Cutting Blocking Sets in Finite Projective Spaces

Master's Thesis

Sára Pituk

Supervisor: György Kiss

Department of Geometry
Faculty of Science
Eötvös Loránd University
Budapest

2022

NYILATKOZAT

Név: Pituk Sára

ELTE Természettudományi Kar, szak: Matematikus MSc

NEPTUN azonosító: AE7FG5

Szakdolgozat címe:
Cutting blocking sets in finite projective spaces

A **szakdolgozat** szerzőjeként fegyelmi felelősségem tudatában kijelentem, hogy a dolgozatom önálló szellemi alkotásom, abban a hivatkozások és idézések standard szabályait következetesen alkalmaztam, mások által írt részeket a megfelelő idézés nélkül nem használtam fel.

Budapest, 2022.05.30.

Pituk Sára

a hallgató aláírása

Acknowledgement

I would like to express my gratitude to my supervisor György Kiss for his guidance on my thesis, and also for all the encouragement and support I recieved from him throughout my academic years. I am also thankful to Leo Storme for his valuable suggestions on this work during my studies at Ghent University.

Contents

Introduction

Blocking sets of finite projective spaces have been studied by finite geometers for quite some time. Beyond the fact that – as combinatorially defined objects in projective spaces – they are of independent interest as well, blocking sets also have applications to other areas of mathematics, such as game theory, finite nets or partial spreads.

A t-fold blocking set in a projective space $PG(k-1,q)$ is a set of points B that intersects every hyperplane in at least t points. A stronger requirement is that B intersects every hyperplane in a generator set. (This property implies that B is a $(k-1)$-fold blocking set.) These objects have been studied in literature under various names, like generator sets [17], and strong blocking sets [14]. However, they have become the focus of interest only very recently, when it was discovered that they are closely related to minimal linear codes [1, 25]. The name *cutting blocking set*, which is most well-spread, was first used for these special blocking sets in [1]. We will also stick to this terminology.

In this master's thesis, we give an overview of the very active research area of cutting blocking sets, with focus on their application to the theory of minimal codes.

This thesis is structured as follows. Chapter 1 contains basic definitions and results about finite projective spaces that are necessary for understanding this text. In Chapter 2, we define minimal linear codes, give two cryptographic applications, and examine the properties of these codes. In Chapter 3, we characterize minimal codes as cutting blocking sets, and we prove results about these geometric objects. Chapter 4 is about constructions of cutting blocking sets.

Chapter 1

Finite projective spaces

Let q be a prime power, and let $GF(q)$ be the unique field of order q. Let $V(k,q)$ be a vector space of dimension k over $GF(q)$. (We know that $V(k,q) \simeq GF(q)^k$). The projective space $PG(k-1,q)$ can be derived from the vector space $V(k,q)$ as follows: We define the $(d-1)$-dimensional projective subspaces of $PG(k-1,q)$ to be the d-dimensional linear subspaces of $V(k,q)$. Thus, the points of $PG(k-1,q)$ are the 1-dimensional subspaces (vector lines) of $V(k,q)$, the lines of $PG(k-1,q)$ are the 2-dimensional subspaces of $V(k,q)$, $\ldots$, and the $(k-2)$-dimensional subspaces (which are also called hyperplanes) are the $(k-1)$-dimensional subspaces of $V(k,q)$.

The points of $PG(k-1,q)$ can be identified via homogeneous coordinates, which we get in the following way: Let $e_1,\ldots,e_k$ be a basis of $V(k,q)$. If P is a fixed projective point, then we can take a vector p representing it, i.e. a vector that generates the 1-dimensional subspace corresponding to P. Then p can be uniquely written as a linear combination of the basis vectors with coefficients $a_1,\ldots,a_k \in GF(q)$, not all of which are zero:

$$p = \sum_{j=1}^{k} a_j e_j.$$

Since the vector representing the point P is only determined up to a scalar multiple, this is also true for the coefficients $(a_1,\ldots,a_k)$. Let us consider the following equivalence relation on $GF(q)^k$:

$$(x_1,\ldots,x_k) \sim (y_1,\ldots,y_k) \Leftrightarrow \exists \lambda \in GF(q)\backslash\{0\}\colon y_i = \lambda x_i \quad (1 \le i \le k).$$

So, if we assign the equivalence class of $(a_1,\ldots,a_k)$ (which we denote by $(a_1 : \cdots : a_k)$) to the point P, we get a bijection between the points of $PG(k-1,q)$ and the non-zero equivalence classes with respect to $\sim$. This mapping defines a homogeneous coordinate system of $PG(k-1,q)$. Of course, there are may choices for the basis, so there are multiple coordinate systems, but they can all be mapped to one another by applying a linear transformation to the vector space $V(k,q)$.

Similarly, we can assign homogeneous coordinate vectors to hyperplanes too. Let H be a hyperplane in $PG(k-1,q)$, corresponding to a hyperplane in $V(k,q)$ with normal vector h (in a fixed basis). Since h and λh determine the same hyperplane for any $\lambda \in GF(q)\backslash\{0\}$, we can define the homogeneous coordinate vector of H as the equivalence class of h under the equivalence relation $\sim$ defined earlier. (A hyperplane can also be viewed as a point in the dual space of $PG(k-1,q)$.)

It is possible to assign coordinates to the lines too. In particular, the projective line l joining the points $A = (a_0 : a_1 : \dots a_{k-1})$ and $B = (b_0 : b_1 : \dots : b_{k-1})$ $(A \neq B)$ can be described by a set of $\frac{k(k-1)}{2}$ numbers $\ell_{ij} = a_i b_j - a_j b_i$ $(i < j)$. These numbers are called the *Plücker coordinates* of ℓ. The Plücker coordinates are homogeneous coordinates too, that is, a Plücker coordinate vector and its non-zero scalar multiples all define the same line, and not all of the values ℓ_{ij} are equal to zero. Also, it does not matter, how we choose the two points on the line, the coordinates obtained in this way will be equal, up to a scalar multiple. However, not all vectors of length $\frac{k(k-1)}{2}$ can be assigned to a line in $PG(k-1,q)$, as the following proposition shows.

Proposition 1.0.1. *A non-zero vector $(\ell_{ij})_{0 \leq i < j \leq k}$ is the Plücker coordinate vector of a line in $PG(k-1,q)$ if and only if*

$$\ell_{i_1 i_2} \ell_{i_3 i_4} - \ell_{i_1 i_3} \ell_{i_2 i_4} + \ell_{i_1 i_4} \ell_{i_2 i_3} = 0$$

for any quadruple (i_1, i_2, i_3, i_4).

In the same way as we have defined the Plücker coordinates of a line joining two different points, we can do this with the subspaces of co-dimension 2 defined as the intersection of two different hyperplanes. (This will be a line in the dual space of $PG(k-1,q)$.)

Definition 1.0.2. Two sets of points in $PG(k-1,q)$ are *projectively equivalent* if they can be mapped into each other by a linear transformation of the ambient space $V(k,q)$.

Proposition 1.0.3. *The number of d-dimensional subspaces of $V(k,q)$, and therefore the number of $(d-1)$-dimensional subspaces of $PG(k-1,q)$, is*

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

In particular, a projective line contains $q+1$ points, and a projective plane contains q^2+q+1 points and the same number of lines.

Proposition 1.0.4. *Let $t \geq d$. The number of t-dimensional subspaces containing a given d-dimensional subspace of $V(k,q)$, and therefore the number of $(t-1)$-dimensional subspaces containing a given $(d-1)$-dimensional subspace of $PG(k-1,q)$, is $\begin{bmatrix} k-d \\ t-d \end{bmatrix}_q$.*

For instance, the number of hyperplanes through a given subspace of co-dimension 2 is always $q+1$.

For two projective subspaces $U, V \subseteq PG(k-1,q)$, we can define the projective subspace $\langle U, V \rangle$ generated by them: Take the linear subspaces in $V(k,q)$ corresponding to U and V. Together, they generate a subspace W in $V(k,q)$. Let $\langle U, V \rangle$ be the projective subspace in $PG(k-1,q)$ corresponding to W.

Proposition 1.0.5. *Let U and V be two projective subspaces in $PG(k-1,q)$. Then*

$$\dim(\langle U, V \rangle) + \dim(U \cap V) = \dim(U) + \dim(V).$$

This immediately implies that the intersection of a line and a hyperplane in $PG(k-1,q)$ cannot be empty.

Definition 1.0.6. Let $1 \leq m \leq k$. We say that m points in $PG(k-1,q)$ are in *general position*, if the m vectors of $V(k,q)$ defining the points are linearly independent.

The field $GF(q)$ is a subfield of $GF(q^h)$ if $h > 1$. It follows that if we have a point in $PG(k-1,q)$, then its coordinates can be seen as coordinates over $GF(q^h)$. In this way, we get a natural inclusion between $PG(k-1,q)$ and $PG(k-1,q^h)$.

Definition 1.0.7. An *order q subgeometry* in $PG(k-1,q^h)$ $(h \geq 2)$ is a set of points projectively equivalent to $PG(k-1,q)$. If $h=2$, then an order q subgeometry is also called a *Baer subgeometry.*

Proposition 1.0.8. *An order q subgeometry in $PG(k-1,q^{k-1})$ intersects each hyperplane in at least one point.*

Proof. The projective space $PG(k-1,q^{k-1})$ arises from $V(k,q^{k-1})$, which is a k-dimensional vector space over $GF(q^{k-1})$. But $GF(q^{k-1})$ is a $(k-1)$-dimensional vector space over $GF(q)$, which means that $V(k,q^{k-1})$ is also a vector space over $GF(q)$, and it has dimension $k(k-1)$. This vector space gives rise to a projective space $PG(k(k-1)-1,q)$. In this setting, a hyperplane in $PG(k-1,q^{k-1})$ corresponds to a subspace of dimension $(k-1)^2-1$ in $PG(k(k-1)-1,q)$, and an order q subgeometry in $PG(k-1,q^{k-1})$ corresponds to a subspace of dimension $k-1$ in $PG(k(k-1)-1,q)$. By Proposition 1.0.5, the two subspaces in $PG(k(k-1)-1,q)$ must intersect each other, so neither can the intersection in $PG(k-1,q^{k-1})$ be empty. □

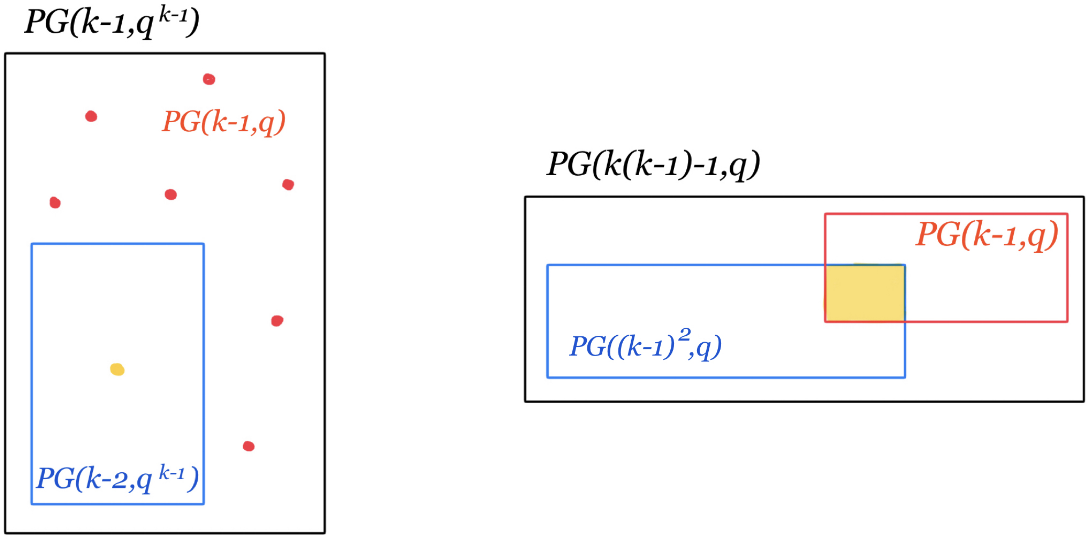


Figure 1.1: The correspondence between the spaces $PG(k-1,q^{k-1})$ and $PG(k(k-1)-1,q)$.

Remark 1.0.9. In the same way, one can prove that an order q subgeometry of dimension d in $PG(k-1,q^h)$ intersects each hyperplane in at least one point if $h \leq d \leq k-1$. For example, a Baer subgeometry in $PG(k-1,q^2)$ intersects each hyperplane too.

Proposition 1.0.10. *There exist $k-1$ pairwise disjoint order q subgeometries in $PG(k-1,q^{k-1})$.*

Proof. It is possible to take $k-1$ pairwise non-intersecting subspaces of dimension $k-1$ in $PG(k(k-1)-1,q)$. The corresponding sets of points in $PG(k-1,q^{k-1})$ form $k-1$ disjoint subgeometries. □

We will also need the following result later.

Proposition 1.0.11. *A Baer subgeometry in $PG(3,q^2)$ intersects each plane in a Baer subplane or a Baer subline.*

Proof. Similarly as above, let us consider the correspondence between $PG(3,q^2)$ and $PG(7,q)$. A plane in $PG(3,q^2)$ corresponds to a 5-dimensional subspace in $PG(7,q)$, and a Baer subgeometry in $PG(3,q^2)$ corresponds to a 3-dimensional subspace in $PG(7,q)$. The intersection of a 3-dimensional and a 5-dimensional subspace in $PG(7,q)$ can have dimension 1, 2, or 3, according to Proposition 1.0.5. If the dimension of the intersection is 3, it means that the smaller subspace is contained in the larger one. But this is impossible in our case, since the 3-dimensional Baer subgeometry is not contained in any plane. Thus, the intersection is a 1- or 2-dimensional subspace, which corresponds to a Baer subline or a Baer subplane in $PG(3,q^2)$, respectively. □

Proposition 1.0.12. *If a set of points $\{P_1,P_2,\ldots,P_s\}$ in $PG(k-1,q^{k-1})$ is fixed by the Frobenius map*

$$F\colon PG(k-1,q^{k-1}) \to PG(k-1,q^{k-1}),$$

$$(r_0 : r_1 : \cdots : r_{k-1}) \mapsto (r_0^q : r_1^q : \cdots : r_{k-1}^q),$$

then the subspace $S = \langle P_1,P_2,\ldots,P_s\rangle$ intersects the subgeometry $PG(k-1,q) \subset PG(k-1,q^{k-1})$ in a subspace of $PG(k-1,q)$, which has the same dimension as S.

Proposition 1.0.13. *Let ℓ_1,ℓ_2, and ℓ_3 be three pairwise disjoint lines in $PG(3,q)$. Then there exist exactly $q+1$ lines that intersect all of the three lines. The union of the points of these $q+1$ lines is projectively equivalent to the set of points determined by the equation*

$$x_0x_1 + x_2x_3 = 0.$$

Definition 1.0.14. A set of points projectively equivalent the set of points determined by the equation

$$x_0x_1 + x_2x_3 = 0$$

in $PG(3,q)$ is called a *hyperbolic quadric.*

Proposition 1.0.15. *Let Q be a hyperbolic quadric in $PG(3,q)$. Then the intersection of Q and a plane π is either*

- *the union of two intersecting lines, or*

- *a conic.*

The latter has no three collinear points.

The interested reader can learn more about finite projective spaces from the textbook [22].

Chapter 2

Minimal linear codes

In this chapter, we introduce a class of linear codes, called minimal linear codes. The first part of the chapter is a review of basic concepts from coding theory. The remainder of the chapter consists of the definition of minimal codewords and minimal codes, two applications of these codes to cryptography, and some fundamental properties of minimal codes.

2.1 Linear codes

In the communication model studied by coding theorists, a sender wants to forward a message to a receiver through some (possibly noisy) channel. They would like to do this in a way such that if a part of the message is changed during transmission, the receiver is still able to recover the original message. To this end, the communicating participants turn to the use of *error-correcting* codes.

Suppose that the message is a string of length n, consisting of elements of $GF(q)$ (the finite field of order q, where q is a prime power). Then it can be viewed as an element of the vector space $GF(q)^n$. In practice, the most common case is when $q = 2$, so the messages are binary strings. This explains why we also use the terminology "bit" for coordinates even if $q \neq 2$.

Definition 2.1.1. We say that during the transmission t *errors* have occurred if t coordinates have been changed, or, in other words, instead of the vector x sent by the sender, the receiver got a vector $x + e$ such that $e \in GF(q)^n$ has exactly t non-zero coordinates.

The aim of the receiver is to decode the message, which means that he wants to find out x knowing $x + e$ and the subset $C \subseteq GF(q)^n$ of possible messages x. The subset C is called a *code*. In general, it can be any subset of $GF(q)^n$. But a lot of nice properties are valid if it is also a linear subspace of $GF(q)^n$. In this master's thesis, we only deal with this case.

Definition 2.1.2. We call a set $C \subseteq GF(q)^n$ a *linear* $[n,k]_q$*-code* if C is a k-dimensional linear subspace of the vector space $GF(q)^n$. The elements of C are called *codewords*.

Definition 2.1.3. Let v and w be two vectors in $GF(q)^n$. Their *Hamming distance* is the number of coordinates in which v and w differ, so

$$d_H(v, w) = |\{i \colon v_i \neq w_i\}|.$$

Proposition 2.1.4. *The Hamming distance is a metric on $GF(q)^n$.*

The metric space $(GF(q)^n, d_H)$ is called the *Hamming space.*

Definition 2.1.5. The *minimum distance* of C is the minimal Hamming distance between any two distinct codewords of C, which is the largest integer d such that any two distinct vectors in C differ from each other in at least d coordinates.

Definition 2.1.6. A linear $[n,k]_q$-code with minimum distance d is also called a *linear $[n,k,d]_q$-code.*

The parameter d is related to the error-correcting quality of the code: the more coordinates are different in any two codewords, the more bits have to be changed during transmission for the receiver not to be able to recover the original message.

Definition 2.1.7. A code is *t-error-correcting* if minimum distance decoding is able to correct t or less errors that may occur in any codeword.

Here, minimum distance decoding means that the receiver chooses a codeword from C that has smallest Hamming distance from the received vector. If there are more than one such codewords, then the decoding is not successful.

Proposition 2.1.8. *A code C is t-error-correcting if and only if its minimum distance d is at least* $2t+1$.

Definition 2.1.9. The *(Hamming) weight* of the codeword c is defined as $w(c) = d_H(c,0)$.

Proposition 2.1.10. *The minimum distance of a linear code is equal to the weight of its minimum weight non-zero codeword(s).*

Proof. If two codewords a and b have Hamming distance d, then the codeword $a-b$ has Hamming weight d. If the codeword c has Hamming weight w, then the Hamming distance between c and 0 is w. So the set of weights and the set of distances between codewords is the same, and it follows that the minima of the two sets is the same too. □

Definition 2.1.11. We define the *(information) rate* of a linear $[n,k]_q$-code as $R = k/n$.

We can define an $[n,k]_q$-code in multiple ways. One possibility is giving the code by its *generator matrix.* This is a matrix of size $k \times n$, the rows of which are the elements of a basis of the subspace C. Another possibility is to give a matrix A of size $(n-k) \times n$ such that $c \in C \Leftrightarrow c \cdot A^T = 0$. This matrix is in fact the generator matrix of the *dual code* of C, which is the $[n, n-k]_q$-code $C^\perp$ defined by the orthogonal complement of C in $GF(q)^n$. In this case, A is called the *parity check matrix* of the code C.

We will also use the following two definitions:

Definition 2.1.12. A code C is *non-degenerate* if there is no coordinate position i such that for all $c \in C$,we have $c_i = 0$.

Definition 2.1.13. Two linear codes are *equivalent* if they can be transformed to each other by finitely many applications of the following two steps:

- switching the same 2 coordinates in every codeword, or
- multiplying the same coordinate by the same nonzero element $\lambda \in GF(q)$ in all of the codewords.

The aim of coding theory is to construct codes as "good" as possible, meaning that for a fixed length, the sender can send many different messages, so the rate of the code is as high as possible. But we also want the receiver to be able to correct many errors. Unfortunately, one of these measures of goodness can only be increased at the expense of the other.

For a more detailed introduction to linear codes, we refer to [20]. The proofs of the propositions listed in this section can be found there too.

2.2 Minimal codewords and codes

Definition 2.2.1. The *support* of the codeword $c \in C$ is the set of its non-zero coordinates:

$$Supp(c) = \{i \in [n] \colon c_i \neq 0\}.$$

Definition 2.2.2. The codeword $c \in C$ is *minimal*, if for all codewords $b \in C$, we have

$$Supp(b) \subseteq Supp(c) \Rightarrow \exists \lambda \in GF(q) \colon b = \lambda c.$$

The code C is *minimal* if all of its non-zero codewords are minimal.

Example 2.2.3. Constant weight codes are always minimal. It is known that linear constant weight codes are duals of Hamming codes. (For the proof, see Theorem A.0.5 in the Appendix.) Unfortunately, they have very bad rates.

2.3 Applications to cryptography

2.3.1 Secret sharing

Minimal codewords were first used in the secret sharing scheme of Massey [23], which is as follows. Suppose that the secret is an element $s \in GF(q)$, and we want to divide it between n players. This means that we give each player a piece of information such that certain subsets of the players can determine s by putting their pieces of information together (in this case, they form an *authorized coalition*), but other subsets cannot determine it. Moreover, they have no more chance to find out the secret from their pieces of information than by taking a random guess. Clearly, the authorized coalitions form a monotone increasing family, so in a scheme, we are always interested in the minimal authorized coalitions.

Let $\mathcal{C}$ be a linear $[n+1, k]_q$-code, and let G be its generator matrix. Let us denote the columns of G by $G_0, G_1, \ldots, G_n$. Suppose that there is no column consisting only of zeros, in other words, that $\mathcal{C}$ is non-degenerate. Now choose a random vector u from $GF(q)^k$ such that $uG_0 = s$, and calculate the vector $uG = (s, v_1, v_2, \ldots, v_n)$. Let us give the element $v_i \in GF(q)$ to player i. (Suppose that the players know their own indices, and the matrix G is also known to each player, but the random vector u is not.)

It is easy to see that a subset $\{i_1, i_2, \ldots, i_m\}$ of players can reveal s if and only if G_0 can be written as a linear combination of the columns $G_{i_1}, G_{i_2}, \ldots, G_{i_m}$. Indeed, if there exist scalars $c_1, \ldots, c_m$ such that $G_0 = c_1 G_{i_1} + \cdots + c_m G_{i_m}$, then we have $s = c_1 v_{i_1} + \cdots + c_m v_{i_m}$. So the players in this subset can determine s by finding the suitable scalars $c_1, \ldots, c_m$, which they can do with a little calculation. On the other hand, if the columns $G_{i_1}, G_{i_2}, \ldots, G_{i_m}$ do not generate G_0, then the equation $xG_{i_j} = v_{i_j}, xG_0 = g$ is a system with at most k equations. So it has a solution $x \in GF(q)^k$ for any value $g \in GF(q)$. So in this case, the players of the coalition do not have any information about the secret.

The condition that an authorized coalition is minimal means that $G_0 = c_1 G_{i_1} + \cdots + c_m G_{i_m}$ with c_j nonzero $(j = 1, \ldots, m)$. This is equivalent to the fact that the vector d with $d_0 = 1$, $d_{i_j} = -c_j$ and $d_k = 0$ for $k \notin \{0, i_1, \ldots, i_m\}$ is a minimal codeword in the dual code of $\mathcal{C}$. So we get that the minimal authorized coalitions of players correspond to the minimal codewords of the dual code $\mathcal{C}^\perp$ with a 1 in the first coordinate.

In general, it is hard to determine the minimal codewords in a code. It makes the situation easier if we use a code every codeword of which is minimal.

2.3.2 Secure two-party computation

Independently from the previous application, another code-based cryptographic protocol was described in [11], which also relies on the minimality of the linear code used in it. In this setting, a function f is given, and there are to parties (we call them Alice and Bob), who hold disjoint parts of the input of f. We denote the part of the input known to Alice by X, and the part known to Bob by Y. The task of the two parties is to compute the value $f(X, Y)$ without revealing their respective parts of the input. A standard example is when two millionaires want to find out which one of them is richer, but neither of them wants to reveal anything about their wealth. We restrict ourselves to the semi-honest setting, which means that both parties are following the protocol, but they might try to infer information about the input of the other party from the information that they receive during the protocol.

We make some assumptions. We suppose that $X \in GF(q)^r$ an $Y \in S$, where S is a given set. Furthermore, let $f\colon GF(q)^r \times S \to GF(q)$ be a function of the form

$$f(X, Y) = \sum_{i=1}^{r} X_i f_i(Y),$$

where $f_i\colon S \to GF(q) \quad (i = 1, \ldots, r)$. We want to find a protocol where Alice learns nothing about Y, Bob learns $f(X, Y)$, but nothing more about X. Note that we could require that Alice learns $f(X, Y)$ too, but this can be attained by adding one last step to the protocol where Bob sends the value $f(X, Y)$ to Alice. So we only deal with the case where it is enough that Bob learns $f(X, Y)$. We also remark that it seems like we made a strict assumption on the form of the function f. However, the class of functions of this specific form include many important cases. For instance, if $S = GF(q)^r$ and f_i is the projection to the i-th coordinate, then we get the scalar product. Or, if we complete the input $X = (X_1, X_2, \ldots, X_r)$ of Alice by an additional bit $X_{r+1} = \sum_{i=1}^r X_i^2$, and we let $f_i(Y) = -2Y_i \quad (i = 1, \ldots, r)$, and $f_{r+1}(Y) = 1$, then if Bob learns $f(X_1, \ldots, X_r, X_{r+1}, Y_1, \ldots, Y_r, Y_{r+1}) = \sum_{i=1}^r X_i^2 - 2\sum_{i=1}^r X_i Y_i$, then by adding $\sum_{i=1}^r Y_i^2$, he can calculate the squared euclidean distance of the vectors X and Y. The secure computation of these function is crucial in some real-world problems.

We also assume that we are aware of an *oblivious transfer protocol.* This protocol assures that Bob can choose a coordinate of X and look at it without Alice knowing which coordinate he chose, and without Bob learning any other bit of information about X than the chosen coordinate. We describe such a protocol in the Appendix.

Now we are ready to give a protocol for computing f securely. Let us choose a linear $[n, n{-}r]_q$-code C which admits parity check matrix $H \in GF(q)^{r\times n}$, which is also the generator matrix of the dual code $C^\perp$. Let us denote the i-th row of H by H_i. The matrix H is known to both parties. First, Alice uniformly randomly picks a vector $Z \in GF(q)^n$ such that $HZ^T = X$. (So we have $X_i = H_i Z^T$.) Bob will query some coordinates of Z, using oblivious transfer, from which he will be able to compute $f(X, Y)$. To see which coordinates he has to choose, we write $f(X, Y)$ as

$$f(X,Y) = \sum_{i=1}^{r} X_i f_i(Y) = \sum_{i=1}^{r} H_i Z^T f_i(Y) = \left(\sum_{i=1}^{r} f_i(Y) H_i\right) Z^T.$$

So, to compute $f(X, Y)$, Bob only needs to know those coordinates of Z where $\sum_{i=1}^{r} f_i(Y)H_i \neq 0$. In other words, he needs to know Z at the positions belonging to the support of the codeword $c = \sum_{i=1}^{r} f_i(Y)H_i$ of the dual code of C. So, in the second step of the protocol, Bob has to query all the bits of Z that belong to this support, using oblivious transfer. Remember that Alice is not supposed to get any information about Y. However, the number of coordinates asked by Bob can reveal some information. To handle this, we can for example have Bob make $m - t$ dummy queries in the end, where t is the actual number of bits that he needs, and m is the maximum of bits that he has to ask for any input Y. Note that since we are in the semi-honest model, we can assume that he will not make real queries here. We still need to make sure that Bob cannot find out any more information about X. But if there is a codeword d in $\mathcal{C}^\perp$ which is linearly independent of c and the support of d in contained in the support of c, then Bob can also get another bit of information (dZ^T) about Z. Therefore, for our protocol to be secure, we need that c is a minimal codeword in $C^\perp$. Since we want that the protocol works for arbitrary f, we have to choose the code in such a way that every codeword is minimal, thus $C^\perp$ has to be a minimal code. Indeed, if we use a minimal linear code, then it is easy to see that Bob will learn only one bit of information about X, which is $f(X, Y)$. We also remark that if $C^\perp$ is a constant weight code (which is minimal), then he always has to query the same number of bits, so he does not have to make dummy queries.

2.4 Properties of minimal codes

Now that we have seen the applications, we can move forward to studying minimal codes. We begin with presenting two results on the rate of minimal codes.

Theorem 2.4.1 ([11]). *Let C be a minimal linear $[n, k]_q$-code. Then we have*

$$R \leq \log_q 2.$$

Proof. This follows from the fact that due to minimality,

$$\mathcal{F} = \{Supp(c) \colon 0 \neq c \in\} \subset 2^{[n]}$$

forms a Sperner family. By Sperner's theorem, we have $|\mathcal{F}| \leq \binom{n}{n/2}$. From this, we get

$$|C| = q^k \leq 1 + (q-1)\binom{n}{n/2},$$

because each set of positions in $\mathcal{F}$ can be the support of only one codeword and its scalar multiples, and C also contains $(0, 0, \ldots, 0)$. So, $R = k/n \leq \log_q 2$. □

Theorem 2.4.2 ([11])**.** *Let $0 \leq R = \frac{k}{n} \leq \frac{1}{2}\log_q\left(\frac{q^2}{q^2-q+1}\right)$. Then there exists a minimal linear $[n, k]_q$-code.*

Proof. Let n and k be integers that satisfy the condition of the theorem. If we fix two linearly independent vectors $a, b \in GF(q)^n$ such that $Supp(b) \subseteq Supp(a)$, then we have exactly $\begin{bmatrix} n-2 \\ k-2 \end{bmatrix}_q$ k-dimensional subspaces of $GF(q)^n$ through the two-dimensional subspace $\langle a, b\rangle$, which is the number of linear $[n, k]_q$-codes containing a and b. Moreover, we can fix such a bad pair of vectors in exactly

$$\sum_{i=1}^{n}(q-1)^i(q^i - q)$$

ways, since there are $(q-1)^i$ vectors a such that $|Supp(a)| = i$, and for every such a, the number of vectors b that are linearly independent of a with $Supp(b) \subseteq Supp(a)$ is $q^i - q$. We have

$$\sum_{i=1}^{n}(q-1)^i(q^i - q) \leq (1 + (q-1)q)^n = (q^2 - q + 1)^n.$$

So, the number of bad codes (that are not minimal) is at most $\begin{bmatrix} n-2 \\ k-2 \end{bmatrix}_q (q^2 - q + 1)^n$, which is smaller than the total number $\begin{bmatrix} n \\ k \end{bmatrix}_q$ of linear $[n, k]_q$-codes, if the condition of the theorem is satisfied. So, the number of minimal codes with these parameters must be positive. □

Unfortunately, the above proof is not constructive.

The following theorem is referred to as the Ashikhmin-Barg condition:

Theorem 2.4.3 ([3])**.** *Let C be a linear $[n, k, d]_q$-code. Let w_{max} and w_{min} stand for the weight of the maximal weight and the minimal weight nonzero codeword(s) in C. If*

$$\frac{w_{max}}{w_{min}} < \frac{q}{q-1},$$

then C is minimal.

Proof. Suppose to the contrary that there is a non-zero codeword $c \in C$ that is not minimal. Let b be a codeword for which $Supp(b) \subseteq Supp(c)$, and b is linearly independent of c. Consider the $q-1$ codewords of the form $c_\lambda = c - \lambda b$, where $\lambda \in GF(q) \backslash \{0\}$. If we sum up the weights of the codewords c_λ, we get $(q-1)w(c) - w(b)$, since every bit of $Supp(b)$ will be zero in c_λ for exactly one value of λ. There must be a value λ such that c_λ has weight at most average:

$$w(c_\lambda) \leq w(c) - \frac{1}{q-1}w(b) \leq w_{max} - \frac{1}{q-1}w_{min},$$

but the right hand side is less than w_{min} by the assumption of the theorem, which leads to a contradiction. □

The Ashikhmin-Barg condition is only sufficient for a linear code to be minimal, but not necessary, as the following example shows.

Example 2.4.4. Let C be the 2-dimensional code over $GF(2)$ generated by the vectors $(1,1,0,0,0,0)$ and $(0,1,1,1,1,1)$. Then the minimum weight of C is $w_{min} = 2$, and the maximum weight of C is $w_{max} = 5$. So,

$$\frac{w_{max}}{w_{min}} = \frac{5}{2} > 2,$$

but C is a minimal linear code.

We can also give a necessary condition for a linear code to be minimal.

Definition 2.4.5. A linear code C is *intersecting* if for any nonzero codewords $c, b \in C$, we have $Supp(c) \cap Supp(b) \neq \emptyset$.

Proposition 2.4.6 ([13]). *Minimal codes are intersecting.*

Proof. Let c and b be two codewords of C such that $Supp(c) \cap Supp(b) = \emptyset$. Since C is a linear subspace of $GF(q)^n$, $c + b$ is also a codeword, and we have $Supp(c) \subset Supp(c+b)$, but c and $c + b$ are two linearly independent vectors; a contradiction. □

If $q = 2$, then this condition is also sufficient.

Proposition 2.4.7 ([13]). *Binary intersecting codes are minimal.*

Proof. In the binary case, the support of a codeword determines the codeword itself. If we have $c \neq 0$ and $b \neq 0$ such that $Supp(c) \subset Supp(b)$, then $Supp(c + b) = Supp(d) \backslash Supp(b)$ does not intersect $Supp(c)$; a contradiction. □

However, if $q > 2$, then intersecting codes are not necessarily minimal, as shown by the following proposition.

Proposition 2.4.8 ([13]). *Let $k \geq 2$. For any two linearly independent codewords c and d of a minimal $[n, k, d]_q$ code C, we have $|Supp(c) \cap Supp(b)| \geq q - 1$.*

Proof. Let c and b be two linearly independent codewords. By Proposition 2.4.6, we know that $Supp(c) \cap Supp(b) \neq \emptyset$. Consider $e = c + \lambda b \in C$, $0 \neq \lambda \in GF(q)$. This is linearly independent of both c and b, so it cannot cover any of them. So codeword e has a zero position which lies in $Supp(c)$ or $Supp(b)$. But this zero position in e must be in $Supp(c) \cap Supp(b)$. Thus, there must exist at least one coordinate position $i \in Supp(c) \cap Supp(b)$ such that $e_{i_\lambda} = 0$. Also, we cannot have $i_\lambda = i_\mu$ if $\lambda \neq \mu$, because $c_i \neq 0 \neq d_i$ for $i \in Supp(c) \cap Supp(b)$. So we have an injection from $GF(q) \backslash \{0\}$ to $Supp(c) \cap Supp(b)$, and therefore $|Supp(c) \cap Supp(b)|$ must contain at least $q - 1$ indices. □

We now construct an intersecting code which is not minimal.

Example 2.4.9. Let C be the 2-dimensional code over $GF(q)$, $q > 2$, generated by the vectors $c = (1,1,1,0,0)$ and $b = (0,0,1,1,1)$. Then $|Supp(c) \cap Supp(b)| = 1$, but for a minimal code, necessarily $|Supp(c) \cap Supp(b)| \geq q - 1 \geq 2$.

Let us also see a sufficient and necessary condition for a linear code to be minimal.

Theorem 2.4.10 ([19])**.** *Let $C \subseteq GF(q)^n$ be a linear code. Then C is minimal if and only if for any two linearly independent codewords $a, b \in C$, we have*

$$\sum_{\lambda \in GF(q) \backslash \{0\}} w(a + \lambda b) \neq (q-1)w(a) - w(b).$$

Proof. We will show that

$$Supp(b) \subseteq Supp(a) \Leftrightarrow \sum_{\lambda \in GF(q) \backslash \{0\}} w(a + \lambda b) = (q-1)w(a) - w(b).$$

For $a = (a_1, \ldots, a_n) \in GF(q)^n$ and $b = (b_1, \ldots, b_n) \in GF(q)^n$, define $a \cap b \in GF(q)^n$ as $(e_1, \ldots, e_n)$, where

$$e_i = \begin{cases} a_i \text{ if } a_i = b_i, \\ 0 \text{ otherwise} \end{cases} \qquad (i = 1, \ldots, n).$$

For example, $(0,1,2,2,1,0) \cap (0,2,2,0,1,1) = (0,0,2,0,1,0) \in GF(3)^6$.

Let $a, b \in GF(q)^n$. Then we have

$$Supp(b) \subseteq Supp(a) \Leftrightarrow \sum_{\lambda \in GF(q) \backslash \{0\}} (\lambda a \cap b) = b.$$

To see this, let us suppose first that $Supp(b) \subseteq Supp(a)$. Then

$$b_i \neq 0 \Rightarrow a_i \neq 0 \Rightarrow \exists! \lambda_i \in GF(q) \backslash \{0\} \colon b_i = \lambda_i a_i.$$

So, the i-th coordinate of $\lambda a \cap b$ will be equal to b_i for exactly one value of λ, and it will be equal to zero in all other cases. It follows that the i-th coordinate of the sum will be equal to b_i. For the other direction, let us suppose that

$$\sum_{\lambda \in GF(q) \backslash \{0\}} (\lambda a \cap b) = b,$$

and $b_i \neq 0$. We need to show that $a_i \neq 0$. But if a_i were equal to zero, then the i-th coordinate of each vector in the sum would be equal to zero, and therefore the i-th coordinate of the sum, which is b_i, would be equal to zero too. This is a contradiction, so we have $a_i \neq 0$.

Note that if $\lambda \neq \mu$, then $Supp(\lambda a \cap b) \cap Supp(\mu a \cap b) = \emptyset$, since the vectors λa and μa do not agree in any of their coordinates. Therefore,

$$\sum_{\lambda \in GF(q) \backslash \{0\}} (\lambda a \cap b) = b \Rightarrow \sum_{\lambda \in GF(q) \backslash \{0\}} w(\lambda a \cap b) = w\left(\sum_{\lambda \in GF(q) \backslash \{0\}} (\lambda a \cap b) \right) = w(b).$$

On the other hand, for any $a, b \in GF(q)^n$, the i-th coordinate of

$$\sum_{\lambda \in GF(q) \backslash \{0\}} (\lambda a \cap b)$$

is b_i if $a_i \neq 0$, and 0 otherwise. Therefore, the implication

$$\sum_{\lambda \in GF(q)\backslash\{0\}} w(\lambda a \cap b) = w(b) \Rightarrow \sum_{\lambda \in GF(q)\backslash\{0\}} (\lambda a \cap b) = b$$

is also true. We have proven that

$$Supp(b) \subseteq Supp(a) \Leftrightarrow \sum_{\lambda \in GF(q)\backslash\{0\}} w(\lambda a \cap b) = w(b). \tag{2.1}$$

The next step of the proof is showing that for any $a, b \in GF(q)^n$, we have

$$(q-1)(w(a) + w(b)) = \sum_{\lambda \in GF(q)\backslash\{0\}} w(a + \lambda b) + q \sum_{\lambda \in GF(q)\backslash\{0\}} w(\lambda a \cap b). \tag{2.2}$$

Indeed, for a fixed $\lambda \in GF(q)\backslash\{0\}$,

$$w(a) + w(b) = w(a + \lambda b) + \sum_{\mu \in GF(q)\backslash\{0\}} w(\mu a \cap b) + w\left(-\frac{1}{\lambda} a \cap b\right).$$

Summing up these equations for all $\lambda \in GF(q)\backslash\{0\}$ yields

$$(q-1)(w(a)+w(b)) = \sum_{\lambda \in GF(q)\backslash\{0\}} w(a+\lambda b) + (q-1) \sum_{\lambda \in GF(q)\backslash\{0\}} w(\lambda a \cap b) + \sum_{\lambda \in GF(q)\backslash\{0\}} w(\lambda a \cap b)$$

$$= \sum_{\lambda \in GF(q)\backslash\{0\}} w(a + \lambda b) + q \sum_{\lambda \in GF(q)\backslash\{0\}} w(\lambda a \cap b).$$

Combining (2.1) and (2.2) finishes the proof. □

Remark 2.4.11. If $q = 2$, then Theorem 2.4.10 states that a linear code $C \subseteq GF(2)^n$ is minimal if and only if

$$w(a + b) \neq w(a) - w(b).$$

Note that this means exactly that C is intersecting.

We recall the Singleton bound, which is a classical result in coding theory.

Theorem 2.4.12 (Singleton bound, [20])**.** *Let C be a linear $[n, k, d]_q$ code. Then*

$$k \leq n - d + 1.$$

Proof. Let C be a linear $[n, k, d]_q$ code. Let us choose $d - 1$ coordinates, and delete these coordinates from each codeword. The words of length $n - d + 1$ that we get in this way, must be pairwise different, because if we got the same words for two different codewords c and c', it would mean that c and c' differ in at most $d - 1$ bits, which is impossible. Thus, the size of C, which is q^k, cannot be larger than the number of different q-ary words of length $n - d + 1$. So we have

$$q^k \leq q^{n-d+1}$$

$$\Rightarrow k \leq n - d + 1.$$

□

From Proposition 2.4.8 and Theorem 2.4.12, we obtain the following result on the minimal distance of a minimal code:

Corollary 2.4.13 ([13]). *Let C be a minimal $[n, k, d]_q$ code. Then*

$$d \geq k + q - 2.$$

Proof. Let $c \in C$ be a minimal weight codeword, so we have $w(c) = d$. Let us consider the projection of C to the support of c. (So, from each codeword, we eliminate those coordinates that do not belong to $Supp(c)$.) This way we get a new code C' of length d and dimension k. By Proposition 2.4.8, we know that each codeword in C' has weight at least $q - 1$, so the minimal distance d' of C' is at least $q - 1$. Now, the Singleton bound gives us

$$d \geq k + d' - 1 \geq k + q - 2.$$

□

We can provide an even stronger lower bound for the minimum distance of a minimal code, which we will do in the next chapter, using geometric arguments.

Chapter 3

Cutting blocking sets

3.1 A geometric characterization of minimal codes

It is common in coding theory that a certain property of a linear code can be formulated in terms of geometry: We can associate a set of points of a finite projective space to the code, and from the property of the code, we obtain a geometric property of this point set. This is the case with minimality as well.

Theorem 3.1.1 ([1])**.** *An equivalence class of minimal linear $[n,k]_q$ codes is equivalent to a set $\mathcal{P}$ of n points in $PG(k-1,q)$ such that every hyperplane of $PG(k-1,q)$ is generated by its points in $\mathcal{P}$.*

Proof. Suppose that the linear $[n,k]_q$ code C is non-degenerate, and consider the generator matrix of C, which is a matrix M of size $k \times n$. If we multiply a column of M by an arbitrary non-zero element of $GF(q)$, we get a code which is equivalent to C, thus the columns are only relevant up to a non-zero scalar multiple. Starting from this observation, we can view the columns of M as the homogeneous coordinate vectors of n points in $PG(k-1,q)$. Let $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$ be the set of these points. (Since C is non-degenerate, there is no column with only 0 entries, therefore these vectors indeed represent points of $PG(k-1,q)$.) The matrix M is a generator matrix of C, which means that each codeword can be written in the form $c = uM$ for some vector $u \in GF(q)^k$. Furthermore, if $c \neq 0$, then $u \neq 0$. These vectors u can be considered as the coordinate vectors of hyperplanes in $PG(k-1,q)$. The hyperplane corresponding to the vector u contains the point P_i corresponding to the i-th column of M if and only if the i-th coordinate of $c = uM$ is 0. So the condition that there are no non-zero codewords c and d that are linearly independent and $Supp(c) \subseteq Supp(d)$ (or equivalently $\overline{Supp(d)} \subseteq \overline{Supp(c)}$), can be reformulated as follows: There are no hyperplanes $U \neq V$ such that $\mathcal{P} \cap U \subseteq \mathcal{P} \cap V$. This is in turn equivalent to the property that for all hyperplanes U, we have $\langle \mathcal{P} \cap U \rangle = U$. □

Sets of points with the property given in Theorem 3.1.1 have already been examined before the discovery of their connection to minimal codes, as special multiple blocking sets, which we define in the next section.

3.2 (Multiple) blocking sets and cutting blocking sets

Definition 3.2.1. A set of points $B \subseteq PG(k-1,q)$ is a

- *blocking set* if it intersects every hyperplane.
- *t-fold blocking set* if it intersects every hyperplane in at least t points.
- *cutting blocking set* if it intersects every hyperplane in a generator set.

Remark 3.2.2. We have defined blocking sets only with respect to hyperplanes. In fact, they can be defined with respect to subspaces of any dimension: A d-blocking set in $PG(k-1,q)$ is a set of points which intersects each subspace of dimension $k-d-1$. We can define t-fold d-blocking sets and cutting d-blocking sets similarly. However, we are interested in 1-blocking sets, because they are the ones that are connected to minimal linear codes. For simplicity, we refer to 1-blocking sets as blocking sets in this thesis.

To generate a hyperplane in $PG(k-1,q)$, we need a set of $k-1$ points in general position. So it follows that cutting blocking sets in $PG(k-1,q)$ are special $(k-1)$-fold blocking sets.

The whole $PG(k-1,q)$ is clearly a cutting blocking set. (This corresponds to the aforementioned simplex code.) Also, if B is a cutting blocking set and $B \subseteq B'$, then B' is a cutting blocking set too. Thus, we are interested in finding cutting blocking sets of the smallest possible size. This is equivalent to finding minimal codes with the best possible rate when the dimension and the size of the alphabet is fixed.

Example 3.2.3. The union of $k-1$ pairwise disjoint lines in $PG(k-1,q)$, or the union of $k-1$ disjoint order q subgeometries in $PG(k-1,q^{k-1})$ is a $(k-1)$-fold blocking set. However, it is not necessarily a cutting blocking set, since it can happen that the $k-1$ intersection points of a hyperplane H with the set of lines lies in a proper subspace of H.

Similarly to blocking sets in the projective space $PG(k-1,q)$, we can define blocking sets in the affine space $AG(k-1,q)$.

Definition 3.2.4. $A \subseteq AG(k-1,q)$ is an *affine blocking set* if it intersects every hyperplane of $AG(k-1,q)$.

Due to the equivalence between minimal linear codes and cutting blocking sets, the statements about minimal linear codes can be formulated for cutting blocking sets and proved geometrically, and vice versa. As an example, we state the Ashikhmin-Barg condition for cutting blocking sets, and give a geometric proof.

Theorem 3.2.5 ([5])**.** *Let $\mathcal{P}$ be a set of n points in $PG(k-1,q)$. Let m and M denote the minimum and the maximum number of points of $\mathcal{P}$ contained in a hyperplane, respectively. If*

$$\frac{n-M}{n-m} > \frac{q-1}{q},$$

then $\mathcal{P}$ is a cutting blocking set.

Proof. Suppose to the contrary that $\mathcal{P}$ is not a cutting blocking set. This means that there is a hyperplane H in $PG(k-1,q)$ such that $\langle \mathcal{P} \cap H \rangle \neq H$. So $\mathcal{P} \cap H$ is contained in a proper subspace of H of dimension $k-2$. Let us denote this subspace by S. Now $PG(k-1,q)$ can be partitioned as

$$PG(k-1,q) = S \cup (H \backslash S) \cup (H_1 \backslash S) \cup (H_2 \backslash S) \cup \cdots \cup (H_q \backslash S),$$

where $\{H, H_1, H_2, \ldots, H_q\}$ is the set of the $q+1$ hyperplanes of $PG(k-1,q)$ through S. Suppose that $|\mathcal{P} \cap H| = |\mathcal{P} \cap S| = x$. Then

$$n = |\mathcal{P}| \leq x + q(M-x) = qM - (q-1)x \leq qM - (q-1)m,$$

a contradiction. □

3.3 Bounds on the size of a cutting blocking set

Lemma 3.3.1 ([18])**.** *B is a cutting blocking set in $PG(k-1,q)$ if and only if for any hyperplane H, it holds that $B \backslash H$ is an affine blocking set in $PG(k-1,q) \backslash H \simeq AG(k-1,q)$.*

Proof. Let us suppose that B intersects every hyperplane of $PG(k-1,q)$ in a generator set, and let H be an arbitrary hyperplane of $PG(k-1,q)$. If $B \backslash H$ is not an affine blocking set in $PG(k-1,q) \backslash H$, then there is a hyperplane H' of $PG(k-1,q)$ such that the affine space $PG(k-1,q) \backslash H$ does not contain any point from B. But then $H' \cap B$ is contained in the subspace $H \cap H'$ that has co-dimension 2, so it cannot be a generator set of H, a contradiction. On the other hand, if every hyperplane H' of $PG(k-1,q)$ contains at least one point from B outside any hyperplane H, then the points of $H' \cap B$ generate H', because any subspace of co-dimension 2 contained in H' can be written as $H' \cap H$ for some hyperplane H. □

Lemma 3.3.2 ([9])**.** *Let $P(x_1, \ldots, x_m) \in GF(q)[x_1, \ldots, x_m]$ be an m-variable polynomial over $GF(q)$. If $P(a_1, \ldots, a_m) = 0$ for all $(a_1, \ldots, a_m) \in GF(q)^m$, then*

$$P(x_1, \ldots, x_m) \in (x_1^q - x_1, x_2^q - x_2, \ldots, x_m^q - x_m)\,.$$

Proof. We prove the lemma by induction on m.

If $m = 1$, then every element of $GF(q)$ is a root of $P(x) \in GF(q)[x]$, so

$$\prod_{a \in GF(q)} (x-a) \quad | \quad P(x),$$

but the product on the left hand side is exactly $(x^q - x)$, so P is a multiple of this polynomial.

Let $m \geq 2$, and let us suppose that the lemma is true for values at most $m-1$. Let P be a polynomial of m variables, and define

$$P^a(x_2, x_3, \ldots, x_m) \coloneqq P(a, x_2, \ldots, x_m).$$

By induction, it follows that

$$P^a(x_2, \ldots, x_m) = P_2^a(x_2, \ldots, x_m)(x_2^q - x_2) + P_3^a(x_2, \ldots, x_m)(x_3^q - x_3)$$

$$+\cdots+P_m^a(x_2,\ldots,x_m)(x_m^q-x_m)$$

for some polynomials $P_2^a(x_2,\ldots,x_m),\ldots,P_m^a(x_1,\ldots,x_m)\in GF(q)[x_2,x_3,\ldots,x_m]$. If we let a vary over $GF(q)$, then, for each $i=2,\ldots,m$, we get a function $P_i^{x_1}(x_2,\ldots,x_m)$. This function is not necessarily a polynomial in x_1, but – as every function over a finite field – it is functionally equivalent to a polynomial $R_i(x_1,x_2,\ldots,x_m)$. This means that for all values $a\in GF(q)$, after substituting a for x_i, the two expressions $P_i^{x_1}(x_2,\ldots,x_m)$ and $R_i(x_1,x_2,\ldots,x_m)$ look the same. Then, by the first part of the proof,

$$(x_1^q-x_1)\quad|\quad P_i^{x_1}(x_2,\ldots,x_m)-R_i(x_1,x_2,\ldots,x_m)$$

$$\Rightarrow (x_1^q-x_1)\quad|\quad P(x_1,x_2,\ldots,x_m)-\sum_{i=2}^{m}R_i(x_1,\ldots,x_k)(x_i^q-x_i),$$

which is exactly what we wanted to prove. □

Theorem 3.3.3 (Jamison [21], Brouwer-Schrijver [9])**.** *The minimum size of an affine blocking set in $AG(k-1,q)$ is $(k-1)(q-1)+1$.*

Proof. Let $A\subseteq AG(k-1,q)$ be an affine blocking set. Without loss of generality, we may assume that A contains the point $0=(0,0,\ldots,0)$. Let B be the set $A\backslash\{0\}$. Since A intersects each hyperplane, B must intersect each hyperplane that does not contain 0. The equation of such a hyperplane can be written as

$$w_1x_1+\ldots w_{k-1}x_{k-1}=1,$$

where $w_1,\ldots,w_{k-1}\in GF(q)$, not all of them are 0. The fact that the hyperplane determined by the above equation contains a point from B, corresponds to the condition that there exists a point $b=(b_1,\ldots,b_{k-1})\in B$ such that

$$w_1b_1+\ldots w_{k-1}b_{k-1}=1.$$

So, if this is true for every hyperplane not through 0, then the polynomial

$$F(x_1,\ldots,x_{k-1})=\prod_{b\in B}(b_1x_1+\cdots+b_kx_k-1)$$

evaluates zero at all $(k-1)$-tuples $(w_1,\ldots,w_{k-1})\in GF(q)^k$, different from 0, since at least one of the terms of the product is zero.

Let us write $F(x_1,\ldots,x_{k-1})$ as

$$F(x_1,\ldots,x_{k-1})=F_1(x_1,\ldots,x_{k-1})(x_1^q-x_1)+\cdots+F_{k-1}(x_1,\ldots,x_{k-1})(x_{k-1}^q-x_{k-1})$$

$$+G(x_1,\ldots,x_{k-1}),$$

where the degree of each x_i in G is at most $q-1$. Let us consider the polynomials $x_iF(x_1,\ldots,x_{k-1})$ for $i=1,\ldots,k-1$. These polynomials all assume zero to every $(k-1)$-tuple from $GF(q)^k$. But this means that the polynomials $x_iG(x_1,\ldots,x_{k-1})\quad(i=1,\ldots,k-1)$ also assume zero to every $(k-1)$-tuple, because $a^q-a=0$ for all $a\in GF(q)$. Therefore we can apply Lemma 3.3.2 to these polynomials, and after using the condition on the degrees of the variables in G, we conclude that

$$(x_i^{q-1} - 1) \quad | \quad G(x_1, \ldots, x_{k-1})$$

for each $i = 1, \ldots, k-1$, which in turn implies that

$$\prod_{i=1}^{k-1} (x_i^{q-1} - 1) \quad | \quad G(x_1, \ldots, x_{k-1}).$$

Note that G is not identically 0 (e.g. $G(0) \neq 0$, because $F(0) \neq 0$), so the degree of G is at least the degree of the polynomial

$$\prod_{i=1}^{k-1} (x_i^{q-1} - 1),$$

which is $(k-1)(q-1)$. The degree of F, which is exactly $|B|$ cannot be less than the degree of G, so we obtained that

$$|A| = |B| + 1 \geq (k-1)(q-1) + 1,$$

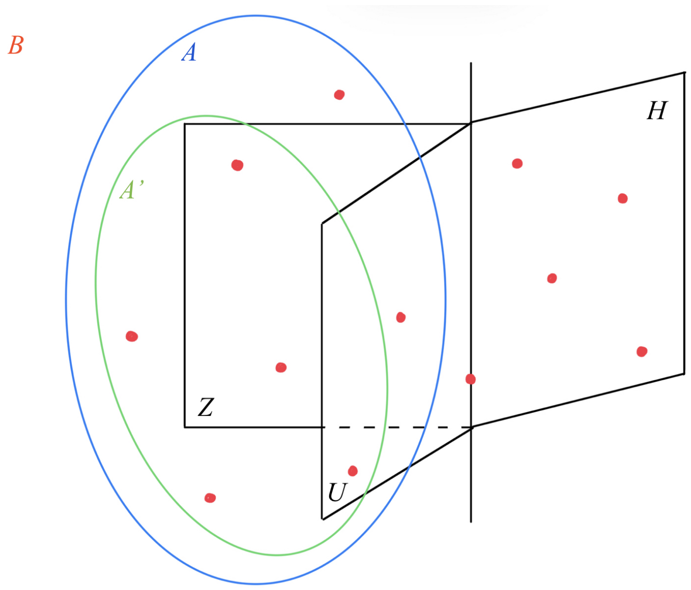
as stated in the theorem.

We have proved that any affine blocking set has size at least $(k-1)(q-1)+1$. This size can be attained: if we take $(k-1)$ independent lines through a fixed point, then the union of these lines intersects each hyperplane in at least one point, and this set has cardinality $|(k-1)(q-1)+1|$. □

Theorem 3.3.4 ([2, 18]). *The size of a cutting blocking set in $PG(k-1, q)$ is at least $(q+1)(k-1)$.*

Proof. Let B be a cutting blocking set, and let us choose a hyperplane H for which $|B \cap H|$ is maximal. Then, by Lemma 3.3.1, $A = B \backslash H$ is an affine blocking set in $PG(k-1, q) \backslash H$. Let $A' \subseteq A$ be an affine blocking set in $PG(k-1, q) \backslash H$ that is minimal (i.e. for any point $P \in A'$, $A' \backslash \{P\}$ is not an affine blocking set). According to Theorem 3.3.3, the size of A' must be at least $(k-1)(q-1)+1$. By the minimality of A', for any point $P \in A'$, there exists a hyperplane U for which $A' \cap U = \{P\}$. Then $|A \backslash U| \geq |A' \backslash U| \geq (k-1)(q-1)$, because we only left one point out.

We know that there are exactly $q+1$ hyperplanes through $H \cap U$, and two of them are H and U. Neither H, nor U contain points from $A \backslash U$, so the points of $A \backslash U$ are divided among $q-1$ hyperplanes. So at least one of them has to contain at least $(k-1)$ points from $A \backslash U$. Let Z be such a hyperplane. Remember that we chose H such that $|B \cap H|$ was maximal.



Thus,

$$|B \cap H| \geq |B \cap Z| = |Z \cap A| + |Z \cap (B \cap H)| = |Z \cap (A \backslash U)| + |U \cap (B \cap H)| =$$

$$= |Z \cap (A \backslash U)| + |B \cap H| + |(B \backslash H) \backslash U| - |B \backslash U| \geq k - 1 + |B \cap H| + (k-1)(q-1) - |B \backslash U|.$$

This implies that $|B \backslash U| \geq (k-1)q$. Also, $|B \cap U| \geq k-1$, because $B \cap U$ is a generator set in the hyperplane U. So we have

$$|B| = |B \backslash U| + |B \cap U| \geq (k-1)q + (k-1) = (k-1)(q+1),$$

which is the desired result. □

Corollary 3.3.5 ([2, 18]). *Let $\mathcal{C}$ be a minimal $[n,k,d]_q$-code. Then $n \geq (k-1)(q+1)$.*

Corollary 3.3.6. *If C is a minimal code of rate R, then asymptotically $R \leq \frac{1}{q+1}$.*

Proof.

$$R = \frac{k}{n} \leq \frac{n+q+1}{nq+n} \to \frac{1}{q+1}$$

as $n \to \infty$. □

One might ask whether the bound of Theorem 3.3.4 is sharp or not. In [7], Beutelspacher characterized the $(k-1)$-blocking sets of size $(q+1)(k-1)$ under the assumption that $4 \leq k \leq \sqrt{q} + 2$:

Theorem 3.3.7 ([7]). *Let $4 \leq k \leq \sqrt{q}+2$, and let B be a $(k-1)$-fold blocking set of size $(k-1)(q+1)$ in $PG(k-1,q)$. Then we have one of the following cases:*

1. *B is the union of $k-1$ pairwise non-intersecting lines.*
2. *$k = \sqrt{q}+2$, and B is a 3-dimensional Baer subspace of $PG(k-1,q)$.*

3. $q = 4, k = 4$, and B is the complement of a hyperoval in a plane of $PG(3,4)$. (A hyperoval *is a set of $q+2$ points in the plane, such that any line contains at most 2 points of it.)*

We can examine these three possibilities, and conclude that in neither case is B a cutting blocking set.

Proposition 3.3.8 ([2])**.** *If $4 \leq k \leq \sqrt{q}+2$ then the bound of Theorem 3.3.4 is never tight.*

Proof. Let B be a cutting blocking set in $PG(k-1,q)$, $4 \leq k \leq \sqrt{q}+2$. By Theorem 3.3.7, we have three possibilities for B. We will show that neither of them is a cutting blocking set.

1. Suppose that B is the union of $k-1$ lines that are pairwise disjoint, say $B = \ell_1 \cup \ell_2 \cup \dots \cup \ell_{k-1}$. Let us choose a point from each line: $P_1 \in \ell_1, P_2 \in \ell_2, \dots, P_{k-1} \in \ell_{k-1}$. Consider the subspace $H = \langle P_1, P_2, \dots, P_{k-1} \rangle$ generated by these points.

   (a) If $\dim H \leq k-3$, then there is a subspace H' of dimension $k-3$, containing H. Consider the $q+1$ hyperplanes through H'. Since B consist of $k-1$ lines, we know that at most $k-1 < q+1$ of these hyperplanes contains a line of B, so there is at least one hyperplane that does not contain a point outside of the subspace H', so it cannot be generated by the points of B.

   (b) If $\dim H = k-2$, then let $\overline{H}$ be the hyperplane $\overline{H} = \langle P_1, P_2, \dots, P_{k-3}, \ell_{k-2} \rangle$. Assume that $\dim \overline{H} < k-2$. Then there exists a point $Q_{k-2} \in \ell_{k-2} \cap \langle P_1, P_2, \dots, P_{k-3} \rangle$. Now if we choose Q_{k-2} from ℓ_{k-2} instead of P_{k-2}, then by case (a), we get that B is not a cutting blocking set. So $\dim \overline{H} = k-2$. Then ℓ_{k-1} cannot be skew to $\overline{H}$, so there exists a point $Q_{k-1} \in \overline{H} \cap \ell_{k-1}$. The point Q_{k-1} cannot be in the subspace $\langle P_1, P_2, \dots, P_{k-3} \rangle$, because then we choose Q_{k-1} from ℓ_{k-1} instead of P_{k-1}, and we get a contradiction as before. So we conclude that $\langle P_1, P_2, \dots, P_{k-3}, Q_{k-1} \rangle$ is a hyperplane of $\overline{H}$. The line ℓ_{k-2} is a line of $\overline{H}$, so it must intersect $\langle P_1, P_2, \dots, P_{k-3}, Q_{k-1} \rangle$ in a point R_{k-2}. Now if we replace P_{k-1} by Q_{k-1}, and P_{k-2} by R_{k-2} when we choose the $k-1$ points, then we get that $\dim H < k-2$, and we again obtain that B is not a cutting blocking set, as in case (a).

2. Assume that $k = \sqrt{q}+2$, and B is a 3-dimensional Baer subspace. A cutting blocking set must generate the whole space, so B cannot be a cutting blocking set, except for the case when $k = q = 4$. It is known that there are two possibilities for the intersection of a Baer subgeometry and a plane in $PG(3,q)$: it is either a Baer subplane, or a Baer subline. (See Proposition 1.0.11.) The planes that intersect B in a Baer subline, are not generated. So B is not a cutting blocking set.

3. Finally, suppose that $q = k = 4$ and B is the complement of a hyperoval in a plane of $PG(3,4)$. Again, a cutting blocking set must generate the whole space, so if B lies in a plane of a 3-dimensional space, then it cannot be a cutting blocking set.

□

Another consequence of Theorem 3.3.3 is the following.

Theorem 3.3.9 ([2, 18])**.** *In a minimal linear $[n, k, d]_q$ code C, the minimum distance d is at least $(k-1)(q-1)+1$.*

Proof. Let C be a minimal linear $[n, k, d]_q$ code with generator matrix G. Then the set of n points in $PG(k-1, q)$ defined by the columns of G form a cutting blocking set. Let us denote this set by B. If $c \in C$ is a codeword, then it can be written as $c = uG$ for some vector $u \in GF(q)^k$. Let H_u be the hyperplane in $GF(k-1, q)$ with coordinate vector u. The weight of the codeword c is the number of non-zero coordinates in c, equivalently, the number of points in B outside of the hyperplane H_u. But we know that $B \backslash H_u$ is an affine blocking set in $PG(k-1, q) \backslash H_u$, and therefore

$$w(c) = |B \backslash H_u| \geq (k-1)(q-1)+1$$

by Theorem 3.3.3. We have seen that the weight of any codeword $c \in C$ is at least $(k-1)(q-1)+1$, so the minimum distance is at least $(k-1)(q-1)+1$ too. □

3.4 Double blocking sets in $PG(2, q)$

In $PG(2, q)$, cutting blocking sets are the same as 2-blocking sets, also known as *double blocking sets*, because two distinct points of a line also generate the line. If we consider the union of three lines that do not intersect in the same point, then we get a double blocking set in $PG(2, q)$ of size $3q$. By the previous section, we can see that if a double blocking set B contains a full line, then this is the lowest possible cardinality of B. This follows from the fact that if we delete the $q+1$ points of this line from B, then the remaining points must form an affine blocking set in $AG(2, q)$, so by the theorem of Jamison and Brouwer-Schrijver, there must be at least $2q-1$ remaining points. If q is a square, then the union of two disjoint Baer subplanes forms a double blocking set of size $2q + 2\sqrt{q} + 2$. If $q \neq 4$, then this value is smaller than $3q$. It will turn out that we cannot do better than this. First, we prove a somewhat weaker lower bound.

Theorem 3.4.1 ([10])**.** *The size of a double blocking set in $PG(2, q)$ is at least $2q + \sqrt{2q} + 2$, if $q > 5$.*

Proof. Let B be a double blocking set. Suppose that some line ℓ contains at least $\sqrt{2q} + 2$ points of B. Take a point P on this line that is outside of B. (If the whole line l is contained in B, then we have seen that $|B| \geq 3q$, which is greater than $2q + \sqrt{2q} + 2$ if $q > 5$.) There are q lines through P other than ℓ, and we need two points on each line to block all of them. So $|B| \geq 2q + \sqrt{2q} + 2$.

From now on, assume that every line contains less than $\sqrt{2q}+2$ points of B. Let n be the largest number of points of B on a line of $PG(2, q)$. Let τ_i denote the number of i-secants to B $(i = 2, \ldots, n)$. Then

$$\sum_{i=2}^{n} \tau_i = q^2 + q + 1,$$

$$\sum_{i=2}^{n} i\tau_i = |B|(q+1),$$

$$\sum_{i=2}^{n} i(i-1)\tau_i = |B|(|B|-1).$$

The first equation holds because the number of lines in $PG(2,q)$ is q^2+q+1. We get the second equation by double counting the pairs (P,l), where P is a point of B, and l is a line through P. The third equation is obtained by double counting the triplets (P,R,l), where $P \in B$ and $R \in B$ are two different points on the line l, using the fact that two different points determine a unique line.

Since $2 \leq |l \cap B| \leq n \leq \sqrt{2q}+1$, we have

$$\sum_{i=2}^{n} (i-2)(i-\sqrt{2q}-1)\tau_i \leq 0,$$

$$\sum_{i=2}^{n} i(i-1)\tau_i - (\sqrt{2q}+2)\sum_{i=2}^{n} i\tau_i + (2\sqrt{2q}+2)\sum_{i=2}^{n} \tau_i \leq 0,$$

$$|B|(|B|-1) - |B|(q+1)(\sqrt{2q}+2) + (2\sqrt{2q}+2)(q^2+q+1) \leq 0,$$

$$(|B|-(2q+\sqrt{2q}+2))(|B|-(\sqrt{2q}q+1)) + \sqrt{2q} \leq 0,$$

which is only possible in the case when

$$|B| > 2q+\sqrt{2q}+2,$$

since

$$|B|-(\sqrt{2q}q+1) < |B|-(2q+\sqrt{2q}+2) \quad \text{if} \quad q > 5,$$

and the product of two numbers is negative if and only if the smaller number is negative and the larger number is positive. □

To prove better lower bounds on the size of a double blocking set in the projective plane, the authors of [4] used the following result of Rédei about *lacunary* polynomials (polynomials that have a long sequence of zeros in the sequence of coefficients).

Theorem 3.4.2 ([24])**.** *Let $q=p^h$. Let $f_1 \in GF(q)[x]$ be a fully reducible polynomial (i.e. it factors into linear factors over $GF(q)$). Suppose that $f_1(x) = x^q g_1(x) + h_1(x)$, where g_1 and h_1 share no common factor. Let $d_1 < q$ be the maximum of the degrees of g_1 and h_1. Let e be the maximal integer such that $f_1(x) = f_2(x)^{p^e}$ for some $f_2 \in GF(q)[x]$. Then one of the following cases holds.*

1. *$e = h$ and $d_1 = 0$;*
2. *$e \geq \frac{h}{2}$ and $d_1 \geq p^e$;*
3. *$e < \frac{h}{2}$ and $d_1 \geq p^e\lceil \frac{p^{h-e}+1}{p^e+1} \rceil$;*
4. *$e = 0, d_1 = 1$, and $f_1(x) = a(x^q - x)$.*

Using this theorem, they could prove the following:

Theorem 3.4.3 ([4])**.** *The size of a double blocking set in $PG(2,q)$ is at least*

- $2q+2\sqrt{q}+2$*, if* $q>16$ *is a square;*
- $2q+p^d\lceil\frac{p^{d+1}+1}{p^d+1}\rceil+2$*, if* $p^{2d+1}=q>3$*.*

Now we are able to examine the tightness of Theorem 3.3.4 when $k=3$.

Proposition 3.4.4 ([2])**.** *If* $k=3$*, then the bound of Theorem 3.3.4 is tight exactly if* $q=2$*.*

Proof. From the above results, it follows that if a double blocking set of $PG(2,q)$ has $2q+2$ points, then q must be equal to 2. □

3.5 Blocking sets and saturating sets

Cutting blocking sets have an interesting application to another area of finite geometry (which also has a coding theoretic aspect), namely, they are related to saturating sets.

Definition 3.5.1. A set of points $S\subseteq PG(k-1,q)$ is a *ρ-saturating set*, if every point of $PG(k-1,q)$ lies in a ρ-dimensional subspace generated by $\rho+1$ points of S, and ρ is the smallest number with this property.

Example 3.5.2. Let ℓ_1 and ℓ_2 be two lines in $PG(3,q)$ that are skew to each other, and let S be the union of their points. Through each point $P\in PG(3,q)\backslash S$, there exists a unique line that intersects both ℓ_1 and ℓ_2. Therefore, S is a 1-saturating set in $PG(3,q)$.

Theorem 3.5.3 ([15])**.** *A cutting blocking set in a subgeometry* $PG(k-1,q)\subset PG(k-1,q^{k-1})$ *is a* $(k-2)$*-saturating set in* $PG(k-1,q^{k-1})$*.*

Proof. Let us take a cutting blocking set B in $PG(k-1,q)\subset PG(k-1,q^{k-1})$. We need to show that any point P is contained in a hyperplane generated by some points of B. If $P\in B$, then this is trivial, since B cannot lie in a subspace of dimension less than $k-2$. Now assume that $P\notin B$. Consider the subspace $S=\langle P,P^q,P^{q^2},\dots,P^{q^{k-2}}\rangle$. The set of points $\{P,P^q,P^{q^2},\dots,P^{q^{k-2}}\}$ is fixed by the Frobenius map $R\mapsto R^q$, since $(P^{q^{k-2}})^q=P$. (For a point $R=(r_0:r_1:\cdots:r_{k-1})\in PG(k-1,q^{k-1})$, by R^h, we mean the point with coordinates $(r_0^h,r_1^h,\dots,r_{k-1}^h)$.) Therefore, by Proposition 1.0.12, the intersection of S and the subgeometry $PG(k-1,q))$ is a subspace of $PG(k-1,q)$, which has the same dimension as S. Any hyperplane of $PG(k-1,q)$ through this subspace is generated by the points of B. Let us choose one of them arbitrarily, say H. Then the hyperplane H' of $PG(k-1,q^{k-1})$ containing this sub-hyperplane H will be a good choice, since it is also generated by the points of B. □

Using the above theorem, one can derive results on $(k-2)$-saturating sets in $PG(k-1,q^{k-1})$ from results on cutting blocking sets in $PG(k-1,q)$.

Let us see how saturating sets are connected to linear codes.

Definition 3.5.4. Let C be a linear $[n,k,d]_q$ code. The *covering radius* of C is the smallest integer R such that the Hamming balls of radius R around the codewords of C cover the whole space $GF(q)^n$. That is,

$$R = \max_{x \in GF(q)^n} d_H(x, C).$$

Proposition 3.5.5. *Let C be a linear $[n,k,d]_q$ code of covering radius R, and let $A \in GF(q)^{(n-k)\times n}$ be its parity check matrix. Then R is equal to the smallest integer R' such that each $u \in GF(q)^{n-k}$ can be written as a linear combination of R' columns of A.*

Proof. First, we prove that $R' \leq R$. Let $u \in GF(q)^{n-k}$. Then there exists a vector $x \in GF(q)^n$ such that $u = xA^T$. The covering radius of C is R, therefore there exists a codeword $c \in C$ such that $d_H(x,c) \leq R$. Since c is a codeword, we also know that $cA^T = 0$. Now consider the word $x - c$. This has Hamming weight at most R, and $(x-c)A^T = xA^T - cA^T = xA^T = u$. We have written u as the linear combination of at most R columns of A, so $R' \leq R$.

Now let us prove that $R \leq R'$. For $w \in GF(q)^n$, define $v = wA^T$. There exists a vector $y \in GF(q)^n$ such that $w(y) \leq R'$, and $v = yA^T$, because any vector can be written as a linear combination of at most R' columns of A. Then $(w-y)A^T = 0$, which implies that $w - y \in C$. Moreover, $d_H(x-y, x) \leq R'$, so we have $R \leq R'$. □

Corollary 3.5.6. *C is a linear $[n,k,d]_q$ code of covering radius R if and only if the columns of its parity check matrix are the homogeneous coordinate vectors of the points of an $(R-1)$-saturating set of size n in $PG(n-k-1,q)$.*

Corollary 3.5.7. *If there exists a minimal linear code with parameters $[n,k,d]_q$, then there exists a linear code of covering radius $k-1$, with parameters $[n, n-k, d']_{q^{k-1}}$.*

Chapter 4

Constructions of cutting blocking sets

4.1 Higgledy-piggledy line sets

Since lines in $PG(k-1,q)$ have the property that they intersect each hyperplane, it seems like a good idea to look for a cutting blocking set that is the union of lines.

Definition 4.1.1. If the union of the points of some lines forms a cutting blocking set in $PG(k-1,q)$, then the set of these lines is called a *higgledy-piggledy line set* in $PG(k-1,q)$.

Let us begin with a simple construction which works for any k and q.

Example 4.1.2 (Simplex construction, [1])**.** Let us take k points in $PG(k-1,q)$ in general position, and let us denote them by $P_1,\dots,P_k$. Let B be the union of the lines joining the pairs of points. In this way, we obtain a cutting blocking set of size $\binom{k}{2}(q-1)+k$. Indeed, let H be a hyperplane in $PG(k-1,q)$. Since H is a hyperplane, it cannot contain k points in general position, so at least one point, say P_1, is not on H. It follows that H intersects the lines $P_1P_2, P_1P_3, \dots, P_1P_k$ in $k-1$ different points $Q_2, Q_3, \dots, Q_k$. We have

$$\langle P_1, P_2, \dots, P_k\rangle \subseteq \langle P_1, Q_2, Q_3, \dots, Q_k\rangle$$

$$\Rightarrow k-1 = \dim\left(\langle P_1, P_2, \dots, P_k\rangle\right) \leq \dim\left(\langle P_1, Q_2, Q_3, \dots, Q_k\rangle\right)$$

$$\Rightarrow \dim\left(\langle Q_2, Q_3, \dots, Q_k\rangle\right) \geq k-2,$$

so the points $Q_2, Q_3, \dots, Q_k$ generate H. (See Figure 4.1.)

We have seen that if a cutting blocking set of the plane contains at least one line, then it has at least $3q$ points. So the simplex construction is optimal in the plane, if we are considering cutting blocking sets that arise from higgledy-piggledy line sets. However, the size of this set is quadratic in the dimension, while the best known lower bound for a cutting blocking set is linear (see Theorem 3.3.4). In fact, the best known lower bound for the size of a higgledy-piggledy line set, which is given in the following theorem, is also linear in the dimension.

Theorem 4.1.3 ([18])**.** *A higgledy-piggledy line set in $PG(k-1,q)$ has size at least $k-1+\lfloor\frac{k-1}{2}\rfloor-\lfloor\frac{k-2}{q}\rfloor$.*

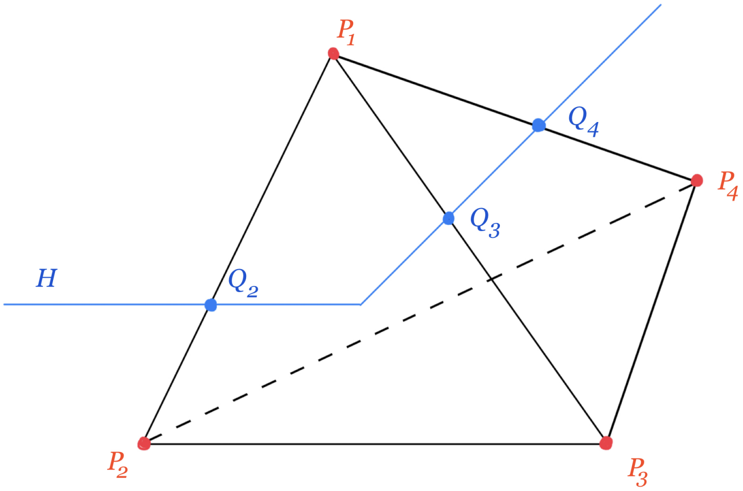


Figure 4.1: The simplex is a higgledy-piggledy line set.

Proof. Let B be a cutting blocking set in $PG(k-1,q)$ that is the union of the points of a set L of m lines. Let us take $\lfloor\frac{k-1}{2}\rfloor$ lines arbitrarily from L. Since r lines generate a subspace of dimension at most $2r-1$, these lines will be contained in a hyperplane H. Then $B\backslash H$ is an affine blocking set in $PG(k-1,q)\backslash H$. So, by Theorem 3.3.3, $B\backslash H$ contains at least $(k-1)(q-1)+1$ points. Now, B is the union of some lines, and a line not in H has 1 point in H and q points outside of H, so at most q points of $B\backslash H$ can be contained in each line. Therefore, we need at least

$$\frac{|B\backslash H|}{q} \geq \frac{(k-1)(q-1)+1}{q} = k-1-\frac{k-2}{q}$$

lines to covers the points of $B\backslash H$. So there are at least $\lfloor\frac{k-1}{2}\rfloor$ lines in H, and at least $k-1-\frac{k-2}{q}$ lines not in H, which is at least $k-1+\lfloor\frac{k-1}{2}\rfloor-\lfloor\frac{k-2}{q}\rfloor$ lines in total. □

In $PG(3,q)$, the lower bound of Theorem 4.1.3 simplifies to 3 if $q=2$, and 4 if $q>2$. These values can be attained too, as described in the following example.

Example 4.1.4 ([17])**.** Let us take three pairwise skew lines ℓ_1,ℓ_2,ℓ_3 in $PG(3,q)$. They determine a unique hyperbolic quadric. The intersection of a plane with this quadric is either a conic or the union of two intersecting lines. If it is a conic, then this conic contains the three intersection points of the plane and the three lines, and no three points on a conic are collinear. However, if a plane intersects the quadric in two lines, and the plane does not contain any of the three lines ℓ_1,ℓ_2,ℓ_3, then the three intersection points are collinear. To handle this case, we have to take a fourth line, which is skew to the quadric. This will intersect the plane in a fourth point, which cannot be on the same line as the other three (since the line through the other three points is on the quadric). Thus, these four lines together form a higgledy-piggledy line set.

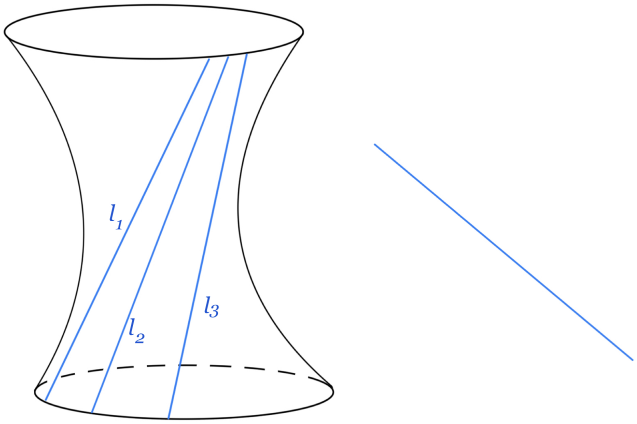


Figure 4.2: 4 lines in higgledy-piggledy arrangement in $PG(3,q)$.

This argument also shows that 3 lines cannot be enough in $PG(3,q)$ to form a cutting blocking set, except for the case when $q = 2$. If this is the case, then every plane that intersects the quadric in a pair of lines, contains one of the three lines ℓ_1, ℓ_2, ℓ_3. So, three pairwise skew lines in $PG(3,2)$ always forms a higgledy-piggledy line set. This implies that the bound of Theorem 3.3.4 is tight if $k = 4$ and $q = 2$. (These values are outside of the region $4 \leq k \leq \sqrt{q} + 2$.)

The simplex construction, which is the only known general construction for a higgledy-piggledy line set that works for all values of k and q, has size quadratic in k, but the lower bound of Theorem 3.3.4 is linear in k. Though we do not know of any construction for a higgledy-piggledy line set with cardinality linear in k, there is a construction for large enough values of q. This is a very nice result, even if – from a coding theoretic point of view – it is not very useful, because in practice, the value of q is usually small.

The following two lemmas will be needed for this construction.

Lemma 4.1.5 ([17])**.** *Let L be a set of lines in $PG(k-1,q)$. If there exists no subspace of co-dimension 2 meeting each element of L, then L is a higgledy-piggledy line set.*

Proof. Suppose that the lines of L are not in higgledy-piggledy arrangement, that is, there exists a hyperplane H such that all of the lines of L intersect H in a subspace U of co-dimension 2. But each element of L meets H, so it follows that each element of L meets U; a contradiction. □

Lemma 4.1.6. *Let L be a set of m lines in $PG(k-1,q)$. Let $\ell(1), \ell(2), \ldots, \ell(m)$ denote the Plücker coordinate vectors of the lines of L. Let U be a subspace of co-dimension two in $PG(k-1,q)$, and let u denote its Plücker coordinate vector. U meets each element of L if and only if*

$$\sum_{i<j} \ell_{ij}(1)u_{ij} = 0, \quad \sum_{i<j} \ell_{ij}(2)u_{ij} = 0, \quad \ldots \quad \sum_{i<j} \ell_{ij}(m)u_{ij} = 0.$$

Thus, there exists a subspace of co-dimension two meeting each element of L if and only if the set of equations

$$\sum_{i<j} \ell_{ij}(1)u_{ij} = 0, \quad \sum_{i<j} \ell_{ij}(2)u_{ij} = 0, \quad \dots \quad \sum_{i<j} \ell_{ij}(m)u_{ij} = 0$$

$$u_{i_1i_2}u_{i_3i_4} - u_{i_1i_3}u_{i_2i_4} + u_{i_1i_4}u_{i_2i_3} = 0 \quad (\forall(i_1, i_2, i_3, i_4)) \tag{4.1}$$

has a non-trivial solution for u.

Proof. The line and a subspace of co-dimension two intersect each other if and only if the scalar product of their Plücker coordinate vectors is zero. Moreover, the vector u is the Plücker coordinate vector of a subspace of co-dimension two if and only if the relations (4.1) hold. □

Theorem 4.1.7 ([17])**.** *If $q \geq 2k-3$ then there is a higgledy-piggledy line set in $PG(k-1, q)$ consisting of $2k-3$ lines.*

Proof. Suppose first, that the characteristic of the field $GF(q)$ is greater than $k-1$.

We construct a line set L such that there exists no subspace of co-dimension two meeting each element of L. By Lemma 4.1.5, this will be a higgledy-piggledy line set.

Let

$$M = \{(1 : t : t^2 : \dots : t^{k-1}) \colon t \in GF(q)\} \cup \{(0 : 0 : \dots : 0 : 1)\}$$

be the *moment curve* in $PG(k-1, q)$. The tangent line of M at point $P(t) = (1 : t : t^2 : \dots : t^{k-1})$ is defined as the line connecting the points $P(t)$ and $P'(t) = (0 : 1 : 2t : 3t^2 : \dots : (k-1)t^{k-2})$. The Plücker coordinates of this line can be written as $\ell_{ij}(t) = (j-i)t^{i+j-1} \quad (i, j \in \{0, 1, \dots, k-1\})$.

Suppose that there exists a non-zero vector u such that

$$u_{i_1i_2}u_{i_3i_4} - u_{i_1i_3}u_{i_2i_4} + u_{i_1i_4}u_{i_2i_3} = 0 \quad (\forall(i_1, i_2, i_3, i_4)),$$

and

$$\sum_{i<j} u_{ij}\ell_{ij}(t) = 0 \quad \forall t \in GF(q)$$

$$\Leftrightarrow \sum_{i=0}^{k-2} \sum_{j=i+1}^{k-1} u_{ij}(j-i)t^{i+j-1} = 0 \quad \forall t \in GF(q)$$

$$\Leftrightarrow \sum_{N=1}^{k-1} t^{N-1} \sum_{i=0}^{\left\lfloor \frac{N}{2} \right\rfloor} (N-2i)u_{i,N-i} + \sum_{N=k}^{2k-3} t^{N-1} \sum_{i=1}^{k-1-\left\lfloor \frac{N}{2} \right\rfloor} (N-2i)u_{i,N-i} = 0 \quad \forall t \in GF(q).$$

This is a degree $2k-4$ polynomial of t, and it has at least $2k-3$ roots (because $|GF(q)| = q \geq 2k-3$), so it must be the zero polynomial. So we have $\sum_i (N-2i)u_{i,N-i} = 0$ for all $0 \leq N < 2k-2$. In detail,

$$u_{01} = 0,$$

$$2u_{02} = 0,$$

$$
\begin{gathered}
3u_{03} + u_{12} = 0,\\
4u_{04} + 2u_{13} = 0,\\
5u_{05} + 3u_{14} + u_{23} = 0,\\
6u_{06} + 4u_{15} + 2u_{24} = 0,\\
\vdots\\
(k-1)u_{0,k-1} + (k-3)u_{1,k-2} + \cdots + \left(\left\lceil \frac{k-1}{2} \right\rceil - \left\lfloor \frac{k-1}{2} \right\rfloor\right) u_{\lfloor \frac{k-1}{2} \rfloor, \lceil \frac{k-1}{2} \rceil} = 0,\\
\vdots\\
3u_{k-4,k-1} + u_{k-3,k-2} = 0,\\
2u_{k-3,k-1} = 0,\\
u_{k-2,k-1} = 0.
\end{gathered}
$$

Since we have assumed that the characteristic of the field is greater than $k-1$, we also know that the coefficients in the above linear system of equations are all non-zero. The first two equations tell us that $u_{01} = u_{02} = 0$. Using this, and the Plücker relations (4.1), we have that $u_{03}u_{12} = 0$. But if one of them is zero, then the other one must be zero as well, by the third equation. If we repeat this argument, we obtain that all coordinates u_{ij} that occur in the first $k-1$ equations, are zero. Similarly, starting from the last two equations, and stepping upwards one by one, we get that all other coordinates of u are equal to zero as well. So, u is the zero vector, and it cannot be the coordinate vector of a subspace of co-dimension two.

We have shown that there exists no subspace of co-dimension two which intersects all tangent lines of the moment curve, so if we take all of them, that will definitely be a higgledy-piggledy line set. Now take arbitrary $2k-3$ tangent lines with Plücker coordinate vectors $\ell(t_1), \ell(t_2), \ldots, \ell(t_{2k-3})$. Suppose that there exists a subspace U with Plücker coordinates $(u_{ij})_{i<j}$ that meets all of these $2k-3$ lines. Then

$$
\sum_{i<j} u_{ij}\ell_{ij}(t_k) = 0 \quad \forall k \in \{1, 2, \ldots, 2k-3\}
$$

$$
\Rightarrow f(t_k) = \sum_{i=0}^{k-2} \sum_{j=i+1}^{k-1} u_{ij}(j-i)t_k^{i+j-1} = 0 \quad \forall k \in \{1, 2, \ldots, 2k-3\}.
$$

A degree $2k-4$ polynomial cannot have more than $2k-4$ roots, so the polynomial f is the zero polynomial. But then each $t \in GF(q)$ is a root of f, which means that all of the tangent lines of M meet the subspace U; a contradiction.

Now we have proved the theorem in the case when the characteristic of $GF(q)$ is greater than $k-1$. When this is not the case, then it can happen that some of the coefficients in the linear equations are zero. But this issue can be fixed if we take so-called *diverted tangent lines* instead of the tangent lines. Let us fix an injection $\phi\colon \{0, 1, \ldots, k-1\} \to GF(q)$. By the assumption of the theorem, $|GF(q)| > k-1$, so such an injection does exist. Then, if we substitute the line joining $P(t)$ and $P'(t)$ by the line joining $P(t)$ and $\widetilde{P}(t) = (0 : 1 : \phi(2)t : \cdots : \phi(k-1)t^{k-2})$ in the proof, then it will still work, but the coefficient of u_{ij} in the system of equations will be $(\phi(j) - \phi(i))$ instead of $j-i$, which is never zero. This concludes the proof of the theorem. □

Remark 4.1.8. The lines of the above theorem do not necessarily form a *minimal* higgledy-piggledy line set. For instance, in $PG(4,11)$, one of the seven lines can be deleted from the set of lines, and it still remains higgledy-piggledy [6].

Remark 4.1.9. In some cases, it is possible to construct higgledy-piggledy line sets in $PG(k-1,q)$ that contain less than $2k-3$ lines. For example, in [6], the authors constructed a set of seven lines in higgledy-piggledy arrangement in $PG(5,q)$, and in [16], we can find a construction of a set of six lines in higgledy-piggledy arrangement in $PG(4,q)$.

Although we do not know of any general constructions for higgledy-piggledy line sets of linear size, we can prove their existence via probabilistic arguments.

Theorem 4.1.10 ([18])**.** *In $PG(k-1,q)$, there exists a set of m lines in higgledy-piggledy arrangement, where*

$$m = \begin{cases} \left\lceil \frac{2}{1+\frac{1}{\ln(q)(q+1)^2}}(k-1) \right\rceil & \text{if } q>2, \\ \lceil 1.95(k-1) \rceil & \text{if } q=2. \end{cases}$$

Proof. Let us take m lines $\ell_1, \ell_2, \dots, \ell_m$ in $PG(k-1,q)$ uniformly at random. Let B denote the union of their points. We want to choose m such that the probability of the event that there is a hyperplane which is not generated, is strictly smaller than 1. This shows that the union of these lines forms a cutting blocking set with positive probability, therefore there must be a choice when they form a cutting blocking set. If a hyperplane H is not generated, then the intersection points of H with all of the lines lie in a subspace of dimension at most $k-3$, so there exists a subspace of dimension at most $k-3$ intersecting all lines. There are two cases: the first case is when there exists a subspace of dimension $k-4$ that intersects all lines, and the second is when the smallest such subspace U has dimension $k-3$. But in this latter case, since we also know that there is a hyperplane (H) through U that is not generated, none of the lines intersect H outside of U. So we get that

$$p = \mathbb{P}(\exists H\colon \dim H = k-2, \langle H \cap B \rangle \neq H) \leq \mathbb{P}(\exists U\colon \dim U = k-4, \forall i \quad U \cap \ell_i \neq \emptyset)$$

$$+\mathbb{P}(\exists V\colon \dim V = k-2, \exists H, \forall i \quad V \cap \ell_i \neq \emptyset, \ell_i \subseteq V \text{ or } \dim H = k-2, \ell_i \not\subseteq H).$$

Using that

$$\mathbb{P}(\exists U\colon \dim U = d, \forall i \quad U \cap \ell_i \neq \emptyset) \leq \begin{bmatrix} k \\ d+1 \end{bmatrix}_q \mathbb{P}(U \cap \ell \neq \emptyset)^m,$$

$$= \begin{bmatrix} k \\ d+1 \end{bmatrix}_q \left(\frac{\begin{bmatrix} d+1 \\ 2 \end{bmatrix}_q + \begin{bmatrix} d+1 \\ 1 \end{bmatrix}_q \frac{1}{q} \left(\begin{bmatrix} k \\ 1 \end{bmatrix}_q - \begin{bmatrix} d+1 \\ 1 \end{bmatrix}_q \right)}{\begin{bmatrix} k \\ 2 \end{bmatrix}_q} \right)^m$$

and that for a fixed subspace V of dimension $k-3$,

$$\mathbb{P}(\exists H\colon \forall i \quad \ell_i \subseteq V \text{ or } \dim H = k-2, \ell_i \not\subseteq H)$$

$$\leq (q+1) \left(\mathbb{P}(\ell \subseteq V | \ell \cap V \neq \emptyset) + \mathbb{P}(\ell \not\subseteq V | \ell \cap V \neq \emptyset) \frac{q}{q+1} \right)^m$$

$$= (q+1)\left(\frac{\begin{bmatrix}k-2\\2\end{bmatrix}_q}{\begin{bmatrix}k-2\\2\end{bmatrix}_q + (q^{k-2}-q^{k-3})\begin{bmatrix}k-2\\1\end{bmatrix}_q} + \left(1 - \frac{\begin{bmatrix}k-2\\2\end{bmatrix}_q}{\begin{bmatrix}k-2\\2\end{bmatrix}_q + (q^{k-2}-q^{k-3})\begin{bmatrix}k-2\\1\end{bmatrix}_q}\right)\frac{q}{q+1}\right)^m,$$

after some calculation, we get that if we choose m as given in the theorem, then p will be smaller than 1. □

4.2 Cutting blocking sets from subgeometries

A standard construction for a $(k-1)$-fold blocking set in $PG(k-1,q)$, other than the union of $k-1$ lines, is the union of $k-1$ disjoint subgeometries of order $q^{\frac{1}{k-1}}$. Similarly to the case of lines, this $(k-1)$-fold blocking set is not necessarily a cutting blocking set. However, it might be possible that if we choose these subgeometries cleverly, then they do form a cutting blocking set. For example, in [6], the authors were able to construct a cutting blocking set in $PG(3,q^3)$ as the union of three disjoint order q subgeometries.

We propose another way to construct cutting blocking sets from subgeometries. Instead of taking disjoint $(k-1)$-dimensional order q subgeometries in $PG(k-1,q^{k-1})$, we consider $k-1$ hyperplanes in $PG(k-1,q^{k-2})$ in general position, and we take order q subgeometries in these hyperplanes.

Example 4.2.1. Let H be a hyperplane in $PG(4,8)$. Let us take three disjoint order 2 subgeometries in H such that they form a cutting blocking set (as in [6]). Let us denote them by B_1, B_2, B_3. Let us also fix three non-collinear points $P_1, P_2, P_3 \in H$, and let π denote the plane generated by them. In $PG(4,8)$, there are 9 hyperplanes through a plane. There exists a 3-dimensional order 2 subgeometry through any 4 points in general position, so it is possible to choose three subgeometries B_4, B_5, B_6 such that B_{3+i} intersects H exactly in P_i $(i = 1,2,3)$, and all of the 9 hyperplanes through π contain at least one point from $B_3 \cup B_4 \cup B_5$ outside of H. Then $B_1 \cup B_2 \cup B_3 \cup B_4 \cup B_5 \cup B_6$ is a cutting blocking set. Indeed, if a plane meets B_i for all i, then this has to be in H, because it contains three non-collinear points R_1, R_2, R_3 $(R_i \in B_i)$. But then it can meet B_{3+i} only in P_i, since this is the unique intersection point of B_{3+i} and H. So the only plane with this property is π. Suppose that there exists a hyperplane H' that is not generated. Since a hyperplane intersects all of the six hyperplanes containing the six subgeometries in a subspace of co-dimension two (a hyperplane of the hyperplane), which contains at least one point of the subgeometry, this means that H' intersects all of the six subgeometries in a subspace of co-dimension two. Then the only possibility is that this subspace of co-dimension two is the plane π. By construction, all hyperplanes through π are generated.

Remark 4.2.2. Note that this construction is not optimal, because in $PG(4,q)$, there is a cutting blocking set formed by the union of seven lines according to Theorem 4.1.7. But it still shows that there exist cutting blocking sets of this form.

Appendix A

Characterization of linear constant weight codes

Definition A.0.1. Take an arbitrary vector from each 1-dimensional subspace of $GF(q)^k$, and let M be the $k \times ((q^k-1)/(q-1))$ matrix which has these vectors as columns. The code $Ham_q(k)$ with parity check matrix M is called a *Hamming code*, and its dual code $Ham_q(k)^\perp$ (the one with generator matrix M) is called a *simplex code.*

Proposition A.0.2 ([20])**.** *Simplex codes are constant weight codes.*

Proof. We prove that each codeword of the simplex code $C = Ham_q(k)^\perp$ has weight q^{k-1}. Let us consider the matrix M from Definition A.0.1. We denote the rows of M by $r_1, r_2, \ldots, r_k$. Any codeword $c \in C$ can be written as $c = \alpha_1 r_1 + \alpha_2 r_2 + \cdots + \alpha_k r_k$ with unique coefficients $\alpha_1, \alpha_2, \ldots, \alpha_k$. Our goal is to determine the number of non-zero coordinates of c. If the j-th column of M is $(x_1, x_2, \ldots, x_k)^T$, then the condition that the j-th coordinate of c is 0, can be written as

$$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_k x_k = 0. \tag{A.1}$$

Since the columns of M can be seen as the projective coordinates of the points of $PG(k-1, q)$, (A.1) defines a hyperplane H in $PG(k-1, q)$. So, the number of vectors not fulfilling (A.1) equals the number of points in $PG(k-1, q)$ outside of H, which is

$$\frac{q^k-1}{q-1} - \frac{q^{k-1}-1}{q-1} = q^{k-1}.$$

Thus, the weight of any codeword $c \in C$ is q^{k-1}. □

Remark A.0.3. Proposition A.0.2 also implies that any two codewords of $Ham_q(k)^\perp$ have the same Hamming distance, so the codewords form a simplex in the Hamming space. Therefore the name simplex code.

It is clear that is we have a constant weight code C, then the code C' that we get from C by adding some 0-coordinates, is still constant weight.

We define the replication of a code as follows.

Definition A.0.4. Let C be a linear $[n, k]_q$-code. The *r-fold replication* of C is the $[rn, rk]_q$-code C^r that we get from C by concatenating each codeword with itself r times.

Obviously, any replication of a constant weight code is constant weight.

So, we know that simplex codes are constant weight codes, and replicating them a few times, or adding some 0-coordinates to them also results in constant weight codes. The following theorem – which is due to Bonisoli [8] – shows that essentially, all constant weight codes can be obtained in this way. Here, we give Bonisoli's result with the shorter and more elegant proof of Ward [26].

Theorem A.0.5 ([8, 26])**.** *Every linear constant weight code C is equivalent to a replicated simplex code, possibly with added 0-coordinates.*

Proof. To prove the theorem, we will use the following equation, which is one of the well-known MacWilliams identities.

$$\sum_{c \in C} w(c) = n(C) q^{k-1}(q-1). \tag{A.2}$$

Here, $n(C)$ denotes the number of coordinate positions in C that are not identically zero. One can obtain (A.2) by double counting the pairs (c, i), where $c \in C$, and i is a non-zero coordinate position of c. When we fix c, we get the left hand side, and when we fix i, we get the right hand side because the number of vectors in the k-dimensional vector space C that are outside of the hyperplane defined by $X_i = 0$, is $q^k - q^{k-1} = q^{k-1}(q-1)$.

Let C be a linear $[n, k]_q$ code with constant weight w ($k \geq 2$), and let M be the generator matrix of C such that

$$C = \{vM \colon v \in GF(q)^k\}.$$

We can safely assume that $n(C) = n$. (If this is not the case, we remove the 0-coordinates.) (A.2) now has the form

$$w(q^k - 1) = nq^{k-1}(q-1) \Leftrightarrow w\frac{q^k - 1}{q-1} = nq^{k-1}.$$

Since q and $\frac{q^k-1}{q-1}$ are co-prime, q^{k-1} must divide w, so we have

$$w = rq^{k-1} \tag{A.3}$$

for some positive integer r.

Let $V = GF(q)^k$, and let us consider its dual space V^* (the space of linear functionals on V.) Take a non-zero element $f \in V^*$. Then the code $C_f = \{vM \in C \colon f(v) = 0\}$ is a constant weight code of dimension $k - 1$, since the kernel of a non-zero linear functional has co-dimension 1. Furthermore, C_f is a subset of C, so it also has constant weight w. If we apply (A.2) to C_f, we get

$$w(q^{k-1} - 1) = n(C_f)q^{k-2}(q-1) \Leftrightarrow w\frac{q^k - 1}{q-1} = nq^{k-1}.$$

By (A.3), we have

$$rq\frac{q^{k-1} - 1}{q-1} = n(C_f),$$

and

$$n - n(C_f) = r\frac{q^k - 1}{q - 1} - rq\frac{q^{k-1} - 1}{q - 1} = r\left(\frac{q^k - 1 - q^k + q}{q - 1}\right) = r.$$

Note that if two linear functionals $f_1 \in V^*$ and $f_2 \in V^*$ have the same kernel K, then f_1 and f_2 are scalar multiples. If $K = V$, then this statement is trivial. If $K \neq V$, then $\dim K = \dim V - 1$, so we can write $V = K + \langle v \rangle$, where we can choose $v \in V$ such that $f_2(v) = 1$. Let $x = k + \lambda v$ be an arbitrary element of V. Then

$$f_1(x) = f_1(k) + \lambda f_1(v) = \lambda f_1(v),$$

and

$$f_2(x) = f_2(k) + \lambda = \lambda.$$

So, for all $x \in V$, we have that $f_1(x) = f_1(v) f_2(x)$.

Now let us consider the columns of M as linear functionals on V. The kernel of the j-th column consists of those vectors $v \in GF(q)^k$ for which the j-th coordinate of the codeword vM is 0. From the previous arguments, it follows that up to scalar multiples, every linear functional appears as a column of M exactly r times. Therefore, after scaling, we get that C is an r-fold replication of a simplex code, completing the proof. □

Appendix B

An oblivious transfer protocol

We will present the oblivious transfer protocol described in [12]. This is based on the idea of the well-known Diffie-Hellman (DH) key exchange protocol. Given a cyclic group $G = \langle g \rangle$ known to both Alice and Bob, they can agree on a secret key K, which they can use later to encrypt and decrypt messages. The DH protocol is as follows. Alice picks a random element a, computes $A = g^a$, and sends it to Bob. Bob picks a random element b, computes $B = g^b$, and sends it to Alice. Finally, Alice computes B^a, and Bob computes A^b, which are both equal to the element $K = g^{ab}$. Now if Alice wants to send the message m, she encrypts it using K, and she sends $e = E(m, K)$ to Bob, who decrypts it by calculating $D(e, K) = m$. This key exchange protocol is safe if we assume that the corresponding computational problem (given g^a and g^b, find g^{ab}), also known as the Computational Diffie-Hellman Problem (CDHP), is hard.

In our oblivious transfer protocol, instead of agreeing on one key, Alice, who holds the input $m = (m_1, m_2, \dots, m_n)$, will compute n different keys $K_1, K_2, \dots, K_n$. Bob, however, will know only one of the keys K_i where i is the index of the bit he wants to query. So Alice can send all the n encrypted messages $E(m_1, K_1), E(m_2, K_2), \dots, E(m_n, K_n)$. Bob will only be able to decrypt m_i.

Let $G = \langle g \rangle = \{1, g, g^2, \dots, g^{p-1}\}$ be a cyclic group of order p, p prime. Suppose that Alice holds the input $m = (m_1, m_2, \dots, m_n)$, and Bob wants to find out m_i. The steps of the oblivious transfer protocol are the following.

1. Alice picks a random element $a \in \{1, 2, \dots, p\}$, and computes $A = g^a$ and $L = A^a$.

2. Alice sends A to Bob.

3. Bob picks a random element $b \in \{1, 2, \dots, p\}$, and computes $B = A^i g^b$ and $K = A^b$.

4. Bob sends B to Alice.

5. For all $j \in [n]$, Alice computes $K_j = \frac{B^a}{L^j}$.

Notice that

$$K_i = \frac{B^a}{L^i} = \frac{A^{ai} g^{ab}}{A^{ai}} = g^{ab} = A^b = K.$$

We need to show two things. First of all, that Alice cannot find out i from B with higher probability than $1/n$. Secondly, that Bob cannot generate any other key $K_j \quad, j \neq i$.

For the first part, we observe that for a fixed $B_0 = g^{b_0}$, the probability that $B = B_0$ when $i = j$ is the probability that $\mathbb{P}(ai + b = b_0) = 1/p$, which is independent of j. This means that the probability of each possible value of B received by Alice is the same, no matter what index Bob chooses.

For the second part, we show that if Bob can generate two different keys K_i and K_j with positive probability, then the CDHP cannot be hard. Indeed, if Bob knows an algorithm that outputs K_i and K_j $(j \neq i)$ on the input $A = g^a$ with probability greater than ϵ, then for inputs $A = g^a$ and $A' = g^{a'}$, he can calculate $A^* = AA' = g^{a+a'}$. Then he can run his algorithm on all of the three inputs A, A', A^*. Let us denote the outputs by $K_i, K_j, K'_i, K'_j, K^*_i, K^*_j$, respectively. Then Bob can calculate

$$\left(\frac{K_i}{K_j}\right)^{\frac{1}{j-i}} = \left(\frac{B^a/L^i}{B^a/L^j}\right)^{\frac{1}{j-i}} = L = g^{a^2}.$$

Similarly, he can calculate $g^{a'^2}$ and $g^{(a+a')^2}$, from which

$$g^{aa'} = \left(\frac{g^{(a+a')^2}}{g^{a^2}g^{a'^2}}\right)^{\frac{p+1}{2}}.$$

The probability that his results are correct is the probability that all three pairs of keys were computed correctly, which is at least ϵ^3.

Bibliography

[1] G. N. Alfarano, M. Borello, and A. Neri. “A geometric characterization of minimal codes and their asymptotic performance”. In: *Advances in Mathematics of Communication* (2020).

[2] G. N. Alfarano et al. “Three combinatorial perspectives on minimal codes”. In: *SIAM Journal on Discrete Mathematics* 36.1 (2022), pp. 461–489.

[3] A. Ashikhmin and A. Barg. “Minimal vectors in linear codes”. In: *IEEE Transactions on Information Theory* 44.5 (1998).

[4] S. Ball and A. Blokhuis. “On the size of a double blocking set in PG(2,q)”. In: *Finite Fields and their Applications* 2.2 (1996), pp. 125–137.

[5] D. Bartoli and M. Borello. *Small strong blocking sets by concatenation.* 2021. arXiv: `2109.00584`.

[6] D. Bartoli et al. “On cutting blocking sets and their codes”. In: *Forum Mathematicum* 34 (2022).

[7] A. Beutelspacher. “On Baer subspaces of finite projective spaces”. In: *Mathematische Zeitschrift* 184.3 (1983), pp. 301–319.

[8] A. Bonisoli. “Every equidistant linear code is a sequence of dual Hamming codes”. In: *Ars Combinatorica* 18 (1984), pp. 181–186.

[9] A. E. Brouwer and A. Schrijver. “The blocking number of an affine space”. In: *Journal of Combinatorial Theory, Series A* 24.2 (1978), pp. 251–253.

[10] A. A. Bruen. “Arcs and multiple blocking sets”. In: *Combinatorica, Symposia Mathematica* 28 (1986).

[11] H. Chabanne, G. D. Cohen, and A. Patey. “Towards secure two-party computation from the wire-tap channel”. In: *Information Security and Cryptology, LNCS* 8565 (2014). Ed. by H. S. Lee and D. G. Han, pp. 34–46.

[12] T. Chou and C. Orlandi. “The simplest protocol for oblivious transfer”. In: *Progress in Cryptology - LATINCRYPT 2015 - 4th International Conference on Cryptology and Information Security in Latin America, Guadalajara, Mexico, August 23-26, 2015, Proceedings* (2015), pp. 40–58.

[13] G. D. Cohen, S. Mesnager, and A. Patey. “On minimal and quasi-minimal linear codes”. In: *IMACC 2013, LNCS* 8308 (2013). Ed. by M. Stam, pp. 85–98.

[14] A. A. Davydov et al. “Linear nonbinary covering codes and saturating sets in projective spaces”. In: *Advances in Mathematics of Communication* 5.1 (2011), pp. 119–147.

[15] A. A. Davydov et al. “Linear nonbinary covering codes and saturating sets in projective spaces”. In: *Advances in Mathematics of Communications* 5.1 (2011), pp. 119–147.

[16] L. Denaux. *Higgledy-piggledy sets in projective spaces of small dimension.* 2021. arXiv: `2109.08572`.

[17] Sz. L. Fancsali and P. Sziklai. “Lines in higgledy-piggledy arrangement.” In: *The Electronic Journal of Combinatorics* 21.2 (2014).

[18] T. Héger and Z. L. Nagy. “Short minimal codes and covering codes via strong blocking sets in projective spaces”. In: *IEEE Transactions on Information Theory* 68.2 (2022), pp. 881–890.

[19] Z. Heng, C. Ding, and Z. Zhou. “Minimal linear codes over finite fields”. In: *Finite Fields and their Applications* 54 (2018), pp. 176–196.

[20] R. Hill. *A first course in coding theory.* Oxford Applied Mathematics and Computing Sciences. The Claredon Press, Oxford University Press, New York, 1986.

[21] R. E. Jamison. “Covering finite fields with cosets of subspaces”. In: *Journal of Combinatorial Theory, Series A* 22 (1977), pp. 253–266.

[22] Gy. Kiss and T. Szőnyi. *Finite Geometries.* Chapman and Hall/CRC, 2019.

[23] J. L. Massey. “Minimal codewords and secret sharing”. In: *Proceedings of the 6th joint Swedish-Russian international workshop on information theory* (1993), pp. 276–279.

[24] L. Rédei. *Lückenhafte Polynome über endliche Körpern.* Birkhäuser Verlag, Basel, 1970.

[25] C. Tang et al. “Full characterization of minimal linear codes as cutting blocking sets”. In: *IEEE Transactions on Information Theory* 67.6 (2021), pp. 3690–3700.

[26] H. N. Ward. “An introduction to divisible codes”. In: *Designs, Codes and Cryptography* 17 (1999), pp. 73–79.