Characterising and constructing codes using finite geometries

Dissertation submitted in partial fulfilment

of the requirements for the Degree of

Doctor of Science: Mathematics

at Ghent University

LINS DENAUX

September 2023

Supervisor
prof. dr. LEO STORME

Co-supervisor
dr. PETER VANDENDRIESSCHE

GHENT UNIVERSITY

FACULTY OF SCIENCES

voor papa

al raak je in 't denken verloren
en lijkt je verstand wel bevroren
je blijft toegewijd
tot absurditeit
zo worden ideeën geboren

Preface

> *"It's the questions we can't answer that teach us the most. They teach us how to think. If you give a man an answer, all he gains is a little fact. But give him a question and he'll look for his own answers."*
>
> — Patrick Rothfuss, *The Wise Man's Fear*

Picture yourself as an entry-level researcher in a mathematical field of choice, eager to discover and build new mathematical theories of your own. You dive into the existing literature to read up on what is already known and what remains a mystery. Authors of renowned papers present their results and meticulously describe the methods to obtain them. And despite being able to replicate known techniques and approaches, all your attempts lead to nothing. Frustrated, you throw away the piece of paper you were writing on and enviously curse those successful scientists.
However, after a while, you slowly crawl your way towards something interesting. Yes, the more you think about it, maybe this small idea has some potential. You progress, you get stuck, you talk to fellow colleagues and progress some more. Maybe you alter your objective or take a slightly different path. Finally, you end up with something decent. Maybe not as spectacular as the achievements of those other authors, but something worth mentioning. Then, once you have written everything down neatly, you realise that you've omitted the largest chunk of your journey: the process, the obstacles, the failures.

Scientific literature seldom portrays which hurdles were conquered to

achieve results. I myself am guilty of doing the very same thing. Because, let's face it, who'd want to publish an article titled 'On some ideas that led to nothing'?[1] Therefore, I gladly break with tradition and dedicate this Preface to all the difficulties one encounters when doing research. A tribute to the process and a tribute to failure.

I started my scientific journey in October of 2017 as the co-supervisor of the master's thesis of Sam Adriaensen, my now most frequent co-author[2]. Under the supervision of prof. Leo Storme, we aimed to characterise some geometric codewords of small weight (Chapter 3). This led to my very first article, which is a textbook example of the staggering difference between process and result.
It took almost two years to finish the article. Results were found in small bits and pieces, constantly improving the previous ones by just a small amount. In the late spring of 2018, I participated in my first conference: 'Combinatorics'. There, I met dr. Zsuzsa Weiner, who took me under her wing and shared some valuable insights. I remember spending many evenings lying on the floor of my residence, surrounded by large amounts of scrap paper. Back in Belgium, I finalized all arguments and heaved a sigh of relief when the article got submitted.

Honestly, after talking about the same topic for about two years, I was getting afraid to be branded as 'the guy who does nothing but characterise codewords'. Hence, in the Spring of 2019, I decided that it was time for something new. And by 'new', I mean some old research problem my supervisor once proposed during my master's. At that time, we tried to generalise a well-known three-dimensional example of a *saturating set* — called the 'oval plus line' construction — to arbitrary odd dimension. Sadly, we failed to do so. But in the Spring of 2019, I managed to succeed ($\star$).
Getting excited, I plunged into the vast world of saturating sets and discovered another interesting example, this time in the projective plane. After playing around with it combinatorially, some results were achieved for

[1] It's tempting, I know.

[2] and vice versa, I will deny any future change of this status.

$\varrho = 1$ $(*)$. A gut feeling convinced me that it was possible to prove the same for general ϱ $(**)$, but I got stuck on some technical details and therefore put the problem temporarily on hold.

In January of 2020, I visited prof. Daniele Bartoli in Perugia, where we worked on some ideas I'd written down in 2018 concerning codewords of small weight (Chapter 4). I also met prof. Fernanda Pambianco, an expert on saturating sets and covering codes. When I proudly presented my results so far, she helpfully pointed me towards some relevant articles, showing me that the results I'd achieved ($(\star)$ and $(*)$) were already known. Needless to say, my soul got slightly crushed.
After allowing myself to have a day or two of self-pity, I took a deep breath and put all my effort into proving $(**)$, determined not to throw in the towel. Thankfully, some perceptive discussions with prof. Maarten De Boeck put me back on track. Then, on a skiing trip[3], I had an epiphany while scribbling down some math in a little notebook: an intriguing link between subgeometries and affine lines (Chapter 9), which allowed me to tackle problem $(**)$ once and for all (Chapter 10).

Saturating sets can be constructed using *strong blocking sets*. So, at the start of 2021, it wasn't that surprising to suddenly find myself playing around with *higgledy-piggledy sets*, which form a fascinating family of strong blocking sets. If one focuses on projective geometries of dimension at most five, several authors show the existence of very small higgledy-piggledy sets. Only a few cases remained open for me to sink my teeth in (Chapter 6).
I recall being on holiday and waiting for a bus in Greece when dr. Geertrui Van de Voorde sent me an e-mail, expressing her interest in higgledy-piggledy sets and their link with linear sets. I couldn't help but feel an overwhelming sense of delight take over me. Several thoughts and ideas were exchanged, and before we knew it, a new research project was born. I discussed this with my colleague and friend dr. Jozefien D'haeseleer, who quickly joined the team[4].

[3]The saying is true: mathematicians have their best ideas doing the most arbitrary stuff.
[4]We could finally check off 'collaborated' from our bucket list.

Although the research matter was quite heavy and high-level, 'the process' had lost some of its cruelty. Or maybe I had gained some experience and confidence. Regardless, the collaboration led to the results bundled in Chapter 7, which finishes the search for small higgledy-piggledy sets in projective geometries of dimension five or less.

Part I embodies all my results concerning the characterisation of codewords arising from points and hyperplanes in a projective geometry. Chapter 2 consists mostly of new results I discovered while writing this thesis.
Parts II and III describe results concerning strong blocking sets and saturating sets, respectively. Although this order reverses the chronology of research, it felt like a more natural way to introduce the reader to these notions.
The first chapter of each part is meant to get the reader familiar with the relevant concepts and literature. Appendix A and Appendix B summarise all work in a language of choice.

This dissertation stands for six years of mathematical research. Six years of hardship and frustration, but also six years of joy and satisfaction when things work out. A lot of care has been put into this thesis, with an eye for detail and clarity, to make it as accessible as possible. The only thing left to do is to read it. So, all in all, I've left the easy bit to you.

Lins Denaux
June 2023

Dankwoord

Dit proefschrift zou nooit hebben bestaan zonder de hulp van een diverse groep lieve mensen. Hulp onder de vorm van intense brainstormsessies en pientere suggesties tot keuvelen in de warme middagzon. Hulp zat ook in de kleine dingen: het vieren van tussentijdse overwinningen, het weglachen van frustraties, een schouderklop, een knipoog.

Bedankt Leo om mijn promotor en mentor te zijn doorheen de afgelopen zes jaar. Jij was diegene die me overtuigde de stap te zetten naar het academisch onderzoek, en hopen werk verzette om dit te mogelijk te maken. Jij was diegene die me introduceerde aan allerlei wiskundigen over heel Europa, wat leidde tot enkele succesvolle samenwerkingen. Jij was diegene die me onmiddellijk het juiste artikel of boek kon voorleggen dat perfect mijn vele vragen kon beantwoorden.
Bedankt Peter om mij onder te dompelen in het computationeel onderzoek. Je nuchtere blik op de onderzoekswereld hielp me de pittige kant van mijn doctoraatsjaren te relativeren.
Bedankt Jan om mij en vele collega's te enthousiasmeren over het eindig meetkundig onderzoek en alles daaromtrent: zij het associatieschema's, brainstormsessies, computationeel onderzoek met FinInG of een lesje over de intrigerende wereld van academische verstandhoudingen.

Thank you Zsuzsa, Daniele and Alessandro for taking the time to meticulously read this thesis. Zsuzsa, thank you for making my very first (and daunting) research stay a joyous experience. Daniele, thank you for inviting

me to the beautiful city of Perugia and teaching me the captivating Italian coffee habits.

Dank je Jozefien, Lisa, Sam, Robin, Michiel, Frans, Ferdinand, Aida en Frederik voor de dagelijkse babbel en lach, zij het in ons vertrouwd bureau in de S8 of op één van de vele internationale congressen. Dank je Jozefien om samen met mij zes jaar geleden aan hetzelfde avontuur te beginnen. Dankzij jou voelde ik me nooit alleen tijdens de grillen van het doctoraatswerk. Het is een plezier om jou als toponderzoeker in mijn jury te hebben. Dank je Sam voor alle fijne samenwerkingen, onze brainstormsessies waren één van de leukste. Binnenkort zie ik je naam wel eens passeren in de krant. Dank je Maarten en Geertrui om jullie deur altijd voor me open te houden. Meermaals heeft een van jullie snuggere suggesties mij op het juiste pad gezet.
Dank je Anneleen, Magali, Paulien, Jeroen en Jens voor de fijne *joint lunches* en avontuurlijke uitstapjes. Dank je Geert voor de eeuwige computertechnische bijstand. Dank je Sam om eender welk administratief probleem helder en nauwkeurig voor me op te lossen.

Bedankt Addie, Amke, Aranka, Arnaud, Hanne, Nathan, Tom, Quinten en Barbara. Velen van ons zaten in een gelijkaardige situatie, wat het heerlijk maakt om wat werkdruk weg te lachen. Laten we onze geregelde spellendagen nooit stopzetten!
Bedankt Sarah voor alle gezellige horrordates en om mij op dat cruciale moment te overtuigen om voor 8 uur wiskunde te gaan. Zie waartoe dat heeft geleid.

Dank je Ibe en Esa, de beste en liefste broer en zus die ik me kan inbeelden. Bedankt voor de interesse, steun en liefde rond mijn onderzoek. Jullie blijven me inspireren om het beste van mezelf naar boven te halen.
Dank je `Ann` en Erasmus voor alle hulp en steun tijdens de laatste, pittige maanden! Jullie vroegen steevast hoe het met mijn onderzoek ging en luisterden nieuwsgierig, ook al was dit een serieuze ver-van-mijn-bedshow.

Dank je dank je dank je lieve mama om me alle kansen van de wereld te geven. Wat jij in de afgelopen jaren voor elkaar hebt gekregen is allesbehalve vanzelfsprekend. Je droeg de verantwoordelijkheid van drie kinderen vol dromen en ambities. Je verzette bergen werk om elk van ons de ruimte te geven te studeren wat we willen en ons eigen pad te kiezen. Je kinderen krijgen simpelweg altijd voorrang. Bedankt om er altijd voor me te zijn en me te vormen tot wie ik nu ben. Niets van dit was mogelijk zonder jou. Look at me now, mama!

Lowiese, je bent mijn liefde, mijn beste vriend en grootste steun. Je duwt me voort bij twijfel en kan de onderzoekswereld op een heerlijk nuchtere manier relativeren. Otis, jouw waanzinnige nieuwsgierigheid en speelsheid werpt een heldere blik op het leven. Het sluit mooi aan bij de houding van een wiskundig onderzoeker: nieuwe mogelijkheden zien, herontdekken, vallen en terug opstaan. Wat kijk ik ernaar uit om samen met jou de eerste wiskundige stapjes te zetten.

Contents

0 Preliminaries

As all works of scientific nature should have, this chapter is devoted to preliminaries — definitions and concepts such that you as a reader are familiar with the objects and structures we are dealing with. However, the mathematical world is vast and virtually boundless, so we do not have the luxury of discussing every elementary principle we build our work upon. Therefore, we expect the reader to be familiar with basic notions of set theory, graph theory, group theory and calculus, and to have a clear understanding of (linear) algebra, emphasising vector spaces over finite fields.

GENERAL ASSUMPTION

Throughout this *work*, we assume that $d \in \mathbb{N} \setminus \{0\}$ and that q is a prime power, i.e. $q := p^h$, where p is prime and $h \in \mathbb{N} \setminus \{0\}$.

Moreover, we generally assume that $k \in \{0, 1, \ldots, d\}$.

The **Galois field** of order q will be denoted by $\mathbb{F}_q$. The d-dimensional **vector space** over a field $\mathbb{F}$ will be denoted by $V(d, \mathbb{F})$, or by $V(d, q)$ if $\mathbb{F} = \mathbb{F}_q$. The **vector dimension** of a **vector subspace** W of $V := V(d, q)$ is denoted by $\dim_V(W)$. Vectors of a vector space are inherently *column* vectors. We denote the zero vector by $\mathbf{0}$ and the all-one vector by $\mathbf{1}$.

0.1 Finite geometries

Although *coding theory* is clearly put forward as the main topic of investigation, the toolkit used to obtain results within this area is of pure geometric nature. In reverse order of generality, this section introduces the reader to all relevant geometries that are needed to navigate through this work.

0.1.1 Incidence geometries

Several geometries will pop up throughout this thesis, and all of these are derived from the general concept of an *incidence geometry*.

Definition 0.1.1 (incidence geometry)

For any $r \in \mathbb{N}$, an **incidence geometry** of **rank** r is a tuple $(\mathcal{V}, I, T_r, t)$, with $\mathcal{V}$ a set, I a symmetric relation on $\mathcal{V}$ and t a surjective map from $\mathcal{V}$ onto the set $T_r := \{0, 1, \ldots, r-1\}$ such that $(v, v') \in I$ implies that $t(v) \neq t(v')$ for all $v, v' \in \mathcal{V}$.

The elements of $\mathcal{V}$ are called **varieties**, I is called the **incidence relation** and t is called the **type map**, hence any element $v \in \mathcal{V}$ is said to have **type** $t(v)$. As such a type map t often describes the *dimension* of a variety in most geometries, varieties of type 0, 1, 2, 3 and $r-1$ are called **points**, **lines**, **planes**, **solids** and **hyperplanes**, respectively.
Any two varieties $v, v' \in \mathcal{V}$ such that $(v, v') \in I$ are called **incident** and are by definition of different types. If $t(v) \leqslant t(v')$, then v is said to *be (lying/contained) in* or *on* v', while v' is said to *contain* or *go through* v. This is denoted by $v \subseteq v'$ or $v' \supseteq v$ (respectively $v \subset v'$ or $v' \supset v$ if $t(v) < t(v')$ and $v \in v'$ or $v' \ni v$ if v is a point). Points incident with a common line are said to be **collinear**, while lines incident with a common point are called **concurrent**. Points or lines lying in a common plane are said to be **coplanar**. If $m \in \mathbb{N}$, a line is called an ***m*-secant** to a point set $\mathcal{P}$ if it contains precisely m points of $\mathcal{P}$. If m is 0, 1 or at least 2, such a line is also called **external**, **tangent** or **secant** to $\mathcal{P}$, respectively.

If $\mathcal{V}$ is finite, then the incidence geometry is said to be a **finite** (incidence) geometry. As one can suspect, all geometries considered in this thesis are assumed to be finite.

If $\mathcal{G} := (\mathcal{V}, I, T_r, t)$ is an incidence geometry of rank r, then $\mathcal{G}' := (\mathcal{V}, I, T_r, t')$ is defined to be its **dual**, where $t' : \mathcal{V} \to T_r$ is a type map defined by $t'(v) := r - t(v) - 1$. Naturally, $\mathcal{G}'$ is an incidence geometry of rank r as well. Note that duality is a symmetric relation, i.e. $\mathcal{G}'$ is the dual of $\mathcal{G}$ if and only if $\mathcal{G}$ is the dual of $\mathcal{G}'$.

An **isomorphism** between two incidence geometries $\mathcal{G}_1 := (\mathcal{V}_1, I_1, T_r, t_1)$ and $\mathcal{G}_2 := (\mathcal{V}_2, I_2, T_r, t_2)$, necessarily of the same rank, is a bijection $\varphi : \mathcal{V}_1 \to \mathcal{V}_2$ such that $t_1(v) = t_2(\varphi(v))$ and $(v, v') \in I_1 \Leftrightarrow (\varphi(v), \varphi(v')) \in I_2$ for all $v, v' \in \mathcal{V}_1$. If $\mathcal{G}_1 = \mathcal{G}_2$ then φ is called an **automorphism**. If $\mathcal{G}_1$ and $\mathcal{G}_2$ are each other's dual, then φ is said to be a **duality**. Although it is always possible to construct the dual of an incidence geometry, a duality does not necessarily exist. If a duality however does exist, the incidence geometry is said to be **self-dual**.

Finally, if $\mathcal{G}_1 := (\mathcal{V}_1, I_1, T_{r_1}, t_1)$ and $\mathcal{G}_2 := (\mathcal{V}_2, I_2, T_{r_2}, t_2)$ are two incidence geometries with the property that $\mathcal{V}_1 \subseteq \mathcal{V}_2$, $t_1(v) = t_2(v)$ and $(v, v') \in I_1 \Leftrightarrow (v, v') \in I_2$ for all $v, v' \in \mathcal{V}_1$, then $\mathcal{G}_1$ is called a **subgeometry** of $\mathcal{G}_2$. Note that this implies that $r_1 \leqslant r_2$.

0.1.2 Point-line geometries and designs

An incidence geometry of rank 0 is a tuple of empty objects, while one of rank 1 is essentially an arbitrary set. As the varieties of an incidence geometry of rank 2 are partitioned into just two types, such a geometry is simply called a **point-line geometry**. The fact that $r = 2$ allows Definition 0.1.1 to be substantially simplified: a point-line geometry is a tuple $(\mathcal{P}, \mathcal{L}, I)$, with $\mathcal{P}$ and $\mathcal{L}$ a non-empty *point* and *line* set, respectively, and $I \subset (\mathcal{P} \times \mathcal{L}) \cup (\mathcal{L} \times \mathcal{P})$ a symmetric (incidence) relation.
Note that the dual of a point-line geometry $\mathcal{G} := (\mathcal{P}, \mathcal{L}, I)$ is simply the point-line geometry $\mathcal{G}' := (\mathcal{L}, \mathcal{P}, I)$.

A broad topic of investigation concerns the concept of a *(block) design*. For any $t, v, k, \lambda \in \mathbb{N} \setminus \{0\}$ with $t < k < v$, a $t-(v,k,\lambda)$ **(block) design** is a point-line geometry $(\mathcal{P}, \mathcal{B}, I)$ such that $|\mathcal{P}| = v$, such that each line (which is often called a **block**) contains precisely k points and such that any t points have precisely λ incident blocks in common. We assume that no two blocks are incident with the same k points, hence any block is uniquely identified by the set of points it contains.

Most designs considered in this work are $2-(v,k,1)$ designs, which are also known as **2-Steiner systems**.

0.1.3 Projective geometries

Denote by $\mathrm{PG}(d, \mathbb{F})$, or $\mathrm{PG}(d, q)$ if $\mathbb{F} = \mathbb{F}_q$, the d-dimensional **projective geometry** over the field $\mathbb{F}$, which is the incidence geometry $(\mathcal{V}, I, T_d, t)$ of rank d arising from the vector space $V(d+1, \mathbb{F})$: the set $\mathcal{V}$ consists of all vector subspaces, the incidence relation I is inherited and the map t maps a subspace W to its **(projective) dimension**[1] $\dim(W) := \dim_V(W) - 1$.
Varieties of $\mathrm{PG}(d, \mathbb{F})$ are called **(projective) subspaces**.

Projective geometries are the key players of this thesis. Without exception, every topic is situated within a (finite) projective geometric context. This is why, throughout this work, whenever 'dimension' or 'subspace' is mentioned, these are implied to be *projective*. A subspace of dimension k is called a *k-dimensional subspace*, or ***k*-subspace** for short. As mentioned before, 0-, 1-, 2-, 3- and $(d-1)$-subspaces of $\mathrm{PG}(d, \mathbb{F})$ are alternatively called **points**, **lines**, **planes**, **solids** and **hyperplanes**, respectively. The unique (-1)-dimensional subspace of $\mathrm{PG}(d, q)$ is called '**the empty set**', while the unique d-dimensional subspace is often referred to as '**the whole space**'.

As any vector subspace is a vector space in itself, any subspace can be viewed as a projective geometry. Conversely, any d-dimensional project-

[1] Note that we mischievously deviate from the formal definition of an incidence geometry by allowing a (unique) variety of (projective) dimension -1.

ive geometry over a field is naturally embeddable as a d-subspace of a projective geometry over the same field but of a larger dimension.

Below, we limit ourselves to all those projective geometric notions needed to manoeuvre through this thesis. For an extensive work on projective geometries and everything related, we refer to Hirschfeld and Thas [80–82].

Subspaces and subgeometries

As $\mathrm{PG}(d,q)$ has a finite number of subspaces, one can count the varieties of each type. This can be done by observing the underlying vector space $V(d+1,q)$. The number of k-subspaces of $\mathrm{PG}(d,q)$ equals the **Gaussian coefficient**

$$\begin{bmatrix} d+1 \\ k+1 \end{bmatrix}_q := \frac{\left(q^{d+1}-1\right)\left(q^{d}-1\right)\cdots\left(q^{d-k+1}-1\right)}{\left(q^{k+1}-1\right)\left(q^{k}-1\right)\cdots\left(q-1\right)}.$$

For simplicity's sake, we denote the number of points (or hyperplanes) of $\mathrm{PG}(d,q)$ by θ_d, i.e.

$$\theta_d := \begin{bmatrix} d+1 \\ 1 \end{bmatrix}_q = \frac{q^{d+1}-1}{q-1} = q^d + q^{d-1} + \cdots + q + 1,$$

where we settle on the convention that $\theta_{-1} := 0$. We write $\theta_{d,q}$ if we want to emphasize the underlying field order.

Notions such as the **span** $\langle \Pi, \Sigma \rangle$ or **intersection** $\Pi \cap \Sigma$ of two (or more) subspaces Π and Σ of $\mathrm{PG}(d,\mathbb{F})$ are naturally inherited from the underlying vector space. Two subspaces are **disjoint** or **skew** if their intersection is empty. If this is not the case, we say that such subspaces **intersect** or **meet** each other. Certain subspaces are said to **cover** a point set $\mathcal{P}$ if every point of $\mathcal{P}$ is contained in at least one of these subspaces. Moreover, as the dimension of a subspace is equal to its vector dimension minus one, **Grassmann's identity** is still valid within a projective geometry:

$$\dim(\Pi) + \dim(\Sigma) = \dim(\langle \Pi, \Sigma \rangle) + \dim(\Pi \cap \Sigma).$$

This identity will be used numerously in arguments and proofs throughout this thesis, often without mention.

A ***k*-spread** of $\mathrm{PG}(d, \mathbb{F})$ is a set of pairwise disjoint k-subspaces covering all points of $\mathrm{PG}(d, \mathbb{F})$.

Certain k-subspaces of $\mathrm{PG}(d, \mathbb{F})$ are said to be in **general position** if

(1) every $\left\lceil \frac{d+1}{k+1} \right\rceil$ of these subspaces span the whole space, and

(2) every $\left\lceil \frac{d+1}{d-k} \right\rceil$ of these subspaces have an empty intersection.

The above definition is commonly only specified for $k = 0$ but is generalised for the sake of this thesis. This notion stays invariant under a duality.
A set of points in general position is called an **arc**. A **basis** is defined to be an arc of size $d + 1$, while an arc of size $d + 2$ is called a **frame**.

For any k-subspace Π and any point set $\mathcal{B}$, the **cone** of $\mathrm{PG}(d, \mathbb{F})$ with **vertex** Π and **base** $\mathcal{B}$ is the set consisting of all points in Π together with all points lying in a line spanned by a point of Π and a point of $\mathcal{B}$. The base $\mathcal{B}$ is always assumed to lie in a $(d - k - 1)$-subspace disjoint to Π.

Finally, we consider three specific types of *subgeometries* of $\mathrm{PG}(d, \mathbb{F})$.

(1) The **point-line geometry** of $\mathrm{PG}(d, \mathbb{F})$ is the rank 2 subgeometry whose set of varieties consists of the points and lines of $\mathrm{PG}(d, \mathbb{F})$; incidence is inherited.

(2) A **projective subgeometry** is a subgeometry that is a projective geometry in itself. Such a subgeometry $\mathrm{PG}(d', \mathbb{F}')$, where $\mathbb{F}'$ necessarily is a subfield of $\mathbb{F}$ and $d' \leqslant d$, will be called a d'-dimensional **$\mathbb{F}'$-subgeometry** of $\mathrm{PG}(d, \mathbb{F})$. Its subspaces are called **$\mathbb{F}'$-subspaces**, its lines and planes will be called **$\mathbb{F}'$-sublines** and **$\mathbb{F}'$-subplanes**, respectively.

As a rule of thumb, an $\mathbb{F}'$-subspace $\mathcal{S}$ is always treated as a variety of $\mathrm{PG}(d', \mathbb{F}')$. We write $\langle \mathcal{S} \rangle_{\mathbb{F}}$ (or simply $\langle \mathcal{S} \rangle_q$ if $\mathbb{F} = \mathbb{F}_q$) to signal that

$\mathcal{S}$ is being viewed as a variety of the ambient projective geometry $\mathrm{PG}(d, \mathbb{F})$.

(3) An **affine geometry**, denoted by $\mathrm{AG}(d, \mathbb{F})$, is a rank d subgeometry whose set of varieties consists of all subspaces of $\mathrm{PG}(d, \mathbb{F})$ except for a hyperplane H_∞ and all subspaces it contains. This hyperplane is called the **hyperplane at infinity**. Varieties of $\mathrm{AG}(d, \mathbb{F})$ are called **affine subspaces**.

As a rule of thumb, an affine subspace $\mathcal{A}$ is always treated as a variety of $\mathrm{AG}(d, \mathbb{F})$. We write $\overline{\mathcal{A}}$, called the **projective completion** of $\mathcal{A}$, to signal that $\mathcal{A}$ is being viewed as a variety of the ambient projective geometry $\mathrm{PG}(d, \mathbb{F})$.

Finally, two affine k-subspaces are said to be **parallel** if the intersection of their projective completions contains a $(k-1)$-subspace of H_∞. Note that parallelism is an equivalence relation on the set of affine k-subspaces.

By considering the underlying vector space of the ambient projective geometry, one can deduce that every projective subgeometry is uniquely determined by a frame and a subfield.

Result 0.1.2 ([25, Theorems **2.6** and **2.8**] and [37, Lemma **1**])

Let $\mathbb{F}'$ be a subfield of a field $\mathbb{F}$. Then for each frame of $\mathrm{PG}(d, \mathbb{F})$, there exists a unique $\mathbb{F}'$-subgeometry containing each point of the frame.

We will frequently make use of projective subgeometries in Parts II and III. In particular, the following observation will prove its usefulness in Chapter 10.

Lemma 0.1.3

Suppose that $t \in \mathbb{N} \setminus \{0\}$, consider a $(d-1)$-dimensional $\mathbb{F}_q$-subgeometry $\mathcal{C}$ of $\mathrm{PG}(d, q^t)$ and define $\Sigma := \langle \mathcal{C} \rangle_{q^t}$. Let $\mathfrak{L}$ be an $\mathbb{F}_q$-subline of $\mathrm{PG}(d, q^t)$ having a point in common with $\mathcal{C}$ such that $\ell := \langle \mathfrak{L} \rangle_{q^t} \nsubseteq \Sigma$. Then there exists a unique

d-dimensional $\mathbb{F}_q$-subgeometry containing both $\mathcal{C}$ and $\mathfrak{L}$.

Proof. Define $P := \mathcal{C} \cap \mathfrak{L}$ and consider a frame $\mathcal{F}_\mathcal{C} := \{P, P_1, P_2, \ldots, P_d\}$ of $\mathcal{C}$. For any two distinct points $Q_1, Q_2 \in \mathfrak{L} \setminus \{P\}$, the set $\mathcal{F} := \{P_1, P_2, \ldots, P_d\} \cup \{Q_1, Q_2\}$ is a frame of $\mathrm{PG}(d, q^t)$. Therefore, by Result 0.1.2, there exists a unique d-dimensional $\mathbb{F}_q$-subgeometry $\mathcal{B}$ containing each point of $\mathcal{F}$.
Note that both $\mathcal{C}$ and $\mathfrak{L}$ are $\mathbb{F}_q$-subspaces within $\mathcal{B}$ and therefore, by Grassmann's identity, they intersect in a point of $\mathcal{B}$, necessarily equal to $\Sigma \cap \ell = P$. Hence, $\mathcal{B}$ contains all points of $\mathcal{F}_\mathcal{C}$ and $\{Q_1, Q_2\}$ and thus, by Result 0.1.2, contains both $\mathcal{C}$ and $\mathfrak{L}$. ∎

Coordinates and collineations

A point P of $\mathrm{PG}(d, \mathbb{F})$ corresponds to a vector line of $V(d+1, \mathbb{F})$. If $(x_0, x_1, \ldots, x_d)^\mathsf{T}$ is a non-zero vector of this line, then the vector line, and therefore the point P, is given by the set of $\mathbb{F}$-multiples of $(x_0, x_1, \ldots, x_d)^\mathsf{T}$. Hence, the coordinates of a point are defined up to a scalar multiple. These are said to be **homogeneous coordinates** or simply **coordinates**.

If δ maps a point with coordinates $(a_0, a_1, \ldots, a_d)^\mathsf{T}$ onto the hyperplane defined by the set of points whose coordinates satisfy $a_0X_0 + a_1X_1 + \cdots + a_dX_d = 0$, and maps any k-subspace $\langle P_0, P_1, \ldots, P_k \rangle$ onto the $(d-k-1)$-subspace $\delta(P_0) \cap \delta(P_1) \cap \cdots \cap \delta(P_k)$, then one can check that δ is a *duality* of $\mathrm{PG}(d, \mathbb{F})$, making $\mathrm{PG}(d, \mathbb{F})$ *self-dual*.

The **canonical frame** is the point set $\{E_0, E_1, \ldots, E_d, E\}$, where E_i has all-zero coordinates except for a 1 in the $(i+1)$th position, and E has coordinates $\mathbf{1} = (1, 1, \ldots, 1)^\mathsf{T}$.

An automorphism of a projective geometry $\mathrm{PG}(d, \mathbb{F})$ is called a **collineation**. The *fundamental theorem of projective geometry* states that every collineation of $\mathrm{PG}(d, \mathbb{F})$, $d \geqslant 2$, arises from an element of the *semilinear group* $\Gamma\mathrm{L}(d+1, \mathbb{F})$, i.e. a mapping $V \to V : v \mapsto Av^\sigma$ of the underlying vector space V, where A is a non-singular square matrix and σ is an automorphism of $\mathbb{F}$. Any

other semilinear map gives rise to the very same collineation if and only if their corresponding field automorphism equals σ and their corresponding matrix is a non-zero $\mathbb{F}$-multiple of A. Therefore, by taking the quotient group, we obtain the **collineation group** $\mathrm{P\Gamma L}(d+1,\mathbb{F}) \cong \mathrm{Aut}(\mathrm{PG}(d,\mathbb{F}))$. A collineation is said to be a **projectivity** if it arises from an element of the *general group* $\mathrm{GL}(d+1,\mathbb{F})$ (i.e. an element of the semilinear group with the identity map as its field automorphism). The set of all projectivities forms the **projectivity group** $\mathrm{PGL}(d+1,\mathbb{F})$. Two subsets of $\mathrm{PG}(d,\mathbb{F})$ are called **projectively equivalent** if there exists a projectivity that maps one onto the other.

The collineation group acts transitively on the set of all (ordered) frames (the projectivity group even acts *sharply* transitively on this set). This is why, given any configuration of subspaces of $\mathrm{PG}(d,\mathbb{F})$, one can choose any frame to be the *canonical frame* to prove any property that remains invariant with respect to collineations.

Axiomatic projective geometries

A projective geometry can be defined axiomatically, which eliminates the need for fields or vector spaces.

Definition 0.1.4 (axiomatic projective geometry)

An **axiomatic projective geometry** is a point-line geometry that satisfies the following three axioms:

(1) every two distinct points are contained in a unique line;

(2) **Veblen's axiom** holds: if A, B, C and D are four distinct points such that the lines AB and CD share a point, then so do the lines AC and BD;

(3) every line contains at least three points.

Contrary to its vectorial counterpart, the above definition does not mention

any notion of *dimension* (or *rank*), nor any concept of a *subspace* (or *variety*). However, these can be derived axiomatically as well.

Definition 0.1.5 (axiomatic subspace and dimension)

A **subspace** of an axiomatic projective geometry is a point set $\mathcal{S}$ such that any point on a line containing at least two points of $\mathcal{S}$ is also contained in $\mathcal{S}$. A subspace $\mathcal{S}$ has **dimension** k if it is the largest integer for which we can find a strictly increasing chain of subspaces $\varnothing \subset \mathcal{S}_0 \subset \mathcal{S}_1 \subset \cdots \subset \mathcal{S}_k = \mathcal{S}$. In this way, the dimension of an axiomatic projective geometry is defined to be equal to the dimension of its entire point set.

One can easily check that the point-line geometry of a projective geometry $\mathrm{PG}(d, \mathbb{F})$ satisfies the axioms of Definition 0.1.4, and that its notions of dimension and subspace coincide with the ones described in Definition 0.1.5.

Veblen and Young [110] proved that an axiomatic projective geometry of dimension $d \geqslant 3$ is isomorphic to the point-line geometry of a projective geometry arising from a vector space over a division ring. As Wedderburn's little theorem implies that every finite division ring is a field, their findings led to the following important result.

Result 0.1.6 ([110])

A finite axiomatic projective geometry of dimension $d \geqslant 3$, extended with its axiomatically defined subspaces and dimension map as described in Definition 0.1.5, is isomorphic to $\mathrm{PG}(d, q)$ for a certain prime power q.

The above theorem is not true for $d = 2$ as numerous counterexamples have been discovered.

0.1.4 Polar spaces

For any $r \in \mathbb{N} \setminus \{0, 1, 2\}$, a **polar space** of **rank** r is an incidence geometry $(\mathcal{V}, I, T_r, t)$ that satisfies the following axioms.

(1) The subgeometry whose set of varieties consists of all elements of $\mathcal{V}$ that are contained in a certain element $v \in \mathcal{V}$ is a $t(v)$-dimensional projective geometry.

(2) If v_1 and v_2 are two distinct elements of $\mathcal{V}$, then their *intersection* (i.e. the set of all elements of $\mathcal{V}$ contained in both v_1 and v_2) is an element of $\mathcal{V}$ as well.

(3) For every non-incident point-hyperplane pair (P, H), there exists a unique hyperplane $H' \ni P$ such that the intersection of H and H' has type $r-2$ and contains all points in H that are collinear with P.

(4) There exist two hyperplanes whose intersection is empty.

The varieties of a polar space are called **subspaces**, which makes sense as these are isomorphic to projective geometries and have a type equal to their (projective) dimension. However, to avoid confusion, hyperplanes of a polar space are called **generators**.

We can include the case $r = 2$ by slightly altering the above system of axioms. Polar spaces of rank 2 are called *generalised quadrangles*; we only consider their finite version. For any $s, t \in \mathbb{N} \setminus \{0\}$, a **generalised quadrangle** of **order** (s, t) is a point-line geometry that satisfies the following axioms.

(1) Two distinct points are contained in at most one line.

(2) Every line contains $s+1$ points; every point is contained in $t+1$ lines.

(3) For every non-incident point-line pair (P, ℓ), there exists a unique point $Q \in \ell$ collinear with P.

Polar spaces are an interesting and broadly studied kind of incidence geometry with many similarities to projective geometries. As with generalised quadrangles, only the *finite* case will be considered. Tits [107] proved that all finite polar spaces of rank $r \geqslant 3$ are **classical**, i.e. one of the following five **types**: an *elliptic*, *parabolic* or *hyperbolic quadric*, a *Hermitian polar space* or

a *symplectic polar space*. Quadrics are by far the most discussed finite polar spaces of this thesis, with Hermitian polar spaces a not-so-close second. As symplectic polar spaces do not emerge at all, we omit their definition.
For simplicity's sake, we view and hence define these substructures as particular point sets of $\mathrm{PG}(d,q)$. Their subspaces are defined to be the subspaces of $\mathrm{PG}(d,q)$ that only contain points of the polar space. This allows us to define finite polar spaces of general rank $r \in \mathbb{N}$. By convention, any polar space of rank 0 is the empty set.

- An **elliptic quadric** of rank r is a point set of $\mathrm{PG}(2r+1,q)$ projectively equivalent to the point set $\mathcal{Q}^-(2r+1,q)$ whose coordinates satisfy

  $$f(X_0,X_1)+X_2X_3+\cdots+X_{2r}X_{2r+1}=0,$$

  where f is an irreducible homogeneous quadratic form over $\mathbb{F}_q$.

- A **parabolic quadric** of rank r is a point set of $\mathrm{PG}(2r,q)$ projectively equivalent to the point set $\mathcal{Q}(2r,q)$ whose coordinates satisfy

  $$X_0^2+X_1X_2+X_3X_4+\cdots+X_{2r-1}X_{2r}=0.$$

  If q is even, then all tangent lines to $\mathcal{P}$ share a point called the **nucleus** of $\mathcal{P}$. A parabolic quadric of rank 1 is called a **non-singular conic**.

- A **hyperbolic quadric** of rank $r \geqslant 1$ is a point set of $\mathrm{PG}(2r-1,q)$ projectively equivalent to the point set $\mathcal{Q}^+(2r-1,q)$ whose coordinates satisfy

  $$X_0X_1+X_2X_3+\cdots+X_{2r-2}X_{2r-1}=0.$$

- A **Hermitian polar space** of rank $r \geqslant 1$ is a point set of $\mathrm{PG}\left(2r-\varepsilon,q^2\right)$ projectively equivalent to the point set $\mathcal{H}\left(2r-\varepsilon,q^2\right)$ whose coordinates satisfy

  $$X_0^{q+1}+X_1^{q+1}+\cdots+X_{2r-\varepsilon}^{q+1}=0,$$

  with $\varepsilon \in \{0,1\}$. Context should make the value of ε clear. A Hermitian polar space of rank 1 is called a **non-singular Hermitian curve**.

Any line of $\mathrm{PG}(d,q)$ intersects a quadric in either 0, 1, 2 or $q+1$ points and any line of $\mathrm{PG}(d,q^2)$ intersects a Hermitian polar space in either 1, $q+1$ or q^2+1 points. From this observation, the definitions of an *oval*, *hyperoval* and *unital* naturally arise.
An **oval**, respectively **hyperoval**, is an arc of $\mathrm{PG}(2,q)$ of size $q+1$, respectively $q+2$. It is not hard to prove that a hyperoval can only exist if q is even. A **unital** $\mathcal{U}$ is a point set of $\mathrm{PG}(2,q^2)$ of size q^3+1 such that any line is either tangent or a $(q+1)$-secant to $\mathcal{U}$.

A classical example of a hyperoval is a non-singular conic of $\mathrm{PG}(2,q)$, q even, together with its nucleus. Clearly, any non-singular conic is an oval and any non-singular Hermitian curve is a unital. However, the converse is generally untrue. The most notable result concerning the classification of ovals is that of Segre [101, 102], who proved that, if q is odd, every oval of $\mathrm{PG}(2,q)$ is indeed a non-singular conic.

One can check that the set of points and the set of generators of $\mathcal{Q}^+(3,q)$ form a generalised quadrangle of order $(q,1)$. The converse is also true.

Result 0.1.7 ([94, **4.4.8**(ii)])

Let $(\mathcal{P},\mathcal{L},I)$ be a generalised quadrangle of order $(q,1)$ naturally embedded in $\mathrm{PG}(3,q)$. Then $\mathcal{P}$ is a hyperbolic quadric of rank 2.

Using the above result, we can detect hyperbolic quadrics of $\mathrm{PG}(3,q)$ combinatorially.

Theorem 0.1.8

Suppose that $\mathcal{P}$ is a point set of $\mathrm{PG}(3,q)$ such that

(1) *each line of $\mathrm{PG}(3,q)$ is either a 0-, 1-, 2- or $(q+1)$-secant to $\mathcal{P}$,*

(2) *each point of $\mathcal{P}$ lies in precisely two $(q+1)$-secants to $\mathcal{P}$, and*

(3) $|\mathcal{P}| = (q+1)^2$.

Then $\mathcal{P}$ is a hyperbolic quadric of rank 2.

Proof. Let $\mathcal{L}$ be the set of all $(q+1)$-secants to $\mathcal{P}$. If $\mathcal{S}$ is the set of all pairs $(P, \ell) \in \mathcal{P} \times \mathcal{L}$ such that $P \in \ell$, then by double counting we obtain $|\mathcal{P}| \cdot 2 = |\mathcal{S}| = |\mathcal{L}| \cdot (q+1)$, which implies that $|\mathcal{L}| = 2(q+1)$.
By (2), each of the $q+1$ points on a line $\ell \in \mathcal{L}$ lies on a unique line of $\mathcal{L}$ different from ℓ. The span of each such line with ℓ produces a unique plane through ℓ. As there exist precisely $q+1$ planes through ℓ, each of those planes contains *on average* 2 lines of $\mathcal{L}$. Due to the pigeonhole principle, this implies that the following statements are equivalent.

(A) There exists a plane that contains precisely one line of $\mathcal{L}$.

(B) There exists a plane that contains at least three lines of $\mathcal{L}$.

We will prove that both of these equivalent statements are false.

Consider the case $q = 2$. Suppose that (B) holds, hence let π be a plane that contains at least three lines of $\mathcal{L}$. Then all but at most one point P of π are contained in $\mathcal{P}$. Note that each of these points is already contained in two elements of $\mathcal{L}$ lying in π. As $|\mathcal{P}| = 9$ and as π contains 7 points, there exists a point $Q \in \mathcal{P}$ not contained in π. By (2), this point Q lies in two lines of $\mathcal{L}$, at least one of which has to intersect π in a point different from P, causing a point of π to lie in least 3 elements of $\mathcal{L}$, a contradiction.
Consider the case $q \geqslant 3$. Suppose that (A) holds, hence let π be a plane that contains precisely one line ℓ of $\mathcal{L}$. Note that π contains at most one point P of $\mathcal{P}$ not contained in ℓ. After all, if π would contain two distinct points $P, Q \in \mathcal{P}$ such that $P, Q \notin \ell$, then $\langle P, Q \rangle$ would intersect ℓ and hence would contain at least 3 points of $\mathcal{P}$, making $\langle P, Q \rangle$ an element of $\mathcal{L}$ contained in π but different from ℓ, contradicting our starting assumption.
All lines of $\mathcal{L} \setminus \{\ell\}$ intersect π in a point that is necessarily contained in $\{P\} \cup \ell$. Hence, by (2), there are at most $2 + (q+1)$ lines of $\mathcal{L} \setminus \{\ell\}$ allowed to intersect π, implying that $|\mathcal{L} \setminus \{\ell\}| \leqslant 2 + (q+1)$, which is equivalent to $q \leqslant 2$, a contradiction.
Alternatively, the case $q \geqslant 3$ could be proven by supposing that (B) holds and using Theorem 2.2.1 to conclude that all points in π must be points of $\mathcal{P}$, contradicting property (2).

By Result 0.1.7, it suffices to prove that $(\mathcal{P}, \mathcal{L})$, together with natural incidence, forms a generalised quadrangle of order $(q, 1)$. Note that only the third axiom isn't trivially fulfilled. Hence, take a point $P \in \mathcal{P}$ and a line $\ell \in \mathcal{L}$ such that $P \notin \ell$. By (2), there exist precisely two lines $\ell_1, \ell_2 \in \mathcal{L}$ that contain P. At least one of these lines does not meet ℓ, as else the plane $\langle \ell_1, \ell_2 \rangle$ would contain at least three lines of $\mathcal{L}$, contradicting the fact that (B) does not hold; without loss of generality, suppose that $\ell_1 \cap \ell = \varnothing$. By the falseness of both (A) and (B), each plane through ℓ_1 contains precisely one line of $\mathcal{L}$ other than ℓ_1. As a consequence of (2), these $q+1$ lines of $\mathcal{L}$ are pairwise disjoint and hence cover precisely $(q+1)^2 = |\mathcal{P}|$ points of $\mathcal{P}$. This implies that points of $\mathcal{P}$ lying in the plane $\langle \ell_1, \ell_2 \rangle$ either lie on ℓ_1 or ℓ_2. As this plane intersects ℓ in a point $Q \in \mathcal{P}$, Q needs to lie on either ℓ_1 or ℓ_2, and as $\ell_1 \cap \ell = \varnothing$, $Q \in \ell_2$. In conclusion, Q is the unique point on ℓ collinear with P. ∎

Corollary 0.1.9

Suppose that $q \geqslant 5$ and let $\mathcal{P}$ be a point set of $\mathrm{AG}(3, q)$ such that

(1) *each affine line of $\mathrm{AG}(3, q)$ is either a 0-, 1-, 2- or q-secant to $\mathcal{P}$,*

(2) *each point of $\mathcal{P}$ lies in precisely two q-secants to $\mathcal{P}$, and*

(3) $|\mathcal{P}| = q(q+1)$.

Then $\mathcal{P}$ is the affine part of a hyperbolic quadric of rank 2 that meets the plane at infinity in a non-singular conic.

Proof. First, we claim that it is impossible for an affine plane π to contain two q-secants s_1 and s_2 to $\mathcal{P}$, together with a point $P \in \mathcal{P} \setminus (s_1 \cup s_2)$. If this is the case, then there are at least $q + 1 - 3 \geqslant 3$ affine lines in π through P that intersect s_1 and s_2 in distinct points. Due to property (1), such affine lines must be concurrent q-secants to $\mathcal{P}$, contradicting (2).
Consider an affine q-secant ℓ to $\mathcal{P}$. By (2), through each of the q points in ℓ, there exists a unique affine q-secant. Moreover, no two of such q-secants

are coplanar, as else, the affine plane that contains these affine lines meets the impossible standard we described at the start of this proof. Hence, for each $i \in \{1, 2, \ldots, q\}$, there exists a unique affine plane π_i through ℓ that contains exactly one q-secant ℓ_i that intersects ℓ precisely in a point.
Moreover, by our first claim, no other point of $\mathcal{P}$ besides the ones in $\ell \cup \ell_i$ lies in π_i. Due to property (3), the unique affine plane π_{q+1} through ℓ different from $\pi_1, \pi_2, \ldots, \pi_q$ must contain exactly q points of $\mathcal{P}$ apart from the ones lying in ℓ. Let Q_1 and Q_2 be two distinct such points. Then $\langle Q_1, Q_2 \rangle$ cannot intersect ℓ, as else, by (1), this affine line would be a q-secant that intersects ℓ in a point that is contained in some ℓ_j, $j \in \{1, 2, \ldots, q\}$, contradicting (2). As Q_1 and Q_2 were chosen arbitrarily, all q points of $\mathcal{P}$ in π_{q+1} that does not lie in ℓ must be the points of a parallel affine line ℓ_{q+1}.

Now consider the plane at infinity π_∞. As no two of the affine q-secants $\ell_1, \ell_2, \ldots, \ell_{q+1}$ are coplanar, each of their projective completions $\overline{\ell_i}$ determines a unique point $P_i \in \pi_\infty$. Define $\overline{\mathcal{P}} := \mathcal{P} \cup \{P_1, P_2, \ldots, P_{q+1}\}$ and consider an affine q-secant ℓ_i. As ℓ was initially chosen arbitrarily, we may let ℓ_i temporarily play the role of ℓ to make two observations:

(1) P_i cannot be contained in the projective completion of an affine 2-secant to $\mathcal{P}$, hence each projective completion of an affine line is either a 0-, 1-, 2- or $(q+1)$-secant to $\overline{\mathcal{P}}$.

(2) P_i is contained in the projective completion of precisely one affine q-secant other than ℓ_i.

Note that no three points of $\{P_1, P_2, \ldots, P_{q+1}\}$ are collinear, as else we find a necessarily unique line that intersects the (pairwise disjoint) projective completions of three affine lines of $\{\ell_1, \ell_2, \ldots, \ell_{q+1}\}$, contradicting the fact that the projective completion of ℓ shares this property (see the concept of *transversal lines* in Section 0.1.6). Therefore, $\overline{\mathcal{P}}$ meets all conditions of Theorem 0.1.8, finishing the proof. ∎

0.1.5 Normal rational curves

The following generalises the idea that a non-singular conic is the 'most standard' type of arc of size $q+1$.

Definition 0.1.10 (normal rational curve)

A **normal rational curve** of $\mathrm{PG}(d,q)$ is a point set of size $q+1$ projectively equivalent to the point set corresponding to the coordinates

$$\{(0,0,\ldots,0,1)^\mathsf{T}\} \cup \left\{ \left(1,\alpha,\alpha^2,\alpha^3,\ldots,\alpha^d\right)^\mathsf{T} \,:\, \alpha \in \mathbb{F}_q \right\}.$$

We will somewhat break tradition by allowing normal rational curves to be contained in a k-subspace (viewed as an embedded $\mathrm{PG}(k,q)$). A normal rational curve $\mathcal{C}$ has **degree** k if k is the smallest integer for which there exists a k-subspace of $\mathrm{PG}(d,q)$ containing $\mathcal{C}$.

As the above coordinates give rise to a Vandermonde matrix, it is easy to check that a normal rational curve of degree k is an *arc* of the k-subspace it is contained in. Note that a normal rational curve of degree 1 is a line, while one of degree 2 is a non-singular conic. A normal rational curve of degree 3 is called a **twisted cubic**. These objects often arise when considering intersections of quadrics.

While a subspace is uniquely defined by a basis and an $\mathbb{F}_q$-subgeometry is uniquely determined by a frame (Result 0.1.2), a slightly larger arc is needed to fix a normal rational curve.

Result 0.1.11 ([76, Theorem **1.18**])

Let $q \geqslant d+2$. Then for each arc of $\mathrm{PG}(d,q)$ of size $d+3$, there exists a unique normal rational curve containing each point of the arc.

The following rather specific result is needed for Chapter 7.

Result 0.1.12 ([82, Lemma **6.31**(i)])

Suppose that $\mathcal{C}$ is a normal rational curve of $\mathrm{PG}(d,q)$ *of degree $k \geqslant 2$. Consider a point $P \in \mathcal{C}$ and a hyperplane $\Pi \not\ni P$. Then*

$$\{\langle P, Q\rangle \cap \Pi \,:\, Q \in \mathcal{C} \setminus \{P\}\}$$

is a point set of size q contained in a normal rational curve of degree $k-1$.

Consider a normal rational curve $\mathcal{C}$ of the projective geometry $\mathrm{PG}(d,q)$ embedded as an $\mathbb{F}_q$-subgeometry of $\mathrm{PG}(d,q^t)$, $t \in \mathbb{N}\setminus\{0\}$. As the $q+1$ points of $\mathcal{C}$ are defined by coordinates that satisfy a particular algebraic condition over $\mathbb{F}_q$, one can observe this condition over $\mathbb{F}_{q^t}$ to find a normal rational curve of $\mathrm{PG}(d,q^t)$ of the same degree that *extends* $\mathcal{C}$, which is called an **$\mathbb{F}_{q^t}$-extension** of $\mathcal{C}$. Note that, by Result 0.1.11, such an $\mathbb{F}_{q^t}$-extension is unique whenever $q \geqslant d+2$.

0.1.6 Reguli and transversal lines

Let $t \in \mathbb{N}\setminus\{0\}$. A **regulus** $\mathcal{R}$ of $\mathrm{PG}(2t-1,q)$ is a set of $q+1$ pairwise disjoint $(t-1)$-subspaces with the property that any line meeting three elements of $\mathcal{R}$, intersects all elements of $\mathcal{R}$. Such a line is said to be a **transversal line** of $\mathcal{R}$.

Suppose that $\mathcal{R} := \{\varrho_0, \varrho_1, \ldots, \varrho_q\}$ is a regulus of $\mathrm{PG}(2t-1,q)$. Let P be a point contained in an element of $\mathcal{R}$; without loss of generality, $P \in \varrho_0$. By Grassmann's identity, the subspace $\langle P, \varrho_1\rangle$ has dimension t and hence has to intersect ϱ_2 in precisely a point R. As the line $\langle P, R\rangle$ necessarily intersects ϱ_1, it is a transversal line of $\mathcal{R}$ through P. In fact, any line through P meeting both ϱ_1 and ϱ_2 has to lie in $\langle P, \varrho_1\rangle$ and hence must contain R, which implies that $\langle P, R\rangle$ is the only transversal line through P.
In conclusion, any transversal line of $\mathcal{R}$ through a point of one of its elements is unique. Therefore, we will often speak of *the* transversal line of $\mathcal{R}$ through P.

Naturally, the set of the $q+1$ transversal lines of a regulus $\mathcal{R}$ of $\mathrm{PG}(3,q)$

defines a regulus as well. Such a line set is called the **opposite regulus** of $\mathcal{R}$.

A well-known fact, provable by fiddling with an appropriate coordinate system, is that any three pairwise disjoint lines of $\mathrm{PG}(3,q)$ are contained in a unique regulus $\mathcal{R}$. Now let $\mathcal{P}$ be the point set covered by the $q+1$ lines of $\mathcal{R}$ and let $\mathcal{L}$ be the line set consisting of all lines of $\mathcal{R}$ together with all its transversal lines. Then it is not hard to check that $(\mathcal{P},\mathcal{L})$, together with natural incidence, forms a generalised quadrangle of order $(q,1)$ and hence, by Result 0.1.7, $\mathcal{P}$ is a hyperbolic quadric of rank 2.
In conclusion, any three pairwise disjoint lines of $\mathrm{PG}(3,q)$ give rise to a unique hyperbolic quadric. This neat fact will often be used in Chapter 6.

0.1.7 Field reduction and Desarguesian spreads

Field reduction is by far the most advanced concept that still deserves a spot in this chapter. The number of interesting substructures in $\mathrm{PG}(d,p^h)$ increases proportionally to the number of divisors of h, and field reduction is a useful tool to visualise these in a projective geometry of a larger dimension. In this way, this technique uncovers elegant connections between certain substructures. A great survey on this topic can be found in [88].

The field reduction map

Let $r,t\in\mathbb{N}\setminus\{0\}$. As $\mathbb{F}_{q^t}$ is a t-dimensional vector space over $\mathbb{F}_q$, a natural isomorphism exists between the vector spaces $V(r,q^t)$ and $V(rt,q)$. The idea behind **field reduction** is exploring the link between the projective geometries $\mathrm{PG}(r-1,q^t)$ and $\mathrm{PG}(rt-1,q)$ that directly emerges from this isomorphism. In this way, one can map subspaces of $\mathrm{PG}(r-1,q^t)$ onto subspaces of $\mathrm{PG}(rt-1,q)$ by 'reducing' the underlying field to a subfield. The authors of [88] formally introduce the **field reduction map**

$$\mathcal{F}_{r,t,q}:\mathrm{PG}(r-1,q^t)\to\mathrm{PG}(rt-1,q)\,, \tag{0.1}$$

which maps subspaces onto subspaces by viewing these as embedded projective geometries and applying field reduction. We extend the domain

of $\mathcal{F}_{r,t,q}$ to point sets as well, in the sense that

$$\mathcal{F}_{r,t,q}(\mathcal{P}) := \{\mathcal{F}_{r,t,q}(P) \,:\, P \in \mathcal{P}\}$$

for any point set $\mathcal{P}$ of $\mathrm{PG}(r-1,q^t)$. The subscript of $\mathcal{F}_{r,t,q}$ is often omitted once the context is clear on what parameters are being considered.

One can easily deduce some strong properties concerning the field reduction map. Any $(k-1)$-subspace is mapped onto a $(kt-1)$-subspace. Moreover, disjoint subspaces are mapped onto disjoint subspaces and incidence is preserved. Finally, the set of all points of $\mathrm{PG}(r-1,q^t)$ is mapped onto a $(t-1)$-spread of $\mathrm{PG}(rt-1,q)$, which is denoted by $\mathcal{D}_{r,t,q}$. Any spread isomorphic to $\mathcal{D}_{r,t,q}$ is called **Desarguesian**. Just as with the field reduction map, we remove the subscript of $\mathcal{D}_{r,t,q}$ if the context leaves no room for confusion.

Result 0.1.13 ([88, Theorem **2.6**])

The field reduction map $\mathcal{F}_{2,t,q}$ maps the point set of an $\mathbb{F}_q$-subline of $\mathrm{PG}(1,q^t)$ onto a regulus of $\mathrm{PG}(2t-1,q)$.

Indicator spaces

There is a way to naturally construct a Desarguesian spread without any need for the field reduction map, which was originally introduced by Segre [103].

Let $r \in \mathbb{N}\setminus\{0\}$, let $t \in \mathbb{N}\setminus\{0,1\}$ and interpret $\Omega \cong \mathrm{PG}(rt-1,q)$ as an $\mathbb{F}_q$-subgeometry of $\mathrm{PG}(rt-1,q^t)$. The subgroup of $\mathrm{P\Gamma L}(rt,q^t)$ pointwise fixing Ω is isomorphic to $\mathrm{Aut}(\mathbb{F}_{q^t}/\mathbb{F}_q)$. Consider a generator g of this group and take note of the following two facts (see [39]).

(1) There exists an $(r-1)$-subspace Π of $\mathrm{PG}(rt-1,q^t)$ disjoint to Ω.

(2) Any k-subspace of $\mathrm{PG}(rt-1,q^t)$ intersects Ω in a k-dimensional $\mathbb{F}_q$-subspace κ if and only if $\langle\kappa\rangle_{q^t}$ is fixed by g.

For any point $P \in \Pi$, it is clear that the $(t-1)$-subspace $\left\langle P, P^g, \ldots, P^{g^{t-1}} \right\rangle$ is fixed by g and hence, by (2), intersects Ω in a $(t-1)$-dimensional $\mathbb{F}_q$-subspace. Repeating this process for every point of Π, one obtains a set of pairwise disjoint $(t-1)$-dimensional $\mathbb{F}_q$-subspaces of Ω, forming a spread $\mathcal{S}$. One can prove that this spread is Desarguesian. The set $\left\{\Pi, \Pi^g, \ldots, \Pi^{g^{t-1}}\right\}$ is called the **indicator set** of $\mathcal{S}$, its elements are called **indicator spaces**. Casse and O'Keefe [39, Theorem 6.1] proved that each Desarguesian $(t-1)$-spread of $\mathrm{PG}(rt-1,q)$ possesses a unique indicator set in $\mathrm{PG}\left(rt-1,q^t\right)$.

0.1.8 Linear sets

We introduce the reader to the basics of *linear sets*, see [88, 95] for a more thorough introduction to this topic.

Let $n, r, t \in \mathbb{N} \setminus \{0\}$. The following definition is a generalisation of the concept of a projective subgeometry.

Definition 0.1.14 (linear set)

A non-empty point set $\mathcal{L}_\pi$ of $\mathrm{PG}\left(r-1,q^t\right)$ is an $\mathbb{F}_q$**-linear set** of rank n if n is the smallest integer such that there exists an $(n-1)$-subspace π of $\mathrm{PG}(rt-1,q)$ for which

$$\mathcal{F}_{r,t,q}(\mathcal{L}_\pi) = \mathcal{B}(\pi)\,,$$

where $\mathcal{B}(\pi)$ is the set of elements of the *Desarguesian spread* $\mathcal{D}_{r,t,q}$ that intersect π.

An $\mathbb{F}_q$-linear set of rank 1 is a point, while one of rank 2 is an $\mathbb{F}_q$-subline.

The **weight** of a point $P \in \mathcal{L}_\pi$ is equal to $\dim(\mathcal{F}(P) \cap \pi) + 1$. The weight of a point of a linear set is however only well-defined if we specify the subspace π defining $\mathcal{L}_\pi$.

Definition 0.1.15 (clubs and scattered linear sets)

An $\mathbb{F}_q$-linear set $\mathcal{L}_\pi$ of rank n is called **scattered** if every point in $\mathcal{L}_\pi$ has weight one. If this is the case, the subspace π is said to be **scattered** as well. If a point $H \in \mathcal{L}_\pi$ has weight $w \in \{2, 3, \ldots, n-1\}$ while all others have weight one, then $\mathcal{L}_\pi$ is called a ***w*-club** and H is called the **head** of the w-club. An $(n-1)$-club is simply called a **club**.

Similar to the weight of a point, the *head* of a club relies on which subspace π is considered.

Clearly, a scattered $\mathbb{F}_q$-linear set of rank n consists of θ_{n-1} points, while a club contains $q^{n-1}+1$ points.

Proposition 0.1.16

Through every three distinct points of a club $\mathcal{L}_\pi$ in $\mathrm{PG}(r-1, q^t)$, one of which is the head, there exists a unique $\mathbb{F}_q$-subline contained in $\mathcal{L}_\pi$.

Proof. Let $P_1, P_2 \in \mathcal{L}_\pi$ be two distinct points different from the head H. Then the line ℓ spanned by the points $\mathcal{F}(P_1) \cap \pi$ and $\mathcal{F}(P_2) \cap \pi$ necessarily intersects the $(n-2)$-subspace $\mathcal{F}(H) \cap \pi$. Therefore, ℓ determines an $\mathbb{F}_q$-linear set of rank 2 — hence an $\mathbb{F}_q$-subline — contained in $\mathcal{L}_\pi$. Result 0.1.2 finishes the proof. ∎

We only concern ourselves with $\mathbb{F}_q$-linear sets of $\mathrm{PG}(1, q^t)$. In this specific case of $r = 2$, Lavrauw and Van de Voorde unravelled some interesting geometric properties.

Result 0.1.17 ([89, Theorem 8])

An $\mathbb{F}_q$-linear set of rank n in $\mathrm{PG}(1, q^t)$ intersects an $\mathbb{F}_q$-subline in at most n or precisely $q+1$ points.

Result 0.1.18 ([89, Corollary **15**], [109, Theorem **3.7.4** and further])

Suppose that $q \geqslant 3$ and consider a scattered $\mathbb{F}_q$-linear set $\mathcal{L}_\pi$ of rank 3 in $\mathrm{PG}(1, q^3)$. Then

(1) *every two distinct points of $\mathcal{L}_\pi$ lie in exactly two $\mathbb{F}_q$-sublines contained in $\mathcal{L}_\pi$, and*

(2) *if $P \in \pi$ is a point, then there exists a unique plane $\pi' \neq \pi$ through P such that $\mathcal{B}(\pi) = \mathcal{B}(\pi')$.*

Result 0.1.19 ([89, Theorem **23**])

Suppose that $q \geqslant 4$. Then two distinct $\mathbb{F}_q$-linear sets of rank 3 in $\mathrm{PG}(1, q^3)$ share at most $2q + 3$ points.

Counting the *number* of $\mathbb{F}_q$-linear sets is generally not an easy task, but manageable in a few specific cases.

Lemma 0.1.20

Let $\mathcal{L}_{\pi_1} = \mathcal{L}_{\pi_2}$ be two clubs of $\mathrm{PG}(1, q^t)$ sharing the same head H. If there exists a point $P \in \pi_1 \cap \pi_2$, $P \notin \mathcal{F}(H)$, then $\pi_1 = \pi_2$.
Therefore, given a club $\mathcal{L}_\pi$ with head H, there exist exactly θ_{t-1} subspaces π' such that the club $\mathcal{L}_{\pi'} = \mathcal{L}_\pi$ has head H as well.

Proof. Suppose, to the contrary, that $\pi_1 \neq \pi_2$. Then there exists a point $Q_1 \in \pi_1$ not lying in π_2 nor in $\mathcal{F}(H)$. As $\mathcal{B}(\pi_1) = \mathcal{B}(\pi_2)$, the spread element $\mathcal{B}(Q_1)$ intersects π_2 in a point Q_2. Both $\langle P, Q_1 \rangle$ and $\langle P, Q_2 \rangle$ necessarily intersect $\mathcal{F}(H)$. Therefore, these lines both intersect $\mathcal{B}(P)$, $\mathcal{B}(Q_1) = \mathcal{B}(Q_2)$ and $\mathcal{F}(H)$ and hence both give rise to a (by Result 0.1.2) unique $\mathbb{F}_q$-subline in $\mathcal{L}_{\pi_1} = \mathcal{L}_{\pi_2}$. However, the spread elements $\mathcal{B}(P)$, $\mathcal{B}(Q_1) = \mathcal{B}(Q_2)$ and $\mathcal{F}(H)$ are pairwise disjoint $(t-1)$-subspaces of $\mathrm{PG}(2t-1, q)$, implying that there exists a unique line through P meeting both $\mathcal{B}(Q_1) = \mathcal{B}(Q_2)$ and $\mathcal{F}(H)$, a contradiction.

Finally, it is known that the collineation subgroup that stabilises each element of the Desarguesian spread $\mathcal{D}$ acts transitively on the points in a spread element (see e.g. [88, proof of Lemma 4.3]). Therefore, if $\mathcal{L}_\pi$ is a club of $\mathrm{PG}(1,q^t)$ with head H and $P \in \mathcal{L}_\pi \setminus \{H\}$, then for all θ_{t-1} points $R \in \mathcal{B}(P)$, we find a unique subspace π' through R with $\mathcal{B}(\pi') = \mathcal{B}(\pi)$ that maximally intersects $\mathcal{F}(H)$. ∎

Proposition 0.1.21

There are $q^{t-n+1}\begin{bmatrix} t \\ n-1 \end{bmatrix}_q$ clubs of $\mathrm{PG}(1,q^t)$ of rank n with a fixed head H.

Proof. There are $\begin{bmatrix} t \\ n-1 \end{bmatrix}_q$ subspaces of dimension $n-2$ in $\mathcal{F}(H)$, and each of these lies in exactly $\theta_{2t-n} - \theta_{t-n}$ subspaces of dimension $n-1$ not contained in $\mathcal{F}(H)$. By Lemma 0.1.20, a fixed club is determined by precisely θ_{t-1} of these $(n-1)$-subspaces. Hence, we find that there are

$$\frac{\begin{bmatrix} t \\ n-1 \end{bmatrix}_q (\theta_{2t-n} - \theta_{t-n})}{\theta_{t-1}} = q^{t-n+1}\begin{bmatrix} t \\ n-1 \end{bmatrix}_q$$

clubs with head H. ∎

Proposition 0.1.22

There are $\begin{bmatrix} t \\ n-1 \end{bmatrix}_q$ clubs of $\mathrm{PG}(1,q^t)$ of rank n through a fixed point P with a fixed head $H \neq P$. In total, there are $q^t\begin{bmatrix} t \\ n-1 \end{bmatrix}_q$ clubs of $\mathrm{PG}(1,q^t)$ of rank n through P with a head different from P.

Proof. An $(n-2)$-subspace $\sigma \subset \mathcal{F}(H)$ and a point $Q \in \mathcal{F}(P)$ span an $(n-1)$-subspace $\langle \sigma, Q \rangle$ which determines a club through P with head H. By Lemma 0.1.20, every club through P with head H is determined by exactly θ_{t-1} such $(n-1)$-subspaces, so the total number of clubs through

P with head H equals

$$\frac{\begin{bmatrix} t \\ n-1 \end{bmatrix}_q \theta_{t-1}}{\theta_{t-1}}.$$

■

Proposition 0.1.23

There are $\frac{1}{2}q^3\left(q^3-1\right)$ *scattered* $\mathbb{F}_q$*-linear sets of* $\mathrm{PG}\left(1,q^3\right)$ *of rank* 3 *through a fixed point.*

Proof. We first discuss the case of $q = 2$. Take any set $\mathcal{P}$ of seven points in $\mathrm{PG}(1,8)$ and let P_1 and P_2 be the two points not contained in $\mathcal{P}$. Define $D_i := \mathcal{F}(P_i)$, $i \in \{1,2\}$.
For every point $Q \in D_i$ and every line $\ell \subset D_{3-i}$, there exists a unique plane that intersects D_i in Q and D_{3-i} in ℓ. For every pair of points $(Q_1,Q_2) \in D_1 \times D_2$, there exist precisely $q^3+q^2-q-1 = 9$ planes that intersects D_i exactly in Q_i, namely all planes through $\langle Q_1,Q_2\rangle$ not contained in the solids $\langle Q_1,D_2\rangle$ or $\langle Q_2,D_1\rangle$, which necessarily intersect each other in $\langle Q_1,Q_2\rangle$. Therefore, we find $2\cdot 7^2+7^2\cdot 9 = 539$ planes that meet both D_1 and D_2. Easier arguments show that there exist 883 planes that intersect D_i, implying that there are exactly

$$\begin{bmatrix} 6 \\ 3 \end{bmatrix}_2 - 2\cdot 883 + 539 = 168 \tag{0.2}$$

planes in $\mathrm{PG}(5,2)$ disjoint to both D_1 and D_2.
Now consider a point $P \in \mathcal{P}$, define $D := \mathcal{F}(P)$ and let ℓ be a line in D. The hyperplane $\langle D_i,\ell\rangle$ meets D_{3-i} in a line ℓ_{3-i}. Each of the $q+1$ points of ℓ_{3-i} determines a unique plane through ℓ that intersects both D_1 and D_2. The other q^2 planes in $\langle D_i,\ell\rangle$ through ℓ meet only D_i. Therefore, there exists a total of $2q^2+q+1$ planes through ℓ that intersects D_1 or D_2, the other $q^3-q^2 = 4$ planes through ℓ are disjoint to these planes. As a consequence, there are exactly

$$|\mathcal{P}|\,(7\cdot 3+1) = 154$$

planes disjoint to both D_1 and D_2 that meet each of the planes in $\mathcal{F}(\mathcal{P})$ in at least a line. By (0.2), there are $168 - 154 = 14$ planes disjoint to both D_1 and D_2 that intersect each of the seven planes of $\mathcal{F}(\mathcal{P})$ in at most a point, and therefore, by the pigeonhole principle, in precisely a point. To conclude, every set of seven points in $\mathrm{PG}(1,8)$ is a scattered $\mathbb{F}_2$-linear set.

Assume that $q \geqslant 3$. We first count the number of scattered planes in $\mathrm{PG}(5,q)$ with respect to the Desarguesian plane spread $\mathcal{D}$. Consider triples (D,ℓ,π), where $D \in \mathcal{D}$, ℓ is a line in D and π is a plane through ℓ different from D. An easy check confirms that there are $\left(q^3+1\right)\left(q^2+q+1\right)\left(q^3+q^2+q\right)$ such triples, and since the choice of π uniquely determines both D and ℓ, we find that there are $\left(q^3+1\right)\left(q^2+q+1\right)\left(q^3+q^2+q\right)$ planes meeting some spread element in exactly a line. Therefore, there are $\begin{bmatrix}6\\3\end{bmatrix}_q - \left(q^3+1\right) - \left(q^3+1\right)\left(q^2+q+1\right)\left(q^3+q^2+q\right) = \left(q^3+1\right)q^3\left(q^3-1\right)$ scattered planes with respect to $\mathcal{D}$.
Now count all triples $(\pi,P,\mathcal{S})$, where π is a scattered plane through the point P such that $\mathcal{S} = \mathcal{L}_\pi$. On one hand, we have $\left(q^3+1\right)q^3\left(q^3-1\right)$ scattered planes π determining a unique $\mathbb{F}_q$-linear set $\mathcal{S}$, and q^2+q+1 points $P \in \pi$. On the other hand, by Result 0.1.18(2), we have that, given P and $\mathcal{S}$, there are exactly two planes π through P such that $\mathcal{S} = \mathcal{L}_\pi$. Therefore, denoting the total number of scattered $\mathbb{F}_q$-linear sets by x, we know that $\left(q^3+1\right)q^3\left(q^3-1\right)\left(q^2+q+1\right) = x\left(q^2+q+1\right)2$ and hence, $x = \frac{\left(q^3+1\right)q^3\left(q^3-1\right)}{2}$. The fact that the number of scattered $\mathbb{F}_q$-linear sets through each of the q^3+1 points of $\mathrm{PG}\left(1,q^3\right)$ is a constant finishes the proof. ∎

0.2 Linear codes

This section describes a branch of discrete mathematics with many (!) practical (and mostly invisible) applications in day-to-day life. Since the dawn of (error-correcting) *coding theory*, researchers began rapidly developing systems of highly optimised communication, significantly reducing the

risk of noise interfering with the message being conveyed. Examples from the endless list of applications include cryptography, data compression, transmission and storage, deep space communication and genetic sequence analysis.
See e.g. [11] for an introduction to the topic of coding theory.

As mentioned before, *finite geometries* will be used to obtain characterisation and construction results within this research domain.

0.2.1 Support, weight, equivalence and duality

A (q-ary) **linear code** $\mathcal{C}$ of **length** n is a vector subspace of $\mathbb{F}_q^n$, its elements are called **codewords**. The **dimension** of $\mathcal{C}$ is equal to $\dim_{\mathbb{F}_q^n}(\mathcal{C})$. By denoting the latter by k, we call $\mathcal{C}$ an $\boldsymbol{[n,k]_q}$**-code**. A **generator matrix** for $\mathcal{C}$ is a $(k \times n)$-matrix whose rows form a basis of $\mathcal{C}$.

In the context of coding theory, we say that any vector $v \in \mathbb{F}_q^n$ consists of *symbols* (of $\mathbb{F}_q$), each appearing in a unique *position* (of $\{1, 2, \ldots, n\}$). We define the **support** of v, denoted by $\mathrm{supp}(v)$, as the set of all positions with non-zero symbols. The size of this set is called the **weight** of v and is denoted by $\mathrm{wt}(v) := |\mathrm{supp}(v)|$. The **minimum weight** of the code $\mathcal{C}$ is defined as $\mathrm{wt}(\mathcal{C}) := \min\{\mathrm{wt}(c) : \mathbf{0} \neq c \in \mathcal{C}\}$.

Two q-ary linear codes are said to be **equivalent** if one can be obtained from the other by performing a sequence of one of the following operations applied to every one of its codewords simultaneously:

(1) permuting its positions;

(2) multiplying the symbol in a fixed position by a fixed non-zero scalar.

If each codeword of a linear code $\mathcal{C}$ has a 0 in a fixed position i, then this particular position entails no contribution to the practical use of $\mathcal{C}$ or any equivalent linear code. Such a linear code $\mathcal{C}$ is called **degenerate**. A linear code is said to be **non-degenerate** if each position i is contained in the support of at least one codeword.

The **dual code** $\mathcal{C}^\perp$ is the orthogonal complement of $\mathcal{C}$ with respect to the dot product for vectors in $\mathbb{F}_q^n$, i.e.

$$\mathcal{C}^\perp := \left\{ v \in \mathbb{F}_q^n \,:\, (\forall c \in \mathcal{C})\,(c \cdot v = 0) \right\}.$$

If $\mathcal{C}$ is an $[n,k]_q$-code, then $\mathcal{C}^\perp$ is an $[n,r]_q$-code, where $r := n-k$ is said to be the **redundancy** of $\mathcal{C}$. A generator matrix of $\mathcal{C}^\perp$ is called a **parity check matrix** of $\mathcal{C}$. For such an $(r \times n)$-dimensional parity check matrix H, the code $\mathcal{C}$ can be *redefined* as

$$\mathcal{C} := \left\{ c \in \mathbb{F}_q^n \,:\, Hc = \mathbf{0} \right\}.$$

0.2.2 Projective geometric codes, minimal codes and covering codes

We now introduce three specific categories of linear codes over a finite field. Each type of code corresponds to one of the three parts of this thesis, in which we discuss geometric methods to improve or extend existing results from the literature.

Projective geometric codes

Interesting classes of linear error-correcting codes can be constructed in a projective geometric setting; see for instance [99]. One such class of codes are *projective geometric codes*, which belongs to the more general family of generalised **Reed-Muller codes**; see [11, 15, 59, 60, 66, 85, 90]. These codes are used in various applications of wireless communication, particularly in deep space communication.

Consider the projective geometry $\mathrm{PG}(d,q)$ and let j and k be natural numbers such that $0 \leqslant j < k < d$. An **incidence matrix** of j- and k-subspaces of $\mathrm{PG}(d,q)$ is an $\mathbb{F}_p$-matrix whose rows are labelled by the k-subspaces and whose columns are labelled by the j-subspaces of $\mathrm{PG}(d,q)$ such that

each entry is equal to 1 if the corresponding row's k-subspace contains the corresponding column's j-subspace, and equal to 0 otherwise.
The p-ary linear code generated by the rows of such an incidence matrix is called a **projective geometric code**. Note that any two incidence matrices of j- and k-subspaces are permutation-similar, hence a different choice of an incidence matrix results in an equivalent code. Therefore, up to equivalence, the parameters j, k, d and q uniquely determine a projective geometric code, which we denote by $\mathcal{C}_{j,k}(d,q)$. If $j = 0$, we simply write $\mathcal{C}_k(d,q)$.

The incidence matrix used to generate $\mathcal{C}_{j,k}(d,q)$ is not a generator matrix. Determining the dimension of $\mathcal{C}_{j,k}(d,q)$ is generally not an easy task, and has only been determined in case $j = 0$ [75] and in case $k = d-1$ [2]. See [85] for a survey on these codes and their duals.

Denote the point set of $\mathrm{PG}(d,q)$ by $\mathcal{P}(d,q)$. In Part I of this work, we focus on the codes $\mathcal{C}_{d-1}(d,q)$ and fix a one-to-one correspondence between the positions of a vector $v \in \mathbb{F}_p^{\theta_d}$ and the points in $\mathcal{P}(d,q)$. In this way, we can interpret any vector of $\mathbb{F}_p^{\theta_d}$ as an element of the p-ary vector space $\mathbb{F}_p^{\mathcal{P}(d,q)}$ that maps any point onto the symbol in its corresponding position. As a consequence, a point $P \in \mathcal{P}(d,q)$ has a fixed **value** $v(P) \in \mathbb{F}_p$ with respect to a vector (or codeword) v.
Moreover, we can *redefine* the notion of the **support** of v as being the set of all points with non-zero values. Points having value 0 with respect to v are called **holes** of v. The **weight** of v remains equal to the size of its support.

By definition, a codeword $c \in \mathcal{C}_{d-1}(d,q)$ is equal to a p-ary linear combination of all incidence vectors v_{H_i} of hyperplanes with respect to the points of $\mathrm{PG}(d,q)$, i.e. there exist scalars $\alpha_1, \alpha_2, \ldots, \alpha_{\theta_d} \in \mathbb{F}_p$ such that

$$c = \sum_{i=1}^{\theta_d} \alpha_i v_{H_i}.$$

As this is rather tedious to work with, we will ignore all incidence vectors *appearing trivially* in the above linear combination, i.e. all incidence vectors corresponding to a zero coefficient. We informally state that "c is a

linear combination of the hyperplanes $H_1, \ldots, H_s$" if c can be written as a linear combination in which the incidence vectors of these hyperplanes are precisely the ones that appear non-trivially.

For any k-subspace $\kappa \in \mathrm{PG}(d,q)$, we can naturally define the **restriction** of v to κ as the map $v|_\kappa \in \mathbb{F}_p^{\mathcal{P}(k,q)}$ restricted to the point set $\mathcal{P}(k,q) \subset \mathcal{P}(d,q)$ of $\kappa \cong \mathrm{PG}(k,q)$. Using the fact that all scalar multiples of the all-one vector $\mathbf{1}$ are codewords of $\mathcal{C}_{d-1}(d,q)$, the following can easily be proved.

Result 0.2.1 ([96, Remark **3.1**])

If c is a codeword of $\mathcal{C}_{d-1}(d,q)$ and κ is a k-subspace of $\mathrm{PG}(d,q)$, then $c|_\kappa$ is a codeword of $\mathcal{C}_{k-1}(k,q)$.

This lemma will be used numerously in arguments and proofs throughout Part I, often without mention.

Keep in mind that the above (re)defined notions and conventions are only of relevance when considering the codes $\mathcal{C}_{d-1}(d,q)$ (see Part I).

Minimal codes

Let $\mathcal{C}$ be a q-ary linear code. A codeword $c \in \mathcal{C}$ is called **minimal** if for each $c' \in \mathcal{C}$ with $\mathrm{supp}(c') \subseteq \mathrm{supp}(c)$, there exists an $\alpha \in \mathbb{F}_q$ such that $c' = \alpha c$. The code $\mathcal{C}$ is called **minimal** if every one of its codewords is minimal, or, equivalently, if the set of supports of its non-zero codewords is an *antichain* with respect to setwise inclusion.

Minimal codewords can be used to describe *access structures* in linear code-based *secret sharing schemes* (see [91, 92]), which is a method to distribute shares of a secret to certain participants $\mathcal{P}$ in such a way that only the authorised subsets of $\mathcal{P}$ (a.k.a. the **access structure**) could reconstruct the secret; see [29, 104]. In [91, 92], Massey proposed the use of a linear code $\mathcal{C}$ for realising **secret sharing schemes** in which the access structure is specified by the supports of minimal codewords in $\mathcal{C}^\perp$ having a 1 in the smallest position of its support.

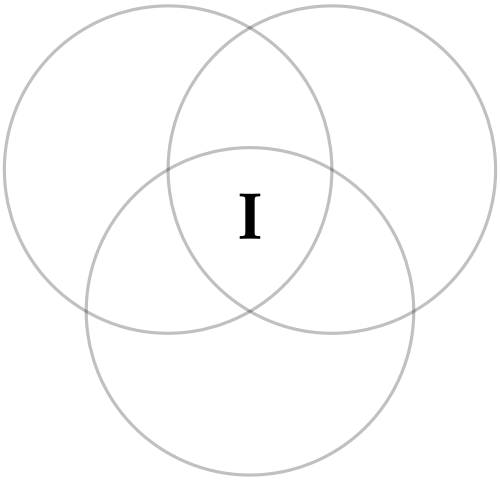
Due to the difficulty of determining the set of minimal codewords of a linear code [27, 35], research is mainly focused on analysing codes for which every codeword is minimal; see for instance [10, 18, 31, 40, 43, 65, 79, 111].
In Part II, we discuss new results concerning minimal codes of a small dimension. Minimality will also pop up in Part I, where we analyse which small weight codewords of a projective geometric code are minimal (see Chapter 4). Note that a projective geometric code is never minimal as $\mathbf{1}$ is a codeword.

Covering codes

To introduce the reader to the concept of a *covering code*, we need a *metric* on the vector space. For this, we can use the *Hamming distance*. The **Hamming distance** between two vectors of $\mathbb{F}_q^n$ equals the number of positions in which their corresponding symbols differ. The **covering radius** of a q-ary linear code $\mathcal{C}$ is the smallest integer R such that every vector of $\mathbb{F}_q^n$ lies within Hamming distance R of a codeword. Whenever linear codes are investigated with the goal of optimising the length or (co)dimension with respect to the covering radius, such codes are called **covering codes**.
Due to their link with saturating sets (see Part III), covering codes are described by their *redundancy* $r := n - k$ rather than their dimension k. If a q-ary linear code $\mathcal{C}$ has length n, redundancy r and covering radius R, then $\mathcal{C}$ is called an $[n, n-r]_q R$-code.

Covering codes are connected to several areas of information theory, such as data compression and storage, and decoding errors and erasures. See [46, Section 1] for an extensive overview of various applications of covering codes.

New results concerning covering codes of small length are discussed in Part III. As the reader will discover, covering codes can be constructed using minimal codes. Therefore, the results presented in Parts II and III are strongly interlinked.



I

Points & hyperplanes

1 A tale of few lines and odd codewords

> *Elodin proved a difficult man to find. He had an office in Hollows, but never seemed to use it. When I visited Ledgers and Lists, I discovered he only taught one class: Unlikely Maths. However, this was less than helpful in tracking him down, as according to the ledger, the time of the class was 'now' and the location was 'everywhere'.*
>
> — Patrick Rothfuss, *The Name of the Wind*

Throughout this and other chapters of Part I, we turn the spotlight on the projective geometric codes $\mathcal{C}_{d-1}(d,q)$. Although these codes are well-defined (see Section 0.2), it is generally hard to capture the behaviour of its codewords. In particular, the *weight distribution* of these codewords is not known and hence a subject of interest to the research world.

Let us consider the non-zero codewords of *small weight*. Naturally, any non-zero scalar multiple of a hyperplane is a codeword of weight θ_{d-1}. Immediately, two questions arise. Does there exist a non-zero codeword having a smaller weight? Are all codewords of weight θ_{d-1} equal to a scalar multiple of a hyperplane?

It turns out that the answers are respectively "no" and "yes", as the following characterisation result is known even for the more general codes $\mathcal{C}_{j,k}(d,q)$.

Result 1.0.1 ([11, 60] and [15, Theorem 1])

The minimum weight of $\mathcal{C}_{j,k}(d,q)$ equals the number of j-subspaces in a fixed k-subspace. The minimum weight codewords are the non-zero scalar multiples of k-subspaces.

In a certain sense, the behaviour of codewords with the smallest non-zero weight is exactly as one can expect. However, what can be said about codewords beyond weight θ_{d-1}? Do these behave equally well? These questions have lingered in the minds of various mathematicians for several years.

1.1 The planar case

To have a clear grasp of the problem, researchers initially investigated the small weight codewords of $\mathcal{C}_1(2,q)$ having weight larger than the minimum weight. Several results emerged in case $q = p$ is prime, starting with McGuire and Ward [93]. They discovered a gap in the weight spectrum by proving that no codeword of $\mathcal{C}_1(2,p)$ has weight $w \in \{p+2,\ldots,\frac{3}{2}(p+1)\}$, $p \neq 2$ [93, Corollary 2.3]. Chouinard [41, Proposition 27] extended this result by showing that no codeword has weight $w \in \{p+2,\ldots,2p-1\}$. A decade later, Fack, Fancsali, Storme, Van de Voorde and Winne [66] generalised this result by proving, if $p \geqslant 11$, that any codeword of $\mathcal{C}_1(2,p)$ of weight smaller than $\frac{5}{2}p$ is equal to a linear combination of at most two lines. Add another decade, then Bagchi [14] extended this result to all codewords of weight smaller than $3p-3$, $p \geqslant 5$.

During this communal quest, researchers cautiously conjectured that all small weight codewords of $\mathcal{C}_1(2,q)$ are equal to a linear combination of *a few* lines. In this context, 'a few' indicates that the weight of such a codeword directly determines the number of lines needed to obtain it.

Open Problem 1.1.1

For a certain bound $W(q)$, every codeword $c \in \mathcal{C}_1(2,q)$ having weight $\mathrm{wt}(c) \leqslant W(q)$ is equal to a linear combination of exactly $\left\lceil \frac{\mathrm{wt}(c)}{q+1} \right\rceil$ lines.

In 1991, Key [83] proved that the incidence vector of a Hermitian variety is a codeword of $\mathcal{C}_{d-1}(d,q^2)$, while Blokhuis, Brouwer and Wilbrink [30] showed that any unital $\mathcal{H}$ of $\mathrm{PG}(2,q^2)$ is a non-singular Hermitian curve if and only if its incidence vector $v_{\mathcal{H}}$ is a codeword of $\mathcal{C}_1(2,q^2)$, or, in other words, if and only if $v_{\mathcal{H}}$ is equal to a p-ary linear combination of lines. By the intersection properties of a non-singular Hermitian curve, a line ℓ appearing in such a linear combination contains at most $q+1$ points of $\mathrm{supp}(v_{\mathcal{H}})$. This means that at least q^2-q points in ℓ are holes of $v_{\mathcal{H}}$, which can only be the case if each of these points is contained in at least one extra line appearing in the linear combination.

This simple argument proves that any linear combination of lines equal to $v_{\mathcal{H}}$ consists of at least q^2-q+1 lines, which is substantially larger than $\left\lceil \frac{\mathrm{wt}(v_{\mathcal{H}})}{q^2+1} \right\rceil = q$ and implies that Open Problem 1.1.1 is false if q is square and $W(q) \geqslant q\sqrt{q}+1$.

Nevertheless, researchers kept trying to prove that the conjecture is true for a bound $W(q)$ as close to $q\sqrt{q}+1$ as possible. However, Bagchi [13, Theorem 5.2] and De Boeck and Vandendriessche [54, Example 1.8] independently discovered a peculiar codeword that rivals the conjecture if q is prime. De Boeck already mentioned this discovery in his PhD thesis [53, Example 10.3.4]. Below, we present a generalisation of this codeword described by Szőnyi and Weiner [105, Example 4.7].

Configuration 1.1.2 ([13, 53, 54, 105])

Suppose that $p \neq 2$ and let $\beta_1, \beta_2, \beta_3 \in \mathbb{F}_p$. Consider a coordinate system

(X_0, X_1, X_2) for $\mathrm{PG}(2,p)$ and define $c \in \mathbb{F}_p^{\mathcal{P}(2,p)}$ as follows:

$$c(P) := \begin{cases} \alpha_1 + \beta_1 & \text{if } P = (0,1,\alpha_1)\,, \\ \alpha_2 + \beta_2 & \text{if } P = (1,0,\alpha_2)\,, \\ -\alpha_3 + \beta_3 & \text{if } P = (1,1,\alpha_3)\,, \\ \beta_1 + \beta_2 + \beta_3 & \text{if } P = (0,0,1)\,, \\ 0 & \text{otherwise.} \end{cases}$$

The points of $\mathrm{supp}(c)$ lie in the union of lines ℓ_1, ℓ_2, ℓ_3 corresponding to the equations $X_0 = 0$, $X_1 = 0$, and $X_0 = X_1$, resp. Furthermore, $\mathrm{wt}(c) = 3p - 3$ if $\beta_1 + \beta_2 + \beta_3 = 0$ and $\mathrm{wt}(c) = 3p - 2$ otherwise.

Solely analysing the above configuration does not make it clear why the described vector is a codeword of $\mathcal{C}_1(2,p)$. The proof of this relies on the fact that $\mathcal{C}_1(2,p)^\perp \subset \mathcal{C}_1(2,p)$ [53, Lemma 10.3.3], as one can manually check that the vector described in Configuration 1.1.2, minus $\sum \beta_i \ell_i$, is indeed an element of $\mathcal{C}_1(2,p)^\perp$ if $p \neq 2$. In this and subsequent chapters, such a codeword will be called an **odd codeword** of $\mathcal{C}_1(2,q)$ and only exists if q is an odd prime.

As the line ℓ_i contains $p-1$ points with distinct non-zero values, an odd codeword can never be written as a linear combination of fewer than $p-1$ lines. If $p > 3$, then $p-1$ is larger than $\left\lceil \frac{\mathrm{wt}(c)}{p+1} \right\rceil \leqslant 3$, implying that Open Problem 1.1.1 is false if $q > 3$ is prime and $W(q) \geqslant 3q - 3$.
Note that the characterisation results of Chouinard and Bagchi imply that the conjecture is in fact true if q is prime and $W(q) < 3q - 3$, and also if $q \in \{2,3\}$ and $W(q) = 3q - 3$.

Using polynomial methods, Szőnyi and Weiner contributed considerably to the characterisation of small weight codewords of $\mathcal{C}_1(2,q)$ for somewhat larger values of q.

Result 1.1.3 ([105, Theorems **4.3**, **4.8** and Corollary **4.10**])

Let c be a codeword of $\mathcal{C}_1(2,q)$, $q=p^h$, p prime.
If $h=1$, $p \geqslant 19$ and $\mathrm{wt}(c) \leqslant \max\{3p+1, 4p-22\}$, then c is either a linear combination of at most three lines or given by Configuration 1.1.2.
If $h \geqslant 2$, $q \geqslant 32$ and

$$\mathrm{wt}(c) < \begin{cases} \frac{(p-1)(p-4)\left(p^2+1\right)}{2p-1} & \text{if } h=2, \\ \left(\lfloor\sqrt{q}\rfloor+1\right)\left(q+1-\lfloor\sqrt{q}\rfloor\right) & \text{if } h \geqslant 3, \end{cases}$$

then c is a linear combination of exactly $\left\lceil \frac{\mathrm{wt}(c)}{q+1} \right\rceil$ lines.

The above result improves the prime case by showing that odd codewords are the only type of codewords of weight $w \approx 3p$ defying our expectations. Moreover, it proves, if q is not small nor prime, that Open Problem 1.1.1 is solved if $W(q) = \mathcal{O}\left(q\sqrt{q}\right)$. If $q \geqslant 32$ and if $h \geqslant 4$ is even, then their result is sharp.

1.2 The general case

If we shift our focus to the small weight codewords of $\mathcal{C}_{d-1}(d,q)$, $d \geqslant 3$, much less is known. Analogous to the planar case, researchers started by investigating whether a gap exists in its weight spectrum. Based on the results of Key [83] and in line with Open Problem 1.1.1, one can speculate that any codeword of $\mathcal{C}_{d-1}(d,q)$ of weight lower than $q^{d-1}\sqrt{q}$ is equal to a linear combination of exactly $\left\lceil \frac{\mathrm{wt}(c)}{\theta_{d-1}} \right\rceil$ hyperplanes. We mainly base this overview on the survey article of Lavrauw, Storme and Van de Voorde [85].

While this was already utilized in the planar case, Lavrauw, Storme and Van de Voorde [86, 87] exploited a strong, general link between codewords of $\mathcal{C}_k(d,q)$ of small weight and k-blocking sets (see Definition 5.1.1). One year later, Lavrauw, Storme, Sziklai and Van de Voorde [84, Theorem 12]

proved that there exist no codewords in $\mathcal{C}_k(d,q) \setminus \mathcal{C}_{d-k}(d,q)^\perp$, $p > 5$, with weight in the interval $\left]\theta_k, 2q^k\right[$. As pointed out in [85, Theorem 3.12], using a known lower bound on the minimum weight of $\mathcal{C}_{d-k}(d,q)^\perp$ [15, Theorem 3], one can show that there exist no codewords of $\mathcal{C}_k(d,q)$, $p > 5$, having weight in the interval $\left]\theta_k, 2\left(\frac{q^d-1}{q^{d-k}-1}\left(1-\frac{1}{p}\right)+\frac{1}{p}\right)\right[$.

By analysing what is known about the codewords in $\mathcal{C}_k(d,q) \cap \mathcal{C}_{d-k}(d,q)^\perp$ and narrowing their view to the cases $k = d-1$ and q prime, Lavrauw, Storme, Sziklai and Van de Voorde managed to prove that no codewords of $\mathcal{C}_k(d,q)$, $p > 5$, have weight in the interval $\left]\theta_k, 2q^k\right[$ if $k = d-1$ or if q is prime [84, Corollaries 19 and 21].

Roughly a decade later, Polverino and Zullo characterised all codewords of $\mathcal{C}_{d-1}(d,q)$ up to the second smallest non-zero weight:

Result 1.2.1 ([96, Theorem **1.4**])

There are no codewords of $\mathcal{C}_{d-1}(d,q)$ with weight in the interval $\left]\theta_{d-1}, 2q^{d-1}\right[$. Any codeword of weight $2q^{d-1}$ is equal to a scalar multiple of the difference of two distinct hyperplanes.

Very recently, Adriaensen [1] gave a significantly shorter proof of the above result.

In the following chapters, we discuss new results concerning the characterisation of small weight codewords of $\mathcal{C}_{d-1}(d,q)$, extending [96] for all but a few small values of q [3].

Based on [3], we also obtained similar results concerning the small weight codewords of the more general code $\mathcal{C}_{j,k}(d,q)$. In addition, new results concerning its dual code $\mathcal{C}_{j,k}(d,q)^\perp$, whose minimum weight is generally unknown, are obtained as well. More specifically, we managed to reduce both problems of determining its minimum weight and characterising its minimum weight codewords to the case $\mathcal{C}_1(d,q)^\perp$ [2]. These results, however, will not be discussed in *this* thesis.

2 Ordinary small weight codewords

This and the following chapter are devoted to characterising small weight codewords of $\mathcal{C}_{d-1}(d,q)$, $d \geqslant 3$, based on known planar results. The core arguments are based on induction, and the results presented in both chapters are an extension of Result 1.1.3 to arbitrary dimension. Just like the planar result, we ignore small values of q.

In this chapter, we focus on the case of q being a composite prime power, $q \geqslant 32$, and prove that all codewords up to weight roughly $\sqrt{q}\theta_{d-1}$ are a linear combination of at most $\sqrt{q}$ hyperplanes (see Theorem 2.4.8). This result is precisely how one would expect small weight codeword to behave, hence the name of this chapter. Note that this significantly improves the main result found in [23], on which this chapter is based.

A partial result concerning the case of q prime is considered as well, but only as a stepping stone to the results presented in Chapter 3.

While most arguments are of a combinatorial nature, they rely on a strong algebraic result concerning point sets that allow m-secants only if m is either small or large (see Section 2.2). The proof is based on a bounding method that is more commonly known as *the standard equations*. We first present this technique in its most general form.

2.1 The standard equations

For $v, k, \lambda \in \mathbb{N} \setminus \{0\}$, $2 < k < v$, let $(\mathcal{P}, \mathcal{B}, I)$ be a $2-(v,k,\lambda)$ design. Define r to be the number of blocks through a fixed point, i.e.

$$r := \frac{(v-1)\,\lambda}{k-1}.$$

Consider a point set $\mathcal{S} \subseteq \mathcal{P}$ and let γ_i denote the number of blocks that contain exactly i points of $\mathcal{S}$, $i \in \{0, 1, \ldots, k\}$. A simple observation yields

$$\sum_{i=0}^{k} \gamma_i = |\mathcal{B}| = \frac{v\,(v-1)\,\lambda}{k\,(k-1)}. \tag{2.1}$$

By double counting the set of all incident point-block pairs, where points are elements of $\mathcal{S}$, we obtain

$$\sum_{i=0}^{k} i\gamma_i = |\{(P,B) \,:\, P \in B \cap \mathcal{S}\}| = |\mathcal{S}|\, r \tag{2.2}$$

and, analogously,

$$\begin{aligned} \sum_{i=0}^{k} i^2\gamma_i &= |\{(P,Q,B) \,:\, P,Q \in B \cap \mathcal{S}\}| \\ &= |\mathcal{S}|\, r + |\mathcal{S}|\,(|\mathcal{S}|-1)\,\lambda \\ &= |\mathcal{S}|^2\,\lambda + |\mathcal{S}|\,(r-\lambda)\,. \end{aligned} \tag{2.3}$$

Now suppose that there exist values $\alpha, \beta \in \{0, 1, \ldots, k\}$, $\alpha \leqslant \beta$, such that every block contains at most α or at least β points of $\mathcal{S}$. Equivalently, for every block $B \in \mathcal{B}$ that contains $i \in \{0, 1, \ldots, k\}$ points of $\mathcal{S}$, we have $(i-\alpha)\,(i-\beta) \geqslant 0$. As a consequence, we know that

$$\sum_{i=0}^{k} i^2\gamma_i - (\alpha+\beta)\sum_{i=0}^{k} i\gamma_i + \alpha\beta\sum_{i=0}^{k}\gamma_i = \sum_{i=0}^{k}(i-\alpha)\,(i-\beta)\,\gamma_i \geqslant 0.$$

Plugging (2.1), (2.2) and (2.3) in the left-hand side, we obtain

$$\lambda |\mathcal{S}|^2 - ((\alpha+\beta-1)r+\lambda)|\mathcal{S}| + \alpha\beta|\mathcal{B}| \geqslant 0. \tag{2.4}$$

By viewing the left-hand side as a quadratic polynomial in $|\mathcal{S}|$, it is clear that this inequality forces the size of the point set $\mathcal{S}$ to be either small or large, mimicking the gap between α and β.

The above method is used for more than just bounding the size of $\mathcal{S}$, as equality in (2.4) implies that every block contains exactly α or β points of $\mathcal{S}$, which can be a crucial argument in characterising such point set.

2.2 A weight spectrum for subspaces

One can now apply the standard equations to an arbitrary point set of a projective geometry. If such a point set intersects every line in either a few or many points, the same should be true for every subspace.

Theorem 2.2.1

Let $\mu_1, \mu_2 \in \{0, 1, \ldots, q\}$ with $(\mu_1+1)(\mu_2+1) \leqslant q+1$. Consider a point set $\mathcal{P}$ of $\mathrm{PG}(d,q)$ such that every line contains either at most μ_1 or at least $q+1-\mu_2$ points of $\mathcal{P}$. Then any k-subspace contains either

$$\textit{at most } \mu_1\theta_{k-1} \qquad \textit{or} \qquad \textit{at least } \theta_k - \mu_2\theta_{k-1}$$

points of $\mathcal{P}$.

Proof. If $\mu_1+\mu_2 \geqslant q$, then $(\theta_k - \mu_2\theta_{k-1}) - (\mu_1\theta_{k-1}) \leqslant 1$, making the statement to be proved trivially true. Therefore, we may assume that

$$\mu_1 + \mu_2 < q. \tag{2.5}$$

We proceed by induction on k. The cases $k=0$ and $k=1$ trivially hold, hence let $k \geqslant 2$ and assume the statement to be true for all $(k-1)$-subspaces. Consider an arbitrary k-subspace κ. The set of points in κ, together with

the set of all $(k-1)$-subspaces incident with κ, form a $2-(\theta_k, \theta_{k-1}, \theta_{k-2})$ design. Thus, using the induction hypothesis, we know that (2.4) is true for $\mathcal{S} := \kappa \cap \mathcal{P}$, $\alpha := \mu_1\theta_{k-2}$ and $\beta := \theta_{k-1} - \mu_2\theta_{k-2}$, where $\alpha < \beta$ due to (2.5). This results in

$$\theta_{k-2}\left|\kappa \cap \mathcal{P}\right|^2 - \left(\left(\mu_1\theta_{k-2} + \theta_{k-1} - \mu_2\theta_{k-2} - 1\right)\theta_{k-1} + \theta_{k-2}\right)\left|\kappa \cap \mathcal{P}\right| + \mu_1\theta_{k-2}\left(\theta_{k-1} - \mu_2\theta_{k-2}\right)\theta_k \geqslant 0,$$

which can be rewritten to

$$\theta_{k-2}\left|\kappa \cap \mathcal{P}\right|^2 - \left(\left(\mu_1\theta_{k-2} + q\theta_{k-2} - \mu_2\theta_{k-2}\right)\theta_{k-1} + \theta_{k-2}\right)\left|\kappa \cap \mathcal{P}\right| + \left(\mu_1\theta_{k-1}\theta_k - \mu_1\mu_2\theta_{k-2}\theta_k\right)\theta_{k-2} \geqslant 0.$$

Dividing both sides by θ_{k-2} yields

$$\left|\kappa \cap \mathcal{P}\right|^2 - \left(\theta_k + \left(\mu_1 - \mu_2\right)\theta_{k-1}\right)\left|\kappa \cap \mathcal{P}\right| + \mu_1\theta_{k-1}\theta_k - \mu_1\mu_2\theta_{k-2}\theta_k \geqslant 0. \tag{2.6}$$

The left-hand side is a quadratic polynomial in $|\kappa \cap \mathcal{P}|$ and reaches its smallest value if $|\kappa \cap \mathcal{P}| = \frac{1}{2}\left(\theta_k + \left(\mu_1 - \mu_2\right)\theta_{k-1}\right)$, which is equal to

$$\frac{\left(\mu_1\theta_{k-1} + 1\right) + \left(\theta_k - \mu_2\theta_{k-1} - 1\right)}{2}.$$

Therefore, by the symmetry of the (parabolic) graph of this polynomial, it obtains the same value regardless of whether $|\kappa \cap \mathcal{P}|$ equals $\mu_1\theta_{k-1} + 1$ or $\theta_k - \mu_2\theta_{k-1} - 1$. If we assume $|\kappa \cap \mathcal{P}| = \mu_1\theta_{k-1} + 1$, (2.6) becomes

$$\mu_1^2\theta_{k-1}^2 + 2\mu_1\theta_{k-1} + 1 - \mu_1\theta_{k-1}\theta_k - \mu_1\left(\mu_1 - \mu_2\right)\theta_{k-1}^2 - \theta_k - \left(\mu_1 - \mu_2\right)\theta_{k-1} + \mu_1\theta_{k-1}\theta_k - \mu_1\mu_2\theta_{k-2}\theta_k \geqslant 0,$$

which simplifies to

$$-\theta_k + \mu_1\mu_2\left(\theta_{k-1}^2 - \theta_{k-2}\theta_k\right) + \left(\mu_1 + \mu_2\right)\theta_{k-1} + 1 \geqslant 0.$$

Using the fact that $\theta_{k-1}^2 - \theta_{k-2}\theta_k = q^{k-1}$, we obtain

$$-q^k + \left(\mu_1\mu_2 + \mu_1 + \mu_2\right)q^{k-1} - \left(q - \mu_1 - \mu_2\right)\theta_{k-2} \geqslant 0.$$

Enlarging the left-hand side using $\mu_1\mu_2 + \mu_1 + \mu_2 \leqslant q$ yields

$$-(q - \mu_1 - \mu_2)\,\theta_{k-2} \geqslant 0,$$

which contradicts (2.5). As the left-hand side of (2.6) is quadratic in $|\kappa \cap \mathcal{P}|$, the observations above imply that

$$|\kappa \cap \mathcal{P}| \notin \{\mu_1\theta_{k-1} + 1, \ldots, \theta_k - \mu_2\theta_{k-1} - 1\}\,. \qquad \blacksquare$$

We can slightly improve [2, Lemma 5.7] by including the case $q = 3$.

Theorem 2.2.2

Let $q \geqslant 3$ and consider a point set $\mathcal{P}$ of $\mathrm{PG}(d, q)$ such that every line contains either at most 1 or at least q points of $\mathcal{P}$. Then there exists a hyperplane that either contains all points of $\mathcal{P}$ or all points of its complement $\mathcal{P}^c$.
Moreover, if $|\mathcal{P}| = \theta_n$, $n \in \mathbb{N}$, then $\mathcal{P}$ is the point set of an n-subspace.

Proof. Suppose the contrary. Then there must exist a basis $\{P_0, P_1, \ldots, P_d\} \subset \mathcal{P}$ and a basis $\{Q_0, Q_1, \ldots, Q_d\} \subset \mathcal{P}^c$ of $\mathrm{PG}(d, q)$.
We claim that the k-subspace $\langle P_0, \ldots, P_k\rangle$ contains at least q^k points of $\mathcal{P}$, for every $k \in \{0, 1, \ldots, d\}$. The proof of this claim is done by induction on k. If $k = 0$, there is nothing to prove, hence assume that $k \geqslant 1$. By the induction hypothesis, the $(k-1)$-subspace $\langle P_0, \ldots, P_{k-1}\rangle$ contains at least q^{k-1} points of $\mathcal{P}$. Connecting each of these points with P_k gives rise to at least q^{k-1} lines, each of which necessarily contains at least q points of $\mathcal{P}$, implying that $\langle P_0, \ldots, P_k\rangle$ contains at least

$$q^{k-1}\,(q-1) + 1 > \theta_{k-1}$$

points of $\mathcal{P}$. Theorem 2.2.1 finishes the proof of the claim. Analogously, $\langle Q_0, \ldots, Q_k\rangle$ contains at least q^k points of $\mathcal{P}^c$. Putting $k := d$, we conclude that $\theta_d = |\mathcal{P}| + |\mathcal{P}^c| \geqslant 2q^d$, a contradiction.

Finally, suppose that $|\mathcal{P}| = \theta_n$. We prove by induction on $i \in \{0, 1, \ldots, d-n\}$ that $\mathcal{P}$ must be contained in a $(d-i)$-subspace. If $i = 0$,

this is trivial. Hence, let $1 \leqslant i \leqslant d-n$ and assume, by the induction hypothesis, that $\mathcal{P}$ is contained in a $(d-i+1)$-subspace κ. If $\mathcal{P}^c$ is contained in a $(d-i)$-subspace of κ, then $|\mathcal{P}| \geqslant q^{d-i+1} > \theta_{d-i} \geqslant \theta_n$, a contradiction. Therefore, by the first part of this proof, $\mathcal{P}$ is contained in a $(d-i)$-subspace. Putting $i := d-n$ finishes the proof. ∎

2.3 Implications for codewords

ASSUMPTION

Throughout this *section*, we assume that $d \geqslant 3$ and $q \geqslant 32$, and fix a codeword $c \in \mathcal{C}_{d-1}(d,q)$.

To simplify notation, we make use of the integer values

$$A_q := \begin{cases} 2 \text{ or } 3 & \text{if } q \text{ is prime,} \\ \lfloor \frac{1}{2}\sqrt{q} - \frac{9}{4} \rfloor & \text{if } q = p^2, \\ \lfloor \sqrt{q} - \frac{1}{2} \rfloor & \text{otherwise;} \end{cases} \qquad B_q := \begin{cases} 3q-3 & \text{if } A_{q=p} = 2, \\ 4q-21 & \text{if } A_{q=p} = 3, \\ A_q(q+1)+1 & \text{otherwise.} \end{cases}$$

One can check that

$$A_q(q+1) < \begin{cases} \frac{(\sqrt{q}-1)(\sqrt{q}-4)(q+1)}{2\sqrt{q}-1} & \text{if } q = p^2, \\ \left(\lfloor \sqrt{q} \rfloor + 1\right)\left(q+1-\lfloor \sqrt{q} \rfloor\right) & \text{if } q = p^h, h \geqslant 3. \end{cases} \tag{2.7}$$

Proposition 2.3.1

Let π be a plane that contains an m-secant ℓ to $\mathrm{supp}(c)$. *Then*

$$\mathrm{wt}(c|_\pi) \geqslant \begin{cases} B_q & \text{if } A_q + 1 \leqslant m \leqslant q - A_q + 1, \\ m(q-m+2) & \text{otherwise.} \end{cases}$$

Proof. Suppose that $\mathrm{wt}(c|_\pi) \leqslant B_q - 1$. Then by (2.7) and Result 1.1.3, there exists a set $\mathcal{L}$ of at most A_q lines covering the points of $\mathrm{supp}(c|_\pi)$, each

such a line containing at least $q - |\mathcal{L}| + 2 \geqslant q - A_q + 2$ unique points of $\text{supp}(c|_\pi)$. If $\ell \in \mathcal{L}$, then $m \geqslant q - A_q + 2$. If $\ell \notin \mathcal{L}$, then it intersects each line of $\mathcal{L}$ in exactly one point, implying that $m \leqslant A_q$.
In conclusion, if $\text{wt}(c|_\pi) \leqslant B_q - 1$, then either $m \leqslant A_q$ or $m \geqslant q - A_q + 2$. Moreover, by the above observation, we know that

$$\text{wt}(c|_\pi) \geqslant |\mathcal{L}|\,(q - |\mathcal{L}| + 2) \geqslant m\,(q - m + 2)\,. \qquad \blacksquare$$

Lemma 2.3.2

Let q be prime.

- *If $q \geqslant 37$ and $\text{wt}(c) \leqslant 3\left(1 - \frac{3}{q}\right)\theta_{d-1}$, then every line contains either at most 2 or at least q points of $\text{supp}(c)$.*
- *If $q \geqslant 53$ and $\text{wt}(c) \leqslant 4\left(1 - \frac{8}{q}\right)\theta_{d-1}$, then every line contains either at most 3 or at least $q - 1$ points of $\text{supp}(c)$.*

Proof. Note that $A_q \in \{2, 3\}$ as q is prime. We aim to prove that every line contains either at most A_q or at least $q - A_q + 2$ points of $\text{supp}(c)$. Suppose, to the contrary, that m is the smallest integer, $A_q + 1 \leqslant m \leqslant q - A_q + 1$, for which there exists an m-secant ℓ to $\text{supp}(c)$. By Proposition 2.3.1, all planes through ℓ must contain at least B_q points of $\text{supp}(c)$, implying that

$$\begin{aligned} &\text{wt}(c) \geqslant B_q\theta_{d-2} - m\,(\theta_{d-2} - 1) \\ \iff\ &m \geqslant \frac{B_q\theta_{d-2} - \text{wt}(c)}{q\theta_{d-3}}. \end{aligned} \tag{2.8}$$

Case 1: $\text{wt}(c) < A_q\left(1 + \frac{1}{q}\right)\theta_{d-1}$.

By the above assumption on $\mathrm{wt}(c)$, (2.8) implies

$$\begin{aligned} m &> \frac{B_q\theta_{d-2} - A_q\left(1+\frac{1}{q}\right)\theta_{d-1}}{q\theta_{d-3}} \\ &= B_q - A_q(q+1) + \frac{\frac{B_q}{q} - A_q\left(1+\frac{1}{q}\right)^2}{\theta_{d-3}} \geqslant B_q - A_q(q+1). \end{aligned}$$

This results, as m is integer, in $m \geqslant B_q - A_q(q+1) + 1$. Let π be any plane through ℓ, thus $\mathrm{wt}(c|_\pi) \geqslant B_q$. As the points and lines in π form a $2-\left(q^2+q+1, q+1, 1\right)$ design and due to the minimality of m, (2.4) holds for $\mathcal{S} \coloneqq \mathrm{supp}(c|_\pi)$, $\alpha \coloneqq A_q$ and $\beta \coloneqq B_q - A_q(q+1) + 1$, which results in

$$\begin{cases} \mathrm{wt}(c|_\pi)^2 - \left(q^2-2q-2\right)\mathrm{wt}(c|_\pi) + 2q^3 - 6q^2 - 6q - 8 \geqslant 0 \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if } A_q = 2, \\ \mathrm{wt}(c|_\pi)^2 - \left(q^2-20q-20\right)\mathrm{wt}(c|_\pi) + 3q^3 - 66q^2 - 66q - 69 \geqslant 0 \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if } A_q = 3. \end{cases}$$

Substituting $\mathrm{wt}(c|_\pi)$ for $\left(A_q+\frac{1}{2}\right)(q-1)$ or $q^2 - \left(A_q^3-3\right)q$ both result in false statements, hence the same can be said for all values in between. This implies that either

$$\mathrm{wt}(c|_\pi) < \frac{2A_q+1}{2}(q-1) \qquad \text{or} \qquad \mathrm{wt}(c|_\pi) > q^2 - \left(A_q^3-3\right)q.$$

The first (upper) bound contradicts the fact that $\mathrm{wt}(c|_\pi) \geqslant B_q$, hence the second (lower) bound must hold for all planes containing ℓ. This immediately gives

$$\begin{aligned} A_q\left(1+\frac{1}{q}\right)\theta_{d-1} > \mathrm{wt}(c) &\geqslant \left(q^2 - \left(A_q^3-3\right)q - m\right)\theta_{d-2} \\ &\geqslant \left(q^2 - \left(A_q^3-2\right)q + A_q - 1\right)\theta_{d-2} \\ &> (q-25)\,q\theta_{d-2}, \end{aligned}$$

which implies that

$$A_q\left(1+\frac{1}{q}\right) > q - 25 - \frac{q-25}{\theta_{d-1}},$$

a contradiction for $q \geqslant 37$.

Case 2: $\mathbf{wt}(c) \geqslant A_q\left(1+\frac{1}{q}\right)\theta_{d-1}$.

The point-line geometry of $\mathrm{PG}(d,q)$ is a $2-(\theta_d, q+1, 1)$ design. Hence, by the minimality of m, (2.4) is true for $\mathcal{S} := \mathrm{supp}(c)$, $\alpha := A_q$ and β equal to the right-hand side of (2.8). Note that $\alpha \leqslant \beta$, as the contrary implies that

$$\begin{aligned} A_q &> \frac{B_q\theta_{d-2} - \mathrm{wt}(c)}{q\theta_{d-3}} \\ \iff \mathrm{wt}(c) &> B_q\theta_{d-2} - A_q q\theta_{d-3} \\ &> \left(B_q - A_q\right)\theta_{d-2}, \end{aligned}$$

which contradicts the given upper bounds on the weight of c. Therefore, (2.4) becomes

$$\begin{aligned} \mathrm{wt}(c)^2 - \left(\left(A_q + \frac{B_q\theta_{d-2} - \mathrm{wt}(c)}{q\theta_{d-3}} - 1\right)\theta_{d-1} + 1\right)\mathrm{wt}(c) \\ + A_q\left(\frac{B_q\theta_{d-2} - \mathrm{wt}(c)}{q\theta_{d-3}}\right)\begin{bmatrix} d+1 \\ 2 \end{bmatrix}_q \geqslant 0. \end{aligned}$$

By multiplying both sides with $q\left(q-1\right)\left(q^2-1\right)\left(q^{d-2}-1\right)$, we obtain

$$\begin{aligned} &(q+1)^2\left(q^{d-1}-1\right)\left((q-1)\,\mathrm{wt}(c)\right)^2 \\ &- \Big(\left(\left(A_q-1\right)q\left(q^{d-2}-1\right) + B_q\left(q^{d-1}-1\right)\right)(q+1)\left(q^d-1\right) \\ &\quad + q\left(q^2-1\right)\left(q^{d-2}-1\right) + A_q\left(q^d-1\right)\left(q^{d+1}-1\right)\Big)\left((q-1)\,\mathrm{wt}(c)\right) \\ &+ A_qB_q\left(q^{d-1}-1\right)\left(q^d-1\right)\left(q^{d+1}-1\right) \geqslant 0. \end{aligned}$$

Now, using some preferred computing software, one can plug in $A_q = 2$, $B_q = 3q - 3$ and either $(q-1)\,\mathrm{wt}(c) = 2\left(1+\frac{1}{q}\right)\left(q^d-1\right)$ or $(q-1)\,\mathrm{wt}(c) = 3\left(1-\frac{3}{q}\right)\left(q^d-1\right)$, to check that the above statement is false if $d \geqslant 3$ and $q \geqslant 37$. The same conclusions can be drawn for $A_q = 3$, $B_q = 4q - 21$, $(q-1)\,\mathrm{wt}(c) = 3\left(1+\frac{1}{q}\right)\left(q^d-1\right)$ or $(q-1)\,\mathrm{wt}(c) = 4\left(1-\frac{8}{q}\right)\left(q^d-1\right)$, $d \geqslant 3$ and $q \geqslant 53$. As the left-hand side of the inequality in question is quadratic in $(q-1)\,\mathrm{wt}(c)$, and by this case's assumption on $\mathrm{wt}(c)$, we obtain

$$\mathrm{wt}(c) > \begin{cases} 3\left(1-\frac{3}{q}\right)\theta_{d-1} & \text{if } A_q = 2, \\ 4\left(1-\frac{8}{q}\right)\theta_{d-1} & \text{if } A_q = 3, \end{cases}$$

a contradiction. ∎

Lemma 2.3.3

Let $\mathrm{wt}(c) \leqslant \left(q - A_q + 1\right)\theta_{d-1}$ *and suppose that every line contains either at most* A_q *or at least* $q - A_q + 2$ *points of* $\mathrm{supp}(c)$. *Then the existence of a* $\left(q - A_q + 2\right)$*-secant implies the existence of an* A_q*-secant to* $\mathrm{supp}(c)$.

Proof. Suppose that there exists a $\left(q - A_q + 2\right)$-secant ℓ to $\mathrm{supp}(c)$. By Theorem 2.2.1, every plane contains either at most $A_q\,(q+1)$ or at least $q^2 - \left(A_q - 2\right)(q+1)$ points of $\mathrm{supp}(c)$. If every plane through ℓ would contain at least $q^2 - \left(A_q - 2\right)(q+1)$ points of $\mathrm{supp}(c)$, we would obtain

$$\begin{aligned} \mathrm{wt}(c) &\geqslant \left(q^2 - \left(A_q - 2\right)(q+1) - \left(q - A_q + 2\right)\right)\theta_{d-2} + q - A_q + 2 \\ &= \left(q - A_q + 1\right)\theta_{d-1} + 1, \end{aligned}$$

a contradiction. Hence, there exists a plane π through ℓ such that $\mathrm{wt}(c|_\pi) \leqslant A_q\,(q+1)$. By Result 1.1.3, all points of $\mathrm{supp}(c|_\pi)$ must be contained in the union of *precisely* A_q lines, each of which containing at least $q - A_q + 2$ unique points of $\mathrm{supp}(c|_\pi)$ as the line ℓ must be one of them and contains

precisely $A_q - 1$ holes. At most $\binom{A_q}{2} < \frac{1}{2}q$ points lie in at least 2 of these lines, hence there must exist a line in π that intersects each of these A_q lines in distinct points, which necessarily lie in $\mathrm{supp}(c)$. ∎

Lemma 2.3.4

Let $m \in \{0, 1, \ldots, A_q\}$ and $\mathrm{wt}(c) \leqslant (q - \sqrt{q})\,\theta_{d-1}$. Suppose that every line contains either at most m or at least $q - A_q + 2$ points of $\mathrm{supp}(c)$. If κ is a k-subspace that contains an m-secant ℓ to $\mathrm{supp}(c)$, then $\mathrm{wt}(c|_\kappa) \leqslant m\theta_{k-1}$.

Proof. Suppose, to the contrary, that $\mathrm{wt}(c|_\kappa) > m\theta_{k-1}$. Due to Theorem 2.2.1, κ contains at least $q^k - (A_q - 2)\,\theta_{k-1}$ points of $\mathrm{supp}(c)$. If $k = d$, we obtain a direct contradiction to the weight assumption on c, hence assume that $k < d$. Consider a $(k+1)$-space κ^+ through κ. By Proposition 2.3.1, every plane in κ^+ through ℓ but not lying in κ contains at least $m\,(q - m + 2)$ points of $\mathrm{supp}(c)$, implying that

$$\begin{aligned}
\mathrm{wt}(c|_{\kappa^+}) &\geqslant q^k - (A_q - 2)\,\theta_{k-1} + q^{k-1}\,(m\,(q - m + 2) - m) \\
&= m\theta_k + q^k - (m^2 + A_q - 2)\,q^{k-1} - (A_q + m - 2)\,\theta_{k-2} \\
&\geqslant m\theta_k + q^k - \left(\left(\sqrt{q} - \frac{1}{2}\right)^2 + \sqrt{q} - \frac{1}{2} - 2\right) q^{k-1} \\
&\quad - \left(2\left(\sqrt{q} - \frac{1}{2}\right) - 2\right)\theta_{k-2} \\
&= m\theta_k + \frac{9}{4}q^{k-1} - 2\theta_{k-2}\sqrt{q} + 3\theta_{k-2} > m\theta_k.
\end{aligned}$$

By Theorem 2.2.1, $\mathrm{wt}(c|_{\kappa^+}) \geqslant q^{k+1} - (A_q - 2)\,\theta_k = (q - A_q + 1)\,\theta_k + 1$. As this holds for all $(k+1)$-spaces through κ, we get

$$\begin{aligned}
\mathrm{wt}(c) &\geqslant \left((q - A_q + 1)\,\theta_k - \theta_k\right)\theta_{d-k-1} \\
&> (q - \sqrt{q})\,\theta_k\theta_{d-k-1} \\
&\geqslant (q - \sqrt{q})\,\theta_{d-1},
\end{aligned}$$

which contradicts the assumption on the weight of c. ∎

2.4 Thin and thick subspaces

ASSUMPTION

Throughout this *section*, we assume that $d \geqslant 3$ and $q \geqslant 32$, and fix a codeword $c \in \mathcal{C}_{d-1}(d,q)$ such that $\mathrm{wt}(c) \leqslant W(d,q)$, where

$$W(d,q) := \begin{cases} 3\left(1-\frac{3}{q}\right)\theta_{d-1} & \text{if } q \text{ is prime,} \\ \left(\left\lfloor \frac{1}{2}\sqrt{q}-\frac{9}{4}\right\rfloor -1\right)\theta_{d-1} & \text{if } q=p^2, \\ \left(\left\lfloor \sqrt{q}-\frac{1}{2}\right\rfloor -1\right)\theta_{d-1} & \text{otherwise.} \end{cases}$$

To simplify notation, we introduce the integer value

$$\Delta_q := \begin{cases} 2 & \text{if } q \text{ is prime,} \\ \left\lfloor \frac{1}{2}\sqrt{q}-\frac{9}{4}\right\rfloor -1 & \text{if } q=p^2, \\ \left\lfloor \sqrt{q}-\frac{1}{2}\right\rfloor -1 & \text{otherwise.} \end{cases}$$

If every line contained at least $\Delta_q + 1$ points of $\mathrm{supp}(c)$, then so would every line through a fixed hole, implying that $\mathrm{wt}(c) \geqslant (\Delta_q+1)\,\theta_{d-1}$, which contradicts $\mathrm{wt}(c) \leqslant W(d,q)$. This allows us to define

$$\delta_q := \max\left\{ m \in \{0,1,\ldots,\Delta_q\} \,:\, \text{there exists an } m\text{-secant to } \mathrm{supp}(c) \right\}. \tag{2.9}$$

The following notions facilitate the use of Theorem 2.2.1.

Definition 2.4.1 (thin and thick subspaces)

A k-subspace κ is called

- **thin** if $\mathrm{wt}(c|_\kappa) \leqslant \delta_q \theta_{k-1}$, and
- **thick** if $\mathrm{wt}(c|_\kappa) \geqslant q^k - (\delta_q - 2)\,\theta_{k-1}$.

Lemma 2.4.2

Every line contains either at most Δ_q *or at least* $q - \Delta_q + 2$ *points of* $\mathrm{supp}(c)$.

Proof. If q is prime, the proof is finished by Lemma 2.3.2, so assume q not to be prime and suppose, to the contrary, that ℓ is an m-secant to $\mathrm{supp}(c)$ with $\Delta_q + 1 \leqslant m \leqslant q - \Delta_q + 1$.
We first consider the case that $\Delta_q + 2 \leqslant m \leqslant q - \Delta_q$. By Proposition 2.3.1, any plane through ℓ has to contain at least $(\Delta_q + 1)(q+1) + 1$ points of $\mathrm{supp}(c)$, which leads to the following contradiction:

$$\begin{aligned}
\mathrm{wt}(c) &\geqslant \left((\Delta_q + 1)(q+1) + 1 - m\right)\theta_{d-2} + m \\
&\geqslant \left((\Delta_q + 1)(q+1) + 1 - (q - \Delta_q)\right)\theta_{d-2} + m \\
&> q\Delta_q\theta_{d-2} + m \\
&= \Delta_q\theta_{d-1} + m - \Delta_q > W(d,q)\,.
\end{aligned}$$

As a result, every line contains either at most $\Delta_q + 1$ or at least $q - \Delta_q + 1$ points of $\mathrm{supp}(c)$. Due to Lemma 2.3.3, it suffices to prove that there cannot exist a $(\Delta_q + 1)$-secant to $\mathrm{supp}(c)$.
Suppose, to the contrary, that ℓ is a $(\Delta_q + 1)$-secant. Then Proposition 2.3.1 states that each plane through ℓ contains at least

$$(\Delta_q + 1)(q - \Delta_q + 1) = q\Delta_q + q - \Delta_q^2 + 1$$

points of $\mathrm{supp}(c)$, implying that

$$\begin{aligned}
\mathrm{wt}(c) &\geqslant \left(q\Delta_q + q - \Delta_q^2 + 1 - (\Delta_q + 1)\right)\theta_{d-2} + \Delta_q + 1 \\
&= \Delta_q\theta_{d-1} + \left(q - \Delta_q^2 - \Delta_q\right)\theta_{d-2} + 1 \\
&> \Delta_q\theta_{d-1} + \left(q - (\sqrt{q} - 1)^2 - (\sqrt{q} - 1)\right)\theta_{d-2} + 1 \\
&= \Delta_q\theta_{d-1} + \sqrt{q}\theta_{d-2} + 1,
\end{aligned}$$

a contradiction. ∎

Lemma 2.4.3

Every line is either thin or thick.

Proof. Consider an arbitrary line ℓ. If all planes through ℓ are not thin, then, by Lemma 2.4.2 and Theorem 2.2.1, each such plane contains at least $q^2 - (\Delta_q - 2)(q+1)$ points of $\mathrm{supp}(c)$, implying that

$$\begin{aligned}\mathrm{wt}(c) &\geqslant \left(q^2 - (\Delta_q - 2)(q+1) - (q+1)\right)\theta_{d-2} + q + 1\\ &> \left(q^2 - (\sqrt{q} - 2)(q+1)\right)\theta_{d-2} + q + 1\\ &= \left(q - \sqrt{q} + 2 - \frac{1}{\sqrt{q}} + \frac{2}{q}\right)\theta_{d-1} + \sqrt{q} - 1 + \frac{1}{\sqrt{q}} - \frac{2}{q}\\ &> (q - \sqrt{q})\,\theta_{d-1},\end{aligned}$$

contradicting the weight assumption on c. Therefore, there exists a thin plane π through ℓ. By Result 1.1.3, $c|_\pi$ is a linear combination of exactly $\left\lceil \frac{\mathrm{wt}(c|_\pi)}{q+1} \right\rceil =: n$ lines of π. If $n > \delta_q$, then we can find a line in π containing more than δ_q but less than $q - \Delta_q + 2$ points of $\mathrm{supp}(c|_\pi)$, thus $n \leqslant \delta_q$. Therefore, all lines of π, including the line ℓ, are either thin or contain at least $q + 1 - (n-1) \geqslant q - \delta_q + 2$ points of $\mathrm{supp}(c)$. ∎

Corollary 2.4.4

Every k-subspace is either thin or thick.

Proof. This follows from Lemma 2.4.3 and Theorem 2.2.1. ∎

Corollary 2.4.5

$\mathrm{wt}(c) \leqslant \delta_q \theta_{d-1}$.

Proof. This is a direct consequence of Corollary 2.4.4, as the whole space cannot be thick due to $\mathrm{wt}(c) \leqslant W(d,q)$. ∎

Proposition 2.4.6

If c is a linear combination of exactly δ_q hyperplanes, then $\delta_q = \left\lceil \frac{\mathrm{wt}(c)}{\theta_{d-1}} \right\rceil$.

Proof. As every two distinct hyperplanes have θ_{d-2} points in common, we can naively state that

$$\begin{aligned}\mathrm{wt}(c) &\geqslant \delta_q \left(\theta_{d-1} - \left(\delta_q - 1\right)\theta_{d-2}\right) \\ &= \left(\delta_q - \frac{\delta_q^2 - \delta_q}{q}\right)\theta_{d-1} + \frac{\delta_q^2 - \delta_q}{q} > \left(\delta_q - 1\right)\theta_{d-1}.\end{aligned}$$

Combining this with Corollary 2.4.5, we obtain $\delta_q - 1 < \left\lceil \frac{\mathrm{wt}(c)}{\theta_{d-1}} \right\rceil \leqslant \delta_q$. ∎

Lemma 2.4.7

If there exists a thick hyperplane, then c is a linear combination of exactly $\left\lceil \frac{\mathrm{wt}(c)}{\theta_{d-1}} \right\rceil$ hyperplanes.

Proof. Let Π be a thick hyperplane, consider a point $Q \in \Pi$ and denote by x the number of thick lines in Π through Q. Making use of Lemma 2.4.3, we get

$$q^{d-1} - \left(\delta_q - 2\right)\theta_{d-2} \leqslant \mathrm{wt}(c|_\Pi) \leqslant \left(\theta_{d-2} - x\right)\delta_q + xq + 1,$$

which implies that

$$\begin{aligned}x &\geqslant \frac{q^{d-1}}{q - \delta_q} - \frac{\left(2\delta_q - 2\right)\theta_{d-2} + 1}{q - \delta_q} \\ &= \frac{q^{d-1}}{q - \delta_q} - \frac{2\delta_q}{q - \delta_q}q^{d-2} + \frac{2q^{d-2} - 2\left(\delta_q - 1\right)\theta_{d-3} - 1}{q - \delta_q} \\ &\geqslant \left(1 - \frac{2\delta_q}{q - \delta_q}\right)q^{d-2}. \qquad (2.10)\end{aligned}$$

Consider a δ_q-secant ℓ to $\mathrm{supp}(c)$. By Lemma 2.3.4, ℓ cannot be contained in the thick hyperplane Π and therefore intersects it in a point P. By Lemma 2.3.4, every plane π spanned by ℓ and a thick line t through P is a unique thin plane. Moreover, by Result 1.1.3, $c|_\pi$ is a linear combination of exactly δ_q (thick) lines. This implies that t is one of these lines, that $P \in \mathrm{supp}(c)$ (as each of the points of $\mathrm{supp}(c|_\ell)$ lies on precisely one thick line of π), and hence that at least $q - \delta_q + 2$ points of t have the non-zero value $c(P)$. By (2.10), at least

$$\left(1 - \frac{2\delta_q}{q - \delta_q}\right) q^{d-2} \left(q - \delta_q + 2 - 1\right)$$

points of Π have the same non-zero value with respect to c. The above expression is at least $\left(\frac{q-6}{q-2}\right) q^{d-2} (q-1) > \frac{1}{2}\theta_{d-1}$ if q is prime and is at least

$$\left(1 - \frac{2\left(\sqrt{q}-1\right)}{q - \sqrt{q}+1}\right)\left(q - \sqrt{q}+1\right) q^{d-2} = \left(q - 3\sqrt{q}+3\right)(q-1) \cdot \frac{q^{d-2}}{q-1}$$
$$\geqslant \frac{q^2}{2} \cdot \frac{q^{d-2}}{q-1} > \frac{1}{2}\frac{q^d-1}{q-1} = \frac{1}{2}\theta_{d-1}$$

if q is not prime.

In conclusion, more than half of the points in Π have a non-zero value $\alpha := c(P)$. This means that $c - \alpha v_\Pi$ is a codeword of a smaller weight than c, where v_Π is the incidence vector of Π.

Now suppose, to the contrary, that c is a codeword of minimal weight, $\mathrm{wt}(c) \leqslant \Delta_q\theta_{d-1}$, with the property that c cannot be written as a linear combination of at most δ_q hyperplanes. Due to the minimal weight of c, the codeword $c - \alpha v_\Pi$ must be equal to a linear combination of at most δ_q hyperplanes, which means that c has to be a linear combination of at most, therefore *precisely*, $\delta_q + 1$ hyperplanes. This, however, implies the existence of a $(\delta_q + 1)$-secant to $\mathrm{supp}(c)$, contradicting the definition of δ_q. We conclude that c is equal to a linear combination of exactly δ_q hyperplanes, hence Proposition 2.4.6 finishes the proof. ∎

Theorem 2.4.8

Let $d \geqslant 2$, $q \geqslant 32$, and consider a codeword $c \in \mathcal{C}_{d-1}(d,q)$ with

$$\mathrm{wt}(c) \leqslant \begin{cases} 3\left(1-\frac{3}{q}\right)\theta_{d-1} & \text{if } q \text{ is prime,} \\ \left(\left\lfloor \frac{1}{2}\sqrt{q}-\frac{9}{4}\right\rfloor -1\right)\theta_{d-1} & \text{if } q \text{ is the square of a prime,} \\ \left(\left\lfloor \sqrt{q}-\frac{1}{2}\right\rfloor -1\right)\theta_{d-1} & \text{otherwise.} \end{cases}$$

Then c is a linear combination of exactly $\left\lceil \frac{\mathrm{wt}(c)}{\theta_{d-1}} \right\rceil$ hyperplanes.

Proof. By Corollary 2.4.5, we may assume that $\delta_q \geqslant 1$.
We proceed by induction on d. The base case follows directly from Result 1.1.3, hence assume that $d \geqslant 3$. Due to Corollary 2.4.4, we may formulate the induction hypothesis as follows: every hyperplane Π is either thin or thick, and in the former case, the codeword $c|_\Pi$ is a linear combination of exactly $\left\lceil \frac{\mathrm{wt}(c|_\Pi)}{\theta_{d-2}} \right\rceil$ $(d-2)$-subspaces of Π. Due to Lemma 2.4.7, it suffices to prove that there exists a thick hyperplane.
Consider a δ_q-secant ℓ. By Proposition 2.3.1, all planes through ℓ contain at least $\delta_q\left(q-\delta_q+2\right)$ points of $\mathrm{supp}(c)$, which implies that

$$\begin{aligned} \mathrm{wt}(c) &\geqslant \left(\delta_q\left(q-\delta_q+2\right)-\delta_q\right)\theta_{d-2}+\delta_q \\ &= \delta_q q^{d-1} - \left(\delta_q^2 - 2\delta_q\right)\theta_{d-2}. \end{aligned} \tag{2.11}$$

Now suppose, to the contrary, that all hyperplanes are thin. Let Π be a thin hyperplane through ℓ. By the induction hypothesis, $c|_\Pi$ is a linear combination of exactly δ_q $(d-2)$-subspaces of Π. Let Σ be one of these $(d-2)$-subspaces. Any hyperplane Π' through Σ is assumed to be thin, hence all points of $\mathrm{supp}(c|_{\Pi'})$ are covered by Σ and $\delta_q - 1$ other $(d-2)$-subspaces of Π', implying that

$$\mathrm{wt}(c) \leqslant (q+1)\left(\delta_q-1\right)q^{d-2}+\theta_{d-2} = \left(\delta_q-1\right)q^{d-1}+\delta_q q^{d-2}+\theta_{d-3}.$$

Combining this with (2.11), we obtain

$$\begin{aligned}\left(\delta_q - 1\right) q^{d-1} + \delta_q q^{d-2} + \theta_{d-3} &\geqslant \delta_q q^{d-1} - \left(\delta_q^2 - 2\delta_q\right) \theta_{d-2} \\ \iff \quad 0 &\geqslant q^{d-1} - \left(\delta_q^2 - \delta_q\right) q^{d-2} - \left(\delta_q - 1\right)^2 \theta_{d-3}.\end{aligned}$$

Using that $\delta_q^2 - \delta_q < \left(\sqrt{q} - 1\right)^2 - \left(\sqrt{q} - 1\right)$ and $\left(\delta_q - 1\right)^2 < q - 1$, we get

$$0 > 3\left(\sqrt{q} - 1\right) q^{d-2} + 1,$$

a contradiction. ∎

3 Odd small weight codewords

Just as Chapter 2, we focus on characterising small weight codewords of $\mathcal{C}_{d-1}(d,q)$, $d \geqslant 3$, but only consider the case of q prime, allowing the existence of odd codewords. This makes the quest of characterising small weight codewords significantly more difficult, as the key argument in the proof of Lemma 2.4.7 cannot be applied here.

If q is prime and $q \geqslant 53$, we show that all codewords up to weight $4\left(1-\frac{8}{q}\right)\theta_{d-1}$ are equal to a linear combination of hyperplanes through a common $(d-3)$-subspace (see Theorem 3.3.2). This turns out to be equivalent to stating that such codewords are equal to either a linear combination of at most three hyperplanes or a certain generalisation of Configuration 1.1.2 (see Lemma 3.1.2).

The results presented in this chapter are slight improvements on the ones given in [3].

ASSUMPTION

Throughout this *chapter*, we assume that $d \geqslant 3$ and q is prime, $q \geqslant 53$, and fix a codeword $c \in \mathcal{C}_{d-1}(d,q)$ such that

$$3\left(1-\frac{3}{q}\right)\theta_{d-1} < \mathrm{wt}(c) \leqslant 4\left(1-\frac{8}{q}\right)\theta_{d-1}.$$

Corollary 3.0.1

Every k-subspace contains either

$$\textit{at most } 3\theta_{k-1} \qquad \textit{or} \qquad \textit{at least } q^k - \theta_{k-1}$$

points of $\mathrm{supp}(c)$.

Proof. This follows directly from Lemma 2.3.2 and Theorem 2.2.1. ∎

3.1 Codeword and subspace types

Using Results 0.2.1 and 1.1.3, we say that any plane π, or similarly that any codeword $c|_\pi$, has **type**

- T_0 if $c|_\pi = \mathbf{0}$,
- T_1 if $c|_\pi$ is a non-zero scalar multiple of a line,
- T_2 if $c|_\pi$ is a linear combination of precisely two lines,
- T_3^{odd} if $c|_\pi$ is a codeword as described in Configuration 1.1.2,
- $T_3^{\triangle}$ if $c|_\pi$ is a linear combination of three nonconcurrent lines, or
- $T_3^{\bigstar}$ if $c|_\pi$ is a linear combination of precisely three concurrent lines.

Define

$$\boldsymbol{\mathcal{T}} := \{T_0, T_1, T_2\} \cup \boldsymbol{\mathcal{T}}_3 \quad \text{where} \quad \boldsymbol{\mathcal{T}}_3 := \left\{T_3^{\mathrm{odd}}, T_3^{\triangle}, T_3^{\bigstar}\right\}.$$

For convenience, we say that the plane π, or the codeword $c|_\pi$, has **type** $\boldsymbol{\mathcal{T}}$ if it has some type $T \in \boldsymbol{\mathcal{T}}$. If π or $c|_\pi$ does not have type $\boldsymbol{\mathcal{T}}$, we say that they are of type $\boldsymbol{\mathcal{O}}$.

Corollary 3.1.1

Every plane of type $\mathcal{O}$ contains at least $q^2 - q - 1$ points of $\mathrm{supp}(c)$.

Proof. This is a consequence of Corollary 3.0.1 and the fact, due to Result 1.1.3, that any plane of type $\mathcal{O}$ contains at least $4q - 21$ points of $\mathrm{supp}(c)$. ∎

Lemma 3.1.2

Consider a k-subspace Π, $k \geqslant 2$, and let κ be a $(k-3)$-subspace of Π. Then $c|_\Pi$ is a linear combination of $(k-1)$-subspaces through κ if and only if there exist a plane $\pi \subset \Pi$ disjoint to κ and a scalar $\mu \in \mathbb{F}_p$ such that

$$c|_\Pi(P) = \begin{cases} \mu & \text{if } P \in \kappa, \\ c(\langle P, \kappa \rangle \cap \pi) & \text{if } P \in \Pi \setminus \kappa. \end{cases} \tag{3.1}$$

If this holds for some plane π, then it holds for all planes in Π disjoint to κ. Moreover, if π has type $T \in \mathcal{T}$, then those planes have type T as well.

Proof. Assume that $c|_\Pi$ is a linear combination of $(k-1)$-subspaces through κ. All points of κ lie in each of these $(k-1)$-subspaces and hence have the same value with respect to $c|_\Pi$. A $(k-1)$-subspace through κ contains a point $P \in \Pi \setminus \kappa$ if and only if it contains $\langle P, \kappa \rangle$. Therefore, all points lying in a $(k-2)$-subspace through κ but not in κ, are contained in the same $(k-1)$-subspaces through κ and thus have the same value with respect to c. The fact that any plane in Π disjoint to κ intersects every $(k-2)$-subspace through κ in a point concludes this part of the proof.
Conversely, assume that there exist a plane $\pi \subset \Pi$ disjoint to κ and a scalar $\mu \in \mathbb{F}_p$ such that all points $P \in \Pi$ satisfy (3.1). If $c|_\pi = \sum_i \alpha_i \ell_i$, with $\alpha_i \in \mathbb{F}_p$ and ℓ_i lines in π, then $c|_\Pi$ takes the same values as the codeword $\sum_i \alpha_i \langle \ell_i, \kappa \rangle$ in all points of $\Pi \setminus \kappa$. Therefore, their Hamming distance is at most $\theta_{k-3} < \theta_{k-1}$, thus, by Result 1.0.1, they must be equal. Hence, $c|_\Pi$ is a linear combination of $(k-1)$-subspaces through κ.

Consider a plane σ in Π disjoint to κ. Since $c|_\Pi$ is a linear combination of $(k-1)$-subspaces through κ, the first part of the proof implies that (3.1) holds when replacing π with σ. Moreover, $c|_\sigma = \sum_i \alpha_i \left(\langle \ell_i, \kappa\rangle \cap \sigma\right)$. Note that mapping ℓ_i onto $\langle \ell_i, \kappa\rangle \cap \sigma$ induces a collineation from $\pi \cong \mathrm{PG}(2,q)$ to $\sigma \cong \mathrm{PG}(2,q)$. This directly implies that if $c|_\pi$ has type $T \in \boldsymbol{\mathcal{T}}$, $c|_\sigma$ must be of type T as well. ∎

Thanks to the above lemma, we can unambiguously extend the notion of *type* to arbitrary subspaces. We say that any k-subspace Π of $\mathrm{PG}(d,q)$, $k \geqslant 2$, or similarly that any codeword $c|_\Pi$, has **type** $T \in \boldsymbol{\mathcal{T}}$ if

(1) there exists a $(k-3)$-subspace $\kappa \subset \Pi$, called an **apex**, and

(2) there exists a plane $\pi \subset \Pi$ of type T disjoint to κ,

such that $c|_\Pi$ is a linear combination of $(k-1)$-subspaces through κ, or equivalently, such that κ and π satisfy (3.1) for some scalar $\mu \in \mathbb{F}_p$. We say that Π, or $c|_\Pi$, has **type** $\boldsymbol{\mathcal{T}}$ if it has some type $T \in \boldsymbol{\mathcal{T}}$, else we say that it is of type $\boldsymbol{\mathcal{O}}$.

Proposition 3.1.3

Suppose that Π is a hyperplane of type $T \in \boldsymbol{\mathcal{T}}_3$, with κ a $(d-4)$-dimensional apex of Π. Let ℓ be a 3-secant contained in Π. Then ℓ is disjoint to κ. The q^{d-3} planes through ℓ that are disjoint to κ are planes of type T, while the other θ_{d-4} planes through ℓ have type $T_3^\bigstar$.

Proof. This follows immediately from Lemma 3.1.2. ∎

The main goal is to prove that the codeword c has type $\boldsymbol{\mathcal{T}}$. As mentioned at the start of this chapter, this is equivalent to saying that c is equal to a linear combination of hyperplanes through a common $(d-3)$-subspace. After all, by Lemma 3.1.2, c having type $\boldsymbol{\mathcal{T}}$ is equivalent to the existence of a $(d-3)$-dimensional apex κ and a plane π of type $\boldsymbol{\mathcal{T}}$ disjoint to κ such that all points satisfy (3.1) for some scalar $\mu \in \mathbb{F}_p$. Therefore, $\mathrm{wt}(c) = \mathrm{wt}(c|_\pi)\, q^{d-2} + \delta\theta_{d-3}$, with $\delta = 0$ if $\mu = 0$ and $\delta = 1$ otherwise. Since

$\mathrm{wt}(c) \leqslant 4\left(1-\frac{8}{q}\right)\theta_{d-1}$, this implies that

$$\mathrm{wt}(c|_\pi) \leqslant 4\left(1-\frac{8}{q}\right)\frac{\theta_{d-1}}{q^{d-2}} \leqslant 4q-22$$

and thus, by Result 1.1.3, π has type $\boldsymbol{\mathcal{T}}$.

3.2 The power of the 3-secant

Before getting to the main result, we first need some properties about certain types of subspaces sharing a specific line.

Definition 3.2.1 (long line)

A line is called **long** if it contains at least $q-1$ points of $\mathrm{supp}(c)$.

Lemma 3.2.2

Let π be a plane of type $T \in \left\{T_3^{\mathrm{odd}}, T_3^{\triangle}\right\}$. Then all planes σ of type $\boldsymbol{\mathcal{T}}$ intersecting π in a long line are planes of type T as well. Moreover, $\mathrm{wt}(c|_\sigma) = \mathrm{wt}(c|_\pi)$.

Proof. Suppose that the plane $\sigma \neq \pi$ is a plane of type $T^{(\sigma)} \in \boldsymbol{\mathcal{T}}$ and let ℓ denote the long line $\pi \cap \sigma$. As $T \in \left\{T_3^{\mathrm{odd}}, T_3^{\triangle}\right\}$, no q points of ℓ have the same non-zero value with respect to c. As a consequence, $T^{(\sigma)} \notin \left\{T_0, T_1, T_2, T_3^{\bigstar}\right\}$. If $T = T_3^{\mathrm{odd}}$, we find at least q points on ℓ with distinct values. If $T = T_3^{\triangle}$, we find at most 3 points on ℓ with distinct values. Hence, if $T^{(\sigma)} \neq T$, then $q \leqslant 3$, a contradiction. Furthermore, it is not hard to check that the set of values of points in ℓ fixes the weight of $c|_\sigma$. ∎

Lemma 3.2.3

There exists a 3-secant to $\mathrm{supp}(c)$.

Proof. Suppose the contrary. By Corollary 3.0.1 and Lemma 2.3.3, all lines intersect $\mathrm{supp}(c)$ in at most 2 or in at least q points. As a consequence, Theorem 2.2.1 (where $k := d$) contradicts the weight assumption on c. ∎

Lemma 3.2.4

If κ is a k-subspace containing a 3-secant, then $\mathrm{wt}(c|_\kappa) \leqslant 3\theta_{k-1}$. In particular, all planes containing a 3-secant have type $\boldsymbol{\mathcal{T}}$.

Proof. Due to the weight assumption on c, Corollary 3.0.1 implies that $\mathrm{wt}(c) \leqslant 3\theta_{d-1}$. The statement therefore follows from Lemma 2.3.4. ∎

Lemma 3.2.5

Let κ and $\widetilde{\kappa}$ be two k-subspaces, $k \geqslant 2$, of type $T, \widetilde{T} \in \boldsymbol{\mathcal{T}}_3$, respectively, having a 3-secant s in common. Then at least one of the following holds:

(1) $T = T_3^{\bigstar}$.

(2) $\widetilde{T} = T_3^{\bigstar}$.

(3) $T = \widetilde{T}$.

Furthermore, if $T = \widetilde{T}$, then $\mathrm{wt}(c|_\kappa) = \mathrm{wt}(c|_{\widetilde{\kappa}})$.

Proof. Consider two planes π and $\widetilde{\pi}$ through s lying in κ and $\widetilde{\kappa}$, respectively, but disjoint to their respective apexes. By definition, these planes inherit the type of their corresponding k-subspace. Define $\Sigma := \langle \pi, \widetilde{\pi} \rangle$.
Furthermore, let P_α, P_β and P_γ be the points of $\mathrm{supp}(c|_s)$ with corresponding non-zero values $\alpha, \beta, \gamma \in \mathbb{F}_p$ with respect to c. For every $x \in \{\alpha, \beta, \gamma\}$, let ℓ_x, respectively $\widetilde{\ell}_x$, be the unique long lines in π, respectively $\widetilde{\pi}$, through P_x.

Case 1: $T \neq \widetilde{T}$.

Suppose, to the contrary, that $T \neq T_3^{\bigstar} \neq \widetilde{T}$. Without loss of generality, we may assume that $T = T_3^{\text{odd}}$ and $\widetilde{T} = T_3^{\triangle}$.
Consider a plane $\sigma \subset \Sigma$ through $\widetilde{\ell_\alpha}$. Note that $\widetilde{\ell_\alpha}$ is a long line containing $q-1$ points with non-zero value α, one point with value $\alpha+\beta$ and one point with value $\alpha+\gamma$. Therefore, the plane σ *cannot* be

- a plane of type T_0, as $\alpha \neq 0$.
- a plane of type T_1, T_2 or $T_3^{\bigstar}$, else $\alpha+\beta=\alpha$ or $\alpha+\gamma=\alpha$.
- a plane of type T_3^{odd}, as $\widetilde{\ell_\alpha}$ contains at least 3 points with the same value α.
- a plane of type $T_3^{\triangle}$, unless each 3-secant in σ contains points with values α, β and γ as well. This is unambiguously determined by the two points of $\widetilde{\ell_\alpha}$ with values $\alpha+\beta$ and $\alpha+\gamma$.

However, the plane σ can only have type $T_3^{\triangle}$ in a few cases. Suppose that σ has type $T_3^{\triangle}$ and intersects π in a 3-secant t. One of the points of $\text{supp}(c|_t)$ must be P_α, as this point belongs to both $\widetilde{\ell_\alpha}$ and π. The other two points of $\text{supp}(c|_t)$ lie in ℓ_β and ℓ_γ and must have (not necessarily corresponding) values β and γ. As π is a plane of type T_3^{odd}, there are only two possibilities for σ to intersect π, namely when the β-valued point of t lies in ℓ_β (then $\sigma = \widetilde{\pi}$), or when the β-valued point of t lies in ℓ_γ. In conclusion, of the at least $q-2$ planes through $\widetilde{\ell_\alpha}$ in Σ that intersect π in a 3-secant, at least $q-4$ of them cannot be a plane of type $T_3^{\triangle}$ and thus must be planes of type $\mathcal{O}$. In addition, the plane $\left\langle \ell_\alpha, \widetilde{\ell_\alpha} \right\rangle$ can never be a plane of type $T_3^{\triangle}$ as well, as ℓ_α contains many differently valued points. Thus, we find at least $q-3$ planes of type $\mathcal{O}$ in Σ through $\widetilde{\ell_\alpha}$, each containing at least q^2-q-1 points of $\text{supp}(c)$ due to Corollary 3.1.1. By Proposition 2.3.1, each of the other planes in Σ through $\widetilde{\ell_\alpha}$ contains at least $3q-3$ points of $\text{supp}(c)$. We get

$$\begin{aligned} \text{wt}(c|_\Sigma) &\geqslant \left(q^2-q-1\right)(q-3) + 4\,(3q-3) - q\,(q+1) \\ &= q^3 - 5q^2 + 13q - 9, \end{aligned}$$

which contradicts Lemma 3.2.4.

Case 2: $T = \widetilde{T}$.

Suppose, to the contrary, that $\mathrm{wt}(c|_\kappa) \neq \mathrm{wt}(c|_{\widetilde{\kappa}})$. Without loss of generality, we can assume that $\mathrm{wt}(c|_\pi) \neq \mathrm{wt}(c|_{\widetilde{\pi}})$ as well.
First, assume that $T = \widetilde{T} \in \left\{T_3^{\mathrm{odd}}, T_3^{\bigstar}\right\}$. By analysing the types of these planes and by Configuration 1.1.2, $\mathrm{wt}(c|_\pi) \neq \mathrm{wt}(c|_{\widetilde{\pi}})$ implies that both $\alpha+\beta+\gamma = 0$ and $\alpha+\beta+\gamma \neq 0$, a contradiction.
Now assume that $T = \widetilde{T} = T_3^{\triangle}$ and consider the pairs of values of the points $\ell_\alpha \cap \ell_\beta$ and $\widetilde{\ell_\alpha} \cap \widetilde{\ell_\beta}$, $\ell_\beta \cap \ell_\gamma$ and $\widetilde{\ell_\beta} \cap \widetilde{\ell_\gamma}$, and $\ell_\alpha \cap \ell_\gamma$ and $\widetilde{\ell_\alpha} \cap \widetilde{\ell_\gamma}$. As $\mathrm{wt}(c|_\pi) \neq \mathrm{wt}(c|_{\widetilde{\pi}})$, at least one of these pairs of values consists of a zero value and a non-zero value, implying conflicting conditions on the corresponding values. ∎

Lemma 3.2.6

No 3-secant is contained in θ_{d-2} hyperplanes of the same type $T \in \left\{T_3^{\mathrm{odd}}, T_3^{\triangle}\right\}$.

Proof. Suppose, to the contrary, that there exists a 3-secant s with the described property.

Case 1: $d = 3$.

Fix a plane π through s. By Lemma 3.2.5, the weight of the codeword c is known, as we can count:

$$\mathrm{wt}(c) = (q+1)\left(\mathrm{wt}(c|_\pi) - 3\right) + 3 = (q+1)\,\mathrm{wt}(c|_\pi) - 3q. \tag{3.2}$$

Note that, regardless of whether π is a plane of type T_3^{odd} or $T_3^{\triangle}$, we can always find a 2-secant r in π such that s and r intersect in a point $P \in \mathrm{supp}(c)$. Consider an arbitrary plane σ through r, different from π. There exists a long line ℓ in σ through P, as else $\mathrm{wt}(c|_\sigma) \leqslant \mathrm{wt}(c|_r) + 2q = 2\,(q+1)$,

which implies, by Result 1.1.3, that there *does* exist a long line in σ through P, a contradiction. Now consider the plane $\langle s, \ell \rangle$. As it contains the 3-secant s, it has the same type as π. However, by Lemma 3.2.2, the plane $\langle s, \ell \rangle$ has the same type as σ as well, as they share the long line ℓ, unless σ is a plane of type $\mathcal{O}$.
In conclusion, any plane σ through r satisfies either $\mathrm{wt}(c|_\sigma) = \mathrm{wt}(c|_\pi)$ (if σ is a plane of type $\mathcal{T}$), or $\mathrm{wt}(c|_\sigma) \geqslant 4q - 21 \geqslant \mathrm{wt}(c|_\pi)$ (if σ is a plane of type $\mathcal{O}$). In both cases, this yields a lower bound on $\mathrm{wt}(c)$, which, combined with (3.2), results in

$$(q+1)\,\mathrm{wt}(c|_\pi) - 3q = \mathrm{wt}(c) \geqslant (q+1)\,(\mathrm{wt}(c|_\pi) - 2) + 2,$$

a contradiction.

Case 2: $d \geqslant 4$.

Define

$$S \coloneqq \{(\pi, \Pi) : s \subset \pi \subset \Pi, \pi \text{ a plane}, \Pi \text{ a hyperplane, both of type } T\}.$$

Fix an arbitrary plane $\pi_0 \supset s$ of type T. As all hyperplanes through s are of the same type T, all hyperplanes through π_0 have this property as well. Thus, the number of elements in S with a fixed first argument π_0 equals θ_{d-3}.
Fix an arbitrary hyperplane $\Pi_0 \supset s$ of type T. By Proposition 3.1.3, the number of elements in S with a fixed second argument Π_0 equals q^{d-3}.
Let x_π be the total number of type-T planes through s. By double counting, we get

$$\begin{aligned} & x_\pi \cdot \theta_{d-3} = |S| = \theta_{d-2} \cdot q^{d-3} \\ \iff\ & x_\pi = \frac{q^{d-1}-1}{q^{d-2}-1} q^{d-3} = q^{d-2} + 1 - \frac{q^{d-3}-1}{q^{d-2}-1}. \end{aligned}$$

As x_π is an integer, the fraction on the right-hand side of the latter equation must also be an integer. This is never the case if $d \geqslant 4$. ∎

3.3 Knitting codewords together

One last, technical lemma is needed before presenting the main result of this chapter.

Lemma 3.3.1

Consider, for $i \in \{1,2\}$, a hyperplane Π_i of type $T_3^\star$ and let $\mathcal{S}_i$ be the set of its three $(d-2)$-subspaces present in the linear combination $c|_{\Pi_i}$, which therefore intersect in a common $(d-3)$-subspace κ_i. If $\mathcal{S}_1 \cap \mathcal{S}_2 \neq \varnothing$, then $\kappa_1 = \kappa_2$.

Proof. Let Σ be a $(d-2)$-subspace that $\mathcal{S}_1$ and $\mathcal{S}_2$ have in common and suppose, to the contrary, that $\kappa_1 \neq \kappa_2$. As these are subspaces of the same dimension, we can find points $P_1 \in \kappa_1 \setminus \kappa_2$ and $P_2 \in \kappa_2 \setminus \kappa_1$ which define a line $\ell := \langle P_1, P_2 \rangle$. All points of $\Sigma \setminus \kappa_i$ lie in $\mathrm{supp}(c)$ and every point of ℓ is contained in $\Sigma \setminus \kappa_i$ for at least one choice of i, which implies that ℓ must be a $(q+1)$-secant to $\mathrm{supp}(c)$. Now consider, for each $i \in \{1,2\}$, a plane π_i in Π_i through ℓ not contained in Σ. Due to this choice, the plane π_i intersects each $(d-2)$-subspace of $\mathcal{S}_i$ in a line (through P_i). Define $\sigma := \langle \pi_1, \pi_2 \rangle$.
Choose a $(q+1)$-secant $\widetilde{\ell}$ in π_1, different from ℓ. As $P_1 \neq P_2$, all planes in σ through $\widetilde{\ell}$ (different to π_1) intersect π_2 in a 3-secant and thus, by Lemma 3.2.4, are planes of type $\boldsymbol{\mathcal{T}}$. As π_1 is a plane of type $\boldsymbol{\mathcal{T}}$ as well, we conclude that all planes in σ through $\widetilde{\ell}$ are planes of type $\boldsymbol{\mathcal{T}}$.
This means that $\mathrm{wt}(c|_\sigma) \leqslant q(2q) + (3q+1) = 2q^2 + 3q + 1 \leqslant 3\left(1 - \frac{3}{q}\right)\theta_2$.
By Theorem 2.4.8, $c|_\sigma$ is a linear combination of at most two planes. As $\widetilde{\ell}$ necessarily lies in one of such planes, we see that not all planes through $\widetilde{\ell}$ in σ can be of type $\boldsymbol{\mathcal{T}}$, resulting in a contradiction. ∎

Theorem 3.3.2

Let $d \geqslant 2$, $q \geqslant 53$ prime, and consider a codeword $c \in \mathcal{C}_{d-1}(d,q)$ with $\mathrm{wt}(c) \leqslant 4\left(1-\frac{8}{q}\right)\theta_{d-1}$. Then c is a linear combination of hyperplanes through a common $(d-3)$-subspace.

Proof. If $\mathrm{wt}(c) \leqslant 3\left(1-\frac{3}{q}\right)\theta_{d-1}$, then Theorem 2.4.8 proves the statement, so assume that $3\left(1-\frac{3}{q}\right)\theta_{d-1} < \mathrm{wt}(c) \leqslant 4\left(1-\frac{8}{q}\right)\theta_{d-1}$. We will prove that there exist a $(d-3)$-subspace κ and a plane π satisfying (3.1) of Lemma 3.1.2; this will be done by induction on d.
If $d = 2$, we refer to Result 1.1.3. Assume that $d \geqslant 3$ and suppose that the statement is true for c restricted to any k-subspace, $2 \leqslant k < d$, given that the weight of this restricted codeword is at most $4\left(1-\frac{8}{q}\right)\theta_{k-1}$. By Lemma 3.2.3, there exists a 3-secant s with corresponding non-zero values α, β and γ. By the induction hypothesis and Lemma 3.2.4, each hyperplane through s is a hyperplane of type $\boldsymbol{\mathcal{T}}$. Therefore, by Lemma 3.2.5, there exist two types $T_A = T_3^{\bigstar}$ and $T_B \in \left\{T_3^{\mathrm{odd}}, T_3^{\triangle}\right\}$ such that each of these hyperplanes has either type T_A or T_B. Furthermore, by Lemma 3.2.6, there must exist a hyperplane Π through s of type T_A, which means that

$$c|_\Pi = \alpha\Sigma_1 + \beta\Sigma_2 + \gamma\Sigma_3$$

for certain $(d-2)$-subspaces Σ_i of Π having a $(d-3)$-subspace κ in common. Note that, by Proposition 3.1.3, each plane through s has either type T_A or T_B as well. Now choose a plane π as follows: if all planes through s are planes of type T_A, choose π to be any plane through s not contained in Π. Else, choose π to be a plane through s of type T_B. By Proposition 3.1.3, π cannot be contained in Π.
Note that $c|_\kappa = (\alpha+\beta+\gamma)\cdot\mathbf{1}$. Moreover, as all lines in Π that intersect κ are either 0-, 1-, q- or $(q+1)$-secants, we know that κ must be disjoint to the 3-secant s and hence also be disjoint to the plane $\pi \supset s$, as $\pi \nsubseteq \Pi$.

The only statement left to prove is that, for every point $P \notin \kappa$,

$$c(P) = c(\langle \kappa, P \rangle \cap \pi)\,. \tag{3.3}$$

Choose an arbitrary 3-secant s_1 in π through the point $\Sigma_1 \cap \pi$, thus having corresponding non-zero values α, β_1 and γ_1. By Lemma 3.2.4, the induction hypothesis implies that $\Pi_1 := \langle \Sigma_1, s_1 \rangle$ is a hyperplane of type $\mathcal{T}$. We claim that Π_1 is a hyperplane of type T_A. Indeed, let π_1 be a plane in Π_1 through s_1, thus intersecting Π in a line ℓ of Σ_1. Then this intersection line ℓ must be a line containing at least q points of $\mathrm{supp}(c)$ with non-zero value α. By Lemma 3.2.4, π_1 has to be a plane of type $\mathcal{T}$ and hence, at it contains both ℓ and s_1, a plane of type T_A. By the arbitrary choice of π_1, all planes in Π_1 through s_1 must be planes of type T_A, thus Π_1 contains at least θ_{d-3} planes of type T_A through a fixed 3-secant (s_1). By Proposition 3.1.3, at least one of these planes is of the same type as Π_1, thus this hyperplane must have type T_A. Let κ_1 be the $(d-3)$-subspace of Π_1 in which the three hyperplanes of $c|_{\Pi_1}$ intersect. By Lemma 3.3.1, we know that $\kappa = \kappa_1$. In this way, it is easy to see that all points in $\Pi_1 \setminus \kappa$ fulfil property (3.3).
We can now repeat the above process by choosing another $(d-2)$-subspace Σ_2 in one of the linear combinations of $c|_{\Pi}$ or $c|_{\Pi_1}$ and considering the span $\Pi_2 = \langle \Sigma_2, s_2 \rangle$, with s_2 an arbitrary 3-secant in π through the point $\Sigma_2 \cap \pi$. All points in $\Pi_2 \setminus \kappa$ fulfil property (3.3) as well. To conclude, if, for each point P in π, there exists a sequence of 3-secants $s_1, s_2, \ldots, s_n \ni P$ in π such that $s \cap s_1 \in \mathrm{supp}(c)$ and $s_i \cap s_{i+1} \in \mathrm{supp}(c)$ for all $i \in \{1, 2, \ldots, n-1\}$, then this theorem is proven by consecutively repeating the above arguments. Unfortunately, not all points in π satisfy this property. However, if a point $P \in \pi$ does not lie in such a (sequence of) 3-secant(s), we can easily prove that this point lies in a 0-, 1- or 2-secant r in π of which the other q points are reached by such a (sequence of) 3-secant(s). Thus, we already know the value of many points in the hyperplane $\langle \kappa, r \rangle$. As $\mathrm{wt}\big(c|_{\langle \kappa, r \rangle}\big) \leqslant 2q^{d-2} + \theta_{d-3} + \mathrm{wt}\big(c|_{\langle \kappa, P \rangle}\big) - \mathrm{wt}(c|_{\kappa}) \leqslant 3q^{d-2} + \theta_{d-3} \leqslant 4\left(1 - \frac{8}{q}\right)\theta_{d-2}$, this hyperplane is a hyperplane of type $\mathcal{T}$ by the induction hypothesis. Therefore, all points in $\langle \kappa, r \rangle \setminus \kappa$ must satisfy property (3.3). ∎

4 Minimal small weight codewords

As mentioned before, projective geometric codes are never minimal, as these always contain the all-one vector. In this chapter, we aim to partially characterise the minimal codewords of $\mathcal{C}_{d-1}(d,q)$. To be more precise, we will only consider codewords of small weight and develop a sufficient condition for which these are minimal. All results of Section 4.2 are based on [23].

We first briefly discuss the odd codeword before moving on to the 'ordinary' case, in which codewords are characterised up to a significantly larger weight (see Chapter 2).

4.1 The odd codeword is minimal

Theorem 4.1.1

Let $q \geqslant 19$ be prime. Then any codeword given by Configuration 1.1.2 is minimal.

Proof. Consider a codeword c as described by Configuration 1.1.2 and suppose that $c' \in \mathcal{C}_1(2,q)$ is a non-zero codeword with $\mathrm{supp}(c') \subseteq \mathrm{supp}(c)$. Then $\mathrm{wt}(c') \leqslant \mathrm{wt}(c) \leqslant 3q-2$ and thus, by Result 1.1.3, c' is characterised. Moreover, as there exist three concurrent lines ℓ_1, ℓ_2 and ℓ_3 such that each contains exactly one hole with respect to c that does not lie in any of the other two, the only remaining option is for c' to be given by Configuration 1.1.2 as well. As $\mathrm{supp}(c') \subseteq \mathrm{supp}(c)$, the holes with respect to c lying

in $\ell_1 \cup \ell_2 \cup \ell_3$ different to $S := \ell_1 \cap \ell_2 \cap \ell_3$ are holes with respect to c' as well. Denote these points by H_1, H_2 and H_3, respectively. We adopt the same notation as used in Configuration 1.1.2 when considering the codeword c'. If $\beta := \beta_1 + \beta_2 + \beta_3 = 0$, then H_1, H_2 and H_3 are collinear. Consider a point $P_1 \in \ell_1$ different from S and H_1. Then the line $\langle P, H_2 \rangle$ has to intersect each of the lines ℓ_1, ℓ_2 and ℓ_3 in points with values summing up to $\beta = 0$, implying that $\langle P, H_2 \rangle$ intersects ℓ_3 in a point Q with value $-c'(P)$. In conclusion, the value of P uniquely defines the value of Q with respect to c'. Starting with the point Q and the hole H_1, we can duplicate this argument to obtain a point $R \in \ell_2$ whose value is uniquely determined by the value of Q, and therefore by the value of P. We can now repeat this process until we end up with at least three points on each line, different from S, each of which has a value that is uniquely determined by $c'(P)$. By the way Configuration 1.1.2 is constructed and due to Result 0.1.2, those three points on ℓ_i fix the values of all points lying in a subline of ℓ_i. As q is prime, this subline must be equal to ℓ_i.
If $\beta \neq 0$, then H_1, H_2 and H_3 are not collinear. The lines $\langle H_1, H_2 \rangle$, $\langle H_2, H_3 \rangle$ and $\langle H_1, H_3 \rangle$ have to intersect each of the lines ℓ_1, ℓ_2 and ℓ_3 in points with values summing up to β, implying that their unique respective intersection points P_1, P_2 and P_3 of $\mathrm{supp}(c')$ have value β. Repeating this argument with P_1, P_2 and P_3 instead of H_1, H_2 and H_3, we yet again find at least three points in each line, different from S, each of which has a value that is uniquely determined by β. ∎

Naturally, one can ask the same question of minimality in case $d \geqslant 3$ and $q \geqslant 53$ is prime. By Theorem 3.3.2, any codeword $c \in \mathcal{C}_{d-1}(d, q)$ of weight at most

$$4\left(1 - \frac{8}{q}\right)\theta_{d-1}$$

is equal to a linear combination of hyperplanes through a common $(d-3)$-subspace κ, which, by Lemma 3.1.2, is equivalent to stating that there exist

a plane π disjoint to κ and a scalar $\mu \in \mathbb{F}_p$ such that

$$c(P) = \begin{cases} \mu & \text{if } P \in \kappa, \\ c(\langle P, \kappa \rangle \cap \pi) & \text{if } P \notin \kappa. \end{cases}$$

If $c|_\pi$ is given by Configuration 1.1.2, then $c|_\pi$ is minimal by Theorem 4.1.1. Due to Lemma 3.1.2, all planes disjoint to κ are also given by Configuration 1.1.2, which forces c to be minimal as well.

4.2 Minimality in the ordinary case

We copy the assumptions made at the start of Section 2.4.

ASSUMPTION

Throughout this *section*, we assume that $q \geqslant 32$ and fix a codeword $c \in \mathcal{C}_{d-1}(d,q)$ such that $\mathrm{wt}(c) \leqslant W(d,q)$, where

$$W(d,q) \coloneqq \begin{cases} 3\left(1 - \frac{3}{q}\right)\theta_{d-1} & \text{if } q \text{ is prime}, \\ \left(\left\lfloor \frac{1}{2}\sqrt{q} - \frac{9}{4} \right\rfloor - 1\right)\theta_{d-1} & \text{if } q = p^2, \\ \left(\left\lfloor \sqrt{q} - \frac{1}{2} \right\rfloor - 1\right)\theta_{d-1} & \text{otherwise.} \end{cases}$$

Due to Theorem 2.4.8, any codeword $c \in \mathcal{C}_{d-1}(d,q)$, $\mathrm{wt}(c) \leqslant W(d,q)$, is equal to a linear combination of exactly

$$t_c \coloneqq \left\lceil \frac{\mathrm{wt}(c)}{\theta_{d-1}} \right\rceil$$

hyperplanes that form a set $\mathcal{H}_c \coloneqq \{H_1, H_2, \ldots, H_{t_c}\}$.

Proposition 4.2.1

If $c' \in \mathcal{C}_{d-1}(d,q)$ with $\mathrm{supp}(c') \subseteq \mathrm{supp}(c)$, then $\mathcal{H}_{c'} \subseteq \mathcal{H}_c$. As a consequence, the following holds.

(1) *The set $\mathcal{H}_c$ is unique, in the sense that there exists no other set of t_c hyper-*

planes of which a linear combination equals c.

(2) *If* $\alpha_i, \beta_i \in \mathbb{F}_p$ *such that* $c = \sum_{i=1}^{t_c} \alpha_i H_i = \sum_{i=1}^{t_c} \beta_i H_i$, *then* $\alpha_i = \beta_i$. *Therefore, we define*[a]

$$c(H) := \begin{cases} \alpha_i & \text{if } H = H_i, \\ 0 & \text{otherwise,} \end{cases} \tag{4.1}$$

for any hyperplane H *of* $\mathrm{PG}(d,q)$.

[a] This naturally extends the definition of the *value* $c(P)$ of a point P (see section 0.2.2).

Proof. Suppose, to the contrary, that there exists a hyperplane $H \in \mathcal{H}_{c'} \setminus \mathcal{H}_c$. Then all hyperplanes in $(\mathcal{H}_c \cup \mathcal{H}_{c'}) \setminus \{H\}$ cover at most

$$(2t_c - 1)\,\theta_{d-2} \leqslant \left(2\left\lceil \frac{W(d,q)}{\theta_{d-1}} \right\rceil - 1\right)\theta_{d-2} \leqslant (2\sqrt{q} - 3)\,\theta_{d-2} < \theta_{d-1}$$

points of H. As a consequence, there exists a point $P \in H$ which is not contained in any hyperplane of $(\mathcal{H}_c \cup \mathcal{H}_{c'}) \setminus \{H\}$ and therefore $P \in \mathrm{supp}(c') \subseteq \mathrm{supp}(c)$. However, as P is not contained in any hyperplane of $\mathcal{H}_c$, $P \notin \mathrm{supp}(c)$, a contradiction.
Statement (1) follows immediately by considering $c' := c$. Statement (2) follows by repeating the above arguments for each element of the unique set $\mathcal{H}_c$. In this way, we observe that each hyperplane of $\mathcal{H}_c$ contains a point that is not contained in any other hyperplane of $\mathcal{H}_c$, hence its coefficient with respect to c is uniquely determined. ∎

Definition 4.2.2 (codeword restricted to a hyperplane set)

Keeping (4.1) in mind, we can define[a]

$$c|_{\mathcal{H}} := \sum_{H \in \mathcal{H}} c\,(H)\,H$$

for any subset $\mathcal{H} \subseteq \mathcal{H}_c$. In particular, $c|_{\mathcal{H}_c} = c$.

[a] This shouldn't cause confusion with the definition of a *restricted codeword* $c|_\kappa$ (see section 0.2.2), as in that context, κ is a subspace.

Definition 4.2.3 (partition graph)

Consider a partition $\mathbb{H}_c$ of $\mathcal{H}_c$ and let $\Gamma_{\mathbb{H}_c}$ be the graph with vertex set $\mathbb{H}_c$, where two vertices $\mathcal{V}_1$ and $\mathcal{V}_2$ are adjacent if and only if there exists a point P such that

(1) P is a hole of c,

(2) P belongs to the support of both $c|_{\mathcal{V}_1}$ and $c|_{\mathcal{V}_2}$, and

(3) P is a hole of $c|_{\mathcal{V}}$ for every $\mathcal{V} \in \mathbb{H}_c \setminus \{\mathcal{V}_1, \mathcal{V}_2\}$.

Definition 4.2.4 (codeword partitions)

Let $\mathbb{H}_c^0 := \binom{\mathcal{H}_c}{1}$ be the set of singletons containing a unique hyperplane of $\mathcal{H}_c$. For each $i \in \mathbb{N}$, we recursively define

$$\mathbb{H}_c^{i+1} := \left\{ \bigcup_{\mathcal{V} \in \mathbb{V}} \mathcal{V} \ : \ \mathbb{V} \text{ is the vertex set of a component in } \Gamma_{\mathbb{H}_c^i} \right\}.$$

Note that $\mathbb{H}_c^i$ is a partition of $\mathcal{H}_c$ and a refinement of $\mathbb{H}_c^{i+1}$. Hence, as $\mathcal{H}_c$ is finite, there exists a $j \in \mathbb{N}$ such that $\mathbb{H}_c^j = \mathbb{H}_c^{j+1} = \mathbb{H}_c^{j+2} = \ldots =: \mathbb{H}_c^\infty$.

Figure 4.1 is an illustration of the way Definition 4.2.4 deals with a specific codeword $c \in \mathcal{C}_1(2, q)$ of small weight, where q is chosen large enough. The drawing consists of four 'stages', and one can check that

(1) $\mathbb{H}_c^0 = \left\{ \{a_0\}, \{a_1\}, \{a_2\}, \{\widetilde{a}\}, \{b_0\}, \{b_1\}, \{b_2\}, \{b_3\}, \left\{\widetilde{b}\right\} \right\}$,

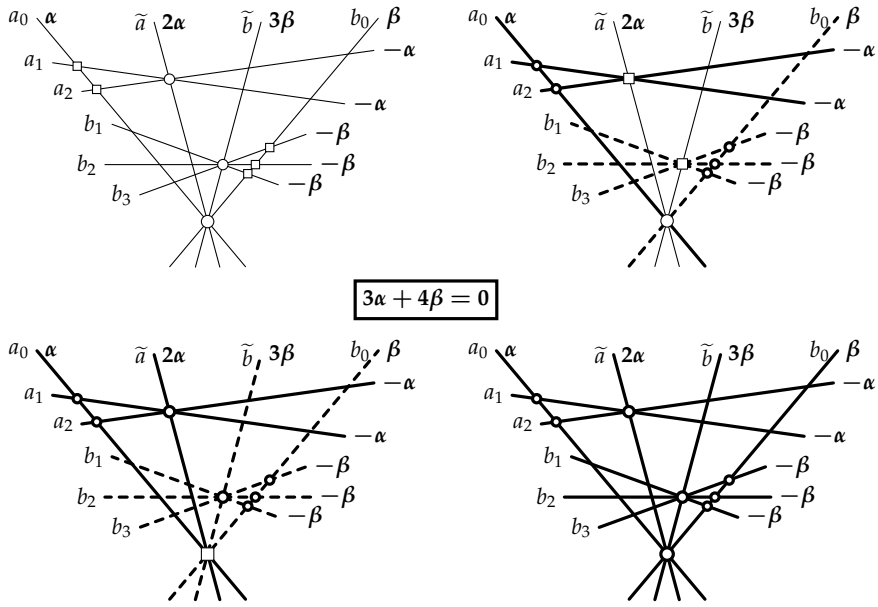


Figure 4.1: The application of Definition 4.2.4 to an example codeword $c \in \mathcal{C}_1(2,q)$ of weight $9q - 12$. More specifically, we consider nine lines of $\mathrm{PG}(2,q)$ and define the codeword $c := \alpha\,(a_0 - a_1 - a_2) + 2\alpha\,\widetilde{a} + \beta\,(b_0 - b_1 - b_2 - b_3) + 3\beta\,\widetilde{b}$. For this specific example, we assume q not prime, $q \geqslant 529$ if $h = 2$ (to be able to apply Result 1.1.3) and $q \geqslant 125$, $p \notin \{2,3,7,11,13\}$, if $h > 2$. Furthermore, $\alpha, \beta \in \mathbb{F}_q$ are two non-zero elements such that $3\alpha + 4\beta = 0$.
Lines are clustered in four 'stages', each of which consists of 'clustering' the lines by following the rule of thumb described in Definitions 4.2.3 and 4.2.4. Holes that are about to 'merge' clusters are indicated by squares instead of circles. In the first stage (top left), every line forms its own cluster. From the second stage (top right) onward, clustered lines are put in bold, with different line patterns to distinguish each cluster.

(2) $\mathbb{H}_c^1 = \left\{ \{a_0, a_1, a_2\}, \{\widetilde{a}\}, \{b_0, b_1, b_2, b_3\}, \left\{\widetilde{b}\right\} \right\}$,

(3) $\mathbb{H}_c^2 = \left\{ \{a_0, a_1, a_2, \widetilde{a}\}, \left\{b_0, b_1, b_2, b_3, \widetilde{b}\right\} \right\}$, and

(4) $\mathbb{H}_c^3 = \left\{ \left\{a_0, a_1, a_2, \widetilde{a}, b_0, b_1, b_2, b_3, \widetilde{b}\right\} \right\} = \mathbb{H}_c^\infty$.

Hence, for this specific codeword c, we end up with $|\mathbb{H}_c^\infty| = 1$, a property which turns out to imply that c is a minimal codeword of $\mathcal{C}_1(2, q)$.

Theorem 4.2.5

Let $q \geqslant 32$ and consider a codeword $c \in \mathcal{C}_{d-1}(d, q)$ with $\mathrm{wt}(c) \leqslant W(d, q)$. If $|\mathbb{H}_c^\infty| = 1$, then c is minimal.

Proof. Consider a codeword $c' \in \mathcal{C}_{d-1}(d, q)$ for which $\mathrm{supp}(c') \subseteq \mathrm{supp}(c)$. We want to prove that there exists an $\alpha \in \mathbb{F}_p$ such that $c' = \alpha c$. Keeping Definition 4.2.2 in mind, this will be done by proving that

$$(\forall i \in \mathbb{N}) \left(\forall \mathcal{V} \in \mathbb{H}_c^i \right) \left(\exists \alpha_i^{\mathcal{V}} \in \mathbb{F}_p \ : \ c'|_{\mathcal{V}} = \alpha_i^{\mathcal{V}} c|_{\mathcal{V}} \right). \tag{4.2}$$

Indeed, if (4.2) is true, then it is true for $i = \infty$ (read: for i large enough). As $\mathbb{H}_c^\infty$ only contains the element $\mathcal{H}_c$, and as $\mathcal{H}_{c'} \subseteq \mathcal{H}_c$ by Proposition 4.2.1, this implies that there exists an $\alpha := \alpha_\infty^{\mathcal{H}_c} \in \mathbb{F}_p$ such that

$$c' = c'|_{\mathcal{H}_{c'}} = c'|_{\mathcal{H}_c} = \alpha c|_{\mathcal{H}_c} = \alpha c.$$

We will prove (4.2) by induction on i. In case $i = 0$, the set $\mathbb{H}_c^0 = \binom{\mathcal{H}_c}{1}$ partitions $\mathcal{H}_c$ in singletons. Hence, for an arbitrary element $\mathcal{V} \in \mathbb{H}_c^0$, there exists a hyperplane $H \in \mathcal{H}_c$ such that $\mathcal{V} = \{H\}$, meaning that $c'|_{\mathcal{V}} = c'(H) H$ and $c|_{\mathcal{V}} = c(H) H$. As $H \in \mathcal{H}_c$ implies that $c(H) \neq 0$, we find an $\alpha_0^{\mathcal{V}} := c'(H) c(H)^{-1}$ meeting the requirements.
Now assume that (4.2) is true for a fixed $i \in \mathbb{N}$. Choose an arbitrary $\mathcal{V} \in \mathbb{H}_c^{i+1}$. As $\mathbb{H}_c^i$ is a refinement of $\mathbb{H}_c^{i+1}$, $\mathcal{V} = \mathcal{V}_1' \sqcup \mathcal{V}_2' \sqcup \cdots \sqcup \mathcal{V}_m'$ for certain pairwise disjoint sets of hyperplanes $\mathcal{V}_1', \mathcal{V}_2', \ldots, \mathcal{V}_m' \in \mathbb{H}_c^i$, $m \in \{1, 2, \ldots, t_c\}$. Moreover, $\mathcal{V}_1', \mathcal{V}_2', \ldots, \mathcal{V}_m'$ are precisely all the vertices of a component in

the graph $\Gamma_{\mathbb{H}_c^i}$. Consider two of these vertices that are adjacent with respect to the graph $\Gamma_{\mathbb{H}_c^i}$; without loss of generality, consider $\mathcal{V}_1'$ and $\mathcal{V}_2'$. By Definition 4.2.3, there exists a point P such that

(1) $c(P) = 0$, which implies that $c'(P) = 0$ as $\mathrm{supp}(c') \subseteq \mathrm{supp}(c)$,

(2) $c|_{\mathcal{V}_1'}(P) \neq 0 \neq c|_{\mathcal{V}_2'}(P)$, and

(3) for all $\mathcal{V}' \in \mathbb{H}_c^i \setminus \{\mathcal{V}_1', \mathcal{V}_2'\}$, $c|_{\mathcal{V}'}(P) = 0$, implying that $c'|_{\mathcal{V}'}(P) = 0$ by the induction hypothesis.

As $\mathbb{H}_c^i$ is a partition of $\mathcal{H}_c$, we know that $c = c|_{\mathcal{H}_c} = \sum_{\mathcal{V}' \in \mathbb{H}_c^i} c|_{\mathcal{V}'}$. Moreover, as $\mathcal{H}_{c'} \subseteq \mathcal{H}_c$ by Proposition 4.2.1, we have $c' = c'|_{\mathcal{H}_{c'}} = c'|_{\mathcal{H}_c} = \sum_{\mathcal{V}' \in \mathbb{H}_c^i} c'|_{\mathcal{V}'}$. Hence, by properties (1) and (3), we obtain

$$0 = c(P) = \left(\sum_{\mathcal{V}' \in \mathbb{H}_c^i} c|_{\mathcal{V}'} \right)(P) = c|_{\mathcal{V}_1'}(P) + c|_{\mathcal{V}_2'}(P), \text{ and} \tag{4.3}$$

$$0 = c'(P) = \left(\sum_{\mathcal{V}' \in \mathbb{H}_c^i} c'|_{\mathcal{V}'} \right)(P) = c'|_{\mathcal{V}_1'}(P) + c'|_{\mathcal{V}_2'}(P). \tag{4.4}$$

By the induction hypothesis, there exist elements $\alpha_i^{\mathcal{V}_1'}, \alpha_i^{\mathcal{V}_2'} \in \mathbb{F}_p$ such that $c'|_{\mathcal{V}_1'} = \alpha_i^{\mathcal{V}_1'} c|_{\mathcal{V}_1'}$ and $c'|_{\mathcal{V}_2'} = \alpha_i^{\mathcal{V}_2'} c|_{\mathcal{V}_2'}$. Combining this with (4.3), (4.4) and the fact that $c|_{\mathcal{V}_1'}(P) \neq 0 \neq c|_{\mathcal{V}_2'}(P)$ (property (2) above), we obtain that

$$\begin{aligned} \alpha_i^{\mathcal{V}_1'} = \left(c|_{\mathcal{V}_1'}(P)\right)^{-1} c'|_{\mathcal{V}_1'}(P) &= \left(-c|_{\mathcal{V}_2'}(P)\right)^{-1} \left(-c'|_{\mathcal{V}_2'}(P)\right) \\ &= \left(c|_{\mathcal{V}_2'}(P)\right)^{-1} c'|_{\mathcal{V}_2'}(P) = \alpha_i^{\mathcal{V}_2'}. \end{aligned}$$

In conclusion, for any two elements $\mathcal{V}_{j_1}', \mathcal{V}_{j_2}' \in \{\mathcal{V}_1', \mathcal{V}_2', \ldots, \mathcal{V}_m'\}$ that are adjacent with respect to the graph $\Gamma_{\mathbb{H}_c^i}$, the corresponding values $\alpha_i^{\mathcal{V}_{j_1}'}$ and $\alpha_i^{\mathcal{V}_{j_2}'}$ (found by the induction hypothesis) are equal. As the elements of

$\{\mathcal{V}'_1, \mathcal{V}'_2, \ldots, \mathcal{V}'_m\}$ are precisely the vertices of a component of $\Gamma_{\mathbb{H}_c^i}$, we can conclude that

$$c'|_{\mathcal{V}'_j} = \alpha_i^{\mathcal{V}'_1} c|_{\mathcal{V}'_j}, \quad \forall j \in \{1, 2, \ldots, m\}.$$

By defining $\alpha_{i+1}^{\mathcal{V}} := \alpha_i^{\mathcal{V}'_1}$, we conclude that, for any $\mathcal{V} \in \mathbb{H}_c^{i+1}$,

$$c'|_{\mathcal{V}} = \sum_{j=1}^{m} c'|_{\mathcal{V}'_j} = \sum_{j=1}^{m} \alpha_{i+1}^{\mathcal{V}} c|_{\mathcal{V}'_j} = \alpha_{i+1}^{\mathcal{V}} \sum_{j=1}^{m} c|_{\mathcal{V}'_j} = \alpha_{i+1}^{\mathcal{V}} c|_{\mathcal{V}}.$$

■

Definition 4.2.6 (support holes)

Define $\mathcal{P}_c^\infty$ to be the set of all holes, each belonging to the support of $c|_{\mathcal{V}}$ for some $\mathcal{V} \in \mathbb{H}_c^\infty$.

Theorem 4.2.7

Let $q \geqslant 32$ and consider a codeword $c \in \mathcal{C}_{d-1}(d, q)$ with $\mathrm{wt}(c) \leqslant W(d, q)$. If $|\mathcal{P}_c^\infty| \leqslant |\mathbb{H}_c^\infty| - 2$, then c is not minimal.

Proof. Define $m := |\mathbb{H}_c^\infty|$ and $n := |\mathcal{P}_c^\infty|$, hence let $\mathbb{H}_c^\infty = \{\mathcal{V}_1, \mathcal{V}_2, \ldots, \mathcal{V}_m\}$ and $\mathcal{P}_c^\infty = \{P_1, P_2, \ldots, P_n\}$. Consider the following system of n linear equations over $\mathbb{F}_p$:

$$c|_{\mathcal{V}_1}(P_i) X_1 + c|_{\mathcal{V}_2}(P_i) X_2 + \cdots + c|_{\mathcal{V}_m}(P_i) X_m = 0, \qquad i = 1, 2, \ldots, n. \tag{4.5}$$

As $n \leqslant m - 2$, the solution space of the above system of linear equations is a vector space over $\mathbb{F}_p$ of dimension at least two. Therefore, we can find a solution $(\alpha_1, \alpha_2, \ldots, \alpha_m)^\intercal \in V(m, p)$ that is not a scalar multiple of $\mathbf{1} \in V(m, p)$. Define

$$c' := \alpha_1 c|_{\mathcal{V}_1} + \alpha_2 c|_{\mathcal{V}_2} + \cdots + \alpha_m c|_{\mathcal{V}_m}.$$

By the choice of $(\alpha_1, \alpha_2, \ldots, \alpha_m)^\intercal$, the codeword c' is not a scalar multiple of

$c = c|_{\mathcal{V}_1} + c|_{\mathcal{V}_2} + \cdots + c|_{\mathcal{V}_m}$. Hence, once we verify that $\operatorname{supp}(c') \subseteq \operatorname{supp}(c)$, the proof is done.
Consider a hole Q of c. Then either $Q \in \mathcal{P}_c^\infty$ or $Q \notin \mathcal{P}_c^\infty$. If $Q \in \mathcal{P}_c^\infty$, then $Q = P_{i'}$ for an $i' \in \{1, 2, \ldots, n\}$. As $(\alpha_1, \alpha_2, \ldots, \alpha_m)^\mathsf{T}$ is a solution to (4.5), $c'(Q) = \alpha_1 c|_{\mathcal{V}_1}(P_{i'}) + \alpha_2 c|_{\mathcal{V}_2}(P_{i'}) + \cdots + \alpha_m c|_{\mathcal{V}_m}(P_{i'}) = 0$. If $Q \notin \mathcal{P}_c^\infty$, then $c|_{\mathcal{V}}(Q) = 0$ for every $\mathcal{V} \in \mathbb{H}_c^\infty$, hence $c'(Q) = \alpha_1 c|_{\mathcal{V}_1}(Q) + \alpha_2 c|_{\mathcal{V}_2}(Q) + \cdots + \alpha_m c|_{\mathcal{V}_m}(Q) = 0 + 0 + \cdots + 0 = 0$. In both cases, $c'(Q) = 0$. As Q was an arbitrarily chosen, all holes of c are holes of c', implying that $\operatorname{supp}(c') \subseteq \operatorname{supp}(c)$. ∎

Corollary 4.2.8

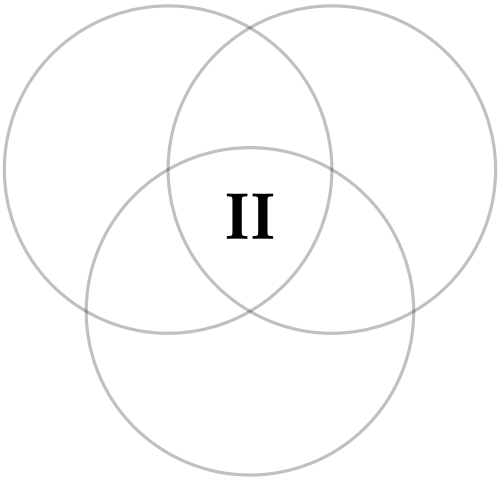
Let $q \geqslant 32$ and consider a codeword $c \in \mathcal{C}_{d-1}(d, q)$ with $\operatorname{wt}(c) \leqslant W(d, q)$. If $|\mathbb{H}_c^\infty| = 2$, then c is not minimal.

Proof. By Theorem 4.2.7, it suffices to prove that $\mathcal{P}_c^\infty = \varnothing$. Let $\mathbb{H}_c^\infty = \{\mathcal{V}_1, \mathcal{V}_2\}$ and suppose, to the contrary, that there exists a point $P \in \mathcal{P}_c^\infty$. Without loss of generality, we can assume that $c|_{\mathcal{V}_1}(P) \neq 0$. As $P \in \mathcal{P}_c^\infty$, we know that P is a hole of c, hence $0 = c(P) = c|_{\mathcal{V}_1}(P) + c|_{\mathcal{V}_2}(P)$, implying that $c|_{\mathcal{V}_2}(P) \neq 0$ as well. However, by Definitions 4.2.3 and 4.2.4, this would imply that $|\mathbb{H}_c^\infty| = 1$, a contradiction. ∎

Theorem 4.2.9

Suppose that $q = p^h$, $p \geqslant 5$. Then there exists a minimal codeword $c \in \mathcal{C}_1(2, q)$ with $\operatorname{wt}(c) \leqslant W(2, q)$, $|\mathbb{H}_c^\infty| = 3$ and $|\mathcal{P}_c^\infty| = 2$.

Proof. Consider a line r and let $S, T \in r$ be two distinct points. Let s_1, s_2 and s' be three distinct lines through S, different from r, and let t_1, t_2 and t' be three distinct lines through T, different from r. Define $c := r - s_1 - s_2 + s' - t_1 - t_2 + t'$.
One can check that $\mathbb{H}_c^\infty = \{\{s_1, s_2, t'\}, \{t_1, t_2, s'\}, \{r\}\}$ and that $\mathcal{P}_c^\infty = \{S, T\}$, and also manually check that this codeword is minimal. ∎



II

Strong blocking sets

5 A tale of wild lines and minimal codes

> *Owl feathers, apple cores and sweet wrappers littered the floor, a number of spellbooks lay higgledy-piggledy among the tangled robes on his bed, and a mess of newspapers sat in a puddle of light on his desk.*
>
> — J. K. Rowling, *Harry Potter and the Half-Blood Prince*

The closure of Part I marks the end of the 'characterising codes' bit of this thesis's title. Part II and III focus on peculiar geometrical constructions that directly prove the existence of codes with favourable properties.

This part is focused on constructions that take the form of so-called *higgledy-piggledy sets* of k-subspaces, which give rise to a particular type of *strong blocking sets*, that in turn produce minimal codes.

The results in this chapter are based on [62, 64].

5.1 Strong blocking sets and minimal codes

One type of structure that is being thoroughly investigated in the literature is a *blocking set*. Occasionally, entire PhD theses are devoted to these fascinating point sets. We adopt the definition used in [52].

Definition 5.1.1 (blocking set)

A ***k*-blocking set** of $\mathrm{PG}(d,q)$ is a point set that meets every $(d-k)$-dimensional subspace. A 1-blocking set will simply be called a **blocking set**.

The point set of a k-subspace is the simplest (and smallest) example of a k-blocking set of $\mathrm{PG}(d,q)$ [32]. A natural generalisation of a k-blocking set of $\mathrm{PG}(d,q)$ is the concept of a ***t*-fold *k*-blocking set**, which is a point set of $\mathrm{PG}(d,q)$ that meets every $(d-k)$-dimensional subspace in at least t points. As an example, the unionised point set of t pairwise disjoint k-subspaces is a t-fold k-blocking set.

Definition 5.1.2 (strong blocking set)

A **strong *k*-blocking set** of $\mathrm{PG}(d,q)$ is a point set that meets every $(d-k)$-dimensional subspace κ in a set of points spanning κ. A strong 1-blocking set will simply be called a **strong blocking set**.

The concept of a strong k-blocking set was introduced in [46, Definition 3.1]. However, these are also known as **generator sets** ([69, Definition 2]) and **cutting blocking sets** ([31, Definition 3.4]) in case $k=1$.

Alfarano, Borello and Neri [6] and Tang, Qiu, Liao and Zhou [106] independently proved that minimal codes have a one-to-one correspondence to strong blocking sets. Recently, this correspondence was reproven "much more transparently" in [77, Corollary 19].

Result 5.1.3 ([6, Theorem **3.4**], [106, Theorem **3.2**])

Suppose that $n,k' \in \mathbb{N}\setminus\{0,1\}$ and let $\mathcal{C}$ be a non-degenerate $[n,k']_q$-code with generator matrix $G := (g_1,g_2,\ldots,g_n)$. Given a coordinate system for $\mathrm{PG}(k'-1,q)$, let $\mathcal{B}$ be the point set corresponding to the coordinate set $\{g_1,g_2,\ldots,g_n\}$. Then $\mathcal{C}$ is a minimal code if and only if $\mathcal{B}$ is a strong blocking set.

As one is generally interested in the smallest possible length of minimal

$[n, k']_q$-codes for fixed parameters k' and q, one defines $m(k', q)$ to be the smallest possible length of such a code. Naturally, researchers try to determine lower and upper bounds for $m(k', q)$. By the above result, this quest goes hand in hand with the search for small strong blocking sets of $\mathrm{PG}(k' - 1, q)$.

5.2 Higgledy-piggledy sets

While any strong k-blocking set is necessarily a $(d - k + 1)$-fold k-blocking set, the converse is generally false. Following this line of thought, one could wonder if a strong k-blocking set could be constructed as the unionised point set of some well-chosen k-subspaces. Although sporadic examples of such point sets were already presented in [46], this idea was thoroughly investigated in [69, 78] for $k = 1$ and later generalised in [68] to arbitrary k.

Definition 5.2.1 (higgledy-piggledy set)

If $\mathcal{K}$ is a set of k-subspaces of $\mathrm{PG}(d, q)$ such that the union of their point sets is a strong k-blocking set, then the elements of $\mathcal{K}$ are said to be in **higgledy-piggledy arrangement** and the set $\mathcal{K}$ itself is said to be a **higgledy-piggledy set of k-subspaces**.

Higgledy-piggledy sets are the protagonists of Part II. The name originates from the mind of Hungarian mathematician Tamás Héger and illustrates the way such sets of k-subspaces are figuratively 'well-spread-out' (copying a well-put description of [68, 69]). By Result 5.1.3, the existence of small *line* sets in higgledy-piggledy arrangement implies the existence of minimal codes and covering codes (see Part III) of relatively small length.

While the case $k = d$ is barely worth mentioning, the cases $k \in \{0, d - 1\}$ are trivial as well. After all, any basis of $\mathrm{PG}(d, q)$ in general position is a higgledy-piggledy point set of smallest size. Conversely (or by duality, see Proposition 5.4.4), any set of $d + 1$ hyperplanes in general position is a higgledy-piggledy set of hyperplanes of smallest size.

If $1 \leqslant k \leqslant d-2$, however, it is generally not an easy task to find small higgledy-piggledy sets of k-subspaces. The following 'almost-equivalent' condition was first derived for sets of lines in [69] and later generalised to sets of k-subspaces in [68] and is a great tool to ease the search for higgledy-piggledy sets.

Result 5.2.2 ([68, Theorem **4** and Proposition **5**])

Let $\mathcal{K}$ be a set of k-subspaces of $\mathrm{PG}(d,q)$. If no $(d-k-1)$-subspace meets each element of $\mathcal{K}$, then $\mathcal{K}$ is a higgledy-piggledy set of k-subspaces. If $|\mathcal{K}| \leqslant q$, the converse holds as well.

As one generally wishes to construct higgledy-piggledy sets of small size, *lower bounds* on the size of such sets were determined to reveal which sizes would (theoretically) be optimal. A lower bound on higgledy-piggledy line sets was determined in [69] for q large enough, and recently strengthened in [77] to all values of q.

Result 5.2.3 ([77, Theorem **28**])

A higgledy-piggledy line set of $\mathrm{PG}(d,q)$ contains at least $d + \left\lfloor \frac{d}{2} \right\rfloor - \left\lfloor \frac{d-1}{q} \right\rfloor$ elements.

Based on the reasoning behind [69, Theorem 14], the authors of [68] inductively determined a lower bound on the size of general higgledy-piggledy sets of k-subspaces.

Result 5.2.4 ([68, Theorem **20**])

A higgledy-piggledy set of k-subspaces of $\mathrm{PG}(d,q)$ contains at least $\min\left\{q, \sum_{i=0}^{k} \left\lfloor \frac{d-k+i}{i+1} \right\rfloor \right\} + 1$ elements.

The latter theorem can in fact be improved if $k > \frac{d-1}{2}$ by using the fact that a projective geometry admits a duality.

Theorem 5.2.5

A higgledy-piggledy set of k-subspaces of $\mathrm{PG}(d,q)$ *contains at least*

$$\min\left\{q, \max\left\{(k+1)+\sum_{i=1}^{k+1}\left\lfloor\frac{d-k-1}{i}\right\rfloor, (d-k)+\sum_{i=1}^{d-k}\left\lfloor\frac{k}{i}\right\rfloor\right\}\right\}+1$$

elements.

Proof. This follows immediately from Result 5.2.4 and Proposition 5.4.4. ∎

The main topic of Part II concerns the flip side of the coin, namely the search for tighter *upper bounds* on the size of the smallest possible higgledy-piggledy sets of k-subspaces of $\mathrm{PG}(d,q)$. This is naturally done by constructing small higgledy-piggledy sets, ideally with a size as close as possible to the theoretical lower bound.
A naive but interesting example of a general higgledy-piggledy line set is the **tetrahedron**, first mentioned in [51, Theorem 6]. This is the set of all lines containing two points of a fixed basis of $\mathrm{PG}(d,q)$, resulting in a set of $\frac{d(d+1)}{2}$ lines in higgledy-piggledy arrangement. Several years later, smaller higgledy-piggledy line sets were found and subsequently generalised.

Result 5.2.6 ([69, Theorem **24**], [68, Proposition **10**])

If $q > (d-k)(k+1)$, then there exist $(d-k)(k+1)+1$ k-subspaces of $\mathrm{PG}(d,q)$ *in higgledy-piggledy arrangement.*

Although the theorems above present very strong upper bounds on the size of the smallest possible higgledy-piggledy sets of k-subspaces, the case of q small is neglected. Using a probabilistic approach, Héger and Nagy [77, Theorems 31 and 37] recently obtained strong upper bounds for all values of q, which coincide with the results above if $q > (d-k)(k+1)$.

Besides these general results, sporadic examples of higgledy-piggledy sets can be found in the literature.

Result 5.2.7 ([46, Theorem **3.7**], [24, Proposition **12**], [19, Theorem **3.15**])

(1) *There exist four pairwise disjoint lines of* $\mathrm{PG}(3,q)$ *in higgledy-piggledy arrangement.*[a]

(2) *If* $q \geqslant 36097$ *is no power of* 2 *or* 3*, then there exist six pairwise disjoint lines of* $\mathrm{PG}(4,q)$ *in higgledy-piggledy arrangement.*

(3) *There exist seven pairwise disjoint lines of* $\mathrm{PG}(5,q)$ *in higgledy-piggledy arrangement.*

[a] Side note: an easy exercise proves that three lines of $\mathrm{PG}(3,2)$ are in higgledy-piggledy arrangement if and only if they are pairwise disjoint.

Fancsali and Sziklai discovered the same construction behind Result 5.2.7(1) in [69, Example 9]. The authors of [46] also prove the existence of nine planes of $\mathrm{PG}(4,q)$ in higgledy-piggledy arrangement. However, if $q \geqslant 7$, Result 5.2.6 improves this result, as it implies the existence of seven planes of $\mathrm{PG}(4,q)$ in higgledy-piggledy arrangement.

5.3 Optimal higgledy-piggledy line sets

Consider a higgledy-piggledy line set of smallest theoretical size (see Result 5.2.3). Is it possible to micro-optimise the strong blocking set arising from this set by making some of these lines intersect? In other words, which are the *optimal* higgledy-piggledy line sets?

Lemma 5.3.1

Consider a higgledy-piggledy line set $\mathcal{L}$ *of* $\mathrm{PG}(d,q)$ *with* $|\mathcal{L}| = d + \left\lfloor \frac{d}{2} \right\rfloor \leqslant q$*. Then every* $\left\lceil \frac{d+1}{2} \right\rceil$ *lines of* $\mathcal{L}$ *span the whole space.*

Proof. Suppose, to the contrary, that there exists a subset $\mathcal{L}' \subset \mathcal{L}$ consisting of $\left\lceil \frac{d+1}{2} \right\rceil$ lines contained in a hyperplane Π. For each $\ell \in \mathcal{L} \setminus \mathcal{L}'$, choose a

point in the subspace $\Pi \cap \ell$. This results in a choice of at most $d + \left\lfloor \frac{d}{2} \right\rfloor - \left\lceil \frac{d+1}{2} \right\rceil = d - 1$ points in Π spanning a subspace $\Sigma \subset \Pi$ of dimension at most $d - 2$. Any $(d-2)$-subspace of Π through Σ is a $(d-2)$-subspace that intersects every line of $\mathcal{L}$, contradicting Result 5.2.2. ∎

Proposition 5.3.2

Consider a higgledy-piggledy line set $\mathcal{L}$ of $\mathrm{PG}(d,q)$ with $|\mathcal{L}| = d + \left\lfloor \frac{d}{2} \right\rfloor \leqslant q$. Then the following holds.

(1) *If d is odd, the lines of $\mathcal{L}$ are pairwise disjoint.*

(2) *If $d \geqslant 4$ is even, at most two lines of $\mathcal{L}$ intersect.*

Proof. Let d be odd. The statement is trivial if $d = 1$, hence we can assume that $d \geqslant 3$. Suppose, to the contrary, that two lines $\ell, \ell' \in \mathcal{L}$ span a plane π. Consider $n := \frac{d-3}{2}$ lines $\ell_1, \ell_2, \ldots, \ell_n \in \mathcal{L} \setminus \{\ell, \ell'\}$. Then $\langle \ell, \ell', \ell_1, \ell_2, \ldots, \ell_n \rangle = \langle \pi, \ell_1, \ell_2, \ldots, \ell_n \rangle$ is a span of $\frac{d+1}{2}$ lines of $\mathcal{L}$ equal to a subspace of dimension at most $d - 1$, contradicting Lemma 5.3.1.
Let $d \geqslant 4$ be even. Suppose, to the contrary, that there exist two doubletons of intersecting lines with corresponding intersection points S_1 and S_2; define $\mathcal{L}'$ to be the set of these lines. We distinguish two cases depending on the size of $\mathcal{L}'$ and on the equality of the intersection points S_1 and S_2.
If $|\mathcal{L}'| = 3$ or if $S_1 = S_2$, then there exists a solid σ containing at least three lines of $\mathcal{L}'$. Consider $n := \frac{d-4}{2}$ lines $\ell_1, \ell_2, \ldots, \ell_n \in \mathcal{L} \setminus \mathcal{L}'$. Then $\langle \sigma, \ell_1, \ell_2, \ldots, \ell_n \rangle$ is a subspace of dimension at most $d - 1$ that contains at least $\frac{d+2}{2}$ lines of $\mathcal{L}$, contradicting Lemma 5.3.1.
If $|\mathcal{L}'| = 4$ and $S_1 \neq S_2$, then the line $s := \langle S_1, S_2 \rangle$ intersects all four lines of $\mathcal{L}'$. Consider $n := \frac{d-2}{2}$ lines $\ell_1, \ell_2, \ldots, \ell_n \in \mathcal{L} \setminus \mathcal{L}'$. As $\langle s, \ell_1, \ell_2, \ldots, \ell_n \rangle$ has dimension at most $d - 1$, we can choose a hyperplane Π through this subspace. For each $\ell \in \mathcal{L} \setminus (\mathcal{L}' \cup \{\ell_1, \ell_2, \ldots, \ell_n\})$, choose a point in the subspace $\Pi \cap \ell$. This results in a choice of at most $d + \frac{d}{2} - (4 + n) =$

$d-3$ points in Π spanning, together with the line s, a subspace $\Sigma \subset \Pi$ of dimension at most $d-2$. Any $(d-2)$-subspace of Π through Σ is a $(d-2)$-subspace that intersects every line of $\mathcal{L}$, contradicting Result 5.2.2. ∎

Proposition 5.3.3

Consider a higgledy-piggledy set $\mathcal{K}$ of $(d-2)$-subspaces of $\mathrm{PG}(d,q)$ with $|\mathcal{K}| = d + \left\lfloor \frac{d}{2} \right\rfloor \leqslant q$. Then every $\left\lceil \frac{d+1}{2} \right\rceil$ elements of $\mathcal{K}$ have no point in common. Moreover, the following holds.

(1) *If $d \geqslant 3$ is odd, the elements of $\mathcal{K}$ pairwise intersect in a $(d-4)$-subspace.*

(2) *If $d \geqslant 4$ is even, at most two elements of $\mathcal{K}$ intersect in a $(d-3)$-subspace.*

Proof. These results follow immediately by combining Lemma 5.3.1 and Proposition 5.3.2 with Proposition 5.4.4 (see Section 5.4). ∎

Note that, alternatively, we could have dualised both statement and proof of Lemma 5.3.1 and Proposition 5.3.2 to obtain Proposition 5.3.3.

Propositions 5.3.2 and 5.3.3 give us an understanding of the best possible set-ups for higgledy-piggledy sets of k-subspaces, $k \in \{1, d-2\}$, of size at most q. Therefore, we define the following accordingly.

Definition 5.3.4 (optimal higgledy-piggledy set)

Let $d \geqslant 3$ and $k \in \{1, d-2\}$, and consider a higgledy-piggledy set $\mathcal{K}$ of k-subspaces of $\mathrm{PG}(d,q)$. Then $\mathcal{K}$ is called **optimal** if $|\mathcal{K}| = d + \left\lfloor \frac{d}{2} \right\rfloor \leqslant q$ and either

(1) d is odd, or

(2) d is even and two elements of $\mathcal{K}$ intersect in a $(k-1)$-subspace.

5.4 Construction methods

There are several ways to construct higgledy-piggledy sets of k-subspaces of $\mathrm{PG}(d,q)$. Constructions via *projection* or *dualisation* make use of the existence of other higgledy-piggledy sets to construct new ones of similar size. Construction via *linear sets* relies on the existing knowledge on $\mathbb{F}_q$-linear sets to prove the existence of higgledy-piggledy sets of k-subspaces contained in Desarguesian spreads.

5.4.1 Projection

Proposition 5.4.1

Suppose that $\mathcal{B}$ is a strong k-blocking set of $\mathrm{PG}(d,q)$. Take a hyperplane Π and a point $P \notin \mathcal{B} \cup \Pi$. Then $\mathcal{B}' := \{\langle P, S\rangle \cap \Pi : S \in \mathcal{B}\}$ is a strong k-blocking set of $\Pi \cong \mathrm{PG}(d-1,q)$.

Proof. Suppose, to the contrary, that there exists a $(d-k-1)$-subspace $\Sigma \subset \Pi$ that meets $\mathcal{B}'$ in a point set contained in a $(d-k-2)$-subspace Σ'. By the definition of $\mathcal{B}'$, this means that $\langle \Sigma, P\rangle$ is a $(d-k)$-subspace that meets $\mathcal{B}$ in a point set contained in the $(d-k-1)$-subspace $\langle \Sigma', P\rangle$, a contradiction. ∎

Corollary 5.4.2

Consider a higgledy-piggledy set $\mathcal{K}$ of k-subspaces of $\mathrm{PG}(d,q)$. Take a hyperplane Π and a point $P \notin \Pi$ not contained in any of the elements of $\mathcal{K}$. Then $\mathcal{K}' := \{\langle P, \kappa\rangle \cap \Pi : \kappa \in \mathcal{K}\}$ is a higgledy-piggledy set of k-subspaces in $\Pi \cong \mathrm{PG}(d-1,q)$ of size at most $|\mathcal{K}|$.

Remark 5.4.3

Let $d \geqslant 3$, $k \in \{1, d-2\}$, and suppose there exists an optimal higgledy-piggledy set of k-subspaces for each odd, respectively even, d. Then, by

Corollary 5.4.2, there exists a higgledy-piggledy set of k-subspaces of size $d + \left\lfloor \frac{d}{2} \right\rfloor + 1$ for each even, respectively odd, d (for d even, one simply has to choose the point of projection within the span of the two k-subspaces that maximally intersect). This reduces the search for small ('near-optimal') higgledy-piggledy sets of k-subspaces, $k \in \{1, d-2\}$, to one parity class of d.

5.4.2 Duality

A second construction technique makes use of a *duality* of $\mathrm{PG}(d,q)$, and although this insight is anything but groundbreaking, we want to note that this has also been pointed out in [68, Theorem 9, Proposition 10].

Proposition 5.4.4

Consider a higgledy-piggledy set $\mathcal{K}$ of k-subspaces of $\mathrm{PG}(d,q)$ with $|\mathcal{K}| \leqslant q$. Then the set $\mathcal{K}^\delta$ consisting of the dual subspaces of the elements in $\mathcal{K}$ is a higgledy-piggledy set of $(d-k-1)$-subspaces of $\mathrm{PG}(d,q)$.

Proof. By Result 5.2.2, no $(d-k-1)$-subspace meets each element of $\mathcal{K}$. Taking the dual of this statement, we know that no k-subspace meets each element of $\mathcal{K}^\delta$. Applying Result 5.2.2 yet again, we conclude that $\mathcal{K}^\delta$ must be a higgledy-piggledy set of $(d-k-1)$-subspaces of $\mathrm{PG}(d,q)$. ∎

Theorem 5.2.5 is an excellent example of the usage of this method. Moreover, as we will discover in Chapter 6, this technique will imply the existence of a small higgledy-piggledy plane set of $\mathrm{PG}(4,q)$ (see Corollary 6.2.6).

Corollary 5.4.5

There exist seven solids of $\mathrm{PG}(5,q)$, $q \geqslant 7$, in higgledy-piggledy arrangement.

Proof. This follows from Result 5.2.7(3) and Proposition 5.4.4. ∎

This set is an optimal higgledy-piggledy set of solids of $\mathrm{PG}(5,q)$. Note that,

by Proposition 5.3.3, these seven solids are in general position.

5.4.3 Linear sets

This particular method for constructing higgledy-piggledy sets is useful if (and only if) $d+1$ is composite. As a side note, a different perspective can be found in (very) recent literature [7].

Let $r,t \in \mathbb{N}\setminus\{0\}$ and recall the definition of an $\mathbb{F}_q$-linear set (see section 0.1.8). Note that an $\mathbb{F}_q$-linear set of $\mathrm{PG}(r-1,q^t)$ has rank $(r-1)\,t+1$ if and only if it equals the whole point set of $\mathrm{PG}(r-1,q^t)$. With this in mind, the following theorem states that any point set that is not contained in a 'proper' $\mathbb{F}_q$-linear set gives rise to a higgledy-piggledy set.

Theorem 5.4.6

Let $r,t \in \mathbb{N}\setminus\{0\}$ and consider a point set $\mathcal{P}$ of $\mathrm{PG}(r-1,q^t)$ that is not contained in an $\mathbb{F}_q$-linear set of rank $(r-1)\,t$. Then $\mathcal{F}_{r,t,q}(\mathcal{P})$ is a higgledy-piggledy set of pairwise disjoint $(t-1)$-subspaces of $\mathrm{PG}(rt-1,q)$.

Proof. Suppose, to the contrary, that $\mathcal{F}_{r,t,q}(\mathcal{P})$ is not a higgledy-piggledy set of $(t-1)$-subspaces of $\mathrm{PG}(rt-1,q)$. By Result 5.2.2, there exists an $((r-1)\,t-1)$-subspace that meets all elements of $\mathcal{F}_{r,t,q}(\mathcal{P})$, implying that the latter is contained in an $\mathbb{F}_q$-linear set of rank $(r-1)\,t$, a contradiction. ∎

This idea of searching for higgledy-piggledy sets as a subset of a Desarguesian spread was first used in [8, 19] (see e.g. Result 5.2.7(3)).

Remark 5.4.7 ([8, Remark **4.3**])

As an $\mathbb{F}_q$-subline of $\mathrm{PG}(1,q^2)$ is uniquely determined by any three of its points (Result 0.1.2), one can choose four points of $\mathrm{PG}(1,q^2)$ not contained in any $\mathbb{F}_q$-subline (which is precisely an $\mathbb{F}_q$-linear set of rank 2). Therefore, Theorem 5.4.6 provides an alternative proof for Result 5.2.7(1).

Eight planes of $\mathrm{PG}(5,q)$

Theorem 5.4.6 can not only be used to prove the existence of higgledy-piggledy *line* sets of $\mathrm{PG}(5,q)$. By Result 5.2.6, we know that there exists a higgledy-piggledy set of planes of $\mathrm{PG}(5,q)$ of size ten. Based on some strong results found in [89], we can prove the following.

Theorem 5.4.8

There exist eight pairwise disjoint planes of $\mathrm{PG}(5,q)$, $q \geqslant 7$, *in higgledy-piggledy arrangement.*

Proof. Consider four distinct points C, B_1, B_2 and B_3 of $\mathrm{PG}(1,q^3)$ that do not lie in an $\mathbb{F}_q$-subline. For every $i \in \{1,2,3\}$, let $\mathfrak{b}_i$ be the (by Result 0.1.2 unique) $\mathbb{F}_q$-subline through the points of the set $\{C,B_1,B_2,B_3\} \setminus \{B_i\}$ and choose a point $D_i \in \mathfrak{b}_i \setminus \{C,B_1,B_2,B_3\}$. In this way, we obtain three distinct $\mathbb{F}_q$-sublines that pairwise intersect in two points and have the point C in common. Define

$$\mathcal{P} := \{C,B_1,B_2,B_3,D_1,D_2,D_3\}.$$

By Result 0.1.17, any $\mathbb{F}_q$-linear set that contains all points of $\mathcal{P}$ has to contain all points of $\mathfrak{b}_1 \cup \mathfrak{b}_2 \cup \mathfrak{b}_3$, as such $\mathbb{F}_q$-linear set contains at least four points of each subline. As $|\mathfrak{b}_1 \cup \mathfrak{b}_2 \cup \mathfrak{b}_3| = 3q-2 > 2q+3$, Result 0.1.19 implies that there exists at most one $\mathbb{F}_q$-linear set $\mathcal{L}$ of rank 3 that contains all points of $\mathcal{P}$. Choose a point $Q \notin \mathcal{L}$. Then $\mathcal{P} \cup \{Q\}$ is a set of eight points of $\mathrm{PG}(1,q^3)$ that is not contained in any $\mathbb{F}_q$-linear set of rank 3. Theorem 5.4.6 finishes the proof. ∎

In Chapter 7, we show, with a bit more effort, how the above result can be improved.

6 lines of PG$(4, q)$

This and the following chapter focus on the construction of small higgledy-piggledy sets of PG$(4, q)$ and PG$(5, q)$, respectively.

Non-trivial higgledy-piggledy sets of k-subspaces of PG$(4, q)$ arise if $k \in \{1, 2\}$. By Theorem 5.2.5, any such set consists of at least six elements. As described in Result 5.2.7(2), Bartoli, Kiss, Marcugini and Pambianco proved the existence of six pairwise disjoint lines of PG$(4, q)$ in higgledy-piggledy arrangement. They however exclude the cases of field characteristic 2 and 3 and impose a relatively large lower bound on the general field size. Therefore, the question arises whether such a construction is possible without any significant field restrictions. Bonus points if such a line set turns out to be optimal.

The results in this chapter are based on [62]. This entire chapter consists of one long chain of arguments leading up to Theorem 6.2.5, many of which rely on Section 0.1.6. We will juggle with points, lines and planes of PG$(4, q)$, and introduce many notations to avoid confusing repetitions of arguments. If you lose track of any such notation, use the index at the end of this work to pinpoint the correct definition.

6.1 The base configuration

A blocking set of PG$(2, q)$ is defined to be a point set meeting every line of the projective plane (see Definition 5.1.1). In the literature, researchers

have also investigated point sets of PG$(2,q)$ that meet every line of a fixed line set. In particular, blocking sets with respect to the external lines of a non-singular conic were considered. In 2006, Aguglia and Korchmáros [4] managed to characterise such blocking sets of minimal size in case q is odd. One year later, Giulietti [71] tackled the case of q even. Although a characterisation is known, for the purpose of this chapter, we only require the following, which will prove its usefulness near the very end of this chapter.

Result 6.1.1 ([4, 71])

The minimum size of a blocking set with respect to the external lines of a non-singular conic of PG$(2,q)$ *equals* $q-1$.

Throughout this chapter, keep the following base configuration in mind.

Configuration 6.1.2

Suppose that Σ_1, Σ_2 and Σ_3 are solids of PG$(4,q)$ such that their intersection $m := \Sigma_1 \cap \Sigma_2 \cap \Sigma_3$ is a line. Let M_1 and M_2 be two distinct points on m. Define, for every $i,j \in \{1,2,3\}$, $i < j$, the plane $\pi_{ij} := \Sigma_i \cap \Sigma_j$ and let $P_{ij} \in \pi_{ij} \setminus m$ be a point. Consider, for each $i \in \{1,2\}$, the line $\ell_{i2} := \langle P_{12}, P_{i3}\rangle$ and the line ℓ_{i1} lying in Σ_i through M_i not intersecting ℓ_{i2} and not contained in π_{12} or π_{i3}. Define the line $s := \langle P_{13}, P_{23}\rangle$, the plane $\beta := \langle \ell_{11}, \ell_{21}\rangle \cap \Sigma_3$ and their intersection point $S := s \cap \beta$. To conclude, consider the following projections:

(1) the line $\ell'_{11} := \langle P_{13}, \ell_{11}\rangle \cap \pi_{12}$, and

(2) the line $\ell''_{i1} := \langle P_{12}, \ell_{i1}\rangle \cap \pi_{i3}$ for each $i \in \{1,2\}$.

See Figure 6.1 for a visualisation of this configuration.

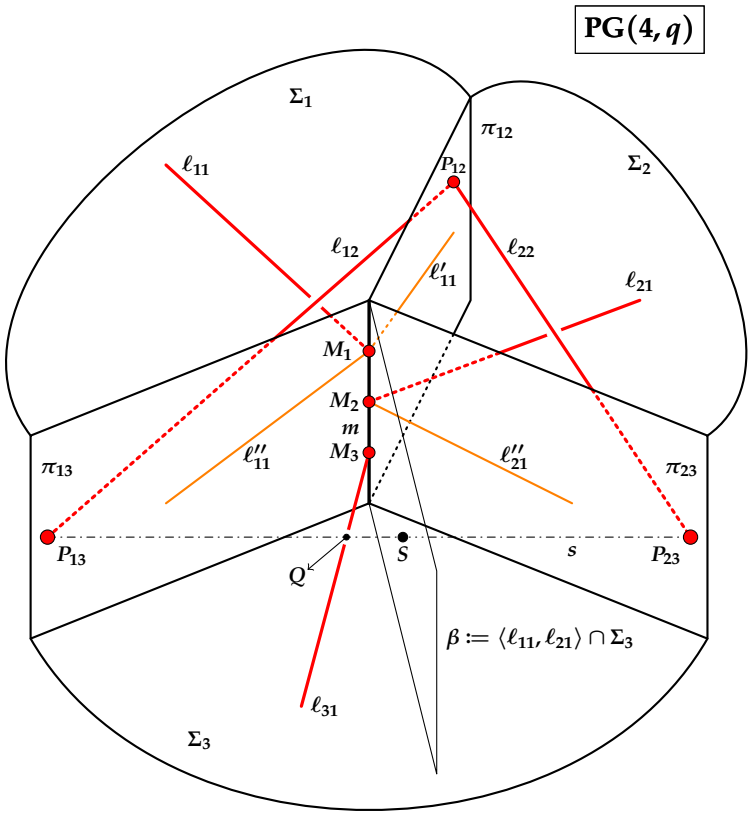


Figure 6.1: The set-up as described in Configurations 6.1.2 and 6.2.4. Note that the lines of interest, namely ℓ_{11}, ℓ_{12}, ℓ_{21} and ℓ_{22} (and ℓ_{31}, see Configuration 6.2.4) are drawn in red, while their projections as defined in Configuration 6.1.2 are shown in orange.

6.2 Pencils and conics

Denote with $\Pi^{(4)}$ the set of all planes of PG$(4,q)$ that intersect each of the lines ℓ_{11}, ℓ_{12}, ℓ_{21} and ℓ_{22}.

Lemma 6.2.1

Each plane of $\Pi^{(4)}$ either

(1) *intersects Σ_3 in a line of π_{13} through M_2 not equal to m,*

(2) *intersects Σ_3 in a line of π_{23} through M_1 not equal to m,*

(3) *is equal to π_{12}, or*

(4) *intersects π_{12} in precisely one point not contained in $\langle M_i, P_{12}\rangle \setminus \{M_i, P_{12}\}$, $i \in \{1,2\}$.*

Moreover, for every point $A \in \pi_{12} \setminus (\langle M_1, P_{12}\rangle \cup \langle M_2, P_{12}\rangle)$, there exists a unique plane of $\Pi^{(4)}$ that intersects π_{12} in precisely the point A.

Proof. Consider a plane $\alpha \in \Pi^{(4)}$ and suppose that α is contained in Σ_i for a certain $i \in \{1,2\}$. Then α has to contain the points M_{3-i} and P_{12} to be able to intersect the lines $\ell_{(3-i)1}$ and $\ell_{(3-i)2}$, respectively, and hence has to intersect Σ_3 in a line $r \subset \pi_{i3}$ through M_{3-i}. If $r \neq m$, then either property (1) or property (2) is true. If $r = m$, then property (3) holds.
Now suppose that α is not contained in Σ_1 nor Σ_2, then α intersects these solids in lines a_1 and a_2, respectively. If α intersects π_{12} in a line, then this line has to be equal to $a_1 = a_2$ which consequently has to contain the non-collinear points M_1, M_2 and P_{12} to be able to intersect the lines ℓ_{11}, ℓ_{21}, ℓ_{12} and ℓ_{22}, a contradiction. Hence, α intersects π_{12} in precisely a point $A := a_1 \cap a_2$ and is therefore equal to $\langle a_1, a_2\rangle$. It is clear that, for $i \in \{1,2\}$, the line a_i has to intersect the disjoint lines ℓ_{i1} and ℓ_{i2}. If $A \notin \{M_1, M_2, P_{12}\}$, then there exists a unique line through A intersecting both of these lines, which hence has to be equal to a_i. This means that A cannot be contained

in $\langle M_i, P_{12}\rangle$, as else $a_i = \langle M_i, P_{12}\rangle \subset \pi_{12}$, and that α is uniquely defined by its intersection point A with π_{12}, finishing the proof. ∎

Thanks to the above lemma, we can now introduce the following notation. For every point $A \in \pi_{12} \setminus (\langle M_1, P_{12}\rangle \cup \langle M_2, P_{12}\rangle)$, let $\alpha^{(A)}$ be the unique plane of $\Pi^{(4)}$ intersecting π_{12} in precisely the point A. For every $i \in \{1,2,3\}$, define the line $a_i^{(A)} := \alpha^{(A)} \cap \Sigma_i$.

Lemma 6.2.2

Let $\mathfrak{a}$ be a line in π_{12} through P_{12} that avoids M_1 and M_2. Then $\left\{a_3^{(A)} : A \in \mathfrak{a} \setminus \{P_{12}\}\right\}$ is a set of q lines that

- *lie in a plane of Σ_3 through s, and*
- *go through a fixed point of β.*

Proof. For every $A \in \mathfrak{a} \setminus \{P_{12}\}$ and each $i \in \{1,2\}$, the line $a_i^{(A)}$ is contained in $\langle \mathfrak{a}, \ell_{i2}\rangle$, a plane independent of the choice of A that intersects ℓ_{i1} necessarily in a point $Q_i \notin (\pi_{12} \cup \pi_{i3})$. The line $a_i^{(A)}$ has to intersect ℓ_{i1}, thus it has to go through the point Q_i. As a first result, all lines of $\left\{a_3^{(A)} : A \in \mathfrak{a} \setminus \{P_{12}\}\right\}$ lie in the plane $\langle \mathfrak{a}, \ell_{12}, \ell_{22}\rangle \cap \Sigma_3$ and hence are coplanar; the corresponding plane contains both P_{13} and P_{23} and hence also the line $\langle P_{13}, P_{23}\rangle = s$. As a second result, all planes of $\left\{\alpha^{(A)} : A \in \mathfrak{a} \setminus \{P_{12}\}\right\}$ go through $\langle Q_1, Q_2\rangle$, which is a line that intersects Σ_3 necessarily in a point $Q_3 \notin \{Q_1, Q_2\}$. Consequently, all lines of $\left\{a_3^{(A)} : A \in \mathfrak{a} \setminus \{P_{12}\}\right\}$ have to go through the point Q_3. As $Q_1 \in \ell_{11}$ and $Q_2 \in \ell_{21}$, the line $\langle Q_1, Q_2\rangle$ lies in $\langle \ell_{11}, \ell_{21}\rangle$ and, hence, Q_3 lies in $\langle \ell_{11}, \ell_{21}\rangle \cap \Sigma_3 = \beta$. ∎

For every line $\mathfrak{a}$ in π_{12} through P_{12} that avoids M_1 and M_2, the q lines of $\left\{a_3^{(A)} : A \in \mathfrak{a} \setminus \{P_{12}\}\right\}$ are coplanar and concurrent. We denote this unique plane by $\gamma^{(\mathfrak{a})} \supset s$ and this unique point of concurrence by $\mathcal{A}^{(\mathfrak{a})} \in \beta$. The q lines will often be called the **pencil of lines** corresponding to $\mathcal{A}^{(\mathfrak{a})}$.

Lemma 6.2.3

The point set $\left\{\mathcal{A}^{(\mathfrak{a})} : P_{12} \in \mathfrak{a} \subset \pi_{12}; M_1, M_2 \notin \mathfrak{a}\right\} \cup \{M_1, M_2\}$ *is a non-singular conic contained in* β *that contains the point* S.

Proof. The fact that ℓ_{11} and ℓ_{12} are disjoint implies that $P_{12} \notin \ell'_{11}$, hence each point $A \in \ell'_{11} \setminus (\{M_1\} \cup \langle M_2, P_{12}\rangle)$ defines a distinct line $\langle A, P_{12}\rangle$. As a consequence, each of the $q-1$ points of $\left\{\mathcal{A}^{(\mathfrak{a})} : P_{12} \in \mathfrak{a} \subset \pi_{12}; M_1, M_2 \notin \mathfrak{a}\right\}$ corresponds to one of the $q-1$ points in $\ell'_{11} \setminus (\{M_1\} \cup \langle M_2, P_{12}\rangle)$. By Lemma 6.2.2, it suffices to prove the statement for the set of intersection points of the lines in $\left\{a_3^{(A)} : A \in \ell'_{11} \setminus (\{M_1\} \cup \langle M_2, P_{12}\rangle)\right\}$ with the plane β.
By the definition of ℓ'_{11}, all lines of $\left\{a_1^{(A)} : A \in \ell'_{11} \setminus (\{M_1\} \cup \langle M_2, P_{12}\rangle)\right\}$ go through P_{13}, hence the lines of $\left\{a_3^{(A)} : A \in \ell'_{11} \setminus (\{M_1\} \cup \langle M_2, P_{12}\rangle)\right\}$ go through P_{13} as well. On the other hand, the lines ℓ'_{11}, ℓ_{21} and ℓ_{22} are pairwise disjoint and lie in the solid Σ_2, hence these define a unique regulus $\mathcal{R}$ corresponding to a hyperbolic quadric $\mathcal{Q}$ (see Section 0.1.6). Let $\mathcal{R}'$ denote its opposite regulus. As the lines of $\left\{a_2^{(A)} : A \in \ell'_{11} \setminus (\{M_1\} \cup \langle M_2, P_{12}\rangle)\right\}$ each have to intersect ℓ'_{11}, ℓ_{21} and ℓ_{22}, these lines are contained in $\mathcal{R}'$.
We claim that $\mathcal{Q} \cap \pi_{23}$ is a non-singular conic. To prove this, first observe that ℓ'_{11} intersects the line $\langle M_2, P_{12}\rangle$ in a point other than M_2 or P_{12}. As M_2 and P_{12} are contained in $\mathcal{Q}$, this implies that $\langle M_2, P_{12}\rangle$ is a generator of $\mathcal{Q}$. Hence, M_2 is contained in the following two generators of $\mathcal{Q}$: $\langle M_2, P_{12}\rangle$ and ℓ_{21}, neither of which are contained in π_{23}. As a consequence, there does not exist a generator of $\mathcal{Q}$ in π_{23} through $M_2 \in \mathcal{Q}$, which implies that $\mathcal{Q} \cap \pi_{23}$ is a non-singular conic $\mathcal{C}$ (containing M_1, M_2 and P_{23}). In conclusion, each of the $q-1$ lines of $\left\{a_3^{(A)} : A \in \ell'_{11} \setminus (\{M_1\} \cup \langle M_2, P_{12}\rangle)\right\}$ intersects the plane π_{13} in the point P_{13} and intersects the plane π_{23} in a distinct point of $\mathcal{C} \setminus \{M_1, M_2\}$. Hence, these lines lie in the cone with vertex P_{13} and base $\mathcal{C}$. Switching our views to the plane β instead of the plane π_{23} simply switches the base of this cone and hence finishes the proof. ∎

Having obtained the above lemma, we can yet again introduce a notation. For every line $\mathfrak{a}$ in π_{12} through P_{12} that avoids M_1 and M_2, let $r^{(\mathfrak{a})}$ be the unique line in $\gamma^{(\mathfrak{a})}$ through $\mathcal{A}^{(\mathfrak{a})}$ not contained in $\left\{a_3^{(A)} \,:\, A \in \mathfrak{a} \setminus \{P_{12}\}\right\}$. Note that such a line is skew to m and differs from s.

We are now ready to choose a fifth line ℓ_{31} that is skew to most planes of $\Pi^{(4)}$.

Configuration 6.2.4

Let $q \neq 2$. We extend Configuration 6.1.2. Let t be the tangent line through S with respect to the non-singular conic described in Lemma 6.2.3, let $M_0 := t \cap m \notin \{M_1, M_2\}$ and consider the line $\mathfrak{a}_0 := \langle M_0, P_{12}\rangle \subset \pi_{12}$. Note that $\mathcal{A}^{(\mathfrak{a}_0)} = S$, as all lines of its corresponding pencil have to intersect β in a point of the conic lying on the tangent line t (which is part of this pencil). Choose a point $M_3 \in m \setminus \{M_0, M_1, M_2\}$ and choose ℓ_{31} to be a line through M_3 intersecting $r^{(\mathfrak{a}_0)}$ in a point outside of $\pi_{13} \cup \pi_{23} \cup \beta$. Note that, in this way, ℓ_{31} is skew to all q lines of $\left\{a_3^{(A)} \,:\, A \in \mathfrak{a}_0 \setminus \{P_{12}\}\right\}$, in particular the line s. Finally, define $Q := \langle m, \ell_{31}\rangle \cap s$.
Be sure to keep Figure 6.1 at hand to maintain an overview of this configuration.

Denote with $\Pi^{(5)}$ the set of all planes of $\Pi^{(4)}$ that intersect ℓ_{31}.

Theorem 6.2.5

There exist six lines of $\mathrm{PG}(4, q)$ *in higgledy-piggledy arrangement, two of which intersect.*

Proof. One can easily check the statement for $q = 2$ using, for example, the package FinInG [17] within GAP [70]. Therefore, we can assume that $q \neq 2$ throughout this proof and consider Configuration 6.2.4. By Result 5.2.2, it suffices to prove that there exists a sixth line ℓ_{32} skew to all planes of $\Pi^{(5)}$. Considering the four properties described in Lemma 6.2.1, all planes of $\Pi^{(5)}$ either meet property (3) or (4) due to the choice of ℓ_{31}. Hence, we can

consider a partition $\{\Pi_1, \Pi_2, \Pi_3, \Pi_4\}$ of $\Pi^{(5)}$, where

- Π_1 is the set of all planes of $\Pi^{(5)}$ intersecting the plane π_{12} in precisely a point not contained in $\langle M_1, P_{12}\rangle \cup \langle M_2, P_{12}\rangle$,
- Π_2 is the set of all planes of $\Pi^{(5)}$ intersecting the plane π_{12} in precisely the point P_{12},
- Π_3 is the set of all planes of $\Pi^{(5)}$ intersecting the plane π_{12} in precisely a point of $\{M_1, M_2\}$, and
- $\Pi_4 := \{\pi_{12}\}$.

By Lemma 6.2.2, the planes of Π_1 intersect the solid Σ_3 in a set of $q^2 - q$ lines, grouped in $q-1$ pencils of q coplanar, concurrent lines; the planes containing each pencil are the $q-1$ planes through s not containing M_1 or M_2, and the points of concurrence of the pencils form, together with M_1 and M_2, a non-singular conic $\mathcal{C}$ of β (Lemma 6.2.3). As ℓ_{31} is skew to s and is not contained in β (nor contains M_1 or M_2), the line ℓ_{31} meets at most one line per pencil. By the choice of ℓ_{31} (see Configuration 6.2.4), this line is skew to all lines of at least one pencil. In conclusion, Π_1 consists of at most $q-2$ planes, one of which intersects Σ_3 in the line $\langle M_3, S\rangle$.
Now consider the planes of Π_2. By the definition of ℓ''_{11} and ℓ''_{21}, each line connecting a point of $\ell''_{11} \setminus \{M_1\}$ with a point of $\ell''_{21} \setminus \{M_2\}$ defines a unique plane of $\Pi^{(4)}$ that intersects π_{12} in precisely the point P_{12}. Of these q^2 planes, only q intersect ℓ_{31} (thus $|\Pi_2| = q$) as part of a regulus of the unique hyperbolic quadric $\mathcal{Q}$ defined by the pairwise disjoint lines ℓ''_{11}, ℓ''_{21} and ℓ_{31}.

Let e be an external line to $\mathcal{C}$ in β through M_3 (note that this always exists, as M_3 lies on the 2-secant m to $\mathcal{C}$ and hence can never be a nucleus) and define the plane $\varepsilon := \langle e, Q\rangle$. We claim that ε intersects $\mathcal{Q}$ in a non-singular conic. Note that, as $M_1, M_2, M_3 \in \mathcal{Q}$, the line m is a generator of $\mathcal{Q}$ through M_3. The second generator of $\mathcal{Q}$ through M_3 is ℓ_{31}. None of these two generators are contained in ε, hence there does not exist a generator of $\mathcal{Q}$

that is contained in ε and goes through $M_3 \in \mathcal{Q}$, implying that $\varepsilon \cap \mathcal{Q}$ must be a non-singular conic.
Observe that all planes of Π_1 intersect ε in at most a point. After all, if this would not be the case, an intersection line of a plane of Π_1 with Σ_3 would lie in ε. Such an intersection line also contains a point of the conic $\mathcal{C}$. However, the plane ε intersects the plane β in the external line e to $\mathcal{C}$, a contradiction.
Note that, as said before, precisely one of the planes of Π_1 intersects Σ_3 in a line going through $M_3 \in \varepsilon$ and hence intersects ε in precisely that point. However, M_3 is already contained in $\mathcal{Q}$. In conclusion, all planes of $\Pi_1 \cup \Pi_2$ intersect the plane ε in a point set $\mathcal{P}$ consisting of all $q+1$ points of a non-singular conic containing M_3 (originating from Π_2), together with at most $q-3$ extra points (originating from Π_1). By Result 6.1.1, we can choose a line ℓ_{32} in ε that avoids all points of $\mathcal{P} \cup \{Q\}$. As $\ell_{32} \subset \Sigma_3$ is consequently skew to the line $m \ni M_3$ (as $m \nsubseteq \varepsilon$), this line is skew to all planes of $\Pi_1 \cup \Pi_2 \cup \Pi_4$.

We claim that ℓ_{32} is skew to all planes of Π_3 as well, finishing the proof. Suppose that $\alpha \in \Pi_3$. Note that $\alpha \nsubseteq \Sigma_3$ as else it has to contain the points M_1, M_2, P_{13} and P_{23} to be able to intersect the lines ℓ_{11}, ℓ_{12}, ℓ_{21} and ℓ_{22}, but those points are not coplanar. Hence, for each $i \in \{1,2,3\}$, α intersects Σ_i in a line a_i. Suppose that α intersects π_{12} in precisely the point M_j for a $j \in \{1,2\}$ (which implies that $a_1 \neq a_2$). Then, for every $i \in \{1,2\}$, the line a_i intersects ℓ_{i2} in a point Q_i. Hence, the plane α contains two distinct points Q_1 and Q_2 of the plane $\langle \ell_{12}, \ell_{22} \rangle$ and hence has to intersect the line s, which means that the line a_3 has to intersect the line s. As a_3 has to intersect the line ℓ_{31} as well, it has to be contained in the plane $\langle M_j, \ell_{31} \rangle$, which intersects the line s in Q; thus a_3 has to go through Q. In conclusion, as a_3 is not contained in ε (because $M_j \notin \varepsilon$), it has to intersect ε in precisely the point Q, which gets avoided by the line ℓ_{32}. ∎

Corollary 6.2.6

There exist six planes of PG$(4,q)$, $q \geqslant 7$, *in higgledy-piggledy arrangement, two of which intersect in a line.*

Proof. This follows from Theorem 6.2.5 and Proposition 5.4.4. ∎

Short minimal codes of dimension 5

The following bundles all known results concerning the smallest possible length of minimal linear codes of dimension 5.

Result 6.2.7 ([6, 8, 19, 24, 69])

$m(5,2) = 13$ *and* $16 \leqslant m(5,3) \leqslant 20$. *In general, the following holds:*

$$4q+4 \leqslant m(5,q) \leqslant \begin{cases} 6q+6 & \text{if } q > 36086 \text{ and } 2,3 \nmid q, \\ 7q+7 & \text{if } q \geqslant 7, \\ 8q-3. & \end{cases}$$

Moreover, if $q \geqslant 9$, *then* $4q+5 \leqslant m(5,q)$.

Proof. The lower bounds on $m(5,q)$ are proved in [8, Theorem 2.14 and Corollary 2.19]. The first two upper bounds arise by combining respectively Result 5.2.7(2) and Result 5.2.6 with Result 5.1.3, while the third upper bound and the cases $q \in \{2,3\}$ are given in [6, Construction 2]. ∎

The main result of this chapter comes down to the following.

Theorem 6.2.8

$m(5,q) \leqslant 6q+5$.

Proof. Directly from Theorem 6.2.5 and Result 5.1.3. ∎

7 planes of PG$(5, q)$

In Chapters 5 and 6, we discussed several higgledy-piggledy sets in projective geometries of small dimension. In PG$(3, q)$, the only non-trivial higgledy-piggledy sets are line sets, which must have size at least 4 if $q \geqslant 3$ (see Result 5.2.4). The existence of a set of four lines in higgledy-piggledy arrangement was already provided by the literature (see Result 5.2.7(1)). In PG$(4, q)$, optimal higgledy-piggledy sets must be line or plane sets of size 6 with two maximally intersecting elements, the existence of which is described in Chapter 6. In PG$(5, q)$, optimal higgledy-piggledy sets are necessarily line or solid sets of size 7, which are proven to exist by Result 5.2.7(3) and Corollary 5.4.5 (if $q \geqslant 7$).

If one restricts their view to projective geometries of dimension at most 5, the only non-trivial case remaining are *higgledy-piggledy plane sets of* PG$(5, q)$, which necessarily contain at least 7 elements. This chapter is devoted to this particular case and is based on [64].

Proposition 7.0.1

Let $q \geqslant 7$. Then any seven planes of PG$(5, q)$ *in higgledy-piggledy arrangement are pairwise disjoint.*

Proof. Let $\mathcal{K} := \{\pi_1, \pi_2, \ldots, \pi_7\}$ be the higgledy-piggledy set in question and suppose, to the contrary (and without loss of generality), that there exists a hyperplane Π containing π_1 and π_2. Define ℓ_3 and ℓ_4 to be lines contained in $\pi_3 \cap \Pi$ and $\pi_4 \cap \Pi$, respectively, and let Σ be a solid in Π that

contains $\langle \ell_3, \ell_4 \rangle$. Choose a point P_i in $\Sigma \cap \pi_i$ for every $i \in \{5,6,7\}$. Then any plane $\pi \subset \Sigma$ that contains $\langle P_5, P_6, P_7 \rangle$ obviously contains a point of π_5, π_6 and π_7. Moreover, as π is contained in $\Sigma \supset \ell_3, \ell_4$, this plane intersects π_3 and π_4 as well. Finally, as $\pi \subset \Pi$, we conclude that π meets all planes of $\mathcal{K}$, contradicting Result 5.2.2. ∎

Two chapters ago, we have shown the existence of eight pairwise disjoint planes in higgledy-piggledy arrangement (see Theorem 5.4.8). Despite the length of this chapter, we already have the tools to prove the existence of seven such planes.

Theorem 7.0.2

There exist seven planes of PG$(5,q)$ *in higgledy-piggledy arrangement.*

Proof. If $q \leqslant 7$, we can easily verify the statement using a computer package such as GAP [17, 70] (see e.g. [62, Code Snippet 56][a]).
Assume that $q \geqslant 8$. By Theorem 5.4.6, it suffices to find seven points of PG$(1,q^3)$ that are not contained in an $\mathbb{F}_q$-linear set of rank 3. Consider a point P of PG$(1,q^3)$. Due to Propositions 0.1.21 to 0.1.23, we know that there are $q\left(q^2+q+1\right)$ clubs with head P, $q^3\left(q^2+q+1\right)$ clubs through P with head different from P, and $\frac{1}{2}q^3\left(q^3-1\right)$ scattered $\mathbb{F}_q$-linear sets containing P. Let x denote the number of tuples $(P_1,P_2,P_3,P_4,P_5,P_6,\mathcal{L})$, where $P_i \neq P_j \neq P$ are points of PG$(1,q^3)$ $(i,j \in \{1,2,\ldots,6\},\ i \neq j)$ and where $\mathcal{L}$ is an $\mathbb{F}_q$-linear set of rank 3 containing P and every P_i. Then

$$x = q\left(q^2+q+1\right)c_q + q^3\left(q^2+q+1\right)c_q + \frac{1}{2}q^3\left(q^3-1\right)s_q,$$

where $c_q := \prod_{i=0}^{5}\left(q^2-i\right)$, respectively $s_q := \prod_{i=0}^{5}\left(q^2+q-i\right)$, equals the number of ways to choose six distinct points, different from P, contained in a club, respectively scattered $\mathbb{F}_q$-linear set, through P. If all choices of 6 points $P_1,\ldots,P_6$ would be contained in at least one $\mathbb{F}_q$-linear set of rank 3 through P, then $x \geqslant \prod_{i=0}^{5}\left(q^3-i\right)$, which leads to a contradiction if $q \geqslant 8$. ∎

[a] In fact, there exist six such planes in PG$(5,3)$ and five such planes in PG$(5,2)$.

So why bother to continue reading this chapter, you might ask? In truth, the above result was only found after meticulously describing the *ABB-representation of linear sets* (see Section 7.2). This description, however, is still of a certain mathematical value and allows us to give a constructive proof of the result above (for infinite values of q, see Theorem 7.3.3).

7.1 Generalising the bundle of conics

ASSUMPTION

Throughout this *section*, we assume that $t \in \mathbb{N} \setminus \{0,1\}$ and consider $\mathrm{PG}(t-1,q^t)$, in which we embed $D_\infty \cong \mathrm{PG}(t-1,q)$ as an $\mathbb{F}_q$-subgeometry. Moreover, let $E_0 \notin D_\infty$ be a point and σ be a collineation fixing every point of D_∞ such that $\left\{E_0, E_0^\sigma, \ldots, E_0^{\sigma^{t-1}}\right\}$ is a basis of $\mathrm{PG}(t-1,q^t)$.[a]

Given a positive divisor $s \mid t$, it is known that $\mathrm{Fix}(\sigma^s) \cong \mathrm{PG}(t-1,q^s)$; define $\Sigma_s := \left\langle E_0, E_0^{\sigma^s}, E_0^{\sigma^{2s}}, \ldots, E_0^{\sigma^{t-s}} \right\rangle \subseteq \mathrm{Fix}(\sigma^s)$. Then the set $\left\{\Sigma_s, \Sigma_s^\sigma, \ldots, \Sigma_s^{\sigma^{s-1}}\right\}$ is the unique indicator set of a Desarguesian $(s-1)$-spread $\mathcal{D}_s$ of D_∞.

[a] This mimics the set-up described in the second part of Section 0.1.7 ($r = 1$).

Consider the case $t = 3$. In [16], Baker, Brown, Ebert and Fisher describe three types of *projective bundles*, which were originally introduced in Glynn's PhD thesis as *packings* [72]. These are collections of q^2+q+1 non-singular conics in D_∞ that mutually intersect in exactly one point. One of the described types is the *circumscribed bundle*, which is the set of all non-singular conics in D_∞ that possess an $\mathbb{F}_{q^3}$-extension containing the points E_0, E_0^σ and $E_0^{\sigma^2}$.
Consider the point-line geometry $(\mathcal{P},\mathcal{L},I)$, where $\mathcal{P}$ consists of all points in D_∞, $\mathcal{L}$ consists of all non-singular conics of the circumscribed bundle and

incidence is symmetric set-theoretic containment. In the literature (see e.g. [72, Section 1.2], or [109, Remark on page 61] combined with [89, Corollary 19]), it is known that this point-line geometry is *isomorphic to the point-line geometry of* PG$(2,q)$.

In this section, we aim to generalise this observation to arbitrary t, proving that a certain collection of normal rational curves in D_∞ gives rise to a point-line geometry isomorphic to the point-line geometry of PG$(t-1,q)$. If t is prime, such a generalisation turns out to be quite straightforward. If t is not prime, however, extra care must be taken.

7.1.1 Choosing the right coordinates

We make use of a particular coordinate system to conveniently deal with normal rational curves.

Configuration 7.1.1

Choose coordinates in such a way that E_0 corresponds to coordinates $(1,0,\ldots,0)^\mathsf{T}$ and that a point $P_x \in D_\infty$ has coordinates

$$\left(\frac{1}{x}, \frac{1}{x^q}, \frac{1}{x^{q^2}}, \ldots, \frac{1}{x^{q^{t-1}}}\right)^\mathsf{T}$$

for a certain $x \in \mathbb{F}_{q^t} \setminus \{0\}$. Let σ be the collineation arising from the map

$$(x_0, x_1, x_2, \ldots, x_{t-1})^\mathsf{T} \mapsto \left(x_{t-1}^q, x_0^q, x_1^q, \ldots, x_{t-2}^q\right)^\mathsf{T}.$$

Note that $E_0^{\sigma^i} = E_i$ for every $i \in \{0,1,\ldots,t-1\}$, where $\{E_0, E_1, \ldots, E_{t-1}\}$ is part of the canonical frame.

Faina, Kiss, Marcugini and Pambianco [67] considered the *cyclic model* of PG$(t-1,q)$, in which the 'additive inverse' of a line is a normal rational curve.

Result 7.1.2 ([67, Theorem **3.4** and further])

If $y, z \in \mathbb{F}_{q^t} \setminus \{0\}$, $y/z \notin \mathbb{F}_q$, then the point set

$$\left\{ P_{yu-zv} \,:\, (u,v) \in \mathbb{F}_q^2 \setminus \{(0,0)\} \right\}$$

is a normal rational curve.

Consider a spread element $D \in \mathcal{D}_s$ and a point $P_x \in D$, where $s \mid t$ and $x \in \mathbb{F}_{q^t} \setminus \{0\}$. As $\Sigma_s = \langle E_0, E_s, E_{2s}, \ldots, E_{t-s} \rangle$, one can check that the point $Q_s := \langle D \rangle_{q^s} \cap \Sigma_s$ has coordinates

$$\left(\frac{1}{x}, 0, \ldots, 0, \frac{1}{x^{q^s}}, 0, \ldots, 0, \frac{1}{x^{q^{2s}}}, 0, \ldots\ldots\ldots, 0, \frac{1}{x^{q^{t-s}}}, 0, \ldots, 0 \right)^{\mathsf{T}}. \tag{7.1}$$

Note that, despite x being present in (7.1), the definition of Q_s does not rely on the choice of $P_x \in D$.

Lemma 7.1.3

Let $s \mid t$ and $y, z \in \mathbb{F}_{q^t} \setminus \{0\}$. Then P_y and P_z lie in the same element of $\mathcal{D}_s$ if and only if $y/z \in \mathbb{F}_{q^s}$.

Proof. The points P_y and P_z lie in the same element of $\mathcal{D}_s$ if and only if the vector in (7.1) represents the coordinates of a fixed point regardless of whether x is replaced by y or z. This is equivalent to the existence of an $\alpha \in \mathbb{F}_{q^t}$ such that

$$\frac{y^{q^{ks}}}{z^{q^{ks}}} = \alpha \qquad \text{for every } k \in \{0, 1, \ldots, t/s - 1\},$$

which is equivalent to $y/z = (y/z)^{q^s}$, finishing the proof. ∎

Lemma 7.1.4

Suppose that $y,z \in \mathbb{F}_{q^t} \setminus \{0\}$, $y/z \notin \mathbb{F}_q$, let s be the smallest integer such that P_y and P_z lie in the same spread element $D \in \mathcal{D}_s$ and define $Q_s := \langle D \rangle_{q^t} \cap \Sigma_s$. Then there exists a unique normal rational curve of degree $s-1$ in $\langle D \rangle_{q^s}$ containing P_y, P_z and the s conjugate points $Q_s, Q_s^{\sigma}, \ldots, Q_s^{\sigma^{s-1}}$. This curve meets D in the normal rational curve

$$\mathcal{C}_{y,z} := \left\{ P_{yu-zv} \,:\, (u,v) \in \mathbb{F}_q^2 \setminus \{(0,0)\} \right\}.$$

Proof. Consider, within $\langle D \rangle_{q^t}$, the point set $\mathcal{C}$ corresponding to the set of coordinates

$$\left\{ \sum_{i=0}^{s-1} \prod_{j=0, j\neq i}^{s-1} \left(y^{q^j} u - z^{q^j} v \right) \boldsymbol{a_i} \,:\, (u,v) \in \mathbb{F}_{q^t}^2 \setminus \{(0,0)\} \right\}, \tag{7.2}$$

where

$$\begin{aligned}
\boldsymbol{a_0} &= y \left(\frac{1}{y}, 0, \ldots, 0, \frac{1}{y^{q^s}}, 0, \ldots\ldots\ldots, 0, \frac{1}{y^{q^{t-s}}}, 0, \ldots, 0 \right)^{\mathsf{T}} \\
\boldsymbol{a_1} &= y^q \left(0, \frac{1}{y^q}, 0, \ldots, 0, \frac{1}{y^{q^{s+1}}}, 0, \ldots\ldots\ldots, 0, \frac{1}{y^{q^{t-s+1}}}, 0, \ldots, 0 \right)^{\mathsf{T}} \\
&\vdots \\
\boldsymbol{a_{s-1}} &= y^{q^{s-1}} \left(0, \ldots, 0, \frac{1}{y^{q^{s-1}}}, 0, \ldots, 0, \frac{1}{y^{q^{2s-1}}}, 0, \ldots\ldots\ldots, 0, \frac{1}{y^{q^{t-1}}} \right)^{\mathsf{T}}.
\end{aligned}$$

From the literature, we know that $\mathcal{C}$ is a normal rational curve and that there are exactly $\deg(\mathcal{C})+1$ points of $\mathrm{PG}(1,q^t)$ corresponding to the coordinates $\mathcal{T} := \left\{ \left(y^{q^i}, z^{q^i} \right)^{\mathsf{T}} \,:\, i \in \{0,\ldots,t-1\} \right\}$ (see e.g. [76, Example 1.17]). By Lemma 7.1.3, s is the smallest integer such that $(y/z)^{q^s} = y/z$, which implies that $\mathcal{T}$ gives rise to s unique points, making the degree of $\mathcal{C}$ equal to $s-1$.

We now prove that points of $\mathcal{C}$ lie in D if and only if either $v = 0$ or $u/v \in \mathbb{F}_q$.

Consider an arbitrary point $P \in \mathcal{C}$ and suppose that $P \in D$, hence $P = P_x$ for an $x \in \mathbb{F}_{q^t} \setminus \{0\}$. As $y/x \in \mathbb{F}_{q^s}$ by Lemma 7.1.3, $y^{q^i}/x^{q^i} \in \mathbb{F}_{q^s}$ as well, implying that $y^{q^i}/x^{q^i} = \left(y^{q^i}/x^{q^i}\right)^{q^{ks}}$ for every $i \in \{0, 1, \ldots, s-1\}$ and every $k \in \{0, 1, \ldots, t/s - 1\}$. Therefore, one can check that

$$\left(\frac{1}{x}, \frac{1}{x^q}, \ldots, \frac{1}{x^{q^{t-1}}}\right)^\intercal = \sum_{i=0}^{s-1} \frac{1}{x^{q^i}} \boldsymbol{a_i}.$$

As $P_x \in \mathcal{C}$, an $\mathbb{F}_{q^t}$-multiple of the above must be an element of (7.2), or, in other words, there must exist an $\alpha \in \mathbb{F}_{q^t} \setminus \{0\}$ and an $(u, v) \in \mathbb{F}_{q^t}^2 \setminus \{(0,0)\}$ such that

$$\begin{aligned}
&\alpha \sum_{i=0}^{s-1} \frac{1}{x^{q^i}} \boldsymbol{a_i} = \sum_{i=0}^{s-1} \prod_{j=0, j\neq i}^{s-1} \left(y^{q^j} u - z^{q^j} v\right) \boldsymbol{a_i} \\
\iff \quad & \mathbf{0} = \sum_{i=0}^{s-1} \left(\prod_{j=0, j\neq i}^{s-1} \left(y^{q^j} u - z^{q^j} v\right) - \frac{\alpha}{x^{q^i}} \right) \boldsymbol{a_i} \\
\iff \quad & 0 = \prod_{j=0, j\neq i}^{s-1} \left(y^{q^j} u - z^{q^j} v\right) - \frac{\alpha}{x^{q^i}}, \qquad \forall i \in \{0, 1, \ldots, s-1\},
\end{aligned}$$

implying that

$$\alpha = x^{q^i} \prod_{j=0, j\neq i}^{s-1} \left(y^{q^j} u - z^{q^j} v\right), \qquad \forall i \in \{0, 1, \ldots, s-1\}.$$

As $\alpha \neq 0$, each factor on the right-hand side is non-zero as well, hence we can divide by $\prod_{j=0}^{s-1} \left(y^{q^j} u - z^{q^j} v\right)$ and take the inverse of both sides to conclude that there exists a value $\beta \in \mathbb{F}_{q^t} \setminus \{0\}$ such that

$$\beta = \left(\frac{y}{x}\right)^{q^i} u - \left(\frac{z}{x}\right)^{q^i} v, \qquad \forall i \in \{0, 1, \ldots, s-1\}.$$

Note that, by Lemma 7.1.3, the above holds for all $i \in \mathbb{N}$. Therefore, it is equivalent to stating that either $v = 0$ or

$$\left(\frac{y}{x}\right)^{q^i} u - \left(\frac{z}{x}\right)^{q^i} v = \left(\frac{y}{x}\right)^{q^{i+1}} u - \left(\frac{z}{x}\right)^{q^{i+1}} v \iff \frac{u}{v} = \frac{\left(\frac{z}{x}\right)^{q^i} - \left(\frac{z}{x}\right)^{q^{i+1}}}{\left(\frac{y}{x}\right)^{q^i} - \left(\frac{y}{x}\right)^{q^{i+1}}},$$

for all $i \in \mathbb{N}$, implying that u/v stays invariant under taking qth powers, thus $u/v \in \mathbb{F}_q$.

Conversely, if $v = 0$, then $u \neq 0$ and (7.2) produces the coordinates

$$\sum_{i=0}^{s-1} \prod_{j=0, j\neq i}^{s-1} \left(y^{q^j} u\right) \boldsymbol{a_i}.$$

As $y^{q^j} \neq 0$, we can divide this by $u^{s-1} \prod_{j=0}^{s-1} y^{q^j}$ to obtain

$$\sum_{i=0}^{s-1} \frac{1}{y^{q^i}} \boldsymbol{a_i},$$

which are the coordinates of the point P_y.
Now suppose that $u, v \in \mathbb{F}_{q^t}$, $v \neq 0$, such that $w := u/v \in \mathbb{F}_q$. Note that if $y^{q^j} u - z^{q^j} v$ is zero, then $(z/y)^{q^j} = w \in \mathbb{F}_q$, implying that $z/y = (z/y)^{q^s} = \left((z/y)^{q^j}\right)^{q^{s-j}} \in \mathbb{F}_q$, a contradiction. Therefore, we may divide the coordinates in (7.2) by $\prod_{j=0}^{s-1} \left(y^{q^j} u - z^{q^j} v\right)$ to obtain

$$\sum_{i=0}^{s-1} \frac{1}{y^{q^i} u - z^{q^i} v} \boldsymbol{a_i}, \tag{7.3}$$

which is equal to a vector of $V\left(t, q^t\right)$ with

$$\frac{y^{q^i}}{y^{q^i} u - z^{q^i} v} \cdot \frac{1}{y^{q^{ks+i}}} = \frac{1}{v} \cdot \left(\frac{y}{yw - z}\right)^{q^i} \cdot \frac{1}{y^{q^{ks+i}}} \tag{7.4}$$

in the $(ks+i+1)$th position ($k \in \{0,1,\ldots,{}^{t}/_{s}-1\}$, $i \in \{0,1,\ldots,s-1\}$). The fact that ${}^{z}/_{y} \in \mathbb{F}_{q^s}$ implies that $\frac{yw-z}{y} = w - \frac{z}{y} \in \mathbb{F}_{q^s}$ as well. Therefore, $\frac{y}{yw-z} \in \mathbb{F}_{q^s}$, hence

$$\frac{y}{yw-z} = \frac{y^{q^{ks}}}{(yw-z)^{q^{ks}}}.$$

Plugging this into (7.4) gives $\frac{1}{v} \cdot \frac{1}{(yw-z)^{q^{ks+i}}}$, making (7.3) equal to

$$\frac{1}{v}\left(\frac{1}{yw-z}, \frac{1}{(yw-z)^{q}}, \ldots, \frac{1}{(yw-z)^{q^{t-1}}}\right)^{\mathsf{T}},$$

which are the coordinates of the point P_{yw-z}. Note that $P_{yw-z} \in D$ due to Lemma 7.1.3 and the fact that $\frac{y}{yw-z} \in \mathbb{F}_{q^s}$.

Finally, for every $l \in \{0,1,\ldots,s-1\}$, one can put $(u,v) = \left(z^{q^l}, y^{q^l}\right)$ in (7.2) to obtain a non-zero $\mathbb{F}_{q^t}$-multiple of $\boldsymbol{a_l}$, representing the coordinates of $Q_s^{\sigma^l}$ (recall the arguments leading up to (7.1)).

By Result 0.1.11, $\mathcal{C}$ is unique in the sense that it lies in $\langle D \rangle_{q^t}$, has degree $s-1$ and contains P_y, P_z and the s conjugate points $Q, Q^{\sigma}, \ldots, Q^{\sigma^{s-1}}$. Due to the arguments above, this normal rational curve meets D precisely in the point set $\left\{P_{yu-zv} : (u,v) \in \mathbb{F}_q^2 \setminus \{(0,0)\}\right\}$, which is a normal rational curve by Result 7.1.2. ∎

7.1.2 A subspace of curves

We can now introduce the following generalisation of the circumscribed bundle of conics.

Definition 7.1.5 (circumscribed bundle of curves)

Keeping Configuration 7.1.1 in mind, consider the point-line geometry $(\mathcal{P}, \mathcal{L}, I)$ with natural incidence, where

- $\mathcal{P}$ is the set of points in D_∞, and
- $\mathcal{L} := \left\{ \mathcal{C}_{y,z} \,:\, y,z \in \mathbb{F}_{q^t} \setminus \{0\}, {}^{y}/_{z} \notin \mathbb{F}_q \right\}$ (see Lemma 7.1.4).

We will call this point-line geometry the **circumscribed bundle of curves**.

If $t = 3$, the above point-line geometry is precisely the one arising from the circumscribed bundle of conics.

Theorem 7.1.6

Let $t \in \mathbb{N} \setminus \{0,1\}$. Then the circumscribed bundle of curves is isomorphic to the point-line geometry of PG$(t-1,q)$.

Proof. By Lemma 7.1.4, this point-line geometry is a $2-(\theta_{t-1}, q+1, 1)$ design. Note that the statement is trivial if $t = 2$ and was already known in the literature in case $t = 3$ ([109, Remark on page 61] combined with [89, Corollary 19]).
If $t \geqslant 4$, by Result 0.1.6, it suffices to prove that the point-line geometry is an axiomatic projective geometry (see Definition 0.1.4). The first and third axioms follow from Lemma 7.1.4; below, we verify Veblen's axiom.
Let P_a, P_b, P_c and P_d be four distinct points in D_∞ such that the normal rational curves $\mathcal{C}_{a,b}$ and $\mathcal{C}_{c,d}$ share a point P ($a,b,c,d \in \mathbb{F}_{q^t} \setminus \{0\}$). Therefore, $P = P_{au_1 - bv_1} = P_{cu_2 - dv_2}$ for certain $(u_1,v_1), (u_2,v_2) \in \mathbb{F}_q^2 \setminus \{(0,0)\}$. By Lemma 7.1.3, ${}^{(au_1 - bv_1)}/_{(cu_2 - dv_2)} \in \mathbb{F}_q$. Hence, there exists an element

$w \in \mathbb{F}_q \setminus \{0\}$ such that

$$\begin{aligned} & au_1 - bv_1 = w\,(cu_2 - dv_2) \\ \iff \quad & au_1 - c\,(wu_2) = bv_1 - d\,(wv_2)\,. \end{aligned} \tag{7.5}$$

Note that $(u_1, wu_2) \neq (0,0)$, as else $v_1 \neq 0 \neq v_2$ and hence (7.5) would imply that ${}^b/_d \in \mathbb{F}_q$, which means, by Lemma 7.1.3, that $P_b = P_d$, a contradiction. Similarly, $(v_1, wv_2) \neq (0,0)$. Therefore, by (7.5), $P_{au_1 - c(wu_2)} = P_{bv_1 - d(wv_2)}$, thus the normal rational curves $\mathcal{C}_{a,c}$ and $\mathcal{C}_{b,d}$ have a point in common as well. ∎

By the theorem above, the circumscribed bundle of curves (see Definition 7.1.5) *admits subspaces of a certain dimension* as explained in Definition 0.1.5. To avoid confusion with subspaces of a projective geometry, we will call these subspaces consisting of normal rational curves **$\mathcal{N}$-subspaces**.

7.2 The ABB-representation of linear sets

André [9] and Bruck and Bose [36] independently derived a representation of an axiomatic projective plane as a point-line geometry embedded in $\mathrm{PG}(2t, q)$. We refer to this correspondence as the **André/Bruck-Bose representation**, or **ABB-representation** for short.

Several researchers have studied the ABB-representation of certain 'nice' substructures in $\mathrm{PG}(2, q^t)$, as this already has been done for $\mathbb{F}_q$-sublines and -subplanes (Result 7.2.2), (sub)conics [97] and Hermitian unitals [26]. Therefore, one can wonder what the ABB-representation of $\mathbb{F}_q$-linear sets looks like, as such information can help us get a better grasp on these exotic point sets.

7.2.1 The André/Bruck-Bose representation

The following description of the ABB-representation is based on [98].

Let H_∞ be a hyperplane of $\mathrm{PG}(2t,q)$ playing the role of hyperplane at infinity for $\mathrm{AG}(2t,q)$ and let $\mathcal{S}$ be a $(t-1)$-spread in H_∞. Let $\mathcal{P}$ be the set consisting of all affine points together with the q^t+1 spread elements of $\mathcal{S}$. Let $\mathcal{L}$ be the set consisting of H_∞ together with all t-subspaces of $\mathrm{PG}(2t,q)$ meeting H_∞ in exactly an element of $\mathcal{S}$. Then the point-line geometry $(\mathcal{P},\mathcal{L},I)$, with I the naturally inherited incidence of $\mathrm{PG}(2t,q)$, is isomorphic to an axiomatic projective plane. This plane is isomorphic to $\mathrm{PG}(2,q^t)$ if and only if the spread $\mathcal{S}$ is Desarguesian.

ASSUMPTION

Throughout this *section*, we assume that $t \in \mathbb{N}\setminus\{0,1\}$ and consider $\mathrm{PG}(2,q^t)$, in which ℓ_∞ plays the role of line at infinity for $\mathrm{AG}(2,q^t)$. Define $H_\infty := \mathcal{F}(\ell_\infty)$, which is a $(2t-1)$-dimensional subspace of $\mathrm{PG}(3t-1,q)$, and fix a $(2t)$-subspace Λ through H_∞. It is not hard to check, within $\mathrm{PG}(2t,q)\cong\Lambda$, that the ABB-representation of a point P of $\mathrm{PG}(2,q^t)$ can be defined as $\mathcal{F}(P)\cap\Lambda$, which is either a point or a $(t-1)$-subspace. We let φ denote the **André/Bruck-Bose map** that maps any point P of $\mathrm{PG}(2,q^t)$ onto

$$\varphi(P) := \mathcal{F}(P)\cap\Lambda$$

and any line different from ℓ_∞ onto the unique t-subspace containing the image of every point on that line.
Consider a line ℓ of $\mathrm{PG}(2,q^t)$ that intersects ℓ_∞ exactly in a point P_∞ and define $D_\infty := \varphi(P_\infty)$ and $\Pi := \varphi(\ell)$.

Finally, recall the set-up and notation described at the start of Section 7.1. Note that we identify the points $E_0, E_0^\sigma, \ldots, E_0^{\sigma^{t-1}}$ as the unique t conjugate points that give rise to the spread element D_∞ of the Desarguesian $(t-1)$-spread $\mathcal{F}(\{P : P\in\ell_\infty\})$ in H_∞. As deduced in Section 7.1, the spread element D_∞ allows $\mathcal{N}$*-subspaces*.

Definition 7.2.1 (tangent and external linear sets)

We call an $\mathbb{F}_q$-linear set in $\ell \cong \mathrm{PG}(1, q^t)$ **tangent** if it contains P_∞ and **external** otherwise.

The ABB-representation of general $\mathbb{F}_{q^s}$-sublines and tangent $\mathbb{F}_{q^s}$-subplanes of $\mathrm{PG}(2, q^t)$ was studied by Rottey, Sheekey and Van de Voorde [98]. We only concern ourselves with a special case of their findings to fit our needs. By slightly rewriting their results, we can remove the original condition that $q \geqslant t$ in the second part of the statement below, as this was mainly introduced because the authors deal with a more common definition of normal rational curves, where one imposes that these are arcs of $\mathrm{PG}(t, q)$.

Result 7.2.2 ([98])

(1) *The ABB-representation of the affine points of a tangent $\mathbb{F}_q$-subline in ℓ are the points of an affine line in Π and vice versa.*

(2) *Consider an external $\mathbb{F}_q$-subline $\mathfrak{L}$ in ℓ for which s is the smallest positive divisor of t such that $\mathfrak{L}$ is contained in a tangent $\mathbb{F}_{q^s}$-subline. Then the ABB-representation of the points in $\mathfrak{L}$ is a set of affine points $\mathcal{C}$ in Π such that*

   (i) *$\mathcal{C}$ is a normal rational curve contained in an s-subspace $\pi \subseteq \Pi$ intersecting D_∞ in an element of $\mathcal{D}_s$, and*

   (ii) *there exists a unique normal rational curve in $\langle \pi \rangle_{q^t}$ of degree s that contains $\mathcal{C}$ and intersects the indicator set $\left\{\Sigma_s, \Sigma_s^\sigma, \ldots, \Sigma_s^{\sigma^{s-1}}\right\}$ of $\mathcal{D}_s$ in s conjugate points.*

   and vice versa, any affine point set $\mathcal{C}$ in Π with those properties (for a smallest s) gives rise to the point set of such an external $\mathbb{F}_q$-subline.

Proof. While (1) is a special case of [98, Theorem 3.3] and (2) follows from [98, Theorem 3.6] if $q \geqslant t$, we provide some additional arguments on why (2) remains true for small values of q.

The first part of the proof of [98, Theorem 3.6] remains true for all q, i.e. the ABB-representation of such an external $\mathbb{F}_q$-subline is a particular normal rational curve with the described properties. Conversely, any three affine, non-collinear points A, B and C in Π are contained in an affine point set $\mathcal{C}$ in Π that satisfies properties (i) and (ii) for some divisor s, which must be minimal by [98, Lemma 3.5]. Now, while an $\mathbb{F}_{q^t}$*-extension* of $\mathcal{C}$ is not necessarily unique, by Result 0.1.11 (as $q^t \geqslant s+2$ due to $t \geqslant s \geqslant 2$), there does exist a unique normal rational curve of degree s in $\langle \pi \rangle_{q^t}$ that contains the 3 points A, B and C, together with the s conjugate points in the indicator set of $\mathcal{D}_s$. Therefore, the proposed counting argument still holds for all q. ∎

7.2.2 Tangent clubs of PG$(1, q^t)$

Proposition 7.2.3

A point set $\mathcal{L}$ in ℓ is a club of rank $n \in \mathbb{N} \setminus \{0\}$ with head P_∞ if and only if the ABB-representation of $\mathcal{L} \setminus \{P_\infty\}$ is equal to the point set of an affine $(n-1)$-subspace of Π.

Proof. Suppose that $\mathcal{L}$ is a club in ℓ of rank n with head P_∞ and let $P_1, P_2 \in \mathcal{L} \setminus \{P_\infty\}$ be two distinct points. By Proposition 0.1.16, the unique $\mathbb{F}_q$-subline through P_1, P_2 and P_∞ is contained in $\mathcal{L}$. Therefore, due to Result 7.2.2(1), all affine points on the line $\langle \varphi(P_1), \varphi(P_2) \rangle$ are part of the ABB-representation of $\mathcal{L} \setminus \{P_\infty\}$. As P_1 and P_2 were chosen arbitrarily, this ABB-representation must be an affine subspace, necessarily of dimension $\log_q(|\mathcal{L} \setminus \{P_\infty\}|) = n-1$.
Conversely, a simple counting argument shows that there exist exactly

$$\frac{q^t\left(q^t-1\right)\left(q^t-q\right)\cdots\left(q^t-q^{n-2}\right)}{q^{n-1}\left(q^{n-1}-1\right)\left(q^{n-1}-q\right)\cdots\left(q^{n-1}-q^{n-2}\right)} = q^{t-n+1}\begin{bmatrix} t \\ n-1 \end{bmatrix}_q$$

affine $(n-1)$-subspaces in Π, which equals the number of clubs of PG$(1, q^t)$ of rank n with a fixed head (Proposition 0.1.21). ∎

Proposition 7.2.4

Let $n \in \mathbb{N} \setminus \{0\}$. Then there exist $q^t \begin{bmatrix} t \\ n-1 \end{bmatrix}_q$ cones in Π with vertex an affine point and base an $(n-2)$-dimensional $\mathcal{N}$-subspace of D_∞.

Proof. Due to Theorem 7.1.6, the number of $(n-2)$-dimensional $\mathcal{N}$-subspaces of D_∞ is equal to the number of $(n-2)$-subspaces in $\mathrm{PG}(t-1,q)$. Each of the q^t affine points in Π and each of such $\mathcal{N}$-subspaces define a unique cone. ∎

Theorem 7.2.5

Suppose that $q \geqslant 3$. A point set $\mathcal{L}$ in ℓ is a tangent club of rank $n \in \mathbb{N} \setminus \{0\}$ with head $H \neq P_\infty$ if and only if the ABB-representation of $\mathcal{L} \setminus \{P_\infty\}$ is equal to the affine point set of a cone in Π with vertex $\varphi(H)$ and base an $(n-2)$-dimensional $\mathcal{N}$-subspace of D_∞.

Proof. Suppose that $\mathcal{L}$ is a tangent club of rank n with head $H \neq P_\infty$ and let $P \in \mathcal{L} \setminus \{H, P_\infty\}$ be a point. By Proposition 0.1.16, the unique $\mathbb{F}_q$-subline through H, P and P_∞ is contained in $\mathcal{L}$. Therefore, due to Result 7.2.2(1), all affine points in the line $\langle \varphi(H), \varphi(P) \rangle$ are part of the ABB-representation of $\mathcal{L} \setminus \{P_\infty\}$. As P was chosen arbitrarily, this ABB-representation is precisely the set of affine points on a union of $\frac{q^{n-1}-1}{q-1} = \theta_{n-2}$ lines through $\varphi(H)$, that is, they form a cone with vertex $\varphi(H)$. Those lines meet D_∞ in a set $\mathcal{B}$ of θ_{n-2} points.
Let B_1 and B_2 be two arbitrary, distinct points of $\mathcal{B}$. For each $i \in \{1,2\}$, choose an affine point $P_i \in \langle \varphi(H), B_i \rangle$ distinct from $\varphi(H)$, which, by the above arguments, is part of the ABB-representation of $\mathcal{L} \setminus \{P_\infty\}$. Therefore, by Proposition 0.1.16, the unique $\mathbb{F}_q$-subline $\mathfrak{L}$ through H, $\varphi^{-1}(P_1)$ and $\varphi^{-1}(P_2)$ is contained in $\mathcal{L}$. Note, as $B_1 \neq B_2$, that the points $\varphi(H)$, P_1 and P_2 cannot be collinear, hence $\mathfrak{L}$ is an external $\mathbb{F}_q$-subline due to Result 7.2.2(1). Let s be the smallest positive divisor of t such that $\mathfrak{L}$ is contained in a tangent $\mathbb{F}_{q^s}$-subline. Then, by Result 7.2.2(2), the ABB-representation of

the points in $\mathfrak{L}$ is a normal rational curve $\mathcal{C}$ going through $\varphi(H)$, P_1 and P_2 for which there exists a normal rational curve $\mathcal{C}^*$ of degree s in $\langle\Pi\rangle_{q^t}$ that intersects the indicator set of $\mathcal{D}_s$ in s conjugate points. By Result 0.1.12, the set

$$\left\{\langle H,Q\rangle \cap \langle D_\infty\rangle_{q^t} \,:\, Q \in \mathcal{C}^* \setminus \{H\}\right\}$$

consists of q^t points contained in a normal rational curve $\widetilde{\mathcal{C}}^*$ of degree $s-1$ in $\langle D_\infty\rangle_{q^t}$ that necessarily contains the aforementioned s conjugate points, as these all lie in $\langle D_\infty\rangle_{q^t}$, and contains at least q points of $\mathcal{B}$. Due to Lemma 7.1.4, $\widetilde{\mathcal{C}}^*$ meets D_∞ in an $\mathcal{N}$-line. As B_1 and B_2 were chosen arbitrary, we conclude that $\mathcal{B}$ is a point set of size θ_{n-2} for which any $\mathcal{N}$-line contains either at most one or at least q points. Therefore, by Theorems 2.2.2 and 7.1.6, $\mathcal{B}$ is an $(n-2)$-dimensional $\mathcal{N}$-subspace.
Conversely, by Propositions 0.1.22 and 7.2.4, the number of such cones equals the number of tangent clubs of rank n with a head different from P_∞. ∎

7.2.3 Tangent scattered linear sets of PG$(1,q^3)$

Proposition 7.2.6

Consider the case $t=3$. There exist $\frac{1}{2}q^3\left(q^3-1\right)$ hyperbolic quadrics in Π that intersect the plane D_∞ in a non-singular conic $\mathcal{C}$ of which an $\mathbb{F}_{q^3}$-extension contains the 3 conjugate points corresponding to D_∞.

Proof. By Theorem 7.1.6, there are θ_2 non-singular conics in D_∞ that have the described properties. It is known that the total number of hyperbolic quadrics in Π is equal to $\frac{1}{2}q^4\left(q^2+1\right)\left(q^3-1\right)$ [82, Lemma 1.1]. The number of non-singular conics contained in a fixed hyperbolic quadric equals the number of non-tangent (hyper)planes, i.e. $\theta_3-(q+1)^2=q\left(q^2-1\right)$, and the number of non-singular conics in a solid is $q^2\left(q^3-1\right)\theta_3$, which is the number of non-singular conics in a fixed plane multiplied by the total number of planes in PG$(3,q)$. We can now perform a double counting

argument to conclude that there exist

$$\frac{\frac{1}{2}q^4\left(q^2+1\right)\left(q^3-1\right)q\left(q^2-1\right)}{q^2\left(q^3-1\right)\theta_3}=\frac{1}{2}q^3\left(q-1\right)$$

hyperbolic quadrics containing a fixed non-singular conic. Hence, in total, there are $\theta_2\frac{1}{2}q^3\left(q-1\right)=\frac{1}{2}q^3\left(q^3-1\right)$ hyperbolic quadrics $\mathcal{Q}$ in Π that intersect the plane D_∞ in a non-singular conic $\mathcal{C}$ of which an $\mathbb{F}_{q^3}-$extension contains the 3 conjugate points corresponding to D_∞. ∎

Theorem 7.2.7

Suppose that $q\geqslant 5$ and consider the case $t=3$. A point set $\mathcal{L}$ in ℓ is a tangent scattered $\mathbb{F}_q$-linear set of rank 3 if and only if the ABB-representation of $\mathcal{L}\setminus\{P_\infty\}$ is equal to the affine point set of a hyperbolic quadric in Π that meets the plane D_∞ in a non-singular conic whose $\mathbb{F}_{q^3}$-extension contains the 3 conjugate points corresponding to D_∞.

Proof. Suppose that $\mathcal{L}$ is a tangent scattered $\mathbb{F}_q$-linear set of rank 3 and define $\mathcal{A}$ to be the ABB-representation of $\mathcal{L}\setminus\{P_\infty\}$. Observe the following properties.

(1) By Result 7.2.2(1), any affine line in Π corresponds to a tangent $\mathbb{F}_q$-subline of ℓ and therefore, due to Result 0.1.17, either contains 0, 1, 2 or q points of $\mathcal{A}$.

(2) Consider an arbitrary point $A\in\mathcal{A}$. By Result 0.1.18(1), through $\varphi^{-1}(A)$ and P_∞, there exist precisely two (tangent) $\mathbb{F}_q$-sublines contained in $\mathcal{L}$. Due to Result 7.2.2(1), this implies that there are exactly two affine q-secants to $\mathcal{A}$ through P in Π.

(3) $|\mathcal{A}|=|\mathcal{L}\setminus\{P_\infty\}|=q\left(q+1\right)$.

Therefore, the affine point set $\mathcal{A}$ meets all conditions of Corollary 0.1.9, stating that $\mathcal{A}$ is the affine part of a hyperbolic quadric $\mathcal{Q}$ of rank 2 that meets D_∞ in a non-singular conic.

Due to Result 0.1.18(1), through any two points of $\mathcal{L} \setminus \{P_\infty\}$, there exist two $\mathbb{F}_q$-sublines contained in $\mathcal{L}$. By Result 0.1.2, at least one of these $\mathbb{F}_q$-sublines, say $\mathfrak{L}$, does not contain P_∞. Due to Result 7.2.2, $\mathfrak{L}$ corresponds to a normal rational curve $\mathcal{C}$ in Π for which there exists a twisted cubic $\mathcal{C}^*$ in $\langle \Pi \rangle_{q^3}$ that contains the 3 conjugate points determining the spread element D_∞. Since $\mathfrak{L} \subset \mathcal{L}$, $\mathcal{C}^*$ is contained in $\langle \mathcal{Q} \rangle_{q^3}$ and hence, $\langle \mathcal{Q} \cap D_\infty \rangle_{q^3}$ contains the 3 conjugate points defining D_∞.
To prove the converse, it suffices to note that the number of such hyperbolic quadrics (Proposition 7.2.6) equals the number of scattered $\mathbb{F}_q$-linear sets containing P_∞ (Proposition 0.1.23). ∎

7.3 Constructing the seven planes

We can now use the results of the previous section to explicitly construct a set of seven planes in PG$(5,q)$ in higgledy-piggledy arrangement. For this, we need to constrict ourselves to the case $t = 3$.

Lemma 7.3.1

Let $\omega \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ and $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{F}_q$ such that $\omega^3 + \lambda_1\omega^2 + \lambda_2\omega + \lambda_3 = 0$. If $\mathcal{C}$ is a conic of PG$(2,q)$ *whose points have coordinates satisfying*

$$aX_0^2 + bX_0X_1 + cX_0X_2 + dX_1^2 + eX_1X_2 + fX_2^2 = 0$$

for certain $a,b,c,d,e,f,g \in \mathbb{F}_q$, not all zero, such that an $\mathbb{F}_{q^3}$-extension contains the points with coordinates $(1,\omega,\omega^2)^\mathsf{T}$, $(1,\omega^q,\omega^{2q})^\mathsf{T}$, $\left(1,\omega^{q^2},\omega^{2q^2}\right)^\mathsf{T}$, then $\mathcal{C}$ is given by

$$\begin{aligned} g_{d,e,f}(X_0,X_1,X_2) \coloneqq\ & (\lambda_3 e - \lambda_1\lambda_3 f)\, X_0^2 \\ & + (\lambda_2 e + (\lambda_3 - \lambda_1\lambda_2)\, f)\, X_0X_1 \\ & + \left(\lambda_1 e + \left(\lambda_2 - \lambda_1^2\right) f - d\right) X_0X_2 \\ & + dX_1^2 + eX_1X_2 + fX_2^2 = 0, \end{aligned} \tag{7.6}$$

for some $d,e,f \in \mathbb{F}_q$, not all zero.

Proof. Note that if the point P with coordinates $\left(1, \omega, \omega^2\right)^\intercal$ lies in an $\mathbb{F}_{q^3}$-extension of $\mathcal{C}$, then so do the points corresponding to $\left(1, \omega^q, \omega^{2q}\right)^\intercal$ and $\left(1, \omega^{q^2}, \omega^{2q^2}\right)^\intercal$. Expressing that P lies in this $\mathbb{F}_{q^3}$-extension, using that $\omega^4 = \left(\lambda_1^2 - \lambda_2\right)\omega^2 + \left(\lambda_1\lambda_2 - \lambda_3\right)\omega + \lambda_1\lambda_3$ and that $\left\{1, \omega, \omega^2\right\}$ is an $\mathbb{F}_q$-independent set, we find the following system of equations:

$$\begin{cases} a - \lambda_3 e + \lambda_1\lambda_3 f & = 0 \\ b - \lambda_2 e + \left(\lambda_1\lambda_2 - \lambda_3\right) f & = 0 \\ c + d - \lambda_1 e + \left(\lambda_1^2 - \lambda_2\right) f & = 0. \end{cases}$$

■

Proposition 7.3.2

Suppose that $q \geqslant 5$ and let $P_1, P_2, \ldots, P_6$ be six non-coplanar points of $\mathrm{AG}(3, q)$ contained in an elliptic quadric that intersects the plane $D_\infty : X_3 = 0$ at infinity in the non-singular conic $X_0X_2 - X_1^2 = 0$. Denote the coordinates of P_i by $\left(x_0^{(i)}, x_1^{(i)}, x_2^{(i)}, 1\right)$, $i \in \{1, 2, \ldots, 6\}$, and consider the quadratic surfaces whose points have coordinates satisfying

$$\begin{aligned} &\mathcal{Q}(d, e, f, s, t, u, v, X_0, X_1, X_2, X_3) \\ &\qquad := g_{d,e,f}(X_0, X_1, X_2) + X_3\left(sX_0 + tX_1 + uX_2 + vX_3\right) = 0. \quad (7.7) \end{aligned}$$

Let A be the (6×7)-matrix whose ith row $(A)_i$ satisfies

$$(A)_i \cdot (d, e, f, s, t, u, v)^\intercal = \mathcal{Q}\left(d, e, f, s, t, u, v, x_0^{(i)}, x_1^{(i)}, x_2^{(i)}, 1\right).$$

If $rk(A) = 6$, then the point set $\{P_1, \ldots, P_6\}$ is the ABB-representation of a set of six points of $\mathrm{PG}\left(1, q^3\right)$ not contained in an $\mathbb{F}_q$-linear set of rank 3 through P_∞.

Proof. We coordinatise Π in such a way that the three conjugate points defining D_∞ have coordinates $\left(1, \omega, \omega^2, 0\right)^\intercal$, $\left(1, \omega^q, \omega^{2q}, 0\right)^\intercal$, $\left(1, \omega^{q^2}, \omega^{2q^2}, 0\right)^\intercal$.

Given Proposition 7.2.3 and Theorems 7.2.5 and 7.2.7, we need to find six affine points of Π such that these are not contained in a plane, nor a cone with vertex not in π and base a non-singular conic of which an $\mathbb{F}_{q^3}$-extension contains the 3 conjugate points, nor a hyperbolic quadric through such a conic. All quadratic surfaces meeting D_∞ in a conic as described in (7.6) are given by an equation of the form

$$g_{d,e,f}(X_0, X_1, X_2) + X_3(sX_0 + tX_1 + uX_2 + vX_3) = 0. \tag{7.8}$$

Hence, if we choose six points contained in an elliptic quadric $\mathcal{E}$ meeting D_∞ in the non-singular conic $X_0X_2 - X_1^2 = 0, X_3 = 0$, we simply need to show that $\mathcal{E}$ is the only quadratic surface corresponding to an equation of the form (7.8) through those six points. This happens if and only if the homogeneous system of six equations in the variables d, e, f, s, t, u, v that arises from substituting the coordinates of the six points has a unique solution up to scalar multiple, which happens if and only if its coefficient matrix A has full rank. ∎

Theorem 7.3.3

Suppose that $q \equiv 1 \pmod 6$ *and let* μ *be a non-square of* $\mathbb{F}_q \setminus \{2^{-1}\}$. *Then the six points of* Π *with coordinates*

$$(1,0,-\mu,1)^\mathsf{T}, (1,0,-\mu,-1)^\mathsf{T}, (1,1,1-\mu,1)^\mathsf{T},$$
$$(1,-1,1-\mu,1)^\mathsf{T}, (1,1,1-\mu,-1)^\mathsf{T}, (1,-1,1-\mu,-1)^\mathsf{T}$$

give rise to a higgledy-piggledy set of seven planes in PG$(5,q)$.

Proof. Since $q \equiv 1 \pmod 3$, there exist elements $\omega \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ and $\lambda \in \mathbb{F}_q$ such that $\omega^3 + \lambda = 0$. Using Lemma 7.3.1, the quadrics of the form (7.7) become

$$\lambda e X_0^2 + \lambda f X_0X_1 - dX_0X_2 + dX_1^2 + eX_1X_2 + fX_2^2 + X_3(sX_0 + tX_1 + uX_2 + vX_3) = 0. \tag{7.9}$$

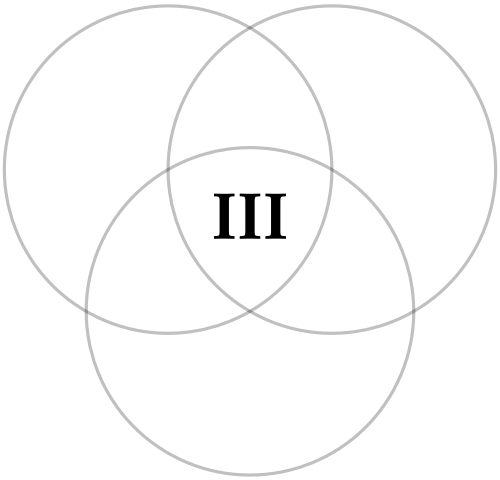
One can check that the given six points are not coplanar. Furthermore, they are contained in the elliptic quadric with equation $X_0X_2 - X_1^2 + \mu X_3^2 = 0$, which meets D_∞ in the non-singular conic $X_0X_2 - X_1^2 = 0, X_3 = 0$. Substituting the coordinates of the six points into (7.9) yields a system of six homogeneous equations in d, e, f, s, t, u, v whose associated coefficient matrix is given by

$$\begin{bmatrix} \mu & \lambda & \mu^2 & 1 & 0 & -\mu & 1 \\ \mu & \lambda & \mu^2 & -1 & 0 & \mu & 1 \\ \mu & 1-\mu+\lambda & (1-\mu)^2+\lambda & 1 & 1 & 1-\mu & 1 \\ \mu & \mu-1+\lambda & (1-\mu)^2-\lambda & 1 & -1 & 1-\mu & 1 \\ \mu & 1-\mu+\lambda & (1-\mu)^2+\lambda & -1 & -1 & \mu-1 & 1 \\ \mu & \mu-1+\lambda & (1-\mu)^2-\lambda & -1 & 1 & \mu-1 & 1 \end{bmatrix}.$$

This matrix has full rank if and only if $(1-\mu)(2\mu-1) \neq 0$. The statement follows from Proposition 7.3.2 and Theorem 5.4.6.

Remark 7.3.4

In the proof of Theorem 5.4.8, we chose eight points in $\mathrm{PG}(1, q^3)$ not contained in an $\mathbb{F}_q$-linear set of rank 3 without knowing their ABB-representation. If you interpret the point C as the point at infinity, then one can now realise that the ABB-representation of the other points in $\mathcal{P}$ are six points of $\mathrm{AG}(3, q)$ lying in the union of three (non-concurrent) affine lines ℓ_1, ℓ_2 and ℓ_3, each of which containing three of the six points.
Clearly, no cone with a non-singular conic as base and no hyperbolic quadric can contain the points of $\mathcal{P} \setminus \{C\}$. The only $\mathbb{F}_q$-linear set containing these points is the club $\mathcal{L}$ with head C for which the ABB-representation of $\mathcal{L} \setminus \{C\}$ is equal to the point set of the affine plane $\langle \ell_1, \ell_2, \ell_3 \rangle$.



III

Saturating sets

8 A tale of mixed lines and covering codes

Flowers for the ones you love
Flowers, flowers
Flowers for the ones you lost
Flowers, flowers

— Deluxe, *Flowers*[1]

Part III adopts the philosophy of its predecessor: the discovery of a particular family of geometrical structures directly leads to finding linear codes with valuable properties. While Part II was devoted to the link between higgledy-piggledy sets and minimal codes, Part III submits itself to constructing small *saturating sets* to obtain short covering codes.

ASSUMPTION

Throughout *Part III*, we assume that $\varrho \in \{0, 1, \ldots, d\}$.

All results found in Part III are based on [61, 63].

8.1 Saturating sets and covering codes

The following combinatorial structures are compelling from a coding theoretical point of view, since they have a one-to-one correspondence to linear covering codes with covering radius $\varrho + 1$.

[1] It is obligatory to put this song on repeat while cruising through Part III.

Definition 8.1.1 (saturating set)

Consider a point set $\mathcal{S}$ of $\mathrm{PG}(d,q)$.

(1) A point P of $\mathrm{PG}(d,q)$ is said to be **ϱ-saturated** by $\mathcal{S}$ (or, conversely, the set $\mathcal{S}$ **ϱ-saturates** P) if there exists a subspace through P of dimension at most ϱ that is spanned by points of $\mathcal{S}$.

(2) The set $\mathcal{S}$ is a **ϱ-saturating set** of $\mathrm{PG}(d,q)$ if ϱ is the smallest integer such that all points of $\mathrm{PG}(d,q)$ are ϱ-saturated by $\mathcal{S}$.

If ϱ is clear from context, the prefix '$\varrho-$' is often omitted.

Let $r, R \in \mathbb{N} \setminus \{0\}$, $R \leqslant r$, and consider a point set $\mathcal{S}$ of $\mathrm{PG}(r-1,q)$ of size n. Given a coordinate system for $\mathrm{PG}(r-1,q)$, denote by $h_1, h_2, \ldots, h_n$ the coordinate vectors of the points in $\mathcal{S}$. We claim that $\mathcal{S}$ is an $(R-1)$-saturating set of $\mathrm{PG}(r-1,q)$ if and only if $H := (h_1, h_2, \ldots, h_n)$ is a parity check matrix of an $[n, n-r]_q R$-code $\mathcal{C}$.
Consider an arbitrary vector $v \in V(n,q)$. If $Hv \neq \mathbf{0}$, then Hv are the coordinates of a certain point P of $\mathrm{PG}(r-1,q)$. Due to the way H is defined, the point P is $(R-1)$-saturated by $\mathcal{S}$ if and only if Hv is equal to an $\mathbb{F}_q$-linear combination of at most R columns of H. This is equivalent to the existence of a vector $w \in V(n,q)$ of weight at most R such that $Hv = Hw \iff H(v-w) = \mathbf{0}$. If $Hv = \mathbf{0}$, the latter statement still holds, as we can choose $w := \mathbf{0}$.
Therefore, $\mathcal{S}$ is an $(R-1)$-saturating set of $\mathrm{PG}(r-1,q)$ if and only if the Hamming distance between v and $v - w \in \mathcal{C}$ is at most $\mathrm{wt}(w) \leqslant R$. Note that if $\mathcal{S}$ is a saturating set of $\mathrm{PG}(r-1,q)$, then the rank of H must equal r, hence all vectors of $V(r,q)$ are reached by left-multiplying vectors of $V(n,q)$ with H.

We conclude that there exists a one-to-one correspondence between saturating sets and linear covering codes. To summarise, any ϱ-saturating set $\mathcal{S}$ of $\mathrm{PG}(d,q)$ corresponds to an $[n, n-r]_q R$-code and vice versa, where

$$n = |\mathcal{S}|, \quad r = d+1 \quad \text{and} \quad R = \varrho + 1.$$

Due to this correspondence, the quest of finding short $[n, n-r]_q R$-codes can be translated to searching for small ϱ-saturating sets in $\mathrm{PG}(d,q)$. In line with the literature (see e.g. [20, 21, 48, 49]), we define

$$s_q(d,\varrho) := \min\{|\mathcal{S}| \,:\, \mathcal{S} \text{ is a } \varrho\text{-saturating set of } \mathrm{PG}(d,q)\}\,,$$

as well as the **length function** (see e.g. [34, 42])

$$\ell_q(r,R) := \min\big\{n \in \mathbb{N} \,:\, \text{there exists an } [n, n-r]_q R \text{ code}\big\}\,.$$

Note that $\ell_q(r,R) = s_q(r-1, R-1)$.

Contrary to the relatively new concept of higgledy-piggledy sets, plenty of extensive research has already been done concerning the topic of saturating sets and covering codes. The existing literature covers decades of work and forms a symbolic jungle for an inexperienced young researcher.

8.2 Approaches of the literature

Based on the way to approach this topic of research, the literature is divided. On the one hand, one can observe the topic geometrically by analysing small ϱ-saturating sets of $\mathrm{PG}(d,q)$. On the other hand, one can convert this geometrical point of view to a coding theoretical one by investigating covering codes of small length.

Contrary to the work on which this chapter is based [61], we mainly restrict ourselves to a geometric viewpoint.

8.2.1 A lower bound defines the quest

In order to know which saturating sets are viewed as being 'small', we will be guided by the following lower bound on the size of arbitrary ϱ-saturating sets. Several variants of this bound were already known in the literature [20–22, 46, 48, 49], but some only state the bound for specific values of ϱ, while others describe an approximate lower bound for large values of q.

Proposition 8.2.1

Consider a ϱ-saturating set $\mathcal{S}$ of $\mathrm{PG}(d,q)$*. Then*

$$|\mathcal{S}| > \frac{\varrho+1}{e}\cdot q^{\frac{d-\varrho}{\varrho+1}} + \frac{\varrho}{2},$$

where e equals Euler's number.

Proof. If $|\mathcal{S}| \leqslant \varrho$, then the points of $\mathcal{S}$ would be contained in a subspace of dimension at most $\varrho - 1 < d$, making it impossible for $\mathcal{S}$ to saturate all points of $\mathrm{PG}(d,q)$, a contradiction. Therefore, we can consider the set $\Pi_{\leqslant\varrho}$ of all subspaces spanned by $\varrho+1$ distinct points of $\mathcal{S}$. As $\mathcal{S}$ saturates $\mathrm{PG}(d,q)$, we know that $\Pi_{\leqslant\varrho}$ has to cover all points, thus

$$\binom{|\mathcal{S}|}{\varrho+1}\theta_\varrho \geqslant \theta_d.$$

Expanding the binomial above and rearranging the inequality, we get

$$\prod_{i=0}^{\varrho}(|\mathcal{S}|-i) \geqslant (\varrho+1)!\cdot\frac{\theta_d}{\theta_\varrho} \geqslant (\varrho+1)!\cdot q^{d-\varrho}. \tag{8.1}$$

Note that the map $f : \mathbb{N}\setminus\{0\} \to \mathbb{R} : n \mapsto \frac{\sqrt[n]{n!}}{n}$ is strictly decreasing with $\lim_{n\to\infty} f(n) = \frac{1}{e}$, hence $f(n) > \frac{1}{e}$ for all $n \in \mathbb{N}\setminus\{0\}$, or, equivalently, $\sqrt[n]{n!} > \frac{n}{e}$. Combining this with (8.1) after taking the $(\varrho+1)$th root of the left- and right-hand side, we obtain

$$\sqrt[\varrho+1]{\prod_{i=0}^{\varrho}(|\mathcal{S}|-i)} > \frac{\varrho+1}{e}\cdot q^{\frac{d-\varrho}{\varrho+1}}.$$

Applying the AM-GM inequality to the left-hand side finishes the proof. ∎

Roughly speaking, Proposition 8.2.1 implies that

$$s_q(d,\varrho) \geqslant c\cdot \varrho\, q^{\frac{d-\varrho}{\varrho+1}}, \qquad \text{or, equivalently,} \qquad \ell_q(r,R) \geqslant c\cdot R\, q^{\frac{r-R}{R}}, \quad (8.2)$$

where $c > \frac{1}{3}$ is a constant independent of these parameters. Naturally, researchers aim to prove that (8.2) is sharp by constructing small ϱ-saturating sets of $\mathrm{PG}(d,q)$ or, equivalently, constructing $[n, n-r]_q R$ covering codes of small length.

Open Problem 8.2.2

Find a value $c_{d,\varrho} > 0$, preferably independent of d and ϱ, such that

$$s_q(d,\varrho) \leqslant c_{d,\varrho}\cdot \varrho\, q^{\frac{d-\varrho}{\varrho+1}},$$

or, equivalently, find a value $c_{r,R} > 0$, preferably independent of r and R, such that

$$\ell_q(r,R) \leqslant c_{r,R}\cdot R\, q^{\frac{r-R}{R}}.$$

With the exception of Remark 8.2.3, all mentioned results within this section solve the above open problem for specific values of d, ϱ and q (equivalently, r, R and q), some in a more effective way than others. *Most* results in the literature present solutions to Open Problem 8.2.2 if

(1) $d+1 \equiv 0 \pmod{\varrho+1}$ (see section 8.2.2), or

(2) $q = (q')^{\varrho+1}$ (see section 8.2.3).

Remark 8.2.3

Some results present upper bounds that are slightly larger than the desired one described in Open Problem 8.2.2. More specifically, the authors of articles [20–22, 47, 48, 50], some with the aid of computer searches, present upper bounds on $s_q(d,\varrho)$, $\varrho \in \{1,2\}$, of the form $s_q(d,\varrho) \leqslant c\cdot q^{\frac{d-\varrho}{\varrho+1}}\sqrt[\varrho+1]{\ln q}$, with $c > 0$ a small constant.

Chapter 10 presents an addition to the case $q = (q')^{\varrho+1}$, see Theorem 10.3.3 and Corollary 10.3.4. These results solve Open Problem 8.2.2 for $c_{d,\varrho}$ independent of d and linearly dependent on ϱ (equivalently, $c_{r,R}$ independent of r and linearly dependent on R).

8.2.2 The case $\varrho + 1 \mid d + 1$

A simple, recursive upper bound on $s_q(d, \varrho)$ can be obtained geometrically by observing saturating sets contained in two disjoint subspaces spanning the whole space. As stated in [51, Theorem 5], the same bound arises from the direct sum construction of linear codes over a common finite field.

Result 8.2.4 ([108, Lemma **10**])

$$s_q(d_1 + d_2 + 1, \varrho_1 + \varrho_2 + 1) \leqslant s_q(d_1, \varrho_1) + s_q(d_2, \varrho_2).$$

Corollary 8.2.5

For any $m \in \mathbb{N}$, $s_q((m+1)(\varrho+1) - 1, \varrho) \leqslant (\varrho+1)\theta_m$.

Proof. We proceed by induction on ϱ. If $\varrho = 0$, this is a trivial statement. Inductively using Result 8.2.4, we obtain

$$\begin{aligned} s_q((m+1)(\varrho+1) - 1, \varrho) &\leqslant s_q((m+1)\varrho - 1, \varrho - 1) + s_q(m, 0) \\ &\leqslant \varrho\theta_m + \theta_m. \end{aligned}$$

∎

Although, for $d + 1$ a multiple of $\varrho + 1$, Corollary 8.2.5 already solves Open Problem 8.2.2 (for $c_{d,\varrho}$ independent of d and ϱ), we want to stress that better upper bounds concerning this special case are known in the literature. Davydov [44, Theorem 5.1] and Davydov and Östergård [51, Theorem 7] slightly improved the bound above in case $m = 1$ and $\varrho = 1, 2$, respectively. The constructions behind these results are commonly denoted as the 'oval plus line' and 'two ovals plus line' constructions. In [46, Theorems 6.1 and 6.2], these bounds are generalised. Davydov, Marcugini and Pambianco

[49, Theorem 1] managed to generalise this 'oval(s) plus line' construction to a ϱ-saturating set of $\mathrm{PG}(2\varrho+1,q)$. Using a coding theoretical tool called 'q^m-concatenating constructions' [44–46, 49], they generalised their results even further and improved the upper bound depicted in Corollary 8.2.5 under some minor restrictions on the parameters.

8.2.3 The case $q=(q')^{\varrho+1}$

In this subsection, we discuss some relevant known results based on the assumption that $q=(q')^{\varrho+1}$ (equivalently, $q=(q')^R$). This assumption allows mathematicians to exploit the existence of $\mathbb{F}_{q'}$-subgeometries. In the literature, one can notice two main approaches for constructing saturating sets using subgeometries. We call these two approaches the *strong blocking set approach* and the *mixed subgeometry approach*.

The strong blocking set approach

The **strong blocking set approach** shifts the focus from finding saturating sets to constructing strong $(d-\varrho)$-blocking sets in $\mathrm{PG}(d,q')$. If one embeds the latter projective geometry as an $\mathbb{F}_{q'}$-subgeometry of $\mathrm{PG}(d,q)$, then such a strong $(d-\varrho)$-blocking set is a ϱ-saturating set.

Result 8.2.6 ([46, Theorem **3.2**])

Let $q=(q')^{\varrho+1}$ and consider a d-dimensional $\mathbb{F}_{q'}$-subgeometry $\mathcal{B}$ of $\mathrm{PG}(d,q)$. Then any strong $(d-\varrho)$-blocking set of $\mathcal{B}\cong\mathrm{PG}(d,q')$ is a ϱ-saturating set of $\mathrm{PG}(d,q)$.

Several results solving Open Problem 8.2.2 were found using this approach and were often generalised using q^m-concatenating constructions.

Result 8.2.7 ([46, Corollary **3.9**, Theorem **5.1**])

Let $t\in\mathbb{N}\setminus\{0\}$ and $r=3t+1$. Suppose that $q=(q')^3$, with $q'\geqslant 4$ if $t\geqslant 2$.

Then

$$\ell_q(r,3) \leqslant 4\left(q'\right)^{r-3} + 4\left(q'\right)^{r-4}.$$

Result 8.2.8 ([46, Theorems **3.16** and **5.2**])

Let $t \in \mathbb{N} \setminus \{0\}$ and $r = 3t+2$. Suppose that $q = (q')^3$, with $q' \geqslant 3$ if $t \geqslant 2$. Then

$$\ell_q(r,3) \leqslant 9\left(q'\right)^{r-3} - 8\left(q'\right)^{r-4} + 4\left(q'\right)^{r-5}.$$

Note that Result 8.2.7 arises from the existence of four lines of $\mathrm{PG}(3,q')$ in higgledy-piggledy arrangement (Result 5.2.7(1)), while Result 8.2.8 is based on the existence of a higgledy-piggledy set of nine planes in $\mathrm{PG}(4,q')$ [46, Theorem 3.16]. The main result of Chapter 10 (Corollary 10.3.4) implies that

$$\ell_q(r,3) \leqslant 6\frac{(q')^{r-2}-1}{q'-1}, \tag{8.3}$$

which clearly does not improve Result 8.2.7 but does improve Result 8.2.8 significantly. However, Chapter 6 offers new results on higgledy-piggledy plane sets of $\mathrm{PG}(4,q')$, which in turn improves (8.3).

Theorem 8.2.9

Let $t \in \mathbb{N} \setminus \{0\}$ and $r = 3t+2$. Suppose that $q = (q')^3$, with $q' \geqslant 3$ if $t \geqslant 2$. Then

$$\ell_q(r,3) \leqslant 6\left(q'\right)^{r-3} + 5\left(q'\right)^{r-4} - 9\left(q'\right)^{r-5}.$$

Proof. This is analogous to the proof of [46, Theorem 5.2], taking Corollary 6.2.6 as a base case. ∎

More generally, the authors of [46] presented the following.

Result 8.2.10 ([46, Theorem **3.15**])

Let $\varrho \leqslant d-2$ and suppose that $q = (q')^{\varrho+1}$. Then

$$s_q(d,\varrho) \leqslant \frac{\sum_{i=0}^{d-\varrho+1} (q'-1)^i \binom{d+1}{i} - 1}{q'-1} \sim \binom{d+1}{\varrho} (q')^{d-\varrho}.$$

At first sight, the main result of Chapter 10 (Theorem 10.3.3) is a significant improvement on the bound presented in Result 8.2.10, as the binomial coefficient $\binom{d+1}{\varrho}$ is reduced to $\frac{(\varrho+1)(\varrho+2)}{2}$. However, a certain degree of nuance is needed, as the authors presented several more technical results in case $q = (q')^{\varrho+1}$, proving that

$$s_q(d,\varrho) \lesssim \binom{\varrho+1+\gamma}{\varrho} (q')^{d-\varrho},$$

if q is large enough, where $0 \neq \gamma \equiv d+1 \pmod{\varrho+1}$ (see [46, Theorems 6.3 and 6.4, and Corollary 7.2]).

Furthermore, Results 5.2.6 and 8.2.6 imply the following.

Result 8.2.11 ([69, Theorem **24**] and [68, Proposition **10**])

Suppose that $q = (q')^{\varrho+1}$, $q' > (d-\varrho+1)\varrho$. Then

$$s_q(d,\varrho) \leqslant ((d-\varrho+1)\varrho+1) \frac{(q')^{d-\varrho+1}-1}{q'-1}.$$

If $q' > (d-\varrho+1)\varrho$, one can check that the main result of Chapter 10 (Theorem 10.3.3) improves Result 8.2.11 if and only if $\varrho < \frac{2d-1}{3}$.

Theorem 8.2.12

$s_{(q')^4}(4,3) \leqslant 6q'+5.$

Proof. Directly from Theorem 6.2.5 and Result 8.2.6 ∎

The mixed subgeometry approach

The **mixed subgeometry approach** is based on constructing saturating sets as a union of the point sets of several distinct subgeometries which are not part of a common, larger subgeometry. This approach is the main source of inspiration for Chapter 10 and is used much less than the *strong blocking set approach*. In fact, Result 8.2.13 below is the only instance using the *mixed subgeometry approach* that we encountered in the literature.

Result 8.2.13 ([44, Theorem **5.2**])

Suppose that $q = (q')^2$. *Let* b_1, b_2 *and* b_3 *be three distinct* $\mathbb{F}_{q'}$*-sublines spanning* $\mathrm{PG}(2,q)$ *and sharing a common point* P, *with the addition that* b_1 *and* b_2 *share a point* $Q \neq P$ *as well. Then* $(b_1 \cup b_2 \cup b_3) \setminus \{P\}$ *is a* 1*-saturating set of* $\mathrm{PG}(2,q)$. *As a consequence,*

$$s_q(2,1) \leqslant 3q' - 1.$$

Better bounds on $s_q(2,1)$, q square, are known (see [49, Proposition 9] for an overview). Interestingly, as noted in [49, Remarks 3 and 4], if q equals the square of a prime number, no better bound on $s_q(2,1)$ than the one depicted in Result 8.2.13 is known. In essence, Configuration 10.2.2 is a highly generalised version of the (sub)geometric construction described in Result 8.2.13.

By making use of variations of q^m-concatenating constructions, the following bound is obtained, generalising the bound of Result 8.2.13.

Result 8.2.14 ([45, Example **6**, Equation **33**])

Let d *be even and* $q \geqslant 16$ *be square. Then*

$$s_q(d,1) \leqslant (3\sqrt{q} - 1)\, q^{\frac{d}{2}-1} + \left\lfloor q^{\frac{d}{2}-2} \right\rfloor.$$

9 Parallel subgeometries

In Section 7.1 of Chapter 7, we established an isomorphism between a certain set of normal rational curves and the line set of a projective geometry. Such a link allowed us to define *subspaces* of normal rational curves.

In this chapter, we put the topic of saturating sets temporarily on hold and aim to do a similar trick by associating certain subgeometries to affine lines. This, in turn, permits us to replicate the notions of *parallelism* and *affine subspaces* to these subgeometries, which is crucial in the arguments used in Chapter 10.

ASSUMPTION

Throughout this *chapter*, we assume that $s, t \in \mathbb{N} \setminus \{0\}$.

All results are based on [61, 63].

9.1 Three peculiar point-line geometries

The key players in this chapter are three particular point-line geometries, each embedded in a certain projective geometry. Although these point-line geometries differ significantly, they will turn out to be isomorphic.

Definition 9.1.1 (point-line geometry X [57, Section 3])

Consider a $(t-1)$-dimensional subspace π of $\mathrm{PG}(s+t-1,q)$. The point-line geometry $X(s,t,q)$ is the incidence structure $(\mathcal{P}_X, \mathcal{L}_X)$ with natural incidence, where

- $\mathcal{P}_X$ is the set of all $(s-1)$-subspaces of $\mathrm{PG}(s+t-1,q)$ disjoint to π, and
- $\mathcal{L}_X$ is the set of all s-subspaces of $\mathrm{PG}(s+t-1,q)$ meeting π exactly in one point.

Definition 9.1.2 (point-line geometry Y)

Consider a hyperplane Σ_Y of $\mathrm{PG}(s,q^t)$ containing an $(s-1)$-dimensional $\mathbb{F}_q$-subgeometry $\mathcal{C}_Y$. The point-line geometry $Y(s,t,q)$ is the incidence structure $(\mathcal{P}_Y, \mathcal{L}_Y)$ with natural incidence, where

- $\mathcal{P}_Y$ is the set of all points of $\mathrm{PG}(s,q^t)$ not contained in Σ_Y, and
- $\mathcal{L}_Y$ is the set of all s-dimensional $\mathbb{F}_q$-subgeometries of $\mathrm{PG}(s,q^t)$ through $\mathcal{C}_Y$.

Definition 9.1.3 (point-line geometry Z)

Consider a hyperplane Σ_Z of $\mathrm{PG}(t,q^s)$ containing a $(t-1)$-dimensional $\mathbb{F}_q$-subgeometry $\mathcal{C}_Z$. The point-line geometry $Z(s,t,q)$ is the incidence structure $(\mathcal{P}_Z, \mathcal{L}_Z)$ with natural incidence, where

- $\mathcal{P}_Z$ is the set of all points of $\mathrm{PG}(t,q^s)$ not contained in Σ_Z, and
- $\mathcal{L}_Z$ is the set of all lines of $\mathrm{PG}(t,q^s)$ meeting both Σ_Z and $\mathcal{C}_Z$ exactly in one and the same point.

The point-line geometry $X(s,t,q)$ considers certain sets of subspaces minimally intersecting a fixed subspace and was first introduced in [57]. The point-line geometry $Y(s,t,q)$ considers subgeometries sharing a fixed subgeometry of one dimension smaller. This point-line geometry hasn't been considered in the literature before.[1]
Finally, the point-line geometry $Z(s,t,q)$ considers certain parallel classes of lines in an affine geometry. In fact, $Z(s,t,q)$ is a special case of what is commonly known as a **linear representation** of a point set $\mathcal{K}$ lying in Σ_Z. Despite the fact that Definition 9.1.3 specifies $\mathcal{K}$ as the point set of a $(t-1)$-dimensional $\mathbb{F}_q$-subgeometry, $\mathcal{K}$ can be any other choice.

The concept of a *linear representation* was independently introduced for hyperovals by Ahrens and Szekeres [5] and Hall [74], and extended to general point sets by De Clerck [55].
Linear representations are mainly investigated when $\mathcal{K}$ is a well-known object, such as a hyperoval (if $s=1$, $t=3$ and q is even, see [28, 73]), a Buekenhout-Metz unital (if $s=2$ and $t=3$, see [56]) or, like Definition 9.1.3, a subgeometry (see [55, 57, 58]). Results on general linear representations were proven as well, see e.g. [12, 38, 57].

Remark 9.1.4

Keeping Result 0.1.2 in mind, one can check that any line of the point-line geometries described in Definitions 9.1.1 to 9.1.3 is uniquely determined by the set of points it is incident with.

Proposition 9.1.5

(1) $|\mathcal{P}_X| = |\mathcal{P}_Y| = |\mathcal{P}_Z| = q^{st}$.

(2) $|\mathcal{L}_X| = |\mathcal{L}_Y| = |\mathcal{L}_Z| = q^{s(t-1)}\theta_{t-1}$.

[1] The case $s=1$ is an exception to this statement, as there exists a well-known isomorphism between the affine parts of $\mathbb{F}_q$-sublines of $\mathrm{PG}(1,q^t)$ through a fixed point and the lines of $\mathrm{AG}(t,q)$ (see e.g. Result 7.2.2(1)).

Proof. (1) Observe that $|\mathcal{P}_Y| = q^{st} = |\mathcal{P}_Z|$ as the sizes of these sets are equal to the number of points in $\mathrm{AG}(s,q^t)$ and $\mathrm{AG}(t,q^s)$, respectively. To prove that $|\mathcal{P}_X| = q^{st}$, one has to count the number of $(s-1)$-subspaces in $\mathrm{PG}(s+t-1,q)$ disjoint to a fixed $(t-1)$-subspace, see e.g. [100, section 170].

(2) By double counting the elements of the set

$$\{(P,L) : P \in \mathcal{P}_X, L \in \mathcal{L}_X, P \in L\},$$

one obtains that $q^{st}\theta_{t-1} = |\mathcal{P}_X|\,\theta_{t-1} = (\theta_s - \theta_{s-1})\,|\mathcal{L}_X|$, implying that $|\mathcal{L}_X| = q^{s(t-1)}\theta_{t-1}$.

By double counting the elements of the set

$$\left\{(\ell,\mathcal{B}) : \ell \text{ is a line of } \mathrm{PG}\left(s,q^t\right), \mathcal{B} \in \mathcal{L}_Y, |\ell \cap (\mathcal{B} \setminus \mathcal{C}_Y)| = q\right\},$$

one obtains that

$$\theta_{s-1}\left(\theta_{s-1,q^t} - \theta_{s-2,q^t}\right)\frac{q^t\left(q^t-1\right)}{q\left(q-1\right)} = \theta_{s-1}\left(\theta_{s-1} - \theta_{s-2}\right)|\mathcal{L}_Y|,$$

where we made use of Lemma 0.1.3 to obtain the factor $\frac{q^t\left(q^t-1\right)}{q(q-1)}$. This implies that $|\mathcal{L}_Y| = q^{s(t-1)}\theta_{t-1}$.

Finally, an easy observation yields $|\mathcal{L}_Z| = \theta_{t-1}\left(\theta_{t-1,q^s} - \theta_{t-2,q^s}\right) = q^{s(t-1)}\theta_{t-1}$. ∎

Result 9.1.6 ([57, Theorem **4.1**])

The point-line geometries $X(s,t,q)$ and $Z(s,t,q)$ are isomorphic.

We will prove that $Y(s,t,q)$ is a member of this isomorphism class by constructing explicit isomorphisms to both $X(s,t,q)$ and $Z(s,t,q)$.

Remark 9.1.7

One can prove that the isomorphism behind Result 9.1.6 transfers the notion of parallelism from $Z(s,t,q)$ to $X(s,t,q)$ in the following way: two elements of $\mathcal{L}_X$ are 'parallel' if and only if they share a point of π. This description does not, however, provide any 'hidden' equivalence relation on the elements of $\mathcal{L}_X$.
Towards the end of this chapter, we show that the presence of parallelism in $Z(s,t,q)$ does, in fact, uncover a beneficial relation on the lines of $Y(s,t,q)$.

9.2 The isomorphism between $Y(s,t,q)$ and $X(s,t,q)$

An explicit isomorphism between $Y(s,t,q)$ and $X(s,t,q)$ will be constructed using field reduction.

9.2.1 Generalised reguli

Lemma 9.2.1

Consider a regulus $\mathcal{R}$ of $\mathrm{PG}(2t-1,q)$ and let $R_1, R_2, \ldots, R_{t-1}$ be $t-1$ points in general position lying in an element of $\mathcal{R}$, with $\ell_1, \ell_2, \ldots, \ell_{t-1}$ their respective transversal lines. Then $\langle \ell_1, \ell_2, \ldots, \ell_{t-1} \rangle$ is a $(2t-3)$-subspace intersecting each element of $\mathcal{R}$ exactly in a $(t-2)$-subspace.

Proof. Let $\mathcal{R} = \{\sigma_0, \sigma_1, \ldots, \sigma_q\}$ and suppose, without loss of generality, that $R_1, R_2, \ldots, R_{t-1} \in \sigma_0$. If $t = 1$, there is nothing left to prove, so assume that $t \geqslant 2$. We will prove by induction on $i \in \{1, 2, \ldots, t-1\}$ that $\langle \ell_1, \ell_2, \ldots, \ell_i \rangle$ is a $(2i-1)$-subspace intersecting each element of $\mathcal{R}$ exactly in an $(i-1)$-subspace. If $i = 1$, then the proof is done as ℓ_1 is a transversal line. Hence, let $i \geqslant 2$ and assume that $\mathcal{T}' := \langle \ell_1, \ell_2, \ldots, \ell_{i-1} \rangle$ is a $(2i-3)$-subspace intersecting each element $\sigma_j \in \mathcal{R}$ exactly in a $(i-2)$-subspace σ'_j.

Suppose, to the contrary, that ℓ_i meets an element of $\{\sigma'_0, \sigma'_1, \ldots, \sigma'_q\}$. If ℓ_i intersects two distinct elements of this set, then $\ell_i \subseteq \mathcal{T}'$, implying that

$R_i \in \sigma'_0 = \langle R_1, R_2, \ldots, R_{i-1} \rangle$, a contradiction. Therefore, ℓ_i meets precisely one element of $\left\{\sigma'_0, \sigma'_1, \ldots, \sigma'_q\right\}$. Without loss of generality, assume that ℓ_i intersects σ'_1 and hence is disjoint to both σ'_0 and σ'_2. Then ℓ_i intersects $\mathcal{T}'$ in a point (of σ'_1), thus $\dim(\langle \mathcal{T}', \ell_i \rangle) \leqslant 2i-2$. However, the disjoint $(i-1)$-subspaces $\langle \sigma'_0, R_i \rangle$ and $\langle \sigma'_2, \ell_i \cap \sigma_2 \rangle$ are contained in $\langle \mathcal{T}', \ell_i \rangle$, implying that $\dim(\langle \mathcal{T}', \ell_i \rangle) \geqslant 2i-1$, a contradiction.
In conclusion, the transversal line ℓ_i does not intersect any element of the set $\left\{\sigma'_0, \sigma'_1, \ldots, \sigma'_q\right\}$, which forces $\mathcal{T} \coloneqq \langle \mathcal{T}', \ell_i \rangle$ to be a $(2i-1)$-subspace that intersects each subspace σ_j at least in an $(i-1)$-subspace, but also at most, as else we can find two disjoint subspaces in $\mathcal{T}$ that span a $(2i)$-subspace. ∎

Lemma 9.2.2

Consider an $(s-1)$-dimensional $\mathbb{F}_q$-subgeometry $\mathcal{C}$ of $\mathrm{PG}(s-1, q^t)$ and let $\mathcal{P}_\mathcal{C}$ be its point set. Then there exists an $(st-s-1)$-dimensional subspace of $\mathrm{PG}(st-1, q)$ intersecting each element of the set $\mathcal{F}_{s,t,q}(\mathcal{P}_\mathcal{C})$ exactly in a $(t-2)$-subspace.

Proof. Within this proof, we extend the notation $\mathcal{P}_\mathcal{A}$ as being the point set of any $\mathbb{F}_q$-subgeometry $\mathcal{A}$ and remove the subscript of $\mathcal{F}_{s,t,q}$.
We proceed by induction on s. If $s = 1$, the statement is trivially true. Hence, let $s \geqslant 2$ and consider an $(s-2)$-dimensional $\mathbb{F}_q$-subgeometry $\mathcal{C}' \subset \mathcal{C}$ for which there exists an $(st-s-t)$-dimensional subspace $\mathcal{T}_{\mathcal{C}'}$ of $\mathcal{F}\left(\langle \mathcal{C}' \rangle_{q^t}\right)$ intersecting each element of the set $\mathcal{F}(\mathcal{P}_{\mathcal{C}'})$ exactly in a $(t-2)$-subspace. Now

- define $\Pi_{\mathcal{C}'} \coloneqq \mathcal{F}\left(\langle \mathcal{C}' \rangle_{q^t}\right)$,
- let $Q \in \mathcal{C}'$ and define $\sigma_Q \coloneqq \mathcal{F}(Q)$ and $\sigma'_Q \coloneqq \mathcal{T}_{\mathcal{C}'} \cap \sigma_Q$,
- consider an $\mathbb{F}_q$-subline $\mathfrak{L}$ of $\mathcal{C}$ through Q not contained in $\mathcal{C}'$ and let $\Pi_\mathfrak{L} \coloneqq \mathcal{F}\left(\langle \mathfrak{L} \rangle_{q^t}\right)$, and

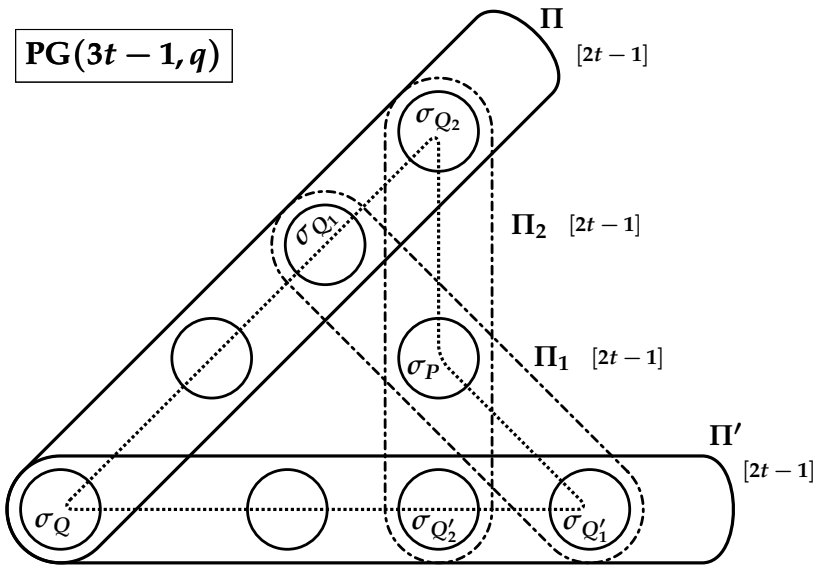


Figure 9.1: A visualisation of the proof of Lemma 9.2.2, or how $\langle \mathcal{T}_{\mathfrak{L}}, \mathcal{T}_{\mathfrak{L}'} \rangle$ should intersect σ_P in a $(t-2)$-subspace, $P \in \langle \mathfrak{L}, \mathfrak{L}' \rangle \setminus (\mathfrak{L} \cup \mathfrak{L}')$. All circles are $(t-1)$-subspaces.

- define $\mathcal{R}_{\mathfrak{L}} := \mathcal{F}(\mathcal{P}_{\mathfrak{L}})$.

By Result 0.1.13, $\mathcal{R}_{\mathfrak{L}}$ is a regulus contained in the $(2t-1)$-subspace $\Pi_{\mathfrak{L}}$. Hence, by Lemma 9.2.1, we can consider a $(2t-3)$-dimensional subspace $\mathcal{T}_{\mathfrak{L}}$ in $\Pi_{\mathfrak{L}}$ through σ'_Q intersecting each element of $\mathcal{R}_{\mathfrak{L}}$ exactly in a $(t-2)$-subspace. Moreover, as the $(2t-1)$-subspace $\Pi_{\mathfrak{L}}$ intersects the $(st-t-1)$-subspace $\Pi_{\mathcal{C}'}$ precisely in the $(t-1)$-subspace σ_Q, we know that $\mathcal{T}_{\mathfrak{L}}$ intersects $\mathcal{T}_{\mathcal{C}'}$ exactly in the $(t-2)$-subspace σ'_Q, hence

$$\mathcal{T} := \langle \mathcal{T}_{\mathfrak{L}}, \mathcal{T}_{\mathcal{C}'} \rangle$$

has dimension $(2t-3)+(st-s-t)-(t-2) = st-s-1$. We will prove that $\mathcal{T}$ is the $(st-s-1)$-subspace of $\mathrm{PG}(st-1,q)$ we are looking for.

Choose an arbitrary point $P \in \mathcal{C}$ and define $\sigma_P := \mathcal{F}(P)$. The only thing left to prove is that $\mathcal{T}$ intersects σ_P exactly in a $(t-2)$-subspace. Note that $\mathcal{T}$ intersects $\Pi_{\mathfrak{L}}$ and $\Pi_{\mathcal{C}'}$ at least in $\mathcal{T}_{\mathfrak{L}}$ and $\mathcal{T}_{\mathcal{C}'}$, respectively, but also *at most*, as else we can use Grassmann's identity to prove that $\dim(\mathcal{T}) > st-s-1$, a contradiction. If $P \in \mathfrak{L} \cup \mathcal{C}'$, then σ_P is contained in either $\Pi_{\mathfrak{L}}$ or $\Pi_{\mathcal{C}'}$, hence $\mathcal{T}$ will intersect σ_P exactly in a $(t-2)$-subspace.
Now suppose that $P \notin \mathfrak{L} \cup \mathcal{C}'$. Let $\mathfrak{P}$ be the $\mathbb{F}_q$-subplane of $\mathcal{C}$ spanned by $\mathfrak{L}$ and P. This subplane intersects $\mathcal{C}'$ in an $\mathbb{F}_q$-subline $\mathfrak{L}'$ through Q. Let $\Pi_{\mathfrak{L}'}$ be the image under $\mathcal{F}$ of $\langle \mathfrak{L}' \rangle_{q^t}$. Note that by the above arguments, $\mathcal{T}$ will intersect $\Pi_{\mathfrak{L}'}$ in a $(2t-3)$-subspace $\mathcal{T}_{\mathfrak{L}'}$ as well. Hence, we can shift our view to the $(3t-1)$-subspace $\langle \Pi_{\mathfrak{L}}, \Pi_{\mathfrak{L}'} \rangle \supset \sigma_P$ to continue this proof (see Figure 9.1).
Let $\mathfrak{L}_1$ and $\mathfrak{L}_2$ be two distinct $\mathbb{F}_q$-sublines in $\mathfrak{P}$ through P, not containing Q. Define

$$Q_1 := \mathfrak{L} \cap \mathfrak{L}_1, \quad Q_2 := \mathfrak{L} \cap \mathfrak{L}_2, \quad Q'_1 := \mathfrak{L}' \cap \mathfrak{L}_1, \quad Q'_2 := \mathfrak{L}' \cap \mathfrak{L}_2.$$

Correspondingly, define

$$\sigma_{Q_1} := \mathcal{F}(Q_1), \quad \sigma_{Q_2} := \mathcal{F}(Q_2), \quad \sigma_{Q'_1} := \mathcal{F}(Q'_1), \quad \sigma_{Q'_2} := \mathcal{F}(Q'_2),$$

and

$$\sigma'_{Q_1} := \mathcal{T} \cap \sigma_{Q_1}, \quad \sigma'_{Q_2} := \mathcal{T} \cap \sigma_{Q_2}, \quad \sigma'_{Q'_1} := \mathcal{T} \cap \sigma_{Q'_1}, \quad \sigma'_{Q'_2} := \mathcal{T} \cap \sigma_{Q'_2}.$$

As $Q_1, Q_2, Q'_1, Q'_2 \in \mathfrak{L} \cup \mathfrak{L}' \subseteq \mathfrak{L} \cup \mathcal{C}'$, we know that the above subspaces have dimension $t-2$. Finally, define

$$\Pi := \langle \sigma_{Q_1}, \sigma_{Q_2} \rangle = \Pi_{\mathfrak{L}}, \quad \Pi_1 := \left\langle \sigma_{Q_1}, \sigma_{Q'_1} \right\rangle,$$
$$\Pi' := \left\langle \sigma_{Q'_1}, \sigma_{Q'_2} \right\rangle = \Pi_{\mathfrak{L}'}, \quad \Pi_2 := \left\langle \sigma_{Q_2}, \sigma_{Q'_2} \right\rangle,$$

these all being $(2t-1)$-subspaces of $\mathrm{PG}(st-1,q)$. Note that σ_Q is contained in both Π and Π'.
Observe that, as $\Pi \cap \Pi' = \sigma_Q$ and as both $\mathcal{T}_{\mathfrak{L}} \subset \Pi$ and $\mathcal{T}_{\mathfrak{L}'} \subset \Pi'$ intersect σ_Q in the $(t-2)$-subspace σ'_Q, the intersection $\mathcal{T}_{\mathfrak{L}} \cap \mathcal{T}_{\mathfrak{L}'}$ has dimension $t-2$, hence $\dim(\langle \mathcal{T}_{\mathfrak{L}}, \mathcal{T}_{\mathfrak{L}'} \rangle) = 3t-4$.
We can prove that $\langle \mathcal{T}_{\mathfrak{L}}, \mathcal{T}_{\mathfrak{L}'} \rangle \cap \Pi_1 = \left\langle \sigma'_{Q_1}, \sigma'_{Q'_1} \right\rangle$. Indeed, we know that $\Pi_1 = \left\langle \sigma_{Q_1}, \sigma_{Q'_1} \right\rangle$; as $\mathcal{T}_{\mathfrak{L}}$ intersects σ_{Q_1} in σ'_{Q_1} and as $\mathcal{T}_{\mathfrak{L}'}$ intersects $\sigma_{Q'_1}$ in $\sigma'_{Q'_1}$, the subspace $\langle \mathcal{T}_{\mathfrak{L}}, \mathcal{T}_{\mathfrak{L}'} \rangle \cap \Pi_1$ contains $\left\langle \sigma'_{Q_1}, \sigma'_{Q'_1} \right\rangle$. If $\langle \mathcal{T}_{\mathfrak{L}}, \mathcal{T}_{\mathfrak{L}'} \rangle$ would contain a subspace of Π_1 of dimension larger than $\dim\left(\left\langle \sigma'_{Q_1}, \sigma'_{Q'_1} \right\rangle\right)$, then $\langle \mathcal{T}_{\mathfrak{L}}, \mathcal{T}_{\mathfrak{L}'} \rangle$ would contain both the $(t-2)$-subspace $\sigma'_Q \subset \sigma_Q$ and a $(2t-2)$-subspace of Π_1, which are disjoint to each other as σ_Q and Π_1 are disjoint. This would imply that $\dim(\langle \mathcal{T}_{\mathfrak{L}}, \mathcal{T}_{\mathfrak{L}'} \rangle) \geqslant (t-2) + 2t - 2 + 1 = 3t-3$, a contradiction.
As a consequence, $\mathcal{T}$ cannot contain σ_P, as else the $(2t-3)$-subspace $\langle \mathcal{T}_{\mathfrak{L}}, \mathcal{T}_{\mathfrak{L}'} \rangle \cap \Pi_1$ contains both the $(t-2)$-subspace σ'_{Q_1} and the $(t-1)$-subspace σ_P, which are disjoint to each other, a contradiction. Hence, $\mathcal{T}$ intersects σ_P at most in a $(t-2)$-subspace. It remains to prove that $\mathcal{T}$ intersects σ_P *at least* in a $(t-2)$-subspace.
As $\Pi \cap \Pi' = \sigma_Q$, we have that

$$\dim(\langle \Pi_1, \Pi_2 \rangle) = \dim\left(\left\langle \sigma_{Q_1}, \sigma_{Q'_1}, \sigma_{Q_2}, \sigma_{Q'_2} \right\rangle\right) = \dim\left(\langle \Pi, \Pi' \rangle\right) = 3t-1.$$

Hence, $\dim(\Pi_1 \cap \Pi_2) = (2t-1) + (2t-1) - (3t-1) = t-1$. As the $(t-1)$-subspace σ_P is contained in both Π_1 and Π_2, this means that $\Pi_1 \cap \Pi_2 = \sigma_P$ (see Figure 9.1).
Recall that $\mathcal{T}_{\mathfrak{L}} = \left\langle \sigma'_{Q_1}, \sigma'_{Q_2} \right\rangle$, $\mathcal{T}_{\mathfrak{L}'} = \left\langle \sigma'_{Q'_1}, \sigma'_{Q'_2} \right\rangle$ and that the span $\langle \mathcal{T}_{\mathfrak{L}}, \mathcal{T}_{\mathfrak{L}'} \rangle$ is a $(3t-4)$-dimensional subspace. Hence, we can make a similar reasoning as above and obtain that

$$\begin{aligned}\dim\left(\left\langle \sigma'_{Q_1}, \sigma'_{Q'_1} \right\rangle \cap \left\langle \sigma'_{Q_2}, \sigma'_{Q'_2} \right\rangle\right) &= 2(2t-3) - \dim\left(\left\langle \sigma'_{Q_1}, \sigma'_{Q'_1}, \sigma'_{Q_2}, \sigma'_{Q'_2} \right\rangle\right) \\ &= 2(2t-3) - \dim(\langle \mathcal{T}_{\mathfrak{L}}, \mathcal{T}_{\mathfrak{L}'} \rangle) \\ &= t-2.\end{aligned}$$

As $\left\langle \sigma'_{Q_1}, \sigma'_{Q'_1} \right\rangle \subset \Pi_1$ and $\left\langle \sigma'_{Q_2}, \sigma'_{Q'_2} \right\rangle \subset \Pi_2$, the $(t-2)$-subspace $\left\langle \sigma'_{Q_1}, \sigma'_{Q'_1} \right\rangle \cap \left\langle \sigma'_{Q_2}, \sigma'_{Q'_2} \right\rangle$ lies in $\Pi_1 \cap \Pi_2 = \sigma_P$. Hence, $\mathcal{T}$ intersects σ_P at least in this $(t-2)$-subspace, and the proof is done. ∎

9.2.2 The isomorphism

We now have all the tools we need to construct an isomorphism between $X(s,t,q)$ and $Y(s,t,q)$. We refer to Figure 9.2 for a visualisation of the map φ_X we are about to define.

Definition 9.2.3 (isomorphism φ_X)

Consider the point-line geometry $Y(s,t,q)$ together with all corresponding notation (see Definition 9.1.2). By Lemma 9.2.2 (and temporarily restricting the field reduction map to $\Sigma_Y \cong \mathrm{PG}(s-1,q^t)$), we can consider an $(st-s-1)$-dimensional subspace χ of the $(st-1)$-subspace $\mathcal{F}(\Sigma_Y)$ that intersects $\mathcal{F}(Q)$ exactly in a $(t-2)$-subspace, for every $Q \in \mathcal{C}_Y$ (see Figure 9.2).
Now consider a duality δ of $\mathrm{PG}(st+t-1,q)$ and define the map

$$\varphi_X : \mathrm{PG}(s,q^t) \to \mathrm{PG}(s+t-1,q) : \tau \mapsto \left(\mathcal{F}(\tau)^\delta \cap \chi^\delta\right),$$

where we identify $\chi^\delta \cong \mathrm{PG}(s+t-1,q)$ and where τ is a subspace of $\mathrm{PG}(s,q^t)$.

Theorem 9.2.4

Let $s,t \in \mathbb{N} \setminus \{0\}$. Then φ_X induces an isomorphism between $Y(s,t,q)$ and $X(s,t,q)$.

Proof. By the properties of a duality, $\chi \subset \mathcal{F}(\Sigma_Y)$ implies $\mathcal{F}(\Sigma_Y)^\delta \subset \chi^\delta$, hence $\varphi_X(\Sigma_Y) = \mathcal{F}(\Sigma_Y)^\delta$. In line with Definition 9.1.1, we

- identify χ^δ with $\mathrm{PG}(s+t-1,q)$, and
- define $\pi := \varphi_X(\Sigma_Y) = \mathcal{F}(\Sigma_Y)^\delta$.

Claim 1: φ_X is a bijection between $\mathcal{P}_Y$ and $\mathcal{P}_X$.

Let P be a point of $\mathcal{P}_Y$. As $P \notin \Sigma_Y$, $\mathcal{F}(P)$ is a $(t-1)$-subspace disjoint to the $(st-1)$-subspace $\mathcal{F}(\Sigma_Y)$. Hence, $\mathcal{F}(P)^\delta$ is an $(st-1)$-subspace of $\mathrm{PG}(st+t-1,q)$ disjoint to the $(t-1)$-subspace $\mathcal{F}(\Sigma_Y)^\delta = \varphi_X(\Sigma_Y) = \pi$. Therefore, χ^δ intersects $\mathcal{F}(P)^\delta$ in a subspace of dimension at least $s-1$, as both subspaces are contained in $\mathrm{PG}(st+t-1,q)$. Conversely, χ^δ intersects $\mathcal{F}(P)^\delta$ in a subspace of dimension at most $s-1$ as π and $\mathcal{F}(P)^\delta \cap \chi^\delta$ are disjoint subspaces that are both contained in the $(s+t-1)$-subspace χ^δ. As a result, φ_X maps elements of $\mathcal{P}_Y$ onto elements of $\mathcal{P}_X$. Note that φ_X inherits injectivity from the field reduction map. Proposition 9.1.5 proves bijectivity.

Claim 2: φ_X maps points contained in a fixed element of $\mathcal{L}_Y$ onto points contained in a fixed element of $\mathcal{L}_X$.

At this point, Figure 9.2 comes in handy to visualise the following arguments.

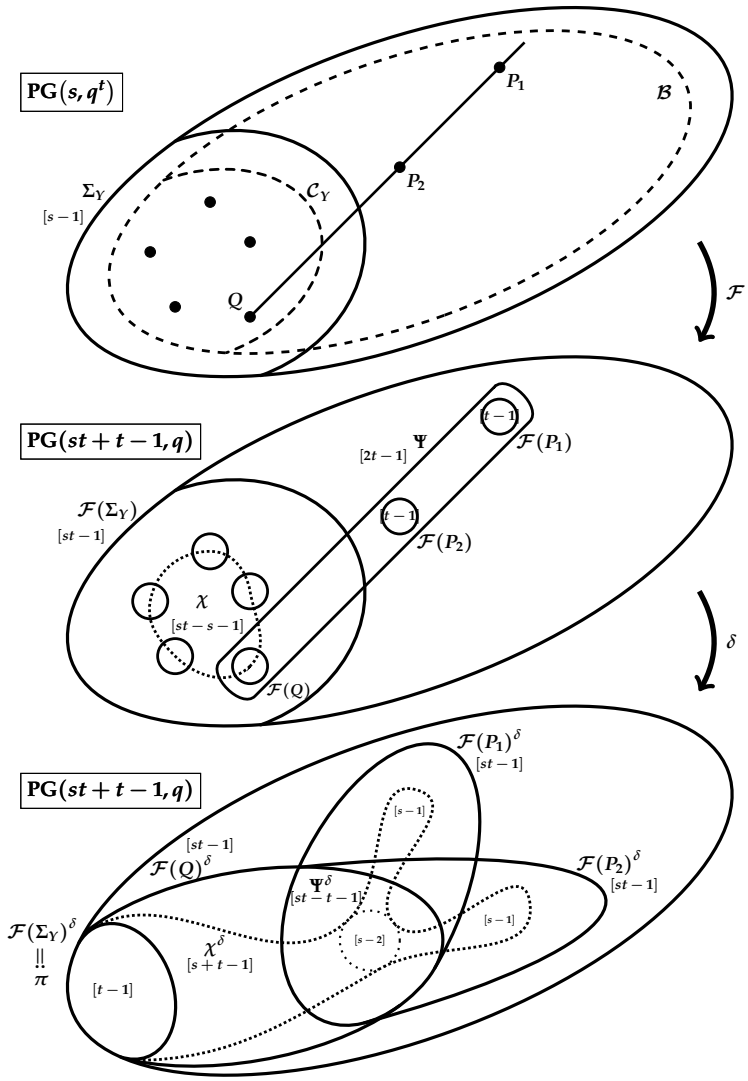


Figure 9.2: Visualisation of the map φ_X, see Definition 9.2.3.

Let $\mathcal{B} \in \mathcal{L}_Y$, consider two distinct points $P_1, P_2 \in \mathcal{B} \setminus \mathcal{C}_Y$ and define $Q := P_1P_2 \cap \mathcal{C}_Y$. Note that $\mathcal{F}(P_1)$ and $\mathcal{F}(P_2)$ are disjoint $(t-1)$-subspaces, each of which is disjoint to the $(st-1)$-subspace $\mathcal{F}(\Sigma_Y) \supset \mathcal{F}(Q)$. Therefore, they span a $(2t-1)$-subspace $\Psi := \langle \mathcal{F}(P_1), \mathcal{F}(P_2) \rangle$. Any two distinct elements of the set $\{\mathcal{F}(P_1), \mathcal{F}(P_2), \mathcal{F}(Q)\}$ span Ψ. Dualising these observations, we know that $\mathcal{F}(P_1)^\delta$, $\mathcal{F}(P_2)^\delta$ and $\mathcal{F}(Q)^\delta$ are $(st-1)$-subspaces intersecting each other in the $(st-t-1)$-subspace Ψ^δ, where $\mathcal{F}(P_1)^\delta$ and $\mathcal{F}(P_2)^\delta$ are disjoint to $\pi = \mathcal{F}(\Sigma_Y)^\delta$. Any two distinct elements of the set $\left\{\mathcal{F}(P_1)^\delta, \mathcal{F}(P_2)^\delta, \mathcal{F}(Q)^\delta\right\}$ intersect each other exactly in Ψ^δ. Moreover, the fact that $Q \in \Sigma_Y$ means that $\mathcal{F}(Q)^\delta$ is an $(st-1)$-subspace going through π.

As χ intersects $\mathcal{F}(Q)$ exactly in a $(t-2)$-subspace, χ^δ intersects $\mathcal{F}(Q)^\delta$ in an $(s+t-2)$-subspace $\varphi_X(Q) = \mathcal{F}(Q)^\delta \cap \chi^\delta$. Moreover, as both χ^δ and $\mathcal{F}(Q)^\delta$ are subspaces through π, their intersection $\varphi_X(Q)$ contains π as well. The subspace Ψ^δ is disjoint to π, so $\mathcal{F}(Q)^\delta$ is spanned by π and Ψ^δ; by Grassmann's identity, the $(s+t-2)$-subspace $\varphi_X(Q) = \mathcal{F}(Q)^\delta \cap \chi^\delta$ intersects Ψ^δ in an $(s-2)$-subspace. This means that χ^δ intersects both $\mathcal{F}(P_1)^\delta$ and $\mathcal{F}(P_2)^\delta$ in an $(s-2)$-subspace, which implies that $\varphi_X(P_1)$ intersects $\varphi_X(P_2)$ in an $(s-2)$-subspace.

As P_1 and P_2 were arbitrarily chosen points of $\mathcal{B} \setminus \mathcal{C}_Y$, we conclude that for any two points of the latter point set, their images under φ_X intersect each other maximally. Hence, this set of images $\varphi_X(\mathcal{B} \setminus \mathcal{C}_Y)$ forms an *Erdős-Ko-Rado set* [33, section 9.3], which means that

(1) either all elements of $\varphi_X(\mathcal{B} \setminus \mathcal{C}_Y)$ lie in an s-subspace, or

(2) all elements of $\varphi_X(\mathcal{B} \setminus \mathcal{C}_Y)$ have a fixed $(s-2)$-subspace in common.

If (1) generally holds, the proof of the claim is done, as this s-subspace is contained in χ^δ and contains (at least) an $(s-1)$-subspace (of $\varphi_X(\mathcal{B} \setminus \mathcal{C}_Y)$) disjoint to π. Hence, by Grassmann's identity, this s-subspace intersects π exactly in one point.

Suppose that (2) holds. As the points of the set $\mathcal{B} \setminus \mathcal{C}_Y$ span the whole space

$\mathrm{PG}(s, q^t)$, the elements of $\mathcal{F}(\mathcal{B} \setminus \mathcal{C}_Y)$ span the whole space $\mathrm{PG}(st + t - 1, q)$. However, as (2) holds, the intersection of all elements of $\varphi_X(\mathcal{B} \setminus \mathcal{C}_Y)$ has dimension at least $s - 2$, hence the intersection of all elements of $\mathcal{F}(\mathcal{B} \setminus \mathcal{C}_Y)^\delta$ has dimension at least $s - 2$ as well. Dualising this statement, we obtain that the span of all elements of $\mathcal{F}(\mathcal{B} \setminus \mathcal{C}_Y)$ has dimension at most $st + t - 1 - (s - 2) - 1 = st - s + t$. This is only possible if $st + t - 1 \leqslant st - s + t \Leftrightarrow s \leqslant 1 \Leftrightarrow s = 1$.
Hence, this implies that $s = 1$. Then χ^δ is a t-subspace of $\mathrm{PG}(2t - 1, q)$ through the $(t - 1)$-subspace π, intersecting each element of $\varphi_X(\mathcal{B} \setminus \mathcal{C}_Y)$ exactly in a point. Denote the set of points in $\mathcal{B}$ by $\mathcal{P}_\mathcal{B}$. As $\mathcal{B} \cong \mathrm{PG}(1, q)$, by Result 0.1.13, $\mathcal{F}(\mathcal{P}_\mathcal{B})$ is a regulus of $\mathrm{PG}(2t - 1, q)$. Let $Q_1, Q_2 \in \mathcal{B} \setminus \mathcal{C}_Y$ and define $Q_1' := \varphi_X(Q_1)$ and $Q_2' := \varphi_X(Q_2)$. Then $Q_1'Q_2'$ lies in the t-subspace χ^δ and hence intersects the $(t - 1)$-subspace $\pi = \mathcal{F}(Q)$ (here, $Q = \mathcal{C}_Y$). In this way, we see that $Q_1'Q_2'$ meets at least three elements of the regulus $\mathcal{F}(\mathcal{P}_\mathcal{B})$ (namely $\mathcal{F}(Q_1)$, $\mathcal{F}(Q_2)$ and $\mathcal{F}(Q)$), hence $Q_1'Q_2'$ has to intersect all elements of that regulus. As $Q_1'Q_2'$ is contained in χ^δ and as each element of $\mathcal{F}(\mathcal{B} \setminus \mathcal{C}_Y)$ intersects χ^δ exactly in a point, all these intersection points have to lie on $Q_1'Q_2'$ and hence the proof of the claim is done.

As φ_X induces a bijection between $\mathcal{P}_Y$ and $\mathcal{P}_X$, by Claim 2 and Remark 9.1.4, this map induces an injection with respect to the line sets $\mathcal{L}_Y$ and $\mathcal{L}_X$. Proposition 9.1.5 proves bijectivity. ∎

9.3 The isomorphism between $Y(s, t, q)$ and $Z(s, t, q)$

An explicit isomorphism between $Y(s, t, q)$ and $Z(s, t, q)$ will be constructed using coordinates.

9.3.1 Coordinate swapping

Consider the following configuration.

Configuration 9.3.1 (Using the notation of Definitions 9.1.2 and 9.1.3)

Choose a coordinate system for $\mathrm{PG}(s,q^t)$ such that

- $\left\{E_0^{(Y)}, E_1^{(Y)}, \ldots, E_s^{(Y)}, E^{(Y)}\right\}$ is the canonical frame,
- $F^{(Y)}$ is the point with coordinates $(0,1,\ldots,1)^\mathsf{T}$, and
- $\mathcal{C}_Y$ is the (by Result 0.1.2 unique) $(s-1)$-dimensional $\mathbb{F}_q$-subgeometry in Σ_Y containing $E_1^{(Y)}, \ldots, E_s^{(Y)}$ and $F^{(Y)}$.

Choose a coordinate system for $\mathrm{PG}(t,q^s)$ such that

- $\left\{E_0^{(Z)}, E_1^{(Z)}, \ldots, E_t^{(Z)}, E^{(Z)}\right\}$ is the canonical frame,
- $F^{(Z)}$ is the point with coordinates $(0,1,\ldots,1)^\mathsf{T}$, and
- $\mathcal{C}_Z$ is the (by Result 0.1.2 unique) $(t-1)$-dimensional $\mathbb{F}_q$-subgeometry in Σ_Z containing $E_1^{(Z)}, \ldots, E_t^{(Z)}$ and $F^{(Z)}$.

Lemma 9.3.2

Consider Configuration 9.3.1. Let $P, Q \notin \Sigma_Y$ be two distinct points of $\mathrm{PG}(s,q^t)$ with coordinates $(1,x_1,x_2,\ldots,x_s)^\mathsf{T}$ and $(1,y_1,y_2,\ldots,y_s)^\mathsf{T}$, $x_i, y_i \in \mathbb{F}_{q^t}$, such that $\langle P,Q\rangle$ intersects Σ_Y in $F^{(Y)}$. If $\mathcal{B}$ is the (by Lemma 0.1.3 unique) s-dimensional $\mathbb{F}_q$-subgeometry containing $\mathcal{C}_Y$, P and Q, then the set of coordinates of the points in $\mathcal{B} \setminus \mathcal{C}_Y$ is equal to

$$\left\{(1, x_1 + k_1(y_1 - x_1), \ldots, x_s + k_s(y_1 - x_1))^\mathsf{T} : k_1, \ldots, k_s \in \mathbb{F}_q\right\}.$$

Proof. It is clear that the hyperplane Σ_Y is defined by the equation $X_0 = 0$. Let $\mathcal{B}_0$ be the (by Result 0.1.2 unique) s-dimensional $\mathbb{F}_q$-subgeometry containing the frame $\left\{E_0^{(Y)}, E_1^{(Y)}, \ldots, E_s^{(Y)}, E^{(Y)}\right\}$. As this is the canonical

frame, the set of coordinates of the points in $\mathcal{B}_0 \setminus \mathcal{C}_Y$ is equal to

$$\left\{(1, k_1, k_2, \ldots, k_s)^\mathsf{T} : k_1, \ldots, k_s \in \mathbb{F}_q\right\}.$$

One can find a unique element of $\mathrm{PGL}(s+1, q^t)$ that maps the (ordered) canonical frame $\left(E_0^{(Y)}, E_1^{(Y)}, \ldots, E_s^{(Y)}, E^{(Y)}\right)$ onto the (ordered) frame $\left(P, E_1^{(Y)}, \ldots, E_s^{(Y)}, Q\right)$, which can be represented by an $\mathbb{F}_{q^t}$-multiple of the following matrix:

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ x_1 & y_1 - x_1 & 0 & \cdots & 0 \\ x_2 & 0 & y_2 - x_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_s & 0 & 0 & \cdots & y_s - x_s \end{pmatrix}.$$

Such a matrix maps a point of $\mathcal{B}_0$ with coordinates $(1, k_1, k_2, \ldots, k_s)^\mathsf{T}$, $k_i \in \mathbb{F}_q$, onto a point of $\mathcal{B}$ with coordinates

$$(1, x_1 + k_1(y_1 - x_1), x_2 + k_2(y_2 - x_2), \ldots, x_s + k_s(y_s - x_s))^\mathsf{T}.$$

As $F^{(Y)} \in \langle P, Q\rangle$, the vector $(0, y_1 - x_1, y_2 - x_2, \ldots, y_s - x_s)^\mathsf{T}$ has to be an $\mathbb{F}_{q^t}$-multiple of $(0, 1, 1, \ldots, 1)^\mathsf{T}$, which implies that $y_i - x_i = y_j - x_j$ for all $i, j \in \{1, 2, \ldots, s\}$. Hence, the set of coordinates of the points in $\mathcal{B} \setminus \mathcal{C}_Y$ can be simplified to

$$\left\{(1, x_1 + k_1(y_1 - x_1), \ldots, x_s + k_s(y_1 - x_1))^\mathsf{T} : k_1, \ldots, k_s \in \mathbb{F}_q\right\}. \qquad \blacksquare$$

9.3.2 The isomorphism

We now introduce the following map φ_Z.

Definition 9.3.3 (isomorphism φ_Z)

Consider Configuration 9.3.1. Choose primitive elements $\alpha \in \mathbb{F}_{q^t}$ and $\beta \in \mathbb{F}_{q^s}$ for field extensions $\mathbb{F}_{q^t}/\mathbb{F}_q$ and $\mathbb{F}_{q^s}/\mathbb{F}_q$, respectively, i.e. $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^t}$ and $\mathbb{F}_q(\beta) = \mathbb{F}_{q^s}$. Define the map $\varphi_Z : \mathcal{P}_Y \to \mathcal{P}_Z$ that maps a point of $\mathcal{P}_Y$ with coordinates

$$(1, z_1, z_2, \ldots, z_s)^\intercal = \left(1, \sum_{j=1}^{t} z_{1j}\alpha^{j-1}, \sum_{j=1}^{t} z_{2j}\alpha^{j-1}, \ldots, \sum_{j=1}^{t} z_{sj}\alpha^{j-1}\right)^\intercal$$

onto the point of $\mathcal{P}_Z$ with coordinates

$$\left(1, \sum_{i=1}^{s} z_{i1}\beta^{i-1}, \sum_{i=1}^{s} z_{i2}\beta^{i-1}, \ldots, \sum_{i=1}^{s} z_{it}\beta^{i-1}\right)^\intercal,$$

where $z_k \in \mathbb{F}_{q^t}$ and $z_{ij} \in \mathbb{F}_q$.

Theorem 9.3.4

Let $s, t \in \mathbb{N} \setminus \{0\}$. Then φ_Z induces an isomorphism between $Y(s,t,q)$ and $Z(s,t,q)$.

Proof. Note that the choice of coordinates made in Configuration 9.3.1 does not affect the generality of the theorem. After all, any collineation of $\mathrm{PG}(s, q^t)$ preserves elements of $\mathcal{L}_Y$ as being s-dimensional $\mathbb{F}_q$-subgeometries containing the image of $\mathcal{C}_Y$, hence the whole set $\mathcal{L}_Y$ is preserved and, furthermore, incidence is retained. The same holds for the point-line geometry $Z(s,t,q)$.
Let $\mathcal{B}$ be an arbitrary element of $\mathcal{L}_Y$. Suppose that $P, Q \in \mathcal{B} \setminus \mathcal{C}_Y$ are two distinct points with coordinates $(1, x_1, x_2, \ldots, x_s)^\intercal$ and $(1, y_1, y_2, \ldots, y_s)^\intercal$, $x_i, y_i \in \mathbb{F}_{q^t}$, such that $\langle P, Q\rangle$ intersects Σ_Y in $F^{(Y)}$. By Lemma 9.3.2, the set of coordinates of the points in $\mathcal{B} \setminus \mathcal{C}_Y$ is equal to

$$\left\{(1, x_1 + k_1(y_1 - x_1), \ldots, x_s + k_s(y_1 - x_1))^\intercal : k_1, \ldots, k_s \in \mathbb{F}_q\right\}.$$

Note that φ_Z is a bijection, as one can easily define its inverse (see Definition 9.3.3). If $x_i = \sum_{j=1}^{t} x_{ij}\alpha^{j-1}$ and $y_i = \sum_{j=1}^{t} y_{ij}\alpha^{j-1}$ for certain values $x_{ij}, y_{ij} \in \mathbb{F}_q$ ($i \in \{1, 2, \ldots, s\}$), then a point is the image of a point in $\mathcal{B} \setminus \mathcal{C}_Y$ under φ_Z if and only if its coordinates are equal to

$$\left(1, \sum_{i=1}^{s} \left(x_{i1} + k_i \left(y_{11} - x_{11}\right)\right) \beta^{i-1}, \ldots, \sum_{i=1}^{s} \left(x_{it} + k_i \left(y_{1t} - x_{1t}\right)\right) \beta^{i-1}\right)^{\mathsf{T}}$$

for certain values $k_1, \ldots, k_s \in \mathbb{F}_q$

$$= \left(1, \sum_{i=1}^{s} x_{i1}\beta^{i-1}, \ldots, \sum_{i=1}^{s} x_{it}\beta^{i-1}\right)^{\mathsf{T}} + \sum_{i=1}^{s} k_i \beta^{i-1} \left(0, y_{11} - x_{11}, \ldots, y_{1t} - x_{1t}\right)^{\mathsf{T}}$$

for certain values $k_1, \ldots, k_s \in \mathbb{F}_q$

$$= \left(1, \sum_{i=1}^{s} x_{i1}\beta^{i-1}, \ldots, \sum_{i=1}^{s} x_{it}\beta^{i-1}\right)^{\mathsf{T}} + k \left(0, y_{11} - x_{11}, \ldots, y_{1t} - x_{1t}\right)^{\mathsf{T}}$$

for a certain value $k \in \mathbb{F}_{q^s}$. (9.1)

Therefore, the images under φ_Z of the points in $\mathcal{B} \setminus \mathcal{C}_Y$ are precisely the points in $\ell \setminus \Sigma_Z$, with ℓ a line of $\mathrm{PG}(t, q^s)$ through $\varphi_Z(P) \notin \Sigma_Z$ intersecting Σ_Z in the point of $\mathcal{C}_Z$ with coordinates $(0, x_{11} - y_{11}, \ldots, x_{1t} - y_{1t})^{\mathsf{T}} \in V(t+1, q)$. Hence, as φ_Z maps points in a fixed line of $Y(s, t, q)$ onto points in a fixed line of $Z(s, t, q)$, this map naturally induces a morphism from $Y(s, t, q)$ to $Z(s, t, q)$. Furthermore, as φ_Z is a bijection between $\mathcal{P}_Y$ and $\mathcal{P}_Z$, by Remark 9.1.4, this map is injective with respect to the line sets $\mathcal{L}_Y$ and $\mathcal{L}_Z$. Proposition 9.1.5 proves bijectivity. ∎

The purpose of the isomorphism described above is to be able to explicitly transfer natural notions of *parallelism* and *affine subspaces* from $Z(s, t, q)$ to $Y(s, t, q)$.

9.3.3 Parallelism, independence and affyne subspaces

Theorem 9.3.4 states that the point-line geometry $Y(s, t, q)$ is isomorphic to $Z(s, t, q)$, whose lines are essentially affine lines of $\mathrm{AG}(t, q^s)$ (see Defini-

tions 9.1.2 and 9.1.3). Therefore, notions of *parallelism* and *affine subspaces* seem transferable to the point-line geometry $Y(s,t,q)$.

Definition 9.3.5 (affine notions of subgeometries)

Consider the point-line geometry $Y(s,t,q)$ and its corresponding (induced) isomorphism φ_Z to $Z(s,t,q)$ (see Definitions 9.1.2, 9.1.3 and 9.3.3). Then

- distinct lines of $\mathcal{L}_Y$ are called **concurrent** if they contain a common point (of $\mathcal{P}_Y$).
- two lines of $\mathcal{L}_Y$ are said to be **parallel** if their images under φ_Z are parallel,
- concurrent lines of $\mathcal{L}_Y$ are called **independent** if their images under φ_Z intersect $\mathcal{C}_Z$ in points that lie in general position, and
- for any $k \in \{0,1,\ldots,t\}$, a set of q^{ks} points of $\mathcal{P}_Y$ is said to be a ***k*-dimensional affyne**[a] **subspace** if the images of its points under φ_Z lie in a fixed k-subspace containing θ_{k-1} points of $\mathcal{C}_Z$.

[a] This is not a typo! The conventional 'i' is replaced by a 'y' as a subtle wink to the point-line geometry $\boldsymbol{Y(s,t,q)}$.

A careful attitude is required when moving forward with the above definitions. Recall, after all, that the isomorphism induced by φ_Z relies on a specific choice of coordinates within the respective projective geometries in which $Y(s,t,q)$ and $Z(s,t,q)$ are embedded.

Lemma 9.3.6

The notions described in Definition 9.3.5 are well-defined.

Proof. Assume that $Y(s,t,q)$ is chosen in such a way that it corresponds to the coordinate system described in Configuration 9.3.1. For this lemma to be true, we want to prove that if one of the last three notions described in Definition 9.3.5 holds for certain points or lines of $Y(s,t,q)$, it still holds for

the images of these points or lines with respect to any collineation of the ambient geometry $\mathrm{PG}(s, q^t)$.
Let $\mathcal{B}$ be an arbitrary element of $\mathcal{L}_Y$ and $P, Q \in \mathcal{B} \setminus \mathcal{C}_Y$ be two distinct points with coordinates $(1, x_1, x_2, \ldots, x_s)^\mathsf{T}$ and $(1, y_1, y_2, \ldots, y_s)^\mathsf{T}$, respectively ($x_i, y_i \in \mathbb{F}_{q^t}$), such that $\langle P, Q\rangle$ intersects Σ_Y in $F^{(Y)}$ (see Configuration 9.3.1), implying that

$$y_1 - x_1 = \cdots = y_s - x_s. \tag{9.2}$$

Assuming that $x_i = \sum_{j=1}^{t} x_{ij}\alpha^{j-1}$ and $y_i = \sum_{j=1}^{t} y_{ij}\alpha^{j-1}$ ($\mathbb{F}_q(\alpha) = \mathbb{F}_{q^t}$ and $x_{ij}, y_{ij} \in \mathbb{F}_q$, see Definition 9.3.3), just as in (9.1), the set of coordinates of the images of the points in $\mathcal{B} \setminus \mathcal{C}_Y$ under φ_Z is equal to

$$\left\{(\text{coordinates of } \varphi_Z(P)) + k \cdot (0, y_{11} - x_{11}, \ldots, y_{1t} - x_{1t})^\mathsf{T} : k \in \mathbb{F}_{q^s}\right\}.$$

Any two elements $\mathcal{B}^{(1)}, \mathcal{B}^{(2)} \in \mathcal{L}_Y$ are therefore parallel if and only if there exists an element $\gamma \in \mathbb{F}_{q^s}$ such that $\left(0, y_{11}^{(1)} - x_{11}^{(1)}, \ldots, y_{1t}^{(1)} - x_{1t}^{(1)}\right)^\mathsf{T} = \gamma \cdot \left(0, y_{11}^{(2)} - x_{11}^{(2)}, \ldots, y_{1t}^{(2)} - x_{1t}^{(2)}\right)^\mathsf{T}$. Moreover, as both of these coordinates are vectors of $V(t+1, q)$ and as the values $y_{1j}^{(2)} - x_{1j}^{(2)}$ cannot all be zero ($P \neq Q$), γ has to be an element of $\mathbb{F}_q$. Combining this with (9.2), we get that $y_{ij}^{(1)} - x_{ij}^{(1)} = \gamma\left(y_{ij}^{(2)} - x_{ij}^{(2)}\right)$ for all $i \in \{1, 2, \ldots, s\}$ and all $j \in \{1, 2, \ldots, t\}$, implying that

$$\left(y_1^{(1)} - x_1^{(1)}, \ldots, y_s^{(1)} - x_s^{(1)}\right)^\mathsf{T} = \gamma \cdot \left(y_1^{(2)} - x_1^{(2)}, \ldots, y_s^{(2)} - x_s^{(2)}\right)^\mathsf{T} \quad \text{for a } \gamma \in \mathbb{F}_q. \tag{9.3}$$

As $\mathbb{F}_q$ is fixed under any automorphism of the ambient field $\mathbb{F}_{q^t}$, we can observe that property (9.3) remains valid if $P^{(1)}$, $Q^{(1)}$, $P^{(2)}$ or $Q^{(2)}$ are moved by an element of $\mathrm{P\Gamma L}(s+1, q^t)$. This implies that parallelism of elements of $\mathcal{L}_Y$ is invariant with respect to collineations, hence this notion is well-defined.
Using this, we can prove the same for the notion of a k-dimensional affyne subspace, $k \in \{0, 1, \ldots, t\}$. If $k = 0$, this is trivially true. If $k \geqslant 1$,

a k-dimensional affyne subspace occurs as a set of q^{ks} points of $\mathcal{P}_Y$ lying in a union of $q^{(k-1)s}$ parallel lines through each of the points of a $(k-1)$-dimensional affyne subspace. As any collineation of $\mathrm{PG}(s,q^t)$ preserves incidence, parallelism and, inductively, $(d-1)$-dimensional affyne subspaces, the claim follows.
Finally, as the points of $\mathcal{P}_Y$ lying on k concurrent, independent lines of $\mathcal{L}_Y$ are contained in a unique k-dimensional affyne subspace, the invariance of the latter affyne subspace implies the invariance of the independence of those lines. ∎

Consider the following configuration.

Configuration 9.3.7

Consider an $(s-1)$-dimensional $\mathbb{F}_q$-subgeometry $\mathcal{C}_Y$ lying in an $(s-1)$-subspace Σ_Y of $\mathrm{PG}(s+1,q^t)$ and choose three distinct hyperplanes Π_1, Π_2 and Π_3 through Σ_Y.
For each $i \in \{1,2,3\}$, consider a point-line geometry $(\mathcal{P}_{Y_i}, \mathcal{L}_{Y_i})$ in $\Pi_i \cong \mathrm{PG}(s,q^t)$ isomorphic to $Y(s,t,q)$ (with $\mathcal{C}_Y$ as a common 'central' subgeometry).

Lemma 9.3.8

Consider Configuration 9.3.7. Let $\mathcal{B} \in \mathcal{L}_{Y_1}$ and $S \in \mathcal{P}_{Y_2}$. Then there exists a unique $(s+1)$-dimensional $\mathbb{F}_q$-subgeometry $\mathcal{A}_{\mathcal{B},S}$ containing $\mathcal{B}$, S and a point of $\mathcal{P}_{Y_3}$.

Proof. Choose a point $R \in \mathcal{B} \setminus \mathcal{C}_Y$. Then the line $\langle R,S\rangle$ has to intersect Π_3 in a point $T \notin \Sigma_Y$. Any $(s+1)$-dimensional $\mathbb{F}_q$-subgeometry that contains $\mathcal{B}$ and S and intersects Π_3 in a point outside of Σ_Y, has to contain T and, in particular, the (by Result 0.1.2) unique $\mathbb{F}_q$-subline defined by R, S and T. By Lemma 0.1.3, there exists exactly one such $\mathbb{F}_q$-subgeometry. ∎

Definition 9.3.9 (projection and shadow map)

Consider Configuration 9.3.7. For any point $S \in \mathcal{P}_{Y_2}$, we introduce the **projection map**

$$\mathrm{proj}^S_{\Pi_1,\Pi_3} : \mathcal{L}_{Y_1} \to \mathcal{L}_{Y_3} : \mathcal{B} \mapsto (\mathcal{A}_{\mathcal{B},S} \cap \Pi_3),$$

and the **shadow map**

$$\mathrm{shad}^S_{\Pi_1,\Pi_3} : \mathcal{L}_{Y_1} \to \mathcal{L}_{Y_2} : \mathcal{B} \mapsto (\mathcal{A}_{\mathcal{B},S} \cap \Pi_2),$$

with $\mathcal{A}_{\mathcal{B},S}$ the (by Lemma 9.3.8) unique $(s+1)$-dimensional $\mathbb{F}_q$-subgeometry containing $\mathcal{B}$, S and a point of $\mathcal{P}_{Y_3}$. Furthermore, for a fixed element $\mathcal{B} \in \mathcal{L}_{Y_1}$, we can naturally extend the maps above and define, for any subset $\mathcal{T} \subseteq \mathcal{P}_{Y_2}$,

$$\mathrm{proj}^{\mathcal{T}}_{\Pi_1,\Pi_3}(\mathcal{B}) := \bigcup_{S\in\mathcal{T}} \left\{ P \in \mathcal{P}_{Y_3} \,:\, P \in \mathrm{proj}^S_{\Pi_1,\Pi_3}(\mathcal{B}) \right\}$$

and

$$\mathrm{shad}^{\mathcal{T}}_{\Pi_1,\Pi_3}(\mathcal{B}) := \bigcup_{S\in\mathcal{T}} \left\{ P \in \mathcal{P}_{Y_2} \,:\, P \in \mathrm{shad}^S_{\Pi_1,\Pi_3}(\mathcal{B}) \right\}.$$

Lemma 9.3.10

Consider Configuration 9.3.7. Let $\mathcal{B} \in \mathcal{L}_{Y_1}$ and $S_1, S_2 \in \mathcal{P}_{Y_2}$. Then $\mathrm{shad}^{S_1}_{\Pi_1,\Pi_3}(\mathcal{B})$ and $\mathrm{shad}^{S_2}_{\Pi_1,\Pi_3}(\mathcal{B})$ are parallel.

Proof. Choose a coordinate system for $\mathrm{PG}(s+1,q^t)$ such that $\{E_0, E_1, \ldots, E_{s+1}, E\}$ is the canonical frame and the points F and G correspond to the coordinates $(0,1,1,\ldots,1)^\mathsf{T}$ and $(0,0,1,\ldots,1)^\mathsf{T}$, respectively. By Lemma 9.3.6, we may assume, without loss of generality, that

- $\mathcal{C}_Y$ is (by Result 0.1.2) uniquely defined by the points $E_2, \ldots, E_{s+1}$ and G,

- E_1 is a point of $\mathcal{B}$, and
- E_0 and E are the points $\ell \cap \Pi_2$ and $\ell \cap \Pi_3$, respectively, with $\ell \nsubseteq \Pi_1$ an arbitrarily chosen line intersecting Π_1 in a point of $\mathcal{B} \setminus (\mathcal{C}_Y \cup \{E_1\})$.

In this way, $\mathcal{B}$ is (indirectly by Lemma 0.1.3) uniquely defined by $\mathcal{C}_Y$, E_1 and $F \in \langle E_0, E\rangle = \ell$. If S_1 has coordinates $(1,0,x_2,\ldots,x_{s+1})^{\mathsf{T}}$ ($x_i \in \mathbb{F}_{q^t}$), the line $\langle F, S_1\rangle$ intersects Π_3 in a point T_1 with coordinates $(1,1,1+x_2,\ldots,1+x_{s+1})^{\mathsf{T}}$.
By Lemma 9.3.8, there exists a unique $(s+1)$-dimensional $\mathbb{F}_q$-subgeometry $\mathcal{A}_{\mathcal{B},S_1}$ containing $\mathcal{B}$, S_1 and T_1. By Lemma 9.3.2, the set of coordinates of the points in $\mathcal{A}_{\mathcal{B},S_1} \setminus \mathcal{B}$ is equal to

$$\left\{(1,k_1,x_2+k_2,\ldots,x_{s+1}+k_{s+1})^{\mathsf{T}} : k_1,\ldots,k_{s+1} \in \mathbb{F}_q\right\}.$$

As a consequence, the set of coordinates of the points of $\mathrm{shad}^{S_1}_{\Pi_1,\Pi_3}(\mathcal{B})$ is equal to

$$\left\{(1,0,x_2+k_2,\ldots,x_{s+1}+k_{s+1})^{\mathsf{T}} : k_2,\ldots,k_{s+1} \in \mathbb{F}_q\right\}. \tag{9.4}$$

Restricting these coordinates to the geometry $\mathrm{PG}(s,q^t) \cong \Pi_2$ (by ignoring the second coordinate 0), the set of coordinates of the images of the points (9.4) under φ_Z is, as in (9.1), equal to

$$\left\{(\text{coordinates of } \varphi_Z(S_1)) + k\cdot(0,1,0,\ldots,0)^{\mathsf{T}} : k \in \mathbb{F}_{q^s}\right\}.$$

As the line parallel class of the affine line that arises in this way does not rely on the choice of the point $S_1 \in \mathcal{P}_{Y_2}$, the lemma is proven. ∎

Lemma 9.3.11

Consider Configuration 9.3.7. Let $\mathcal{B}_1,\mathcal{B}_2,\ldots,\mathcal{B}_j \in \mathcal{L}_{Y_1}$ be j independent lines sharing a point $R \in \mathcal{P}_{Y_1}$, $j \in \{1,2,\ldots,t\}$, and suppose that $\mathcal{T} \subseteq \mathcal{P}_{Y_2}$ is a $(j-1)$-dimensional affyne subspace. Then there exists a $k \in \{1,2,\ldots,j\}$ such

that $\mathrm{proj}^{\mathcal{T}}_{\Pi_1,\Pi_3}(\mathcal{B}_k)$ *is a j-dimensional affyne subspace.*

Proof. Choose a point $S \in \mathcal{T}$ and define $T := \langle R, S\rangle \cap \Pi_3$. The projection of points of Π_1 onto Π_2 via the point T is a natural projectivity between the subspaces when interpreted as distinct projective geometries. Hence, if one projects each of the subgeometries $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_j$ onto Π_2 via T, we obtain j independent lines $\mathcal{B}'_1, \mathcal{B}'_2, \ldots, \mathcal{B}'_j \in \mathcal{L}_{Y_2}$ sharing the point $S \in \mathcal{T}$. As $\mathcal{T}$ is a $(j-1)$-dimensional affyne subspace, there has to exist a $\mathcal{B}'_k$ which has only the point S in common with $\mathcal{T}$. Moreover, it is easy to see that $\mathcal{B}'_k = \mathrm{shad}^{S}_{\Pi_1,\Pi_3}(\mathcal{B}_k)$. Hence, by Lemma 9.3.10, $\mathrm{shad}^{\mathcal{T}}_{\Pi_1,\Pi_3}(\mathcal{B}_k)$ is a union of $|\mathcal{T}|$ distinct, parallel elements of $\mathcal{L}_{Y_2}$, each containing a unique point of $\mathcal{T}$. In other words, $\mathrm{shad}^{\mathcal{T}}_{\Pi_1,\Pi_3}(\mathcal{B}_k)$ is a j-dimensional affyne subspace. By considering the natural projection of points of Π_2 onto Π_3 via R, one can check that $\mathrm{shad}^{\mathcal{T}}_{\Pi_1,\Pi_3}(\mathcal{B}_k)$ gets projected onto $\mathrm{proj}^{\mathcal{T}}_{\Pi_1,\Pi_3}(\mathcal{B}_k)$. ∎

10 Flowers in bloom

This final chapter puts us back on track concerning the topic of *saturating sets*. By exploiting the presence of *parallelism* and affine subspaces (see Chapter 9), we are able to construct relatively small saturating sets by 'mixing' certain several distinct, partially overlapping subgeometries.

The results of this chapter can be found in [61].

10.1 One flower is almost enough

First, let us define what we mean by a *flower*.

Definition 10.1.1 (flower)

Let $m \in \mathbb{N}$. A set $\mathcal{F}$ of $\varrho + 1$ m-subspaces of $\mathrm{PG}(d, q)$ is said to be an ***m*-flower** if

- they share an $(m-1)$-subspace called the **pistil** of $\mathcal{F}$, and
- their span has dimension $m + \varrho$.

The elements of $\mathcal{F}$ are called the **petals** of the m-flower.

Lemma 10.1.2

Let $\mathcal{F} := \{\tau_1, \tau_2, \ldots, \tau_{\varrho+1}\}$ be a $(d-\varrho)$-flower of $\mathrm{PG}(d, q^{\varrho+1})$ whose pistil Σ_Y contains a $(d-\varrho-1)$-dimensional $\mathbb{F}_q$-subgeometry $\mathcal{C}_Y$. For every $j \in \{1, 2, \ldots, \varrho+1\}$, consider the point-line geometry $\left(\mathcal{P}_Y^{\tau_j}, \mathcal{L}_Y^{\tau_j}\right) \cong Y(d-\varrho, \varrho+1, q)$ (see Definition 9.1.2) and take j independent lines $\mathcal{B}_j^{(1)}, \mathcal{B}_j^{(2)}, \ldots, \mathcal{B}_j^{(j)} \in \mathcal{L}_Y^{\tau_j}$ sharing a point $F_j \in \mathcal{P}_Y^{\tau_j}$. Then the point set

$$\mathfrak{B} := \bigcup_{j=1}^{\varrho+1} \bigcup_{k=1}^{j} \left(\mathcal{B}_j^{(k)} \setminus \mathcal{C}_Y\right)$$

ϱ-saturates all points of $\mathrm{PG}(d, q^{\varrho+1})$ not lying in the span of ϱ petals of $\mathcal{F}$.

Proof. Let P be an arbitrary point not contained in the span of any ϱ petals of $\mathcal{F}$. Define $\Pi_j := \langle \tau_j, \tau_{j+1}, \ldots, \tau_{\varrho+1} \rangle$ for every $j \in \{1, 2, \ldots, \varrho+1\}$. Note that Π_1 is equal to the whole space, hence $P \in \Pi_1$.

Now consider the $(d-\varrho)$-subspace $\pi_0 := \langle \Sigma_Y, P \rangle$ with its corresponding point-line geometry $\left(\mathcal{P}_Y^{\pi_0}, \mathcal{L}_Y^{\pi_0}\right) \cong Y(d-\varrho, \varrho+1, q)$, and define the point set $\mathcal{T}_0 := \{P\}$. One can now iterate through the following process, for j going from 1 to ϱ.

(1) Define π_j. Note that π_{j-1} and τ_j are distinct $(d-\varrho)$-subspaces through Σ_Y, contained in Π_j but not contained in Π_{j+1}. As Π_{j+1} is a hyperplane of Π_j, $\langle \pi_{j-1}, \tau_j \rangle$ intersects Π_{j+1} in a $(d-\varrho)$-subspace π_j with corresponding point-line geometry $\left(\mathcal{P}_Y^{\pi_j}, \mathcal{L}_Y^{\pi_j}\right) \cong Y(d-\varrho, \varrho+1, q)$.

(2) Define $\mathcal{T}_j$. Observe that π_{j-1}, τ_j and π_j are three distinct $(d-\varrho)$-subspaces through Σ_Y that span a $(d-\varrho+1)$-subspace. Moreover, $\mathcal{T}_{j-1} \subset \mathcal{P}_Y^{\pi_{j-1}}$ is a $(j-1)$-dimensional affyne subspace. By Lemma 9.3.11, there exists a $\mathcal{B}_j^{(k)} \in \mathcal{L}_Y^{\tau_j}$ such that $\mathcal{T}_j :=$

$\mathrm{proj}_{\tau_j,\pi_j}^{\mathcal{T}_{j-1}}\left(\mathcal{B}_j^{(k)}\right) \subset \mathcal{P}_Y^{\pi_j}$ is a j-dimensional affyne subspace.

(3) Define Q_j. Note that any point $T_j \in \mathcal{T}_j$ lies in the span of a point of $\mathfrak{B} \cap \tau_j$ and a point of $\mathcal{T}_{j-1}$. Indeed, by definition of $\mathrm{proj}_{\tau_j,\pi_j}^{\mathcal{T}_{j-1}}$, there has to exist a point $T_j' \in \mathcal{T}_{j-1}$ such that $T_j \in \mathrm{proj}_{\tau_j,\pi_j}^{T_j'}\left(\mathcal{B}_j^{(k)}\right)$. Hence, there exists a point $Q_j \in \mathcal{B}_j^{(k)} \setminus \mathcal{C}_Y$ that is projected via T_j' onto T_j.

Eventually, we conclude that $\mathcal{T}_\varrho \subset \mathcal{P}_Y^{\pi_\varrho}$ is a ϱ-dimensional affyne subspace, which is an affyne hyperplane. Furthermore, note that $\mathcal{T}_\varrho \subset \pi_\varrho \subseteq \Pi_{\varrho+1} = \tau_{\varrho+1}$. As $\mathfrak{B} \cap \tau_{\varrho+1}$ is a union of $\varrho+1$ concurrent, independent $\mathbb{F}_q$-subgeometries, there has to exist a point $Q_{\varrho+1} \in \mathcal{T}_\varrho \cap \left(\mathfrak{B} \cap \tau_{\varrho+1}\right)$, since any union of $\varrho+1$ concurrent, independent lines of $\mathrm{AG}\left(\varrho+1, q^{d-\varrho}\right)$ meets any hyperplane in at least one point. By recursively backtracking the observation obtained in step (3), we conclude that $Q_{\varrho+1}$ lies in $\left\langle Q_\varrho, Q_{\varrho-1}, \ldots, Q_1, P\right\rangle$, with $Q_j \in \mathfrak{B} \cap \tau_j$ ($j \in \{1, 2, \ldots, \varrho+1\}$). This implies that $P \in \left\langle Q_1, Q_2, \ldots, Q_{\varrho+1}\right\rangle$, as no point of $\left\{Q_1, Q_2, \ldots, Q_{\varrho+1}\right\}$ can lie in the span of the others by the definition of a flower. ∎

By the lemma above, we can find a relatively small point set that ϱ-saturates 'most' of the points of $\mathrm{PG}\left(d, q^{\varrho+1}\right)$. We could end our quest right here and now, by recursively copying smaller versions of similar point sets in the span of any ϱ petals of $\mathcal{F}$. However, as this would dramatically increase the size of the saturating set, a need to optimise the construction arises.

To compensate for the somewhat restricted ϱ-saturating capabilities described by the lemma above, we construct a ϱ-saturating set as a mix of several *layers* of flowers.

10.2 An intricate bouquet

ASSUMPTION

Throughout this *section*, we fix the following value:

$$\lambda := \min\{\varrho, d-\varrho\}\,.$$

Definition 10.2.1 (ceilfloor map)

For every $i \in \{1,\dots,\lambda\}$, define the map

$$\begin{aligned}\lceil\cdot\rfloor^{(i)} : \{\varrho+2-\lambda,\dots,\varrho+1\} &\to \{\varrho+2-\lambda,\dots,\varrho+1\}\\ : j \mapsto \lceil j\rfloor^{(i)} &:= \begin{cases} j+i-1 & \text{if } j+i-1 \leqslant \varrho+1,\\ \varrho+2-i & \text{otherwise.}\end{cases}\end{aligned}$$

As the map above could induce some confusion, we will give the reader an intuition of Configuration 10.2.2 (further on) before plunging into the technical details.

10.2.1 The general idea

As said before, the main construction will be built by making use of a mix of multiple flowers. These flowers will be stacked upon each other, forming a total of λ 'layers', in the sense that

- the 'largest' layer (layer $i = 1$) is a $(d-\varrho)$-flower whose petals are numbered $1, 2, \dots, \varrho+1$,
- within this layer, we consider a $(d-\varrho-1)$-flower (layer $i = 2$), whose petals are each contained in a unique petal of the layer 'above',
- ...
- the 'smallest' layer (layer $i = \lambda$) is a $(d-\varrho-\lambda+1)$-flower whose petals are each contained in a unique petal of the layer 'above'.

In this way, we obtain $\varrho + 1$ 'layered' petals. Inspired by Lemma 10.1.2, we now choose a set of concurrent, independent $\mathbb{F}_q$-subgeometries in certain petals. The number of such subgeometries depends on the number of the layer (i) and the number of the petal (j). If $j \leqslant \varrho + 1 - \lambda$, we choose j concurrent, independent $\mathbb{F}_q$-subgeometries in the top layer ($i = 1$) of petal j, and none in any of its other layers. If $j > \varrho + 1 - \lambda$, we choose $\lceil j \rfloor^{(i)}$ concurrent, independent $\mathbb{F}_q$-subgeometries in layer i of petal j, i.e.

- $\lceil j \rfloor^{(1)} = j$ concurrent, independent $\mathbb{F}_q$-subgeometries in the top layer of petal j,
- $\lceil j \rfloor^{(2)} = j + 1$ concurrent, independent $\mathbb{F}_q$-subgeometries in the next layer ($i = 2$) of petal j,
- ...
- $\lceil j \rfloor^{(\varrho+2-j)} = \varrho + 1$ concurrent, independent $\mathbb{F}_q$-subgeometries in the next layer ($i = \varrho + 2 - j$) of petal j,
- $\lceil j \rfloor^{(\varrho+3-j)} = j - 1$ concurrent, independent $\mathbb{F}_q$-subgeometries in the next layer ($i = \varrho + 3 - j$) of petal j,
- ...
- $\lceil j \rfloor^{(\lambda)} = \varrho + 2 - \lambda$ concurrent, independent $\mathbb{F}_q$-subgeometries in the bottom layer ($i = \lambda$) of petal j.

The reason for this sophisticated way of choosing certain $\mathbb{F}_q$-subgeometries is to ensure that for every point P, there exists an adequate flower within this particular configuration that ϱ-saturates P (described in Lemma 10.1.2).

10.2.2 The nitty-gritty

We now formalise the intuitive configuration of the previous subsection and hence introduce the main configuration of this chapter. Be sure to keep Figure 10.1 at hand for a visualisation of an example case with three two-layered petals.

Configuration 10.2.2

Consider two sets $\{\mathcal{C}_1, \ldots, \mathcal{C}_\lambda\}$ and $\{\Sigma_1, \ldots, \Sigma_\lambda\}$ of $\mathbb{F}_q$-subgeometries and subspaces of $\mathrm{PG}(d, q^{\varrho+1})$, respectively, such that

- for every $i \in \{1, \ldots, \lambda\}$, $\mathcal{C}_i$ is a $(d-\varrho-i)$-dimensional $\mathbb{F}_q$-subgeometry with $\langle \mathcal{C}_i \rangle_{q^{\varrho+1}} = \Sigma_i$, and
- $\mathcal{C}_1 \supset \mathcal{C}_2 \supset \cdots \supset \mathcal{C}_\lambda$, implying that $\Sigma_1 \supset \Sigma_2 \supset \cdots \supset \Sigma_\lambda$.

Moreover, let $\{\mathcal{F}_1, \ldots, \mathcal{F}_\lambda\}$ be a set of flowers such that

- for every $i \in \{1, \ldots, \lambda\}$, $\mathcal{F}_i := \left\{\tau_{i1}, \ldots, \tau_{i(\varrho+1)}\right\}$ is a $(d-\varrho-i+1)$-flower with pistil Σ_i, and
- for every $j \in \{1, \ldots, \varrho+1\}$, $\tau_{1j} \supset \tau_{2j} \supset \cdots \supset \tau_{\lambda j}$.

For every $i \in \{1, \ldots, \lambda\}$ and $j \in \{1, \ldots, \varrho+1\}$, consider the point-line geometry $\left(\mathcal{P}_Y^{\tau_{ij}}, \mathcal{L}_Y^{\tau_{ij}}\right) \cong Y(d-\varrho-i+1, \varrho+1, q)$ with respect to $\mathcal{C}_i$. Now define, for every $j \in \{1, \ldots, \varrho+1\}$,

$$\mathfrak{P}_j := \begin{cases} \bigcup_{k=1}^{j} \left(\mathcal{B}_{1j}^{(k)} \setminus \mathcal{C}_1\right) & \text{if } j \leqslant \varrho+1-\lambda, \\ \bigcup_{i=1}^{\lambda} \bigcup_{k=1}^{\lceil j \rfloor^{(i)}} \left(\mathcal{B}_{ij}^{(k)} \setminus \mathcal{C}_i\right) & \text{if } j > \varrho+1-\lambda, \end{cases}$$

where $\mathcal{B}_{ij}^{(1)}, \mathcal{B}_{ij}^{(2)}, \ldots, \mathcal{B}_{ij}^{\left(\lceil j \rfloor^{(i)}\right)} \in \mathcal{L}_Y^{\tau_{ij}}$ are $\lceil j \rfloor^{(i)}$ independent lines sharing a point $F_{ij} \in \mathcal{P}_Y^{\tau_{ij}} \setminus \tau_{(i+1)j}$ ($i \in \{1, \ldots, \lambda\}$, $\tau_{(\lambda+1)j} := \varnothing$).
Finally, define

$$\mathfrak{P}_1' := \begin{cases} \bigcup_{i=2}^{\lambda} \left(\mathcal{B}_{i1}' \setminus \mathcal{C}_i\right) & \text{if } q = 2, \\ \varnothing & \text{if } q \neq 2, \end{cases}$$

with $\mathcal{B}_{i1}' \in \mathcal{L}_Y^{\tau_{i1}}$ such that $\langle \mathcal{B}_{i1}' \rangle_{q^{\varrho+1}}$ intersects $\mathcal{B}_{(i-1)1}'$ only in $\mathcal{C}_i$ ($i \in \{2, \ldots, \lambda\}$, $\mathcal{B}_{11}' := \mathcal{B}_{11}^{(1)}$).

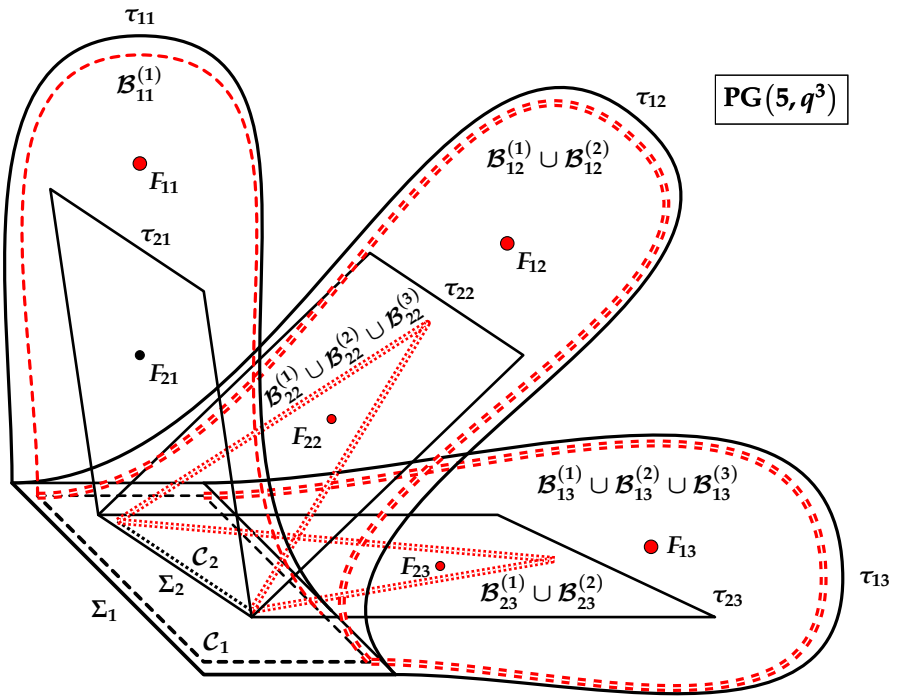


Figure 10.1: A visualisation of Configuration 10.2.2 in case $d = 5$ and $\varrho = 2$; we observe two stacked flowers, resulting in three two-layered petals. The 2-saturating set is shown in red. The petal τ_{11} has a number $j = 1$ not exceeding $\varrho + 1 - \lambda = 1$. The petals with number $j = 2$ correspond to $\lceil 2 \rfloor^{(1)} = 2$ chosen $\mathbb{F}_q$-subgeometries in the top layer and $\lceil 2 \rfloor^{(2)} = 3$ chosen $\mathbb{F}_q$-subgeometries in the bottom layer (increasing). The petals with number $j = 3$ correspond to $\lceil 3 \rfloor^{(1)} = 3$ chosen $\mathbb{F}_q$-subgeometries in the top layer and $\lceil 3 \rfloor^{(2)} = 2$ chosen $\mathbb{F}_q$-subgeometries in the bottom layer (decreasing).

Lemma 10.2.3

Consider a $(d-1)$-dimensional $\mathbb{F}_q$-subgeometry $\mathcal{C}_1$ of $\mathrm{PG}(d, q^{\varrho+1})$ and a $(d-2)$-dimensional $\mathbb{F}_q$-subgeometry $\mathcal{C}_2 \subset \mathcal{C}_1$. Define $\Sigma_i := \langle \mathcal{C}_i \rangle_{q^{\varrho+1}}$. Let $\mathcal{B}_1$ and $\mathcal{B}_2$ be two distinct d-dimensional $\mathbb{F}_q$-subgeometries, both containing $\mathcal{C}_1$ and a point $F \notin \Sigma_1$, and suppose that Π is a $(d-1)$-subspace through Σ_2 not equal to Σ_1 and not containing F. Then Π cannot intersect both $\mathcal{B}_1$ and $\mathcal{B}_2$ in a $(d-1)$-dimensional $\mathbb{F}_q$-subgeometry.

Proof. Suppose that the contrary is true. Choose a point $F' \in \mathcal{C}_1 \setminus \mathcal{C}_2$. Then the line $\langle F, F' \rangle_{q^{\varrho+1}}$ intersects Π in a point P. As Π intersects both $\mathcal{B}_1$ and $\mathcal{B}_2$ in an $\mathbb{F}_q$-subgeometry of maximal dimension, P has to be a point of both $\mathcal{B}_1$ and $\mathcal{B}_2$. Moreover, as both these subgeometries contain $\mathcal{C}_1 \ni F'$ and F, the unique $\mathbb{F}_q$-subline containing F, F' and P has to be contained in both $\mathcal{B}_1$ and $\mathcal{B}_2$. By Lemma 0.1.3, this would imply that $\mathcal{B}_1 = \mathcal{B}_2$, a contradiction. ∎

Lemma 10.2.4

Consider Configuration 10.2.2. Then the point set

$$\mathfrak{B}_{(d,\varrho)} := \mathfrak{P}'_1 \cup \bigcup_{j=1}^{\varrho+1} \mathfrak{P}_j$$

ϱ-saturates all points of $\mathrm{PG}(d, q^{\varrho+1})$ not contained in Σ_1.

Proof. Let P be an arbitrary point not contained in Σ_1 and let

$$\mu := \min\{|\mathcal{F}| \,:\, \mathcal{F} \subseteq \mathcal{F}_1, P \in \langle \tau \,:\, \tau \in \mathcal{F} \rangle\} \in \{1, 2, \ldots, \varrho+1\}.$$

Hence, there exists a subset $\mathcal{F}'_1 := \left\{\tau'_{11}, \tau'_{12}, \ldots, \tau'_{1\mu}\right\}$ of the $(d-\varrho)$-flower $\mathcal{F}_1$ with pistil Σ_1 such that P lies in the span of all petals of $\mathcal{F}'_1$ but does not lie in the span of any $\mu - 1$ petals of $\mathcal{F}'_1$.
For each petal τ'_{1j}, $j \in \{2, 3, \ldots, \mu-1\}$, only the points of $\mathfrak{B}_{(d,\varrho)}$ in the top layer ($i = 1$) of τ'_{1j} will be used to prove point saturation. As a consequence,

we can assume without loss of generality that $\tau'_{1j} = \tau_{1j}$ for every $j \in \{2, 3, \ldots, \mu - 1\}$. If $q > 2$, the same can be said about petal τ'_{11}. If $q = 2$, however, two possibilities can occur:

(i) either there exist at least two $(d - \varrho)$-dimensional $\mathbb{F}_q$-subgeometries $\mathcal{B}_1$ and $\mathcal{B}_2$ in τ'_{11}, both containing $\mathcal{C}_1$ and a point $F \in \tau'_{11} \setminus \Sigma_1$, such that $(\mathcal{B}_1 \cup \mathcal{B}_2) \setminus \mathcal{C}_1 \subset \mathfrak{B}_{(d,\varrho)}$, or

(ii) $\tau'_{11} = \tau_{11}$.

Note that for both (i) and (ii), there exists one $(d - \varrho)$-dimensional $\mathbb{F}_q$-subgeometry $\mathcal{B}$ in τ'_{11} containing $\mathcal{C}_1$ such that $\mathcal{B} \setminus \mathcal{C}_1 \subset \mathfrak{B}_{(d,\varrho)}$; this is the only property needed of petal τ'_{11} in Case 1, Case 2 and Case 3 (step (1) and (2)) below. Only in Case 3 (step (3)), a distinction between possibility (i) and (ii) has to be made. In light of this, we assume, for now, that $\tau'_{11} = \tau_{11}$, and remove this assumption in the third step of Case 3. Finally, we may assume that $\tau'_{1\mu} \in \left\{\tau_{1\mu}, \tau_{1(\mu+1)}, \ldots, \tau_{1(\varrho+1)}\right\}$, hence there has to exist a $j' \geqslant \mu$ such that $\tau'_{1\mu} = \tau_{1j'}$.
Hence, to recap, we assume that $\mathcal{F}'_1 = \left\{\tau_{11}, \tau_{12}, \ldots, \tau_{1(\mu-1)}, \tau_{1j'}\right\}$ for a certain $j' \geqslant \mu$.

If $\mu = \varrho + 1$, the proof follows immediately due to Lemma 10.1.2. We consider three cases, depending on the other possible values of μ.

Case 1: $\mu = 1$.

In this case, P is contained in τ_{11}, which is a $(d - \varrho)$-dimensional subspace containing $\mathcal{B}^{(1)}_{11} \setminus \mathcal{C}_1 \subset \mathfrak{B}_{(d,\varrho)}$. As the affine point set of $\mathrm{PG}(d - \varrho, q)$ is a strong $(d - \varrho)$-blocking set, Result 8.2.6 proves the claim.

Case 2: $1 < \mu \leqslant \varrho + 1 - \lambda$.

Note that the occurrence of this case implies that $\lambda = d - \varrho$.

Choose $d-\varrho+1$ points of $\mathcal{B}_{1j'}^{(1)} \setminus \mathcal{C}_1$ spanning the subspace $\tau_{1j'} \supset \Sigma_1$ and pick one point of each set $\mathcal{B}_{11}^{(1)} \setminus \mathcal{C}_1, \ldots, \mathcal{B}_{1(\mu-1)}^{(1)} \setminus \mathcal{C}_1$. These choices result in a total of $(d-\varrho+1)+(\mu-1) \leqslant (d-\varrho+1)+(\varrho-\lambda) = \varrho+1$ points spanning $\left\langle \tau_{11}, \tau_{12}, \ldots, \tau_{1(\mu-1)}, \tau_{1j'} \right\rangle \ni P$.

Case 3: $\varrho+1-\lambda < \mu \leqslant \varrho$.

Consider the following series of steps within 'layer' $i=2$.

(1) For every $j \in \{1,2,\ldots,\mu-1\} \cup \{j'\}$, define $\widetilde{\tau}_{2j} := \langle \Sigma_2, F_{1j} \rangle$ and consider, for every $k \in \{1,2,\ldots,j\}$, the $(d-\varrho-1)$-dimensional $\mathbb{F}_q$-subgeometry $\mathcal{A}_{2j}^{(k)} := \mathcal{B}_{1j}^{(k)} \cap \widetilde{\tau}_{2j}$. In this way, we obtain a union $\mathcal{A}_{2j}^{(1)} \cup \mathcal{A}_{2j}^{(2)} \cup \cdots \cup \mathcal{A}_{2j}^{(j)}$ of j independent $(d-\varrho-1)$-dimensional $\mathbb{F}_q$-subgeometries contained in the $(d-\varrho-1)$-dimensional subspace $\widetilde{\tau}_{2j}$ of τ_{1j}, each containing $\mathcal{C}_2$ and sharing the point F_{1j}.

(2) Consider the union $\mathcal{B}_{2j'}^{(1)} \cup \mathcal{B}_{2j'}^{(2)} \cup \cdots \cup \mathcal{B}_{2j'}^{\left(\lceil j' \rfloor^{(2)}\right)}$ consisting of $\lceil j' \rfloor^{(2)}$ independent $(d-\varrho-1)$-dimensional $\mathbb{F}_q$-subgeometries contained in the $(d-\varrho-1)$-dimensional subspace $\tau_{2j'} \neq \widetilde{\tau}_{2j'}$ of $\tau_{1j'}$, each containing $\mathcal{C}_2$ and sharing the point $F_{2j'}$. It is clear that $\tau_{2j'}$ and $\widetilde{\tau}_{2j'}$ span the subspace $\tau_{1j'}$, as these are distinct hyperplanes of the latter subspace.

(3) As described at the start of this proof, we remove the assumption that $\tau'_{11} = \tau_{11}$.

Note that $\left\langle \tau_{22}, \tau_{23}, \ldots, \tau_{2(\mu-1)}, \tau_{2j'} \right\rangle$ and $\left\langle \tau_{22}, \tau_{23}, \ldots, \tau_{2(\mu-1)}, \widetilde{\tau}_{2j'} \right\rangle$ both span hyperplanes of $\left\langle \tau'_{11}, \tau_{12}, \ldots, \tau_{1(\mu-1)}, \tau_{1j'} \right\rangle$ that do not contain τ'_{11}, hence each of these hyperplanes intersects τ'_{11} in a $(d-\varrho-1)$-subspace $\overline{\tau}_{21}$ and $\widetilde{\tau}_{21}$, respectively, both containing $\mathcal{C}_2$.

The goal is to find a subset of a $(d-\varrho-1)$-flower consisting of $\mu+1$ petals such that the jth petal contains j concurrent, independent

$(d-\varrho-1)$-dimensional $\mathbb{F}_q$-subgeometries contained in $\mathfrak{B}_{(d,\varrho)} \cup \mathcal{C}_2$, with the additional property that P lies in the span of these petals, but not in the span of any μ petals. It is clear that, if we can find a $(d-\varrho-1)$-subspace $\widehat{\tau}_{21} \notin \{\overline{\tau}_{21}, \widetilde{\tau}_{21}\}$ in τ'_{11}, not lying in Σ_1 and containing a $(d-\varrho-1)$-dimensional $\mathbb{F}_q$-subgeometry $\mathcal{B} \supset \mathcal{C}_2$, $\mathcal{B} \setminus \mathcal{C}_2 \subset \mathfrak{B}_{(d,\varrho)}$, then $\left\{\widehat{\tau}_{21}, \tau_{22}, \ldots, \tau_{2(\mu-1)}, \tau_{2j'}, \widetilde{\tau}_{2j'}\right\}$ is the subset we are looking for.

- If $q > 2$, then there exists a $(d-\varrho-1)$-dimensional subspace of $\mathcal{B}^{(1)}_{11}$ spanning a $(d-\varrho-1)$-subspace $\widehat{\tau}_{21}$ that contains Σ_2, but is not equal to Σ_1, $\overline{\tau}_{21}$ or $\widetilde{\tau}_{21}$.
- If $q = 2$, we distinguish the two possibilities described at the start of the proof:
  - (i) suppose that there exist at least two $(d-\varrho)$-dimensional $\mathbb{F}_q$-subgeometries $\mathcal{B}_1$ and $\mathcal{B}_2$ in τ'_{11}, both containing $\mathcal{C}_1$ and a point $F \in \tau'_{11} \setminus \Sigma_1$, such that $(\mathcal{B}_1 \cup \mathcal{B}_2) \setminus \mathcal{C}_1 \subset \mathfrak{B}_{(d,\varrho)}$. By Lemma 10.2.3, we find at least three $(d-\varrho-1)$-subspaces through Σ_2, not lying in Σ_1, that intersect either $\mathcal{B}_1$ or $\mathcal{B}_2$ in a $(d-\varrho-1)$-dimensional $\mathbb{F}_q$-subgeometry. Hence, one of these three $(d-\varrho-1)$-dimensional subspaces $\widehat{\tau}_{12}$ cannot be equal to $\overline{\tau}_{21}$ or $\widetilde{\tau}_{21}$.
  - (ii) if $\tau'_{11} = \tau_{11}$, then, by the definition of the set $\mathfrak{P}'_1$, we can always find a $(d-\varrho-1)$-dimensional subspace $\widehat{\tau}_{21}$ with the desired properties.

Intuitively, the steps above split the initial $(d-\varrho)$-subflower with μ petals into a $(d-\varrho-1)$-subflower with $\mu+1$ petals. For this new (sub)flower, the property that P is contained in the span of all of its petals, but not in the span of any fewer petals, still holds. We execute the steps above a total of $\varrho+1-\mu$ times, leaving us with a $(d-2\varrho+\mu-1)$-flower $\mathcal{F}'_{\varrho+2-\mu}$. Note that this is always possible, as by the assumption corresponding to this case, $\varrho+1-\mu \leqslant \lambda-1$, which means that, in each step, one can always

choose smaller petals containing subgeometries (see Configuration 10.2.2) which fulfil the desired conditions.
Moreover, for each $j \in \{1, \dots, \varrho+1\}$, there must exist a petal in $\mathcal{F}'_{\varrho+2-\mu}$ with j concurrent, independent $(d-2\varrho+\mu-1)$-dimensional $\mathbb{F}_q$-subgeometries contained in $\mathfrak{B}_{(d,\varrho)} \cup \mathcal{C}_1$. Indeed, let L_i be the tuple of numbers of concurrent, independent $(d-\varrho-i)$-dimensional $\mathbb{F}_q$-subgeometries we can find in the respective petals of the flower we obtain after going through the steps i times. Then, by considering the nature of the maps $\lceil \cdot \rfloor^{(\cdot)}$ (see Definition 10.2.1), we get

$$\begin{aligned}
L_0 &= (1, 2, \dots, \mu-1, j'), \\
L_1 &= (1, 2, \dots, \mu-1, j', j'+1), \\
L_2 &= (1, 2, \dots, \mu-1, j', j'+1, j'+2), \\
&\vdots \\
L_{\varrho+1-j'} &= (1, 2, \dots, \mu-1, j', j'+1, \dots, \varrho+1), \\
L_{\varrho-j'} &= (1, 2, \dots, \mu-1, j'-1, j', j'+1, \dots, \varrho+1), \\
&\vdots \\
L_{\varrho+1-\mu} &= (1, 2, \dots, \mu-1, \mu, \mu+1, \dots, j'-1, j', j'+1, \dots, \varrho+1).
\end{aligned}$$

Hence, Lemma 10.1.2 finishes the proof. ∎

10.2.3 Examining the size

Lemma 10.2.5

Consider Configuration 10.2.2. Then

$$|\mathfrak{P}'_1| = \begin{cases} (2^{\lambda-1}-1) \cdot 2^{d-\varrho-\lambda+1} & \text{if } q = 2, \\ 0 & \text{if } q \neq 2. \end{cases}$$

Lemma 10.2.6

Consider Configuration 10.2.2. Let $j \in \{1, \dots, \varrho+1\}$. If $j \leqslant \varrho+1-\lambda$, then

$$\left|\mathfrak{P}_j\right| = jq^{d-\varrho} - (j-1)\,.$$

If $j > \varrho+1-\lambda$, then one can choose $\mathfrak{P}_j$ in such a way that

$$\left|\mathfrak{P}_j\right| = jq^{d-\varrho} + \sum_{k=1}^{\varrho+1-j} (j-1+k)\, q^{d-\varrho-k} + \sum_{k=\varrho+2-j}^{\lambda-1} (\varrho-k)\, q^{d-\varrho-k} - \frac{\lambda\,(2\varrho-\lambda+1)}{2}.$$

Proof. If $j \leqslant \varrho+1-\lambda$, this result is easily obtained, as distinct elements of $\mathcal{L}_Y^{\tau_{1j}}$ can share at most one point of $\mathcal{P}_Y^{\tau_{1j}}$. Hence, assume that $j > \varrho+1-\lambda$. To minimise the size of $\mathfrak{P}_j$, we can choose $\mathcal{B}_{ij}^{(1)}$ to be a subspace of $\mathcal{B}_{(i-1)j}^{(1)}$, for every $i \in \{2, \dots, \lambda\}$. In this way, keeping the nature of $\lceil\cdot\rfloor^{(\cdot)}$ in mind (see Definition 10.2.1), we obtain the following:

$$\begin{aligned}
\left|\mathfrak{P}_j\right| = {} & jq^{d-\varrho} && -(j-1)\\
& + jq^{d-\varrho-1} && -j\\
& + (j+1)\, q^{d-\varrho-2} && -(j+1)\\
& \vdots && \vdots\\
& + \varrho q^{d-\varrho-(\varrho+1-j)} && -\varrho\\
& + (j-2)\, q^{d-\varrho-(\varrho+2-j)} && -(j-2)\\
& + (j-3)\, q^{d-\varrho-(\varrho+3-j)} && -(j-3)\\
& \vdots && \vdots\\
& + (\varrho+1-\lambda)\, q^{d-\varrho-(\lambda-1)} && -(\varrho+1-\lambda)\,.
\end{aligned}$$

Viewing the expression above as a polynomial in q, the corresponding

constant term equals

$$-\left((\varrho+1-\lambda)+\cdots+\varrho\right) = \frac{(\varrho-\lambda)(\varrho+1-\lambda)}{2} - \frac{\varrho(\varrho+1)}{2}$$
$$= -\frac{\lambda(2\varrho-\lambda+1)}{2}.$$

Lemma 10.2.7

Consider Configuration 10.2.2. One can choose $\mathfrak{P}_1,\dots,\mathfrak{P}_{\varrho+1}$ in such a way that

$$\sum_{i=1}^{\varrho+1}|\mathfrak{P}_i| = \frac{(\varrho+1)(\varrho+2)}{2}q^{d-\varrho} + \sum_{j=1}^{\lambda-1} a(d,\varrho,j)\,q^{d-\varrho-j} - c(d,\varrho),$$

with

$$a(d,\varrho,j) := \frac{\lambda(2\varrho-\lambda+2j+1) - j(3j+1)}{2}$$

and

$$c(d,\varrho) := \frac{\varrho(\varrho+1)+\lambda(\lambda-1)(2\varrho-\lambda+1)}{2}.$$

Proof. Let $\mathfrak{P}_1,\dots,\mathfrak{P}_{\varrho+1}$ be sets of size equal to the values described in Lemma 10.2.6. Interpret $\sum_{i=1}^{\varrho+1}|\mathfrak{P}_i|$ as a polynomial in q of degree $d-\varrho$; let $a(d,\varrho,j)$ be the coefficient corresponding to $q^{d-\varrho-j}$ ($j\in\{0,1,\dots,d-\varrho-1\}$) and let $-c(d,\varrho)$ be the constant term.
It is clear that $a(d,\varrho,0) = \sum_{i=1}^{\varrho+1} i = \frac{(\varrho+1)(\varrho+2)}{2}$. Furthermore, we can deduce that

$$a(d,\varrho,j) = \underbrace{(\varrho+j+1-\lambda)+(\varrho+j+2-\lambda)+\cdots+(\varrho)}_{\text{from }\mathfrak{P}_{\varrho+2-\lambda},\mathfrak{P}_{\varrho+3-\lambda},\dots,\mathfrak{P}_{\varrho+1-j}} + \underbrace{j(\varrho-j)}_{\text{from }\mathfrak{P}_{\varrho+2-j},\dots,\mathfrak{P}_{\varrho+1}}$$
$$= \frac{\lambda(2\varrho-\lambda+2j+1) - j(3j+1)}{2},$$

if $j \in \{1, 2, \ldots, \lambda - 1\}$ and that $a(d, \varrho, j) = 0$ if $j \in \{\lambda, \lambda + 1, \ldots, d - \varrho - 1\}$. Furthermore, we have that

$$\begin{aligned} -c(d,\varrho) &= \underbrace{-1-2-3-\cdots-(\varrho-\lambda)}_{\text{from } \mathfrak{P}_2, \mathfrak{P}_3, \ldots, \mathfrak{P}_{\varrho+1-\lambda}} + \underbrace{\lambda\left(-\frac{\lambda\,(2\varrho-\lambda+1)}{2}\right)}_{\text{from } \mathfrak{P}_{\varrho+2-\lambda}, \mathfrak{P}_{\varrho+3-\lambda}, \ldots, \mathfrak{P}_{\varrho+1}} \\ &= -\frac{\varrho\,(\varrho+1) + \lambda\,(\lambda-1)\,(2\varrho-\lambda+1)}{2}. \end{aligned}$$

10.3 Reaping the rewards

Theorem 10.3.1

Let $\varrho \in \{0, 1, \ldots, d\}$ such that $\varrho + 1 \nmid d + 1$. Then

$$\begin{aligned} s_{q^{\varrho+1}}(d,\varrho) \leqslant & \sum_{i=1}^{m(d,\varrho)} \left(\frac{(\varrho+1)\,(\varrho+2)}{2} q^{d+1-i(\varrho+1)}\right) \\ & + \sum_{i=1}^{m(d,\varrho)-1} \sum_{j=1}^{\varrho-1} \widetilde{a}(\varrho, j)\, q^{d+1-i(\varrho+1)-j} \\ & + \sum_{j=1}^{\ell(d,\varrho)-1} \overline{a}(d,\varrho,j)\, q^{\ell(d,\varrho)-j} - \widetilde{c}(d,\varrho) - \overline{c}(d,\varrho) \\ & + \delta_{q=2}\left(\left(2^{\varrho-1}-1\right) \sum_{i=1}^{m(d,\varrho)-1} \left(2^{d-\varrho+2-i(\varrho+1)}\right) + 2^{\ell(d,\varrho)} - 2\right), \end{aligned}$$

with

- $m(d,\varrho) \coloneqq \left\lceil \frac{d-\varrho}{\varrho+1} \right\rceil$,
- $\ell(d,\varrho) \coloneqq d + 1 - m(d,\varrho) \cdot (\varrho+1) = (d \pmod{\varrho+1}) + 1$,
- $\widetilde{a}(\varrho, j) \coloneqq \frac{\varrho(\varrho+2j+1) - j(3j+1)}{2} \leqslant \frac{\varrho(2\varrho+1)}{3}$,

- $\overline{a}(d,\varrho,j) := \frac{\ell(d,\varrho)(2\varrho-\ell(d,\varrho)+2j+1)-j(3j+1)}{2} \leqslant \widetilde{a}(\varrho,j)$,
- $\widetilde{c}(d,\varrho) := (m(d,\varrho)-1)\,\frac{\varrho^2(\varrho+1)}{2} \geqslant 0$,
- $\overline{c}(d,\varrho) := \frac{\varrho(\varrho+1)+\ell(d,\varrho)(\ell(d,\varrho)-1)(2\varrho-\ell(d,\varrho)+1)}{2} \geqslant 0$,
- $\delta_{q=2} := \begin{cases} 1 & \text{if } q=2, \\ 0 & \text{if } q\neq 2. \end{cases}$

Proof. By Lemma 10.2.4, we can choose a point set $\mathfrak{B}_{(d,\varrho)}$ in $\mathrm{PG}\left(d,q^{\varrho+1}\right)$ (described in Configuration 10.2.2) which ϱ-saturates all points of $\mathrm{PG}\left(d,q^{\varrho+1}\right)$, except for the points contained in a certain $(d-\varrho-1)$-subspace Σ.
If $d-\varrho-1 \leqslant \varrho$, then $d-\varrho-1 < \varrho$, as else $d+1$ would be a multiple of $\varrho+1$. Hence, in this case, all points of Σ are ϱ-saturated by $\mathfrak{B}_{(d,\varrho)}$ as well, as we can simply choose $\varrho+1$ points in $\mathfrak{P}_1$ that span the subspace $\tau_{11} \supset \Sigma$.
If $d-\varrho-1 > \varrho$, then, by Lemma 10.2.4, we can choose a point set $\mathfrak{B}_{(d-(\varrho+1),\varrho)}$ in Σ which ϱ-saturates all points of Σ, except for the points contained in a certain $(d-2(\varrho+1))$-subspace of Σ. We can repeat this process to obtain a union

$$\mathfrak{B}_{(d,\varrho)} \cup \mathfrak{B}_{(d-(\varrho+1),\varrho)} \cup \cdots \cup \mathfrak{B}_{(d-(m(d,\varrho)-1)(\varrho+1),\varrho)}$$

of $m(d,\varrho)$ point sets that ϱ-saturates all points of $\mathrm{PG}\left(d,q^{\varrho+1}\right)$. One only needs to determine the size of this particular ϱ-saturating set.
For each $i \in \{1,2,\ldots,m(d,\varrho)\}$, the size of the point set $\mathfrak{B}_{(d-(i-1)(\varrho+1),\varrho)}$ can be calculated using Lemma 10.2.5 and Lemma 10.2.7, where every instance of d has to be replaced by $d-(i-1)(\varrho+1)$, hence every instance of λ has to be replaced by $\lambda_i := \min\{\varrho, d-(i-1)(\varrho+1)-\varrho\}$.

- If $i \in \{1,2,\ldots,m(d,\varrho)-1\}$, then $\varrho < d-(i-1)(\varrho+1)-\varrho$, which implies that $\lambda_i = \varrho$.
- If $i = m(d,\varrho)$, then $\varrho \geqslant d-(m(d,\varrho)-1)(\varrho+1)-\varrho$ (keeping in mind that $d+1$ is no multiple of $\varrho+1$), which implies that $\lambda_{m(d,\varrho)} = \ell(d,\varrho)$.

Finally, we claim that $\overline{a}(d,\varrho,j) \leqslant \widetilde{a}(\varrho,j) \leqslant \frac{\varrho(2\varrho+1)}{3}$, for all $j \in \{1,\ldots,\varrho\}$. Indeed, for the first inequality, one can interpret $\frac{\ell(d,\varrho)(2\varrho-\ell(d,\varrho))}{2}$ as a quadratic polynomial in $\ell(d,\varrho)$, which reaches its maximum value if $\ell(d,\varrho)=\varrho$. For the second inequality, one can interpret $\widetilde{a}(\varrho,j)$ as a quadratic polynomial in j, which reaches its maximum value if $j=\frac{2\varrho-1}{6}$. However, the latter is never an integer. Hence, one can conclude that

$$\widetilde{a}(\varrho,j) \leqslant \max\left\{a\left(\varrho,\frac{2\varrho-1}{6}-\frac{1}{6}\right),a\left(\varrho,\frac{2\varrho-1}{6}+\frac{1}{6}\right)\right\} = \frac{\varrho\,(2\varrho+1)}{3},$$

for all $j \in \{1,\ldots,\varrho\}$. ∎

Remark 10.3.2

Theorem 10.3.1's condition that $\varrho+1 \nmid d+1$ can be omitted, as one can prove that Corollary 8.2.5 directly implies the described upper bound on $s_{q^{\varrho+1}}(d,\varrho)$ (see [61, Theorem 7.2.9]).

As the upper bound presented in Theorem 10.3.1 is not easy to work with in practice, a simplified upper bound is desired. If ϱ is large enough, the upper bound of Theorem 10.3.1 simplifies considerably. More precisely, if $\varrho \geqslant \frac{d-1}{2}$, then $m(d,\varrho)=1$ and $\ell(d,\varrho)=d-\varrho$, hence the bound of Theorem 10.3.1 becomes the following:

$$s_{q^{\varrho+1}}(d,\varrho) \leqslant \frac{(\varrho+1)\,(\varrho+2)}{2}q^{d-\varrho} + \sum_{j=1}^{d-\varrho-1}\overline{a}(d,\varrho,j)\,q^{d-\varrho-j} - \overline{c}(d,\varrho) + \delta_{q=2}\cdot\left(2^{d-\varrho}-2\right).$$

In case $\varrho > 1$, one can deduce from Theorem 10.3.1 the following easy-to-read but slightly weaker bound, which is considered the main result.

Theorem 10.3.3

Let $\varrho \in \{2, 3, \ldots, d-1\}$ such that $\varrho + 1 \nmid d + 1$. Then

$$s_{q^{\varrho+1}}(d, \varrho) \leqslant \frac{(\varrho+1)(\varrho+2)}{2} q^{d-\varrho} + \varrho(\varrho+1)\frac{q^{d-\varrho}-1}{q-1}.$$

Translating the result above in coding theoretical terminology (see Section 8.1), one obtains the following.

Corollary 10.3.4

Let $R \in \{3, 4, \ldots, r-1\}$ such that $R \nmid r$. Then

$$\ell_{q^R}(r, R) \leqslant \frac{R(R+1)}{2} q^{r-R} + (R-1)R\frac{q^{r-R}-1}{q-1}.$$

A English summary

This thesis is split into three main parts. In Part I, we discuss **characterisation** results concerning small weight codewords of projective geometric codes, while in Parts II and III, we focus on **construction** results related to minimal codes and covering codes, respectively. Various finite geometries form the toolkit used to obtain these coding-theoretical results.

In Part I, we consider projective geometric codes arising from the incidence of points and hyperplanes of a projective geometry. Over the span of several years, numerous mathematicians worked towards determining the weight spectrum of such codes. Characterising the codewords of relatively small weight is commonly accepted to be a natural place to start.
We essentially generalise planar results to arbitrary dimension d. A distinction needs to be made whether the order of the underlying field q is prime, as the existence of odd codewords complicates the characterisation quest considerably. If q is prime, all codewords up to weight roughly $4q^{d-1}$ are successfully characterised. If q is not prime, we characterise all codewords up to weight roughly $q^{d-1}\sqrt{q}$.
Finally, using both old and new characterisation results, we determine a graph-theoretical sufficient condition to determine which small weight codewords are minimal.

We take a completely different track in Part II. A known one-to-one correspondence between minimal codes and strong blocking sets justifies the search for certain subspaces in *higgledy-piggledy arrangement*.

We focus on higgledy-piggledy sets in projective geometries of dimension at most 5 and describe which of these are deemed to be theoretically optimal. Known existence results are then listed and extended. Two open problems concerning the existence of a particular line and plane set are solved.
We first show the existence of six lines of $\mathrm{PG}(4,q)$ in higgledy-piggledy arrangement, two of which intersect in a point. The arguments leading up to this result are extensive but of pure geometric nature. We then constructively prove the existence of seven planes of $\mathrm{PG}(5,q)$ in higgledy-piggledy arrangement. By carefully characterising the André/Bruck-Bose representation of $\mathbb{F}_q$-linear sets living on the projective line, a particular point set of $\mathrm{PG}\left(1,q^3\right)$ is selected, which eventually, using field reduction, gives rise to the desired higgledy-piggledy plane set.

Part III is of the same nature as its predecessor. We search for small saturating sets, as such structures imply the existence of short covering codes.
First, an isomorphism is determined between particular point-line geometries which involve projective subgeometries. As one of these point-line geometries is embedded in an affine geometry, notions of parallelism and affine subspaces are transcribed to $\mathbb{F}_q$-subgeometries. This sheds more light on the intricate interplay between subgeometries that share a (subgeometric) hyperplane.
Subsequently, we exploit these insights to describe a tricky construction of so-called *flowers*, which contain a number of well-chosen $\mathbb{F}_q$-subgeometries. We prove that this floral construction turns out to be a ϱ-saturating set of $\mathrm{PG}\left(d,q^{\varrho+1}\right)$ of size roughly $\frac{1}{2}\varrho^2\cdot q^{d-\varrho}$, which is relatively close to the theoretical lower bound of roughly $\varrho\cdot q^{d-\varrho}$.

B Nederlandstalige samenvatting

Dit proefschrift bestaat uit drie delen. In Deel I bespreken we **karakterisatie**resultaten rond codewoorden van projectief-meetkundige codes van klein gewicht, terwijl we ons in Delen II en III concentreren op **constructie**resultaten gerelateerd aan minimale codes, respectievelijk bedekkingscodes. Diverse eindige meetkundes vormen de gereedschapskist die gebruikt wordt om deze codeertheoretische resultaten te bekomen.

In Deel I beschouwen we projectief-meetkundige codes die voortkomen uit de incidentie van punten en hypervlakken van een projectieve meetkunde. Gedurende verschillende jaren hebben talrijke wiskundigen gewerkt aan het bepalen van het gewichtsspectrum van dergelijke codes. Het karakteriseren van de codewoorden van relatief klein gewicht wordt algemeen beschouwd als een natuurlijk beginpunt.
In essentie veralgemenen we resultaten in het vlak naar algemene dimensie d. Het is nodig onderscheid te maken of de orde van het onderliggend veld q priem is, gezien het bestaan van bizarre codewoorden de tocht naar karakterisatie merkbaar bemoeilijkt. Als q priem is, zijn alle codewoorden tot en met gewicht ruwweg $4q^{d-1}$ succesvol gekarakteriseerd. Als q niet priem is, karakteriseren we alle codewoorden tot een gewicht van ruwweg $q^{d-1}\sqrt{q}$.
Tenslotte bepalen we met behulp van oude en nieuwe karakterisatieresultaten een graaftheoretische voldoende voorwaarde om te bepalen welke codewoorden van klein gewicht minimaal zijn.

In Deel II gooien we het over een volledig andere boeg. Een gekende

één-op-één-correspondentie tussen minimale codes en sterke blokkerende verzamelingen rechtvaardigt de zoektocht naar bepaalde deelruimten in *higgledy-piggledy-opstelling*.
We concentreren ons op higgledy-piggledy-verzamelingen in projectieve meetkundes van dimensie ten hoogste 5 en beschrijven welke hiervan theoretisch worden bestempeld als optimaal. Gekende bestaansresultaten worden vervolgens opgesomd en uitgebreid. Twee open problemen rond het bestaan van een specifieke rechten- en vlakkenverzameling worden opgelost.
Eerst tonen we het bestaan van zes rechten van $\mathrm{PG}(4,q)$ in higgledy-piggledy-opstelling aan, waarvan er twee elkaar snijden in een punt. De argumenten die tot dit resultaat leiden zijn uitgebreid, maar van zuiver meetkundige aard. Vervolgens bewijzen we constructief het bestaan van zeven vlakken van $\mathrm{PG}(5,q)$ in higgledy-piggledy-opstelling. Door middel van de André/Bruck-Bose-representatie van $\mathbb{F}_q$-lineaire verzamelingen op de projectieve rechte zorgvuldig te karakteriseren, kunnen we een specifieke puntenverzameling van $\mathrm{PG}\left(1,q^3\right)$ selecteren, die uiteindelijk via veldreductie leidt tot de gewenste higgledy-piggledy-vlakkenverzameling.

Deel III is van dezelfde aard als haar voorganger. We gaan op zoek naar kleine verzadigende verzamelingen, gezien dergelijke structuren leiden tot het bestaan van korte bedekkingscodes.
Eerst wordt er een isomorfisme bepaald tussen specifieke punt-rechte-meetkundes die te maken hebben met projectieve deelmeetkundes. Gezien een van deze punt-rechte-meetkundes is ingebed in een affiene meetkunde, worden begrippen als parallellisme en affiene deelruimten vertaald naar deelmeetkundes. Dit werpt meer licht op de delicate wisselwerking tussen deelmeetkundes die een (deelmeetkundig) hypervlak gemeen hebben.
Vervolgens gebruiken we deze inzichten om een complexe constructie bestaande uit zogenaamde *bloemen* te beschrijven, die een aantal goedgekozen $\mathbb{F}_q$-deelmeetkundes bevatten. We bewijzen dat deze bloemenconstructie een ϱ-verzadigende verzameling van $\mathrm{PG}\left(d,q^{\varrho+1}\right)$ blijkt te zijn, waarvan de grootte ruwweg gelijk is aan $\frac{1}{2}\varrho^2\cdot q^{d-\varrho}$, wat relatief dicht ligt bij de theoretische ondergrens van ruwweg $\varrho\cdot q^{d-\varrho}$.

Bibliography

[1] S. Adriaensen. 'A Note on Small Weight Codewords of Projective Geometric Codes and on the Smallest Sets of Even Type'. *SIAM J. Discrete Math.* 37.3 (2023), pp. 2072–2087 (on page 40).

[2] S. Adriaensen and **L. Denaux**. 'Small weight codewords of projective geometric codes'. *J. Combin. Theory Ser. A* 180 (2021), Paper No. 105395, 34 (on pages 29, 40, 45).

[3] S. Adriaensen, **L. Denaux**, L. Storme and Zs. Weiner. 'Small weight code words arising from the incidence of points and hyperplanes in $\mathrm{PG}(n, q)$'. *Des. Codes Cryptogr.* 88.4 (2020), pp. 771–788 (on pages 40, 59).

[4] A. Aguglia and G. Korchmáros. 'Blocking sets of external lines to a conic in $\mathrm{PG}(2, q)$, q odd'. *Combinatorica* 26.4 (2006), pp. 379–394 (on page 96).

[5] R. W. Ahrens and G. Szekeres. 'On a combinatorial generalization of 27 lines associated with a cubic surface'. *J. Austral. Math. Soc.* 10 (1969), pp. 485–492 (on page 141).

[6] G. N. Alfarano, M. Borello and A. Neri. 'A geometric characterization of minimal codes and their asymptotic performance'. *Adv. in Math. of Commun.* 16.1 (2022), pp. 115–133 (on pages 84, 104).

[7] G. N. Alfarano, M. Borello and A. Neri. *Outer Strong Blocking Sets*. 2023. arXiv: 2301.09590 [math.CO] (on page 93).

[8] G. N. Alfarano, M. Borello, A. Neri and A. Ravagnani. 'Three combinatorial perspectives on minimal codes'. *SIAM J. Discrete Math.* 36.1 (2022), pp. 461–489 (on pages 93, 104).

[9] J. André. 'Über nicht-Desarguessche Ebenen mit transitiver Translationsgruppe'. *Math. Z.* 60 (1954), pp. 156–186 (on page 115).

[10] A. Ashikhmin and A. Barg. 'Minimal vectors in linear codes'. *IEEE Trans. Inform. Theory* 44.5 (1998), pp. 2010–2017 (on page 31).

[11] E. F. Assmus Jr. and J. D. Key. *Designs and their codes*. Vol. 103. Cambridge Tracts in Mathematics. Cambridge University Press, Cambridge, 1992, pp. x+352 (on pages 27, 28, 36).

[12] L. Bader and G. Lunardon. 'Desarguesian spreads'. *Ric. Mat.* 60.1 (2011), pp. 15–37 (on page 141).

[13] B. Bagchi. 'On characterizing designs by their codes'. In: *Buildings, finite geometries and groups*. Vol. 10. Springer Proc. Math. Springer, New York, 2012, pp. 1–14 (on page 37).

[14] B. Bagchi. *The fourth smallest Hamming weight in the code of the projective plane over $\mathbb{Z}/p\mathbb{Z}$*. 2017. arXiv: 1712.07391 [math.CO] (on pages 36, 38).

[15] B. Bagchi and S. P. Inamdar. 'Projective geometric codes'. *J. Combin. Theory Ser. A* 99.1 (2002), pp. 128–142 (on pages 28, 36, 40).

[16] R. D. Baker, J. M. N. Brown, G. L. Ebert and J. C. Fisher. 'Projective bundles'. In: vol. 1. 3. A tribute to J. A. Thas (Gent, 1994). 1994, pp. 329–336 (on page 107).

[17] J. Bamberg, A. Betten, P. Cara, J. De Beule, M. Lavrauw, M. Neunhoeffer and M. Horn. *FinInG, Finite Incidence Geometry, Version 1.5.6*. https://gap-packages.github.io/FinInG. Refereed GAP package. July 2023 (on pages 101, 106).

[18] D. Bartoli and M. Bonini. 'Minimal linear codes in odd characteristic'. *IEEE Trans. Inform. Theory* 65.7 (2019), pp. 4152–4155 (on page 31).

[19] D. Bartoli, A. Cossidente, G. Marino and F. Pavese. 'On cutting blocking sets and their codes'. *Forum Math.* 34.2 (2022), pp. 347–368 (on pages 88, 93, 104).

[20] D. Bartoli, A. A. Davydov, M. Giulietti, S. Marcugini and F. Pambianco. 'New bounds for linear codes of covering radii 2 and 3'. *Cryptogr. Commun.* 11.5 (2019), pp. 903–920 (on pages 131, 133).

[21] D. Bartoli, A. A. Davydov, M. Giulietti, S. Marcugini and F. Pambianco. 'New bounds for linear codes of covering radius 2'. In: *Coding theory and applications*. Vol. 10495. Lecture Notes in Comput. Sci. Springer, Cham, 2017, pp. 1–10 (on pages 131, 133).

[22] D. Bartoli, A. A. Davydov, S. Marcugini and F. Pambianco. *Tables, bounds and graphics of short linear codes with covering radius* 3 *and codimension* 4 *and* 5. 2017. arXiv: 1712.07078 [cs.IT] (on pages 131, 133).

[23] D. Bartoli and **L. Denaux**. 'Minimal codewords arising from the incidence of points and hyperplanes in projective spaces'. *Adv. Math. Commun.* 17.1 (2023), pp. 56–77 (on pages 41, 71).

[24] D. Bartoli, Gy. Kiss, S. Marcugini and F. Pambianco. 'Resolving sets for higher dimensional projective spaces'. *Finite Fields Appl.* 67 (2020), pp. 101723, 14 (on pages 88, 95, 104).

[25] S. Barwick and G. Ebert. *Unitals in projective planes*. Springer Monographs in Mathematics. Springer, New York, 2008, pp. xii+193 (on page 7).

[26] S. G. Barwick, L. R. A. Casse and C. T. Quinn. 'The André/Bruck and Bose representation in PG$(2h, q)$: unitals and Baer subplanes'. *Bull. Belg. Math. Soc. Simon Stevin* 7.2 (2000), pp. 173–197 (on page 115).

[27] E. R. Berlekamp, R. J. McEliece and H. C. A. van Tilborg. 'On the inherent intractability of certain coding problems'. *IEEE Trans. Inform. Theory* IT-24.3 (1978), pp. 384–386 (on page 31).

[28] A. Bichara, F. Mazzocca and C. Somma. 'On the classification of generalized quadrangles in a finite affine space $AG(3, 2^h)$'. *Boll. Un. Mat. Ital. B (5)* 17.1 (1980), pp. 298–307 (on page 141).

[29] G. R. Blakley. 'Safeguarding cryptographic keys'. In: 1979, pp. 313–318 (on page 30).

[30] A. Blokhuis, A. Brouwer and H. Wilbrink. 'Hermitian unitals are code words'. *Discrete Math.* 97.1-3 (1991), pp. 63–68 (on page 37).

[31] M. Bonini and M. Borello. 'Minimal linear codes arising from blocking sets'. *J. Algebraic Combin.* 53.2 (2021), pp. 327–341 (on pages 31, 84).

[32] R. C. Bose and R. C. Burton. 'A characterization of flat spaces in a finite geometry and the uniqueness of the Hamming and the MacDonald codes'. *J. Combinatorial Theory* 1 (1966), pp. 96–104 (on page 84).

[33] A. E. Brouwer, A. M. Cohen and A. Neumaier. *Distance-regular graphs*. Vol. 18. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]. Springer-Verlag, Berlin, 1989, pp. xviii+495 (on page 151).

[34] R. A. Brualdi, S. Litsyn and V. S. Pless. 'Covering radius'. In: *Handbook of coding theory, Vol. I, II*. North-Holland, Amsterdam, 1998, pp. 755–826 (on page 131).

[35] J. Bruck and M. Naor. 'The hardness of decoding linear codes with preprocessing'. *IEEE Trans. Inform. Theory* 36.2 (1990), pp. 381–385 (on page 31).

[36] R. H. Bruck and R. C. Bose. 'The construction of translation planes from projective spaces'. *J. Algebra* 1 (1964), pp. 85–102 (on page 115).

[37] A. A. Bruen. 'Intersection of Baer subgeometries'. *Arch. Math. (Basel)* 39.3 (1982), pp. 285–288 (on page 7).

[38] Ph. Cara, S. Rottey and G. Van de Voorde. 'The isomorphism problem for linear representations and their graphs'. *Adv. Geom.* 14.2 (2014), pp. 353–367 (on page 141).

[39] L. R. A. Casse and C. M. O'Keefe. 'Indicator sets for t-spreads of $\mathrm{PG}((s+1)(t+1)-1,\ q)$'. *Boll. Un. Mat. Ital. B (7)* 4.1 (1990), pp. 13–33 (on pages 20, 21).

[40] H. Chabanne, G. Cohen and A. Patey. 'Towards secure two-party computation from the wire-tap channel'. In: *Information security and cryptology—ICISC 2013*. Vol. 8565. Lecture Notes in Comput. Sci. Springer, Cham, 2014, pp. 34–46 (on page 31).

[41] K. Chouinard. 'Weight Distributions of Codes from Finite Planes'. PhD thesis. University of Virginia, 2000 (on pages 36, 38).

[42] G. Cohen, I. Honkala, S. Litsyn and A. Lobstein. *Covering codes*. Vol. 54. North-Holland Mathematical Library. North-Holland Publishing Co., Amsterdam, 1997, pp. xxii+542 (on page 131).

[43] G. D. Cohen, S. Mesnager and A. Patey. 'On minimal and quasi-minimal linear codes'. In: *Cryptography and coding*. Vol. 8308. Lecture Notes in Comput. Sci. Springer, Heidelberg, 2013, pp. 85–98 (on page 31).

[44] A. A. Davydov. 'Constructions and families of covering codes and saturated sets of points in projective geometry'. *IEEE Trans. Inform. Theory* 41.6, part 2 (1995), pp. 2071–2080 (on pages 134, 135, 138).

[45] A. A. Davydov. 'Constructions and families of nonbinary linear codes with covering radius 2'. *IEEE Trans. Inform. Theory* 45.5 (1999), pp. 1679–1686 (on pages 135, 138).

[46] A. A. Davydov, M. Giulietti, S. Marcugini and F. Pambianco. 'Linear nonbinary covering codes and saturating sets in projective spaces'. *Adv. Math. Commun.* 5.1 (2011), pp. 119–147 (on pages 31, 84, 85, 88, 131, 134–137).

[47] A. A. Davydov, S. Marcugini and F. Pambianco. 'Bounds for Complete Arcs in $\mathrm{PG}(3,q)$ and Covering Codes of Radius 3, Codimension 4, Under a Certain Probabilistic Conjecture'. In: *Computational Science and Its Applications – ICCSA 2020*. Cham: Springer International Publishing, 2020, pp. 107–122 (on page 133).

[48] A. A. Davydov, S. Marcugini and F. Pambianco. 'New bounds for linear codes of covering radius 3 and 2-saturating sets in projective spaces'. In: *2019 XVI International Symposium "Problems of Redundancy in Information and Control Systems" (REDUNDANCY)*. 2019, pp. 52–57 (on pages 131, 133).

[49] A. A. Davydov, S. Marcugini and F. Pambianco. 'New covering codes of radius R, codimension tR and $tR + \frac{R}{2}$, and saturating sets in projective spaces'. *Des. Codes Cryptogr.* 87.12 (2019), pp. 2771–2792 (on pages 131, 135, 138).

[50] A. A. Davydov, S. Marcugini and F. Pambianco. 'Upper bounds on the length function for covering codes with covering radius R and codimension $tR + 1$'. *Adv. Math. Commun.* 17.1 (2023), pp. 98–118 (on page 133).

[51] A. A. Davydov and P. R. J. Östergård. 'On saturating sets in small projective geometries'. *European J. Combin.* 21.5 (2000), pp. 563–570 (on pages 87, 134).

[52] J. De Beule and L. Storme, eds. *Current research topics in Galois geometry*. Mathematics Research Developments. Nova Science Publisher, Jan. 2012 (on page 83).

[53] M. De Boeck. 'Intersection problems in finite geometries'. PhD thesis. Ghent University, 2014 (on pages 37, 38).

[54] M. De Boeck and P. Vandendriessche. 'On a Peculiar Weighted Sum of Lines'. *Submitted* (2020) (on page 37).

[55] F. De Clerck. 'Een kombinatorische studie van de eindige partiële meetkunden'. PhD thesis. Ghent University, 1978 (on page 141).

[56] S. De Winter. 'Non-isomorphic semipartial geometries'. *Des. Codes Cryptogr.* 47.1-3 (2008), pp. 3–9 (on page 141).

[57] S. De Winter, S. Rottey and G. Van de Voorde. 'Linear representations of subgeometries'. *Des. Codes Cryptogr.* 77.1 (2015), pp. 203–215 (on pages 140–142).

[58] I. Debroey. 'Semi-partiële meetkunden'. PhD thesis. Ghent University, 1978 (on page 141).

[59] P. Delsarte. 'On cyclic codes that are invariant under the general linear group'. *IEEE Trans. Inform. Theory* IT-16 (1970), pp. 760–769 (on page 28).

[60] P. Delsarte, J. M. Goethals and F. J. MacWilliams. 'On generalized Reed-Muller codes and their relatives'. *Information and Control* 16 (1970), pp. 403–442 (on pages 28, 36).

[61] **L. Denaux**. 'Constructing saturating sets in projective spaces using subgeometries'. *Des. Codes Cryptogr.* 90.9 (2022), pp. 2113–2144 (on pages 129, 131, 139, 163, 179).

[62] **L. Denaux**. 'Higgledy-piggledy sets in projective spaces of small dimension'. *Electron. J. Combin.* 29.3 (2022), Paper No. 3.29, 25 (on pages 83, 95, 106).

[63] **L. Denaux**. *Two disguises of the linear representation of a subgeometry*. 2021. arXiv: 2112.12452 [math.CO] (on pages 129, 139).

[64] **L. Denaux**, J. D'haeseleer and G. Van de Voorde. 'A higgledy-piggledy set of planes based on the ABB-representation of linear sets'. *Discrete Math.* 346.12 (2023), Paper No. 113603 (on pages 83, 105).

[65] C. Ding, Z. Heng and Z. Zhou. 'Minimal binary linear codes'. *IEEE Trans. Inform. Theory* 64.10 (2018), pp. 6536–6545 (on page 31).

[66] V. Fack, Sz. L. Fancsali, L. Storme, G. Van de Voorde and J. Winne. 'Small weight codewords in the codes arising from Desarguesian projective planes'. *Des. Codes Cryptogr.* 46.1 (2008), pp. 25–43 (on pages 28, 36).

[67] G. Faina, Gy. Kiss, S. Marcugini and F. Pambianco. 'The cyclic model for PG(n, q) and a construction of arcs'. *European J. Combin.* 23.1 (2002), pp. 31–35 (on pages 108, 109).

[68] Sz. L. Fancsali and P. Sziklai. 'Higgledy-piggledy subspaces and uniform subspace designs'. *Des. Codes Cryptogr.* 79.3 (2016), pp. 625–645 (on pages 85–87, 92, 137).

[69] Sz. L. Fancsali and P. Sziklai. 'Lines in higgledy-piggledy arrangement'. *Electron. J. Combin.* 21.2 (2014), Paper 2.56, 15 (on pages 84–88, 104, 137).

[70] *GAP – Groups, Algorithms, and Programming, Version 4.12.2*. The GAP Group. 2022 (on pages 101, 106).

[71] M. Giulietti. 'Blocking sets of external lines to a conic in $\mathrm{PG}(2,q)$, q even'. *European J. Combin.* 28.1 (2007), pp. 36–42 (on page 96).

[72] D. G. Glynn. 'Finite projective planes and related combinatorial systems'. PhD thesis. University of Adelaide, 1978 (on pages 107, 108).

[73] T. Grundhöfer, M. Joswig and M. Stroppel. 'Slanted symplectic quadrangles'. *Geom. Dedicata* 49.2 (1994), pp. 143–154 (on page 141).

[74] M. Hall Jr. 'Affine generalized quadrilaterals'. In: *Studies in Pure Mathematics (Presented to Richard Rado)*. Academic Press, London, 1971, pp. 113–116 (on page 141).

[75] N. Hamada. 'The rank of the incidence matrix of points and d-flats in finite geometries'. *J. Sci. Hiroshima Univ. Ser. A-I Math.* 32 (1968), pp. 381–396 (on page 29).

[76] J. Harris. *Algebraic geometry*. Vol. 133. Graduate Texts in Mathematics. A first course, Corrected reprint of the 1992 original. Springer-Verlag, New York, 1995, pp. xx+328 (on pages 17, 110).

[77] T. Héger and Z. L. Nagy. 'Short minimal codes and covering codes via strong blocking sets in projective spaces'. *IEEE Trans. Inform. Theory* 68.2 (2022), pp. 881–890 (on pages 84, 86, 87).

[78] T. Héger, B. Patkós and M. Takáts. 'Search problems in vector spaces'. *Des. Codes Cryptogr.* 76.2 (2015), pp. 207–216 (on page 85).

[79] Z. Heng, C. Ding and Z. Zhou. 'Minimal linear codes over finite fields'. *Finite Fields Appl.* 54 (2018), pp. 176–196 (on page 31).

[80] J. W. P. Hirschfeld. *Finite projective spaces of three dimensions*. Oxford Mathematical Monographs. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1985, pp. x+316 (on page 5).

[81] J. W. P. Hirschfeld. *Projective geometries over finite fields*. Second. Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, 1998, pp. xiv+555 (on page 5).

[82] J. W. P. Hirschfeld and J. A. Thas. *General Galois geometries*. Springer Monographs in Mathematics. Springer, London, 2016, pp. xvi+409 (on pages 5, 18, 120).

[83] J. D. Key. 'Hermitian varieties as codewords'. *Des. Codes Cryptogr.* 1.3 (1991), pp. 255–259 (on pages 37, 39).

[84] M. Lavrauw, L. Storme, P. Sziklai and G. Van de Voorde. 'An empty interval in the spectrum of small weight codewords in the code from points and k-spaces of $\mathrm{PG}(n,q)$'. *J. Combin. Theory Ser. A* 116.4 (2009), pp. 996–1001 (on pages 39, 40).

[85] M. Lavrauw, L. Storme and G. Van de Voorde. 'Linear codes from projective spaces'. In: *Error-correcting codes, finite geometries and cryptography*. Vol. 523. Contemp. Math. Amer. Math. Soc., Providence, RI, 2010, pp. 185–202 (on pages 28, 29, 39, 40).

[86] M. Lavrauw, L. Storme and G. Van de Voorde. 'On the code generated by the incidence matrix of points and k-spaces in $\mathrm{PG}(n,q)$ and its dual'. *Finite Fields Appl.* 14.4 (2008), pp. 1020–1038 (on page 39).

[87] M. Lavrauw, L. Storme and G. Van de Voorde. 'On the code generated by the incidence matrix of points and hyperplanes in $PG(n,q)$ and its dual'. *Des. Codes Cryptogr.* 48.3 (2008), pp. 231–245 (on page 39).

[88] M. Lavrauw and G. Van de Voorde. 'Field reduction and linear sets in finite geometry'. In: *Topics in finite fields*. Vol. 632. Contemp. Math. Amer. Math. Soc., Providence, RI, 2015, pp. 271–293 (on pages 19–21, 24).

[89] M. Lavrauw and G. Van de Voorde. 'On linear sets on a projective line'. *Des. Codes Cryptogr.* 56.2-3 (2010), pp. 89–104 (on pages 22, 23, 94, 108, 114).

[90] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes. II*. North-Holland Mathematical Library, Vol. 16. North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977, i–ix and 370–762 (on page 28).

[91] J. L. Massey. 'Minimal codewords and secret sharing'. In: *Proc. 6th Joint Swedish-Russian Int. Workshop on Info. Theory*. 1993, pp. 276–279 (on page 30).

[92] J. L. Massey. 'Some applications of coding theory in cryptography'. In: *Codes and Cyphers: Cryptography and Coding IV*. 1995, pp. 33–47 (on page 30).

[93] G. McGuire and H. N. Ward. 'The weight enumerator of the code of the projective plane of order 5'. *Geom. Dedicata* 73.1 (1998), pp. 63–77 (on page 36).

[94] S. E. Payne and J. A. Thas. *Finite generalized quadrangles*. Second. EMS Series of Lectures in Mathematics. European Mathematical Society (EMS), Zürich, 2009, pp. xii+287 (on page 13).

[95] O. Polverino. 'Linear sets in finite projective spaces'. *Discrete Math.* 310.22 (2010), pp. 3096–3107 (on page 21).

[96] O. Polverino and F. Zullo. 'Codes arising from incidence matrices of points and hyperplanes in $\mathrm{PG}(n,q)$'. *J. Combin. Theory Ser. A* 158 (2018), pp. 1–11 (on pages 30, 40).

[97] C. T. Quinn. 'The André/Bruck and Bose representation of conics in Baer subplanes of $\mathrm{PG}(2,q^2)$'. *J. Geom.* 74.1-2 (2002), pp. 123–138 (on page 115).

[98] S. Rottey, J. Sheekey and G. Van de Voorde. 'Subgeometries in the André/Bruck-Bose representation'. *Finite Fields Appl.* 35 (2015), pp. 115–138 (on pages 115, 117, 118).

[99] L. D. Rudolph. 'A Class of Majority Logic Decodable Codes'. *IEEE Trans. Inform. Theory* 13.2 (1967), pp. 305–307 (on page 28).

[100] B. Segre. *Lectures on modern geometry*. Vol. 7. Consiglio Nazionale delle Ricerche Monografie Matematiche. With an appendix by Lucio Lombardo-Radice. Edizioni Cremonese, Rome, 1961, pp. xv+479 (on page 142).

[101] B. Segre. 'Ovals in a finite projective plane'. *Canadian J. Math.* 7 (1955), pp. 414–416 (on page 13).

[102] B. Segre. 'Sulle ovali nei piani lineari finiti'. *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Nat. (8)* 17 (1954), pp. 141–142 (on page 13).

[103] B. Segre. 'Teoria di Galois, fibrazioni proiettive e geometrie non desarguesiane'. *Ann. Mat. Pura Appl. (4)* 64 (1964), pp. 1–76 (on page 20).

[104] A. Shamir. 'How to share a secret'. *Comm. ACM* 22.11 (1979), pp. 612–613 (on page 30).

[105] T. Szőnyi and Zs. Weiner. 'Stability of k mod p multisets and small weight codewords of the code generated by the lines of PG(2, q)'. *J. Combin. Theory Ser. A* 157 (2018), pp. 321–333 (on pages 37–39).

[106] C. Tang, Y. Qiu, Q. Liao and Z. Zhou. 'Full characterization of minimal linear codes as cutting blocking sets'. *IEEE Trans. Inform. Theory* 67.6, part 2 (2021), pp. 3690–3700 (on page 84).

[107] J. Tits. *Buildings of spherical type and finite BN-pairs*. Lecture Notes in Mathematics, Vol. 386. Springer-Verlag, Berlin-New York, 1974, pp. x+299 (on page 11).

[108] E. Ughi. 'Saturated configurations of points in projective Galois spaces'. *European J. Combin.* 8.3 (1987), pp. 325–334 (on page 134).

[109] G. Van de Voorde. 'Blocking Sets in Finite Projective Spaces and Coding Theory'. PhD thesis. Ghent University, 2010 (on pages 23, 108, 114).

[110] O. Veblen and J. W. Young. 'A Set of Assumptions for Projective Geometry'. *Amer. J. Math.* 30.4 (1908), pp. 347–380 (on page 10).

[111] J. Yuan and C. Ding. 'Secret sharing schemes from three classes of linear codes'. *IEEE Trans. Inform. Theory* 52.1 (2006), pp. 206–212 (on page 31).

Index