred to as access, requires a comparison of the reconstructed value and the secret, and if they match, access is granted.
    - The second one involves the applications designed to generate secrets, such as transport of the cryptographic key to a computer, where it is supposed to be reconstructed and persuaded that the estimated result is not only random but the secret indeed with a high probability. Due to this, robust secret sharing schemes have been created.

A secret sharing scheme construction indicates a concrete demonstration of the scheme. We can see it as a mapping of the shares and secret onto the elements of an incidence structure, such that the scheme's properties are reflected in the incidence structure's properties [21]. Let us now define and discuss the geometric construction of the secret sharing schemes described in the introduction.

2.1 THRESHOLD SHARING SCHEMES

In 1979, Adi Shamir [25] and George Blakley [5] came up with the concept of a secret sharing scheme. They introduced the term (t, n)-threshold scheme to describe a scheme in which any t out of n shares can reconstruct the secret X, but $t - 1$ or fewer shares do not reveal any information of X. This number t is also known as the *quorum*. Shamir's solution relied on polynomial interpolation, while Blakley employed hyperplane geometry to address the secret sharing problem.

Many other techniques of sharing secrets have emerged since Shamir and Blakley proposed the idea and their methodologies, based on other mathematical tools and rules. Let us go through the core concept of Shamir's and Blakely's construction. We adopt the descripction given in [5, 18, 25].

Shamir's construction: Denote the users by the non-zero elements of a finite field $\mathbb{F}$ and by p the polynomial, whose degree is at most $t-1$ over $\mathbb{F}$ chosen at random. The share that corresponds to the user i is $p(i)$, while the secret corresponds to $p(0)$.

Blakely's construction: Denote by V a t-dimensional vector space over a finite field. Pick a point $X \in V$ randomly and take the first coordinate of X as the secret. The shares correspond to the hyperplanes that contain X and are specified by their normal vectors in V.

2.1.1 Construction

We will describe how threshold schemes can be constructed in $\mathbf{P} = \mathrm{PG}(t, q)$. Before this, let us look at the case when $t = 2$. It was also mentioned in the beginning when we introduced the notion of the projective plane.

Example 2.4. When $t = 2$, at least 2 shares are needed to reconstruct the secret. So far, there is a line l, and we know that $X \in l$.
If we only know one share, i.e., one point, then by the combinatorial properties of the projective plane, there are $q+1$ lines through this point and, hence, $q+1$ possibilities to intersect these lines with l to obtain the secret. So, one share is not enough.
If we know two shares, there is a unique line m through them by the axioms. Hence, $X = m \cap l$, and so, 2 shares are enough.

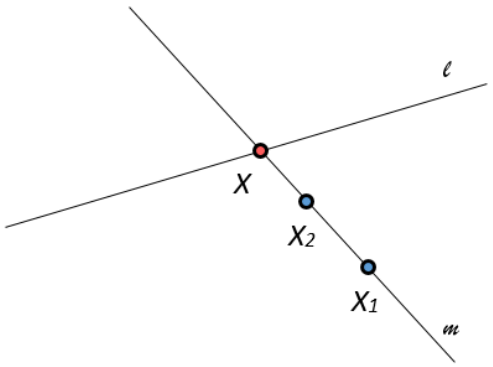

Figure 3: Trivial threshold scheme for $t = 2$.

Let us describe the construction in general as given in [2]. First, fix a line l that contains a secret X predetermined by the dealer. Apart from the dealer, the other points of l are also potential secrets. There is a method that allows the dealer to select the hyperplane $\mathbf{H}$ such that:

- $\mathbf{H}$ goes through X,
- $\mathbf{H}$ does not contain l, i.e., $l \notin \mathbf{H}$,
- $\mathbf{H}$ contains a set of points $\mathbf{T}$ in a general position containing X, where points distinct from X are taken into account as shares.

The following explanation clarifies how the given construction can be seen as a secret sharing scheme.

1. The dealer outlined the conditions. We will soon show that the probability of every non-legal constellation is the same, proving the perfectness of the system, which will complete the definition phase.
2. The mathematical phase is satisfied with the construction based on the geometry.
3. The dealer fixed the line l and chose shares as elements of $\mathbf{T}$ that will generate the secret.
4. In the last phase, shares are sent to the system, which further evaluates the subspace through them and intersects it with l. By sending at least t shares to the system, as the points are in a general position, it will yield to the generated subspace $\mathbf{H}$. Hence, intersecting the hyperplane $\mathbf{H}$ and the line l, with only a secret X in common, gives the correct secret X, confirming that any t participants can reconstruct the secret.

We could also describe the construction of the threshold scheme as done in [14]. Suppose that $\mathbf{H}$ is a hyperplane in $\mathrm{PG}(t, q)$, $X, X_1, \ldots, X_n$ is an $(n+1)$-arc in $\mathbf{H}$ and l is a line with $\mathbf{H} \cap l = X$. All the points X_1, X_2, $\ldots$, X_n represent the shares distributed to the users who are all familiar with the information that $X \in l$, whereas the hyperplane $\mathbf{H}$ remains only known to the dealer. If there are less than t users, only shares X_1, X_2, $\ldots$, X_k are seen, $k < t$, and points X_i with $i \in \{1, \ldots, k\}$ span the space of the dimension $(k-1)$ skew to l. Moreover, for every point $X' \in l$, there is a hyperplane $\mathbf{H}'$ with an arc containing X', X_1, $\ldots$, X_k, implying that it is impossible to determine the point on the line l that corresponds to the secret. If there are at least t users, then their shares correpsond to the hyperplane spaned by $X_i, \forall i \in \{1, 2, \ldots, t\}$, i.e., $\langle X_1, X_2, \ldots, X_t \rangle = \mathbf{H}$. The secret X is obtained as $X = \mathbf{H} \cap l$.

We are left to show the perfectness, which will be proved in the following theorem.

Theorem 2.5. *Knowing at most $t-1$ shares, the probability for an attacker to cheat successfully always has the same value of $\frac{1}{q+1}$.*

Proof. As we are in $\mathrm{PG}(t,q)$, first recall that any line consists of $q+1$ points. Since the secret X is on the fixed-line l, it means that the probability to guess the secret is the same for every point of the line, and hence, it is $\frac{1}{q+1}$ regardless of any additional assumptions. We will show that this probability remains the same even when we know $t-1$ shares.
Suppose that the set $\mathbf{T}'$ consists of at most $t-1$ shares. This set generates some subspace $\mathbf{V}$ and $\dim(\mathbf{V})$ is at most $t-1$, i.e., $\dim(\mathbf{V}) \leq t-1$. Since $\mathbf{T}'$ is the set of independent points, $\mathbf{T}' \cup \{X\}$ will still remain independent, and so $\mathbf{V}$ and l do not intersect. If the attacker knows the line l, as well as the set $\mathbf{T}'$, it does not reveal anything except that any additional share is not in $\mathbf{V}$ nor l.
Now, let us argue that each point X_0 on l has the same chance of being the secret. For any $X_0 \neq X \in l$, the subspace $\mathbf{V}' = \langle X_0, \mathbf{V} \rangle$ has the same number of shares. As there are $q+1$ points on l, it follows that the attacker's probability of success is $\frac{1}{q+1}$. □

2.2 COMPARTMENT SCHEMES

In the compartment scheme, users are split into distinct portions, called compartments, where each of them has equal rights. To participate in reconstructing the secret, each compartment needs a particular quorum, i.e., a minimal number of users. Furthermore, there must also be a particular number of compartments. Each compartment scheme can be seen as a threshold scheme, whereas the set of all compartments could be another threshold scheme. There are more complicated compartment schemes, but we will stick to the simpler ones.

2.2.1 Construction

Our focus will be a particular compartment scheme. Denote the compartments by $\mathcal{G}_1$, $\mathcal{G}_2$, …, $\mathcal{G}_n$, where the access structure consists of the following requirements:

- for every compartment, at least two users are necessary to enable the participation of that compartment in the secret's reconstruction,
- at least two compartments described above are enough to reconstruct the secret.

Example 2.6. Let's have a look at a simple compartment scheme where two compartments with the appropriate number of shares reconstruct the secret.

Each line g_i in the figure symbolizes a compartment, the green points represent shares, the blue points (G_1 and G_2) are representatives or heads of the corresponding compartment, and the red one is the secret.

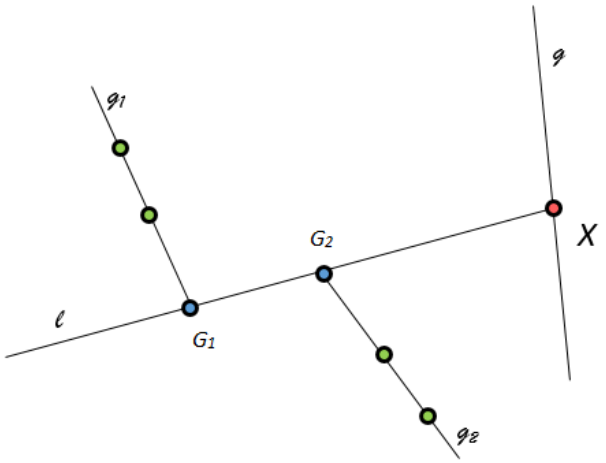

Figure 4: Trivial compartment scheme.

Let us describe the corresponding construction in $\mathbf{P} = \mathrm{PG}(n+2, q)$. Similar construction can be found in [2]. To start, fix a line g that contains a secret X predetermined by the dealer. Then, the dealer selects a line l at random such that $X \in l$ but $l \neq g$. Moreover, he chooses n points on l, say G_1, G_2, ..., G_n, and n lines g_1, g_2, ..., g_n that go through the corresponding points G_i, in such a way that the set $\{\langle l, g_i\rangle \cup \langle l, g\rangle : \{i \in \{1, \ldots, n\}\}$ is independent. Note that G_is are the representatives or heads of the compartments $\mathcal{G}_i$, while X_is are shares corresponding to that compartment. We can see lines g_i as compartments $\mathcal{G}_i$, with each compartment containing at least two shares (it is consistent with the geometric axiom that the line is determined by at least two points).

The following argument explains how the given construction can be viewed as a secret sharing scheme.

1. The conditions are provided by the dealer. We will later show that the probability of every non-legal constellation is the same, demonstrating the system's perfectness and completing the definition phase.

2. The mathematical phase is satisfied with the construction based on the geometry.

3. Each compartment $\mathcal{G}_i$, corresponding to the line g_i, consists of at least two shares, as otherwise, we cannot determine the line g_i. At least two compartments $\mathcal{G}_i$, i.e., two lines g_i, with their representatives G_i, are enough to generate the secret.

4. In the last phase, shares are sent to the system. If at least two shares come from one compartment, that compartment will generate a corresponding line g_i. Furthermore, if at least two compartments are obtained, their representatives, say G_i and G_j, generate the line l. Finally, the secret is reconstructed when lines l and g are intersected, i.e., $X = l \cap g$.

Theorem 2.7. *A compartment scheme described above is perfect.*

Proof. The method is straightforward. The subspace $\mathbf{V}$ formed by all provided points is calculated and intersected with g. We achieve the secret if the constellation of participants is legal, i.e., if there are at least two compartments, say g_i and g_j, the corresponding points G_i and G_j with $i \neq j$ are in $\mathbf{V}$. Those two points generate the line l, and hence, $l \in \mathbf{V}$, as well as X, that is, $X \in \mathbf{V} \cap g$. Nothing except X is in the mentioned intersection, as the planes $\langle l, g\rangle$, and $\langle l, g_i\rangle$ are presumed to be independent. But, what if the constellation of participants is not legal? In that case, we will prove that the attacker's chances of success are always the same.
Suppose that the attacker has two shares, say, X_1 and X_1' corresponding to the compartment $\mathcal{G}_1$ and one share, say X_i corresponding to the some other compartment $\mathcal{G}_i$, $i \in \{2, \ldots, n\}$. Let's say that X' represents any point on g. To show that attacker has the same probability for every non-legal constellation of participants, it is enough to establish that $\dim(\mathbf{V}') = n + 1$ and it intersects the line l precisely in X'. $\mathbf{V}'$ is a subspace generated by the points X_1, X_1', X_2, …, X_n, and X', i.e.:

$$\mathbf{V}' = \langle X_1, X_1', X_2, \ldots, X_n, X'\rangle.$$

First of all, recall that g and g_i are independent, and in a case that the secret X does not coincide with X', the subspace generated by $\mathbf{V}'$ and l is of dimension $n + 2$, i.e.,

$$\dim(\langle \mathbf{V}', l\rangle) = n + 2 \quad \text{if} \quad X \neq X'.$$

Hence,

$$\dim(\langle \mathbf{V}', X'\rangle) = n + 1 \quad \text{if} \quad X \neq X'.$$

We are left to show that $X \notin \mathbf{V}'$ if $X \neq X'$. We will provide the arguments for $n \in \{1, 2, 3\}$.

$n = 1$: In this case, the subspace $\mathbf{V}_1' = \langle X_1, X_1', X'\rangle$ and it is a plane as three non-collinear points generate a plane. In a case that both X and X' are in $\mathbf{V}_1'$, there would be two skew lines g and g_1 in our plane $\mathbf{V}_1'$, which is not possible. Since we have derived a contradiction, it follows that $X \notin \mathbf{V}_1'$.

$n = 2$: In this case, the subspace $\mathbf{V}_2' = \langle X_1, X_1', X_2, X'\rangle$. Let us find the dimension of $\mathbf{V}_2'$:

$$\dim(\mathbf{V}_2') = \dim(\langle X_1, X_1', X_2, X'\rangle) = \dim(\langle \mathbf{V}_1', X_2\rangle) \leq \dim(\mathbf{V}_1') + 1 = 3.$$

In deriving the equation above, we first used the property that $\mathbf{V}'_1 \subset \mathbf{V}'_2$. Moreover, the inequality is a corollary of the Dimension Formula (Theroem 1.1). So, we derived the upper bound for the dimension of $\mathbf{V}'_2$, i.e., $\dim(\mathbf{V}'_2) \leq 3$. Moreover, $\dim(\mathbf{V}'_2) \geq \dim(\mathbf{V}'_1) = 2$. Thus, we have the following relation:

$$2 \leq \dim(\mathbf{V}'_2) \leq 3,$$

implying that $\dim(\mathbf{V}'_2)$ can be either 2 or 3.
Suppose that $\dim(\mathbf{V}'_2) = 2$. Then, $\mathbf{V}'_2$ corresponds to a plane, whereas $\langle \mathbf{V}'_2, l\rangle$ would correspond to a 3-dimensional space that contains three independet planes, $\langle l, g\rangle$, $\langle l, g_1\rangle$, and $\langle l, g_2\rangle$, which yields a contradiction. Hence, $\dim(\mathbf{V}'_2) = 3$.

$n = 3$: In this case, the subspace $\mathbf{V}'_3 = \langle X_1, X'_1, X_2, X_3, X'\rangle$. Let us find the dimension of $\mathbf{V}'_3$:

$$\dim(\mathbf{V}'_3) = \dim(\langle X_1, X'_1, X_2, X_3, X'\rangle) = \dim(\langle \mathbf{V_2}', X_3\rangle) \leq \dim(\mathbf{V}'_2) + 1 = 4.$$

As in the previous case, we used Theroem 1.1 to derive the above equation and the result from the case when $n = 2$. We have the upper bound for the dimension of $\mathbf{V}'_3$, i.e., $\dim(\mathbf{V}'_3) \leq 4$. Moreover, $\dim(\mathbf{V}'_3) \geq \dim(\mathbf{V}'_2) = 3$. Thus, we have the following relation:

$$3 \leq \dim(\mathbf{V}'_3) \leq 4,$$

implying that $\dim(\mathbf{V}'_3)$ can be either 3 or 4.
Suppose that $\dim(\mathbf{V}'_3) = 3$. Then, $\mathbf{V}'_3$ corresponds to a 3-dimensional space, whereas $\langle \mathbf{V}'_3, l\rangle$ would correspond to a 4-dimensional space that contains four independet planes $\langle l, g\rangle$, $\langle l, g_1\rangle$, $\langle l, g_2\rangle$, and $\langle l, g_3\rangle$, a contradiction, as for skew planes, we need at least 5-dimensional space. Hence, $\dim(\mathbf{V}'_3) = 4$.

Analogously, one can show that the same holds for $n \geq 4$. □

Remark 2.8. Since $\langle l, g\rangle$, $\langle l, g_1\rangle$, $\langle l, g_2\rangle$, and $\langle l, g_3\rangle$ are independent planes, they must be skew as there are no such things as parallel planes in projective geometry.

We can also generalize the construction of compartment schemes so that t groups are required for reconstruction, with t_i users committing to each group $\mathcal{G}_i$. We summarize it in the following theorem.

Theorem 2.9. *Let X be a secret predetermined by the dealer. Then t shadows (shares) are represented by hyperplanes $\mathcal{H}_i$ of n-dimensional space V, such that $\mathcal{H}_i$ and the specific coordinate plane that passes through X are in a general position. We obtain the secret X by intersecting these t distinct hyperplanes $\mathcal{H}_i$. However, if only t' shadows are known with $t' < t$, then by intersecting these t' hyperplanes, we get $(t - t')$-dimensional linear variety strictly containing X. In that case, there is no revealed information about the secret.*

2.3 MULTILEVEL SCHEMES

We employ multilevel secret sharing schemes when commitments must be distributed to a group of participants rather than a single individual. The scheme must guarantee that no participant may obtain the secret or discover how the pieces are allocated to other participants until the conditions for the minimum number of participants are satisfied. We can see multilevel sharing schemes as a generalization of the threshold sharing schemes. Participants are divided into hierarchically organized subgroups. Our interest is the most commonly used multilevel schemes, known as 2-level sharing schemes or multilevel $(2, s)$-schemes.

2.3.1 Construction

As already mentioned, there are two different participant subgroups, denoted by $\mathbf{T}$ and $\mathbf{S}$. Hierarchically, the participants of a subgroup $\mathbf{T}$ are at a higher level than the participants of a subgroup $\mathbf{S}$. The secret can be reconstructed if the constellation of participants consists of:

- any set of at least two participants from $\mathbf{T}$,
- any set of at least s participants from $\mathbf{S}$,
- any participant from $\mathbf{T}$ and at least $s-1$ participants from $\mathbf{S}$.

Let us describe the corresponding construction in $\mathbf{P} = \mathrm{PG}(s, q)$. See also [2]. To start, fix a line g that contains a secret X predetermined by the dealer. Then, the dealer selects a line l at random such that $X \in l$ but $l \neq g$ and a hyperplane $\mathcal{H}$ through l such that the only common point of g and $\mathcal{H}$ is a secret X. $\mathbf{T}_l$ is the set of points on l different from X representing the shares of the participant of $\mathbf{T}$. Furthermore, $\mathbf{S}_H$ is the set of points on $\mathcal{H}$ different from X representing the points of $\mathbf{S}$, with $\mathbf{S}_H \cup \{X\}$ being a set of points in general position, and the property that there is no point of $\mathbf{T}_l$ in any subspace that passes through $s-1$ points of $\mathcal{H}$.

The following explanation clarifies how the given construction can be seen as a secret sharing scheme.

1. The conditions are provided by the dealer. We will later show that the probability of every non-legal constellation is the same, demonstrating the system's perfectness and completing the definition phase.
2. The mathematical phase is satisfied with the construction based on the geometry.

3. The legal constellation of participants consists of either
   - at least two participants from a higher level **T**,
   - at least s participants from a lower-level **S**,
   - any participant from **T** and at least $s-1$ participants from **S**.
4. In the last phase, shares are sent to the system.
   - In the case of at least two shares from **T**, the line through these two points intersected with the fixed-line g gives the secret X.
   - In the case of at least s participants from **S**, the hyperplane through these points intersected with the fixed-line g gives the secret X.
   - In the case of any participant from **T** and at least $s-1$ participants from S, the hyperplane through overall these s points, as a point of **T** can act as a point of **S**, intersected with the fixed-line g gives the secret X.

Example 2.10. Consider now an example of multilevel $(2,3)$-scheme in $\mathbf{P} = \mathrm{PG}(3,q)$. So, we fix a line g and the secret $X \in g$; we choose a line l through X different from g, a plane π such that $l \in \pi$ but $g \notin \pi$ and a normal rational curve (a conic when $s=3$) $\mathcal{K}$ of π through X whose tangent is l. Furthermore, we have to choose the sets $\mathbf{T}_l \subseteq l$ and $\mathbf{S}_\pi \subseteq \mathcal{K}$ in such a way that every line passing through the two points of $\mathbf{S}_\pi$ intersects l in a point that is not in $\mathbf{T}_l$. The following figure illustrates the described construction.

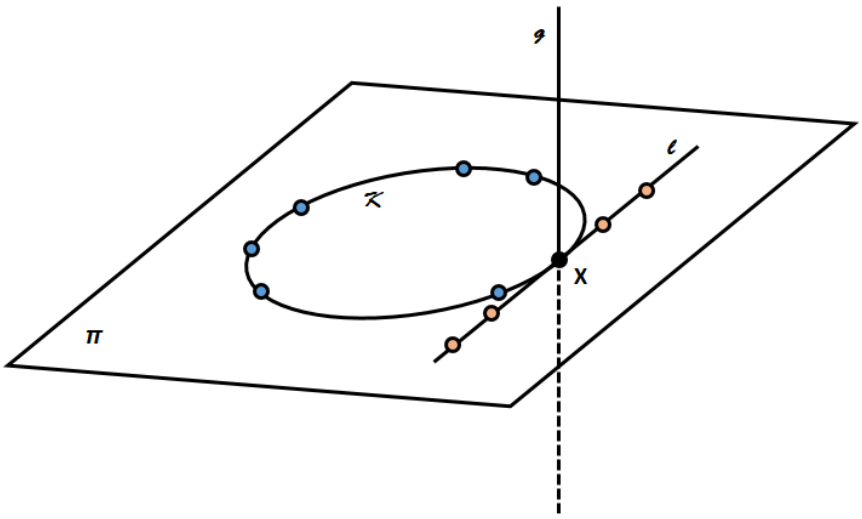

Figure 5: Multilevel $(2,3)$-scheme.

Theorem 2.11. *A multilevel $(2, s)$-scheme is perfect.*

Proof. Let us first consider the case when $s = 3$. We will show that a multilevel $(2, 3)$-scheme is perfect. As earlier stated, we have a fixed-line g with $X \in g$.

- If there are two points of $\mathbf{T}$, then there is a unique line l through these two points and hence, $X = g \cap l$.
- If there are at least $s = 3$ points in $\mathbf{S}$, then there is a unique plane π containing them and $X = g \cap \pi$.
- If there are at least $s - 1 = 2$ points of $\mathbf{S}$ and one point of $\mathbf{T}$, then as a point of $\mathbf{T}$ can act as a point of $\mathbf{S}$, we again have a unique plane π such that $X = g \cap \pi$.

Now consider a non-legal constellation of participants. We will show that each point of g, representing a potential secret, can be revealed with the same probability. The best situation for an attacker is to know one share belonging to the participants of $\mathbf{T}$ and $s - 2$ shares belonging to the participants of $\mathbf{S}$. As $s = 3$, it means that the best situation for an attacker is to know 1 share belonging to $\mathbf{T}$ and 1 share belonging to $\mathbf{S}$. These two points yield a unique line through them. There are $q+1$ planes through this line and each of them intersects g in a unique point. In other words, the probability for every point, and hence for the secret, is the same and corresponds to $\frac{1}{q+1}$.

To finish the proof, we discuss a generalization for every s.

If we know s points, the hyperplane $\mathcal{H}$ is uniquely determined, as $s - 1$ points in a general position determine a hyperplane of $\mathbf{P}$. The secret is obtained as $\mathcal{H} \cap g = X$.

However, if we know $s' \leq s - 1$ points, then s' points on $\mathbf{S}$ determine a subspace U of dimension s', and $U \cap g = \emptyset$. Moreover, for every point $X' \in g$, the subspace U and the point $X' \in g$ generate a subspace that intersects g in X'. But, there are $q + 1$ such points on g as we are in $\mathbf{P} = \mathrm{PG}(n, q)$, and thus, there are $q + 1$ points to intersect with our s' dimensional subspace. Hence, the probability of guessing the secret or that $X' = X$ is the same for every point on g and it corresponds to $\frac{1}{q+1}$. □

If we consider the example illustrated in Figure 5, the components of $\mathbf{S}$ were picked from points on a k-arc, and the elements of $\mathbf{T}$ were chosen from points on a tangent line to this k-arc in such a way that no two points of $\mathbf{S}$ and a point of $\mathbf{T}$ were collinear. In the following chapter, we will deal with the development of the most efficient scheme such that the orders of $\mathbf{S}$ and $\mathbf{T}$, i.e., $|\mathbf{S}|$ and $|\mathbf{T}|$, are as large as possible. One can observe that choosing a larger number of points on the arc reduces the number of tangent points available. Moreover, a k-arc has $k - 1$ secants passing through any of its points intersecting l in distinct points. Thus, it should not come as a surprise that we cannot increase the order of $\mathbf{S}$ and $\mathbf{T}$ arbitrarily.

3 AFFINELY REGULAR POLYGONS AND PROJECTIVE k-ARCS

Simmons [23, 24] proposed the geometric model of a sharply focused arc to design such an effective secret sharing scheme using k-arcs of $\mathrm{PG}(2, q)$ with q being large enough.

Definition 3.1. Denote by $\mathcal{K}$ a k-arc and by l an exterior line to $\mathcal{K}$.

- If the secants of $\mathcal{K}$ cover precisely $k-1$ points of l, we say that $\mathcal{K}$ is *very sharply focused*, or *hyperfocused* on l.
- If the secants of $\mathcal{K}$ cover precisely k points of l, we say that $\mathcal{K}$ is *sharply focused* on l.

Sharply focused arcs are extremal objects because the secants of a k-arc cover at least $k-1$ points of any external line. Bichara and Korchmáros [4] made their contribution by establishing the following.

Theorem 3.2. *If there is a very sharply focused or hyperfocused k-arc with $k > 2$ in a projective plane $\mathrm{PG}(2, q)$, then q must be even.*

On the other hand, sharply focused arcs exist for even and odd q. If we remove a point from a hyperfocused k-arc $\mathcal{K}$, we will get a sharply focused $(k-1)$-arc with the same focus set as $\mathcal{K}$. We use the term *extendable* to a hyperfocused arc for these sharply focused $(k-1)$-arcs. We introduce the concepts of affinely regular polygons and generalized affinely regular polygons to describe sharply focused and hyperfocused sets.

3.1 INTRODUCTION

Generally, the most important property of an arbitrary affine plane (coordinatized by a field) is that its theorems are still relevant after applying an affine transformation or affinity

$$x' = ax + by + l, \quad y' = cx + dy + m$$

or

$$A = \begin{bmatrix} a & c & 0 \\ b & d & 0 \\ l & m & 1 \end{bmatrix} \quad \text{and} \quad D = \det(A) = ad - bc \neq 0.$$

Moreover, a composition of affine transformations is also an affine transformation. Let us list some properties of the affine transformations:

- it maps collinear points to collienar points as well as non-collinear to non-collinear,
- it maps a line on the plane to some line on the same plane,
- if p is a polygon, then the image of p under an affine transformation is again a polygon p' with the same number of sides,
- it preserves the ratio of lengths of two parallel segments over the reals,
- it preserves the ratio of areas of two figures over the reals.

We will present and prove the following properties in the form of lemmas [31].

Lemma 3.3 (Parallelism preservation)**.** *Two different parallel lines are mapped to some other two parallel lines by an affine transformation.*

Proof. Let l and p be two parallel lines, and let f be some affine transformation such that $f(l) = l'$ and $f(p) = p'$. If l' and p' intersect in some point P, then $f^{-1}(P)$ would be the intersection of lines l and p, i.e., $l \cap p = P$, a contradiction. Hence, p' and l' are also parallel. □

Lemma 3.4 (Ratios preservation)**.** *Let f be an affine transformation that maps the line l to the line p, and let P, Q and R be three points on the line l. Then the ratio PQ/PR on l is the same as the ratio of their images $f(P)f(Q)/f(P)f(R)$ on p, i.e.,*

$$\frac{PQ}{PR} = \frac{f(P)f(Q)}{f(P)f(R)}.$$

Proof. Since P, Q and R are three points on l, then we can represent the point P as an affine combination of Q and R, i.e.,

$$P = (1-\lambda)Q + \lambda R \iff P' = (1-\lambda)Q' + \lambda R'. \tag{3.1}$$

Applying the affinity f on C entails multiplying C' by a matrix A_v, resulting in

$$A_v \cdot P' = (1-\lambda)A_v \cdot Q' + \lambda A_v \cdot R' \iff f(P) = (1-\lambda)f(Q) + \lambda f(R). \tag{3.2}$$

The proof follows from (3.1) and (3.2). □

Corollary 3.5 (Middle point presevation)**.** *Let f be an affine transformation mapping the line-segment PQ to the line-segment $P'Q'$. Then it also maps the middle point M of PQ to the middle point M' of $P'Q'$.*

Proof. It is just the consequnce of the previous lemma when $\lambda = \frac{1}{2}$. □

Let us remark that formulas (3.1) and (3.2) are valid in affine planes coordinatized by any field. The value λ determines the affine ratio (QRP) of the points $P, Q, R \in \mathrm{AG}(2, \mathbb{K})$, and affinities preserve the affine ratio.

Corollary 3.6. *Two arbitrary plane parallelograms are affine equivalent. Moreover, a square is the affine equivalent of every parallelogram. (See Figure 6.)*

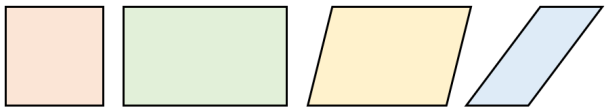

Figure 6: Affinely regular parallelograms.

In the following figure, we have affine equivalent hexagons.

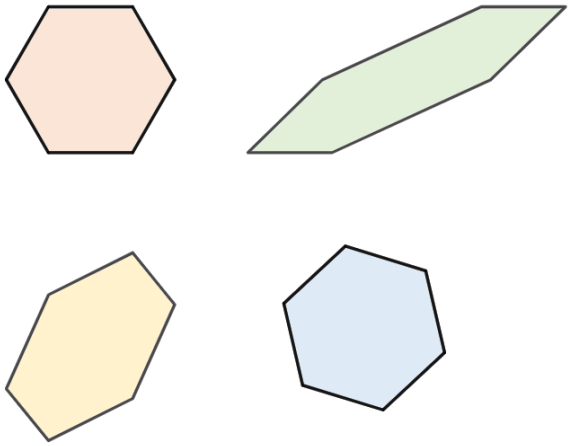

Figure 7: Affinely regular hexagons.

Some particular affinities for which $D = 1$ lead to the term *equiaffinity*. If the vertices $A_0A_1A_2\ldots$ form an orbit for equiaffinity, a polygon $A_0A_1A_2\ldots$ is said to be affinely regular. Affinely regular polygons have been used to solve a variety of mathematical problems. They are regular polygons whose image is created by an affine transformation of the plane. Affine transformations include, for instance, translation, scaling, homothety, similarity, reflection, rotation, shear mapping, and compositions of them in any order or combination. Let us provide the classical definition of the affinely regular polygons, which can also be found in [13].

Definition 3.7. Let $\mathcal{A}$ be an affine plane and points P_0, P_1, ..., P_{n-1} be n points in this plane. We name the sequence $P_0P_1 \dots P_{n-1}$ as an *affinely regular polygon*, if there is a one-to-one mapping ϕ sending all P_i's with $i \in \{0, 1, \dots, n-1\}$ to the set of vertices of a regular n-gon in the classical Eucledian plane in such a way that P_iP_j is parallel to P_kP_l in the affine plane $\mathcal{A}$ if and only if $\phi(P_i)\phi(P_j)$ is parallel to $\phi(P_k)\phi(P_l)$ in the classical Euclidean plane.

Moreover, Fisher and Jamison [11] provided in their article seven equivalent definitions of affinely regular polygons.

Theorem 3.8. *Denote by $P = (P_i)$ a polygon in the affine plane $\mathrm{AG}(2, \mathbb{F})$ such that $P_{i+2} \notin P_iP_{i+1}$ for any i, where $i = 0, 1, 2, \dots, n-1$ and indices are calculated $\pmod n$. Each of the seven statements given below can be used to define a nondegenerate affinely regular polygon, where nondegenerate means that it has no three collinear vertices.*

- *For each $i \in \mathbb{Z}$, $\phi\colon P_{i-1}P_iP_{i+1} \to P_iP_{i+1}P_{i+2}$ defines an equiaffine transformation mapping each vertex into the next.*
- *(Coxeter [9]) For each $i \in \mathbb{Z}$, there is a pair of affine reflections*
  1. *$\rho_1\colon P_iP_{i-1}P_{i+1} \to P_iP_{i+1}P_{i-1}$ interchanging P_{i-k} with P_{i+k} for all $k \in \mathbb{Z}$, and*
  2. *$\rho_2\colon P_{i-1}P_iP_{i+1} \to P_{i+2}P_{i+1}P_i$ interchanging P_{i-k} with P_{i+k+1} for all $k \in \mathbb{Z}$.*
- *(Coxeter [9]) For all $i \in \mathbb{Z}$, there exists $t \in \mathbb{F}$ such that $P_{i+2} - P_{i-1} = t(P_{i+1} - P_i)$.*
- *(Nizette [20]) For all $i \in \mathbb{Z}$*
  1. *$P_iP_{i+1} \parallel P_{i-1}P_{i+2}$, and*
  2. *$P_iP_{i+2} \parallel P_{i-1}P_{i+3}$.*
- *(Korchmáros [15]) A polygon P is inscribed in a conic or pair of parallel lines, and for all $i \in \mathbb{Z}$, $P_{i-1}P_{i+1} \parallel P_{i-1}P_{i+2}$.*
- *One of the following occurs*
  1. *A polygon P is inscribed in a conic and $P_{i-1}P_{i+1}$ is parallel to the tangent at P_i for all $i \in \mathbb{Z}$, or*
  2. *The points alternatively lie on two lines for every $i \in \mathbb{Z}$; the even points P_{2i} lie on a line parallel to the line containing the odd points P_{2i+1}. Moreover, the line segments $P_{2i}P_{2i-1}$ have the same midpoint, as do the segments $P_{2i}P_{2i+1}$.*
- *(Jamison [11]) For each of four fixed values of k picked from a set of five consecutive integers and for all $i \in \mathbb{Z}$, the lines P_iP_{k-i} are parallel.*

3.2 CLASSIFICATION

Korchmáros [13,15] classified affinely regular polygons in the finite affine plane $\mathrm{AG}(2,q)$, where q is odd. There are three types of these polygons.

Theorem 3.9. *Let $\mathbb{F} = GF(q)$ and $q = p^r$, where p is an odd prime. An affine transformation can map any affinely regular polygon on the affine plane $\mathcal{A} = \mathrm{AG}(2,\mathbb{F})$ to one of affinely regular polygons given in the following three categories:*

1. *Let G be a multiplicative subgroup of $\mathbb{F}$. If $|G| = n$, then there exists an affinely regular n-gon in $\mathcal{A}$ inscribed in the hyperbola with equation $XY = 1$. Choose a non-zero element $f \in \mathbb{F}$ and a generator g of G and let $P_i = ((g^i f)^{-1}, g^i f)$ for $i \in \{1,2,\ldots,n-1\}$. Then the sequence of points $P_0P_1\ldots P_{n-1}$ is an affinely regular n-gon inscribed in the hyperbola.*

2. *Let $f \in \mathbb{F}$ and P_i be the point with coordinates $(f+i,(f+i)^2)$, $i \in \{1,\ldots,p\}$ with $p > 0$. Then the sequence of points $P_1P_2\ldots P_p$ is an affinely regular p-gon inscribed in the parabola with the equation $Y = X^2$.*

3. *Define $\widehat{\mathbb{F}} = \mathbb{F}(i)$ to be a quadratic extension of $\mathbb{F}$ with $X^2 - m = 0$, such that m is a non-square in $\mathbb{F}$. We express the elements of $\widehat{\mathbb{F}}$ as $a + bi$, $a,b \in \mathbb{F}$ and identify them with points (a,b) in affine plane $\mathcal{A} = \mathrm{AG}(2,\mathbb{F})$. It is actually a bijection between the points of $\mathcal{A}$ and the elements of $\widehat{\mathbb{F}}$. The line given by $[C,A,B]$ is mapped to the subset $\{x+yi \in \widehat{\mathbb{F}}, a,b \in \mathbb{F}, Ax+By+C=0\}$. The elements of $\widehat{\mathbb{F}}$ fullfiling the equation $a^2 - mb^2 = 1$ form a multiplicative subgroup H of $\widehat{\mathbb{F}}^*$ with $|H| = q+1$. Finally, define G to be a subgroup of H. If $|G| = n$, $\mathcal{A}$ contains an affinely regular n-gon inscribed in ellipse with the equation $X^2 - mY^2 = 1$. If $g \in G$ is a generator, $g^j = x_j + y_j i$ and P_j corresponds to the point with coordinates (x_j, y_j), then the sequence $P_0P_1\ldots P_{n-1}$ is an affinely regular n-gon.*

Remark 3.10. Complex numbers are equivalent to the points of the Euclidean plane.

Proof. We will derive the proof for each class.

1. Take a canonical hyperbola on the affine plane $\mathcal{A} = \mathrm{AG}(2,\mathbb{F})$, $\mathbb{F} = GF(q)$ with the equation $XY = 1$. In the projective plane, a hyperbola consists of $q+1$ points. However, we will show that this number is $q-1$ in the affine plane.
   Consider $\mathrm{PG}(2,\mathbb{K})$ as $\mathrm{AG}(2,\mathbb{K}) \cup l_\infty$. An affine point $P(1:x:y)$ is on the curve $H(X_0,X_1,X_2) = 0$ if and only if it is on the curve $F(X_1/X_0, X_2/X_0) = 0$. To show that hyperbola contains $q-1$ points in an affine plane, we will show that it has two points on the line at infinity. Point is on l_∞ if $X_0 = 0$. So,

$$XY = 1 \iff \left(\frac{X_1}{X_0}\right) \cdot \left(\frac{X_2}{X_0}\right) = 1.$$

Now,

$$\left.\begin{aligned}\mathcal{H} : X_1X_2 = X_0^2\\ l_\infty : X_0 = 0\end{aligned}\right\} \Rightarrow X_1X_2 = 0 \Rightarrow X_1 = 0 \text{ or } X_2 = 0.$$

So, there are two points at infinity, $(0:0:1)$ and $(0:1:0)$, indicating that $q-1$ points are on the affine plane of the form $\{(1/a, a) : q \in GF(q)\}$.
The multiplicative group of the non-zero elements in $GF(q)$ is cyclic, and there exists an element a, such that $(q-1)$ non-zero elements of $GF(q)$ are $(a, a^2, \ldots, a^{q-1} = 1)$. Take two points $A = (1/a, a)$ and $B = (1/b, b)$ of the hyperbola $XY = 1$. Then

- the slope of the chord is

$$\frac{b-a}{\frac{1}{b}-\frac{1}{a}} = \frac{b-a}{\frac{a-b}{ab}} = \frac{-(a-b)\cdot ab}{a-b} = -ab.$$

- the midpoinf ot the chord is

$$M\Big(\frac{\frac{1}{a}+\frac{1}{b}}{2}, \frac{a+b}{2}\Big) = \Big(\frac{\frac{a+b}{ab}}{2}, \frac{a+b}{2}\Big) = \frac{a+b}{2}\Big(\frac{1}{ab}, 1\Big).$$

For the parallel chords the slope is constant and the midpoints of the parallel chords lie on the line $x = -aby$.
Now, let us define the points $P_i = (1/g^i, g^i)$, $P_j = (1/g^j, g^j)$, $P_{i+k} = (1/g^{i+k}, g^{i+k})$, and $P_{j-k} = (1/g^{j-k}, g^{j-k})$. To show that the sequence $P_0P_1 \ldots P_{n-1}$ is an affinely regular n-gon, we have to prove that $P_iP_j \parallel P_{i+k}P_{j-k}$, i.e., P_iP_j and $P_{i+k}P_{j-k}$ have the same slope for all i, j and k calculated modulo n, $i \neq j$.

- Slope of P_iP_j:

$$\frac{g^j-g^i}{\frac{1}{g^j}-\frac{1}{g^i}} = \frac{g^j-g^i}{\frac{g^i-g^j}{g^ig^j}} = \frac{-(g^i-g^j)\cdot g^{i+j}}{g^i-g^j} = -g^{i+j}.$$

- Slope of $P_{i+k}P_{j-k}$:

$$\frac{g^{j-k}-g^{i+k}}{\frac{1}{g^{j-k}}-\frac{1}{g^{i+k}}} = \frac{g^{j-k}-g^{i+k}}{\frac{g^{i+k}-g^{j-k}}{g^{i+k}g^{j-k}}} = \frac{-(g^{i+k}-g^{j-k})\cdot g^{i+k+j-k}}{g^{i+k}-g^{j-k}} = -g^{i+j}.$$

Since we established that the slopes P_iP_j and $P_{i+k}P_{j-k}$ are equal, it follows from Theorem 3.8 that the sequence $P_0P_1 \ldots P_{n-1}$ is an affinely regular n-gon.

2. Take a canonical parabola on the affine plane $\mathcal{A} = \mathrm{AG}(2, \mathbb{F})$, $\mathbb{F} = GF(q)$ with the equation $Y = X^2$. In the projective plane, a parabola consists of $q+1$ points. However, we will show that this number is q in the affine plane.
Consider $\mathrm{PG}(2, \mathbb{K})$ as $\mathrm{AG}(2, \mathbb{K}) \cup l_\infty$. An affine point $P(1 : x : y)$ is on the curve $H(X_0, X_1, X_2) = 0$ if and only if it is on the curve $F(X_1/X_0, X_2/X_0) = 0$.

To show that parabola contains q points in an affine plane, we will show that it has one point on the line at infinity. Point is on l_∞ if $X_0 = 0$. So,

$$Y = X^2 \iff \left(\frac{X_2}{X_0}\right) = \left(\frac{X_1}{X_0}\right)^2.$$

Now,

$$\left.\begin{aligned} \mathcal{P} : X_2X_0 - X_1^2 = 0 \\ l_\infty : X_0 = 0 \end{aligned}\right\} \Rightarrow X_1^2 = 0 \Rightarrow X_1 = 0.$$

So, there is one point at infinity, $(0:0:1)$, indicating that q points are on the affine plane of the form $\{(a+i,(a+i)^2) : a \in G\}$, $i \in \{1,\dots p\}$ and G is the additive subgroup of $GF(q)$. We can order the vertices $1,\dots,p$ as the additive group is generated by the unit element 1, and hence,

$$\begin{aligned} 1 \\ 1+1 = 2 \\ 1+1+1 = 3 \\ \vdots \\ \underbrace{1+1+1\cdots+1}_{p \text{ times}} = p = 0. \end{aligned}$$

Take two points $A = (a+i,(a+i)^2)$ and $B = (b+i,(b+i)^2)$ of the parabola $Y = X^2$. Then the slope of the chord is

$$\frac{(b+i)^2-(a+i)^2}{(b+i)-(a+i)} = \frac{(b+i-a-i)(b+i+a+i)}{b+i-a-i} = a+b+2i.$$

Now, let us define the points $P_i = (i, i^2)$, where $i = \underbrace{1+1+\cdots 1}_{i}$ times and $P_j = (j, j^2)$, where $j = \underbrace{1+1+\cdots 1}_{j}$ times as well as the points $P_{i+k} = (i+k,(i+k)^2)$, and $P_{j-k} = (j-k,(j-k)^2)$. To show that the sequence $P_1P_2\dots P_p$ is an affinely regular p-gon, we have to prove that $P_iP_j \parallel P_{i+k}P_{j-k}$, i.e., P_iP_j and $P_{i+k}P_{j-k}$ have the same slope for all i, j and k calculated modulo p, $i \neq j$.

- Slope of P_iP_j:
$$\frac{j^2-i^2}{j-i} = \frac{(j-i)(j+i)}{j-i} = i+j.$$
- Slope of $P_{i+k}P_{j-k}$:
$$\frac{(j-k)^2-(i+k)^2}{(j-k)-(i+k)} = \frac{(j-k-i-k)(j-k+i+k)}{j-k-i-k} = i+j.$$

  Since we established that the slopes P_iP_j and $P_{i+k}P_{j-k}$ are equal, it follows from Theorem 3.8 that the sequence $P_1P_1\dots P_p$ is an affinely regular p-gon.

3. Take the canonical ellipse on the affine plane $\mathcal{A} = \mathrm{AG}(2, \mathbb{F})$, $\mathbb{F} = GF(q)$ with the equation $X^2 - mY^2 = 1$. In the projective plane, ellipse consists of $q + 1$ points. Let us show that this number is not changed in the affine plane.
Consider $\mathrm{PG}(2, \mathbb{K})$ as $\mathrm{AG}(2, \mathbb{K}) \cup l_\infty$. An affine point $P(1 : x : y)$ is on the curve $H(X_0, X_1, X_2) = 0$ if and only if it is on the curve $F(X_1/X_0, X_2/X_0) = 0$. To show that an ellipse contains $q + 1$ points in an affine plane, we will show that it does not have any points on the line at infinity. Point is on l_∞ if $X_0 = 0$. So, take $X^2 - mY^2 = 1$, where m is a non-square in $\mathbb{F} = GF(q)$. Then,

$$X^2 - mY^2 = 1 \iff \Big(\frac{X_1}{X_0}\Big)^2 - m\Big(\frac{X_2}{X_0}\Big)^2 = 1.$$

Now,

$$\left.\begin{aligned} \varepsilon : X_1^2 - mX_2^2 = X_0^2 \\ l_\infty : X_0 = 0 \end{aligned}\right\} \Rightarrow X_1^2 = mX_2^2 \Rightarrow m = \Big(\frac{X_1}{X_2}\Big)^2$$

This yields to a contradiction as m is supposed to be a non-square in $\mathbb{F} = GF(q)$. Hence, there are no points at l_∞, implying that there are $q + 1$ points on the affine plane.

As already stated, we can represent complex numbers as the points of the Euclidean plane. For sake of completeness, we recall this representation, and later we will give its finite analogous. A complex number $x + yi$, with $x, y \in \mathbb{R}$, represents the point of the plane whose Cartesian coordinates (considering an appropriate origin) are (x, y). The distance between a complex number's location on a plane and the origin is known as the magnitude or absolute value. The collection of complex numbers of magnitude one represents the unit circle. They create a circle with a radius of one on the complex plane, with its center at the origin. A complex number $z = x + yi$ will lie on the unit circle when $X^2 + Y^2 = 1$. Take four points, say $a = x_1 + y_1 i$, $b = x_2 + y_2 i$, $c = x_3 + y_3 i$ and $d = x_4 + y_4 i$, on the circle as given in the Figure 8.

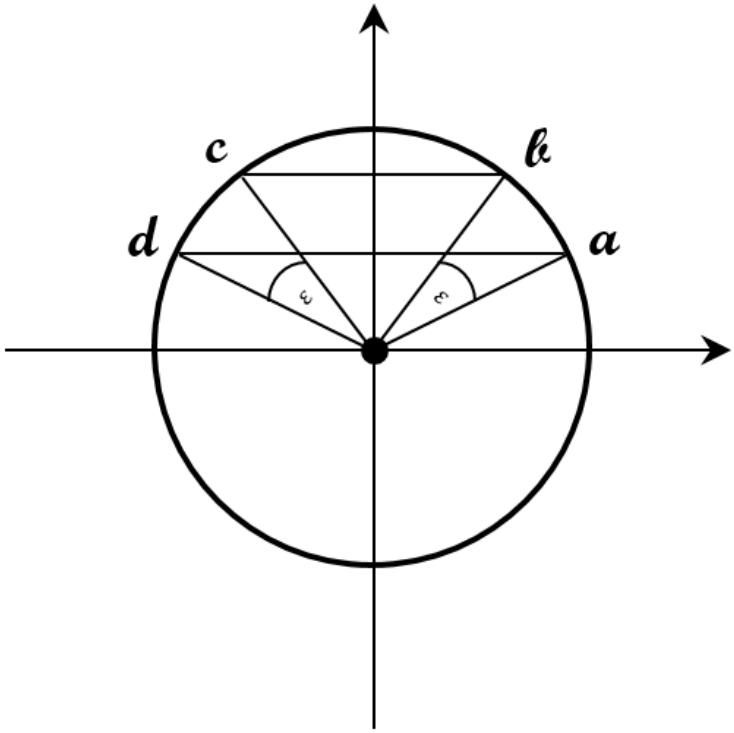

Figure 8: Unit circle.

Considering the figure above and applying the properties of complex numbers, we have that

$$\frac{b}{a} = \cos\epsilon + i\sin\epsilon = \cos\epsilon + i\sin\epsilon = \frac{d}{c}.$$

So,

$$\frac{b}{a} = \frac{d}{c} \iff ad = bc.$$

On the other hand, this is true if and only if ad and bc are parallel (see Figure 8).

Considering our equation $X^2 - mY^2 = 1$, where m is a non-square element in $\mathbb{F}$, it follows that

$$X^2 + Y^2 = 1 \iff X^2 - mY^2 = 1, \text{ with } m = i^2.$$

We claim that taking q's power in the complex case corresponds to the complex conjugate of the number. To prove it, we will first show that $i^q = -i$.

Lemma 3.11. *Let m be a non-square element in $\mathbb{F}$, and $m = i^2$, $i \in \widehat{\mathbb{F}} = \mathbb{F}[i]$, but $i \notin \mathbb{F}$. Then $i^q = -i$.*

Proof. Since $i^2 = m$, it follows that $i^{2(q-1)} = m^{q-1} = 1$. The last equality is a consequence of the fact that $m^q = m, \forall m \in \mathbb{F}$. So, if $m \neq 0$, then $m^{q-1} = 1$ and

$$(i^{q-1})^2 = 1 \Rightarrow i^{q-1} = 1 \text{ or } i^{q-1} = -1.$$

If $i^{q-1} = 1$, then it would mean that $i \in \mathbb{F}$, which yields to the contradiction as $i \notin \mathbb{F}$. Hence,

$$i^{q-1} = -1 \Rightarrow i^q = -i.$$

□

Since our main goal refers to a parallelism, let us first recall the condition from the classical geometry needed to establish that two lines containg complex numbers are parallel. Let AB and CD be two lines, such that AB passes through z_1 and z_2 and CD through z_3 and z_4. The slopes of AB and CD are determined by:

$$k_{AB} = \frac{z_2 - z_1}{\overline{z_2} - \overline{z_1}}$$
$$k_{CD} = \frac{z_4 - z_3}{\overline{z_4} - \overline{z_3}}.$$

Then, we say that these to lines are parallel, if

$$\text{Arg}\Big(\frac{z_2 - z_1}{z_4 - z_3}\Big) = 0 \text{ or } \pi.$$

So,

$$\frac{z_2 - z_1}{z_4 - z_3} = \text{Real number} \Rightarrow \frac{z_2 - z_1}{z_4 - z_3} = \frac{\overline{z_2} - \overline{z_1}}{\overline{z_4} - \overline{z_3}} \Rightarrow z = \overline{z}.$$

In other words, when we are considering four points in Eucledian plane, say A, B, C and D, with the corresponding complex numbers z_1, z_2, z_3 and z_4, we say that

$$AB \parallel CD \iff \exists \alpha \in \mathbb{R} \text{ such that } z_2 - z_1 = \alpha(z_4 - z_3).$$

Similar statement is true in the affine plane. It can also be found in [13].

Lemma 3.12. *Let $P_j = (x_j, y_j)$, $j \in \{1, 2, 3, 4\}$ be four points in an affine plane* $\text{AG}(2, \mathbb{K})$ *with the corresponding elements $x_j + iy_j = z_j \in \mathbb{F}$. Then,*

$$P_1P_2 \parallel P_3P_4 \iff \exists \alpha \in \mathbb{K} \text{ such that } z_4 - z_3 = \alpha(z_2 - z_1).$$

Proof. Let us first write the equation of the lines P_1P_2 and P_3P_4:

- $P_1P_2 : Y - y_1 = \frac{y_2 - y_1}{x_2 - x_1}(X - x_1) \Rightarrow (y_2 - y_1)X + (x_1 - x_2)Y + (y_1x_2 - y_2x_1) = 0,$
- $P_3P_4 : Y - y_3 = \frac{y_4 - y_3}{x_4 - x_3}(X - x_3) \Rightarrow (y_4 - y_3)X + (x_3 - x_4)Y + (y_3x_4 - y_4x_3) = 0.$

These two lines are parallel if and only if the following determinant is 0:

$$\begin{vmatrix} y_2 - y_1 & x_1 - x_2 \\ y_4 - y_3 & x_3 - x_4 \end{vmatrix} = 0$$

This determinant is 0 if and only if the above rows are linearly dependent, which is true if and only if

$$x_3 - x_4 = \alpha(x_1 - x_2) \quad \text{and} \quad y_4 - y_3 = \alpha(y_2 - y_1).$$

Subtracting these two, it means that this is true if and only if

$$x_3 + y_3 - (x_4 + y_4) = \alpha(x_1 + y_1 - (x_2 + y_2)) \iff z_3 - z_4 = \alpha(z_1 - z_2).$$

□

Now, applying Lemma 3.11, we have that

$$(x_1 + iy_1)^q = x_1^q + i^q y_1^q = x_1 - iy_1. \tag{3.3}$$

So, we established that q's power of the complex number corresponds to its conjugate.

Furthermore, since a, b, c, and d (as in Figure 8) satisfy that the equation $X^2 - mY^2 = 1$, it follows that

- for $a = x_1 + iy_1$, $x_1^2 - my_1^2 = 1$,
- for $b = x_2 + iy_2$, $x_2^2 - my_2^2 = 1$,
- for $c = x_3 + iy_3$, $x_3^2 - my_3^2 = 1$,
- for $d = x_4 + iy_4$, $x_4^2 - my_4^2 = 1$.

We will derive the expression for $a^q = (x_1 + iy_1)^q$, and apply it with the indices corresponding to b, c and d. So,

$$\begin{aligned} x_1^2 - my_1^2 = 1 &\Rightarrow x_1^2 - i^2 y_1^2 = 1 \\ &\Rightarrow (x_1 - iy_1) \cdot (x_1 + iy_1) = 1 \\ &\Rightarrow x_1 + iy_1 = \frac{1}{x_1 - iy_1} = \frac{1}{(x_1 + iy_1)^q}. \end{aligned}$$

The last equality follows from the expression derived in Equation (3.3). It indicates that

$$a = x_1 + iy_1 = \frac{1}{(x_1 + iy_1)^q} = \frac{1}{a^q}.$$

Applying it with the indices corresponding to b, c and d, we have

$$\begin{aligned} b = x_2 + iy_2 &= \frac{1}{(x_2 + iy_2)^q} = \frac{1}{b^q} \\ c = x_3 + iy_3 &= \frac{1}{(x_3 + iy_3)^q} = \frac{1}{c^q} \\ d = x_4 + iy_4 &= \frac{1}{(x_4 + iy_4)^q} = \frac{1}{d^q}. \end{aligned}$$

Furthermore, applying the expressions derived for a, b, c and d, we will show that

$$\frac{a-d}{b-c} = \left(\frac{a-d}{b-c}\right)^q \iff ad = bc.$$

So,

$$\begin{aligned} \frac{a-d}{b-c} = \left(\frac{a-d}{b-c}\right)^q &= \frac{a^q - d^q}{b^q - c^q} \\ &= \frac{1/a - 1/d}{1/b - 1/c} \\ &= \frac{a-d}{b-c} \cdot \frac{bc}{ad} \end{aligned}$$

The above expression holds if and only if $\frac{bc}{ad} = 1$, i.e.,

$$\frac{a-d}{b-c} = \frac{a-d}{b-c} \cdot \frac{bc}{ad} \iff \frac{bc}{ad} = 1 \iff ad = bc.$$

Hence, we established that

$$\frac{a-d}{b-c} = \left(\frac{a-d}{b-c}\right)^q \iff ad = bc \tag{3.4}$$

which is true if and only if ad and bc are parallel.

Before applying this result, let us also show that the elements of $\widehat{\mathbb{F}}$ fullfiling the equation $a^2 - mb^2 = 1$ form a multiplicative subgroup H of $\widehat{\mathbb{F}}^*$.

Take two arbitrary elements of H such that $a^2 - mb^2 = c^2 - md^2 = 1$. Then, $(a + bi)(c + di) = ac + mbd + i(ad + bc)$. We need to show that

$$(ac + mbd)^2 - m(ad + bc)^2 = 1.$$

So,

$$\begin{aligned} (ac + mbd)^2 - m(ad + bc)^2 &= a^2c^2 + 2acmbd + m^2b^2d^2 - m(a^2d^2 + 2adbc + b^2c^2) \\ &= a^2c^2 + 2abcdm + m^2b^2d^2 - ma^2d^2 - 2abcdm - mb^2c^2 \\ &= a^2c^2 + m^2b^2d^2 - ma^2d^2 - mb^2c^2 \\ &= c^2(a^2 - mb^2) - md^2(a^2 - mb^2) \\ &= (a^2 - mb^2)(c^2 - md^2) \\ &= 1 \cdot 1 = 1. \end{aligned}$$

Finally, take a generator ot a multiplicative subgroup H. The points of ellipse can be represented in this way:

- $g_l = x_l + iy_l$, and P_l is the point with coordinates (x_l, y_l),
- $g_j = x_j + iy_j$, and P_j is the point with coordinates (x_j, y_j),
- $g_{l+k} = x_{l+k} + iy_{l+k}$, and P_{l+k} is the point with coordinates (x_{l+k}, y_{l+k}),
- $g_{j-k} = x_{j-k} + iy_{j-k}$, and P_{j-k} is the point with coordinates (x_{j-k}, y_{j-k}),

Applying the result obtained by the expression (3.4), it follows that $P_lP_j \parallel P_{l+k}P_{j-k}$ if and only if g^lg^j and $g^{l+k}g^{j-k}$ have the same slopes. It's trivial as

$$g^{l+k}g^{j-k} = g^{l+k+j-k} = g^{l+j} = g^lg^j.$$

Since we established that the slopes P_lP_j and $P_{l+k}P_{j-k}$ are equal, it follows from Theorem 3.8 that the sequence $P_1P_2 \dots P_n$ is an affinely regular n-gon.

□

Furthermore, the existence of the affinely regular n-gon in $\mathcal{A} = \mathrm{AG}(2, q)$, coordinatized by $GF(q)$, $q = p^r$, is guaranteed by the following theorem.

Theorem 3.13. *An affinely regular n-gon in $\mathcal{A} = \mathrm{AG}(2, q)$, coordinatized by $GF(q)$, $q = p^r$, exists if and only if*

- $n|(q + 1)$ *and the n-gon is inscribed in an ellipse, or*
- $n|(q - 1)$ *and the n-gon is inscribed in a hyperbola, or*
- $n = p$ *and the n-gon is inscribed in a parabola.*

In the previous subsection, we have defined an affinely regular polygon in several different ways. Let us also define the generalized affinely regular polygons.

Definition 3.14. Denote by $\mathcal{P}$ a parabola in $A = \mathrm{AG}(2, q)$ with the equation $Y = X^2$. Furthermore, let g be an element of $\mathrm{GF}(q)$ and $H = \{h_0, h_1, \dots, h_{n-1}\}$ be a subgroup of $(GF(q), +)$. If $P_i = (g + h_i, (g + h_i)^2)$, $i = 0, 1, \dots, n - 1$, then we name the n-gon $P_0P_1 \dots P_{n-1}$ a *generalized affinely regular polygon.*

Example 3.15. Recall from the introductory part that $GI(q) = \langle G(q), \bigoplus, * \rangle$, with $G(q) = \{a + ib, a, b \in GF(q)\}$, is isomorphic to $GF(q^2)$. We will find the coordinates and depict the figure for $q = 7$. When we consider an affine plane over complex numbers, we will use the elements of $GF(q^2)$. Hence, in our case, there are 49 elements. The nonzero elements of $GF(q)$ are $1, 2, 3, 4, 5, 6$, i.e., $\pm1, \pm2, \pm3$. We divide them into groups based on whether they are quadric or non-quadric residues of $q = 7$.

A classical representation would be the following. First, the 0 element corresponds to the origin and the non-zero elements of $GF(q)$, i.e., 1, 2, 3, 4, 5 and 6 are on the horizontal axis left or right to zero based on whether they are quadric or non-quadric residues of $q = 7$. A similar situation occurs for i, $2i$, $3i$, $4i$, $5i$ and $6i$ on the vertical axis. Now, for each element of the form $a + bi$, we find the magnitude modulo 7 and determine if it is on the circle of radius 1, 2, or 4. We put the elements in each quadrant according to the square and non-square parts. Note that the residues 1 and -1, 2 and -2, as well as 4 and -4, are in the same circles.

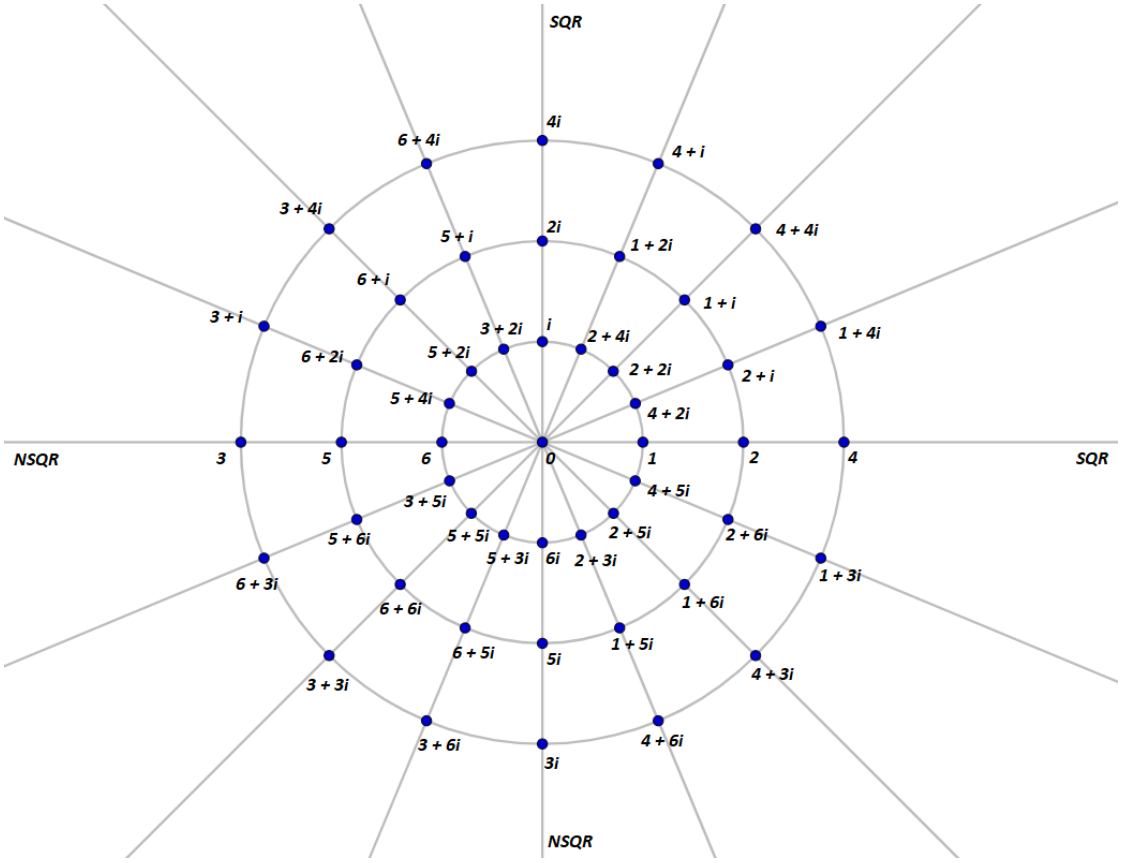

Figure 9: The Z plane over $GF(7)$.

However, we distinguish those that give residues ± 1, ± 2, and ± 4. We represent positive residues with blue circles and negative ones with red circles. Starting from the point 1 and taking every second point, we get the first blue circle. In the other circles, the process is the same, i.e., we start from 2 and 4 and take every second point. The remaining points form three red circles according to the residues.

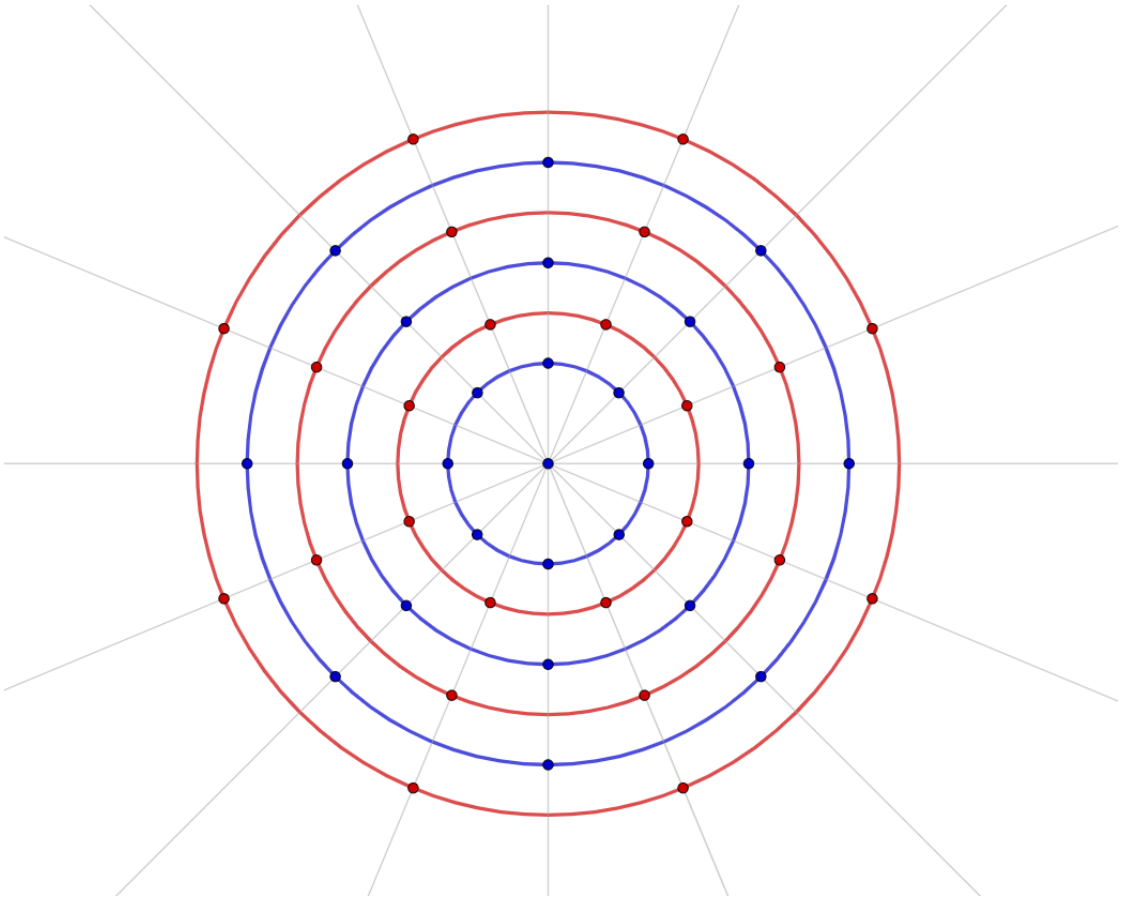

Figure 10: The Z plane over $GF(7)$ - modified.

3.3 SHAPE-REGULAR POLYGONS

Some attractive theorems require so-called shape-regularity, which appears to be more metric than affine. We will use the notation of $\mathbb{K}$ representing the quadratic extension of $\mathbb{F}$, that is, either $\mathbb{C}$ or $GF(q^2)$, with q being odd.

Definition 3.16. Denote by u, v and w the vertices of an ordered triangle (uvw) with $u, v, w \in \mathbb{K}$. We define the *shape* of this triangle in the following way

$$S(uvw) = (u - w)(u - v)^{-1} \in \mathbb{K}.$$

Artzy and Kiss [1] proved the following.

Lemma 3.17. *Let $\mathbb{F} = GF(q)$, where q is odd.*

- *There exist no shape-regular triangles for $q \equiv 0, 1 \pmod 3$.*
- *There exist exatcly two types of shape-regular triangles for $q \equiv 2 \pmod 3$.*

Definition 3.18. Denote by u_i, $i \in \{1, 2, \ldots, n\}$, n distinct points in $\mathbb{K}$. We name the ordered n-gon $(u_1 u_2 \cdots u_n)$ a *shape-regular n-gon* having the shape $s \in \mathbb{K}$ if $S(u_{i+1} u_i u_{i+2}) = s \in \mathbb{K}$, $i \in \mathbb{Z}$ is calculated modulo n.

The existence of shape-regular n-gons is summarized in the following theorem.

Theorem 3.19. *The shape-regular n-gon, with shape s, exists in $\mathcal{A} = \mathrm{AG}(2, \mathbb{F})$ if and only if the following holds: $s \notin \mathbb{F}$, $(-s)^n = 1$, $(-s)^m \neq 1$, $i \leq m \leq n$.*

It can also be interpreted in the following way.

Theorem 3.20. *The existence of a shape-regular n-gon is guaranteed in $\mathcal{A} = \mathrm{AG}(2, q)$ if and only if $n \mid q^2 - 1$ but $n \nmid q - 1$.*

Corollary 3.21. *Let m be an odd prime and $l \in \mathbb{N}$. Then, $\mathcal{A} = \mathrm{AG}(2, q)$ contains a shape-regular m^l-gon if and only if $l \mid q + 1$.*

The reason for considering shape-regular n-gons is, as Artzy and Kiss [1] discovered, a nice link with affinely regular polygons.

Theorem 3.22. *A shape-regular regular n-gon with the shape $s \in \mathbb{K} = GF(q^2)$ is an affinely regular if and only if $s + 1/s \in \mathbb{F} = GF(q)$.*

Proof. Let $(u_1 u_2 \ldots u_n)$ be a shape-regular n-gon with $S(u_{i+1} u_i u_{i+2}) = s$. Assume also that

$$u_i = \frac{t^{i-1} - 1}{t - 1} \tag{3.5}$$

and $t = -s$.

($\Longrightarrow$) Let us first prove the right implication, i.e, if $(u_1 u_2 \ldots u_n)$ is affinely regular, then $s + 1/s \in \mathbb{F}$. If $(u_1 u_2 \ldots u_n)$ is affinely regular, then by defintion, the lines $u_i u_j \parallel u_{i+k} u_{j-k}$. So, it means that $u_1 u_4 \parallel u_2 u_3$, and hence, $\frac{u_4 - u_1}{u_3 - u_2} \in \mathbb{F}$. Applying the formula in (3.5) for each u_i, with $i \in \{1, 2, 3, 4\}$, we get the following

$$\begin{aligned}
\frac{u_4 - u_1}{u_3 - u_2} &= \frac{\frac{t^3-1}{t-1} - \frac{t^0-1}{t-1}}{\frac{t^2-1}{t-1} - \frac{t-1}{t-1}} \\
&= \frac{\frac{t^3-1}{t-1}}{\frac{t^2-1-t+1}{t-1}} \\
&= \frac{(t-1)(t^2+t+1)}{t(t-1)} \\
&= \frac{t^2+t+1}{t} \\
&= t + 1 + \frac{1}{t}.
\end{aligned}$$

So,

$$t+1+\frac{1}{t}\in\mathbb{F} \iff -s-\frac{1}{s}\in\mathbb{F} \iff s+\frac{1}{s}\in\mathbb{F}.$$

($\Longleftarrow$) Let us also prove the left implication, i.e., if $s+1/s\in\mathbb{F}$, then $(u_1u_2\dots u_n)$ is affinely regular. If $s+1/s\in\mathbb{F}$, then $t+1/t\in\mathbb{F}$ as well. Furthermore, $t^q=t$ if and only if t is in a small field. So,

$$\left(t+\frac{1}{t}\right)^q=t^q+\frac{1}{t^q}=t+\frac{1}{t}.$$

From the equallity above, we have established the following

$$\begin{aligned}
t^q+\frac{1}{t^q}=t+\frac{1}{t} &\iff \frac{t^{2q}+1}{t^q}=\frac{t^2+1}{t}\\
&\iff t^{2q}+1=t^{q-1}(t^2+1)\\
&\iff t^{2q}-t^{q+1}-t^{q-1}+1=0\\
&\iff t^{q-1}(t^{q+1}-1)-1\cdot(t^{q-1}-1)=0\\
&\iff (t^{q-1}-1)(t^{q+1}-1)=0.
\end{aligned}$$

Thus, either $t^{q-1}-1=0$ or $t^{q+1}-1=0$. However, $t=-s\notin\mathbb{F}$. Hence, $t^q\neq t\Rightarrow t^{q-1}\neq 1$. So,

$$t^{q+1}-1=0\Rightarrow t^{q+1}=1.$$

Since n is the smallest integer for which $t^n=1$, it follows that $n|q+1$. Hence, a shape regular n-gon which is also an affinely regular has to be in the third class of affinely regular polygons described in Theorem 3.9, as $n|(q+1)$ and the n-gon is inscribed in an ellipse by Theorem 3.13. We are left to show that $u_ku_l \parallel u_{k+j}u_{l-j}$, where all k, l and j are calculated modulno n. Applying the formula in (3.5) for each u, we have

- $u_k=\frac{t^{k-1}-1}{t-1}$,
- $u_l=\frac{t^{l-1}-1}{t-1}$,
- $u_{k+j}=\frac{t^{k+j-1}-1}{t-1}$,
- $u_{l-j}=\frac{t^{l-j-1}-1}{t-1}$.

We need to show that

$$H(t)=\frac{\frac{t^{k-1}-1}{t-1}-\frac{t^{l-1}-1}{t-1}}{\frac{t^{k+j-1}-1}{t-1}-\frac{t^{l-j-1}-1}{t-1}}=\frac{t^{k-1}-t^{l-1}}{t^{k+j-1}-t^{l-j-1}}\in\mathbb{F},$$

i.e., $(H(t))^q=H(t)$. It yields

$$\begin{aligned}
\frac{t^{(k-1)q}-t^{(l-1)q}}{t^{(k+l-1)q}-t^{(l-j-1)q}}&=\frac{t^k-t^{l-1}}{t^{k+l-1}-t^{l-j-1}}\\
t^{(k-1)(q+1)+jq}+t^{(l-1)(q+1)-jq}-t^{(k+j)q+l}-t^{(l-j)q+k}&\\
=t^{(k-1)(q+1)+j}+t^{(l-1)(q+1)-j}-t^{kq+l-j}-t^{lq+k+j}&
\end{aligned}$$

Since $t^{q+1} = 1$, we have

$$\begin{aligned} t^{(k-1)(q+1)+jq} &= t^{(k-1)(q+1)+j} \\ t^{(l-1)(q+1)-jq} &= t^{(l-1)(q+1)-j} \\ -t^{(k+j)q+l} &= -t^{kq+l-j} \\ -t^{(l-j)q+k} &= -t^{lq+k+j} \end{aligned}$$

The needed condition is given by the sum of the four equations above. □

Corollary 3.23. *Let m be an odd prime, $l \in \mathbb{N}$ and $(u_1u_2 \dots u_{m^i})$ be a shape-regular $m^i - gon$ in affine plane. Then, it follows that $(u_1u_2 \dots u_{m^i})$ is also an affinely regular m^i-gon.*

Proof. Let $S(u_{k+1}u_ku_{k+2}) = s$.

- First, from Theorem 3.19, we have $(-s)^{m^i} = 1$.
- Further, it follows from Corollary 3.21 that $m^i \mid q + 1$.
- Thus, $(-s)^{m^i} = (-s)^{q+1} = 1$ and hence, $s + 1/s \in \mathbb{F}$.
- Finally, Theorem 3.22 implies that $(u_1u_2 \dots u_{m^i})$ is an affinely regular m^i-gon.

□

3.4 SOME RESULTS INVOLVING PROJECTIVE ARCS AND AFFINELY POLYGONS

Now, going back to our sets of points **S** and **T**, we could also observe the following. If **S** is sharply focused on l and **T** is the set of non-covered points of l, then every line passing through a point of **S** has at most one additional point of $\mathbf{S} \cup \mathbf{T}$. Moreover, in the studying of sharply focused sets, we will also use some results regarding the nuclues.

We could also define the sharply focused and hyperfocused arcs using the notion of the focus set, which represents a set of points used to build a conic section. The following definition is the equivalence of the Definition 3.19.

Definition 3.24. Let $\mathcal{K}$ be a k-arc and l an exterior line to $\mathcal{K}$. We say that

- $\mathcal{K}$ is *very sharply focused*, or hyperfocused on l, with focus set $\mathcal{F}$ containing all points of l covered by the chords of $\mathcal{K}$ if $|\mathcal{F}| = k - 1$,
- $\mathcal{K}$ is *sharply focused* on l with focus set $\mathcal{F}$ if $|\mathcal{F}| = k$.

Before stating the result on the bounds of $\mathbf{S}$ and $\mathbf{T}$, let us define the term of nucleus.

Definition 3.25. Let $\mathcal{K}$ be a set of k points in a projective plane $\mathrm{PG}(2,q)$. We call a point $P \in \mathcal{K}$ a *nucleus*, if every line through P has at most one more point of $\mathcal{K}$.

Notation: We denote the set of nuclei of $\mathcal{K}$ by $N(\mathcal{K})$.

If $\mathcal{K} = \mathbf{S} \cup \mathbf{T}$, then $N(\mathcal{K}) = \mathbf{S}$. Moreover, if $|\mathbf{T}| > 2$, $N(\mathbf{S} \cup \mathbf{T}) = \mathbf{S}$. Regarding the size of the union of $\mathbf{S}$ and $\mathbf{T}$, Bichara and Korchmáros, Wettl, and Szőnyi proved some upper bounds of order summarized in the following theorem in [3].

Theorem 3.26. *Suppose that* $\mathbf{S}$ *and* $\mathbf{T}$ *are two nonempty sets of points in a projective plane* $\mathrm{PG}(2,q)$*, such that* $\mathbf{S}$ *is an arc,* $\mathbf{T}$ *is a subset of line* l*,* $\mathbf{S} \cap l = \emptyset$*, and no secant of* $\mathbf{S}$ *has a point in* $\mathbf{T}$*. The following results are obtained:*

1. $|\mathbf{S} \cup \mathbf{T}| \leq q + 2$.
2. *If* $|\mathbf{S} \cup \mathbf{T}| = q + 2$ *and* $|\mathbf{S}| \geq 3$*, then* q *is even and* $|\mathbf{S}| \leq q/2$*. (Bichara and Korchmáros)*
3. *If* $|\mathbf{S} \cup \mathbf{T}| = q + 1$*, where* q *is odd or even, and* $\mathbf{S}$ *is a subarc of a conic, then* $|\mathbf{S}| \leq (q+1)/2$*. (Wettl)*
4. *If* $|\mathbf{S} \cup \mathbf{T}| = q + 1$ *and* q *is odd, then* $\mathbf{S}$ *is a subarc of a conic, and*
$$|\mathbf{S}| \mid q+1, \quad |\mathbf{S}| \mid q, \quad \text{or} \quad |\mathbf{S}| \mid q-1. \text{ (Wettl)}$$
5. *If* $|\mathbf{S} \cup \mathbf{T}| \geq q - \sqrt{q}/8 + 2$*,* q *is odd and* $q > q_0$*, then* $|\mathbf{S}| \leq (q+1)/2$*. (Szőny)*

Proof. We will prove the first and the third parts of the theorem. We omit the proofs of the others as they are beyond the scope of this thesis.

1. Let $\mathcal{K}$ be a nonempty set in $\mathrm{PG}(2,q)$ such that $\mathcal{K} = \mathbf{S} \cup \mathbf{T}$. So, $\mathcal{K} > 2$. Then if you take an arbitrary point, there exists at least $q+1$ other points in the set. But through that point, there are $q+1$ lines. So, by the Pigenhole principle $|\mathcal{K}| \leq 1 + q + 1 = q + 2$.

3. Let us now show that for $|\mathcal{K}| = |\mathbf{S} \cup \mathbf{T}| = q+1$, where q is odd or even, and $\mathbf{S}$ is a subarc of a conic, we have $|\mathbf{S}| \leq (q+1)/2$.
We will use the result from Wettl [28] in the case when q is even.

Lemma 3.27. *If* $\mathcal{K}$ *is a* $(q+1)$*-pointset of* $\mathrm{PG}(2,q)$*,* q *is even,* $|N(\mathcal{K})| \geq 3$*, then the tangents of* $\mathcal{K}$ *to the points of* $N(\mathcal{K})$ *belong to the same pencil. The support of this pencil is the only point such that* $N(\mathcal{K}) \leq N(\mathcal{K}')$*, where* $\mathcal{K}' = \mathcal{K} \cup O$.

– If q is even, then the set $\mathcal{K}'$ from Lemma 3.27 is a $(q+2)$-set, i.e.,

$$|\mathcal{K}| = q+1 \Rightarrow |\mathcal{K}'| = |\mathcal{K}| + 1 = q+1+1 = q+2.$$

Hence, we derive the following relation

$$\begin{aligned} |\mathbf{S}| = |N(\mathcal{K})| &\leq |\mathcal{K}'| \quad \text{follows from Lemma 3.27} \\ &\leq \frac{q}{2} \quad \text{follows from the previous part as } \mathcal{K}' \text{ is a } (q+2)\text{-set} \\ &\leq \frac{q}{2} + \frac{1}{2} \\ &= \frac{q+1}{2}. \end{aligned}$$

Hence, we establish that in the case of even q, $|\mathbf{S}| \leq (q+1)/2$.

– If q is odd, we will use the hypothesis that $\mathbf{S}$ is a subarc of some conic $\mathcal{C}$. Let $P \in \mathcal{K} \setminus \mathbf{S}$ be a point.

∗ If P is an inner point of $\mathcal{C}$, then every secant of $\mathcal{C}$ through P is incident with at most one more point of $\mathbf{S}$, i.e., of $N(\mathcal{K})$ (by the definition of $N(\mathcal{K})$). So,

$$|\mathbf{S}| \leq |N(\mathcal{K})| \leq \frac{q+1}{2}.$$

∗ If P is an outer point, then two tangents of $\mathcal{C}$ through P are not the tangents of $\mathbf{S}$, i.e, of $N(\mathcal{K})$, and there are only $(q+1)/2$ secants of $\mathcal{C}$ through P. So,

$$|S| = |N(\mathcal{K})| \leq \frac{q-1}{2} \leq \frac{q+1}{2}.$$

Hence, in both cases $|\mathbf{S}| \leq (q+1)/2$.

□

Lemma 3.28. *Suppose that* $\mathbf{S}$ *and* $\mathbf{T}$ *are two nonempty sets of points in a projective plane* $\mathrm{PG}(2,q)$*, such that* $\mathbf{S}$ *is an arc,* $\mathbf{T}$ *is a subset of line* l*,* $\mathbf{S} \cap l = \emptyset$*, and no secant of* $\mathbf{S}$ *has a point in* $\mathbf{T}$*. Then* $|\mathbf{S}| < q$*.*

Proof. Using The Principle of Inclusion and Exclusion (PIE), we know that

$$|\mathbf{S} \cup \mathbf{T}| = |\mathbf{S}| + |\mathbf{T}| - |\mathbf{S} \cap \mathbf{T}|. \tag{3.6}$$

Furthermore, we have the following data:

- $|\mathbf{S} \cup \mathbf{T}| = q+2$,
- $\mathbf{S} \cap \mathbf{T} = \emptyset \Rightarrow |\mathbf{S} \cap \mathbf{T}| = 0$,
- $|\mathbf{T}| > 2 \Rightarrow -|\mathbf{T}| < -2$.

Rearranging formula in PIE and applying these results, we obtain the following

$$\begin{aligned}|\mathbf{S}| &= |\mathbf{S} \cup \mathbf{T}| - |\mathbf{T}| \\ |\mathbf{S}| &= q + 2 - |\mathbf{T}| \\ |\mathbf{S}| &< q + 2 - 2 \\ |\mathbf{S}| &< q.\end{aligned}$$

Recall that we have defined $\mathcal{K} = \mathbf{S} \cup \mathbf{T}$ and $N(\mathcal{K}) = \mathbf{S}$. Thus,

$$|\mathbf{S}| = |N(\mathcal{K})| < q.$$

□

Wettl [28] used the idea of nuclei and provided some results on k-arcs and affinely regular polygons. Before starting his results, let us describe what the idea behind them is. From the affinely regular n-gons, we can create sets such that the points that are not in the nucleus-set are collinear. We pick vertices of the n-gon and points on the line at infinity l_∞ (ideal line). This set's nucleus is an n-gon. The strategy is to identify all $(q+1)$-sets with collinear non-nucleus points. Recall that $(q+1)$-arc is named oval, while $(q+2)$-arc is named hyperovals. Let $\mathcal{O}$ be an oval and l_∞ be an ideal line. We denote the points of $\mathcal{O}$ different from those on l_∞ by O_1, O_2, …, O_m, and by L_1, L_2, …, L_m points on l_∞ that are not on $\mathcal{O}$ with $O_1O_iL_i$ being collinear for $i = 1, 2, \ldots, m$ and $m = q+1$, $m = q$ or $m = q-1$. We define the following operation on indicies

$$i * j = k \iff O_iO_jO_k \text{ is collinear}, \quad i, j, k \in \{1, 2, \ldots, m\}. \tag{3.7}$$

We also need the notion of Pascal line, which involves the notion of hexagon of an oval.

Definition 3.29. An ordered set $(P_1, P_2, P_3, Q_1, Q_2, Q_3)$ of an oval $\mathcal{O}$ with $P_i \neq P_j$, $Q_i \neq Q_j$ and $P_i \neq Q_i$, $i, j \in \{1, 2, 3\}$ represents a *hexagon* $\mathcal{H}$ of $\mathcal{O}$ with the diagonal points depicted by the intersection of the lines $P_iQ_j \cap P_jQ_i$, $i \neq j$.

Definition 3.30. The line l represents a *Pascal line* with respect to an oval $\mathcal{O}$, if every hexagon of $\mathcal{O}$ with two diagonal points on l also has the third one on l.

The set of indicies with respect to the operation defined in (3.7) is a group if and only if the oval is Pascalian with respect to the ideal line. If $\mathcal{O}'$ is a subarc of $\mathcal{O}$, then the indices of points on $l_\infty \setminus \mathcal{O}$ that are covered by the secants of $\mathcal{O}'$ represents the set $\{i * j |\ i, j \in \mathcal{O}', i \neq j\}$. We take $i \neq j$ as we are only interested in secants, not tangents. $\mathcal{O}'$ is an affinely regular polygon of order $|\mathcal{O}'|$ if $\mathcal{O}'$ is a cyclic coset.

Let us now state the result provided by Wettl in [28].

Theorem 3.31 (Wettl)**.** *Let $q = p^i$, with odd p and $\mathcal{K}$ be a k-arc in $\mathrm{AG}(2, q)$. If the secants of $\mathcal{K}$ cover exactly k points of l_∞ then*

$$k \mid q+1, \quad k \mid q \quad or \quad k \mid q-1.$$

Moreover, the k-arc is an affinely regular k-gon if $p^2 \nmid k$.

Proof. Denote ba $\mathcal{L}$ the set of points on l_∞ that are not covered by the secants and points of $\mathcal{K}$. The set of nuclei of $\mathcal{L}$ corresponds to $\mathcal{K}$, i.e., $N(\mathcal{L}) = \mathcal{K}$. Furthermore, from Theorem 3.26, $\mathcal{K}$ is a subset of an irreducible conic $\mathcal{C}$. We can eliminate the restriction of $i \neq j$ because the tangents of $\mathcal{L}$ to the points of $\mathcal{K}$ are also tangents of $\mathcal{O}$. So $\mathcal{K}$ covers $|\mathcal{K}|$ ideal points if $|\mathcal{K} * \mathcal{K}| = |\mathcal{K}|$, i.e., if $\mathcal{K}$ is a coset. However, this coset is cyclic only in the case that p^2 does not divide k, i.e., $p^2 \nmid k$. □

Similar proof can be derived when q is even. We will only state the theorem for this case.

Theorem 3.32 (Wettl)**.** *Let $\mathcal{K}$ be a k-arc of an oval $\mathcal{O}$ with the ideal line l_∞ being Pascal line in $\mathcal{A} = \mathrm{AG}(2, q)$, q is even. If the secants of $\mathcal{K}$ cover exactly k points of l_∞ then*

$$k \mid q+1, \quad k \mid q-1 \quad or \quad k+1 \mid q.$$

Moreover, the k-arc is affinely regular k-gon if $\mathcal{O}$ is an ellipse or hyperbola.

4 CONSTRUCTIONS

Throughout the second and third chapter, we pointed out some properties and bounds regarding the sets **S** and **T**. Since we will be working on their constructions in this chapter, let us emphasize the conditions that the sets **S** and **T** should meet. Recall also from the second chapter that we denoted the secret by X.

Lemma 4.1. *Let l be a line in* $\mathrm{PG}(n,q)$*. Then* **S** *and* **T** *are sets of points that satisfy the following conditions:*

1. $|\mathbf{T}| > 2$, $\mathbf{T} \subseteq l$ *and* $X \in \mathbf{T}$,
2. $|\mathbf{S}| > n$,
3. *sets* **S** *and* **T** *are disjoint, i.e.,* $\mathbf{S} \cap \mathbf{T} = \emptyset$.
4. *no more points of* $\mathbf{S} \cup \mathbf{T}$ *are in any subspace generated by n points of* **S**,
5. $\mathbf{S} \subset \mathcal{G}_n$, *where* $\mathcal{G}_n = \{(1, t, \ldots, t^{n-1}, t^n)\mid\ t \in GF(q)^+\}$.

Remark 4.2. $GF(q)^+$ represents $GF(q) \cup \{\infty\}$ and P_∞ is a point at infinity with coordinates $(0 : 0 : \cdots : 0 : 1)$.

The conditions (2) and (4) imply that **S** is an arc in $\mathrm{PG}(n,q)$. Moreover, if $\{P_1, P_2, P_3\} \subset \mathbf{T}$, then $\mathbf{S} \cup \{P_i\}$ is an arc but $\mathbf{S} \cup \{P_1, P_2, P_3\}$ is not. We obtain an upper bound of **S** by using findings regarding the lower bound of k for a k-arc with just one completion. In the previous chapter, we have seen in Theorem 3.26 that for $n = 2$, $|\mathbf{S}| \leq (q+1)/2$, which is proved by Szőnyi. For $n \geq 2$, Blokhuis, Bruen and Thas [6] provided the upper bounds for **S** based on the parity of q. It is given in the following theorem.

Theorem 4.3 (Blokhuis, Bruen and Thas)**.** *We have the following upper bounds for* **S** *based on the parity of q:*

- *If q is even, then* $|\mathbf{S}| \leq \frac{1}{2}q + n - 1$.
- *If q is odd, then* $|\mathbf{S}| \leq \frac{2}{3}(q-1) + n$.

Moreover, from the propety given in (5), we have the following consequence.

Corollary 4.4. $\mathbf{S} \subset \mathcal{G}_n \Rightarrow n \leq q$.

Proof. This is straightforward. Since $|\mathbf{S}| > n$ and $\mathbf{S} \subset \mathcal{G}_n$, it follows that

$$n+1 \leq |\mathbf{S}| \leq |\mathcal{G}_n| = q+1 \Rightarrow n \leq q.$$

□

Let us first define the notion of the elementary symmetric polynomial. See also [13].

Definition 4.5. Let $t_1, t_2, \ldots, t_n$ be variables and $\mathbb{K}$ be an arbitrary field. In the polynomial ring $\mathbb{K}[t_1, t_2, \ldots, t_n]$ let

$$S_k(t_1, t_2, \ldots, t_n) = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} t_{i_1} t_{i_2} \cdots t_{i_k}.$$

S_k is called the *k-th symmetric elementary polynomial* of the variables $t_1, t_2, \ldots, t_n$.

Lemma 4.6. *Let $P(t) = (1 : t : \cdots : t^{i-1} : t^i)$. Take n different points*

$$P(t_1), P(t_2), \ldots, P(t_n).$$

Then the hyperplane through these points has coordinate vector

$$\Big((-1)^n t_1 t_2 \ldots t_n : \cdots : (t_1t_2 + \cdots + t_1t_n + t_2t_3 + \cdots + t_2t_n + \cdots t_{n-1}t_n) : -(t_1 + \cdots + t_n) : 1\Big).$$

Proof. The point $(X_0 : X_1 : \cdots : X_n)$ is on the hyperplane if its coordinates can be expressed as a linear combination of $P(t_1), P(t_2), \ldots, P(t_n)$. So, the equation is

$$\begin{vmatrix} X_0 & X_1 & \cdots & X_n \\ 1 & t_1 & \cdots & t_1^n \\ \vdots & \vdots & \ddots & \vdots \\ 1 & t_n & \cdots & t_n^n \end{vmatrix} = 0. \tag{4.1}$$

We are looking for a simpler form of (4.1).
Expand it according to the first row. So,

$$X_0 \cdot \begin{vmatrix} t_1 & \cdots & t_1^n \\ \vdots & \ddots & \vdots \\ t_n & \cdots & t_n^n \end{vmatrix} - X_1 \cdot \begin{vmatrix} 1 & \cdots & t_1^n \\ \vdots & \ddots & \vdots \\ 1 & \cdots & t_n^n \end{vmatrix} + \cdots + (-1)^n X_n \cdot \begin{vmatrix} 1 & \cdots & t_1^{n-1} \\ \vdots & \ddots & \vdots \\ 1 & \cdots & t_n^{n-1} \end{vmatrix} = 0.$$

We apply a trick for calculating the coefficients. Consider the Vandermonde determinant of $n+1$ variables

$$V = \begin{vmatrix} 1 & T & \cdots & T^n \\ 1 & t_1 & \cdots & t_1^n \\ \vdots & \vdots & \ddots & \vdots \\ 1 & t_n & \cdots & t_n^n \end{vmatrix}.$$

On the one hand, it is well-known that

$$\begin{aligned} V &= \prod_{i=1}^{n}(T-t_i)\prod_{i\neq j}(t_i-t_j) \\ &= [T^n-(t_1+\cdots+t_n)T^{n-1}+(t_1t_2+\cdots+t_1t_n+t_2t_3+\cdots t_2t_n+\cdots+t_{n-1}t_n)T^{n-2} \\ &-\cdots+(-1)^n(t_1t_2\ldots t_n)]\prod_{i\neq j}(t_i-t_j) \\ &= [T^n-S_1T^{n-1}+S_2T^{n-2}+\cdots+(-1)^nS_n]\prod_{i\neq j}(t_i-t_j). \end{aligned} \tag{4.2}$$

On the other hand, expanding it according to the first row, we get

$$1\cdot\begin{vmatrix} t_1 & \cdots & t_1^n \\ \vdots & \ddots & \vdots \\ t_n & \cdots & t_n^n \end{vmatrix} - T\cdot\begin{vmatrix} 1 & \cdots & t_1^n \\ \vdots & \ddots & \vdots \\ 1 & \cdots & t_n^n \end{vmatrix} + \cdots + (-1)^nT_n\cdot\begin{vmatrix} 1 & \cdots & t_1^{n-1} \\ \vdots & \ddots & \vdots \\ 1 & \cdots & t_n^{n-1} \end{vmatrix} = 0. \tag{4.3}$$

Thus, the coefficient of T^k is the same as the coefficient of X_k. Comparing the coefficients in (4.2) and (4.3), we have the coordinates of the hyperplane

$$\Big((-1)^nS_n\prod(t_i-t_j):\cdots:S_2\prod(t_i-t_j):-S_1\prod(t_i-t_j):\prod(t_i-t_j)\Big), \tag{4.4}$$

and because of the homogenity, it is equivalent to

$$((-1)^nS_n:\cdots:S_2:-S_1:1). \tag{4.5}$$

□

Based on the previously metioned conditions, Beutelspacher and Wettl [3] provided the following constructions.

Proposition 4.7. *For every divisor q' of q, there are* $\mathbf{S}$ *and* $\mathbf{T}$ *satisfying previously defined conditions* $(1)-(5)$ *with*

$$|\mathbf{S}\cup\mathbf{T}| = q+1 \quad \textit{and} \quad |\mathbf{S}| = q'.$$

Proof. Now, take a line l through $(0:0:\cdots:0:1)$ and $(0:0:\cdots:1:0)$. The points of this line are given in the following form:

$$Q(t) = t(0:0:\cdots:0:1)+(0:0:\cdots:1:0) = (0:0:\cdots:1:t).$$

This point is incident with the hyperplane given by coordinates in (4.4) if and only if

$$\begin{aligned} Q(t) \in \mathcal{H} &\iff \Big\langle (0 : \cdots : 1 : t), ((-1)^n t_1 t_2 \dots t_n : \cdots : -(t_1 + \cdots + t_n) : 1) \Big\rangle = 0 \\ &\iff -(t_1 + t_2 + \cdots + t_n) + t = 0 \\ &\iff t = t_1 + t_2 + \cdots + t_n. \end{aligned}$$

Now, let G_1 be a coset of a subgroup of order q' of $(GF(q), +)$, i.e., the additive group of $GF(q)$ and let $G_2 = G_1 + G_1 + \cdots + G_1 = nG_1$. Finally, let $\mathbf{S} = \{P(t) |\ t \in G_1\}$ and $\mathbf{T} = \{Q(t) |\ t \in GF(q) \backslash G_2\} \cup \{P_\infty\}$. Then, from the group theory, we know that order of subgroup, and hence the order of a coset, divides the order of the group. So, since the order of our group is q, $|\mathbf{S}| = |G_1| = q'$ as we denoted by q' some divisor of q. However, as every coset wrt G_1 is of the same order, then $|G_2| = |nG_1| = |G_1| = q'$. Thus, $|\mathbf{T}| = |GF(q)| - |nG_2| = q - q' + 1$, where $+1$ stands for $|\{P_\infty\}|$. Finally, since $\mathbf{S} \cap \mathbf{T} = \emptyset$, we have that

$$|\mathbf{S} \cup \mathbf{T}| = |\mathbf{S}| + |\mathbf{T}| - |\mathbf{S} \cap \mathbf{T}| = q' + q - q' + 1 = q + 1.$$

□

Proposition 4.8. *For every divisor q' of $q-1$, there are* $\mathbf{S}$ *and* $\mathbf{T}$ *satisfying previously defined conditions* (1) − (5) *with*

$$|\mathbf{S} \cup \mathbf{T}| = q + 1 \quad \textit{and} \quad |\mathbf{S}| = q'.$$

Proof. Again, let $P_n(t) = (1 : t : \cdots : t^{n-1} : t^n)$, where $t \in GF(q)$. The coordinates of the hyperplane $\mathcal{H}$ through different points $P(t_1)$, $P(t_2)$, …, $P(t_n)$ correspond to the coefficients of the elementary symmetric polynomial in $t_1, t_2, \dots, t_n$, where $t_i \in GF(q)$. So, the coordinates of this hyperplane are described in the previous theorem by the equation given in (4.4). Now, take a line l through zero point and point at infinity, i.e., $(0 : 0 : \cdots : 0 : 1)$ and $(1 : 0 : \cdots : 0 : 0)$. The points of this line are given in the following form:

$$Q(t) = (-1)^{n-1} t (0 : 0 : \cdots : 0 : 1) + (1 : 0 : \cdots : 0 : 0) = (1 : 0 : \cdots : 0 : (-1)^{n-1} t).$$

This point is incident with the hyperplane given by coordinates in (4.4) if and only if

$$\begin{aligned} Q(t) \in \mathcal{H} &\iff \Big\langle (1 : 0 : \cdots : (-1)^{n-1} t), ((-1)^n t_1 \dots t_n : \cdots : -(t_1 + \cdots + t_n) : 1) \Big\rangle = 0 \\ &\iff (-1)^n t_1 t_2 \dots t_n + (-1)^{n-1} t = 0 \\ &\iff (-1)^{n-1} t = -(-1)^{n-1} (-1) t_1 t_2 \cdots, t_n \\ &\iff t = t_1 t_2 \cdots t_n. \end{aligned}$$

Now, let G_1 be a coset of a subgroup of order q' of $(GF(q)^*, \cdot)$, i.e., the multiplicative group of the field of order q and let $G_2 = G_1 \cdots G_1 = G_1^n$.

Finally, let $\mathbf{S} = \{P(t)|\ t \in G_1\}$ and $\mathbf{T} = \{Q(t)|\ t \in (GF(q)^*, \cdot)\backslash G_2\} \cup \{P_0\} \cup \{P_\infty\}$. Then, from the group theory, we know that order of subgroup, and hence the order of a coset, divides the order of the group. So, since the order of our group is q, $|\mathbf{S}| = |G_1| = q'$ as we denoted by q' some divisor of q. However, as every coset wrt G_1 is of the same order, then $|G_2| = |G_1^n| = |G_1| = q'$. Thus, $|\mathbf{T}| = |GF(q)^*| - |G_2| = (q-1) - q' + 2 = q - q' + 1$, where $+2$ stands for $|\{P_0\}|$ and $|\{P_\infty\}|$. Finally, since $\mathbf{S} \cap \mathbf{T} = \emptyset$, we have that

$$|\mathbf{S} \cup \mathbf{T}| = |\mathbf{S}| + |\mathbf{T}| - |\mathbf{S} \cap \mathbf{T}| = q' + q - q' + 1 = q + 1.$$

□

Proposition 4.9. *For every divisor q' of $q+1$, there are $\mathbf{S}$ and $\mathbf{T}$ satisfying previously defined conditions $(1) - (5)$ with*

$$|\mathbf{S} \cup \mathbf{T}| = q + 1 \quad \textit{and} \quad |\mathbf{S}| = q'.$$

Proof. We will only consider the case when q is odd. For the other case, i.e., when q is even, we refer the reader to [3].
Let $m \in GF(q)\backslash\{0\}$ be a non-square, and let $i \in GF(q^2)$ with $i^2 = m$. Denote by l a line containing the points $P(i)$ and $P(-i)$ corresponding to the conjugate points of $\mathcal{G}_n$. Moreover, l contains the points $(1:0:m:0:m^2:0:\cdots)$ and $(0:1:0:m:0:m^2:\cdots)$. Let's check it. First, the homogeneous coordinates of $P(i)$ and $P(-i)$ are

$$\begin{aligned} P(i) &= (1 : i : i^2 : i^3 : i^4 : i^5 : \cdots : i^n) = (1 : i : m : im : m^2 : im^2 \cdots) \\ P(-i) &= (1 : -i : i^2 : -i^3 : i^4 : -i^5 : \cdots : (-i)^n) = (1 : -i : m : -im : m^2 : -im^2 \cdots). \end{aligned}$$

Now, if we take the following linear combinations of $P(i)$ and $P(-i)$, we will obtain the required points, i.e.,

$$\begin{aligned} \frac{1}{2}P(i) + \frac{1}{2}P(-i) &= (1:0:m:0:m^2:0:\cdots) \\ \frac{1}{2i}P(i) - \frac{1}{2i}P(-i) &= (0:1:0:m:0:m^2:0:\cdots). \end{aligned}$$

So, the real points of this line are given in the following form

$$\begin{aligned} Q(t) &= (1:0:m:0:m^2:0:\cdots) + t(0:1:0:m:0:m^2:\cdots) \\ &= (1:t:m:mt:m^2:m^2t:\cdots). \end{aligned}$$

This point is incident with the hyperplane given by coordinates in (4.5) if and only if

$$Q(t) \in \mathcal{H} \iff \Big\langle (1:t:m:mt:m^2:m^2t:\cdots), ((-1)^n S_n : \cdots : S_2 : -S_1 : 1) \Big\rangle = 0.$$

If n is even, then

$$\begin{aligned} Q(t) \in \mathcal{H} &\iff \Big\langle (1 : t : m : mt : m^2 : m^2t : \cdots), (S_n : -S_{n-1} : S_{n-2} : \cdots : -S_1 : 1) \Big\rangle = 0 \\ &\iff S_n - tS_{n-1} + mS_{n-2} - mtS_{n-3} + m^2S_{n-4} - m^2tS_{n-5} + \cdots = 0 \\ &\iff S_n + mS_{n-2} + m^2S_{n-4} + \cdots = t(S_{n-1} + mS_{n-3} + m^2S_{n-5} + \cdots) \\ &\iff t = \frac{S_n + mS_{n-2} + m^2S_{n-4} + \cdots}{S_{n-1} + mS_{n-3} + m^2S_{n-5} + \cdots}. \end{aligned}$$

If n is odd, then

$$\begin{aligned} Q(t) \in \mathcal{H} &\iff \Big\langle (1 : t : m : mt : m^2 : m^2t : \cdots), (-S_n : S_{n-1} : -S_{n-2} : \cdots : S_1 : 1) \Big\rangle = 0 \\ &\iff -S_n + tS_{n-1} - mS_{n-2} + mtS_{n-3} - m^2S_{n-4} + m^2tS_{n-5} - \cdots = 0 \\ &\iff t(S_{n-1} + mS_{n-3} + m^2S_{n-5} + \cdots) = S_n + mS_{n-2} + m^2S_{n-4} + \cdots \\ &\iff t = \frac{S_n + mS_{n-2} + m^2S_{n-4} + \cdots}{S_{n-1} + mS_{n-3} + m^2S_{n-5} + \cdots}. \end{aligned}$$

So, in both cases, we derived that

$$t = \frac{S_n + mS_{n-2} + m^2S_{n-4} + \cdots}{S_{n-1} + mS_{n-3} + m^2S_{n-5} + \cdots}.$$

Now, define a group $(G, \circ)$ in $GF(q)^+$ such that

$$t_1 \circ t_2 = \frac{t_1t_2 + m}{t_1 + t_2}, \quad t_1, t_2, \in GF(q)^+.$$

Moreover, consider the following correspondence:

$$\begin{aligned} t_1 \to T_1 &= \{\rho_1(t_1 + i) |\ \rho_1 \in GF(q)^*\}, \\ \infty \to T_\infty &= \{\rho \in GF(q)^*\}. \end{aligned}$$

Recall that $|GF(q)^*| = q-1$. Furthermore, the multiplication between the above $(q-1)$-element subsets correspond to the ordinary multiplication of the complex numbers, i.e.,

$$T_1T_2 = \{\rho_1(t_1 + i)\} \cdot \{\rho_2(t_2 + i)\} = \Big\{(t_1 + t_2)\rho_1\rho_2\Big(\frac{t_1t_2 + m}{t_1 + t_2} + i\Big)\Big\},$$

where T_1T_2 corresponds to $t_1 \circ t_2$.

Recall also that $|GF(q^2)| = q^2 - 1$. As every set of $GF(q)^*$ contains $q - 1$ elements, it yields that $|G| = q + 1$, where $(G, \circ)$ is a cyclic group.
Now, the hyperplane through $P(t_1), P(t_2), \ldots, P(t_n)$ contains $Q(t)$ if and only if $t = t_1 \circ t_2 \circ \cdots \circ t_n$.
As in the previous cases, let G_1 be a coset of a subgroup of order q' of G and let $G_2 = G_1 \circ \cdots \circ G_1$. Finally, let $\mathbf{S} = \{P(t) |\ t \in G_1\}$ and $\mathbf{T} = \{Q(t) |\ t \in G \backslash G_2\}$. Then,

$$|\mathbf{S} \cup \mathbf{T}| = |\mathbf{S}| + |\mathbf{T}| - |\mathbf{S} \cap \mathbf{T}| = q' + q + 1 - q' = q + 1.$$

□

If the index of G_1 in the constructions above is 2, we get the maximum values for the order of $\mathbf{S}$. This is explicitly stated in the following corollary:

Corollary 4.10. *There are sets* $|\mathbf{S}|$ *and* $|\mathbf{T}|$ *that satisfy* $(1)-(5)$ *such that:*

- *If* q *is odd, then*
  - $|\mathbf{S}| = \frac{q+1}{2}, \quad |\mathbf{T}| = \frac{q+1}{2}$ *or*
  - $|\mathbf{S}| = \frac{q-1}{2}, \quad |\mathbf{T}| = \frac{q+3}{2}$.
- *If* q *is even, then*

$$|\mathbf{S}| = \frac{q}{2}, \quad |\mathbf{T}| = \frac{q+2}{2}.$$

We have seen that $\mathbf{S}$ is a noncomplete arc that can be extended with points from the set $\mathbf{T}$. Storme and Szőnyi [3] investigated $(k+1)$-arcs in $\mathrm{PG}(n,q)$, $n \geq 3$, with k points from a normal rational curve and found the following.

Theorem 4.11. *If* q *is large enough, being even or a power of a prime greater than* 5*, and* $\mathbf{S}'$ *satisfies the conditions given in* $(1)-(5)$*, then* $|\mathbf{S}| \leq \frac{q+1}{2}$*. If*

$$\begin{aligned} 0.42q + n - 3 \leq \quad |\mathbf{S}'| \quad &\leq \frac{q+1}{2} \quad \text{or} \\ 0.41(q+1) + n - 2 \leq \quad |\mathbf{S}'| \quad &\leq \frac{q}{2} + 1 \end{aligned}$$

depending on the parity of q*, then* $\mathbf{S}' \subseteq \mathbf{S}$*, where* $\mathbf{S}$ *corresponds to the one of the sets in Corollary 4.10, and* $|\mathbf{S}' \cup \mathbf{T}| \leq q+1$.

5 CONCLUSION

Secret sharing schemes are perfect for storing sensitive and vital information. They enable the distributor to securely store the secret with the group even if not all members can be trusted at all times. The secret is safe as long as the number of illegal constellations does not exceed the critical number required to reconstruct the secret. We mentioned the three most important secret-sharing schemes: Threshold schemes, Compartment schemes, and Multilevel schemes. Using the concepts from finite geometry, we described each of them and proved their perfectness. Under this term, we meant that no proper subset of shares releases any information about the secret. We also illustrated the trivial examples for each of them. In the rest of the thesis, we focused on the specified type of the multilevel scheme, $(2, s)$-level schemes. As there are two levels, whose sets of participants we denote by $\mathbf{S}$ and $\mathbf{T}$, we discussed some bounds on these sets. In that manner, we introduced the affinely regular polygons and projective k-arcs. The classification of affinely regular polygons, based on the conic in which it is described (hyperbola, ellipse, parabola), played the most important part of the third chapter. Based on the properties we derived, we described constructions of sets $\mathbf{S}$ and $\mathbf{T}$ in the fourth chapter. We have seen that these bounds were a topic of interest for several researchers who established different bounds depending on the predefined conditions. Hence, one could see that these bounds were not chosen arbitrarily, but they arose from finite geometry. The reason for taking the geometry is that, as Beutelspacher and Rosenbaum [2] pointed out, an issue given in an application could be translated into a geometrical problem, commonly only considering the incidence structure. The applications focus on projective and affine spaces over finite fields because of their calculation efficiency. A scheme that is built on geometry preserves all of the underlying geometric structure. Furthermore, geometries' complex structures are used to create efficient models for hierarchical structures and systems. Unlike some algorithms, the security of crypto-systems derived from geometry can be verified as they rely on proven assumptions.

6 DALJŠI POVZETEK V SLOVENSKEM JEZIKU

Kot smo že povedali, magistrsko delo se osredotoča na to, kako je sheme delitve skrivnosti mogoče videti skozi končno geometrijo z uporabo lastnosti afine in projektivne geometrije. Pojem sheme za delitev skirvnosti je vedno obstajal. Zdaj je povezan predvsem s procesom varstva podatkov. Danes je nujno zaščititi pomembne in občutljive podatke, ki so pogosto izpostavljeni napadom. Skrivnost je moč rekonstruirati, ko je pridobljeno zadostno število skrivnih delov. Za pojasnitev pojma sheme za skupno rabo skrivnosti si oglejmo naslednji primer. Recimo, da želite sestaviti skrivni X, n-bitni niz in ga razdeliti na delne skrivnosti, imenovane deleži, tako da ga je mogoče rekonstruirati le, če sta znani vsaj dva deleža. Uporabimo projektivno ravnino $\mathrm{PG}(2, q)$, da zgradimo takšno metodo skupne rabe skrivnosti. Kot je predlagano v članku [21], če razmišljamo o udeležencih kot točkah in dostopni skupini kot blokih, bi lahko modelirali takšno shemo z uporabo končne geometrije. Razlog za uporabo geometrije je, kot sta poudarila Beutelspacher in Rosenbaum [2], da bi lahko težavo, podano v uporabi, prevedli v geometrijski problem, ki običajno upošteva samo incidenčno strukturo. Aplikacije se zaradi učinkovitosti računanja osredotočajo na projektivne prostore nad končnimi polji. Shema, ki temelji na geometriji, ohranja vso osnovno geometrijsko strukturo. Poleg tega se kompleksne strukture geometrij uporabljajo za ustvarjanje učinkovitih modelov za hierarhične strukture in sisteme. Za razliko od nekaterih algoritmov je varnost kriptosistemov, ki izhajajo iz geometrije, mogoče preveriti, saj temeljijo na dokazanih predpostavkah. V magistrski nalogi so obravnavane tri naj-pomembnejše sheme za izmenjavo skrivnosti: sheme pragov, predelkov in večnivojskih shem. Če nobena ustrezna podmnožica deležev ne izda nobenih informacij o skrivnosti, velja, da je shema skupne rabe skrivnosti popolna. Ta lastnost je dokazana za vse omenjene sheme skupaj z njihovimi ustreznimi konstrukcijami. Na kratko pojasnimo glavno idejo vsakega od njih.

Leta 1979 sta Adi Shamir [25] in George Blakley [5] uvedla izraz (t, n)-pražna shema, da bi opisala shemo, v kateri lahko vsak t od n deležev rekonstruira skrivnost X, vendar $t - 1$ ali manj deležev ne razkrijejo nobenih informacij o X. Pri konstrukciji te sheme je skrivni X na fiksni premici l in trgovec izbere hiperravnino $\mathbf{H}$ tako, da gre $\mathbf{H}$ skozi X, $l \in \mathbf{H}$, in $\mathbf{H}$ vsebuje niz točk $\mathbf{T}$ v splošnem položaju, ki vsebuje X, kjer se točke, ki se razlikujejo od X, upoštevajo kot deleži [2].

V shemi predelkov so uporabniki razdeljeni na ločene dele, imenovane predelki, z enakimi pravicami. Za sodelovanje pri rekonstrukciji skrivnosti potrebuje vsak oddelek določen kvorum, to je minimalno število uporabnikov. Poleg tega mora obstajati tudi določeno število predelkov [2]. Če predelke označimo z $\mathcal{G}_1, \mathcal{G}_2, \ldots, \mathcal{G}_n$, je struktura dostopa sestavljena iz naslednjih zahtev:

- za vsak predelek sta potrebna vsaj dva uporabnika, ki omogočata sodelovanje tega predelka pri rekonstrukciji skrivnosti,
- za rekonstrukcijo skrivnosti sta dovolj vsaj dva zgoraj opisana predelka.

Uporabljamo sheme za skupno rabo skrivnosti na več ravneh, kadar je treba zaveze razdeliti skupini udeležencev in ne enemu posamezniku. Zanimajo nas najpogosteje uporabljene večnivojske sheme, znane kot 2-nivojske sheme delitve ali večnivojske $(2, s)$-sheme. Obstajata dve različni podskupini udeležencev, označeni s $\mathbf{T}$ in $\mathbf{S}$. Hierarhično so udeleženci podskupine $\mathbf{T}$ na višji ravni, kot udeleženci podskupine $\mathbf{S}$. Skrivnost je mogoče rekonstruirati, če ozvezdje udeležencev sestavljajo:

- kateri koli niz vsaj dveh udeležencev iz $\mathbf{T}$,
- kateri koli niz vsaj s udeležencev iz $\mathbf{S}$,
- vsak udeleženec iz $\mathbf{T}$ in vsaj $s-1$ udeleženec iz $\mathbf{S}$.

Pojem večnivojskih $(2, s)$-shem nas popelje v svet afino pravilnih poligonov in projektivnih k-lokov. Simmons [23, 27] je predlagal geometrijski model ostro fokusiranega loka za načrtovanje učinkovite sheme delitve skrivnosti z uporabo k-lokov $\mathrm{PG}(2, q)$, pri čemer je q dovolj velik [13]. Če je κ k-lok in je l zunanja premica na κ, pravimo, da je κ zelo ostro fokusirana ali hiperfokusirana na l, ko sekante κ pokrivajo natančno $k-1$ točk na l in je κ ostro fokusirana na l, če njene sekante pokrivajo natančno k točk od l. Bichara in Korchmáros [4] sta ugotovila, da če obstaja zelo ostro fokusiran ali hiperfokusiran k-lok s $k > 2$ v $\mathrm{PG}(2, q)$, mora biti q sod. Po drugi strani pa ostro fokusirani loki obstajajo za sodo in liho q. Uvedemo zasnove afinih pravilnih poligonov in posplošenih afinih pravilnih poligonov za opis ostro fokusiranih in hiperfokusiranih množic. Na splošno je najpomembnejša lastnost afine ravnine ta, da so njeni izreki še vedno pomembni po uporabi afine preobrazbe ali podobnosti. Ohranjajo razmerja, vzporedne črte itd. Tukaj je na voljo veliko lepih lastnosti in izrekov. Kiss in Szőnyi sta v knjigi [13] uporabila sledečo definicijo. Če je $\mathcal{A}$ afina ravnina z n točkami $P_0, P_1, \ldots, P_{n-1}$, poimenujemo zaporedje $P_0P_1 \ldots P_{n-1}$ afino pravilen mnogokotnik, če obstaja bijektivna preslikava ϕ, ki slika vse P_i z $i \in \{0, 1, \ldots, n-1\}$ v množico oglišč pravilnega n-kotnika v klasični evklidski ravnini tako, da je P_iP_j vzporeden s P_kP_l v afini ravnini $\mathcal{A}$, če in samo če je $\phi(P_i)\phi(P_j)$ vzporeden z $\phi(P_k)\phi(P_l)$ v klasični evklidski ravnini.

Korchmáros [15] je pokazal, da afino pravilni n-kotnik v $\mathcal{A} = \mathrm{AG}(2, q)$, koordiniran z $GF(q)$, $q = p^k$, obstaja, če in samo če je $n \mid (q+1)$ in n-kotnik je vpisan v elipso ali $n \mid (q-1)$ in je n-kotnik vpisan v hiperbolo ali pa je $n = p$ in je n-kotnik vpisan v parabolo. V nadaljevanju se vrnemo k množicam $\mathbf{S}$ in $\mathbf{T}$, pri čemer razpravo najprej omejimo na projektivno ravnino. V tem primeru je nujen pogoj $|\mathbf{S} \cup \mathbf{T}| \leq q+2$. V vseh drugih primerih potrebujemo tudi nekaj dodatnih predpostavk glede moči množice $\mathbf{S}$, paritete števil q, $\mathbf{S}$, predposvke, da je $\mathbf{S}$ podlok štožnice in tako dalja (glej [3]). V splošnem primeru, tj. ko je $n \geq 2$, in je l premica in v $\mathrm{PG}(n, q)$, potem zahtevamo naslednje pogoje na množici $\mathbf{S}$ in $\mathbf{T}$: $\mathbf{T} \in l$, $X \in \mathbf{T}$ in $|\mathbf{T}| > 2$, $|\mathbf{S}| > n$, $\mathbf{S} \cap \mathbf{T} = \emptyset$, noben podprostor, ki ga generirajo točke $\mathbf{S}$, ne vsebuje več točk $\mathbf{S} \cup \mathbf{T}$ in $\mathbf{S} \in \mathcal{G}_n$, kjer je $\mathcal{G}_i = \{(1, t, \ldots, t_{n-1}, t_n) \mid t \in GF(q)^+\}$; $GF(q)^+$ označuje $GF(q) \cup \infty$. Končno konstruiramo nekaj množic $\mathbf{S}$ in $\mathbf{T}$, ki izpolnjujejo te pogoje, z uporabo skupine avtomorfizmov, ki določa $\mathcal{G}_i$, pri čemer se večinoma opiramo na članek [3].

7 REFERENCES

[1] R. Artzy and Gy. Kiss, Shape-regular polygons in finite planes. *J Geom.* 57 (1996) 20–26. *(Cited on pages 37 in 38.)*

[2] A. Beutelspacher and U. Rosenbaum, *Projective Geometry: From Foundations to Applications*. Cambridge University Press, 1998. *(Cited on pages 11, 12, 15, 17, 20, 52, 53 in 54.)*

[3] A. Beutelspacher and F. Wettl, On 2-level secret sharing. *Des Codes Crypt.* 3 (1993) 127–134. *(Cited on pages 10, 41, 47, 49, 51 in 55.)*

[4] A. Bichara and G. Korchmáros, Note on $(q+2)$-sets in Galois plane of order q. *Annals of Discrete Math.* 14 (1982) 117–122. *(Cited on pages 23 in 54.)*

[5] G.R. Blakley, Safeguarding cryptographic keys. *In Proceedings of the nationalcomputer conference* 48 (1979) 313–317. *(Cited on pages 13, 14 in 53.)*

[6] A. Blokhius, A.A. Bruen and J.A. Thas, Arc in PG(n, q), MDS-codes and three fundamental probles of B. Segre - some extensions. *Geom. Dedicate* 35 (1990) 1–11. *(Cited on page 45.)*

[7] R.M. Campello de Souza, H.M. de Olivera and D. Silva, The Z Transform over Finite Fields. *nternational Telecommunications Symposium* Natal, Brazil (2002) . *(Not cited.)*

[8] S. Caputo, G. Korchmáros and A. Sonnino, Multilevel secret sharing schemes arising from the normal rational curve. *Discrete Applied Mathematics* 284 (2020) 158–165. *(Not cited.)*

[9] H. S. M. Coxeter, Affinely regular polygons. *Abh. Math. Sem. Univ. Hamburg* 34 (1970) 38–58. *(Cited on page 26.)*

[10] J.C. Fisher, *A classification of Pappian affinities*, Ph.D. Thesis, University of Toronto, 1972. *(Not cited.)*

[11] G.C. Fisher and E.R. Jamison, Properties of affinely regular polygons. *Geom. Dedicata.* 69 (1998) 241–259. *(Cited on page 26.)*

[12] C. Huck, A note on affinely regular polygons. *European Journal of Combinatorics* 30 (2009) 387–395. *(Not cited.)*

[13] Gy. Kiss and T. Szőnyi, *Finite Geometries*. Chapman and Hall/CRC, 2019. *(Cited on pages 5, 6, 25, 27, 32, 46 in 54.)*

[14] A. Klein and L. Storme, Applications of finite geometry in coding theory and cryptography. *Comp. Sci., Math* 29 (2011) 38–58. *(Cited on page 15.)*

[15] G. Korchmáros, Poligoni affin-regolari dei piani di Galois d'ordine dispari. *Atti Aacad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur* 56 (1974) 690–697. *(Cited on pages 26, 27 in 55.)*

[16] G. Korchmáros, V. Lanzone and A. Sonnino, Projective k-arcs and 2-level secret sharing schemes. *Des. Codes Crytogr.* 64 (2012) 3–15. *(Not cited.)*

[17] Z. Lángi, A characterization of affinely regular polygons. *Aequat. Math.* 92 (2018) 1037–1049. *(Not cited.)*

[18] P. Ligeti, P. Sziklai and A. Takáts, Generalized treshold secret sharing and finite geometry. *Des. Codes Crytogr.* 89 (2021) 2067–2078. *(Cited on pages 12 in 14.)*

[19] G. Nicollier, A characterization of affinely regular polygons. *Beitr Algebra Geom* 57 (2016) 453–458. *(Not cited.)*

[20] N. Nizette, Les polygones réguliers des plas affins arguésiens. *Acad. Roy. Belg. Bull. Cl. Sci.* 63 (1977) 844–851. *(Cited on page 26.)*

[21] C.M. O'keefe, Applications of Finite Geometries to Information Security. *Australasian J. Combinatorics* 7 (1993) 195–212. *(Cited on pages 11, 13 in 53.)*

[22] J.S. Rose, *A Course on Group Theory*, Dover Publications, 1994. *(Not cited.)*

[23] G.J. Simmons, How to (really) share a secret. *Advances in Cryptology - CRYPTO 88, LNCS* 403 (1989) 390–448. *(Cited on pages 23 in 54.)*

[24] G.J. Simmons, Sharply focused sets of lines on a conic in $\mathrm{PG}(2, q)$. *Congressus Numerantium* 73 (1990) 181–204. *(Cited on page 23.)*

[25] A. Shamir, How to share a secret. *Commun ACM* 22 (1979) 612–613. *(Cited on pages 13, 14 in 53.)*

[26] L. Storme, Small arcs in projective spaces. *J Geom* 58 (1997) 179-191. *(Not cited.)*

[27] T. Szőnyi, k-sets in PG$(2, q)$ having a large set of internal nuclei. *Combinatorics 88* 2 (1991) 449–458. *(Cited on page 54.)*

[28] F. Wettl, On the nuclei of a pointset of a finite projective plane. *J. of Geometry* 30 (1987) 157–163. *(Cited on pages 41, 43 in 44.)*

[29] *Complex Numbers in Geometry*,
`https://brilliant.org/wiki/complex-numbers-in-geometry/`.
(Datum ogleda: 10. 8. 2022.) *(Not cited.)*

[30] *Finite Field*,
`https://mathworld.wolfram.com/FiniteField.html`.
(Datum ogleda: 25. 7. 2022.) *(Not cited.)*

[31] *Geometrikon; Affine transformations of the plane (Affinities)*,
`http://users.math.uoc.gr/ pamfilos/eGallery/Gallery.html`.
(Datum ogleda: 23. 5. 2022.) *(Cited on page 24.)*

[32] *Trigonometry in Galois fields*,
`https://en-academic.com/dic.nsf/enwiki/3118936`.
(Datum ogleda: 15. 7. 2022.) *(Not cited.)*

Appendices

APPENDIX A Complex numbers and Euclidean plane

Definition A.1. We define a set of *complex number* as $\mathbb{C} = \{z|\ z = a + bi,\ a, b \in \mathbb{R}\}$, where a is a *real* part and b represents an *imaginary* part. We call i an *imaginary unit* satisfying $i^2 = -1$. The *magnitude* or absolute *value* of $z = a + bi$ is given by $|z| = \sqrt{a^2 + b^2}$. Furthermore, if $z = a + bi$, we define the *complex conjugate* $\overline{z}$ as $\overline{z} = a - bi$.

Every point in the complex plane is assigned a complex number, such that the point P with Cartesian coordinates (a, b) is assigned $a + bi$. The real and imaginary axes are the complex plane's equivalents to the xy-axes. Moreover, the representation $z = |z|(\cos\varphi + i\sin\varphi) = |z|e^{i\varphi}$ corresponds to Cartesian polar coordinates.

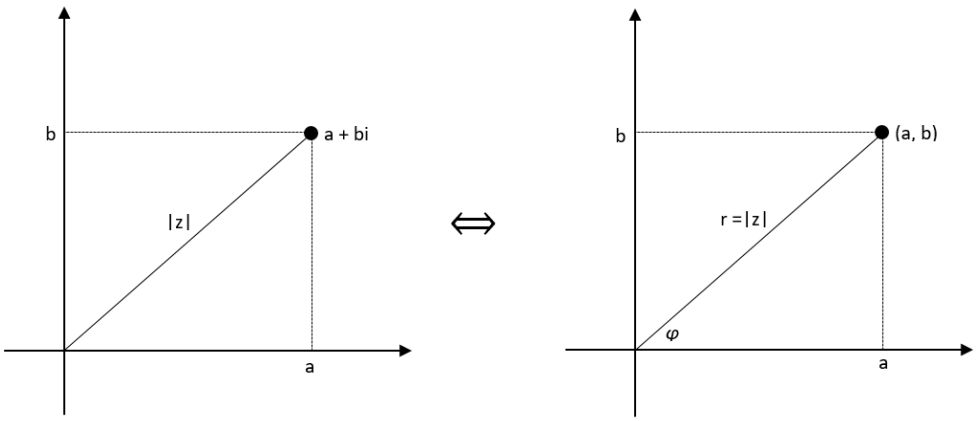

Figure 11: A complex number in the form of $a + bi$, whose point is (a, b) in rectangular form.

From the Figure 11, one can observe that

$$\sin\varphi = \frac{b}{r} \qquad \Rightarrow r\sin\varphi = b, \tag{A.1}$$

$$\cos\varphi = \frac{a}{r} \qquad \Rightarrow r\cos\varphi = a \tag{A.2}$$

Applying $(A.1)$ and $(A.2)$, we convert the complex number z from its recangular form to polar form as

$$\begin{aligned} z &= a + bi \\ &= (r\cos\varphi) + (r\sin\varphi)i \\ &= r\cos\varphi + ri\sin\varphi \\ &= r(\cos\varphi + i\sin\varphi). \end{aligned}$$

Lemma A.2 (Angle between two lines)**.** *Let ϕ be an angle, formed by the lines AB and CD (corresponding to z_1, z_2, z_3 and z_4 respectively) in the clockwise direction, i.e., $\phi = \angle(AB, CD)$. Then*

$$\frac{z_1 - z_2}{|z_1 - z_2|} = e^{i\varphi}\frac{z_3 - z_4}{|z_3 - z_4|}.$$

If we square both sides, the expression is equivalent to

$$\frac{z_1 - z_2}{\overline{z_1} - \overline{z_2}} = e^{2i\varphi}\frac{z_1 - z_2}{\overline{z_1} - \overline{z_2}}.$$

Corollary A.3. *We call points A, B and C (corresponding to z_1, z_2 and z_3 respectively) collinear if and only if*

$$\frac{z_1 - z_2}{\overline{z_1} - \overline{z_2}} = \frac{z_3 - z_2}{\overline{z_3} - \overline{z_2}}.$$

Lemma A.4. *If AB is a line passing through z_1 and z_2, its slope is determined by*

$$k_{AB} = \frac{z_2 - z_1}{\overline{z_2} - \overline{z_1}}.$$

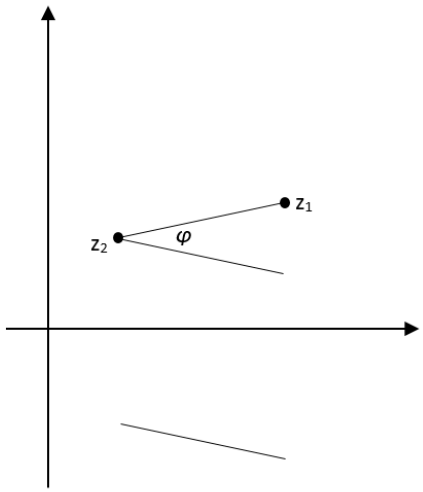

Figure 12: Determination of the slope.

We observed that $z_1 - z_2 = r(\cos\varphi + i\sin\varphi)$. Thus,

$$\begin{aligned}\frac{z_1 - z_2}{\overline{z_1} - \overline{z_2}} &= \frac{\cos\varphi + i\sin\varphi}{\cos\varphi - i\sin\varphi} \\ &= \frac{(\cos\varphi + i\sin\varphi)^2}{\cos^2\varphi + \sin^2\varphi} \\ &= \cos 2\varphi + i\sin 2\varphi.\end{aligned}$$