Construction and Classification of Geometrical Structures

Daniele Bartoli

Introduction

The topic of this thesis is the construction and the classification of geometrical structures in projective spaces over Galois fields, using both theoretical and computational tools. The main directions of our work have been the determination and the characterization of extremal examples, the investigation on the spectrum of sizes, the geometric classification as well as symmetry properties; we have also investigated relevant applications to Coding Theory.

Galois geometries are strongly connected to several branches of Mathematics, both classical (Number Theory, Algebraic Geometry in positive characteristic, Group Theory) and applied (Graph Theory, Coding Theory, Cryptography, Quantum Information Theory).

One of the first applications of Projective Geometry over Galois fieds was introduced by Bose ([30]), who showed that certain statistical problems of design of experiments can be attacked fruitfully by interpreting the statistical terms involved in terms of Finite Geometries. He referred to the class of these statistical problems as to the *packing problem* (see [97]). In geometrical terms, the packing problem concerns the determination of the maximum and minimum sizes of certain substructures of finite projective spaces (see [98]). In general, the full classification of geometrical structures in finite projective spaces are interesting both from a geometrical point of view and for a large class of problems in Coding Theory, Cryptography and Statistics that can be translated into equivalent geometrical problems (see [97] and [98]).

In this thesis applications to Coding Theory have received much attention.

In recent years not only the military world, but also the area of trade have required faster and faster transmission of digital informations. One of the main applications of geometrical structures is the construction of error correcting codes with good parameters: these codes are fundamental instruments to protect information against transmission errors. Among the geometrical objects relevant for applications, of particular interest are both arcs and $(n,3)$-arcs in $PG(2,q)$, which correspond to MDS and NMDS linear q-ary codes of dimension 3, respectively. These types of linear codes are the best in terms of minimum distance, among the linear codes with the same length and dimension. In general (n,k)-arcs in $PG(2,q)$ correspond to linear q-ary codes with Singleton defect equal to $k-2$. Caps of size n in $PG(k-1,q)$ correspond to $[n,n-k,4]_q$ linear codes. It should also be remarked that the classification of $(n,3)$-arcs serves as basis for search for NMDS codes of higher dimension using an extension process. One of the main achievements of the present thesis is the solution of the packing problem for $(n,3)$-arcs in $PG(2,16)$. We obtained that the maximum size of an $(n,3)$-arc is 28 and that the minimum size of a complete $(n,3)$-arc is 15. Moreover we determined the spectrum of sizes of complete caps in $PG(3,7)$ and found many examples of small complete arcs in $PG(2,q)$, where q is a prime-power, $q \leq 9109$.

A natural method for constructing (n,k)-arcs in $PG(2,q)$ is that of considering the set of $\mathbb{F}_q$-rational points of an irreducible plane algebraic curve of degree k defined over $\mathbb{F}_q$. More generally, not necessarily plane algebraic curves over finite fields with many rational points with respect to their genus can be used to construct linear codes, which in many cases turn out to have better parameters than those of generic linear codes. Curves with many automorphisms have received a great deal of attention: on one hand these curves have a large number of rational points, and on the other hand the decoding process of the corresponding linear code can be sped up by using algorithms like the permutation decoding. Our main result in this context is that a projective, non-singular, algebraic plane curve of genus $g \geq 2$

defined over an algebraically closed field $\mathbb{K}$ of positive characteristic $p > 2$ having many automorphisms is birationally equivalent to the Hermitian curve.

A class of codes associated to algebraic varieties over finite fields is that of functional codes, which can be viewed as generalizations of Reed-Muller codes. In this thesis we establish a lower bound for the minimum distance of the functional code $\mathcal{C}_{Herm}(\mathcal{Q})$, studying the maximum size of the intersection of an arbitrary Hermitian variety with a fixed quadric $\mathcal{Q}$.

A linear code can be useful not only for error correction, but also for *covering* vector spaces over finite fields with a small number of Hamming spheres. When a linear code is used for this purposes, then it is normally called a *covering code*.

Covering codes can be applied to many branches of Combinatorics and Information Theory, such as data compression and steganography (see [25]). The geometrical equivalent of a covering code is a saturating set in a finite projective space. Our main results in this context are the classification of the minimal 1-saturating sets in $PG(2, 9)$ and $PG(2, 11)$, and the determination and classification of the minimal 1-saturating sets of smallest size for $16 \leq q \leq 23$. It should be remarked that small saturating sets in spaces of smaller dimension are of particular interest, as they can be used as a base in inductive constructions of covering codes with higher redundancy but similar covering density (see [46]).

It is interesting to note that if $k+t = q+1$, then (n, k)-arcs and t-fold blocking sets are complements of each other in a projective plane. This means that the classification of 1-fold blocking sets is equivalent the classification of (n, q)-arcs. Blocking sets are also important tools for the determination of maximal partial spreads, i.e. sets of skew lines such that each line of the space meets at least one line of the set. We classified the minimal blocking sets in $PG(2, 7)$ and give partial classifications in $PG(2, 8)$, $PG(2, 9)$ and $PG(2, 11)$.

One of the most promising areas of Coding Theory is that of *quantum codes*. Quantum error correcting

codes are related with Quantum Information and Quantum Computing. In the implementation of long quantum computations, there are several major sources of errors: decoherence, dissipation, measurement errors, depolarization errors of spin and phase flips, etc. Therefore error correction is indispensable in quantum computing, even more so than in classical computing. The setting in which quantum error correcting codes exist is $\mathbb{H}^{2^n} = \mathbb{H}^2 \otimes \ldots \otimes \mathbb{H}^2$, where $\mathbb{H}$ is an Hilbert space. An encoding of k qubits into n is a linear mapping $\Psi : \mathbb{H}^{2^k} \to \mathbb{H}^{2^n}$. We usually call $\Psi(\mathbb{H}^{2^k})$ itself the quantum error correcting code, since the error correction properties depend only on the subspace rather than on the mapping. Recently (see [35]) the problem of finding a particular type of quantum error correcting codes has been translated in geometrical way (determining additive codes over $GF(4)$ which are self-orthogonal with respect to a particular trace inner product). We investigated pure $[[n, n-10, 4]]$ quantum codes through their correspondence to *quantum n-caps* in $PG(4, 4)$, i.e. caps having hyperplane intersection of size of the same parity of n (see [6] and [7]); we determined the spectrum of quantum caps and classified the caps of some extremal sizes. These examples have been the starting point for the definition of theoretical recursive constructions for quantum caps in higher dimensions.

The thesis is organized as follows.

In Chapter 1 it is proven that if $\mathcal{X}$ is a curve over an algebraic close field of positive characteristic $p > 2$ admitting a non-singular plane model having more than $3(2g2 + g)(\sqrt{8g+1} + 3)$ automorphisms, then $\mathcal{X}$ is birationally equivalent to a Hermitian curve. The theoretical techniques involved are principally the Stöhr-Voloch theory and some results from finite Group Theory. The bound improves the result by Henn [90] for the class of non-singular plane curves.

In Chapter 2 some particular functional codes are investigated. Let $\mathcal{X} = \{P_1, \ldots, P_n\} \subset PG(N, q)$ be the set of $\mathbb{F}_q$-rational points of a fixed algebraic variety defined over $\mathbb{F}_q$. The functional code $\mathcal{C}_h(\mathcal{X})$ is defined as $\{(f(P_1), \ldots, f(P_n)) | f \in \mathcal{F}_h\} \cup \{0\}$, where $\mathcal{F}_h$ is the set of the homogeneous polynomials

of degree h over the finite field $\mathbb{F}_q$. In this work we deal with the case in where $\mathcal{X}$ consists of the point of a non-singular quadric $\mathcal{Q}$, and f ranges over the subspace of $\mathcal{F}_h$ consisting of polynomials associated to Hermitian varieties. In this case the functional code is denoted as $\mathcal{C}_{Herm}(\mathcal{Q})$. The small weight codewords of $\mathcal{C}_{Herm}(\mathcal{Q})$ have been investigated. Codewords of small weight arise from Hermitian varieties having big intersection with the fixed non singular quadric $\mathcal{Q}$, and our result here is that the minimum distance of the code $\mathcal{C}_{Herm}(\mathcal{Q}(N, q2))$ is at least $|\mathcal{Q}(N, q2)| - \overline{W}_N$, with $\overline{W}_N$ approximately $q^{2N-3} + q^{2N-4} + 4q^{2N-5} - 2q^{2N-8}$.

In the subsequent chapters both theoretical and computational tools are used to construct and classify different geometrical structures.

In Chapter 3 a brief introduction to the main ideas used in our computer searches is given. The back-tracking algorithm which exploits projective equivalence properties to prune the search space used for the exhaustive searches is described. Then it is presented the randomized greedy algorithm used to find extremal examples when exhaustive searches are not feasible.

In Chapter 4 these techniques are applied in order to determine the spectrum of quantum caps in $PG(4, 4)$. As a byproduct of our search, it is proven that no quantum 37 and 39-caps exist, along with the uniqueness of the quantum 38-cap in $PG(4, 4)$. Finally some recursive constructions of quantum caps are presented.

In Chapter 5 some constructions of complete arcs of small size in $PG(2, q)$ are given. Moreover, with the help of computational tools, new lower bounds for complete arcs in $PG(2, q)$ are determined for $q < 9109$.

The main topic of Chapter 6 is the determination of the maximum and the minimum size of complete $(n, 3)$-arcs in $PG(2, 16)$. To do this, in order to reduce the execution time and make the search possible, some improvements have been done, involving both algorithmic and geometrical ideas. It has been

determined that the maximum size is 28 and the minimum size is 15.

In Chapter 7 the problem of determining the spectrum of complete caps in $PG(3,7)$ is solved, verifying that no compete 31-cap exists. As a byproduct of our search the uniqueness of the complete 32-cap in $PG(3,7)$ is proven.

The object of Chapter 8 is the determination of minimal 1-saturating sets in projective planes. In particular, the complete classification of minimal 1-saturating sets in $PG(2,9)$ and $PG(2,11)$, and the classification of the examples of minimum size in $PG(2,q)$ with $16 \leq q \leq 23$ are given.

In Chapter 9 the complete classification of blocking sets in $PG(2,q)$, with $q \leq 7$, and a partial classification in $PG(2,8)$ and $PG(2,9)$ are given. All the minimal blocking sets of Rédey type in $PG(2,q)$, $q \leq 11$, are determined.

Chapter 1

On the size of the automorphism group of a plane algebraic curve in positive characteristic

1.1 Introduction

In this chapter, $\mathbb{K}$ denotes an algebraically closed field of positive characteristic p. Let $\mathrm{Aut}(\mathcal{X})$ be the $\mathbb{K}$-automorphism group of a projective, non-singular, geometrically irreducible, algebraic curve $\mathcal{X}$ of genus $g \geq 2$. It is well known that $\mathrm{Aut}(\mathcal{X})$ is finite and that the classical Hurwitz bound $|\mathrm{Aut}(\mathcal{X})| \leq 84(g-1)$ holds provided that $p \nmid |\mathrm{Aut}(\mathcal{X})|$. If p divides $|\mathrm{Aut}(\mathcal{X})|$ then the curve $\mathcal{X}$ may happen to have much larger $\mathbb{K}$-automorphism group compared to its genus. This was first pointed out by Roquette [151]. Later on, Stichtenoth [164, 165] proved that if

$$|\mathrm{Aut}(\mathcal{X})| \geq 16g^4,$$

then $\mathcal{X}$ is birational equivalent to a Hermitian curve $\mathcal{H}(n)$, that is, to a non-singular plane curve with affine equation $Y^n + Y - X^{n+1} = 0$, for some $n = p^h \geq 3$. Here, $g = (n^2 - n)/2$, $\mathrm{Aut}(\mathcal{H}(n)) \cong \mathrm{PGU}_3(n)$, and $|\mathrm{Aut}(\mathcal{H}(n))| = n^3(n^3+1)(n^2-1)$.

The curves $\mathcal{X}$ with $|\mathrm{Aut}(\mathcal{X})| \geq 8g^3$ were classified by Henn [90]; see also [96, Theorem 11.127]. As a corollary of Henn's classification, if

$$|\mathrm{Aut}(\mathcal{X})| > 16g^3 + 24g^2 + g, \tag{1.1}$$

then $\mathcal{X}$ is birationally equivalent to a Hermitian curve. The main ingredients in the papers [164, 165, 90] are the Hurwitz genus formula and Hilbert's ramification theory.

The aim of this work is to improve the bound (1.1) in the case where $\mathcal{X}$ is a non-singular plane curve. Our main result is the following.

Theorem 1.1. *Let $\mathcal{X}$ be a projective, non-singular, algebraic plane curve of genus $g \geq 2$ defined over an algebraically closed field $\mathbb{K}$ of positive characteristic $p > 2$. Let G be an automorphism group of $\mathcal{X}$. Then either*

- *$\mathcal{X}$ is birationally equivalent to the Hermitian curve $\mathcal{H}(n)$ for some $n = p^h$, or*
- *$|G| \leq 3(2g^2 + g)(\sqrt{8g+1} + 3)$.*

Our proof also depends on Hilbert's ramification theory. A key result of independent interest valid for any non-singular plane curve $\mathcal{X}$ is that the higher ramification groups of G at any inflection point have a faithful action in the projective plane as elation groups preserving $\mathcal{X}$. This gives heavy restrictions on the possible structure of the higher ramification groups, and hence it allows us to obtain useful information on the p-subgrups of the one-point stabilizers of G. Our proof also uses the Stöhr-Voloch theory on Weierstrass points with respect to a base-point-free linear series [166], together with some deeper results on finite groups, such as the Kantor-O'Nan-Seitz theorem.

The chapter is organized as follows. In Section 2 we review some of the standard facts on automorphism groups of curves. We also briefly sketch the basics of Stöhr-Voloch theory and the theory of

central collineations of projective planes; moreover, we summarize without proofs the material on Group Theory that will be relevant to our proofs. Section 3 presents some preliminary results on the size of the automorphism group of a plane non-singular curve, and a characterization of higher ramification groups in terms of elations preserving the curve. The proof of Theorem 1.1 is the object of Section 4.

1.2 Background

Throughout this section, $\mathcal{X}$ is a projective, non-singular, geometrically irreducible, algebraic curve of genus $g \geq 2$ defined over an algebraically closed field $\mathbb{K}$ of positive characteristic p.

1.2.1 Automorphism groups of algebraic curves

For a finite subgroup G of $\mathrm{Aut}(\mathcal{X})$ let G^* denote the associated automorphism group of the function field $\mathbb{K}(\mathcal{X})$, namely $G^* = \{\phi^* \mid \phi \in G\}$, where $\phi^* : \mathbb{K}(\mathcal{X}) \to \mathbb{K}(\mathcal{X})$ is the pull-back of ϕ.

The subfield $\mathbb{K}(\mathcal{X})^{G^*}$ consisting of all elements of $\mathbb{K}(\mathcal{X})$ fixed by every element in G^*, also has transcendency degree one over $\mathbb{K}$. Let $\mathcal{Y}$ be a non-singular model of $\mathbb{K}(\mathcal{X})^{G^*}$, that is, a projective, non-singular, geometrically irreducible, algebraic curve with function field $\mathbb{K}(\mathcal{X})^{G^*}$. Then there exists a covering $\pi_G : \mathcal{X} \to \mathcal{Y}$ of degree $|G|$ such that $\pi_G^*(\mathbb{K}(\mathcal{Y}))$ coincides with $\mathbb{K}(\mathcal{X})^{G^*}$; also, two points $P, Q \in \mathcal{X}$ belong to the same orbit under G if and only if $\pi_G(P) = \pi_G(Q)$. Sometimes, $\mathcal{Y}$ is called the quotient curve of $\mathcal{X}$ by G and denoted by $\mathcal{X}/G$.

If P is a point of $\mathcal{X}$, the stabilizer G_P of P in G is the subgroup of G consisting of all elements fixing P. The orbit

$$\mathcal{O}_G(P) = \{Q \mid Q = \alpha(P),\, \alpha \in G\}$$

is *long* if $|\mathcal{O}_G(P)| = |G|$, otherwise $\mathcal{O}_G(P)$ is *short*.

For a non-negative integer i, the i-th ramification group of $\mathcal{X}$ at P is denoted by $G_P^{(i)}$ (or $G_i(P)$ as in [157, Chapter IV]) and defined to be

$$G_P^{(i)} = \{\alpha \mid \mathrm{ord}_P(\alpha^*(t) - t) \geq i + 1, \alpha \in G_P\},$$

where t is a uniformizing element (local parameter) at P. Here $G_P^{(0)} = G_P$ and $G_P^{(1)}$ is the unique Sylow p-subgroup of G_P. Moreover, $G_P^{(1)}$ has a cyclic complement H in G_P, that is,

$$G_P = G_P^{(1)} \rtimes H \tag{1.2}$$

with a cyclic group H of order coprime with p. Furthermore, for $i \geq 1$, $G_P^{(i)}$ is a normal subgroup of G_P and the factor group $G_P^{(i)}/G_P^{(i+1)}$ is an elementary abelian p-group. For i big enough, $G_P^{(i)}$ is trivial.

For any point Q of $\mathcal{X}$, let $e_Q = |G_Q|$ and

$$d_Q = \sum_{i \geq 0} (|G_Q^{(i)}| - 1).$$

Then $d_Q \geq e_Q - 1$ and equality holds if and only if $\gcd(p, |G_Q|) = 1$.

Let g' be the genus of the quotient curve $\mathcal{X}/G$. Hurwitz's Theorem states that

$$2g - 2 = |G|(2g' - 2) + \sum_{Q \in \mathcal{X}} d_Q. \tag{1.3}$$

Equation (1.3) is known as the Hurwitz genus formula. Assume that $G_P^{(1)}$ only ramifies at P. Then (1.3) applied to $G_P^{(1)}$ gives

$$2g - 2 = |G_P^{(1)}|(2g' - 2) + 2(|G_P^{(1)}| - 1) + \sum_{i \geq 2} (|G_P^{(i)}| - 1), \tag{1.4}$$

where g' denotes the genus of the quotient curve $\mathcal{X}/G_P^{(1)}$.

If G is tame, that is, $p \nmid |G|$, or more generally if $p \nmid e_Q$ for every $Q \in \mathcal{X}$, Equation (1.3) is simpler and may be written as

$$2g - 2 = |G|(2g' - 2) + \sum_{i=1}^{k}(|G| - \ell_i) \tag{1.5}$$

where $\ell_1, \ldots, \ell_k$ are the sizes of the short orbits of G on $\mathcal{X}$.

The following theorem summarizes some of the known upper bounds on the size of G related to the action of G on the set of points of $\mathcal{X}$.

Theorem 1.2. *Let r be the number of short orbits of $\mathcal{X}$ under the action of G, and let g' be the genus of the quotient curve $\mathcal{X}/G$. Let $Q_1, \ldots, Q_r$ be representatives from each short orbit, and let $d'_i = d_{Q_i}/e_{Q_i}$, so that*

$$2g - 2 = |G|(d'_1 + \ldots + d'_r + 2g' - 2) \geq |G|(d'_1 + \ldots + d'_r - 2). \tag{1.6}$$

Assume without loss of generality that $d'_i \leq d'_j$ for $i \leq j$.

(i) *If $g' > 0$, then $|G| \leq 4(g-1)$* [96, Theorem 11.56].

(ii) *$|G| \leq 84(g-1)$, with exceptions occurring only in the following cases* [96, Theorem 11.56]*:*

(iia) *$r = 1$ and the only short orbit is non-tame; here $|G| \leq 8g^3$* [96, Theorem 11.127]*;*

(iib) *$r = 2$ and both short orbits are non-tame; here $|G| \leq 16g^2$* [96, Theorem 11.127]*;*

(iic) *$r = 3$ with precisely one non-tame orbit; here $|G| \leq 24g^2$* [96, Theorem 11.127]*;*

(iid) *$r = 2$ and one short orbit is tame, one non-tame.*

(iii) *If $r \geq 5$, then $|G| \leq 4(g-1)$* [96, Theorem 11.56].

(iv) *If $G = G_P$ and p does not divide $|G|$, then $|G| \leq 4g + 2$* [164]; see also [96, Theorem 11.60].

Upper bounds on the size of $G_P^{(1)}$ are provided by the following result due to Stichtenoth [164, 165]; see also [96, Theorem 11.78].

Theorem 1.3. *Let $\mathcal{X}$ be a non-singular curve of genus $g > 1$ and let P be a point of $\mathcal{X}$. Let $\mathcal{X}_i$ be the quotient curve $\mathcal{X}/G_P^{(i)}$, and let g_i denote the genus of $\mathcal{X}_i$. Then one of the following holds:*

(i) *$g_1 > 0$ and $|G_P^{(1)}| \leq g$;*

(ii) *$g_1 = 0$, $G_P^{(1)}$ has a short orbit other than $\{P\}$, and $|G_P^{(1)}| \leq \frac{p}{p-1} g$;*

(iii) *$g_1 = g_2 = 0$, $\{P\}$ is the unique short orbit of $G_P^{(1)}$, and $|G_P^{(1)}| \leq \frac{4|G_P^{(2)}|}{(|G_P^{(2)}|-1)^2} g^2$.*

1.2.2 The Stöhr-Voloch theory

The idea to investigate the local properties of a non-singular algebraic curve $\mathcal{X}$ using the intersection numbers $I(P, \mathcal{X} \cap \Pi)$ of $\mathcal{X}$ with hyperplanes Π through $P \in \mathcal{X}$ was developed for complex curves in the early Nineteen century; see for instance [158, Section 25]. In [166] the authors extended the classical treatment to curves defined over a field of positive characteristic. The original motivation was to find an upper bound for the number of $\mathbb{F}_q$-rational points of an algebraic curve defined over a finite field of order q. Here we use some of their results on ramification divisors of non-singular plane algebraic curves.

Assume that $\mathcal{X}$ is a non-singular plane curve. For a point $P \in \mathcal{X}$, the order sequence of $\mathcal{X}$ at P is the strictly increasing sequence

$$j_0(P) = 0 < j_1(P) = 1 < j_2(P)$$

such that each $j_i(P)$ is the intersection number $I(P, \mathcal{X} \cap \ell_i)$ of $\mathcal{X}$ and some line ℓ_i at P, see [166], and [96, Chapter 7.6]. For $i = 2$, such a line ℓ_2 is uniquely determined being the tangent line $T_P(\mathcal{X})$ to $\mathcal{X}$

at P. A point P for which $j_2(P) > 2$ is a flex (or an inflection point) of $\mathcal{X}$. The order sequence is the same for all but a finite number of points.

Definition 1.4. The curve $\mathcal{X}$ is said to be classical if the generic order sequence is $(\epsilon_0, \epsilon_1, \epsilon_2) = (0, 1, 2)$.

Theorem 1.5 (Corollary 2.2 in [141])**.** *Assume that $p \geq 3$. If $\mathcal{X}$ is a non-classical curve of degree d, then $p|(d-1)$.*

The concept of order sequence can be given for any linear series. Let $\mathcal{D}$ be a base-point-free linear series with degree d and dimension r. Let $\pi : \mathcal{X} \to \mathrm{PG}(r, \mathbb{K})$, $\pi = (x_0 : x_1 : \ldots : x_r)$, be the morphism associated to $\mathcal{D}$. For a point P of $\mathcal{X}$, let γ_P be the branch of $\pi(\mathcal{X})$ corresponding to P via π. Then the $(\mathcal{D}, P)$-order sequence of $\mathcal{X}$ is the strictly increasing sequence

$$j_0^{\mathcal{D}}(P) = 0 < j_1^{\mathcal{D}}(P) < \ldots < j_r^{\mathcal{D}}(P)$$

such that each $j_i^{\mathcal{D}}(P)$ is the intersection number $I(\gamma_P, \mathcal{X} \cap \Pi_i)$ of $\mathcal{X}$ and some hyperplane Π_i at the branch γ_P. The $(\mathcal{D}, P)$-order sequence is the same, say $\epsilon_0^{\mathcal{D}} < \ldots < \epsilon_r^{\mathcal{D}}$, for all but finitely many points of $\mathcal{X}$. This constant sequence is the *$\mathcal{D}$-order sequence of $\mathcal{X}$*. The curve is *$\mathcal{D}$-classical* if $\epsilon_i^{\mathcal{D}} = i$ for each i. The *ramification divisor* $R^{\mathcal{D}}$ of $\mathcal{D}$ is

$$R^{\mathcal{D}} = \mathrm{div}(\det(D_\xi^{(\epsilon_i^{\mathcal{D}})} x_j)) + (\epsilon_0^{\mathcal{D}} + \ldots + \epsilon_r^{\mathcal{D}})\mathrm{div}(d\xi) + (r+1)\sum e_P P,$$

where $e_P = -\min\{ord_P(x_0), \ldots, ord_P(x_r)\}$ and $D_\xi^{(\epsilon_i^{\mathcal{D}})}$ is the $\epsilon_i^{\mathcal{D}}$-th Hasse derivative with respect to a separating element ξ of $\mathbb{K}(\mathcal{X})$. The support of $R^{\mathcal{D}}$ is the set of points of $\mathcal{X}$ whose $(\mathcal{D}, P)$-orders are different from $(\epsilon_0^{\mathcal{D}}, \ldots, \epsilon_r^{\mathcal{D}})$. Some of the properties of order sequences and ramification divisors are summarized in the following theorem. For a proof, see [166] or [96, Chapter 7].

Theorem 1.6. *Let $\mathcal{D}$ be a base-point-free linear series with degree d and dimension r. Then*

(i) $j_i^{\mathcal{D}}(P) \geq \epsilon_i^{\mathcal{D}}$ *for each* $P \in \mathcal{X}$ *and each* $i = 0, \ldots, r$*;*

(ii) *for each* $P \in \mathcal{X}$, $v_P(R^{\mathcal{D}}) \geq \sum_i (j_i^{\mathcal{D}}(P) - \epsilon_i^{\mathcal{D}})$*; equality holds if and only if* $\det(\binom{j_i^{\mathcal{D}}(P)}{\epsilon_j^{\mathcal{D}}}) \not\equiv 0 \pmod{p}$*;*

(iii) $\deg(R^{\mathcal{D}}) = (2g-2)\big(\sum_i \epsilon_i^{\mathcal{D}}\big) + (r+1)d$*;*

(iv) *if* $p \geq r$ *and* $\epsilon_i^{\mathcal{D}} = i$ *for each* $i = 0, 1, \ldots, r-1$*, then either* $\epsilon_r^{\mathcal{D}} = r$*, or* $\epsilon_r^{\mathcal{D}}$ *is a power of* p*.*

Definition 1.7. A projective irreducible plane curve $\mathcal{X}$ is said to be strange if there exists a point belonging to every tangent line at any non-singular point of $\mathcal{X}$.

Theorem 1.8 ([125])**.** *A non-singular projective irreducible plane curve* $\mathcal{X}$ *is strange if and only if* $\mathcal{X}$ *is a conic in characteristic* 2*.*

The following classification result due to Hefez [89] (see also [96, Theorem 7.72]) will be a key lemma for our Theorem 1.1.

Theorem 1.9. *Let* $\mathcal{X}$ *be a non-singular, non-strange plane curve of degree* $d > 3$*. If* $d = \epsilon_2 + 1$*, then* $\mathcal{X}$ *is projectively equivalent to the Hermitian curve.*

1.2.3 Central collineations

Some notions from Projective Geometry will play a role in the sequel.

A *collineation* of a projective space $\mathrm{PG}(r, \mathbb{K})$ is a bijective map from the point set and line set of $\mathrm{PG}(r, \mathbb{K})$ that preserves incidence. A collineation is *projective* if it is induced by a linear map of $\mathbb{K}^{r+1}$, that is, if it is an element of $\mathrm{PGL}_{r+1}(\mathbb{K})$, viewed as a permutation group acting on $\mathrm{PG}(r, \mathbb{K})$.

A collineation ϕ of $\mathrm{PG}(r, \mathbb{K})$, $r \geq 2$, is a *central* collineation if there is a hyperplane Π (the *axis* of ϕ) and a point C (the *center* of ϕ) such that every point of Π is a fixed point of ϕ and every line through C is a fixed line of ϕ.

If Π is a hyperplane of $\mathrm{PG}(r,\mathbb{K})$ and C, P, P' are distinct collinear points of $\mathrm{PG}(r,\mathbb{K})$ with P, P' not in Π, then there is precisely one central collineation of $\mathrm{PG}(r,\mathbb{K})$ with axis Π and center C mapping P to P'. In particular, axis and center of a non-identical central collineation are uniquely determined.

A non-identical central collineation ϕ is an *elation* if its center is incident with its axis, and a *homology* if center and axis are not incident (the identity is considered both as homology and elation).

A collineation of $\mathrm{PG}(r,\mathbb{K})$, $r \geq 2$, is an *axial* collineation if there is a hyperplane Π such that every point of Π is a fixed point of ϕ. Each axial collineation is central [17, Lemma 3.1.9]. Each central collineation is a projective collineation [17, Theorem 3.6.1].

Let $p > 0$ be the characteristic of $\mathbb{K}$. A projectivity of $\mathrm{PG}(2,\mathbb{K})$ of order a power of p fixing two distinct points P and R is an elation whose axis is the line through P and R.

1.2.4 Some results from Group Theory

From finite Group Theory, the following notions and results will play a role in the proofs. Given a group $\mathcal{G}$ and a subgroup S of $\mathcal{G}$, the normalizer of S in $\mathcal{G}$ will be denoted as $N_{\mathcal{G}}(S)$. As usual, $Z(\mathcal{G})$ will stand for the center of $\mathcal{G}$.

(i) The projective linear group $\mathcal{G} = \mathrm{PGL}_2(p^a)$ has order $p^a(p^a-1)(p^a+1)$. It is the automorphism group of $\mathrm{PG}(1,p^a)$; equivalently, $\mathcal{G}$ acts on the set Ω of size p^a+1 consisting of all $\mathbb{F}_{p^a}$-rational points of the projective line defined over $\mathbb{F}_{p^a}$. For every point $P \in \Omega$, the stabilizer $\mathcal{G}_P$ has size $p^a(p^a-1)$. The natural 2-transitive representation of $\mathrm{PSL}_2(p^a)$ is obtained when $\mathrm{PSL}_2(p^a)$ is viewed as a subgroup of $\mathrm{PGL}_2(p^a)$, see [103, Chapters II.7 and II.8] and [96, Appendix A, Example A.7]. For $p = 2$, $\mathrm{PGL}_2(p^a) = \mathrm{PSL}_2(p^a)$. For $p > 2$, $\mathrm{PSL}_2(p^a)$ has order $\frac{1}{2}p^a(p^a-1)(p^a+1)$. For $p^a \geq 4$, $\mathrm{PSL}_2(p^a)$ is a simple group and $\mathrm{PGL}_2(p^a)$ is a non-solvable group.

(ii) The projective unitary group $\mathcal{G} = \mathrm{PGU}_3(p^a)$ has order $(p^{3a}+1)p^{3a}(p^{2a}-1)$. It is the linear

collineation group in the projective plane $\mathrm{PG}(2, p^{2a})$ preserving the classical unital Ω of size $p^{3a}+1$ consisting of all absolute points of a non-degenerate unitary polarity of $\mathrm{PG}(2, p^{2a})$, see [101, Chapter II.8] and [96, Appendix A, Example A.9]. For every point $P \in \Omega$, the stabilizer $\mathcal{G}_P$ has size $p^{3a}(p^{2a}-1)$. Furthermore, $\mathcal{G}$ is the automorphism group of the Hermitian curve, regarded as a non-singular plane curve defined over the finite field with p^{2a} elements $\mathbb{F}_{p^{2a}}$, acting on the set Ω of all its $\mathbb{F}_{p^{2a}}$-rational points. The special projective unitary group $\mathrm{PSU}_3(p^a)$ either coincides with $\mathrm{PGU}_3(p^a)$ or is a subgroup of $\mathrm{PGU}_3(p^a)$ of index 3 according as $\mu = 1$ or $\mu = 3$ with $\mu = \gcd(3, p^a+1)$. In its action on Ω, $\mathrm{PSU}_3(p^a)$ is still 2-transitive and this is the natural 2-transitive representation of $\mathrm{PSU}_3(p^a)$, see [101, Chapter II.8] and [100]. For $p^a \geq 4$, $\mathrm{PSU}_3(p^a)$ is a simple group and $\mathrm{PGU}_3(p^a)$ is a non-solvable group.

(iii) The Suzuki group $\mathcal{G} = {}^2B_2(n)$ with $n = 2n_0^2$, $n_0 = 2^a$ and $a \geq 1$ has order $(n^2+1)n^2(n-1)$. It is the linear collineation group of $\mathrm{PG}(3, n)$ preserving the Tits ovoid Ω of size n^2+1 , see [104, Chapter XI.3] and [96, Appendix A, Example A.11]. For every point $P \in \Omega$, the stabilizer $\mathcal{G}_P$ has size $n^2(n-1)$. Furthermore, $\mathcal{G}$ is the automorphism group of the DLS curve, regarded as a non-singular curve defined over the finite field $\mathbb{F}_n$, acting on the set Ω of all its $\mathbb{F}_n$-rational points, see [82]. ${}^2B_2(n)$ is a simple group.

(iv) The Ree group $\mathcal{G} = {}^2G_2(n)$ with $n = 3n_0^2$, $n_0 = 3^a$ has order $(n^3+1)n^3(n-1)$. It is the linear collineation group of $\mathrm{PG}(6, n)$ preserving the Ree ovoid Ω of size n^3+1, see [104, Chapter XI.13] and [96, Appendix A, Example A.13]. For every point $P \in \Omega$, the stabilizer $\mathcal{G}_P$ has size $n^3(n-1)$. Furthermore, $\mathcal{G}$ is the automorphism group of the DLR curve, regarded as a non-singular curve defined over the finite field $\mathbb{F}_n$, acting on the set Ω of all its $\mathbb{F}_n$-rational points, see [87] and [34], For $n > 3$, ${}^2G_2(n)$ is simple, while ${}^2G_2(3) \cong \mathrm{P\Gamma L}_2(8)$.

For each of the above linear groups, the structure of the 1-point stabilizer and its action in the natural 2-transitive permutation representation, as well as its automorphism group, are explicitly given in the papers quoted.

The following classification results on finite groups with trivially intersecting Sylow p-subgroups will be used in the sequel.

Theorem 1.10 (Theorem 3.16 in [85]). *Let S be a Sylow p-subgroup of a finite group $\mathcal{G}$ with $S \subsetneq \mathcal{G}$. Set $I := N_{\mathcal{G}}(S)$ and $M := Z(I)$. Suppose that $p > 2$, and*

- *$I = SC$, with C cyclic;*
- *for $h \in \mathcal{G} \setminus I$, $S \cap h^{-1}Sh = \{id\}$.*

Then

- *M is a normal subgroup of $\mathcal{G}$;*
- *$\mathcal{G}/M$ has a unique minimal normal subgroup, which is non-abelian simple and isomorphic to one of the following groups: $PSL_2(p^a)$ with $a \geq 2$, $PSU_3(p^a)$ with $p^a > 2$, and for $p = 3$ the group ${}^2G_2(3^{2a+1})'$ with $a \geq 0$.*

In particular, $\mathcal{G}$ acts 2-transitively on the set of Sylow p-subgroups of $\mathcal{G}$.

Theorem 1.11 (The Kantor-O'Nan-Seitz Theorem [108]). *Let $\mathcal{G}$ be a finite 2-transitive permutation group whose 2-point stabilizer is cyclic. Then either $\mathcal{G}$ has an elementary abelian regular normal subgroup, or $\mathcal{G}$ is one of the following groups in their natural 2-transitive permutation representations: $PSL_2(p^a)$, $p^a \geq 4$, $\mathrm{PGL}_2(p^a)$, $p^a \geq 4$, $PSU_3(p^a)$ with $p^a > 2$, $PGU_3(p^a)$ with $p^a > 2$, the Suzuki group ${}^2B_2(n)$, ${}^2G_2(3^{2a+1})$ with $a \geq 0$.*

We end this section with a classical result on primitive permutation groups. For a proof, see e.g. [122, Corollary 2].

Lemma 1.12. *If $\mathcal{G}$ is a finite primitive permutation group, then $\mathcal{G}$ contains at most 2 minimal normal subgroup and if $\mathcal{G}$ has an abelian normal subgroup then it has a unique minimal normal subgroup.*

1.3 Preliminary results

From now on, $(x_0 : x_1 : x_2)$ are homogeneous coordinates for $\mathrm{PG}(2, \mathbb{K})$, with $\mathbb{K}$ an algebraically closed field with positive characteristic $p > 2$. We also let $x = x_1/x_0$ and $y = x_2/x_0$ be the corresponding non-homogeneous coordinates. Also, $\mathcal{X}$ denotes a projective, non-singular, geometrically irreducible, plane algebraic curve defined over $\mathbb{K}$ by the equation $F(x_0, x_1, x_2) = 0$, F being an irreducible polynomial of degree $d > 3$. Let $\mathbb{K}(\mathcal{X})$ be the function field of $\mathcal{X}$ and denote by $\bar{x}$ and $\bar{y}$ the rational functions associated to the non-homogeneous coordinates x and y, namely

$$\bar{x} = \frac{x_1 + (F)}{x_0 + (F)}, \qquad \bar{y} = \frac{x_2 + (F)}{x_0 + (F)}.$$

Let $g = (d-1)(d-2)/2$ be the genus of $\mathcal{X}$. Here and subsequently, G stands for an automorphism group of $\mathcal{X}$. By a result due to B. Segre [154], see also [96, Theorem 11.29], every $h \in G$ is the restriction of a projectivity of $\mathrm{PG}(2, \mathbb{K})$ preserving $\mathcal{X}$. Therefore, G can be viewed as a subgroup of $\mathrm{PGL}_3(\mathbb{K})$ fixing $\mathcal{X}$. For an element $h \in G$, we denote by h^* the pull-back of h, that is, the associated automorphism of the function field $\mathbb{K}(\mathcal{X})$. For a non-singular 3×3 matrix A over $\mathbb{K}$, denote by $\bar{A}$ the associated projectivity of $\mathrm{PGL}_3(\mathbb{K})$. Also, for $a, b, c \in \mathbb{K}$ let

$$A_{a,b,c} = \begin{pmatrix} 1 & 0 & 0 \\ b & 1 & 0 \\ c & a & 1 \end{pmatrix}.$$

The set of points of $\mathcal{X}$ for which $j_2(P)$ is larger than ϵ_2 will be denoted by W. Equivalently, W is the support of the ramification divisor $R^{\mathcal{D}}$ when $\mathcal{D}$ is the linear series cut out by the lines of $\mathrm{PG}(2,\mathbb{K})$. Finally, denote by ℓ_∞ the line with equation $x_0 = 0$, and set $X_\infty = (0:1:0)$, $Y_\infty = (0:0:1)$.

Proposition 1.13. *Let P be a point of $\mathcal{X}$ such that $I(P, \mathcal{X} \cap T_P(\mathcal{X})) = r > 2$. Then the group $G_P^{(2)}$ consists of elations with axis $T_P(\mathcal{X})$. If in addition*

- *$r = d$,*
- *G is a p-group such that $\{P\}$ is the only short orbit of G, and*
- *the genus g' of the quotient curve $\mathcal{X}/G$ is equal to 0,*

then either

$$|G_P^{(2)}| = d, \quad \text{or} \quad |G_P^{(2)}| = d - 1.$$

Proof. Assume without loss of generality that $P = Y_\infty$ and that $T_P(\mathcal{X}) = \ell_\infty$. To prove the first assertion we will show that $G_P^{(2)} \subseteq \{\bar{A}_{0,b,c} \mid b, c \in \mathbb{K}\}$. It is straightforward to check that any p-element in $\mathrm{PGL}_3(q)$ fixing both ℓ_∞ and Y_∞ is equal to $\bar{A}_{a,b,c}$ for some $a, b, c \in \mathbb{K}$. Note that $\bar{x}/\bar{y}$ is a local parameter of $\mathcal{X}$ at Y_∞. Also,

$$(\bar{A}_{a,b,c})^* \left(\frac{\bar{x}}{\bar{y}}\right) - \frac{\bar{x}}{\bar{y}} = \frac{b + \bar{x}}{c + a\bar{x} + \bar{y}} - \frac{\bar{x}}{\bar{y}} = \frac{b\bar{y} - c\bar{x} - a\bar{x}^2}{\bar{y}(c + a\bar{x} + \bar{y})} \, .$$

As $v_P(\bar{x}) = 1 - r$ and $v_P(\bar{y}) = -r$,

$$v_P\left((\bar{A}_{a,b,c})^* \left(\frac{\bar{x}}{\bar{y}}\right) - \frac{\bar{x}}{\bar{y}}\right) = \begin{cases} 2(1-r) - (-r-r) = 2, & \text{if } a \neq 0 \\ -r - (-r-r) = r, & \text{if } a = 0, b \neq 0 \\ 1 - r - (-r-r) = r+1, & \text{if } a = 0, b = 0 \end{cases} \tag{1.7}$$

Therefore, $\bar{A}_{a,b,c} \in G_P^{(2)}$ implies $a = 0$, and the first assertion is proved.

Assume now that G is a p-group fixing P, so that $G = G_P = G_P^{(1)}$. Suppose also that $r = d$ and that $\{P\}$ is the only short orbit of G; then by the Hurwitz genus formula

$$(d-1)(d-2) = \sum_{i=2}^{\infty}(|G_P^{(i)}| - 1). \tag{1.8}$$

By Equation (1.7) we have $G_P^{(2)} = G_P^{(3)} = \ldots = G_P^{(d-1)}$, and $G_P^{(i)} = \{id\}$ for every $i \geq d+1$. Now we prove that either $G_P^{(d)} = G_P^{(d-1)}$ or $G_P^{(d)} = \{id\}$. Assume on the contrary that there exist $\varphi_1 = A_{0,b_1,c_1} \in G_P^{(d-1)} \setminus G_P^{(d)}$ and $\varphi_2 = A_{0,0,c_2} \in G_P^{(d)} \setminus \{id\}$. Both φ_1 and φ_2 are elations with axis ℓ_∞. The center of φ_2 is P, whereas the center of φ_1 is $Q = (0 : b : c)$ with $b \neq 0$. Since $\mathcal{X}$ is non-strange, there exist lines ℓ_1 through Q and ℓ_2 through P having exactly d and $d-1$ intersection points of $\mathcal{X} \setminus \{P\}$, respectively. As for $i = 1, 2$, the elation φ_i has order p and fixes the point set $(\mathcal{X} \setminus \{P\}) \cap \ell_i$, we have that $p|d$ and $p|(d-1)$, which is a contradiction. Hence, either $G_P^{(d)} = G_P^{(d-1)}$ or $G_P^{(d)} = \{id\}$. Then by Equation (1.8), either $|G_P^{(2)}| = d-1$ or $|G_P^{(2)}| = d$, according to whether $G_P^{(d)} = G_P^{(d-1)}$ or $G_P^{(d)} = \{id\}$. □

Lemma 1.14. *Let $\mathcal{X}$ be a non-singular curve of genus $g > 1$ and let P be a point of $\mathcal{X}$. If the genus g' of the quotient curve $\mathcal{X}/G_P^{(1)}$ is positive, then*

$$|G_P| \leq 6g.$$

Proof. By (1.2), together with Theorem 1.2(iv), $G_P = G_P^{(1)} \rtimes H$ with a cyclic group H of order coprime with p and not greater than $4g+2$. Then H is isomorphic to the factor group $G/G_P^{(1)}$, which is an automorphism group of $\mathcal{X}/G_P^{(1)}$ fixing the point of $\mathcal{X}/G_P^{(1)}$ lying under P. As $g' \geq 1$, the size of H is at most $4g'+2$; this follows from Theorem 1.2(iv) for $g' \geq 2$, and from [96, Theorem 11.94] for $g' = 1$. Also, by (1.3) for $G_P^{(1)}$ we have $|G_P^{(1)}| \leq g/g'$. Then,

$$|G_P| = |G_P^{(1)}||H| \leq \frac{g}{g'}(4g'+2) \leq 4g + 2\frac{g}{g'} \leq 6g.$$

□

Lemma 1.15. *Let P be a point of W. If $|G_P| \leq 6g$, then $|G| \leq (12g^2 + 6g)d$.*

Proof. Taking into account that $\epsilon_1 = 1$ and $\epsilon_2 < d$, by Theorem 1.6(iii) it follows that the size of W is at most $(2g-2)d + 3d$. By the orbit stabilizer theorem we obtain

$$|G| = |G_P||W| \leq 6g(2g+1)d.$$

□

Lemma 1.16. *Let P be a point of W. Suppose that for some $\varphi \in G_P^{(1)}$, $\varphi \neq id$, there exists $Q \in W \setminus \{P\}$ with $\alpha(Q) = Q$. Let Δ be an orbit under G_P, such that $\Delta \neq \{P\}$ and $\Delta \neq \mathcal{O}_{G_P}(Q)$.*

(i) *If Δ is either a long or a short tame orbit under G_P, then*

$$|G_P| \leq (2g-2) + |\Delta|.$$

(ii) *If Δ is a non-tame orbit under G_P, then*

$$|G_P| \leq 2g - 2.$$

Proof. (i) If Δ is a long orbit under G_P, then $|G_P| = |\Delta|$ and the assertion holds. Assume then that Δ is a short orbit. Therefore, we have at least three short orbits under G_P, two of which are non-tame. By Equation (1.6) for G_P, we have

$$2g - 2 \geq |G_P|\Big(\frac{|G_{P,R}| - 1}{|G_{P,R}|}\Big),$$

with R being any point of Δ. From $|G_{P,R}| = |G_P|/|\Delta|$, we obtain

$$|G_P|\Big(\frac{|G_{P,R}| - 1}{|G_{P,R}|}\Big) = |G_P| - |\Delta|,$$

whence the assertion.

(ii) In this case there are three different non-tame orbits under G_P. The assertion then follows from Equation (1.6) for G_P. □

Lemma 1.17. *Assume that $G_P^{(1)}$ is non-trivial. If G_P has at least three short tame orbits, then $|G_P| \leq 4(g-1)$.*

Proof. By Theorem 1.2, we can assume that the genus of the quotient curve $\mathcal{X}/G_P$ is equal to 0. Let r be the number of short orbits of G. If $r \geq 5$, then the assertion follows by Theorem 1.2. Then $r = 4$ and Equation (1.6) reads

$$2g - 2 = |G_P|(d_1' + d_2' + d_3' + d_4' - 2),$$

with $d_4' \geq 1$ and $d_1' + d_2' + d_3' \geq 3/2$. This implies $|G_P| \leq 4(g-1)$. □

Lemma 1.18. *Assume that $G_P^{(1)}$ is non-trivial, and that G_P has precisely 2 short tame orbits on $\mathcal{X}$, say Δ_1 and Δ_2, with $|\Delta_1| \geq |\Delta_2|$. Then $|G_P| \leq \max\{6(g-1), 2|\Delta_1|\}$.*

Proof. By Theorem 1.2, we can assume that the genus of the quotient curve $\mathcal{X}/G_P$ is equal to 0. Then Equation (1.6) for G_P reads

$$2g - 2 = |G_P|(d_1' + d_2' + d_3' - 2),$$

with $d_3' \geq 1$ and $d_2' \geq d_1' \geq 1/2$. If $d_1' = 1/2$, then the stabilizer in G_P of a point $Q \in \Delta_1$ has size 2; that is, $G_P = 2|\Delta_1|$. On the other hand, if $d_1' \geq 2/3$, then $d_1' + d_2' + d_3' \geq 7/3$, whence $|G_P| \leq 6(g-1)$. □

In the rest of the work, the following conditions will be considered.

(C1) W is the only non-tame orbit of G;

(C2) the size of W is greater than 1;

(C3) every p-element of G fixes precisely one point of W;

(C4) for each point P in W, the size of $G_P^{(2)}$ is equal to $d-1$.

Lemma 1.19. *Assume that both conditions* (C1) *and* (C3) *holds. Then each Sylow p-subgroup of G coincides with $G_R^{(1)}$ for some point R in W. In particular, any two distinct Sylow p-subgroups of G intersect trivially.*

Proof. Let S be a p-Sylow subgroup of G. Let h be a central element in S of order p. Then by (C3) there exists $R \in W$ such that $h(R) = R$. For any $s \in S$, $s(R) = sh(R) = hs(R)$ holds; i.e. h fixes $s(R)$ as well. By (C3), $s(R) = R$ and therefore $s \in G_R$. This proves that $S = G_R^{(1)}$. □

Lemma 1.20. *Assume that both conditions* (C1) *and* (C3) *holds. Then $N_G(G_P^{(1)}) = G_P$.*

Proof. As in general $G_P^{(1)} \lhd G_P$, we only need to show that any $s \in G$ such that $sG_P^{(1)}s^{-1} \subseteq G_P^{(1)}$ belongs to G_P. From $sG_P^{(1)}s^{-1} \subseteq G_P^{(1)}$ it follows that $sh = h's$ for some $h, h' \in G_P^{(1)}$. Therefore, $s(P) = sh(P) = h's(P)$ holds. By (C3) applied to h' we get $s(P) = P$, that is, $s \in G_P$. □

Lemma 1.21. *Assume that conditions* (C1), (C2), (C3) *and* (C4) *hold. Suppose in addition that $|W| > d$, $G_P^{(1)}$ is not cyclic, $I(P, \mathcal{X} \cap T_P(\mathcal{X})) = d$, and that the genus of $\mathcal{X}/G_P^{(1)}$ is equal to* 0*. Then*

(i) *the action of G on W is faithful;*

(ii) *G satisfies all the assumptions of Theorem* 1.10 *with $M = \{id\}$; in particular, G acts* 2*-transitively on W;*

(iii) *either $G_P^{(1)}$ is abelian, or $Z(G_P^{(1)}) = G_P^{(2)}$.*

Proof. (i) We show that W contains 4 points, no three of which collinear; this is enough to ensure that no non-trivial element in G fixes W pointwise. Let $R \in W \setminus \{P\}$, and let ℓ be the line passing through P and R. By the proof of Proposition 1.13, condition (C4) implies that $G_P^{(2)}$ consists of elations with center P. Therefore, $G_P^{(2)}$ acts on $\mathcal{X} \cap \ell$; i.e. $\mathcal{O}_{G_P^{(2)}}(R) \subseteq \mathcal{X} \cap \ell$. By condition (C3), $|\mathcal{O}_{G_P^{(2)}}(R)| = d - 1$, whence $\mathcal{X} \cap \ell = (\mathcal{O}_{G_P^{(2)}}(R)) \cup \{P\}$. As $|W| > d$, there exists a point R' of W not on ℓ. Then the line through R' and P contains d points of W, which proves the assertion.

(ii) By Lemma 1.19, a Sylow p-subgroup S of G coincides with $G_P^{(1)}$ for some point P in W. Therefore, S is not a cyclic group. Also, condition (C2) ensures that S is a proper subgroup of G. Lemma 1.20 implies that the normalizer of S in G is G_P, which is isomorphic to a semidirect product of $S = G_P^{(1)}$ by a cyclic group H. By Lemma 1.19, for each $h \in G \setminus G_P$ we have that $h^{-1}Sh = G_R^{(1)}$ for some R distinct from P, and hence the intersection of S and $h^{-1}Sh$ is trivial. It remains to show that the center of G_P is trivial. Let h be a central element in G_P, and let $Q \in W$, Q distinct from P. Let $m \in G$ be such that $m(P) = Q$. By Theorem 1.10, the center of G_P is a normal subgroup of G. Then for some $h' \in Z(G_P)$ we have

$$h(Q) = hm(P) = mh'(P) = m(P) = Q.$$

This shows that h fixes each point in W, and then the claim follows by (i).

(iii) Without loss of generality, suppose that $P = Y_\infty$ and that $T_P(\mathcal{X}) = \ell_\infty$. First we prove that $G_P^{(2)} \subseteq Z(G_P^{(1)})$, that is, for any $A \in G_P^{(2)}$ and for any $B \in G_P^{(1)}$,

$$ABA^{-1}B^{-1} = id \tag{1.9}$$

holds. It has been noticed in the proof of Proposition 1.13 that $B = \bar{A}_{a,b,c}$ and that $A = \bar{A}_{0,b',c'}$ for some $a, b, c, b', c' \in \mathbb{K}$; also, condition (C4) implies that $b' = 0$. Then (1.9) follows.

Suppose now that there exists $C \in Z(G_P^{(1)}) \setminus G_P^{(2)}$. Then $C = \bar{A}_{a_1,b_1,c_1}$ with $(a_1, b_1) \neq (0, 0)$. By

straightforward computation

$$C\bar{A}_{a,b,c}C^{-1}\bar{A}^{-1}_{a,b,c} = \bar{A}_{0,0,a_1b-ab_1}. \tag{1.10}$$

Then $C\bar{A}_{a,b,c}C^{-1}\bar{A}^{-1}_{a,b,c} = id$ implies that $ab_1 = a_1b$. If $b_1 \neq 0$, then $a = (a_1/b_1)b$ and

$$G_P^{(1)} \leq \left\{ \bar{A}_{(\frac{a_1}{b_1})b,b,c} \mid b, c \in \mathbb{K} \right\};$$

otherwise, $a_1 \neq 0$ and

$$G_P^{(1)} \leq \left\{ \bar{A}_{a,0,c} \mid a, c \in \mathbb{K} \right\}.$$

This proves that $G_P^{(1)}$ is abelian. □

1.4 Proof of the main Theorem

We keep the notation of Section 1.3. In particular, $\mathcal{X}$ denotes a projective, non-singular, geometrically irreducible, plane algebraic curve defined over $\mathbb{K}$ by the equation $F(x_0, x_1, x_2) = 0$, F being an irreducible polynomial of degree $d > 3$, and $g = (d-1)(d-2)/2 > 2$ is the genus of $\mathcal{X}$. Here $\mathbb{K}$ is an algebraically closed field with characteristic $p > 2$.

We are going to prove that if G is an automorphism group of $\mathcal{X}$, then either

$$|G| \leq (12g^2 + 6g)d, \tag{1.11}$$

or $\mathcal{X}$ is birationally equivalent to a Hermitian curve. As $g = (d-1)(d-2)/2$, this will prove Theorem 1.1.

Lemma 1.22. *If G has more than one non-tame orbit, then* (1.11) *holds.*

Proof. The assertion follows from Theorem 1.2(ii). □

Lemma 1.23. *If either W is a long orbit, or W contains a short tame orbit under the action of G, then* (1.11) *holds.*

Proof. By Theorem 1.2(iv), the stabilizer G_P of a point $P \in W$ has size at most $4g+2$. Then the claim follows from Lemma 1.15. □

By Lemmas 1.22 and 1.23, condition (C1) can be assumed.

Lemma 1.24. *Assume that* (C1) *holds. If $W = \{P\}$, then* (1.11) *holds.*

Proof. By Lemmas 1.14 and 1.15 we may assume that the genus g' of the quotient curve $\mathcal{X}/G_P^{(1)}$ is equal to 0. Note that $W = \{P\}$ implies $G = G_P$. If $j_2(P) < d$, then there exists $R \in (T_P(\mathcal{X}) \cap \mathcal{X}) \setminus \{P\}$. Clearly, $\mathcal{O}_G(R)$ is contained in $(T_P(\mathcal{X}) \cap \mathcal{X}) \setminus \{P\}$, whence $|\mathcal{O}_G(R)| < d$. As $R \notin W$, $\mathcal{O}_G(R)$ is either a long or a short tame orbit. Taking into account Theorem 1.2(iv), by the orbit stabilizer theorem we obtain

$$|G| \le (4g+2)|\mathcal{O}_G(R)| < (4g+2)d < 3g^2 d.$$

If on the contrary $j_2(P) = d$, then Proposition 1.13 applies to $G_P^{(1)}$. Therefore, either $|G_P^{(2)}| = d$ or $|G_P^{(2)}| = d-1$. By Theorem 1.3, $|G_P^{(1)}| \le \frac{4|G_P^{(2)}|}{(|G_P^{(2)}|-1)^2} g^2$ holds. This gives $|G_P^{(1)}| \le (d-1)^3$. Then the assertion follows from (1.2), together with $G = G_P$. □

As a corollary, condition (C2) can be assumed as well. In Lemmas 1.25, 1.26 and 1.27 we deal with the case where condition (C3) does not hold.

Lemma 1.25. *Assume that both conditions* (C1) *and* (C2) *hold. Suppose in addition that P and Q are distinct points of W such that $G_P^{(1)} \cap G_Q^{(1)}$ is not trivial. Then $j_2(P) < d$.*

Proof. Let ϕ be a non-trivial element in $G_P^{(1)} \cap G_Q^{(1)}$. Assume that $j_2(P) = d$. Therefore, $T_P(\mathcal{X})$ and $T_Q(\mathcal{X})$ are distinct lines, both fixed by ϕ. The intersection point of $T_P(\mathcal{X})$ and $T_Q(\mathcal{X})$ is fixed by ϕ as well. Note that ϕ is a p-element fixing two points on $T_P(\mathcal{X})$; therefore, ϕ actually fixes $T_P(\mathcal{X})$ pointwise. Similarly, ϕ fixes $T_Q(\mathcal{X})$ pointwise. But this is impossible as ϕ is assumed to be non-trivial. □

Lemma 1.26. *Assume that both conditions* (C1) *and* (C2) *hold. Suppose in addition that P and Q are distinct points of W such that $G_P^{(1)} \cap G_Q^{(1)}$ is not trivial. If there exists $R \in (T_P(\mathcal{X}) \cap \mathcal{X}) \setminus \{P\}$ such that $\Delta := \mathcal{O}_{G_P}(R)$ is either a long or a short tame orbit, then* (1.11) *holds.*

Proof. Since G_P fixes $T_P(\mathcal{X})$, we have that $\Delta \subseteq (T_P(\mathcal{X}) \cap \mathcal{X}) \setminus \{P\}$. Therefore, $|\Delta| \leq d - j_2(P)$. By Lemma 1.16(i),

$$|G_P| \leq 2g - 2 + |\Delta| \leq 2g - 2 + d - j_2(P) < 2g + d.$$

Then (1.11) follows from Lemma 1.15. □

Lemma 1.27. *Assume that both conditions* (C1) *and* (C2) *hold. Suppose in addition that P and Q are distinct points of W such that $G_P^{(1)} \cap G_Q^{(1)}$ is not trivial. If for each $R \in (T_P(\mathcal{X}) \cap \mathcal{X}) \setminus \{P\}$ the orbit $\Delta := \mathcal{O}_{G_P}(R)$ is non-tame, then* (1.11) *holds.*

Proof. By Lemma 1.25 we have $j_2(P) < d$. Also, by condition (C1), we have that $(T_P(\mathcal{X}) \cap \mathcal{X}) \subset W$. Assume that $(T_P(\mathcal{X}) \cap \mathcal{X}) \setminus \{P\}$ is not an orbit under G_P. In this case, G_P has at least 3 non-tame orbits, and $|G_P| \leq 2g - 2$ holds by (1.6); then (1.11) follows from Lemma 1.15.

Therefore, we may assume that $(T_P(\mathcal{X}) \cap \mathcal{X}) \setminus \{P\}$ is an orbit under G_P. Write $(T_P(\mathcal{X}) \cap \mathcal{X}) \setminus \{P\} = \{R_1, \ldots, R_h\}$.

Assume first that $T_{R_{i_0}}(\mathcal{X}) \neq T_P(\mathcal{X})$ for some $i_0 \in \{1, \ldots, h\}$. Note that as $T_P(\mathcal{X})$ is fixed by G_P, actually $T_{R_i}(\mathcal{X}) \neq T_P(\mathcal{X})$ holds for all $i = 1, \ldots, h$. As R_i and P belong to the same orbit under G,

$j_2(R_i) = j_2(P)$ holds. In particular, $j_2(R_1) < d$ and there exists a point $S \in (T_{R_1}(\mathcal{X}) \cap \mathcal{X}) \setminus T_P(\mathcal{X})$. Let $\Delta' := \mathcal{O}_{G_P}(S)$. Then $\Delta' \subseteq \cup_{i=1}^{h}(T_{R_i}(\mathcal{X}) \cap \mathcal{X})$, and therefore

$$|\Delta'| \leq (d - j_2(P))^2 \leq (d-3)^2 < 2g.$$

We can assume that Δ' is a tame orbit under G_P, otherwise G_P would have 3 non-tame orbits. Hence, $|G_P| < 4g$ by Lemma 1.16(i). Then (1.11) follows from Lemma 1.15.

Then we may assume that $T_{R_i}(\mathcal{X}) = T_P(\mathcal{X})$ for all $i = 1, \ldots, h$. We are going to prove that the size of $G_P^{(2)}$ is at most d. Since $j_2(P) > 2$, by Lemma 1.13 the group $G_P^{(2)}$ coincides with the group E of elations with axis $T_P(\mathcal{X})$ fixing $\mathcal{X}$. Arguing as in the proof of Lemma 1.13, it is easy to deduce that $E = G_P^{(2)} = \cdots = G_P^{(j_2(P)-1)}$. Since $T_{R_i}(\mathcal{X}) = T_P(\mathcal{X})$, actually

$$E = G_{R_i}^{(2)} = \cdots = G_{R_i}^{(j_2(P)-1)}$$

holds for each $i = 1, \ldots, h$. Then, by the Hurwitz Genus Formula for E, we have

$$2g - 2 \geq |E|(2g' - 2) + (h+1)\left(\sum_{i=0}^{j_2(P)-1}(|E| - 1)\right),$$

where g' denotes the genus of the quotient curve $\mathcal{X}/E$. Therefore,

$$2g - 2 \geq |E|(2g' - 2) + \frac{d}{j_2(P)} j_2(P)(|E| - 1) = |E|(2g' - 2 + d) - d,$$

and hence

$$|E| = |G_P^{(2)}| \leq \frac{2g + d - 2}{d - 2} = d. \tag{1.12}$$

We distinguish a number of cases, according to the order sequence $(0, 1, \epsilon_2)$ of $\mathcal{X}$ and the order sequence $(0, 1, j_2(P))$ at P. For the sake of simplicity, for the rest of the proof the value $j_2(P) = j_2(R_1) = \ldots = j_2(R_h)$ will be denoted as j_2.

(i) $\epsilon_{\mathbf{2}} = \mathbf{2}$. Assume first that W coincides with $T_P(\mathcal{X}) \cap \mathcal{X}$. Then clearly $|W| = \frac{d}{j_2}$ holds. Note that the stabilizer of R_1 in $G_P^{(1)}$ consists of elations with axis $T_P(\mathcal{X})$, and hence coincides with $G_P^{(2)}$. Then by the orbit-stabilizer theorem $|G_P^{(1)}| \leq h|G_P^{(2)}|$ holds. Therefore, taking into account (1.2) and (1.12),

$$|G| = |G_P||W| \leq hd(4g+2)\frac{d}{j_2} < d(4g+2)\left(\frac{d}{j_2}\right)^2 < d(4g+2)g < 5dg^2.$$

Assume now that there exists $S \in W \setminus T_P(\mathcal{X})$. Let $\Delta' := \mathcal{O}_{G_P}(S)$. Since $\mathcal{X}$ is classical and Δ' is contained in $W \setminus (T_P(\mathcal{X}) \cap \mathcal{X})$, we have $|\Delta'| \leq 6g - 6 + 3d - (h+1) \leq 6g - 8 + 3d$. Then, by Lemma 1.16, $|G_P| \leq 8g - 10 + 3d$ holds. Therefore,

$$|G| = |G_P||W| \leq (8g - 10 + 3d)(6g - 6 + 3d). \tag{1.13}$$

Note that $d \geq 6$, as $T_P(\mathcal{X})$ contains at least two points of W. Then (1.13) implies (1.11).

(ii) $\epsilon_{\mathbf{2}} > \mathbf{2}$. Let $\mathcal{D}_0$ be the base-point-free linear series cut out on $\mathcal{X}$ by the lines through P. Let W_0 and $R^{\mathcal{D}_0}$ be the set of Weierstrass points and the ramification divisor of $\mathcal{D}_0$, respectively. The $(\mathcal{D}_0, P)$-order sequence is $(0, j_2 - 1)$, whereas for a point $Q \neq P$ the $(\mathcal{D}_0, Q)$-order sequence is $(0, I(P, \mathcal{X} \cap \ell_{P,Q}))$, $\ell_{P,Q}$ being the line joining P and Q. Note that since $\mathcal{X}$ is non-strange, the $\mathcal{D}_0$-order sequence of $\mathcal{X}$ is $(0, 1)$. Then the degree of the ramification divisor R_0 is

$$\deg(R^{\mathcal{D}_0}) = 2g - 2 + 2(d-1). \tag{1.14}$$

Clearly, each point in $T_P(\mathcal{X}) \cap \mathcal{X}$ is a point of W_0. Assume that there exists $S \in W_0 \setminus (T_P(\mathcal{X}) \cap \mathcal{X})$, and let $\Delta' := \mathcal{O}_{G_P}(S) \subset W_0$. Note that $\{P\}$ and $\mathcal{O}_{G_P}(R_1)$ are (non-tame) orbits under G_P disjoint from Δ'. Then Lemma 1.16 applies, and hence

$$|G_P| \leq 2g - 2 + |\Delta'| < 2g - 2 + |W_0| \leq 2g - 2 + \deg(R^{\mathcal{D}_0}) < 4g + 2d.$$

Then (1.11) follows from Lemma 1.15. Therefore, we can assume that

$$W_0 = T_P(\mathcal{X}) \cap \mathcal{X}. \tag{1.15}$$

As $\mathcal{X}$ is non-classical, $p \mid d-1$ holds by Theorem 1.5.

(iia) $\mathbf{p \nmid j_2 - 1}$. As $p \mid d-1$, we have that $p \nmid d$; taking into account that $(h+1)j_2 = d$, this implies $p \nmid j_2$. Then Theorem 1.6(ii) yields that $v_P(R^{\mathcal{D}_0}) = j_2 - 2$, whereas $v_{R_i}(R^{\mathcal{D}_0}) = j_2 - 1$ for each $i = 1, \ldots, h$. Therefore, (1.15) implies

$$\deg(R^{\mathcal{D}_0}) = (j_2 - 2) + h(j_2 - 1) = d - h - 2,$$

which contradicts (1.14).

(iib) $\mathbf{p \mid j_2 - 1}$. Note that $h > 1$, otherwise both $p \mid d - 1 = 2j_2 - 1$ and $p \mid j_2 - 1$ hold. We are going to show that G_{P,R_1,R_2} is contained in $G_P^{(2)}$. Let ϕ be a non-trivial element in G_{P,R_1,R_2}. As ϕ fixes three points on the same line $T_P(\mathcal{X})$, ϕ is a central collineation with axis $T_P(\mathcal{X})$. Assume that ϕ is a homology with center C. Let $\ell_1 = \ell_{P,C}$ be the line joining P and C, and let ℓ_2 be a line through C, not tangent to $\mathcal{X}$ at any of its points, and such that the intersection point of ℓ_2 and $T_P(\mathcal{X})$ does not belong to $\mathcal{X}$. Note that since W_0 is contained in $T_P(\mathcal{X})$, $I(Q, \mathcal{X} \cap \ell_i) = 1$ for any $Q \in \mathcal{X} \cap \ell_i$ and for each $i = 1, 2$. If $C \notin \mathcal{X}$, then ϕ acts semiregularly on both $(\ell_1 \cap \mathcal{X}) \setminus \{P\}$ and $\ell_2 \cap \mathcal{X}$. This is impossible as the former set has size $d-1$, whereas the latter has size d. Similarly, if $C \in \mathcal{X}$, then ϕ acts semiregularly both on a set of size $d-2$, namely $(\ell_1 \cap \mathcal{X}) \setminus \{P, C\}$, and on a set of size $d-1$, that is $(\ell_2 \cap \mathcal{X}) \setminus \{C\}$. This contradiction shows that ϕ must be an elation with axis $T_P(\mathcal{X})$. By Proposition 1.13, ϕ lies in $G_P^{(2)}$. This proves that G_{P,R_1,R_2} is contained in $G_P^{(2)}$. Hence,

$$|G| = |W||G_P| \leq |W||G_{P,R_1}|h \leq |W||G_{P,R_1,R_2}|(h-1)h < |W||G_P^{(2)}|h^2;$$

taking into account (1.12), this implies

$$\begin{aligned} |G| &< [(1+\epsilon_2)(2g-2)+3d]\frac{2g+d-2}{d-2}\left(\frac{d}{j_2}\right)^2 \\ &< [(1+\epsilon_2)(2g-2+d)]\frac{2g+d-2}{d-2}\left(\frac{d}{j_2}\right)^2 < d(2g+d-2)^2 = \\ &= d(2g+((2g)/(d-1)))^2 = 4dg^2(1+(1/(d-1)))^2 < 8dg^2. \end{aligned}$$

Here, we have used both $\frac{1+\epsilon_2}{j_2} \leq 1$ and $\frac{d}{(d-2)j_2} \leq 1$. □

A consequence of Lemmas 1.26 and 1.27 is that condition (C3) can be assumed.

Lemma 1.28. *Assume that conditions* (C1), (C2) *and* (C3) *hold. If there exists* $P \in W$ *such that* $j_2(P) < d$, *then* (1.11) *holds.*

Proof. Let $T_P(\mathcal{X}) \cap \mathcal{X} = \{P, R_1, \ldots, R_h\}$. By condition (C3), $G_P^{(1)}$ acts semiregularly on $\{R_1, \ldots, R_h\}$. Then $(T_P(\mathcal{X}) \cap \mathcal{X}) \setminus \{P\}$ consists of either a long or a short tame orbit under G_P, and $|G_P^{(1)}| \mid h$ holds. Also, $G_P^{(1)}$ contains no non-trivial elation with axis $T_P(\mathcal{X})$; by Proposition 1.13 this yields $G_P^{(2)} = \{id\}$. We distinguish four cases.

(i) $(\mathbf{T_P}(\mathcal{X}) \cap \mathcal{X}) \setminus \{\mathbf{P}\}$ **is the only short tame orbit of** $\mathbf{G_P}$. Let g' be the genus of $\mathcal{X}/G_P$. Then, by the Hurwitz Genus Formula,

$$2g-2 = |G_P|(2g'-2) + (|G_P|-1) + (|G_P^{(1)}|-1) + h(|G_{P,R_1}|-1).$$

Since $h|G_{P,R_1}| = |G_P|$, we have

$$2g = 2g'|G_P| + |G_P^{(1)}| - h.$$

Since $g > 2$ and $|G_P^{(1)}| \leq h$, g' must be a positive integer. Then $2g \geq 2|G_P| - d$, and hence $|G_P| \leq g + \frac{d}{2}$. Then (1.11) follows from Lemma 1.15.

(ii) $(\mathbf{T_P}(\mathcal{X}) \cap \mathcal{X}) \setminus \{\mathbf{P}\}$ **is one of the** $\mathbf{s \geq 2}$ **short tame orbits of** $\mathbf{G_P}$. By Lemma 1.15, it is enough to prove that $|G_P| \leq 6(g-1)$. If $s \geq 3$, by Lemma 1.17 we have $|G_P| \leq 4(g-1)$. Assume then that $s = 2$. If the short tame orbit Δ_1 of G_P different from $(T_P(\mathcal{X}) \cap \mathcal{X}) \setminus \{P\}$ has size less than d, then the assertion follows from Lemma 1.18. Assume then that the size of Δ_1 is larger than $d-1$. Let $\Delta_2 = (T_P(\mathcal{X}) \cap \mathcal{X}) \setminus \{P\}$. Then $|\Delta_1| > |\Delta_2|$. Arguing as in Lemma 1.18, we have

$$2g - 2 = |G_P|(d_1' + d_2' + d_3' - 2),$$

with $d_3' \geq 1$ and $d_2' > d_1' \geq 1/2$. If $d_1' \geq 2/3$ then $d_1' + d_2' + d_3' \geq 7/3$, whence $|G_P| \leq 6(g-1)$. Then we may assume $d_1' = 1/2$. Note that $d_2' = (|G_{P,R_1}| - 1)/|G_{P,R_1}|$. Therefore,

$$2g - 2 \geq |G_P|\Big(\frac{|G_{P,R_1}| - 1}{|G_{P,R_1}|} - \frac{1}{2}\Big). \tag{1.16}$$

If $|G_{P,R_1}| < 6$, then $|G_P| \leq 6(d-1) < 6(g-1)$; if $|G_{P,R_1}| \geq 6$, the same inequality follows from (1.16).

(iii)$(\mathbf{T_P}(\mathcal{X}) \cap \mathcal{X}) \setminus \{\mathbf{P}\}$ **contains a long orbit of** $\mathbf{G_P}$. Then $|G_P| < d$, and the claim follows from Lemma 1.15.

(iv) $\mathbf{G_P}$ **acts with at least 2 short orbits on** $(\mathbf{T_P}(\mathcal{X}) \cap \mathcal{X}) \setminus \{\mathbf{P}\}$. Clearly, the size of a short orbit of G_P contained in $(T_P(\mathcal{X}) \cap \mathcal{X}) \setminus \{P\}$ is less than $d-1$. Then by Lemmas 1.17 and 1.18 it follows that $|G_P| \leq 6(g-1)$. By Lemma 1.15, (1.11) holds. □

The following lemma will complete the proof of Theorem 1.1.

Lemma 1.29. *Assume that conditions* (C1), (C2) *and* (C3) *hold. If* $j_2(P) = d$ *for every point* $P \in W$, *then either* (1.11) *holds, or* $\mathcal{X}$ *is birationally equivalent to a Hermitian curve.*

Proof. By (1.2), we can write $G_P = G_P^{(1)} \ltimes H$, where H is a cyclic group of order prime to p. We consider the quotient curve $\mathcal{X}/G_P^{(1)}$. Let g' be the genus of $\mathcal{X}/G_P^{(1)}$. By Lemmas 1.14 and 1.15, $g' = 0$

can be assumed. Also, either $|G_P^{(2)}| = d$ or $|G_P^{(2)}| = d-1$ holds by Proposition 1.13. A number of cases will be considered.

(i) $\mathbf{G_P^{(1)}}$ **is cyclic**. Without loss of generality, assume that $P = Y_\infty$ and that $T_P(\mathcal{X}) = \ell_\infty$. Then a generator ϕ of $G_P^{(1)}$ is equal to $\bar{A}_{a,b,c}$ for some $a, b, c \in \mathbb{K}$. As $p > 2$, by straightforward computation we have

$$\phi^p = \bar{A}_{pa,pb,p\frac{p-1}{2}ab+pc} = id \ .$$

Therefore, $|G_P^{(1)}| = p$ holds. As $G_P^{(2)}$ is not trivial, we also have $G_P^{(2)} = G_P^{(1)}$.

Assume that $\mathcal{X}$ is non-classical. Then $p \mid d-1$ by Theorem 1.5. Actually, $|G_P^{(2)}| = p = d-1$ holds by Proposition 1.13, and $\epsilon_2 = p$ by Theorem 1.6(iv). Then by Theorem 1.9, $\mathcal{X}$ is projectively equivalent to a Hermitian curve.

If $\mathcal{X}$ is classical, then by Theorem 1.6 the size of W is at most $\frac{6g-6+3d}{d-2} = 3d$. As $G_P^{(2)} = G_P^{(1)}$, by Proposition 1.13 it follows that $|G_P^{(1)}| \leq d$. Hence, taking into account (1.2), by the orbit stabilizer theorem we obtain

$$|G| = |G_P^{(1)}||H||W| \leq d(4g+2)3d.$$

If $d > 4$, then (1.11) holds. If $d = 4$, then $p = d$ cannot occur; hence, $|G_P^{(1)}| = d-1$, and (1.11) is obtained from $|G| = (d-1)|H||W|$.

(ii) $\mathbf{G_P^{(1)}}$ **is not cyclic**. As $G_P^{(1)}$ acts semiregularly on $W \setminus \{P\}$, and $|G_P^{(1)}| \geq |G_P^{(2)}| \geq d-1$, we have that $|W| \geq d$. Actually, $|W| > d$ may be assumed. In fact, if $|W| = d$, then $|W| - 1 = |G_P^{(1)}| = |G_P^{(2)}| = d-1$ and hence

$$|G| = |H||G_P^{(1)}||W| \leq (4g+2)(d-1)d < (12g^2+6g)d.$$

Suppose that $|G_P^{(2)}| = d$. Then $p|d$ and $\mathcal{X}$ is classical by Theorem 1.5. Then, by Theorem 1.6, $|W| \leq \frac{6g-6+3d}{d-2} = 3d$. Since $G_P^{(1)}$ acts semiregularly on $W \setminus \{P\}$, d divides $|W|-1$. Therefore, $|W| \leq 2d+1$

and $|G_P^{(1)}| = d$. Then we have

$$|G| = |H||G_P^{(1)}||W| \leq (4g+2)d(2d+1) \leq (12g^2+6g)d.$$

Then we may assume that $|G_P^{(2)}| = d-1$. Note that all the hypothesis of Lemma 1.21 are satisfied, and then Theorem 1.10 applies with $M = \{id\}$. Moreover, by the proof of Proposition 1.13, any non-trivial element of $G_P^{(2)}$ is an elation with axis $T_P(\mathcal{X})$ and center P. Therefore, for any point $R \in W \setminus \{P\}$, the line $\ell_{P,R}$ joining P and R is fixed by $G_P^{(2)}$, and as $G_P^{(2)}$ acts semiregularly on $W \setminus \{P\}$, the d distinct points of $\mathcal{X}$ in $\ell_{P,R}$ all belong to W. By Lemma 1.21, G acts 2-transitively on W; in particular the action of G is primitive on W. Let N be a minimal normal subgroup of G. Note that for any point $Q \in W$, $Q \neq P$, the two-point stabilizer $G_{P,Q}$ has size prime to p and is a subgroup of G_P; therefore, it is a cyclic group by (1.2). Then the Kantor-O'Nan-Seitz Theorem 1.11 applies to G. If N is abelian, then by Lemma 1.12 N is the only minimal normal subgroup of G, which contradicts Theorem 1.10. Therefore, Theorem 1.11 together with Theorem 1.10 imply that G is one of the following groups in their natural 2-transitive permutation representations: $\mathrm{PSL}_2(p^a)$, $p^a \geq 4$, $\mathrm{PGL}_2(p^a)$, $p^a \geq 4$, $\mathrm{PSU}_3(p^a)$ with $p^a > 2$, $\mathrm{PGU}_3(p^a)$ with $p^a > 2$, ${}^2G_2(3^{2a+1})$ with $a \geq 0$.

1. Suppose that G is $\mathrm{PSL}_2(p^a)$ in its natural 2-transitive permutation representation. Let $q = p^a$. Then the size of W is $q+1$, and the size of the Sylow p-subgroup $G_P^{(1)}$ in a 1-point stabilizer G_P is q. Moreover, a complement H of $G_P^{(1)}$ in G_P is a cyclic group of order $(q-1)/2$ fixing a point $R \in W \setminus \{P\}$ and acting with two long orbits on $W \setminus \{P, R\}$. Clearly, H acts on $(\ell_{P,R} \cap \mathcal{X}) \setminus \{P, R\}$. Therefore, $(q-1)/2 = d-2$ holds. Now take a point $Q \in W \setminus \ell_{P,R}$. It has already been noticed that on $\ell_{Q,P}$ there are $d-1$ points of W distinct from P. But then $|W| \geq 2d-1 = 2(d-2)+3 \geq q+2$, which contradicts $|W| = q+1$.

2. Suppose that G is $\mathrm{PGL}_2(p^a)$ in its natural 2-transitive permutation representation. Let $q = p^a$.

Then the size of W is $q+1$, and the size of the Sylow p-subgroup $G_P^{(1)}$ in a 1-point stabilizer G_P is q. Unlike the previous case, a complement H of $G_P^{(1)}$ in G_P is a cyclic group of order $(q-1)$ fixing a point $R \in W \setminus \{P\}$ and acting regularly on $W \setminus \{P, R\}$. Then clearly H acts on $(\ell_{P,R} \cap \mathcal{X}) \setminus \{P, R\}$. Therefore, $q = d - 1$ holds. But this contradicts $q + 1 = |W| > d$.

3. Suppose that G is ${}^2G_2(3^{2a+1})$, $p = 3$, in its natural 2-transitive permutation representation. Therefore, the size of W is q^3+1, and the size of the Sylow p-subgroup $G_P^{(1)}$ in a 1-point stabilizer G_P is q^3. Moreover, the commutator subgroup of $G_P^{(1)}$ has size q^2, whereas the center of $G_P^{(1)}$ has order q (see [96, Lemma 12.32]). By Lemma 1.21, $G_P^{(2)}$ is the center of $G_P^{(1)}$, whence $|G_P^{(2)}| = q$. On the other hand, in the proof of Lemma 1.21(iii) it has been showed that the commutator subgroup of $G_P^{(1)}$ is contained in $G_P^{(2)}$ (see (1.10)). Then $q^2 \le |G_P^{(2)}|$, which is clearly a contradiction.

4. Suppose that G is either $\mathrm{PSU}_3(q)$ or $\mathrm{PGU}_3(q)$, $q = p^a > 2$, in its natural 2-transitive permutation representation. Therefore, the size of W is $q^3 + 1$, and the size of the Sylow p-subgroup $G_P^{(1)}$ in a 1-point stabilizer G_P is q^3. Moreover, the center of $G_P^{(1)}$ has order q (see [96, Example A.9]). By Lemma 1.21, $|G_P^{(2)}| = q = d - 1$. Then the genus g of $\mathcal{X}$ is $\frac{q(q-1)}{2}$. Therefore,

$$|G| \ge \frac{(q^3+1)q^3(q^2-1)}{3} > 16g^3 + 24g^2 + g.$$

Then (1.1) holds, and $\mathcal{X}$ is birationally equivalent to a Hermitian curve.

□

Chapter 2

On the functional codes defined by quadrics and Hermitian varieties

2.1 Introduction

In recent years, functional codes have received a lot of attention. In his PhD thesis, F.A.B. Edoukou investigated various functional codes linked to quadrics and Hermitian varieties defined in finite projective spaces [63]. This work was continued in [64, 65, 86], where the results of the PhD thesis of F.A.B. Edoukou were improved and extended. In particular, Hallez and Storme investigated the functional codes $C_2(\mathcal{H})$, with $\mathcal{H}$ a non-singular Hermitian variety in $\mathrm{PG}(N, q^2)$. The codewords of this code are defined by evaluating the points of $\mathcal{H}$ in the quadratic polynomials defined over $\mathbb{F}_{q^2}$. We now present the similar results for the functional code $C_{Herm}(\mathcal{Q})$. The codewords of this latter code are defined by evaluating the points of a non-singular quadric $\mathcal{Q}$ in $\mathrm{PG}(N, q^2)$ in the polynomials defining the Hermitian varieties of $\mathrm{PG}(N, q^2)$. Consider a fixed algebraic variety $\mathcal{X}$ in $\mathrm{PG}(N, q)$. We denote the point set of $\mathcal{X}$ by $\{P_1, \ldots, P_n\}$, where we normalize the coordinates of the points P_i with respect to the leftmost non-zero coordinate. The functional code $C_h(\mathcal{X})$ is equal to

$$C_h(\mathcal{X}) = \{(f(P_1), \ldots, f(P_n)) || f \in \mathcal{F}_h\} \cup \{0\},$$

with $\mathcal{F}_h$ the set of the homogeneous polynomials of degree h over the finite field $\mathbb{F}_q$ in the variables $X_0, \ldots, X_N$ [119].

Consider for instance a non-singular quadric $\mathcal{Q}$ of $\mathrm{PG}(N, q)$. Then the functional code $C_2(\mathcal{Q})$ is the linear code

$$C_2(\mathcal{Q}) = \{(f(P_1), \ldots, f(P_n)) || f \in \mathcal{F}_2\} \cup \{0\},$$

defined over $\mathbb{F}_q$. The small weights of this functional code were investigated by Edoukou *et al.* in [65].

This research inspired the authors of [65] to investigate similar functional codes defined by Hermitian varieties in $\mathrm{PG}(N, q^2)$. Let $\mathcal{F}$ be the $\mathbb{F}_q$-vector space of the zero polynomial and all homogeneous polynomials $(X_0, \ldots, X_N)A(X_0^q, \ldots, X_N^q)$ of degree $q+1$ in $N+1$ variables, with $A = (a_{ij}), 0 \leqslant i, j \leqslant N$, $a_{ij}^q = a_{ji}$, $a_{ij} \in \mathbb{F}_{q^2}$, defining Hermitian varieties of $\mathrm{PG}(N, q^2)$. In this article, a Hermitian form will always denote a non-zero polynomial belonging to $\mathcal{F}$. For any algebraic variety $\mathcal{X}$, the functional code $C_{Herm}(\mathcal{X})$ is the linear code

$$C_{Herm}(\mathcal{X}) = \{(f(P_1), \ldots, f(P_n)) || f \in \mathcal{F}\},$$

defined over $\mathbb{F}_q$.

Let $\mathcal{H}$ be a non-singular Hermitian variety in $\mathrm{PG}(N, q^2)$ [99, Chapter 23]. In [64], the small weight codewords of the functional code $C_{Herm}(\mathcal{H})$ were characterized.

In a third article [86], Hallez and Storme investigated the functional codes $C_2(\mathcal{H})$, with $\mathcal{H}$ a non-singular Hermitian variety in $\mathrm{PG}(N, q^2)$. The codewords of this code are defined by evaluating the points of $\mathcal{H}$ in the quadratic polynomials defined over $\mathbb{F}_{q^2}$.

The crucial element in obtaining the results of [64] and [65] were the facts that two distinct quadrics define a pencil of quadrics and that two distinct Hermitian varieties define a pencil of Hermitian varieties. This fact is no longer true when considering a quadric in combination with a Hermitian variety. This

meant that, in [86], different arguments had to be used, leading to results which were only valid for small dimensions $N < O(q^2)$. However, for N satisfying this condition, the small weight codewords were characterized as arising from the intersections of $\mathcal{H}$ with the quadrics which are the union of two hyperplanes. In Section 2.2, we will improve their results for the case $N = 4$ and in Section 2.3, we will prove that their results about the small weight codewords are valid in general dimension N.

After investigating the functional codes $C_2(\mathcal{H})$, with $\mathcal{H}$ a non-singular Hermitian variety in $\mathrm{PG}(N, q^2)$, the question was posed to investigate the functional codes $C_{Herm}(\mathcal{Q})$, with $\mathcal{Q}$ a non-singular quadric in $\mathrm{PG}(N, q^2)$, in which the codewords are obtained by evaluating the points of $\mathcal{Q}$ in all the polynomials of $\mathcal{F}$ defining Hermitian forms of $\mathrm{PG}(N, q^2)$. In Sections 2.4, 2.5, 2.6 and 2.7, we present results on these functional codes $C_{Herm}(\mathcal{Q})$. As in the previous articles [64, 65, 86], the small dimensions need to be discussed separately.

In general, the results about the minimum distance of $C_2(\mathcal{H})$ with $\mathcal{H}$ a non-singular Hermitian variety, respectively $C_{Herm}(\mathcal{Q})$ with $\mathcal{Q}$ a non-singular quadric, are stated as results about the maximum size of the intersection of an arbitrary quadric with $\mathcal{H}$, respectively the intersection of an arbitrary Hermitian variety with $\mathcal{Q}$. In this article, we will also state the results in this form.

2.2 The functional code $C_2(\mathcal{H})$ for $N = 4$

In the main sections of this article, the small weight codewords of $C_{Herm}(\mathcal{Q})$ are discussed. In this discussion, we will use the results about the code $C_2(\mathcal{H})$, with $\mathcal{H}$ a non-singular Hermitian variety. The best known results about this code were presented in [86]. In this section and the next section, we will give some improvements to these results. Hereby we will denote a non-singular Hermitian variety, respectively a non-singular quadric in $\mathrm{PG}(4, q^2)$ by $\mathcal{H}(4, q^2)$, respectively $\mathcal{Q}(n, q^2)$.

The first lemma is an improvement of [86, Lemma 3.3].

Lemma 2.1. *Assume that a line L of $\mathcal{Q}(4,q^2)$ contains at most q points of $\mathcal{Q}(4,q^2)\cap\mathcal{H}(4,q^2)$, then $|\mathcal{Q}(4,q^2)\cap\mathcal{H}(4,q^2)|\leq q^5+q^4+4q^3-3q+1$.*

Proof. It follows immediately that L contains one point of $\mathcal{H}(4,q^2)$. Let $P\in L$ with $P\notin\mathcal{H}(4,q^2)$. Take a line M of $\mathcal{Q}(4,q^2)$ intersecting L in P. Consider the plane $\pi=\langle L,M\rangle$. Then π lies in the tangent hyperplane $T_P(\mathcal{Q}(4,q^2))$ and in q^2 hyperplanes containing a hyperbolic quadric $Q^+(3,q^2)$ of $Q(4,q^2)$; L is a line on each of these hyperbolic quadrics. We denote these hyperbolic quadrics by $\mathcal{Q}_i$, $i=1,\ldots,q^2$. For a given hyperbolic quadric $\mathcal{Q}_i$, we denote the regulus containing L by $\mathcal{R}_i$ and the opposite one by $\mathcal{R}_i'$.

Assume that $L\cap\mathcal{H}(4,q^2)=\{R\}$. In $\mathcal{R}_i'$, $i=1,\ldots,q^2$, there is at most one line contained in $\mathcal{H}(4,q^2)$, namely the one through R. All the lines through R which are contained in the intersection $\mathcal{Q}(4,q^2)\cap\mathcal{H}(4,q^2)$ are contained in both $T_R(\mathcal{Q}(4,q^2))\cap\mathcal{Q}(4,q^2)=R\mathcal{Q}(2,q^2)$ and $T_R(\mathcal{H}(4,q^2))\cap\mathcal{H}(4,q^2)=R\mathcal{H}(2,q^2)$. Then there can be at most $k=|\mathcal{Q}(2,q^2)\cap\mathcal{H}(2,q^2)|\leq 2(q+1)$ such lines. Hence, there are at most k hyperbolic quadrics containing one line of $\mathcal{Q}(4,q^2)\cap\mathcal{H}(4,q^2)$ through R.

Let $\mathcal{Q}_i$ be a hyperbolic quadric containing a line of $\mathcal{H}(4,q^2)$ through R. Counting the points of $\mathcal{Q}_i\cap\mathcal{H}(4,q^2)$ according to the lines of $\mathcal{R}_i'$, we find $|\mathcal{Q}_i\cap\mathcal{H}(4,q^2)|\leq(q^2+1)+q^2(q+1)=q^3+2q^2+1$. Now, let $\mathcal{Q}_j$ be a hyperbolic quadric not containing a line of $\mathcal{H}(4,q^2)$ through R. Counting the points of $\mathcal{Q}_j\cap\mathcal{H}(4,q^2)$ according to the lines of $\mathcal{R}_j'$, we find $|\mathcal{Q}_j\cap\mathcal{H}(4,q^2)|\leq(q^2+1)(q+1)=q^3+q^2+q+1$.

We denote $a=|\pi\cap\mathcal{Q}(4,q^2)\cap\mathcal{H}(4,q^2)|=1+|M\cap\mathcal{H}(4,q^2)|$. We may assume $a\in\{2,q+2\}$ and we

conclude

$$\begin{aligned}|\mathcal{Q}(4,q^2)\cap\mathcal{H}(4,q^2)| &\le k(q^3+2q^2+1-a)+(q^2-k)(q^3+q^2+q+1-a)\\ &\quad +|T_P(\mathcal{Q}(4,q^2))\cap\mathcal{Q}(4,q^2)\cap\mathcal{H}(4,q^2)|\\ &\le q^2(q^3+q^2+q+1)+k(q^2-q)+(q+1)(q^2-1)-a(q^2-1)\\ &\le q^5+q^4+2q^3+2q^2-q-1+2(q+1)(q^2-q)-2(q^2-1)\\ &= q^5+q^4+4q^3-3q+1,\end{aligned}$$

where we used the upper bound $(q+1)(q^2-1)+a$ for $|T_P(\mathcal{Q}(4,q^2))\cap\mathcal{Q}(4,q^2)\cap\mathcal{H}(4,q^2)|$. □

The second lemma is an improvement of [86, Lemma 3.6].

Lemma 2.2. *Assume that all lines of $\mathcal{Q}(4,q^2)$ share $q+1$ or q^2+1 points with $\mathcal{H}(4,q^2)$, then $|\mathcal{Q}(4,q^2)\cap\mathcal{H}(4,q^2)|\le q^5+q^4+2q^3-q+1$.*

Proof. Let P be a point of $\mathcal{Q}(4,q^2)$, not lying on $\mathcal{H}(4,q^2)$. Let L and M be lines on $\mathcal{Q}(4,q^2)$ through P. All lines on $\mathcal{Q}(4,q^2)$ through P, including L and M, contain precisely $q+1$ points of $\mathcal{H}(4,q^2)$. Hence, the tangent hyperplane $T_P(\mathcal{Q}(4,q^2))$ contains $(q+1)(q^2+1)$ points of $\mathcal{Q}(4,q^2)\cap\mathcal{H}(4,q^2)$ since $T_P(\mathcal{Q}(4,q^2))\cap\mathcal{Q}(4,q^2)$ is a cone with P as vertex and a conic $\mathcal{Q}(2,q^2)$ as base.

Let R be a point of $L\cap\mathcal{H}(4,q^2)$. There are q^2+1 lines of $\mathcal{Q}(4,q^2)$ through R. We show that at most 2 of those can be contained in $\mathcal{Q}(4,q^2)\cap\mathcal{H}(4,q^2)$. Assume there are 3 lines through R contained in $\mathcal{Q}(4,q^2)\cap\mathcal{H}(4,q^2)$. These lines generate a hyperplane, since a plane cannot contain 3 lines of $\mathcal{Q}(4,q^2)$. This hyperplane must be $T_R(\mathcal{Q}(4,q^2))$ since all lines of $\mathcal{Q}(4,q^2)$ through R are contained in $T_R(\mathcal{Q}(4,q^2))$. In the same way this hyperplane also equals $T_R(\mathcal{H}(4,q^2))$. However, this is a contradiction by [86, Lemma 3.5]. We have proved that there are at most 2 lines through each of the $q+1$ points of $L\cap\mathcal{H}(4,q^2)$ contained in $\mathcal{Q}(4,q^2)\cap\mathcal{H}(4,q^2)$.

We consider the plane $\pi = \langle L, M\rangle$ and the q^2+1 hyperplanes through it. One of those hyperplanes is $T_P(\mathcal{Q}(4,q^2))$. All the other ones intersect $\mathcal{Q}(4,q^2)$ in a hyperbolic quadric $\mathcal{Q}^+(3,q^2)$. Each line of such a hyperbolic quadric contains by assumption $q+1$ or q^2+1 points of $\mathcal{H}(4,q^2)$. Hence, in both reguli of such a hyperbolic quadric there is the same number of lines which contain $q+1$ respectively q^2+1 points of $\mathcal{H}(4,q^2)$. Considering the fact that L contains $q+1$ points of $\mathcal{H}(4,q^2)$ and using [86, Lemma 3.1], we find that in each of those hyperbolic quadrics, both reguli contain $q+1$, 2, 1 or 0 lines of $\mathcal{H}(4,q^2)$. Let a_i be the number of hyperbolic quadrics in which both reguli contain i lines of $\mathcal{H}(4,q^2)$. Obviously, $a_{q+1}+a_2+a_1+a_0 = q^2$ and $(q+1)a_{q+1}+2a_2+a_1 = k \leq 2(q+1)$, with k the total number of lines of $\mathcal{H}(4,q^2)$ through the points of $L \cap \mathcal{H}(4,q^2)$. Counting the points of $\mathcal{H}(4,q^2)$ according to the lines of one regulus, it can be found that the hyperbolic quadrics in which both reguli contain i lines of $\mathcal{H}(4,q^2)$, contain precisely $i(q^2+1)+(q^2+1-i)(q+1) = (q^2+1)(q+1)+i(q^2-q)$ points of $\mathcal{H}(4,q^2)$.

Now, we compute the total number of points in the intersection. Hereby, $I = \{0,1,2,q+1\}$. We find

$$\begin{aligned}
|\mathcal{Q}(4,q^2)\cap\mathcal{H}(4,q^2)| &= (q+1)(q^2+1)+\sum_{i\in I} a_i\left((q^2+1)(q+1)+i(q^2-q)-2(q+1)\right)\\
&= (q+1)(q^2+1)+(q^2-1)(q+1)\sum_{i\in I} a_i + (q^2-q)\sum_{i\in I} a_i i\\
&= (q+1)(q^2+1)+q^2(q^2-1)(q+1)+(q^2-q)k\\
&\leq (q+1)\left(q^2(q^2-1)+q^2+1\right)+(q^2-q)2(q+1)\\
&= q^5+q^4+2q^3-q+1,
\end{aligned}$$

which completes the proof. □

Using these lemmata, we can now state an improved version of [86, Theorem 3.8].

Theorem 2.3. *Let Q be a quadric in* $\mathrm{PG}(4, q^2)$*. If* $|Q \cap \mathcal{H}(4, q^2)| > q^5 + q^4 + 4q^3 - 3q + 1$*, then Q is the union of two hyperplanes.*

Proof. Combine the results of Lemma 2.1 and Lemma 2.2 with the results of [86, Section 3]. □

2.3 The functional code $C_2(\mathcal{H})$ for $N \geq 4$

Definition 2.4. $W_4 := q^5+q^4+4q^3-3q+1$; $W_n := q^2W_{n-1}+q^{n-2}+2q^{n-3}$ if n is odd, $W_n := q^2W_{n-1}-q^{n-2}$ if n is even, $n > 4$.

Lemma 2.5. *For $n \geq 4$: $W_n := q^{2n-8}W_4 + \sum_{i=n-2}^{2n-7} q^i + 2\delta q^{n-3}$, with $\delta = 1$ if n is odd and $\delta = 0$ if n is even.*

Proof. Immediate, using induction on n. □

Some examples:

- $W_5 = q^7 + q^6 + 4q^5 - 2q^3 + 3q^2$,
- $W_6 = q^9 + q^8 + 4q^7 - 2q^5 + 2q^4$,
- $W_7 = q^{11} + q^{10} + 4q^9 - 2q^7 + 2q^6 + q^5 + 2q^4$
- $W_n = q^{2n-3} + q^{2n-4} + 4q^{2n-5} - 2q^{2n-7} + 2q^{2n-8} + q^{2n-9} + \ldots + q^{n-2}$ if $n \geq 8$ is even.
- $W_n = q^{2n-3} + q^{2n-4} + 4q^{2n-5} - 2q^{2n-7} + 2q^{2n-8} + q^{2n-9} + \ldots + q^{n-2} + 2q^{n-3}$ if $n \geq 8$ is odd.

Theorem 2.6. *Let Q be a quadric in* $\mathrm{PG}(n, q^2)$*, $n \geq 4$. If* $|Q \cap \mathcal{H}(n, q^2)| > W_n$*, then Q is the union of two hyperplanes.*

Proof. We prove this theorem by induction on n. The theorem is true for $n = 4$ by Theorem 2.3. Now, we suppose the theorem is valid for $n-1$. We prove it for dimension n.

By assumption, $|Q \cap \mathcal{H}(n, q^2)| > W_n$. Assume now that every non-tangent hyperplane contains at most W_{n-1} points of $Q \cap \mathcal{H}(n, q^2)$. We count the number N of tuples (P, H), with $P \in Q \cap \mathcal{H}(n, q^2)$, H a hyperplane not tangent to $\mathcal{H}(n, q^2)$, and $P \in H$. On the one hand,

$$N > W_n(\frac{q^{2n}-1}{q^2-1} - q^2|\mathcal{H}(n-2, q^2)| - 1) = W_n \frac{q^{2n} - q^2 - q^2(q^{n-1} + (-1)^{n-2})(q^{n-2} + (-1)^{n-1})}{q^2-1}.$$

On the other hand, counting this number of incidences otherwise,

$$N \leq W_{n-1}(\frac{q^{2n+2}-1}{q^2-1} - |\mathcal{H}(n, q^2)|) = W_{n-1}(\frac{q^{2n+2} - 1 - (q^{n+1} + (-1)^n)(q^n + (-1)^{n+1})}{q^2-1}).$$

Thus,

$$W_n < W_{n-1}\left[\frac{q^{2n+2} - 1 - (q^{n+1} + (-1)^n)(q^n + (-1)^{n+1})}{q^{2n} - q^2 - q^2(q^{n-1} + (-1)^{n-2})(q^{n-2} + (-1)^{n-1})}\right].$$

We look first at the case n even. We find

$$\begin{aligned}
W_n &< W_{n-1}\left[\frac{q^{2n+2} - 1 - (q^{n+1}+1)(q^n - 1)}{q^{2n} - q^2 - q^2(q^{n-1}+1)(q^{n-2}-1)}\right] \\
&= W_{n-1}q^2 - W_{n-1}\frac{q^{n+3} - q^{n+2} - q^{n+1} + q^n}{q^{2n} - q^{2n-1} + q^{n+1} - q^n} \\
&< W_{n-1}q^2 - (q^{2n-5} + q^{2n-6})\frac{q^{n+3} - q^{n+2} - q^{n+1} + q^n}{q^{2n} - q^{2n-1} + q^{n+1} - q^n} \\
&= W_{n-1}q^2 - \frac{q^{3n-2} - 2q^{3n-4} + q^{3n-6}}{q^{2n} - q^{2n-1} + q^{n+1} - q^n} \\
&= W_{n-1}q^2 - q^{n-2} - \frac{q^{3n-3} - 2q^{3n-4} + q^{3n-6} - q^{2n-1} + q^{2n-2}}{q^{2n} - q^{2n-1} + q^{n+1} - q^n} \\
&< W_{n-1}q^2 - q^{n-2}.
\end{aligned}$$

Now we look at the case n odd. If $q \geq 4$, we find

$$\begin{aligned}
W_n &< W_{n-1}\left[\frac{q^{2n+2}-1-(q^{n+1}-1)(q^n+1)}{q^{2n}-q^2-q^2(q^{n-1}-1)(q^{n-2}+1)}\right] \\
&= q^2W_{n-1} + W_{n-1}\frac{q^{n+3}-q^{n+2}-q^{n+1}+q^n}{q^{2n}-q^{2n-1}-q^{n+1}+q^n} \\
&< q^2W_{n-1} + (q^{2n-5}+2q^{2n-6})\frac{q^{n+3}-q^{n+2}-q^{n+1}+q^n}{q^{2n}-q^{2n-1}-q^{n+1}+q^n} \\
&= q^2W_{n-1} + \frac{q^{3n-2}+q^{3n-3}-3q^{3n-4}-q^{3n-5}+2q^{3n-6}}{q^{2n}-q^{2n-1}-q^{n+1}+q^n} \\
&= q^2W_{n-1} + q^{n-2} + 2q^{n-3} - \frac{q^{3n-4}+q^{3n-5}-2q^{3n-6}-q^{2n-1}-q^{2n-2}+2q^{2n-3}}{q^{2n}-q^{2n-1}-q^{n+1}+q^n} \\
&< q^2W_{n-1} + q^{n-2} + 2q^{n-3}.
\end{aligned}$$

If $q = 2, 3$ the inequality $W_{n-1} < q^{2n-5} + 2q^{2n-6}$, used in this derivation is not valid. However, the inequality

$$W_{n-1}\left[\frac{q^{2n+2}-1-(q^{n+1}-1)(q^n+1)}{q^{2n}-q^2-q^2(q^{n-1}-1)(q^{n-2}+1)}\right] < q^2W_{n-1} + q^{n-2} + 2q^{n-3}$$

is still valid in these cases. In order to prove this, it is enough to show that

$$W_{n-1}\frac{q^{n+3}-q^{n+2}-q^{n+1}+q^n}{q^{2n}-q^{2n-1}-q^{n+1}+q^n} < q^{n-2} + 2q^{n-3}.$$

We first consider $q = 2$:

$$\begin{aligned}
& W_{n-1}\frac{2^{n+3}-2^{n+2}-2^{n+1}+2^n}{2^{2n}-2^{2n-1}-2^{n+1}+2^n} < 2^{n-2} + 2\cdot 2^{n-3} \\
\Leftrightarrow \quad & W_{n-1}(2^{n+2}-2^n) < 2^{n-1}(2^{2n-1}-2^n) \\
\Leftrightarrow \quad & W_{n-1}(4+2) < 2^{2n-1}-2^n \\
\Leftrightarrow \quad & 2^{2n-2}+2^{2n-3}+2^{2n-4}+2^{2n-5}-2^{2n-8}-2^{2n-9}-2^{n-1}-2^{n-2} < 2^{2n-1}-2^n\,,
\end{aligned}$$

which clearly holds if $n \geq 5$. Hereby we used that $W_{n-1} = 2^{2n-4} + 2^{2n-6} - 2^{2n-10} - 2^{n-3}$ if n is odd and $q = 2$. Now, we consider $q = 3$:

$$\begin{aligned} & W_{n-1}\frac{3^{n+3} - 3^{n+2} - 3^{n+1} + 3^n}{3^{2n} - 3^{2n-1} - 3^{n+1} + 3^n} < 3^{n-2} + 2 \cdot 3^{n-3} \\ \Leftrightarrow \quad & W_{n-1}(2 \cdot 3^{n+2} - 2 \cdot 3^n) < (2 \cdot 3^{2n-1} - 2 \cdot 3^n)(3^{n-2} + 2 \cdot 3^{n-3}) \\ \Leftrightarrow \quad & W_{n-1}(9-1) < (3^{n-1} - 1)(3^{n-2} + 2 \cdot 3^{n-3}) \\ \Leftrightarrow \quad & 3^{2n-3} + 2 \cdot 3^{2n-4} - 2 \cdot 3^{2n-6} - 2 \cdot 3^{2n-7} \\ & -3^{2n-10} - 3^{n-2} - 3^{n-3} < 3^{2n-3} + 2 \cdot 3^{2n-4} - 3^{n-2} - 2 \cdot 3^{n-3}, \end{aligned}$$

which clearly holds if $n \geq 5$. Hereby we used that $W_{n-1} = 3^{2n-5} + 2 \cdot 3^{2n-6} + 3^{2n-7} - 3^{2n-9} - \frac{3^{2n-10}+3^{n-3}}{2}$ if n is odd and $q = 3$.

We conclude that in all cases, we find a contradiction. Hence, there is a non-tangent hyperplane π containing more than W_{n-1} points of $Q \cap \mathcal{H}(n, q^2)$. We can continue as in part 2 of the proof of Hallez and Storme ([86, Theorem 4.1]).

The intersection $\mathcal{H} = \pi \cap \mathcal{H}(n, q^2)$ is a non-singular $(n-1)$-dimensional Hermitian variety. We conclude from the previous that $|\mathcal{H} \cap Q| > W_{n-1}$. By the induction hypothesis, $Q \cap \pi$ is the union of two $(n-2)$-spaces. The only quadrics in $\mathrm{PG}(n, q^2)$ containing $(n-2)$-spaces, are $\pi_{n-4}\mathcal{Q}^+(3, q^2)$, $\pi_{n-3}\mathcal{Q}(2, q^2)$, $\pi_{n-2}\mathcal{Q}^-(1, q^2)$, which is just an $(n-2)$-space, and $\pi_{n-2}Q^+(1, q^2)$, which is the union of two hyperplanes. We want to eliminate the first three possibilities. Each of those three quadrics can be described as the union of 1 or q^2+1 distinct $(n-2)$-dimensional spaces. The largest intersection of an $(n-2)$-space and $\mathcal{H}(n, q^2)$ is achieved if n is odd and the intersection is a cone with a line as vertex and a $\mathcal{H}(n-4, q^2)$ as base. The cardinality of such an intersection is

$$q^{2n-5} + q^{2n-7} + \ldots + q^{n+2} + q^n + q^{n-1} + q^{n-3} + \ldots + q^2 + 1.$$

Hence, the cardinality of the intersection of each of those quadrics with $\mathcal{H}(n, q^2)$ is at most

$$\begin{aligned}
&(q^2+1)(q^{2n-5}+q^{2n-7}+\ldots+q^{n+2}+q^n+q^{n-1}+q^{n-3}+\ldots+q^2+1)\\
&=q^{2n-3}+2q^{2n-5}+2q^{2n-7}+\cdots+2q^{n+2}+q^{n+1}+q^n+2q^{n-1}+2q^{n-3}+\cdots+2q^2+1\\
&<W_n.
\end{aligned}$$

Since the cardinality of the intersection is smaller than W_n, those three quadrics can be eliminated. The only possibility remaining for Q is the union of two hyperplanes. □

The structure of the small weight codewords of $C_2(\mathcal{H})$, with $\mathcal{H}$ a non-singular Hermitian variety in $\mathrm{PG}(N, q^2)$, can be derived from this theorem. We refer to [86, Section 5] for a detailed analysis, which was performed for $N < O(q^2)$, but which is valid in general by the previous theorem.

2.4 The functional code $C_{Herm}(\mathcal{Q})$ for $N = 2$

In the twodimensional case, the result is immediate.

Theorem 2.7. *Let $\mathcal{Q}(2, q^2)$ be a non-singular conic in $\mathrm{PG}(2, q^2)$ and let $\mathcal{H}(2, q^2)$ be an arbitrary Hermitian curve in $\mathrm{PG}(2, q^2)$. Then $|\mathcal{H}(2, q^2) \cap \mathcal{Q}(2, q^2)| \leq 2(q+1) = \overline{W}_2$.*

Proof. This follows directly from Bézout's theorem. □

2.5 The functional code $C_{Herm}(\mathcal{Q})$ for $N = 3$

To simplify notations, we both denote the non-singular elliptic quadric $\mathcal{Q}^-(3, q^2)$ and the non-singular hyperbolic quadric $\mathcal{Q}^+(3, q^2)$ by $\mathcal{Q}(3, q^2)$. Let H be an arbitrary threedimensional Hermitian variety.

2.5.1 $H = \mathcal{H}(3, q^2)$ is a non-singular Hermitian variety

Edoukou, in [63], gives upper bounds for $|\mathcal{H}(3, q^2) \cap Q|$, with Q an arbitrary quadric. In particular, the following theorem is valid.

Theorem 2.8. *Let $\mathcal{H}(3, q^2)$ and $\mathcal{Q}(3, q^2)$ be a non-singular Hermitian variety and a non-singular quadric in* $\mathrm{PG}(3, q^2)$*, then*

$$|\mathcal{H}(3, q^2) \cap \mathcal{Q}(3, q^2)| \leq 2q^3 + q^2 + 1 = W_3.$$

2.5.2 $H = P\mathcal{H}(2, q^2)$

This Hermitian variety is the union of q^3+1 lines through P and the points of a non-singular Hermitian variety $\mathcal{H}(2, q^2)$.

$P \in \mathcal{Q}(3, q^2)$

Consider the tangent plane $T_P(\mathcal{Q}(3, q^2))$. Here, $T_P(\mathcal{Q}(3, q^2)) \cap \mathcal{Q}(3, q^2) = P\mathcal{Q}(1, q^2)$, where $\mathcal{Q}(1, q^2)$ is of the same type as the quadric $\mathcal{Q}(3, q^2)$. All the lines of $P\mathcal{H}(2, q^2)$ not in this tangent plane contain one extra point of the quadric $\mathcal{Q}(3, q^2)$. The number of lines contained in the intersection $T_P(\mathcal{Q}(3, q^2)) \cap P\mathcal{H}(2, q^2)$ is at most two, leading to at most $2q^2 + 1$ intersection points, since this tangent plane contains two lines of the quadric $\mathcal{Q}(3, q^2)$ in case this is a hyperbolic quadric and zero lines of the quadric $\mathcal{Q}(3, q^2)$ in case this is an elliptic quadric. The number of lines of $P\mathcal{H}(2, q^2)$, not contained in $T_P(\mathcal{Q}(3, q^2))$, is $q^3 + 1 - (q + 1) = q^3 - q$ or $q^3 + 1 - 1 = q^3$ depending on whether this plane contains $q + 1$ lines or one line of $P\mathcal{H}(2, q^2)$. Then

$$|P\mathcal{H}(2, q^2) \cap \mathcal{Q}(3, q^2)| \leq 2q^2 + (q^3 - q) + 1 = q^3 + 2q^2 - q + 1,$$

in case the tangent plane $T_P(\mathcal{Q}(3,q^2))$ contains two lines of $\mathcal{Q}(3,q^2) \cap H$. All the other cases lead to smaller upper bounds on the intersection size.

$P \notin \mathcal{Q}(3,q^2)$

Any line through P in the cone $P\mathcal{H}(2,q^2)$ contains at most two points of the quadric $\mathcal{Q}(3,q^2)$, then

$$|P\mathcal{H}(2,q^2) \cap \mathcal{Q}(3,q^2)| \leq 2(q^3+1) = 2q^3+2.$$

2.5.3 $H = L\mathcal{H}(1,q^2)$

This Hermitian variety is the union of $q+1$ planes through the line L.

$L \cap \mathcal{Q}(3,q^2) = \emptyset$

No plane of $L\mathcal{H}(1,q^2)$ can contain a line or two lines of $\mathcal{Q}(3,q^2)$, for in this case there would be at least one intersection point belonging to L, so such a plane contains at most q^2+1 points of $\mathcal{Q}(3,q^2)$. Consequently,

$$|L\mathcal{H}(1,q^2) \cap \mathcal{Q}(3,q^2)| \leq (q^2+1)(q+1) = q^3+q^2+q+1.$$

$L \cap \mathcal{Q}(3,q^2) = \{P\}$

Since L only shares the point P with $\mathcal{Q}(3,q^2)$, it is a tangent line to $\mathcal{Q}(3,q^2)$, and so it could be that one of the planes of the cone $L\mathcal{H}(1,q^2)$ is the tangent plane $T_P(\mathcal{Q}(3,q^2))$ to $\mathcal{Q}(3,q^2)$ in P.

Consider this tangent plane $T_P(\mathcal{Q}(3,q^2))$. Then $T_P(\mathcal{Q}(3,q^2)) \cap \mathcal{Q}(3,q^2) = P\mathcal{Q}(1,q^2)$, where $\mathcal{Q}(1,q^2)$ is of the same type as the quadric $\mathcal{Q}(3,q^2)$. If a plane of $L\mathcal{H}(1,q^2)$ is equal to $T_P(\mathcal{Q}(3,q^2))$, then, as in the previous subsection, it contains at most $2q^2$ extra points of the intersection, otherwise it contains at most q^2 extra points of the intersection. This implies that

$$|L\mathcal{H}(1,q^2) \cap \mathcal{Q}(3,q^2)| \leq 2q^2 + q \cdot q^2 + 1 = q^3 + 2q^2 + 1.$$

$L \cap \mathcal{Q}(3, q^2) = \{P, R\}$

Here, at most two planes of the cone $L\mathcal{H}(1, q^2)$ could be tangent planes $T_{P'}(\mathcal{Q}(3, q^2))$ and $T_{R'}(\mathcal{Q}(3, q^2))$ since the polar line of L with respect to $\mathcal{Q}(3, q^2)$ is a line L' intersecting $\mathcal{Q}(3, q^2)$ in at most two points P' and R'. This maximum is attained if $\mathcal{Q}(3, q^2)$ is a hyperbolic quadric.

Using the same arguments as in the previous case, we can have that $T_{P'}(\mathcal{Q}(3, q^2))$ and $T_{R'}(\mathcal{Q}(3, q^2))$ are two of the $q + 1$ planes of $L\mathcal{H}(1, q^2)$ through L and then

$$|L\mathcal{H}(1, q^2) \cap \mathcal{Q}(3, q^2)| \leq 2 \cdot (2q^2 - 1) + (q - 1) \cdot (q^2 - 1) + 2 = q^3 + 3q^2 - q + 1.$$

If at most one of the planes of the cone $L\mathcal{H}(1, q^2)$ is a tangent plane to $\mathcal{Q}(3, q^2)$, then the same arguments give a smaller upper bound on the intersection size.

$L \subset \mathcal{Q}(3, q^2)$

For every plane of $\mathcal{H}(3, q^2)$, there are at most q^2 extra intersection points and then

$$|L\mathcal{H}(1, q^2) \cap \mathcal{Q}(3, q^2)| \leq q^2 \cdot (q + 1) + q^2 + 1 = q^3 + 2q^2 + 1.$$

The following theorem is therefore valid.

Theorem 2.9. *Let $\mathcal{Q}(3, q^2)$ be a non-singular quadric in $\mathrm{PG}(3, q^2)$ and let $\mathcal{H}$ be an arbitrary Hermitian variety in $\mathrm{PG}(3, q^2)$, then*

$$|\mathcal{H} \cap \mathcal{Q}(3, q^2)| \leq 2q^3 + q^2 + 1 = \overline{W}_3.$$

2.6 The functional code $C_{Herm}(\mathcal{Q})$ for $N = 4$

Let $W_4 = q^5 + q^4 + 4q^3 - 3q + 1$. The following is a special case of Theorem 2.3:

Theorem 2.10. *Let $\mathcal{H}(4,q^2)$ be a non-singular Hermitian variety in* $\mathrm{PG}(4,q^2)$ *and let $\mathcal{Q}(4,q^2)$ be an arbitrary quadric in* $\mathrm{PG}(4,q^2)$. *If $|\mathcal{H}(4,q^2)\cap\mathcal{Q}(4,q^2)| > W_4$, then $\mathcal{Q}(4,q^2)$ is the union of two hyperplanes.*

Assume now that $\mathcal{Q}(4,q^2)$ is a non-singular quadric in $\mathrm{PG}(4,q^2)$ intersecting a Hermitian variety H in more than W_4 points, then the preceding theorem implies that H is singular. We therefore start a discussion depending on the dimension of the space of singular points of H.

2.6.1 $H = P\mathcal{H}(3,q^2)$

In this case, the Hermitian variety is the union of $|\mathcal{H}(3,q^2)|$ lines through the point P.

$P \in \mathcal{Q}(4,q^2)$

In this case, the tangent hyperplane $T_P(\mathcal{Q}(4,q^2))$ intersects the quadric $\mathcal{Q}(4,q^2)$ in a cone $P\mathcal{Q}(2,q^2)$, where the conic $\mathcal{Q}(2,q^2)$ lies in a plane π. Consider $\mathcal{H}' = \pi \cap P\mathcal{H}(3,q^2)$. By Bézout's theorem, $|\mathcal{Q}(2,q^2)\cap\mathcal{H}'| \leq 2(q+1)$ whether π shares a non-singular Hermitian curve or a singular Hermitian curve consisting of $q+1$ concurrent lines with $P\mathcal{H}(3,q^2)$. All the points in this intersection correspond to lines through P contained in $\mathcal{Q}(4,q^2)\cap P\mathcal{H}(3,q^2)$. Then, in $T_P(\mathcal{Q}(4,q^2))$, $P\mathcal{H}(3,q^2)$ and $\mathcal{Q}(4,q^2)$ share at most

$$2(q+1)q^2+1$$

points. Every line in the cone $P\mathcal{H}(3,q^2)$, that is not contained in $T_P(\mathcal{Q}(4,q^2))$, contains one extra point of the quadric $\mathcal{Q}(4,q^2)$. The number of such lines is at most

$$|\mathcal{H}(3,q^2)| - (q^3+1) = (1+q^2)(q^3+1) - q^3 - 1 = q^5+q^2,$$

with equality in the case that $\pi\cap\mathcal{H}'$ is a Hermitian curve. Then

$$|P\mathcal{H}(3,q^2)\cap\mathcal{Q}(4,q^2)| \leq q^5+q^2+2q^3+2q^2+1 = q^5+2q^3+3q^2+1 < W_4.$$

Note that this example exists with equality; there exist conics and Hermitian curves in $\mathrm{PG}(2,q^2)$ sharing $2(q+1)$ points.

$P \notin \mathcal{Q}(4,q^2)$

Suppose that

$$|P\mathcal{H}(3,q^2) \cap \mathcal{Q}(4,q^2)| > q^5 + 2q^4 - \frac{1}{3}q^3 + 2q^2 + q + 1 = \overline{W}_4.$$

In the following arguments, we fix a particular basis of the cone $P\mathcal{H}(3,q^2)$. Let M be a line of $\mathcal{H}(3,q^2)$. Consider the q^3+q lines of $\mathcal{H}(3,q^2)$ intersecting M. They define q^3+q planes through P. A plane intersects $\mathcal{Q}(4,q^2)$ in one point, q^2+1 points (line or conic) or $2q^2+1$ points (two lines). Let α_M be the number of points in the intersection $\mathcal{Q}(4,q^2) \cap \langle P, M\rangle$.

First of all, we determine a lower bound on the number of planes through P sharing two lines with $\mathcal{Q}(4,q^2)$. If all these q^3+q planes contain at most q^2+1 points of $\mathcal{Q}(4,q^2)$, then there still remain more than

$$\overline{W}_4 - \left[(q^3+q)(q^2+1) - (q-1)\alpha_M\right]$$

extra points in the intersection, since we count every one of the α_M intersection points precisely q times. So at least

$$(\overline{W}_4 - (q^3+q)(q^2+1) + (q-1)\alpha_M)/q^2$$

of the q^3+q planes share two lines with $\mathcal{Q}(4,q^2)$.

We can repeat this argument for all the lines M of $\mathcal{H}(3,q^2)$, of which there are q^4+q^3+q+1. A plane is counted at most q^3+q times. So, taking the sum over all lines M of the fixed basis $\mathcal{H}(3,q^2)$,

we have at least

$$\begin{aligned}
&\frac{1}{q^2(q^3+q)} \sum_{M\in\mathcal{H}(3,q^2)} \left(\overline{W}_4 - (q^3+q)(q^2+1) + (q-1)\alpha_M\right) \\
&= \frac{1}{q^2(q^3+q)} \left((q^4+q^3+q+1)(\overline{W}_4 - (q^3+q)(q^2+1)) + (q-1) \sum_{M\in\mathcal{H}(3,q^2)} \alpha_M \right) \\
&> \frac{1}{q^2(q^3+q)} \left((q^4+q^3+q+1)(\overline{W}_4 - (q^3+q)(q^2+1)) + (q-1)(q+1)\overline{W}_4 \right) \\
&= \frac{q^4+q^3+q^2+q}{q^2(q^3+q)}\overline{W}_4 - \frac{(q+1)(q^2+1)(q^3+1)}{q^2} \\
&= \frac{q+1}{q^2}(q^5+2q^4-\frac{1}{3}q^3+2q^2+q+1) - \frac{(q+1)(q^2+1)(q^3+1)}{q^2} \\
&> 2q^3+\frac{2}{3}q^2-\frac{1}{3}q+2
\end{aligned}$$

planes of $P\mathcal{H}(3,q^2)$ containing two lines of $\mathcal{Q}(4,q^2)$.

Remark 2.11. *There is a point $R \in \mathcal{H}(3,q^2)$ contained in at least three lines of $\mathcal{H}(3,q^2)$ such that the planes through these lines and P contain two lines of $\mathcal{Q}(4,q^2)$.*

Proof. If every point of $\mathcal{H}(3,q^2)$ belongs to at most two of these lines, then we will have at most $2q^3+2$ such lines, but according to the calculations above, there are at least $2q^3+\frac{2}{3}q^2-\frac{1}{3}q+2$ such lines. □

Let R be one of these points lying on at least three lines of $\mathcal{H}(3,q^2)$ such that the planes through these lines and P contain two lines of $\mathcal{Q}(4,q^2)$.

Lemma 2.12. *The line PR is tangent to $\mathcal{Q}(4,q^2)$, so these six lines of $\mathcal{Q}(4,q^2)$ in the planes of $P\mathcal{H}(3,q^2)$ through PR all pass through the same point of PR.*

Proof. The quadric $\mathcal{Q}(4,q^2)$ intersects the 3-space $\langle P, T_R(\mathcal{H}(3,q^2))\rangle$ in either a non-singular hyperbolic quadric $\mathcal{Q}^+(3,q^2)$, a non-singular elliptic quadric $\mathcal{Q}^-(3,q^2)$ or a cone $S\mathcal{Q}(2,q^2)$. Since there are lines of $\mathcal{Q}(4,q^2)$ in this 3-space, the quadric $\mathcal{Q}^-(3,q^2)$ is not possible. Since three planes through PR share two lines with $\mathcal{Q}(4,q^2)$, and no more than two points of PR can belong to these six lines, then there is at least a point of PR which lies on three of these six lines. This eliminates the quadric $\mathcal{Q}^+(3,q^2)$. Then all these six lines lie on a cone $S\mathcal{Q}(2,q^2)$, so they all pass through S and $PR \cap \mathcal{Q}(4,q^2) = \{S\}$ since some point of $PR \cap \mathcal{Q}(4,q^2)$ lies on at least three lines of this cone $S\mathcal{Q}(2,q^2)$. □

Lemma 2.13. *Let M be a line of $\mathcal{H}(3,q^2)$ defining a plane $\langle P, M\rangle$ intersecting $\mathcal{Q}(4,q^2)$ in two lines. Then M contains at most one point R of the type described in Remark 2.11.*

Proof. The plane $\langle P, M\rangle$ shares two lines M' and M'' with $\mathcal{Q}(4,q^2)$. The point R can only be the intersection point of the two lines M and $\langle P, M' \cap M''\rangle$. □

Lemma 2.14. *Let $\mathcal{L}$ be the set of lines M of $\mathcal{H}(3,q^2)$ defining a plane $\langle P, M\rangle$ that intersects $\mathcal{Q}(4,q^2)$ in two lines. Then*

$$A = |\mathcal{L}| \leq 2q^3 + \frac{2}{3}q^2 - \frac{1}{3}q + 2.$$

Proof. Let $\mathcal{P}$ be the set of points of $\mathcal{H}(3,q^2)$ lying on at least three lines of $\mathcal{L}$ and denote $|\mathcal{P}| = \alpha$. Let β be the number of points of $\mathcal{H}(3,q^2)$ lying on at most two lines of $\mathcal{L}$. On the one hand,

$$(q+1)\alpha + 2\beta \geq (q^2+1)A.$$

Since $\beta = |\mathcal{H}(3,q^2)| - \alpha = q^5 + q^3 + q^2 + 1 - \alpha$, we can rewrite this as

$$\begin{aligned} \alpha(q-1) + 2(q^5+q^3+q^2+1) &\geq A(q^2+1), \\ \alpha \geq \frac{A(q^2+1) - 2(q^5+q^3+q^2+1)}{q-1}&. \end{aligned}$$

On the other hand, we know that every point of $\mathcal{P}$ lies on at least three lines of $\mathcal{L}$, but every line of $\mathcal{L}$ contains at most one point of $\mathcal{P}$ by the previous remark. Hence, $3\alpha \leq A$.

Combining both inequalities, we find

$$\begin{aligned} A &\geq 3\frac{A(q^2+1)-2(q^5+q^3+q^2+1)}{q-1} \\ \Rightarrow A &\leq 2q^3+\frac{2}{3}q^2-\frac{1}{3}q+2 \end{aligned}$$

□

The result of Lemma 2.14 contradicts the result of the calculations just above Remark 2.11. Hence, the assumption we made at the beginning of this subsection was wrong. Then

$$|P\mathcal{H}(3,q^2)\cap\mathcal{Q}(4,q^2)| \leq q^5+2q^4-\frac{1}{3}q^3+2q^2+q+1 = \overline{W}_4.$$

2.6.2 $H = L\mathcal{H}(2,q^2)$

In this case, H is the union of q^3+1 planes through L and a point of a non-singular Hermitian curve $\mathcal{H}(2,q^2)$ in a plane π skew to L.

$L\cap\mathcal{Q}(4,q^2)=\emptyset$

In this case, all the planes through L share at most a conic with $\mathcal{Q}(4,q^2)$, then we have

$$|L\mathcal{H}(2,q^2)\cap\mathcal{Q}(4,q^2)| \leq (q^3+1)(q^2+1) = q^5+q^3+q^2+1 < \overline{W}_4.$$

$L\cap\mathcal{Q}(4,q^2)=\{P\}$

Since the line L is a tangent line to $\mathcal{Q}(4,q^2)$, necessarily $\pi \not\subseteq T_P(\mathcal{Q}(4,q^2))$.

Consider the tangent hyperplane $T_P(\mathcal{Q}(4,q^2))$ to P which intersects the quadric $\mathcal{Q}(4,q^2)$ in a cone $P\mathcal{Q}(2,q^2)$. Denote the intersection line $\pi\cap T_P(\mathcal{Q}(4,q^2))$ by r. If r is a tangent line to $\mathcal{H}(2,q^2)$, then

$|r \cap \mathcal{Q}(2,q^2) \cap \mathcal{H}(2,q^2)| \leq 1$. Since $T_P(\mathcal{Q}(4,q^2)) \cap \mathcal{Q}(4,q^2)$ is a cone $P\mathcal{Q}(2,q^2)$, there is at most one plane through L of the Hermitian variety $L\mathcal{H}(2,q^2)$ containing lines of this tangent cone. All the other $q^3 \cdot q^2$ lines of $L\mathcal{H}(2,q^2)$ through P, those not contained in $T_P(\mathcal{Q}(4,q^2))$, contain precisely one extra point of the quadric $\mathcal{Q}(4,q^2)$. Consequently, the following upper bound arises

$$|L\mathcal{H}(2,q^2) \cap \mathcal{Q}(4,q^2)| \leq 2q^2 + q^3q^2 + 1 = q^5 + 2q^2 + 1 < \overline{W}_4.$$

If r is a secant line to $\mathcal{H}(2,q^2)$, then $|r \cap \mathcal{Q}(2,q^2) \cap \mathcal{H}(2,q^2)| \leq 2$. Since $T_P(\mathcal{Q}(4,q^2)) \cap \mathcal{Q}(4,q^2)$ is a cone $P\mathcal{Q}(2,q^2)$, there are at most two planes through L of the Hermitian variety $L\mathcal{H}(2,q^2)$ containing lines of this tangent cone. All the other $(q^3-q)q^2$ lines of $L\mathcal{H}(2,q^2)$ through P, those not contained in $T_P(\mathcal{Q}(4,q^2))$, contain precisely one extra point of the quadric $\mathcal{Q}(4,q^2)$. Consequently, the following upper bound arises

$$|L\mathcal{H}(2,q^2) \cap \mathcal{Q}(4,q^2)| \leq 2 \cdot 2q^2 + (q^3-q)q^2 + 1 = q^5 - q^3 + 4q^2 + 1 < \overline{W}_4.$$

$L \cap \mathcal{Q}(4,q^2) = \{P, R\}$

Lines contained in the intersection $\mathcal{Q}(4,q^2) \cap L\mathcal{H}(2,q^2)$ pass through P or R, so lie in $T_P(\mathcal{Q}(4,q^2))$ or in $T_R(\mathcal{Q}(4,q^2))$. We apply the same arguments as in the previous case. We can assume $\pi = T_P(\mathcal{Q}(4,q^2)) \cap T_R(\mathcal{Q}(4,q^2))$ since both hyperplanes intersect L only in P or in R. Then by Bézouts theorem, there are at most $2(q+1)$ planes through L containing lines of the intersection, all the other planes through L, at least $q^3 - 2q - 1$ of them, contain $q^2 - 1$ extra points. Consequently,

$$|L\mathcal{H}(2,q^2) \cap \mathcal{Q}(4,q^2)| \leq 2(q+1) \cdot (2q^2-1) + (q^3-2q-1)(q^2-1) + 2 = q^5 + q^3 + 3q^2 + 1 < \overline{W}_4.$$

$L \subset \mathcal{Q}(4, q^2)$

Every plane through L contains at most one extra line of the quadric $\mathcal{Q}(4, q^2)$, then

$$|L\mathcal{H}(2, q^2) \cap \mathcal{Q}(4, q^2)| \leq \underbrace{(q^3+1)}_{|\mathcal{H}(2,q^2)|} q^2 + \underbrace{q^2+1}_{|L|} = q^5 + 2q^2 + 1 < \overline{W}_4.$$

2.6.3 $H = \pi\mathcal{H}(1, q^2)$

In this case, the Hermitian variety $\pi\mathcal{H}(1, q^2)$ is composed of $q+1$ hyperplanes through π. The plane π can contain one, q^2+1 or $2q^2+1$ points of $\mathcal{Q}(4, q^2)$.

1. $\pi \cap \mathcal{Q}(4, q^2) = \{P\}$: every hyperplane of $\pi\mathcal{H}(1, q^2)$ contains at most $q^4 + q^2$ extra points of the intersection since such a hyperplane cannot intersect $\mathcal{Q}(4, q^2)$ in a non-singular hyperbolic quadric $\mathcal{Q}^+(3, q^2)$. So

$$|\pi\mathcal{H}(1, q^2) \cap \mathcal{Q}(4, q^2)| \leq (q+1)(q^4+q^2) + 1 = q^5 + q^4 + q^3 + q^2 + 1 < \overline{W}_4.$$

2. $|\pi \cap \mathcal{Q}(4, q^2)| = q^2 + 1$: every hyperplane of $\pi\mathcal{H}(1, q^2)$ contains at most $q^4 + q^2$ extra points of the intersection. So

$$|\pi\mathcal{H}(1, q^2) \cap \mathcal{Q}(4, q^2)| \leq (q+1)(q^4+q^2) + q^2 + 1 = q^5 + q^4 + q^3 + 2q^2 + 1 < \overline{W}_4.$$

3. $|\pi \cap \mathcal{Q}(4, q^2)| = 2q^2 + 1$: every hyperplane of $\pi\mathcal{H}(1, q^2)$ contains at most q^4 extra points of the intersection. So

$$|\pi\mathcal{H}(1, q^2) \cap \mathcal{Q}(4, q^2)| \leq (q+1)q^4 + 2q^2 + 1 = q^5 + q^4 + 2q^2 + 1 < \overline{W}_4.$$

2.6.4 $H = \pi_3$

In this case, the Hermitian variety H equals a hyperplane π_3. Obviously, the maximal intersection of one hyperplane with the quadric cannot be larger than the maximal intersection of $q+1$ hyperplanes with the quadric. Hence, by the preceding case, $|\pi_3 \cap \mathcal{Q}(4,q^2)| < \overline{W}_4$.

2.6.5 Conclusion

Resuming the results of this section, we can state the following theorem.

Theorem 2.15. *Let $\mathcal{Q}(4,q^2)$ be a non-singular quadric in $\mathrm{PG}(4,q^2)$ and let H be an arbitrary Hermitian variety in $\mathrm{PG}(4,q^2)$. Then $|\mathcal{Q}(4,q^2) \cap H| \leq \overline{W}_4 = q^5 + 2q^4 - \frac{1}{3}q^3 + 2q^2 + q + 1$. Hence, the minimum distance of the code $C_{Herm}(\mathcal{Q}(4,q^2))$ is at least $|\mathcal{Q}(4,q^2)| - \overline{W}_4 = q^6 - q^5 - q^4 + \frac{1}{3}q^3 - q^2 - q$.*

2.7 The functional code $C_{Herm}(\mathcal{Q})$ for $N \geq 5$

We now determine upper bounds on the intersection size of a non-singular quadric $\mathcal{Q}(N,q^2)$ in $\mathrm{PG}(N,q^2)$ with an arbitrary Hermitian variety H in $\mathrm{PG}(N,q^2)$. By Theorem 2.6, if the intersection size is more than W_N, then the Hermitian variety H must be singular. As in four dimensions, we present a discussion based on the dimension of the space of singular points of H. Let

$$\overline{W}_N = \begin{cases} q^7 + 2q^6 + 2q^5 - \frac{1}{2}q^4 - \frac{21}{4}q^3 + \frac{15}{8}q^2 + \frac{195}{16}q + 8, & N = 5 \text{ and } q > 2\,, \\ q^9 + q^8 + 3q^7 + 3q^6 - q^5 - 3q^4 - 4q^3 + 5q^2 + 16q + 16, & N = 6 \text{ and } q = 2\,, \\ W_N & \text{else}\,, \end{cases}$$

for $N \geq 5$. Note that $\overline{W}_N \geq W_N$ for each $N \geq 5$. Hence, if the Hermitian variety H intersects $\mathcal{Q}(N,q^2)$ in more than $\overline{W}_N$ points, it must be singular.

2.7.1 $H = P\mathcal{H}(N-1, q^2)$

$P \in \mathcal{Q}(N, q^2)$

Let $T_P(\mathcal{Q}(N, q^2))$ be the tangent hyperplane to the quadric $\mathcal{Q}(N, q^2)$. Then $T_P(\mathcal{Q}(N, q^2)) \cap \mathcal{Q}(N, q^2) = P\mathcal{Q}(N-2, q^2)$, where $\mathcal{Q}(N-2, q^2)$ is of the same type as the quadric $\mathcal{Q}(N, q^2)$. Then the intersection contains all points of the lines through P and a point of $\mathcal{Q}(N-2, q^2) \cap \mathcal{H}(N-2, q^2)$ or $\mathcal{Q}(N-2, q^2) \cap R\mathcal{H}(N-3, q^2)$, whereby $\mathcal{H}(N-2, q^2)$ or $R\mathcal{H}(N-3, q^2)$ is the intersection of H with the $(N-2)$-space containing the base $\mathcal{Q}(N-2, q^2)$. By induction on the dimension N, the results on the code $C_{Herm}(\mathcal{Q}(N-2, q^2))$ show that this intersection contains at most $\overline{W}_{N-2}$ points, not depending on the case. All the other lines through P of the tangent hyperplane $T_P(\mathcal{Q}(N, q^2))$ have no extra points of the intersection. The other lines through P of the Hermitian variety $P\mathcal{H}(N-1, q^2)$ contain one extra point of the quadric $\mathcal{Q}(N, q^2)$. There are either

$$\begin{aligned} |\mathcal{H}(N-1, q^2) \setminus \mathcal{H}(N-2, q^2)| &= \frac{(q^N + (-1)^{N-1})(q^{N-1} + (-1)^N)}{q^2 - 1} \\ &\quad - \frac{(q^{N-1} + (-1)^{N-2})(q^{N-2} + (-1)^{N-1})}{q^2 - 1} \\ &\leq q^{2N-3} + q^{N-2} \end{aligned}$$

such points, or

$$\begin{aligned} |\mathcal{H}(N-1, q^2) \setminus R\mathcal{H}(N-3, q^2)| &= \frac{(q^N + (-1)^{N-1})(q^{N-1} + (-1)^N)}{q^2 - 1} \\ &\quad - q^2 \frac{(q^{N-2} + (-1)^{N-3})(q^{N-3} + (-1)^{N-2})}{q^2 - 1} - 1 \\ &= q^{2N-3} \end{aligned}$$

such points.

Hence, in this case,

1. if $N = 5$, then

$$\begin{aligned}|P\mathcal{H}(N-1,q^2)\cap\mathcal{Q}(N,q^2)| &\leq \overline{W}_{N-2}q^2+(q^{2N-3}+q^{N-2})+1\\ &= \overline{W}_3q^2+(q^7+q^3)+1\\ &= (2q^3+q^2+1)q^2+(q^7+q^3)+1\\ &= q^7+2q^5+q^4+q^3+q^2+1<\overline{W}_5\,,\end{aligned}$$

2. if $N \geq 6$, then

$$\begin{aligned}|P\mathcal{H}(N-1,q^2)\cap\mathcal{Q}(N,q^2)| &\leq \overline{W}_{N-2}q^2+(q^{2N-3}+q^{N-2})+1\\ &< q^2(q^{2N-7}+2q^{2N-8}+4q^{2N-9})+q^{2N-3}+q^{N-2}+1\\ &< q^{2N-3}+q^{2N-5}+2q^{2N-6}+5q^{2N-7}<\overline{W}_N.\end{aligned}$$

$P \notin \mathcal{Q}(N,q^2)$

The arguments are the same for N odd and N even. We again fix a particular base $\mathcal{H}(N-1,q^2)$ of the cone $P\mathcal{H}(N-1,q^2)$.

Let M be a given line of $\mathcal{H}(N-1,q^2)$. This line M corresponds to a plane $\langle P,M\rangle$ through P. Any plane through P intersects the quadric $\mathcal{Q}(N,q^2)$ in 1, q^2+1 or $2q^2+1$ points. This last case occurs when the intersection equals two lines. We say that a line M is of type (2) if the plane $\langle P,M\rangle$ contains $2q^2+1$ points of the quadric $\mathcal{Q}(N,q^2)$.

Lemma 2.16. *If $|P\mathcal{H}(N-1,q^2)\cap\mathcal{Q}(N,q^2)| > \overline{W}_N$, there are at least $\frac{a_N}{b_N}\overline{W}_N - c_N$ lines of type (2) in*

$\mathcal{H}(N-1,q^2)$, *with*

$$\begin{aligned}
a_N &= (|\mathcal{H}(N-1,q^2)| + (q^2+1)(|\mathcal{H}(N-3,q^2)|-2)) \cdot |\mathcal{H}(N-3,q^2)|\,,\\
b_N &= q^2(q^2+1)^2(|\mathcal{H}(N-3,q^2)|-1)\,,\\
c_N &= \frac{|\mathcal{H}(N-1,q^2)| \cdot |\mathcal{H}(N-3,q^2)|}{q^2}\,.
\end{aligned}$$

Proof. Let M be a given line of $\mathcal{H}(N-1,q^2)$. The number of lines of $\mathcal{H}(N-1,q^2)$ which intersect M in one point equals $(q^2+1)(|\mathcal{H}(N-3,q^2)|-1)$. Let α_M be the number of points in the intersection of the plane $\langle P,M\rangle$ and $P\mathcal{H}(N-1,q^2)\cap\mathcal{Q}(N,q^2)$. An easy counting argument shows that for at least

$$\frac{\overline{W}_N-(q^2+1)^2(|\mathcal{H}(N-3,q^2)|-1)+(|\mathcal{H}(N-3,q^2)|-2)\alpha_M}{q^2}$$

lines M' of $\mathcal{H}(N-1,q^2)$ intersecting M, the plane $\langle P,M'\rangle$ contains two lines of the quadric $\mathcal{Q}(N,q^2)$.

We can repeat the same argument for all the lines of $\mathcal{H}(N-1,q^2)$, of which there are

$$\frac{|\mathcal{H}(N-1,q^2)| \cdot |\mathcal{H}(N-3,q^2)|}{q^2+1}.$$

In order to count the total number of lines of type (2), we sum over all lines in $\mathcal{H}(N-1,q^2)$. In this way, every such line is counted $(q^2+1)(|\mathcal{H}(N-3,q^2)|-1)$ times. Hence, the total number of lines of

type (2) is at least

$$\begin{aligned}
&\sum_{M\subseteq\mathcal{H}(N-1,q^2)} \frac{\overline{W}_N-(q^2+1)^2(|\mathcal{H}(N-3,q^2)|-1)+(|\mathcal{H}(N-3,q^2)|-2)\alpha_M}{q^2(q^2+1)(|\mathcal{H}(N-3,q^2)|-1)}\\
&=\frac{|\mathcal{H}(N-1,q^2)|\cdot|\mathcal{H}(N-3,q^2)|\cdot(\overline{W}_N-(q^2+1)^2(|\mathcal{H}(N-3,q^2)|-1))}{q^2(q^2+1)^2(|\mathcal{H}(N-3,q^2)|-1)}\\
&\quad+\frac{|\mathcal{H}(N-3,q^2)|-2}{q^2(q^2+1)(|\mathcal{H}(N-3,q^2)|-1)}\sum_{M\subseteq\mathcal{H}(N-1,q^2)}\alpha_M\\
&\geq\frac{|\mathcal{H}(N-1,q^2)|\cdot|\mathcal{H}(N-3,q^2)|}{q^2(q^2+1)^2(|\mathcal{H}(N-3,q^2)|-1)}\overline{W}_N-\frac{|\mathcal{H}(N-1,q^2)|\cdot|\mathcal{H}(N-3,q^2)|}{q^2}\\
&\quad+\frac{(|\mathcal{H}(N-3,q^2)|-2)\cdot|\mathcal{H}(N-3,q^2)|}{q^2(q^2+1)(|\mathcal{H}(N-3,q^2)|-1)}\overline{W}_N\\
&=\frac{(|\mathcal{H}(N-1,q^2)|+(q^2+1)(|\mathcal{H}(N-3,q^2)|-2))\cdot|\mathcal{H}(N-3,q^2)|}{q^2(q^2+1)^2(|\mathcal{H}(N-3,q^2)|-1)}\overline{W}_N\\
&\quad-\frac{|\mathcal{H}(N-1,q^2)|\cdot|\mathcal{H}(N-3,q^2)|}{q^2}.
\end{aligned}$$

In the penultimate step, we made use of the fact that every intersection point lies on $|\mathcal{H}(N-3,q^2)|$ planes through P of $P\mathcal{H}(N-1,q^2)$, hence is counted $|\mathcal{H}(N-3,q^2)|$ times. □

We define

$$\delta_N=\begin{cases}1+q^2|\mathcal{Q}^+(N-4,q^2)|\,, & \text{for } N \text{ odd},\\ |\mathcal{Q}^+(N-3,q^2)|\,, & \text{for } N \text{ even},\end{cases}$$

whereby $\mathcal{Q}^+(N-4,q^2)$ and $\mathcal{Q}^+(N-3,q^2)$ are non-singular hyperbolic quadrics in respectively $N-4$ and $N-3$ dimensions.

Lemma 2.17. *Assume that the number of lines of type (2) is larger than* $\frac{|\mathcal{H}(N-1,q^2)|\delta_N}{q^2+1}$. *Then there exists a point* $R\in\mathcal{H}(N-1,q^2)$ *such that* $R\mathcal{H}(N-3,q^2)=T_R(\mathcal{H}(N-1,q^2))\cap\mathcal{H}(N-1,q^2)$ *contains at least* δ_N+1 *lines of type (2) in* $\mathcal{H}(N-1,q^2)$ *and through* R.

Proof. Every line through R of the cone $R\mathcal{H}(N-3,q^2)$ lies in q^2+1 of such tangent cones to the Hermitian variety $\mathcal{H}(N-1,q^2)$. If every cone has at most δ_N lines of type (2), then the total number

of such lines would be at most

$$\frac{|\mathcal{H}(N-1,q^2)|\delta_N}{q^2+1},$$

a contradiction. □

From now on, in this subsection, we assume that the number of lines of type (2) is larger than $\frac{|\mathcal{H}(N-1,q^2)|\delta_N}{q^2+1}$. We will see at the end that this is no problem. Let R be one of the points fulfilling the requirements of the previous lemma.

Lemma 2.18. *There exists a point $S \in \mathcal{Q}(N,q^2)$ such that $\langle P, T_R(\mathcal{H}(N-1,q^2))\rangle \cap \mathcal{Q}(N,q^2) = S\mathcal{Q}(N-2,q^2)$.*

Proof. Remark that $\delta_N \geq |\mathcal{Q}(N-3,q^2)|$ and $\delta_N \geq 1+q^2|\mathcal{Q}(N-4,q^2)|$ for any non-singular quadric $\mathcal{Q}(N-3,q^2)$ and $\mathcal{Q}(N-4,q^2)$, as well in case N is even, as in case N is odd.

Let Q be the $(N-1)$-dimensional quadric $\langle P, T_R(\mathcal{H}(N-1,q^2))\rangle \cap \mathcal{Q}(N,q^2)$. This quadric Q either is a non-singular quadric, or a singular quadric with vertex a point. We wish to show that only the last possibility occurs, that the line PR only shares one point S with Q and that the point S is the vertex of this singular quadric.

Assume first that the quadric Q is non-singular. Then every point of Q lies on $|\mathcal{Q}(N-3,q^2)|$ lines of Q, whereby $\mathcal{Q}(N-3,q^2)$ has the same type as Q. In any case, $|\mathcal{Q}(N-3,q^2)| \leq \delta_N$. The line PR however intersects $\mathcal{Q}(N,q^2)$ in either one or two points since this line PR is contained in at least one plane intersecting $\mathcal{Q}(N,q^2)$ in two lines, but $P \notin \mathcal{Q}(N,q^2)$. These intersection points therefore lie on at least δ_N+1 lines of Q, but then we have a contradiction.

So the quadric Q is singular with a point S as vertex and a non-singular $(N-2)$-dimensional quadric $\mathcal{Q}(N-2,q^2)$ as base. We show that this point S belongs to the line PR and that this point S is the only intersection point of the line PR with the quadric $\mathcal{Q}(N,q^2)$. Again, the line PR shares one or two

points with the quadric $\mathcal{Q}(N, q^2)$. Assume that these, one or two, intersection points are non-singular, then they belong to at most $1 + q^2|\mathcal{Q}(N-4, q^2)|$ lines of the quadric Q, whereby $\mathcal{Q}(N-4, q^2)$ has the same type as $\mathcal{Q}(N-2, q^2)$. But, in any case, this number of lines is smaller than $\delta_N + 1$. So the line PR contains the vertex S of the quadric Q contained in $\mathcal{Q}(N, q^2)$. □

Remark 2.19. *Let M be a line of $\mathcal{H}(N-1, q^2)$ defining a plane $\langle P, M\rangle$ intersecting $\mathcal{Q}(N, q^2)$ in two lines. Then M contains at most one point R of the type described in Lemma 2.17.*

Proof. This line M defines a plane $\langle P, M\rangle$ intersecting $\mathcal{Q}(N, q^2)$ in two lines M' and M''. The point S is the intersection point of the lines M' and M''. The point $R = SP \cap M$ is the only point that can be the one described in Lemma 2.17. □

Lemma 2.20. *The number of lines of type (2) is at most*

$$d_N = \frac{\delta_N(\delta_N+1)\,|\mathcal{H}(N-1, q^2)|}{(q^2+2)\delta_N + q^2 + 1 - |\mathcal{H}(N-3, q^2)|}\,.$$

Proof. Let A be the number of lines of type (2). Define $\mathcal{P}$ as the set of points on $\mathcal{H}(N-1, q^2)$ lying on at least $\delta_N + 1$ lines of type (2), and denote $\alpha = |\mathcal{P}|$. Let β be the number of points of $\mathcal{H}(N-1, q^2)$ lying on at most δ_N lines of type (2). Then, using a double counting argument, we find

$$\alpha|\mathcal{H}(N-3, q^2)| + \beta\delta_N \geq A(q^2+1)\,.$$

Since $\alpha + \beta = |\mathcal{H}(N-1, q^2)|$, we can rewrite this as

$$\alpha \geq \frac{A(q^2+1) - \delta_N|\mathcal{H}(N-1, q^2)|}{|\mathcal{H}(N-3, q^2)| - \delta_N}\,.$$

Now, using the previous remark and a double counting argument, we also find

$$A \geq (\delta_N + 1)\alpha\,.$$

Combining both inequalities, we find

$$A \geq (\delta_N + 1) \cdot \frac{A(q^2+1) - \delta_N |\mathcal{H}(N-1,q^2)|}{|\mathcal{H}(N-3,q^2)| - \delta_N}\,.$$

It follows immediately that

$$A \leq \frac{\delta_N(\delta_N+1)\,|\mathcal{H}(N-1,q^2)|}{(q^2+2)\delta_N + q^2 + 1 - |\mathcal{H}(N-3,q^2)|}.$$

It should be noted that this deduction does not hold if $N = 5$ and $q = 2$ since $|\mathcal{H}(2,2^2)| = 9 = \delta_5$ in this case. From the first inequality and the result $\alpha + \beta = |\mathcal{H}(N-1,q^2)|$ however, if follows immediately that $A \leq 165$. Hence, the final inequality is definitely valid. □

Remark that

$$\frac{|\mathcal{H}(N-1,q^2)|\delta_N}{q^2+1} \leq \frac{\delta_N(\delta_N+1)\,|\mathcal{H}(N-1,q^2)|}{(q^2+2)\delta_N + q^2 + 1 - |\mathcal{H}(N-3,q^2)|},$$

since $\delta_N \leq |\mathcal{H}(N-3,q^2)|$. Hence, the condition that the number of lines of type (2) must be larger than $\frac{|\mathcal{H}(N-1,q^2)|\delta_N}{q^2+1}$ is redundant in the following.

We now compare the results of Lemma 2.16 and Lemma 2.20. We find a contradiction if $d_N < \frac{a_N}{b_N}\overline{W}_N - c_N$. Equivalently, if $|P\mathcal{H}(N-1,q^2) \cap \mathcal{Q}(N,q^2)| > \overline{W}_N \geq \frac{b_N(c_N+d_N)}{a_N}$, with

$$\begin{aligned}
a_N &= (|\mathcal{H}(N-1,q^2)| + (q^2+1)(|\mathcal{H}(N-3,q^2)| - 2)) \cdot |\mathcal{H}(N-3,q^2)|\,,\\
b_N &= q^2(q^2+1)^2(|\mathcal{H}(N-3,q^2)| - 1)\,,\\
c_N &= \frac{|\mathcal{H}(N-1,q^2)| \cdot |\mathcal{H}(N-3,q^2)|}{q^2}\,,\\
d_N &= \frac{\delta_N(\delta_N+1)\,|\mathcal{H}(N-1,q^2)|}{(q^2+2)\delta_N + q^2 + 1 - |\mathcal{H}(N-3,q^2)|}\,.
\end{aligned}$$

For the small cases, the inequalities

$$\overline{W}_5 \geq q^7 + 2q^6 + 2q^5 - \frac{1}{2}q^4 - \frac{21}{4}q^3 + \frac{15}{8}q^2 + \frac{195}{16}q + 8\,,$$
$$\overline{W}_6 \geq q^9 + q^8 + 3q^7 + 3q^6 - q^5 - 3q^4 - 4q^3 + 5q^2 + 16q + 16\,,$$
$$\overline{W}_7 \geq q^{11} + q^{10} + 3q^9 + 2q^8 - q^7 - 3q^6 - 3q^5 + 9q^4 + 19q^3 + 3q^2 - 49q + 3\,.$$

are fulfilled. For $N \geq 8$, the inequality

$$\frac{b_N(c_N + d_N)}{a_N} < q^{2N-3} + q^{2N-4} + 4q^{2N-5} - 2q^{2N-7} + 2q^{2N-8} < \overline{W}_N$$

holds.

2.7.2 $H = L\mathcal{H}(N-2, q^2)$

In this case, $\mathcal{H}(N, q^2)$ is the union of $|\mathcal{H}(N-2, q^2)|$ planes through L.

$L \cap \mathcal{Q}(N, q^2) = \emptyset$

Each plane π through L, with $\pi \subset H$, contains at most a conic of $\mathcal{Q}(N, q^2)$. Then

$$\begin{aligned} |L\mathcal{H}(N-2, q^2) \cap \mathcal{Q}(N, q^2)| &\leq |\mathcal{H}(N-2, q^2)|(q^2+1) \\ &\leq (q^{2N-5} + 2q^{2N-7})(q^2+1) \\ &= q^{2N-3} + 3q^{2N-5} + 2q^{2N-7} < \overline{W}_N. \end{aligned}$$

$L \cap \mathcal{Q}(N, q^2) = \{P\}$

The tangent hyperplane $T_P(\mathcal{Q}(N, q^2))$ contains the line L, so intersects the base $\mathcal{H}(N-2, q^2)$ of the Hermitian variety $L\mathcal{H}(N-2, q^2)$ in an $(N-3)$-dimensional Hermitian variety H'. This intersection is either a non-singular Hermitian variety or a singular Hermitian variety with a point as vertex.

In both cases, the number $1 + q^2|H'|$ is a trivial upper bound on the number of intersection points of $\mathcal{Q}(N, q^2)$ and $L\mathcal{H}(N-2, q^2)$ in $T_P(\mathcal{Q}(N, q^2))$.

There are $|\mathcal{H}(N-2, q^2)| - |H'|$ other points in the base $\mathcal{H}(N-2, q^2)$. They all define, together with L, a plane contained in $L\mathcal{H}(N-2, q^2)$. Such a plane contains q^2 lines through P, not contained in $T_P(\mathcal{Q}(N, q^2))$. They all contain one extra point of $\mathcal{Q}(N, q^2)$. So, this gives $q^2(|\mathcal{H}(N-2, q^2)| - |H'|)$ extra intersection points.

In total, this gives at most $1+q^2|\mathcal{H}(N-2, q^2)| < \overline{W}_N$ intersection points for $\mathcal{Q}(N, q^2) \cap L\mathcal{H}(N-2, q^2)$.

$L \cap \mathcal{Q}(N, q^2) = \{P, R\}$

Let π_{N-2} contain the base $\mathcal{H}(N-2, q^2)$ of $L\mathcal{H}(N-2, q^2)$. Since $L \cap \mathcal{Q}(N, q^2) = \{P, R\}$, the vertex L is not contained in $T_P(\mathcal{Q}(N, q^2))$, so we can assume that π_{N-2} lies in $T_P(\mathcal{Q}(N, q^2))$.

Now, $\pi_{N-2} \cap \mathcal{Q}(N, q^2)$ is a non-singular quadric $\mathcal{Q}(N-2, q^2)$ of the same type as $\mathcal{Q}(N, q^2)$. By induction on N, the quadric $\mathcal{Q}(N-2, q^2)$ shares at most $\overline{W}_{N-2}$ points with a Hermitian variety in $N-2$ dimensions. So, this implies that there are at most $1 + q^2\overline{W}_{N-2}$ intersection points in $T_P(\mathcal{Q}(N, q^2))$.

Every point T of the base $\mathcal{H}(N-2, q^2)$ of $L\mathcal{H}(N-2, q^2)$ defines, together with L, a plane contained in $L\mathcal{H}(N-2, q^2)$. As before, such a plane contains q^2-1 intersection points of $\mathcal{Q}(N, q^2)$ and $L\mathcal{H}(N-2, q^2)$, different from R and not lying in $T_P(\mathcal{Q}(N, q^2))$.

So we have found the upper bound

$$1 + q^2\overline{W}_{N-2} + 1 + (q^2-1)|\mathcal{H}(N-2, q^2)| < \overline{W}_N$$

for the intersection size of $\mathcal{Q}(N, q^2) \cap L\mathcal{H}(N-2, q^2)$.

$L \subset \mathcal{Q}(N, q^2)$

We have that $T_L(\mathcal{Q}(N, q^2)) \cap \mathcal{Q}(N, q^2) = L\mathcal{Q}(N-4, q^2)$. All the planes through L and a point of this base $\mathcal{Q}(N-4, q^2)$ can be in the intersection, then we have at most

1. $N = 5$

   $q^4|\mathcal{Q}(1, q^2)| + q^2 + 1 = 2q^4 + q^2 + 1$;

2. $N \geq 6$

   $q^4|\mathcal{Q}(N-4, q^2)| + q^2 + 1 \leq q^4(q^{2N-10} + 2q^{2N-12} + 1) + q^2 + 1 = q^{2N-6} + 2q^{2N-8} + q^4 + q^2 + 1$.

Outside of $T_L(\mathcal{Q}(N, q^2))$, every plane of $L\mathcal{H}(N-2, q^2)$ through L shares at most one other line with $\mathcal{Q}(N, q^2)$. Then we have at most

1. $N = 5$

   $2q^4 + q^2 + 1 + q^2|\mathcal{H}(3, q^2)| = q^7 + q^5 + 3q^4 + 2q^2 + 1 \leq \overline{W}_5$;

2. $N \geq 6$

   $q^{2N-6} + 2q^{2N-8} + q^4 + q^2 + 1 + q^2|\mathcal{H}(N-2, q^2)| \leq q^{2N-6} + 2q^{2N-8} + q^4 + q^2 + 1 + q^{2N-3} + 2q^{2N-5} \leq \overline{W}_N$.

2.7.3 $H = \pi_s\mathcal{H}(N-s-1, q^2)$, with $s \geq 2$

In this case, since the vertex π_s of $\pi_s\mathcal{H}(N-s-1, q^2)$ is at least a plane, there is at least a point $P \in \pi_s \cap \mathcal{Q}(N, q^2)$. Let $T_P(\mathcal{Q}(N, q^2))$ be the tangent hyperplane to $\mathcal{Q}(N, q^2)$ in P. This tangent hyperplane intersects $\mathcal{Q}(N, q^2)$ in a cone with vertex P and base a non-singular quadric $\mathcal{Q}(N-2, q^2)$ of the same type as $\mathcal{Q}(N, q^2)$. Let π_{N-2} be the $(N-2)$-dimensional space containing $\mathcal{Q}(N-2, q^2)$. This space intersects the Hermitian variety $\pi_s\mathcal{H}(N-s-1, q^2)$ in a Hermitian variety $\pi'_{s-i}\mathcal{H}(N-s-3+i, q^2)$, $i = 0, 1, 2$. The tangent hyperplane $T_P(\mathcal{Q}(N, q^2))$ then intersects $\pi_s\mathcal{H}(N-s-1, q^2)$ in a Hermitian

variety $\pi''_{s-i+1}\mathcal{H}(N-s-3+i,q^2)$, $i=0,1,2$. By induction on N, the base $\mathcal{Q}(N-2,q^2)$ shares at most $\overline{W}_{N-2}$ points with the Hermitian variety $\pi'_{s-i}\mathcal{H}(N-s-3+i,q^2)$. Hence, $|T_P(\mathcal{Q}(N,q^2))\cap\mathcal{Q}(N,q^2)\cap\pi_s\mathcal{H}(N-s-1,q^2)|\leq 1+q^2\overline{W}_{N-2}$.

The number of points of $\pi_s\mathcal{H}(N-s-1,q^2)$ outside of $T_P(\mathcal{Q}(N,q^2))$ equals $|\pi_s\mathcal{H}(N-s-1,q^2)\setminus\pi''_{s-i+1}\mathcal{H}(N-s-3+i,q^2)|$, which can be upper bounded by $q^{2s+2}|\mathcal{H}(N-s-1,q^2)|$ in all three cases. They all lie on lines through P contained in $\pi_s\mathcal{H}(N-s-1,q^2)$. Since these lines do not lie in $T_P(\mathcal{Q}(N,q^2))$, they all contain, besides the point P, one extra point of $\mathcal{Q}(N,q^2)$. Hence, there are at most $q^{2s}|\mathcal{H}(N-s-1,q^2)|$ other intersection points of $\mathcal{Q}(N,q^2)$ and $\pi_s\mathcal{H}(N-s-1,q^2)$. So

$$1+q^2\overline{W}_{N-2}+q^{2s}|\mathcal{H}(N-s-1,q^2)|\leq q^{2N-3}+3q^{2N-5}+3q^{2N-6}+1<\overline{W}_N$$

is an upper bound on the intersection size $|\mathcal{Q}(N,q^2)\cap\pi_s\mathcal{H}(N-s-1,q^2)|$. Remark that the leftmost inequality is not valid if $N=8$, $q=2$ and $s=6$. However, one can easily calculate that the inequality $1+q^2\overline{W}_{N-2}+q^{2s}|\mathcal{H}(N-s-1,q^2)|\leq\overline{W}_N$ is still valid.

2.7.4 Conclusion

Resuming the results of this section, we can state the following theorem.

Theorem 2.21. *Let $\mathcal{Q}(N,q^2)$ be a non-singular quadric in $\mathrm{PG}(N,q^2)$ and let H be an arbitrary Hermitian variety in $\mathrm{PG}(N,q^2)$. Then $|\mathcal{Q}(N,q^2)\cap H|\leq\overline{W}_N$. Hence, the minimum distance of the code $C_{Herm}(\mathcal{Q}(N,q^2))$ is at least $|\mathcal{Q}(N,q^2)|-\overline{W}_N$.*

2.8 Some small weight codewords

In this section we will give some examples of small weight codewords; codewords with weights a little above $|\mathcal{Q}(N,q^2)|-\overline{W}_N$. Although we have proven that in most cases, the lower bound for this minimum

weight (minimum distance) arises from the non-singular Hermitian varieties, we will have a look on codewords arising from the Hermitian varieties $\pi_{N-2}\mathcal{H}(1,q^2)$. These Hermitian varieties can be seen as the union of $q+1$ hyperplanes through a fixed $(N-2)$-space π_{N-2}. The difference between our bound $\overline{W}_N$ on the intersection size of $\mathcal{Q}(N,q^2)$ with the Hermitian variety H and the intersection size of the examples that we will present is $O(q^{2N-5})$.

It should be observed that not any union of $q+1$ hyperplanes through a fixed $(N-2)$-space, is a Hermitian variety. Such a set of hyperplanes defines a Hermitian variety if and only if it corresponds to a Baer subline of a line disjoint to the fixed $(N-2)$-space π_{N-2}.

Remark 2.22. *Each quadric has an index w, related to its type. Its index equals* 2 *if the quadric is hyperbolic,* 1 *if the quadric is parabolic, and* 0 *if it is elliptic.*

Example 2.23. Let π_{N-2} be an $(N-2)$-space intersecting the quadric $\mathcal{Q}(N,q^2)$ in a cone $L\mathcal{Q}(N-4,q^2)$ with vertex a line. Each of the q^2+1 hyperplanes through π_{N-2} intersects $\mathcal{Q}(N,q^2)$ in a cone with vertex a point. Hence, any Hermitian variety with π_{N-2} as vertex consists of $q+1$ hyperplanes intersecting $\mathcal{Q}(N,q^2)$ in a singular quadric.

We now calculate the weight of the codeword that such a Hermitian variety H gives rise to. The weight of this codeword equals the number of points of $\mathcal{Q}(N,q^2)$, not on H. Each of these points lies on a hyperplane through π_{N-2} that does not belong to the $q+1$ hyperplanes of H. There are q^2-q such hyperplanes through π_{N-2} and each of those hyperplanes contains q^{2N-6} planes, not in π_{N-2}, through L. Such a plane contains precisely two lines of $\mathcal{Q}(N,q^2)$, one of them L. Consequently, the weight of the codewords is $(q^2-q)\cdot q^2\cdot q^{2N-6}=q^{2N-2}-q^{2N-3}$.

Note that the size of the intersection $H\cap\mathcal{Q}(N,q^2)$ equals $\frac{q^{2N-2}-1}{q^2-1}+q^{2N-3}+(w-1)q^{N-1}$, with w the index of $\mathcal{Q}(N,q^2)$.

Example 2.24. Let π_{N-2} be an $(N-2)$-space intersecting the quadric $\mathcal{Q}(N,q^2)$ in a cone $P\mathcal{Q}(N-3,q^2)$ with vertex a point. All but one of the hyperplanes through π_{N-2} intersect $\mathcal{Q}(N,q^2)$ in a non-singular quadric $\mathcal{Q}(N-1,q^2)$. One of those q^2+1 hyperplanes through π_{N-2}, the tangent hyperplane to $\mathcal{Q}(N,q^2)$ in P, intersects $\mathcal{Q}(N,q^2)$ in a singular quadric with vertex a point (namely P). Hence, the Hermitian varieties with π_{N-2} as vertex can be split up in two groups: the ones that contain the tangent hyperplane $T_P(\mathcal{Q}(N,q^2))$ and the ones that do not.

We now calculate the weight of the codewords any of these Hermitian varieties H gives rise to. If a hyperplane π is not $T_P(\mathcal{Q}(N,q^2))$, then the number of points of $\mathcal{Q}(N,q^2)$ in this hyperplane π, not in π_{N-2}, equals q^{2N-4} since every line through P in π, but not in π_{N-2}, is a bisecant to $\mathcal{Q}(N,q^2)$. The number of points of $\mathcal{Q}(N,q^2)$ in $T_P(\mathcal{Q}(N,q^2))$, not in π_{N-2}, equals $|P\mathcal{Q}(N-2,q^2)|-|P\mathcal{Q}(N-3,q^2)| = q^2(|\mathcal{Q}(N-2,q^2)|-|\mathcal{Q}(N-3,q^2)|) = q^{2N-4}+(w'-1)q^{N-1}-(w''-1)q^{N-2}$. Hereby w' is the index of $\mathcal{Q}(N-2,q^2)$ and w'' is the index of $\mathcal{Q}(N-3,q^2)$.

In case the Hermitian variety contains the hyperplane $T_P(\mathcal{Q}(N,q^2))$, then the weight of the corresponding codeword is $q^{2N-2}-q^{2N-3}$. In case the Hermitian variety does not contain the hyperplane $T_P(\mathcal{Q}(N,q^2))$, then the weight of the corresponding codeword equals $q^{2N-2}-q^{2N-3}-q^{N-1}$ or $q^{2N-2}-q^{2N-3}+q^{N-1}$ if N is odd, and $q^{2N-2}-q^{2N-3}-q^{N-2}$ or $q^{2N-2}-q^{2N-3}+q^{N-2}$ if N is even.

Note that the size of the intersection $H\cap\mathcal{Q}(N,q^2)$ equals $\frac{q^{2N-2}-1}{q^2-1}+q^{2N-3}+(w'-1)q^{N-1}$ in the former case and $\frac{q^{2N-2}-1}{q^2-1}+q^{2N-3}+(w''-1)q^{N-2}$ in the latter case, with w',w'' as before.

In case the $(N-2)$-space intersects $\mathcal{Q}(N,q^2)$ in a non-singular quadric we need to distinguish several cases.

Example 2.25. We assume N odd. Let π_{N-2} be an $(N-2)$-space intersecting the quadric $\mathcal{Q}(N,q^2)$ in a non-singular quadric $\mathcal{Q}(N-2,q^2)$. If $\mathcal{Q}(N,q^2)$ and $\mathcal{Q}(N-2,q^2)$ are of the same type, then two

hyperplanes through π_{N-2} are tangent hyperplanes. The remaining q^2-1 hyperplanes through π_{N-2} intersect $\mathcal{Q}(N,q^2)$ in a parabolic quadric. If $\mathcal{Q}(N,q^2)$ and $\mathcal{Q}(N-2,q^2)$ are of a different type, then all q^2+1 hyperplanes through π_{N-2} intersect $\mathcal{Q}(N,q^2)$ in a parabolic quadric.

Let w be the index of $\mathcal{Q}(N,q^2)$ and let w' be the index of $\mathcal{Q}(N-2,q^2)$. Let π be a hyperplane through π_{N-2}. If π intersects $\mathcal{Q}(N,q^2)$ in a parabolic quadric, then $\pi\setminus\pi_{N-2}$ contains $q^{2N-4}-(w'-1)q^{N-3}$ points of $\mathcal{Q}(N,q^2)$. If π is a tangent hyperplane to $\mathcal{Q}(N,q^2)$, then $\pi\setminus\pi_{N-2}$ contains $q^{2N-4}+(w'-1)(q^{N-1}-q^{N-3})$ points of $\mathcal{Q}(N,q^2)$.

Hence, if $w\neq w'$, this codeword has weight $q^{2N-2}-q^{2N-3}-(w'-1)(q^{N-1}-q^{N-2})$. If $w=w'$, this codeword has weight $q^{2N-2}-q^{2N-3}-(w'-1)(q^{N-1}-q^{N-2})$ or $q^{2N-2}-q^{2N-3}+(w'-1)q^{N-2}$ or $q^{2N-2}-q^{2N-3}+(w'-1)(q^{N-1}+q^{N-2})$ depending on the number of tangent hyperplanes contained in the Hermitian variety: 2, 1 or 0. Among these, the smallest codeword has weight $q^{2N-2}-q^{2N-3}-q^{N-1}-q^{N-2}$. This corresponds to a codeword arising from an elliptic quadric $\mathcal{Q}(N,q^2)$ and a Hermitian variety which is the union of $q+1$ hyperplanes, zero of them tangent hyperplanes, through an $(N-2)$-space intersecting the quadric $\mathcal{Q}(N,q^2)$ in a non-singular elliptic quadric.

Note that in this case the intersection size equals $\frac{q^{2N-2}-1}{q^2-1}+q^{2N-3}+q^{N-2}$.

Example 2.26. We assume N even and q odd. Let π_{N-2} be an $(N-2)$-space intersecting the parabolic quadric $\mathcal{Q}(N,q^2)$ in a non-singular parabolic quadric $\mathcal{Q}(N-2,q^2)$. Let L be the polar line of π_{N-2}, necessarily disjoint to π_{N-2}. There are two possibilities. If L is a secant line to $\mathcal{Q}(N,q^2)$, with $L\cap\mathcal{Q}(N,q^2)=\{Q,R\}$, two of the hyperplanes through π_{N-2} are tangent hyperplanes, namely $T_Q(\mathcal{Q}(N,q^2))$ and $T_R(\mathcal{Q}(N,q^2))$, precisely $\frac{q^2-1}{2}$ of the remaining hyperplanes intersect $\mathcal{Q}(N,q^2)$ in an $(N-1)$-dimensional hyperbolic quadric (*hyperbolic hyperplanes*) and precisely $\frac{q^2-1}{2}$ of them intersect $\mathcal{Q}(N,q^2)$ in an $(N-1)$-dimensional elliptic quadric (*elliptic hyperplanes*). If L is a line disjoint from $\mathcal{Q}(N,q^2)$, then $\frac{q^2+1}{2}$ of the hyperplanes through π_{N-2} intersect $\mathcal{Q}(N,q^2)$ in a hyperbolic quadric and

$\frac{q^2+1}{2}$ of them intersect $\mathcal{Q}(N,q^2)$ in an elliptic quadric.

Let π be a hyperplane through π_{N-2}. If π is a tangent hyperplane, then $\pi \setminus \pi_{N-2}$ contains q^{2N-4} points of $\mathcal{Q}(N,q^2)$. If π intersects $\mathcal{Q}(N,q^2)$ in a hyperbolic quadric, then $\pi \setminus \pi_{N-2}$ contains $q^{2N-4}+q^{N-2}$ points of $\mathcal{Q}(N,q^2)$. If π intersects $\mathcal{Q}(N,q^2)$ in an elliptic quadric, then $\pi \setminus \pi_{N-2}$ contains $q^{2N-4}-q^{N-2}$ points of $\mathcal{Q}(N,q^2)$.

We look at an example in the case L is a secant line. We consider the standard equation $X_0^2 + X_1X_2 + \cdots + X_{N-1}X_N = 0$ of $\mathcal{Q}(N,q^2)$ and let π_{N-2} be the $(N-2)$-space $X_{N-1} = X_N = 0$. The two tangent hyperplanes through π_{N-2} are given by $X_{N-1} = 0$ $(= T_Q(\mathcal{Q}(N,q^2))$ for $Q = (0,\ldots,0,0,1))$ and $X_N = 0$ $(= T_R(\mathcal{Q}(N,q^2))$ for $R = (0,\ldots,0,1,0))$. The other hyperplanes through π_{N-2} are given by $X_{N-1} + \alpha X_N = 0$, $\alpha \in \mathbb{F}_{q^2}^*$, which we denote by shortened coordinates $\overline{[1,\alpha]}$. The tangent hyperplanes correspond to $\overline{[1,0]}$ and $\overline{[0,1]}$. The hyperplane $\overline{[1,\alpha]}$ intersects $\mathcal{Q}(N,q^2)$ in a hyperbolic quadric, respectively an elliptic quadric, if and only if α is a non-zero square, respectively a non-square. We now investigate how a dual Baer subline can intersect these sets.

First assume that the Hermitian variety contains both tangent hyperplanes (the dual Baer subline contains $\overline{[1,0]}$ and $\overline{[0,1]}$). The dual Baer subline is then defined by choosing a third hyperplane $\overline{[1,y]}$: all $q-1$ hyperplanes of this dual Baer subline, different from $\overline{[1,0]}$ and $\overline{[0,1]}$, can be written as $\overline{[1,\beta y]}$, with $\beta \in \mathbb{F}_q^* \subset \mathbb{F}_{q^2}$. Since $\beta \in \mathbb{F}_q^* \subset (\mathbb{F}_{q^2}^*)^2$, $\beta y \in (\mathbb{F}_{q^2}^*)^2$ if and only if $y \in (\mathbb{F}_{q^2}^*)^2$. Hence, either all of the hyperplanes in the dual Baer subline, different from $\overline{[1,0]}$ and $\overline{[0,1]}$, intersect $\mathcal{Q}(N,q^2)$ in a hyperbolic quadric or all of the hyperplanes in the dual Baer subline, different from $\overline{[1,0]}$ and $\overline{[0,1]}$, intersect $\mathcal{Q}(N,q^2)$ in an elliptic quadric. The $q+1$ dual Baer sublines through $\overline{[1,0]}$ and $\overline{[0,1]}$, which we denote by $l_0,\ldots,l_q$, partition the q^2-1 remaining points of the dual line. Next to the two tangent hyperplanes, $\frac{q+1}{2}$ of these dual Baer sublines, say $l_0,\ldots,l_{\frac{q-1}{2}}$, only contain hyperbolic hyperplanes and $\frac{q+1}{2}$ of these dual Baer sublines, say $l_{\frac{q+1}{2}},\ldots,l_q$, only contain elliptic hyperplanes. We find codewords

of weight

$$\frac{q^2-1}{2}(q^{2N-4}-q^{N-2})+\left(\frac{q^2-1}{2}-(q-1)\right)(q^{2N-4}+q^{N-2})=q^{2N-2}-q^{2N-3}-q^{N-1}+q^{N-2}$$

and of weight

$$\frac{q^2-1}{2}(q^{2N-4}+q^{N-2})+\left(\frac{q^2-1}{2}-(q-1)\right)(q^{2N-4}-q^{N-2})=q^{2N-2}-q^{2N-3}+q^{N-1}-q^{N-2}\,.$$

Secondly, we assume that the dual Baer subline only contains one of the two tangent hyperplanes, say $\overline{[1,0]}$. Since two distinct dual Baer sublines have at most two hyperplanes in common, such a dual Baer subline contains at most one hyperbolic or elliptic hyperplane of each l_i, $0 \le i \le q$. A dual Baer subline contains precisely $q+1$ hyperplanes, so all but one of the dual Baer sublines l_i contribute one hyperplane. Let l_j be the one dual Baer subline that does not contribute an additional hyperplane. If $j \le \frac{q-1}{2}$, then the corresponding codeword has weight

$$\left(\frac{q^2-1}{2}-\frac{q+1}{2}\right)(q^{2N-4}-q^{N-2})+\left(\frac{q^2-1}{2}-\frac{q-1}{2}\right)(q^{2N-4}+q^{N-2})+q^{2N-4}$$
$$=q^{2N-2}-q^{2N-3}+q^{N-2}\,;$$

if $j \ge \frac{q+1}{2}$, then the corresponding codeword has weight

$$\left(\frac{q^2-1}{2}-\frac{q-1}{2}\right)(q^{2N-4}-q^{N-2})+\left(\frac{q^2-1}{2}-\frac{q+1}{2}\right)(q^{2N-4}+q^{N-2})+q^{2N-4}$$
$$=q^{2N-2}-q^{2N-3}-q^{N-2}\,.$$

By looking at some small examples one can see that both possibilities occur.

2.9 A divisibility condition on the weights

Definition 2.27. Let C be a linear code over $\mathbb{F}_q$ and let $\delta > 1$ be an integer such that the weight of every codeword of C is divisible by δ. Then δ is called a divisor of the code C.

All functional codes studied so far, have been shown to have a divisor of the form q^e, see e.g. [65, 66]. The proofs of these results all rely on the following theorem.

Theorem 2.28 (Ax-Katz [109])**.** *Let S be a finite set of variables and let $T = \{f_i | i \in I\}$ be a collection of polynomials in $\mathbb{F}_q[S]$, with $d_i = \deg(f_i)$. Denote the number of common zeros of the polynomials of T by N. Then $N \equiv 0 \pmod{q^\mu}$, with*

$$\mu = \left\lceil \frac{|S| - \sum_{i \in I} d_i}{\sup_{i \in I} d_i} \right\rceil .$$

Now we prove that also the code $C_{Herm}(\mathcal{Q})$ that we have studied in this article, has a divisor of the form q^e.

Lemma 2.29. *Let H be a Hermitian variety in $\mathrm{PG}(N, q^2)$ and let Q be a quadric in $\mathrm{PG}(N, q^2)$, which both can be singular. Then $|Q \cap H| \equiv \frac{q^{N-2}-1}{q^2-1} \pmod{q^{N-2}}$ if N is even and $|Q \cap H| \equiv \frac{q^{N-1}-1}{q^2-1} \pmod{q^{N-2}}$ if N is odd.*

Proof. We can choose a coordinate system such that the equation of H can be written as $X_0^{q+1} + \cdots + X_i^{q+1} = g(X_0, \ldots, X_N) = 0$, with $1 \leq i \leq N$. The quadric Q is given by an equation $f(X_0, \ldots, X_N) = 0$, with f a quadratic polynomial. Every point of $Q \cap H$ corresponds vectorially to $q^2 - 1$ solutions of the system of equations

$$\begin{cases} f(X_0, \ldots, X_N) = 0 \\ g(X_0, \ldots, X_N) = 0 \end{cases} , \tag{2.1}$$

and every non-zero solution of this system corresponds to a point of $Q \cap H$. Let α be an element of $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Then every element $x \in \mathbb{F}_{q^2}$ can be written as $x = y + \alpha z$, with $y, z \in \mathbb{F}_q$. Now we write

$X_i = Y_i + \alpha Z_i$, with Y_i and Z_i variables in $\mathbb{F}_q$. In these new variables, the equation of H is given by

$$0 = \sum_{j=0}^{i} (Y_j + \alpha Z_j)^{q+1} = \sum_{j=0}^{i} (Y_j^{q+1} + \alpha Y_j^q Z_j + \alpha^q Y_j Z_j^q + \alpha^{q+1} Z_j^{q+1})$$

$$= \sum_{j=0}^{i} (Y_j^2 + (\alpha + \alpha^q) Y_j Z_j + \alpha^{q+1} Z_j^2)\,,$$

a quadratic equation over $\mathbb{F}_q$, since $\alpha + \alpha^q, \alpha^{q+1} \in \mathbb{F}_q$. Hereby we used the identity $x^q = x$ that holds for any $x \in \mathbb{F}_q$. We denote $\sum_{j=0}^{i} (Y_j^2 + (\alpha + \alpha^q) Y_j Z_j + \alpha^{q+1} Z_j^2)$ by $\overline{g}(Y_0, Z_0, \ldots, Y_N, Z_N)$. The equation of Q in the variables Y_j and Z_j is of the form

$$f_0(Y_0, \ldots, Y_N) + \alpha f_1(Y_0, Z_0, \ldots, Y_N, Z_N) + \alpha^2 f_2(Z_0, \ldots, Z_N) = 0\,.$$

Writing $\alpha^2 = a_2 + b_2\alpha$, with $a_2, b_2 \in \mathbb{F}_q$, we can rewrite this equation as

$$0 = [f_0(Y_0, \ldots, Y_N) + a_2 f_2(Z_0, \ldots, Z_N)] + \alpha\,[f_1(Y_0, Z_0, \ldots, Y_N, Z_N) + b_2 f_2(Z_0, \ldots, Z_N)]$$

$$= \overline{f}_0(Y_0, Z_0, \ldots, Y_N, Z_N) + \alpha \overline{f}_1(Y_0, Z_0, \ldots, Y_N, Z_N)\,.$$

The quadric Q is thus defined by a system of two equations over the variables Y_j, Z_j:

$$\begin{cases} \overline{f}_0(Y_0, Z_0, \ldots, Y_N, Z_N) = 0 \\ \overline{f}_1(Y_0, Z_0, \ldots, Y_N, Z_N) = 0 \end{cases}.$$

Now we look to the system of equations

$$\begin{cases} \overline{g}(Y_0, Z_0, \ldots, Y_N, Z_N) = 0 \\ \overline{f}_0(Y_0, Z_0, \ldots, Y_N, Z_N) = 0 \\ \overline{f}_1(Y_0, Z_0, \ldots, Y_N, Z_N) = 0 \end{cases}. \tag{2.2}$$

Every solution $(x_0, \ldots, x_N)$, $x_i \in \mathbb{F}_{q^2}$, with $x_i = y_i + \alpha z_i$, $y_i, z_i \in \mathbb{F}_q$, of (2.1) corresponds to a unique solution $(y_0, z_0, \ldots, y_N, z_N)$ of (2.2) and vice versa. Let M be the number of solutions of (2.2) in $V(2N+2, q)$. By Theorem 2.28, we know that

$$M \equiv 0 \pmod{q^\mu}, \quad \text{with} \quad \mu = \left\lceil \frac{2(N+1) - 3 \cdot 2}{2} \right\rceil = N - 2.$$

Thus we can write $M = mq^{N-2}$ for an integer m. Obviously the all-zero vector is a solution of (2.2). Since Q and H are defined by homogeneous polynomials over $\mathbb{F}_{q^2}$, we know that $|Q \cap H| = \frac{M-1}{q^2-1}$. Hence, $M \equiv 1 \pmod{(q^2-1)}$.

On the one hand, if N is even, we find that

$$1 \equiv M \equiv mq^{N-2} \equiv m(q^2)^{(N-2)/2} \equiv m \pmod{(q^2-1)}.$$

So, $m = m'(q^2-1)+1$ for an integer m'. Consequently,

$$|Q \cap H| = \frac{mq^{N-2}-1}{q^2-1} = m'q^{N-2} + \frac{q^{N-2}-1}{q^2-1}\,.$$

On the other hand, if N is odd, we find that

$$1 \equiv M \equiv mq^{N-2} \equiv m(q^2)^{(N-3)/2}q \equiv mq \pmod{(q^2-1)}.$$

So, $m = m'(q^2-1)+q$ for an integer m'. Consequently,

$$|Q \cap H| = \frac{mq^{N-2}-1}{q^2-1} = m'q^{N-2} + \frac{q^{N-1}-1}{q^2-1}\,.$$

In both cases the statement follows. □

Theorem 2.30. *The value q^{N-2} is a divisor of the code $C_{Herm}(\mathcal{Q})$, $\mathcal{Q}$ a non-singular quadric in $\mathrm{PG}(N,q^2)$, $N \geq 3$.*

Proof. Let c be a codeword of the code $C_{Herm}(\mathcal{Q})$. This codeword is generated by a polynomial f which gives rise to a Hermitian variety H. We need to distinguish two cases.

First we assume N even. By Lemma 2.29, we know that $|\mathcal{Q} \cap H| \equiv \frac{q^{N-2}-1}{q^2-1} \pmod{q^{N-2}}$. Furthermore $|\mathcal{Q}| = \frac{q^{2N}-1}{q^2-1} = q^{N-2}\left(\frac{q^{N+2}-1}{q^2-1}\right) + \frac{q^{N-2}-1}{q^2-1} \equiv \frac{q^{N-2}-1}{q^2-1} \pmod{q^{N-2}}$. We conclude:

$$\mathrm{wt}(c) = |\mathcal{Q}| - |\mathcal{Q} \cap H| \equiv 0 \pmod{q^{N-2}}\,.$$

Now we assume N odd. By Lemma 2.29, we know that $|\mathcal{Q} \cap H| \equiv \frac{q^{N-1}-1}{q^2-1} \pmod{q^{N-2}}$. Furthermore $|\mathcal{Q}| = \frac{q^{2N}-1}{q^2-1} \pm q^{N-1} = q^{N-1}\left(\frac{q^{N+1}-1}{q^2-1} \pm 1\right) + \frac{q^{N-1}-1}{q^2-1} \equiv \frac{q^{N-1}-1}{q^2-1} \pmod{q^{N-2}}$. We conclude:

$$\mathrm{wt}(c) = |\mathcal{Q}| - |\mathcal{Q} \cap H| \equiv 0 \pmod{q^{N-2}}.$$

Since c is an arbitrary codeword, the theorem is proven. □

Comparing the proof of Lemma 2.29 to the proof of [66, Theorem 3.4], we note that in their proof the Hermitian variety needs to be non-singular, whereas it is allowed to be singular in our proof. In their proof however, the Hermitian variety is intersected by a hypersurface of degree h, whereas we only considered $h = 2$. The techniques of the above proof could be used to prove a generalization of this lemma, involving hypersurfaces of degree $h < N$. We did not do this here since we do not need it for the proof of Theorem 2.30. Note also that there is a small mistake in the proof of [66, Theorem 3.4]: in fact they count the number of intersection points in $\mathrm{PG}(2N+1, q)$.

Chapter 3

Introduction on Computation

The problem of finding non-equivalent geometrical structures using computational instruments is very popular in literature (see for instance [40], [41], [44], [58], [128]).
In this work we perform exhaustive searches using a chronological backtracking algorithm. Some strategies have to be used to reduce the search space as in this kind of problems there are many equivalent parts of the search space and a large number of copies of equivalent solutions could be found.

3.1 Two different kinds of problems

When searching for geometrical structures, two cases can occur.
If the structure we are searching for has some *hereditary feature* (algorithm of type A) we can use this feature to prune the search space.
With *hereditary feature* we intend a feature which is conserved in all the subsets of a partial solution. Examples of this type of structures are (n, k)-arcs or caps. The caps have the property that no three points of them are collinear: a $(k+1)$-cap is obtained from k-sets which also are caps. After every step the number of candidates for the extension of the partial solution decreases. This property is used

directly to reduce the number of points candidates for the extension process: in the case of caps we consider only points not lying on bisecansts of the expanding partial set.

The second type of structures are those without any hereditary feature (algorithm of type B). 1-Saturating sets (i.e. sets covering with they bisecants all the points of the space) or blocking sets (i.e. sets such that every line of the space contains at least one point of the set) belong to this class.

In fact a saturating $(k+1)$-set could not contain a saturating k-set (actually, as we are interested in *minimal* 1-saturating sets, it should not contain saturating k-sets). Hence, when extending a k-set $\mathcal{K}$, we have to consider as candidates for the extension all the points of $PG(2,q) \setminus \mathcal{K}$. Therefore in this second case the search is in general more computational expansive than in the first case.

In both cases a solution is found when a condition of completeness is satisfied. In the first case it usually means that no more points can be added without violating the feature of the structure.

In the second case (for instance searching for saturating sets or blocking sets) it means that a certain condition is achieved; however a condition of minimality has to be tested since the condition for the termination could also hold for some subset of the found solution. For instance if $\{A_1, \ldots, A_n\}$ is not a saturating set and $\{B, A_1, \ldots, A_n\}$ is a saturating set it could happen that $\{B, A_2 \ldots, A_n\}$ is a saturating set too.

When considering a plane arc, the feature used in the search is that no three points of the solution are collinear and we use it during the extension process not considering as candidates the points lying on bisecants of the partial solution. The condition of termination, the completeness, is that no more points can be added to the partial solution. In this case, when this condition is reached, then the minimality condition, i.e. no subset of the solution is a solution too, is true by construction.

When considering a saturating set (a blocking set) we can not use any feature during the extension process, so all the points can be considered as candidates for the extension of the partial solution; the

condition of termination is that all the points of the space $PG(n, q)$ lye on bisecants of the solution (every line of the space meets the solution in at least one point). When this condition is reached, the minimality condition has to be checked, verifying if some subset of the solution (solution minus a point) is a solution too.

3.2 Backtracking

To perform exhaustive searches we use backtracking.

In a backtracking approach, to generate an m-tuple which is a solution, we extend *partial solutions*. A partial solution of length $k \leq m$ is a k-tuple $(P_1, \ldots, P_k)$ contained in the putative m-solution. If a $k-$partial solution is obtained, we try to extend it to a $(k+1)-$partial solution. If we obtained a solution or if the all possible extensions (if any) have been considered, we go back to the $(k-1)-$partial solution already obtained and we attempt to generate a $k-$partial solution different from the previous one (chronological backtracking).

It is possible then to organize the partial solutions in a tree. In fact we can consider the empty partial solution as root of the tree and if we get the $k-$partial $(P_1, \ldots, P_k)$ solution from the $(k-1)-$partial $(P_1, \ldots, P_{k-2}, P_{k-1})$, then $(P_1, \ldots, P_k)$ is represented as a child of $(P_1, \ldots, P_{k-1})$.

Each subset in the extension process is considered only one time. This systematicity is reached simply ordering the points of the space in a particular way and considering for the extension only sets having points in ascending order.

3.3 Using equivalence

When using backtracking, one proceeds expanding a partial set to obtain larger sets until a solution or a dead end is reached. In both cases the search continues backtracking to the previous step changing the previous choice. In particular to generate a k-solution from a partial $(k-1)$-solution $(P_1, \ldots, P_{k-1})$ we have to control all the possible k-set of type $(P_1, \ldots, P_{k-1}, Q)$, with Q different from $P_i \; \forall \; i = 1, \ldots, k-1$. At each step, this process increases the number of leaves in exponential way.

However due to the large symmetry group of the geometrical spaces, there are many equivalent parts in the search space and some strategies to avoid obtaining many copies of the same solutions should be adopted. This process of reducing the search space using symmetry properties is called *isomorph rejection*. To use this method we have to define an equivalence relationship, which allows us to say when two different node of the tree are *isomorphic*. The fundamental idea is that it is not necessary to extend all the partial solutions, but only the non-isomorphic ones. For instance, in the search for geometrical structure in projective spaces, we use collineations and we say that two partial solutions $\mathbf{S_1}$ and $\mathbf{S_2}$ are isomorphic if there exists a collineation φ such that $\varphi(\mathbf{S_1}) = \mathbf{S_2}$.

When extending a partial solution $\mathcal{K}$, we create a list of *candidate points*, (in the case of saturating sets this set consists of all the points of the space not in $\mathcal{K}$). If this set is not empty, we introduce the following equivalence relationship:

$$P \sim Q \iff \mathcal{K} \cup \{P\} \cong \mathcal{K} \cup \{Q\},$$

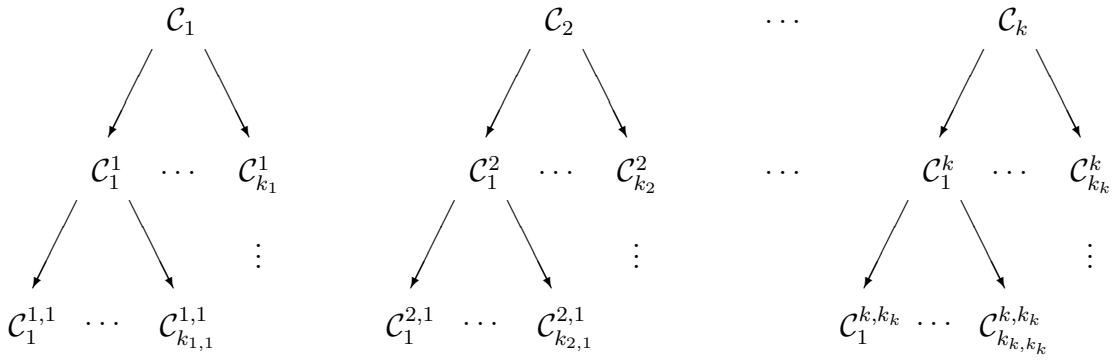
where $\cong$ means that there is a collineation between the two sets. This relationship splits the candidates in equivalence classes $\mathcal{O}_1, \ldots, \mathcal{O}_k$.

It is sufficient to choose the next point to add to $\mathcal{K}$ among the representatives of the equivalence classes, as two partial solutions, one containing $\mathcal{K} \cup \{P\}$ and the other one containing $\mathcal{K} \cup \{Q\}$, with P and Q

in $\mathcal{O}_{\bar{i}}$, are equivalent.

Suppose now that we have constructed all the partial solutions containing $\mathcal{K} \cup \{P_i\}$, with $i \leq \bar{i}$. When considering the partial solutions containing $\mathcal{K} \cup \{P_j\}$ with $\bar{i} < j$, all the points of the classes $\mathcal{O}_k$ with $k < \bar{i}$ can be avoided. In fact a partial solution containing $\mathcal{K} \cup \{P_j\} \cup \{\overline{P}_k\}$, with $\overline{P}_k \in \mathcal{O}_k$ and $k < \bar{i}$, is projectively equivalent to a partial solution containing $\mathcal{K} \cup \{P_k\} \cup \{P_j\}$, already studied.

Iterating the process we can build a tree similar to the following:



Using the previous observations we can build a tree such that every partial solution of the desired size is equivalent to a partial solution containing a leaf of the tree.

After building the tree, we extend the leaves using a chronological backtracking algorithm.

Again, during the backtracking, after having computed all solutions containing $\mathcal{K} \cup \{P_i\}$, $i \leq \bar{i}$, when considering the solutions containing $\mathcal{K} \cup \{P_j\}$, $\bar{i} < j$, we can avoid to add to the partial solution the points belonging to the classes $\mathcal{O}_k$, $k \leq \bar{i}$. In fact, if such a point were added to the partial solution, we should obtain a solution equivalent to a solution previously computed.

3.4 Greedy algorithms

When it is not possible to perform a complete exploration of the whole search space, some heuristic techniques can be utilized to obtain interesting examples. For example in the search for complete arcs in projective planes $PG(2,q)$ with large q (see Chapter 5) a greedy randomized algorithm has been used to obtain small complete arcs.

At every step the algorithm maximizes an objective function f, but some steps are executed in random manner, to avoid the algorithm to concentrate around a local maximum of the objective function. The number of these steps, their positions and some other parameters of the algorithm have been taken intuitively. Also, if the same maximum of f can be obtained in distinct ways, one way is chosen randomly.

In particular greedy algorithms are used to obtain small complete arcs in projective planes. We begin to construct a complete arc by using a starting set of points S_0. At the i-th step one point is added to the set S_{i-1} to obtain the point set S_i. The objective function f we consider counts the number of covered points in $PG(2,q)$, i.e. points lying on bisecants of the set S_{i-1}. On every *random* i-th step we take $d_{q,i}$ randomly chosen points of $PG(2,q)$ uncovered by S_{i-1} and compute the objective function f adding each of these $d_{q,i}$ points to S_{i-1}. The point providing the maximum of f is added to S_{i-1} to get S_i. On every *non-random* j-th step we consider all points uncovered by S_{j-1} and we add to S_{j-1} the point providing the maximum of f. As S_0 we can use a subset of points of an arc obtained in previous stages of the search. A generator of random numbers is used for random choice. To get arcs with distinct sizes, starting conditions of the generator are changed for the same set S_0. In this way the algorithm works in a convenient limited region of the search space to obtain examples improving the size of the arc from which the fixed points have been taken. In order to obtain arcs with new sizes

one should make sufficiently many attempts with the randomized greedy algorithm.

Chapter 4

The spectrum of quantum caps in $PG(4,4)$

In the second half of the 20-th Century the new frontiers of modern physics led to the introduction of new concepts in information theory. In particular quantum mechanics has given rise to the concept of quantum information.

The fundamental unit of quantum information is the *quantum bit* (qubit). The qubit is described by a quantum state in a two-state quantum mechanical system. One example of a two state quantum system is the polarization of a single photon.

Feyman in the 1980s [74] showed that there seemed to be essential difficulties in simulating quantum mechanical systems on classical computers and proposed to avoid those difficulties with the construction of computers based on the principles of quantum mechanics.

In 1985 Deutsch [59] asked whether it is possible for a quantum computer to efficiently solve computational problems which have no efficient solution on classical computers. Constructing a simple example, he suggested that quantum computers might be more powerful than classical computers.

This first idea of Deutsch was improved during the subsequent decade. In 1994 Shor [159] presented an algorithm which can factor an integer in polynomial time on a quantum computer.

In the implementation of long quantum computations, there are several major sources of errors: deco-

herence, dissipation, measurement errors, depolarization errors of spin and phase flips, etc. Therefore error correction is indispensable in quantum computing, even more so than in classical computing. In general, errors in quantum computing systems are more complicated than their classical counterparts and therefore correction schemes are also more sophisticated.

In classical computing a basic idea is the *repetition code*, i.e., for instance, the code $0 \mapsto 000, 1 \mapsto 111$. This idea cannot be generalized in a trivial way to quantum computing, as the *No-Cloning Theorem* states that cloning is a non linear operation and cannot be realized by unitary operators, and we cannot create backup copies of a state in the middle of a quantum computation and use them to correct subsequent errors.

The idea behind quantum error correction is to encode quantum states into qubits so that errors or decoherence in a small number of individual qubits will have little or no effect on the encoded data.

The 9-qubit error correction code presented by Shor in 1995 ([160]) is the earliest and also the simplest example of quantum error correcting code (QECC). Shor presented a procedure to encode a single qubit in nine qubits which can restore the original state if no more than one error occurs. It is an example of a quantum $[[9, 1, 3]]$-code.

In 1996 Calderbank and Shor ([36]) and Steane ([161], [162]) presented the 7-qubit CSS QECC. In the same year Laflamme, Miguel, Paz and Zurek ([120]) presented a QECC using only 5 qubits.

In 1998 Calderbank, Rains, Shor and Sloane [35] translated the problem of finding quantum error correcting codes into the problem of determining additive codes over $GF(4)$ which are self-orthogonal with respect to a particular trace inner product. The setting in which quantum error correcting codes exist is $\mathbb{H}^{2^n} = \mathbb{H}^2 \otimes \ldots \otimes \mathbb{H}^2$, where $\mathbb{H}$ is an Hilbert space. An encoding of k qubits into n is a linear mapping $\Psi : \mathbb{H}^{2^k} \to \mathbb{H}^{2^n}$. We usually call $\Psi(\mathbb{H}^{2^k})$ itself the quantum error correcting code, since the error correction properties depend only on the subspace rather than on the mapping (see [35]). For a

more detailed introduction to quantum codes refer to [18], [37], [112], [136], [152], [163].

In the projective space $PG(r,q)$ over the Galois Field $GF(q)$, an n-cap is a set of n points no 3 of which are collinear. An n-cap is called *complete* if it is not contained in an $(n+1)$-cap.

We call a set of n points an *n-quantum* set if the code generated by its matrix is a *quantum stabilizer code* (see Definitions 4.4 and 4.5). If an n-quantum set is a cap in a projective space we call rblue(i.e. the values k such that there exists a quantum k-cap in $PG(4,4)$). They are in one-to-one correspondence with linear pure $[[n, n-10, 4]]$-codes (see [8], [12]).

In 1999 Bierbrauer and Edel showed that 41 is the maximum size of complete caps in $PG(4,4)$ and one of the two non projective equivalent biggest caps is a quantum cap (see [19]). In 2003 the same authors presented a complete 40-cap in $AG(4,4)$ which is also a quantum cap (see [20]).

In 2008 Tonchev constructed quantum caps of sizes $10, 12, 14-27, 29, 31, 33, 35$ (see [176]), starting from the complete 41-quantum cap in $PG(4,4)$ (see [19]).

It is not difficult to see ([7]) that this method cannot produce quantum caps of sizes between 36 and 40 in $PG(4,4)$.

In 2009 we found examples of quantum caps of sizes $13, 28, 30, 32, 34, 36, 38$, see [7].

We determine in Section 4.5, by a computer based search, the set of sizes (called in this contest spectrum) of quantum caps in $PG(4,4)$ (and therefore of pure linear quantum $[[n, n-10, 4]]$-codes) proving that there exist no examples of quantum caps of sizes 11, 37 and 39. Thus we proved the following:

Theorem 4.1. *If $\mathcal{K} \subset PG(4,4)$ is a quantum cap, then $|\mathcal{K}| \in [10, 41] \setminus \{11, 37, 39\}$.*

In Section 4.1 we present some theoretical results which have been utilized in the computer-based search of quantum caps in $PG(4,4)$ (see 4.5.1). Similar results appeared in [83], but we decide to give them with the proofs since they were obtained independently. In Section 7.2 we determine all the

lengths of linear pure quantum codes of type $[[n, n-10, 4]]$ and in Section 4.5.3 we give examples of quantum caps not equivalent to those already known.

4.1 Theoretical background

A classical linear code $\mathcal{C}$ over $GF(q)$ is determined by three parameters n, k, d which measure length, dimension and minimum distance of the code (which gives a rating of the number of errors the code can correct), respectively.

The main problem of coding theory is the optimization of one of these parameters when the others are fixed; for instance maximizing the minimum distance for a fixed length and dimension.

A linear q-ary $[n, k]$-code $\mathcal{C}$ is a k-dimensional subspace of $GF(q)^n$. A q-linear q^m-ary $[n, k]$-code is a km-dimensional $GF(q)$-subspace of $GF(q^m)^n$. Observe that the dimension k need not be integral (it can have m in the denominator). In particular an *additive* code $\mathcal{C}$ over $GF(4)$ is a subset of $GF(4)^n$ closed under addition. Most of the quantum codes known today are the so-called stabilizer codes.

Definition 4.2. Let $\mathbf{V}$ be a vectorial space over $GF(q)$. A *symplectic form* is a function $f : \mathbf{V} \times \mathbf{V} \to GF(q)$ satisfying the following:

1. $f(\alpha_1 x_1 + \alpha_2 x_2, y) = \alpha_1 f(x_1, y) + \alpha_2 f(x_2, y) \quad \forall\, x_1, x_2, y \in \mathbf{V},\ \alpha_1, \alpha_2 \in GF(q)$
2. $f(y, x) = -f(x, y) \quad \forall\, x, y \in \mathbf{V}$
3. $f(x, x) = 0 \quad \forall x \in \mathbf{V}$
4. $f(x, y) = 0 \quad \forall\, y \in \mathbf{V} \iff x = 0.$

It can be shown that $\dim_{GF(q)}(\mathbf{V}) = 2n$ and there exists only one type of symplectic form up to base change. It is always possible to choose a base of the space $\mathbf{V}$ such that if $x = (x_1, x_2, \ldots, x_{2n-1}, x_{2n})$,

$y = (y_1, y_2, \ldots, y_{2n-1}, y_{2n}) \in \mathbf{V}$ then

$$f(x, y) = x_1 y_2 - x_2 y_1 + \ldots + x_{2n-1} y_{2n} - x_{2n} y_{2n-1}.$$

Given a vector $x = (x_1, x_2, \ldots, x_{2n-1}, x_{2n}) \in \mathbf{V}$ we define the *weight* of x $(w(x))$ the number of $i \in \{1 \ldots n\}$ such that at least one of x_{2i-1} and x_{2i} is $\neq 0$.

In particular, in our work, we consider $q = 2$ and then $w(0,0) = 0$, $w(1,0) = 1$, $w(0,1) = 1$ and $w(1,1) = 1$. It is possible to associate in a natural way a particular element of $GF(q^2)$ to an element in $GF(q)^2$. For our purposes we consider $\varphi : GF(4) \to GF(2)^2$, with $\varphi(0) = (0,0)$, $\varphi(1) = (0,1)$, $\varphi(\omega) = (1,0)$ and $\varphi(\omega + 1) = (1,1)$, where $\omega \in GF(4)$ is such that $\omega^2 + \omega + 1 = 0$. Observe that φ is an homomorphism between the groups $(GF(4), +)$ and $(GF(2)^2, +)$. The function φ can be extended to a function $\Phi : GF(4)^n \to GF(2)^{2n}$ in a natural way: $\Phi(w_1, \ldots, w_n) = (\varphi(w_1), \ldots, \varphi(w_n))$.

The following theorem gives a connection between quantum error correcting codes and classical linear codes.

Theorem 4.3 (Theorem 1, [35])**.** *Suppose $\mathcal{C}$ is a linear $(n-k)$-dimensional subspace of $GF(2)^{2n}$ such that $\mathcal{C} \subseteq \mathcal{C}^{\perp}$, where the duality is with respect to the symplectic form. If there are no vectors of weight $< d$ in $\mathcal{C}^{\perp} \setminus \mathcal{C}$, then there is a quantum error correcting code mapping k qubits to n qubits which can correct $\lfloor \frac{d-1}{2} \rfloor$ errors.*

By the previous theorem the following definitions are quite natural:

Definition 4.4. A *quaternary quantum stabilizer code* is an additive quaternary code $\mathcal{C}$ contained in its dual $\mathcal{C}^{\perp}$, where the duality is with respect to the symplectic form.

In particular:

Definition 4.5. A quantum code $\mathcal{C}$ with parameters n, k, d ($[[n, k, d]]$-code), where $k > 0$, is a quaternary quantum stabilizer code of binary dimension $n - k$ satisfying the following: any codeword of $\mathcal{C}^{\perp}$ having weight at most $d - 1$ is in $\mathcal{C}$.

The code is *pure* if $\mathcal{C}^{\perp} \setminus \{\overline{0}\}$ does not contain codewords of weight $< d$, equivalently if $\mathcal{C}$ has strength $t \geq d - 1$.

An $[[n, 0, d]]$-code $\mathcal{C}$ is a self-dual quaternary quantum stabilizer code of strength $t = d - 1$.

Since any $GF(2)$-base of an $[[n, k, d]]$-code $\mathcal{C}$ can be translated in a set of elements of $GF(2)^{2n}$ using the function Φ described above, the generator matrix over $GF(2)$ of $\mathcal{C}$ has dimension $(n - k) \times 2n$ and assumes the form:

$$\begin{pmatrix} P_{1,1} & Q_{1,1} & P_{1,2} & Q_{1,2} & \dots & P_{1,n} & Q_{1,n} \\ P_{2,1} & Q_{2,1} & P_{2,2} & Q_{2,2} & \dots & P_{2,n} & Q_{2,n} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ P_{n-k,1} & Q_{n-k,1} & P_{n-k,2} & Q_{n-k,2} & \dots & P_{n-k,n} & Q_{n-k,n} \end{pmatrix}$$

with $P_{i,j}, Q_{i,j} \in \mathbb{Z}_2 \ \forall i = 1, \dots, n - k \quad j = 1, \dots, n$.

We can view each column as a point in the binary projective space $PG(n - k - 1, 2)$ and it is possible to associate a line to each pair of columns. Hence the geometric description of the quantum code is in terms of a system of n lines (*codelines*) generated by the n pairs of columns corresponding to the n coordinate sections. However it is possible that the 0-column occurs and that two different columns in the same coordinate section are identical.

For a more detailed geometric description of quantum codes in terms of points and lines in finite projective spaces see [23] and [83].

Let w_1 and w_2 be two codewords of the code $\mathcal{C}$, $w_1 = A_{h_1} + \ldots + A_{h_{j_1}}$ and $w_2 = A_{i_1} + \ldots + A_{i_{j_2}}$, where A_h is the h-th row of the generator matrix. We can associate with them two hyperplanes H_1 and H_2 in

$PG(n-k-1,2)$ with equations

$$H_1 : x_{h_1} + \ldots + x_{h_{j_1}} = 0 \qquad \text{and} \qquad H_2 : x_{i_1} + \ldots + x_{i_{j_2}} = 0.$$

Lemma 4.6. *Let L_s $(s = 1, \ldots, n)$ be a line of the $[[n,k,d]]$-code $\mathcal{C}$, w_1, w_2 two codewords of $\mathcal{C}$ and H_1, H_2 the corresponding hyperplanes. Let $\mathcal{S}$ be the secundum $H_1 \cap H_2$. Then L_s meets the secundum $\mathcal{S}$ if and only if the symplectic product of the s-th coordinate section of w_1 and w_2 is 0.*

Proof. We can suppose that the s-th entries of w_1 and w_2 are the pairs

$$(P_{h_1,s} + \ldots + P_{h_{j_1},s}, Q_{h_1,s} + \ldots + Q_{h_{j_1},s}) = (H_1(P_s), H_1(Q_s))$$

and

$$(P_{i_1,s} + \ldots + P_{i_{j_2},s}, Q_{i_1,s} + \ldots + Q_{i_{j_2},s}) = (H_2(P_s), H_2(Q_s)).$$

Let S be the secundum $H_1 \cap H_2$ and $L_s = \{P_s, Q_s, R_s = P_s + Q_s\}$.

We have to examine two cases:

1. $S \cap L_s \neq \emptyset$. We can have only one of the following situations:

   - $P_s \in \mathcal{S} \cap L_s$ or $Q_s \in \mathcal{S} \cap L_s$. The s-th entries of w_1 and w_2 are $(0, \alpha)$ and $(0, \beta)$ or $(\alpha, 0)$ and $(\beta, 0)$ with $\alpha, \beta \in \mathbb{Z}_2$. The symplectic product of these entries is 0.
   - $R_s \in \mathcal{S} \cap L_s$. We have $Q_s = P_s + R_s$. Then $H_1(Q_s) = Q_{h_1,s} + \ldots + Q_{h_{j_1},s} = H_1(P_s + R_s) = (P_{h_1,s} + \ldots + P_{h_{j_1},s}) + (R_{h_1,s} + \ldots + R_{h_{j_1},s}) = P_{h_1,s} + \ldots + P_{h_{j_1},s} = H_1(P_s)$ and $H_2(Q_s) = Q_{i_1,s} + \ldots + Q_{i_{j_2},s} = H_2(P_s + R_s) = (P_{i_1,s} + \ldots + P_{i_{j_2},s}) + (R_{i_1,s} + \ldots + R_{i_{j_2},s}) = P_{i_1,s} + \ldots + P_{i_{j_2},s} = H_2(P_s)$, and the s-th entries of w_1 and w_2 are (α, α) and (β, β) and their symplectic product is 0, for all α and β in $\mathbb{Z}_2$.

2. $S \cap L_s = \emptyset$. In this case one point of L_s belongs to H_1, another one (different from the previous one) belongs to H_2 and the third point of L_s does not belong to H_1 nor to H_2. We can have only one of the following situations.

   - $R_s \notin H_1 \cup H_2$. If $H_1(P_s) = 1$, i.e. P_s does not belong to H_1, P_s has to belong to H_2, and then $H_2(P_s) = 0$; moreover $H_1(Q_s) = 0$ and $H_2(Q_s) = 1$. Instead, if $H_1(P_s) = 0$ then $H_2(P_s) = 1$, $H_1(Q_s) = 1$ and $H_2(Q_s) = 0$. Briefly, the s-th entry of w_1 is $(H_1(P_s), H_1(Q_s))$, i.e. $(1, 0)$ or $(0, 1)$, and the s-th entry of w_2 is respectively $(0, 1)$ or $(1, 0)$. The symplectic product of these entries is 1.
   - $P_s \notin H_1 \cup H_2$. Then $H_1(P_s) = H_2(P_s) = 1$, and Q_s belongs to only one of the hyperplanes, i.e. $H_1(Q_s) = 1$ and $H_2(Q_s) = 0$ or $H_1(Q_s) = 0$ and $H_2(Q_s) = 1$. The s-th entries of w_1 and w_2 are $(1, 0)$ and $(1, 1)$ or $(1, 1)$ and $(1, 0)$. The symplectic product of these entries is 1.
   - $Q_s \notin H_1 \cup H_2$. We can do the same considerations of the previous point and the s-th entries of w_1 and w_2 are $(0, 1)$ and $(1, 1)$ or $(1, 1)$ and $(0, 1)$. The symplectic product of these entries is 1.

From the above considerations, the line L_s meets the secundum S if and only if the symplectic product of the s-th coordinate section is 0. □

The following theorem gives a first geometrical characterization of quantum codes.

Theorem 4.7. *The following are equivalent:*

1. *a* pure *quantum* $[[n, k, t + 1]]_2$*-code* $\mathcal{C}$*;*
2. *a set of* n *lines in* $PG(n - k - 1, 2)$ *any* t *of which are in general position and such that for each* **secundum** S *(subspace of codimension 2) the number of lines which are skew to* S *is even.*

Proof. We know by Lemma 4.6 that a line L_s meets the secundum $\mathcal{S}$ corresponding to the codewords w_1 and w_2 if and only if the symplectic product of the s-th coordinate section of w_1 and w_2 is 0. Then the symplectic product of two codewords is given by the number of $s \in \{1, \ldots, n\}$ (mod 2) such that L_s is skew to S.

$1 \Rightarrow 2$. If $\mathcal{C}$ is a pure quantum code, then all the codewords are orthogonal to each other with respect to the symplectic product and then, for each secundum S, the number of lines skew to S must be even.

$2 \Rightarrow 1$. If for each secundum $S = H_1 \cap H_2$ the number of lines skew to it is even, then the symplectic product between the codewords corresponding to H_1 and H_2 is equal to 0 and the set of codewords $\mathcal{C}$ is a pure quantum code. □

According to Definition 4.5, a quantum code is required to be linear only over $GF(2)$.

Let

$$G = \begin{pmatrix} P_{1,1} & Q_{1,1} & P_{1,2} & Q_{1,2} & \ldots & P_{1,n} & Q_{1,n} \\ P_{2,1} & Q_{2,1} & P_{2,2} & Q_{2,2} & \ldots & P_{2,n} & Q_{2,n} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ P_{n-k,1} & Q_{n-k,1} & P_{n-k,2} & Q_{n-k,2} & \ldots & P_{n-k,n} & Q_{n-k,n} \end{pmatrix}$$

be a generator matrix of the code $\mathcal{G}$ over $GF(2)$ and $G_1 \ldots, G_{n-k}$ its rows. If moreover the code is linear over $GF(4)$, i.e. it is closed under multiplication by ω (where ω is such that $\omega^2 + \omega + 1 = 0$), we associate to $00, 10, 01, 11 \in GF(2)^2$ the elements $0, 1, \omega, \omega + 1 \in GF(4)$ and then to $v \in GF(2)^{2n}$ an element $\phi(v) \in GF(4)^n$. By $GF(4)$-linearity, we can suppose that $\exists\, v_1, \ldots, v_{\frac{n-k}{2}} \in GF(2)^{2n}$: $\langle v_1, \phi^{-1}(\omega\phi(v_1)), \ldots, v_{\frac{n-k}{2}}, \phi^{-1}(\omega\phi(v_{\frac{n-k}{2}}))\rangle = \langle G_1, \ldots, G_{n-k}\rangle$ as subspace of $GF(2)^{2n}$. Then a generator matrix over $GF(4)$ of the code is:

$$\overline{G} = \begin{pmatrix} W_{1,1} & W_{1,2} & \ldots & W_{1,n} \\ W_{2,1} & W_{2,2} & \ldots & W_{2,n} \\ \vdots & \vdots & & \vdots \\ W_{\frac{n-k}{2},1} & W_{\frac{n-k}{2},2} & \ldots & W_{\frac{n-k}{2},n} \end{pmatrix}$$

with $\phi(v_i) = (W_{i,1}, \ldots, W_{i,n}) \in GF(4)^n \ \forall i = 1, \ldots, \frac{n-k}{2}$. Therefore a $[[n,k,d]]$-quantum code linear over $GF(4)$ can be described by a generator matrix of dimensions $\frac{n-k}{2} \times n$.

Let H be a hyperplane of $PG(\frac{n-k}{2} - 1, 4)$ of equation:

$$H : \alpha_1 z_1 + \ldots + \alpha_{\frac{n-k}{2}} z_{\frac{n-k}{2}} = 0 \text{ with } \alpha_i = a_i + \omega b_i \quad a_i, b_i \in GF(2) \quad \forall i = 1, \ldots, \frac{n-k}{2}.$$

Let $z_i \in GF(4)$ be $x_i + \omega y_i$, with $x_i, y_i \in GF(2)$. Then we can associate with H two different hyperplanes of $PG(n-k-1, 2)$:

$$\alpha_1 z_1 + \ldots + \alpha_{\frac{n-k}{2}} z_{\frac{n-k}{2}} = 0 \iff (a_1 + \omega b_1)(x_1 + \omega y_1) + \ldots + (a_{\frac{n-k}{2}} + \omega b_{\frac{n-k}{2}})(x_{\frac{n-k}{2}} + \omega y_{\frac{n-k}{2}}) = 0$$

$$\iff a_1 x_1 + \ldots + a_{\frac{n-k}{2}} x_{\frac{n-k}{2}} + \omega(b_1 x_1 + \ldots + b_{\frac{n-k}{2}} x_{\frac{n-k}{2}} + a_1 y_1 + \ldots + a_{\frac{n-k}{2}} y_{\frac{n-k}{2}}) + \omega^2(b_1 y_1 + \ldots + b_{\frac{n-k}{2}} y_{\frac{n-k}{2}}) = 0$$

$$\iff a_1 x_1 + \ldots + a_{\frac{n-k}{2}} x_{\frac{n-k}{2}} + b_1 y_1 + \ldots + b_{\frac{n-k}{2}} y_{\frac{n-k}{2}} +$$

$$\omega(b_1 x_1 + \ldots + b_{\frac{n-k}{2}} x_{\frac{n-k}{2}} + a_1 y_1 + \ldots + a_{\frac{n-k}{2}} y_{\frac{n-k}{2}} + b_1 y_1 + \ldots + b_{\frac{n-k}{2}} y_{\frac{n-k}{2}}) = 0$$

$$\iff a_1 x_1 + \ldots + a_{\frac{n-k}{2}} x_{\frac{n-k}{2}} + b_1 y_1 + \ldots + b_{\frac{n-k}{2}} y_{\frac{n-k}{2}} = 0 \quad \wedge$$

$$b_1 x_1 + \ldots + b_{\frac{n-k}{2}} x_{\frac{n-k}{2}} + a_1 y_1 + \ldots + a_{\frac{n-k}{2}} y_{\frac{n-k}{2}} + b_1 y_1 + \ldots + b_{\frac{n-k}{2}} y_{\frac{n-k}{2}} = 0,$$

since $\omega^2 = \omega + 1$. Then we can associate with H the following secundum

$$S : \begin{cases} a_1 x_1 + \ldots + a_{\frac{n-k}{2}} x_{\frac{n-k}{2}} + b_1 y_1 + \ldots + b_{\frac{n-k}{2}} y_{\frac{n-k}{2}} & = & 0 \\ b_1 x_1 + \ldots + b_{\frac{n-k}{2}} x_{\frac{n-k}{2}} + (a_1 + b_1) y_1 + \ldots + (a_{\frac{n-k}{2}} + b_{\frac{n-k}{2}}) y_{\frac{n-k}{2}} & = & 0 \end{cases} \tag{4.1}$$

Clearly not each secundum in $PG(n-k-1, 2)$ corresponds to a hyperplane of $PG(\frac{n-k}{2} - 1, 4)$: a secundum

$$S' : \begin{cases} a_1 x_1 + \ldots + a_{\frac{n-k}{2}} x_{\frac{n-k}{2}} + b_1 y_1 + \ldots + b_{\frac{n-k}{2}} y_{\frac{n-k}{2}} & = & 0 \\ a'_1 x_1 + \ldots + a'_{\frac{n-k}{2}} x_{\frac{n-k}{2}} + b'_1 y_1 + \ldots + b'_{\frac{n-k}{2}} y_{\frac{n-k}{2}} & = & 0 \end{cases}$$

is a hyperplane in $PG(\frac{n-k}{2} - 1, 4) \iff (b_i = a'_i) \wedge (a_i + b_i = b'_i) \quad \forall i = 1, \ldots, \frac{n-k}{2}$. In this case we say S is $GF(4)$-hyperplane.

Let $U = (z_1, \ldots, z_{\frac{n-k}{2}}) = (x_1 + \omega y_1, \ldots, x_{\frac{n-k}{2}} + \omega y_{\frac{n-k}{2}}) \in PG(\frac{n-k}{2} - 1, 4)$ be a point. It corresponds to the line $l_U \subset PG(n-k-1, 2)$ through the points

$$P_U = (x_1, y_1, \ldots, x_{\frac{n-k}{2}}, y_{\frac{n-k}{2}}) \quad \text{and} \quad Q_U = (y_1, x_1 + y_1, \ldots, y_{\frac{n-k}{2}}, x_{\frac{n-k}{2}} + y_{\frac{n-k}{2}}).$$

Remark 4.8. *Let H be a hyperplane in $PG(\frac{n-k}{2} - 1, 4)$ and $\mathcal{S}$ the corresponding secundum in $PG(n-k-1, 2)$. Let $U \in PG(\frac{n-k}{2} - 1, 4)$ be a point and $l_U = \{P_U, Q_U, P_U + Q_U\} \subset PG(n-k-1, 2)$ the corresponding line. Then*

$$U \in H \iff l_U \cap \mathcal{S} \neq \emptyset$$

Proof. Let $\mathcal{S}$ be the intersection of two hyperplanes $\mathcal{S}_1$ and $\mathcal{S}_2$.

- If $U \in H$ then, by (4.1), $\mathcal{S}_1(P_U) = \mathcal{S}_2(P_U) = 0$ and $P_U \in l_U \cap \mathcal{S}$.

- If $U \notin H$ then either $\mathcal{S}_1(P_U) \neq 0$ or $\mathcal{S}_2(P_U) \neq 0$. We have $\mathcal{S}_2(P_U) = \mathcal{S}_1(Q_U)$, $\mathcal{S}_1(P_U) = \mathcal{S}_2(P_U + Q_U)$ and $\mathcal{S}_2(Q_U) = \mathcal{S}_1(P_U + Q_U)$. Note that a line intersects a hyperplane in 1 or 3 points.
  Suppose $\mathcal{S}_1(P_U) \neq 0$. Then $\mathcal{S}_2(P_U + Q_U) \neq 0$. Hence $P_U, P_U + Q_U \notin \mathcal{S}$. If $Q_U \in \mathcal{S}$ then $\mathcal{S}_1(Q_U) = \mathcal{S}_2(Q_U) = 0$, $\mathcal{S}_2(P_U) = \mathcal{S}_1(P_U + Q_U) = 0$, $l_U \cap \mathcal{S}_1 = \{Q_U, P_U + Q_U\}$ and we have a contradiction. Therefore $Q_U \notin \mathcal{S}$ and $l_U \cap \mathcal{S} = \emptyset$.
  Suppose $\mathcal{S}_2(P_U) \neq 0$. Then $\mathcal{S}_1(Q_U) \neq 0$. Hence $P_U, Q_U \notin \mathcal{S}$. If $(P_U + Q_U) \in \mathcal{S}$ then $\mathcal{S}_1(P_U + Q_U) = \mathcal{S}_2(P_U + Q_U) = 0$, $\mathcal{S}_1(P_U) = \mathcal{S}_2(Q_U) = 0$, $l_U \cap \mathcal{S}_1 = \{P_U, P_U + Q_U\}$ and we have a contradiction. Therefore $(P_U + Q_U) \notin \mathcal{S}$ and then $l_U \cap \mathcal{S} = \emptyset$.

□

The following theorem gives a geometrical description of pure linear quantum codes.

Theorem 4.9 ([23], [35], [83])**.** *The following are equivalent:*

1. *A pure quantum $[[n,k,d]]$-code which is linear over $GF(4)$.*

2. *A set of n points in $PG(\frac{n-k}{2}-1,4)$ of strength $t=d-1$, such that the intersection size with any hyperplane has the same parity as n.*

3. *An $[n,k]_4$ linear code of strength $t=d-1$, all of whose weights are even.*

4. *An $[n,k]_4$ linear code of strength $t=d-1$ which is self-orthogonal with respect to the Hermitian form.*

Proof. $1 \Rightarrow 2$. Let $\mathcal{C}$ be a $[[n,k,d]]$-code. By Theorem 4.7, for each secundum $S \subset PG(n-k-1,2)$ the number of codelines which are skew to S is even. Then, by Remark 4.8, for each hyperplane $H \subset PG(\frac{n-k}{2}-1,4)$ the number of codepoints not belonging to the hyperplane is even.

$2 \Rightarrow 1$. We have to prove that for each secundum $S \subset PG(n-k-1,2)$ the number of codelines skew to S is even.

Let S be a secundum of $PG(n-k-1,2)$. If S is a $GF(4)$-hyperplane then by Remark 4.8 the number of codelines skew to S is even.

Consider now a secundum S which is not a hyperplane of $PG(\frac{n-k}{2}-1,4)$ and

$$\omega S = \{\omega P \in PG(n-k-1,2) \mid P \in S\} =$$

$$\{(y_1, x_1+y_1, \ldots, y_{\frac{n-k}{2}}, x_{\frac{n-k}{2}}+y_{\frac{n-k}{2}}) \in PG(n-k-1,2) \mid (x_1,y_1,\ldots,x_{\frac{n-k}{2}},y_{\frac{n-k}{2}}) \in S\}.$$

$K = S \cap \omega S$ is the greater $GF(4)$-subspace contained in S. In fact K is clearly a subspace of $PG(n-k-1,2)$, it is closed under multiplication by ω and then is a $GF(4)$-subspace. Finally every other $GF(4)$-subspace contained in S is closed under multiplication by ω and then contained in ωS. Let S be described by these equations:

$$S : \begin{cases} a_1 x_1 + \ldots + a_{\frac{n-k}{2}} x_{\frac{n-k}{2}} + b_1 y_1 + \ldots + b_{\frac{n-k}{2}} y_{\frac{n-k}{2}} &= 0 \\ a'_1 x_1 + \ldots + a'_{\frac{n-k}{2}} x_{\frac{n-k}{2}} + b'_1 y_1 + \ldots + b'_{\frac{n-k}{2}} y_{\frac{n-k}{2}} &= 0 \end{cases}$$

then ωS is described by the equations:

$$\omega S : \begin{cases} (a_1+b_1)x_1 + \ldots + (a_{\frac{n-k}{2}} + b_{\frac{n-k}{2}}) x_{\frac{n-k}{2}} + a_1 y_1 + \ldots + a_{\frac{n-k}{2}} y_{\frac{n-k}{2}} &= 0 \\ (a'_1+b'_1)x_1 + \ldots + (a'_{\frac{n-k}{2}} + b'_{\frac{n-k}{2}}) x_{\frac{n-k}{2}} + a'_1 y_1 + \ldots + a'_{\frac{n-k}{2}} y_{\frac{n-k}{2}} &= 0 \end{cases}$$

Then K is described by:

$$K : \begin{cases} a_1 x_1 + \ldots + a_{\frac{n-k}{2}} x_{\frac{n-k}{2}} + b_1 y_1 + \ldots + b_{\frac{n-k}{2}} y_{\frac{n-k}{2}} &= 0 \\ a'_1 x_1 + \ldots + a'_{\frac{n-k}{2}} x_{\frac{n-k}{2}} + b'_1 y_1 + \ldots + b'_{\frac{n-k}{2}} y_{\frac{n-k}{2}} &= 0 \\ (a_1+b_1)x_1 + \ldots + (a_{\frac{n-k}{2}} + b_{\frac{n-k}{2}}) x_{\frac{n-k}{2}} + a_1 y_1 + \ldots + a_{\frac{n-k}{2}} y_{\frac{n-k}{2}} &= 0 \\ (a'_1+b'_1)x_1 + \ldots + (a'_{\frac{n-k}{2}} + b'_{\frac{n-k}{2}}) x_{\frac{n-k}{2}} + a'_1 y_1 + \ldots + a'_{\frac{n-k}{2}} y_{\frac{n-k}{2}} &= 0 \end{cases}$$

Since S is not a $GF(4)$-hyperplane and the dimension of K has to be even (it is the binary image of a $GF(4)$-space), its four equations are independent and then K has binary codimension equal to 4.

We know that there exist exactly five $GF(4)$-hyperplanes H_1, H_2, H_3, H_4, H_5 (corresponding to the secunda $S_1, S_2, S_3, S_4, S_5 \subset PG(n-k-1,2)$) which contain K and partition the remaining points. Let m be the number of points belonging to K and a_i the number of them contained in $H_i \setminus K$. Then we have

$$n = m + \sum_{i=1}^{5} a_i.$$

By hypothesis we know that the number of points not belonging to a $GF(4)$-hyperplane is even. In particular for the H_i we have that

$$n - (m + a_j) = \sum_{i=1, i \neq j}^{5} a_i$$

is even for each $j = 1, \ldots, 5$ and then each a_i has the same parity. By hypothesis the secundum S is not a $GF(4)$-hyperplane, therefore it cannot coincide with any secundum S_i. We can see how the points of S are divided in the secunda S_i:

- Let $x_0 \in S \setminus K$ be a point; then it belongs to some S_{i_1} and then $K' = (K + x_0) \cup \{x_0\} = \{x + x_0 \mid x \in K\} \cup \{x_0\} \subset S_{i_1}$ by linearity. In this way we have obtained $|K| + |K| + 1 = 2|K| + 1$ points.

- Let y_0 be a point of $S \setminus K'$: then y_0 is not in S_{i_1} since we would have $S = S_{i_1}$ that is absurd. Then $y_0 \in S_{i_2}$ with $i_1 \neq i_2$ and $K'' = (K + y_0) \cup \{y_0\} \subset S_{i_2}$ by linearity. We have now $3|K| + 2$ points.

- We consider $K''' = K' + y_0$: it cannot be contained in S_{i_2}, because we would have $x_0 \in S_{i_2}$, but $x_0 \in S_{i_1}$. Then we have $K''' \subset H_{i_3}$, with $i_3 \neq i_1, i_2$. We have obtained $4|K| + 3$ points.

- We have also that $|S| = 2^{n-k-2} - 1$, and $|K| = 2^{n-k-4} - 1$. Then $4|K| + 3 = 4(2^{n-k-4} - 1) + 3 = 2^{n-k-2} - 4 + 3 = 2^{n-k-2} - 1 = |S|$ and $S = K \cup K' \cup K'' \cup K'''$.

It is clear that S is contained in three different secunda S_i which are $GF(4)$-hyperplanes. All the quaternary points belonging to these particular $GF(4)$-hyperplanes correspond to lines which do not intersect the S_i. In fact, as each set $K \cup K'$, $K \cup K''$ e $K \cup K'''$ is a subspace of S_{i_1}, S_{i_2}, S_{i_3} of binary codimension 3, a line contained in S_{i_1}, S_{i_2} or S_{i_3} must meet them. Then only the $GF(4)$-points belonging to H_j, with $j \neq i_1, i_2, i_3$ correspond to lines which do not intersect S and the number of these lines is the sum of two particular a_i, and it is even.

2 $\iff$ 3. We consider the correspondence between a codeword and a hyperplane of $PG(\frac{n-k}{2} - 1, 4)$

$$x = \alpha_1 A_{i_1} + \ldots + \alpha_i A_{i_j} \leftrightsquigarrow H : \alpha_1 x_{i_1} + \ldots + \alpha_i x_{i_j} = 0.$$

where $\alpha_i \in GF(4)$. If a codepoint belongs to H then the corresponding entry in the codeword is equal to 0 and viceversa: the entries not equal to 0 correspond to codepoints not belonging to the hyperplane. Then if every hyperplane contains a number of points with the same parity of n, the remaining even codepoints correspond to entries not equal to 0 in the codeword. Viceversa if a codeword has even weight, i.e. the number of entries not equal to 0 is even, we have that the number of the points which do not belong to the hyperplane is even and therefore the number of the codepoints belonging to H has the same parity with n (the total number of points).

3 $\iff$ 4. It follows from Theorem 3 and Theorem 4 of [35]. □

These theoretical results provide a framework for the search of quantum caps in $PG(4,4)$, corresponding to $GF(4)$-linear pure $[[n, n-10, 4]]$-codes.

4.2 Theoretical recursive constructions

In this section some recursive constructions of quantum caps are presented.

Theorem 4.10. *Let K_1, K_2 be disjoint pre-quantum sets in $PG(m-1,4)$. Then $K_1 \cup K_2$ is pre-quantum.*

Let $K_1 \subset K_2$ be pre-quantum sets. Then also $K_2 \setminus K_1$ is pre-quantum.

Theorem 4.11. *Let Π_1, Π_2 be different hyperplanes of $PG(m,4)$ and $K_i \subset \Pi_i$ be pre-quantum caps such that $K_1 \cap \Pi_1 \cap \Pi_2 = K_2 \cap \Pi_1 \cap \Pi_2$. Then the symmetric sum $K_1 + K_2 = (K_1 \setminus K_2) \cup (K_2 \setminus K_1)$ is a pre-quantum cap.*

Proof. As $K_1 + K_2$ does not meet $\Pi_1 \cap \Pi_2$, it is a cap. Only the quantum condition needs to be verified. Let H be a hyperplane. If H contains $\Pi_1 \cap \Pi_2$ there is no problem. Assume this is not the case. Then H meets each of $\Pi_1, \Pi_2, \Pi_1 \cap \Pi_2$ in a hyperplane. By the pre-quantum condition applied to $K_i \subset \Pi_i$ it follows that the sets $(K_1 \cap K_2) \setminus H, K_1 \setminus (K_2 \cup H), K_2 \setminus (K_1 \cup H)$ all have the same parity. □

Here are two applications of Theorem 4.11: Let $K_i \subset E_i$ be hyperovals in planes E_i of $PG(3,4), i = 1,2$. If $E_1 \cap E_2$ is an exterior line of both K_1 and K_2, then $K_1 \cup K_2$ is a quantum 12-cap in $PG(3,4)$. If K_1 and K_2 meet in two points, then $K_1 + K_2$ is a quantum 8-cap.

Theorem 4.12. *Π_1, Π_2 be different hyperplanes of $PG(m,4), S = \Pi_1 \cap \Pi_2$. Let $K_1 \subset \Pi_1$ be a quantum cap in Π_1 and $K_2 \subset \Pi_2 \setminus S$ an (affine) pre-quantum cap. Assume $K_2 \cup (K_1 \cap S)$ is a cap. Then $K_1 \cup K_2$ is a quantum cap.*

Proof. $K_1 \cup K_2$ is pre-quantum by Theorem 4.10. It is a cap if and only if $K_2 \cup (K_1 \cap E)$ is a cap. Clearly it is not contained in a hyperplane. □

Theorem 4.12 applies in particular when $|K_1 \cap S| = 1$ and K_2 is a pre-quantum cap which can be extended to a cap by a point in the secundum S.

Theorem 4.13. *Let Π_1, Π_2 be different $(m-2)$-dimensional subspaces of $PG(m,4)$ which together generate $PG(m,4)$. Let $K_i \subset \Pi_i$ be pre-quantum caps such that $K_1 \cap \Pi_1 \cap \Pi_2 = K_2 \cap \Pi_1 \cap \Pi_2$. Then the symmetric sum $K_1 + K_2$ is a pre-quantum cap.*

4.3 Quantum caps in $PG(2,4)$

It is an elementary and important fact that the hyperoval in $PG(2,4)$ is the only quantum cap in projective dimension ≤ 2.

Proposition 4.14. *There is no quantum cap in the projective line. The only quantum cap in $PG(2,4)$ is the hyperoval. This is the uniquely determined smallest quantum cap in any projective dimension.*

Proof. It is immediately clear that sets of one or two points in $PG(1,4)$ are not quantum. All caps in $PG(2,4)$ are contained in the hyperoval. For any proper subset K of the hyperoval there are lines

avoiding the set as well a tangents. This shows that K is not quantum. Consider a quantum cap K of size $n \leq 6$ in $PG(m,4)$. Observe that a contradiction is obtained if we can find hyperplanes intersecting K in different parities. If $n = 3$, then the ambient space is $PG(2,4)$, contradiction. If $n = 4$, then K is in general position in $PG(3,4)$, contradiction. If $n = 5$, then either K is in general position in $PG(4,4)$ or K is a coordinate frame in $PG(3,4)$ or $K \subset PG(3,4)$ with some 4 points on a plane, contradiction in all cases. Let finally $n = 6$ and K not in $PG(2,4)$. If $K \subset PG(3,4)$ then some 4 points are in a plane and a contradiction is obtained. If $K \subset PG(5,4)$ then K is in general position and a contradiction results. The last case is $K \subset PG(4,4)$. Let Π be a plane meeting K in precisely 3 points. Each of the 5 solids containing Π must pick up at least one additional point of K. This yields the contradiction $|K| \geq 3 + 5$. endproof

$\mathcal{K}(2,6)$					
1	0	0	1	1	1
0	1	0	1	ω^2	ω
0	0	1	1	ω	ω^2

The quantum code described by the hyperoval has parameters $[[6,0,4]]$.

4.4 Quantum caps in $PG(3,4)$

In this section we give a complete description of the quantum caps in $PG(3,4)$. This is useful in view of general recursive constructions. Equivalence is with respect to the action of the group $G = P\Gamma L(4,4)$ of order $g = 2^{13}(4^4-1)(4^3-1)(4^2-1) = 2^{13} \times 3^4 \times 5^2 \times 7 \times 17$.

Theorem 4.15. *The sizes of quantum caps in $PG(3,4)$ are $8, 12, 14$ and 17. For each of these cardinalities there is exactly one quantum cap in $PG(3,4)$ up to equivalence.*

The unique quantum cap in projective dimension 2, the hyperoval in $PG(2,4)$, will be denoted by $\mathcal{K}(2,6)$. The quantum caps in $PG(3,4)$ will be denoted $\mathcal{K}(3,8), \mathcal{K}(3,12), \mathcal{K}(3,14), \mathcal{K}(3,17)$. Let G_i be

the automorphism group of $\mathcal{K}(3,i)$ (the stabilizer in G) and $g_i = |G_i|$. Denote by a_j the number of planes meeting K in cardinality j (the j-planes). In the remainder of this section we prove Theorem 4.15 and give various descriptions of these four quantum caps.

The elliptic quadric $\mathcal{K}(3,17)$.

The upper bound is obvious: it is known that the unique largest cap in $PG(3,q)$ for $q > 2$ is the elliptic quadric of q^2+1 points. As it meets each hyperplane in 1 or $q+1$ points it follows that the elliptic quadric in $PG(3,4)$ is indeed quantum. G_{17} has order $g_{17} = 16320 = 17 \times 16 \times 15 \times 4$ and contains the simple group $SL(2,16)$ in its sharply triply transitive action on $\mathcal{K}(3,17)$. Clearly $a_1 = 17$ and $a_5 = 68$.

It is known that caps of size 15 or 16 are embedded in the elliptic quadric. It follows that such caps cannot be quantum (see Theorem 4.10). Because of Proposition 4.14 we are reduced to cardinalities between 7 and 14.

A standard counting method is **secundum counting:** in the case of $PG(3,4)$ a secundum is a line. We fix a secant line and study the distribution of points on the 5 planes through the secant. In the case of cardinality 13 this shows because of the quantum condition (see Definitions 4.4 and 4.5) that each secant is contained in precisely 3 planes meeting the cap in 5 points. The number of such planes is therefore $\binom{13}{2} \times 3/10$, contradiction. Cardinality 9 is excluded by the same argument. In cardinality 7 this argument shows that any 4 points are in general position. This defines a $[7,4]_4$-code whose dual has parameters $[7,3,5]_4$ contradicting the Griesmer bound. In cardinality 11, let $e_i, i = 1,3,5$ be the number of planes meeting K in i points. By secundum counting we obtain $e_5 = 11, e_3 = 55$. This implies $e_1 = 19$. On the other hand, let $P \in K$. Consider the pairs (g,E) where g is a secant, $P \in g, g \subset E$ and E a 5-plane. There are 10×2 such pairs. This shows that P is contained in five 5-planes. An analogous count shows that P is in fifteen 3-planes. This shows that P must be on one 1-plane which

yields the contradiction $e_1 = 11 \neq 19$. On the non-existence side it remains to exclude cardinality 10.

Lemma 4.16. *There is no quantum* 10*-cap in* $PG(3,4)$.

Proof. Observe that planes intersect the cap in $0, 2$ or 4 points. In fact, a hyperoval as intersection is excluded as otherwise the complement would be a quantum 4-cap in $PG(3,4)$ or in $PG(2,4)$ which is not possible. The standard counting argument based on secant lines shows that each secant is in precisely four 4-planes. There are 30 such planes and they define a Steiner system $S(3,4,10)$. A generator matrix can be given the form

$$\left(\begin{array}{cccc|cccc|cc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & & & & \\ 0 & 0 & 1 & 0 & 1 & & 0 & & & \\ 0 & 0 & 0 & 1 & 1 & & & 0 & & \end{array}\right)$$

Comparison with the first row shows that in each of the remaining rows the four entries to be determined must be such that each entry occurs twice or not at all. Comparison of two rows shows that the triples of nonzero entries in columns to the right of the sixth column agree in precisely one coordinate and they also satisfy the proportionality condition: if the triples are abc and ade, respectively, then $d/b = e/c$. Moreover no two of the columns to be completed can agree in more than 2 coordinates as otherwise we had a line with more than 2 points.

Clearly we can choose the basis such that $z_1 + z_2$ has weight 6. This means that two of the remaining entries in z_2 are 1. By applying a field automorphism the two last entries can be chosen as ω. There are three non-equivalent possibilities how the entries 1 can be distributed. Assume at first

$$\left(\begin{array}{cccc|cccc|cc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & & \\ 0 & 0 & 1 & 0 & 1 & a & 0 & b & c & d \\ 0 & 0 & 0 & 1 & 1 & & & 0 & & \end{array}\right)$$

Case $b = 1$ is impossible. We can choose $c = \omega$. It follows $(a, b, c, d) = (\omega^2, \omega, \omega, \omega^2)$. The entries in the last row are $efef$ and cannot be completed.

Next consider

$$\left(\begin{array}{cccc|cccc|cc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & \omega & \omega & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & a & 0 & b & c & d \\ 0 & 0 & 0 & 1 & 1 & & & 0 & & \end{array}\right)$$

Clearly $b = \omega$ and $a = 1$ are impossible. We have $b = 1$. By proportionality $a = \omega^2$ and we have

$$\left(\begin{array}{cccc|cccc|cc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & \omega & \omega & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & \omega^2 & 0 & 1 & \omega^2 & 1 \\ 0 & 0 & 0 & 1 & 1 & & & 0 & & \end{array}\right)$$

and this cannot be completed. Finally consider the case

$$\left(\begin{array}{cccc|cccc|cc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & \omega & 1 & \omega \\ 0 & 0 & 1 & 0 & 1 & a & 0 & b & c & d \\ 0 & 0 & 0 & 1 & 1 & & & 0 & & \end{array}\right)$$

$c = 1$ is impossible as then $b = d$. If $d = \omega$, then $c = b\omega^2$. It follows $b = \omega^2$ and this cannot be completed. This shows $b = \omega$ and $c = d\omega^2$. It follows

$$\left(\begin{array}{cccc|cccc|cc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & \omega & 1 & \omega \\ 0 & 0 & 1 & 0 & 1 & \omega^2 & 0 & \omega & \omega & \omega^2 \\ 0 & 0 & 0 & 1 & 1 & e & x & 0 & y & f \end{array}\right)$$

The assumption $x = e, y = f$ leads to a contradiction. We have $x = f, y = e$. The proportionality condition yields $e = \omega^2, f = 1$. The matrix is

$$\left(\begin{array}{cccc|cccc|cc} 1&0&0&0&0&1&1&1&1&1\\ 0&1&0&0&1&0&1&\omega&1&\omega\\ 0&0&1&0&1&\omega^2&0&\omega&\omega&\omega^2\\ 0&0&0&1&1&\omega^2&1&0&\omega^2&1 \end{array}\right)$$

Here the first and the two last points are collinear, contradiction. □

The quantum 8-cap $\mathcal{K}(3,8)$.

Clearly a quantum 8-cap K cannot contain a hyperoval. It follows that each secant is on 3 planes meeting K in cardinality 4. There are therefore 14 such planes and they define a Steiner system $S(3,4,8)$. Write a generator matrix in the form $(I|P)$. Then P has one entry zero in each column, and these occur in different rows. We have the form

$$\left(\begin{array}{cccc|cccc} 1&0&0&0&0&1&1&1\\ 0&1&0&0&1&0&a&b\\ 0&0&1&0&1&c&0&d\\ 0&0&0&1&1&e&f&0 \end{array}\right)$$

(without restriction). Comparison of the first row with others shows $a=b, c=d, e=f$. Comparison of the later rows shows $a=\cdots=f(\neq 0)$. A final obvious manipulation produces the standard generator matrix $(I|I+J)$ of the extended Hamming code. We define $K=\mathcal{K}_8$ to consist of the vectors of odd weight in $\mathbb{F}_2^4$ when interpreted as points in $PG(3,4)$. The automorphism group G_8 has then the form $G_8=E_8GL(3,2)\times Z_2$ of order $g_8=16\times 168$, the direct product of its center (generated by the Frobenius automorphism) and the stabilizer of a plane (the plane $x_1+x_2+x_3+x_4=0$) in $GL(4,2)$. In particular there are precisely $g/g_8=64\times 27\times 25\times 17$ copies of $\mathcal{K}_8$ in $PG(3,4)$. The group G_8 is 3-transitive on the points of the cap.

Here is a different description of $\mathcal{K}_8$: choose hyperovals $\mathcal{O}_1,\mathcal{O}_2$ on two planes which share a common secant. The symmetric sum $\mathcal{O}_1+\mathcal{O}_2$ is then a quantum cap. This is a special case of Theorem 4.11. It follows that we have a copy of $\mathcal{K}(3,8)$. Clearly $a_4=14, a_2=56, a_0=15$. For future reference we think

of $\mathcal{K}(3,8)$ as the set of points in $PG(3,4)$ represented by the vectors of weights 1 or 3 with entries in $\mathbb{F}_2$.

The quantum 14-cap $\mathcal{K}(3,14)$

A 14-cap contained in the elliptic quadric cannot be quantum as otherwise the complementary set of 3 would have to be pre-quantum (see Theorem 4.10). It is known that there is only one 14-cap which is not embedded. This is the complete 14-cap and it is quantum. The complete 14-cap and its automorphism group were described in [19]. Here we want to describe it from scratch.

Proposition 4.17. *The complete* 14*-cap in* $PG(3,4)$ *is the disjoint union of* $\mathcal{K}(3,8)$ *and a hyperoval in a plane.*

Proof. Secundum counting shows that each secant of K must be contained in a plane which meets K in a hyperoval. In particular K contains hyperovals. It follows from Theorem 4.10 that its complement in K must be a quantum 8-cap and therefore a copy of $\mathcal{K}(3,8)$. □

Let X be the set of points in $PG(3,4)$ extending $\mathcal{K}(3,8)$ to a 9-cap. A moment's thought shows that X consists of the points generated by the vectors of weight 3 whose nonzero entries are pairwise different and by the weight 4 vectors whose entries sum to 0. It follows $|X| = 8 + 6 = 14$ and X is contained in the plane $H : x_1 + x_2 + x_3 + x_4 = 0$. In fact X consists of the points of H which are not in the Fano subplane of H consisting of its points with coordinates in $\mathbb{F}_2$. This shows the following:

Proposition 4.18. *Let* H *be the plane* $x_1 + x_2 + x_3 + x_4 = 0$ *and* E *its Fano subplane consisting of points with coordinates in* $\mathbb{F}_2$. *Then* $\mathcal{K}(3,8) \cup Y$ *is a cap in* $PG(3,4)$ *if and only if* $Y \subset H, Y \cap E = \emptyset$ *and* Y *is a cap, and* $\mathcal{K}(3,8) \cup Y$ *is a quantum cap if and only if moreover* Y *is a hyperoval.*

Recall that $PG(2,4)$ and its hyperovals and Fano planes play a central role in the construction of the large Witt design as it is described for example in Hughes-Piper [102]. There are 360 Fano planes and 168 hyperovals in $PG(2,4)$.

Proposition 4.19. *Each Fano plane $E \subset PG(2,4)$ is disjoint from 7 hyperovals. Here each point $P \in E$ determines a hyperoval disjoint from E which consists of the points off E in the union of the bundle of lines of E that concur in P.*

Proof. Each of the 7 lines of E contains two points $\notin E$. A hyperoval disjoint from E must be the union of three such pairs of points from three lines of E. The fact that E is a blocking set in $PG(2,4)$ shows that a hyperoval is obtained if and only if those three lines are concurrent. □

Theorem 4.20. *Each $\mathcal{K}(3,8)$ is contained in precisely seven $\mathcal{K}(3,14)$. Each $\mathcal{K}(3,14)$ contains precisely seven copies of $\mathcal{K}(3,8)$ and seven hyperovals. We have $g_{14} = g_8 = 2^7 \times 3 \times 7$. Each pair of hyperovals intersects in a secant, and this secant is in precisely three hyperovals.*

Proof. Propositions 4.18 and 4.19 show that $\mathcal{K}(3,8)$ is in precisely 7 copies of $\mathcal{K}(3,14)$. Fix $K = \mathcal{K}(3,14)$. Let a_j be the number of planes meeting K in cardinality j (the j-planes), where $j \in \{0,2,4,6\}$. Let l be a secant of K. If l is in j of the 6-planes, then it is in $6-2j$ of the 4-planes and in $j-1$ of the 2-planes. It follows $j \in \{1,2,3\}$. Let l_j be the corresponding number of secants. Then $l_1 + l_2 + l_3 = \binom{14}{2} = 91$ and the obvious equations expressing a_2, a_4, a_6 in terms of the l_i have a unique solution:

$$a_6 = 7, a_4 = 56, a_2 = 14, a_0 = 8.$$

Each pair of hyperovals contained in K must intersect in a secant. The symmetric sum of those two hyperoval is a copy of $\mathcal{K}(3,8)$. It follows that the secant is on a third hyperoval. In terms of the system of equations this implies $l_3 = 7, l_2 = 0, l_1 = 84$. □

This indicates also how to construct $\mathcal{K}(3,14)$ in terms of hyperovals: there is a configuration in $PG(3,4)$ consisting of three collinear planes and a hyperoval in each plane, where all hyperovals share the same two points on the line of intersection. The symmetric sum of two hyperovals is then $\mathcal{K}(3,8)$ and the union of all three hyperovals is $\mathcal{K}(3,14)$.

The quantum 12-cap $\mathcal{K}(3,12)$

Assume K does not contain a hyperoval. Then K intersects each plane in at most 4 points. This yields a $[12,4,8]_4$-code. Concatenation with a $[4,2,3]_2$-code yields a $[48,8,24]_2$-code. This contradicts the Griesmer bound. We conclude that K is the disjoint union of two hyperovals (where each hyperoval is in a plane and those planes intersect in a line avoiding K, see the construction in the previous section. It is easy to see that K is uniquely determined. The fact that each $PG(2,4)$ contains precisely 168 hyperovals and that each line in $PG(2,4)$ is disjoint from 48 hyperovals shows that the total number of $\mathcal{K}(3,12)$ in $PG(3,4)$ is $85 \times 168 \times 6 \times 4 \times 48/2 = g/240$. This shows $g_{12} = 240$. Obvious counting arguments show

$$a_6 = 2, a_4 = 45, a_2 = 30, a_0 = 8.$$

4.5 The spectrum of quantum caps in $PG(4,4)$

In this section we present a search algorithm, helped by the theoretical results illustrated in the previous sections, to look for quantum caps in $PG(4,4)$.

Using a similar algorithm we proved in [10] that the minimum size of complete caps in $PG(4,4)$ is 20.

4.5.1 The search algorithm

The algorithm used in this search is, according to Chapter 3, of type A, since in particular quantum caps are sets of points no three of which are collinear and then possess a hereditary feature.
We start from caps, complete or incomplete, in $PG(3,4)$ where the classification is known (see [13] and [67]), and we try to extend every starting cap joining new points in $PG(4,4) \setminus PG(3,4)$. The search algorithm, implemented in C language, organizes the caps in a tree and the extension process ends when the obtained caps are complete. Some considerations about equivalence of caps allow us to avoid considering, during the process, caps that will produce caps already found or equivalent to one of these.

The search starts from the non-equivalent caps in $PG(3,4)$ of size s, $s \geq \overline{s}$, where $\overline{s}$ is determined according to the following theorem (see [18], [26] and [91, Theorem 4.1]) and the non existence of particular linear codes, as described in the next subsection.

Theorem 4.21. *The following are equivalent:*

1. *An $[n,k,d']_q$-code with $d' \geq d$.*

2. *A multiset $\mathcal{M}$ of points of the projective space $PG(k-1,q)$, which has cardinality n and satisfies the following: for every hyperplane $H \subset PG(k-1,q)$ there are at least d points of $\mathcal{M}$ outside H (in the multiset sense).*

The caps in $PG(3,4)$ are extended in the following way:

1. A cap $\mathcal{C}$ in $PG(3,4)$ of size s is extended joining points in $PG(4,4) \setminus PG(3,4)$.

2. The first point $\overline{P}$ can be chosen arbitrary since the collineations of $PG(4,4)$ which fix $PG(3,4)$ act transitively on the remaining points. Let $\mathcal{C}_1 = \mathcal{C} \cup \{\overline{P}\}$.

3. We compute the stabilizer in $P\Gamma L(5,4)$ of $\mathcal{C}_1$ and the orbits in which the points of $PG(4,4) \setminus PG(3,4)$ are divided.

4. For each orbit we select a particular point M and we consider only the orbits such that $\mathcal{C}_2 = \mathcal{C}_1 \cup \{M\}$ is a cap.

5. The program extends the caps (of size $h = s + 2$) determined previously, by exhaustive search, to obtain complete caps of size less than or equal to an integer $t > h$. To do this, the program builds a tree. First of all it creates a list of *candidate points*, i.e. points not belonging to any secant to the cap $\mathcal{C}_2$. If this set is not empty we introduce the following equivalence relationship:

$$P \sim Q \iff \mathcal{C}_2 \cup \{P\} \cong \mathcal{C}_2 \cup \{Q\},$$

where $\cong$ means that there is a collineation between the two sets. This relationship spreads the candidates in equivalence classes $\mathcal{O}_1, \ldots, \mathcal{O}_k$.

6. It is sufficient to choose the next point to add to $\mathcal{C}_2$ among the representatives of the equivalence classes, as two caps, one containing $\mathcal{C}_2 \cup \{P\}$ and the other one containing $\mathcal{C}_2 \cup \{Q\}$, with P and Q in $\mathcal{O}_{\bar{i}}$, are equivalent.
Suppose now that we have constructed all the caps containing $\mathcal{C}_2 \cup \{P_i\}$, with $i \leq \bar{i}$. When considering the caps containing $\mathcal{C}_2 \cup \{P_j\}$ with $\bar{i} < j$, all the points of the classes $\mathcal{O}_k$ with $k < \bar{i}$ can be avoided. In fact a cap containing $\mathcal{C}_2 \cup \{P_j\} \cup \{\overline{P}_k\}$, with $\overline{P}_k \in \mathcal{O}_k$ and $k < \bar{i}$, is projectively equivalent to a cap containing $\mathcal{C}_2 \cup \{P_k\} \cup \{P_j\}$, already studied.

7. Using the previous observations we can build a tree of caps such that every cap of the desired size is equivalent to a cap containing a leaf of the tree.

8. After building the tree, we extend the leaves using a backtracking algorithm.

4.5.2 Results

First of all we have determined, up to equivalence, all the quantum caps in $PG(4,4)$ of sizes less than or equal to 12, finding only two examples of 10-incomplete quantum caps and five examples of 12-incomplete quantum caps. They correspond to pure $[[10,0,4]]$ and $[[12,2,4]]$-quantum codes. We already know that there exist quantum caps in $PG(4,4)$ of sizes $10, 12-36, 38, 40, 41$ ([7], [20], [19] and [176]).

We have proven by a direct backtracking algorithm that quantum caps of size 11 do not exist. Then we have established the non existence of quantum caps of sizes 37 and 39.

Searching for 37 and 39 quantum caps we can consider starting caps in $PG(3,4)$ of odd size only, since Theorem 4.9 states that in this case a hyperplane intersection must have odd size.

Moreover we consider only caps of sizes 13, 15 and 17 in $PG(3,4)$, since Theorem 4.21 and the non-existence of linear $[n,k,d]$ codes with $n = 37, 39$, $k = 5$ and $d > n-12$ (see [84]) guarantee the existence of a hyperplane containing at least 12 points of such quantum caps.

The following table lists the non-equivalent caps in $PG(3,4)$ to be extended in this case:

Table 4.1: Number and type of non-equivalent caps $\mathcal{K} \subset PG(3,4)$, with $|\mathcal{K}| = 13, 15, 17$

$\lvert\mathcal{K}\rvert$	# COMPLETE CAPS	# INCOMPLETE CAPS
13	1	3
15	0	1
17	1	0

We finish our search, finding no examples of quantum caps in $PG(4,4)$ of sizes 37 and 39. According with [7], [19], [20] and [176] we have proven the following:

Theorem 4.22. *If $\mathcal{K} \subset PG(4,4)$ is a quantum cap, then $10 \leq |\mathcal{K}| \leq 41$, with $|\mathcal{K}| \neq 11, 37, 39$.*

4.5.3 List of found caps

The following table shows the size and the number of some examples of non-equivalent complete quantum caps we found by a non exhaustive search.

Table 4.2: Examples of non-equivalent complete quantum caps in $PG(4,4)$

Size of obtained Caps	Number of obtained Caps	Size and Type of starting Caps
20	1	12 complete
29	1	17 complete
29	1	13 incomplete
30	1	16 incomplete
32	1	16 incomplete
33	3	13 incomplete
34	162	16 incomplete
36	2	16 incomplete
38	1	16 incomplete

We list all the non equivalent quantum caps of sizes ≤ 12 and some examples of complete quantum caps of sizes $20, 29, 30, 32, 33, 34, 36, 38$. These examples are not equivalent to those constructed in [176], since the latter are subsets of the complete quantum 41-cap. Let $GF(4) = \{0, 1, \omega, \omega^2\}$. For every quantum cap we list a generator matrix of the associated code, the weight enumerator and the size (or the name if the size is small enough) of its stabilizer group G in $P\Gamma L(5, 4)$.

The incomplete quantum 10-caps

They correspond to pure $[[10, 0, 4]]$-quantum codes.

$$\begin{array}{cccccccccc}
1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & \omega^2 & 1 & 0 & \omega & \omega & \omega \\
0 & 0 & 0 & 0 & \omega & 1 & 1 & \omega^2 & \omega^2 & \omega^2
\end{array}$$

$$[< 4, 30 >, < 6, 300 >, < 8, 585 >, < 10, 108 >]$$

$$|G| = 3840$$

$$\begin{array}{cccccccccc}
1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
0 & 1 & \omega^2 & 0 & 0 & 0 & 1 & 0 & 0 & \omega \\
0 & 0 & \omega & 1 & 0 & 0 & 1 & 1 & 1 & \omega^2 \\
0 & 0 & \omega & 0 & 1 & 0 & 1 & \omega & \omega^2 & \omega^2 \\
0 & 0 & \omega & 0 & 0 & 1 & 1 & \omega^2 & \omega & \omega^2
\end{array}$$

$$[< 4, 30 >, < 6, 300 >, < 8, 585 >, < 10, 108 >]$$

$$|G| = 14400$$

The incomplete quantum 12-caps

They correspond to pure $[[12, 2, 4]]$-quantum codes.

$$\begin{array}{cccccccccccc}
1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & \omega & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & \omega & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & \omega & 1 & \omega \\
0 & \omega & 0 & 0 & \omega & 1 & 0 & 1 & 1 & \omega^2 & 1 & 1 \\
0 & \omega & 0 & 0 & \omega & 0 & 1 & 1 & \omega & 0 & \omega^2 & 0
\end{array}$$

$$[< 6, 84 >, < 8, 405 >, < 10, 468 >, < 12, 66 >]$$

$$G = D_{12}$$

$$\begin{array}{cccccccccccc}
1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & \omega^2 & 0 & 1 & 1 & \omega & 1 & 0 \\
0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & \omega^2 & 1 \\
0 & 0 & 1 & 0 & 1 & \omega^2 & 0 & 1 & \omega & \omega & \omega^2 & \omega \\
0 & 0 & \omega & 0 & 0 & \omega^2 & 1 & 1 & \omega & \omega & \omega^2 & 1
\end{array}$$

$$[< 4, 6 >, < 6, 60 >, < 8, 441 >, < 10, 444 >, < 12, 72 >]$$

$$|G| = 192$$

$$\begin{array}{cccccccccccc}
0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\
1 & 0 & 0 & 0 & \omega^2 & 1 & 0 & 0 & \omega & 1 & 1 & 0 \\
1 & 0 & 0 & 0 & \omega^2 & 0 & 1 & 0 & 0 & 1 & 1 & \omega \\
\omega & 0 & \omega & 0 & \omega^2 & 0 & 0 & 1 & \omega & 1 & \omega^2 & \omega
\end{array}$$

$$[< 4, 6 >, < 6, 60 >, < 8, 441 >, < 10, 444 >, < 12, 72 >]$$

$$|G| = 128$$

$$\begin{array}{cccccccccccc}
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 0 & \omega & 0 & 1 & 1 & \omega^2 & 0 \\
1 & 0 & 0 & \omega & 0 & 1 & 0 & 0 & 1 & 1 & \omega^2 & 0 \\
\omega & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1
\end{array}$$

$$[< 4, 9 >, < 6, 48 >, < 8, 459 >, < 10, 432 >, < 12, 75 >]$$

$$|G| = 768$$

$$\begin{array}{cccccccccccc}
1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 1 & \omega^2 & 1 & 1 & \omega & \omega \\
0 & 0 & 0 & 1 & 0 & 1 & \omega^2 & \omega^2 & 1 & \omega & \omega & \omega \\
0 & 0 & 0 & 0 & 1 & 1 & \omega^2 & \omega^2 & \omega & 1 & \omega & \omega
\end{array}$$

$$[< 4, 18 >, < 6, 12 >, < 8, 513 >, < 10, 396 >, < 12, 84 >]$$

$$|G| = 2304$$

A complete quantum 20-cap

Starting from a complete 12-cap in $PG(3, 4)$ a quantum 20-cap has been obtained. Since in [10] it is shown that 20 is the minimum size of complete caps in $PG(4, 4)$, this is an example of minimal complete quantum cap. This cap generates a pure $[[20, 10, 4]]$-quantum code.

$$\begin{array}{cccccccccccccccccc}
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & \omega & 1 & 0 & 1 & 1 & 0 & 1 & 0 & \omega & \omega^2 & 1 & \omega^2 \\
1 & 0 & 0 & 0 & 1 & \omega^2 & 0 & 0 & \omega & 1 & 1 & \omega & 1 & 1 & 1 & \omega^2 & 1 & 0 & \omega^2 & \omega^2 \\
1 & 0 & 0 & \omega & 0 & 1 & 1 & 0 & \omega^2 & \omega^2 & \omega & \omega & 0 & \omega^2 & 1 & 1 & \omega & 1 & \omega & 0 \\
\omega & 0 & 0 & 1 & 0 & \omega & 0 & 1 & 0 & \omega^2 & 1 & 1 & \omega & \omega^2 & 1 & \omega & \omega & 1 & 0 & \omega^2
\end{array}$$

$$[< 0, 1 >, < 8, 3 >, < 12, 117 >, < 14, 432 >, < 16, 312 >, < 18, 144 >, < 20, 15 >]$$

The size of the stabilizer group of this cap in $P\Gamma L(5,4)$ is 48 and it is generated by the following collineations:

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \overline{\omega} & 0 \\ 0 & \omega & 0 & \overline{\omega} & \omega \\ 0 & \overline{\omega} & \omega & 1 & 0 \\ 0 & 1 & \overline{\omega} & 1 & \omega \end{pmatrix} G_2 = \begin{pmatrix} 1 & 0 & \overline{\omega} & 1 & \omega \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} G_3 = \begin{pmatrix} 1 & \omega & \omega & \overline{\omega} & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Two complete quantum 29-caps

They correspond to pure $[[29, 19, 4]]$-quantum codes. This complete 29-cap has been obtained from a complete 17-cap in $PG(3,4)$. This cap is the unique complete quantum 29-cap containing a complete 17-cap (the elliptic quadric in $PG(3,4)$) as hyperplane intersection.

$$\begin{array}{ccccccccccccccccccccccccccc} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & \omega^2 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & \omega & 0 & 1 & 1 & 1 & 1 & 1 & 1 & \omega & 1 & \omega^2 \\ 0 & 0 & 1 & 0 & 0 & 0 & \omega & \omega^2 & 0 & 1 & 1 & 1 & 1 & 0 & \omega & \omega^2 & 1 & 1 & \omega & 0 & \omega^2 & \omega^2 & 0 & \omega^2 & 1 & \omega & \omega & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & \omega & 1 & \omega & \omega^2 & \omega^2 & \omega^2 & 1 & \omega & \omega & \omega & 1 & \omega^2 & 1 & 0 & 1 & \omega^2 & 1 & \omega^2 \\ 0 & 0 & 0 & 0 & 1 & \omega^2 & 1 & \omega & 1 & \omega & 0 & 0 & \omega & 1 & \omega & 0 & \omega^2 & 1 & 0 & \omega & \omega^2 & 0 & \omega^2 & \omega & \omega & \omega^2 & \omega^2 & \omega & 1 \end{array}$$

$$[< 12, 3 >, < 18, 42 >, < 20, 360 >, < 22, 420 >, < 24, 81 >, < 26, 90 >, < 28, 27 >]$$

$$G = Z_6$$

The following complete 29-cap has been obtained from an incomplete 13-cap in $PG(3,4)$.

$$\begin{array}{ccccccccccccccccccccccccccc} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ \omega & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & \omega & 1 & \omega & 1 & 0 & 1 & 0 & 1 & 1 & \omega^2 & \omega^2 & 1 & 0 & \omega^2 & 1 & \omega^2 & \omega^2 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & \omega & \omega & 1 & \omega & \omega^2 & 1 & 1 & 0 & 0 & \omega & 1 & \omega^2 & 1 & \omega^2 & 1 & 0 & \omega & 0 & 0 \\ \omega & 0 & \omega & 0 & 0 & 1 & 0 & 0 & 0 & \omega & \omega^2 & 1 & \omega^2 & 0 & 0 & \omega & 1 & 1 & \omega & \omega^2 & 0 & \omega^2 & \omega^2 & \omega^2 & 1 & 1 & \omega & 1 & \omega^2 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & \omega^2 & 1 & 1 & \omega & 1 & 1 & 0 & 1 & \omega & \omega & \omega & 1 & \omega^2 & \omega^2 & 1 & \omega^2 & \omega & 1 & \omega & \omega & 0 & \omega^2 \end{array}$$

$$[< 16, 6 >, < 18, 57 >, < 20, 348 >, < 22, 366 >, < 24, 159 >, < 26, 57 >, < 28, 30 >]$$

$$G = Z_4$$

A complete quantum 30-cap

This complete 30-cap has been obtained from an incomplete 16-cap in $PG(3,4)$. This cap is the unique complete quantum 30-cap containing an incomplete 16-cap as hyperplane intersection. It corresponds

to a pure $[[30, 20, 4]]$-quantum code.

$$\begin{array}{cccccccccccccccccccccccccccccc}
1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & \omega^2 & 1 & 0 & 1 & 0 & \omega & 1 & 1 & 1 & 0 & 1 & \omega & 1 & 0 & 1 & 1 & 1 & 1 & \omega & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 1 & 0 & 0 & \omega & 0 & \omega^2 & 1 & 1 & 1 & 1 & 0 & \omega & 0 & 1 & 1 & \omega & \omega^2 & 1 & 0 & \omega & \omega^2 & 1 & 1 & \omega & 0 & \omega \\
0 & \omega & 0 & 0 & 1 & 1 & 0 & 0 & \omega & 1 & \omega & \omega & 1 & \omega^2 & \omega & \omega^2 & \omega & \omega^2 & 1 & 0 & \omega & 0 & \omega^2 & \omega & 1 & 0 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & \omega^2 & 0 & 1 & 1 & 0 & 1 & \omega & 0 & \omega & \omega & 1 & \omega & \omega & \omega^2 & 1 & \omega & \omega^2 & \omega^2 & \omega^2 & 1 & \omega & \omega & 1 & \omega^2 & \omega & \omega
\end{array}$$

$$[< 14, 3 >, < 20, 258 >, < 22, 438 >, < 24, 165 >, < 26, 108 >, < 28, 48 >, < 30, 3 >]$$

$$G = Z_2 \times Z_2$$

A complete quantum 32-cap

This complete 32-cap has been obtained from an incomplete 16-cap in $PG(3, 4)$. It corresponds to a pure $[[32, 22, 4]]$-quantum code. This cap is the unique complete quantum 32-cap containing an incomplete 16-cap as hyperplane intersection.

$$\begin{array}{cccccccccccccccccccccccccccccc}
1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\
\omega^2 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & \omega & \omega & \omega & 1 & 0 & 1 & 1 & 0 & 1 & 0 & \omega & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & \omega^2 & \omega & 1 & \omega^2 \\
\omega^2 & 0 & 0 & 1 & 1 & 0 & 0 & \omega & \omega & 0 & 1 & 1 & 1 & 0 & \omega & 1 & 1 & 0 & \omega^2 & \omega^2 & 1 & 0 & 0 & \omega^2 & 1 & \omega & 1 & \omega^2 & \omega & 0 & \omega & 1 \\
\omega & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & \omega & 1 & \omega & \omega^2 & \omega^2 & 1 & \omega & 1 & \omega & 0 & 1 & \omega^2 & 1 & \omega & \omega & 0 & 1 & \omega & 0 & 1 & \omega^2 \\
0 & 0 & 0 & 0 & \omega^2 & 0 & 1 & 1 & 1 & \omega^2 & 0 & 0 & \omega & 1 & \omega & \omega^2 & 1 & \omega & \omega & \omega^2 & \omega^2 & 0 & \omega^2 & 0 & 1 & 1 & \omega & \omega & \omega^2 & 1 & \omega^2 & 0
\end{array}$$

$$[< 16, 3 >, < 20, 39 >, < 22, 312 >, < 24, 429 >, < 26, 120 >, < 28, 69 >, < 30, 48 >, < 32, 3 >]$$

$$G = Z_2 \times Z_2 \times Z_2$$

Three complete quantum 33-caps

We have found 3 non equivalent quantum caps of size 33, starting from an incomplete cap of size 13 in $PG(3, 4)$. The computer search is not complete. They correspond to pure $[[33, 23, 4]]$-quantum codes.

$$\begin{array}{ccccccccccccccccccccccccccccccc}
1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\
0 & 1 & \omega & 0 & 0 & 0 & \omega & 1 & \omega & 1 & 0 & \omega & 1 & 0 & 1 & \omega^2 & \omega^2 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & \omega^2 & \omega^2 & \omega & 1 & 0 & \omega^2 & 1 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & \omega & \omega^2 & 1 & \omega & \omega & 1 & \omega & 0 & 0 & 1 & 1 & 0 & 0 & \omega^2 & \omega & 1 & 1 & 0 & \omega^2 & 1 & \omega^2 & 0 & \omega^2 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & \omega & 0 & 1 & 0 & \omega & \omega^2 & 1 & 0 & \omega & 0 & \omega^2 & \omega & 1 & \omega & 1 & \omega^2 & \omega^2 & \omega^2 & 1 & \omega & \omega & \omega & 1 & \omega^2 & 1 & 1 & \omega^2 \\
0 & 0 & 1 & 0 & 0 & 1 & 1 & \omega^2 & 0 & \omega & 1 & \omega & 1 & \omega & 0 & 1 & 0 & \omega & \omega & 1 & \omega & 1 & 1 & \omega^2 & 1 & \omega & \omega & 1 & \omega & \omega^2 & 1 & \omega & \omega
\end{array}$$

$$[< 18, 3 >, < 20, 6 >, < 22, 204 >, < 24, 435 >, < 26, 219 >, < 28, 84 >, < 30, 54 >, < 32, 18 >]$$

$$G = Z_4$$

$$\begin{array}{ccccccccccccccccccccccccccccccc}
1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & \omega & 1 & 1 & 0 & \omega & 0 & 0 & 1 & \omega & 0 & 0 & 0 & \omega & 1 & 1 & 1 & \omega^2 & \omega & 1 & 1 & 1 & 0 & \omega^2 & 1 & 1 & \omega^2 & \omega & 0 & 0 & 1 & \omega & 0 \\
0 & 1 & \omega^2 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & \omega & 1 & \omega & \omega & 0 & \omega & 0 & 1 & \omega^2 & 0 & 0 & 1 & 1 & \omega^2 & 1 & \omega & 1 & 0 & \omega & \omega \\
0 & 0 & \omega & 0 & 0 & \omega^2 & 1 & 0 & \omega^2 & 1 & \omega & 1 & \omega & 0 & 1 & \omega^2 & 1 & \omega & \omega^2 & 1 & 1 & \omega^2 & 1 & 0 & \omega & 0 & \omega^2 & \omega & 1 & \omega^2 & \omega & \omega & 0 \\
0 & \omega & 0 & 0 & 0 & \omega^2 & 0 & 1 & \omega^2 & 1 & 1 & \omega & \omega^2 & 0 & 1 & \omega^2 & 1 & 1 & \omega & \omega & \omega^2 & 1 & 1 & \omega^2 & \omega & \omega^2 & 0 & 0 & 0 & \omega^2 & 1 & \omega^2 & 1
\end{array}$$

$$[< 16, 3 >, < 20, 27 >, < 22, 108 >, < 24, 573 >, < 26, 144 >, < 28, 105 >, < 30, 36 >, < 32, 27 >]$$

$$G = Q_4 \times Z_2$$

$$\begin{array}{ccccccccccccccccccccccccccccccc}
1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 1 & 1 & 0 & 0 & \omega^2 & 0 & \omega^2 & 1 & 0 & 0 & 0 & 0 & \omega & 1 & 1 & 1 & \omega & 1 & 0 & \omega & 1 & 1 & 0 & 1 & 1 & \omega^2 & \omega^2 & \omega^2 & 0 & 1 & \omega & \omega \\
0 & \omega^2 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & \omega^2 & 0 & \omega & 1 & \omega & \omega & \omega & 0 & \omega^2 & 0 & 1 & \omega^2 & 0 & 1 & 1 & \omega^2 & 1 & 1 & 1 & 0 & \omega & 0 \\
0 & \omega & 0 & 0 & 1 & \omega & 0 & \omega^2 & \omega^2 & \omega & 1 & \omega & \omega & 0 & 1 & \omega^2 & 1 & \omega^2 & 1 & 0 & 0 & 1 & \omega^2 & 1 & \omega & 0 & \omega^2 & 1 & 0 & \omega^2 & \omega & \omega & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & \omega^2 & 1 & \omega & 1 & \omega^2 & 0 & 1 & \omega^2 & 1 & \omega & \omega & \omega^2 & 1 & \omega^2 & 1 & 1 & \omega & \omega^2 & 0 & \omega & \omega^2 & \omega^2 & 1 & \omega^2 & 0
\end{array}$$

$$[< 16, 3 >, < 20, 18 >, < 22, 144 >, < 24, 516 >, < 26, 192 >, < 28, 78 >, < 30, 48 >, < 32, 24 >]$$

$$|G| = 64$$

Complete quantum 34-caps

We have found 162 non equivalent quantum caps of size 34, starting from an incomplete cap of size 16 in $PG(3, 4)$. The computer search is not complete. They correspond to pure $[[34, 24, 4]]$-quantum codes. All have stabilizer group in $P\Gamma L(5, 4)$ equal to $\mathbb{Z}_1$. An example is:

$$\begin{array}{ccccccccccccccccccccccccccccccc}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & \omega & 1 & 0 & \omega & 0 & 0 & 1 & \omega & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & \omega & 1 & \omega & \omega^2 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 1 & \omega^2 & 0 & 0 & \omega^2 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & \omega & \omega & 1 & \omega & 0 & 1 & \omega & \omega & \omega & 1 & 0 & \omega & 1 & \omega & 1 & \omega & 1 & 0 & \omega & \omega^2 \\
0 & 0 & 0 & \omega & 1 & 0 & 1 & \omega^2 & 1 & \omega & 1 & \omega^2 & \omega & 0 & \omega^2 & 0 & 1 & \omega^2 & 1 & 0 & 1 & \omega & \omega^2 & 1 & 0 & \omega & \omega^2 & 0 & \omega^2 & 1 & \omega^2 & \omega & 0 & 1 \\
0 & 0 & 0 & \omega^2 & 0 & 1 & \omega & \omega^2 & 1 & 0 & \omega & 1 & 1 & \omega^2 & \omega & 0 & 1 & \omega^2 & \omega & \omega & \omega^2 & \omega & 0 & \omega^2 & \omega & 1 & \omega & 1 & 1 & 0 & \omega^2 & 1 & 1 & \omega^2
\end{array}$$

$$[< 18, 3 >, < 20, 6 >, < 22, 60 >, < 24, 447 >, < 26, 291 >, < 28, 132 >, < 30, 30 >, < 32, 54 >]$$

$$G = Z_1$$

Two complete quantum 36-caps

These 36-complete caps have been obtained from an incomplete 16-cap in $PG(3, 4)$. These caps are the unique complete quantum 36-caps containing an incomplete 16-cap as hyperplane intersection. They correspond to pure $[[36, 26, 4]]$-quantum codes.

$$\begin{array}{ccccccccccccccccccccccccccccccccccc}
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & \omega & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & \omega & 1 & 0 & 1 & 1 & \omega & 0 & 0 & 1 & 1 & 1 & \omega & 1 & \omega^2 & \omega^2 & 1 & \omega & \omega^2 & \omega^2 & \omega^2 & 0 & 0 & 1 & 1 \\
0 & 1 & \omega^2 & 0 & 1 & \omega^2 & 0 & 0 & \omega^2 & 0 & 1 & 1 & \omega^2 & 1 & 1 & \omega & 1 & \omega^2 & \omega & 0 & 1 & \omega & 1 & 0 & \omega^2 & \omega & 0 & \omega & 1 & \omega & 0 & \omega^2 & \omega & 1 & 0 & \omega \\
0 & 0 & \omega & 0 & 0 & \omega & 1 & 0 & 1 & \omega^2 & \omega & 1 & \omega^2 & 0 & 0 & \omega^2 & 1 & 1 & \omega^2 & 1 & 0 & 1 & 1 & \omega & 0 & \omega & \omega & \omega & 1 & 0 & \omega^2 & 0 & 1 & \omega^2 & \omega & 0 \\
0 & \omega & 0 & 0 & 0 & \omega^2 & 0 & 1 & \omega & \omega^2 & 0 & \omega & 1 & 1 & \omega^2 & \omega & 1 & \omega & \omega^2 & \omega & \omega & \omega^2 & \omega^2 & \omega & \omega^2 & \omega & 0 & 1 & 0 & 1 & \omega & 0 & 0 & \omega^2 & 1 & 1
\end{array}$$

$$[< 20, 6 >, < 24, 138 >, < 26, 492 >, < 28, 234 >, < 30, 48 >, < 32, 69 >, < 34, 36 >]$$

$$G = D_4 \times Z_2$$

$$\begin{array}{ccccccccccccccccccccccccccccccccccc}
1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & \omega^2 & \omega^2 & \omega^2 & 1 & 0 & 0 & 1 & 0 & \omega^2 & 1 & 0 & 1 & \omega & \omega^2 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \omega & 1 & 0 & \omega \\
0 & 0 & 1 & 1 & 0 & 0 & \omega^2 & \omega & 0 & 0 & \omega & 1 & 1 & \omega & 0 & \omega^2 & \omega^2 & \omega & 1 & 1 & 0 & \omega & \omega^2 & 1 & 0 & 0 & \omega & 1 & \omega^2 & \omega^2 & \omega & 1 & 1 & 1 & \omega & \omega^2 \\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & \omega & \omega^2 & 0 & \omega & 1 & 1 & \omega & \omega^2 & 0 & \omega^2 & \omega^2 & 1 & \omega & \omega & \omega & 0 & 1 & \omega^2 & \omega & 0 & 1 & \omega & 1 & 0 & \omega^2 & \omega^2 & 0 & \omega^2 \\
0 & 0 & 0 & \omega^2 & 0 & 1 & \omega^2 & 1 & 0 & \omega & 1 & 0 & \omega & 0 & 1 & \omega & 0 & \omega & \omega^2 & 1 & \omega & \omega & \omega^2 & \omega^2 & 0 & \omega^2 & 1 & \omega & \omega & 0 & \omega^2 & 1 & \omega^2 & \omega & \omega & 1
\end{array}$$

$$[< 20, 6 >, < 22, 6 >, < 24, 120 >, < 26, 510 >, < 28, 222 >, < 30, 66 >, < 32, 51 >, < 34, 42 >]$$

$$G = Z_2 \times Z_2 \times Z_4$$

4.6 The unique quantum complete 38-cap

This 38-complete cap has been obtained from an incomplete 16-cap in $PG(3, 4)$. It corresponds to a $[[38, 28, 4]]$-quantum code. This cap is the unique quantum cap in $PG(4, 4)$ of size 38 (see Section 4.9).

$$\begin{array}{ccccccccccccccccccccccccccccccccccc}
1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & \omega & 0 & 0 & 0 & 1 & \omega^2 & \omega & \omega^2 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & \omega & \omega^2 & 0 & 1 & 1 & \omega^2 & 1 & 1 & \omega & \omega^2 & \omega & 0 & 1 & \omega & \omega^2 \\
0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & \omega & \omega^2 & 0 & 1 & 1 & 1 & \omega & 0 & 1 & 0 & 0 & \omega^2 & 1 & \omega^2 & 1 & \omega & \omega^2 & 1 & \omega & 0 & 0 & 1 & 1 & 1 & \omega^2 & \omega^2 & 1 & 0 & \omega & \omega \\
0 & 0 & 0 & \omega^2 & 1 & 0 & 0 & \omega^2 & \omega^2 & 0 & 1 & \omega & 1 & 0 & 0 & \omega & 1 & 1 & 1 & 0 & 1 & \omega & \omega^2 & \omega^2 & \omega & 1 & \omega & \omega^2 & \omega^2 & \omega & 0 & 1 & \omega^2 & 1 & \omega^2 & \omega & \omega & \omega \\
0 & 0 & 0 & \omega^2 & 0 & \omega & 1 & \omega^2 & \omega & 0 & 0 & 1 & \omega & 1 & \omega^2 & \omega^2 & 1 & \omega & \omega & \omega^2 & \omega^2 & \omega & 0 & 1 & 0 & 0 & \omega^2 & \omega & \omega^2 & 0 & 0 & \omega^2 & \omega^2 & 1 & \omega^2 & 1
\end{array}$$

$$[< 22, 6 >, < 24, 12 >, < 26, 288 >, < 28, 288 >, < 30, 372 >, < 32, 3 >, < 36, 48 >, < 38, 6 >]$$

$$|G| = 384$$

4.7 The spectrum of quantum caps in $PG(4, 4)$

We already know that there exist quantum caps in $PG(4, 4)$ of sizes $10, 12 - 36, 38, 40, 41$ ([7], [20], [19] and [176]).

According with [7], [19], [20] and [176] we have proven the following:

Theorem 4.23. *If $\mathcal{K} \subset PG(4, 4)$ is a quantum cap, then $10 \leq |\mathcal{K}| \leq 41$, with $|\mathcal{K}| \neq 11, 37, 39$.*

4.8 Quantum caps in higher-dimensional spaces

Obviously a lower bound on the size of a quantum cap in $PG(m,4)$ is $2(m+1)$ (corresponding to linear $[[2(m+1),0,4]]$ quantum codes). The quantum caps $\mathcal{K}(2,6)$ and $\mathcal{K}(4,10,2)$ belong to an infinite family which shows that quantum $2(m+1)$-caps exist in $PG(m,4)$ when m is odd.

Theorem 4.24. *$PG(m,4)$ for even m contains a quantum $2(m+1)$-cap possessing $m+1$ points in general position such that each additional point completes it to a frame.*

In fact, choose a generator matrix $(I|P)$ where $P = \begin{pmatrix} 1111\ldots \\ 1322\ldots \\ 1232\ldots \\ 1223\ldots \\ \ldots \end{pmatrix}$.

Then it is easy to see that this generates a cap and that any two rows are Hermitian orthogonal to each other.

Theorem 4.25. *$PG(m,4)$ for odd $m \geq 3$ contains a quantum $2(m+1)$-cap.*

In fact, use $(I|I+J)$ as generator matrix. The smallest member of the family is $\mathcal{K}(3,8)$ in $PG(3,4)$.

The largest known quantum caps in $PG(5,4), PG(7,4), PG(9,4)$ are also the largest known caps in those spaces. These are the Glynn 126-cap in $PG(5,4)$, a 756-cap in $PG(7,4)$ and a 5040-cap in $PG(9,4)$ (see [22]).

4.9 The classification of 38-caps in $PG(4,4)$

As the computational instruments are very similar to those used to establish the non existence of quantum 37 and 39-caps in $PG(4,4)$, the classification of complete and non-complete 38-caps has been performed. The algorithm used is described in Section 4.5.1. Searching for quantum 38-caps we can consider starting caps in $PG(3,4)$ of even size only, since Theorem 4.9 states that in this case a

hyperplane intersection must have even size.

Moreover we consider only caps of sizes 12, 14 and 16 in $PG(3,4)$, since Theorem 4.21 and the non-existence of linear $[n,k,d]$ codes with $n = 38$, $k = 5$ and $d > n - 12$ (see [84]) guarantee the existence of a hyperplane containing at least 12 points of such quantum caps.

Table 4.3 lists the non-equivalent caps in $PG(3,4)$ to be extended in this case:

Table 4.3: Number and type of non-equivalent caps $\mathcal{K} \subset PG(3,4)$, with $|\mathcal{K}| = 12, 14, 16$

$\lvert\mathcal{K}\rvert$	# COMPLETE CAPS	# INCOMPLETE CAPS
12	5	8
14	1	1
16	0	1

In this first table for each type of starting cap in $PG(3,4)$ are listed the non equivalent examples of complete and non complete 38-caps obtained. The column *Type* indicates if the the starting cap is Complete (C) or Incomplete (I) and the number the caps.

$\#\mathcal{C}$	Type	# Inc.	# Inc. Quant.	# Compl.	# Compl. Quant.
16	I	83	0	1	1
14	C	0	0	1	1
14	I	105	0	1	0
12	C 1	0	0	1	0
12	C 2	7	0	0	0
12	C 3	0	0	1	1
12	C 4	0	0	3	0
12	C 5	17	0	0	0
12	I 1	86	0	3	0
12	I 2	9	0	0	0
12	I 3	12	0	0	0
12	I 4	78	0	3	0
12	I 5	94	0	3	0
12	I 6	25	0	4	0
12	I 7	45	0	2	0
12	I 8	14	0	0	0

This second table summarizes the results according to the size of the starting cap in $PG(3,4)$. To have a complete classifications of the 38-caps in $PG(4,4)$ also the results obtained starting from caps in $PG(3,4)$ of size $13, 15, 17$ are presented. In total there exist 138 incomplete and 6 complete 38-caps up to equivalence. In particular there exists only one quantum 38-cap, which is complete, having as hyperplane intersections $12, 14, 16$.

$\#\mathcal{C}$	# Inc.	# Inc. Quant.	# Compl.	# Compl. Quant.
17	39	0	0	0
16	83	0	1	1
15	95	0	0	0
14	105	0	2	1
13	121	0	5	0
12	138	0	6	1
TOT.	138	0	6	1

In Table 4.4 all the non-equivalent complete 38-caps in $PG(4,4)$ are presented. Also the weight enumerators of the associated codes and the stabilizers of the caps are listed. The first example in the

Table 4.4: The non-equivalent complete 38-caps in $PG(4,4)$

$\mathcal{C}$	Weight enumerators	Stabilizer
$1\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 1\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 1\ 0\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 1\ 1$ $0\ 1\ 0\ \omega\ 0\ 0\ 0\ 1\ \omega^2\ \omega\ \omega^2\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ \omega\ \omega^2\ 0\ 1\ 1\ \omega^2\ 1\ 1\ \omega\ \omega^2\ \omega\ 0\ 1\ \omega\ \omega^2$ $0\ 0\ 1\ 1\ 0\ 1\ 0\ 0\ \omega\ \omega^2\ 0\ 1\ 1\ 1\ \omega\ 0\ 1\ 0\ 0\ \omega^2\ 1\ \omega^2\ 1\ \omega\ \omega^2\ 1\ \omega\ 0\ 0\ 1\ 1\ 1\ \omega^2\ \omega^2\ 1\ 0\ \omega\ \omega$ $0\ 0\ 0\ \omega^2\ 1\ 0\ 0\ \omega^2\ \omega^2\ 0\ 1\ \omega\ 1\ 0\ 0\ \omega\ 1\ 1\ 1\ 0\ 1\ \omega\ \omega^2\ \omega^2\ \omega\ 1\ \omega\ \omega^2\ \omega^2\ \omega\ 0\ 1\ \omega^2\ 1\ \omega^2\ \omega\ \omega\ \omega$ $0\ 0\ 0\ \omega^2\ 0\ \omega\ 1\ \omega^2\ \omega\ 0\ 0\ 1\ \omega\ 1\ \omega^2\ \omega^2\ 1\ \omega\ \omega\ \omega^2\ \omega^2\ 0\ 0\ 1\ \omega\ 1\ 0\ 0\ \omega^2\ \omega\ \omega^2\ 0\ 0\ \omega^2\ \omega^2\ 1\ \omega^2\ 1$	$22^{6}24^{12}26^{288}28^{288}$ $30^{372}32^{3}36^{48}38^{6}$	G_{384}
$1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 1\ 0\ 1$ $0\ \omega\ 1\ 0\ 0\ 0\ 1\ 1\ 0\ \omega\ 0\ \omega\ 1\ \omega^2\ \omega\ 1\ 0\ 0\ 1\ 1\ 1\ 0\ 1\ \omega\ 1\ 1\ \omega^2\ \omega^2\ \omega\ \omega^2\ \omega^2\ 0\ 0\ 1\ \omega^2\ 1\ 1\ 1$ $0\ 1\ 0\ 1\ 0\ 0\ 0\ 1\ 1\ \omega^2\ 0\ \omega^2\ \omega\ \omega\ \omega^2\ 1\ \omega\ 0\ 1\ 1\ \omega\ \omega\ 1\ 1\ \omega^2\ \omega^2\ 0\ 0\ 1\ 0\ \omega\ \omega\ 1\ 0\ \omega\ 1\ \omega\ \omega^2$ $0\ 0\ 0\ 0\ 1\ 0\ \omega^2\ \omega\ 1\ \omega^2\ \omega\ \omega\ \omega^2\ 1\ 1\ 1\ \omega^2\ 1\ \omega\ 0\ 1\ \omega\ 1\ \omega\ 0\ 1\ \omega\ \omega^2\ 1\ 1\ 0\ 1\ \omega^2\ \omega\ \omega\ \omega^2\ 0\ \omega$ $0\ \omega\ 0\ 0\ 0\ 1\ \omega^2\ 0\ \omega\ 1\ 1\ 0\ \omega\ \omega^2\ \omega\ 1\ \omega^2\ \omega\ \omega\ \omega\ \omega^2\ \omega\ \omega^2\ \omega^2\ 0\ 1\ 0\ \omega^2\ 0\ 1\ \omega\ 0\ \omega^2\ 1\ 1\ 1\ 1\ \omega^2$	$24^{9}25^{72}26^{63}27^{228}28^{288}29^{126}$ $30^{54}31^{72}33^{36}34^{27}35^{36}36^{6}37^{6}$	G_{48}
$1\ 1\ 0\ 0\ 0\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 0$ $0\ 1\ 1\ 0\ 0\ 0\ 0\ \omega\ \omega^2\ 0\ \omega\ \omega\ 0\ \omega\ 1\ \omega\ 1\ 0\ 1\ 1\ \omega^2\ 0\ 1\ 0\ \omega^2\ 1\ \omega\ \omega^2\ \omega^2\ 1\ 0\ \omega^2\ 0\ 1\ 1\ 0\ 1\ 1$ $0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ \omega\ 1\ 0\ 0\ 1\ \omega^2\ 1\ \omega^2\ \omega^2\ 0\ 1\ 0\ 1\ 1\ 1\ \omega\ \omega^2\ \omega^2\ 0\ \omega^2\ 0\ \omega\ \omega\ \omega\ 1\ \omega\ \omega\ 1\ 0\ \omega$ $0\ \omega^2\ 0\ 0\ 1\ 0\ 0\ 0\ 1\ \omega\ 1\ 0\ 1\ \omega^2\ 1\ 1\ \omega^2\ 1\ \omega\ \omega\ \omega^2\ \omega\ 0\ \omega\ \omega\ 1\ \omega\ 0\ \omega\ \omega\ 1\ \omega^2\ 1\ 1\ 1\ \omega^2\ \omega\ 0$ $0\ \omega^2\ 0\ 0\ 0\ \omega\ 1\ 0\ \omega\ 1\ 1\ \omega^2\ \omega\ 0\ 1\ \omega\ \omega\ \omega\ \omega\ 0\ \omega\ \omega^2\ \omega\ \omega\ 0\ \omega^2\ \omega\ \omega\ \omega^2\ 1\ \omega^2\ \omega^2\ 0\ 0\ \omega\ \omega^2\ 1\ 1$	$25^{48}26^{168}27^{144}28^{288}29^{120}$ $30^{108}31^{24}32^{3}33^{24}34^{60}35^{24}36^{12}$	G_{16}
$1\ 1\ 1\ 0\ 0\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 1\ 1\ 1\ 1\ 0\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ 0\ 0$ $0\ \omega\ \omega\ 1\ 0\ 0\ \omega^2\ \omega\ 0\ \omega^2\ \omega^2\ 0\ 1\ 0\ 1\ \omega^2\ 0\ 1\ 1\ \omega\ 0\ \omega\ 0\ 1\ \omega\ 1\ 0\ 1\ \omega^2\ \omega^2\ \omega^2\ 0\ 1\ 0\ 1\ 1\ 1\ 1$ $0\ 1\ 0\ 0\ 1\ 0\ 1\ \omega^2\ 0\ \omega\ 0\ 1\ 1\ 1\ 1\ \omega^2\ 1\ \omega^2\ 1\ \omega^2\ \omega\ 0\ 0\ 1\ 1\ \omega^2\ \omega\ 1\ \omega\ \omega^2\ 0\ 1\ \omega\ 1\ \omega\ \omega\ 0\ \omega$ $0\ 0\ \omega\ 0\ 0\ 1\ \omega\ 0\ 0\ 1\ 1\ \omega\ \omega\ 1\ 0\ \omega^2\ 0\ \omega^2\ 1\ 1\ \omega^2\ \omega^2\ 1\ 0\ 1\ 0\ 0\ \omega\ \omega^2\ 1\ \omega\ \omega^2\ \omega\ 1\ 1\ 1\ \omega\ 0$ $0\ \omega\ 1\ 0\ 0\ 0\ 0\ 1\ 1\ \omega\ 0\ 1\ 0\ \omega\ 1\ \omega\ \omega^2\ 0\ 1\ \omega\ \omega^2\ \omega^2\ \omega\ \omega\ \omega^2\ \omega^2\ \omega\ \omega^2\ 1\ 1\ \omega^2\ \omega\ 1\ 0\ 0\ \omega\ 1\ 1$	$25^{48}26^{120}27^{216}28^{360}30^{84}$ $31^{48}32^{27}33^{48}34^{36}35^{24}36^{12}$	G_{16}
$1\ 1\ 1\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 1\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 1$ $1\ 0\ \omega\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ \omega^2\ 1\ 0\ \omega\ 0\ 1\ 1\ \omega^2\ \omega\ 1\ 1\ 0\ 1\ \omega\ 1\ 1\ 1\ \omega^2\ \omega^2\ \omega^2\ 1\ \omega^2\ 1\ \omega\ 1\ \omega\ \omega\ 0$ $0\ 0\ \omega^2\ 0\ 1\ 0\ \omega\ 1\ 0\ 0\ \omega\ \omega\ 1\ 0\ 0\ 1\ \omega\ \omega\ \omega\ \omega^2\ 1\ 1\ 0\ \omega^2\ 1\ \omega^2\ 1\ 0\ \omega^2\ 1\ 1\ \omega^2\ \omega\ 1\ 0\ 0\ \omega\ \omega^2$ $0\ 0\ \omega\ 0\ 0\ 1\ \omega\ 0\ 0\ \omega^2\ \omega^2\ \omega^2\ 1\ \omega^2\ 1\ 1\ \omega^2\ 1\ 0\ \omega\ 0\ \omega\ 1\ \omega^2\ 1\ 0\ \omega\ \omega\ \omega^2\ 1\ \omega^2\ \omega\ 1\ 0\ \omega\ 1\ \omega\ 1$ $\omega^2\ 0\ 1\ 0\ 0\ 0\ 0\ \omega\ 1\ \omega^2\ \omega\ 0\ \omega\ 0\ \omega^2\ 1\ \omega^2\ 1\ \omega\ 0\ \omega\ \omega^2\ 1\ \omega^2\ \omega^2\ 0\ 1\ 0\ 0\ \omega\ 0\ \omega^2\ \omega\ 1\ 1\ \omega\ \omega^2\ 0$	$25^{48}26^{168}27^{144}28^{288}29^{120}30^{108}$ $31^{24}32^{3}33^{24}34^{60}35^{24}36^{12}$	G_{16}
$1\ 1\ 1\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 1\ 1$ $1\ 0\ \omega\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ \omega^2\ 1\ 0\ \omega\ 0\ 1\ \omega\ 1\ \omega^2\ \omega\ 1\ 1\ 0\ 1\ \omega\ 1\ 1\ 1\ \omega^2\ \omega^2\ \omega^2\ 1\ \omega^2\ 1\ \omega\ 1\ \omega\ 0$ $0\ 0\ \omega^2\ 0\ 1\ 0\ 1\ \omega\ 0\ 0\ \omega\ \omega\ 1\ 0\ 0\ 1\ \omega^2\ \omega\ \omega\ \omega\ \omega^2\ 1\ 1\ 0\ \omega^2\ 1\ \omega^2\ 1\ 0\ \omega^2\ 1\ 1\ \omega^2\ \omega\ 1\ 0\ \omega\ \omega^2$ $0\ 0\ \omega\ 0\ 0\ 1\ 0\ \omega\ 0\ \omega^2\ \omega^2\ \omega^2\ 1\ \omega^2\ 1\ 1\ 1\ \omega^2\ 1\ 0\ \omega\ 0\ \omega\ 1\ \omega^2\ 1\ 0\ \omega\ \omega\ \omega^2\ 1\ \omega^2\ \omega\ 1\ 0\ \omega\ \omega\ 1$ $\omega^2\ 0\ 1\ 0\ 0\ 0\ \omega\ 0\ 1\ \omega^2\ \omega\ 0\ \omega\ 0\ \omega^2\ 1\ \omega\ \omega^2\ 1\ \omega\ 0\ \omega\ \omega^2\ 1\ \omega^2\ \omega^2\ 0\ 1\ 0\ 0\ \omega\ 0\ \omega^2\ \omega\ 1\ 1\ \omega^2\ 0$	$25^{48}26^{156}27^{192}28^{216}29^{168}$ $30^{96}31^{24}32^{3}33^{24}34^{60}35^{24}36^{12}$	$\mathcal{D}_4$

list is the unique complete quantum 38-cap in $PG(4,4)$.

4.10 The classification of quantum caps in $PG(4,4)$ containing the Hermitian variety of dimension 3

In this section the results about the classification of quantum caps, complete and non-complete in $PG(4,4)$ containing the $\mathcal{K}(3,17)$ is given. Note that it is not possible obtain in this search quantum caps $\mathcal{K}$ of size $k < 23$, since by Theorem 4.10 the set $\mathcal{C} \setminus \mathcal{H}(3,17)$ should be quantum and there exists no quantum caps of size less than 6 in $PG(4,4)$. Moreover the possible sizes are all odd, since any hyperplane intersection must have a number of points of the parity as k. Table 4.5 presents the results:

Table 4.5: Non-equivalent k-quantum caps $\mathcal{K}$ in $PG(4,4)$ containing $\mathcal{K}(3,17)$

k	Compl.	Incompl.
23	0	1
25	0	4
27	1	1
29	1	1
31	0	7
33	5	2
35	0	1

for each size is indicated the number of complete and incomplete quantum caps.

Chapter 5

Complete Arcs in $PG(2, q)$

5.1 Introduction

Let $PG(2, q)$ be the projective plane over the Galois field F_q. An n -arc is a set of n points no three of which are collinear. An n-arc is called complete if it is not contained in an $(n + 1)$-arc of $PG(2, q)$. For an introduction in projective geometries over finite fields, see [95], [153], [156].

In [97],[98] the close relationship between the theory of n-arcs, coding theory and mathematical statistics is presented. In particular, a complete arc in a plane $PG(2, q)$, points of which are treated as 3-dimensional q-ary columns, defines a parity check matrix of a q-ary MDS linear code with codimension 3, Hamming distance 4, and covering radius 2. Arcs are related to optimal coverings arrays [88] and to superregular matrices [110].

One of the main problems in the study of projective planes, which is also of interest in coding theory, is finding of the spectrum of possible sizes of complete arcs. The maximum size $m_2(2, q)$ of complete arcs in projective planes is well known. In fact we have that

$$m_2(2, q) = \begin{cases} q + 1 & q \text{ odd} \\ q + 2 & q \text{ even} \end{cases}$$

and examples of arcs of such sizes are conics for q odd and hyperovals for q even.

In particular, the value of $t_2(2,q)$, the smallest size of a complete arc in $PG(2,q)$, is interesting. Finding an estimation of the minimum size $t_2(2,q)$ is a hard open problem.

In particular in this chapter *upper bounds* on $t_2(2,q)$ are studied.

Surveys of results on the sizes of plane complete arcs, methods of their construction and comprehension of the relating properties can be found in [11], [51], [71], [93],[98], [153], [172].

Problems connected with small complete plane arcs are considered in [9], [11], [51], [54], [55], [72], [77], [81], [111], [123], [128], [135], [149], [153], [169], see also the references therein.

The exact values of $t_2(2,q)$ are known only for $q \leq 32$, see [128] and the recent work [129] where the equalities $t_2(2,31) = t_2(2,32) = 14$ are proven. Also, there are the following lower bounds (see [149],[153]):

$$t_2(2,q) > \begin{cases} \sqrt{2q}+1 & \text{for any } q \\ \sqrt{3q}+\frac{1}{2} & \text{for } q = p^h,\ p \text{ prime},\ h = 1,2,3 \end{cases}.$$

Let $t(\mathcal{P}_q)$ be the size of the smallest complete arc in any (not necessarily Galois) projective plane $\mathcal{P}_q$ of order q. In [111], for *sufficiently large* q, the following result is proven (we give it in the form of [98, Tab. 2.6]):

$$t(\mathcal{P}_q) \leq d\sqrt{q}\log^c q,\ c \leq 300, \tag{5.1}$$

where c and d are constants independent of q (i.e. universal constants). The logarithm basis is not noted as the estimate is asymptotic.

Following to [11], we denote the aggregates of q values:

$$\begin{aligned} T_2 &= \{5119, 5147, 5153, 5209, 5231, 5237, 5261, 5279, 5281, 5303, 5347, 5641, 5843, 6011, \\ &\quad 8192\}; \\ T_3 &= \{2^{14}, 2^{15}, 2^{18}\}; \\ Q &= \{961, 1024, 1369, 1681, 2401\} = \{31^2, 2^{10}, 37^2, 41^2, 7^4\}. \end{aligned}$$

Let $\bar{t}_2(2,q)$ be the smallest *known* size of a complete arc in $PG(2,q)$.

For $q \leq 841$ the values of $\bar{t}_2(2,q)$ are collected in [51, Tab. 1] whence it follows that $\bar{t}_2(2,q) < 4\sqrt{q}$ for $q \leq 841$. In [77], see also [81], complete $(4\sqrt{q}-4)$-arcs are obtained for $q = p^2$ odd, $q \leq 1681$ or $q = 2401$. In [55],[72] complete $(4\sqrt{q}-4)$-arcs are obtained for even $q = 64, 256, 1024$.

In this work we show that $\bar{t}_2(2,857) = 117 < 4\sqrt{857}$.

So, it holds that

$$t_2(2,q) < 4\sqrt{q} \quad \text{for } 2 \leq q \leq 841,\ q = 857,\ q \in Q. \tag{5.2}$$

For $q \leq 5107$ and $q \in T_2 \cup T_3$ the values of $\bar{t}_2(2,q)$ (up to June 2011) are collected in [11, Tabs. 1-4] where the following results are obtained:

$$t_2(2,q) < 4.5\sqrt{q} \quad \text{for } q \leq 2593,\ q = 2693, 2753. \tag{5.3}$$

$$t_2(2,q) < 4.79\sqrt{q} \quad \text{for } q \leq 5107. \tag{5.4}$$

$$t_2(2,q) < 4.98\sqrt{q} \quad \text{for } q \in T_2. \tag{5.5}$$

$$t_2(2,q) < 0.9987\sqrt{q}\ln^{0.75} q \quad \text{for } 23 \leq q \leq 5107,\ q \in T_2 \cup T_3. \tag{5.6}$$

Moreover, in [11] the following conjectures were proposed:

Conjecture 5.1. *[11]* In $PG(2,q)$,

$$t_2(2,q) < \sqrt{q}\ln^{0.75} q \quad \text{for } q \geq 23. \tag{5.7}$$

Conjecture 5.2. *[11]* In $PG(2,q)$,

$$t_2(2,q) < 5\sqrt{q} \qquad \text{for } q \leq 8192. \tag{5.8}$$

In this chapter we have obtained many new small arcs and extended and improved results of [11]. We have proven Conjecture 5.2, see Theorem 5.3.

Results of this chapter allow us to hope that Conjectures 5.1 is true.

We denote the aggregates of q values:

$$
\begin{aligned}
T_4 &= \{359, 367, 401, 419, 512, 541, 571, 643, 653, 719, 773, 787\};\\
T_5 &= \{857, 881, 919, 929, 941, 953, 967, 1019, 1031, 1069, 1097, 1109, 1123, 1151, 1163, 1187,\\
&\quad 1201, 1217, 1231, 1259, 1289, 1301, 1319, 1331, 1361, 1373, 1433, 1447, 1493, 1511, 1523,\\
&\quad 1553, 1567, 1571, 1583, 1597, 1601, 1613, 1627, 1663, 1693, 1697, 1723, 1741, 1759, 1777,\\
&\quad 1789, 1823, 1871, 1873, 1889, 1907, 1973, 1987, 1993, 2003, 2039, 2111, 2113, 2129, 2131,\\
&\quad 2141, 2143, 2179, 2197, 2213, 2237, 2251, 2269, 2287, 2309, 2339, 2341, 2357, 2399, 2411,\\
&\quad 2417, 2437, 2467, 2473, 2531, 2609, 2617, 2621\};\\
T_6 &= \{2657, 2659, 2663, 2677, 2683, 2699, 2719, 2741, 2797, 2801, 2819, 2833, 2837, 2851, 2857,\\
&\quad 2879, 2897, 2917, 2953, 2957, 2971, 2999, 3011, 3019, 3037, 3041, 3061, 3137, 3181, 3217,\\
&\quad 3221, 3259, 3307, 3329, 3331, 3371, 3373, 3391, 3407, 3449, 3461, 3527, 3541, 3547, 3557,\\
&\quad 3581, 3613, 3631, 3671, 3673, 3677, 3691, 3697, 3701, 3719, 3721, 3761, 3767, 3823, 3833,\\
&\quad 3847, 3851, 3877, 3917, 3923, 3943, 3947, 3989, 4007, 4051, 4079, 4096, 4127, 4129, 4201,\\
&\quad 4337, 4339, 4391, 4409, 4451, 4483, 4507, 4603, 4621, 4673, 4729, 4751, 4793, 4799, 4903,\\
&\quad 4931, 4973, 4999, 5023, 5051, 5077, 5081, 5099, 5101, 5153, 5209, 5231, 5261, 5279, 5281,\\
&\quad 5347, 5641, 6011, 8192\}.
\end{aligned}
$$

In this chapter we have obtained complete arcs with sizes smaller than in [11] (i.e. we improve upper bounds on $t_2(2, q)$) for $q \in T_4$ (in the region $q \leq 841$), for $q \in T_5$ (in the region $853 \leq q \leq 2621$), and for $q \in T_6$ (in the region $2633 \leq q$).

Theorem 5.3. *In $PG(2,q)$, the following holds.*

$$\begin{aligned} t_2(2,q) &< 4.5\sqrt{q} \quad \textit{for } q \le 2621,\ q = 2659, 2663, 2683, 2693, 2753, 2801. \\ t_2(2,q) &< 4.8\sqrt{q} \quad \textit{for } q \le 5399,\ q = 5413, 5417, 5419, 5441, 5443, 5471, 5483, 5501, 5521. \\ t_2(2,q) &< 5\sqrt{q} \quad \textit{for } q \le 9067. \end{aligned}$$

Theorem 5.4. *In $PG(2,q)$,*

$$t_2(2,q) < 0.9987\sqrt{q}\ln^{0.75} q \quad \textit{for } 23 \le q \le 9109,\ q \in T_3. \tag{5.9}$$

In whole, this chapter can be considered as development of work [11].

5.2 Small complete k-arcs in $PG(2,q)$, $q \le 9109$

Throughout the chapter, in all tables we denote $A_q = \left\lfloor a_q\sqrt{q} - \bar{t}_2(2,q) \right\rfloor$ where

$$a_q = \begin{cases} 4 & \text{if } q \le 841,\ q \in Q \\ 4.5 & \text{if } 853 \le q \le 2621,\ q = 2659, 2663, 2683, 2693, 2753, 2801,\ q \notin Q \\ 5 & \text{if } 2623 \le q \le 9067,\ q \notin \{2659, 2663, 2683, 2693, 2753, 2801\}. \end{cases}.$$

Also, in all tables, B_q is a superior approximation of $\bar{t}_2(2,q)/\sqrt{q}$.

For $q \le 841$, the values of $\bar{t}_2(2,q)$ (up to June 2011) are collected in [11, Tab. 1]. In this chapter we have obtained small arcs with new sizes for $q \in T_1$. The new arcs are obtained by computer search, based on randomized greedy algorithms (see Section 3.4). The current values of $\bar{t}_2(2,q)$ for $q \le 841$ are given in Table 1. The data for $q \in T_1$ improving results of [11, Tab. 1] are written in Table 1 in bold font. The exact values $\bar{t}_2(2,q) = t_2(2,q)$ are marked by the dot "**.** ". In particular, due to the recent result [129] we noted the values $t_2(2,31) = t_2(2,32) = 14$.

From Table 1 and the results of [77, 81], on complete $(4\sqrt{q}-4)$-arcs for $q = p^2$ (see Introduction 5.1) we obtain Theorem 5.5 improving and extending the results of [11, Th. 3.1].

Table 1. The smallest known sizes $\bar{t}_2 = \bar{t}_2(2,q) < 4\sqrt{q}$ of complete arcs in planes PG$(2,q)$, $q \le 841$.

$$A_q = \left\lfloor 4\sqrt{q} - \bar{t}_2(2,q) \right\rfloor,\ B_q \ge \bar{t}_2(2,q)/\sqrt{q}$$

q	$\bar{t}_2$	A_q	B_q	q	$\bar{t}_2$	A_q	B_q	q	$\bar{t}_2$	A_q	B_q	q	$\bar{t}_2$	A_q	B_q
2	**4.**	1	2.83	128	34	11	3.01	347	67	7	3.60	599	94	3	3.85
3	**4.**	2	2.31	131	36	9	3.15	349	67	7	3.59	601	90	8	3.68
4	**6.**	2	3.00	137	37	9	3.17	353	68	7	3.62	607	95	3	3.86
5	**6.**	2	2.69	139	37	10	3.14	**359**	**68**	**7**	**3.59**	613	96	3	3.88
7	**6.**	4	2.27	149	39	9	3.20	361	69	7	3.64	617	96	3	3.87
8	**6.**	5	2.13	151	39	10	3.18	**367**	**69**	**7**	**3.61**	619	96	3	3.86
9	**6.**	6	2.00	157	40	10	3.20	373	70	7	3.63	625	96	4	3.84
11	**7.**	6	2.12	163	41	10	3.22	379	71	6	3.65	631	97	3	3.87
13	**8.**	6	2.22	167	42	9	3.26	383	71	7	3.63	641	98	3	3.88
16	**9.**	7	2.25	169	42	10	3.24	389	72	6	3.66	**643**	**98**	**3**	**3.87**
17	**10.**	6	2.43	173	43	9	3.27	397	73	6	3.67	647	99	2	3.90
19	**10.**	7	2.30	179	44	9	3.29	**401**	**73**	**7**	**3.65**	**653**	**99**	**3**	**3.88**
23	**10.**	9	2.09	181	44	9	3.28	409	74	6	3.66	659	100	2	3.90
25	**12.**	8	2.40	191	46	9	3.33	**419**	**75**	**6**	**3.67**	661	90	12	3.51
27	**12.**	8	2.31	193	46	9	3.32	421	76	6	3.71	673	101	2	3.90
29	**13.**	8	2.42	197	47	9	3.35	431	77	6	3.71	677	102	2	3.93
31	**14.**	8	2.52	199	47	9	3.34	433	77	6	3.71	683	102	2	3.91
32	**14.**	8	2.48	211	49	9	3.38	439	78	5	3.73	691	103	2	3.92
37	15	9	2.47	223	51	8	3.42	443	78	6	3.71	701	104	1	3.93
41	16	9	2.50	227	51	9	3.39	449	79	5	3.73	709	104	2	3.91
43	16	10	2.45	229	51	9	3.38	457	80	5	3.75	**719**	**105**	**2**	**3.92**
47	18	9	2.63	233	52	9	3.41	461	80	5	3.73	727	106	1	3.94
49	18	10	2.58	239	53	8	3.43	463	80	6	3.72	729	104	4	3.86
53	18	11	2.48	241	53	9	3.42	467	81	5	3.75	733	107	1	3.96
59	20	10	2.61	243	53	9	3.40	479	82	5	3.75	739	107	1	3.94
61	20	11	2.57	251	55	8	3.48	487	83	5	3.77	743	108	1	3.97
64	22	10	2.75	256	55	9	3.44	491	83	5	3.75	751	108	1	3.95
67	23	9	2.81	257	55	9	3.44	499	84	5	3.77	757	109	1	3.97
71	22	11	2.62	263	56	8	3.46	503	85	4	3.79	761	109	1	3.96
73	24	10	2.81	269	57	8	3.48	509	85	5	3.77	769	110	0	3.97
79	26	9	2.93	271	57	8	3.47	**512**	**85**	**5**	**3.76**	**773**	**110**	**1**	**3.96**
81	26	10	2.89	277	58	8	3.49	521	86	5	3.77	**787**	**111**	**1**	**3.96**
83	27	9	2.97	281	59	8	3.52	523	86	5	3.77	797	112	0	3.97
89	28	9	2.97	283	59	8	3.51	529	87	5	3.79	809	113	0	3.98
97	30	9	3.05	289	60	8	3.53	**541**	**88**	**5**	**3.79**	811	113	0	3.97
101	30	10	2.99	293	60	8	3.51	547	89	4	3.81	821	114	0	3.98
103	31	9	3.06	307	62	8	3.54	557	90	4	3.82	823	114	0	3.98
107	32	9	3.10	311	63	7	3.58	563	91	3	3.84	827	115	0	4.00
109	32	9	3.07	313	63	7	3.57	569	91	4	3.82	829	115	0	4.00
113	33	9	3.11	317	63	8	3.54	**571**	**91**	**4**	**3.81**	839	115	0	3.98
121	34	10	3.10	331	65	7	3.58	577	92	4	3.84	841	112	4	3.87
125	35	9	3.14	337	66	7	3.60	587	93	3	3.84				
127	35	10	3.11	343	66	8	3.57	593	94	3	3.87				

Theorem 5.5. *In $PG(2,q)$, the following holds.*

$$
\begin{aligned}
t_2(2,q) &< 4\sqrt{q} \ \textit{ for } 2 \le q \le 841,\ q = 857,\ q \in Q. \qquad (5.10)\\
t_2(2,q) &\le 3\sqrt{q} \ \textit{ for } 2 \le q \le 89, \quad q = 101;\\
t_2(2,q) &< 3.5\sqrt{q} \ \textit{ for } 2 \le q \le 277;\\
t_2(2,q) &< 3.6\sqrt{q} \ \textit{ for } 2 \le q \le 349,\ q = 359, 661;\\
t_2(2,q) &< 3.7\sqrt{q} \ \textit{ for } 2 \le q \le 419,\ q = 601, 661;\\
t_2(2,q) &< 3.8\sqrt{q} \ \textit{ for } 2 \le q \le 541,\ q = 601, 661;\\
t_2(2,q) &< 3.9\sqrt{q} \ \textit{ for } 2 \le q \le 673,\ q = 729, 961, 1024.
\end{aligned}
$$

Also,

$$
\begin{aligned}
t_2(2,q) &\le 4\sqrt{q} - 9 \ \textit{ for } \ 37 \le q \le 211,\ q = 23, 227, 229, 233, 241, 243, 256, 257, 661;\\
t_2(2,q) &\le 4\sqrt{q} - 8 \ \textit{ for } \ 23 \le q \le 307,\ q = 317, 343, 601, 661;\\
t_2(2,q) &\le 4\sqrt{q} - 7 \ \textit{ for } \ 19 \le q \le 373,\ q = 383, 401, 601, 661;\\
t_2(2,q) &\le 4\sqrt{q} - 6 \ \textit{ for } \ 9 \le q \le 433,\ q = 443, 463, 601, 661;\\
t_2(2,q) &\le 4\sqrt{q} - 5 \ \textit{ for } \ 8 \le q \le 499,\ q = 509, 512, 521, 523, 529, 541, 601, 661;\\
t_2(2,q) &\le 4\sqrt{q} - 4 \ \textit{ for } \ 7 \le q \le 557,\ q = 569, 571, 577, 601, 625, 661, 729, 841,\ q \in Q;\\
t_2(2,q) &< 4\sqrt{q} - 3 \ \textit{ for } \ 7 \le q \le 643,\ q = 653, 661, 729, 841,\ q \in Q;\\
t_2(2,q) &\le 4\sqrt{q} - 2 \ \textit{ for } \ 3 \le q \le 691,\ q = 709, 719, 729, 841,\ q \in Q;\\
t_2(2,q) &< 4\sqrt{q} - 1 \ \textit{ for } \ 2 \le q \le 761,\ q = 773, 787, 841,\ q \in Q.
\end{aligned}
$$

For $853 \le q \le 2621$, the values of $\bar{t}_2(2,q)$ (up to June 2011) are collected in [11, Tabs 2,3]. In this chapter we have obtained small arcs with new sizes for $q \in T_5$. The new arcs are obtained by computer

search, based on randomized greedy algorithms (see Section 3.4). The current values of $\bar{t}_2(2,q) < 4.5\sqrt{q}$ for $853 \le q \le 2621$ are given in Table 2. The data for $q \in T_5$ improving results of [11, Tabs 2,3] are written in Table 2 in bold font. The data for $q = p^2$ with $\bar{t}_2(2,q) = 4\sqrt{q} - 4$ [77, 81] and for $q = 857$ with $\bar{t}_2(2,857) = 117 < 4\sqrt{857}$ are written in italic font.

From Table 2 and the results of [77, 81], on complete $(4\sqrt{q} - 4)$-arcs for $q = p^2$ (see Introduction 5.1) we obtain Theorem 5.6 improving and extending the results of [11, Th. 3.2].

Table 2. The smallest known sizes $\bar{t}_2 = \bar{t}_2(2,q) < 4.5\sqrt{q}$ of complete arcs in planes $PG(2,q)$,

$853 \le q \le 2621$, $A_q = \left\lfloor a_q\sqrt{q} - \bar{t}_2(2,q) \right\rfloor$, $B_q \ge \bar{t}_2(2,q)/\sqrt{q}$

q	$\bar{t}_2$	A_q	B_q	q	$\bar{t}_2$	A_q	B_q	q	$\bar{t}_2$	A_q	B_q	q	$\bar{t}_2$	A_q	B_q
853	117	14	4.01	1279	150	10	4.20	1699	178	7	4.32	2161	205	4	4.41
857	*117*	*0*	*4.00*	1283	150	11	4.19	1709	178	8	4.31	**2179**	**206**	**4**	**4.42**
859	118	13	4.03	**1289**	**150**	**11**	**4.18**	1721	179	7	4.32	2187	207	3	4.43
863	118	14	4.02	1291	151	10	4.21	**1723**	**179**	**7**	**4.32**	**2197**	**207**	**3**	**4.42**
877	119	14	4.02	1297	151	11	4.20	1733	180	7	4.33	2203	208	3	4.44
881	**119**	**14**	**4.01**	**1301**	**151**	**11**	**4.19**	**1741**	**180**	**7**	**4.32**	2207	208	3	4.43
883	120	13	4.04	1303	151	11	4.19	1747	181	7	4.34	2209	208	3	4.43
887	120	14	4.03	1307	152	10	4.21	1753	181	7	4.33	**2213**	**208**	**3**	**4.43**
907	122	13	4.06	**1319**	**152**	**11**	**4.19**	**1759**	**181**	**7**	**4.32**	2221	209	3	4.44
911	122	13	4.05	1321	153	10	4.21	**1777**	**182**	**7**	**4.32**	**2237**	**209**	**3**	**4.42**
919	**122**	**14**	**4.03**	1327	153	10	4.21	1783	183	7	4.34	2239	210	2	4.44
929	**123**	**14**	**4.04**	**1331**	**153**	**11**	**4.20**	1787	183	7	4.33	2243	210	3	4.44
937	124	13	4.06	**1361**	**155**	**11**	**4.21**	**1789**	**183**	**7**	**4.33**	**2251**	**210**	**3**	**4.43**
941	**124**	**14**	**4.05**	1367	156	10	4.22	1801	184	6	4.34	2267	211	3	4.44
947	125	13	4.07	*1369*	*144*	*4*	*3.90*	1811	184	7	4.33	**2269**	**211**	**3**	**4.43**
953	**125**	**13**	**4.05**	**1373**	**156**	**10**	**4.22**	**1823**	**185**	**7**	**4.34**	2273	212	2	4.45
961	*120*	*4*	*3.88*	1381	157	10	4.23	1831	186	6	4.35	2281	212	2	4.44
967	**126**	**13**	**4.06**	1399	158	10	4.23	1847	187	6	4.36	**2287**	**212**	**3**	**4.44**
971	127	13	4.08	1409	159	9	4.24	1849	187	6	4.35	2293	213	2	4.45
977	127	13	4.07	1423	160	9	4.25	1861	188	6	4.36	2297	213	2	4.45
983	128	13	4.09	1427	160	9	4.24	1867	188	6	4.36	**2309**	**213**	**3**	**4.44**
991	127	14	4.04	1429	160	10	4.24	**1871**	**188**	**6**	**4.35**	2311	214	2	4.46
997	129	13	4.09	**1433**	**160**	**10**	**4.23**	**1873**	**188**	**6**	**4.35**	2333	215	2	4.46
1009	130	12	4.10	1439	161	9	4.25	1877	189	5	4.37	**2339**	**215**	**2**	**4.45**
1013	130	13	4.09	**1447**	**161**	**10**	**4.24**	1879	189	6	4.37	**2341**	**214**	**3**	**4.43**
1019	**130**	**13**	**4.08**	1451	162	9	4.26	**1889**	**189**	**6**	**4.35**	2347	216	2	4.46
1021	131	12	4.10	1453	162	9	4.25	1901	190	6	4.36	2351	216	2	4.46
1024	*124*	*4*	*3.88*	1459	162	9	4.25	**1907**	**190**	**6**	**4.36**	**2357**	**216**	**2**	**4.45**

Table 2 (continue)

q	$\bar{t}_2$	A_q	B_q	q	$\bar{t}_2$	A_q	B_q	q	$\bar{t}_2$	A_q	B_q	q	$\bar{t}_2$	A_q	B_q
1031	**131**	**13**	**4.08**	1471	163	9	4.25	1913	191	5	4.37	2371	217	2	4.46
1033	132	12	4.11	1481	164	9	4.27	1931	192	5	4.37	2377	216	3	4.44
1039	132	13	4.10	1483	164	9	4.26	1933	192	5	4.37	2381	217	2	4.45
1049	133	12	4.11	1487	164	9	4.26	1949	193	5	4.38	2383	218	1	4.47
1051	133	12	4.11	1489	164	9	4.26	1951	193	5	4.37	2389	218	1	4.47
1061	134	12	4.12	**1493**	**164**	**9**	**4.25**	**1973**	**194**	**5**	**4.37**	2393	218	2	4.46
1063	134	12	4.11	1499	165	9	4.27	1979	195	5	4.39	**2399**	**218**	**2**	**4.46**
1069	**134**	**13**	**4.10**	**1511**	**165**	**9**	**4.25**	**1987**	**195**	**5**	**4.38**	*2401*	*192*	*4*	*3.92*
1087	136	12	4.13	**1523**	**166**	**9**	**4.26**	**1993**	**195**	**5**	**4.37**	**2411**	**219**	**1**	**4.47**
1091	136	12	4.12	1531	167	9	4.27	1997	196	5	4.39	**2417**	**219**	**2**	**4.46**
1093	136	12	4.12	1543	167	9	4.26	1999	196	5	4.39	2423	220	1	4.47
1097	**136**	**13**	**4.11**	1549	168	9	4.27	**2003**	**196**	**5**	**4.38**	**2437**	**220**	**2**	**4.46**
1103	137	12	4.13	**1553**	**168**	**9**	**4.27**	2011	197	4	4.40	2441	221	1	4.48
1109	**137**	**12**	**4.12**	1559	169	8	4.29	2017	197	5	4.39	2447	221	1	4.47
1117	138	12	4.13	**1567**	**169**	**9**	**4.27**	2027	198	4	4.40	2459	222	1	4.48
1123	**138**	**12**	**4.12**	**1571**	**169**	**9**	**4.27**	2029	198	4	4.40	**2467**	**222**	**1**	**4.47**
1129	139	12	4.14	1579	170	8	4.28	**2039**	**198**	**5**	**4.39**	**2473**	**222**	**1**	**4.47**
1151	**140**	**12**	**4.13**	**1583**	**170**	**9**	**4.28**	2048	199	4	4.40	2477	223	0	4.49
1153	141	11	4.16	**1597**	**171**	**8**	**4.28**	2053	199	4	4.40	2503	224	1	4.48
1163	**141**	**12**	**4.14**	**1601**	**171**	**9**	**4.28**	2063	200	4	4.41	2521	225	0	4.49
1171	142	11	4.15	1607	172	8	4.30	2069	200	4	4.40	**2531**	**225**	**1**	**4.48**
1181	143	11	4.17	1609	172	8	4.29	2081	201	4	4.41	2539	226	0	4.49
1187	**143**	**12**	**4.16**	**1613**	**172**	**8**	**4.29**	2083	201	4	4.41	2543	226	0	4.49
1193	144	11	4.17	1619	173	8	4.30	2087	201	4	4.40	2549	226	1	4.48
1201	**144**	**11**	**4.16**	1621	173	8	4.30	2089	201	4	4.40	2551	227	0	4.50
1213	145	11	4.17	**1627**	**173**	**8**	**4.29**	2099	202	4	4.41	2557	227	0	4.49
1217	**145**	**11**	**4.16**	1637	174	8	4.31	**2111**	**202**	**4**	**4.40**	2579	228	0	4.49
1223	146	11	4.18	1657	175	8	4.30	**2113**	**202**	**4**	**4.40**	2591	229	0	4.50
1229	146	11	4.17	**1663**	**175**	**8**	**4.30**	**2129**	**203**	**4**	**4.40**	2593	229	0	4.50
1231	**146**	**11**	**4.17**	1667	176	7	4.32	**2131**	**203**	**4**	**4.40**	**2609**	**229**	**0**	**4.49**
1237	147	11	4.18	1669	176	7	4.31	2137	204	4	4.42	**2617**	**230**	**0**	**4.50**
1249	148	11	4.19	*1681*	*160*	*4*	*3.91*	**2141**	**204**	**4**	**4.41**	**2621**	**230**	**0**	**4.50**
1259	**148**	**11**	**4.18**	**1693**	**177**	**8**	**4.31**	**2143**	**204**	**4**	**4.41**				
1277	150	10	4.20	**1697**	**177**	**8**	**4.30**	2153	205	3	4.42				

Theorem 5.6. *In $PG(2,q)$, the following holds.*

$$
\begin{aligned}
t_2(2,q) &< 4.5\sqrt{q} \ \ \textit{for } q \le 2621,\ q = 2659, 2663, 2683, 2693, 2753, 2801. \qquad (5.11)\\
t_2(2,q) &< 4.1\sqrt{q} \ \ \textit{for } q \le 1031,\ q = 1039, 1069, 1369, 1681, 2401;\\
t_2(2,q) &< 4.2\sqrt{q} \ \ \textit{for } q \le 1289,\ q = 1297, 1301, 1303, 1319, 1331, 1369, 1681, 2401;\\
t_2(2,q) &< 4.3\sqrt{q} \ \ \textit{for } q \le 1627,\ q = 1657, 1663, 1681, 1697, 2401;\\
t_2(2,q) &< 4.4\sqrt{q} \ \ \textit{for } q \le 2053,\ q = 2069, 2087, 2089, 2111, 2113, 2129, 2131, 2401.
\end{aligned}
$$

Also,

$$
\begin{aligned}
t_2(2,q) &< 4.5\sqrt{q} - 13 \ \ \textit{for } q \le \ 997,\ q = 1013, 1019, 1024, 1031, 1039, 1069, 1097, 1369, 1681,\\
&\qquad\qquad 2401;\\
t_2(2,q) &< 4.5\sqrt{q} - 12 \ \ \textit{for } q \le 1151,\ q = 1163, 1187, 1369, 1681, 2401;\\
t_2(2,q) &< 4.5\sqrt{q} - 11 \ \ \textit{for } q \le 1259,\ q = 1283, 1289, 1297, 1301, 1303, 1331, 1319, 1331, 1361,\\
&\qquad\qquad 1369, 1681, 2401;\\
t_2(2,q) &< 4.5\sqrt{q} - 10 \ \ \textit{for } q \le 1399,\ q = 1429, 1433, 1447, 1681, 2401;\\
t_2(2,q) &< 4.5\sqrt{q} - 9 \ \ \textit{for } q \le 1553,\ q = 1567, 1571, 1583, 1601, 1681, 2401;\\
t_2(2,q) &< 4.5\sqrt{q} - 8 \ \ \textit{for } q \le 1663,\ q = 1681, 1693, 1697, 1709, 2401;\\
t_2(2,q) &< 4.5\sqrt{q} - 7 \ \ \textit{for } q \le 1789,\ q = 1811, 1823, 2401;\\
t_2(2,q) &< 4.5\sqrt{q} - 6 \ \ \textit{for } q \le 1873,\ q = 1879, 1889, 1901, 1907, 2401;\\
t_2(2,q) &< 4.5\sqrt{q} - 5 \ \ \textit{for } q \le 2003,\ q = 2017, 2039, 2401;\\
t_2(2,q) &< 4.5\sqrt{q} - 4 \ \ \textit{for } q \le 2143,\ q = 2161, 2179, 2401;\\
t_2(2,q) &< 4.5\sqrt{q} - 3 \ \ \textit{for } q \le 2237,\ q = 2243, 2251, 2267, 2269, 2287, 2309, 2341, 2377, 2401;\\
t_2(2,q) &< 4.5\sqrt{q} - 2 \ \ \textit{for } q \le 2381,\ q = 2393, 2399, 2401, 2417, 2437;\\
t_2(2,q) &< 4.5\sqrt{q} - 1 \ \ \textit{for } q \le 2473,\ q = 2503, 2531, 2549.
\end{aligned}
$$

For $2633 \le q \le 5107$ and for a few sporadic $q > 5107$, the values of $\bar{t}_2(2,q)$ (up to June 2011) are collected in [11, Tabs 3,4]. In this chapter we have obtained small arcs with new sizes for $q \in T_6$. The new arcs are obtained by computer search, based on randomized greedy algorithms (see Section 3.4). The current values of $\bar{t}_2(2,q) < 4.8\sqrt{q}$ for $2633 \le q \le 5399$ are given in Table 3. The data for $q \in T_6$

and other data (obtained in this work) improving and extending results of [11, Tabs 3,4] are written in Table 3 in bold font. The data for $q = 2659, 2663, 2683, 2693, 2753, 2801$ with $\bar{t}_2(2,q) < 4.5\sqrt{q}$ are written in italic font.

Table 3. The smallest known sizes $\bar{t}_2 = \bar{t}_2(2,q) < 4.8\sqrt{q}$ of complete arcs in planes $PG(2,q)$, $2633 \le q \le 5399$, $A_q = \left\lfloor a_q\sqrt{q} - \bar{t}_2(2,q) \right\rfloor$, $B_q \ge \bar{t}_2(2,q)/\sqrt{q}$

q	$\bar{t}_2$	A_q	B_q	q	$\bar{t}_2$	A_q	B_q	q	$\bar{t}_2$	A_q	B_q	q	$\bar{t}_2$	A_q	B_q
2633	231	25	4.51	**3307**	**264**	**23**	**4.60**	**3947**	**293**	**21**	**4.67**	4663	323	18	4.74
2647	232	25	4.51	3313	265	22	4.61	3967	294	20	4.67	**4673**	**323**	**18**	**4.73**
2657	**232**	**25**	**4.51**	3319	265	23	4.60	**3989**	**295**	**20**	**4.68**	4679	324	18	4.74
2659	*232*	*0*	*4.50*	3323	265	23	4.60	4001	296	20	4.68	4691	324	18	4.74
2663	*232*	*0*	*4.50*	**3329**	**265**	**23**	**4.60**	4003	296	20	4.68	4703	325	17	4.74
2671	233	25	4.51	**3331**	**265**	**23**	**4.60**	**4007**	**296**	**20**	**4.68**	4721	326	17	4.75
2677	**233**	**25**	**4.51**	3343	265	24	4.59	4013	296	20	4.68	4723	326	17	4.75
2683	*233*	*0*	*4.50*	3347	266	23	4.60	4019	296	20	4.67	**4729**	**325**	**18**	**4.73**
2687	234	25	4.52	3359	267	22	4.61	4021	296	21	4.67	4733	326	17	4.74
2689	234	25	4.52	3361	267	22	4.61	4027	296	21	4.67	**4751**	**327**	**17**	**4.75**
2693	*233*	*0*	*4.49*	**3371**	**267**	**23**	**4.60**	4049	298	20	4.69	4759	327	17	4.75
2699	**234**	**25**	**4.51**	**3373**	**267**	**23**	**4.60**	**4051**	**298**	**20**	**4.69**	4783	328	17	4.75
2707	235	25	4.52	3389	268	23	4.61	4057	298	20	4.68	4787	329	16	4.76
2711	235	25	4.52	**3391**	**267**	**24**	**4.59**	4073	299	20	4.69	4789	329	17	4.76
2713	235	25	4.52	**3407**	**269**	**22**	**4.61**	**4079**	**299**	**20**	**4.69**	**4793**	**329**	**17**	**4.76**
2719	**235**	**25**	**4.51**	3413	269	23	4.61	4091	300	19	4.70	**4799**	**329**	**17**	**4.75**
2729	236	25	4.52	3433	270	22	4.61	4093	300	19	4.69	4801	329	17	4.75
2731	236	25	4.52	**3449**	**271**	**22**	**4.62**	**4096**	**300**	**20**	**4.69**	4813	330	16	4.76
2741	**236**	**25**	**4.51**	3457	271	22	4.61	4099	300	20	4.69	4817	329	18	4.75
2749	237	25	4.53	**3461**	**271**	**23**	**4.61**	4111	301	19	4.70	4831	329	18	4.74
2753	*236*	*0*	*4.50*	3463	272	22	4.63	**4127**	**301**	**20**	**4.69**	4861	331	17	4.75
2767	238	25	4.53	3467	272	22	4.62	**4129**	**301**	**20**	**4.69**	4871	332	16	4.76
2777	238	25	4.52	3469	272	22	4.62	4133	302	19	4.70	4877	332	17	4.76
2789	239	25	4.53	3481	272	23	4.62	4139	302	19	4.70	4889	333	16	4.77
2791	239	25	4.53	3491	273	22	4.63	4153	301	21	4.68	**4903**	**333**	**17**	**4.76**
2797	**239**	**25**	**4.52**	3499	273	22	4.62	4157	303	19	4.70	4909	334	16	4.77
2801	*238*	*0*	*4.50*	3511	274	22	4.63	4159	302	20	4.69	4913	334	16	4.77
2803	240	24	4.54	3517	274	22	4.63	4177	303	20	4.69	4919	334	16	4.77
2809	240	25	4.53	**3527**	**274**	**22**	**4.62**	**4201**	**304**	**20**	**4.70**	**4931**	**334**	**17**	**4.76**
2819	**240**	**25**	**4.53**	3529	275	22	4.63	4211	305	19	4.71	4933	335	16	4.77
2833	**240**	**26**	**4.51**	3533	275	22	4.63	4217	305	19	4.70	4937	335	16	4.77
2837	**241**	**25**	**4.53**	3539	275	22	4.63	4219	305	19	4.70	4943	334	17	4.76
2843	242	24	4.54	**3541**	**275**	**22**	**4.63**	4229	305	20	4.70	4951	335	16	4.77
2851	**242**	**24**	**4.54**	**3547**	**275**	**22**	**4.62**	4231	306	19	4.71	4957	335	17	4.76
2857	**242**	**25**	**4.53**	**3557**	**276**	**22**	**4.63**	4241	306	19	4.70	4967	336	16	4.77

Table 3 (continue)

q	$\bar{t}_2$	A_q	B_q	q	$\bar{t}_2$	A_q	B_q	q	$\bar{t}_2$	A_q	B_q	q	$\bar{t}_2$	A_q	B_q
2861	243	24	4.55	3559	276	22	4.63	4243	306	19	4.70	4969	336	16	4.77
2879	**243**	**25**	**4.53**	3571	277	21	4.64	4253	306	20	4.70	**4973**	**336**	**16**	**4.77**
2887	243	25	4.53	**3581**	**277**	**22**	**4.63**	4259	307	19	4.71	4987	336	17	4.76
2897	**244**	**25**	**4.54**	3583	277	22	4.63	4261	307	19	4.71	4993	337	16	4.77
2903	245	24	4.55	3593	278	21	4.64	4271	307	19	4.70	**4999**	**337**	**16**	**4.77**
2909	245	24	4.55	3607	278	22	4.63	4273	306	20	4.69	5003	337	16	4.77
2917	**245**	**25**	**4.54**	**3613**	**278**	**22**	**4.63**	4283	308	19	4.71	5009	337	16	4.77
2927	245	25	4.53	3617	278	22	4.63	4289	308	19	4.71	5011	337	16	4.77
2939	246	25	4.54	3623	279	21	4.64	4297	308	19	4.70	5021	338	16	4.78
2953	**246**	**25**	**4.53**	**3631**	**279**	**22**	**4.64**	4327	310	18	4.72	**5023**	**338**	**16**	**4.77**
2957	**247**	**24**	**4.55**	3637	280	21	4.65	**4337**	**310**	**19**	**4.71**	5039	339	15	4.78
2963	248	24	4.56	3643	278	23	4.61	**4339**	**310**	**19**	**4.71**	5041	339	16	4.78
2969	248	24	4.56	3659	281	21	4.65	4349	311	18	4.72	**5051**	**339**	**16**	**4.77**
2971	**247**	**25**	**4.54**	**3671**	**281**	**21**	**4.64**	4357	311	19	4.72	5059	339	16	4.77
2999	**249**	**24**	**4.55**	**3673**	**280**	**23**	**4.63**	4363	310	20	4.70	**5077**	**340**	**16**	**4.78**
3001	250	23	4.57	**3677**	**281**	**22**	**4.64**	4373	312	18	4.72	**5081**	**340**	**16**	**4.77**
3011	**250**	**24**	**4.56**	**3691**	**282**	**21**	**4.65**	**4391**	**312**	**19**	**4.71**	5087	341	15	4.79
3019	**250**	**24**	**4.55**	**3697**	**282**	**22**	**4.64**	4397	313	18	4.73	**5099**	**341**	**16**	**4.78**
3023	251	23	4.57	**3701**	**282**	**22**	**4.64**	**4409**	**313**	**19**	**4.72**	**5101**	**341**	**16**	**4.78**
3037	**251**	**24**	**4.56**	3709	283	21	4.65	4421	314	18	4.73	5107	341	16	4.78
3041	**251**	**24**	**4.56**	**3719**	**283**	**21**	**4.65**	4423	312	20	4.70	**5113**	**341**	**16**	**4.77**
3049	252	24	4.57	**3721**	**283**	**22**	**4.64**	4441	315	18	4.73	5119	341	16	4.77
3061	**252**	**24**	**4.56**	3727	284	21	4.66	4447	314	19	4.71	5147	343	15	4.79
3067	253	23	4.57	3733	284	21	4.65	**4451**	**315**	**18**	**4.73**	**5153**	**342**	**16**	**4.77**
3079	253	24	4.56	3739	283	22	4.63	4457	315	18	4.72	**5167**	**344**	**15**	**4.79**
3083	253	24	4.56	**3761**	**284**	**22**	**4.64**	4463	315	19	4.72	**5171**	**344**	**15**	**4.79**
3089	254	23	4.58	**3767**	**285**	**21**	**4.65**	4481	315	19	4.71	**5179**	**344**	**15**	**4.79**
3109	255	23	4.58	3769	286	20	4.66	**4483**	**316**	**18**	**4.72**	**5189**	**344**	**16**	**4.78**
3119	255	24	4.57	3779	286	21	4.66	4489	316	19	4.72	**5197**	**345**	**15**	**4.79**
3121	255	24	4.57	3793	287	20	4.67	4493	317	18	4.73	**5209**	**345**	**15**	**4.79**
3125	256	23	4.58	3797	287	21	4.66	**4507**	**317**	**18**	**4.73**	**5227**	**346**	**15**	**4.79**
3137	**256**	**24**	**4.58**	3803	287	21	4.66	4513	318	17	4.74	**5231**	**346**	**15**	**4.79**
3163	257	24	4.57	3821	288	21	4.66	4517	317	19	4.72	**5233**	**346**	**15**	**4.79**
3167	258	23	4.59	**3823**	**288**	**21**	**4.66**	4519	318	18	4.74	5237	347	14	4.80
3169	258	23	4.59	**3833**	**288**	**21**	**4.66**	4523	318	18	4.73	**5261**	**347**	**15**	**4.79**
3181	**258**	**24**	**4.58**	**3847**	**288**	**22**	**4.65**	4547	319	18	4.74	**5273**	**348**	**15**	**4.80**
3187	258	24	4.58	**3851**	**288**	**22**	**4.65**	4549	319	18	4.73	**5279**	**348**	**15**	**4.79**
3191	259	23	4.59	3853	289	21	4.66	4561	319	18	4.73	**5281**	**348**	**15**	**4.79**
3203	259	23	4.58	3863	290	20	4.67	4567	320	17	4.74	**5297**	**349**	**14**	**4.80**
3209	260	23	4.59	**3877**	**290**	**21**	**4.66**	4583	320	18	4.73	5303	349	15	4.80
3217	**260**	**23**	**4.59**	3881	291	20	4.68	4591	321	17	4.74	**5309**	**349**	**15**	**4.79**
3221	**260**	**23**	**4.59**	3889	291	20	4.67	4597	321	18	4.74	**5323**	**349**	**15**	**4.79**
3229	260	24	4.58	3907	292	20	4.68	**4603**	**321**	**18**	**4.74**	**5329**	**350**	**15**	**4.80**
3251	262	23	4.60	3911	292	20	4.67	**4621**	**321**	**18**	**4.73**	**5333**	**349**	**16**	**4.78**
3253	261	24	4.58	**3917**	**291**	**21**	**4.65**	4637	322	18	4.73	**5347**	**350**	**15**	**4.79**
3257	262	23	4.60	3919	292	21	4.67	4639	323	17	4.75	**5351**	**350**	**15**	**4.79**
3259	**262**	**23**	**4.59**	**3923**	**292**	**21**	**4.67**	4643	323	17	4.75	**5381**	**352**	**14**	**4.80**
3271	263	22	4.60	3929	293	20	4.68	4649	323	17	4.74	**5387**	**352**	**14**	**4.80**
3299	264	23	4.60	3931	293	20	4.68	4651	323	17	4.74	**5393**	**352**	**15**	**4.80**
3301	264	23	4.60	**3943**	**293**	**20**	**4.67**	4657	323	18	4.74	**5399**	**352**	**15**	**4.80**

The current values of $\bar{t}_2(2,q)$ for $5407 \le q \le 8353$ and $8363 \le q \le 9109$ are given in Tables 4 and 5, respectively. All results in these tables (see also [9]) are new and they have been obtained in this chapter by computer search, based on randomized greedy algorithms (see Section 3.4). Data for $q = 5413, 5417, 5419, 5441, 5443, 5471, 5483, 5501, 5521$ with $\bar{t}_2(2,q) < 4.8\sqrt{q}$ are written in Table 4 in italic font.

From Tables 3 - 5 we obtain Theorem 5.7 improving and extending the results of [11, Th. 3.3].

Table 4. The smallest known sizes $\bar{t}_2 = \bar{t}_2(2,q)$ of complete arcs in planes $PG(2,q)$, $5407 \le q \le 8353$, $A_q = \left\lfloor 5\sqrt{q} - \bar{t}_2(2,q) \right\rfloor, B_q \ge \bar{t}_2(2,q)/\sqrt{q}$

q	$\bar{t}_2$	A_q	B_q	q	$\bar{t}_2$	A_q	B_q	q	$\bar{t}_2$	A_q	B_q	q	$\bar{t}_2$	A_q	B_q
5407	353	14	4.81	6121	380	11	4.86	6841	404	9	4.89	7589	430	5	4.94
5413	*353*	*14*	*4.80*	6131	380	11	4.86	6857	405	9	4.90	7591	430	5	4.94
5417	*353*	*15*	*4.80*	6133	380	11	4.86	6859	405	9	4.90	7603	430	5	4.94
5419	*353*	*15*	*4.80*	6143	379	12	4.84	6863	405	9	4.89	7607	430	6	4.94
5431	354	14	4.81	6151	380	12	4.85	6869	405	9	4.89	7621	431	5	4.94
5437	354	14	4.81	6163	380	12	4.85	6871	405	9	4.89	7639	432	5	4.95
5441	*354*	*14*	*4.80*	6173	382	10	4.87	6883	406	8	4.90	7643	431	6	4.93
5443	*354*	*14*	*4.80*	6197	382	11	4.86	6889	406	9	4.90	7649	432	5	4.94
5449	355	14	4.81	6199	383	10	4.87	6899	406	9	4.89	7669	431	6	4.93
5471	*355*	*14*	*4.80*	6203	383	10	4.87	6907	407	8	4.90	7673	432	5	4.94
5477	356	14	4.82	6211	383	11	4.86	6911	408	7	4.91	7681	433	5	4.95
5479	356	14	4.81	6217	383	11	4.86	6917	408	7	4.91	7687	433	5	4.94
5483	*355*	*15*	*4.80*	6221	383	11	4.86	6947	408	8	4.90	7691	433	5	4.94
5501	*356*	*14*	*4.80*	6229	383	11	4.86	6949	408	8	4.90	7699	433	5	4.94
5503	357	13	4.82	6241	384	11	4.87	6959	409	8	4.91	7703	434	4	4.95
5507	357	14	4.82	6247	384	11	4.86	6961	408	9	4.90	7717	434	5	4.95
5519	357	14	4.81	6257	384	11	4.86	6967	409	8	4.91	7723	435	4	4.95
5521	356	15	4.80	6263	385	10	4.87	6971	409	8	4.90	7727	434	5	4.94
5527	357	14	4.81	6269	384	11	4.85	6977	410	7	4.91	7741	435	4	4.95
5531	358	13	4.82	6271	384	11	4.85	6983	408	9	4.89	7753	436	4	4.96
5557	358	14	4.81	6277	385	11	4.86	6991	410	8	4.91	7757	436	4	4.96
5563	359	13	4.82	6287	385	11	4.86	6997	409	9	4.89	7759	436	4	4.95
5569	359	14	4.82	6299	385	11	4.86	7001	409	9	4.89	7789	437	4	4.96
5573	359	14	4.81	6301	386	10	4.87	7013	411	7	4.91	7793	437	4	4.96
5581	359	14	4.81	6311	386	11	4.86	7019	411	7	4.91	7817	437	5	4.95
5591	359	14	4.81	6317	387	10	4.87	7027	412	7	4.92	7823	438	4	4.96
5623	361	13	4.82	6323	387	10	4.87	7039	410	9	4.89	7829	437	5	4.94
5639	362	13	4.83	6329	387	10	4.87	7043	412	7	4.91	7841	438	4	4.95
5641	362	13	4.82	6337	388	10	4.88	7057	413	7	4.92	7853	438	5	4.95
5647	362	13	4.82	6343	388	10	4.88	7069	412	8	4.91	7867	440	3	4.97
5651	362	13	4.82	6353	388	10	4.87	7079	413	7	4.91	7873	440	3	4.96
5653	362	13	4.82	6359	387	11	4.86	7103	414	7	4.92	7877	438	5	4.94
5657	363	13	4.83	6361	388	10	4.87	7109	414	7	4.92	7879	440	3	4.96
5659	363	13	4.83	6367	389	9	4.88	7121	414	7	4.91	7883	438	5	4.94
5669	363	13	4.83	6373	389	10	4.88	7127	414	8	4.91	7901	441	3	4.97

Table 4 (continue)

q	$\bar{t}_2$	A_q	B_q	q	$\bar{t}_2$	A_q	B_q	q	$\bar{t}_2$	A_q	B_q	q	$\bar{t}_2$	A_q	B_q
5683	363	13	4.82	6379	389	10	4.88	7129	415	7	4.92	7907	440	4	4.95
5689	363	14	4.82	6389	388	11	4.86	7151	416	6	4.92	7919	441	3	4.96
5693	363	14	4.82	6397	389	10	4.87	7159	415	8	4.91	7921	440	5	4.95
5701	364	13	4.83	6421	390	10	4.87	7177	416	7	4.92	7927	440	5	4.95
5711	363	14	4.81	6427	391	9	4.88	7187	415	8	4.90	7933	442	3	4.97
5717	364	14	4.82	6449	391	10	4.87	7193	415	9	4.90	7937	442	3	4.97
5737	365	13	4.82	6451	392	9	4.89	7207	417	7	4.92	7949	442	3	4.96
5741	366	12	4.84	6469	391	11	4.87	7211	418	6	4.93	7951	441	4	4.95
5743	365	13	4.82	6473	392	10	4.88	7213	417	7	4.91	7963	442	4	4.96
5749	365	14	4.82	6481	392	10	4.87	7219	417	7	4.91	7993	443	4	4.96
5779	367	13	4.83	6491	393	9	4.88	7229	418	7	4.92	8009	444	3	4.97
5783	366	14	4.82	6521	392	11	4.86	7237	418	7	4.92	8011	444	3	4.97
5791	367	13	4.83	6529	393	11	4.87	7243	419	6	4.93	8017	443	4	4.95
5801	367	13	4.82	6547	394	10	4.87	7247	419	6	4.93	8039	444	4	4.96
5807	368	13	4.83	6551	395	9	4.89	7253	418	7	4.91	8053	445	3	4.96
5813	366	15	4.81	6553	395	9	4.88	7283	420	6	4.93	8059	446	2	4.97
5821	369	12	4.84	6561	395	10	4.88	7297	421	6	4.93	8069	446	3	4.97
5827	369	12	4.84	6563	395	10	4.88	7307	418	9	4.89	8081	445	4	4.96
5839	369	13	4.83	6569	395	10	4.88	7309	420	7	4.92	8087	446	3	4.96
5843	370	12	4.85	6571	396	9	4.89	7321	421	6	4.93	8089	447	2	4.98
5849	369	13	4.83	6577	396	9	4.89	7331	422	6	4.93	8093	447	2	4.97
5851	370	12	4.84	6581	396	9	4.89	7333	421	7	4.92	8101	447	3	4.97
5857	370	12	4.84	6599	396	10	4.88	7349	422	6	4.93	8111	448	2	4.98
5861	370	12	4.84	6607	397	9	4.89	7351	422	6	4.93	8117	448	2	4.98
5867	370	12	4.84	6619	398	8	4.90	7369	422	7	4.92	8123	448	2	4.98
5869	370	13	4.83	6637	398	9	4.89	7393	423	6	4.92	8147	448	3	4.97
5879	371	12	4.84	6653	398	9	4.88	7411	425	5	4.94	8161	448	3	4.96
5881	371	12	4.84	6659	398	10	4.88	7417	423	7	4.92	8167	448	3	4.96
5897	372	11	4.85	6661	398	10	4.88	7433	425	6	4.93	8171	448	3	4.96
5903	372	12	4.85	6673	399	9	4.89	7451	422	9	4.89	8179	449	3	4.97
5923	372	12	4.84	6679	399	9	4.89	7457	424	7	4.92	8191	449	3	4.97
5927	372	12	4.84	6689	399	9	4.88	7459	425	6	4.93	8192	449	3	4.97
5939	373	12	4.85	6691	399	9	4.88	7477	426	6	4.93	8209	450	3	4.97
5953	372	13	4.83	6701	400	9	4.89	7481	426	6	4.93	8219	451	2	4.98
5981	375	11	4.85	6703	400	9	4.89	7487	426	6	4.93	8221	451	2	4.98
5987	374	12	4.84	6709	400	9	4.89	7489	426	6	4.93	8231	451	2	4.98
6007	375	12	4.84	6719	400	9	4.88	7499	427	5	4.94	8233	451	2	4.98
6011	376	11	4.85	6733	401	9	4.89	7507	427	6	4.93	8237	452	1	4.99
6029	375	13	4.83	6737	401	9	4.89	7517	427	6	4.93	8243	451	2	4.97
6037	377	11	4.86	6761	402	9	4.89	7523	428	5	4.94	8263	451	3	4.97
6043	377	11	4.85	6763	402	9	4.89	7529	428	5	4.94	8269	453	1	4.99
6047	377	11	4.85	6779	403	8	4.90	7537	428	6	4.93	8273	452	2	4.97
6053	377	12	4.85	6781	403	8	4.90	7541	428	6	4.93	8287	450	5	4.95
6067	378	11	4.86	6791	403	9	4.90	7547	428	6	4.93	8291	453	2	4.98
6073	377	12	4.84	6793	403	9	4.89	7549	428	6	4.93	8293	453	2	4.98
6079	378	11	4.85	6803	402	10	4.88	7559	429	5	4.94	8297	453	2	4.98
6089	378	12	4.85	6823	404	9	4.90	7561	429	5	4.94	8311	453	2	4.97
6091	379	11	4.86	6827	404	9	4.89	7573	429	6	4.93	8317	454	1	4.98
6101	379	11	4.86	6829	404	9	4.89	7577	428	7	4.92	8329	454	2	4.98
6113	379	11	4.85	6833	404	9	4.89	7583	429	6	4.93	8353	454	2	4.97

Table 5. The smallest known sizes $\bar{t}_2 = \bar{t}_2(2,q)$ of complete arcs in planes $PG(2,q)$, $8363 \le q \le 9109$, $A_q = \left\lfloor 5\sqrt{q} - \bar{t}_2(2,q) \right\rfloor, B_q \ge \bar{t}_2(2,q)/\sqrt{q}$

q	$\bar{t}_2$	A_q	B_q	q	$\bar{t}_2$	A_q	B_q	q	$\bar{t}_2$	A_q	B_q	q	$\bar{t}_2$	A_q	B_q
8363	455	2	4.98	8573	462	0	4.99	8737	466	1	4.99	8929	471	1	4.99
8369	456	1	4.99	8581	461	2	4.98	8741	467	0	5.00	8933	472	0	5.00
8377	454	3	4.97	8597	463	0	5.00	8747	466	1	4.99	8941	472	0	5.00
8387	456	1	4.98	8599	462	1	4.99	8753	467	0	5.00	8951	473	0	5.00
8389	456	1	4.98	8609	463	0	5.00	8761	467	1	4.99	8963	473	0	5.00
8419	457	1	4.99	8623	463	1	4.99	8779	468	0	5.00	8969	473	0	5.00
8423	457	1	4.98	8627	464	0	5.00	8783	468	0	5.00	8971	472	1	4.99
8429	457	2	4.98	8629	464	0	5.00	8803	468	1	4.99	8999	473	1	4.99
8431	457	2	4.98	8641	464	0	5.00	8807	468	1	4.99	9001	474	0	5.00
8443	457	2	4.98	8647	463	1	4.98	8819	469	0	5.00	9007	474	0	5.00
8447	457	2	4.98	8663	465	0	5.00	8821	469	0	5.00	9011	472	2	4.98
8461	459	0	5.00	8669	465	0	5.00	8831	469	0	5.00	9013	474	0	5.00
8467	458	2	4.98	8677	465	0	5.00	8837	470	0	5.00	9029	475	0	5.00
8501	459	2	4.98	8681	464	1	4.99	8839	470	0	5.00	9041	475	0	5.00
8513	460	1	4.99	8689	465	1	4.99	8849	470	0	5.00	9043	475	0	5.00
8521	460	1	4.99	8693	465	1	4.99	8861	470	0	5.00	9049	475	0	5.00
8527	460	1	4.99	8699	465	1	4.99	8863	470	0	5.00	9059	475	0	5.00
8537	460	1	4.98	8707	466	0	5.00	8867	470	0	5.00	9067	476	0	5.00
8539	460	2	4.98	8713	466	0	5.00	8887	469	2	4.98	9091	477		5.01
8543	461	1	4.99	8719	466	0	5.00	8893	471	0	5.00	9103	479		5.03
8563	461	1	4.99	8731	466	1	4.99	8923	472	0	5.00	9109	479		5.02

Theorem 5.7. *In $PG(2,q)$, the following holds.*

$$t_2(2,q) < 5\sqrt{q} \quad \text{for } q \le 9067. \tag{5.12}$$

$$t_2(2,q) < 4.6\sqrt{q} \quad \text{for } q \le 3307,\ q = 3319, 3323, 3329, 3331, 3343, 3347, 3371, 3373, 3391;$$

$$t_2(2,q) < 4.7\sqrt{q} \quad \text{for } q \le 4201,\ q = 4217, 4219, 4229, 4241, 4243, 4253, 4271, 4273, 4297, 4363, 4423.$$

$$t_2(2,q) < 4.8\sqrt{q} \quad \text{for } q \le 5399,\ q = 5413, 5417, 5419, 5441, 5443, 5471, 5483, 5501, 5521;$$

$$t_2(2,q) < 4.9\sqrt{q} \quad \text{for } q \le 6907,\ q = 6947, 6949, 6961, 6971, 6983, 6997, 7001, 7039, 7187, 7193, 7307, 7451.$$

Also,

$$
\begin{aligned}
t_2(2,q) &< 5\sqrt{q}-22 \text{ for } q \le 3559,\ q = 3581,3583,3607,3613,3617,3631,3643,3673,3677,\\
&\qquad 3697,3701,3721,3739,3761,3847,3851;\\
t_2(2,q) &< 5\sqrt{q}-21 \text{ for } q \le 3767,\ q = 3779,3797,3803,3821,3823,3833,3847,3851,3853,\\
&\qquad 3877,3917,3919,3923,3947,4021,4027,4153;\\
t_2(2,q) &< 5\sqrt{q}-20 \text{ for } q \le 4079,\ q = 4096,4099,4127,4129,4153,4159,4177,4201,4229,\\
&\qquad 4253,4273,4363,4423;\\
t_2(2,q) &< 5\sqrt{q}-19 \text{ for } q \le 4297,\ q = 4337,4339,4357,4363,4391,4409,4423,4447,4463,\\
&\qquad 4481,4489,4517;\\
t_2(2,q) &< 5\sqrt{q}-16 \text{ for } q \le 5023,\ q = 5041,5051,5059,5077,5081,5099,5101,5107,5113,\\
&\qquad 5119,5153,5189,5333;\\
t_2(2,q) &< 5\sqrt{q}-14 \text{ for } q \le 5501,\ q = 5507,5519,5521,5527,5557,5569,5573,5581,5591,\\
&\qquad 5689,5693,5711,5717,5749,5783,5813;\\
t_2(2,q) &< 5\sqrt{q}-12 \text{ for } q \le 5881,\ q = 5903,5923,5927,5939,5953,5987,6007,6029,6053,\\
&\qquad 6073,6089,6143,6151,6163.
\end{aligned}
$$

5.3 Observations on $\bar{t}_2(2,q)$ values

We look for upper estimates of the collection of $\bar{t}_2(2,q)$ values from Tables 1-5 in the form (5.1), see [111], [98, Tab. 2.6], and [11, Sec. 4]. For definiteness, we use the natural logarithms. Let c be a constant independent of q. We introduce $D_q(c)$ and $\overline{D}_q(c)$ as follows:

$$
\begin{aligned}
t_2(2,q) &= D_q(c)\sqrt{q}\ln^c q,\\
\bar{t}_2(2,q) &= \overline{D}_q(c)\sqrt{q}\ln^c q. \qquad (5.13)
\end{aligned}
$$

Let $\overline{D}_{\text{aver}}(c,q_0)$ be the average value of $\overline{D}_q(c)$ calculated in the region $q_0 \le q \le 9109$ under condition $q \notin N$.

From Tables 1-5, we obtain Observation 1.

Observation 1. *Let* $173 \le q \le 9109$ *under condition* $q \notin N$. *Then when* q *grows, the values of* $\overline{D}_q(0.75)$ *oscillate about the average value* $\overline{D}_{\rm aver}(0.75, 173) = 0.95579$. *Also,*

$$\begin{array}{ll} 0.946 < \overline{D}_q(0.75) < 0.9634 & \text{if } 173 \le q < 1000, \\ 0.953 < \overline{D}_q(0.75) < 0.9605 & \text{if } 1000 < q < 2000, \\ 0.950 < \overline{D}_q(0.75) < 0.9595 & \text{if } 2000 < q < 3000, \\ 0.950 < \overline{D}_q(0.75) < 0.9588 & \text{if } 3000 < q < 4000, \\ 0.951 < \overline{D}_q(0.75) < 0.9584 & \text{if } 4000 < q < 5000, \\ 0.950 < \overline{D}_q(0.75) < 0.9579 & \text{if } 5000 < q < 6000, \\ 0.951 < \overline{D}_q(0.75) < 0.9577 & \text{if } 6000 < q < 7000, \\ 0.947 < \overline{D}_q(0.75) < 0.9573 & \text{if } 7000 < q < 8000, \\ 0.949 < \overline{D}_q(0.75) < 0.9573 & \text{if } 8000 < q. \end{array} \tag{5.14}$$

By Observation 1 it seems that the values of $D_q(0.75)$ and $\overline{D}_q(0.75)$ are sufficiently convenient for estimates of $t_2(2, q)$ and $\bar{t}_2(2, q)$.

From Tables 1-5, we obtain Theorem 5.8.

Theorem 5.8. *In* $PG(2, q)$,

$$t_2(2, q) < 0.9987\sqrt{q}\ln^{0.75} q \quad \textit{for } 23 \le q \le 9109,\ q \in T_3. \tag{5.15}$$

We denote

$$\widehat{t}_2(2, q) = \overline{D}_{\rm aver}(0.75, 173)\sqrt{q}\ln^{0.75} q, \quad \overline{\Delta}_q = \bar{t}_2(2, q) - \widehat{t}_2(2, q), \quad \overline{P}_q = \frac{100\overline{\Delta}_q}{\bar{t}_2(2, q)}\%. \tag{5.16}$$

One can treat $\widehat{t}_2(2, q)$ as a *predicted* value of $t_2(2, q)$. Then $\overline{\Delta}_q$ is the difference between the smallest known size $\bar{t}_2(2, q)$ of complete arcs and the predicted value. Finally, $\overline{P}_q$ is this difference in percentage terms of the smallest known size.

Observation 2. *Let* $173 \le q \le 9109$, $q \notin N$. *Then*

$$-3.70 < \overline{\Delta}_q < 0.81. \tag{5.17}$$

$$
\begin{array}{ll}
-0.94\% < \overline{P}_q < 0.79\% & \text{if } 173 \le q < 1000, \\
-0.28\% < \overline{P}_q < 0.49\% & \text{if } 1000 < q < 2000, \\
-0.52\% < \overline{P}_q < 0.38\% & \text{if } 2000 < q < 3000, \\
-0.57\% < \overline{P}_q < 0.32\% & \text{if } 3000 < q < 4000, \\
-0.48\% < \overline{P}_q < 0.27\% & \text{if } 4000 < q < 5000, \\
-0.59\% < \overline{P}_q < 0.22\% & \text{if } 5000 < q < 6000, \\
-0.46\% < \overline{P}_q < 0.20\% & \text{if } 6000 < q < 7000, \\
-0.88\% < \overline{P}_q < 0.16\% & \text{if } 7000 < q < 8000, \\
-0.66\% < \overline{P}_q < 0.16\% & \text{if } 8000 < q.
\end{array} \tag{5.18}
$$

By (5.17) and (5.18) the upper bounds of $\overline{\Delta}_q$ and $\overline{P}_q$ are relatively small. Moreover, the upper bound of $\overline{P}_q$ decreases when q grows. Therefore the values of $\overline{\Delta}_q$ and $\overline{P}_q$ are useful for computer search of small arcs.

The relations (5.14)–(5.18), Theorems 5.4 and 5.8 are the foundation for Conjecture 5.1.

Remark 5.9. *By above, $\sqrt{q}\ln^{0.75} q$ seems to be a reasonable upper bound on the current collection of $\bar{t}_2(2,q)$ values. It gives some reference points for computer search and foundations for Conjecture 5.1 on the upper bound for $t_2(2,q)$. In principle, the constant $c = 0.75$ can be sightly reduced to move the curve $\sqrt{q}\ln^c q$ near to the curve of $\bar{t}_2(2,q)$, see [11, Th. 4.3].*

5.4 Some geometrical constructions of arcs in $PG(2,q)$

In this section some constructions of arcs in $PG(2,q)$ having great intersection size with conics are presented.

In the homogenous coordinates of a point (x_0, x_1, x_2) we put $x_0 \in \{0,1\}$, $x_1, x_2 \in F_q$. Let $F_q^* = F_q \backslash \{0\}$. Let ξ be a primitive element of F_q. Remind that *indexes of powers of ξ are calculated modulo $q-1$.*

5.4.1 Arcs with two points on a tangent to a conic

Throughout this section we use the conic $\mathcal{C}$ of equation $x_1^2 = x_0x_2$. We denote points of $\mathcal{C}$ as follows:

$$A_i = (1, i, i^2),\ i \in F_q; \quad \overline{A}_d = (1, \xi^d, \xi^{2d}),\ d \in \{0, 1, \ldots, q-2\}; \quad A_\infty = (0, 0, 1).$$

Through this subsection, $q \geq 19$ is an *odd prime*. Let H be an integer in the region

$$\left\lfloor \frac{q-1}{3} \right\rfloor \leq H \leq \frac{q-1}{2}. \tag{5.19}$$

We denote by $\mathcal{V}_H$ the following $(H+1)$-subset of the conic $\mathcal{C}$:

$$\mathcal{V}_H = \{A_i : i = 0, 1, 2, \ldots, H\} \subset \mathcal{C}. \tag{5.20}$$

We denote the points of $PG(2, q)$:

$$P = (0, 1, 0),\ T_H = (0, 1, b_H),\ b_H = \begin{cases} 2H+1 & \text{if } H = \left\lfloor \frac{1}{3}(q-1) \right\rfloor \\ 2H & \text{if } \left\lfloor \frac{1}{3}(q-1) \right\rfloor < H \leq \frac{1}{2}(q-1) \end{cases}. \tag{5.21}$$

Let ℓ_0 be the line of equation $x_0 = 0$. It is the *tangent* to $\mathcal{C}$ at A_∞. It holds that $\{P, T_H\} \subset \ell_0$.

Construction A

Let q be an *odd prime*. Let H, $\mathcal{V}_H$, P and T_H be given by (5.19)–(5.21). We construct a point $(H+3)$-set $\mathcal{K}_H$ in the plane $PG(2, q)$ as follows:

$$\mathcal{K}_H = \mathcal{V}_H \cup \{P, T_H\}.$$

The following lemma can be proven by elementary calculations.

Lemma 5.10. (i) *Let $i \neq j$. A point $(0, 1, b)$ is collinear with the points A_i, A_j if and only if*

$$b = i + j. \tag{5.22}$$

(ii) *Let $i \neq j$, $a, b \in F_q$, $b \neq a^2$. Then a point $(1, a, b)$ is collinear with A_i, A_j if and only if $b = a(i+j) - ij$.*

(iii) *Let $a \in F_q$, $a \neq i$. Then a point $(1, a, i^2)$ is collinear with P, A_i.*

Theorem 5.11. *The $(H+3)$-set $\mathcal{K}_H$ of Construction A is an arc in $PG(2, q)$.*

Proof. By (5.19),(5.20), the sum $i + j$ in (5.22) is running on $\{1, 2, \ldots, 2H-1\}$ where $2H - 1 \leq q - 2$ if $\left\lfloor \frac{1}{3}(q-1) \right\rfloor < H$ and $2H - 1 < \frac{2}{3}(q-1)$ if $H = \left\lfloor \frac{1}{3}(q-1) \right\rfloor$. So, $\{0, b_H\} \cap \{1, 2, \ldots, 2H-1\} = \emptyset$, see (5.21). Therefore P and T_H do not lie on bisecants of $\mathcal{V}_H$. In other side, any point of $\mathcal{V}_H$ does not lie on the line PT_H as PT_H is a tangent to $\mathcal{C}$ in A_∞. □

Theorem 5.12. *Let H be given by* (5.19). *Then all points of $\ell_0 \cup \mathcal{C} \backslash \mathcal{V}_H$ lie on bisecants of $\mathcal{K}_H$.*

Proof. All points of ℓ_0 are covered as two points P and T_H of this line belong to $\mathcal{K}_H$.

Let $\mathcal{R}$ and $\mathcal{S}$ be sets of integers modulo q, i.e. $\mathcal{R} \cup \mathcal{S} \subset F_q$.

Let $\mathcal{R} = \{-H, -(H-1), \ldots, -1\} = \{q-H, q-(H-1), \ldots, q-1\}$. By Lemma 5.10(i), the points A_j, A_{-j}, P are collinear. Therefore, a point A_j of $\mathcal{C} \backslash \mathcal{V}_H$ with $j \in \mathcal{R}$ lies on the bisecant of $\mathcal{K}_H$ through P and A_{-j} where $-j \in \{H, H-1, \ldots, 1\}$, $A_{-j} \in \mathcal{V}_H$.

Let $\mathcal{S} = \{b_H - H, b_H - (H-1), \ldots, b_H - 1, b_H\}$. By Lemma 5.10(i), a point A_j of $\mathcal{C} \backslash \mathcal{V}_H$ with $j \in \mathcal{S}$ lies on the bisecant $T_H A_{b_H - j}$ where $b_H - j \in \{H, H-1, \ldots, 1, 0\}$, $A_{b_H - j} \in \mathcal{V}_H$.

Let $b_H = 2H + 1$. Then $\mathcal{S} = \{H+1, H+2, \ldots, 2H+1\}$. Also, by (5.21), $H = \left\lfloor \frac{1}{3}(q-1) \right\rfloor$ whence $H = \frac{1}{3}(q - v)$ where $v \in \{1, 2\}$ and $v \equiv q \pmod 3$. Hence, $3H = q - v$, $2H + 1 = q - H - v + 1 \in \{q - H, q - H - 1\}$.

Let $b_H = 2H$. Then $\mathcal{S} = \{H, H+1, \ldots, 2H\}$. Also, by (5.21), $H > \left\lfloor \frac{1}{3}(q-1) \right\rfloor$ whence $H > \frac{1}{3}(q - v)$ where $v \in \{1, 2\}$ is as above. Therefore $3H > q - v$, $2H > q - H - v$, $2H \geq q - H - v + 1 \in \{q - H, q - H - 1\}$.

We proved that $\{H+1, H+2, \ldots, q-1\} \subseteq \mathcal{S} \cup \mathcal{R}$. Also we showed that the points A_j of $\mathcal{C}\backslash\mathcal{V}_H$ with $j \in \mathcal{S} \cup \mathcal{R}$ are covered by bisecants of $\mathcal{K}_H$ through P (if $j \in \mathcal{R}$) or through T_H (if $j \in \mathcal{S}$). In the other side, $\mathcal{C}\backslash\mathcal{V}_H = \{A_j : j = H+1, H+2, \ldots, q-1\} \cup \{A_\infty\}$ where $A_\infty \in \ell_0$. So, all points of $\mathcal{C}\backslash\mathcal{V}_H$ are covered. □

Definition 5.13. Let q be an *odd prime*. Let $\overline{H}$ be an integer and let

$$\mathcal{P}_{\overline{H}} = \{P\} \cup \{A_i : i = 0, 1, 2, \ldots, \overline{H}\}.$$

We call *critical value of* $\overline{H}$ and denote by $\overline{H}_q$ the *smallest* value of $\overline{H}$ such that all points of the form $(1, a, b)$, $a, b \in F_q$, $b \neq a^2$, lie on bisecants of $\mathcal{P}_{\overline{H}}$.

Theorem 5.14. *Let* $q \geq 19$ *be an* odd prime. *Let* $\overline{H}_q \leq \frac{1}{2}(q-1)$ *and let*

$$\max\{\overline{H}_q, \left\lfloor \frac{q-1}{3} \right\rfloor\} \leq H \leq \frac{q-1}{2}.$$

Then the arc $\mathcal{K}_H$ *of Construction A is complete.*

Proof. We use Theorem 5.12 and Definition 5.13. □

In this subsection, we put $q \geq 19$ as we checked by computer that $\frac{1}{2}(q-1) < \overline{H}_q$ if $q \leq 17$.

Corollary 5.15. *Let* $q \geq 19$ *be an* odd prime. *Let* $\overline{H}_q \leq \frac{1}{2}(q-1)$. *Then Construction A forms a family of complete* k*-arcs in* $PG(2, q)$ *containing arcs of all sizes* k *in the region*

$$\max\{\overline{H}_q, \left\lfloor \frac{q-1}{3} \right\rfloor\} + 3 \leq k \leq \frac{q+5}{2}.$$

If $\overline{H}_q \leq \left\lfloor \frac{1}{3}(q-1) \right\rfloor$ *then cardinality of this family is equal to* $\left\lceil \frac{1}{6}(q+5) \right\rceil$ *and size of the smallest complete arc of the family is* $\left\lfloor \frac{1}{3}(q+8) \right\rfloor$.

By computer search using Lemma 5.10(ii),(iii) we obtained the following theorem.

Theorem 5.16. *Let $q \geq 19$ be an* odd prime. *Let $\overline{H}_q$ be given by Definition* 5.13. *We introduce D_q and Δ_q as follows: $\overline{H}_q = D_q\sqrt{q}\ln^{0.9} q$, $\Delta_q = \left\lfloor \frac{1}{3}(q-1) \right\rfloor - \overline{H}_q$. Then the following holds.*

$$\text{(i)} \quad \left\lfloor \frac{q-1}{3} \right\rfloor < \overline{H}_q \leq \frac{q-1}{2} \text{ if } 19 \leq q \leq 71 \text{ and } q = 79, 83, 89, 107.$$

$$\text{(ii)} \quad \overline{H}_q \leq \left\lfloor \frac{q-1}{3} \right\rfloor \text{ if } 109 \leq q \leq 1367,\ 2003 \leq q \leq 2063,\ q = 73, 97, 101, 103.$$

$$\text{(iii)} \quad \overline{H}_q < 0.98\sqrt{q}\ln^{0.9} q \quad \text{if } 19 \leq q \leq 1367,\ 2003 \leq q \leq 2063. \tag{5.23}$$

$$\text{(iv)} \quad \begin{array}{lll} 0 \leq \Delta_q \leq 99, & 0.74 < D_q < 0.98, & \text{if } 109 \leq q \leq 599; \\ 89 \leq \Delta_q \leq 198, & 0.75 < D_q < 0.94, & \text{if } 601 \leq q \leq 1049; \\ 187 \leq \Delta_q \leq 288, & 0.72 < D_q < 0.95, & \text{if } 1051 \leq q \leq 1367; \\ 417 \leq \Delta_q \leq 464, & 0.78 < D_q < 0.91, & \text{if } 2003 \leq q \leq 2063. \end{array}$$

For situations $\left\lfloor \frac{1}{3}(q-1) \right\rfloor < \overline{H}_q$, the values of $\overline{H}_q$ are given in Table 6.

Table 6
The values $\overline{H}_q, \overline{G}_q, \overline{J}_q$ for cases $\overline{H}_q, \overline{G}_q > \left\lfloor \frac{1}{3}(q-1) \right\rfloor, \overline{J}_q > \frac{1}{4}(q-3)$

q	$\overline{H}_q$	$\overline{G}_q$	$\overline{J}_q$	q	$\overline{H}_q$	$\overline{G}_q$	$\overline{J}_q$	q	$\overline{H}_q$	$\overline{G}_q$	$\overline{J}_q$	q	$\overline{H}_q$	$\overline{G}_q$	$\overline{J}_q$	q	$\overline{J}_q$
19	9			43	19		16	71	24		25	103			34	167	42
23	11			47	18		18	73		27		107	36		30	179	62
27			12	49		18		79	29		27	125		43		191	49
29	13			53	20	19		81		29		127			39	211	54
31	14		14	59	23		24	83	29		29	131			38	223	60
32		15		61	22	22		89	32			139			38	343	86
37	16	16		64		24		97		33		151			42		
41	16	19		67	24		23	101		35		163			41		

Theorem 5.17. *Let q be an* odd prime *with $109 \leq q \leq 1367$, $2003 \leq q \leq 2063$, or $q = 73, 97, 101, 103$. Then Construction A forms a family of complete k-arcs in $PG(2, q)$ containing arcs of all sizes k in the region*

$$\left\lfloor \frac{q+8}{3} \right\rfloor \leq k \leq \frac{q+5}{2}.$$

Proof. We use Corollary 5.15 and Theorem 5.16(ii). □

5.4.2 Arcs with two points on a bisecant of a conic

Throughout this subsection, $q \geq 32$ is a *prime power*. Let G be an integer in the region

$$\left\lfloor \frac{q-1}{3} \right\rfloor \leq G \leq \left\lceil \frac{q-3}{2} \right\rceil. \tag{5.24}$$

We denote by $\mathcal{D}_G$ the following $(G+1)$-subset of the conic $\mathcal{C}$:

$$\mathcal{D}_G = \{\overline{A}_d : d = 0, 1, 2, \ldots, G\} \subset \mathcal{C}. \tag{5.25}$$

Clearly, $A_0 \notin \mathcal{D}_G$. Let

$$\gamma \in F_q,\ \gamma = \begin{cases} -1 = \xi^{(q-1)/2} & \text{for } q \text{ odd} \\ 1 & \text{for } q \text{ even} \end{cases}. \tag{5.26}$$

We denote the points of $PG(2,q)$:

$$Z = (1, 0, \gamma\xi^0),\ B_G = (1, 0, \gamma\xi^{\beta_G}),\ \beta_G = 2G. \tag{5.27}$$

Let ℓ_1 be the line of equation $x_1 = 0$. It is the *bisecant* $A_\infty A_0$ of $\mathcal{C}$. We have $\{Z, B_G\} \subset \ell_1$.

Using (5.24),(5.26), by elementary calculations we obtained the following lemma.

Lemma 5.18. (i) Let $d \neq t$. *A point* $(0,1,b)$ *is collinear with the points* $\overline{A}_d$, $\overline{A}_t$ *if and only if*

$$b = \xi^d + \xi^t. \tag{5.28}$$

(ii) *A point* $(0,1,b)$ *is collinear with the points* $\overline{A}_d$ *and* $(1,0,\gamma U)$ *if and only if*

$$b = \frac{\xi^{2d} + U}{\xi^d}. \tag{5.29}$$

Corollary 5.19. (i) *For all q, the point $P = (0, 1, 0)$ does not lie on any bisecant of $\mathcal{D}_G$.*

(ii) *Let q be even. Then the points $P, Z, \overline{A}_d$ are collinear if and only if $d = 0$. Also, the points $P, B_G, \overline{A}_d$ are collinear if and only if $d = G$.*

(iii) *Let $q \equiv 1 \pmod 4$. Then the points $P, Z, \overline{A}_d$ are collinear if and only if $d \in \{\frac{1}{4}(q-1), \frac{3}{4}(q-1)\}$. Also, the points $P, B_G, \overline{A}_d$ are collinear if and only if $d \in \{G + \frac{1}{4}(q-1),\ G - \frac{1}{4}(q-1)\}$.*

(iv) *Let $q \equiv 3 \pmod 4$. Then the points $P, Z, \overline{A}_d$ and $P, B_G, \overline{A}_d$ are not collinear for any d.*

Proof. (i) In (5.28), the case $b = 0$ implies $\xi^d + \xi^t = 0$. For even q, it is impossible. For odd q, we obtain $\xi^d = -\xi^t$ whence, by (5.26), $d = t + (q-1)/2$. By (5.24), it is impossible.

(ii)-(iv) In (5.29), the case $b = 0$ implies $\xi^{2d} + U = 0$ whence $\xi^{2d} + 1 = 0$ if $(1, 0, \gamma U) = Z$ and $\xi^{2d} + \xi^{\beta_G} = 0$ if $(1, 0, \gamma U) = B_G$. Remind that $\beta_G = 2G$ and $d \le q - 2$.

(ii) Here q is even but $q - 1$ is odd. For $(1, 0, \gamma U) = Z$, we have $\xi^{2d} = 1$ whence $d = 0$. For $(1, 0, \gamma U) = B_G$, it holds that $\xi^{2d} = \xi^{\beta_G}$ whence $2d \equiv 2G \pmod{q-1}$. So, $d = G$.

(iii) Here both $q - 1$ and $\frac{1}{2}(q-1)$ are even. If $(1, 0, \gamma U) = Z$ then $\xi^{2d} = -1 = \xi^{(q-1)/2}$ whence $2d \equiv \frac{1}{2}(q-1) \pmod{q-1}$. It is possible if $d = \frac{1}{4}(q-1)$ or $d = \frac{3}{4}(q-1)$. If $(1, 0, \gamma U) = B_G$ then, by (5.26), $\xi^{2d} = -\xi^{\beta_G} = \xi^{\beta_G + (q-1)/2}$ whence $2d \equiv 2G + (q-1)/2 \pmod{q-1}$. So, $d = G + \frac{1}{4}(q-1)$ or $d = G - \frac{1}{4}(q-1)$.

(iv) Here $q - 1$ is even whereas $\frac{1}{2}(q-1)$ is odd. If $(1, 0, \gamma U) = Z$ then $\xi^{2d} = -1 = \xi^{(q-1)/2}$ whence $2d \equiv \frac{1}{2}(q-1) \pmod{q-1}$. It is impossible. For $(1, 0, \gamma U) = B_G$, it holds that $\xi^{2d} = -\xi^{\beta_G} = \xi^{2G + (q-1)/2}$ that is impossible. □

Construction B

Let q be a *prime power.* Assume that $q \not\equiv 3 \pmod 4$. Let G, $\mathcal{D}_G$, Z, and B_G be given by (5.24)–(5.27). We construct a point $(G+3)$-set $\mathcal{W}_G$ in $PG(2,q)$ as follows:

$$\mathcal{W}_G = \mathcal{D}_G \cup \{Z, B_G\}.$$

From Lemma 5.10 it follows.

Lemma 5.20. *Let $d \neq t$. A point $(1,0,\gamma\xi^\beta)$ is collinear with $\overline{A}_d$, $\overline{A}_t$ if and only if*

$$\beta = d + t. \tag{5.30}$$

Theorem 5.21. *The $(G+3)$-set $\mathcal{W}_G$ of Construction B is an arc.*

Proof. By (5.24),(5.25), the sum $d+t$ in (5.30) is running on $\{1,2,\ldots,2G-1\}$ where $2G-1 \le q-3$. So, $\{0,\beta_G\} \cap \{1,2,\ldots,2G-1\} = \emptyset$, see (5.27). Therefore Z and B_G do not lie on bisecants of $\mathcal{D}_G$. In other side, any point of $\mathcal{D}_G$ does not lie on the line ZB_G as ZB_G is the bisecant of $\mathcal{C}$ through A_∞ and A_0 where $\{A_\infty, A_0\} \cap \mathcal{D}_G = \emptyset$. □

Theorem 5.22. *Let q be a* prime power. *Assume that $q \not\equiv 3 \pmod 4$. Let G be given by* (5.24). *Then all points of $\{P\} \cup \ell_1 \cup \mathcal{C} \setminus \mathcal{D}_G$ lie on bisecants of the arc $\mathcal{W}_G$ of Construction B.*

Proof. By (5.24),(5.25), $\{\overline{A}_0, \overline{A}_{(q-1)/4}\} \subset \mathcal{D}_G$. So, the point P is covered by Corollary 5.19(ii),(iii).

All points of ℓ_1 are covered as two points Z and B_G of this line belong to $\mathcal{W}_G$.

Throughout this proof, $\mathcal{R}$ and $\mathcal{S}$ are sets of integers modulo $q-1$. It can be said that $\mathcal{R}$ and $\mathcal{S}$ are sets of indexes of powers of ξ.

Let $\mathcal{R} = \{-G, -(G-1), \ldots, -1\} = \{q-1-G, q-1-(G-1), \ldots, q-2\}$. By Lemma 5.20, the

points $\overline{A}_t, \overline{A}_{-t}, Z$ are collinear. Therefore, a point $\overline{A}_t$ of $\mathcal{C} \setminus \mathcal{D}_G$ with $t \in \mathcal{R}$ lies on the bisecant of $\mathcal{W}_G$ through $\overline{A}_{-t}$ and Z where $-t \in \{G, G-1, \ldots, 1\}$, $\overline{A}_{-t} \in \mathcal{D}_G$.

Let $\mathcal{S} = \{\beta_G - G, \beta_G - (G-1), \ldots, \beta_G - 1, \beta_G\}$. By Lemma 5.20, a point $\overline{A}_t$ of $\mathcal{C} \setminus \mathcal{D}_G$ with $t \in \mathcal{S}$ lies on the bisecant $B_G\overline{A}_{\beta_G - t}$ where $\beta_G - t \in \{G, G-1, G-2, \ldots, 1, 0\}$, $\overline{A}_{\beta_G - t} \in \mathcal{D}_G$.

As $\beta_G = 2G$, we have $\mathcal{S} = \{G, G+1, \ldots, 2G\}$. Also, $G \geq \left\lfloor \frac{1}{3}(q-1) \right\rfloor$. If $3|(q-1)$ then $G \geq \frac{1}{3}(q-1)$ whence $2G \geq q - G - 1$. If $3 \nmid (q-1)$ then $G \geq \frac{1}{3}(q-2)$ whence $2G \geq q - G - 2$.

We proved that $\{G+1, G+2, \ldots, q-2\} \subseteq \mathcal{S} \cup \mathcal{R}$. Also we showed that the points $\overline{A}_t$ of $\mathcal{C} \setminus \mathcal{D}_G$ with $t \in \mathcal{S} \cup \mathcal{R}$ are covered by bisecants of $\mathcal{W}_G$ either through Z (if $t \in \mathcal{R}$) or through B_G (if $t \in \mathcal{S}$). In the other side, $\mathcal{C} \setminus \mathcal{D}_G = \{\overline{A}_t : t = G+1, G+2, \ldots, q-2\} \cup \{A_\infty, A_0\}$ where $\{A_\infty, A_0\} \subset \ell_1$. So, all points of $\mathcal{C} \setminus \mathcal{D}_G$ are covered. □

Definition 5.23. Let q be a *prime power.* Let $q \not\equiv 3 \pmod 4$. For integer $\overline{G}$, let

$$\mathcal{Z}_{\overline{G}} = \{Z\} \cup \{\overline{A}_d : d = 0, 1, 2, \ldots, \overline{G}\}.$$

We call *critical value of* $\overline{G}$ and denote by $\overline{G}_q$ the *smallest* value of $\overline{G}$ such that all points $(1, a, b)$ with $a \in F_q^*, b \in F_q, b \neq a^2$, and all points $(0, 1, b)$ with $b \in F_q^*$, lie on bisecants of $\mathcal{Z}_{\overline{G}}$.

Theorem 5.24. *Let* $q \geq 32$ *be a* prime power. *Let* $q \not\equiv 3 \pmod 4$. *If* $\overline{G}_q \leq \left\lceil \frac{1}{2}(q-3) \right\rceil$ *and*

$$\max\{\overline{G}_q, \left\lfloor \frac{q-1}{3} \right\rfloor\} \leq G \leq \left\lceil \frac{q-3}{2} \right\rceil,$$

then the arc $\mathcal{W}_G$ *of Construction B is complete.*

Proof. We use Theorem 5.22 and Definition 5.23. □

In this subsection, we put $q \geq 32$ as we checked by computer that $\left\lceil \frac{1}{2}(q-3) \right\rceil < \overline{G}_q$ if $q \leq 29$.

Corollary 5.25. *Let $q \not\equiv 3 \pmod 4$ be a* prime power. *If $\overline{G}_q \le \left\lceil \frac{1}{2}(q-3) \right\rceil$ then Construction B forms a family of complete k-arcs in $PG(2,q)$ containing arcs of all sizes k in the region*

$$\max\{\overline{G}_q, \left\lfloor \frac{q-1}{3} \right\rfloor\} + 3 \le k \le \left\lceil \frac{q-3}{2} \right\rceil + 3 = \begin{cases} \frac{1}{2}(q+3) & \text{if } q \text{ odd} \\ \frac{1}{2}(q+4) & \text{if } q \text{ even} \end{cases}.$$

If $\overline{G}_q \le \left\lfloor \frac{1}{3}(q-1) \right\rfloor$ then size of the smallest complete arc of the family is $\left\lfloor \frac{1}{3}(q+8) \right\rfloor$.

By computer search using Lemmas 5.10, 5.18, 5.20 we obtained the following theorem.

Theorem 5.26. *Let $q \not\equiv 3 \pmod 4$ be a* prime power. *Let $\overline{G}_q$ be given by Definition* 5.23. *We introduce d_q and δ_q as follows: $\overline{G}_q = d_q \sqrt{q} \ln^{0.95} q$, $\delta_q = \left\lfloor \frac{1}{3}(q-1) \right\rfloor - \overline{G}_q$. Then the following holds.*

(i) $\left\lfloor \frac{q-1}{3} \right\rfloor < \overline{G}_q \le \left\lceil \frac{q-3}{2} \right\rceil$ *if* $32 \le q \le 81$ *and* $q = 97, 101, 125$.

(ii) $\overline{G}_q \le \left\lfloor \frac{q-1}{3} \right\rfloor$, *if* $128 \le q \le 1367$, $2003 \le q \le 2063$, $q = 89, 109, 113, 121$.

(iii) $\overline{G}_q < 0.92 \sqrt{q} \ln^{0.95} q$ *if* $32 \le q \le 1367$, $2003 \le q \le 2063$. (5.31)

(iv)
$$\begin{array}{lll} 1 \le \delta_q \le 93, & 0.66 < d_q < 0.89, & \text{if } 128 \le q \le 593; \\ 89 \le \delta_q \le 196, & 0.71 < d_q < 0.92, & \text{if } 601 \le q \le 1049; \\ 183 \le \delta_q \le 267, & 0.68 < d_q < 0.88, & \text{if } 1061 \le q \le 1361; \\ 401 \le \delta_q \le 464, & 0.70 < d_q < 0.88, & \text{if } 2003 \le q \le 2063. \end{array}$$

For situations $\left\lfloor \frac{1}{3}(q-1) \right\rfloor < \overline{G}_q$, the values of $\overline{G}_q$ are given in Table 6.

Theorem 5.27. *Let $q \not\equiv 3 \pmod 4$ be a* prime power. *Let $128 \le q \le 1367$, $2003 \le q \le 2063$, or $q = 89, 109, 113, 121$. Then Construction B forms a family of complete k-arcs in $PG(2,q)$ containing arcs of all sizes k in the region*

$$\left\lfloor \frac{q+8}{3} \right\rfloor \le k \le \begin{cases} \frac{1}{2}(q+3) & \text{if } q \text{ odd} \\ \frac{1}{2}(q+4) & \text{if } q \text{ even} \end{cases}.$$

Proof. We use Corollary 5.25 and Theorem 5.26(ii). □

5.4.3 Arcs with three points outside a conic

Throughout this subsection, $q \geq 27$ is a *prime power* and also $q \equiv 3 \pmod 4$.

Let J be an integer in the region

$$\frac{q-3}{4} \leq J \leq \frac{q-3}{2}. \tag{5.32}$$

Notations $\mathcal{D}_J$, B_J, and β_J are taken from (5.25) and (5.27) with substitution G by J. Using (5.32), it is easy to see that Corollary 5.19(i),(iv), Theorem 5.21 and their proofs hold for $\mathcal{D}_J$, B_J, and β_J as well as for $\mathcal{D}_G, B_G$, and β_G.

Construction C

Let $q \equiv 3 \pmod 4$ be a *prime power.*. Let P, J, $\mathcal{D}_J$, Z, and B_J be given by (5.21),(5.32),(5.25), and (5.27). We construct a point $(J+4)$-set $\mathcal{E}_J$ in $PG(2,q)$ as follows:

$$\mathcal{E}_J = \mathcal{D}_J \cup \{P, Z, B_J\}.$$

Theorem 5.28. *The $(J+4)$-set $\mathcal{E}_J$ of Construction C is an arc.*

Proof. The set $\mathcal{D}_J \cup \{Z, B_J\}$ is an arc due to Theorem 5.21. By Corollary 5.19(i),(iv), the point P does not lie on bisecants of $\mathcal{D}_J$ and $\mathcal{D}_J \cup \{Z, B_J\}$. Finally, P, Z, B_J are not collinear. □

Theorem 5.29. *Let $q \equiv 3 \pmod 4$ be a* prime power. *Let J be given by* (5.32). *Then all points of $\ell_1 \cup \mathcal{C} \setminus \mathcal{D}_J$ lie on bisecants of the arc $\mathcal{E}_J$ of Construction C.*

Proof. All points of ℓ_1 are covered as two points Z and B_J of this line belong to $\mathcal{E}_J$.

Throughout this proof, $\mathcal{R}, \mathcal{S}$, and $\mathcal{T}$ are sets of integers modulo $q-1$. It can be said that $\mathcal{R}, \mathcal{S}$, and $\mathcal{T}$ are sets of indexes of powers of ξ. We act similarly to the proof of Theorem 5.22.

Let $\mathcal{R} = \{-J, -(J-1), \ldots, -1\} = \{q-1-J, q-1-(J-1), \ldots, q-2\}$. By Lemma 5.20, a point $\overline{A}_t$ of $\mathcal{C} \setminus \mathcal{D}_J$ with $t \in \mathcal{R}$ lies on the bisecant of $\mathcal{E}_J$ through $\overline{A}_{-t}$ and Z where $-t \in \{J, J-1, \ldots, 1\}$, $\overline{A}_{-t} \in \mathcal{D}_J$.

Let $\mathcal{S} = \{\beta_J - J, \beta_J - (J-1), \ldots, \beta_J - 1, \beta_J\}$. By Lemma 5.20, a point $\overline{A}_t$ of $\mathcal{C} \setminus \mathcal{D}_J$ with $t \in \mathcal{S}$ lies on the bisecant $B_J\overline{A}_{\beta_J - t}$ where $\beta_J - t \in \{J, J-1, J-2, \ldots, 1, 0\}$, $\overline{A}_{\beta_J - t} \in \mathcal{D}_J$.

Let $\mathcal{T} = \{\frac{1}{2}(q-1), \frac{1}{2}(q-1)+1, \ldots, \frac{1}{2}(q-1)+J\}$. By (5.26),(5.28), the points $P, \overline{A}_t$, and $\overline{A}_{t+(q-1)/2}$ are collinear. Therefore, a point $\overline{A}_t$ of $\mathcal{C} \setminus \mathcal{D}_J$ with $t \in \mathcal{T}$ lies on the bisecant $P\overline{A}_{t+(q-1)/2}$ where $t + \frac{1}{2}(q-1) \in \{q-1, q, \ldots, q-1+J\} = \{0, 1, \ldots, J\}$, $\overline{A}_{t+(q-1)/2} \in \mathcal{D}_J$.

As $\beta_J = 2J$, we have $\mathcal{S} = \{J, J+1, \ldots, 2J\}$ where $2J \geq \frac{1}{2}(q-1) - 1$, see (5.32). Also, by (5.32), $\frac{1}{2}(q-1) + J \geq \frac{1}{4}(3q-5)$ while $q - 1 - J \leq \frac{1}{4}(3q-5) + 1$.

We proved that $\{J+1, J+2, \ldots, q-2\} \subseteq \mathcal{S} \cup \mathcal{R} \cup \mathcal{T}$. Also we showed that the points $\overline{A}_t$ of $\mathcal{C} \setminus \mathcal{D}_J$ with $t \in \mathcal{S} \cup \mathcal{R} \cup \mathcal{T}$ are covered by bisecants of $\mathcal{E}_J$ either through Z (if $t \in \mathcal{R}$) or through B_J (if $t \in \mathcal{S}$) or, finally, through P (if $t \in \mathcal{T}$). In the other side, $\mathcal{C} \setminus \mathcal{D}_J = \{\overline{A}_t : t = J+1, J+2, \ldots, q-2\} \cup \{A_\infty, A_0\}$ where $\{A_\infty, A_0\} \subset \ell_1$. So, all points of $\mathcal{C} \setminus \mathcal{D}_J$ are covered. □

Definition 5.30. Let $q \equiv 3 \pmod 4$ be a *prime power*. For integer $\overline{J}$, let

$$\mathcal{Q}_{\overline{J}} = \{P, Z\} \cup \{\overline{A}_d : d = 0, 1, 2, \ldots, \overline{J}\}.$$

We call *critical value of* $\overline{J}$ and denote by $\overline{J}_q$ the *smallest* value of $\overline{J}$ such that all points $(1, a, b)$ with $a \in F_q^*, b \in F_q, b \neq a^2$, and all points $(0, 1, b)$ with $b \in F_q^*$, lie on bisecants of $\mathcal{Q}_{\overline{J}}$.

Theorem 5.31. *Let* $q \geq 27$ *be a* prime power. *Let* $q \equiv 3 \pmod 4$. *If* $\overline{J}_q \leq \frac{1}{2}(q-3)$ *and*

$$\max\{\overline{J}_q, \frac{q-3}{4}\} \leq J \leq \frac{q-3}{2},$$

then the arc $\mathcal{E}_J$ *of Construction C is complete.*

Proof. We use Theorem 5.29 and Definition 5.30. □

In this subsection, we put $q \geq 27$ as we checked by computer that $\frac{1}{2}(q-3) < \overline{J}_q$ if $q \leq 23$.

Corollary 5.32. *Let $q \equiv 3 \pmod 4$ be a* prime power. *If $\overline{J}_q \leq \frac{1}{2}(q-3)$ then Construction C forms a family of complete k-arcs in $PG(2,q)$ containing arcs of all sizes k in the region*

$$\max\{\overline{J}_q, \frac{q-3}{4}\} + 4 \leq k \leq \frac{q+5}{2}.$$

If $\overline{J}_q \leq \frac{1}{4}(q-3)$ then cardinality of this family is equal to $\frac{1}{4}(q-3)$ and size of the smallest complete arc of the family is $\frac{1}{4}(q+13)$.

By computer search using Lemmas 5.10, 5.18, 5.20 we obtained the following theorem.

Theorem 5.33. *Let $q \equiv 3 \pmod 4$ be a* prime power. *Let $\overline{J}_q$ be given by Definition* 5.30. *We introduce r_q and θ_q as follows: $\overline{J}_q = r_q\sqrt{q}\ln^{0.95} q$, $\theta_q = \frac{1}{4}(q-3) - \overline{J}_q$. Then it holds that*

$$\begin{aligned}
&\text{(i)} && \frac{q-3}{4} < \overline{J}_q \leq \frac{q-3}{2} \text{ if } 27 \leq q \leq 191 \text{ and } q = 211, 223, 343;\\
&\text{(ii)} && \overline{J}_q \leq \frac{q-3}{4}, \text{ if } 347 \leq q \leq 1367,\ 2003 \leq q \leq 2063,\\
& && q = 199, 227, 239, 243, 251, 263, 271, 283, 307, 311, 331;\\
&\text{(iii)} && \overline{J}_q < 0.98\sqrt{q}\ln^{0.95} q \text{ if } 27 \leq q \leq 1367,\ 2003 \leq q \leq 2063;\\
&\text{(iv)} && \begin{array}{lll} 3 \leq \theta_q \leq 44, & 0.67 < r_q < 0.86, & \text{if } 347 \leq q \leq 599;\\ 18 \leq \theta_q \leq 111, & 0.67 < r_q < 0.94, & \text{if } 607 \leq q \leq 991;\\ 89 \leq \theta_q \leq 167, & 0.67 < r_q < 0.84, & \text{if } 1019 \leq q \leq 1367;\\ 261 \leq \theta_q \leq 294, & 0.67 < r_q < 0.80, & \text{if } 2003 \leq q \leq 2063. \end{array}
\end{aligned} \tag{5.33}$$

For situations $\frac{1}{4}(q-3) < \overline{J}_q$, the values of $\overline{J}_q$ are given in Table 6.

Theorem 5.34. *Let $q \equiv 3 \pmod 4$ be a* prime power. *Let $347 \leq q \leq 1367$ or $q = 199, 227, 239, 243, 251, 263, 271, 283, 307, 311, 331$. Then Construction C forms a family of complete k-arcs in $PG(2,q)$ containing*

arcs of all sizes k in the region

$$\frac{q+13}{4} \le k \le \frac{q+5}{2}.$$

Proof. We use Corollary 5.32 and Theorem 5.33(ii). □

Basing on Theorems 5.16, 5.26, 5.33 and taking into account that $\sqrt{q}\ln^{0.9} q < \sqrt{q}\ln q$, $\sqrt{q}\ln^{0.95} q < \sqrt{q}\ln q$, we conjecture the following

Conjecture 5.35. Let $\overline{H}_q$, $\overline{G}_q$, $\overline{J}_q$ be given by Definitions *5.13*, *5.23*, *5.30*. Let for $\overline{H}_q$, q be prime while for $\overline{G}_q$ and $\overline{J}_q$ it holds that q is a prime power. Finally, let $q \not\equiv 3 \pmod 4$ for $\overline{G}_q$ and $q \equiv 3 \pmod 4$ for $\overline{J}_q$. Then the following holds.

$$\overline{H}_q \le \left\lfloor \frac{q-1}{3} \right\rfloor \text{ if } q \ge 109;\ \overline{G}_q \le \left\lfloor \frac{q-1}{3} \right\rfloor \text{ if } q \ge 128;\ \overline{J}_q \le \frac{q-3}{4} \text{ if } q \ge 347.$$

$$\overline{H}_q < \sqrt{q}\ln q \text{ if } q \ge 19;\ \overline{G}_q < \sqrt{q}\ln q \text{ if } q \ge 32;\ \overline{J}_q < \sqrt{q}\ln q \text{ if } q \ge 27. \tag{5.34}$$

Remark 5.36. *It is interesting to compare the relations (5.23),(5.31),(5.33),(5.34) with Theorems 5.4, 5.8 and to compare also computer results providing Theorems 5.16, 5.26, 5.33 with Tables 1 and 2. One can see that the upper estimates of $t_2(2,q)$, $\overline{H}_q$, $\overline{G}_q$, and $\overline{J}_q$ have the same structure and the values of $\overline{t}_2(2,q)$, $\overline{H}_q$, $\overline{G}_q$, and $\overline{J}_q$ have a close order. This seems to be natural as* almost all *points of $PG(2,q)$ lie on bisecants of $\mathcal{P}_{\overline{H}_q}$, $\mathcal{Z}_{\overline{G}_q}$, and $\mathcal{Q}_{\overline{J}_q}$, see Definitions 5.13, 5.23 and 5.30.*

Remark 5.37. *The complete arcs of Constructions A, B, C can be used as starting objects in inductive constructions. For example, for even q, arcs of Construction B can be used in constructions of [55, Ths 1.1,3.14-3.17,4.6-4.8]. In that way, one can generate infinite sets of families of complete caps in projective spaces $PG(v,2^n)$ of growing dimensions v. For every v, constructions of [55] can obtain a complete cap from every complete arc of Construction B. Also, it can be shown that in Constructions A, B, C all points not on conic are* external. *So, the arcs of Constructions A and C for $q \equiv 3 \pmod 4$*

can be used as starting objects in constructions of [114], see [114, Th. 23]. Thereby, infinite families of large complete arcs in $PG(2, q^n)$ with growing n can be obtained.

Chapter 6

$(n, 3)$-arcs in projective planes

In the projective plane $PG(2, q)$ over the finite field $GF(q)$ an (n, r)-arc is a set of n points no $(r+1)$ of which are collinear, containing r collinear points. An (n, r) arc is called *complete* if it is not contained in a $(n+1, r)$-arc of the same projective plane. An $(n, 2)$-arc is called n-arc. For a more detailed introduction to (n, r)-arcs and in particular $(n, 3)$ arcs see [95], [130], [132], [41], [133]. The largest size of an (n, r)-arc of $PG(2, q)$ is indicated by $m_r(2, q)$. In particular $m_3(2, q) \leq 2q + 1$ for $q \geq 4$ (see [173]). In [98] bounds for $m_r(2, q)$ and the relationship between the theory of complete (n, r)-arcs, coding theory and mathematical statistics are given.

6.1 $(n, 3)$-arcs containing an arc

The algorithm used in the search for $(n, 3)$-arcs is of type A (see Section 3.1), since $(n, 3)$-arcs possess hereditary features. The problem of finding complete $(n, 3)$-arcs of particular size is divided in different tasks. In fact the following theorem states a lower bounds on the size of the arcs that an $(n, 3)$-arc contains (see [132]).

Theorem 6.1. *An $(n, 3)$-arc $\mathcal{K}$ in $PG(2, q)$, $n \geq \alpha + \binom{\alpha}{2}$, contains an arc of size $\alpha + 1$.*

6.2 The algorithm

The base algorithm used is the same described in [133] and [130]. The algorithm searches for complete 3-arcs containing arcs of fixed size n and, at least at the beginning, not containing arcs of size $n+1$. In particular the search is divided in three steps.

1. All the non-equivalent arcs C_s^i of a certain size s complete and non-complete are generated.

2. The classification process continues until it reaches the level $s+h$ (usually $h = 1, 2, 3$). Given a particular arc C_s^i the candidates considered for the extension at level $r < s+h$ are those points P lying on bisecants of C_s^i and such that $C_r^i \cup \{P\}$ is a 3-arc.

3. When all the non equivalent 3-arcs of size $s+h$ are generated, the leaves are extended to reach the desired length using a backtracking algorithm.

Unfortunately, when looking for $m_3(2, 16)$, the great number of leaves in the tree and levels in the backtracking search make impossible finish the tasks in reasonable time. In particular the cases with more difficulties are those starting from arcs of sizes 9 and 10.

6.3 The improved algorithm

The main improvements to the program use both computational and theoretical instrument.
The first problem of the algorithm described in the previous section is that, searching for complete $(n, 3)$-arcs containing an $(s, 2)$-arc, during the backtracking we cannot avoid that the $(t, 3)$-arcs considered contains an arc of size greater than s. Such a 3-arc should not be considered since it has been examined when starting from $(s', 2)$-arcs, with $s' > s$. In order to avoid the greatest possible number of such 3-arcs the following two ideas are used.

1. Before starting the backtracking algorithm some informations are computed. Let C' be the 3-arc to extend and C be the $(s,2)$-arc contained in C'. The program computes all the pairs (P,Q), with $P,Q \in PG(2,q) \setminus C'$, such that there exists $R \in C$ with $(C \setminus \{R\}) \cup \{P,Q\}$ is a $(s+1,2)$-arc. The program collects all these pairs in a table. This information is used during the backtracking; in fact when adding the point P to the partial solution, all the points Q such that the pair (P,Q) is the table are avoided.

2. The first step described in the previous point does not assure that a 3-arc generated during the backtracking does not contain an $(s+1,2)$-arc. In fact it is possible that there exist $R_1,\ldots,R_\ell \in C$ and $P_1,\ldots,P_{\ell+1} \in PG(2,q) \setminus C'$ such that $(C \setminus \{R_1 \ldots,R_\ell\}) \cup \{P_1,\ldots,P_{\ell+1}\}$ is an $(s+1,2)$-arc. To reduce the number of these cases a random control have been added. In this way it is possible at a certain level of the backtracking to control if the the partial solution contains an arc too big and therefore can be pruned. The problem of using this procedure is that in general this control requires too many calculations: it is possible to set the level on which to perform this control and the percentage of times the procedure must be done. To improve the execution time it is important to set these two parameters in a convenient way. In particular if the control is made too early it is possible that few partial solutions are pruned since the procedure described in the previous point (using the pairs) eliminates lots of *bad* candidates; if the control is made too late, even if some partial solutions are deleted, the backtracking search is almost finished and there is no convenience to make it.

The other ideas used to make the search possible, trying to reduce the time executions of the worse cases, i.e. searching for complete $(n,3)$-arcs of size $29 \leq n \leq 33$ and containing an arc of size 9 or 10, concerns the ordering of the candidates at each step of the backtracking algorithm (see [39]).

At the beginning, when extending an $(s, 2)$-arc, the candidates points for the extension process belong to bisecants of the arc. It is possible to organize all the candidate in the following way.

1. Consider all the k lines ℓ_j containing the m candidates points P_i (each point is present only one time): these lines are a subset of the bisecants of the contained arc.

2. Let α_i be the number of candidates contained in ℓ_i: order the lines ℓ_j according to α_i in descending order, as in the example presented in the following table:

Line	Points contained	α_i	β
ℓ_1	$P_1, \ldots, P_{10}$	10	10
ℓ_2	$P_{11}, \ldots, P_{20}$	10	9
ℓ_3	$P_{21}, \ldots, P_{29}$	9	8
ℓ_4	$P_{30}, \ldots, P_{37}$	8	7
ℓ_5	$P_{38}, \ldots, P_{43}$	6	6
ℓ_6	$P_{44}, \ldots, P_{48}$	5	5
ℓ_7	$P_{49}, \ldots, P_{53}$	5	4
ℓ_8	$P_{54}, \ldots, P_{56}$	3	3
ℓ_9	P_{57}, P_{58}	2	2
ℓ_{10}	P_{59}, P_{60}	2	1
ℓ_{11}	P_{61}, P_{62}	2	0
ℓ_{12}	P_{63}	1	0
ℓ_{13}	P_{64}	1	0
ℓ_{14}	P_{65}	1	0
ℓ_{15}	P_{66}	1	0
ℓ_{16}	P_{67}	1	0
ℓ_{17}	P_{68}	1	0
ℓ_{18}	P_{69}	1	0

3. Suppose now that the number of points to add (i.e. the number of backtracking level) is 11. Note that only one point for each line can be added, since all these lines contain already two points of the 3-arc. The points are ordered according to their row in descending order, and the point P_i can be added to $C' \cup \{P_{j_1}, \ldots, P_{j_l}\}$ only if $i > j_k$ for $k = 1, \ldots, l$. The number β in the previous table gives informations about the points to consider at each level: the first point to add can be chosen only between the points contained in the lines with $\beta < 1$ and in general the j-th points in

the lines with $\beta < j$. For instance, it is not possible to choose as first point P_{57}, since it belongs to the 9-th line and the other 10 points should be chosen only in eight lines, which is impossible.

4. Observe that since the lines with the most points are the last to be added to the candidates, it is possible to avoid a great number of candidates during the backtracking.

6.4 The maximum and the minimum order in $PG(2, 16)$

In our search we have faced the problem of finding the maximum and the minimum size of complete $(n, 3)$-arcs in $PG(2, 16)$. The maximum size of known complete $(n, 3)$-arcs is 28: in [24] a complete $(28, 3)$-arc is obtained as union of orbits of some subgroup of $P\Gamma L(3, 16)$; the same size is equal to the one presented in [31]. Therefore, by Theorem 6.1, it is sufficient to investigate if there exist complete $(n, 3)$-arcs with $29 \leq n \leq 33$, containing at least an 8-arc. Using the ideas explained in the previous sections, we performed an exhaustive search of $(n, 3)$-arcs in $PG(2, 16)$ of size greater than 28 and we found no examples. Then the following theorem holds.

Theorem 6.2. *The maximum size of complete* $(n, 3)$*-arcs in* $PG(2, 16)$ *is* 28.

The classification of complete $(28, 3)$-arcs is in progress.
Moreover we have determined the smallest size of complete $(n, 3)$-arcs.

Theorem 6.3. *The minimum size of complete* $(n, 3)$*-arcs in* $PG(2, 16)$ *is* 15.

Proof. Using ideas described in the previous sections, we performed an exhaustive search of $(n, 3)$-arcs in $PG(2, 16)$ of size less than 15 and we found no examples. We also proved that a complete $(15, 3)$-arc must contain a $(9, 2)$-arc. As a result of a partial search for complete $(15, 3)$-arcs, we have obtained only the example presented in Table 6.1; it contains a $(9, 2)$-arc. □

We denote $GF(16) = \{0, 1 = \alpha^0, 2 = \alpha^1, \ldots, 15 = \alpha^{14}\}$, where α is a primitive element such that $\alpha^4 + \alpha^3 + 1 = 0$. The columns ℓ_i indicate the number of i-secant of the $(n, 3)$-arc and G indicates the description of the stabilizer in $P\Gamma L(3, 16)$ (see [175]).

Table 6.1: $(15, 3)$-arc in $PG(2, 16)$

Points	ℓ_0	ℓ_1	ℓ_2	ℓ_3	G
1 0 0 1 1 1 1 1 1 1 1 1 1 1 1 0 1 0 1 0 1 2 2 4 9 9 11 11 13 13 0 0 1 1 11 8 5 10 10 2 8 2 11 1 12	92	138	12	31	$\mathcal{S}_3$

The execution time of the extension process is exponential respect to the number of points to join to the starting arc. It has been very important for this reason to have the possibility to introduce in algorithm the ideas presented in Section 6.3.

The machines used are 2.4 Ghz Intel Quadcore and Exacore having 8 Gb and 16 Gb of memory respectively. In the search for the minimum order in $PG(2, 16)$ the total execution time to establish the non-extincence of $(14, 3)$-arcs has been about 11 days. Table 6.2 describes the execution regarding the search for $(n, 3)$-arcs, $n \geq 29$, in $PG(2, 16)$.

Table 6.2: Execution Time: search for $(n, 3)$-arcs in $PG(2, 16)$ with $n \geq 29$ containing an arc $\mathcal{A}$

$\lvert\mathcal{A}\rvert$	8	9	10	11	12	13	14	15	16	17
Time	2 d	22 d	20 d	4 d	2 d	1.2 h	15 minutes	3 minutes	$<$ 1 minute	few seconds

6.5 On extremal $(n, 3)$-arcs in $PG(2, 17)$

Using the algorithms described in previous sections, we performed searches in $PG(2, 17)$ in order to find examples of complete $(n, 3)$-arcs of extremal size. The following theorems hold.

Table 6.3: $(18,3)$-arcs in $PG(2,17)$, containing an arc $\mathcal{A}$

$\lvert\mathcal{A}\rvert$	Points	ℓ_0	ℓ_1	ℓ_2	ℓ_3	G
9	1 0 0 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 0 1 1 1 3 3 4 4 9 10 10 12 13 13 14 14 0 0 1 1 2 5 7 13 4 5 13 3 4 0 1 2 2 7	94	144	27	42	$\mathcal{Z}_1$
10	1 0 0 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 0 1 1 1 2 2 3 3 10 10 12 13 15 15 16 16 0 0 1 1 5 8 4 11 7 12 4 7 9 1 0 16 8 16	97	135	36	39	$\mathcal{Z}_1$

Theorem 6.4. *There exist no complete* $(n,3)$*-arcs in* $PG(2,17)$*, with* $n > 28$ *containing an arc of size greater than* 12*.*

Proof. We performed an exhaustive search of $(n,3)$-arcs in $PG(2,17)$ of size greater than 28 containing an s-arc with $s > 12$, and we found no examples. □

Theorem 6.5. *There exist no complete* $(n,3)$*-arcs in* $PG(2,17)$*, with* $n \leq 17$ *containing an arc of size less than* 8*. The smallest size of complete* $(n,3)$*-arcs in* $PG(2,17)$ *is at most* 18*.*

Proof. We performed an exhaustive search of $(n,3)$-arcs in $PG(2,17)$ of size less than 18 containing an s-arc with $s < 8$ and we found no examples. Moreover we have found two examples of complete $(18,3)$-arcs (see [15]), containing a 9 and a 10 arc respectively, presented in Table 6.3. □

In Table 6.3, the columns ℓ_i indicate the number of i-secant of the $(n,3)$-arc and G indicates the description of the stabilizer in $PGL(3,17)$ (see [175]).

6.6 On extremal $(n, 3)$-arcs in $PG(2, 19)$

Using the algorithms described in previous sections, we performed searches in $PG(2, 19)$ in order to find examples of complete $(n, 3)$-arcs of extremal size. The following theorems hold.

Theorem 6.6. *The maximum size of complete* $(n, 3)$*-arcs in* $PG(2, 19)$ *is at least* 31*.*

Proof. We have found four non-equivalent examples of complete $(31, 3)$-arcs (see [15]), containing a 14-arc, presented in Table 6.4. □

Theorem 6.7. *There exist no complete* $(n, 3)$*-arcs in* $PG(2, 19)$*, with* $n \geq 31$ *containing an arc of size greater than* 14*.*

Proof. We performed an exhaustive search of $(n, 3)$-arcs in $PG(2, 19)$ of size greater than or equal to 31 containing an s-arc with $s > 14$ and we found no examples. □

Theorem 6.8. *The smallest size of complete* $(n, 3)$*-arcs in* $PG(2, 19)$ *is at most* 20*.*

Proof. We have found several examples of complete $(20, 3)$-arcs (see [15]); in Table 6.5 we present one example containing a 10-arc. □

In Tables 6.4 and 6.5, the columns ℓ_i indicate the number of i-secant of the $(n, 3)$-arc and G indicates the description of the stabilizer in $PGL(3, 19)$ (see [175]).

Table 6.4: $(31, 3)$-arcs in $PG(2, 19)$, containing a 14-arc

Points	ℓ_0	ℓ_1	ℓ_2	ℓ_3	G
1 0 0 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 0 1 1 0 1 2 2 3 4 4 5 6 6 7 7 8 8 9 10 11 11 12 15 15 16 16 17 17 18 0 0 1 1 14 5 13 5 18 7 6 11 10 3 17 16 17 6 18 12 4 4 8 12 3 8 0 1 2 9 9	101	65	90	125	$\mathcal{Z}_1$
1 0 0 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 0 1 1 0 1 2 2 3 4 4 5 7 7 8 8 9 9 10 11 11 12 13 13 14 15 16 16 18 18 0 0 1 1 14 16 8 5 9 16 7 12 10 14 15 3 18 0 4 6 12 17 3 6 14 7 8 10 17 4 15	96	80	75	130	$\mathcal{Z}_1$
1 0 0 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 0 1 1 0 1 2 2 3 4 4 5 5 6 6 7 8 8 9 10 11 11 12 15 15 16 16 17 17 18 0 0 1 1 14 5 13 5 18 7 6 11 10 16 3 17 16 6 18 12 4 4 8 12 3 8 0 1 2 9 9	100	68	87	126	$\mathcal{Z}_1$
1 0 0 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 0 1 1 2 3 4 4 5 5 6 6 7 7 8 8 9 9 10 10 12 13 13 14 15 15 16 16 18 18 0 0 1 1 13 5 7 6 9 7 10 0 10 6 16 14 18 12 13 1 4 4 12 13 8 8 16 5 15 9 14	92	92	63	134	$\mathcal{Z}_4$

Table 6.5: $(20, 3)$-arcs in $PG(2, 19)$, containing a 10-arc

Points	ℓ_0	ℓ_1	ℓ_2	ℓ_3	G
1 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 0 1 0 1 2 2 3 3 5 5 6 8 8 12 13 15 15 17 0 0 1 1 11 9 2 5 0 8 9 10 2 4 18 11 17 8 10 18	121	170	40	50	$\mathcal{Z}_1$

Chapter 7

The spectrum of complete caps in $PG(3,7)$

7.1 Introduction

In this chapter it has been verified that in $PG(3,7)$ there are no 31-complete caps and that the values $\{17-30, 32, 50\}$ form the spectrum of possible sizes of complete caps. This result has been obtained by a computer-based proof helped by the non existence of some codes. In the projective space $PG(r,q)$ over the Galois Field F_q, an n-cap is a set of n points no three of which are collinear. An n-cap is called complete if it is not contained in an $(n+1)$-cap.

Let an $[n,k,d]_q R$ code be a linear q-ary code of length n, dimension k, minimum distance d, and covering radius R. This code is a k dimension subspace of the space of vectors of length n with components from F_q. The points of a complete n-cap in $PG(r,q)$ can be treated as columns of a parity check matrix of an $[n, n-(r+1), d]_q 2$ linear code of distance $d=4$, with the exceptions of the complete 5-cap in $PG(3,2)$ and the complete 11-cap in $PG(4,3)$ corresponding to the binary $[5,1,5]_2 2$ code and to the Golay $[11,6,5]_3 2$ code respectively.

In this table we can find for each size k of complete caps in $PG(3,7)$ the reference where it is possible to find an example.

Size	17	18	19	20	21	22	23	24	25	26	27	28	29	30	32	50
References	[135],[26]	[131]	[131]		[69][70]		[69]	[131]	[131]	[145]	[131]	[68][139]		[1]	[62]	[5][140]

In particular this theorem establishes the uniqueness of the complete 50-cap.

Theorem 7.1 ([5], [140])**.** *For q odd or $q = 4$ any $(q^2 + 1)$-cap of $PG(3, q)$ is an elliptic quadric.*

In [145] it should be proved that there exist complete caps in $PG(3, 7)$ of sizes 22, 24, 26, but a computer search can easily prove that the constructions of the complete caps of these sizes presented in the chapter are not consistent. In 2000 Östergård ([135]) constructed a complete 17 cap. In 2006 Bierbrauer, Marcugini and Pambianco ([26]) showed that the minimum size of complete caps in $PG(3, 7)$ is 17 and that there exist exactly four projectively inequivalent such caps. In 2000 Pambianco and Ughi ([139]) constructed a complete 28-cap, which belongs to a family of complete $\frac{q^2+7}{2}$-caps with having 2 points on a line external to en elliptic quadric E and the remaining points on E, is constructed. In 2007 Edel, Storme and Sziklai ([62]) showed that $m'_2(3, 7) = 32$. In 2008 Abatangelo and Larato ([1]) presented a complete 30-cap, which belongs to an infinite family of complete $\frac{q^2+q+4}{2}$-caps with $q \equiv 3 \bmod 4$, $q \geq 7$. In Table 2 an example of complete cap is given for each size.

The main result of this chapter is the following theorem, see Section 7.2.

Theorem 7.2. *There exist no complete caps of size* 31 *in $PG(3, 7)$.*

The existence of a complete caps in $PG(3, 7)$ is presented as an open problem in [44].
By Theorem 7.2 and the results contained in [1], [26], [45], [62], [68], [69], [70], [71], [92], [94], [95], [97], [98], [135], [139], [153] it is possible to give the following theorem:

Theorem 7.3. *In $PG(3, 7)$ a complete k-cap exists if and only if $k \in \{17 - 30, 32, 50\}$.*

To determine if there exist in $PG(3,7)$ complete caps of size 31, we start from caps $\mathcal{K}$, complete and incomplete, in $PG(2,7)$ of size 7 and 8, and then we extend them to complete caps in $PG(3,7)$. We consider only caps in $PG(2,7)$ of sizes 7 and 8 because of the non existence of particular linear codes and the following theorem, see [26] and [91, Theorem 4.1]:

Theorem 7.4. *The following are equivalent:*

1. *An $[n,k,d']_q$-code with $d' \geq d$.*
2. *A multiset $\mathcal{M}$ of points of the projective space $PG(k-1,q)$, which has cardinality n and satisfying the following: for every hyperplane $H \subset PG(k-1,q)$ there are at least d points of $\mathcal{M}$ outside H (in the multiset sense).*

Proposition 7.5. *[84] A linear $[31,4]_7$ has minimum distance $d = 24$.*

By Theorem 7.4 and Proposition 7.5, there exists a hyperplane containing at least 7 points of the corresponding 31-caps. Table 1 presents the classification of the complete and incomplete k-caps in $PG(2,7)$ of size $k = 7, 8$.

TABLE 1. Complete classification of non equivalent caps $\mathcal{K}$ in $PG(2,7)$ of sizes 7 and 8

$\lvert\mathcal{K}\rvert$	7	8
# of complete caps $\mathcal{K}$	1	0
# of incomplete caps $\mathcal{K}$	0	1

7.2 Results

Searching for complete caps of size 31, we extend k-caps in $PG(2,7)$ of size $7, 8$. In the extension process no points belonging to the plane containing the starting cap are added and properties of equivalence among arcs are used to prune the search space. The algorithm is described in details in [10] and is of

type A (see Chapter 3). No complete 31-caps have been found, so Theorem 7.2 is proven. The execution time for the extension of all the cases has been about 200 hours. We used a computer with CPU Intel Quad-Core 8 Thread i7 920 and 12 Gb of memory. The extension processes of the caps in $PG(2,7)$ are independent each other, so they could be computed in different processors. In this way we realized a simple but efficient example of data parallelism.

7.3 Complete Caps

In the following tables for each size k of complete caps in $PG(3,7)$ an example is presented.

TABLE 2. Caps $\mathcal{K}$ in $PG(2,7)$

Size	Cap	Reference
17	0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 1 1 1 2 3 3 3 4 4 4 5 6 1 2 4 6 6 1 2 5 2 0 1 5 2 3 4 4 5 6 2 6 0 1 0 0 2 4 3 4 4 0 2 2 5 5	[26]
18	0 0 0 1 1 0 0 0 1 1 1 1 1 1 1 1 1 0 0 1 0 1 1 1 1 0 0 0 1 1 1 6 6 6 6 0 1 0 0 1 1 2 3 1 2 3 0 5 6 0 2 3 4 1 0 0 0 1 2 1 3 2 1 3 2 5 4 1 0 4 3	[131]
19	0 0 0 1 1 0 0 0 1 1 1 1 1 1 1 1 1 1 0 0 1 0 1 1 1 1 0 0 0 1 1 1 2 2 2 5 6 0 1 0 0 1 1 2 3 1 2 3 0 2 5 0 1 6 4 4 1 0 0 0 1 2 1 3 2 1 3 2 3 0 6 5 4 6 1	[131]
20	1 0 1 0 0 1 0 0 1 1 1 0 0 0 1 1 1 1 1 5 1 0 1 0 0 0 1 1 4 5 1 1 1 6 1 1 0 0 3 4 6 0 0 1 2 0 1 1 1 5 5 4 2 1 4 0 3 1 4 3 1 0 0 0 2 1 5 1 5 6 3 2 6 2 4 2 4 3 5	
21	0 1 0 1 4 1 5 6 3 0 5 2 6 3 5 3 2 0 2 0 1 1 1 0 0 0 1 4 0 1 4 0 1 4 5 6 2 3 5 6 3 2 0 0 1 1 0 0 0 1 1 1 2 2 2 3 3 4 4 5 5 6 6 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	[70]
22	0 1 0 0 1 0 0 1 1 1 1 0 0 0 1 1 1 1 1 1 1 1 0 1 0 0 0 1 2 1 2 3 1 1 1 1 1 1 0 0 3 2 4 6 0 0 1 2 0 1 2 1 0 5 5 4 2 0 4 2 3 1 4 5 0 1 0 0 0 2 1 5 5 1 1 1 3 2 6 2 6 3 4 3 5 6 4	

Size	Cap	Reference
23	0 1 4 1 5 6 3 0 5 2 6 1 5 2 1 5 2 5 2 6 6 3 0 1 1 0 1 4 0 1 4 0 1 4 0 1 4 0 1 4 0 1 4 0 1 4 0 0 0 0 0 1 1 1 2 2 2 3 3 3 4 4 4 5 5 5 6 6 6 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	[69]
24	0 0 0 1 1 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0 1 1 1 1 0 0 0 1 1 1 1 1 2 2 3 3 3 4 6 6 0 1 0 0 1 1 2 3 1 2 3 0 2 3 4 5 1 2 1 3 6 5 3 5 1 0 0 0 1 2 1 3 2 1 3 2 3 4 6 5 6 0 5 1 0 0 5 2	[131]
25	0 0 0 1 1 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0 1 1 1 1 0 0 0 1 1 1 1 1 2 2 5 5 5 5 6 6 6 0 1 0 0 1 1 2 3 1 2 3 0 2 3 4 5 1 3 0 1 2 5 1 4 5 1 0 0 0 1 2 1 3 2 1 3 2 3 4 6 5 6 0 6 3 2 4 4 2 3	[131]
26	1 0 0 0 0 0 1 1 0 0 1 1 1 1 1 1 0 1 1 1 1 1 1 1 1 0 1 1 1 1 0 0 1 0 1 1 2 0 2 3 2 1 3 0 3 1 1 3 5 3 2 0 2 0 5 6 1 2 4 0 1 2 3 1 4 5 6 4 2 3 6 0 1 3 6 0 0 0 6 0 3 1 0 2 6 1 5 3 2 3 3 5 6 2 4 4 0 2 1 6 1 3 1	
27	0 0 0 1 1 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0 1 1 1 1 0 0 0 1 1 1 1 2 2 3 3 3 4 4 5 5 5 6 6 0 1 0 0 1 1 2 3 1 2 3 0 2 3 5 2 5 1 2 6 1 6 2 3 5 3 4 1 0 0 0 1 2 1 3 2 1 3 2 3 4 5 6 1 5 4 6 3 4 2 6 4 5 2	[131]
28	1 1 1 1 1 1 0 1 1 1 1 1 1 0 1 1 1 1 1 1 1 1 1 1 1 0 1 1 5 2 4 6 4 2 1 1 1 3 4 0 3 0 0 2 5 1 2 6 0 3 5 6 1 0 0 3 5 0 4 5 6 3 0 1 2 1 5 1 2 0 2 1 4 0 2 4 0 0 6 6 3 1 3 3 1 6 6 3 2 0 0 5 3 2 0 1 0 1 6 3 0 1 1 2 4 5 3 5 2 0 5 6	[68] [139]
29	1 0 0 0 1 1 1 1 1 1 1 1 1 0 1 1 1 1 1 1 0 0 1 1 1 1 0 1 0 0 1 0 0 4 1 1 1 3 0 0 3 6 1 6 1 2 5 4 1 1 1 5 2 5 0 1 1 1 0 0 1 0 3 5 4 3 5 2 3 0 5 4 6 0 1 2 1 6 2 1 5 0 3 1 5 1 6 0 0 0 1 6 6 4 5 2 2 4 5 5 2 3 2 2 6 5 0 6 5 3 3 0 3 3 1 1	
30	1 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 0 1 1 1 0 0 1 1 1 1 0 1 1 0 0 1 0 0 5 1 5 1 4 3 3 5 1 3 0 0 1 4 4 6 1 1 2 4 2 0 1 1 6 1 0 0 1 0 1 5 3 4 5 3 0 4 6 5 2 3 4 1 0 6 2 1 6 6 0 1 5 1 3 6 0 0 0 1 2 6 6 4 1 5 4 3 3 0 2 4 2 4 2 0 6 5 2 6 3 3 3 1 2 1	[1]
32	1 0 1 6 2 4 3 5 1 6 2 4 3 5 1 2 6 0 3 5 6 2 5 3 1 6 5 3 6 2 5 1 0 1 1 6 4 2 5 3 1 6 4 2 5 3 0 1 2 3 4 6 1 2 4 6 1 2 3 4 1 3 4 6 0 0 1 1 1 1 1 1 0 0 0 0 0 0 1 1 1 1 1 1 2 2 2 2 4 4 4 4 6 6 6 6 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	[62] [61]
50	1 0 1 6 2 4 3 5 1 6 2 4 3 5 1 2 6 0 3 5 6 2 5 3 1 6 5 3 6 2 5 1 0 1 1 6 4 2 5 3 1 6 4 2 5 3 0 1 2 3 4 6 1 2 4 6 1 2 3 4 1 3 4 6 0 0 1 1 1 1 1 1 0 0 0 0 0 0 1 1 1 1 1 1 2 2 2 2 4 4 4 4 6 6 6 6 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	[5] [140]

7.4 The uniqueness of the complete 32-cap in $PG(3,7)$

As byproduct of our search, it has been verified that there exists only one example of complete 32-cap in $PG(3,7)$. In fact in [62] it has been proven that $m'(3,7) = 32$, without discussing its uniqueness. In particular by [84] a linear $[32,4]_7$-code has minimum distance $d = 25$, then by Theorem 7.4 there exists a hyperplane containing at least 7 points of the corresponding 32-caps.

Cap	H_0	H_1	H_2	H_3	H_4	H_5	H_6	H_7	H_8
1 0 0 0 1 1 1 1 1 1 1 0 1 1 1 1 1 1 1 1 0 0 1 1 0 1 1 0 1 1 1 1 0 1 0 0 6 1 2 1 3 5 0 1 3 4 4 4 0 5 3 1 1 1 6 5 1 6 1 1 3 2 2 5 0 0 1 0 1 5 3 4 3 3 2 4 5 2 5 1 1 4 2 6 2 1 6 2 5 0 1 6 6 0 6 0 0 0 0 0 1 3 6 3 4 6 4 2 2 4 5 0 4 5 6 1 0 6 5 1 3 3 5 1 1 2 6 5 2	20	0	80	0	32	96	160	0	12

Chapter 8

Saturating sets

8.1 Introduction

Let $PG(n, q)$ be the n-dimensional projective space over the Galois field $GF(q)$. For an introduction to such spaces and the geometrical objects therein, see [95] - [99].

Definition 8.1. A point set S in the space $PG(n, q)$ is ϱ-saturating if ϱ is the least integer such that for any point $x \in PG(n, q)$ there exist $\varrho + 1$ points in S generating a subspace of $PG(n, q)$ in which x lies.

Definition 8.2. [177] A ϱ-saturating set of l points is called minimal if it does not contain a ϱ-saturating set of $l - 1$ points.

A q-ary linear code with codimension r has covering radius R if every r-positional q-ary column is equal to a linear combination of R columns of a parity check matrix of this code and R is the smallest value with such property. For an introduction to coverings of vector spaces over finite fields and to the concept of code covering radius, see [38]. Covering codes can be applied to many branches of Combinatorics and Information Theory, such as data compression and steganography (see [25]).

The points of a $\varrho-$saturating set in $PG(n,q)$ can be considered as columns of a parity check matrix of a q-ary linear code with codimension $n+1$. So, in terms of the coding theory, a $\varrho-$saturating l-set in $PG(n,q)$ corresponds to a parity check matrix of a q-ary linear code with length l, codimension $n+1$, and covering radius $\varrho+1$ [42],[48],[107]. Such code is denoted by an $[l,\, l-(n+1)]_q(\varrho+1)$ code.

Note that a ϱ-saturating set in $PG(n,q)$, $\varrho+1 \leq n$, can generate an infinite family of ϱ-saturating sets in $PG(N,q)$ with $N=n+(\varrho+1)m$, $m=1,2,3,\ldots$, see [38, Chapter 5.4],[42],[43, Example 6] and references therein, where such infinite families are considered as linear codes with covering radius $\varrho+1$.

The complete arcs of $PG(2,q)$ are examples of minimal 1-saturating sets, but there are minimal 1-saturating sets that are not complete arcs. Properties of the ϱ-saturating sets in $PG(n,q)$ are presented in [47].

This chapter deals with the minimal 1-saturating sets in $PG(2,q)$.

We use the following notations in $PG(2,q)$: $m(2,q,1)$ is the size of the largest minimal 1-saturating sets, $m'(2,q,1)$ is the size of the second largest minimal 1-saturating sets and $l(2,q,1)$ is the size of the smallest minimal 1-saturating sets.

The values of $m(2,q,1)$ and $m'(2,q,1)$ have been determined in [47]. These results and some constructions of minimal 1-saturating sets of such sizes have been reported in Section 2. Section 3 contains the description of the algorithm (of type B, see Chapter 3) we used to classify the minimal 1-saturating sets. Section 8.3.1 and Section 8.3.2 contain the classification of all the minimal 1-saturating sets in $PG(2,9)$ and $PG(2,11)$. In Section 8.3.3 the classification of minimal 1-saturating sets of minimal size is presented.

8.2 The values of $m(2,q,1)$, and $m'(2,q,1)$

In this section we recall some theorems from [47] that allow us to determine the values of $m(2,q,1)$ and $m'(2,q,1)$ and give constructions of minimal 1-saturating sets of such sizes. Let $\theta(n,q) = (q^{n+1}-1)/(q-1) = |PG(n,q)|$.

Theorem 8.3. *In the space $PG(n,q)$, let S_A be a $(\theta(n-1,q)+1)$-set consisting of a whole hyperplane V of $\theta(n-1,q)$ points, plus one point P not belonging to V. The point set S_A is a minimal 1-saturating $(\theta(n-1,q)+1)$-set in the space $PG(n,q)$.*

Remark 8.4. *Theorem 1 can be considered as an example of using [177, Lemma 10]. This lemma is treated as the "direct sum" construction in covering codes theory [38, Section 3.2].*

Theorem 8.5. *Any $\theta(n-1,q)+1$ points in the space $PG(n,q)$ are a 1-saturating set.*

Corollary 8.6. *The greatest cardinality of a minimal 1-saturating set in a space $PG(n,q)$ is equal to $\theta(n-1,q)+1$, i.e., $m(n,q,1) = \theta(n-1,q)+1$ for all q.*

Corollary 8.7. *In the plane $PG(2,q)$, $m(2,q,1) = q+2$ and a $(q+2)$-set containing a whole line l of $q+1$ points and one point $P \notin l$ is a largest minimal 1-saturating set.*

Example 8.8. For q even in the plane $PG(2,q)$ a hyperoval of $q+2$ points is another considerable example of a largest minimal 1-saturating set.

Theorem 8.9. *Let $l = \{L_1, L_2, \ldots, L_{q+1}\}$ be a line in the plane $PG(2,q)$ consisting of the points L_i. Denote by P an external point for l. Let T be a point on the line through the points L_1 and P and $P \neq T \neq L_1$. Let us consider a $(q+1)$-set $S_B = \{L_3, L_4, \ldots, L_{q+1}, P, T\}$. Then the point set S_B is a minimal 1-saturating $(q+1)$-set in a plane $PG(2,q)$, $q \geq 3$.*

Corollary 8.10. *In $PG(2,q)$, $q \geq 3$, $m'(2,q,1) = q+1$.*

Remark 8.11. *For q odd, in the plane $PG(2,q)$ an oval of $q+1$ points is another example of minimal 1-saturating $(q+1)$-set.*

Remark 8.12. *As in the plane $PG(2,q)$ a q-arc is always incomplete [95], the minimal 1-saturating sets of size q cannot be arcs.*

Theorem 8.13. *In $PG(2,q)$ there exists a unique minimal 1-saturating set not containing a projective frame. It consists of a whole line and an external point. Its stabilizer has size $\frac{|PGL(3,q)|}{q^2(q^2+q+1)}$ $\left(or\ \frac{|P\Gamma L(3,q)|}{q^2(q^2+q+1)}\right)$.*

Proof. Let $\mathcal{S}$ be a minimal 1-saturating set containing no projective frame and P a point of $\mathcal{S}$. Then, without loss of generality, we can suppose that $\mathcal{S}$ is contained in two lines ℓ_1 and ℓ_2 through P. Let $Q_1, R_1 \in \mathcal{S}$ such that $Q_1 \in \ell_1$ and $R_1 \in \ell_2$. If there exist other two points $Q_2, R_2 \in \mathcal{S}$ such that $Q_2 \in \ell_1$ and $R_2 \in \ell_2$ then the set Q_1, Q_2, R_1, R_2 is a projective frame. Hence all the other points of $\mathcal{S}$ are contained either in ℓ_1 or ℓ_2. Therefore suppose $\mathcal{S} \subseteq Q_1 \cup \ell_2$. If $\mathcal{S} \subsetneq Q_1 \cup \ell_2$, let $U \in \ell_2 \setminus \mathcal{S}$. Then the line Q_1U is not covered by $\mathcal{S}$ and the set $\mathcal{S}$ is not a 1-saturating set, contradiction. The uniqueness up to projectivities of this set is clear. The number of equivalent sets of this type is given by

$$\underbrace{|PG(2,q)|}_{\#lines} \times \underbrace{|PG(2,q) \setminus PG(1,q)|}_{\#external\ points} = (q^2+q+1) \times q^2.$$

Therefore the size of the stabilizer is

$$\frac{|PGL(3,q)|}{q^2(q^2+q+1)} \quad \left(\text{or } \frac{|P\Gamma L(3,q)|}{q^2(q^2+q+1)}\right).$$

□

8.3 The computer search for the non-equivalent minimal 1-saturating sets

Our goal is to determine the full classification of saturating sets up to projective equivalence in $PG(2, q)$. To do this an exhaustive search is obtained using program of type B (see Chapter 3) since, as in for blocking sets, saturating sets do not have any hereditary feature which can be used to prune the search space.

The program builds a tree using equivalence considerations as described in Chapter 3; each leaf is extended using a backtracking algorithm, which utilizes the informations obtained during the previous classification in order to avoid solutions containing leaf examined previously. The backtracking algorithm exploits the search space systematically, not considering the same t-uple more than one time. The program checks if the sets of the desired size obtained during the backtracking are saturating sets and if they satisfy the minimality condition.

8.3.1 Full classification of the minimal 1-saturating sets in $PG(2, 9)$

The following tables present the results obtained. We denote $GF(9) = \{0, 1 = \alpha^0, 2 = \alpha^1, \ldots, 8 = \alpha^7\}$ where α is a primitive element. This defines multiplication. For addition we use a primitive polynomial generating the field ($x^2 + x + 2$, [121]). We found no examples of minimal 11-saturating sets containing the projective frame and then the unique example is that one described in Theorem 8.13. In the following table we describe for each $6 \leq k \leq 11$ the type of the stabilizer of the minimal 1-saturating sets of size k. With the symbol G_i we denote a group of order i; for the other symbols we refer to [175]. When complete arcs exist, their number is indicated in bold font and the number of the rest of minimal

saturating sets is indicated in plain font.

Saturating sets in $PG(2,9)$					
$k=6$	G_{120}: **1**				
$k=7$	$\mathbb{Z}_4$: 1	G_{42}: **1**	G_{120}: 1		
$k=8$	$\mathbb{Z}_1$: 88	$\mathbb{Z}_2$: 52	$\mathbb{Z}_2\times\mathbb{Z}_2$: 11	$\mathcal{S}_3$: 1	$\mathbb{Z}_2\times\mathbb{Z}_4$: 1
	$\mathcal{D}_4$: 1	$\mathcal{D}_6$: 3	G_{16}: 1+**1**	G_{24}: 2	G_{48}: 1
$k=9$	$\mathbb{Z}_1$: 667	$\mathbb{Z}_2$: 87	$\mathbb{Z}_3$:9	$\mathbb{Z}_2\times\mathbb{Z}_2$: 4	$\mathcal{S}_3$: 2
	$\mathcal{D}_4$: 1	$\mathcal{D}_6$: 1	G_{16}: 1	G_{48}: 1	
$k=10$	$\mathbb{Z}_1$: 58	$\mathbb{Z}_2$: 22	$\mathbb{Z}_4$:5	$\mathbb{Z}_2\times\mathbb{Z}_2$: 4	$\mathcal{D}_4$: 2
	G_{16}: 1	G_{20}: 1	G_{32}: 1+**1**	G_{1440}: 1	
$k=11$	G_{11520}: 1				

In the following tables we list all the non-equivalent examples of the minimal 1-saturating sets in $PG(2,9)$ of sizes $6,7,10$. In the tables, the column "G" describes the stabilizer group, the columns "ℓ_i"contain the number of lines intersecting the minimal 1-saturating set in exactly i points.

Table of the saturating sets of size 6 and 7 in $PG(2,9)$

Size	Saturating set	ℓ_0	ℓ_1	ℓ_2	ℓ_3	G
6	1 0 1 0 1 1 0 1 1 0 2 8 0 0 1 1 8 7	46	30	15	0	G_{120}
7	1 0 1 0 0 1 1 0 1 1 0 1 2 7 0 0 1 1 2 8 2	41	31	18	1	$\mathbb{Z}_4$
7	1 0 0 1 0 1 1 0 1 0 1 1 2 5 0 0 1 1 2 1 2	40	34	15	2	$\mathcal{Z}_2\times\mathcal{Z}_4$
7	1 0 0 1 1 1 1 0 1 0 1 5 6 8 0 0 1 1 2 7 6	42	28	21	0	G_{42}

Table of the saturating sets of size 10 in $PG(2,9)$

Saturating set	ℓ_0	ℓ_1	ℓ_2	ℓ_3	ℓ_4	ℓ_5	ℓ_6	ℓ_7	ℓ_8	G
1 0 0 1 0 0 1 1 1 1 0 1 0 1 1 1 2 2 2 4 0 0 1 1 1 2 1 2 8 4	22	47	17	2	2	1	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 1 1 1 1 1 0 1 0 1 1 0 2 2 7 8 0 0 1 1 2 2 2 8 8 8	23	47	12	7	2	0	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 0 1 1 1 1 0 1 0 1 1 1 0 2 4 8 0 0 1 1 1 2 8 8 4 8	22	47	17	2	2	1	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 1 1 1 1 1 0 1 0 1 1 2 2 2 5 8 0 0 1 1 2 1 3 8 6 1	22	47	17	2	2	1	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 0 0 1 1 1 0 1 0 1 1 1 1 2 2 7 0 0 1 1 2 4 7 5 8 5	22	48	14	5	1	1	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 0 0 1 1 1 0 1 0 1 1 1 1 1 2 6 0 0 1 1 2 5 7 0 8 2	23	46	14	7	0	1	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 0 0 0 1 1 0 1 0 1 1 1 1 1 2 6 0 0 1 1 2 4 6 7 8 6	22	46	18	4	0	0	1	0	0	$\mathcal{Z}_1$
1 0 0 1 0 0 0 1 1 1 0 1 0 1 1 1 1 0 2 8 0 0 1 1 1 2 4 7 8 0	21	49	16	3	0	2	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 0 0 1 1 1 0 1 0 1 1 1 1 2 2 2 0 0 1 1 1 2 7 1 2 8	22	47	17	2	2	1	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 0 1 1 1 1 0 1 0 1 1 1 0 2 7 8 0 0 1 1 1 2 2 8 8 8	23	46	15	4	3	0	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 0 1 1 1 1 0 1 0 1 1 1 0 0 2 3 0 0 1 1 1 2 1 7 8 4	23	46	15	4	3	0	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 1 1 1 1 1 0 1 0 1 1 2 2 2 4 8 0 0 1 1 2 1 2 8 4 8	22	48	14	5	1	1	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 0 0 1 1 1 0 1 0 1 1 1 1 2 2 5 0 0 1 1 1 2 7 2 8 2	22	48	14	5	1	1	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 0 1 1 1 1 0 1 0 1 1 1 2 2 4 8 0 0 1 1 1 2 1 8 4 8	22	48	14	5	1	1	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 0 1 1 1 1 0 1 0 1 1 1 0 1 2 5 0 0 1 1 2 8 6 0 8 5	24	44	15	6	2	0	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 1 1 1 1 1 0 1 0 1 1 2 2 2 2 2 0 0 1 1 2 0 1 2 7 8	21	49	15	5	0	0	1	0	0	$\mathcal{Z}_1$
1 0 0 1 0 1 1 1 1 1 0 1 0 1 1 0 0 1 2 8 0 0 1 1 2 1 6 0 8 0	23	46	15	4	3	0	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 0 1 1 1 1 0 1 0 1 1 1 0 2 2 6 0 0 1 1 1 2 1 2 8 2	23	47	12	7	2	0	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 1 1 1 1 1 0 1 0 1 1 0 2 2 2 8 0 0 1 1 2 2 1 2 8 8	22	49	12	5	3	0	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 1 1 1 1 1 0 1 0 1 1 1 2 2 3 4 0 0 1 1 2 0 5 8 0 0	24	43	17	6	0	1	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 0 0 1 1 1 0 1 0 1 1 1 1 0 2 8 0 0 1 1 1 2 6 1 8 1	22	48	14	5	1	1	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 0 1 1 1 1 0 1 0 1 1 1 1 2 2 3 0 0 1 1 2 2 1 2 8 8	22	48	14	5	1	1	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 0 1 1 1 1 0 1 0 1 1 1 2 2 5 8 0 0 1 1 2 1 3 8 6 1	21	49	15	5	0	0	1	0	0	$\mathcal{Z}_1$
1 0 0 1 0 0 0 1 1 1 0 1 0 1 1 1 1 1 2 6 0 0 1 1 2 3 4 7 8 0	24	43	18	3	3	0	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 0 0 1 1 1 0 1 0 1 1 1 1 0 1 2 0 0 1 1 1 2 7 1 0 8	22	49	11	8	0	1	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 0 1 1 1 1 0 1 0 1 1 1 1 2 6 8 0 0 1 1 2 4 0 8 2 0	22	47	17	2	2	1	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 1 1 1 1 1 0 1 0 1 1 0 0 1 2 5 0 0 1 1 2 1 6 0 8 2	23	45	17	4	1	1	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 1 1 1 1 1 0 1 0 1 1 0 1 2 2 5 0 0 1 1 2 7 0 0 8 5	23	47	12	7	2	0	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 0 1 1 1 1 0 1 0 1 1 1 0 0 2 2 0 0 1 1 1 2 1 7 7 8	23	47	12	7	2	0	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 0 0 0 0 1 1 0 1 0 1 1 1 1 1 2 6 0 0 1 1 2 4 5 7 8 2	21	48	18	2	1	0	1	0	0	$\mathcal{Z}_1$
1 0 0 1 0 1 1 1 1 1 0 1 0 1 1 0 1 2 2 7 0 0 1 1 2 1 5 5 8 5	25	42	15	8	1	0	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 1 1 1 1 1 0 1 0 1 1 2 6 6 8 0 0 1 1 2 0 8 0 2 0	22	48	14	5	1	1	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 0 1 1 1 1 0 1 0 1 1 1 0 0 2 5 0 0 1 1 2 7 1 3 8 3	23	46	15	4	3	0	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 1 1 1 1 1 0 1 0 1 1 2 2 2 7 0 0 1 1 2 0 0 2 8 0	22	48	14	5	1	1	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 0 1 1 1 1 0 1 0 1 1 2 2 2 8 0 0 1 1 2 7 1 2 8 8	23	46	15	4	3	0	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 1 1 1 1 1 0 1 0 1 1 0 2 2 5 8 0 0 1 1 2 2 2 8 8 8	24	44	15	6	2	0	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 0 0 1 1 1 0 1 0 1 1 1 1 1 2 4 0 0 1 1 1 2 7 0 8 4	21	50	14	3	2	1	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 0 0 0 1 1 0 1 0 1 1 1 1 1 2 6 0 0 1 1 1 2 6 7 8 6	21	48	18	2	1	0	1	0	0	$\mathcal{Z}_1$
1 0 0 1 0 1 1 1 1 1 0 1 0 1 1 0 2 2 2 5 0 0 1 1 2 7 0 2 8 5	23	46	15	4	3	0	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 0 0 1 1 1 0 1 0 1 1 1 1 0 2 2 0 0 1 1 2 3 4 2 5 8	23	45	17	4	1	1	0	0	0	$\mathcal{Z}_1$

Saturating set	ℓ_0	ℓ_1	ℓ_2	ℓ_3	ℓ_4	ℓ_5	ℓ_6	ℓ_7	ℓ_8	G
1 0 0 1 0 1 1 1 1 1 0 1 0 1 1 1 2 2 5 5 0 0 1 1 2 0 3 8 5 6	24	45	12	9	1	0	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 0 1 1 1 1 0 1 0 1 1 1 0 2 2 6 0 0 1 1 2 7 4 0 8 0	22	49	12	5	3	0	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 1 1 1 1 1 0 1 0 1 1 1 1 2 4 5 0 0 1 1 2 2 6 8 5 6	23	45	17	4	1	1	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 0 0 0 1 1 0 1 0 1 1 1 1 1 2 7 0 0 1 1 1 2 4 7 8 4	21	48	18	2	1	0	1	0	0	$\mathcal{Z}_1$
1 0 0 1 0 0 0 0 1 1 0 1 0 1 1 1 1 1 2 2 0 0 1 1 1 2 7 8 1 8	21	49	15	5	0	0	1	0	0	$\mathcal{Z}_1$
1 0 0 1 0 1 1 1 1 1 0 1 0 1 1 1 1 1 2 5 0 0 1 1 2 0 2 6 8 6	22	48	14	5	1	1	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 0 1 1 1 1 0 1 0 1 1 1 0 2 2 8 0 0 1 1 1 2 1 3 8 1	23	46	15	4	3	0	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 0 1 1 1 1 0 1 0 1 1 1 1 2 2 5 0 0 1 1 2 4 2 3 8 6	22	47	17	2	2	1	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 0 1 1 1 1 0 1 0 1 1 1 0 1 2 5 0 0 1 1 1 2 1 0 8 0	22	49	12	5	3	0	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 0 1 1 1 1 0 1 0 1 1 1 0 1 2 5 0 0 1 1 2 7 8 8 8 3	23	46	15	4	3	0	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 1 1 1 1 1 0 1 0 1 1 0 2 2 4 7 0 0 1 1 2 2 5 8 0 8	24	43	17	6	0	1	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 1 1 1 1 1 0 1 0 1 1 1 2 2 2 6 0 0 1 1 2 0 0 2 8 0	22	48	14	5	1	1	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 1 1 1 1 1 0 1 0 1 1 2 2 5 5 5 0 0 1 1 2 3 8 3 6 8	23	47	12	7	2	0	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 1 1 1 1 1 0 1 0 1 1 1 1 2 2 6 0 0 1 1 2 0 7 7 8 0	22	49	12	5	3	0	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 1 1 1 1 1 0 1 0 1 1 1 1 1 2 8 0 0 1 1 2 0 2 7 8 1	22	48	14	5	1	1	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 0 1 1 1 1 0 1 0 1 1 1 2 2 2 7 0 0 1 1 2 4 5 7 8 5	23	46	15	4	3	0	0	0	0	$\mathcal{Z}_1$
1 0 0 1 0 0 0 0 1 1 0 1 0 1 1 1 1 1 2 8 0 0 1 1 2 4 7 0 0 8	20	52	12	6	0	0	1	0	0	$\mathcal{Z}_2$
1 0 0 1 0 0 1 1 1 1 0 1 0 1 1 1 0 0 5 8 0 0 1 1 2 5 3 5 0 3	21	50	14	3	2	1	0	0	0	$\mathcal{Z}_2$
1 0 0 1 0 0 1 1 1 1 0 1 0 1 1 1 1 1 2 7 0 0 1 1 2 7 5 7 8 5	22	47	17	2	2	1	0	0	0	$\mathcal{Z}_2$
1 0 0 1 0 1 1 1 1 1 0 1 0 1 1 1 2 2 2 3 0 0 1 1 2 0 3 5 8 0	24	44	15	6	2	0	0	0	0	$\mathcal{Z}_2$
1 0 0 1 0 1 1 1 1 1 0 1 0 1 1 2 2 5 8 1 0 0 1 1 2 1 5 8 1 4	25	40	21	2	3	0	0	0	0	$\mathcal{Z}_2$

Saturating set	ℓ_0	ℓ_1	ℓ_2	ℓ_3	ℓ_4	ℓ_5	ℓ_6	ℓ_7	ℓ_8	G
1 0 0 1 0 0 0 1 1 1 0 1 0 1 1 1 1 2 2 4 0 0 1 1 1 2 4 2 8 4	21	49	16	3	0	2	0	0	0	$\mathcal{Z}_2$
1 0 0 1 0 0 1 1 1 1 0 1 0 1 1 1 1 1 2 7 0 0 1 1 1 2 0 5 8 5	23	47	12	7	2	0	0	0	0	$\mathcal{Z}_2$
1 0 0 1 0 0 1 1 1 1 0 1 0 1 1 1 1 2 2 4 0 0 1 1 2 7 0 0 8 5	22	49	12	5	3	0	0	0	0	$\mathcal{Z}_2$
1 0 0 1 0 0 0 0 0 1 0 1 0 1 1 1 1 1 1 0 0 0 1 1 1 2 3 5 6 5	18	54	15	3	0	0	0	1	0	$\mathcal{Z}_2$
1 0 0 1 0 1 1 1 1 1 0 1 0 1 1 0 2 3 5 7 0 0 1 1 2 3 8 2 8 5	22	46	18	4	0	0	1	0	0	$\mathcal{Z}_2$
1 0 0 1 0 1 1 1 1 1 0 1 0 1 1 0 0 0 2 2 0 0 1 1 2 1 6 7 7 8	23	46	14	7	0	1	0	0	0	$\mathcal{Z}_2$
1 0 0 1 0 1 1 1 1 1 0 1 0 1 1 0 1 1 2 7 0 0 1 1 2 8 0 3 8 0	23	47	12	7	2	0	0	0	0	$\mathcal{Z}_2$
1 0 0 1 0 1 1 1 1 1 0 1 0 1 1 0 1 1 5 6 0 0 1 1 2 5 0 7 0 7	22	49	12	5	3	0	0	0	0	$\mathcal{Z}_2$
1 0 0 1 0 1 1 1 1 1 0 1 0 1 1 0 0 0 0 4 0 0 1 1 2 1 3 5 6 6	20	51	15	3	1	0	1	0	0	$\mathcal{Z}_2$
1 0 0 1 0 0 0 0 0 1 0 1 0 1 1 1 1 1 1 2 0 0 1 1 1 2 4 5 8 8	19	51	18	2	0	0	0	1	0	$\mathcal{Z}_2$
1 0 0 1 0 0 0 1 1 1 0 1 0 1 1 1 1 2 7 7 0 0 1 1 1 2 7 5 8 5	22	48	14	5	1	1	0	0	0	$\mathcal{Z}_2$
1 0 0 1 0 0 1 1 1 1 0 1 0 1 1 1 2 2 3 8 0 0 1 1 2 7 1 8 1 1	22	47	17	2	2	1	0	0	0	$\mathcal{Z}_2$
1 0 0 1 0 0 1 1 1 1 0 1 0 1 1 1 0 1 2 5 0 0 1 1 2 7 2 4 8 8	26	39	18	7	1	0	0	0	0	$\mathcal{Z}_2$
1 0 0 1 0 1 1 1 1 1 0 1 0 1 1 1 1 2 2 7 0 0 1 1 2 0 3 2 8 0	24	44	15	6	2	0	0	0	0	$\mathcal{Z}_2$
1 0 0 1 0 0 0 1 1 1 0 1 0 1 1 1 1 2 6 8 0 0 1 1 1 2 6 8 6 8	22	46	19	2	0	2	0	0	0	$\mathcal{Z}_2$
1 0 0 1 0 1 1 1 1 1 0 1 0 1 1 1 2 2 2 6 0 0 1 1 2 0 1 5 8 5	24	44	15	6	2	0	0	0	0	$\mathcal{Z}_2$
1 0 0 1 0 1 1 1 1 1 0 1 0 1 1 2 2 2 4 6 0 0 1 1 2 0 2 8 4 0	24	43	18	3	3	0	0	0	0	$\mathcal{Z}_2$
1 0 0 1 0 0 0 1 1 1 0 1 0 1 1 1 1 0 2 2 0 0 1 1 2 4 7 1 0 8	22	49	11	8	0	1	0	0	0	$\mathcal{Z}_4$
1 0 0 1 0 0 0 0 0 1 1 0 1 0 1 1 1 1 1 2 2 0 0 1 1 1 2 4 5 3 8	22	46	18	4	0	0	1	0	0	$\mathcal{Z}_2 \times \mathcal{Z}_2$
1 0 0 1 0 0 0 1 1 1 1 0 1 0 1 1 1 2 3 4 8 0 0 1 1 2 7 8 1 5 1	23	45	18	1	4	0	0	0	0	$\mathcal{Z}_2 \times \mathcal{Z}_2$
1 0 0 1 0 1 1 1 1 1 0 1 0 1 1 0 1 5 6 8 0 0 1 1 2 5 0 0 0 0	20	52	12	6	0	0	1	0	0	$\mathcal{Z}_2 \times \mathcal{Z}_2$

Saturating set	ℓ_0	ℓ_1	ℓ_2	ℓ_3	ℓ_4	ℓ_5	ℓ_6	ℓ_7	ℓ_8	G
1 0 0 1 0 1 1 1 1 1 0 1 0 1 1 2 2 5 5 5 0 0 1 1 2 4 8 3 6 8	25	42	15	8	1	0	0	0	0	$\mathcal{Z}_4$
1 0 0 1 0 0 1 1 1 1 0 1 0 1 1 1 1 2 4 5 0 0 1 1 1 2 0 8 4 0	22	48	15	2	4	0	0	0	0	$\mathcal{Z}_2 \times \mathcal{Z}_2$
1 0 0 1 0 0 0 1 1 1 0 1 0 1 1 1 1 2 2 8 0 0 1 1 2 4 7 2 8 8	23	45	17	4	1	1	0	0	0	$\mathcal{Z}_4$
1 0 0 1 0 1 1 1 1 1 0 1 0 1 1 1 2 2 5 6 0 0 1 1 2 2 5 8 4 5	28	34	21	8	0	0	0	0	0	$\mathcal{Z}_4$
1 0 0 1 0 0 1 1 1 1 0 1 0 1 1 1 0 0 2 7 0 0 1 1 2 7 2 3 8 5	24	42	21	0	4	0	0	0	0	$\mathcal{Z}_4$
1 0 0 1 0 0 1 1 1 1 0 1 0 1 1 1 0 0 5 6 0 0 1 1 2 5 3 5 0 0	21	50	15	0	5	0	0	0	0	$\mathcal{D}_4$

Saturating set	ℓ_0	ℓ_1	ℓ_2	ℓ_3	ℓ_4	ℓ_5	ℓ_6	ℓ_7	ℓ_8	G
1 0 0 1 0 0 1 1 1 1 0 1 0 1 1 1 0 2 4 7 0 0 1 1 2 4 2 8 2 5	26	38	21	4	2	0	0	0	0	$\mathcal{D}_4$
1 0 0 1 0 1 1 1 1 1 0 1 0 1 1 0 0 1 6 7 0 0 1 1 2 1 5 7 7 7	22	50	9	8	2	0	0	0	0	G_{16}
1 0 0 1 0 0 1 1 1 1 0 1 0 1 1 1 0 0 2 3 0 0 1 1 1 2 2 3 2 2	21	50	15	0	5	0	0	0	0	G_{20}
1 0 0 1 0 0 0 0 0 0 0 1 0 1 1 1 1 1 1 1 0 0 1 1 2 3 5 6 7 8	15	58	17	0	0	0	0	0	1	G_{32}
1 0 0 1 0 1 1 1 1 1 0 1 0 1 1 0 0 6 6 7 0 0 1 1 2 1 5 0 7 5	22	50	9	8	2	0	0	0	0	G_{32}
1 0 0 1 1 1 1 1 1 1 0 1 0 1 2 3 5 6 7 8 0 0 1 1 6 5 2 4 8 3	36	10	45	0	0	0	0	0	0	G_{1440}

8.3.2 Full classification of the minimal 1-saturating sets in $PG(2, 11)$

The following tables present the results obtained. We denote $GF(11) = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. We found no examples of minimal 13-saturating sets containing the projective frame and then the unique example is that one described in Theorem 8.13. In the following table we describe, for each $7 \leq k \leq 13$, the type of the stabilizer of the minimal 1-saturating sets of size k. With the symbol G_i we denote a group of order i; for the other symbols we refer to [175]. When complete arcs exist, their number is indicated in bold font and the number of the rest of minimal saturating sets is indicated in plain font.

Saturating sets in $PG(2, 11)$					
$k = 7$	$\mathbb{Z}_7 \rtimes \mathbb{Z}_3$: **1**				
$k = 8$	$\mathbb{Z}_1$: 22 G_{16}: **1**	$\mathbb{Z}_2$: 26+**5**	$\mathbb{Z}_2 \times \mathbb{Z}_2$: 2+**1**	$\mathcal{D}_4$: 1 + **1**	$\mathcal{D}_5$: **1**
$k = 9$	$\mathbb{Z}_1$: 10686 $\mathcal{S}_3$: 10+**1**	$\mathbb{Z}_2$: 265+**1** $\mathbb{Z}_{10}$: 1	$\mathbb{Z}_3$: 40 +**1** $\mathcal{Q}_6$: 1	$\mathbb{Z}_4$: 2	$\mathbb{Z}_2 \times \mathbb{Z}_2$: 3
$k = 10$	$\mathbb{Z}_1$: 115731 $\mathbb{Z}_5$: 2 $\mathcal{Q}_6$:1	$\mathbb{Z}_2$: 1332 $\mathcal{S}_3$: 8 G_{60}:**1**	$\mathbb{Z}_3$: 31 $\mathcal{D}_4$: 2	$\mathbb{Z}_4$: 15 $\mathcal{D}_5$: 2	$\mathbb{Z}_2 \times \mathbb{Z}_2$: 13 $\mathbb{Z}_{10}$: 1
$k = 11$	$\mathbb{Z}_1$: 30802	$\mathbb{Z}_2$: 147	$\mathbb{Z}_4$: 1	$\mathbb{Z}_2 \times \mathbb{Z}_2$: 3	$\mathcal{D}_4$: 3
$k = 12$	$\mathbb{Z}_1$: 119 G_{20}: 1	$\mathbb{Z}_2$: 7 G_{1320}: **1**	$\mathbb{Z}_3$: 5	$\mathcal{S}_3$: 1	$\mathcal{Q}_6$: 1
$k = 13$	G_{13200}: 1				

8.3.3 Full classification of the minimal 1-saturating sets of smallest size in $PG(2,q)$, $16 \leq q \leq 23$

The following tables present the results obtained. In the examples we represent the elements of the Galois fields as follows. We denote

$$GF(16) = \{0, 1 = \alpha^0, 2 = \alpha^1, \ldots, 15 = \alpha^{14}\}$$

where α is a primitive element such that $\alpha^4 + \alpha^3 + 1 = 0$,

$$GF(17) = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\},$$

$$GF(19) = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18\},$$

$$GF(23) = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22\}.$$

With the symbol G_i we denote a group of order i; for the other symbols we refer to [175]. When complete arcs exist, their number is indicated in bold font and the number of the rest of minimal saturating sets is indicated in plain font.

$q = 16$	$k = 9$	$\mathbb{Z}_3$: **1**	$\mathbb{Z}_6$: **1**	$\mathcal{D}_6$: 1	$\mathcal{G}_{54}$: 1	
	$k = 10$	$\mathbb{Z}_1$: 7744+**342** $\mathbb{Z}_6$: 2 $\mathbb{Z}_4 \times \mathbb{Z}_4$: 1 G_{48}: 1	$\mathbb{Z}_2$: 699+**130** $\mathcal{S}_3$: 4+**3** G_{16}: 4+**3**	$\mathbb{Z}_3$: 3 $\mathcal{D}_4$: 8 G_{20}: **1**	$\mathbb{Z}_4$: 12+**8** $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$: 18+**10** G_{24}: 1	$\mathbb{Z}_2 \times \mathbb{Z}_2$: 27+**4** $\mathcal{Q}_6$: 1 G_{32}: 1
$q = 17$	$k = 10$	$\mathbb{Z}_1$: 2591+**341** $\mathcal{S}_3$: 7+**9** G_{18}: **1**	$\mathbb{Z}_2$: 460+**179** $\mathcal{D}_4$: 4 G_{24}: **1**	$\mathbb{Z}_3$: 8+**10** $\mathcal{Q}_4$: **1**	$\mathbb{Z}_4$: 4+**7** $\mathcal{Q}_6$: **2**	$\mathbb{Z}_2 \times \mathbb{Z}_2$: 5+**8** G_{16}: 1+**1**
$q = 19$	$k = 10$	$\mathbb{Z}_1$: 1+**1** $\mathcal{S}_3$: **2**	$\mathbb{Z}_2$: 6+**18** $\mathcal{D}_5$: **2**	$\mathbb{Z}_3$: **1** $\mathcal{Q}_6$: **1**	$\mathbb{Z}_4$: **1** G_{60}: **1**	$\mathbb{Z}_2 \times \mathbb{Z}_2$: **2**
$q = 23$	$k = 10$	$\mathcal{S}_3$: **1**				

In the following tables all the minimal 1-saturating sets of minimal size in $PG(2,16)$, $PG(2,19)$ and $PG(2,23)$ and all the examples of minimal 1-saturating sets of size 10 in $PG(2,17)$ having stabilizer of size greater than or equal to 6 are presented.

q	k	Saturating set	ℓ_0	ℓ_1	ℓ_2	ℓ_3	ℓ_4	G
16	9	1 0 0 1 1 1 1 1 1 1 0 1 0 1 2 4 11 12 13 0 0 1 1 10 5 3 6 12	156	81	36	0	0	$\mathcal{Z}_3$
16	9	1 0 0 1 1 1 1 1 1 1 0 1 0 1 2 10 11 12 13 0 0 1 1 10 11 14 6 12	156	81	36	0	0	$\mathcal{Z}_6$
16	9	1 0 0 1 1 1 1 1 1 1 0 1 0 1 2 10 11 13 13 0 0 1 1 10 13 9 0 12	153	90	27	3	0	$\mathcal{D}_6$
16	9	1 0 0 1 1 1 1 1 1 1 0 1 0 1 0 2 7 9 10 0 0 1 1 15 10 10 3 11	153	90	27	3	0	G_{54}
17	10	1 0 0 1 1 1 1 1 1 1 0 1 0 1 3 6 8 10 13 13 0 0 1 1 7 2 2 10 6 8	169	99	36	3	0	$\mathcal{S}_3$
17	10	1 0 0 1 1 1 1 1 1 1 0 1 0 1 0 3 5 6 10 13 0 0 1 1 13 7 15 2 14 1	169	99	36	3	0	$\mathcal{S}_3$
17	10	1 0 0 1 1 1 1 1 1 1 0 1 0 1 2 3 10 11 13 15 0 0 1 1 6 7 4 13 15 8	172	90	45	0	0	$\mathcal{S}_3$
17	10	1 0 0 1 1 1 1 1 1 1 0 1 0 1 3 6 6 7 12 16 0 0 1 1 7 2 7 3 14 10	169	99	36	3	0	$\mathcal{S}_3$
17	10	1 0 0 1 0 1 1 1 1 1 0 1 0 1 1 1 3 14 16 16 0 0 1 1 7 15 7 3 8 11	169	99	36	3	0	$\mathcal{S}_3$
17	10	1 0 0 1 1 1 1 1 1 1 0 1 0 1 0 3 10 11 12 13 0 0 1 1 10 7 4 15 8 15	169	99	36	3	0	$\mathcal{S}_3$
17	10	1 0 0 1 1 1 1 1 1 1 0 1 0 1 2 3 6 7 8 10 0 0 1 1 13 7 15 16 6 4	172	90	45	0	0	$\mathcal{S}_3$
17	10	1 0 0 1 1 1 1 1 1 1 0 1 0 1 0 3 6 10 12 16 0 0 1 1 13 7 12 4 16 7	169	99	36	3	0	$\mathcal{S}_3$
17	10	1 0 0 1 1 1 1 1 1 1 0 1 0 1 3 4 5 6 10 12 0 0 1 1 7 5 11 10 16 13	172	90	45	0	0	$\mathcal{S}_3$
17	10	1 0 0 1 1 1 1 1 1 1 0 1 0 1 0 2 3 10 11 13 0 0 1 1 2 14 7 4 15 16	171	93	42	1	0	$\mathcal{S}_3$
17	10	1 0 0 1 1 1 1 1 1 1 0 1 0 1 3 4 9 10 13 16 0 0 1 1 7 12 5 4 9 10	172	90	45	0	0	$\mathcal{S}_3$
17	10	1 0 0 1 1 1 1 1 1 1 0 1 0 1 3 5 7 10 12 16 0 0 1 1 7 9 10 4 14 8	172	90	45	0	0	$\mathcal{S}_3$
17	10	1 0 0 1 1 1 1 1 1 1 0 1 0 1 3 4 5 6 9 10 0 0 1 1 7 16 9 15 12 4	172	90	45	0	0	$\mathcal{S}_3$
17	10	1 0 0 1 1 1 1 1 1 1 0 1 0 1 3 7 9 10 13 14 0 0 1 1 7 8 13 4 9 3	172	90	45	0	0	$\mathcal{S}_3$
17	10	1 0 0 1 1 1 1 1 1 1 0 1 0 1 3 6 10 13 14 15 0 0 1 1 7 2 14 4 5 10	172	90	45	0	0	$\mathcal{S}_3$
17	10	1 0 0 1 1 1 1 1 1 1 0 1 0 1 2 3 7 9 10 12 0 0 1 1 13 7 16 10 4 5	172	90	45	0	0	$\mathcal{S}_3$
17	10	1 0 0 1 1 1 1 1 1 1 0 1 0 1 1 2 3 4 4 7 0 0 1 1 12 3 7 2 7 16	166	108	27	6	0	$\mathcal{D}_4$
17	10	1 0 0 1 1 1 1 1 1 1 0 1 0 1 3 8 10 13 14 16 0 0 1 1 7 16 4 11 15 13	172	90	45	0	0	$\mathcal{Q}_8$
17	10	1 0 0 1 1 1 1 1 1 1 0 1 0 1 1 3 4 5 10 10 0 0 1 1 9 7 6 10 5 10	166	108	27	6	0	$\mathcal{D}_4$
17	10	1 0 0 1 1 1 1 1 1 1 0 1 0 1 0 3 4 5 8 10 0 0 1 1 7 7 6 10 6 5	166	108	27	6	0	$\mathcal{D}_4$
17	10	1 0 0 1 1 1 1 1 1 1 0 1 0 1 2 3 3 6 10 14 0 0 1 1 8 7 10 10 0 3	168	102	33	4	0	$\mathcal{D}_4$
17	10	1 0 0 1 1 1 1 1 1 1 0 1 0 1 3 5 6 8 11 13 0 0 1 1 7 10 2 9 4 6	172	90	45	0	0	$\mathcal{Q}_6$
17	10	1 0 0 1 1 1 1 1 1 1 0 1 0 1 2 3 7 10 11 16 0 0 1 1 8 7 14 5 9 3	172	90	45	0	0	$\mathcal{Q}_6$
17	10	1 0 0 1 0 0 1 1 1 1 0 1 0 1 1 1 3 9 11 12 0 0 1 1 5 12 7 8 14 15	166	106	33	0	2	G_{16}
17	10	1 0 0 1 1 1 1 1 1 1 0 1 0 1 3 4 6 8 11 16 0 0 1 1 7 8 13 15 12 5	172	90	45	0	0	G_{16}
17	10	1 0 0 1 1 1 1 1 1 1 0 1 0 1 3 4 6 7 14 15 0 0 1 1 7 8 11 16 9 14	172	90	45	0	0	G_{18}
17	10	1 0 0 1 1 1 1 1 1 1 0 1 0 1 3 4 5 6 10 12 0 0 1 1 7 6 10 2 5 14	172	90	45	0	0	G_{24}
19	10	1 0 0 1 1 1 1 1 1 1 0 1 0 1 0 2 5 8 13 18 0 0 1 1 17 5 12 18 6 10	225	113	42	1	0	$\mathcal{Z}_1$
19	10	1 0 0 1 1 1 1 1 1 1 0 1 0 1 2 8 11 15 17 18 0 0 1 1 5 18 4 14 3 9	226	110	45	0	0	$\mathcal{Z}_1$
19	10	1 0 0 1 1 1 1 1 1 1 0 1 0 1 2 7 8 11 12 16 0 0 1 1 5 12 18 7 9 11	226	110	45	0	0	$\mathcal{Z}_2$
19	10	1 0 0 1 1 1 1 1 1 1 0 1 0 1 2 3 8 11 15 17 0 0 1 1 5 9 18 4 14 3	225	113	42	1	0	$\mathcal{Z}_2$
19	10	1 0 0 1 1 1 1 1 1 1 0 1 0 1 2 4 5 6 8 17 0 0 1 1 5 12 10 16 18 2	226	110	45	0	0	$\mathcal{Z}_2$
19	10	1 0 0 1 1 1 1 1 1 1 0 1 0 1 2 6 8 9 10 13 0 0 1 1 5 16 18 2 11 6	226	110	45	0	0	$\mathcal{Z}_2$
19	10	1 0 0 1 1 1 1 1 1 1 0 1 0 1 2 3 4 5 6 8 0 0 1 1 5 7 17 6 17 18	225	113	42	1	0	$\mathcal{Z}_2$
19	10	1 0 0 1 1 1 1 1 1 1 0 1 0 1 2 5 6 8 9 12 0 0 1 1 5 10 16 18 12 17	226	110	45	0	0	$\mathcal{Z}_2$
19	10	1 0 0 1 1 1 1 1 1 1 0 1 0 1 2 3 4 7 8 17 0 0 1 1 5 7 11 18 15 13	226	110	45	0	0	$\mathcal{Z}_2$
19	10	1 0 0 1 1 1 1 1 1 1 0 1 0 1 1 2 7 10 13 15 0 0 1 1 16 5 18 9 12 7	225	113	42	1	0	$\mathcal{Z}_2$
19	10	1 0 0 1 1 1 1 1 1 1 0 1 0 1 2 4 5 6 8 9 0 0 1 1 5 12 10 16 18 7	226	110	45	0	0	$\mathcal{Z}_2$

q	k	Saturating set	ℓ_0	ℓ_1	ℓ_2	ℓ_3	ℓ_4	G
19	10	1 0 0 1 1 1 1 1 1 1 1 0 1 0 1 2 4 7 9 10 14 0 0 1 1 5 11 18 16 8 7	226	110	45	0	0	$\mathcal{Z}_2$
19	10	1 0 0 1 1 1 1 1 1 1 1 0 1 0 1 2 5 8 9 12 13 0 0 1 1 5 7 18 10 9 14	226	110	45	0	0	$\mathcal{Z}_2$
19	10	1 0 0 1 1 1 1 1 1 1 1 0 1 0 1 2 5 6 8 14 18 0 0 1 1 5 4 13 18 7 17	226	110	45	0	0	$\mathcal{Z}_2$
19	10	1 0 0 1 1 1 1 1 1 1 1 0 1 0 1 2 3 4 6 16 18 0 0 1 1 5 18 16 13 15 9	226	110	45	0	0	$\mathcal{Z}_2$
19	10	1 0 0 1 1 1 1 1 1 1 1 0 1 0 1 2 4 6 8 10 18 0 0 1 1 5 7 13 18 11 12	224	116	39	2	0	$\mathcal{Z}_2$
19	10	1 0 0 1 1 1 1 1 1 1 1 0 1 0 1 2 7 8 13 16 18 0 0 1 1 5 4 7 17 9 14	226	110	45	0	0	$\mathcal{Z}_2$
19	10	1 0 0 1 1 1 1 1 1 1 1 0 1 0 1 2 3 7 15 17 18 0 0 1 1 5 6 18 10 12 3	226	110	45	0	0	$\mathcal{Z}_2$
19	10	1 0 0 1 1 1 1 1 1 1 1 0 1 0 1 2 4 6 8 10 18 0 0 1 1 5 2 13 18 3 15	226	110	45	0	0	$\mathcal{Z}_2$
19	10	1 0 0 1 1 1 1 1 1 1 1 0 1 0 1 2 6 7 8 17 18 0 0 1 1 5 13 14 18 6 9	225	113	42	1	0	$\mathcal{Z}_2$
19	10	1 0 0 1 1 1 1 1 1 1 1 0 1 0 1 2 3 5 7 15 17 0 0 1 1 5 6 14 18 10 4	226	110	45	0	0	$\mathcal{Z}_2$
19	10	1 0 0 1 1 1 1 1 1 1 1 0 1 0 1 2 3 7 11 12 15 0 0 1 1 5 17 18 9 9 7	224	116	39	2	0	$\mathcal{Z}_2$
19	10	1 0 0 1 1 1 1 1 1 1 1 0 1 0 1 2 6 8 9 14 15 0 0 1 1 5 16 18 8 11 12	226	110	45	0	0	$\mathcal{Z}_2$
19	10	1 0 0 1 1 1 1 1 1 1 1 0 1 0 1 2 3 7 8 10 15 0 0 1 1 5 16 18 3 12 13	226	110	45	0	0	$\mathcal{Z}_2$

q	k	Saturating set	ℓ_0	ℓ_1	ℓ_2	ℓ_3	ℓ_4	G
19	10	1 0 0 1 1 1 1 1 1 1 1 0 1 0 1 2 3 5 8 14 17 0 0 1 1 5 12 15 18 17 2	226	110	45	0	0	$\mathcal{Z}_2$
19	10	1 0 0 1 1 1 1 1 1 1 1 0 1 0 1 2 6 8 14 17 18 0 0 1 1 5 3 18 4 6 15	226	110	45	0	0	$\mathcal{Z}_2$
19	10	1 0 0 1 1 1 1 1 1 1 1 0 1 0 1 2 8 10 11 12 16 0 0 1 1 5 18 7 6 13 9	226	110	45	0	0	$\mathcal{Z}_3$
19	10	1 0 0 1 1 1 1 1 1 1 1 0 1 0 1 2 4 6 8 10 18 0 0 1 1 5 6 13 18 17 14	226	110	45	0	0	$\mathcal{Z}_4$
19	10	1 0 0 1 1 1 1 1 1 1 1 0 1 0 1 2 4 6 8 16 18 0 0 1 1 5 17 12 18 9 13	226	110	45	0	0	$\mathcal{Z}_2 \times \mathcal{Z}_2$
19	10	1 0 0 1 1 1 1 1 1 1 1 0 1 0 1 2 6 7 8 9 12 0 0 1 1 5 14 4 7 8 10	226	110	45	0	0	$\mathcal{Z}_2 \times \mathcal{Z}_2$
19	10	1 0 0 1 1 1 1 1 1 1 1 0 1 0 1 2 8 11 12 13 17 0 0 1 1 5 18 4 17 7 3	226	110	45	0	0	$\mathcal{S}_3$
19	10	1 0 0 1 1 1 1 1 1 1 1 0 1 0 1 2 6 7 13 16 18 0 0 1 1 5 12 2 14 18 13	226	110	45	0	0	$\mathcal{S}_3$
19	10	1 0 0 1 1 1 1 1 1 1 1 0 1 0 1 2 3 7 8 9 10 0 0 1 1 5 8 4 7 11 12	226	110	45	0	0	$\mathcal{D}_5$
19	10	1 0 0 1 1 1 1 1 1 1 1 0 1 0 1 2 5 7 8 12 13 0 0 1 1 5 2 3 9 17 7	226	110	45	0	0	$\mathcal{D}_5$
19	10	1 0 0 1 1 1 1 1 1 1 1 0 1 0 1 2 4 7 8 15 18 0 0 1 1 5 14 10 18 4 11	226	110	45	0	0	$\mathcal{Q}_6$
19	10	1 0 0 1 1 1 1 1 1 1 1 0 1 0 1 2 4 13 15 16 17 0 0 1 1 5 16 7 18 3 4	226	110	45	0	0	G_{60}
23	10	1 0 0 1 1 1 1 1 1 1 1 0 1 0 1 2 7 14 17 19 22 0 0 1 1 6 13 15 9 20 19	358	150	45	0	0	$\mathcal{S}_3$

Chapter 9

Blocking Sets

9.1 Blocking sets in projective planes

Definition 9.1 ([168])**.** A *blocking set* in a projective plane is a set of points which intersects every line.

A line $\ell \subset PG(2,q)$ is the simplest example of blocking set. A blocking set which contains a line is called *trivial*. We can give the following definition.

Definition 9.2. A *blocking set* $\mathcal{K}$ is called *minimal* if it contains no proper subsets $\mathcal{K}'$ which are blocking sets. A point $P \in \mathcal{K}$ is called *essential* if $\mathcal{K} \setminus \{P\}$ is not a blocking set.

It is clear that a blocking set is minimal if and only if all its points are essential and that a blocking set containing properly a line is not minimal.

A blocking set is called *small* if it has size less than $3(q+1)/2$. There exist no examples of minimal blocking sets of size cq, where $c > 3$. For a more detailed introduction to blocking sets see ([168], [95, Chapter 13], [98]).

It is interesting to note that if $k+t = q+1$, then (n,k)-arcs and t-fold blocking sets are complements of each other in a projective plane. This means that the classification of 1-fold blocking sets is equivalent

the classification of (n, q)-arcs. Blocking sets are also important tools for the determination of maximal partial spreads, i.e. sets of skew lines such that each line of the space meets at least one line of the set.

9.2 Theoretical results

One of the most important theoretical construction of minimal blocking sets is the so called *Rédey's construction*.

Let U be a subsets of size q in $AG(2, q)$ and D be the set of all directions determined by U, that is the set of all the points $Q \in \ell_\infty$ such that there exist two points $P_1, P_2 \in U$ with P_1, P_2, Q collinear. If the set D is not the entire line, then $B = U \cup D$ is a minimal blocking set. When U is the graph of a function B is a blocking set of *Rédey type*.

Let B a blocking set of size $q + m$, with $m \leq q$, such that there exists a line ℓ having exactly m points of B. Since it is always possible, changing the coordinates, to choose $B \setminus \ell$ as a graph of a function f and $B \cap \ell$ to be the set of directions determined by U, B can be obtained by Rédey construction.

An other construction described in [118] and [117] gives minimal blocking sets of size k, with $2q - 1 \leq k \leq 3q - 5$. This construction is called *IMI construction*.

The following theorems summarized the main results about the spectrum of minimal blocking sets in projective planes.

Theorem 9.3. *1. ([32]) The smallest non-trivial blocking sets in $PG(2, q)$, q square, have cardinality $q + \sqrt{q} + 1$ and are equal to Baer subplanes $PG(2, \sqrt{q})$.*

2. ([29]) In $PG(2, q)$, q non-square, $q = p^h$, $h > 2$, $p \geq 5$, p prime, $|B| \geq q + q^{2/3} + 1$ for every non-trivial blocking set B.

3. ([27]) In $PG(2, q)$, q prime, $q > 2$, $|B| \geq 3(q + 1)/2$ for every non-trivial blocking set B.

4. *([29]) In $PG(2,q)$, q square, $q = p^h$, $h > 2$, $p \geq 5$ prime, every non-trivial blocking set B of cardinality $|B| < q + q^{2/3} + 1$ contains a Baer subplane.*

5. *([167]) In $PG(2,q)$, $q = p^2$, p prime, every non-trivial blocking set B of cardinality $|B| < 3(q+1)/2$ contains a Baer subplane.*

6. *([150]) If $q = p^3$, p prime, $p \geq 7$, then small minimal non-trivial blocking sets in $PG(2,p^3)$ have size $p^3 + p^2 + 1$ or $p^3 + p^2 + p + 1$ and they are of Rédey type.*

Theorem 9.4. *Consider the Gaolis plane $PG(2,q^t)$.*

1. *([147]) For the size of a linear blocking set B we have $|B| \leq q^t + q^{t-1} + \ldots + q + 1$.*

2. *([126]) There are at least two non-isomorphic blocking sets of cardinality $q^t + q^{t-1} + \ldots + q + 1$, for $t \geq 4$.*

3. *([127]) There are at least three non-isomorphic blocking sets of cardinality $q^t + q^{t-1} + 1$, for $t \geq 4$.*

4. *([147]) There are non-Rédey type blocking sets of size $q^t + q^{t-1} + \ldots + q^{t-r} + 1$, if $r \leq t - 2$.*

5. *([148]) Let B be a $GF(q)$-linear blocking set in $PG(2,q^4)$. If B is of Rédey type with at least two Rédey lines, then either B is a Baer subplane or B has $q^4 + q^3 + 1$ points, $q + 1$ Rédey lines and it is equivalent to the blocking set obtained from the graph of the trace function from $GF(q^4)$ to $GF(q)$. If B is of Rédey type with a unique Rédey line, then the possible sizes of B are $q^4 + q^3 + 1$ and $q^4 + q^3 + q^2 + cq + 1$ with $c = -1, 0, 1$. Finally, if B is not of Rédey type, then B has size $q^4 + q^3 + q^2 + dq + 1$, with $d = 0, 1$.*

Theorem 9.5. *([118] and [117]) In $PG(2,q)$, $q \geq 4$, there exists a minimal blocking set of size k, contained in the union of four lines, for every k $2q-1 \leq k \leq 3q-5$. There are minimal blocking sets of size $3q-4$ and $3q-3$ too.*

9.3 The algorithm

Our goal is to determine the full classification of blocking sets up to projective equivalence in $PG(2,q)$. To do this, an exhaustive search is obtained using a program of type B (see Chapter 3) since, as for saturating sets, blocking sets do not have any hereditary feature which can be used to prune the search space. Therefore we followed the same approach described in Section 8.3.

9.4 Some classifications

In the following subsections classifications for blocking sets in $PG(2,5)$ and $PG(2,7)$ are given. Moreover all the blocking sets in $PG(2,8)$ of sizes less than or equal to 16 is given. We denote $GF(5) = \{0,1,2,3,4\}$, $GF(7) = \{0,1,2,3,4,5,6\}$. Moreover we denote $GF(8) = \{0, 1 = \alpha^0, 2 = \alpha^1, \ldots, 8 = \alpha^6\}$ where α is a primitive element. This defines multiplication. For addition we use a primitive polynomial generating the field (x^3+x^2+1, [121]). In the following we give the classification of the minimal blocking set up to $PGL(3,q)$ if $q = p$ prime, or $P\Gamma L(3,q)$ if $q = p^h$ with $h > 1$.

9.4.1 $PG(2,5)$

Table 9.1 summarizes the spectrum of the non-equivalent blocking sets in $PG(2,5)$. In [16] is presented the theoretical construction of 6 blocking sets of size 10 in $PG(2,5)$, but one of these is not minimal. In particular the blocking set called $\mathcal{C}_4$ in [16] is constructed in the following way.

Let r and s be two lines of $PG(2,5)$ and $V = r \cap s$. Fix three points R_1, R_2, R_3 on r and three points S_1, S_2, S_3 on s different from V. The 7-set $\{V, R_1, R_2, R_3, S_1, S_2, S_3\}$ has four external lines e_1, e_2, e_3, e_4. Let $P = e_1 \cap e_2$, $Q = e_3 \setminus e_4$, $T = e_4 \setminus e_3$ such that P, Q, V are collinear and T is on the line PV. This blocking set $\mathcal{C}_4$ has no 5-secants and four 4-secants, but it is not minimal, since it contains a 9-blocking set. In fact let $Z \in \{R_1, R_2, R_3\} \setminus (PT \cup QT)$, then $\mathcal{C}_4 \setminus \{Z\}$ is a 9-blocking set.

In Table 9.2 for each size it is given the description of the stabilizer of the blocking sets. When minimal blocking sets of Rédey type exist, their number is indicated in bold font and the number of the rest of minimal blocking sets is indicated in plain font. In Table 9.3 the non-equivalent examples are described. G indicates the stabilizer of the blocking set in $PGL(3,5)$.

Table 9.1: Classification of minimal blocking sets in $PG(2,5)$

Size	# non-equivalent examples	reference
9	1	[28], [60]
10	5	[16]
11	1	[16]
12	1	[16]

Table 9.2: Stabilizer of minimal blocking sets in $PG(2,5)$

$k = 9$	G_{24}: **1**
$k = 10$	$\mathbb{Z}_2$: **2** $\quad$ $\mathbb{Z}_2 \times \mathbb{Z}_4$: **1*** $\quad$ $\mathcal{D}_6$: 1 $\quad$ G_{24}: **1**
$k = 11$	G_{20}: 1
$k = 12$	G_{96}: 1

*Unique example of minimal 10-blocking set with two Rédey lines.

Table 9.3: Non-equivalent minimal blocking sets in $PG(2,5)$

Size	Blocking set	G
9	1 1 0 0 1 0 1 0 1 1 0 1 0 0 1 0 1 1 1 0 0 1 1 1 1 0 0	G_{24}
10	1 1 0 0 0 1 1 0 1 1 1 0 1 0 1 1 0 1 1 0 1 0 0 1 1 0 1 0 0 0	$\mathcal{D}_6$
10	1 0 0 1 0 0 1 0 1 1 0 1 0 0 1 1 1 1 0 0 0 0 1 0 1 0 0 0 0 1	$\mathbb{Z}_2 \times \mathbb{Z}_4$
10	1 0 0 0 1 1 0 1 1 0 0 1 0 1 1 0 1 1 0 1 0 0 1 1 0 1 0 0 0 0	$\mathbb{Z}_2$
10	1 1 0 0 0 1 1 0 1 0 1 0 1 0 1 1 0 1 0 1 1 0 0 1 1 0 1 0 0 0	G_{20}
10	1 0 0 0 1 1 0 1 1 0 0 1 0 1 0 0 1 1 0 1 0 0 1 1 0 1 0 0 0 0	$\mathbb{Z}_2$
11	1 1 0 0 0 1 1 1 0 1 1 1 0 1 0 1 1 0 0 1 0 0 1 0 0 1 1 0 0 1 0 0 0	G_{20}
12	1 1 0 0 1 1 1 1 0 1 1 1 1 0 1 0 1 0 0 0 1 1 0 0 1 0 0 1 0 0 1 0 0 0 0 0	G_{96}

9.4.2 $PG(2,7)$

There exist two blocking sets with 12 points. One of them is the projective triangle; the other one is described in [75] or [27]. The IMI construction (see [117], [118]) gives blocking sets of sizes $13, 14, 15, 16, 17, 18$. There exists only one example of blocking set of size 19 (see [118]).

Table 9.4 summarizes the spectrum of the non-equivalent blocking sets in $PG(2,7)$. In Table 9.5 for each size it is given the description of the stabilizer of the blocking sets. When minimal blocking sets of Rédey type exist, their number is indicated in bold font and the number of the rest of minimal blocking sets is indicated in plain font. In Table 9.6 all the non-equivalent examples of blocking sets in $PG(2,7)$

of sizes 12, 13, 18, 19 are presented.

Table 9.4: Classification of minimal blocking sets in $PG(2,7)$

size	# non-equivalent examples
12	2
13	9
14	227
15	446
16	702
17	38
18	7
19	1

Table 9.5: Stabilizer of minimal blocking sets in $PG(2,7)$

$k=12$	G_{54}: **1**	G_{216}: 1			
$k=13$	$\mathbb{Z}_2$: **1**	$\mathbb{Z}_2 \times \mathbb{Z}_2$: 1+**1**	$\mathbb{Z}_6$: 1	$\mathcal{S}_3$: 1+**1**	$\mathcal{D}_4$: **1**
	$\mathcal{D}_6$: **1**	G_{24}: 1			
$k=14$	$\mathbb{Z}_1$: 101+**53**	$\mathbb{Z}_2$: 36+**18**	$\mathbb{Z}_3$: 1+**5**	$\mathbb{Z}_2 \times \mathbb{Z}_2$: 5	$\mathcal{Z}_6$: 1+**1**
	$\mathcal{S}_3$: 2	$\mathbb{Z}_2 \times \mathbb{Z}_6$: **1***	G_{18} : 1	G_{24} : 1	G_{42} : **1**
$k=15$	$\mathbb{Z}_1$: 402	$\mathbb{Z}_2$: 25	$\mathbb{Z}_3$: 12	$\mathbb{Z}_4$: 5	$\mathbb{Z}_6$: 1
	$\mathcal{Q}_6$:1				
$k=16$	$\mathbb{Z}_1$: 642	$\mathbb{Z}_2$: 49	$\mathbb{Z}_3$: 5	$\mathbb{Z}_2 \times \mathbb{Z}_2$: 3	$\mathbb{Z}_4$: 1
	$\mathbb{Z}_6$: 1	$\mathcal{S}_3$: 1			
$k=17$	$\mathbb{Z}_1$: 28	$\mathbb{Z}_2$: 2	$\mathbb{Z}_3$: 4	$\mathbb{Z}_6$: 3	$\mathcal{S}_3$: 1
$k=18$	$\mathbb{Z}_2$: 3	$\mathcal{S}_3$: 1	$\mathbb{Z}_3 \times \mathbb{Z}_3$: 1	$\mathcal{Q}_6$: 1	G_{216}: 1
$k=19$	G_{57}: 1				

*Unique example of minimal 14-blocking set with two Rédey lines.

Table 9.6: Non-equivalent minimal blocking sets in $PG(2,7)$ of sizes 12, 13, 18, 19

Size		Stabilizer
12	1 0 0 1 0 0 0 1 1 1 1 1 1 0 1 0 1 1 1 1 0 0 0 2 4 0 0 1 1 1 2 5 1 3 6 3 0	G_{54}
12	1 0 0 1 0 0 1 1 1 1 1 1 1 0 1 0 1 1 1 0 0 2 3 3 3 0 0 1 1 1 5 1 3 3 1 3 4	G_{216}
13	1 0 0 1 0 0 1 1 1 1 1 1 1 0 1 0 1 1 1 0 1 2 2 2 5 6 0 0 1 1 4 6 2 4 0 1 3 4 3	$\mathbb{Z}_2$
13	1 0 0 1 0 1 1 1 1 1 1 1 1 0 1 0 1 1 0 1 1 2 2 2 3 4 0 0 1 1 4 5 4 5 1 3 5 5 0	$\mathbb{Z}_2 \times \mathbb{Z}_2$
13	1 0 0 1 0 1 1 1 1 1 1 1 1 0 1 0 1 1 1 1 2 2 2 3 3 6 0 0 1 1 4 4 5 1 3 5 1 5 3	$\mathbb{Z}_2 \times \mathbb{Z}_2$
13	1 0 0 1 0 0 1 1 1 1 1 1 1 0 1 0 1 1 1 1 2 2 2 3 3 4 0 0 1 1 4 5 5 1 3 5 1 5 6	$\mathcal{S}_3$
13	1 0 0 1 0 0 0 1 1 1 1 1 1 0 1 0 1 1 1 1 1 1 2 2 3 3 0 0 1 1 2 4 5 4 5 1 3 1 5	$\mathcal{S}_3$
13	1 0 0 1 0 0 1 1 1 1 1 1 1 0 1 0 1 1 1 1 2 2 2 3 3 4 0 0 1 1 2 4 4 1 3 4 1 5 1	$\mathbb{Z}_6$
13	1 0 0 1 0 0 0 0 1 1 1 1 1 0 1 0 1 1 1 1 1 1 2 3 3 4 0 0 1 1 1 2 4 5 5 3 1 5 6	$\mathcal{D}_4$
13	1 0 0 1 0 1 1 1 1 1 1 1 1 0 1 0 1 1 0 0 1 2 2 2 2 2 0 0 1 1 4 1 2 5 0 1 2 3 5	$\mathcal{D}_6$

Size		Stabilizer
13	1 0 0 1 0 0 1 1 1 1 1 1 1 0 1 0 1 1 1 0 0 1 1 2 2 2 0 0 1 1 1 4 1 2 2 5 1 2 3	G_{24}
18	1 0 0 1 0 1 1 1 1 1 1 1 1 1 1 1 1 0 1 0 1 1 0 0 1 2 2 3 3 3 4 4 5 5 5 0 0 1 1 4 1 4 6 3 5 0 3 6 0 6 4 5 6	$\mathbb{Z}_2$
18	1 0 0 1 0 0 1 1 1 1 1 1 1 1 1 1 1 0 1 0 1 1 1 0 0 2 2 3 3 3 4 4 5 5 5 0 0 1 1 1 4 1 4 3 5 0 3 6 0 6 4 5 6	$\mathbb{Z}_2$
18	1 0 0 1 0 1 1 1 1 1 1 1 1 1 1 1 1 0 1 0 1 1 1 1 1 2 2 2 3 3 3 4 5 5 5 0 0 1 1 4 0 2 6 1 2 3 1 3 6 6 2 4 6	$\mathbb{Z}_2$
18	1 0 0 1 0 0 0 1 1 1 1 1 1 1 1 1 1 0 1 0 1 1 1 1 1 2 2 2 3 3 4 4 5 5 0 0 1 1 1 2 4 0 5 3 4 5 0 6 3 6 4 6	$\mathcal{S}_3$
18	1 0 0 1 0 0 1 1 1 1 1 1 1 1 1 1 1 0 1 0 1 1 1 0 0 1 2 2 2 3 4 4 5 5 5 0 0 1 1 2 4 1 4 2 0 2 3 6 0 6 1 4 6	$\mathbb{Z}_3 \times \mathbb{Z}_3$
18	1 0 0 1 0 0 1 1 1 1 1 1 1 1 1 1 1 0 1 0 1 1 1 0 0 1 1 2 2 3 4 4 5 5 5 0 0 1 1 1 4 2 4 0 2 2 3 6 0 6 1 4 6	$\mathcal{Q}_6$
18	1 0 0 1 0 0 0 0 1 1 1 1 1 1 1 1 1 0 1 0 1 1 1 1 1 0 1 2 2 3 3 4 4 5 5 0 0 1 1 1 2 4 6 5 5 3 4 0 1 3 6 4 6	G_{216}
19	1 0 0 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 0 1 1 0 0 1 1 2 2 2 3 3 4 4 4 5 5 0 0 1 1 4 4 5 5 6 0 1 3 5 6 1 3 4 3 4	G_{57}

9.4.3 $PG(2,8)$

There exists a unique blocking set with 13 points (see [106]). There is no minimal blocking sets of size 14 (see [4]), the IMI construction (see [117], [118]) gives blocking sets of sizes $15, 16, 17, 18, 19, 20, 21$. In [3] is presented the construction of minimal blocking sets of size $22, 23$.

Table 9.7 summarizes the classification of the non-equivalent blocking sets in $PG(2,8)$ of size ≤ 17. In

Table 9.8 for each size it is given the description of the stabilizer of the blocking sets. When minimal blocking sets of Rédey type exist, their number is indicated in bold font and the number of the rest of minimal blocking sets is indicated in plain font. In Table 9.9 all the non-equivalent examples of blocking sets in $PG(2,8)$ of sizes 13, 15, and the blocking sets of size 16 having stabilizer of size greater than 3 are presented.

Table 9.7: Classification of minimal blocking sets in $PG(2,8)$ of size ≤ 17

size	# non-equivalent examples
13	1
14	0
15	17
16	852
17	6156

Table 9.8: Stabilizer of minimal blocking sets in $PG(2,8)$ of size ≤ 17

$k=13$	G_{288}: **1**				
$k=15$	$\mathbb{Z}_1$: 1	$\mathbb{Z}_2$: 2+**2**	$\mathbb{Z}_3$: 1+**1**	$\mathbb{Z}_2 \times \mathbb{Z}_2$: **1**	$\mathcal{S}_3$: 1
	$\mathbb{Z}_6$: **2**	G_{21}: **1**	G_{24}: 2+**1**	G_{42}: **1**	G_{168}: **1**
$k=16$	$\mathbb{Z}_1$: 547+**210**	$\mathbb{Z}_2$: 61+**3**	$\mathbb{Z}_3$: 7+**21**	$\mathbb{Z}_2 \times \mathbb{Z}_2$: 1	$\mathcal{Z}_6$: **1**
	G_{42}: **1***				
$k=17$	$\mathbb{Z}_1$: 6004	$\mathbb{Z}_2$: 102	$\mathbb{Z}_3$: 31	$\mathbb{Z}_2 \times \mathbb{Z}_2$: 9	$\mathcal{Z}_4$: 3
	$\mathcal{Z}_6$: 4	$\mathcal{Z}_{12}$: 1	G_{24}: 1	G_{96}: 1	

*Unique example of minimal 16-blocking set with two Rédey lines.

9.4.4 $PG(2,9)$

There exists a unique blocking set with 13 points which is a Baer subplane. There is no minimal blocking sets of size 14 (see [33]), the IMI construction (see [117], [118]) gives blocking sets of sizes

Table 9.9: Non-equivalent minimal blocking sets in $PG(2,8)$ of sizes 13, 15 and of size 16 with stabilizer of size greater than 3

Size		Stabilizer
13	1 0 0 1 0 1 1 1 1 1 1 1 1 0 1 0 1 1 0 0 0 1 3 3 7 7 0 0 1 1 2 1 3 6 6 1 3 0 1	G_{288}
15	1 0 0 1 0 0 1 1 1 1 1 1 1 1 1 0 1 0 1 1 1 0 0 3 4 5 5 5 6 6 0 0 1 1 1 2 3 6 3 6 0 5 6 6 7	$\mathbb{Z}_1$
15	1 0 0 1 0 0 0 1 1 1 1 1 1 1 1 0 1 0 1 1 1 1 0 3 3 5 5 6 6 7 0 0 1 1 1 2 4 3 3 5 4 5 5 7 0	$\mathbb{Z}_2$
15	1 0 0 1 0 0 0 1 1 1 1 1 1 1 1 0 1 0 1 1 1 1 0 1 2 3 3 3 5 6 0 0 1 1 1 2 4 3 3 5 1 3 5 5 7	$\mathbb{Z}_2$
15	1 0 0 1 0 0 0 1 1 1 1 1 1 1 1 0 1 0 1 1 1 1 0 3 3 5 5 6 6 7 0 0 1 1 1 2 4 3 1 3 5 6 6 7 7	$\mathbb{Z}_2$
15	1 0 0 1 0 0 0 0 1 1 1 1 1 1 1 0 1 0 1 1 1 1 1 0 0 3 5 6 7 7 0 0 1 1 1 2 4 5 3 7 3 5 7 0 7	$\mathbb{Z}_2$
15	1 0 0 1 0 0 0 0 1 1 1 1 1 1 1 0 1 0 1 1 1 1 1 0 1 3 3 5 6 7 0 0 1 1 1 2 3 4 3 3 3 5 4 7 0	$\mathbb{Z}_3$
15	1 0 0 1 0 0 1 1 1 1 1 1 1 1 1 0 1 0 1 1 1 0 2 3 5 5 6 6 6 6 0 0 1 1 1 2 3 3 3 5 6 3 5 6 7	$\mathbb{Z}_3$
15	1 0 0 1 0 0 1 1 1 1 1 1 1 1 1 0 1 0 1 1 1 0 0 3 3 4 4 6 7 7 0 0 1 1 2 4 1 3 3 5 2 7 7 0 3	$\mathbb{Z}_2 \times \mathbb{Z}_2$
15	1 0 0 1 0 1 1 1 1 1 1 1 1 1 1 0 1 0 1 1 0 0 0 1 3 3 5 5 6 6 0 0 1 1 2 1 3 6 5 3 7 0 5 6 7	$\mathcal{S}_3$
15	1 0 0 1 0 0 1 1 1 1 1 1 1 1 1 0 1 0 1 1 1 0 3 3 3 5 5 5 6 7 0 0 1 1 2 4 3 3 4 5 0 4 5 7 0	$\mathbb{Z}_6$

Size		Stabilizer
15	1 0 0 1 0 0 1 1 1 1 1 1 1 1 1 0 1 0 1 1 1 0 0 3 5 5 6 6 6 7 0 0 1 1 1 2 3 6 3 5 6 5 6 7 7	$\mathbb{Z}_6$
15	1 0 0 1 0 0 1 1 1 1 1 1 1 1 1 0 1 0 1 1 1 0 0 1 1 3 3 4 6 7 0 0 1 1 2 4 2 3 0 2 3 5 2 7 0	G_{21}
15	1 0 0 1 0 0 0 0 0 1 1 1 1 1 1 0 1 0 1 1 1 1 1 1 0 3 4 4 6 7 0 0 1 1 1 2 3 4 6 3 5 2 7 7 0	G_{24}
15	1 0 0 1 0 0 1 1 1 1 1 1 1 1 1 0 1 0 1 1 1 0 0 3 4 6 7 7 7 7 0 0 1 1 2 4 1 3 3 7 7 0 1 3 7	G_{24}
15	1 0 0 1 0 0 0 1 1 1 1 1 1 1 1 0 1 0 1 1 1 1 0 0 0 3 4 6 7 7 0 0 1 1 1 2 4 1 3 7 3 7 7 0 7	G_{24}
15	1 0 0 1 0 1 1 1 1 1 1 1 1 1 1 0 1 0 1 1 0 0 0 0 0 1 3 3 6 6 0 0 1 1 2 1 2 3 6 7 0 3 6 2 7	G_{42}
15	1 0 0 1 0 1 1 1 1 1 1 1 1 1 1 0 1 0 1 1 0 1 2 2 5 5 6 6 7 7 0 0 1 1 2 3 2 0 3 6 7 6 7 1 2	G_{168}
16	1 0 0 1 0 1 1 1 1 1 1 1 1 1 1 1 0 1 0 1 1 0 0 1 3 4 5 6 7 7 7 7 0 0 1 1 2 1 3 2 3 4 4 7 0 1 2 7	$\mathbb{Z}_2 \times \mathbb{Z}_2$
16	1 0 0 1 0 0 0 0 0 0 1 1 1 1 1 1 0 1 0 1 1 1 1 1 1 1 0 3 3 4 5 6 0 0 1 1 1 2 3 4 6 7 3 5 6 7 1 7	$\mathbb{Z}_6$
16	1 0 0 1 0 0 0 0 0 0 1 1 1 1 1 1 0 1 0 1 1 1 1 1 1 1 0 3 4 5 6 7 0 0 1 1 1 2 3 4 6 7 3 5 2 4 7 0	G_{42}

15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26. There exist only 2 minimal 15-blocking sets (see [137]). There exists no minimal blocking set of size 27 (see [105]). The minimal blocking set of size 28 are the unitals. Table 9.10 summarizes the classification of the non-equivalent blocking sets in $PG(2,9)$ of size ≤ 16. In

Table 9.11 for each size it is given the description of the stabilizer of the blocking sets. When minimal blocking sets of Rédey type exist, their number is indicated in bold font and the number of the rest of minimal blocking sets is indicated in plain font. In Table 9.12 all the non-equivalent examples of blocking sets in $PG(2,9)$ of sizes 13, 15 and 16 are presented.

Table 9.10: Classification of minimal blocking sets in $PG(2,9)$ of size ≤ 16

size	# non-equivalent examples
13	1
14	0
15	2
16	3

Table 9.11: Stabilizer of minimal blocking sets in $PG(2,9)$ of size ≤ 16

$k=13$	G_{11232}: **1**		
$k=15$	G_{120}: 1	G_{192}: **1**	
$k=16$	$\mathbb{S}_3$: **1**	G_{16}: 1	G_{72}: **1**

9.4.5 Blocking sets of Rédey type for $q \leq 11$

In this section the classification of minimal blocking sets of Rédey type in $PG(2,q)$, with $5 \leq q \leq 11$, is given. Table 9.13 gives the description of the stabilizer of the blocking sets of Rédey type. In Table 9.14 the blocking sets of Rédey type of size $18, 19, 20$ in $PG(2,11)$ are presented.

Table 9.12: Non-equivalent minimal blocking sets in $PG(2,9)$ of sizes 13, 15 and 16

Size		Stabilizer
14	1 0 0 1 0 0 1 1 1 1 1 1 1 0 1 0 1 1 1 0 0 1 1 5 5 5 0 0 1 1 1 5 1 5 0 5 0 1 5	G_{11232}
15	1 0 0 1 0 0 0 1 1 1 1 1 1 1 1 0 1 0 1 1 1 1 0 1 1 1 2 2 3 8 0 0 1 1 2 4 7 7 0 4 7 0 8 1 0	G_{120}
15	1 0 0 1 0 0 0 0 1 1 1 1 1 1 1 0 1 0 1 1 1 1 1 0 1 5 6 6 8 8 0 0 1 1 1 2 4 5 5 0 0 0 7 0 3	G_{192}
16	1 0 0 1 0 0 1 1 1 1 1 1 1 1 1 0 1 0 1 1 1 0 1 1 2 2 2 2 5 6 7 0 0 1 1 2 7 3 0 7 0 5 7 8 8 0 5	$\mathcal{S}_3$
16	1 0 0 1 0 0 0 1 1 1 1 1 1 1 1 1 0 1 0 1 1 1 1 0 0 1 2 2 2 4 5 7 0 0 1 1 2 4 6 7 8 4 5 7 8 7 8 4	G_{16}
16	1 0 0 1 0 1 1 1 1 1 1 1 1 1 1 1 0 1 0 1 1 1 1 1 1 1 2 2 4 4 6 8 0 0 1 1 2 0 2 4 7 8 0 8 0 4 0 0	G_{72}

Table 9.13: Blocking sets of Rédey type in $PG(2,p)$, with $5 \leq p \leq 11$

$PG(2,5)$	$k=9$	G_{24}: **1**				
	$k=10$	$\mathbb{Z}_2$: **2**	$\mathbb{Z}_2 \times \mathbb{Z}_4$: $\mathbf{1}^*$	G_{24}: **1**		
$PG(2,7)$	$k=12$	G_{54}: **1**				
	$k=13$	$\mathbb{Z}_2$: **1**	$\mathbb{Z}_2 \times \mathbb{Z}_2$: **1**	$\mathcal{S}_3$: **1**	$\mathcal{D}_4$: **1**	$\mathcal{D}_6$: **1**
	$k=14$	$\mathbb{Z}_1$: **53**	$\mathbb{Z}_2$: **18**	$\mathbb{Z}_3$: **5**	$\mathcal{Z}_6$: **1**	$\mathbb{Z}_2 \times \mathbb{Z}_6$: **1**
		G_{42} : **1**				
$PG(2,8)$	$k=13$	G_{288}: **1**				
	$k=15$	$\mathbb{Z}_2$: **2**	$\mathbb{Z}_3$: **1**	$\mathbb{Z}_2 \times \mathbb{Z}_2$: **1**	$\mathbb{Z}_6$: **2**	G_{21}: **1**
		G_{24}: **1**	G_{42}: **1**	G_{168}: **1**		
	$k=16$	$\mathbb{Z}_1$: 547+**210**	$\mathbb{Z}_2$: 61+**3**	$\mathbb{Z}_3$: 7+**21**	$\mathbb{Z}_2 \times \mathbb{Z}_2$: 1	$\mathcal{Z}_6$: **1**
		G_{42}: $\mathbf{1}^*$				
$PG(2,9)$	$k=13$	G_{11232}: **1**				
	$k=15$	G_{192}: **1**				
	$k=16$	$\mathcal{S}_3$: **1**	G_{72}: **1**			
	$k=17$	$\mathbb{Z}_1$: **4**	$\mathbb{Z}_2$: **21**	$\mathbb{Z}_4$: **1**	$\mathbb{Z}_2 \times \mathbb{Z}_2$: **6**	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$: **1**
		$\mathcal{D}_4$: **1**	$\mathcal{D}_6$: **1**	G_{16}: **2**	G_{32}: **1**	
	$k=18$	$\mathbb{Z}_1$: **3988**	$\mathbb{Z}_2$: **236**	$\mathbb{Z}_3$: **3**	$\mathbb{Z}_2 \times \mathbb{Z}_2$: **15**	$\mathbb{Z}_4$: **20**
		$\mathcal{S}_4$: **3**	$\mathbb{Z}_6$: **2**	$\mathcal{D}_4$: **3**	$\mathcal{Q}_8$:**2**	$\mathcal{D}_6$: **2**
		G_{16} : **2**	G_{18} : **1**	G_{144} : **1**		
$PG(2,11)$	$k=18$	G_{150}: **1**				
	$k=19$	$\mathbb{Z}_2 \times \mathbb{Z}_2$: **1**	$\mathcal{S}_3$: **1**			
	$k=20$	$\mathbb{Z}_1$: **3**	$\mathbb{Z}_2$: **2**			
	$k=21$	$\mathbb{Z}_1$: **1473**	$\mathbb{Z}_2$: **310**	$\mathbb{Z}_2 \times \mathbb{Z}_2$: **27**	$\mathbb{Z}_5$: **2**	$\mathcal{D}_4$: **1**
		$\mathbb{Z}_{10}$: **1**	$\mathcal{D}_5$: **2**	G_{20} : **1**		

Table 9.14: Blocking sets of Rédey type of size $18, 19, 20$ in $PG(2, 11)$

Size		Stabilizer
18	1 0 0 1 0 1 0 1 0 1 1 1 0 1 1 1 0 1 0 1 0 10 1 9 1 9 1 3 6 10 1 6 1 0 1 1 0 0 1 1 2 0 9 9 5 3 6 10 1 10 9 6 3 1	G_{150}
19	1 1 1 1 1 0 1 0 1 1 1 0 1 1 1 0 1 1 1 6 0 1 2 1 1 5 0 0 1 4 1 0 1 9 1 2 2 1 9 0 0 1 7 0 1 1 6 1 0 9 7 9 7 8 2 9 10	$\mathbb{Z}_2 \times \mathbb{Z}_2$
20	1 0 1 1 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 3 3 0 1 2 0 9 0 5 8 0 0 1 6 2 0 1 6 0 0 6 8 1 6 1 8 0 1 7 8 9 6 2 1 9 7 1 3	$\mathbb{Z}_1$
20	1 0 1 0 1 1 1 1 0 1 1 1 1 1 1 1 1 0 1 0 1 3 0 4 7 7 5 1 9 1 0 1 3 1 1 2 2 1 1 0 0 8 1 2 4 7 9 2 0 4 1 8 4 9 2 9 3 8 1	$\mathbb{Z}_1$
20	1 0 1 0 1 1 1 1 1 1 1 0 1 1 1 1 1 0 1 1 0 1 3 0 0 3 3 1 2 1 5 1 9 6 2 3 4 1 2 2 0 0 3 1 10 4 9 4 3 1 5 2 1 3 6 6 0 4 5 9	$\mathbb{Z}_1$
20	1 0 0 1 1 1 1 1 0 1 0 1 1 0 1 1 1 1 1 1 0 1 0 3 1 7 1 10 1 5 1 0 3 1 2 1 2 2 4 2 0 0 1 4 4 8 1 0 10 5 2 4 6 4 1 9 5 9 1 7	$\mathbb{Z}_2$
20	1 1 1 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 2 1 1 0 6 0 4 1 7 6 3 4 1 2 3 9 0 1 0 0 1 0 1 1 0 6 1 1 4 7 9 8 2 9 4 2 1 2	$\mathbb{Z}_2$

Bibliography

[1] V. Abatangelo and B. Larato, *Complete caps in $PG(3,q)$ with q odd*, Discrete Math. **308** (2008), 184-187.

[2] V. Abatangelo, *A class of complete $[(q+8)/3]$-arcs of $PG(2,q)$, with $q=2^h$ and h (≥ 6) even*, Ars Combinatoria **16** (1983) 103-111.

[3] J. Barát, S. Innamorati, *Largest minimal blocking sets in $PG(2,8)$*, Journal of Comb. Designs **11** (2003), 162-169.

[4] J. Barát, A. Del Fra, S. Innamorati and L. Storme, *Minimal blocking sets in $PG(2,8)$ and maximal partial spreads in $PG(3,8)$*, Designs, Codes and Cryptography (2004), 15-26.

[5] A. Barlotti, *Un'estensione del teorema di Segre-Kustaanheimo*, Bollettino dell'Unione Matematica Italiana **10** (1955), 498-506.

[6] D. Bartoli, *Quantum codes and related geometric properties* (in Italian), Degrees Thesis (2008), Università degli Studi di Perugia.

[7] D. Bartoli, J. Bierbrauer, S. Marcugini and F. Pambianco, *Geometric constructions of quantum codes*, Error-Correcting Codes, Finite Geometries and Cryptography, AMS, Series: Contemporary Mathematics 523, Eds. Aiden A. Bruen and David L. Wehlau (2010), 149-154.

[8] D. Bartoli, J. Bierbrauer, G. Faina, Y. Edel, S. Marcugini and F. Pambianco, *The structure of quaternary quantum caps*, preprint.

[9] D. Bartoli, A. A. Davydov, G. Faina, S. Marcugini and F. Pambianco, *Upper on the smallest size of a complete arc in the plane $PG(2,q)$*, http://arxiv.org/abs/1111.3403.

[10] D. Bartoli, A. A. Davydov, S. Marcugini and F. Pambianco, *The minimum order of complete caps in $PG(4,4)$*, Advances in Mathematics of Communications **5** (2011), 37-40.

[11] D. Bartoli, A.A. Davydov, G. Faina, S. Marcugini, F. Pambianco, *On sizes of complete arcs in* $PG(2,q)$, Discrete Math. **312** (2012), 680-698.

[12] D. Bartoli, G. Faina, S. Marcugini, and F. Pambianco, *New quantum caps in* $PG(4,4)$, submitted.

[13] D. Bartoli, S. Marcugini, and F. Pambianco, *A computer based classification of caps in* $PG(3,4)$, Rapporto Tecnico 8/2009, Dipartimento di Matematica e Informatica, Università degli Studi di Perugia, Perugia, Italy.

[14] D. Bartoli, S. Marcugini, and F. Pambianco, *The maximum and the minimum size of complete* $(n,3)$*-arcs in* $PG(2,16)$, (2012), http://arxiv.org/abs/1201.2260.

[15] D. Bartoli, S. Marcugini, and F. Pambianco, *On complete* $(n,3)$*-arcs in* $PG(2,q)$*, with* $q \geq 17$, (2012), preprint.

[16] L. Berardi and S. Innamorati, *Irreducible blocking sets in the projective plane of order five*, Atti Sem. Mat. Fis. Univ. Modena **38**, (1990), 293-311.

[17] A. Beutelspacher and U. Rosenbaum, *Projective Geometry*, in Foundations to Applications, Cambridge University Press, Cambridge, (1998).

[18] J. Bierbrauer, *Introduction to Coding Theory*, CHAPMAN & HALL/CRC (2005).

[19] J.Bierbrauer and Y. Edel, *41 is the Largest Size of a Cap in* $PG(4,4)$, Designes, Codes and Cryptography **16** (1999), 151-160.

[20] J.Bierbrauer and Y. Edel, *The largest cap in* $AG(4,4)$ *and its uniqueness*, Des. Codes Cryptogr. **29** (2003), 99-104.

[21] J. Bierbrauer and Y. Edel: *Quantum twisted codes,* Journal of Combinatorial Designs **8** (2000), 174-188.

[22] J. Bierbrauer and Y. Edel: *Large caps in projective Galois spaces,* Current research topics in Galois geometry, J. de Beule and L. Storme (eds), Nova Science Publishers (2010), 81-94.

[23] J. Bierbrauer, G. Faina, M. Giulietti, S. Marcugini and F. Pambianco, *The geometry of quantum codes*, Innov. Incidence Geom. **6/7** (2007/2008), 53-71.

[24] J. Bierbrauer, G. Faina, S. Marcugini and F. Pambianco, *On the structure of the (n, r)-arcs in $PG(2, q)$*, Proceedings of the Tenth International Workshop on Algebraic and Combinatorial Coding Theory, Zvenigorod, Russia, 3-9 September 2006, 19-23.

[25] J. Bierbrauer and J. Fridich, *Constructing good covering codes for applications in steganography*, in Transactions on data hiding and multimedia security III, Springer-Verlag (2008), 1-22.

[26] J. Bierbrauer, S. Marcugini and F. Pambianco, *The smallest size of a complete cap in $PG(3, 7)$*, Discrete Math. **306** (2006), 1257-1263.

[27] A. Blokhuis, *On the size of a blocking set in $PG(2, p)$*, Combinatorica **14** (1994), 111-114.

[28] A. Blokhuis, *Blocking sets in Desarguesian planes*, Paul Erdősh is eighty, Bolyai Soc. Math. Studies, (1996), 273-276.

[29] A. Blokhuis, L. Storme and T. Szőnyi, *Lacunary polynomials, multiple blocking sets and Baer subplanes*, J. London Math. Soc. (2) **60** (1999), 321-332.

[30] R. C. Bose, *On some connections between the design of experiments and information theory*, Bull. Inst. Internat. Statis. **38** (1961), 257-271.

[31] M. Braun, A. Kohnert and A. Wassermann, *Construction of linear codes with prescribed distance*, OC05 The fourth International Workshop on Optima Codes and related Topics, PAMPOROVO, Bulgaria (2005), 59-63.

[32] A.A. Bruen, *Baer subplanes and blocking sets*, Bull. Amer. Math. Soc. **76** (1970), 342-344.

[33] A. A. Bruen and J. A. Thas, *Blocking sets*, Geom. Dedicata **6** (1977), 193-203.

[34] E. Çakçak and F. Özbudak, *Subfields of the function field of the Deligne–Lusztig curve of Ree type*, Acta Arith. **115** (2004), 133-180.

[35] A. R. Calderbank, E. M. Rains , P. M. Shor and N. J. A. Sloane, *Quantum error correction via codes over $GF(4)$*, IEEE Transactions on Information Theory **44** (1998), 1369-1387.

[36] A. R. Calderbank and P. M. Shor, *Good quantum error correcting codes exist*, Phys. Rev. **A 54** (1996), 1098-1105.

[37] G. Chen, D. Church, B.-G. Englert, C. Henkel, B. Rohwedder, M.O. Scully and M. S. Zubairy, *Quantum computing devices: princicples, designes and analysis*, CHAPMAN & HALL/CRC Applied Mathematics and Non Linear Science Series (2007).

[38] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering Codes.* North-Holland, Amsterdam, (1997).

[39] G. R. Cook, *Arcs in a Finite Projective Plane*, PhD Thesis, available on internet http://sro.sussex.ac.uk/

[40] K. Coolsaet, H. Sticker, *Arcs with large conical subsets*, Electr. J. Combin. **17** (2010).

[41] K. Coolsaet, H. Sticker, *The complete* $(k, 3)$*-arcs of* $PG(2, q)$*,* $q \leq 13$, Journal of Combinatorial Designs **20** (2012), 89-111.

[42] A. A. Davydov, *Constructions and families of covering codes and saturated sets of points in projective geometry*, IEEE Trans. Inform. Theory , **41** (1995), 2071-2080.

[43] A. A. Davydov, *Constructions and families of nonbinary linear codes with covering radius* 2, IEEE Trans. Inform. Theory , **45** (1999), 1679-1686.

[44] A. A. Davydov, G. Faina, S. Marcugini and F. Pambianco, *On Sizes of Complete Caps in Projective Spaces* $PG(n, q)$ *and Arcs in Planes* $PG(2, q)$, Journal of Geometry, **94** (2009), 31-58.

[45] A. A. Davydov, S. Marcugini and F. Pambianco, *Complete caps in projective spaces* $PG(n, q)$, J. Geom. **80** (2004) 23-30.

[46] A. A. Davydov, S. Marcugini and F. Pambianco, *Linear codes with covering radius* 2*,* 3 *and saturating sets in projective geometry*, IEEE Transactions on Information Theory III **20**, (2004) 537-541.

[47] A. A. Davydov, S. Marcugini, and F. Pambianco, *On Saturating Sets in Projective Spaces*, J. Comb. Theory Ser. A. **103** (2003), 1-15.

[48] A. A. Davydov and P. R. J. Östergard, *On saturating sets in small projective geometries*, European J. Combin. **21** (2000), 563-570.

[49] A.A. Davydov, G. Faina, S. Marcugini and F. Pambianco, *Computer search in projective planes for the sizes of complete arcs*, J. Geom. **82** (2005), 50-62.

[50] A.A. Davydov, G. Faina, S. Marcugini and F. Pambianco, *On the spectrum of sizes of complete caps in projective spaces $PG(n,q)$ of small dimension*, in Proc. XI Int. Workshop on Algebraic and Combin. Coding Theory, ACCT2008, Pamporovo, Bulgaria, (2008), 57-62. http://www.moi.math.bas.bg/acct2008/b10.pdf

[51] A.A. Davydov, G. Faina, S. Marcugini and F. Pambianco, *On sizes of complete caps in projective spaces $PG(n,q)$ and arcs in planes $PG(2,q)$*, J. Geom. **94** (2009), 31-58.

[52] A.A. Davydov, G. Faina, S. Marcugini and F. Pambianco, *New sizes of complete arcs in $PG(2,q)$*, in Proc. XII Int. Workshop on Algebraic and Combin. Coding Theory, ACCT2010, Novosibirsk, Russia, (2010), 103-108.

[53] A.A. Davydov, G. Faina, S. Marcugini and F. Pambianco, *New sizes of complete arcs in $PG(2,q)$*. http://arxiv.org/PS_cache/arxiv/pdf/1004/1004.2817v5.pdf

[54] A.A. Davydov, M. Giulietti, S. Marcugini and F. Pambianco, *On sharply transitive sets in $PG(2,q)$*, Innov. Incid. Geom. **6-7** (2009), 139-151.

[55] A.A. Davydov, M. Giulietti, S. Marcugini and F. Pambianco, *New inductive constructions of complete caps in $PG(N,q)$, q even*, J. Combin. Des. **18** (2010), 176-201.

[56] A.A. Davydov, M. Giulietti, S. Marcugini and F. Pambianco, *Linear nonbinary covering codes and saturating sets in projective spaces*, Advanc. Math. Commun. **5** (2011), 119-147.

[57] A.A. Davydov, S. Marcugini and F. Pambianco, *Complete $(q^2+q+8)/2$-caps in the spaces $PG(3,q)$, $q \equiv 2 \pmod 3$ an odd prime, and a complete 20-cap in $PG(3,5)$*, Des. Codes Cryptogr. **50** (2009), 359-372.

[58] A.A. Davydov, S. Marcugini and F. Pambianco, *A geometric construction of complete arcs sharing $(q+3)/2$ points with a conic*, in Proc. XII Int. Workshop on Algebraic and Combin. Coding Theory, ACCT2010, Novosibirsk, Russia (2010), 109-115.

[59] D. Deutsch, *Quantum theory, the Church-Turing principle and the universal quantum computer*, Proc. R. Soc. Lond. A 400, **97** (1985).

[60] J. Di Paola, *On minimum blocking coalitions in small projective plane games*, SIAM J. Appl. Math. **17** (1969), 378-392.

[61] Y. Edel, Yves Edel's home page, http://www.mathi.uni-heidelberg.de/ yves/

[62] Y. Edel, L. Storme and P. Sziklai, *New upper bounds on the sizes of caps in $PG(N,5)$ and $PG(N,7)$*, J. Combin. Math. Combin. Comput. **60** (2007), 7-32.

[63] F.A.B. Edoukou, *Codes correcteurs d'erreurs construits à partir des variétés algébriques*, PhD Thesis, Université de la Méditerranée Aix-Marseille II (2007).

[64] F.A.B. Edoukou, A. Hallez, F. Rodier, and L. Storme, *On the small weight codewords of the functional codes C_{herm}(X), X a non-singular Hermitian variety*, Des. Codes Cryptogr. **56** (2010), 219-233.

[65] F.A.B. Edoukou, A. Hallez, F. Rodier and L. Storme, *A study of intersections of quadrics having applications on the small weight codewords of the functional codes $C_2(Q)$, Q a non-singular quadric*, J. Pure Applied Algebra **214** (2010), 1729-1739.

[66] F.A.B. Edoukou, S. Ling and C. Xing, *Structure of functional codes defined on non-degenerate Hermitian varieties*, J. Combin. Theory, Ser. A **118** (2011), 2436-2444.

[67] G. Faina, S. Marcugini, A. Milani, and F. Pambianco, *The size k of the complete k-caps in $PG(n,q)$ for small q and $3 \leq n \leq 5$*, Ars Combinatoria **50** (1998), 235-243.

[68] G. Faina, *Complete k-caps in $PG(3,q)$ with $k < (q^2+q+4)/2$*, Ars Combin. **33** (1992), 311-317.

[69] G. Faina and F. Pambianco, *A class of complete k-caps in $PG(3,q)$ for q an odd prime*, J. Geom. **57** (1996), 93-105.

[70] G. Faina and F. Pambianco, *Small complete caps in $PG(r,q)$, $r \geq 3$*, Discrete Math. **174** (1997), 117-123.

[71] G. Faina and F. Pambianco, *On the spectrum of the values k for which a complete k-cap in $PG(n,q)$ exists*, J. Geom. **62** (1998), 84-98.

[72] G. Faina and M. Giulietti, *On small dense arcs in Galois planes of square order*, Discrete Math **267** (2003), 113-125.

[73] G. Faina and F. Pambianco, *On some* 10*-arcs for deriving the minimum order for complete arcs in small projective planes*, Discrete Math. **208-209** (1999), 261-271.

[74] R. P. Feynman, *Quantum mechanical computers*, Foundations of Physics, (1986).

[75] A . Gács, P. Sziklai and T. Szőnyi, *Two remarks on blocking sets and nuclei in planes of prime order*, Designs, Codes and Cryptography **10** (1997), 29-39.

[76] V. Giordano, *Arcs in cyclic affine planes*, Innov. Incid. Geom. **6-7** (2009), 203-209.

[77] M. Giulietti, *Small complete caps in $PG(2,q)$ for q an odd square*, J. Geom. **69** (2000), 110-116.

[78] M. Giulietti, *Small complete caps in Galois affine spaces*, J. Algebraic. Combin. **25** (2007), 149-168.

[79] M. Giulietti, *Small complete caps in $PG(N,q)$, q even*, J. Combin. Des. **15** (2007), 420-436.

[80] M. Giulietti, G. Korchmáros, S. Marcugini and F. Pambianco, *Arcs in $PG(2,q)$ left invariant by A_6*, Designs, Codes and Cryptography , to appear.

[81] M. Giulietti and E. Ughi, *A small complete arc in $PG(2,q)$, $q=p^2$, $p \equiv 3$ (mod 4)*, Discrete Math. **208-209** (1999), 311-318.

[82] M. Giulietti, G. Korchmáros and F. Torres, *Quotient curves of the Deligne-Lusztig curve of Suzuki type*, Acta Arith. **122** (2006), 245-274.

[83] D. G. Glynn, T. A. Gulliver, J. G. Maks and M. K. Gupta, *The Geometry of Additive Quantum Codes*, http://www.maths.adelaide.edu.au/rey.casse/DavidGlynn/QMonoDraft.pdf.

[84] M. Grassl, *Bounds on the minimum distance of linear codes*, http://www.codetables.de.

[85] R. Guralnick, B. Malmskog and R. Pries, *The automorphism groups of a family of maximal curves*, arXiv:1105.3952.

[86] A. Hallez and L. Storme, *Functional codes arising from quadric intersection with Hermitian varieties*, Finite Fields Appl. **16** (2010), 27-35.

[87] J.P. Hansen and J.P. Pedersen, *Automorphism group of Ree type, Deligne-Lusztig curves and function fields*, J. Reine Angew. Math. **440** (1993), 99-109.

[88] A. Hartman, L. Raskin, *Problems and algorithms for covering arrays*, Discrete Math. **284** (2004), 149-156.

[89] A. Hefez, *Non-reflexive curves*, Composition Math. **69** (1989), 3-35.

[90] H.W. Henn, *Funktionenkörper mit groβer Automorphismengruppe*, J. Reine Angew. Math. **302** (1978), 96-115.

[91] R. Hill, Caps and codes, *Discrete Mathematics* **22** (1978), 111-137.

[92] J. W. P. Hirschfeld, *Caps in elliptic quadrics*, in: Combinatorics '81, Ann. Discrete Math. **18** North-Holland, Amsterdam, 1983 (Rome, 1981), 449-466.

[93] J.W.P. Hirschfeld, *Maximum sets in finite projective spaces*, in: Lloyd, E.K. (Ed.): Surveys in Combinatorics, London Math. Soc. Lecture Note Ser. **82**, Cambridge University Press, Cambridge (1983), 55-76.

[94] J. W. P. Hirschfeld, *Finite Projective Spaces of Three Dimensions*, Oxford University Press, Oxford, (1985).

[95] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, second edition, Oxford University Press, Oxford, (1998).

[96] J. W. P. Hirschfeld, G. Korchmáros and F. Torres, *Algebraic curves over finite fields*, Princeton University Press, Princeton and Oxford, 2008.

[97] J. W. P. Hirschfeld and L. Storme, *The packing problem in statistics, coding theory and finite projective spaces*, J. Statist. Planning Infer. **72** (1998), 355-380.

[98] J. W. P. Hirschfeld and L. Storme, *The packing problem in statistics, coding theory, and finite projective spaces*: update 2001, in: Finite Geometries, Proceedings of the Fourth Isle of Thorns Conference, A. Blokhuis, J. W. P. Hirschfeld, D. Jungnickel and J. A. Thas, Eds., Developments in Mathematics 3, Kluwer Academic Publishers, Boston, (2000), 201-246.

[99] J.W.P. Hirschfeld and J. A. Thas, *General Galois Geometries*, Oxford Mathematical Monographs. Oxford University Press, (1991).

[100] A.R. Hoffer, *On unitary collineation groups*, J. Algebra **22** (1972), 211-218.

[101] D.R. Hughes and F.C. Piper, *Projective Planes*, Graduate Texts in Mathematics **6**, Springer, New York, 1973.

[102] D.R. Hughes and F.C. Piper: *Design Theory,* Cambridge University Press 1985.

[103] B. Huppert, *Endliche Gruppen. I*, Grundlehren der Mathematischen Wissenschaften **134**, Springer, Berlin, 1967.

[104] B. Huppert and B.N. Blackburn, *Finite groups. III*, Grundlehren der Mathematischen Wissenschaften **243**, Springer, Berlin, 1982.

[105] S. Innamorati, *The non existence of certain large minimal blocking sets*, Mitt. Math. Sem. Giessen **235** (1998), 1-23.

[106] S. Innamorati and F. Zuanni, *Minimal blocking configurations*, J of Geometry **55** (1996), 86-98.

[107] H. Janwa, *Some optimal codes from algebraic geometry and their covering radii*, European J. Combin. **11** (1990), 249-266.

[108] W.M. Kantor, M. O'Nan and G.M. Seitz, 2-*transitive groups in which the stabilizer of two points is cyclic*, J. Algebra **21** (1972), 17-50.

[109] N.M. Katz, *On a theorem of Ax,* Amer. J. Math. **93** (1971), 485-499.

[110] G. Keri, *Types of superregular matrices and the number of* n*-arcs and complete* n*-arcs in* $PG(r, q)$, J. Combin. Des. **14** (2006), 363-390.

[111] J.H. Kim and V. Vu, *Small complete arcs in projective planes*, Combinatorica **23** (2003), 311-363.

[112] E. Knill and R. Laflamme, *A theory of quantum error-correcting codes*, Phys. Rev. **A 55** (1997), 900-911.

[113] G. Korchmáros, *New examples of complete* k*-arcs in* $PG(2, q)$, Europ. J. Combin. **4** (1983), 329-334.

[114] G. Korchmáros and N. Pace, *Infinite family of large complete arcs in* $PG(2, q^n)$*, with* q *odd and* $n > 1$ *odd*, Des. Codes Cryptogr. **55** (2010), 285-296.

[115] G. Korchmáros and A. Sonnino, *Complete arcs arising from conics*, Discrete Math. **267** (2003), 181-187.

[116] G. Korchmáros and A. Sonnino, *On arcs sharing the maximum number of points with an oval in a Desarguesian plane of odd order*, J. Combin. Des. **18** (2010), 25-47.

[117] T. Illés, T. Szőnyi and F. Wettl, *Blocking sets and maximal strong representative system in finite projective planes*, Mitt. Math. Sem. Giessen **201** (1991), 97-107.

[118] S. Innamorati and A. Maturo, *The spectrum of minimal blocking sets*, Discrte Math. **208/209** (1999), 339-347.

[119] G. Lachaud, *Number of points of plane sections and linear codes defined on algebraic varieties*, in Arithmetic, Geometry, and Coding Theory. (Luminy, France, 1993), Walter De Gruyter, Berlin-New York, (1996), 77-104.

[120] R. Laflamme, C. Miquel, J.-P- Paz and W. H. Zurek, *A perfect quantum error correcting code*, Phys. Rev. Lett. **7** (1996), 198-201.

[121] R. Lidl and H. Niedereiter, *Finite fields*, Encyclopedia of Mathematics and its applications, 20, Addison-Wesley Publishing Company, Reading, (1983).

[122] M. W. Liebeck, C. E. Praeger and J. Saxl, *On the O'Nan-Scott Theorem for Finite Primitive Permutation Groups*, J. Austral. Math. Soc. Series A **44** (1988), 389-396.

[123] P. Lisoněk, S. Marcugini and F. Pambianco, *Constructions of small complete arcs with prescribed symmetry*, Contribut. Discrete Math. **3** (2008), 14-19.

[124] L. Lombardo-Radice, *Sul problema dei k-archi completi di $S_{2,q}$*, Boll. Un. Mat. Ital. **11** (1956), 178-181.

[125] E. Lluis, *Variedades algebraicas con ciertas condiciones en sus tangentes*, Bol. Soc. Mat. Mexicana (2) **7** (1962), 47-56.

[126] G. Lunardon and O. Polverino, *Blocking sets of size $q^t + q^{t-1} + 1$*, J. Comb. Theory Ser. A **90** (2000), 148-158.

[127] G. Lunardon and O. Polverino, *Blocking sets and derivable partial spreads*, J. Algebraic Comb. **14** (2001), 49-56.

[128] S. Marcugini, A. Milani and F. Pambianco, *Minimal complete arcs in $PG(2, q)$, $q \leq 29$*, J. Combin. Math. Combin. Comput. **47** (2003) 19-29.

[129] S. Marcugini, A. Milani and F. Pambianco, *Minimal complete arcs in $PG(2, q)$, $q \leq 32$*, in Proc. XII Int. Workshop on Algebraic and Combin. Coding Theory, ACCT2010, Novosibirsk, Russia (2010), 217-222.

[130] S. Marcugini, A. Milani and F. Pambianco, *Classification of the* $(n, 3)$*-arcs in* $PG(2, 7)$, Journal of Geometry **80** (2004), 179-184.

[131] S. Marcugini, A. Milani and F. Pambianco, *A computer search for complete caps in* $PG(d, q)$, Rapporto Tecnico 19/95 Dipartimento di Matematica Università degli Studi di Perugia, (1995).

[132] S. Marcugini, A. Milani and F. Pambianco, *Maximal* $(n, 3)$*-arcs in* $PG(2, 11)$, Discrete Mathematics **208/209**(1999), 421-426.

[133] S. Marcugini, A. Milani and F. Pambianco, *Maximal* $(n, 3)$*-arcs in* $PG(2, 13)$, Discrete Mathematics **294** (2005), 139-145.

[134] S. Marcugini and F. Pambianco, *Minimal* 1*-saturating sets in* $PG(2, q)$*,* $q \leq 16$, Australian J. of Combinatorics. **28** (2003), 161-169.

[135] P. R. J. Östergård, *Computer search for small complete caps*, J. Geom. **69** (2000), 172-179.

[136] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*, Cambridge University Press, (2000).

[137] F. Pambianco and L. Storme, *Minimal blocking sets in* $PG(2, 9)$, Ars Combinatoria **89** (2008), 223-234.

[138] F. Pambianco, *A class of complete* k*-caps of small cardinality in projective spaces over fields of characteristic three*, Discrete Math. **208/209** (1999), 463-468.

[139] F. Pambianco and E. Ughi, *A class of* k*-caps having* $k - 2$ *points in common with an elliptic quadric and two points on an external line*, Austral. J. Combin. **21** (2000), 299-310.

[140] G. Panella, *Caratterizzazione delle quadriche di uno spazio (tridimensionale) lineare sopra un corpo finito*, Bollettino dell'Unione Matematica Italiana **10** (1955), 507-513.

[141] R. Pardini, *Some remarks on plane curves over finite fields of finite characteristic*, Compositio Math. **60** (1986), 3-17.

[142] G. Pellegrino, *Un'osservazione sul problema dei* k*-archi completi in* $S_{2,q}$*, con* $q \equiv 1$ $(mod\ 4)$, Atti Accad. Naz. Lincei Rend. **63** (1977), 33-44.

[143] G. Pellegrino, *Sur les* k*-arcs complets des plans de Galois d'ordre impair*, Ann. Discrete Math. **18** (1983), 667-694.

[144] G. Pellegrino, *Sugli archi completi dei piani $PG(2,q)$, con q dispari, contenenti $(q+3)/2$ punti di una conica*, Rend. Mat. **12** (1992) 649-674.

[145] G. Pellegrino, *Sulle calotte complete, non ovaloidi, dello spazio $PG(3,q)$, q dispari*, Rendiconti Circolo Matematico di Palermo Ser. II **47** (1998), 141-168.

[146] G. Pellegrino, *Archi completi, contenenti $(q+1)/2$ punti di una conica, nei piani di Galois di ordine dispari*, Rend. Circ. Mat. Palermo (2) **62** (1993), 273-308.

[147] P. Polito and O. Polverino, *On small blocking sets*, Combinatorica **18** (1998), 133-137.

[148] P. Polito and O. Polverino, *Linear blocking sets in $PG(2,q^4)$*, Australas. J. Comb. **36** (2002), 41-48.

[149] O. Polverino, *Small minimal blocking sets and complete k-arcs in $PG(2,p^3)$*, Discrete Math. **208-209** (1999), 469-476.

[150] O. Polverino, *Small blocking sets in $PG(2,p^3)$*, Des. Codes Cryptogr. **20** (2000), 319-324.

[151] P. Roquette, *Abschätzung der Automorphismenanzahl von Funktionenkörpern bei Primzahlcharakteristik*, Math. Z. **117** (1970), 157-163.

[152] B. Schumacher, *Quantum coding*, Phys. Rev. **A 51** (1995), 2738-2747.

[153] B. Segre, *Le geometrie di Galois*, Ann. Mat. Pura Appl. **48** (1959), 1-97.

[154] B. Segre, *Sulle curve algebriche che ammettono come trasformata razionale una curva piana dello stesso ordine, priva di punti multipli*, Math. Ann. **109** (1933), 1-3.

[155] B. Segre, *Ovali e curve σ nei piani di Galois di caratteristica due*, Atti Accad. Naz. Lincei Rend. **32** (1962), 785-790.

[156] B. Segre, *Introduction to Galois geometries*, Atti Accad. Naz. Lincei Mem. **8** (1967), 133-236.

[157] J.P. Serre, *Local Fields*, Graduate Texts in Mathematics **67**, Springer, New York, 1979.

[158] F. Severi, *Trattato di Geometria Algebrica*, Zanichelli, Bologna, 1926.

[159] P. W. Shor, *Algorithms for quantum computation: discrete logarithms and factoring*, Proceedings, 35th Annual Symposium on Fundamentals of Comp. Science (1994), 124-134.

[160] P. W. Shor, *Scheme for reducing decoherence in quantum memory*, Phys. Rev. **A 52** (1995), 2493-2496.

[161] A. M. Steane, *Error correcting codes in quantum theory*, Phys. Rev. Lett. **77** (1996), 793-797.

[162] A. M. Steane, *Multi-particle interference and quantum error correction*, Proc. Roy. Soc. London **A. 452** (1996), 2551-2577.

[163] A. M. Steane, *Introduction to quantum error correction,* Phil. Trans. R. Soc. Lond. **356** (1998), 1739-1758.

[164] H. Stichtenoth, *Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. I. Eine Abschätzung der Ordnung der Automorphismengruppe*, Arch. Math. **24** (1973), 527-544.

[165] H. Stichtenoth, *Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. II. Ein spezieller Typ von Funktionenkörpern*, Arch. Math. **24** (1973), 615-631.

[166] K.O. Stöhr and J. F. Voloch, *Weierstrass points and curves over finite fileds*, Proc. London Math. Soc. (3) **52** (1986), 1-19.

[167] T. Szőnyi, *Blocking sets in Desarguesian affine and projective planes*, Finite Fields Appl. **3** (1997), 187-202.

[168] T. Szőnyi, A. Gács and Z. Weiner, *On the spectrum of minimal blocking sets in $PG(2,q)$*, (2002), http://matmod.elte.hu/gacs/atzs.ps.

[169] T. Szőnyi, *Small complete arcs in Galois planes*, Geom. Dedicata **18** (1985), 161-172.

[170] T. Szőnyi, *Note on the order of magnitude of k for complete k-arcs in $PG(2,q)$*, Discrete Math. **66** (1987) 279-282.

[171] T. Szőnyi, *Complete arcs in Galois planes: survey*, Quaderni del Seminario di Geometrie Combinatorie, Università degli studi di Roma, La Sapienza, **94** (1989).

[172] T. Szőnyi, *Arcs, caps, codes and 3-independent subsets*, in: G. Faina, G. Tallini (Eds.) Giornate di Geometrie Combinatorie, Università degli Studi di Perugia, Perugia, (1993), 57-80.

[173] J. Thas, *Some results concerning* $((q+1)(n-1), n)$*-arcs*, J. Combin. Theory Ser. A **19** (1975), 228-232.

[174] J.A. Thas, *M.D.S. codes and arcs in projective spaces: a survey*, Le Matematiche (Catania) **47** (1992), 315-328.

[175] A. D. Thomas and G. V. Wood, *Group Tables*, Orpington, U.K.: Shiva mathematics series **2**, (1980).

[176] V. Tonchev, *Quantum codes from caps*, Discrete Mathematics **308** (2008), 6368-6372.

[177] E. Ughi, *Saturated configurations of points in projective Galois spaces*, European J. Combin. **8** (1987), 325-334.

[178] J.F. Voloch, *On the completeness of certain plane arcs*, European J. Combin. **11** (1990), 491-496.

[179] W. K. Wooters and W. H. Zurek, *A single quantum cannot be cloned*, Nature **299** (1982), 802-803.

[180] S. Yu, J. Bierbrauer, Y. Dong, Q. Chen, C.H. Oh: *All the stabilizer codes of distance* 3, submitted.

Contents