On products of linear error correcting codes

Mirandola, D.

On Products of Linear Error Correcting Codes

Proefschrift
ter verkrijging van
de graad van Doctor aan de Universiteit Leiden
op gezag van Rector Magnificus prof. mr. C.J.J.M. Stolker,
volgens besluit van het College voor Promoties
te verdedigen op woensdag 6 december 2017
klokke 15:00 uur

door

Diego Mirandola
geboren te Verona, Italië,
in 1988

Promotores:	Prof. dr. Ronald Cramer (CWI & Universiteit Leiden)
	Prof. dr. Gilles Zémor (Université de Bordeaux)
Copromotor:	Dr. Ignacio Cascudo (Aalborg University)

Samenstelling van de promotiecommissie:

Dr. Anne Canteaut (Inria Paris)

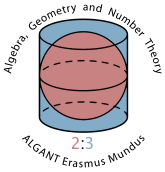
Dr. Ruud Pellikaan (Technische Universiteit Eindhoven)

Prof. dr. Bart de Smit (Universiteit Leiden)

Prof. dr. Aad van der Vaart (Universiteit Leiden)

Prof. dr. Qing Xiang (University of Delaware)

This work was funded by Erasmus Mundus Algant-Doc and was carried out at Universiteit Leiden, Université de Bordeaux and CWI Amsterdam.



Universiteit Leiden

université de BORDEAUX

CWI

Universiteit Leiden

THÈSE EN COTUTELLE PRÉSENTÉE

POUR OBTENIR LE GRADE DE

DOCTEUR

DE L'UNIVERSITÉ DE BORDEAUX

ET DE L'UNIVERSITÉ DE LEYDE

ÉCOLE DOCTORALE DE MATHÉMATIQUES ET INFORMATIQUE

INSTITUT DES MATHÉMATIQUES DE L'UNIVERSITÉ DE LEYDE

SPÉCIALITÉ Mathématiques Pures

Par Diego MIRANDOLA

Sur les Produits de Codes Correcteurs d'Erreurs Linéaires

Sous la direction de Ronald CRAMER et Gilles ZÉMOR

Soutenue le : 6 decembre 2017 à Leyde

Rapporteurs :

Ruud PELLIKAAN	Universitair Docent, TU Eindhoven
Qing XIANG	Professeur, University of Delaware

Membres du jury :

Anne CANTEAUT	Directrice de recherche, Inria Paris	Examinatrice
Ruud PELLIKAAN	Universitair Docent, TU Eindhoven	Rapporteur
Bart DE SMIT	Professeur, Universiteit Leiden	Président
Aad VAN DER VAART	Professeur, Universiteit Leiden	Examinateur

Ai miei nonni

Contents

Chapter 1

A Survey on Code Products

1.1 Codes and Code Products

In this thesis we study products of linear error correcting codes. We show three main results on such products and discuss applications to cryptography. Our methods are typically algebraic-combinatorial in nature, though sometimes probabilistic techniques will be involved. In this survey chapter we introduce codes and code products, and motivate our interest by showing how code products have appeared and are relevant in several topics. Finally, we will conclude this chapter with an overview of our results and a discussion putting their significance into perspective.

The following scenario, outlined by MacWilliams and Sloane in their handbook [48], may appear slightly old fashioned, but still helps introducing error correcting codes, as a mean to correct the errors introduced by some noisy communication channel.

> Suppose there is a telegraph wire from Boston to New York down which 0's and 1's can be sent. Usually when a 0 is sent it is received as a 0, but occasionally a 0 will be received as a 1, or a 1 as a 0. Let's say that [...] for each symbol there is a probability $p = 1/100$ that the channel will make a mistake.

Modern settings in which error correcting codes are used are for instance deep space communications, broadcasting and mass storage. These share a common

feature: retransmission of data is impossible, due to economic or practical constraints. As an example, suppose that, ten years ago, we recorded our favourite song on a disc, and now we want to listen to that song again. If we had done it "naively", that is if we saved one bit of the song (whatever it means) as one bit of information in the disc (whatever it means), then we would have no way to recover corrupted bits. Note that in this case retransmission, i.e. asking our ten-years-ago self to record the disc again, is not an option.

Roughly speaking, an error correcting code is given by a pair of functions `Enc` and `Dec`, standing for encode and decode respectively, with the following property: if a message m is encoded as $x = \texttt{Enc}(m)$, and x is turned into $\tilde{x}$ by a "small" error e, then $\tilde{x}$ is correctly decoded as $\texttt{Dec}(\tilde{x}) = m$. This situation is represented in Figure 1.1. Of course it shall be ensured that $\texttt{Dec}(\texttt{Enc}(m)) = m$, i.e. decoding always works properly if no corruption occurred.

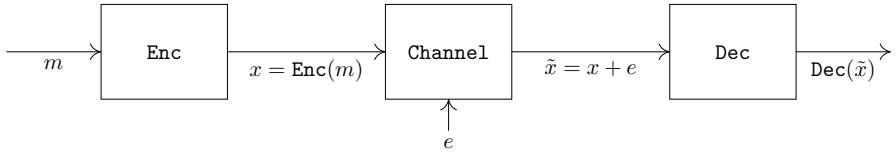


Figure 1.1

Refraining again from a proper mathematical formalization, we give an intuition of how encoding and decoding are possible. The encoding function `Enc` embeds a set $\mathcal{M}$ of allowed messages into a larger set $\mathcal{E}$ which contains, beside the set $\texttt{Enc}(\mathcal{M})$ of all meaningful encodings, all their corrupted variants. In addition, $\mathcal{E}$ is endowed with a metric structure, i.e. a notion of distance between any two elements of $\mathcal{E}$ is defined. In particular, this allows us to quantify an error, by measuring the distance between an encoding x and its corrupted version $\tilde{x}$. Now, assume that `Enc` maps the elements of $\mathcal{M}$ into elements of $\mathcal{E}$ which are sufficiently far apart from each other, with respect to this notion of distance. As above, assume that a message m is encoded as $x = \texttt{Enc}(m)$ and turned into $\tilde{x}$ by some error. If the error is sufficiently small, then x will be uniquely identified as the closest-to-$\tilde{x}$ element of $\texttt{Enc}(\mathcal{M})$, and the original message computed as $m = \texttt{Enc}^{-1}(x)$. Figure 1.2 represents this situation.

We are finally ready to formalize this setting. Prominent notions are those of linear code and Hamming distance, which model the copy of $\mathcal{M}$ in $\mathcal{E}$ containing all meaningful encodings and the metric structure of the ambient space $\mathcal{E}$. We will not be concerned with more general families of codes or with different metrics in this work. A wider introduction to the theory of linear error correcting codes is given in Section 2.5. Among the standard references on the topic we cite [37, 48, 71].

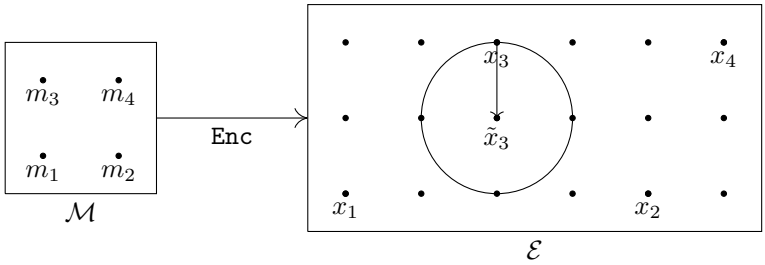


Figure 1.2: The message space is $\mathcal{M} = \{m_1, m_2, m_3, m_4\}$, its image is $\texttt{Enc}(\mathcal{M}) = \{x_1, x_2, x_3, x_4\} \subseteq \mathcal{E}$. The message m_3 is encoded as $x_3 = \texttt{Enc}(m_3)$ and transmitted, then turned into $\tilde{x}_3$ by some error. As x_3 is the closest element of $\texttt{Enc}(\mathcal{M})$, $\texttt{Dec}(\tilde{x}_3) = \texttt{Enc}^{-1}(x_3) = m_3$ is decoded correctly.

Let $\mathbb{F}$ be a finite field and let q denote its size[1]. Let $k \leq n$ be two positive integers. The encoding function $\texttt{Enc}$ maps messages from the $\mathbb{F}$-vector space $\mathcal{M} := \mathbb{F}^k$ into elements of the $\mathbb{F}$-vector space $\mathcal{E} := \mathbb{F}^n$. It is required to be injective, so that any encoded message can be unambiguously recovered. The image $C := \texttt{Enc}(\mathcal{M}) \subseteq \mathcal{E}$ is called a *code*, and it is *linear* if the encoding function is $\mathbb{F}$-linear. The elements of a code are called *codewords*. If this is the case, we can associate a $k \times n$ matrix G, a *generator matrix* of C, to the linear map $\texttt{Enc}$ so that $\texttt{Enc}(m) = mG$ and $C = \{mG : m \in \mathbb{F}^k\} \cong \mathbb{F}^k$. Here we write vectors in row form as it is customary in coding theory.

The *(Hamming) distance* between two vectors

$$x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \mathbb{F}^n$$

is

$$d(x, y) := |\{i : x_i \neq y_i\}|,$$

that is the number of positions in which x and y differ[2]. The *weight* of a vector is its distance from the zero vector, i.e. the number of positions in which it has a non-zero entry. The *minimum distance* of the code C is

$$d_{\min}(C) := \min\{d(x, y) : x, y \in C, x \neq y\} = \min\{\mathrm{wt}(x) : x \in C, x \neq 0\},$$

that is the minimal distance between any two distinct codewords, or equivalently the minimal weight of any non-zero codeword.

The decoding function $\texttt{Dec}$, for all $x \in \mathbb{F}^n$, is defined as follows: if there exists a unique $y \in C$ which minimizes $d(x, y)$ then $\texttt{Dec}(x) := \texttt{Enc}^{-1}(y)$;

[1] It is a well-known fact that q is a prime power.

[2] The Hamming distance between two vectors is always a non-negative integer and is indeed a distance in the usual mathematical sense: for any $x, y, z \in \mathbb{F}^n$ it holds that (i) $d(x, y) \geq 0$, and $d(x, y) = 0$ if and only if $x = y$, (ii) $d(x, y) = d(y, x)$, (iii) $d(x, y) \leq d(x, z) + d(z, y)$.

otherwise $\texttt{Dec}(x) := \perp$, an abort symbol. Observe that, even though such a function is well defined[3], it may be practically unfeasible to compute it by exhaustive search as the definition seems to require. Efficient, specific decoding algorithms are used instead in all applications: for instance, if a code has a t-error correcting pair (see the next section) then it has a t-error correcting algorithm with complexity $O(n^3)$. The minimum distance quantifies the error tolerance of a code. Errors are modeled as vectors which are added to the message: a vector $x \in \mathbb{F}^n$, corrupted by $e \in \mathbb{F}^n$, becomes $\tilde{x} = x + e$, and in this case we say that $\mathrm{wt}(e)$ errors occurred. It is easy to see that, for all $m \in \mathbb{F}^k$ and $e \in \mathbb{F}^n$ with $\mathrm{wt}(e) < d_{\min}(C)/2$, we have

$$\texttt{Dec}(\texttt{Enc}(m) + e) = m,$$

i.e. a code can tolerate errors of weight up to half of its minimum distance.

We continue with a remark about the relevant parameters of a code, namely length, dimension (as an $\mathbb{F}$-vector space) and minimum distance. For fixed length, it is of course desirable for dimension and minimum distance to be as large as possible, as these measure the size of the messages that we can encode and the amount of errors that we can tolerate. The trade-off between them is quantified by several classical bounds. Among them, the *Singleton Bound* claims that, for a code C of length n, it holds that

$$\dim C + d_{\min}(C) \leq n + 1.$$

If C attains this bound, i.e. if

$$\dim C + d_{\min}(C) = n + 1,$$

then it is said to be *maximum distance separable (MDS)*.

In order to define the product of two codes, we need to define some additional structure on the ambient space. Observe that the n-fold cartesian product $\mathbb{F}^n$ has a natural structure of $\mathbb{F}$-algebra, with multiplication induced by componentwise application of multiplication in $\mathbb{F}$, i.e. for all $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \mathbb{F}^n$ we define

$$xy := (x_1 y_1, \ldots, x_n y_n).$$

We also define $x^2 := xx$ and higher powers in the obvious way.

Given two codes $C, D \subseteq \mathbb{F}^n$, their *product* is the $\mathbb{F}$-linear span of the set of all products xy with $x \in C$ and $y \in D$,

$$CD := \langle xy : x \in C, y \in D \rangle.$$

[3]As $\texttt{Enc}$ is injective, $\texttt{Enc}^{-1}(y)$ is well defined for all $y \in C$.

Observe that the set of all products is not necessarily additively closed, so it is strictly contained in the code product in general. We also define the *square* $C^2 := CC$ of a code, and higher powers inductively. We are using the same notation for set cartesian product and code componentwise product, but the context will always help clarifying this ambiguity.

The product of two codes $C, D \subseteq \mathbb{F}^n$, sometimes called the *Schur product*, has usually been denoted by $C * D$, but we shall drop the star symbol to lighten notation. Products of codes turn up in a variety of situations, such as algebraic error correction, secret sharing and multiparty computation, algebraic complexity theory, additive combinatorics, and lately cryptanalysis. This survey will briefly encompass all these topics. A number of efforts have gone into describing the code-theoretic structure of code products, see [28, Chapter 12] and [65] for an extensive review of the current state of the art. In particular, [65] collects several technical results which will be cited explicitly and used in this thesis.

We can immediately state a trivial upper bound for the product dimension. For any pair of codes C, D it holds that

$$\dim CD \leq \dim C \dim D \quad \text{and} \quad \dim C^2 \leq \frac{\dim C(\dim C + 1)}{2}.$$

To see this, observe that if $\{x_1, \ldots, x_k\}$ and $\{y_1, \ldots, y_\ell\}$, where $k := \dim C$ and $\ell := \dim D$, are $\mathbb{F}$-bases of C and D respectively then the elements $x_i y_j$ with $1 \leq i \leq k, 1 \leq j \leq \ell$ generate CD and the elements $x_i x_j$ with $1 \leq i \leq j \leq k$ generate C^2. In fact it holds that these bounds are achieved by most codes: roughly speaking, code products typically fill the whole space. This is shown in Chapter 3, which is based on [13], for the second inequality, while for the first inequality the reader is referred to [64].

We conclude this section with an example. The codes we are going to describe not only have a nice mathematical structure, but are also widely used in practical applications. Fix $k \leq n \leq q$ and n pairwise distinct elements $\alpha_1, \ldots, \alpha_n \in \mathbb{F}$. Let $\mathbb{F}[X]_{<k}$ denote the vector space of all polynomials in the indeterminate X, with coefficients in $\mathbb{F}$, and degree less than k. The image of the evaluation map

$$\begin{array}{ccc} \mathbb{F}[X]_{<k} & \hookrightarrow & \mathbb{F}^n \\ f & \mapsto & (f(\alpha_1), \ldots, f(\alpha_n)) \end{array}$$

is a linear space, called a *Reed-Solomon code*. This map is injective because any polynomial of degree at most $k-1$ is uniquely determined by any k distinct evaluations, hence the code has dimension k. Moreover, a polynomial of degree at most $k-1$ has at most $k-1$ zeros, hence any codeword has weight at least

$n-k+1$. It follows that the code has minimum distance at least $n-k+1$, hence it is an MDS code.

The image of the standard basis of $\mathbb{F}[X]_{<k}$ is a basis of the code, and gives a generator matrix in Vandermonde form, namely

$$\begin{pmatrix} 1 & \cdots & 1 \\ \alpha_1 & \cdots & \alpha_n \\ \vdots & & \vdots \\ \alpha_1^{k-1} & \cdots & \alpha_n^{k-1} \end{pmatrix}.$$

Now let C and D be Reed-Solomon codes of length n with the same evaluation points $\alpha_1, \ldots, \alpha_n \in \mathbb{F}$. It is easy to see that also CD is a Reed-Solomon code with the same evaluation points and that

$$\dim CD = \dim C + \dim D - 1,$$

provided that this quantity is smaller than n. Indeed, if C and D are the images of $\mathbb{F}[X]_{<k}$ and $\mathbb{F}[X]_{<\ell}$ respectively, where $k := \dim C$ and $\ell := \dim D$, then CD is the image of $\mathbb{F}[X]_{<k+\ell-1}$, because $\mathbb{F}[X]_{<k+\ell-1}$ is spanned by the polynomials of the form fg with $f \in \mathbb{F}[X]_{<k}, g \in \mathbb{F}[X]_{<\ell}$. Observe that in this case the dimension is significantly smaller than the general upper bound obtained above[4].

The rest of this survey is dedicated to motivating our systematic code-theoretic study of code products, by showing a number of different contexts in which questions related to their possible parameters arise. An outline of the structure of this thesis concludes the chapter.

1.2 Error Locating Pairs

Possibly one of the earliest appearances of code products goes back to [57, 58, 59, 43] where it is relevant to the notion of error locating pairs used for algebraic decoding. On a historical note, we mention earlier appearances of code products in work on a proof of the Roos bound for cyclic codes [70] and on secure multiparty computation [6, 18].

Throughout this section, let t denote a positive integer. According to [57, 58], a *t-error locating pair* for a code $C \subseteq \mathbb{F}^n$ is a pair of codes $A, B \subseteq \mathbb{F}^n$ satisfying

(i) $AB \subseteq C^\perp$,

[4] We are comparing $\dim C + \dim D - 1$ with $\dim C \dim D$.

(ii) $\dim A > t$,

(iii) $d_{\min}(B^{\perp}) > t$.

Here the symbol "$\perp$" denotes the dual with respect to the standard inner product in $\mathbb{F}^n$. Observe that the product of A and B appears in the first property. If in addition it holds that

(iv) $d_{\min}(A) + d_{\min}(C) > n$

then the pair is said to be *t-error correcting*. In [59, 60] this definition was extended by allowing A and B to be defined over a finite extension of $\mathbb{F}$.

As an example, consider a pair of Reed-Solomon codes A and B with the same sequence of evaluation points. Assume that $\dim A = t + 1$ and $\dim B = t$. Then (A, B) is a t-error correcting pair for $C := (AB)^{\perp}$. Other constructions of error correcting pairs can be found in [58, 60] for algebraic-geometric codes and in [31] for cyclic codes.

These objects are relevant to the decoding problem. Suppose that the sum $\tilde{x} = x + e$ of a codeword $x \in C$ and of an error vector $e \in \mathbb{F}^n$ of weight t is known. Is it possible to correct the t errors in $\tilde{x}$, i.e. recover x, efficiently? The existence of error correcting pairs allows one to answer positively [57, 58]: given a t-error correcting pair, it is possible to build a t-error correcting algorithm with complexity $O(n^3)$, where n denotes the length of the code.

We show how this works in practice for a Reed-Solomon code C. Recall that in this case a codeword is of the form $x = (f(\alpha_1), \ldots, f(\alpha_n))$, where $f \in \mathbb{F}[X]_{<k}$ is a polynomial of degree less than k and $\alpha_1, \ldots, \alpha_n \in \mathbb{F}$ are pairwise distinct. Suppose that the vector

$$\tilde{x} = (\tilde{x}_1, \ldots, \tilde{x}_n) \in \mathbb{F}^n$$

is received, and that $\mathrm{wt}(\tilde{x} - x) \leq t$, i.e. at most t errors occurred. Our purpose is to recover the original codeword x, or equivalently the error vector $e := \tilde{x} - x$. The key observation is the following: a polynomial $\ell \in \mathbb{F}[X]$ of degree t which is zero at all error positions, i.e. $\ell(\alpha_i) = 0$ for all i such that $\tilde{x}_i - f(\alpha_i) \neq 0$, satisfies

$$f(\alpha_i)\ell(\alpha_i) = \tilde{x}_i \ell(\alpha_i)$$

for all $i = 1, \ldots, n$. This is a system of n equations which is quadratic in the coefficients of the polynomials f and ℓ. Let A denote the Reed-Solomon code corresponding to the polynomial space $\mathbb{F}[X]_{<t+1}$ with evaluation points $\alpha, \ldots, \alpha_n$, so that $(\ell(\alpha_1), \ldots, \ell(\alpha_n)) \in A$. Observe that at the left-hand side we have the entries of the vector

$$(f(\alpha_1)\ell(\alpha_1), \ldots, f(\alpha_n)\ell(\alpha_n)),$$

which belongs to the product code CA. We can transform this quadratic system into a linear system by replacing the left-hand side with a polynomial $g \in \mathbb{F}[X]$ of degree at most $k + t$ which needs to satisfy

$$g(\alpha_i) = \tilde{x}_i \ell(\alpha_i)$$

for all $i = 1, \ldots, n$. Now the unknowns are the $k + 2t$ coefficients of the polynomials g and ℓ. Finally, if a solution of the form $g = f\ell$ is obtained, then $f = g/\ell$ can be recovered.

The codes C and A in our example correspond to C and A in the definition of an error correcting pair. The code B in the definition corresponds to the dual of the product code CA in our example, fulfilling the first requirement of the definition. The other conditions ensure that the quadratic system above has a solution, that such a solution is of the desired form and, finally, that it is unique.

1.3 Secret Sharing and Secure Multiparty Computation

"Products" and "squares" of codes are the primary focus of work on arithmetic secret sharing [19, 11, 15, 16] and its application to secure multi-party computation [27]. In this thesis we will not be concerned with notions of secret sharing without arithmetic properties, and the interested reader is referred to [5, 56]. Secret sharing has as main motivation and application secure multiparty computation (MPC). Secure multiparty computation studies the problem of evaluating a function on inputs submitted by several players, while guaranteeing privacy and correctness even in presence of dishonest players, who may try to acquire more information than they are supposed to, possibly deviating from the protocol.

Secret sharing deals with the problem of protecting a *secret* by distributing *shares* among a number of *players*, in a way so that only some privileged player coalitions are *accepted*, i.e. can recover the secret by putting together their shares, while other player coalitions are *rejected*, i.e. any possible secret is equally likely to them. An algebraic structure which implements this functionality is called a *secret sharing scheme*. The family of all accepted set and the family of all rejected set are called the *access structure* and the *adversary structure* respectively. A scheme has *t-privacy* if the adversary structure contains any set of (at most) t players, and has *r-reconstruction* if the access structure contains any set of (at least) r players. Here t and r are positive integers with $1 \leq t < r \leq n$, where n denotes the number of players. A scheme with $(r-1)$-privacy and r-reconstruction is called *r-threshold*.

To share a secret $s \in \mathbb{F}$ among n players using a linear code $C \subseteq \mathbb{F}^{n+1}$, one standardly chooses a random codeword whose 0-th coordinate equals s and define the i-th share to be the i-th coordinate[5] [50]. Then the privacy and reconstruction parameters of the scheme can be estimated from the parameters of the code: precisely, the scheme has $(d_{\min}(C^{\perp}) - 2)$-privacy and $(n - d_{\min}(C) + 2)$-reconstruction[6]. Analogously, to share a secret vector $s \in \mathbb{F}^k$ among n players using a linear code $C \subseteq \mathbb{F}^{n+k}$, one standardly chooses a random codeword with some fixed k-tuple of coordinates equal to s and distributes the other coordinates as shares. Again, privacy and reconstruction of the scheme can be estimated using the minimum distance of the dual and of the code itself respectively.

When two secrets s and s' are shared in this way, summing coordinatewise the share vectors gives naturally a share vector of the coordinatewise sum $s + s'$ of the secrets[7]. When one considers the product of the share vectors, one obtains a share of the product ss', but for a different secret sharing scheme, namely that associated to the product code C^2. We say that a secret sharing scheme is *arithmetic* if it supports multiplication, i.e. if the product of two secrets can be reconstructed from the product of the share vectors. To prevent a common misunderstanding, we highlight here that, in practical applications, the product reconstruction property is not used in the straightforward way, i.e. to recover the secret product given the share products. Instead, it allows to reduce a secure multiplication to a secure computation of a linear functional.

If C is a Reed-Solomon code, the above construction defines the well-known Shamir scheme [67]. Let $\alpha_1, \ldots, \alpha_n$ be non-zero, pairwise distinct elements of $\mathbb{F}$. To share a secret $s \in \mathbb{F}$, one picks uniformly at random a polynomial f of degree less than a fixed parameter k, under the constraint that $f(0) = s$, and defines the i-th share to be $f(\alpha_i)$. It turns out that the scheme has $(k-1)$-privacy and k-reconstruction, hence in particular it is k-threshold. Assuming that $2k - 1 \leq n$, we have that the code square C^2 is also a Reed-Solomon code, hence it defines a scheme with $(2k-1)$-reconstruction. It follows that Shamir's scheme is arithmetic in this case.

The above operational definition of secret sharing can be formalized in several equivalent ways. Among these we mention the notion of *codex*[8], introduced in [16] and extensively treated in [28]. For instance, using this definition, an $(n, t, 1, r)$-codex for $\mathbb{F}$ over $\mathbb{F}$ is a secret sharing scheme among n players with t-privacy and r-reconstruction, while an $(n, 1, 2, n)$-codex is an arithmetic secret sharing scheme among n players. An $(n, t, 2, n-t)$-codex is an arithmetic secret sharing scheme with t-privacy and $(n-t)$-product reconstruction, i.e.

[5] We index the coordinates of $\mathbb{F}^{n+1}$ with $\{0, 1, \ldots, n\}$.
[6] Here $C^{\perp}$ denotes the dual of C with respect to the standard inner product in $\mathbb{F}^{n+1}$.
[7] Because the code is linear.
[8] The plural of codex is *codices*.

the product of two secrets can be reconstructed from any set of $n - t$ products of shares. Such a secret sharing scheme is called *t-strongly multiplicative*. Roughly speaking, given an (n, t, d, r)-codex, n is the number of players, t is the privacy threshold, d is the multiplicative depth and r is the product reconstruction threshold. Moreover we can have codices for arbitrary $\mathbb{F}$-algebras, such as $\mathbb{F}^k$ or finite extension fields of $\mathbb{F}$, meaning that the secret lies in this algebra. The strength of this notion is that it encompasses all known relevant variations on arithmetic secret sharing, and notions from other fields, such as the one of bilinear multiplication algorithm introduced in Section 1.4, as well. In addition, in [28, Section 12.5.4] codices are used to present a variation on the decoding method based on error correcting pairs.

Since the parameters of a code are relevant to the associated secret sharing scheme, studying the parameters of C^2 becomes important. In order to be useful for strongly multiplicative secret sharing, a code needs to have a dual with good minimum distance (to control the privacy threshold) and a square with good minimum distance as well (to control the product reconstruction threshold). Hence interest is focused on families of linear codes $(C_i)_{i\in\mathbb{N}}$ of unbounded length, such that the families of the dual codes $(C_i^\perp)_{i\in\mathbb{N}}$ and of the squares $(C_i^2)_{i\in\mathbb{N}}$ are asymptotically good, i.e.

$$\limsup_{i\to\infty} \frac{d_{\min}(C_i^\perp)}{n_i} > 0, \quad \limsup_{i\to\infty} \frac{d_{\min}(C_i^2)}{n_i} > 0,$$

where, for all $i \in \mathbb{N}$, n_i denotes the length of C_i [11].

Such families were first constructed, over all finite fields of size $q \geq 49$ with q square, in [19] using techniques from algebraic geometry, namely asymptotically good towers of algebraic function fields. In [11] these families of codes were combined with a dedicated field descent technique to obtain arithmetic secret sharing schemes with good parameters over any field[9]. This work was subsequently extended in [15, 17], with the construction of asymptotically good families of codes over fields of size $q = 8, 9$ and $q \geq 16$, involving novel algebraic-geometric ideas such as torsion limits and Riemann-Roch systems of equations for function fields. We remark that no elementary construction of such families of codes is known so far.

Besides its original application, the result of [19] played a central role in the paper [40] on the "secure MPC in the head" paradigm: here secure MPC is used as an abstract primitive for efficient two-party cryptography[10]. Among other subsequent fundamental results, let us mention that asymptotically good codes whose dual and square are also asymptotically good are an essential in-

[9] The corresponding codes may be bad.

[10] For an extensive treatment of the interplay between secure multiparty computation, (arithmetic) secret sharing, codes and algebraic geometry, please consult [28].

gredient in the recent constructions of efficient unconditionally secure oblivious transfer protocols from noisy channels [38].

Bilinear complexity theory, briefly discussed in Section 1.4, is concerned with a similar problem, namely the construction of asymptotically good families of codes whose squares are also asymptotically good. As opposed to the case of secret sharing, in this setting no condition is imposed on the duals. Such families have been shown to exist for all finite fields in [63]. This construction carefully combines algebraic geometric codes that have asymptotically good higher powers, which can be constructed over large enough finite fields, with a field descent concatenation technique. Again, no elementary construction is known in this case.

Finally, recent work [1], inspired by [53], exploited combinatorial properties of codes and code products to prove that, among all t-strongly multiplicative secret sharing schemes on n players, only Shamir's scheme can achieve the optimal $t = (n-1)/3$.

1.4 Bilinear Multiplication Algorithms

Code products also appear in algebraic complexity theory [21]. There one wishes to express multiplication in some finite extension field $\mathbb{L}/\mathbb{F}$ through a bilinear algorithm involving a small number of multiplications in $\mathbb{F}$: given $x, y \in \mathbb{L}$, instead of computing their product directly, one wants to map them into $\mathbb{F}^n$ using a linear map σ, componentwise multiply $\sigma(x)$ and $\sigma(y)$, and then map their product back to $\mathbb{L}$ using another linear map ρ. The requirement is that

$$xy = \rho(\sigma(x)\sigma(y))$$

for all $x, y \in \mathbb{L}$, where the multiplication at the left-hand side is in $\mathbb{L}$ while the multiplication at the right-hand side is in $\mathbb{F}^n$. In other words, the following diagram has to be commutative.

$$\begin{array}{ccccc}
\mathbb{F}^n & & \mathbb{F}^n & & \mathbb{F}^n \\
\cup\!| & & \cup\!| & & \cup\!| \\
C & \times & C & \longrightarrow & C^2 \\
\sigma \uparrow & & \sigma \uparrow & & \downarrow \rho \\
\mathbb{L} & \times & \mathbb{L} & \longrightarrow & \mathbb{L}
\end{array}$$

To better highlight how this topic is related to code squares, we remark that the image C of $\mathbb{L}$ via σ is a linear subspace of $\mathbb{F}^n$, i.e. a code, and that the

image of C via the componentwise multiplication in $\mathbb{F}^n$ spans C^2.

The pair (σ, ρ) is called a *bilinear multiplication algorithm* for $\mathbb{L}$ over $\mathbb{F}$, and n is its *expansion*. The minimal among the expansions of all bilinear multiplication algorithms for $\mathbb{L}$ over $\mathbb{F}$ is called the *bilinear complexity* of $\mathbb{L}$ over $\mathbb{F}$. If a bilinear multiplication algorithm for $\mathbb{L}$ over $\mathbb{F}$ with expansion n exists, then we can reduce multiplication in $\mathbb{L}$ to n multiplications in $\mathbb{F}$ (and application of two linear maps).

As an example, textbook multiplication in $\mathbb{L}$, which consists of identifying elements of $\mathbb{L}$ with univariate polynomials with coefficients in $\mathbb{F}$ and multiplying them as such, is a bilinear multiplication algorithm with expansion $n = \binom{k+1}{2}$, where k denotes the degree of the field extension.

As anticipated in the previous section, this notion is encompassed by the codex definition: a bilinear multiplication algorithm for $\mathbb{L}$ over $\mathbb{F}$ is an $(n, 0, 2, n)$-codex for $\mathbb{L}$ over $\mathbb{F}$. Recall that an $(n, 0, 2, n)$-codex is a secret sharing scheme among n players with 0-privacy and n-product reconstruction. In order to obtain a bilinear multiplication algorithm from such a scheme, it suffices to define σ to be the map which assigns to a secret a set of valid shares, and ρ the map which reconstructs the product of two secrets from the products of the shares. In addition, we require that the dimension of $\sigma(\mathbb{L})$ as an $\mathbb{F}$-vector space equals the degree of $\mathbb{L}$ as an extension field of $\mathbb{F}$. This prevents redundancies in the bilinear multiplication algorithm.

Among the first results on the topic, we mention [74] and [46]. In [74] it is proved that any bilinear multiplication algorithm has expansion $n \geq 2k - 1$, where k denotes the degree of the field extension. In [46] it is proved that the bilinear complexity is a quasi-linear function of the extension degree k, i.e. it is bounded by $f(k)k$ where f satisfies

$$f(k) < \log \log \cdots \log k$$

for any number of applications of the logarithm function. For recent developments, we refer to [3, 14, 61, 17].

1.5 Additive Combinatorics

Additive combinatorics [69] investigates the additive structure of sets. Given an abelian group G and two non-empty subsets $A, B \subseteq G$, additive combinatorics studies, for instance, the size of the sum set

$$A + B := \{a + b : a \in A, b \in B\}$$

and the necessary conditions so that the sum set size is minimal. This problem is the object of the classical theorems of Kneser [42] and Vosper [72]. For background on and proofs of Kneser and Vosper's Theorems we refer to [69]. Kneser's Theorem implies in particular that if A, B are subsets of an abelian group such that

$$|A + B| < |A| + |B| - 1$$

then $A + B$ must be periodic, i.e. there exists a non-zero element g of the abelian group that stabilizes $A + B$ so that we have $A + B + g = A + B$. Vosper's Theorem is a characterization of pairs of subsets A, B of the integers modulo a prime p with the property that $|A + B| = |A| + |B| - 1$. It states that, excluding some degenerate cases, A, B must be arithmetic progressions with the same difference.

The purpose of some recent works [36, 2, 4, 53] is to translate questions from classical additive combinatorics to different contexts. As an example, one can take a field extension $\mathbb{L}/\mathbb{K}$ instead of an abelian group as ambient space. In this context, we can consider two $\mathbb{K}$-vector spaces S, T contained in $\mathbb{L}$ and study the dimension of the product vector space

$$ST := \langle st : s \in S, t \in T \rangle,$$

where the product is the field multiplication in $\mathbb{L}$ and the brackets $\langle \cdot \rangle$ mean that the linear span is taken. It was proved in [36] that an analogue of Kneser's Theorem carries over to this case[11].

A subsequent step is to translate additive combinatorics into the context of coding theory: consider $\mathbb{F}^n$, where $\mathbb{F}$ is finite field, as ambient space, and let $C, D \subseteq \mathbb{F}^n$ be two $\mathbb{F}$-vector spaces, i.e. two codes. In this setting, the natural counterpart of the sum set size is the dimension of the code product CD. An even more general context is considered in [4], where $\mathbb{F}^n$ is replaced by an arbitrary algebra over the base field.

1.6 Cryptanalysis of McEliece Cryptosystem

As a last motivation, there has been some recent use of code squares in the cryptanalysis of variants of the McEliece cryptosystem. McEliece cryptosystem [52] is a code-based public-key cryptosystem which relies on the hardness of the general decoding problem [8].

Let C be a code, with encoding and decoding algorithm `Enc` and `Dec`, and assume that `Dec` can correct efficiently t errors. For instance, one may think that C admits a t-error correcting pair. Then a secret message m can be

[11] Under the additional assumption that the field extension is separable.

encrypted as $c := \texttt{Enc}(m) + e$, where e is a random vector of weight t. Due to the error correcting property of the algorithm, it is possible to recover the original message as

$$m = \texttt{Dec}(c) = \texttt{Dec}(\texttt{Enc}(m) + e).$$

An external adversary (who does not know Dec, or in our example a t-error correcting pair for C), in order to recover m, is required to solve the general decoding problem, which is known to be hard.

Concretely, the private key consists of C and Dec, while the public key is a generator matrix G of C together with the decoding capability t of Dec. The matrix G is "scrambled" in a way so that the original structure of the code is hidden[12], and consequently the efficient decoding algorithm as well,. To build this cryptosystem, Goppa codes [48, Chapter 12] are standardly used. One immediately notices that the public key, being a matrix, is huge: this is the main disadvantage of this cryptosystem.

The main advantage is the reliance on the general decoding problem, which makes this cryptosystem resistant even in a post-quantum scenario. On the other hand, recent attacks aim to recover the "hidden" structure of the code from the "scrambled" matrix, hence the efficient decoding algorithm, rather than the original message directly via general decoding algorithms. The idea exploited in [34, 23, 25, 26] is that Goppa codes have a square that has a substantially smaller dimension than typical random linear codes: this allows to build a distinguisher which can be used to attack the cryptosystem.

As an example, we quickly sketch how code squares were used in [24] to attack Wieschebrink's encryption scheme [73]. To give a bit of context, we recall that McEliece cryptosystem based on Reed-Solomon codes, as proposed in [55], was proved to be insecure in [68]: here it was shown that, in the case of a Reed-Solomon code, a generator matrix in standard form can be recovered efficiently from any scrambled one. To fix this, Wieschebrink [73] proposed to insert in the generator matrix some random columns: this suffices to make the algorithm [68] fail, while preserving the decryption capability of the code. This variant was broken in [24], using arguments based on code squares. The idea that is exploited is that the dimension of the square of a Reed-Solomon code C is

$$\dim C^2 = 2 \dim C - 1,$$

while in the general, random case the square of a code tends to fill the full space[13]. Let C be a code obtained by inserting in a Reed-Solomon code some random columns. Let i be a coordinate and let $C_{\overline{i}}$ be the code obtained

[12] To obtain such a matrix, one can take any generator matrix G' and define $G := HG'P$ where H is invertible and P is a permutation matrix.

[13] This is formalized and proved in Chapter 3, which is based on [13].

by puncturing C at i, i.e. the code obtained from C by removing the i-th coordinate of all its codewords. Now compare the dimension of the squares of C and $C_{\bar{i}}$: if the square dimension decreased after puncturing, i.e. if

$$\dim C_{\bar{i}}^2 < \dim C^2,$$

then the i coordinate corresponds to a random column. Iterating this argument, one can remove all random columns, and finally be able to apply [68] to recover the original Reed-Solomon code.

1.7 Outline of the Thesis

The main body of this thesis consists of three chapters, dedicated to the following three different published works.

[13] I. Cascudo, R. Cramer, D. Mirandola, and G. Zémor. Squares of Random Linear Codes. *IEEE Transactions on Information Theory*, 61(3):1159–1173, March 2015.

[53] D. Mirandola and G. Zémor. Critical Pairs for the Product Singleton Bound. *IEEE Transactions on Information Theory*, 61(9):4928–4937, Sept. 2015.

[12] I. Cascudo, R. Cramer, D. Mirandola, C. Padró, and C. Xing. On secret sharing with nonlinear product reconstruction. *SIAM Journal on Discrete Mathematics*, 29(2):1114–1131, 2015.

This is preceded by a preliminary chapter where all the mathematical background necessary to read and understand the discussed topics is introduced.

The purpose of Chapter 3, which is based on [13], is to answer the following question: does the square of a code "typically" fill the whole space? We give a positive answer, for codes of dimension k and length roughly $k^2/2$ or smaller. Moreover, the convergence speed is exponential if the difference $k(k+1)/2 - n$ is at least linear in k. The proof uses random coding and combinatorial arguments, together with algebraic tools involving the precise computation of the number of quadratic forms of a given rank, and the number of their zeros. As a consequence of this work, it is impossible to rely on random codes in situations where properties of the code square are required, as it will be the full space, hence trivial, with high probability. This impacts for instance secret sharing: it is known [20] that linear, non-multiplicative secret sharing schemes with optimal privacy and reconstruction parameters can be constructed using

random codes; however, due to the results of Chapter 3, such schemes will most likely not be arithmetic[14].

In Chapter 4, based on [53], we characterize Product-MDS pairs of linear codes, i.e. pairs of codes C, D whose product under coordinatewise multiplication has maximum possible minimum distance as a function of the code length and the dimensions $\dim C, \dim D$. We prove in particular, for $C = D$, that if the square of the code C has minimum distance at least 2, and (C, C) is a Product-MDS pair, then either C is a generalized Reed-Solomon code, or C is a direct sum of self-dual codes. The proof is based on new coding-theory analogues of classical theorems of additive combinatorics, namely Kneser's and Vosper's Theorems. More recently [1], these techniques have been used to prove that, among all t-strongly multiplicative secret sharing schemes on n players, only Shamir's scheme can achieve the optimal $t = (n-1)/3$.

Chapter 5, based on [12] focuses on a foundational question which is novel to the best of our knowledge. Multiplicative linear secret sharing is a fundamental notion in the area of secure multiparty computation and, since recently, in the area of two-party cryptography as well. In a nutshell, this notion guarantees that "the product of two secrets is obtained as a linear function of the vector consisting of the coordinatewise product of two respective share-vectors". Suppose we abandon the linearity condition and instead require that this product is obtained by some, not-necessarily-linear "product reconstruction function". Is the resulting notion equivalent to multiplicative linear secret sharing? We show the (perhaps somewhat counter-intuitive) result that this relaxed notion is strictly more general. Concretely, fix a finite field as the base field over which linear secret sharing is considered. Then we show there exists an (exotic) linear secret sharing scheme with an unbounded number of players n such that it has t-privacy with $t = \Omega(n)$ and such that it does admit a product reconstruction function, yet this function is necessarily nonlinear. In addition, we determine the minimum number of players for which those exotic schemes exist. Our proof is based on combinatorial arguments involving quadratic forms. It extends to similar separation results for important variations, such as strongly multiplicative secret sharing.

The first section of each chapter is an overview of the contents of the chapter itself.

[14] For completeness, we mention that [20] points out that also random self-dual codes yield secret sharing schemes with optimal privacy and reconstruction parameters. In addition, this schemes are trivially multiplicative: as the inner product of any two codewords is zero, any coordinate of the product word can be expressed as a linear function of the others. However, this construction does not support more general notions of secret sharing, such as those that require larger secrets or that can tolerate an adversary who deviates from the protocol.

Chapter 2

Preliminaries

2.1 Overview

In this preliminary chapter we introduce all the mathematical background necessary to read and understand the discussed topics.

Section 2.2 introduces the notation used throughout the whole thesis.

Section 2.3 refreshes some basic notions from the theory of bilinear forms and establish a correspondence between bilinear forms and tensor products that will be useful in the future. Most of the material can be found in textbooks like [45].

Section 2.4 introduces the basic theory of quadratic forms, we outline their classification, and we prove some combinatorial results that will be useful later on in this work. Our main reference is [44]. More specific references will be given throughout the section.

Section 2.5 expands the discussion started in Section 1.1 on the theory of linear error correcting codes by giving a better formalization of the definitions and results that we have already mentioned, and by introducing new results as well. Standard references are [37, 48, 71]. We will be especially focused on the theory of code products, to which Section 2.5.2 is dedicated. The literature concerning this topic is quite limited, we cite [65].

Section 2.6 introduces arithmetic secret sharing, which is the main motivation for our study of code products. In particular, Section 2.6.3 is dedicated to showing how codes and secret sharing schemes are closely related. We conclude this section with a quick sketch of how a secure multiparty computation

protocol can be built from a secret sharing scheme. The main reference on this topic is [28]. Among the possible equivalent definitions of secret sharing scheme, we pick the one which best suits our needs.

2.2 Notation

We introduce the notation that will be used throughout the whole thesis.

We denote by $\mathbb{N}$ the set of natural numbers, with $\mathbb{R}$ the field of real numbers and with $\mathbb{R}_{>0}$ the set of positive real numbers. We write $\mathbb{K}$ to denote an arbitrary field, or $\mathbb{F}$ in the case of a finite field. If the field size needs to be highlighted, we write $\mathbb{F}_q$ instead of $\mathbb{F}$, where q is the field size. If we need to introduce an additional field, e.g. an extension, we use $\mathbb{L}$. We denote by $\mathbb{K}[X]$ the ring of polynomials in the indeterminate X, with coefficients in the field $\mathbb{K}$. The subspace of $\mathbb{K}[X]$ containing only the polynomials of degree less than k, where k is a positive integer, is denoted by $\mathbb{K}[X]_{<k}$.

We also use some standard notation to describe the asymptotic behavior of some functions. Let f and g be functions and assume that it makes sense to consider their limit at $x \to +\infty$, for instance one may think that f and g are defined over $\mathbb{R}_{>0}$ or over $\mathbb{N}$. Then we say that

- $f = o(g)$ if $f(x)/g(x) \to 0$ as $x \to +\infty$,
- $f = O(g)$ if $|f(x)| \leq \alpha |g(x)|$ as $x \to +\infty$, for some $\alpha \in \mathbb{R}_{>0}$,
- $f = \Omega(g)$ if $f(x) \geq \beta g(x)$ as $x \to +\infty$, for some $\beta \in \mathbb{R}_{>0}$.

2.3 Bilinear Algebra

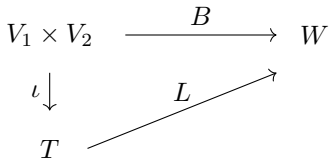
In this section we refresh some basic notions from the theory of bilinear forms and establish a correspondence between bilinear forms and tensor products that will be useful in the future. Most of the material can be found in textbooks like [45].

Throughout this section, let $\mathbb{K}$ be an arbitrary field. Let V_1, V_2 and W be $\mathbb{K}$-vector spaces. Recall that a map $B\colon V_1 \times V_2 \to W$ is *bilinear* if, for all $v_1 \in V_1$ and $v_2 \in V_2$, the maps

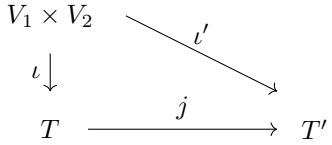
$$B(v_1, \cdot)\colon \begin{array}{ccc} V_2 & \longrightarrow & W \\ y & \longmapsto & B(v_1, y) \end{array} \qquad B(\cdot, v_2)\colon \begin{array}{ccc} V_1 & \longrightarrow & W \\ x & \longmapsto & B(x, v_2) \end{array}$$

are linear. We recall the fundamental notion of tensor product.

THEOREM 2.3.1. *There exists a unique pair (T, ι), where T is a $\mathbb{K}$-vector space and $\iota\colon V_1 \times V_2 \to T$ is a bilinear map, with the following property: for all $\mathbb{K}$-vector spaces W and for all bilinear maps $B\colon V_1 \times V_2 \to W$ there exists a unique linear map $L\colon T \to W$ such that $B = L \circ \iota$, i.e. the following diagram commutes.*



Here uniqueness means that if (T', ι') is another pair with the same property then there exists a unique isomorphism $j\colon T \to T'$ such that $j \circ \iota = \iota'$, i.e. the following diagram commutes.



DEFINITION 2.3.2. We call the unique vector space given by the previous theorem the *tensor product* of V_1 and V_2 and we denote it by $V_1 \otimes V_2$.

The tensor product of two $\mathbb{K}$-vector spaces V_1 and V_2 is a $\mathbb{K}$-vector space as well. If $\{x_1, \ldots, x_k\}$ and $\{y_1, \ldots, y_\ell\}$ are $\mathbb{K}$-bases of V_1 and V_2 respectively then $\{x_i \otimes y_j : 1 \leq i \leq k, 1 \leq j \leq \ell\}$ is a $\mathbb{K}$-basis of $V_1 \otimes V_2$ and $\dim V_1 \otimes V_2 = \dim V_1 \dim V_2$. The elements of $V_1 \otimes V_2$ are (finite) formal sums of simple tensors $x \otimes y$, with $x \in V_1, y \in V_2$, under the conditions:

1. $(x + x') \otimes y = x \otimes y + x' \otimes y$ for all $x, x' \in V_1$ and $y \in V_2$;
2. $x \otimes (y + y') = x \otimes y + x \otimes y'$ for all $x \in V_1$ and $y, y' \in V_2$;
3. $(\lambda x) \otimes y = \lambda(x \otimes y) = x \otimes (\lambda y)$ for all $x \in V_1$, $y \in V_2$ and $\lambda \in \mathbb{K}$.

Let V be a $\mathbb{K}$-vector space of finite dimension k.

DEFINITION 2.3.3. We call a bilinear map $B\colon V \times V \to \mathbb{K}$ a *bilinear form* on V. We say that B is

a. *non-degenerate* if $B(x, y) = 0$ for all $y \in V$ implies $x = 0$,

b. *symmetric* $B(x,y) = B(y,x)$ for all $x, y \in V$,

c. *alternating* if $B(x,x) = 0$ for all $x \in V$.

We denote by $\mathrm{Bil}(V)$ the $\mathbb{K}$-vector space of all bilinear forms on V. Its subspaces of all symmetric and alternating forms are denoted by $\mathrm{Sym}(V)$ and $\mathrm{Alt}(V)$ respectively.

Given $B \in \mathrm{Bil}(V)$, its *transpose* is the bilinear map $B^T \colon V \times V \to \mathbb{K}$ defined by $B^T(y,x) := B(x,y)$ for all $x, y \in V$. So by definition B is symmetric if and only if $B = B^T$. Also note that if B is alternating then $B = -B^T$, i.e. $B(x,y) = -B(y,x)$ for all $x, y \in V$: this follows by the identity $B(x+y, x+y) = B(x,x) + B(x,y) + B(y,x) + B(y,y)$ and by the definition of alternating form. If $\mathrm{char}\,\mathbb{K} \neq 2$ then the converse also holds, as in this case $B(x,x) = -B(x,x)$ implies that $B(x,x) = 0$.

Observe that $\mathrm{Bil}(V) = \mathrm{Sym}(V) \oplus \mathrm{Alt}(V)$ if $\mathrm{char}\,\mathbb{K} \neq 2$. Indeed, we can write any $B \in \mathrm{Bil}(V)$ as

$$B := \frac{1}{2}(B + B^T) + \frac{1}{2}(B - B^T),$$

where the first summand is in $\mathrm{Sym}(V)$ and the second summand is in $\mathrm{Alt}(V)$. As $\mathrm{char}\,\mathbb{K} \neq 2$, $\mathrm{Sym}(V) \cap \mathrm{Alt}(V) = 0$ follows from the previous observation. On the other hand, if $\mathrm{char}\,\mathbb{K} = 2$ then we have $\mathrm{Alt}(V) \subseteq \mathrm{Sym}(V)$.

Let V^* denote the dual space of V, i.e. the vector space of all linear forms on V. By the universal property of the tensor product, there exists an isomorphism $V^* \otimes V^* \cong \mathrm{Bil}(V)$ which maps, for all $\pi, \tau \in V^*$, $\pi \otimes \tau$ into the bilinear form on V defined by $\pi \otimes \tau(x,y) := \pi(x)\tau(y)$ for all $x, y \in V$. We will freely identify the tensor product of two linear forms with the corresponding bilinear form. If $\{\pi_i : 1 \leq i \leq k\}$ is a basis of V^*, then $\{\pi_i \otimes \pi_j : 1 \leq i, j \leq k\}$ is a basis of $\mathrm{Bil}(V)$ and in particular this implies that $\dim \mathrm{Bil}(V) = k^2$.

The subspace of $V^* \otimes V^*$ corresponding to $\mathrm{Sym}(V) \subseteq \mathrm{Bil}(V)$ via the above isomorphism is the span of all forms $\pi \otimes \pi$ with $\pi \in V^*$. If $\{\pi_i : 1 \leq i \leq k\}$ is a basis of V^*, then the forms $\pi_i \otimes \pi_i$ with $1 \leq i \leq k$ and $(\pi_i + \pi_j) \otimes (\pi_i + \pi_j)$ with $1 \leq i < j \leq k$ constitute a basis of $\mathrm{Sym}(V)$, hence in particular $\dim \mathrm{Sym}(V) = k(k+1)/2$.

Definition 2.3.4. We define the *rank* of a bilinear form $B \in \mathrm{Bil}(V)$ to be the minimum number of simple tensors needed to express its image in $V^* \otimes V^*$, and we denote it by $\mathrm{rk}\, B$. In other words, $\mathrm{rk}\, B$ is the minumum non-negative integer r such that there exist linear forms $\pi_1, \ldots, \pi_r, \tau_1, \ldots, \tau_r \in V^*$ with $B = \sum_{i=1}^{r} \pi_i \otimes \tau_i$.

It will be useful to write bilinear forms as matrices. Fixing a $\mathbb{K}$-basis of V allows us to identify $V \cong \mathbb{K}^k \cong V^*$ and $\mathrm{Bil}(V) \cong \mathbb{K}^{k \times k}$ in a way so that $\pi(x) = \pi^T x$

and $B(x,y) = x^T By$, for all $x, y \in V$, $\pi \in V^*$ and $B \in \mathrm{Bil}(V)$. Here vectors and bilinear forms are identified with the corresponding coordinate vectors and matrices, and coordinate vectors are written as column vectors. We identify $V^* \otimes V^* \cong \mathbb{K}^{k \times k}$ via $\pi \otimes \tau \mapsto \pi\tau^T$ for all $\pi, \tau \in V^*$. Under these identifications, isomorphic elements in $V^* \otimes V^* \cong \mathrm{Bil}(V)$ are mapped into the same matrix. In particular, we remark the following property of the rank.

LEMMA 2.3.5. *Let $B \in \mathrm{Bil}(V)$. Then its rank as a bilinear form (Definition 2.3.4) is equal to its rank as a matrix.*

PROOF. We denote by r the rank of B as a bilinear form and with r' its rank as a matrix. If $B = \sum_{i=1}^{r} \pi_i \otimes \tau_i$ then $\{\pi_1, \ldots, \pi_r\}$ is a $\mathbb{K}$-generator set for the columns of B, hence $r \geq r'$. Conversely, if $\{\pi_1, \ldots, \pi_{r'}\}$ is a $\mathbb{K}$-basis for the columns of B, then we can express every column of B as a linear combination of the π_i's, and the coefficients of these linear combinations give τ_i's such that $B = \sum_{i=1}^{r'} \pi_i \otimes \tau_i$, hence $r \leq r'$. □

2.4 Quadratic Forms

In this section we introduce the basic theory of quadratic forms, we outline their classification, and we prove some combinatorial results that will be useful later on in this work. Our main reference is [44]. More specific references will be given throughout the section.

Let $\mathbb{K}$ be a finite field and let V be a finite-dimensional $\mathbb{K}$-vector space.

DEFINITION 2.4.1. A *quadratic form* on V is a map $Q\colon V \to \mathbb{K}$ such that

(i) $Q(\lambda x) = \lambda^2 Q(x)$ for all $x \in V, \lambda \in \mathbb{K}$,
(ii) the map $(x,y) \mapsto Q(x+y) - Q(x) - Q(y)$ is a bilinear form on V.

We denote by $\mathrm{Quad}(V)$ the $\mathbb{K}$-vector space of all quadratic forms on V. The vector space V, endowed with a quadratic form Q on V, is called a $\mathbb{K}$-*quadratic space*.

Every quadratic form $Q \in \mathrm{Quad}(V)$ defines a bilinear form $\tilde{B}_Q \in \mathrm{Bil}(V)$ by

$$\tilde{B}_Q(x,y) := Q(x+y) - Q(x) - Q(y)$$

for all $x, y \in V$. If $\mathrm{char}\,\mathbb{K} \neq 2$ we also define the symmetric bilinear form $B_Q := \frac{1}{2}\tilde{B}_Q$, which satisfies $B_Q(x,x) = Q(x)$ for all $x \in V$. If $\mathrm{char}\,\mathbb{K} = 2$ note

that $\tilde{B}_Q$ is alternating. Conversely, every bilinear form $B \in \mathrm{Bil}(V)$ defines a quadratic form $Q_B \in \mathrm{Quad}(V)$ by $Q_B(x) := B(x,x)$ for every $x \in V$. This induces an isomorphism $\mathrm{Bil}(V)/\mathrm{Alt}(V) \cong \mathrm{Quad}(V)$. If $\mathrm{char}\,\mathbb{K} \neq 2$ this induces an isomorphism $\mathrm{Sym}(V) \cong \mathrm{Quad}(V)$ as well, namely the map $B \mapsto Q_B$ with inverse $Q \mapsto B_Q$. In particular, using these isomorphisms, we can always associate to a quadratic form an upper triangular matrix and, in the case of $\mathrm{char}\,\mathbb{K} \neq 2$, a symmetric matrix.

LEMMA 2.4.2. *There exists an isomorphism* $\phi\colon \mathrm{Quad}(V^*) \to \mathrm{Sym}(V)^*$ *such that* $\phi(Q)(\pi \otimes \pi) = Q(\pi)$ *for all* $Q \in \mathrm{Quad}(V^*)$ *and all* $\pi \in V^*$.

PROOF. By the universal property of the tensor product, we have an isomorphism $\mathrm{Bil}(V^*) \cong \mathrm{Bil}(V)^*$ that maps $B \in \mathrm{Bil}(V^*)$ into the linear form on $\mathrm{Bil}(V) \cong V^* \otimes V^*$ determined by $\pi \otimes \tau \mapsto B(\pi, \tau)$. Composing it with the restriction map $\mathrm{Bil}(V)^* \to \mathrm{Sym}(V)^*$, we obtain a surjective linear map $\mathrm{Bil}(V^*) \to \mathrm{Sym}(V)^*$ whose kernel is $\mathrm{Alt}(V^*)$. Indeed, $B \in \mathrm{Bil}(V^*)$ is in the kernel if and only if $B(\pi, \pi) = 0$ for every $\pi \in V^*$. This gives an isomorphism $\mathrm{Bil}(V^*)/\mathrm{Alt}(V^*) \cong \mathrm{Sym}(V)^*$, and the lemma follows composing it with the isomorphism $\mathrm{Quad}(V^*) \cong \mathrm{Bil}(V^*)/\mathrm{Alt}(V^*)$ considered above. □

Fix now $Q \in \mathrm{Quad}(V)$, so V has a structure of K-quadratic space. Any subspace of V inherits a natural structure of quadratic space, defined by the restriction of Q. The symmetric bilinear form $\tilde{B}_Q$ defines a scalar product on V, thus notions as radical, non degeneracy, orthogonality and isotropy. As a shorthand, if there is no ambiguity we write $x \cdot y$ instead of $\tilde{B}_Q(x,y)$ for $x, y \in V$.

DEFINITION 2.4.3. The *radical* of the quadratic space V is the $\mathbb{K}$-vector space

$$\mathrm{Rad}\, V := \{x \in V : x \cdot y = 0 \text{ for all } y \in V\}.$$

We say that V is *non-degenerate* (as a quadratic space) if $\tilde{B}_Q$ is non-degenerate (as a bilinear form), i.e. if $\mathrm{Rad}\, V = 0$.

The radical is indeed a $\mathbb{K}$-vector space, as $\tilde{B}_Q$ is bilinear.

DEFINITION 2.4.4. Let $\mathrm{Rad}^0 V := \{x \in \mathrm{Rad}\, V : Q(x) = 0\}$. We define the *rank* of Q to be

$$\mathrm{rk}\, Q := \dim V - \dim \mathrm{Rad}^0 V.$$

A remark concerning the definitions of radical and rank follows. If $\mathrm{char}\,\mathbb{K} \neq 2$ then Q vanishes on $\mathrm{Rad}\, V$: indeed, for all $x \in \mathrm{Rad}\, V$ we have $Q(x) = B_Q(x,x) = \frac{1}{2} x \cdot x = 0$ by definition of the radical. Therefore $\mathrm{Rad}^0 V = \mathrm{Rad}\, V$ and in this case the rank of a quadratic form equals the rank of the associated bilinear form. If $\mathrm{char}\,\mathbb{K} = 2$ this is not always the case: for example, consider

the quadratic form on $\mathbb{F}_2$ defined by $Q(x) := x^2$; note that $\tilde{B}_Q$ is identically zero, hence the radical is the whole space, but Q does not vanish at $x = 1$. So in the characteristic 2 case $\operatorname{Rad}^0 V$, the zero locus of the restriction of Q to $\operatorname{Rad} V$, is not necessarily trivial. Following [29], we have defined the rank of a quadratic form to be the codimension of this zero locus.

In the characteristic 2 case, under the additional assumption that $\mathbb{K}$ is perfect, i.e. squaring is an automorphism of $\mathbb{K}$ (which is always the case if $\mathbb{K}$ is a finite field), one can prove that the difference between the rank of Q and the codimension of the radical of V is either zero or one.

We define orthogonality and isotropy with respect to $\tilde{B}_Q$, as follows.

Two vectors $x, y \in V$ are *orthogonal* if $x \cdot y = 0$. A set of vectors, and in particular a basis of V, is orthogonal if its elements are pairwise orthogonal. Two subspaces $V_1, V_2 \subseteq V$ are orthogonal if $x \cdot y = 0$ for all $x \in V_1, y \in V_2$. We use the symbol $\perp$ for the orthogonality relation. The orthogonal of a subspace $V_1 \subseteq V$ is

$$V_1^\perp := \{x \in V : x \cdot y = 0 \text{ for all } y \in V_1\}.$$

Note that $V_1 \cap V_1^\perp = \operatorname{Rad} V_1$, so $\operatorname{Rad} V_1 = 0$ implies $V_1 \cap V_1^\perp = 0$. Moreover, by basic linear algebra $\dim V_1 + \dim V_1^\perp = \dim V$. Hence in this case $V_1^\perp$ is a complement of V_1, called the orthogonal complement of V_1. Finally, a decomposition of V is orthogonal if the components are pairwise orthogonal.

A non-zero vector $x \in V$ is *isotropic* if $x \cdot x = 0$. A subspace of V is isotropic if it contains an isotropic vector, anisotropic otherwise. Note that if $\operatorname{char} \mathbb{K} = 2$ then every vector is isotropic, as $\tilde{B}_Q$ is alternating, hence it does not make sense to use this notion.

In the next sections, first we outline the classification of quadratic spaces, then we use this classification to prove some combinatorial results about quadratic forms.

2.4.1 Classification in $\operatorname{char} \mathbb{K} \neq 2$

Quadratic forms are classified according to the decomposition they induce on the quadratic space. If this happens, i.e. if there exists an automorphism ψ of V such that $Q_1 = Q_2 \circ \psi$, we say that Q_1 and Q_2 are *equivalent*. The first step is the following theorem, which actually works in any characteristic. This will allow us to always assume that V is non-degenerate.

THEOREM 2.4.5. *Any quadratic space V admits an orthogonal decomposition $V = \operatorname{Rad} V \oplus V_0$, for some non-degenerate subspace $V_0 \subseteq V$.*

PROOF. Clearly there exists a subspace $V_0 \subseteq V$ such that $V = \operatorname{Rad} V \oplus V_0$ and this decomposition is orthogonal, so we only have to prove that such a V_0 is necessarily non degenerate. Let $x \in \operatorname{Rad} V_0$, then $x \cdot y = 0$ for all $y \in V_0$. Also, $x \cdot y = 0$ for all $y \in \operatorname{Rad} V$. As $V = \operatorname{Rad} V \oplus V_0$, it follows that $x \cdot y = 0$ for all $y \in V$, i.e. $x \in \operatorname{Rad} V$. Hence $x \in \operatorname{Rad} V \cap V_0 = 0$ and this proves that V_0 is non-degenerate. □

From here on we assume that $\operatorname{char} \mathbb{K} \neq 2$ and set $x \cdot y := B_Q(x, y)$ for all $x, y \in V$. We first show that any quadratic space admits an orthogonal basis and then Witt's decomposition into hyperbolic planes.

THEOREM 2.4.6. *Any quadratic space over an odd characteristic field admits an orthogonal basis.*

PROOF. By Theorem 2.4.5 we may assume that the quadratic space V is non-degenerate. We argue by induction on $\dim V$. If $\dim V = 1$ then the statement is trivial. If $\dim V > 1$ then, as V is non-degenerate, there exists $x \in V$ such that $x \cdot x \neq 0$, hence we have $V = \langle x \rangle \oplus \langle x \rangle^{\perp}$ and we can conclude by induction hypothesis. □

REMARK 2.4.7. In the characteristic 2 case this argument fails, even replacing B_Q with $\tilde{B}_Q$, as this map is alternating.

REMARK 2.4.8. The matrix associated to Q with respect to an orthogonal basis of V is a diagonal matrix, and the number of non-zero entries equals the rank of Q.

We now introduce Witt's decomposition, which uses hyperbolic planes as "building blocks".

DEFINITION 2.4.9. A *hyperbolic plane* is a non-degenerate 2-dimensional subspace which admits a basis of isotropic vectors.

Note that any hyperbolic plane H admits a basis $\{x_1, x_2\}$ of isotropic vectors such that $x_1 \cdot x_2 = 1$. Indeed, for any basis $\{x_1, y\}$, with x_1, y isotropic, it holds that $\alpha := x_1 \cdot y \neq 0$ as H is non-degenerate, hence $\{x_1, x_2\}$ with $x_2 := \alpha^{-1} y$ satisfies the property.

THEOREM 2.4.10 (Witt's decomposition). *The quadratic space V orthogonally decomposes as*

$$V = \operatorname{Rad} V \oplus \bigoplus_{i=1}^{m} H_i \oplus W,$$

where the H_i's are hyperbolic planes and W is anisotropic.

PROOF. By Theorem 2.4.5 we may assume that V is non-degenerate. If V is anisotropic we are done, with $m = 0$ and $V = W$. Otherwise there exists an isotropic vector $v_1 \in V$, hence $x \in V$ such that $\alpha := v_1 \cdot x \neq 0$, as V is non-degenerate. Now take

$$v_2 := \frac{1}{\alpha} x - \frac{x \cdot x}{2\alpha^2} v_1,$$

$H_1 := \langle v_1, v_2 \rangle$ and apply induction. □

REMARK 2.4.11. A stronger result actually holds. The decomposition above is unique, in the sense that the number m of hyperbolic planes is unique while the anisotropic space W is unique up to "isometry". For details, see [44, 66]. However, this stronger result is not needed here.

If we assume that $\mathbb{K} = \mathbb{F}$ is a finite field, this classification can be further improved. The notion of discriminant will be relevant.

DEFINITION 2.4.12. The *discriminant* $\operatorname{disc} Q$ of a full-rank quadratic form Q is defined to be the class in the group $\mathbb{F}^*/(\mathbb{F}^*)^2 \cong \{1, -1\}$ of the determinant of any matrix associated to Q. The discriminant of a non-full-rank quadratic form is defined to be the discriminant of its restriction to the non-degenerate component V_0 of V in the decomposition $V = \operatorname{Rad} V \oplus V_0$.

The discriminant is well-defined: if M_1 and M_2 are two different matrices associated to Q, then $M_1 = PM_2P^T$ for some invertible matrix P, hence $\det M_1 = \det M_2 \ (\det P)^2$.

THEOREM 2.4.13. *Any non-degenerate quadratic space over a finite field with odd characteristic admits an orthogonal basis* $\{x_1, \ldots, x_k\}$ *such that* $x_i \cdot x_i = 1$ *for all* $i = 1, \ldots, k-1$ *and* $x_k \cdot x_k = \operatorname{disc} Q$.

PROOF. It follows by Theorem 2.4.5 and Lemma 2.4.14 below, using induction. □

LEMMA 2.4.14. *Assume that* $\operatorname{rk} Q \geq 2$. *Then for all* $\gamma \in \mathbb{F}, \gamma \neq 0$ *there exists* $x \in V$ *such that* $x \cdot x = \gamma$.

PROOF. This can be viewed as a consequence of the Chevalley-Warning Theorem, see for example [66], or directly proved as follows. By Theorem 2.4.6, V admits an orthogonal basis. Let $x_1, x_2 \in V$ be two elements of this basis such that $\alpha := x_1 \cdot x_1 \neq 0$ and $\beta := x_2 \cdot x_2 \neq 0$. They exist as $\operatorname{rk} Q \geq 2$. Let $\gamma \in \mathbb{F}, \gamma \neq 0$, consider the two sets

$$A := \{\gamma - \alpha a^2 : a \in \mathbb{F}\} \subseteq \mathbb{F} \qquad \text{and} \qquad B := \{\beta b^2 : b \in \mathbb{F}\} \subseteq \mathbb{F}.$$

As $|A| = (q+1)/2 = |B|$, where q denotes the size of $\mathbb{F}$, A and B cannot have empty intersection, hence there exist $a, b \in \mathbb{F}$ such that $\alpha a^2 + \beta b^2 = \gamma$. Now $x := ax_1 + bx_2$ satisfies the required property. □

Theorem 2.4.13 proves that quadratic forms over odd-characteristic finite fields are equivalent if they have the same rank and discriminant. Moreover, as the discriminant is an element of $\mathbb{F}^*/(\mathbb{F}^*)^2 \cong \{1, -1\}$, for any given rank there exists only two different quadratic forms, up to equivalence.

2.4.2 Classification in $\operatorname{char}\mathbb{K} = 2$

Assume now that $\operatorname{char}\mathbb{K} = 2$, and $x \cdot y := \tilde{B}_Q(x, y)$ for all $x, y \in V$. In this case, the "building blocks" in the decomposition are symplectic planes.

Definition 2.4.15. A *symplectic plane* is a subspace which admits a basis $\{x_1, x_2\}$ such that $x_1 \cdot x_2 = 1$.

Observe that non-degeneracy is implied by this definition.

Theorem 2.4.16. *The quadratic space V orthogonally decomposes as*

$$V = \operatorname{Rad} V \oplus \bigoplus_{i=1}^{m} S_i,$$

where the S_i's are symplectic planes.

Proof. Again, we may assume that V is non-degenerate. Let $x_1 \in V$, let $y \in V$ be such that $\alpha := x_1 \cdot y \neq 0$. Take $x_2 := \frac{1}{\alpha} y$, $S_1 := \langle x_1, x_2 \rangle$ and argue by induction. □

From here on, we will not give any proof of our statement, but we refer to [29, 32]. Recall that in the characteristic 2 case the rank of the quadratic form may differ from the codimension of the radical. If this happens, i.e. if there exists $x \in \operatorname{Rad} V$ with $Q(x) \neq 0$, then $\operatorname{rk} Q = 2m + 1$, otherwise $\operatorname{rk} Q = 2m$, where m is as in the previous theorem. It holds that all quadratic forms of odd rank induce the same decomposition on V, as stated by the following theorem.

Theorem 2.4.17. *If $\operatorname{rk} Q$ is odd, the quadratic space V orthogonally decomposes as*

$$V = \operatorname{Rad} V_0 \oplus \langle x \rangle \oplus \bigoplus_{i=1}^{m} S_i,$$

where $\operatorname{Rad} V_0$ is defined in Definition 2.4.4, $x \in \operatorname{Rad} V$, and the S_i's are symplectic planes satisfying the following additional property: for all $i = 1, \ldots, m$, S_i has a basis $\{x_{i,1}, x_{i,2}\}$ such that $x_{i,1} \cdot x_{i,2} = 1$ and $Q(x_{i,1}) = Q(x_{i,2}) = 0$.

If $\operatorname{rk} Q$ is even, a new parameter has to be taken into account, namely the Arf invariant.

DEFINITION 2.4.18. The *Arf invariant* $\operatorname{Arf} Q$ of a rank-2 quadratic form Q on a space V of dimension 2 is defined to be the class of

$$\frac{Q(x_1)Q(x_2)}{x_1 \cdot x_2}$$

in $\mathbb{K}/L$, where $L := \{\lambda^2 + \lambda : \lambda \in \mathbb{K}\}$ and $\{x_1, x_2\}$ is any basis of V. The Arf invariant of an even-rank quadratic form Q on a space which orthogonally decomposes as

$$V = \operatorname{Rad} V \oplus \bigoplus_{i=1}^{m} S_i,$$

where the S_i's are symplectic planes, is

$$\operatorname{Arf}(Q) := \sum_{i=1}^{m} \operatorname{Arf}(Q_i) \in \mathbb{K}/L,$$

where, for all $i = 1, \ldots, m$, Q_i denotes the restriction of Q to S_i.

THEOREM 2.4.19. *If $\operatorname{rk} Q$ is even, the quadratic space V orthogonally decomposes as*

$$V = \operatorname{Rad} V \oplus \bigoplus_{i=1}^{m} S_i,$$

where the S_i's are symplectic planes satisfying the following additional properties:

(i) for all $i = 1, \ldots, m-1$, S_i has a basis $\{x_{i,1}, x_{i,2}\}$ such that $x_{i,1} \cdot x_{i,2} = 1$ and $Q(x_{i,1}) = Q(x_{i,2}) = 0$, and in particular the restriction of Q to S_i has Arf invariant zero;

(ii) S_m has a basis $\{x_{m,1}, x_{m,2}\}$ such that $x_{m,1} \cdot x_{m,2} = 1$, $Q(x_{m,1}) = 0$ and $Q(x_{m,2}) = \operatorname{Arf}(Q)$, and in particular the restriction of Q to S_m has Arf invariant equal to the Arf invariant of Q.

To sum up, in the characteristic 2 case, it holds that two quadratic forms having the same, odd rank are equivalent, while two quadratic forms having the same, even rank are equivalent if and only if they have the same Arf invariant.

If $\mathbb{K} = \mathbb{F}$ is a finite field, observe that L is the kernel of the trace map $\operatorname{Tr}\colon \mathbb{F} \to \mathbb{F}_2$, hence $\mathbb{F}/L \cong \mathbb{F}_2$ and this means that for any given even rank there exists only two different quadratic forms, up to equivalence.

2.4.3 Number of Zeros of a Quadratic Form

From here on, we assume that $\mathbb{K} = \mathbb{F}$ is a finite field of size q. In this section we compute the number of zeros in V of the quadratic form Q, as a function of the dimension k of V, the rank r of Q and the cardinality q of the base field. Even though the definition of rank is essentially dependent on $\operatorname{char}\mathbb{F}$, the formula we give is characteristic-free.

THEOREM 2.4.20. *The number of vectors $x \in V$ such that $Q(x) = 0$ is*

a. q^{k-1} if r is odd,
b. either $q^{k-1} - (q-1)q^{k-\frac{r}{2}-1}$ or $q^{k-1} + (q-1)q^{k-\frac{r}{2}-1}$ if r is even.

REMARK 2.4.21. The "$\pm$" in claim b of Theorem 2.4.20 (and of the forthcoming Theorem 2.4.23) only depends on the "last component" in the orthogonal decomposition of V given by Theorem 2.4.10 and Theorem 2.4.16.

In [47, Chapter 6, Section 2] the number of vectors $x \in V$ such that $Q(x) = b$, for any full-rank quadratic form Q on V and any $b \in \mathbb{F}$, is computed. Theorem 2.4.23 below, whence Theorem 2.4.20 easily follows, is an instance of this result. However, for completeness, and to show an application of the classification theorems, we include a full proof of Theorem 2.4.23.

Here, it is convenient to view quadratic forms as polynomials, as follows. This correspondence holds over an arbitrary field $\mathbb{K}$ (so we abandon for a moment the assumption that the base field is finite). Fixing a $\mathbb{K}$-basis $\{x_1, \ldots, x_k\}$ of V we can associate to Q a homogeneous quadratic k-variate polynomial $f_Q \in \mathbb{K}[X_1, \ldots, X_k]$ such that, for all $(\alpha_1, \ldots, \alpha_k) \in K^k$,

$$Q(\alpha_1 x_1 + \cdots + \alpha_k x_k) = f_Q(\alpha_1, \ldots, \alpha_k),$$

namely

$$f_Q := \sum_{1 \le i \le k} Q(v_i) X_i^2 + \sum_{1 \le i < j \le k} \tilde{B}_Q(x_i, x_j) X_i X_j.$$

Clearly there is a one-to-one correspondence between zeros of Q and zeros of f_Q, independently of the basis choice. We remark that the rank of Q can be equivalently defined as the minimal number of variables appearing in the polynomial f_Q associated to Q, where minimality is taken over all possible basis choices.

Back to the case of $\mathbb{K} = \mathbb{F}$, we have the following straightforward consequence of the classification theorems.

COROLLARY 2.4.22. *Assume that $r \ge 3$. Then the polynomial f_Q associated to Q in some suitable basis can be written as*

$$f_Q = g_Q + X_{k-1} X_k, \qquad \text{with} \qquad g_Q \in \mathbb{F}[X_1, \ldots, X_{k-2}].$$

PROOF. As $r \geq 3$, the classification theorems give an $\mathbb{F}$-basis $\{x_1, \ldots, x_k\}$ of V such that $\tilde{B}_Q(x_{k-1}, x_k) = 1$, $Q(x_{k-1}) = Q(x_k) = 0$ and $\langle x_1, \ldots, x_{k-2} \rangle \perp \langle x_{k-1}, x_k \rangle$. The polynomial f_Q associated to Q with respect to this basis has the desired form. □

We are ready to proceed. We start with the case of full-rank forms, and then we show how the general case easily follows.

THEOREM 2.4.23. *Assume that $r = k$, i.e. that Q has full rank. Then the number of vectors $x \in V$ such that $Q(x) = 0$ is*

a. q^{k-1} *if k is odd,*
b. either $q^{k-1} - (q-1)q^{\frac{k}{2}-1}$ *or* $q^{k-1} + (q-1)q^{\frac{k}{2}-1}$ *if k is even.*

PROOF. Denote by $Z_k(f)$ the number of zeros in $\mathbb{F}^k$ of a polynomial $f \in \mathbb{F}[X_1, \ldots, X_k]$. The proof is by induction on k. If $k = 1$ (case a) then in some basis $f_Q = \alpha X_1^2$ and its only zero is the zero vector. If $k = 2$ (case b) then, by classification theorems, we have two possible situations: either the only zero of f_Q is the zero vector or $f_Q = X_1 X_2$ has $2q - 1$ zeros.

Now let $k \geq 3$. By Corollary 2.4.22 we can write

$$f_Q = g_Q + X_{k-1}X_k, \qquad \text{with} \qquad g_Q \in \mathbb{F}[X_1, \ldots, X_{k-2}].$$

Note that the zeros of f_Q are exactly all k-tuples (x, α_1, α_2) with $x \in \mathbb{F}^{k-2}$, $\alpha_1, \alpha_2 \in \mathbb{F}$ such that

- x is a zero of g_Q and $\alpha_1 \alpha_2 = 0$ or
- x is not a zero of g_Q, $\alpha_1 \neq 0$ and $\alpha_2 = -\alpha_1^{-1} g_Q(x)$.

Hence we get the recursion formula

$$\begin{aligned} Z_k(f_Q) &= (2q-1)Z_{k-2}(g_Q) + \\ &\quad + (q-1)(q^{k-2} - Z_{k-2}(g_Q)) = \\ &= q^{k-1} - q^{k-2} + qZ_{k-2}(g_Q) \end{aligned}$$

for $k \geq 3$. This gives the result. □

PROOF OF THEOREM 2.4.20. In a suitable basis, the polynomial associated to Q is r-variate, i.e. $f_Q \in \mathbb{F}[X_1, \ldots, X_r]$. This defines a full-rank quadratic form on $\mathbb{F}^r$, hence Theorem 2.4.23 applies. The conclusion now follows as any zero of f_Q in $\mathbb{F}^r$ gives q^{k-r} zeros of f_Q in $\mathbb{F}^k$ by padding. □

2.4.4 Number of Quadratic Forms of Given Rank

In this section we compute the number $N(k,r)$ of rank r quadratic forms on any $\mathbb{F}$-vector space of dimension k, where k, r are non-negative integers with $k \geq r$. First we deal with the case $k = r$, i.e. of full-rank quadratic forms, then we address the general case. In the full-rank case we write $N(k)$ instead of $N(k,k)$, as a shorthand. We now state the results: Theorem 2.4.24 for the first case, Theorem 2.4.25 for the latter.

THEOREM 2.4.24. *For all non-negative integers k, the number of full-rank quadratic forms on an $\mathbb{F}$-vector space of dimension k is*

$$N(k) = q^{\lfloor \frac{k}{2} \rfloor (\lfloor \frac{k}{2} \rfloor + 1)} \prod_{i=1}^{\lceil \frac{k}{2} \rceil} (q^{2i-1} - 1) =$$

$$= \begin{cases} q^{\frac{k-1}{2}\frac{k+1}{2}} \prod_{i=1}^{\frac{k+1}{2}} (q^{2i-1} - 1) & \text{if } k \text{ is odd,} \\ q^{\frac{k}{2}(\frac{k}{2}+1)} \prod_{i=1}^{\frac{k}{2}} (q^{2i-1} - 1) & \text{if } k \text{ is even.} \end{cases}$$

THEOREM 2.4.25. *For all non-negative integers $k \geq r$, the number of rank r quadratic forms on an $\mathbb{F}$-vector space of dimension k is*

$$N(k,r) = \begin{bmatrix} k \\ r \end{bmatrix}_q N(r),$$

where

$$\begin{bmatrix} k \\ r \end{bmatrix}_q := \prod_{i=1}^{r} \frac{q^{k-r+i} - 1}{q^i - 1}$$

denotes the q-ary Gaussian binomial coefficient.

REMARK 2.4.26. By convention, we define a product with no factors to be equal to 1. This is the case if $r = 0$. As q is assumed to be fixed, it will be suppressed from the notation from here on. It is well-known that the Gaussian binomial coefficient $\begin{bmatrix} k \\ r \end{bmatrix}$ equals the number of r-dimensional subspaces of any $\mathbb{F}$-vector space of dimension k.

Our proofs of Theorems 2.4.24 and 2.4.25 follow. Our strategy consists of constructing all quadratic forms on a given space as "combinations" (in the sense of Definition 2.4.27 and Construction 2.4.28 below) of quadratic forms on subspaces. Counting recursively the number of forms constructed in this way and dividing by the number of repetitions will give the required quantity.

Towards a proof of Theorem 2.4.24, we fix a non-negative integer k and an $\mathbb{F}$-vector space V of dimension k. We define the following "sum" of quadratic forms.

DEFINITION 2.4.27. Let $V_1, V_2 \leq V$ be subspaces such that $V_1 \cap V_2 = 0$, let Q_1 be a quadratic form on V_1 and Q_2 a quadratic form on V_2. We define $Q := Q_1 \oplus Q_2$ to be the unique quadratic form on $V_1 \oplus V_2$ defined by the conditions $Q|_{V_1} = Q_1$, $Q|_{V_2} = Q_2$ and $V_1 \perp V_2$.

In other words, for $v \in V_1 \oplus V_2$, we define $Q(v) := Q_1(v_1) + Q_2(v_2)$, where $v_1 \in V_1$ and $v_2 \in V_2$ are the unique vectors such that $v_1 + v_2 = v$. Also note that $\operatorname{Rad}(V_1 \oplus V_2) = \operatorname{Rad} V_1 \oplus \operatorname{Rad} V_2$. So we construct quadratic forms on V as follows.

CONSTRUCTION 2.4.28. Let $h \leq k$ be a non-negative integer. Let (V_1, V_2, Q_1, Q_2) be a 4-tuple consisting of a subspace $V_1 \leq V$ of dimension h, a complement $V_2 \leq V$ of V_1, a full-rank quadratic form Q_1 on V_1 and a full-rank quadratic form Q_2 on V_2. Define $Q := Q_{(V_1,V_2,Q_1,Q_2)} := Q_1 \oplus Q_2 \in \operatorname{Quad}(V)$.

The choice of the parameter h is determined by the characteristic of $\mathbb{F}$ and the parity of the dimension k of V, as follows:

1. $h = 1$ if k is odd and $\operatorname{char} \mathbb{F} \neq 2$,
2. $h = 2$ if k is even and $\operatorname{char} \mathbb{F} \neq 2$,
3. $h = 2$ if $\operatorname{char} \mathbb{F} = 2$.

We prove that, with this choice of h, all full-rank quadratic forms on V are obtained by Construction 2.4.28 and, conversely, all forms defined using Construction 2.4.28 have full rank.

LEMMA 2.4.29. *Any full-rank quadratic form on V is an instance of Construction 2.4.28 with h chosen as above.*

PROOF. First assume that $\operatorname{char} \mathbb{F} \neq 2$. If Q is a full-rank quadratic form on V then by Theorem 2.4.10 we have an orthogonal decomposition

$$V = \bigoplus_{i=1}^{m} H_i \oplus W,$$

with $\dim H_i = 2$ for all $i = 1, \ldots, m$ and $\dim W \leq 2$. If k is odd then $\dim W$ is also odd, hence it must equal 1. Let $V_1 := W$, $V_2 := \bigoplus_{i=1}^{m} H_i$, $Q_1 := Q|_{V_1}$ and $Q_2 := Q|_{V_2}$, then $Q = Q_{(V_1,V_2,Q_1,Q_2)}$ with $h = \dim W = 1$. If k is even, let $V_1 := H_1, V_2 := \bigoplus_{i=2}^{m} H_i \oplus W, Q_1 := Q|_{V_1}, Q_2 := Q|_{V_2}$, then $Q = Q_{(V_1,V_2,Q_1,Q_2)}$ with $h = \dim H_1 = 2$.

Now assume $\operatorname{char} \mathbb{F} = 2$. If Q is a full-rank quadratic form on V then by Theorem 2.4.16 we have an orthogonal decomposition

$$V = \operatorname{Rad} V \oplus \bigoplus_{i=1}^{m} S_i$$

with $\dim \operatorname{Rad} V = 0$ or 1. Let $V_1 := S_1, V_2 := \operatorname{Rad} V \oplus \bigoplus_{i=2}^{m} S_i, Q_1 := Q|_{V_1}, Q_2 := Q|_{V_2}$, then $Q = Q_{(V_1,V_2,Q_1,Q_2)}$ with $h = \dim S_1 = 2$. □

LEMMA 2.4.30. *Any instance of Construction 2.4.28, with h chosen as above, is a full-rank quadratic form on V.*

PROOF. Let V_1, V_2, Q_1, Q_2 be as required in Construction 2.4.28, and let $Q := Q_{(V_1,V_2,Q_1,Q_2)}$. The statement is obvious if $\operatorname{char} \mathbb{F}$ is odd: in this case both $\operatorname{Rad} V_1 = \operatorname{Rad} V_2 = 0$, hence $\operatorname{Rad}(V_1 \oplus V_2) = 0$ as well. The same happens in the characteristic 2 case if both h and k are even.

The only non trivial case is the one of $\operatorname{char} \mathbb{F} = 2$ and k odd. We have chosen h to be even, hence $\operatorname{Rad} V_1 = 0$ while $\operatorname{Rad} V_2 = \langle w \rangle$ for some $w \in V_2$ such that $Q(w) \neq 0$. Then $\operatorname{Rad}(V_1 \oplus V_2) = \langle w \rangle$ and $Q(w) = Q_2(w) \neq 0$, hence Q has full rank. □

It follows that the number of full-rank quadratic forms on V is given by the number of suitable 4-tuples (V_1, V_2, Q_1, Q_2) divided by the number of repetitions. The number of possible choices for V_1 is given by a Gaussian binomial coefficient. The following combinatorial lemma computes the number of possible choices for V_2.

LEMMA 2.4.31. *Let $h \leq k$ be a non-negative integer. The number of complements of an h-dimensional subspace of V is $q^{h(k-h)}$.*

PROOF. Let W be an h-dimensional subspace of V, with basis $\{v_1, \ldots, v_h\}$. This can be completed to a basis of V in $(q^k - q^h)(q^k - q^{h+1}) \cdots (q^k - q^{k-1})$ ways. Any complement of W has dimension $k - h$, hence $(q^{k-h} - 1)(q^{k-h} - q) \cdots (q^{k-h} - q^{k-h-1})$ different bases. Hence the number of complements of W is

$$\frac{q^k - q^h}{q^{k-h} - 1} \cdot \frac{q^k - q^{h+1}}{q^{k-h} - q} \cdots \frac{q^k - q^{k-1}}{q^{k-h} - q^{k-h-1}} = q^{h(k-h)}.$$

□

Finally, we count how many times a quadratic form is repeated.

LEMMA 2.4.32. *Let Q be a full-rank quadratic form on V. For any non-degenerate h-dimensional subspace V_1 of V, with h chosen as above, we have a unique complement V_2 of V_1 and unique full-rank quadratic forms Q_1 and Q_2 on V_1 and V_2 respectively such that $Q = Q_{(V_1,V_2,Q_1,Q_2)}$.*

PROOF. Let V_1 be a non-degenerate h-dimensional subspace of V. We want to define V_2, Q_1, Q_2 such that $Q_{(V_1,V_2,Q_1,Q_2)} = Q$. Clearly we have to take $Q_1 := Q|_{V_1}$. The choice of h implies that $\operatorname{Rad} V_1 = 0$, hence V_1 has an

orthogonal complement. So take $V_2 := V_1^\perp$ and $Q_2 := Q|_{V_2}$. Note that these are the only possible choices, hence this proves the lemma. □

For all full-rank quadratic forms Q on V and all non-negative integers h we denote by $R(Q,h)$ the number of non-degenerate h-dimensional subspaces of V. A priori, this number depends on Q, but we will see that under our choice of h it only depends on k and h. In those cases we denote it by $R(k,h)$.

All lemmas above together prove the following.

LEMMA 2.4.33. *Let h be chosen as above, assume that $R(k,h) = R(Q,h)$ is independent of the choice of a quadratic form Q. Then*

$$N(k) = \frac{\begin{bmatrix} k \\ h \end{bmatrix} q^{h(k-h)}}{R(k,h)} N(h)N(k-h).$$

REMARK 2.4.34. By classification theorems, any quadratic form can be obtained by Construction 2.4.28 with $h = 2$, independently of the rank parity. So it is natural to ask why, in the odd characteristic case, we are dealing separately with odd rank and even rank quadratic forms, using $h = 1$ in the first case and $h = 2$ in the second. The reason is that if $\operatorname{rk} Q$ is odd then $R(Q,2)$ depends on Q, yielding a formula more complicated than the one given by Lemma 2.4.33, involving terms which also depend on Q. So our strategy allows a simpler proof.

Computing the number $R(k,h)$ is the last non trivial step towards the computation of $N(k)$. We are going to do that in the next two sections, obtaining the following recursion formula.

THEOREM 2.4.35. *For $k \geq 1$,*

$$N(k) = \begin{cases} (q^k - 1)N(k-1) & \text{if } k \text{ is odd,} \\ q^k N(k-1) & \text{if } k \text{ is even.} \end{cases}$$

Theorem 2.4.35 will be proved in the next two sections, dealing with the odd characteristic case and with the characteristic 2 case separately. We now use it to prove the closed-form expression for $N(k)$ stated by Theorem 2.4.24. Then we will conclude this section with the proof of Theorem 2.4.25.

PROOF OF THEOREM 2.4.24. We argue by induction on k. First note that $N(0) = 1$ and $N(1) = q - 1$. Now let $k > 1$ and assume that the statement is true for $k - 1$. We use the recursion formula given by Theorem 2.4.35. If k is

odd then

$$\begin{aligned} N(k) &= (q^k-1)N(k-1) = \\ &= (q^k-1)q^{\frac{k-1}{2}\left(\frac{k-1}{2}+1\right)}\prod_{i=1}^{\frac{k-1}{2}}(q^{2i-1}-1) = \\ &= q^{\frac{k-1}{2}\frac{k+1}{2}}\prod_{i=1}^{\frac{k+1}{2}}(q^{2i-1}-1). \end{aligned}$$

If k is even then

$$\begin{aligned} N(k) &= q^k N(k-1) = \\ &= q^k q^{\frac{k}{2}\left(\frac{k}{2}-1\right)}\prod_{i=1}^{\frac{k}{2}}(q^{2i-1}-1) = \\ &= q^{\frac{k}{2}\left(\frac{k}{2}+1\right)}\prod_{i=1}^{\frac{k}{2}}(q^{2i-1}-1). \end{aligned}$$

□

Proof of Theorem 2.4.25. Consider the following construction. For any choice of a subspace V_0 of dimension r, a full-rank quadratic form Q_0 on V_0 and a direct complement R of V_0 we can define the quadratic form $Q := Q_{(V_0,Q_0,R)} := Q_0 \oplus 0 \in \mathrm{Quad}(V)$ of rank r, i.e. the unique quadratic form on V defined by the conditions $Q|_{V_0} = Q_0, Q|_R = 0$ and $V_0 \perp R$. By classification of quadratic forms, any rank r quadratic form is given by $Q_{(V_0,Q_0,R)}$ for some triple (V_0, Q_0, R).

So we only need to compute the number of times each form is repeated, i.e. the number of triples (V_0', Q_0', R') such that $Q_{(V_0',Q_0',R')} = Q_{(V_0,Q_0,R)} =: Q$, where (V_0, Q_0, R) is a fixed triple. First note that

$$R' = \{x \in \operatorname{Rad} V : Q(x) = 0\} = R,$$

hence V_0' has to be a direct complement of R. But for any direct complement V_0' of R we have that the triple $(V_0', Q|_{V_0'}, R)$ defines the form Q. So, for any triple (V_0, Q_0, R), the number of triples (V_0', Q_0', R') such that $Q_{(V_0',Q_0',R')} = Q_{(V_0,Q_0,R)}$ is equal to the number of direct complements of R.

We are ready to conclude. We have $\begin{bmatrix} k \\ r \end{bmatrix}$ choices for V_0, $N(r)$ choices for Q_0 by definition, $q^{r(k-r)}$ choices for R by Lemma 2.4.31 and any form occurs $q^{r(k-r)}$ times. Hence $N(k,r) = \begin{bmatrix} k \\ r \end{bmatrix} N(r)$, as claimed. □

The next two sections constitute the proof of Theorem 2.4.35. They share a similar structure: first we compute $R(k,h)$ in some interesting cases, then we

use it, together with Lemma 2.4.33, to prove Theorem 2.4.35. The first deals with the odd characteristic case, the second deals with the characteristic 2 case.

Odd Characteristic Case

In this section, assume that $\operatorname{char}\mathbb{F}$ *is odd.*

LEMMA 2.4.36. *We have that*

1. $R(k,1) = q^{k-1}$ *if* k *is odd,*
2. $R(k,2) = q^{k-2}\frac{q^k-1}{q^2-1}$ *if* k *is even.*

These numbers are independent of the choice of a full-rank quadratic form Q*.*

PROOF. Let Q be a full-rank quadratic form on V. All 1-dimensional subspaces $V_1 \leq V$ such that $Q|_{V_1}$ has full rank are given by $V_1 = \langle v_1 \rangle$ for some vector $v_1 \in V$ such that $Q(v_1) \neq 0$. As Q has odd rank, it has q^{k-1} zeros, hence we have $q^k - q^{k-1}$ possible choices for v_1. But $\langle \lambda v_1 \rangle = \langle v_1 \rangle$ for any $\lambda \in \mathbb{F}, \lambda \neq 0$, hence each subspace is counted $q-1$ times. So $R(k,1) = \frac{q^k-q^{k-1}}{q-1} = q^{k-1}$, and this proves the first claim.

We now prove the second claim. We can choose any non zero $v_1 \in V$ as first basis vector of V_1 and we want to count the number of vectors $v_2 \in V \setminus \langle v \rangle$ such that $Q|_{\langle v_1, v_2 \rangle}$ has full rank. This holds if and only if

$$\det \begin{pmatrix} \tilde{B}_Q(v_1,v_1) & \tilde{B}_Q(v_1,v_2) \\ \tilde{B}_Q(v_1,v_2) & \tilde{B}_Q(v_2,v_2) \end{pmatrix} \neq 0,$$

i.e. if and only if v_2 is not a zero of the quadratic form on V defined by

$$Q'(x) := \tilde{B}_Q(v_1,v_1)\tilde{B}_Q(x,x) - \tilde{B}_Q(v_1,x)^2$$

for $x \in V$. One can easily verify that this is indeed a quadratic form and that the associated bilinear form is defined by

$$\tilde{B}_{Q'}(x,y) = 2\tilde{B}_Q(v_1,v_1)\tilde{B}_Q(x,y) - 2\tilde{B}_Q(v_1,x)\tilde{B}_Q(v_1,y)$$

for $x, y \in V$. We distinguish two cases. If $\tilde{B}_Q(v_1,v_1) = 0$ then $Q'(x) = -\tilde{B}_Q(v_1,x)^2$ is the square of a non zero linear form, hence it has rank 1. If $\tilde{B}_Q(v_1,v_1) \neq 0$ then the radical of V with respect to $\tilde{B}_{Q'}$ is exactly the span

of v_1, hence $\operatorname{rk} Q' = \operatorname{rk} Q - 1$ is odd as $\operatorname{rk} Q$ is even. In order to prove this, let $w \in \operatorname{Rad} V$ (with respect to $\tilde{B}_{Q'}$), i.e. $\tilde{B}_{Q'}(w, y) = 0$ for all $y \in V$. Then

$$\begin{aligned}\tilde{B}_{Q'}(w, y) &= 2\tilde{B}_Q(v_1, v_1)\tilde{B}_Q(w, y) - 2\tilde{B}_Q(v_1, w)\tilde{B}_Q(v_1, y) = \\ &= 2\tilde{B}_Q(\tilde{B}_Q(v_1, v_1)w - \tilde{B}_Q(v_1, w)v_1, y) = 0\end{aligned}$$

for all $y \in V$. But $\tilde{B}_Q$ is non-degenerate, hence this implies that $\tilde{B}_Q(v_1, v_1)w = \tilde{B}_Q(v_1, w)v_1$, therefore $w \in \langle v_1 \rangle$ as $\tilde{B}_Q(v_1, v_1) \neq 0$. This proves that $\operatorname{Rad} V \subseteq \langle v_1 \rangle$, and the converse inclusion is obvious. So in any case $\operatorname{rk} Q'$ is odd, hence Q' has q^{k-1} zeros. We can finally conclude. We have $q^k - 1$ choices for v_1 and $q^k - q^{k-1}$ choices for v_2, and any subspace is given by $(q^2-1)(q^2-q)$ different choices of v_1, v_2 (corresponding to the number of bases of $\langle v_1, v_2 \rangle$). So we have $R(k, 2) = \frac{(q^k-1)(q^k-q^{k-1})}{(q^2-1)(q^2-q)} = q^{k-2}\frac{q^k-1}{q^2-1}$. This concludes the proof. □

The following theorem implies Theorem 2.4.35 in the odd characteristic case. First we need two remarks. Full-rank quadratic forms on $\mathbb{F}$ correspond to non zero elements of $\mathbb{F}$, hence $N(1) = q - 1$. Full-rank quadratic forms on $\mathbb{F}^2$ correspond to triples $(x, y, z) \subseteq \mathbb{F}^3$ such that $xy - z^2 \neq 0$, which is a quadratic form of rank 3, hence $N(2) = q^3 - q^2 = q^2(q - 1)$.

THEOREM 2.4.37. *For $k \geq 1$,*

$$N(k) = \begin{cases} (q^k - 1)N(k-1) & \text{if } k \text{ is odd,} \\ q^k(q^{k-1} - 1)N(k-2) & \text{if } k \text{ is even.} \end{cases}$$

PROOF. If k is odd then we apply Construction 2.4.28 with $h = 1$. By Lemma 2.4.33 and the first claim of Lemma 2.4.36 we have

$$\begin{aligned}N(k) &= \frac{\begin{bmatrix} k \\ 1 \end{bmatrix} q^{k-1}}{R(k, 1)} N(1)N(k-1) = \\ &= \frac{q^k - 1}{q - 1}\frac{q^{k-1}}{q^{k-1}}(q-1)N(k-1) = \\ &= (q^k - 1)N(k-1).\end{aligned}$$

If k is even then we apply Construction 2.4.28 with $h = 2$. By Lemma 2.4.33 and the second claim of Lemma 2.4.36 we have

$$\begin{aligned}N(k) &= \frac{\begin{bmatrix} k \\ 2 \end{bmatrix} q^{2(k-2)}}{R(k, 2)} N(2)N(k-2) = \\ &= \frac{(q^k - 1)(q^{k-1} - 1)}{(q^2 - 1)(q - 1)} q^{2(k-2)} \times \\ &\times \frac{1}{q^{k-2}}\frac{q^2 - 1}{q^k - 1} q^2(q-1)N(k-2) = \\ &= q^k(q^{k-1} - 1)N(k-2).\end{aligned}$$

□

Characteristic 2 Case

In this section, assume that $\operatorname{char}\mathbb{F} = 2$.

LEMMA 2.4.38. *We have that*

1. $R(k,2) = q^{k-2}\frac{q^k-q}{q^2-1}$ *if* k *is odd,*
2. $R(k,2) = q^{k-2}\frac{q^k-1}{q^2-1}$ *if* k *is even.*

These numbers are independent of the choice of a full-rank quadratic form Q.

PROOF. The proof is similar to the proof of the second claim of Lemma 2.4.36. Let Q be a full-rank quadratic form on V. In order to obtain a plane $\langle v_1, v_2\rangle \leq V$ such that $Q|_{\langle v_1,v_2\rangle}$ has full rank, we can choose any $v_1 \in V \setminus \operatorname{Rad} V$ and any $v_2 \in V \setminus \langle v_1\rangle$ which is not a zero of the quadratic form defined by

$$Q'(x) := \tilde{B}_Q(v_1,v_1)\tilde{B}_Q(x,x) - \tilde{B}_Q(v_1,x)^2 = \tilde{B}_Q(v_1,x)^2$$

for $x \in V$. In the characteristic 2 case this form always has rank 1, hence it has q^{k-1} zeros. So we have $q^k - |\operatorname{Rad} V|$ choices for v_1 and $q^k - q^{k-1}$ choices for v_2, and any subspace is given by $(q^2-1)(q^2-q)$ different choices of v_1, v_2, hence $R(k,2) = \frac{(q^k-|\operatorname{Rad} V|)(q^k-q^{k-1})}{(q^2-1)(q^2-q)} = q^{k-2}\frac{q^k-|\operatorname{Rad} V|}{q^2-1}$. Now note that $|\operatorname{Rad} V| = q$ if k is odd and $|\operatorname{Rad} V| = 1$ if k is even, hence both claims follow at once. □

We are going to conclude the proof of Theorem 2.4.35. Again, we use the fact that $N(2) = q^2(q-1)$.

THEOREM 2.4.39. *For* $k \geq 1$,

$$N(k) = \begin{cases} q^{k-1}(q^k-1)N(k-2) & \text{if } k \text{ is odd,} \\ q^k(q^{k-1}-1)N(k-2) & \text{if } k \text{ is even.} \end{cases}$$

PROOF. Recall that in this case we use Construction 2.4.28 with $h = 2$. By Lemma 2.4.33 we have

$$\begin{aligned} N(k) &= \frac{\begin{bmatrix} k \\ 2 \end{bmatrix} q^{2(k-2)}}{R(k,2)} N(2)N(k-2) = \\ &= \frac{1}{R(k,2)} q^{2(k-2)} q^2(q-1) \times \\ &\times \frac{(q^k-1)(q^{k-1}-1)}{(q^2-1)(q-1)} N(k-2). \end{aligned}$$

If k is odd then by claim *1* of Lemma 2.4.38 we have

$$\begin{aligned} N(k) &= \frac{q^2-1}{q^k-q}\frac{1}{q^{k-2}}q^{2(k-2)}q^2(q-1)\times \\ &\times \frac{(q^k-1)(q^{k-1}-1)}{(q^2-1)(q-1)}N(k-2) = \\ &= q^{k-1}(q^k-1)N(k-2). \end{aligned}$$

If k is even then by claim *2* of Lemma 2.4.38 we have

$$\begin{aligned} N(k) &= \frac{q^2-1}{q^k-1}\frac{1}{q^{k-2}}q^{2(k-2)}q^2(q-1)\times \\ &\times \frac{(q^k-1)(q^{k-1}-1)}{(q^2-1)(q-1)}N(k-2) = \\ &= q^{k}(q^{k-1}-1)N(k-2). \end{aligned}$$

□

2.5 Coding Theory

In this section we expand the discussion started in Section 1.1 on the theory of linear error correcting codes by giving a better formalization of the definitions and results that we have already mentioned, and by introducing new results as well. Standard references are [37, 48, 71]. We will be especially focused on the theory of code products, to which Section 2.5.2 is dedicated. The literature concerning this topic is quite limited, we cite [65].

Let $\mathbb{F}$ be a finite field of size q and let n be a positive integer. The natural setting of coding theory is the vector space $\mathbb{F}^n$ endowed with the Hamming metric, i.e. the notion of distance defined below. In coding theory, it is customary to write vectors in row form, and we will stick to this convention here.

Definition 2.5.1. For all $x = (x_1, \dots, x_n), y = (y_1, \dots, y_n) \in \mathbb{F}^n$, we define

$$d(x, y) := |\{i : x_i \neq y_i\}|,$$

the *(Hamming) distance* between x and y.

One can readily check that the distance between two vectors is always a non-negative integer and is indeed a distance in the usual mathematical sense: for any $x, y, z \in \mathbb{F}^n$ it holds that

(i) $d(x, y) \geq 0$, and $d(x, y) = 0$ if and only if $x = y$,

(ii) $d(x,y) = d(y,x)$,

(iii) $d(x,y) \leq d(x,z) + d(z,y)$.

Given a vector $x = (x_1, \ldots, x_n) \in \mathbb{F}^n$, we define its *support* $\operatorname{supp} x := \{i : x_i \neq 0\}$ and its *weight* $\operatorname{wt}(x) := |\operatorname{supp} x|$. The support of a subset of $\mathbb{F}^n$ is defined as the union of the supports of all its elements, and we shall say that a subset of $\mathbb{F}^n$ has full support if its support is $\{1, \ldots, n\}$.

The space $\mathbb{F}^n$ is also equipped with the standard inner product, defined by

$$(x \,|\, y) := \sum_{i=1}^{n} x_i y_i$$

for all $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \mathbb{F}^n$. Orthogonality is defined with respect to this notion of product.

DEFINITION 2.5.2. A (q-ary, linear) *code* of *length* n is a linear subspace $C \subseteq \mathbb{F}^n$. Its elements are called *codewords*. The *dimension* of C is its dimension as an $\mathbb{F}$-vector space and is denoted by $\dim C$. The *minimum distance* of C is

$$d_{\min}(C) := \min\{d(x,y) : x, y \in C, x \neq y\} = \min\{\operatorname{wt}(x) : x \in C, x \neq 0\}.$$

A *generator matrix* of a code $C \subseteq \mathbb{F}^n$ is a matrix whose rows are an $\mathbb{F}$-basis of C. Set $k := \dim C$, then a generator matrix G of C is a full-rank $k \times n$ matrix with coefficients in $\mathbb{F}$, and it defines in a natural way a linear embedding $\mathbb{F}^k \to \mathbb{F}^n$ whose image is C. We say that G is in *systematic form* if its first k columns form a $k \times k$ identity matrix. An *information set* for C is a subset $I \subseteq \{1, \ldots, n\}$ of size k such that the columns of G indexed by I are linearly independent. By definition any code admits an information set, hence, possibly after renumbering the coordinates, any code admits a generator matrix in systematic form.

The *dual* of a code $C \subseteq \mathbb{F}^n$ is

$$C^\perp := \{x \in \mathbb{F}^n : (x \,|\, y) = 0 \text{ for all } y \in C\},$$

which is a code of length n and dimension $n - \dim C$. We say that C is self-orthogonal if $C \subseteq C^\perp$ and self-dual if $C = C^\perp$.

It will be convenient to allow coordinate sets, such as the index set of the n-fold cartesian product $\mathbb{K}^n$ of a field $\mathbb{K}$, to be arbitrary: if I is an arbitrary set then $\mathbb{K}^I$ is the set of all vectors $(x_i)_{i \in I}$ with all entries in $\mathbb{K}$. Equivalently, we can view $\mathbb{K}^I$ as the set of all functions $I \to \mathbb{K}$. If J is a subset of I then the projection of a subset S of $\mathbb{K}^I$ onto $\mathbb{K}^J$ is the set of restrictions to J of all functions in S.

This convention is particularly useful to define some standard constructions which allow to construct new codes from a given one. Fixed a coordinate $i \in \{1, \dots, n\}$, we can puncture or shorten a given code $C \subseteq \mathbb{F}^n$ at i. The *punctured* code is

$$C_{\overline{i}} := \{(x_j)_{j \neq i} : x = (x_1, \dots, x_n) \in C\},$$

the code obtained from C by removing the i-th coordinate of all its codewords, or equivalently the projection of C onto $\{1, \dots, n\} \setminus \{i\}$. The *shortened* code is

$$C^{\overline{i}} := \{(x_j)_{j \neq i} : x = (x_1, \dots, x_n) \in C \text{ and } x_i = 0\}.$$

In other words, it is the code obtained by puncturing at i the intersection of C with the hyperplane $\{x \in \mathbb{F}^n : x_i = 0\}$. These definitions can be extended, in a natural way, so that we can puncture and shorten codes at coordinate sets, instead of a single coordinate. The bar in the above notation signifies that the coordinate i is being excluded. In some situations, it will be convenient to highlight the coordinates which are preserved, and in these cases we will denote by C_I and C^I the codes obtained by puncturing and shortening C at the complement of $I \subseteq \{1, \dots, n\}$.

Given two codes $C \subseteq \mathbb{F}^{n_1}$ and $D \subseteq \mathbb{F}^{n_2}$, their cartesian product can be viewed as a code in $\mathbb{F}^{n_1+n_2}$, and it is called the *direct sum* of C and D and denoted by $C \oplus D$. It holds that $\dim C \oplus D = \dim C + \dim D$ and $d_{\min}(C \oplus D) = \min\{d_{\min}(C), d_{\min}(D)\}$.

The last construction is somewhat less standard, and harder to find in the literature. A reference is [22, Section 4.1]. Given two codes $C \subseteq \mathbb{F}^{n_1}$ and $D \subseteq \mathbb{F}^{n_2}$, their *amalgamated direct sum* is defined as

$$C \dot{\oplus} D := \{(x, z, y) : (x, z) \in C \text{ and } (z, y) \in D\}.$$

To lighten the above definition, we omitted that $x \in \mathbb{F}^{n_1-1}, y \in \mathbb{F}^{n_2-1}, z \in \mathbb{F}$ and consequently $(x, z, y) \in \mathbb{F}^{n_1+n_2-1}$. This is a linear subspace of $\mathbb{F}^{n_1+n_2-1}$. Equivalently, we can obtain $C \dot{\oplus} D$ as the kernel of the linear map

$$\begin{array}{ccc} C \oplus D & \longrightarrow & \mathbb{F} \\ (x, y) & \longmapsto & x_{n_1} - y_1 \end{array}$$

punctured at n_1. In particular it follows immediately that $\dim C \dot{\oplus} D = \dim C + \dim D - 1$.

2.5.1 MDS Codes and Reed-Solomon Codes

Length, dimension and minimum distance of a code are related by several classical results, the most important for us being the following.

THEOREM 2.5.3 (Singleton Bound reference!). *Let C be a code of length n. Then*

$$\dim C + d_{\min}(C) \leq n + 1.$$

DEFINITION 2.5.4. A code C of length n is *maximum distance separable* (MDS) if

$$\dim C + d_{\min}(C) = n + 1.$$

We recall the following well-known properties and characterizations of MDS codes [48].

LEMMA 2.5.5. *Given a code $C \subseteq \mathbb{F}^n$, the following statements are equivalent:*

1. *C is MDS,*
2. *$C^\perp$ is MDS,*
3. *any coordinate set of size $\dim C$ is an information set for C,*
4. *for any coordinate set I of size $n + 1 - \dim C$, there is a codeword whose support equals I.*

The following property is somewhat less standard.

LEMMA 2.5.6. *Let $C \subseteq \mathbb{F}^n$ be a code. It is MDS if and only if any systematic generator matrix of C has all its rows of weight $n + 1 - \dim C$.*

PROOF. It is clear that if C is MDS the property must hold. The converse implication is an immediate consequence of the following claim: if $C \subseteq \mathbb{F}^n$ is any code and $x \in C$ is a codeword of minimal weight, then there is a systematic generator matrix of C whose first row is x.

We now prove this claim. Renumbering the coordinates, we may assume that $\operatorname{supp} x = \{1, 2 + n - \operatorname{wt}(x), \ldots, n\}$ and that

$$x = (1, 0, \ldots, 0, *, \ldots, *),$$

where the stars denote non-zero entries. Let $\{x_1 = x, x_2, \ldots, x_k\}$ be an $\mathbb{F}$-basis of C containing x, where $k := \dim C$, and let G be the generator matrix of C whose rows are the x_i's. If G can be made systematic in the first $1 + n - \operatorname{wt}(x)$ positions then we are done. Otherwise, we obtain a contradiction as follows. We have that $\operatorname{wt}(x) > 1$ and the rank of the matrix G restricted to its first $1 + n - \operatorname{wt}(x)$ columns is $< k$. There exists therefore a linear combination

$$\tilde{x} = \sum_{i=2}^{k} \alpha_i x_i,$$

with $\alpha_2, \ldots, \alpha_k \in \mathbb{F}$, which has zeros in positions $\{2, \ldots, 1+n-\mathrm{wt}(x)\}$, but with $\tilde{x} \neq 0$. Now a suitable combination of x and $\tilde{x}$ yields a non-zero word of weight smaller than $\mathrm{wt}(x)$, contradicting the minimality of $\mathrm{wt}(x)$. □

Punctured and shortened MDS codes are still MDS codes, provided that the set of excluded coordinates is not too big. More precisely, if $C \subseteq \mathbb{F}^n$ is an MDS code and $I \subseteq \{1, \ldots, n\}$ has size at least $\dim C$ then the codes C_I and C^I obtained by puncturing and shortening C at the complement of I are MDS codes of length $|I|$ and dimensions $\dim C_I = \dim C$ and $\dim C^I = \dim C - (n - |I|)$.

We introduce now a well-known family of MDS codes, namely Reed-Solomon codes. Fix a positive integer k and n pairwise distinct elements $\alpha_1, \ldots, \alpha_n \in \mathbb{F}$. This in particular implies that we additionally require $n \leq q$. Let $\mathbb{F}[X]_{<k}$ denote the vector space of all polynomials in the indeterminate X, with coefficients in $\mathbb{F}$, and degree less than k. The image of the evaluation map

$$\begin{array}{ccc} \mathbb{F}[X]_{<k} & \longrightarrow & \mathbb{F}^n \\ f & \longmapsto & (f(\alpha_1), \ldots, f(\alpha_n)) \end{array}$$

is a linear space, called a *Reed-Solomon code*. This map is injective because any polynomial of degree at most $k-1$ is uniquely determined by any k distinct evaluations, hence the code has dimension k. Moreover, a polynomial of degree at most $k-1$ has at most $k-1$ zeros, hence any codeword has weight at least $n-k+1$. It follows that the code has minimum distance at least $n-k+1$, hence it is an MDS code.

The image of the standard basis of $\mathbb{F}[X]_{<k}$ is a basis of the code, and gives a generator matrix in Vandermonde form, namely

$$\begin{pmatrix} 1 & \cdots & 1 \\ \alpha_1 & \cdots & \alpha_n \\ \vdots & & \vdots \\ \alpha_1^{k-1} & \cdots & \alpha_n^{k-1} \end{pmatrix}.$$

One can notice that the third property of Lemma 2.5.6 is satisfied, and this gives an alternative proof that the code is MDS.

To better fit our needs, we generalize this notion in two senses. First, we allow one of the α_i's to be a "special" element ∞, with the convention that, for any $f \in \mathbb{F}[X]_{<k}$, $f(\infty)$ equals the coefficient of X^{k-1} in f. Observe that $f(\infty) = 0$ if $\deg f < k-1$. Second, we allow each coordinate of the code to be scaled by a non-zero factor. This leads to the following definition.

Definition 2.5.7. A *Reed-Solomon code* of dimension k and length n is a code

of the form

$$\{(g_1 f(\alpha_1), \ldots, g_n f(\alpha_n)) : f \in \mathbb{F}[X]_{<k}\},$$

where $\alpha_1, \ldots, \alpha_n \in \mathbb{F} \cup \{\infty\}$ are pairwise distinct and $g_1, \ldots, g_n \in \mathbb{F}$ are non-zero. We shall call $(\alpha_1, \ldots, \alpha_n)$ an *evaluation-point sequence* for the Reed-Solomon code.

The codes called generalized, extended, and doubly-extended Reed-Solomon codes are included in this family. From the geometric point of view, they may be thought of as the projective version of Reed-Solomon codes. In [30] they are named "Cauchy codes" and have also been called "Cauchy Reed-Solomon codes". We shall simply refer to them as "Reed-Solomon codes".

The above observations concerning generator matrix and minimum distance can easily be extended as well: the code

$$\{(g_1 f(\alpha_1), \ldots, g_n f(\alpha_n)) : f \in \mathbb{F}[X]_{<k}\},$$

with pairwise distinct $\alpha_1, \ldots, \alpha_n \in \mathbb{F} \cup \{\infty\}$ and non-zero $g_1, \ldots, g_n \in \mathbb{F}$, is generated by the $k \times n$ matrix whose i-th column is $g_i(1, \alpha_i, \ldots, \alpha_i^{k-1})^T$ if $\alpha_i \neq \infty$, $(0, \ldots, 0, g_i)^T$ otherwise. Again, the code is MDS as it satisfies the third property of Lemma 2.5.6.

All results concerning Reed-Solomon codes are consequences of Lagrange's Interpolation Theorem, which we include for future reference.

THEOREM 2.5.8 (Lagrange Interpolation). *Let $\mathbb{K}$ be a field and k a positive integer. Let $\alpha_1, \ldots, \alpha_k \in \mathbb{K}$ be pairwise distinct. Then the evaluation map*

$$\begin{array}{ccc} \mathbb{K}[X]_{<k} & \longrightarrow & \mathbb{K}^k \\ f & \longmapsto & (f(\alpha_1), \ldots, f(\alpha_k)) \end{array}$$

is an isomorphism of $\mathbb{K}$-vector spaces. Its inverse maps $(y_1, \ldots, y_k) \in \mathbb{K}^k$ into $\sum_{i=1}^k y_i \delta_i \in \mathbb{K}[X]_{<k}$, where for all $i = 1, \ldots, k$

$$\delta_i := \prod_{\substack{j=1,\ldots,k \\ j \neq i}} \frac{X - \alpha_j}{\alpha_i - \alpha_j}.$$

PROOF. We need to prove that, for all $f \in \mathbb{K}[X]_{<k}$,

$$f = \sum_{i=1}^{k} f(\alpha_i)\delta_i, \tag{2.1}$$

where the δ_i's are defined as above. Observe that, for all $i = 1, \ldots, k$,

(i) $\deg \delta_i = k - 1$,

(ii) $\delta_i(\alpha_i) = 1$,

(iii) $\delta_i(\alpha_j) = 0$ for all $j = 1, \ldots, k, j \neq i$.

From these properties it follows immediately that the two sides of (2.1) are polynomials of degree less than k which coincide at k points, namely the α_i's, hence the polynomials themselves must coincide. □

Also this theorem can be extended to include the special element ∞. For more details on this subject, and alternative proofs as well, we refer to [28].

Finally, we remark that the evaluation-point sequence of a Reed-Solomon code is not unique, but it is unique up to the action of the general linear group on $(\mathbb{F} \cup \{\infty\})^n$, which is defined as follows. We can identify the set $\mathbb{F} \cup \{\infty\}$ with the projective line $\mathbb{P}^1(\mathbb{F})$, mapping $\alpha \in \mathbb{F}$ into the class of $(1, \alpha)$ and ∞ into the class of $(0, 1)$. The general linear group

$$\mathrm{GL}_2(\mathbb{F}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{F}, ad - bc \neq 0 \right\}$$

acts on $\mathbb{P}^1(\mathbb{F})$ by multiplication, and on $(\mathbb{P}^1(\mathbb{F}))^n$ by coordinatewise application of the action. Moreover, as the action of $\mathrm{GL}_2(\mathbb{F})$ on $\mathbb{P}^1(\mathbb{F})$ is triply transitive[1], we can always fix three points on any evaluation-point sequence. For instance, we can always assume that an evaluation-point sequence starts with $0, 1, \infty$. For a fully detailed explanation, the reader is referred to [30].

2.5.2 Code Products

For an arbitrary field $\mathbb{K}$, the space $\mathbb{K}^n$ is, with the coordinatewise product, a commutative unitary $\mathbb{K}$-algebra: for all $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \mathbb{K}^n$, we define

$$xy := (x_1 y_1, \ldots, x_n y_n).$$

Its unit element is the all-one vector, denoted by $\mathbf{1}$. The multiplicative group of its invertible elements is $(\mathbb{K}^n)^\times = (\mathbb{K}^\times)^n$, meaning that $x \in \mathbb{K}^n$ is invertible if and only if all entries of x are non-zero. Given $x \in (\mathbb{K}^n)^\times$, its inverse is denoted by x^{-1}.

We use this notion of product to multiply spaces as well. Given two vector spaces $V, W \subseteq \mathbb{K}^n$, we define their product VW to be the $\mathbb{K}$-linear span of the set of all products xy, with $x \in V$ and $y \in W$. Note that, in general, this set

[1] I.e. for any pair of triples $(\alpha_1, \alpha_2, \alpha_3), (\beta_1, \beta_2, \beta_3) \in \mathbb{F}^3$ there exists $\sigma \in \mathrm{GL}_2(\mathbb{F})$ such that $\sigma(\alpha_i) = \beta_i$ for $i = 1, 2, 3$.

is not additively closed, hence it is strictly contained in its span. Likewise we shall denote the square of a space V by V^2. Context should prevent confusion with cartesian products.

We will be particularly interested in products of codes, i.e. in the case of a finite base field $\mathbb{F}$. The product of two codes $C, D \subseteq \mathbb{F}^n$, sometimes called the *Schur product*, has usually been denoted by $C * D$, but we shall drop the star symbol to lighten notation. For an exhaustive discussion on why our study of code products is well-motivated, the reader is referred to Chapter 1. We can immediately state a trivial upper bound for the product dimension.

THEOREM 2.5.9. *Let $C, D \subseteq \mathbb{F}^n$ be two codes. Then*

$$\dim CD \leq \dim C \dim D \quad \textit{and} \quad \dim C^2 \leq \frac{\dim C(\dim C + 1)}{2}.$$

PROOF. Let $\{x_1, \ldots, x_k\}$ and $\{y_1, \ldots, y_\ell\}$ be bases of C and D respectively, where we set $k := \dim C$ and $\ell := \dim D$. Then the products $x_i y_j$ with $1 \leq i \leq k$ and $1 \leq j \leq \ell$ span CD and the products $x_i x_j$ with $1 \leq i \leq j \leq k$ span C^2. □

In fact it holds that these bounds are achieved by most codes. This is shown in Chapter 3 for the second inequality, while for the first inequality the reader is referred to [64].

The following simple observation will be freely used later.

LEMMA 2.5.10. *Let $x \in (\mathbb{K}^n)^\times$. For any vector space $V \subseteq \mathbb{K}^n$, we have $\dim V = \dim xV$.*

Lemma 2.5.11 below classifies all subalgebras of $\mathbb{K}^n$. For all $i = 1, \ldots, n$, let e_i denote the i-th unit vector in $\mathbb{K}^n$. We call a vector of the form $\sum_{i \in I} e_i$ for some $I \subseteq \{1, \ldots, n\}$ a *projector*[2]. In particular, $\mathbf{1}$ is the projector with support $\{1, \ldots, n\}$. A family of projectors is *disjoint* if the projectors have pairwise disjoint supports.

LEMMA 2.5.11. *Any K-subalgebra of $\mathbb{K}^n$ admits a $\mathbb{K}$-basis of disjoint projectors.*

PROOF. Let $A \subseteq \mathbb{K}^n$ be a $\mathbb{K}$-subalgebra. We argue by induction on $k := \dim A$. If $k = 1$ then A is generated by a vector x whose non-zero coordinates must be all equal, otherwise x^2 is not a $\mathbb{K}$-multiple of x. If $k > 1$, pick $x \in A, x \neq 0$ of minimal support with one of its coordinates equal to 1, and let $\{x_1 = x, \ldots, x_k\}$

[2]To justify our terminology, note that if $V \subseteq \mathbb{K}^n$ is a vector space and and $x \in \mathbb{K}^n$ is a projector, then xV can be viewed as the projection of V onto the support of x.

be a $\mathbb{K}$-basis of A containing x. Then x is a projector, otherwise $x^2 - x \neq 0$ would have smaller support. For all $i = 2, \ldots, k$, if $\operatorname{supp} x_i$ and $\operatorname{supp} x$ intersect, say in position j, then we can choose $\lambda_i \in \mathbb{K}$ so that $x_i + \lambda_i x$ has a zero in position j, hence $x(x_i + \lambda_i x) \in A$ has support strictly smaller than x. By minimality of $\operatorname{supp} x$, $x(x_i + \lambda_i x) = 0$, i.e. x and $x_i + \lambda_i x$ have disjoint support. Replacing if need be x_i by $x_i + \lambda_i x$, we obtain that A is a direct sum $A = \langle x \rangle \oplus \langle x_2, \ldots, x_k \rangle$ and the conclusion follows by applying the induction hypothesis to the second summand. □

REMARK 2.5.12. Lemma 2.5.11 implies in particular that the number of subalgebras of $\mathbb{K}^n$ is finite.

Let $V \subseteq \mathbb{K}^n$ be a $\mathbb{K}$-vector space. We define $\operatorname{St}(V) := \{x \in \mathbb{K}^n : xV \subseteq V\}$, the *stabilizer* of V in $\mathbb{K}^n$. As V is linear, $\operatorname{St}(V)$ is a $\mathbb{K}$-algebra, hence Lemma 2.5.11 applies. In particular, as $\operatorname{St}(V)$ has a basis of vectors whose entries are all 0's and 1's, it is invariant under base-field extension[3], i.e. the following lemma holds.

LEMMA 2.5.13. *Let $\mathbb{K}'/\mathbb{K}$ be a field extension. Let $V \subseteq \mathbb{K}^n$ be a $\mathbb{K}$-vector space. Then*

$$\operatorname{St}(V \otimes \mathbb{K}') = \operatorname{St}(V) \otimes \mathbb{K}'.$$

Let $C \subseteq \mathbb{F}^n$ be a code. As in the vector-space case, we can define its stabilizer and apply Lemma 2.5.11, which yields an $\mathbb{F}$-basis $\{\pi_1, \ldots, \pi_h\}$ of $\operatorname{St}(C)$ of disjoint projectors, where $h := \dim \operatorname{St}(C)$. When $h = 1$ we say that C has trivial stabilizer, or that it is indecomposable. We have the following lemma, whose proof is straightforward.

LEMMA 2.5.14. *Any full-support code $C \subseteq \mathbb{F}^n$ decomposes as*

$$C = \pi_1 C \oplus \cdots \oplus \pi_h C$$

where $\{\pi_1, \ldots, \pi_h\}$ is an $\mathbb{F}$-basis of disjoint projectors of $\operatorname{St}(C)$. Moreover, each summand $\pi_i C$, viewed as a code in $\mathbb{F}^{\operatorname{wt}(\pi_i)}$, is indecomposable and has full support.

Facts on stabilizers, including Lemmas 2.5.13 and 2.5.14, can be found in [65, from §2.6 onwards].

Lemma 2.5.14 states in particular that a full-support code has non-trivial stabilizer if and only if it decomposes as a direct sum of codes, and the dimension of the stabilizer equals the number of indecomposable components. It follows that all MDS codes, except the trivial code $\mathbb{F}^n$, have trivial stabilizer.

[3] If $\mathbb{K}'/\mathbb{K}$ is a field extension, the base-field extension $V \otimes \mathbb{K}'$, where the tensor product is taken over $\mathbb{K}$, of V is the $\mathbb{K}'$-span of V.

We continue this section with two refinements of the classical Singleton Bound, involving the dimension of $\mathrm{St}(C)$ beside the usual parameters. They naturally reduce to the classical Singleton Bound when the code C is indecomposable, i.e. $\dim \mathrm{St}(C) = 1$.

LEMMA 2.5.15. *Let $C \subseteq \mathbb{F}^n$ be a code.*

1. *If $d_{\min}(C) > 1$ then*

$$d_{\min}(C) \leq n - \dim C + 1 - (\dim \mathrm{St}(C) - 1).$$

2. *If C has full support then*

$$d_{\min}(C) \leq \frac{n - \dim C}{\dim \mathrm{St}(C)} + 1.$$

PROOF. We may assume that C has full support, as the first claim in the general case follows immediately from the first claim in the full-support case. Set $k := \dim C$, $d := d_{\min}(C)$ and $h := \dim \mathrm{St}(C)$. By Lemma 2.5.14 we have that C is a direct sum $C = C_1 \oplus \cdots \oplus C_h$ of full-support codes. For all $i = 1, \ldots, h$, let n_i, k_i and d_i denote the support size, the dimension and the minimum distance of C_i respectively. We have $\sum_{i=1}^{h} n_i = n, \sum_{i=1}^{h} k_i = k$ and

$$d = \min_i\{d_i\} \leq \min_i\{n_i - k_i\} + 1$$

by the classical Singleton Bound. In the case $d > 1$ we have $n_i - k_i \geq d_i - 1 \geq 1$ for all $i = 1, \ldots, h$, hence, for all $j = 1, \ldots, h$,

$$n_j - k_j = n - k - \sum_{i \neq j}(n_i - k_i) \leq n - k - (h - 1).$$

Putting everything together we have

$$d = \min_i\{d_i\} \leq \min_i\{n_i - k_i\} + 1 \leq n - k + 1 - (h - 1),$$

which proves the first claim. To prove the second claim, note that

$$n - k = \sum_{i=1}^{h}(n_i - k_i) \geq h \min_i\{n_i - k_i\},$$

hence $\min_i\{n_i - k_i\} \leq (n - k)/h$ and the conclusion follows. □

We conclude this section with some remarks on the effect of the product operation on MDS codes. The two results below relate the dimension of the product of two codes with the MDS property.

THEOREM 2.5.16. *Let $C, D \subseteq \mathbb{F}^n$ be full-support codes. If (at least) one of them is MDS, then*

$$\dim CD \geq \min\{n, \dim C + \dim D - 1\}.$$

PROOF. See [65, §3.5]. □

LEMMA 2.5.17. *Let $C, D \subseteq \mathbb{F}^n$ be MDS codes such that*

$$\dim CD = \dim C + \dim D - 1.$$

Then CD is MDS.

PROOF. By Lemma 2.5.5, it suffices to show that for any choice of $I \subseteq \{1, \ldots, n\}$ with $|I| = d^* := n + 1 - \dim CD$ there exist $x \in C, y \in D$ with $\operatorname{supp} xy = I$. Without loss of generality, assume that $I = \{1, \ldots, d^*\}$. As C and D are both MDS, there exist $x \in C$ and $y \in D$ such that $\operatorname{supp} x = I \cup \{d^* + 1, \ldots, d_C\}$ and $\operatorname{supp} y = I \cup \{n - (d_D - d^*) + 1, \ldots, n\}$, where d_C and d_D denote the minimum distance of C and D respectively. One checks that $d_C = n - (d_D - d^*)$, hence indeed $\operatorname{supp} xy = \operatorname{supp} x \cap \operatorname{supp} y = I$. □

Finally, we observe that if C and D are two Reed-Solomon codes with a common evaluation-point sequence α, then the product CD is also Reed-Solomon with evaluation-point sequence α and we have $\dim CD = \min\{n, \dim C + \dim D - 1\}$ which, as Theorem 2.5.16 states, is the minimum possible dimension of the product of MDS codes.

2.5.3 Error Correcting Pairs

Code products where first used by Pellikaan [57, 58] and by Kötter [43] to define error correcting pairs.

Let $C \subseteq \mathbb{F}^n$ be a code and let t be a positive integer.

DEFINITION 2.5.18. A pair (A, B) of codes is a *t-error correcting pair* for C if

(i) $AB \subseteq C^\perp$,

(ii) $\dim A > t$,

(iii) $d_{\min}(B^\perp) > t$,

(iv) $d_{\min}(A) + d_{\min}(C) > n$.

This definition was subsequently extended in [59, 60], allowing A and B to be defined over a finite extension of $\mathbb{F}$.

A first example of error correcting pair comes from MDS codes: if $A, B \subseteq \mathbb{F}^n$ are MDS codes with $\dim A = t + 1$ and $\dim B = t$ then (A, B) is a t-error correcting pair for $C := (AB)^{\perp}$. Indeed, the first three properties are straightforward, while the last one follows from [60, Corollary 3.4]. Moreover, by Theorem 2.5.16 it follows that $\dim C \leq n - 2t$. This bound is attained if A and B are Reed-Solomon codes with a common evaluation-point sequence, and in this case C is a Reed-Solomon code as well. We will show in Section 4.3.1 that the converse also holds, i.e. that a code of dimension $n - 2t$ with a t-error correcting pair is necessarily Reed-Solomon.

These objects are relevant to the decoding problem. Suppose that the sum $\tilde{x} = x + e$ of a codeword $x \in C$ and of an error vector $e \in \mathbb{F}^n$ of weight t is known. Is it possible to correct the t errors in $\tilde{x}$, i.e. recover x, efficiently? The existence of error correcting pairs allows one to answer positively.

THEOREM 2.5.19 ([57, 58]). *If C admits a t-error correcting pair over a finite extension of $\mathbb{F}$ then there exists a t-error correcting algorithm with complexity $O(n^3)$.*

We now outline how the algorithm mentioned in Theorem 2.5.19 works in practice. Suppose that a vector $\tilde{x} \in \mathbb{F}^n$ is given, and that $\tilde{x} = x + e$ for some $x \in C$ and $e \in \mathbb{F}^n$ with $\mathrm{wt}(e) \leq t$. Our purpose is to recover x, or equivalently e.

The key observation is the following: a vector $y \in \mathbb{F}^n$ which is zero at every coordinate in the support of e satisfies

$$xy = \tilde{x}y. \tag{2.2}$$

On the left-hand side, the componentwise product of two vectors appears. Suppose that there exists a code $A \subseteq \mathbb{F}^n$ satisfying the following property: for each set of t coordinates, there exists a codeword of A which is zero at each of the chosen coordinates. In particular, the vector y satisfying (2.2) can always be chosen from A and in this case the product xy belongs to the code product $B' := CA$. So, instead of solving (2.2), we solve

$$z = \tilde{x}y \tag{2.3}$$

with $z \in B'$ and $y \in A$. By expressing z and y as linear combinations of basis vectors, this is a linear system with n equations and $\dim B' + \dim A$ unknowns.

Let B denote the dual of B'. We have just defined a pair (A, B) which satisfies the first condition of Definition 2.5.18. We now show how the other conditions are used to guarantee the existence of a solution to (2.3), to prove that such

a solution solves (2.2) as well, and finally to prove its uniqueness. First, if $\dim A > t$ then, for each set of t coordinates, there exists a codeword of A which is zero at each of the chosen coordinates, hence there exists a solution (x, y) to (2.2) with $y \in A$, which yields a solution (xy, y) to (2.3). Now assume that there exists a solution (z, y) to (2.3), and we want to prove that $z = xy$ for some $x \in C$. If this is the case, then we can recover the coordinates of x corresponding to non-error positions by "dividing z by y", hence the whole x by solving the erasure decoding problem. We have that

$$z = \tilde{x}y = (x + e)y = xy + ey,$$

hence $ey \in B'$. Assuming that $d_{\min}(B') > t$ implies $ey = 0$, hence z is of the required form. Finally, if there exists $x, x' \in C$ such that (xy, y) and $(x'y, y)$, for some $y \in A$, are both solutions of (2.3), then $x - x'$ is a non-zero codeword which is zero on the support of y. This cannot happen if we assume $d_{\min}(A) + d_{\min}(C) > n$.

2.5.4 Code Products and Bilinear Maps

In this section we introduce a new perspective on codes which will be particularly useful to analyze the parameters of code products.

Let $C \subseteq \mathbb{F}^n$ be a code of dimension k, and let G be a generator matrix of C. As anticipated in Section 2.5, G defines in a natural way a linear embedding $\mathbb{F}^k \to \mathbb{F}^n$ whose image is C, namely the map $x \mapsto xG$. If we denote the columns of G by $y_1, \ldots, y_n$, then the entries of the codeword xG are the inner products $(x \,|\, y_i)$, for $i = 1, \ldots, n$. Recall that, by classical linear algebra, the map $x \mapsto (x \,|\, \cdot)$ gives an isomorphism between any vector space and its dual. It follows that the image of the linear map

$$\begin{array}{ccc} (\mathbb{F}^k)^* & \longrightarrow & \mathbb{F}^n \\ \phi & \longmapsto & (\phi(y_1), \ldots, \phi(y_n)) \end{array}$$

equals C and in particular is independent of the choice of the y_i's. Conversely, given any $\mathbb{F}$-vector space V and $v_1, \ldots, v_n \in V$, the image of the linear map

$$\begin{array}{ccc} V^* & \longrightarrow & \mathbb{F}^n \\ \phi & \longmapsto & (\phi(v_1), \ldots, \phi(v_n)) \end{array}$$

is a code and, provided that the y_i's generate V, has dimension $\dim V$.

Let now $C, D \subseteq \mathbb{F}^n$ be two codes of dimension k_C and k_D respectively, and let $y_1, \ldots, y_n \in \mathbb{F}^{k_C}$ and $z_1, \ldots, z_n \in \mathbb{F}^{k_D}$ be the columns of a generator matrix

of C and of a generator matrix of D respectively. As above, we can view the codes C and D as images of evaluation maps. In addition, we define the map

$$\begin{array}{ccc} \mathrm{Bil}(\mathbb{F}^{k_C} \times \mathbb{F}^{k_D}) & \longrightarrow & \mathbb{F}^n \\ B & \longmapsto & (B(y_1, z_1), \ldots, B(y_n, z_n)) \end{array}$$

where $\mathrm{Bil}(\mathbb{F}^{k_C} \times \mathbb{F}^{k_D})$ denotes the $\mathbb{F}$-vector space of all bilinear forms $\mathbb{F}^{k_C} \times \mathbb{F}^{k_D} \to \mathbb{F}$. This map is linear as well and its image is independent of the choice of y_i's and z_i's and equals the code product CD. In the symmetric case $C = D$ we obtain the code square C^2 as the image of the evaluation map

$$\begin{array}{cccc} \mathrm{ev}_C\colon & \mathrm{Quad}(\mathbb{F}^{k_C}) & \longrightarrow & \mathbb{F}^n. \\ & Q & \longmapsto & (Q(y_1), \ldots, Q(y_n)) \end{array}$$

In this case the classical identity

$$\dim C^2 = \dim \mathrm{Quad}(\mathbb{F}^{k_C}) - \dim \ker \mathrm{ev}_C$$

allows us to relate the dimension of the code square with a combinatorial problem about quadratic forms, namely counting the number of quadratic forms which vanish at a given set of points. Chapter 3 proceeds further in this direction, exploiting this relation to estimate the dimension of the square of a random linear code.

Finally, we show how this perspective can be twisted in a way that will be useful when analyzing code-based secret sharing schemes in Section 2.6.3. First, we can see the columns of G as linear forms on $\mathbb{F}^k$, and obtain C as the image of the linear map

$$\begin{array}{ccc} \mathbb{F}^k & \longrightarrow & \mathbb{F}^n. \\ x & \longmapsto & (y_1(x), \ldots, y_n(x)) \end{array}$$

Then $C \times D$ is the image of the evaluation map

$$\begin{array}{ccc} \mathbb{F}^{k_C} \times \mathbb{F}^{k_D} & \longrightarrow & \mathbb{F}^n. \\ (x, w) & \longmapsto & (y_1 \otimes z_1(x, w), \ldots, y_n \otimes z_n(x, w)) \end{array}$$

2.6 Arithmetic Secret Sharing

We introduce arithmetic secret sharing, which is the main motivation for our study of code products. In particular, Section 2.6.3 is dedicated to showing

how codes and secret sharing schemes are closely related. We conclude this section with a quick sketch of how a secure multiparty computation protocol can be built from a secret sharing scheme. The main reference on this topic is [28]. Among the possible equivalent definitions of secret sharing schemes, we first give a general definition based on codices [16], and then we pick the one which best suits our needs.

DEFINITION 2.6.1. Let $\mathbb{K}$ be an arbitrary field and let A be a finite-dimensional $\mathbb{K}$-algebra. Let n, t, d, r be integers with $d \geq 1$ and $0 \leq t < r \leq n$. An (n, t, d, r)-*codex* (for A over $\mathbb{K}$) is a pair (C, ψ) where $C \subseteq \mathbb{K}^n$ is a $\mathbb{K}$-vector space and $\psi \colon C \to A$ is a $\mathbb{K}$-linear map satisfying the following properties:

(i) ψ is surjective;

(ii) (C, ψ) satisfies (d, r)-*multiplicativity*, i.e. there exists a unique $\mathbb{K}$-linear map $\overline{\psi} \colon C^d \to A$ which satisfies

$$\overline{\psi}(x_1 \cdots x_d) = \psi(x_1) \cdots \psi(x_d)$$

for all $x_1, \ldots, x_d \in C$ and is r-wise determined[4];

(iii) (C, ψ) satisfies t-*disconnection*, i.e. for each $B \subseteq \{1, \ldots, n\}$ with $|B| = t$ the projection map

$$\begin{array}{ccc} C & \longrightarrow & \psi(C) \times C_B \\ x & \longmapsto & (\psi(x), x_B) \end{array}$$

is surjective.

REMARK 2.6.2. As to the second condition, we remark that here C^d denotes the d-th code power of C (and not a cartesian product) and that, in the multiplicative relation, the product on the left-hand side is componentwise while the product on the right-hand side is multiplication in the algebra A. In the third condition, C_B denotes the projection of C onto B and x_B is a shorthand for $(x_i)_{i \in B}$.

DEFINITION 2.6.3. If $\mathbb{K}$ is a finite field, $d \geq 2$ and $t \geq 1$ then a codex as in Definition 2.6.1 is called an (n, t, d, r)-*arithmetic secret sharing scheme* with secret space A and share space $\mathbb{K}$.

The strength of this notion is that it encompasses all known relevant variations on arithmetic secret sharing. For instance, an $(n, t, 2, n)$-codex is a multiplicative scheme and an $(n, t, 2, n - t)$-codex is a t-strongly multiplicative scheme in the sense of upcoming Definitions 2.6.5 and 2.6.7 respectively. Even more,

[4] If $z, z' \in C^d$ are equal at r coordinates then their images via $\overline{\psi}$ are also equal, i.e. $\overline{\psi}(z) = \overline{\psi}(z')$.

it captures notions from other fields such as the one of bilinear multiplication algorithm introduced in Section 2.3.

We now focus on the definition which best suits our needs. Let $\mathbb{F}$ be a finite field of size q, n a positive integer, and let V be a finite-dimensional $\mathbb{F}$-vector space.

DEFINITION 2.6.4. A (linear) *secret sharing scheme* (for $\mathbb{F}$, over $\mathbb{F}$, among n players) is a sequence of linear forms $\Sigma = (\pi_0, \pi_1, \ldots, \pi_n) \subseteq V^*$ such that

(i) π_0 is non zero,

(ii) π_0 belongs to the span of $\{\pi_i : i = 1, \ldots, n\}$.

The set $\mathcal{P} := \{1, \ldots, n\}$ is the *player set*. Given a non-empty subset $I \subseteq \mathcal{P}$ we define $\Sigma_I := (\pi_i : i \in \{0\} \cup I)$ and we say that I is *accepting* if $\pi_0 \in \langle \pi_i : i \in I \rangle$, i.e. if Σ_I is also a secret sharing scheme, *rejecting* otherwise. The *access structure* of the scheme collects the accepting sets, whereas the *adversary structure* collects the rejecting sets. Let t, r be integers with $0 \leq t < r \leq n$. The scheme has *r-reconstruction* if all subsets of $\mathcal{P}$ of cardinality at least r are accepting and it has *t-privacy* if all subsets of $\mathcal{P}$ of cardinality at most t are rejecting.

Note that we will not consider any of the more general definitions of secret sharing from the literature, such as non-linear secret sharing and those allowing the secrets (and/or the shares) to be vectors rather than single field elements.

A secret sharing scheme $\Sigma = (\pi_0, \pi_1, \ldots, \pi_n) \subseteq V^*$ implements the following two functionalities. Given a secret element $s \in \mathbb{F}$, it can be *shared* as follows: select $x \in V$ uniformly at random such that $\pi_0(x) = s$, which is possible by assumption (i); define the i-th share to be $\pi_i(x) \in \mathbb{F}$. If a secret element $s \in \mathbb{F}$ has been shared, with shares $x_1, \ldots, x_n \in \mathbb{F}$, then it can be *reconstructed* as follows: by implementation of the sharing functionality there exists $x \in V$ such that $s = \pi_0(x)$ and $x_i = \pi_i(x)$ for all $i = 1, \ldots, n$; by assumption (ii) there exists $\lambda_1, \ldots, \lambda_n \in \mathbb{F}$ such that $\pi_0 = \sum_{i=1}^n \lambda_i \pi_i$; hence we can compute

$$s = \pi_0(x) = \left(\sum_{i=1}^n \lambda_i \pi_i \right)(x) = \sum_{i=1}^n \lambda_i \pi_i(x) = \sum_{i=1}^n \lambda_i x_i.$$

In other words, there exists an $\mathbb{F}$-linear form $\rho \colon \mathbb{F}^n \to \mathbb{F}$, the *reconstruction function*, such that $\rho(\pi_1(x), \ldots, \pi_n(x)) = \pi_0(x)$ for all $x \in V$. Observe that ρ does not depend on the secret, but only on the scheme.

In addition, a secret sharing scheme defined as above has the following linearity property. Suppose that two secrets $s, s' \in \mathbb{F}$ are shared, sampling $x, x' \in V$

such that $\pi_0(x) = s$ and $\pi_0(x') = s'$ and obtaining $x_i = \pi_i(x)$ and $x'_i = \pi_i(x')$, for all $i = 1, \ldots, n$, as valid shares of s and s' respectively. Then the i-th player can compute a valid i-th share for the sum of the two secrets, namely $x + x'$, without interacting with other players. Indeed by linearity of the π_i's we have that

$$\pi_i(x + x') = \pi_i(x) + \pi_i(x') = x_i + x'_i$$

and

$$\pi_0(x + x') = \pi_0(x) + \pi_0(x') = s + s'.$$

In other words, the sum of the shares of the secrets is a share of the sum of the secrets. Analogously, each player can individually compute a valid share for any multiple λs, with $\lambda \in \mathbb{F}$, of the secret.

If a subset $I \subseteq \mathcal{P}$ is accepting then there is an $\mathbb{F}$-linear form $\rho_I \colon \mathbb{F}^{|I|} \to \mathbb{F}$, the reconstruction function for I, such that $\rho_I((\pi_i(x))_{i \in I}) = \pi_0(x) = s$ for all $x \in \mathbb{F}^k$. In other words, if I is accepting, the secret can be reconstructed (linearly) from the joint shares of I. Again, such a function does not depend on the secret, but only on the scheme.

On the other hand, if I is non-empty and rejecting, then, for any $x \in V$, $(\pi_i(x))_{i \in I}$ is (part of) a set of valid shares for any possible secret. To prove this claim, the key observation is that $\pi_0 \notin \langle \pi_i : i \in I \rangle$ if and only if there exists $z \in V$ (where z may depend on I) such that $\pi_0(z) = 1$ and $\pi_i(z) = 0$ for all $i \in I$. This is trivial by linear algebra. Let $x \in V$, let $s := \pi_0(x)$ be the secret corresponding to x and let $s' \in \mathbb{F}$ be an arbitrary secret. Set $\lambda := s' - s$, then $s' = \pi_0(x) + \lambda\pi_0(z) = \pi_0(x + \lambda z)$, i.e. s' corresponds to the vector $x + \lambda z$. On the other hand, for all $i \in I$ we have $\pi_i(x + \lambda z) = \pi_i(x) + \lambda\pi_i(z) = \pi_i(x)$, i.e. $(\pi_i(x))_{i \in I}$ is (part of) a set of valid shares for s'.

We remark that, in the case of linear secret sharing schemes, a non-empty player subset is either accepting, i.e. can recover the secret, or rejecting, i.e. sees all possible secrets as equally likely. No subset has partial information about the secret. If this happens, the secret sharing scheme is said to be *perfect*. This is a property of linear secret sharing schemes, but is not necessarily satisfied by more general classes of schemes.

Finally, we introduce the notion of multiplicativity.

Definition 2.6.5. A secret sharing scheme $(\pi_0, \pi_1, \ldots, \pi_n) \subseteq V^*$ is *multiplicative* if there is an $\mathbb{F}$-linear form $\rho^* \colon \mathbb{F}^n \to \mathbb{F}$ such that, for all $x, y \in V$,

$$\rho^*(\pi_1(x)\pi_1(y), \ldots, \pi_n(x)\pi_n(y)) = \pi_0(x)\pi_0(y).$$

In other words, the product of two secrets is obtained as a linear function of the vector consisting of the coordinate-wise product of two respective share-vectors. Such a function is called a *product reconstruction function*. This is a

special property that is not generally satisfied by linear secret sharing schemes. Please refer to [27, 20] for more information about constructions and bounds.

The multiplicative property can be stated in terms of the properties of the symmetric bilinear forms $\pi_i \otimes \pi_i$.

PROPOSITION 2.6.6. *A secret sharing scheme $(\pi_0, \pi_1, \ldots, \pi_n) \subseteq V^*$ is multiplicative if and only if $\pi_0 \otimes \pi_0$ is in the span of $\{\pi_i \otimes \pi_i : i = 1, \ldots, n\}$.*

Let $1 \leq t \leq n$ be an integer.

DEFINITION 2.6.7. A secret sharing scheme $\Sigma = (\pi_0, \pi_1, \ldots, \pi_n) \subseteq V^*$ is *t-strongly multiplicative* if it has t-privacy and $(n-t)$-product reconstruction, i.e., for every set $I \subseteq \mathcal{P}$ of $n-t$ players, the scheme Σ_I is multiplicative.

A secret sharing scheme which supports one of the above multiplication properties is said to be *arithmetic*.

Proposition 2.6.6 suggests that, given a secret sharing scheme $(\pi_0, \ldots, \pi_n) \subseteq V^*$, we can consider the *product scheme* generated by the symmetric bilinear forms $(\pi_0 \otimes \pi_0, \ldots, \pi_n \otimes \pi_n) \subseteq V^* \otimes V^*$. This is a secret sharing scheme as defined by Definition 2.6.4 if and only if the original scheme is multiplicative. Moreover, we have that a secret sharing scheme is t-strongly multiplicative if and only if it has t-privacy and its product has $(n-t)$-reconstruction.

LEMMA 2.6.8. *If a secret sharing scheme among n players has t-privacy and r^*-product reconstruction then it has $(r^* - t)$-reconstruction.*

PROOF. Let $(\pi_0, \ldots, \pi_n) \subseteq V^*$ be a secret sharing scheme with t-privacy and r^*-product reconstruction. Let $I \subseteq \mathcal{P}$ be a set of $r^* - t$ players, and assume towards a contradiction that it is rejecting, i.e. that $\pi_0 \notin \langle \pi_i : i \in I \rangle$. By linear algebra, this means that there exists $x \in V$ such that $\pi_0(x) = 1$ while $\pi_i(x) = 0$ for all $i \in I$. Let $J \subseteq \mathcal{P}$ be a set of t players disjoint from I. By t-privacy, $\pi_0 \notin \langle \pi_j : j \in J \rangle$, hence there exists $y \in V$ such that $\pi_0(y) = 1$ while $\pi_j(y) = 0$ for all $j \in J$. Now consider the set $I \cup J$, which has r^* players. We have that $\pi_0 \otimes \pi_0(x, y) = 1$ while $\pi_i \otimes \pi_i(x, y) = 0$ for all $i \in I \cup J$, hence $\pi_0 \otimes \pi_0 \in \langle \pi_i \otimes \pi_i : i \in I \cup J \rangle$ against r^*-product reconstruction. It follows that I is accepting, hence the scheme has $(r^* - t)$-reconstruction. □

PROPOSITION 2.6.9. *If a secret sharing scheme among n players is t-strongly multiplicative then $n \geq 3t + 1$.*

PROOF. This is a straightforward consequence of the previous lemma: a t-strongly multiplicative scheme among n players has t-privacy and $(n-t)$-product reconstruction, hence $(n-2t)$-reconstruction, hence $n - 2t > t$ and the conclusion follows. □

2.6.1 Composition of Secret Sharing Schemes

Let V' and V'' be $\mathbb{F}$-vector spaces. Let $\Sigma' = (\pi'_0, \ldots, \pi'_{n'}) \subseteq (V')^*$ and $\Sigma'' = (\pi''_0, \ldots, \pi''_{n''}) \subseteq (V'')^*$ be secret sharing schemes among n' and n'' players respectively.

We define a new secret sharing scheme $\Sigma = \Sigma'[\Sigma'']$ among $n := n' + n'' - 1$ players, the *composition* of Σ' with Σ'', which implements the following sharing functionality. To share $s \in \mathbb{F}$ among n players, first share it using Σ', so that n' shares $x'_1, \ldots, x'_{n'}$ are obtained. Then use Σ'' to share $x'_{n'}$ and obtain n'' shares $x''_1, \ldots, x''_{n''}$. The n shares of s in the scheme Σ are $x'_1, \ldots, x'_{n'-1}$ and $x''_1, \ldots, x''_{n''}$. In other words, in this composition the n'-th player of the scheme Σ' has been substituted by the set of players of the scheme Σ''.

The player sets of Σ' and Σ'' can be identified, respectively, with $\{1, \ldots, n' - 1, p_0\}$ and $\{n', \ldots, n\}$, where p_0 denotes the player of the scheme Σ' corresponding to the linear form $\pi'_{n'}$. For a set $I \subseteq \{1, \ldots, n\}$, define $I' := I \cap \{1, \ldots, n' - 1\}$ and $I'' := I \cap \{n', \ldots, n\}$. Then I is accepting for Σ if and only if I' is accepting for Σ', or $I' \cup \{p_0\}$ is accepting for Σ' and I'' is accepting for Σ''. In particular, if Σ' has t-privacy then Σ has t-privacy.

As to the multiplicativity property, observe that if the scheme $\Sigma'_{\{1,\ldots,n'-1\}}$ obtained by removing player p_0 from Σ' is multiplicative then $\Sigma'[\Sigma'']$ is always multiplicative. So it makes sense to exclude this case in the proposition below.

PROPOSITION 2.6.10. *Suppose that $\Sigma'_{\{1,\ldots,n'-1\}}$ is not a multiplicative secret sharing scheme. If $\Sigma = \Sigma'[\Sigma'']$ is a multiplicative secret sharing scheme then both Σ' and Σ'' are so.*

Clearly the converse is also true. Before proving this proposition, we formalize the mathematical framework we are working with. Define the vector space

$$V := \{(x', x'') \in V' \times V'' \,:\, \pi'_{n'}(x') = \pi''_0(x'')\} \subseteq V' \times V''.$$

Then $V^* = ((V')^* \times (V'')^*)/\langle(\pi'_{n'}, -\pi''_0)\rangle$. Given a vector $(\pi, \tau) \in (V')^* \times (V'')^*$, we denote its class in V^* with $\overline{(\pi, \tau)}$. The composition $\Sigma = \Sigma'[\Sigma'']$ of Σ' with Σ'' is the secret sharing scheme $\Sigma = (\pi_0, \ldots, \pi_n) \subseteq V^*$ among $n := n' + n'' - 1$ players defined by

- $\pi_i := \overline{(\pi'_i, 0)}$ for all $i = 0, \ldots, n' - 1$,
- $\pi_{n'+j-1} := \overline{(0, \pi''_j)}$ for all $j = 1, \ldots, n''$.

We are now ready to prove the above proposition.

PROOF OF PROPOSITION 2.6.10. Define $\tau_0 := \overline{(\pi'_{n'}, 0)} = \overline{(0, \pi''_0)} \in V^*$ and observe that:

1. $\langle \pi_i : i = 0, \ldots, n'-1 \rangle \cap \langle \pi_i : i = n', \ldots, n \rangle \subseteq \langle \tau_0 \rangle$;
2. $\langle \pi_i \otimes \pi_i : i = 0, \ldots, n'-1 \rangle \cap \langle \pi_i \otimes \pi_i : i = n', \ldots, n \rangle \subseteq \langle \tau_0 \otimes \tau_0 \rangle$.

The first property is obvious, while the second one is a straightforward consequence of the first one.

If $\Sigma = \Sigma'[\Sigma'']$ is multiplicative then the inclusion in the property 2 above is an equality. Indeed, by definition there exists $\lambda_1, \ldots, \lambda_n \in \mathbb{F}$ such that

$$\pi_0 \otimes \pi_0 = \sum_{i=1}^{n} \lambda_i \pi_i \otimes \pi_i,$$

hence

$$\pi_0 \otimes \pi_0 - \sum_{i=1}^{n'-1} \lambda_i \pi_i \otimes \pi_i = \sum_{i=n'}^{n} \lambda_i \pi_i \otimes \pi_i.$$

The left-hand side of this identity is in $\langle \pi_i \otimes \pi_i : i = 0, \ldots, n'-1 \rangle$ and is non-zero as otherwise $\Sigma'_{\{1,\ldots,n'-1\}}$ would be multiplicative, while the right-hand side is in $\langle \pi_i \otimes \pi_i : i = n', \ldots, n \rangle$. This proves that the intersection between these two spaces is non-trivial, hence equals $\langle \tau_0 \otimes \tau_0 \rangle$. In particular $\langle \tau_0 \otimes \tau_0 \rangle$ belongs to both spaces, hence it is easy to conclude that both Σ' and Σ'' are multiplicative. □

2.6.2 Threshold Schemes and Shamir's Scheme

DEFINITION 2.6.11. A secret sharing scheme is *threshold* if, for some integer $0 \leq r \leq n$, it has $(r-1)$-privacy and r-reconstruction. In this case we will also say that the scheme is r-threshold.

The most famous example of secret sharing scheme belongs to this family. Let $V := \mathbb{F}[X]_{<k}$ be the space of polynomials of degree less than k, where $k \leq n$ is a fixed positive integer. Pick $n+1$ pairwise distinct elements $\alpha_0, \ldots, \alpha_n \in \mathbb{F}$ and, for all $i = 0, \ldots, n$, define $\pi_i \in V^*$ to be the evaluation map $\pi_i(f) := f(\alpha_i)$ for all $f \in V$. In addition, we may allow one of the α_i's to be equal to ∞, with the convention that, for any $f \in \mathbb{F}[X]_{<k}$, $f(\infty)$ equals the coefficient of X^{k-1} in f, as in section 2.5.1. This defines a secret sharing scheme, called *Shamir's scheme* [67]. Moreover, it is a threshold scheme with $(k-1)$-privacy and k-reconstruction, i.e. a k-threshold scheme.

In order to prove this, identify any polynomial $f = f_0 + f_1 X + \cdots + f_{k-1} X^{k-1} \in V$ with its coefficient list $(f_0, f_1, \ldots, f_{k-1}) \in \mathbb{F}^k$ and, for all $i = 0, \ldots, n$, the linear form π_i with the vector $(1, \alpha_i, \ldots, \alpha_i^{k-1}) \in \mathbb{F}^k$ if $\alpha_i \neq \infty$ or the vector $(0, \ldots, 0, 1) \in \mathbb{F}^k$ otherwise, so that the evaluation $\pi_i(f)$ is simply a vector inner product. Then it is straightforward to see that any k of the π_i's constitute an $\mathbb{F}$-basis of V^*, hence the claims about privacy and reconstruction of the scheme follow.

To share a secret $s \in \mathbb{F}$, we choose uniformly at random a polynomial $f \in \mathbb{F}[X]_{<k}$ such that $f(\alpha_0) = s$, and we define the i-th share to be $f(\alpha_i)$. On the other hand, a reconstruction function $\rho_I \colon \mathbb{F}^k \to \mathbb{F}$ for any subset $I \subseteq \{1, \ldots, n\}$ of size k can be explicitly obtained using Lagrange's Interpolation Theorem 2.5.8. Assume that $I = \{1, \ldots, k\}$ for ease of notation, and that $y_1, \ldots, y_k$ are the corresponding shares. Then $f := \sum_{i=1}^{k} y_i \delta_i \in \mathbb{F}[X]_{<k}$, where the δ_i's are as in Theorem 2.5.8, is the unique polynomial satisfying $f(\alpha_i) = y_i$ for all $i = 1, \ldots, k$, and in particular $s = f(\alpha_0)$ can be recovered.

As to the multiplicativity of this scheme, recall that, for all $i = 0, \ldots, n$, $\pi_i \otimes \pi_i$ is the bilinear form on $\mathbb{F}[X]_{<k}$ defined by

$$\pi_i \otimes \pi_i(f, g) := f(\alpha_i) g(\alpha_i) = (fg)(\alpha_i)$$

for all $f, g \in \mathbb{F}[X]_{<k}$. The matrix associated to $\pi_i \otimes \pi_i$ is

$$\begin{pmatrix} 1 \\ \alpha_i \\ \vdots \\ \alpha_i^{k-1} \end{pmatrix} (1, \alpha_i, \ldots, \alpha_i^{k-1})$$

and any $2k - 1$ such matrices (with distinct α_i's) generate all the others. This can be argued using again Vandermonde's determinants. It follows from Proposition 2.6.6 that, provided that $2k - 1 \leq n$, Shamir's scheme is multiplicative. If in addition $2k - 1 \leq n - (k - 1)$, i.e. $n \geq 3(k - 1) + 1$, then Shamir's scheme is $(k-1)$-strongly multiplicative. In particular this allows us to construct a scheme which attains the bound given in Proposition 2.6.9. We will show in Section 4.3.1 that the converse also holds, i.e. that a secret sharing scheme which attains the bound of Proposition 2.6.9 is necessarily based on a Reed-Solomon code.

2.6.3 Connection between Coding Theory and Secret Sharing

Let $\mathbb{F}$ be a finite field of size q, n a positive integer, and let V be a finite-dimensional $\mathbb{F}$-vector space. In the ambient space $\mathbb{F}^{n+1}$, coordinates are in-

dexed by $\{0, 1, \ldots, n\}$. First observe that we can naturally associate a code to a secret sharing scheme.

DEFINITION 2.6.12. Let $\Sigma = (\pi_0, \ldots, \pi_n) \subseteq V^*$ be a linear secret sharing scheme. The code associated to Σ is the code

$$C(\Sigma) := \{(\pi_0(x), \ldots, \pi_n(x)) : x \in V\} \subseteq \mathbb{F}^{n+1}.$$

This is indeed a linear space by linearity of Σ. It is a code of length $n+1$ and dimension

$$\dim C(\Sigma) = \dim\langle \pi_1, \ldots, \pi_n \rangle.$$

Moreover the properties (i), (ii) required by Definition 2.6.4 are equivalent to $e_0 \notin C(\Sigma)^\perp$ and $e_0 \notin C(\Sigma)$ respectively, where e_0 denotes the 0-th unit vector of $\mathbb{F}^{n+1}$. One can view $C(\Sigma)$ as the set of all $(n+1)$-tuples $(s, x_1, \ldots, x_n)$ where s is a secret and $x_1, \ldots, x_n$ is a valid set of shares for s in the scheme Σ.

The parameters of a secret sharing scheme give an estimate of the dimension of the associated code as follows.

THEOREM 2.6.13. *If the secret sharing scheme Σ has t-privacy and r-reconstruction then the code $C(\Sigma)$ has dimension*

$$t < \dim C(\Sigma) \leq r.$$

PROOF. Let $I \subseteq \mathcal{P}$ be a set of t players. By t-privacy $\pi_0 \notin \langle \pi_i : i \in I \rangle$, while $\pi_0 \in \langle \pi_1, \ldots, \pi_n \rangle$, hence

$$\dim C(\Sigma) = \dim\langle \pi_1, \ldots, \pi_n \rangle > \dim\langle \pi_i : i \in I \rangle \geq t.$$

As to the second inequality, let $I \subseteq \mathcal{P}$ be a set of $r+1$ players, and for simplicity assume $I = \{1, \ldots, r+1\}$. We need to prove that $\pi_1, \ldots, \pi_{r+1}$ are linearly dependent. By r-reconstruction $\pi_0 \in \langle \pi_1, \ldots, \pi_r \rangle$, i.e. there exist $\lambda_1, \ldots, \lambda_r \in \mathbb{F}$ such that

$$\pi_0 = \lambda_1 \pi_1 + \cdots + \lambda_r \pi_r$$

and at least one of the λ_i's is non-zero, so we may assume that $\lambda_1 \neq 0$. Again by r-reconstruction $\pi_0 \in \langle \pi_2, \ldots, \pi_{r+1} \rangle$, i.e. there exist $\mu_2, \ldots, \mu_{r+1} \in \mathbb{F}$ such that

$$\pi_0 = \mu_2 \pi_2 + \cdots + \mu_{r+1} \pi_{r+1}.$$

Subtracting the two identities we obtain

$$0 = \lambda_1 \pi_1 + (\lambda_2 - \mu_2)\pi_2 + \cdots + (\lambda_r - \mu_r)\pi_r - \mu_{r+1}\pi_{r+1},$$

which is a trivial linear combination of $\pi_1, \ldots, \pi_{r+1}$ with a non-zero coefficient, hence these vectors are linearly dependent. □

COROLLARY 2.6.14. *If Σ is r-threshold then $\dim C(\Sigma) = r$ and $C(\Sigma)$ is MDS.*

PROOF. The statement about the dimension is a trivial consequence of the previous theorem. As to the MDS property, it is easy to see that the third property in Lemma 2.5.5 is satisfied. □

Conversely, a code $C \subseteq \mathbb{F}^{n+1}$ of length $n+1$ with $e_0 \notin C^\perp$ and $e_0 \notin C$ can be used to share a secret $s \in \mathbb{F}$ as follows: select $x \in C$ uniformly at random such that its 0-th entry equals s; define the i-th share to be the i-th entry of x. This can be formalized as follows.

DEFINITION 2.6.15. The secret sharing scheme associated to C is the scheme $\Sigma(C) = (\pi_0, \ldots, \pi_n) \subseteq \mathbb{F}^k$, where $k := \dim C$ and the π_i's are the columns of a generator matrix of C.

This construction is due to Massey [50, 51]. First of all, observe that the conditions $e_0 \notin C^\perp$ and $e_0 \notin C$ ensure that the properties required by Definition 2.6.4 are satisfied. Second, this scheme gives the share functionality described above, and this is clearly independent of the choice of the generator matrix of C. So, even though the sequence $(\pi_0, \ldots, \pi_n)$ which defines the scheme depends on this choice, the possible sets of shares corresponding to a given secret do not. In particular, access and adversary structures of the scheme do not depend on this choice.

The following results characterize these families, based on properties of the code and of its dual. As in the previous section, $\mathcal{P} := \{1, \ldots, n\}$ denotes the player set.

LEMMA 2.6.16. *Let $I \subseteq \mathcal{P}$ be non-empty. The following holds.*

1. *I is accepting for $\Sigma(C)$ if and only if there exists $x \in C^\perp$ such that $\operatorname{supp} x \subseteq I \cup \{0\}$.*
2. *I is rejecting for $\Sigma(C)$ if and only if there exists $x \in C$ such that $0 \in \operatorname{supp} x$ and $I \cap \operatorname{supp} x = \emptyset$.*

PROOF. Let $\Sigma(C) = (\pi_0, \ldots, \pi_n)$. I is accepting if and only if

$$\pi_0 = \sum_{i \in I} \lambda_i \pi_i = \sum_{i=1}^{n} \lambda_i \pi_i$$

for some $\lambda_1, \ldots, \lambda_n \in \mathbb{F}$ where $\lambda_i = 0$ if $i \notin I$. The vector $x = (-1, \lambda_1, \ldots, \lambda_n)$ satisfies the required properties, and this proves the first claim.

As to the second claim, observe that $\pi_0 \notin \langle \pi_i : i \in I \rangle$ if and only if there exists $y \in \mathbb{F}^k$ such that $(\pi_0 \,|\, y) \neq 0$ and $(\pi_i \,|\, y) = 0$ for all $i \in I$. This is a basic result

from linear algebra. The codeword yG, where G is the generator matrix of C whose columns are the π_i's, satisfies the required properties, and this proves the second claim. □

THEOREM 2.6.17. *The secret sharing scheme $\Sigma(C)$ has $(n - d_{\min}(C) + 2)$-reconstruction and $(d_{\min}(C^\perp) - 2)$-privacy.*

PROOF. This follows from the previous lemma. Let $I \subseteq \mathcal{P}$ be non-empty.

First assume that $|I| \geq n - d_{\min}(C) + 2$ and, towards a contradiction, that I is rejecting. Then there exists $x \in C$ such that $0 \in \operatorname{supp} x$ and $I \cap \operatorname{supp} x = \emptyset$. The first property implies that $x \neq 0$ and the second that $\operatorname{wt}(x) \leq n+1-|I| \leq n + 1 - n + d_{\min}(C) - 2 = d_{\min}(C) - 1$, which is clearly impossible.

Now assume that $|I| \leq d_{\min}(C^\perp) - 2$ and that I is accepting. Then there exists $x \in C^\perp$ such that $\operatorname{supp} x \subseteq I \cup \{0\}$, i.e. $x \in C^\perp, x \neq 0, \operatorname{wt}(x) \leq |I|+1 \leq d_{\min}(C^\perp) - 2 + 1 = d_{\min}(C^\perp) - 1$, which is another contradiction. □

Finally, we show how the multiplicativity properties of the scheme relate to the product of the original code. Recall that the code $C^2 \subseteq \mathbb{F}^{n+1}$ is defined as the span of all componentwise products xy of codewords $x, y \in C$. Moreover, as shown in Section 2.5.4, it can be obtained as the image of

$$\begin{array}{ccc} \mathbb{F}^k \times \mathbb{F}^k & \longrightarrow & \mathbb{F}^{n+1}. \\ (x, y) & \longmapsto & (\pi_0 \otimes \pi_0(x, y), \ldots, \pi_n \otimes \pi_n(x, y)) \end{array}$$

This shows that the scheme associated to the square of the code C is the product of the scheme $\Sigma(C)$. Then from Theorem 2.6.17 we immediately have the following.

THEOREM 2.6.18. *The secret sharing scheme $\Sigma(C)$ is t-strongly multiplicative, where*

$$t := \min\{d_{\min}(C^\perp) - 2, d_{\min}(C^2) - 2\}.$$

2.6.4 From Secret Sharing to Multiparty Computation

In this section we give a very high level overview of how an arithmetic secret sharing scheme can be used to build a secure multiparty computation protocol.

The purpose of secure multiparty computation is to implement the following functionality: n players want to jointly evaluate a function $f\colon \mathbb{F}^n \to \mathbb{F}$ of their inputs $x_1, \ldots, x_n$ in a way that ensures the correctness of the outcome and protects the privacy of the parties. We assume the existence of an external

adversary who can corrupt a fixed number of players in order to obtain addition information about the other inputs. Here privacy is meant against such an adversary. We now sketch how this is performed in practice and how the properties of the scheme are exploited.

At the beginning of the protocol, each player uses the secret sharing scheme to share his own input with all other players. The privacy property of the scheme hides each input from other players.

Throughout the protocol, the function f is modeled as a sequence of $+$ and $\times$ binary gates, and the arithmetic properties of the scheme are used to guarantee the following: if a player enters the gate $y + z$ ($y \times z$ respectively) with valid shares of y and z, then he exits the gate with a valid share of $y + z$ ($y \times z$ respectively).

At the end of the protocol, each player possesses a valid share of the output $f(x_1, \ldots, x_n)$, which can therefore be reconstructed thanks to the reconstruction property of the scheme.

We give more details on how the protocol proceeds through the gates. For all $i = 1, \ldots, n$, let y_i and z_i denote the i-th share of y and z respectively. As seen in the previous section, $y_i + z_i$ is a valid share of $y + z$, hence at every $+$ gate each player is simply required to sum the shares in his possession. On the other hand, $\times$ gates require more work and actual interaction among the players.

Recall that, as the scheme is multiplicative, there exists a linear product reconstruction function $\rho^* \colon \mathbb{F}^n \to \mathbb{F}$ such that, for any pair of secrets $s, s' \in \mathbb{F}$ with corresponding shares $x_1, \ldots, x_n \in \mathbb{F}$ and $x'_1, \ldots, x'_n \in \mathbb{F}$, we have $\rho^*(x_1 x'_1, \ldots, x_n x'_n) = ss'$. As ρ^* is linear, we can identify it with a list of coefficients $\rho^*_1, \ldots, \rho^*_n \in \mathbb{F}$ such that

$$ss' = \sum_{i=1}^{n} \rho^*_i x_i x'_i$$

for any pair of secrets and list of shares as above. Let us highlight that the reconstruction function, being a property of the scheme, is assumed to be publicly known by all players, and so are the coefficients ρ^*_i's.

For all $i = 1, \ldots, n$, the i-th player processes a $\times$ gate following these instructions:

1. compute $w_i := \rho^*_i y_i z_i$;
2. share w_i and send the j-th share $w_{i,j}$ to the j-th player;
3. compute $t_i := \sum_{j=1}^{n} w_{j,i}$.

It turns out that the t_i's constitute a valid share of $y \times z$. Indeed, we have that the i-th share of

$$yz = \sum_{j=1}^{n} \rho_j^* y_j z_j = \sum_{j=1}^{n} w_j$$

equals $\sum_{j=1}^{n} w_{j,i}$ by linearity. Finally, we point out that step 1 and 3 only require local computation, whereas step 2 requires one round of communication in which each player sends an element of $\mathbb{F}$ to each other player, for a total of n^2 transmitted elements of $\mathbb{F}$.

Chapter 3

Squares of Random Linear Codes

3.1 Overview

As shown in Chapter 1, the motivation for a systematic code-theoretic study of squares is quite strong. With a view to contributing to such an endeavor, our concern in this chapter is with the dimension of squares of random linear codes. Specifically, our purpose is to answer the following question: does the square of a code "typically" fill the whole space? We give a positive answer, for codes of dimension k and length roughly $k^2/2$ or smaller. Moreover, the convergence speed is exponential in the difference $k(k+1)/2 - n$, if this difference is at least linear in k. The proof uses random coding and combinatorial arguments, together with algebraic tools involving the precise computation of the number of quadratic forms of a given rank, and the number of their zeros.

Even though the main results of this chapter involve probability measures, we shall not give any introduction to probability theory, as we are only concerned with discrete probability and uniform distributions, hence essentially combinatorics. That is, given a finite sample space $\mathcal{U}$, an event $\mathcal{E}$ is a subset of $\mathcal{U}$, and its *probability* $\Pr(\mathcal{E})$ is simply defined to be the ratio between the size of the event itself and the size of the sample space. A *random variable* is a function defined over the sample space and with values in a subset of $\mathbb{R}$. The *expectation* of a random variable X is $\mathbb{E}[X] := \sum_{x \in \mathbb{R}} x \Pr(X = x)$. Here $\Pr(X = x)$ is a standard notation for the event corresponding to the preimage of x in the sample space. Observe that in the discrete case this is zero for all but a finite number of $x \in \mathbb{R}$, hence the sum defining the expectation is finite.

Throughout this chapter, $\mathbb{F}$ denotes a finite field of size q, where q is a fixed prime power, and all codes are $\mathbb{F}$-linear. Since a generating set of vectors for the square of a code $C \subseteq \mathbb{F}^n$ of dimension k can be constructed by taking all possible $k(k+1)/2$ products of two elements of a basis of the code C, it is reasonable to expect that a randomly chosen code of length $n < k(k+1)/2$ has a square which fills up the whole space, i.e. $C^2 = \mathbb{F}^n$. However, linear relations between products of elements of C are not typically independent random events, and one has to overcome a certain number of obstacles to prove such a statement. Our main result is indeed to show that when the difference $k(k+1)/2 - n$ goes to infinity as a function of k, however slowly, the probability that a random code of length n and dimension k has a square different from $\mathbb{F}^n$ goes to zero. We also study the speed of convergence, which is exponential in the difference $k(k+1)/2 - n$, if this difference is at least linear in k, and the limiting case $n = k(k+1)/2$. We shall also consider the slightly easier case when the length n is such that $n \geq k(k+1)/2$: we obtain that with probability tending to 1 when $n - k(k+1)/2$ goes to infinity, the dimension of the square of the random code is exactly $k(k+1)/2$. Again, this convergence is exponentially fast if $n - k(k+1)/2$ is at least linear in k. Previously, the best-known fact on this problem was given by Faugère et al. in [34] who proved that for $n \geq k(k+1)/2$ and for any function $\omega(k)$ that goes to infinity with k, the dimension of the square of the random code is at least $k(k+1)/2 - k\omega(k)$ with probability tending to 1 when k goes to infinity. Our techniques break significantly with the approach of [34] and combine the study of the dual distance of the square of a random code, and the distribution of zeros of random quadratic forms. In the rest of this section we describe our results precisely and give an overview of our proofs and the structure of the chapter.

We first define the probabilistic model we shall work with. For all positive integers $n \geq k$, we define $\mathcal{C}(n,k)$ to be the family of all codes of length n and dimension k whose first k coordinates make up an information set: equivalently, members of $\mathcal{C}(n,k)$ have a generator matrix which can be written in systematic form, i.e. as

$$G = \left(\begin{array}{ccc|c} 1 & & & \\ & \ddots & & A \\ & & 1 & \end{array}\right),$$

for some $k \times (n-k)$ matrix A. We endow $\mathcal{C}(n,k)$ with the uniform distribution. Since codes of $\mathcal{C}(n,k)$ are in one-to-one correspondence with $k \times (n-k)$ matrices A, choosing a random element of $\mathcal{C}(n,k)$ amounts to choosing a random uniform matrix A.

Remark 3.1.1. There are several possible choices for the probabilistic model. An alternative way of choosing a random code consists of choosing its generator

matrix uniformly at random among all $k \times n$ matrices. Yet another alternative is to consider the uniform distribution among all codes of length n and dimension k. The first alternative probability distribution has the disadvantage that the resulting code may be of dimension $< k$. The second alternative distribution is perhaps the most theoretically elegant but makes it somewhat cumbersome to use the puncturing arguments that we will work with, hence the above choice of a probabilistic model. In Section 3.5 we shall argue however that our results are not altered significantly under these alternative probability distributions.

Our main result is the following.

MAIN THEOREM 3.1.2. *Let $n\colon \mathbb{N} \to \mathbb{N}$ be such that $k(k+1)/2 \geq n(k) \geq k$ for all $k \in \mathbb{N}$ and define $t\colon \mathbb{N} \to \mathbb{N}, t(k) := k(k+1)/2 - n(k)$. Then there exist constants $\gamma, \delta \in \mathbb{R}_{>0}$ such that, for all large enough k,*

$$\Pr(C^2 = \mathbb{F}^{n(k)}) \geq 1 - 2^{-\gamma k} - 2^{-\delta t(k)},$$

where C is chosen uniformly at random from $\mathcal{C}(n(k), k)$.

For lengths n that are larger than $k(k+1)/2$, we also have:

THEOREM 3.1.3. *Let $n\colon \mathbb{N} \to \mathbb{N}$ be such that $n(k) \geq k(k+1)/2$ for all $k \in \mathbb{N}$ and define $s\colon \mathbb{N} \to \mathbb{N}, s(k) := n(k) - k(k+1)/2$. Then there exists a constant $\hat{\delta} \in \mathbb{R}_{>0}$ such that, for all large enough k,*

$$\Pr\left(\dim C^2 = \frac{k(k+1)}{2}\right) \geq 1 - 2^{-\hat{\delta} s(k)},$$

where C is chosen uniformly at random from $\mathcal{C}(n(k), k)$.

Strangely enough, Theorems 3.1.2 and 3.1.3 are not quite symmetrical. In particular the term $2^{-\gamma k}$ is absent from the statement of Theorem 3.1.3 but can not be avoided in Theorem 3.1.2: this is because with probability at least $1/q^k$, the random matrix G will contain a column of zeros, or two identical columns, in which case the square C^2 can not be equal to $\mathbb{F}^{n(k)}$. The two theorems will not require exactly the same methods and Theorem 3.1.2 will need more work than Theorem 3.1.3. We shall deal with them separately.

Our first step towards establishing Theorem 3.1.2 will be to estimate the expected minimum distance of the dual of the square of a random code of length $k(k+1)/2$. Specifically, we shall prove:

PROPOSITION 3.1.4. *There exist constants (depending only on q) $c, \widetilde{c} \in \mathbb{R}_{>0}$ such that, for all large enough k, if C is chosen uniformly at random from $\mathcal{C}(k(k+1)/2, k)$ then*

$$\Pr\left(d_{\min}((C^2)^{\perp}) \leq c \cdot \frac{k(k+1)}{2}\right) \leq 2^{-\widetilde{c}k}.$$

This last proposition enables us to use puncturing arguments. In our probabilistic model, a random code of length n can be obtained by first choosing a random code of length $n+t$ and then puncturing t times on a random position. The probability that a punctured code has the same dimension as the original code is well-separated from zero whenever the dual distance of the original code is large enough. This fact will be enough in itself to establish the following weaker version of Main Theorem 3.1.2.

THEOREM 3.1.5. *There exist constants (depending only on q) $c, \widetilde{c} \in \mathbb{R}_{>0}$ such that, if $n\colon \mathbb{N} \to \mathbb{N}$ satisfies*

$$k \leq n(k) \leq c \cdot \frac{k(k+1)}{2}$$

for all $k \in \mathbb{N}$ then, for all large enough k,

$$\Pr(C^2 = \mathbb{F}^{n(k)}) \geq 1 - 2^{-\widetilde{c}k},$$

where C is chosen uniformly at random from $\mathcal{C}(n(k), k)$.

However, in order to deal with block lengths that approach the upper bound $k(k+1)/2$ on the dimension of the square of C, and prove the full-fledged Main Theorem 3.1.2, we need some additional ingredients.

Given an code C of length n and dimension k and denoting by $\pi_1, \ldots, \pi_n \in \mathbb{F}^k$ the columns of a generator matrix of C, define the linear map

$$\begin{array}{rccc} \mathrm{ev}_C\colon & \mathrm{Quad}(\mathbb{F}^k) & \to & \mathbb{F}^n, \\ & Q & \mapsto & (Q(\pi_1), \ldots, Q(\pi_n)) \end{array}$$

where $\mathrm{Quad}(\mathbb{F}^k)$ denotes the vector space of quadratic forms on $\mathbb{F}^k$. As observed in Section 2.5.4, the image of ev_C does not depend on the choice of a generator matrix of C, and it is equal to C^2. In particular, $C^2 = \mathbb{F}^n$ if and only if ev_C is surjective. Moreover, by basic linear algebra $C^2 = \mathbb{F}^n$ if and only if

$$\dim \ker \mathrm{ev}_C = \dim \mathrm{Quad}(\mathbb{F}^k) - n = \frac{k(k+1)}{2} - n.$$

So it makes sense to focus on this kernel. We view its cardinality as a random variable, with distribution induced by the uniform distribution of C over $\mathcal{C}(n,k)$: formally, for all positive integers $n \geq k$ we define

$$X(n,k) := |\ker \mathrm{ev}_C|.$$

Our main intermediate result, of interest in its own right, is:

THEOREM 3.1.6. *We have that*

$$\lim_{k\to\infty} \mathbb{E}\left[X\left(\frac{k(k+1)}{2}, k\right)\right] = 2.$$

A simple use of Markov's inequality will then give us that, for a random code C of length $k(k+1)/2$, the probability that the codimension of C^2 does not exceed ℓ,

$$\Pr\left(\dim C^2 \geq \frac{k(k+1)}{2} - \ell\right)$$

tends to 1 when ℓ goes to infinity, furthermore exponentially fast if ℓ is linear in k. Puncturing arguments, again relying on Proposition 3.1.4, will enable us to conclude the proof of Theorem 3.1.2 when the block length n is well separated from $k(k+1)/2$.

As a by-product, Theorem 3.1.6 also enables us to deal easily with the case when $n \geq k(k+1)/2$. Theorem 3.1.3 will follow as a straightforward consequence.

We conclude this overview by giving a rough idea of the proof of Theorem 3.1.6. It involves computing the number of zeros of a quadratic form of given rank and the number of quadratic forms of given rank. The results we need are stated in Section 3.3 and proved in Section 2.4.

By definition, for all positive integers $m \geq k$ we have

$$\begin{aligned}\mathbb{E}[X(m,k)] &= \\ &= \mathbb{E}[|\{Q \in \mathrm{Quad}(\mathbb{F}^k) : Q(\pi_1) = \cdots = Q(\pi_m) = 0\}|],\end{aligned}$$

where we can assume that, for $i = 1, \ldots, k$, $\pi_i = e_i$ is the i-th unit vector while $\pi_{k+1}, \ldots, \pi_m \in \mathbb{F}^k$ have independent, uniform distribution over $\mathbb{F}^k$, by definition of the family $\mathcal{C}(m,k)$ and our probabilistic model.

Note that the conditions $Q(e_1) = \cdots = Q(e_k) = 0$ are independent (in the sense of linear algebra), hence the subspace

$$S := \{Q \in \mathrm{Quad}(\mathbb{F}^k) : Q(e_1) = \cdots = Q(e_k) = 0\}$$

of $\mathrm{Quad}(\mathbb{F}^k)$ has dimension $k(k-1)/2$. Moreover, as $\pi_{k+1}, \ldots, \pi_m \in \mathbb{F}^k$ are independent (in the sense of probability), we have

$$\begin{aligned}\Pr(Q(\pi_{k+1}) = \cdots = Q(\pi_m) = 0) &= \\ &= \Pr(Q(\pi_{k+1}) = 0)^{m-k} = \left(\frac{|Z(Q)|}{q^k}\right)^{m-k}\end{aligned}$$

for any $Q \in \mathrm{Quad}(\mathbb{F}^k)$. Here $Z(Q)$ denotes the zero set of Q and q is the cardinality of $\mathbb{F}$. Finally, by linearity of the expectation we have

$$\begin{aligned}\mathbb{E}[X(m,k)] &= \\ &= \mathbb{E}[|\{Q \in S : Q(\pi_{k+1}) = \cdots = Q(\pi_m) = 0\}|] = \\ &= \sum_{Q \in S} \left(\frac{|Z(Q)|}{q^k}\right)^{m-k}. \qquad (3.1)\end{aligned}$$

Now if it were true (it is not) that all non-zero quadratic forms on $\mathbb{F}^k$ have q^{k-1} zeros, we would have, when we set $m = k(k+1)/2$,

$$\mathbb{E}[X(m,k)] = 1 + \frac{1}{q^{m-k}}(q^{\frac{k(k-1)}{2}} - 1) \longrightarrow 2$$

"proving" Theorem 3.1.6. However, even though it is false that all non-zero quadratic forms on $\mathbb{F}^k$ have q^{k-1} zeros, this still holds "on average": roughly speaking, most quadratic forms have q^{k-1} zeros, quadratic forms whose number of zeros is far from this value are those of small rank, and the number of such forms is so small that it contributes almost nothing to the expectation. In other words, the expectation behaves as if it were true that all non zero quadratic forms on $\mathbb{F}^k$ have q^{k-1} zeros.

The rest of the chapter is organized as follows. Section 3.2 is devoted to proving Proposition 3.1.4 and Theorem 3.1.5. In Section 3.3 we recall some basic definitions and state the results that we need on quadratic forms, namely the number of forms of a given rank, and the number of their zeros. This can be found in Section 2.4 as well, but we prefer to repeat those notions in order to make this section self-contained. In Section 3.4 we use the results of Section 2.4 to derive Theorem 3.1.6. Theorem 3.1.3 is then derived as an almost immediate consequence. We then apply the methods and results of Section 3.2 to conclude the proof of Theorem 3.1.2. Finally, in Section 3.5 we expand Remark 3.1.1, with the purpose of showing that, even though our probabilistic model may appear restrictive, our analysis gives all the ingredients necessary to consider different models.

3.2 Proof of Theorem 3.1.5

In this section we prove Proposition 3.1.4 and Theorem 3.1.5, the weaker version of our main result. We start by introducing some notation and classical results that we shall need.

Recall that, for all non-negative integers $n \geq k$, we define

$$\begin{bmatrix} n \\ k \end{bmatrix}_q := \prod_{i=1}^{k} \frac{q^{n-k+i} - 1}{q^i - 1},$$

the Gaussian binomial coefficient, and by convention we define a product with no factors to be equal to 1. As q is assumed to be fixed, it will be suppressed from the notation from here on.

Remark 3.2.1. For all non-negative integers $n \geq k$, we bound

$$\begin{bmatrix} n \\ k \end{bmatrix} \leq 2^k q^{k(n-k)}.$$

This holds as $\begin{bmatrix} n \\ k \end{bmatrix}$ is the product of k terms, and each term is bounded by $2q^{n-k}$.

DEFINITION 3.2.2 (entropy function). The q-ary entropy function is defined by

$$H_q(x) := x \log_q(q-1) - x \log_q x - (1-x) \log_q(1-x)$$

for all $0 < x \leq 1 - q^{-1}$.

Again, from here on q will be suppressed from the notation. In particular, all logarithms will be in base q. The following lemma is folklore, see e.g. [37, §2.10.3] for a proof.

LEMMA 3.2.3. *For all $0 < \delta \leq 1 - q^{-1}$ and all integers n, we have*

$$\sum_{i=0}^{\lfloor \delta n \rfloor} \binom{n}{i} (q-1)^i \leq q^{nH(\delta)}.$$

For ease of notation, we define $m \colon \mathbb{N} \to \mathbb{N}$ by $m(k) := k(k+1)/2$. Also, recall that, given a code C, we denote by $C^\perp$ its dual and by $d_{\min}(C)$ its minimum distance.

We prove now Proposition 3.1.4.

PROOF OF PROPOSITION 3.1.4. Let $C \in \mathcal{C}(m(k), k)$. By definition, C admits a generator matrix of the form

$$\left(\begin{array}{ccc|c} 1 & & & g_1 \\ & \ddots & & \vdots \\ & & 1 & g_k \end{array}\right).$$

Note that a uniform random selection of C from $\mathcal{C}(m(k), k)$ induces an independent, uniform random selection of $g_1, \ldots, g_k$ from $\mathbb{F}^{m(k)-k}$. We consider the code

$$\langle g_i g_j : 1 \leq i \leq k/2 < j \leq k \rangle$$

and we define D to be its dual. This is a code of length $k(k-1)/2$ and it is easy to see that

$$d_{\min}((C^2)^\perp) \geq d_{\min}(D).$$

In the following, when D is involved in some probability measure, we implicitly mean that it has the distribution induced by the uniform distribution of C on $\mathcal{C}(m(k), k)$. We remark that this does not necessarily correspond to a uniform distribution on the set of all possible D's.

For any positive integer w and any code C', denote by $\mathcal{E}_w(C')$ the event "there exists a non-zero codeword of C' of weight w". We shall now prove the following statement, which clearly implies the Proposition. There exist constants $c, \widetilde{c} \in \mathbb{R}_{>0}$ such that, for all large enough k,

$$\sum_{w=1}^{cm(k)} \Pr(\mathcal{E}_w(D)) \leq 2^{-\widetilde{c}k}.$$

Note that, for any positive integer w,

$$\Pr(\mathcal{E}_w(D)) = \sum_{\substack{z \in \mathbb{F}^{k(k-1)/2} \\ \text{of weight } w}} \Pr(z \in D). \tag{3.2}$$

So we need to estimate, for all positive integers w and all vectors z of weight w, the probability that z belongs to D.

We do that as follows. For $1 \leq i \leq k/2$, let x_i be the projection of g_i on the support of z. Similarly, for $k/2 < j \leq k$, let y_j be the projection of g_j on the support of z. This defines k vectors in $\mathbb{F}^w$. Moreover, a uniform random selection of C from $\mathcal{C}(m(k), k)$ induces an independent, uniform random selection of the x_i's and the y_j's from $\mathbb{F}^w$. Note now that if we identify z with a vector of $\mathbb{F}^w$, we can define the non-degenerate bilinear form that to any two vectors a, b of $\mathbb{F}^w$ associates the quantity

$$(a|b)_z := (\mathbf{1} \,|\, zab)$$

where $\mathbf{1}$ denotes the all-one vector of $\mathbb{F}^w$ and $(\cdot \,|\, \cdot)$ denotes the standard inner product. Let us say that a and b are *z-orthogonal* if $(a|b)_z = 0$. The purpose of this definition is to note that $z \in D$ if and only if, for all $1 \leq i \leq k/2 < j \leq k$, x_i is z-orthogonal to y_j. In the computation that follows we assume that k is even, thus avoiding cumbersome floor and ceiling notation, and giving us the same number of x_i's and of y_j's, namely $k/2$. It is readily seen that the case k odd can be dealt with in a similar fashion.

For all positive integers $r < k/2$, denote by $\mathcal{H}_r$ the event "$\dim\langle x_i : 1 \leq i \leq k/2\rangle < r$". Conditioning by this event, we have

$$\begin{aligned} \Pr(z \in D) &= \Pr(\mathcal{H}_r) \Pr(z \in D | \mathcal{H}_r) + \\ &\quad + \Pr(\overline{\mathcal{H}}_r) \Pr(z \in D | \overline{\mathcal{H}}_r) \leq \\ &\leq \Pr(\mathcal{H}_r) + \Pr(z \in D | \overline{\mathcal{H}}_r), \end{aligned}$$

for any choice of r. In order to estimate $\Pr(\mathcal{H}_r)$, note that $\dim\langle x_i : 1 \leq i \leq k/2\rangle < r$ if and only if there exists an $(r-1)$-dimensional subspace of $\mathbb{F}^w$ containing all x_i's. The probability that an x_i falls into a given subspace of dimension $r-1$ is $1/q^{w-r+1}$ and since the x_i's are independent random variables,

the probability that all the x_i's fall into the same subspace is $1/q^{(w-r+1)k/2}$. We have therefore,

$$\Pr(\mathcal{H}_r) \leq \begin{bmatrix} w \\ r-1 \end{bmatrix} \frac{1}{q^{\frac{k}{2}(w-r+1)}} \leq \frac{2^r}{q^{(w-r)(k/2-r)}},$$

where we have used the upper bound of Remark 3.2.1 on the number $\begin{bmatrix} w \\ r-1 \end{bmatrix}$ of subspaces of dimension $r-1$.

On the other hand, $z \in D$ if and only if all y_j's are z-orthogonal to the space $\langle x_i : 1 \leq i \leq k/2 \rangle$, which has dimension at least r, under the condition $\overline{\mathcal{H}}_r$. Therefore, using the independence of the random variables y_i,

$$\Pr(z \in D | \overline{\mathcal{H}}_r) \leq \left(\frac{1}{q^r}\right)^{\frac{k}{2}} = \frac{1}{q^{\frac{rk}{2}}}.$$

Now fixing $r := \min\{w/2, k/4\}$ it follows that there exist two positive constants c' and c'' such that

$$\Pr(z \in D) \leq \frac{1}{q^{c'kw}} + \frac{1}{q^{c''k^2}}.$$

Applying this last upper bound to (3.2), we now have

$$\begin{aligned} \Pr(\mathcal{E}_w(D)) &= \sum_{\substack{z \in \mathbb{F}^{k(k-1)/2} \\ \text{of weight } w}} \Pr(z \in D) \leq \\ &\leq \binom{\frac{k(k-1)}{2}}{w} (q-1)^w \left(\frac{1}{q^{c'kw}} + \frac{1}{q^{c''k^2}}\right) \end{aligned}$$

for any positive integer w. Therefore, for any constant c we have

$$\begin{aligned} \sum_{w=1}^{cm(k)} \Pr(\mathcal{E}_w(D)) \leq &\left(\sum_{w=1}^{cm(k)} \binom{\frac{k(k-1)}{2}}{w} \frac{(q-1)^w}{q^{c'kw}} \right) + \\ &+ \frac{1}{q^{c''k^2}} \sum_{w=1}^{cm(k)} \binom{\frac{k(k-1)}{2}}{w} (q-1)^w. \end{aligned} \tag{3.3}$$

We deal with the two terms separately.

We bound the first sum in (3.3) as follows,

$$\begin{aligned} \sum_{w=1}^{cm(k)} \binom{\frac{k(k-1)}{2}}{w} \frac{(q-1)^w}{q^{c'kw}} &\leq \sum_{w=1}^{cm(k)} \left(\frac{k(k-1)}{2}\right)^w \frac{(q-1)^w}{q^{c'kw}} \leq \\ &\leq \sum_{w=1}^{cm(k)} q^{w(-c'k+o(k))} \leq q^{-c'k+o(k)} \end{aligned}$$

since there are not more than $m(k) = q^{o(k)}$ terms in the sum and none is larger than $q^{-c'k+o(k)}$.

Writing $\binom{\frac{k(k-1)}{2}}{w} \leq \binom{m(k)}{w}$ for any $w \leq cm(k)$, the second term in (3.3) is upper bounded by

$$\frac{1}{q^{c''k^2}} \sum_{w=1}^{cm(k)} \binom{m(k)}{w} (q-1)^w.$$

We now set $c \leq 1 - q^{-1}$ and apply Lemma 3.2.3:

$$\frac{1}{q^{c''k^2}} \sum_{w=1}^{cm(k)} \binom{m(k)}{w} (q-1)^w \leq \frac{1}{q^{c''k^2}} q^{m(k)H(c)} \leq$$
$$\leq q^{(\frac{1}{2}H(c)-c'')k^2+o(k^2)}.$$

If c is such that $H(c) < 2c''$ we obtain an exponentially small upper bound. Putting everything together, we obtain

$$\sum_{w=1}^{cm(k)} \Pr(\mathcal{E}_w(D)) \leq \frac{1}{q^{c'k+o(k)}} + \frac{1}{q^{\frac{1}{2}(c''-H(c)/2)k^2+o(k^2)}}$$

and the proposition is proved. □

Remark 3.2.4. In the proof of the previous proposition we can take $c'' = \frac{1}{8}$. Therefore the proposition holds for any c with $H(c) < 1/4$. For example, for $q = 2$, $c = 0.041$ suffices.

We can now prove Theorem 3.1.5.

Proof of Theorem 3.1.5. Let $c, \widetilde{c}$ be the constants given by Proposition 3.1.4. Let $n\colon \mathbb{N} \to \mathbb{N}$ be as in the hypothesis of the theorem. Given $C \in \mathcal{C}(n(k), k)$, we create $V \in \mathcal{C}(m(k), k)$ by adding $m(k) - n(k)$ columns to the systematic generator matrix of C. Moreover, if C and all the new columns are chosen uniformly at random from $\mathcal{C}(n(k), k)$ and $\mathbb{F}^k$ respectively then V has the uniform distribution on $\mathcal{C}(m(k), k)$. A codeword in the dual of C^2 gives a codeword in the dual of V^2 of the same weight (padding with zeros). Hence

$$\Pr\left(C^2 \neq \mathbb{F}^{n(k)}\right) \leq \Pr\left(d_{\min}((V^2)^{\perp}) \leq cm(k)\right) \leq 2^{-\widetilde{c}k}$$

by Proposition 3.1.4 and the conclusion follows. □

3.3 Quadratic Forms

In this section we state the results that we need in the proof of our Main Theorem, as well as the definitions necessary to read such results. For a more involved discussion, see Section 2.4, where we include full proofs of the results stated here as well. Even though these can be found, at least partly, in the literature, we have felt it necessary to derive what we need in a unified way.

Throughout this section, let $\mathbb{K}$ be an arbitrary field and let V be a finite dimensional $\mathbb{K}$-vector space.

DEFINITION 3.3.1. A *quadratic form* on V is a map $Q\colon V \to \mathbb{K}$ such that

(i) $Q(\lambda x) = \lambda^2 Q(x)$ for all $x \in V, \lambda \in \mathbb{K}$,
(ii) the map $(x, y) \mapsto Q(x + y) - Q(x) - Q(y)$ is a bilinear form on V.

We denote by $\mathrm{Quad}(V)$ the $\mathbb{K}$-vector space of all quadratic forms on V. The vector space V, endowed with a quadratic form Q on V, is called a $\mathbb{K}$-*quadratic space*.

Every quadratic form $Q \in \mathrm{Quad}(V)$ defines a bilinear form $\tilde{B}_Q \in \mathrm{Bil}(V)$ by

$$\tilde{B}_Q(x, y) := Q(x + y) - Q(x) - Q(y)$$

for all $x, y \in V$.

DEFINITION 3.3.2. The *radical* of the quadratic space V is the $\mathbb{K}$-vector space

$$\operatorname{Rad} V := \{x \in V : \tilde{B}_Q(x, y) = 0 \text{ for all } y \in V\}.$$

We say that V is *non-degenerate* (as a quadratic space) if $\tilde{B}_Q$ is non-degenerate (as a bilinear form), i.e. if $\operatorname{Rad} V = 0$.

DEFINITION 3.3.3. Let $\operatorname{Rad}^0 V := \{x \in \operatorname{Rad} V : Q(x) = 0\}$. We define the *rank* of Q to be

$$\operatorname{rk} Q := \dim V - \dim \operatorname{Rad}^0 V.$$

REMARK 3.3.4. Note that in the case $\operatorname{char} \mathbb{K} \neq 2$, it holds that $Q(x) = \frac{1}{2}\tilde{B}_Q(x, x)$ and therefore $\operatorname{Rad}^0 V = \operatorname{Rad} V$. Hence in this case (V, Q) is non-degenerate if and only if Q has full rank. This is not the case if $\operatorname{char} \mathbb{K} = 2$.

We are now ready to state the results we need. Theorem 3.3.5 counts the number of zeros of a given quadratic form. Theorem 3.3.6 counts the number of quadratic forms of a given rank.

THEOREM 3.3.5. *Let V be an $\mathbb{F}$-vector space of dimension k, Q a quadratic form on V of rank r. The number of vectors $x \in V$ such that $Q(x) = 0$ is*

a. q^{k-1} if r is odd,

b. either $q^{k-1} - (q-1)q^{k-\frac{r}{2}-1}$ or $q^{k-1} + (q-1)q^{k-\frac{r}{2}-1}$ if r is even.

THEOREM 3.3.6. *For all non-negative integers k, the number $N(k)$ of full-rank quadratic forms on an $\mathbb{F}$-vector space of dimension k is*

$$N(k) = q^{\lfloor \frac{k}{2} \rfloor (\lfloor \frac{k}{2} \rfloor + 1)} \prod_{i=1}^{\lceil \frac{k}{2} \rceil} (q^{2i-1} - 1) =$$

$$= \begin{cases} q^{\frac{k-1}{2}\frac{k+1}{2}} \prod_{i=1}^{\frac{k+1}{2}} (q^{2i-1} - 1) & \text{if } k \text{ is odd,} \\ q^{\frac{k}{2}(\frac{k}{2}+1)} \prod_{i=1}^{\frac{k}{2}} (q^{2i-1} - 1) & \text{if } k \text{ is even.} \end{cases}$$

For all non-negative integers $k \geq r$, the number of rank r quadratic forms on an $\mathbb{F}$-vector space of dimension k is

$$N(k, r) = \begin{bmatrix} k \\ r \end{bmatrix} N(r),$$

where $\begin{bmatrix} k \\ r \end{bmatrix}$ denotes the q-ary Gaussian binomial coefficient.

A more general result implying Theorem 3.3.5 appears in [47, Chapter 6, Section 2].

As to Theorem 3.3.6, the following references need to be mentioned. In [10, Lemma 9.5.9] the number of symmetric bilinear forms of given rank is computed. In the odd characteristic case, as symmetric bilinear forms correspond to quadratic forms and the two notions of rank coincide, this result is equivalent to Theorem 3.3.6. As to the arbitrary characteristic case, [10] refers to [33]. The latter uses the language of association schemes and gives a result that allows to compute (even though this is not explicitly stated) the number $N'(k, s)$ of quadratic forms of rank $r \in \{2s-1, 2s\}$ on an $\mathbb{F}$-vector space of dimension k. This result is slightly weaker than our theorem, as it allows to compute the sum $N(k, 2s-1) + N(k, 2s)$ instead of $N(k, 2s-1)$ and $N(k, 2s)$ separately, but it would be sufficient for the main purpose of this work.

3.4 Proof of Main Theorem 3.1.2

We recall the notation introduced in Section 3.1. Given a code C of length n and dimension k and denoting by $\pi_1, \ldots, \pi_n \in \mathbb{F}^k$ the *columns* of a generator

matrix of C (i.e. a matrix whose *rows* form a basis of C), we define the linear map

$$\begin{array}{rccc} \mathrm{ev}_C\colon & \mathrm{Quad}(\mathbb{F}^k) & \to & \mathbb{F}^n, \\ & Q & \mapsto & (Q(\pi_1),\dots,Q(\pi_n)) \end{array}$$

whose image is C^2.

Recall that we have defined the random variable $X(n,k) := |\ker \mathrm{ev}_C|$, with distribution induced by a uniform random selection of C from $\mathcal{C}(n,k)$. For simplicity, we will write X_k as a shorthand for $X(k(k+1)/2,k)$.

It is convenient to measure "how far" C^2 is from being the full space by defining, for all positive integers $n \geq k$ and all non-negative integers ℓ, the probabilities:

$$p_\ell(n,k) := \Pr(\mathrm{codim}\, C^2 \leq \ell),$$

where C is chosen uniformly at random from $\mathcal{C}(n,k)$. Using this notation, Main Theorem 3.1.2 claims that there exists $\delta \in \mathbb{R}_{>0}$ such that, for all large enough k, $p_0(n(k),k) \geq 1 - 2^{-\delta t(k)}$.

As mentioned before, crucial to the proof of Main Theorem 3.1.2 is to estimate the expected value of $X_k = X(k(k+1)/2,k)$: this is precisely the purpose of Theorem 3.1.6, that states that $\lim_{k\to\infty} \mathbb{E}[X_k] = 2$. We now proceed to its proof.

Proof of Theorem 3.1.6. In Section 3.1 we defined the space S of all quadratic forms vanishing at all unit vectors and we proved that, for all positive integers $m \geq k$,

$$\mathbb{E}[X(m,k)] = \sum_{Q\in S} \left(\frac{|Z(Q)|}{q^k}\right)^{m-k}. \tag{3.1}$$

We now fix a rank threshold, i.e. a fraction of k, and we classify the forms in S accordingly. Precisely, for any $0 < \alpha < 1$ we define

$$\begin{aligned} S^-(\alpha) &:= \{Q \in S : 0 < \mathrm{rk}\, Q \leq \alpha k\}, \\ S^+(\alpha) &:= \{Q \in S : \mathrm{rk}\, Q > \alpha k\}, \end{aligned}$$

so $S = \{0\} \cup S^+(\alpha) \cup S^-(\alpha)$. We observe that

$$|S^-(\alpha)| \leq q^{(-\frac{\alpha^2}{2}+\alpha)k^2+o(k^2)}. \tag{3.4}$$

Indeed, by Theorem 3.3.6 we have

$$|S^-(\alpha)| = \sum_{r=1}^{\alpha k} N(k,r) = \sum_{r=1}^{\alpha k} \begin{bmatrix} k \\ r \end{bmatrix} N(r).$$

We loosely bound $\begin{bmatrix} k \\ r \end{bmatrix} \leq q^{r(k-r+1)}$ and $N(r) \leq |\operatorname{Quad}(\mathbb{F}^r)| = q^{r(r+1)/2}$ and we obtain

$$|S^-(\alpha)| \leq \sum_{r=1}^{\alpha k} q^{r(k-r+1)} q^{r(r+1)/2} = \sum_{r=1}^{\alpha k} q^{-\frac{r^2}{2}+(k+\frac{3}{2})r} \leq$$
$$\leq \alpha k q^{(-\frac{\alpha^2}{2}+\alpha)k^2+\frac{3}{2}\alpha k},$$

proving (3.4). This yields

$$\frac{|S^-(\alpha)|}{|S|} \leq \frac{q^{(-\frac{\alpha^2}{2}+\alpha)k^2+o(k^2)}}{q^{\frac{k(k-1)}{2}}} = q^{-\frac{1}{2}(\alpha-1)^2k^2+o(k^2)}$$

which tends to 0 as $k \to \infty$. Hence, noting that $|S^+(\alpha)| = |S| - 1 - |S^-(\alpha)|$, we obtain

$$\lim_{k\to\infty} \frac{|S^+(\alpha)|}{|S|} = 1. \tag{3.5}$$

In view to using the observations (3.4) and (3.5) on the "density" of $S^+(\alpha)$ and $S^-(\alpha)$ in S, we apply the partition of S to (3.1) and write

$$\mathbb{E}[X(m,k)] =$$
$$= 1 + \sum_{Q\in S^+(\alpha)} \left(\frac{|Z(Q)|}{q^k}\right)^{m-k} + \sum_{Q\in S^-(\alpha)} \left(\frac{|Z(Q)|}{q^k}\right)^{m-k}. \tag{3.6}$$

We now prove that the first sum tends to 1 while the second one (for some suitable value of α) tends to 0.

By Theorem 3.3.5, the number of zeros of any form $Q \in S^+(\alpha)$ is bounded by

$$|Z(Q)| \leq q^{k-1} + (q-1)q^{k-\frac{\alpha k}{2}-1} \leq q^{k-1}\left(1 + \frac{1}{q^{\frac{\alpha k}{2}-1}}\right)$$

and

$$|Z(Q)| \geq q^{k-1} - (q-1)q^{k-\frac{\alpha k}{2}-1} \geq q^{k-1}\left(1 - \frac{1}{q^{\frac{\alpha k}{2}-1}}\right).$$

It follows that

$$\frac{1}{q}\left(1 - \frac{1}{q^{\frac{\alpha k}{2}-1}}\right) \leq \frac{|Z(Q)|}{q^k} \leq \frac{1}{q}\left(1 + \frac{1}{q^{\frac{\alpha k}{2}-1}}\right)$$

hence

$$\left(1 - \frac{1}{q^{\frac{\alpha k}{2}-1}}\right)^{m-k} \frac{|S^+(\alpha)|}{q^{m-k}} \leq \sum_{Q\in S^+(\alpha)} \left(\frac{|Z(Q)|}{q^k}\right)^{m-k} \leq$$
$$\leq \left(1 + \frac{1}{q^{\frac{\alpha k}{2}-1}}\right)^{m-k} \frac{|S^+(\alpha)|}{q^{m-k}}.$$

Setting $m = k(k+1)/2$, we get

$$\left(1 - \frac{1}{q^{\frac{\alpha k}{2}-1}}\right)^{\frac{k(k-1)}{2}} \frac{|S^+(\alpha)|}{|S|} \leq \sum_{Q \in S^+(\alpha)} \left(\frac{|Z(Q)|}{q^k}\right)^{\frac{k(k-1)}{2}} \leq$$
$$\leq \left(1 + \frac{1}{q^{\frac{\alpha k}{2}-1}}\right)^{\frac{k(k-1)}{2}} \frac{|S^+(\alpha)|}{|S|}.$$

So the first sum in (3.6) is bounded, from above and from below, by functions which tend to 1 (by (3.5)), hence it tends to 1, too.

We now prove that if we take any $0 < \alpha < 1 - \sqrt{\log_q(2q-1) - 1}$, the last sum in (3.6) tends to 0, which will conclude the proof of the theorem.

By Theorem 3.3.5, all forms $Q \in S^-(\alpha)$ satisfy

$$|Z(Q)| \leq q^{k-1} + (q-1)q^{k-2} = 2q^{k-1} - q^{k-2}.$$

This is trivial for odd rank forms, as they always have exactly q^{k-1} zeros. We get

$$\sum_{Q \in S^-(\alpha)} \left(\frac{|Z(Q)|}{q^k}\right)^{m-k} \leq \left(\frac{2q-1}{q^2}\right)^{m-k} |S^-(\alpha)|.$$

Setting $m = k(k+1)/2$ and using (3.4) we finally obtain

$$\sum_{Q \in S^-(\alpha)} \left(\frac{|Z(Q)|}{q^k}\right)^{m-k} \leq$$
$$\leq \left(\frac{2q-1}{q^2}\right)^{\frac{k(k-1)}{2}} q^{(-\frac{\alpha^2}{2}+\alpha)k^2 + o(k^2)} = q^{\mu(\alpha)k^2 + o(k^2)},$$

where $\mu(\alpha) := -\frac{1}{2}(\alpha^2 - 2\alpha + 2 - \log_q(2q-1)) < 0$ under the assumptions on α. Therefore the right hand side tends to 0. This concludes the proof. □

As a first consequence of Theorem 3.1.6, we derive a proof of Theorem 3.1.3.

Proof of Theorem 3.1.3. As before, set $m(k) := k(k+1)/2$. Given a code $C \in \mathcal{C}(n(k), k)$, we obtain a code $C' \in \mathcal{C}(m(k), k)$ puncturing the last $s(k)$ coordinates of C. We define $\mathcal{N}$ to be the event "$\dim C^2 = m(k)$" and, for all $j \in \mathbb{N}$, we define $\mathcal{E}_j$ to be the event "$|\ker \mathrm{ev}_{C'}| = j$". We observe that $\dim C^2 = m(k)$ if and only if $\ker \mathrm{ev}_C = 0$, and this holds if and only if for all nonzero $Q \in \ker \mathrm{ev}_{C'}$ there exists $i \in \{m(k)+1, \ldots, n(k)\}$ such that $Q(\pi_i) \neq 0$.

Hence, if in the case of $\mathcal{E}_j$ we write $\ker \mathrm{ev}_{C'} \setminus \{0\} = \{Q_1, \dots, Q_{j-1}\}$, we have

$$\begin{aligned}
&\Pr(\overline{\mathcal{N}}|\mathcal{E}_j) = \\
&\quad = \Pr\left(\bigcup_{i=1}^{j-1} \left\{Q_i(\pi_{m(k)+1}) = \cdots = Q_i(\pi_{n(k)}) = 0\right\}\right) \leq \\
&\quad \leq \sum_{i=1}^{j-1} \Pr(Q_i(\pi) = 0)^{s(k)},
\end{aligned}$$

for all $j \in \mathbb{N}$, where $\pi \in \mathbb{F}^k$ is chosen uniformly at random. Moreover, for any nonzero quadratic form $Q \in \mathrm{Quad}(\mathbb{F}^k)$,

$$\Pr(Q(\pi) = 0) \leq \frac{q^{k-1} + (q-1)q^{k-2}}{q^k} = \frac{2q-1}{q^2}.$$

Note that $(2q-1)/q^2$ is a constant strictly smaller than 1. It follows that

$$\Pr(\overline{\mathcal{N}}|\mathcal{E}_j) \leq \sum_{i=1}^{j-1} \left(\frac{2q-1}{q^2}\right)^{s(k)} = (j-1)\left(\frac{2q-1}{q^2}\right)^{s(k)}.$$

Applying the law of total probability to $\Pr(\overline{\mathcal{N}})$ together with the above observations we finally have

$$\begin{aligned}
\Pr(\overline{\mathcal{N}}) &= \sum_{j \in \mathbb{N}} \Pr(\mathcal{E}_j) \Pr(\overline{\mathcal{N}}|\mathcal{E}_j) \leq \\
&\leq \left(\frac{2q-1}{q^2}\right)^{s(k)} \sum_{j \in \mathbb{N}} \Pr(\mathcal{E}_j)(j-1) = \\
&= \left(\frac{2q-1}{q^2}\right)^{s(k)} (\mathbb{E}[X_k] - 1).
\end{aligned}$$

The conclusion follows by Theorem 3.1.6. □

Next, we derive from the estimation of the expectation of X_k given by Theorem 3.1.6, a lower bound for the probability of X_k being smaller than some fixed constant. Precisely, the following holds.

PROPOSITION 3.4.1. *For any $\varepsilon > 0$ there exists $k_\varepsilon \in \mathbb{N}$ such that, for all $k \geq k_\varepsilon$, for every non-negative integer ℓ we have*

$$\Pr\left(\dim C^2 \geq \frac{k(k+1)}{2} - \ell\right) \geq 1 - \frac{2+\varepsilon}{q^{\ell+1}},$$

where C is chosen uniformly at random from $\mathcal{C}(k(k+1)/2, k)$.

PROOF. We apply Markov's inequality to the random variable X_k, namely:

$$\Pr(X_k < \delta) \geq 1 - \frac{\mathbb{E}[X_k]}{\delta} \tag{3.7}$$

for any $\delta > 0$. By Theorem 3.1.6 there exists $k_\varepsilon \in \mathbb{N}$ such that, for all $k \geq k_\varepsilon$, we have $\mathbb{E}[X_k] \leq 2 + \varepsilon$, hence for any $\delta > 0$, (3.7) gives

$$\Pr(X_k < \delta) \geq 1 - \frac{2 + \varepsilon}{\delta}$$

if $k \geq k_\varepsilon$. Now setting $\delta = q^{\ell+1}$ and noting that $\Pr(X_k < q^{\ell+1}) = \Pr(\dim C^2 \geq k(k+1)/2 - \ell)$ we conclude. □

Proposition 3.4.1 together with Proposition 3.1.4 allow us to conclude the proof of Main Theorem 3.1.2.

PROOF OF MAIN THEOREM 3.1.2.

Let $k \leq n < m := k(k+1)/2$ be positive integers, and let $t := m - n$. We use a puncturing argument. The key observation is that a random code of length n can be obtained by first choosing a random code of length m and then deleting $m - n$ random coordinates. We shall look closely at the probability that non-zero words survive in the dual of the punctured code.

Precisely, consider a uniform random code $C \in \mathcal{C}(m, k)$: let $C' \in \mathcal{C}(n, k)$ be obtained from C by removing t random coordinates among the last $m-k$. Let these t coordinates be chosen uniformly, independently of C.

In order to estimate $p_0(n, k)$, we define the following events. Call $\mathcal{E}$ the event studied in Proposition 3.1.4, namely $d_{\min}((C^2)^\perp) \leq cm$ where c is the constant of Proposition 3.1.4. For all non-negative integers i, call $\mathcal{E}_i$ the event $\operatorname{codim} C^2 = i$. As before, bar denotes the complement event.

For any positive integer ℓ we have

$$p_0(n, k) \geq \sum_{i=1}^{\ell} \Pr(\overline{\mathcal{E}} \cap \mathcal{E}_i) \Pr(\operatorname{codim}(C')^2 = 0 | \overline{\mathcal{E}} \cap \mathcal{E}_i). \tag{3.8}$$

Let C_0 be a fixed code of length m and suppose x is a codeword of $C_0^\perp$ of weight w. Puncture C_0 by removing t random coordinates among the last $m - k$. The probability that none of the random t coordinates belong to the support of x is at most

$$\frac{\binom{m-w}{t}}{\binom{m-k}{t}} \tag{3.9}$$

(and actually equal to (3.9) if the support of x contains the first k coordinates). If the dual code $C_0^\perp$ contains exactly $q^i - 1$ non-zero codewords all of which

have weight at least cm, then the probability that the t random coordinates miss the support of at least one codeword of $C_0^\perp$ is, by (3.9) and the union bound, bounded from above by

$$(q^i - 1)\frac{\binom{m-cm}{t}}{\binom{m-k}{t}}.$$

Now observing that a non-zero codeword in $((C')^2)^\perp$ exists only if there exists a non-zero codeword in $(C^2)^\perp$ with support disjoint from the chosen t coordinates, we obtain that, for all $i = 1, \ldots, \ell$,

$$\begin{aligned}\Pr(\operatorname{codim}(C')^2 \neq 0 | \overline{\mathcal{E}} \cap \mathcal{E}_i) &\leq (q^i - 1)\frac{\binom{m-cm}{t}}{\binom{m-k}{t}} \leq \\ &\leq q^\ell \, \frac{\binom{m-cm}{t}}{\binom{m-k}{t}}.\end{aligned}$$

We bound the fraction as follows:

$$\begin{aligned}\frac{\binom{m-cm}{t}}{\binom{m-k}{t}} &= \frac{(m-cm)\cdots(m-cm-t+1)}{(m-k)\cdots(m-k-t+1)} \leq \\ &\leq \left(\frac{m-cm}{m-k}\right)^t = (1-c)^t\left(\frac{k+1}{k-1}\right)^t\end{aligned}$$

from which we obtain

$$\Pr(\operatorname{codim}(C')^2 \neq 0 | \overline{\mathcal{E}} \cap \mathcal{E}_i) \leq q^{\ell + t(\log(1-c) + \log\frac{k+1}{k-1})}.$$

Since $\log\frac{k+1}{k-1}$ goes to zero when k goes to infinity and $\log(1-c)$ is negative, by fixing $\ell = \alpha t$ we get the existence of a positive β such that, for any k large enough,

$$\Pr(\operatorname{codim}(C')^2 \neq 0 | \overline{\mathcal{E}} \cap \mathcal{E}_i) \leq q^{-\beta t}. \tag{3.10}$$

Now note that by the union bound

$$\begin{aligned}\Pr(\overline{\mathcal{E}} \cap \mathcal{E}_i) &= 1 - \Pr(\mathcal{E} \cup \overline{\mathcal{E}}_i) \geq 1 - \Pr(\mathcal{E}) - \Pr(\overline{\mathcal{E}}_i) = \\ &= \Pr(\mathcal{E}_i) - \Pr(\mathcal{E}).\end{aligned}$$

Therefore, (3.10) with (3.8) give

$$\begin{aligned}p_0(n,k) &\geq (1 - q^{-\beta t})\sum_{i=1}^{\ell}(\Pr(\mathcal{E}_i) - \Pr(\mathcal{E})) \\ &\geq (1 - q^{-\beta t})(1 - \Pr(\dim C^2 \leq m - \ell) - \ell \Pr(\mathcal{E})).\end{aligned} \tag{3.11}$$

Proposition 3.4.1 gives us, since $\ell = \alpha t$, that $\Pr(\dim C^2 \leq m - \ell) \leq 2^{\beta' t}$ for a constant β'. Proposition 3.1.4 gives us, since $\ell \leq k^2$, that $\ell \Pr(\mathcal{E}) \leq 2^{-\gamma k}$ for some constant γ. From (3.11) we therefore get

$$p_0(n,k) \geq 1 - 2^{-\gamma k} - 2^{-\delta t}.$$

for constants γ and δ. □

3.5 Changing the Probabilistic Model

In this section we expand Remark 3.1.1, with the purpose of showing that, even though our probabilistic model may appear restrictive, our analysis gives all the ingredients necessary to consider different models.

For all positive integers $n \geq k$ we define the following two families of codes. Let $\mathcal{A}(n,k)$ be the family of all codes of length n and dimension at most k with the following distribution: choose a $k \times n$ matrix A uniformly at random and pick the code spanned by the rows of A. Let $\mathcal{U}(n,k)$ be the family of all codes of length n and dimension k, with uniform distribution. Note that it is equivalent to a uniform random choice of a $k \times n$ full-rank matrix, as each such a code has the same number of bases, hence the same number of generator matrices.

We first argue that all our results hold if we replace $\mathcal{C}(n,k)$ with $\mathcal{A}(n,k)$. The two probability distributions are subtly different and it is not easy to derive results for $\mathcal{A}(n,k)$ from the results for $\mathcal{C}(n,k)$ seen as "black boxes". However, if we go over the proofs of our theorems, we see that they will carry over to $\mathcal{A}(n,k)$ with no significant change of strategy. Specifically, in the proof of Theorem 3.1.6, one will replace the study of the quantity $\sum_{Q \in S} \left(\frac{|Z(Q)|}{q^k}\right)^{m-k}$ in (3.1) by

$$\sum_{Q} \left(\frac{|Z(Q)|}{q^k}\right)^{m}$$

where Q ranges over all quadratic forms on k variables. The quantity to be studied is simply the expected number of quadratic forms that vanish on m random values. Going over the proof one will end up with exactly the same expected value. We sum over a space with q^k more quadratic forms but replace probabilities of the form $(|Z(Q)|/q^k)^{m-k}$ by $(|Z(Q)|/q^k)^m$ which behaves like $1/q^k$ times less. Regarding the probabilistic analysis that proves Proposition 3.1.4, we see that it is virtually unchanged when the first k coordinates become random. Also the puncturing argument that proves Theorem 3.1.2 sees only the punctured coordinates being chosen from $\{1, \ldots, m\}$ rather than from $\{k+1, \ldots, m\}$.

Regarding the second distribution $\mathcal{U}(n,k)$, we argue differently and relate it to $\mathcal{A}(n,k)$. From here on n and k will be suppressed from the notation, since they are assumed to be fixed. We add indices as $C \leftarrow \mathcal{A}$ or $C \leftarrow \mathcal{U}$ to our probability notation to make the probabilistic model explicit. Observe that for any fixed code C_0 of dimension k, we have

$$\Pr_{C \leftarrow \mathcal{A}}(C = C_0 | \dim C = k) = \Pr_{C \leftarrow \mathcal{U}}(C = C_0).$$

It follows that, if $\mathcal{P}(C)$ denotes a property that a code C may have,

$$\Pr_{D \leftarrow \mathcal{U}}(\mathcal{P}(D)) = \Pr_{C \leftarrow \mathcal{A}}(\mathcal{P}(C) | \dim C = k).$$

We deduce from this observation that:

LEMMA 3.5.1. *For any property $\mathcal{P}$,*

$$\Pr_{D \leftarrow \mathcal{U}}(\mathcal{P}(D)) \geq \Pr_{C \leftarrow \mathcal{A}}(\mathcal{P}(C)) - \Pr_{C \leftarrow \mathcal{A}}(\dim C < k).$$

PROOF. We have

$$\begin{aligned}\Pr_{C \leftarrow \mathcal{A}}(\mathcal{P}(C)) &= \Pr_{C \leftarrow \mathcal{A}}(\mathcal{P}(C) | \dim C = k) \Pr_{C \leftarrow \mathcal{A}}(\dim C = k) + \\ &+ \Pr_{C \leftarrow \mathcal{A}}(\mathcal{P}(C) | \dim C < k) \Pr_{C \leftarrow \mathcal{A}}(\dim C < k) \leq \\ &\leq \Pr_{D \leftarrow \mathcal{U}}(\mathcal{P}(D)) + \Pr_{C \leftarrow \mathcal{A}}(\dim C < k).\end{aligned}$$

□

Next, recall this well-known result on random matrices:

$$\Pr_{C \leftarrow \mathcal{A}}(\dim C < k) \leq \frac{1}{q^{n-k}}.$$

Together with Lemma 3.5.1 this gives us:

$$\Pr_{D \leftarrow \mathcal{U}}(\mathcal{P}(D)) \geq \Pr_{C \leftarrow \mathcal{A}}(\mathcal{P}(C)) - \frac{1}{q^{n-k}}.$$

We can now apply this to versions of our Theorems for $\mathcal{A}(n,k)$. In particular, our main Theorem 3.1.2 will read, under the uniform distribution $\mathcal{U}(n,k)$, that there exist some positive real constants γ, δ such that

$$\Pr_{C \leftarrow \mathcal{U}}(C^2 = \mathbb{F}^{n(k)}) \geq 1 - 2^{-\gamma k} - 2^{-\delta t(k)} - \frac{1}{q^{n(k)-k}}.$$

This simple argument is enough to recover an asymptotically optimal version of our main result for the uniform distribution, except for code rates that tend to 1.

Chapter 4

Critical Pairs for the Product Singleton Bound

4.1 Overview

Let $\mathbb{F}$ be a finite field, let n be a positive integer. Our goal in this chapter is to characterize pairs (C, D) of codes that attain the following bound.

THEOREM 4.1.1 (Product Singleton Bound [62]). *Let $C, D \subseteq \mathbb{F}^n$ be linear codes. Then*

$$d_{\min}(CD) \leq \max\{1, n - (\dim C + \dim D) + 2\}. \tag{4.1}$$

A slightly stronger version of Theorem 4.1.1 is actually proved in [62], as is a version involving the product of more than two codes, but the above statement is really what motivates our discussion. We shall call the upper bound (4.1) the *Product Singleton Bound*, that can be thought of as a generalization of the classical Singleton Bound. Indeed, the classical Singleton Bound for a single code C is recovered by taking the code D in Theorem 4.1.1 to be of dimension 1 and minimum distance n.

We make the remark that if $d_{\min}(CD)$ is allowed to be equal to 1, then pairs achieving equality in (4.1) can be almost anything, since typical pairs of codes will have a product equal to the whole space $\mathbb{F}^n$. This phenomenon has been studied in Chapter 3 in the case of $C = D$ and in [64] in the general case. So we shall disregard the situation when $d_{\min}(CD) = 1$ and call (C, D) a *Product-MDS (PMDS)* pair if it achieves equality in (4.1) and $d_{\min}(CD) \geq 2$.

As mentioned above, a PMDS pair can consist of an ordinary MDS code and a code of dimension 1. It is a natural question to ask what other PMDS pairs exist. It turns out that there is a surprisingly complete answer to this question. We shall show in particular that if (C, D) is a PMDS pair such that $\dim C \geq 2$, $\dim D \geq 2$, and $d_{\min}(CD) \geq 3$, then C and D can only be Reed-Solomon codes. By this we mean Reed-Solomon code in the widest sense, i.e. generalized, possibly extended or doubly extended in the terminology of [48], or Cauchy codes as in [30]. PMDS pairs with $d_{\min}(CD) = 2$ will also be described quite precisely. To be more specific, in the symmetric case $C = D$ we shall prove:

THEOREM 4.1.2. *If (C, C) is a PMDS pair, then C is either a Reed-Solomon code or a direct sum of self-dual codes.*

Self-duality in the above statement should be understood to be relative to a non-degenerate bilinear form which is not necessarily the standard inner product.

To establish these results we shall import methods from additive combinatorics and establish coding-theoretic analogues of the classical theorems of Kneser [42] and Vosper [72]. For background on and proofs of Kneser and Vosper's Theorems we refer to [69]. Kneser's Theorem implies in particular that if A, B are subsets of an abelian group such that

$$|A + B| < |A| + |B| - 1$$

then $A + B$ must be periodic, i.e. there exists a non-zero element g of the abelian group that stabilizes $A + B$ so that we have $A + B + g = A + B$. Our coding-theoretic variant of Kneser's Theorem will imply that if C and D are two codes such that

$$\dim CD < \dim C + \dim D - 1,$$

then the code C is necessarily the direct sum of two non-zero codes, which is equivalent to the existence of a non-constant vector x of F^n such that $xCD = CD$.

Vosper's Theorem is a characterization of pairs of subsets A, B of the integers modulo a prime p with the property that $|A+B| = |A|+|B|-1$. It states that, excluding some degenerate cases, A, B must be arithmetic progressions with the same difference. We make the remark that if a code C has a generator matrix with rows $g, g\alpha, \ldots, g\alpha^{k-1}$, i.e. has a basis of elements in "geometric" progression then, provided g is of weight n and α has distinct coordinates, C must be a Reed-Solomon code. This is why a code-theoretic version of Vosper's Theorem forces the appearance of Reed-Solomon codes. There will be some twists to the analogy however that we shall discuss later in the paper.

Our main result takes the following form.

MAIN THEOREM 4.1.3. *Let $C, D \subseteq F^n$ be codes such that the pair (C, D) is Product MDS. Then one of the following situations occurs.*

(i) C and D are MDS and, if none of them has dimension 1, they are Reed-Solomon codes with a common evaluation-point sequence.

(ii) There is a partition of the coordinate set into non-empty subsets

$$\{1, \ldots, n\} = I_1 \cup \cdots \cup I_h$$

and there exist h pairs $(C_1, D_1), \ldots, (C_h, D_h)$ of codes of F^n, such that $\operatorname{supp} C_i = \operatorname{supp} D_i = I_i$, for all $i = 1, \ldots, h$, and such that C and D decompose as:

$$C = C_1 \oplus \cdots \oplus C_h,$$
$$D = D_1 \oplus \cdots \oplus D_h.$$

Furthermore, for all $i = 1, \ldots, h$, when C_i and D_i are identified with codes of $F^{|I_i|}$ through the natural projection on their support, we have that $C_i = (g_i D_i)^\perp$ for some $g_i \in (F^{|I_i|})^\times$.

REMARK 4.1.4. The codes C_i and D_i are mutually orthogonal relative to the non-degenerate bilinear form $(x, y) \mapsto (x \,|\, g_i y) = (g_i x \,|\, y)$, where $(\cdot \,|\, \cdot)$ denotes the standard inner product. Hence the wording of Theorem 4.1.2 in the case $C = D$.

The rest of the chapter is organized as follows. Section 4.2 states and proves the coding-theory equivalent of Kneser's Theorem. Section 4.3 is dedicated to a coding-theory version of Vosper's Theorem. Section 4.4 shows how to recover a version of the Product Singleton Bound as a straightforward consequence of Kneser's Theorem and goes on to derive the proof of Theorem 4.1.3. Section 4.5 concludes with some comments.

4.2 Kneser's Theorem

As usual, $\mathbb{F}$ will denote a finite field, but we shall need, in a couple of occasions, to deal with fields that may be infinite in which case we will use the notation $\mathbb{K}$. All codes will be linear. We will call them simply "codes" when the ambient space is $\mathbb{F}^n$, and use the terminology of vector spaces in the general setting of $\mathbb{K}^n$.

Kneser's Addition Theorem below involves the stabilizer $\mathrm{St}(X) = \{g \in G : g + X = X\}$ of a subset X of an abelian group G. The (Minkowski) sum

$A + B$ of two subsets A, B of G is defined as the set of sums $a + b$ when a and b range over A and B respectively.

THEOREM 4.2.1 (Kneser [42]). *Let G be an abelian group. Let $A, B \subseteq G$ be non-empty, finite subsets. Then*

$$|A + B| \geq |A| + |B| - |\operatorname{St}(A + B)|.$$

Kneser's original Theorem was transposed to the extension field setting by Hou, Leung and Xiang in [36]. Let $\mathbb{L}/\mathbb{K}$ be a field extension. For $\mathbb{K}$-linear subspaces $S, T \subseteq \mathbb{L}$, we may consider the product of subspaces ST defined as the $\mathbb{K}$-linear span of the set of elements of the form $st, s \in S, t \in T$. Hou et al.'s Theorem is concerned with the structure of pairs of subspaces whose product has small dimension. Again, the stabilizer of a K-subspace $X \subseteq \mathbb{L}$ is involved and is defined in the expected way $\operatorname{St}(X) = \{z \in \mathbb{L} : zX \subseteq X\}$.

THEOREM 4.2.2 (Generalized Kneser Theorem [36]). *Let $\mathbb{L}/\mathbb{K}$ be a separable field extension. Let $S, T \subseteq \mathbb{L}$ be non-zero, finite-dimensional $\mathbb{K}$-vector spaces. Then*

$$\dim ST \geq \dim S + \dim T - \dim \operatorname{St}(ST).$$

Remarkably, Kneser's original Theorem for groups can be recovered easily from Hou et al.'s version.

We will now proceed to show that there is a variant of Kneser's Theorem for the algebra induced by coordinatewise multiplication.

THEOREM 4.2.3. *Let $S, T \subseteq \mathbb{K}^n$ be non-zero $\mathbb{K}$-vector spaces. Then*

$$\dim ST \geq \dim S + \dim T - \dim \operatorname{St}(ST).$$

REMARK 4.2.4. The products ST in Theorems 4.2.2 and 4.2.3 are in different algebras. The statement of Theorem 4.2.2 is the only instance of the paper where the product ST does not refer to a coordinatewise product.

REMARK 4.2.5. Assuming that Theorem 4.2.3 holds in the case of full-support S and T, the general case can be derived as follows. Let $S_0, T_0 \subseteq \mathbb{K}^{n_0}$ be the projections of S, T respectively on $\operatorname{supp} ST$, where $n_0 := |\operatorname{supp} ST|$. The spaces S_0 and T_0 both have full support, hence

$$\dim S_0T_0 \geq \dim S_0 + \dim T_0 - \dim \operatorname{St}(S_0T_0).$$

Clearly $\dim S_0T_0 = \dim ST$ and $\dim \operatorname{St}(ST) = \dim \operatorname{St}(S_0T_0) + n - n_0$. It remains to prove that

$$\dim S_0 + \dim T_0 \geq \dim S + \dim T - (n - n_0).$$

Let $S_1, T_1 \subseteq \mathbb{K}^{n-n_0}$ be the projections of S, T respectively on the complement of $\operatorname{supp} ST$. Observe that $\operatorname{supp} S_1$ and $\operatorname{supp} T_1$ cannot intersect, hence $\dim S_1 + \dim T_1 \leq n - n_0$. Moreover $\dim S \leq \dim S_0 + \dim S_1$ and $\dim T \leq \dim T_0 + \dim T_1$. Putting everything together we obtain the desired inequality.

From here on "Kneser's Theorem" will refer to Theorem 4.2.3 rather than to the original result. Our proof is strongly inspired by Hou et al.'s proof of Theorem 4.2.2 [36], itself drawing upon the e-transform technique of additive combinatorics (see e.g. [69]).

If V is a $\mathbb{K}$-subspace of $\mathbb{K}^n$, we use the notation $V^\times$ to mean the subset of invertible elements of V.

LEMMA 4.2.6. *Let $S, T \subseteq \mathbb{K}^n$ be non-zero $\mathbb{K}$-vector spaces. Assume that T has a basis of invertible elements. Then, for all $x \in S^\times$, there exist a $\mathbb{K}$-algebra $H_x \subseteq \mathbb{K}^n$ and a $\mathbb{K}$-vector space $V_x \subseteq \mathbb{K}^n$ such that $H_x V_x = V_x$, $xT \subseteq V_x \subseteq ST$ and*

$$\dim V_x + \dim H_x \geq \dim S + \dim T.$$

PROOF. Assume that the lemma is proved for $x = \mathbf{1}$. Then, if $S^\times$ is non-empty, for any $x \in S^\times$ we may apply the result for the case $x = \mathbf{1}$ to $x^{-1}S$ and T. So we only need to prove the Lemma for $\mathbf{1} \in S$ and $x = \mathbf{1}$. Analogously, we may assume that $\mathbf{1} \in T$.

We argue by induction on $k := \dim S$. If $k = 1$, $H := \mathbb{K}\mathbf{1}$ and $V := T$ do the job. So assume that $k > 1$ and the result holds for smaller dimension. For each $e \in T^\times$, define

$$S(e) := S \cap Te^{-1}, \quad T(e) := T + Se.$$

We have $S(e)T \subseteq ST$, $S(e)Se \subseteq TS$, therefore $S(e)T(e) \subseteq ST$. Furthermore,

$$\begin{aligned} \dim T(e) &= \dim T + \dim Se - \dim(T \cap Se) \\ &= \dim T + \dim S - \dim(Te^{-1} \cap S) \end{aligned}$$

by Lemma 2.5.10, hence

$$\dim S(e) + \dim T(e) = \dim S + \dim T.$$

We distinguish two cases.

Assume that $S(e) = S$ for all $e \in T^\times$, i.e. $S \subseteq Te^{-1}$ for all $e \in T^\times$. Then, since T has a basis of invertible elements, we have $ST \subseteq T$. The result then holds with H the subalgebra generated by S and $V := T$.

Assume that there exists $e \in T^\times$ such that $S(e) \subsetneqq S$. Then $0 < \dim S(e) < k$ hence the induction hypothesis applied to $S(e)$ and $T(e)$ gives an algebra H

and a vector space V such that $HV = V$,

$$T \subseteq T(e) \subseteq V \subseteq S(e)T(e) \subseteq ST$$

and

$$\dim V + \dim H \geq \dim S(e) + \dim T(e) = \dim S + \dim T.$$

□

Proof of Theorem 4.2.3. By Remark 4.2.5 we may assume that both S and T have full support. The key to the proof is the following observation. Assume that T has a basis of invertible elements. Recall that, by Lemma 4.2.6, for all $x \in S^\times$ there exist a K-algebra $H_x \subseteq \mathbb{K}^n$ and a $\mathbb{K}$-vector space $V_x \subseteq \mathbb{K}^n$ such that

$$\begin{aligned} H_x V_x &= V_x && (4.2)\\ xT &\subseteq V_x \subseteq ST && (4.3)\\ \dim V_x + \dim H_x &\geq \dim S + \dim T. && (4.4) \end{aligned}$$

Set $k := \dim S$ and assume furthermore that there exists a $\mathbb{K}$-basis $\{x_1, \ldots, x_k\}$ of S contained in $S^\times$ such that

$$H_{x_1} = \cdots = H_{x_k} =: H. \tag{4.5}$$

Then $ST = V_{x_1} + \cdots + V_{x_k}$ by (4.3), and therefore $HST = ST$ by (4.2), in other words $H \subseteq \mathrm{St}(ST)$. From (4.4) it follows therefore that

$$\dim ST + \dim \mathrm{St}(ST) \geq \dim V_{x_1} + \dim H \geq \dim S + \dim T,$$

hence the conclusion.

We shall first prove the Theorem when $\mathbb{K}$ is an infinite field, by showing in that case that T always has a basis of invertible elements and that there always exists a basis $\{x_1, \ldots, x_n\}$ of invertible elements of S satisfying (4.5).

Since T has full support, it should be clear enough that it has a basis of invertible elements for $\mathbb{K}$ infinite. In this case Lemma 4.2.6 applies. Now fix a $\mathbb{K}$-basis $\{s_1, \ldots, s_k\}$ of S and define, for all $\alpha \in \mathbb{K}$, $y_\alpha := \sum_{i=1}^k \alpha^{i-1} s_i \in S$. For any choice of non-zero, pairwise distinct $\alpha_1, \ldots, \alpha_k \in \mathbb{K}$, the matrix transforming $s_1, \ldots, s_k$ into $y_{\alpha_1}, \ldots, y_{\alpha_k}$ is Vandermonde, and therefore $y_{\alpha_1}, \ldots, y_{\alpha_k}$ is also a $\mathbb{K}$-basis of S. We now observe that the set $\{\alpha \in \mathbb{K} : y_\alpha \in S^\times\}$ is infinite: indeed its complement in $\mathbb{K}$ is finite, as it is a finite union of zero-sets of non-zero polynomials. That these polynomials are non-zero is guaranteed by the full-support property of S. On the other hand, the number of subalgebras of $\mathbb{K}^n$ is finite by Remark 2.5.12, in particular the number of subalgebras H_x guaranteed by Lemma 4.2.6 is finite. It follows that there exist $\alpha_1, \ldots, \alpha_k$

such that $\{x_1 = y_{\alpha_1}, \ldots, x_k = y_{\alpha_k}\}$ is a $\mathbb{K}$-basis of S whose elements are all invertible and such that $H_{x_1} = \cdots = H_{x_k}$. This concludes the proof in the case $\mathbb{K}$ infinite.

Assume now that $\mathbb{K}$ is finite, and consider an infinite field extension $\mathbb{K}'$ of $\mathbb{K}$, for example the rational function field $\mathbb{K}' := \mathbb{K}(t)$, where t is transcendental over $\mathbb{K}$. The infinite base-field case applies to $\mathbb{K}'$-vector spaces. Our purpose is to draw our conclusion from this. Define the base-field extensions $S' := S \otimes \mathbb{K}', T' := T \otimes \mathbb{K}'$, where tensor products are taken over $\mathbb{K}$. By construction S' and T' are $\mathbb{K}'$-vector spaces and we have just proved that

$$\dim_{\mathbb{K}'} S'T' \geq \dim_{\mathbb{K}'} S' + \dim_{\mathbb{K}'} T' - \dim_{\mathbb{K}'} \mathrm{St}(S'T').$$

It is clear that $S'T' = ST \otimes \mathbb{K}'$, $\dim_{\mathbb{K}'} S' = \dim S$, $\dim_{\mathbb{K}'} T' = \dim T$ and $\dim_{\mathbb{K}'} S'T' = \dim ST$, where non-indexed dimensions are taken over $\mathbb{K}$. Moreover $\mathrm{St}(S'T') = \mathrm{St}(ST) \otimes \mathbb{K}'$ by Lemma 2.5.13 and the conclusion follows. □

Theorem 4.2.3 implies in particular that if C and D are two codes such that CD has trivial stabilizer, i.e. is indecomposable, then we must have

$$\dim CD \geq \dim C + \dim D - 1. \tag{4.6}$$

The next section studies pairs of codes C, D such that CD is indecomposable and achieves equality in (4.6).

4.3 Vosper's Theorem

We start by recalling Vosper's Addition Theorem.

THEOREM 4.3.1 (Vosper [72]). *Let G be an abelian group of prime order p. Let $A, B \subseteq G$ be subsets, with $|A|, |B| \geq 2$ and $|A + B| \leq p - 2$. If*

$$|A + B| = |A| + |B| - 1$$

then A and B are arithmetic progressions with the same difference.

We point out that an extension-field version of Vosper's Theorem for finite fields was recently proved in [2].

Since the stabilizer of a subset of a group G must be a subgroup, when G is of prime order and has no proper subgroup, Kneser's Addition Theorem 4.2.1 implies that subsets A, B of G such that $A + B \neq G$ must satisfy

$$|A + B| \geq |A| + |B| - 1.$$

This result is known as the Cauchy-Davenport Inequality, see [54, 69]. Vosper's Theorem is therefore concerned with characterizing pairs of sets achieving equality in the Cauchy-Davenport Inequality.

In the algebra setting, the inequality (4.6) may be thought of as a code-product version of the Cauchy-Davenport Inequality. But contrary to the group case, the algebra $\mathbb{F}^n$ always has proper subalgebras (for $n > 1$) so we cannot hope to ensure (4.6) purely by a condition on $\mathbb{F}^n$. However, we have seen that (4.6) holds when (at least one of) the codes involved is MDS (Theorem 2.5.16). The following theorem may be seen as a version of Vosper's Theorem for MDS codes, and is the main result of this section.

THEOREM 4.3.2. *Let $C, D \subseteq \mathbb{F}^n$ be MDS codes, with $\dim C, \dim D \geq 2$ and $\dim CD \leq n-2$. If*

$$\dim CD = \dim C + \dim D - 1$$

then C and D are Reed-Solomon codes with a common evaluation-point sequence.

REMARK 4.3.3. The hypotheses $\dim C, \dim D \geq 2$ clearly cannot be removed. The value $n-2$ is also best possible in the hypothesis $\dim CD \leq n-2$, since by taking C to be an arbitrary MDS (non Reed-Solomon) code, and taking $D = C^{\perp}$, we will have a pair of MDS codes such that $\dim CD = \dim C + \dim D - 1 = n-1$. A slight relaxation of the MDS hypothesis is presented in [1]: here it is observed that only the projections C_I and D_I of C and D onto a sufficiently large coordinate set $I \subseteq \{1, \ldots, n\}$ are required to be MDS in order to make our argument work.

We introduce the following notation for Vandermonde-type matrices. Given a positive integer k and $\alpha = (\alpha_1, \ldots, \alpha_n) \in (\mathbb{F} \cup \{\infty\})^n$ we denote by $V_k(\alpha)$ the $k \times n$ matrix whose i-th column is $(1, \alpha_i, \ldots, \alpha_i^{k-1})^T$ if $\alpha_i \neq \infty$, $(0, \ldots, 0, 1)^T$ otherwise. Note that the possible presence of this last column makes $V_k(\alpha)$ a Vandermonde matrix in a generalized sense. We remark that if the entries of α are pairwise distinct then $V_k(\alpha)$ has full rank. With this notation, a Reed-Solomon code of length n and dimension k is a code of the form gC, where $g \in (\mathbb{F}^{\times})^n$ (i.e. g has no zero entries) and C is generated by $V_k(\alpha)$ for some $\alpha \in (\mathbb{F} \cup \{\infty\})^n$ with pairwise-distinct entries. The vector α is an evaluation-point sequence of C.

LEMMA 4.3.4. *Let $C \subseteq \mathbb{F}^n$ be a full-support code with $\dim C \geq 2$ and $d_{\min}(C) > 1$. Assume that there exists a 2-dimensional MDS code $A \subseteq \mathbb{F}^n$, generated by $V_2(\alpha)$ for some $\alpha \in \mathbb{F}^n$ with pairwise distinct entries, such that*

$$\dim AC = \dim C + 1 \leq n - 1.$$

Then C is generated by $gV_{\dim C}(\alpha)$ for some $g \in C$.

PROOF. Since α has at most one zero coordinate, $d_{\min}(C) > 1$ implies that $\dim \alpha C = \dim C$. We therefore have

$$\dim AC = \dim(C + \alpha C) = 2 \dim C - \dim(C \cap \alpha C),$$

hence

$$\dim(C \cap \alpha C) = \dim C - 1.$$

Moreover, $C' = C \cap \alpha C$ has support strictly larger than its dimension, otherwise it would have minimum distance 1 and this would imply the existence of a word of weight 1 in C. We prove the lemma by induction on $k := \dim C$.

In the case $k = 2$, pick $g' \in C \cap \alpha C$, which exists as $\dim(C \cap \alpha C) = 1$, and let $g \in C$ be such that $g' = g\alpha$. Then g and $g' = g\alpha$ are linearly independent, as $|\operatorname{supp} g| \geq |\operatorname{supp} g'| \geq 2$ and α has pairwise distinct entries. It follows that C is generated by g and $g\alpha$, i.e. by $gV_2(\alpha)$.

Now assume that $k > 2$. We have

$$k = \dim C' + 1 \leq \dim AC' \leq \dim \alpha C = k,$$

where the right inequality follows from the inclusion $AC' = C' + \alpha C' \subseteq \alpha C$, and the left inequality follows from Theorem 2.5.16 (recall that A is MDS). Strictly speaking, Theorem 2.5.16 only applies to full-support codes and C' may have a support of cardinality $n - 1$ if α has a zero coordinate. But if this happens we may puncture A and C' by deleting this coordinate to obtain full-support codes of the same dimension as A and C and still apply Theorem 2.5.16.

Since $C' \subseteq C$ we have $d_{\min}(C') \geq d_{\min}(C) > 1$, and we have just shown $\dim AC' = \dim C' + 1 \leq (n-1) - 1$, since $\dim C' = \dim C - 1$. Therefore the induction hypothesis applies to C', possibly after puncturing one zero coordinate to make C' full support. Hence C' is generated by $g'V_{k-1}(\alpha)$ for some $g' \in C'$. Let $g \in C$ be such that $g' = g\alpha$. The matrix whose rows are the elements of the set $\{g, g' = g\alpha, \ldots, g'\alpha^{k-2} = g\alpha^{k-1}\} \subseteq C$ is $gV_k(\alpha)$, which has rank k as $|\operatorname{supp} g| \geq |\operatorname{supp} C'| \geq k$. It follows that this set is linearly independent and $gV_k(\alpha)$ generates C. □

LEMMA 4.3.5. *Let $C, D \subseteq \mathbb{F}^n$ be MDS codes satisfying*

$$\dim CD = \dim C + \dim D - 1.$$

Assume that there exists an index set $I \subseteq \{1, \ldots, n\}$ with $|I| \geq \dim CD$ such that the punctured codes $C_I, D_I \subseteq \mathbb{F}^{|I|}$ obtained by projecting C and D on the coordinates indexed by I are Reed-Solomon codes with a common evaluation-point sequence. Then C and D are Reed-Solomon codes with a common evaluation-point sequence.

PROOF. Set $k := \dim C$, $\ell := \dim D$. Since $|I| \geq \dim CD$ we have $|I| \geq k$ and $|I| \geq \ell$ and since C and D are MDS we must have $\dim C_I = \dim C = k$, $\dim D_I = \dim D = \ell$. Note that we may suppose $k, \ell \geq 2$, otherwise there is nothing to prove.

Reformulating the hypothesis, there exist $g_I, g'_I \in \mathbb{F}^{|I|}$, $\alpha_I \in (\mathbb{F} \cup \{\infty\})^{|I|}$, where α_I has pairwise-distinct entries, such that C_I and D_I are generated by $g_I V_k(\alpha_I)$ and $g'_I V_\ell(\alpha_I)$ respectively. In other words there are unique generator matrices G_C and G_D of C and D whose I-indexed columns form $g_I V_k(\alpha_I)$ and $g'_I V_\ell(\alpha_I)$ respectively. It also follows that $g_I g'_I V_{k+\ell-1}(\alpha_I)$ generates $C_I D_I$ (as $k + \ell - 1 \leq |I|$), $\dim C_I D_I = k + \ell - 1 = \dim CD$ and there is a unique generator matrix G_{CD} of CD whose I-indexed columns form $g_I g'_I V_{k+\ell-1}(\alpha_I)$.

Let $x_0, \ldots x_{k-1}$ and $y_0, \ldots, y_{\ell-1}$ denote the rows of G_C and G_D respectively.

The key observation is the following: let u, v, s, t be integers, with $0 \leq u, s \leq k-1$ and $0 \leq v, t \leq \ell - 1$, such that

$$u + v = s + t.$$

Since $x_u y_v$ and $x_s y_t$ coincide in the I-indexed coordinates, and $\dim C_I D_I = \dim CD$, the vectors $x_u y_v$ and $x_s y_t$ must coincide in every coordinate of $\{1, \ldots, n\}$. In other words, if $\pi = (\pi_0, \pi_1, \ldots, \pi_{k-1})^T$ and $\tau = (\tau_0, \tau_1 \ldots, \tau_{\ell-1})^T$ are the j-th column of G_C and G_D respectively, for some $j \notin I$, then

$$\pi_u \tau_v = \pi_s \tau_t.$$

We now exploit this property in order to prove the lemma. Pick two columns π, τ of G_C, G_D as above.

First assume that $\pi_0 \neq 0$ and $\tau_0 \neq 0$. Without loss of generality we may assume $\pi_0 = \tau_0 = 1$. It follows from $\pi_0 \tau_1 = \pi_1 \tau_0$ that $\tau_1 = \pi_1 =: \beta \in \mathbb{F}$. For all $i \leq k-1$, it holds that $\pi_i = \pi_i \tau_0 = \pi_{i-1} \tau_1$. Applying this formula recursively we obtain $\pi_i = \beta^i$ for all $i \leq k-1$, i.e. π corresponds to the evaluation point $\beta \in \mathbb{F}$. The same argument applies to τ, which corresponds to the evaluation point $\beta \in \mathbb{F}$ as well.

Now assume that $\pi_0 = 0$. If $\tau_0 \neq 0$, then $\pi_1 \tau_0 = \pi_0 \tau_1 = 0$ implies $\pi_1 = 0$. Continuing in this way, we see that if $\pi_i = 0$, then $\pi_{i+1} \tau_0 = \pi_i \tau_1 = 0$ implies $\pi_{i+1} = 0$ and by induction we obtain $\pi = 0$ which contradicts the full-support property of the MDS code C. Therefore $\tau_0 = 0$. Assume without loss of generality that $k \leq \ell$. If $k = \ell = 2$, then both π_1 and τ_1 are non zero as C and D have full support, hence the columns π and τ correspond to the evaluation point ∞. If $k = 2$ and $\ell \geq 3$ then as $\tau_i \pi_1 = \tau_{i+1} \pi_0 = 0$ for all $i < \ell - 1$ and as $\pi_1 \neq 0$ it follows that $\tau_i = 0$ for all $i < \ell - 1$ and again the full-support property of D implies that the column τ corresponds to the evaluation point

∞. If $k > 2$, then the same procedure that we applied to π_0, τ_0 again yields $\pi_1 = \tau_1 = 0$. Iterating in this way, we obtain that both π and τ correspond to the evaluation point ∞.

We have proved that up to multiplication by vectors g, g', the codes C and D have generator matrices of the form $V_k(\alpha)$ and $V_\ell(\alpha)$. Since C and D are MDS, the evaluation-sequence α must have distinct entries and C and D are Reed-Solomon codes with the same evaluation-point sequence. □

Proof of Theorem 4.3.2. Set $k := \dim C$, $\ell := \dim D$, $k^* := \dim CD = k + \ell - 1$. Let $C_0, D_0 \subseteq \mathbb{F}^{n_0}$ be the punctured codes obtained by projecting C, D on the first $n_0 := k^* + 2$ coordinates. As C_0, D_0 and C_0D_0 are MDS, we have $\dim C_0 = \dim C$, $\dim D_0 = \dim D$, $\dim C_0D_0 = \dim CD$ and

$$k^* = \dim C_0D_0 = \dim C_0 + \dim D_0 - 1 = n_0 - 2. \tag{4.7}$$

Define the code $A \subseteq \mathbb{F}^{n_0}$ by

$$A := (C_0D_0)^\perp.$$

By Lemma 2.5.17 the code C_0D_0 is MDS, therefore A is MDS and furthermore has dimension 2 by (4.7). Now observe that for any $a \in A$, $x \in C_0$, $y \in D_0$, orthogonality of A and C_0D_0 translates into

$$(a \,|\, xy) = 0$$

which is equivalent to

$$(ax \,|\, y) = 0.$$

We have therefore $(AC_0)^\perp \supseteq D_0$, from which we deduce

$$\dim AC_0 \leq n_0 - \dim D_0 = \dim C_0 + 1 \leq n_0 - 1$$

whence

$$\dim AC_0 = \dim C_0 + 1 \tag{4.8}$$

by Theorem 2.5.16. Similarly we also have

$$\dim AD_0 = \dim D_0 + 1. \tag{4.9}$$

Now A is an MDS code of dimension 2 and therefore has a generator matrix with at most two zero entries. By puncturing one coordinate if need be, we obtain a generator matrix with at most one zero entry. The two rows of this matrix are clearly of the form $g, g\alpha$ for some $g \in \mathbb{F}^n$ and $\alpha \in \mathbb{F}^n$ with pairwise distinct coordinates. Finally, consider that $\dim C_0 = n_0 - 1 - \dim D_0 \leq n_0 - 3$, and similarly $\dim D_0 \leq n_0 - 3$. Hence (4.8) and (4.9) imply

$$\dim AC_0 \leq n_0 - 2,$$
$$\dim AD_0 \leq n_0 - 2.$$

Therefore Lemma 4.3.4 applies to A, C_0 and to A, D_0, possibly after puncturing one coordinate. From there we obtain that C_0 and D_0 (possibly punctured on a common coordinate) are Reed-Solomon codes with a common evaluation-point sequence, and Lemma 4.3.5 gives the desired conclusion. □

4.3.1 Consequences of Theorem 4.3.2

A first interesting consequence of Theorem 4.3.2 is the following characterization of Reed-Solomon codes among MDS codes.

COROLLARY 4.3.6. *Let $C \subseteq \mathbb{F}^n$ be an MDS code, with $\dim C \leq (n-1)/2$. The code C is Reed-Solomon if and only if*

$$\dim C^2 = 2\dim C - 1. \tag{4.10}$$

REMARK 4.3.7. If $\dim C \geq (n+1)/2$, then C being MDS we must have $C^2 = \mathbb{F}^n$ and the dimension of the square cannot yield any information on the structure of C. However in that case, whether C is Reed-Solomon is betrayed by the dimension of the square of the dual code $C^\perp$. The remaining case in which Corollary 4.3.6 does not say anything is the case $\dim C = n/2$. One may wonder whether it still holds that C is Reed-Solomon if and only if $\dim C^2 = 2\dim C - 1$, and possibly Theorem 4.3.2 and Corollary 4.3.6 have not managed to capture this fact. The answer to this question is negative, indeed there exist plenty of MDS codes of dimension $n/2$ satisfying (4.10) which are not Reed-Solomon. For instance, the codes denoted $C_{11,8,8}$ and $C_{13,8,21}$ in [9], of length 8 over the fields with 11 and 13 elements respectively are self-dual, therefore satisfy (4.10), and can be shown not to be Reed-Solomon.

In addition, as our proofs are constructive, they can be used to design an algorithm that, given an MDS code which satisfies (4.10) (and is henceforth a Reed-Solomon code), recovers its defining parameters, i.e. the α_i's and g_i's as in Definition 2.5.7.

A second consequence concerns error correcting pairs, which we defined in Section 2.5.3. Recall that a pair of MDS codes (A, B) with $\dim A = t+1$ and $\dim B = t$ is a t-error correcting pair for $C := (AB)^\perp$, and $\dim C \leq n - 2t$. Moreover, this bound is attained if A and B are Reed-Solomon codes with a common evaluation-point sequence, and in this case C is a Reed-Solomon code as well. The converse also holds.

THEOREM 4.3.8. *Let $2 \leq t < n/2$ be an integer. Let $C \subseteq \mathbb{F}^n$ be a code of dimension $n-2t$ that has a t-error correcting pair (A, B) over a finite extension of $\mathbb{F}$. Then A, B, C are Reed-Solomon codes with a common evaluation-point sequence.*

This results first appeared in [49, Theorem 6.2]. In the original statement, it was further assumed that C is MDS, but this is actually implied by the existence of a t-error correcting pair: as observed in [58, Corollary 2.15] if C can correct t errors, then $d_{\min}(C) \geq 2t+1$, hence $\dim C + d_{\min}(C) \geq n - 2t + 2t + 1 = n + 1$. The paper [49] gives two separate proofs of this result: a first direct one, and a second one based on our Main Theorem 4.1.3. In fact, this second proof can be further simplified by using Theorem 4.3.2 as follows. For simplicity, we assume that the error correcting pair is defined over $\mathbb{F}$ (and not over an extension). For the full proof the reader is referred to [1].

First observe that, as in the original proof, A is MDS of dimension $t+1$, and B, possibly after an extension of the base field, contains a subcode B' which is MDS of dimension t such that (A, B') is a t-error correcting pair for C. We have that

$$2t = n - \dim C \geq \dim AB \geq \dim A + \dim B - 1 \geq \dim A + \dim B' - 1 = 2t,$$

where the dimensions are taken over the field of definition of B', hence $B' = B$, and in particular this field extension was not even necessary. The inequality $\dim AB \geq \dim A + \dim B - 1$ holds because A is MDS. Moreover, we have that $\dim AB = \dim A + \dim B - 1$, hence Theorem 4.3.2 applies and yields that A, B, AB and $C = (AB)^{\perp}$ are Reed-Solomon codes with a common evaluation-point sequence.

Finally we show that a t-strongly multiplicative secret sharing scheme among n players such that $n = 3t+1$, i.e. attains the bound given in Proposition 2.6.9, is necessarily based on a Reed-Solomon code. Recall that given a secret sharing scheme $\Sigma = (\pi_0, \ldots, \pi_n) \subseteq V^*$, where V is an $\mathbb{F}$-vector space, we define the code

$$C(\Sigma) := \{(\pi_0(x), \ldots, \pi_n(x)) : x \in V\}.$$

THEOREM 4.3.9. *Let t be a positive integer. Let Σ be a t-strongly multiplicative secret sharing scheme among n players. If $n = 3t+1$ then $C(\Sigma)$ is a Reed-Solomon code.*

PROOF. By assumption Σ has t-privacy and $(n - t = 2t + 1)$-product reconstruction. By Lemma 2.6.8 it also has $(n - 2t = t + 1)$-reconstruction, hence it is $(t+1)$-threshold. It follows by Corollary 2.6.14 that the associated code $C(\Sigma)$ is MDS of dimension $t+1$. Its square has dimension

$$\dim C(\Sigma)^2 \geq 2 \dim C(\Sigma) - 1 = 2t + 1$$

by Theorem 2.5.16 and

$$\dim C(\Sigma)^2 \leq 2t + 1$$

as the product scheme has $(2t+1)$-reconstruction. The conclusion now follows by our variant of Vosper's Theorem. □

This result was first proved in [1], together with two generalizations. The first one consider secret sharing schemes for a finite extension $\mathbb{L}$ of $\mathbb{F}$, i.e. schemes which allow the secret to be in $\mathbb{L}$. To capture this notion in full generality, one can use the definition of codex introduced in [16]. Alternatively one can adapt Definition 2.6.4 allowing π_0 to be an $\mathbb{F}$-linear map $V \to \mathbb{L}$, or can consider secret sharing schemes associated to $\mathbb{F}$-linear subspaces of $\mathbb{L} \times \mathbb{F}^n$ in the sense of Definition 2.6.15. In this setting, one can prove that a t-strongly multiplicative secret sharing scheme among n players satisfies

$$n \geq 3t + 2k - 1,$$

where k is the degree of the field extension. If $\mathbb{L} = \mathbb{F}$ this is simply Proposition 2.6.9.

THEOREM 4.3.10. *Let t be a positive integer. Let Σ be a t-strongly multiplicative secret sharing scheme for $\mathbb{L}$ among n players. If $n = 3t + 2k - 1$ then $C(\Sigma)$ is a Reed-Solomon code in $\mathbb{L} \times \mathbb{F}^n$.*

By a Reed-Solomon code in $\mathbb{L} \times \mathbb{F}^n$, we mean a code of the form

$$\{(g_0 f(\alpha_0), g_1 f(\alpha_1), \ldots, g_n f(\alpha_n)) : f \in \mathbb{F}[X]_{<k}\},$$

where $\alpha_1, \ldots, \alpha_n \in \mathbb{F} \cup \{\infty\}$ are pairwise distinct and $g_1, \ldots, g_n \in \mathbb{F}$ are non-zero, $\alpha_0 \in \mathbb{L}$ is different from the other α_i's and $g_0 \in \mathbb{L}$ is non-zero.

We only quickly sketch the proof. First, one proves that the $\mathbb{L}$-span of $C(\Sigma)$, which is an $\mathbb{L}$-liner code, defines a secret sharing scheme which has $(t+k-1)$-privacy and $(2t+2k-1)$-product reconstruction, hence $(t+k)$-reconstruction, hence the scheme is $(t+k)$-threshold. It follows that the $\mathbb{L}$-span of $C(\Sigma)$ is an MDS code of dimension $t+k$. Then, one notices that this implies $\dim_{\mathbb{L}} C(\Sigma)^2 = 2\dim_{\mathbb{L}} C(\Sigma) - 1$, hence the $\mathbb{L}$-span of $C(\Sigma)$ is a Reed-Solomon code. The last step consists of proving that $C(\Sigma)$ itself is a Reed-Solomon code in $\mathbb{L} \times \mathbb{F}^n$.

The second generalization allows not only the secret, but also each share to lie in a possibly different field extension of $\mathbb{F}$. For all $i = 1, \ldots, n$, let us denote by $\mathbb{F}_i$ the field where the i-th share lies. The idea is to focus on projections of $C(\Sigma)$: for all sufficiently large subsets $I \subseteq \{1, \ldots, n\}$, we can prove that $C(\Sigma_I)$ is a Reed-Solomon code in $\mathbb{L} \times \mathbb{F}_I^{|I|}$, where $\mathbb{F}_I$ denotes the compositum of the $\mathbb{F}_i$'s with $i \in I$. Then two such projections can be glued together if their supports intersect in at least three points, using the fact that the set of all evaluation-point sequences of a given Reed-Solomon code is an orbit under the action of a triply transitive group. Finally, if i belong to the intersection of two different supports I and J then $\alpha_i \in \mathbb{F}_I \cap \mathbb{F}_J$ and if $\mathbb{F}_I$ and $\mathbb{F}_J$ are "sufficiently different" then it may be the case that $\mathbb{F}_I \cap \mathbb{F}_J = \mathbb{F}_i$ as desired. We refer the reader to [1, Section 7] for a fully detailed discussion and a precise statement of the results.

4.4 Classification of PMDS pairs

We now are finally ready to focus on the chapter's central result, namely Theorem 4.1.3.

First, we show how Randriambololona's Product Singleton Bound can be obtained as a consequence of Theorem 4.2.3. To be precise we obtain:

THEOREM 4.4.1. *Let $C_1, \dots, C_t \subseteq \mathbb{F}^n$ be codes. Assume that their product $C_1 \cdots C_t$ has full support. Then*

$$d_{\min}(C_1 \cdots C_t) \leq \max\{t-1, n - (\dim C_1 + \cdots + \dim C_t) + t\}.$$

REMARK 4.4.2. The full result of [62] is actually stronger than Theorem 4.4.1, as it ensures that an element of weight at most $\max\{t-1, n-(\dim C_1 + \cdots + \dim C_t) + t\}$ can be found in the set

$$\{x_1 \cdots x_t : x_1 \in C_1, \dots, x_t \in C_t\},$$

and not only in its span. The support condition given here is also not the same as the apparently weaker hypothesis given in [62], but the two conditions are really interchangeable, as argued in [62, Remark 3(c)].

PROOF OF THEOREM 4.4.1. For ease of notation, set $k_i := \dim C_i$ for all $i = 1, \dots, t$, $P := C_1 \cdots C_t$, $k^* := \dim P$, $d^* := d_{\min}(P)$. Assume that $d^* \geq t$. The classical Singleton Bound, applied to P, says that

$$k^* \leq n - d^* + 1. \tag{4.11}$$

Repeatedly applying Kneser's Theorem 4.2.3 we obtain

$$k^* \geq k_1 + \cdots + k_t - (t-1)\dim \mathrm{St}(P). \tag{4.12}$$

Combining it with (4.11), we get

$$d^* \leq n - (k_1 + \cdots + k_t) + 1 + (t-1)\dim \mathrm{St}(P), \tag{4.13}$$

which is apparently a weaker statement than Theorem 4.4.1. To improve it, we "correct" (4.11) to transform it into an identity, namely we define $m := n - d^* + 1 - k^*$. Thus, by definition, P is "m-far from being MDS". The combination of this identity with (4.12) gives an improved version of (4.13), namely

$$d^* = n - k^* + 1 - m \leq n - (k_1 + \cdots + k_t) + 1 + (t-1)\dim \mathrm{St}(P) - m. \tag{4.14}$$

In the case of $t = 2$, the first claim of Lemma 2.5.15, rewritten as

$$\dim \mathrm{St}(P) - (n - d^* + 1 - k^*) \leq 1$$

immediately proves the theorem. In the general case, using the second claim of Lemma 2.5.15 instead we obtain

$$\begin{aligned}(t-1)\dim \mathrm{St}(P) - m &\leq (t-1)\ \frac{n-k^*}{d^*-1} - m \\ &= t-1+(t-1)\ \frac{m}{d^*-1} - m \\ &= t-1-\frac{d^*-t}{d^*-1}\ m. \end{aligned} \tag{4.15}$$

As $d^* \geq t$ the conclusion follows. □

From here on we focus on the case of $t = 2$. Recall that a pair of codes $C, D \subseteq \mathbb{F}^n$ is defined to be PMDS if

$$2 \leq d_{\min}(CD) = n - \dim C - \dim D + 2.$$

Observe that for a PMDS pair (C, D) all inequalities in the proof of Theorem 4.4.1 are actually identities. From this simple observation we obtain some corollaries which relate the Product Singleton Bound with Kneser's Theorem and with the classical Singleton Bound.

COROLLARY 4.4.3. *Let $C, D \subseteq \mathbb{F}^n$ be codes such that the pair (C, D) is PMDS. Then the following hold.*

1. *The pair (C, D) attains the bound of Kneser's Theorem, i.e.*

$$\dim CD = \dim C + \dim D - \dim \mathrm{St}(CD).$$

2. *Either CD is MDS or $d_{\min}(CD) = 2$.*

PROOF. From the above observation, (4.12) is an identity if (C, D) is PMDS, hence the first claim is immediately proved. From (4.14) and (4.15) we obtain

$$\frac{d_{\min}(CD)-2}{d_{\min}(CD)-1}\ m = 0,$$

where $m := n - d_{\min}(CD) + 1 - \dim CD$, hence either $m = 0$ meaning CD is MDS, or $d_{\min}(CD) = 2$. □

The two possible cases in our main Theorem 4.1.3 arise from the two possible situations given by the second claim of the above corollary. We distinguish the case of $d_{\min}(CD) > 2$, which implies that CD is MDS, and $d_{\min}(CD) = 2$.

PROPOSITION 4.4.4. *Let $C, D \subseteq \mathbb{F}^n$ be codes such that the pair (C, D) is PMDS, and assume $d_{\min}(CD) > 2$. Then C, D and CD are MDS. Moreover, if $\dim C, \dim D \geq 2$ then C, D and CD are Reed-Solomon codes with a common evaluation-point sequence.*

PROOF. By the above corollary CD is MDS. Moreover the PMDS property immediately yields $n > \dim C + \dim D$. We now proceed to prove that C and D are also MDS through Lemma 2.5.6.

Set $k := \dim C, \ell := \dim D$. Without loss of generality, we can choose a generator matrix G_C of C that is systematic in the first k positions. Let G_D be a generator matrix of D. The matrix formed by the last $n-k$ columns of G_D has full rank, otherwise there is a non-zero vector of D that is zero in the last $n-k$ positions, and taking the product with a row of G_C we would obtain a vector of CD of weight 1, contradicting that CD is MDS and not the whole space $\mathbb{F}^n$. So we can now assume that G_C is systematic in the first k positions and G_D is systematic in the subsequent ℓ positions.

Now we focus on G_C. Assume that there is a zero entry in the j-th column of G_C for some $j > k + \ell$, say in position (i, j) of G_C. Then, since the j-th column of G_D is not all-zero (otherwise CD would not be full support and would not be MDS), the product of the i-th row of G_C with some row of G_D yields non-zero vector of CD of weight at most $n - k - \ell + 1 = d_{\min}(CD) - 1$, a contradiction. Therefore, all columns of G_C indexed by $j > k + \ell$, that exist since $n > k + \ell$, have no zero entries. For the same reason, this is also true of G_D, and we obtain that the product of any row of G_C with any row of G_D is non-zero.

From this last fact, we get that G_C cannot have zero entries in the columns indexed by $\{k + 1, \ldots, k + \ell\}$, or again, by taking a product of a row of G_C with a row of G_D, we would have a non-zero vector of CD of weight at most $n - k - \ell + 1$. Now Lemma 2.5.6 allows us to conclude that C is MDS. Analogously, one has that D is MDS as well.

The last statement now follows immediately by Theorem 4.3.2. Note that $n > \dim C + \dim D$ is equivalent to the hypothesis $\dim CD \leq n - 2$. □

The following lemma will be useful to deal with the second case.

LEMMA 4.4.5. *Let $C, D \subseteq \mathbb{F}^n$ be codes such that CD is MDS and*

$$\dim CD = \dim C + \dim D - 1 = n - 1.$$

Then there exists $g \in (\mathbb{F}^n)^\times$ such that $C = (gD)^\perp$.

PROOF. Let $g \in \mathbb{F}^n$ be a generator of $(CD)^\perp$, which is invertible as $(CD)^\perp$ is MDS of dimension 1. For any $x \in C$, $y \in D$, we have

$$(x \,|\, gy) = (xy \,|\, g) = 0$$

so that $C \subseteq (gD)^\perp$, and equality follows by comparing dimensions. □

PROPOSITION 4.4.6. *Let $C, D \subseteq \mathbb{F}^n$ be codes such that the pair (C, D) is PMDS. Set $h := \dim \mathrm{St}(CD)$ and let $\{\pi_1, \ldots, \pi_h\}$ be an $\mathbb{F}$-basis of $\mathrm{St}(CD)$ of disjoint projectors with supports $I_1, \ldots, I_h$. Then C, D and CD decompose as*

$$\begin{aligned} C &= \pi_1 C \oplus \cdots \oplus \pi_h C, \\ D &= \pi_1 D \oplus \cdots \oplus \pi_h D, \\ CD &= \pi_1 CD \oplus \cdots \oplus \pi_h CD \end{aligned}$$

and, for all $i = 1, \ldots, h$, we have $\operatorname{supp} \pi_i C = \operatorname{supp} \pi_i D = \operatorname{supp} \pi_i CD = I_i$ and

$$\dim \pi_i CD = \dim \pi_i C + \dim \pi_i D - 1. \tag{4.16}$$

Moreover, if $d_{\min}(CD) = 2$ then, for all $i = 1, \ldots, h$, when $\pi_i C$ and $\pi_i D$ are identified with codes of $\mathbb{F}^{|I_i|}$ through the natural projection on their support, then $\pi_i C = (g_i \pi_i D)^\perp$ for some $g_i \in (\mathbb{F}^{|I_i|})^\times$.

PROOF. By Kneser's Theorem we have, for all $i = 1, \ldots, h$,

$$\dim \pi_i CD \geq \dim \pi_i C + \dim \pi_i D - 1 \tag{4.17}$$

since $\pi_i CD$ has trivial stabilizer. Therefore

$$\dim CD = \sum_{i=1}^{h} \dim \pi_i CD \geq \sum_{i=1}^{h} (\dim \pi_i C + \dim \pi_i D - 1). \tag{4.18}$$

Observing that

$$C \subseteq \pi_1 C \oplus \cdots \oplus \pi_h C, \quad D \subseteq \pi_1 D \oplus \cdots \oplus \pi_h D \tag{4.19}$$

we get

$$\sum_{i=1}^{h} (\dim \pi_i C + \dim \pi_i D - 1) \geq \dim C + \dim D - h,$$

but the right hand side of this inequality equals $\dim CD$ by the first claim of Corollary 4.4.3. From (4.18) we obtain therefore that all inequalities in (4.17) are equalities, i.e. for all $i = 1, \ldots, h$,

$$\dim \pi_i CD = \dim \pi_i C + \dim \pi_i D - 1,$$

and we obtain also

$$\sum_{i=1}^{h} (\dim \pi_i C + \dim \pi_i D) = \dim C + \dim D,$$

hence both inclusions in (4.19) are actually identities.

Now assume that $d_{\min}(CD) = 2$. Observe that $n = \dim C + \dim D$ by the Product Singleton Bound. From here on all codes are identified with full-support codes through the natural projection on their support. For all $i = 1, \ldots, h$, we have $d_{\min}(\pi_i CD) \geq 2$, hence $|I_i| \geq \dim \pi_i CD + 1$ by the classical Singleton Bound applied to $\pi_i CD$. Therefore

$$\begin{aligned} n = \sum_{i=1}^{h} |I_i| &\geq \sum_{i=1}^{h} (\dim \pi_i CD + 1) \\ &= \sum_{i=1}^{h} (\dim \pi_i C + \dim \pi_i D) \\ &= \dim C + \dim D = n. \end{aligned}$$

It follows that

$$\dim \pi_i CD = \dim \pi_i C + \dim \pi_i D - 1 = |I_i| - 1$$

and $d_{\min}(\pi_i CD) \geq 2 = |I_i| - \dim \pi_i CD + 1$ proves that $\pi_i CD$ is MDS. Now the conclusion follows by Lemma 4.4.5. □

Propositions 4.4.4 and 4.4.6 constitute the proof of Theorem 4.1.3.

4.5 Concluding Comments

As mentioned in Section 4.3, Theorem 4.3.2 is arguably a coding-theoretic analogue of Vosper's Addition Theorem. The analogy with its additive counterpart is not as clear-cut however as in the case of Theorem 4.2.3 and Kneser's Addition Theorem. More precisely, the MDS hypothesis in Theorem 4.3.2 is not a very natural analogue of the prime order of the ambient group hypothesis in Vosper's original Theorem, and there may possibly be other coding-theoretic analogues to consider.

The natural question raised by Theorem 4.2.3 and Theorem 4.3.2 is whether there exists a satisfying characterization of pairs C, D such that CD is indecomposable and of codimension at least 2, and $\dim CD = \dim C + \dim D - 1$. Beside pairs of Reed-Solomon codes, one now has Reed-Solomon codes with duplicate coordinates. Beside these, other examples turn up.

THEOREM 4.5.1 ([1, Theorem 4.9]). *For any finite field $\mathbb{F}$ and positive integer ℓ there exists a code C of length n (which in general depends on ℓ) which is not MDS, and whose square is indecomposable and satisfies*

$$\dim C^2 = 2 \dim C - 1 = n - \ell.$$

Such codes are constructed by taking the amalgamated direct sum, defined in the end of Section 2.5, of self-dual codes. Given two self-dual codes $C \subseteq \mathbb{F}^{n_1}$ and $D \subseteq \mathbb{F}^{n_2}$ such that $\dim C^2 = 2\dim C - 1 = n_1 - 1$ and $\dim D^2 = 2\dim D - 1 = n_2 - 1$, we have that

$$\begin{aligned}\dim(C \dot{\oplus} D)^2 &= 2\dim C \dot{\oplus} D - 1 = 2(\dim C + \dim D - 1) - 1 \\ &= (2\dim C + 2\dim D - 1) - 2 = n - 2\end{aligned}$$

where $n = n_1 + n_2 - 1$ is the length of $C \dot{\oplus} D$. The theorem is then proved by iterating this construction.

If the analogy with additive combinatorics is to be trusted, a full characterization may be tractable, though probably difficult, and would be a coding-theory equivalent of Kemperman's Structure Theorem for small sumsets [41].

Finally, it is natural to wonder whether the characterization of PMDS pairs extends to products of more than two codes. Our techniques (Corollary 4.4.3 and Proposition 4.4.4) allow to deal with the analogue of the first case of Theorem 4.1.3 and to prove the following: if $(C_1, \ldots, C_t)$ is a t-PMDS tuple, i.e. satisfies

$$d_{\min}(C_1 \cdots C_t) = n - (\dim C_1 + \cdots + \dim C_t) + t,$$

if none of the C_i's has dimension 1 and

$$d_{\min}(C_1 \cdots C_t) > t,$$

then all C_i's are Reed-Solomon codes with a common evaluation-point sequence. On the other hand the arguments in the paper do not seem quite sufficient to deal with the case of

$$d_{\min}(C_1 \cdots C_t) = t$$

corresponding to the second case of our main theorem. We leave the matter open for further study.

A version of Kneser's Theorem for a family of algebras was independently posted by Beck and Lecouvey [4], and is a more general version of Theorem 4.2.3. The proof follows similar arguments. Moreover, [4, Section 6] shows how Kneser's original Theorem can be recovered from the new variant. The very same argument, which is based on the embedding of the group G into the complex group algebra $\mathbb{C}[G]$ and on the isomorphism $\mathbb{C}[G] \cong \mathbb{C}^{|G|}$, allows one to recover the original theorem from our variant as well.

Chapter 5

On Secret Sharing with Non-linear Product Reconstruction

5.1 Overview

Multiplicative linear secret sharing is a fundamental notion in the area of secure multi-party computation (MPC). By extension, this holds in the area of two-party cryptography as well, by virtue of recently discovered deep applications of MPC to two-party cryptography as initiated in [39].

While linear secret sharing is additive in the sense that "the sum of share vectors corresponds to the sum of the secrets", multiplicative linear secret sharing enjoys the further property that "the product of two secrets is obtained as a linear function of the vector consisting of the coordinatewise product of two respective share vectors". There are several important (more demanding) variations on this notion, such as strongly multiplicative secret sharing. First framed and studied in [27] in the late 1990s as an abstract property of a linear secret sharing scheme[1], it had been implicit in several results since the mid 1980s (notably [7, 18, 35]) in the context of the application of Shamir's secret sharing scheme [67] to (information-theoretically) secure multi-party computation. The *asymptotical* (constant-rate) theory of strongly multiplica-

[1] It was shown, in particular, when and how a multiplicative scheme can be obtained from just a linear secret sharing scheme. However, this does not work for strong multiplicativity.

tive schemes has been initiated in [19], using algebraic geometry[2]. It has found several notable applications, starting with [39]. For a full discussion and references, please refer to [15].

This chapter focuses on the following foundational question, which is novel to the best of our knowledge. Suppose we *abandon the latter linearity condition* and instead require that the product of the two secrets is obtained by application of *some*, *not-necessarily-linear* "product reconstruction function". *Is the resulting notion equivalent to multiplicative linear secret sharing?* We show the (perhaps somewhat counter-intuitive) result that this relaxed notion is strictly *more general*.

Throughout this chapter, let $\mathbb{F}$ be a finite field of size q, n a positive integer, and let V be a finite-dimensional $\mathbb{F}$-vector space. When the field size needs to be put in evidence, we will use the notation $\mathbb{F}_q$ for the base field.

Definition 5.1.1. Let $(\pi_0, \ldots, \pi_n) \subseteq V^*$ be a secret sharing scheme. The scheme has *product reconstruction* if, for all $x, x', y, y' \in V$ with

$$\pi_1(x)\pi_1(y) = \pi_1(x')\pi_1(y'), \ldots, \pi_n(x)\pi_n(y) = \pi_n(x')\pi_n(y'),$$

it holds that

$$\pi_0(x)\pi_0(y) = \pi_0(x')\pi_0(y').$$

Note that the product reconstruction condition is equivalent to the existence of a *product reconstruction function* $\rho' : \mathbb{F}^n \longrightarrow \mathbb{F}$ such that

$$\rho'(\pi_1(x)\pi_1(y), \ldots, \pi_n(x)\pi_n(y)) = \pi_0(x)\pi_0(y),$$

for all $x, y \in V$. In particular, a multiplicative secret sharing scheme (see Definition 2.6.5) is one for which a *linear* product reconstruction function exists. To separate and compare the two multiplicativity notions, we say that a scheme is *M1* if it is multiplicative in the sense of Definition 2.6.5, *M2* if it admits a non-necessarily-linear product reconstruction function as required by Definition 5.1.1. Thus, an M1 scheme is also M2. As a consequence of our results the converse does not hold.

Remark 5.1.2. There does not appear to be much that one can say, a priori, about the complexity of such not-necessarily-linear product reconstruction functions. At best, one can say that in order to determine the product of two secrets from the coordinatewise product of two corresponding share vectors, it suffices to solve a system of quadratic equations.

The main result of this chapter is the following.

[2]Later, this asymptotical theory has also been developed in the case of *multiplicative* schemes using classical coding theory in [5]. The results there do not seem to carry over easily to strong multiplicative schemes.

MAIN THEOREM 5.1.3. *For any prime power q, there exists a function $t_q(n) \in \Omega(n)$ such that, for infinitely many $n \in \mathbb{N}$, there exists an $\mathbb{F}_q$-vector space V and a secret sharing scheme $(\pi_0, \ldots, \pi_n) \subseteq V^*$ which has $t_q(n)$-privacy and admits a product reconstruction function. However, such function is necessarily not $\mathbb{F}_q$-linear. Therefore, the scheme is M2 but not M1.*

The existence of such counterexamples can be explained from the difference between linear and algebraic independence of certain multivariate polynomials. For instance, the polynomials X, Y, XY are linearly independent but algebraically dependent. Nevertheless, since the involved polynomials are homogeneous with degree 2, quadratic forms are a powerful tool to solve our problem. Indeed, by means of combinatorial arguments involving bilinear and quadratic forms, we find examples of linear secret sharing schemes with non-linear product reconstruction on a small number of players.

THEOREM 5.1.4. *For every finite field $\mathbb{F}_q$ of size $q \geq 3$, there exists an $\mathbb{F}_q$-linear secret sharing scheme on 9 players that is M2 but not M1. In addition, there exists an $\mathbb{F}_2$-linear secret sharing scheme on 14 players that is M2 but not M1.*

Our main result is then obtained by composing those small examples with multiplicative linear secret sharing schemes on n players that have t-privacy with $t = \Omega(n)$. The existence of such schemes over any fixed base field was proved in [11, 20]. As an additional result, we prove that, for every finite field $\mathbb{F}_q$ of size $q \geq 3$, $n = 9$ is the minimum value for which there exists an $\mathbb{F}_q$-linear secret sharing scheme on n players that is M2 but not M1. This value remains undetermined for $q = 2$, but it is at least 9.

THEOREM 5.1.5. *Every M2 secret sharing scheme on less than 9 players is also M1.*

Our results extend to similar separation results for important variations, such as strongly multiplicative secret sharing.

THEOREM 5.1.6. *For any prime power q, there exists a function $\hat{t}_q(n) \in \Omega(n)$ such that, for infinitely many $n \in \mathbb{N}$, there exists an $\mathbb{F}_q$-vector space V and a secret sharing scheme $\Sigma = (\pi_0, \ldots, \pi_n) \subseteq V^*$ which has $\hat{t}_q(n)$-privacy and such that, for each set $I \subseteq \mathcal{P}$ consisting of $n - \hat{t}_q(n)$ players, the scheme Σ_I admits a product reconstruction function (M2). However there exists a set $J \subseteq \mathcal{P}$ with $n - \hat{t}_q(n)$ players such that Σ_J is not M1. Therefore, Σ is not $\hat{t}_q(n)$-strongly multiplicative.*

It is an interesting question whether there are applications of this "exotic",

novel class of secret sharing schemes with non-linear product reconstruction[3] to cryptographic protocols, but we will not offer any speculations here.

We remark that, while the notion of multiplicativity defined in [27] applies to linear secret sharing schemes where each share may consist of an arbitrary number of elements of the base field, in this work our definitions and results concern only *ideal* linear secret sharing schemes, i.e., those where each share is a *single* field element. This is the notion considered in e.g. [11, 19, 20]. If the local function is the component-wise product of the share-vectors, then the analysis is the same for both cases. If any bilinear function can be used in the local computations, then the general case can be reduced to the case of ideal schemes (maybe except for fields of characteristic 2) [4].

This chapter is organized as follows. In Section 5.2 we show that both the multiplicativity notion and its relaxed notion of product reconstruction can be captured in terms of the existence of quadratic forms with certain algebraic conditions imposed on them (see Propositions 5.2.1 and 5.2.2). This leads us to defining the "separating quadratic forms", which are characterized in Propositions 5.2.4 and 5.2.5 by using the classification of quadratic forms over finite fields. For any necessary theoretical background, the reader is referred to the introductory Sections 2.3 and 2.4.

By using those results, several examples of linear secret sharing schemes that prove the separation between the two notions are presented in Section 5.3. Specifically, for every finite field $\mathbb{F}_q$, we present examples of $\mathbb{F}_q$-linear secret sharing schemes with non-linear product reconstruction on n players, where $n = 9$ if $q \geq 3$ and $n = 14$ if $q = 2$. This constitute the proof of Theorem 5.1.4.

In Section 5.4, we analyze the behavior of the relaxed notion of product reconstruction under the composition of secret sharing schemes defined in Section 2.6.1 and we prove Main Theorem 5.1.3 by composing the examples on a small number of players presented in Section 5.3 with multiplicative linear secret sharing schemes whose privacy is linear in the number of players. Moreover, we show how to extend our results to strongly multiplicative secret sharing using the same composition technique, proving Theorem 5.1.6.

Finally, in Section 5.5 we prove Theorem 5.1.5, which states that it is not possible to find examples separating the two notions on less than 9 players. Therefore, the examples presented in Section 5.3 are among the smallest ones.

[3] All applications of multiplicative linear secret sharing we are aware of make essential use of linearity of product reconstruction.

[4] Of course our results do not rule out that separating examples with a smaller number of players exist in the non-ideal case, but we do not elaborate further on this matter.

5.2 Separating Quadratic Forms

In this section we characterize properties M1 and M2, or rather, their negations, separately. The characterization of the M2 property is given in terms of a class of quadratic forms, which we call separating as they allow us to distinguish the two multiplicativity notions. Finally, we provide a characterization for this class.

PROPOSITION 5.2.1. *A secret sharing scheme $(\pi_0, \ldots, \pi_n) \subseteq V^*$ is not M1 if and only if there exists a quadratic form $Q \in \mathrm{Quad}(V^*)$ such that $Q(\pi_1) = \cdots = Q(\pi_n) = 0$ and $Q(\pi_0) \neq 0$.*

PROOF. Straightforward from Proposition 2.6.6 and the isomorphism between $\mathrm{Sym}(V)^*$ and $\mathrm{Quad}(V^*)$ in Lemma 2.4.2. Here we use the following trivial fact from linear algebra: if V is an $\mathbb{F}$-vector space, $W \subseteq V$ is a subspace and $x \in V$ is a vector, then $x \notin W$ if and only if there exists a linear form $\pi \in V^*$ such that $\pi(x) \neq 0$ and $\pi(y) = 0$ for all $y \in W$. □

Given $x, y, x', y' \in V$, define the bilinear form $T_{x,y,x',y'} := x \otimes y - x' \otimes y' \in \mathrm{Bil}(V^*)$ and its associated quadratic form $Q_{x,y,x',y'} \in \mathrm{Quad}(V^*)$.

PROPOSITION 5.2.2. *A secret sharing scheme $(\pi_0, \ldots, \pi_n) \subseteq V^*$ is not M2 if and only if there exist vectors $x, y, x', y' \in V$ such that $Q_{x,y,x',y'}(\pi_1) = \cdots = Q_{x,y,x',y'}(\pi_n) = 0$ and $Q_{x,y,x',y'}(\pi_0) \neq 0$.*

PROOF. Obvious from Definition 5.1.1. □

DEFINITION 5.2.3. A quadratic form $Q \in \mathrm{Quad}(V^*)$ is called *separating* if $Q \neq Q_{x,y,x',y'}$ for every $x, y, x', y' \in V$, *non-separating* otherwise.

Using this notion, Proposition 5.2.2 claims that $(\pi_0, \ldots, \pi_n)$ is not M2 if and only if there exists a non-separating quadratic form $Q \in \mathrm{Quad}(V^*)$ such that $Q(\pi_1) = \cdots = Q(\pi_n) = 0$ and $Q(\pi_0) \neq 0$.

As a consequence of the two propositions above, a secret sharing scheme $(\pi_0, \ldots, \pi_n) \subseteq V^*$ is M2 but not M1 if and only if there exists a quadratic form $Q \in \mathrm{Quad}(V^*)$ such that $Q(\pi_1) = \cdots = Q(\pi_n) = 0$ and $Q(\pi_0) \neq 0$, and all such quadratic forms are separating.

Next two propositions provide a characterization of the separating forms.

PROPOSITION 5.2.4. *No quadratic form of rank $r \leq 3$ is separating. All quadratic forms of rank $r \geq 5$ are separating.*

PROOF. Let Q be not separating, i.e. $Q = Q_{x,y,x',y'}$ for some $x, y, x', y' \in V$. Then the associated bilinear form $\tilde{B}_Q$ is given by $\tilde{B}_Q = x \otimes y + y \otimes x - x' \otimes y' - y' \otimes x'$ and its rank is at most 4. This directly implies that non-separating forms have rank at most 4, since in the case of characteristic 2, when the rank of $\tilde{B}_Q$ is exactly 4 it is easy to see that Q is identically zero on $\operatorname{Rad} V$. This proves the second claim of the theorem.

We prove the first statement for forms of rank $r = 3$, being the cases with $r \leq 2$ similar. Let $Q \in \operatorname{Quad}(V^*)$ be a quadratic form of rank 3. Clearly, we can assume that $k := \dim V = 3$.

Suppose first that $\operatorname{char} \mathbb{F} \neq 2$. By the classification of quadratic forms, there exists a basis $\{e_1, e_2, e_3\}$ of V such that, for some $\alpha \in \mathbb{F}^*$, the matrix associated to the symmetric bilinear form B_Q is

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & \alpha \end{pmatrix}.$$

Therefore, Q is not separating because $B_Q = e_1 \otimes e_2 + e_2 \otimes e_1 + \alpha e_3 \otimes e_3$, and this implies that $Q = Q_{x,y,x',y'}$ with $x = 2e_1$, $y = e_2$, $x' = \alpha e_3$ and $y' = -e_3$.

Assume now that $\operatorname{char} \mathbb{F} = 2$. By the classification of quadratic forms, Q is determined by a bilinear form $T \in \operatorname{Bil}(V^*)$ such that its matrix in some suitable basis $\{e_1, e_2, e_3\}$ of V is

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Then $T = T_{e_1,e_2,e_3,e_3}$, and hence Q is not separating. □

It remains to study what happens for quadratic forms of rank $r = 4$. Briefly, up to equivalence, there are two quadratic forms of rank 4, and only one of them is separating.

PROPOSITION 5.2.5. *If* $\operatorname{char} \mathbb{F} \neq 2$*, a quadratic form of rank* $r = 4$ *is separating if and only if its discriminant is* -1*. If* $\operatorname{char} \mathbb{F} = 2$*, a quadratic form of rank* $r = 4$ *is separating if and only if its Arf invariant is* 1*.*

PROOF. Let $Q \in \operatorname{Quad}(V^*)$ be a quadratic form of rank $r = 4$. As before, we can assume that $k = \dim V = 4$. Suppose that Q is not separating, that is, $Q = Q_{x,y,x',y'}$ for some x, y, x', y'.

Suppose that $\operatorname{char} \mathbb{F} \neq 2$. Then the symmetric bilinear form associated to Q is

$$B_Q = \frac{1}{2}(x \otimes y + y \otimes x) - \frac{1}{2}(x' \otimes y' + y' \otimes x').$$

If $\{x, y, x', y'\}$ is a linearly dependent set, then $\operatorname{rk} B_Q \leq 3$. Therefore, $\{x, y, x', y'\}$ is a basis of V. The determinant of the matrix of B_Q in this basis is equal to $(1/4)^2$, and hence the discriminant of Q is equal to 1.

If $\operatorname{char} \mathbb{F} = 2$, then $\widetilde{B}_Q = x \otimes y + y \otimes x + x' \otimes y' + y' \otimes x'$. Again, $\{x, y, x', y'\} = \{e_1, e_2, e_3, e_4\}$ is a basis of V. Let $\{\pi_1, \pi_2, \pi_3, \pi_4\}$ be the dual basis of V^*. The Arf invariant of Q is equal to 0 because $Q(\pi_i) = 0$ for $i = 1, \ldots, 4$ and hence $Q(\pi_1)Q(\pi_2) + Q(\pi_3)Q(\pi_4) = 0$. □

5.3 Finding "Exotic Schemes"

We apply here the results in Section 5.2 to find examples of linear secret sharing schemes that are M2 but not M1. Specifically, we prove Theorem 5.1.4 and we present some additional examples of interest.

Associated to a secret sharing scheme $\Sigma = (\pi_0, \ldots, \pi_n) \subseteq V^*$, consider the subspace

$$W(\Sigma) = \langle \pi_i \otimes \pi_i : i = 1, \ldots, n \rangle \subseteq \operatorname{Sym}(V)$$

and its annihilator

$$I(\Sigma) = \{\phi \in \operatorname{Sym}(V)^* : \phi(B) = 0 \text{ for every } B \in W(\Sigma)\} \subseteq \operatorname{Sym}(V)^*.$$

Recall that Σ is M1 if and only if $\pi_0 \otimes \pi_0 \in W(\Sigma)$. By linear algebra, these subspaces satisfy

$$\dim W(\Sigma) + \dim I(\Sigma) = \dim \operatorname{Sym}(V) = \frac{k(k+1)}{2}.$$

If $W(\Sigma) = \operatorname{Sym}(V)$, then $\pi_0 \otimes \pi_0 \in W(\Sigma)$, and hence Σ is M1. In the case $\dim W(\Sigma) = \dim \operatorname{Sym}(V) - 1$, we obtain the following sufficient condition for a linear secret sharing scheme to be M2 but not M1.

PROPOSITION 5.3.1. *Suppose Σ satisfies the following conditions.*

(i) $\dim W(\Sigma) = \dim \operatorname{Sym}(V) - 1$.

(ii) There exists a separating quadratic form $Q \in \operatorname{Quad}(V^*)$ such that $Q(\pi_i) = 0$ for all $i = 1, \ldots, n$ while $Q(\pi_0) \neq 0$.

Then Σ has product reconstruction (is M2) but is not multiplicative (is not M1).

PROOF. Condition *(ii)* implies that Σ is not M1. The subspace $I(\Sigma) \subseteq \operatorname{Sym}(V)^*$ has dimension 1, so $I(\Sigma) = \langle Q \rangle$, where Q is the separating form in

Condition *(ii)*. Therefore, all non-zero elements in $I(\Sigma)$ are separating, which implies that Σ is M2 by Proposition 5.2.2. □

At this point, we can apply this sufficient condition to present the first example of a linear secret sharing scheme that is M2 but not M1. Take $q = 5$ and $V = \mathbb{F}_5^5$, and fix a basis of V. Consider the symmetric bilinear form $T \in \mathrm{Sym}(V^*)$ that is represented by the 5×5 identity matrix and the quadratic form Q that is determined by T. Obviously, $\operatorname{rk} Q = 5$, and hence Q is separating by Proposition 5.2.4. Our example is a linear secret sharing scheme Σ among $n = 14$ players such that $\dim W(\Sigma) = \dim \mathrm{Sym}(V) - 1 = 14$ and $I(\Sigma) = \langle Q \rangle$. That is, we have to find $\pi_0, \ldots, \pi_{14} \in V^*$ such that $\{\pi_i \otimes \pi_i : i = 1, \ldots, 14\}$ is linearly independent, $Q(\pi_i) = 0$ for all $i = 1, \ldots, 14$, and $Q(\pi_0) \neq 0$. Then Σ is M2 but not M1 by Proposition 5.3.1. A suitable choice for $(\pi_0, \ldots, \pi_{14})$ is given by the column vectors of the following matrix.

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 2 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 3 & 0 & 0 & 0 \\ 1 & 0 & 2 & 0 & 0 & 2 & 0 & 0 & 1 & 1 & 0 & 0 & 3 & 0 & 0 \\ 1 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 2 & 0 & 1 & 0 & 0 & 3 & 0 \\ 2 & 0 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 2 & 2 & 0 & 0 & 0 & 3 \end{pmatrix}.$$

It is easy to see that Σ achieves 2-privacy.

We use again Proposition 5.3.1 to present a similar example over $\mathbb{F}_2$. Take $V = \mathbb{F}_2^5$ and fix a basis for V. Consider the quadratic form $Q \in \mathrm{Quad}(V^*)$ defined by the bilinear form T with matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Observe that Q is separating because it has rank 5. Reasoning as in the previous example we obtain that the linear secret sharing scheme determined by the matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

is M2 but not M1.

Similarly to the first one, the following example is again linear secret sharing scheme Σ with dimension $k = 5$ over $\mathbb{F}_5$, but in this case the number of players

is reduced to $n = 13$. This is achieved by taking $\dim I(\Sigma) = 2$. Consider the quadratic forms $Q_1, Q_2 \in \mathrm{Quad}(V^*)$ determined by the symmetric bilinear forms with matrices

$$M_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 2 \end{pmatrix}, \qquad M_2 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 2 & 0 \\ 0 & 1 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix},$$

respectively. One can check that all nonzero linear combinations of these two matrices have rank 5. As a consequence, all nonzero forms in $\langle Q_1, Q_2 \rangle$ have rank 5, and hence they are separating. Next, we present a linear secret sharing scheme Σ among 13 players such that it is not M1 and $I(\Sigma) = \langle Q_1, Q_2 \rangle$. Clearly, Σ is M2. A possible choice is given by the columns of the matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 2 & 3 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 4 & 1 & 1 & 4 \\ 0 & 0 & 0 & 2 & 3 & 0 & 0 & 1 & 3 & 3 & 1 & 4 & 1 & 4 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 3 & 1 & 1 & 1 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 3 & 0 & 3 & 2 & 0 & 0 & 4 & 4 \end{pmatrix}.$$

There exist separating quadratic forms of rank 4, and they have been characterized in Proposition 5.2.5. Therefore, we can apply Proposition 5.3.1 to find examples with dimension $k = 4$ on $9 = k(k+1)/2 - 1$ players. In each of the three following examples, we consider $V = \mathbb{F}_q^4$, where the characteristic of the field is different from 2, and a quadratic form $Q \in \mathrm{Quad}(V^*)$ that is determined by a symmetric matrix

$$D = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \alpha \end{pmatrix}.$$

Take $q = 3$ and $\alpha = -1$. As the determinant of D is not a square in $\mathbb{F}_3$, Q is separating. In addition, Q has at least 9 different zeros in $\mathbb{F}_3^4$, so we can construct a linear secret sharing scheme Σ among 9 players which is M2 but not M1. An example is

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 2 & 0 & 0 & 2 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 2 & 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 2 & 1 & 1 & 2 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

The previous example generalizes as follows. Take $\alpha = -1$ and a prime power q such that -1 is not a square in $\mathbb{F}_q$. As before, Q is separating. Observe that

$a^2 + b^2 \neq 0$ for every $a, b \in \mathbb{F}_q^*$ because -1 is not a square in $\mathbb{F}_q$. Therefore, there exist $a, b, c \in \mathbb{F}_q^*$ with $a^2 + b^2 + c^2 = 0$. The previous discussion implies that the matrix

$$\begin{pmatrix} 1 & 1 & 0 & 0 & -1 & 0 & 0 & -a & a & a \\ 0 & 0 & 1 & 0 & 0 & -1 & 0 & b & -b & b \\ 0 & 0 & 0 & 1 & 0 & 0 & -1 & c & c & -c \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

defines a linear secret sharing scheme Σ among 9 players that is M2 but not M1.

We now consider the case of a field $\mathbb{F}_q$ with $\operatorname{char} \mathbb{F}_q \neq 2$ containing a square root i of -1. Let α be a non-square in $\mathbb{F}_q$, and assume further that $\alpha \neq i$. Note that this choice is always possible, replacing i with $-i$ if necessary. Again, Q is separating and we find another linear secret sharing scheme that is M2 but not M1.

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 1 & \frac{\alpha+1}{2} & \frac{\alpha+1}{2} & 0 & \frac{\alpha+1}{2} \\ 0 & i & 0 & 1 & -i & 0 & \frac{i(\alpha-1)}{2} & 0 & \frac{\alpha+1}{2} & \frac{i(\alpha-1)}{2} \\ 0 & 0 & i & i & 0 & -i & 0 & \frac{i(\alpha-1)}{2} & \frac{i(\alpha-1)}{2} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & i & i & i & -i \end{pmatrix}.$$

Finally, we present another example on 9 players, this time over fields of characteristic 2. Let $\mathbb{F}_q = \mathbb{F}_2[\alpha]$, with $\alpha \notin \mathbb{F}_2$, be an arbitrary field extension of $\mathbb{F}_2$, and assume $\operatorname{Tr}(\alpha) = 1$. Note that it is always possible to choose such an α. So the form

$$Q = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & \alpha \end{pmatrix}$$

is separating and yields the separating scheme

$$\Sigma = \begin{pmatrix} 1 & 1 & 0 & 1 & \alpha^{1/2} & \alpha^{1/2} & \alpha^{1/2} & 1 & \alpha^2 & 1 \\ 1 & 0 & 1 & 1 & \alpha^{1/2} & \alpha^{1/2} & 1 & \alpha^{1/2} & 1 & \alpha^2 \\ 1 & 0 & 0 & 1 & 0 & 1 & \alpha^{1/2} & \alpha^{1/2} & \alpha & \alpha \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Note that in the case of $\mathbb{F}_q = \mathbb{F}_2$ we have $\alpha = \alpha^2 = \alpha^{1/2} = 1$ and this construction gives a scheme that is M1.

5.4 Composition and Proof of the Main Result

We discuss here how to obtain larger examples from small ones by using the composition of secret sharing schemes defined in Section 2.6.1. Recall that this

operation consists in substituting a player by several players by distributing its share using another secret sharing scheme. By using this tool and the examples in Section 5.3, we present proofs for Main Theorem 5.1.3 and Theorem 5.1.6.

Let V' and V'' be $\mathbb{F}$-vector spaces. Let $\Sigma' = (\pi'_0, \ldots, \pi'_{n'}) \subseteq (V')^*$ and $\Sigma'' = (\pi''_0, \ldots, \pi''_{n''}) \subseteq (V'')^*$ be secret sharing schemes. Let $\Sigma = \Sigma'[\Sigma''] = (\pi_0, \ldots, \pi_n) \subseteq V^*$ be the composition of Σ' with Σ'', where the vector space V as well as the linear forms π_i are defined as in Section 2.6.1.

We investigate how the multiplicativity properties of Σ' and Σ'' are inherited by their composition. As to the M1 property, recall that we have proved in Proposition 2.6.10 that if $\Sigma = \Sigma'[\Sigma'']$ is multiplicative in the sense of Definition 2.6.5 and $\Sigma'_{\{1,\ldots,n'-1\}}$ is not, then both Σ' and Σ'' are multiplicative. As to the M2 property, the following holds.

PROPOSITION 5.4.1. *If both Σ' and Σ'' have product reconstruction, then the composition $\Sigma = \Sigma'[\Sigma'']$ has product reconstruction too.*

PROOF. Suppose that Σ is not M2 and Σ'' is M2, and let us prove that Σ' is not M2. By Proposition 5.2.2 there exists a non-separating quadratic form $Q \in \mathrm{Quad}(V^*)$ such that $Q(\pi_i) = 0$ for all $i = 1, \ldots, n$ and $Q(\pi_0) \neq 0$. Consider the quadratic forms $Q' \in \mathrm{Quad}((V')^*)$ and $Q'' \in \mathrm{Quad}((V'')^*)$ defined by

$$Q'(\pi') = Q\left(\overline{(\pi', 0)}\right) \quad \text{and} \quad Q''(\pi'') = Q\left(\overline{(0, \pi'')}\right).$$

Observe that both Q' and Q'' are non-separating. Since Σ'' is M2 and $Q''(\pi''_j) = 0$ for every $j = 1, \ldots, n''$, we have that $Q''(\pi''_0) = 0$, hence

$$Q'(\pi'_{n'}) = Q(\tau_0) = Q''(\pi''_0) = 0,$$

where $\tau_0 := \overline{(\pi'_{n'}, 0)} = \overline{(0, \pi''_0)} \in V^*$. Therefore, Σ' is not M2 because $Q' \in \mathrm{Quad}((V')^*)$ is a non-separating quadratic form such that $Q'(\pi'_i) = 0$ for all $i = 1, \ldots, n'$ and $Q'(\pi'_0) = Q(\pi_0) \neq 0$. □

By composing Shamir's threshold secret sharing scheme with the small examples in Section 5.3, linear secret sharing schemes that are M2 but not M1 are obtained for an arbitrarily large number of players. Indeed, for every integer $t \geq 1$ and every prime power $q \geq 2t + 1$, Shamir's scheme among $2t + 1$ players, with t-privacy and $(t + 1)$-reconstruction, provides a multiplicative (M1) $\mathbb{F}_q$-linear secret sharing scheme Σ' with the additional property that, for every proper subset $I \subsetneqq \{1, \ldots, 2t + 1\}$, Σ'_I is not multiplicative. If Σ'' is one of the examples over $\mathbb{F}_q$ on 9 players in Section 5.3, then by Propositions 2.6.10 and 5.4.1 the composition $\Sigma = \Sigma'[\Sigma'']$ is an $\mathbb{F}_q$-linear secret sharing scheme on $n = 2t + 9$ players with t-privacy that is M2 but not M1.

The same idea can be used to construct examples for the notion of strong multiplication. For every integer $t \geq 1$ and every prime power $q \geq 3t + 1$,

a t-strongly multiplicative $\mathbb{F}_q$-linear secret sharing scheme Σ' on $n' = 3t+1$ players is obtained from Shamir's threshold scheme. Consider, as before, a scheme Σ'' conveniently chosen among the examples in Section 5.3 and the composition $\Sigma = \Sigma'[\Sigma'']$. Then, Σ is an $\mathbb{F}_q$-linear secret sharing scheme on $n = 3t+9$ players with t-privacy such that the scheme Σ_I is M2 for every set $I \subseteq \{1,\ldots,n\}$ of $n-t$ players, but Σ_J is not M1 for some set $J \subseteq \{1,\ldots,n\}$ with $n-t$ players.

The previous constructions prove neither Theorem 5.1.3 nor Theorem 5.1.6, but the proofs for those results are derived in a very similar way.

The algebraic geometric constructions from [11, 15, 19] provide, for every finite field $\mathbb{F}_q$ and for infinitely many values of $n' \in \mathbb{N}$, multiplicative (M1) linear secret sharing schemes Σ' over $\mathbb{F}_q$ on n' players that have t-privacy with $t = \Omega(n')$. By removing some players, we can assume that there is a player p_0 such that $\Sigma'_{\{1,\ldots,n'-1\}}$ is not M1. Let Σ'' be one of the schemes over $\mathbb{F}_q$ on 9 (or 14 if $q=2$) players presented in Section 5.3. Then the composition $\Sigma = \Sigma'[\Sigma'']$ is an $\mathbb{F}_q$-linear secret sharing scheme on $n = n'+8$ (or $n = n'+13$ if $q=2$) players that has t-privacy with $t = \Omega(n)$. By Propositions 2.6.10 and 5.4.1, The scheme Σ is M2 but not M1. This concludes the proof of Main Theorem 5.1.3.

The constructions from [11, 15, 19] provide as well, for every finite field $\mathbb{F}_q$ and for infinitely many values of $n' \in \mathbb{N}$, t-strongly multiplicative linear secret sharing schemes over $\mathbb{F}_q$ with $t = \Omega(n')$. Therefore, Theorem 5.1.6 can be proved similarly to Main Theorem 5.1.3.

5.5 The Smallest Examples

We presented in Section 5.3 examples of linear secret sharing schemes of dimension $k=4$ on 9 players that are M2 but not M1. The aim of this section is to prove Theorem 5.1.5, which implies that $n=9$ is the minimum required number of players in order to have a separation between the two multiplicativity notions.

We begin with some technical lemmas. We notate $\mathcal{P} = \{1,\ldots,n\}$ for the set of players and $\mathcal{P}_0 = \{0,1,\ldots,n\}$. An access structure Γ is $\mathcal{Q}_2$ if the set of players is not covered by any two rejecting sets. It is well-known that the access structure of every multiplicative (M1) linear secret sharing scheme is $\mathcal{Q}_2$, and it is easy to prove that the same applies to the M2 property.

LEMMA 5.5.1. *If a linear secret sharing scheme is M2, then its access structure is $\mathcal{Q}_2$.*

PROOF. Suppose that I and J with $I \cup J = \mathcal{P}$ are rejecting sets for $\Sigma = (\pi_0, \ldots, \pi_n) \subseteq V^*$. Then there exist $x, y \in V$ such that $\pi_0(x) = \pi_0(y) = 1$, while $\pi_i(x) = 0$ for every $i \in I$ and $\pi_j(y) = 0$ for every $j \in J$. By applying Proposition 5.2.2 to $x, y, x' = 0, y' = 0$, this implies that Σ is not M2. □

LEMMA 5.5.2. *Every 2-threshold linear secret sharing scheme among 3 players is M1.*

PROOF. Let $\Sigma = (\pi_0, \pi_1, \pi_2, \pi_3) \subseteq V^*$ be a 2-threshold linear secret sharing scheme. Then we can assume that $\dim V = 2$. Moreover, $\{\pi_i, \pi_j\}$ is linearly independent for every two different $i, j \in \mathcal{P}_0$. Therefore, there exists a basis of V such that, for some $a, b \in \mathbb{F}^*$ with $a \neq b$, the linear forms $(\pi_0, \pi_1, \pi_2, \pi_3)$ are given by the columns of the matrix

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & a & b \end{pmatrix}.$$

It is easy to check that Σ is M1. □

Given $\Sigma = (\pi_0, \ldots, \pi_n) \subseteq V^*$ and $I \subseteq \mathcal{P}$, the linear secret sharing scheme $\Sigma \setminus I$ is obtained from Σ by removing the players in I. This operation is called *puncturing*. For example, $\Sigma \setminus \{n\} = (\pi_0, \ldots, \pi_{n-1})$.

LEMMA 5.5.3. *Suppose that $\Sigma = (\pi_0, \ldots, \pi_n) \subseteq V^*$ is M2. If there exists a partition $\mathcal{P}_0 = I_0 \cup I_1$ with $0 \in I_0$ and $I_1 \neq \emptyset$ such that the span of $\{\pi_i : i \in I_0\}$ has trivial intersection with the span of $\{\pi_j : j \in I_1\}$, then the scheme $\Sigma \setminus I_1$ is also M2.*

PROOF. Suppose that $\Sigma \setminus I_1$ is not M2. Then there exist $x, y, x', y' \in V$ such that $Q_{x,y,x',y'}(\pi_i) = 0$ for every $i \in I_0 \setminus \{0\}$ and $Q_{x,y,x',y'}(\pi_0) \neq 0$. It is not difficult to check that we can select $x, y, x', y' \in V$ in such a way that $Q_{x,y,x',y'}(\pi_j) = 0$ for every $j \in I_1$. This implies that Σ is not M2. □

Given a tuple of vectors $(\pi_0, \ldots, \pi_n) \subseteq V^*$, a set $B \subseteq \mathcal{P}_0$ is said to be a *basis* (or an *independent set*) if $\{\pi_i : i \in B\}$ is a basis of V^* (or, respectively, it is linearly independent). The following is a well-known result from linear algebra and also matroid theory.

LEMMA 5.5.4. *Let $B, B' \subseteq \mathcal{P}_0$ be two different bases. Then the following properties are satisfied.*

1. *If $i \in B' \setminus B$, then $(B' \setminus \{i\}) \cup \{j\}$ is a basis for some $j \in B \setminus B'$.*
2. *If $i \in B' \setminus B$, then $(B \setminus \{j\}) \cup \{i\}$ is a basis for some $j \in B \setminus B'$.*

We proceed now with the proof of Theorem 5.1.5. Let $\Sigma = (\pi_0, \ldots, \pi_n) \subseteq V^*$ be a linear secret sharing scheme over $\mathbb{F}$ on $n \leq 8$ players. Suppose that Σ is M2. We want to prove that Σ is also M1.

The access structure of Σ is denoted by Γ and $\min\Gamma$ denotes the family of the minimal accepting sets. Take $k = \dim V$. We can suppose that $V^* = \langle \pi_i : i = 1, \ldots, n \rangle$. If there exists an accepting set formed by a single player, then Σ is M1. From now on, we assume that all accepting sets have at least two players.

Claim 5.5.5. *$k < n$.*

Proof. Obviously, $k \leq n$. If $k = n$, there exists a basis $B \subseteq \mathcal{P}_0$ with $0 \in B$. Then $\mathcal{P} = (B \setminus \{0\}) \cup \{j\}$ because $|B| = n - 1$. Therefore, $\mathcal{P}$ is the union of two rejecting sets and Γ is not $\mathcal{Q}_2$, a contradiction. □

We prove in Claim 5.5.7 that Σ is M1 if $k \leq 4$. We need the following lemma.

Lemma 5.5.6. *Assume $\dim V = 4$ and let $\{\pi_1, \ldots, \pi_4\}$ be an $\mathbb{F}$-basis of V^*. Let $Q_1, Q_2 \in \mathrm{Quad}(V^*)$ be linearly independent and such that $Q_j(\pi_i) = 0$ for all $i = 1, \ldots, 4$ and $j = 1, 2$. Then there exists $\lambda \in \mathbb{F}$ such that $Q_1 + \lambda Q_2$ is not separating.*

Proof. Let $U_1, U_2 \in \mathbb{F}^{4\times 4}$ be the unique upper-triangular matrices associated to Q_1 and Q_2, respectively, in the basis $\{\pi_1, \ldots, \pi_4\}$ of V^*. Then

$$U_1 = \left(\begin{array}{cc|cc} 0 & \alpha_1 & \multicolumn{2}{c}{\multirow{2}{*}{A_1}} \\ 0 & 0 & & \\ \hline \multicolumn{2}{c|}{\multirow{2}{*}{0}} & 0 & \beta_1 \\ \multicolumn{2}{c|}{} & 0 & 0 \end{array}\right), \qquad U_2 = \left(\begin{array}{cc|cc} 0 & \alpha_2 & \multicolumn{2}{c}{\multirow{2}{*}{A_2}} \\ 0 & 0 & & \\ \hline \multicolumn{2}{c|}{\multirow{2}{*}{0}} & 0 & \beta_2 \\ \multicolumn{2}{c|}{} & 0 & 0 \end{array}\right)$$

for some $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{F}, A_1, A_2 \in \mathbb{F}^{2\times 2}$. Reordering the basis, we may assume that $\alpha_2 \neq 0$. Take $\lambda = -\alpha_1/\alpha_2$. Then the matrix $U_3 = U_1 + \lambda U_2$ has rank at most 2, hence the bilinear form whose associated matrix is U_3 is of the form $x \otimes y - x' \otimes y'$ for some $x, y, x', y' \in \mathbb{F}^4$ and therefore $Q_1 + \lambda Q_2$ is not separating. □

Claim 5.5.7. *If $k \leq 4$, then Σ is M1.*

Proof. By Proposition 5.2.4, Σ is M1 if $k \leq 3$. Suppose that $k = 4$. Since $\dim \mathrm{Sym}(V) = 10$, we have that $\dim I(\Sigma) \geq 2$. By iterated application of Lemma 5.5.6, we can replace all separating forms in a basis of $I(\Sigma)$ with non-separating forms, obtaining a basis $\{Q_1, \ldots, Q_r\}$ of $I(\Sigma)$ consisting entirely of non-separating forms. Since Σ is M2, $Q_j(\pi_0) = 0$ for all $j = 1, \ldots, r$, and hence $\pi_0 \in W(\Sigma)$. Therefore, Σ is M1. □

From now on, we suppose that $5 \leq k \leq n-1$, and hence $6 \leq n \leq 8$. Take a set $B \subseteq \mathcal{P}_0$ such that $0 \in B$ and B is a basis (such a set always exists). Then $X = B \setminus \{0\} \notin \Gamma$, and hence $Y = \mathcal{P} \setminus X \in \Gamma$ because Γ is $\mathcal{Q}_2$. In addition, $|Y| = n - k + 1$.

CLAIM 5.5.8. *If Y is a minimal accepting set, then Σ is M1.*

PROOF. If Y is a minimal accepting subset, then Y is independent. Since π_0 is in the span of $\{\pi_j\}_{j \in Y}$, there exists $X_1 \subseteq X$ such that $B' = X_1 \cup Y$ is a basis. By Lemma 5.5.4, for every $i \in X \setminus X_1 \subseteq B \setminus B'$, there exists $j \in B' \setminus B = Y$ such that $B_i'' = (B \setminus \{i\}) \cup \{j\}$ is a basis. This implies that $B_i'' \setminus \{0\} = (X \setminus \{i\}) \cup \{j\}$ is not in Γ, and hence its complement $(Y \setminus \{j\}) \cup \{i\}$ is accepting. Then π_i is in the span of $\{\pi_\ell : \ell \in (Y \setminus \{j\}) \cup \{0\}\}$ because $Y \setminus \{j\} \notin \Gamma$, and hence π_i is in the span of $\{\pi_\ell\}_{\ell \in Y}$. Therefore, every vector π_i with $i \in \mathcal{P}_0 \setminus X_1$ is in the span of $\{\pi_\ell\}_{\ell \in Y}$. Take $X_0 = \mathcal{P}_0 \setminus X_1$. Since $X_1 \cup Y$ is a basis, the span of $\{\pi_i\}_{i \in X_0}$ has trivial intersection with the span of $\{\pi_j\}_{j \in X_1}$. Therefore, $\Sigma' = \Sigma \setminus \{X_1\}$ is M2 by Lemma 5.5.3. The dimension of Σ' is $k - |X_1| = n - k + 1 \leq 4$. Then Σ' is M1 by Claim 5.5.7, and hence so is Σ. □

CLAIM 5.5.9. *If $k = n - 1$, then Σ is M1.*

PROOF. Since $|Y| = n - k + 1 = 2$, we have that Y is a minimal accepting set. Apply Claim 5.5.8. □

As a consequence, Σ is M1 if $n = 6$. From now on, we assume that $7 \leq n \leq 8$ and $5 \leq k \leq n - 2$.

CLAIM 5.5.10. *If every pair $\{i, j\} \subseteq \mathcal{P}_0$ with $i \neq j$ is independent and $k = n-2$, then Σ is M1.*

PROOF. Without loss of generality, we can suppose that $B = \{0, 4, \ldots, n\}$ and $Y = \{1, 2, 3\}$. If Y is a minimal accepting set, then Σ is M1 by Claim 5.5.8. Otherwise, we can assume that $\{1, 2\} \in \min \Gamma$. If π_3 is in the span of $\{\pi_1, \pi_2\}$, then $\Sigma' = \Sigma \setminus (\mathcal{P} \setminus Y)$ is a $(2, 3)$-threshold scheme and Σ' is M1 by Lemma 5.5.2. This implies that Σ is M1. Otherwise, we can assume that $\{1, 2, 3, \ldots, n-2\}$ is a basis. Since π_0 is a linear combination of $\{\pi_1, \pi_2\}$, then $\{0, 2, 3, \ldots, n-2\}$ is a basis, and hence $\{1, n-1, n\} \in \Gamma$. If this is a minimal accepting set, then Σ is M1 by Claim 5.5.8. Since $B = \{0, 4, \ldots, n\}$ is a basis, $\{n-1, n\} \notin \Gamma$. Without loss of generality, we can assume that $\{1, n\} \in \Gamma$. Then $\Sigma \setminus (\mathcal{P} \setminus \{1, 2, n\})$ is a $(2, 3)$-threshold scheme, and hence Σ is M1. □

CLAIM 5.5.11. *If $k = n - 2$, then Σ is M1.*

PROOF. Suppose $n = 7$ and $k = 5$. If the pair $\{\pi_i, \pi_j\}$ is linearly dependent, then by removing (puncturing) one of these players an M2 LSSS on 6 players is obtained, which is also M1. Otherwise, Σ is M1 by Claim 5.5.10. The proof is analogous for the case $n = 8$ and $k = 6$. □

At this point, only the case $n = 8$, $k = 5$ remains unproven. Since every M2 linear secret sharing scheme on 7 players is M1, we can suppose that every pair $\{i, j\} \subseteq \mathcal{P}_0$ with $i \neq j$ is independent.

CLAIM 5.5.12. *Consider $Z \subseteq \mathcal{P}_0$ with $3 \leq |Z| \leq 4$ and $0 \in Z$. Let W be the span of $\{\pi_j\}_{j \in Z}$ and take $C = \{i \in \mathcal{P}_0 : \pi_i \in W\}$. If $|C| \geq |Z| + 3$, then Σ is M1.*

PROOF. Take $Z' \subseteq Z$ such that $\{\pi_j\}_{j \in Z'}$ is a basis of W. Take $A = \mathcal{P}_0 \backslash C \subseteq P$. By a simple case analysis, it is not difficult to check that there exist disjoint sets $A_1, A_2 \subseteq A$ such that $A_1 \cup A_2 = A$ and $\{\pi_j\}_{j \in Z' \cup A_i}$ is linearly independent for $i = 1, 2$.

Suppose that Σ is not M1. Then $\Sigma' = \Sigma \setminus A$ is not M1 and, since its dimension is $|Z'| \leq 4$, it is not M2. Then there exists a quadratic form $Q = Q_{x,y,x',y'} \in \text{Quad}(V^*)$ such that $Q(\pi_0) \neq 0$ while $Q(\pi_i) = 0$ for every $i \in C \setminus \{p_0\}$. Moreover, by basic linear algebra there exist vectors $u, v, u', v' \in V$ such that

- $\pi(u) = \pi(x)$, $\pi(v) = \pi(y)$, $\pi(u') = \pi(x')$, and $\pi(v') = \pi(y')$ for all $\pi \in W$, and
- $\pi_i(u) = \pi_i(u') = 0$ for every $i \in A_1$, and
- $\pi_j(v) = \pi_j(v') = 0$. for every $j \in A_2$.

Consider the quadratic form $Q' = Q_{u,v,u',v'}$. Observe that $Q'(\pi_i) = Q(\pi_i)$ if $i \in C$ and $Q'(\pi_j) = 0$ if $j \notin C$. This implies that Σ is not M2, a contradiction. □

Without loss of generality $B = \{0, 5, 6, 7, 8\}$ is a basis. Let $Y = \{1, 2, 3, 4\}$. Remember that Y is an accepting set. If Y is a minimal accepting set, then Σ is M1 by Claim 5.5.8. Otherwise, we distinguish two cases

Case 1 $\{1, 2, 3\}$ *is a minimal accepting set.* We consider two subcases, depending on whether π_4 is in the span of $\{\pi_1, \pi_2, \pi_3\}$ or not. If yes, we can assume that $\{1, 2, 3, 5, 6\}$ is a basis. Then every set of the form $\{0, x, y, 5, 6\}$ with $x, y \in \{1, 2, 3\}$ and $x \neq y$ is a basis, and hence every set of the form $\{i, 4, 7, 8\}$ with $i \in \{1, 2, 3\}$ is accepting. If one of them is a minimal accepting set, then Σ is M1 by Claim 5.5.8. Observe that $\{7, 8\} \notin \Gamma$ because $\{7, 8\} \subseteq B$.

If $\{i, 4, j\} \in \Gamma$ for some $i \in \{1, 2, 3\}$ and $j \in \{7, 8\}$ such that $\{i, 4\} \notin \Gamma$, then π_j is in the span of $\{\pi_0, \pi_i, \pi_4\}$ and Σ is M1 by Claim 5.5.12 with $Z = \{0, 1, 2\}$ (since π_3,π_4,π_j are in the span of $\{\pi_0, \pi_1, \pi_2\}$). If a set of the form $\{i, 7, 8\}$ with $i \in \{1, 2, 3, 4\}$ is accepting, then π_8 is in the span of $\{\pi_0, \pi_i, \pi_7\}$, and hence the dimension of the span of $\{\pi_0, \pi_1, \pi_2, \pi_3, \pi_4, \pi_7, \pi_8\}$ is at most 4. Again, Σ is M1 by Claim 5.5.12. Suppose now that π_4 is not in the span of $\{\pi_1, \pi_2, \pi_3\}$. Then we can assume that $\{1, 2, 3, 4, 5\}$ is a basis. By using a similar argument as before, every set of the form $\{i, 6, 7, 8\}$ with $i = 1, 2, 3$ is accepting. Since $\{6, 7, 8\}$ is not accepting, the vector π_i is in the span of $\{\pi_0, \pi_6, \pi_7, \pi_8\}$ for every $i = 1, 2, 3$. Apply Claim 5.5.12 with $Z = \{0, 6, 7, 8\}$.

Case 2 *All minimal accepting subsets of Y have exactly 2 players.* We can assume that $\{1, 2\} \in \Gamma$. By Lemma 5.5.2, we can assume that $\{\pi_1, \pi_2, \pi_3\}$ is linearly independent. Suppose that π_4 is in the span of $\{\pi_1, \pi_2, \pi_3\}$ and that $\{1, 2, 3, 5, 6\}$ is a basis. Then $B' = \{p_0, 2, 3, 5, 6\}$ is a basis and $Y' = \{1, 4, 7, 8\} \in \Gamma$. If Y' is a minimal accepting set or $\{1, 4\} \in \Gamma$, then Σ is M1. If there is a minimal accepting subset of Y' with cardinality 3, then we can reduce to Case 1. Since $\{7, 8\} \subseteq B$, this set is not accepting. The only remaining case is that there exists an accepting set $\{i, j\}$ with $i \in \{1, 4\}$ and $j \in \{7, 8\}$. Then π_j is in the span of $\{\pi_1, \pi_2, \pi_3\}$ and Σ is M1 by Claim 5.5.12. Suppose now that π_4 is not in the span of $\{\pi_1, \pi_2, \pi_3\}$. Then we can assume that $\{1, 2, 3, 4, 5\}$ is a basis. Then $B' = \{p_0, 2, 3, 4, 5\}$ is a basis and $Y' = \{1, 6, 7, 8\} \in \Gamma$. The proof is concluded by using a similar argument as before.

Bibliography

[1] Mark A. Abspoel. Shamir's scheme is the only strongly multiplicative LSSS with maximal adversary. Master's thesis, Universiteit Leiden, 2016. Preprint: `https://www.math.leidenuniv.nl/scripties/MasterAbspoel.pdf`.

[2] Christine Bachoc, Oriol Serra, and Gilles Zémor. An analogue of Vosper's Theorem for Extension Fields. *Math. Proc. Cambridge Philos. Soc.*, to appear. Preprint: `https://arxiv.org/pdf/1501.00602v1.pdf`, 2015.

[3] Stéphane Ballet and Julia Pieltant. On the Tensor Rank of Multiplication in Any Extension of $\mathbb{F}_2$. *J. Complex.*, 27(2):230–245, April 2011.

[4] Vincent Beck and Cédric Lecouvey. Additive combinatorics methods in associative algebras. Preprint: `https://arxiv.org/pdf/1504.02287v2.pdf`, 2015.

[5] Amos Beimel. *Secure Schemes for Secret Sharing and Key Distribution.* PhD thesis, Technion Haifa, 1996.

[6] Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, STOC '88, pages 1–10, New York, NY, USA, 1988. ACM.

[7] Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness Theorems for Non-cryptographic Fault-tolerant Distributed Computation. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, STOC '88, pages 1–10, New York, NY, USA, 1988. ACM.

[8] E. Berlekamp, R. J. McEliece, and H. van Tilborg. On the inherent intractability of certain coding problems (Corresp.). *IEEE Transactions on Information Theory*, 24(3):384–386, May 1978.

[9] Koichi Betsumiya, Stelios Georgiou, T. Aaron Gulliver, Masaaki Harada, and Christos Koukouvinos. On self-dual codes over some prime fields. *Discrete Mathematics*, 262(1):37 – 58, 2003.

[10] Andries E. Brouwer, Arjeh M. Cohen, and Arnold Neumaier. *Distance-regular graphs*. Ergebnisse der Mathematik und ihrer Grenzgebiete. Springer, 1989.

[11] Ignacio Cascudo, Hao Chen, Ronald Cramer, and Chaoping Xing. Asymptotically Good Ideal Linear Secret Sharing with Strong Multiplication over Any Fixed Finite Field. In Shai Halevi, editor, *Advances in Cryptology - CRYPTO 2009: 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2009. Proceedings*, pages 466–486. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.

[12] Ignacio Cascudo, Ronald Cramer, Diego Mirandola, Carles Padró, and Chaoping Xing. On secret sharing with nonlinear product reconstruction. *SIAM Journal on Discrete Mathematics*, 29(2):1114–1131, 2015.

[13] Ignacio Cascudo, Ronald Cramer, Diego Mirandola, and Gilles Zémor. Squares of Random Linear Codes. *IEEE Transactions on Information Theory*, 61(3):1159–1173, March 2015.

[14] Ignacio Cascudo, Ronald Cramer, Chaopin Xing, and An Yang. Asymptotic Bound for Multiplication Complexity in the Extensions of Small Finite Fields. *IEEE Transactions on Information Theory*, 58(7):4930–4935, July 2012.

[15] Ignacio Cascudo, Ronald Cramer, and Chaoping Xing. The Torsion-Limit for Algebraic Function Fields and Its Application to Arithmetic Secret Sharing. In Phillip Rogaway, editor, *Advances in Cryptology – CRYPTO 2011: 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings*, pages 685–705. Springer Berlin Heidelberg, Berlin, Heidelberg, 2011.

[16] Ignacio Cascudo, Ronald Cramer, and Chaoping Xing. The arithmetic codex. In *Information Theory Workshop (ITW), 2012 IEEE*, pages 75–79, Sept. 2012.

[17] Ignacio Cascudo, Ronald Cramer, and Chaoping Xing. Torsion Limits and Riemann-Roch Systems for Function Fields and Applications. *IEEE Transactions on Information Theory*, 60(7):3871–3888, July 2014.

[18] David Chaum, Claude Crépeau, and Ivan Damgård. Multiparty Unconditionally Secure Protocols. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, STOC '88, pages 11–19, New York, NY, USA, 1988. ACM.

[19] Hao Chen and Ronald Cramer. Algebraic Geometric Secret Sharing Schemes and Secure Multi-Party Computations over Small Fields. In Cynthia Dwork, editor, *Advances in Cryptology - CRYPTO 2006: 26th*

Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2006. Proceedings, pages 521–536. Springer Berlin Heidelberg, Berlin, Heidelberg, 2006.

[20] Hao Chen, Ronald Cramer, Shafi Goldwasser, Robbert de Haan, and Vinod Vaikuntanathan. Secure Computation from Random Error Correcting Codes. In Moni Naor, editor, *Advances in Cryptology - EUROCRYPT 2007: 26th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Barcelona, Spain, May 20-24, 2007. Proceedings*, pages 291–310. Springer Berlin Heidelberg, Berlin, Heidelberg, 2007.

[21] D. V. Chudnovsky and G. V. Chudnovsky. Algebraic complexities and algebraic curves over finite fields. *Journal of Complexity*, 4(4):285 – 316, 1988.

[22] Gérard Cohen, Iiro Honkala, Simon Litsyn, and Antoine Lobstein. *Covering Codes*. North-Holland Mathematical Library. Elsevier Science, 1997.

[23] Alain Couvreur, Philippe Gaborit, Valérie Gauthier-Umaña, Ayoub Otmani, and Jean-Pierre Tillich. Distinguisher-based Attacks on Public-key Cryptosystems Using Reed—Solomon Codes. *Des. Codes Cryptography*, 73(2):641–666, November 2014.

[24] Alain Couvreur, Philippe Gaborit, Valérie Gauthier-Umaña, Ayoub Otmani, and Jean-Pierre Tillich. Distinguisher-based attacks on public-key cryptosystems using Reed–Solomon codes. *Designs, Codes and Cryptography*, 73(2):641–666, 2014.

[25] Alain Couvreur, Ayoub Otmani, and Jean-Pierre Tillich. New Identities Relating Wild Goppa Codes. *Finite Fields Appl.*, 29:178–197, September 2014.

[26] Alain Couvreur, Ayoub Otmani, and Jean-Pierre Tillich. Polynomial Time Attack on Wild McEliece over Quadratic Extensions. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology – EUROCRYPT 2014: 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings*, pages 17–39. Springer Berlin Heidelberg, Berlin, Heidelberg, 2014.

[27] Ronald Cramer, Ivan Damgård, and Ueli Maurer. General Secure Multiparty Computation from any Linear Secret-Sharing Scheme. In Bart Preneel, editor, *Advances in Cryptology — EUROCRYPT 2000: International Conference on the Theory and Application of Cryptographic Techniques Bruges, Belgium, May 14–18, 2000 Proceedings*, pages 316–334. Springer Berlin Heidelberg, Berlin, Heidelberg, 2000.

[28] Ronald Cramer, Ivan B. Damgård, and Jesper B. Nielsen. *Secure Multiparty Computation and Secret Sharing*. Cambridge University Press, 2015.

[29] Jean Alexandre Dieudonné. *La géométrie des groupes classiques*. Ergebnisse der Mathematik und ihrer Grenzgebiete. Springer-Verlag, 1971.

[30] Arne Dür. The automorphism groups of Reed-Solomon codes. *Journal of Combinatorial Theory, Series A*, 44(1):69 – 82, 1987.

[31] Iwan M. Duursma and Ralf Kötter. Error-Locating Pairs for Cyclic Codes. *IEEE Transactions on Information Theory*, 40(4):1108–1121, 1994.

[32] Roger H. Dye. On the Arf invariant. *Journal of Algebra*, 53(1):36 – 39, 1978.

[33] Yoshimi Egawa. Association schemes of quadratic forms. *Journal of Combinatorial Theory, Series A*, 38(1):1 – 14, 1985.

[34] Jean-Charles Faugère, Valérie Gauthier-Umaña, Ayoub Otmani, Ludovic Perret, and Jean-Pierre Tillich. A Distinguisher for High-Rate McEliece Cryptosystems. *IEEE Transactions on Information Theory*, 59(10):6830–6844, Oct 2013.

[35] Matthew Franklin and Moti Yung. Communication Complexity of Secure Computation (Extended Abstract). In *Proceedings of the Twenty-fourth Annual ACM Symposium on Theory of Computing*, STOC '92, pages 699–710, New York, NY, USA, 1992. ACM.

[36] Xiang-Dong Hou, Ka Hin Leung, and Qing Xiang. A Generalization of an Addition Theorem of Kneser. *Journal of Number Theory*, 97(1):1 – 9, 2002.

[37] W. Cary Huffman and Vera Pless. *Fundamentals of Error-Correcting Codes*. Cambridge University Press, 2010.

[38] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, Manoj Prabhakaran, Amit Sahai, and Jürg Wullschleger. Constant-Rate Oblivious Transfer from Noisy Channels. In Phillip Rogaway, editor, *Advances in Cryptology – CRYPTO 2011: 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings*, pages 667–684. Springer Berlin Heidelberg, Berlin, Heidelberg, 2011.

[39] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Zero-knowledge from Secure Multiparty Computation. In *Proceedings of the Thirty-ninth Annual ACM Symposium on Theory of Computing*, STOC '07, pages 21–30, New York, NY, USA, 2007. ACM.

[40] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Zero-Knowledge Proofs from Secure Multiparty Computation. *SIAM Journal on Computing*, 39(3):1121–1152, 2009.

[41] Johannes H. B. Kemperman. On small sumsets in an abelian group. *Acta Mathematica*, 103(1):63–88, 1960.

[42] Martin Kneser. Abschätzung der asymptotischen Dichte von Summenmengen. *Mathematische Zeitschrift*, 58:459–484, 1953.

[43] Ralf Kötter. A Unified Description of an Error Locating Procedure for Linear Codes. In *Proceedings of the International Workshop on Algebraic and Combinatorial Coding Theory*, pages 113–117, Voneshta Voda, Bulgaria, 1992.

[44] Tsit-Yuen Lam. *Introduction to Quadratic Forms over Fields*. Number 67 in Graduate Studies in Mathematics. American Mathematical Soc., 2005.

[45] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer New York, 2005.

[46] A. Lempel, G. Seroussi, and S. Winograd. On the complexity of multiplication in finite fields. *Theoretical Computer Science*, 22(3):285 – 296, 1983.

[47] Rudolf Lidl and Harald Niederreiter. *Finite Fields*. Number 20, pt. 1 in EBL-Schweitzer. Cambridge University Press, 1997.

[48] Florence Jessie MacWilliams and Neil James Alexander Sloane. *The Theory of Error-correcting Codes*. North-Holland mathematical library. North-Holland Publishing Company, 1977.

[49] Irene Márquez-Corbella and Ruud Pellikaan. A Characterization of MDS Codes That Have an Error Correcting Pair. *Finite Fields Appl.*, 40(C):224–245, July 2016.

[50] James L. Massey. Minimal Codewords and Secret Sharing. In *Proceedings of the 6th Joint Swedish-Russian Workshop on Information Theory*, pages 269–79, Institutionen för informationsteori, Tekniska högsk. Lund, Sweden, 1993.

[51] James L. Massey. Some Applications of Coding Theory in Cryptography. In *Codes and Ciphers: Cryptography and Coding IV*, pages 33–47, 1995.

[52] R. J. McEliece. A Public-Key Cryptosystem Based On Algebraic Coding Theory. *DSN Progress Report*, 42–44:114–116, 1978.

[53] Diego Mirandola and Gilles Zémor. Critical Pairs for the Product Singleton Bound. *IEEE Transactions on Information Theory*, 61(9):4928–4937, Sept. 2015.

[54] Melvyn B. Nathanson. *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*. Graduate Texts in Mathematics. Springer New York, 1996.

[55] Harald Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information theory*, 15(2):159–166, 1986.

[56] Carles Padró. Lecture Notes in Secret Sharing. `https://mat-web.upc.edu/people/carles.padro/arc02v03.pdf`, 2013.

[57] Ruud Pellikaan. On decoding linear codes by error locating pairs. Preprint: `http://www.win.tue.nl/~ruudp/paper/15-ecp-preprint.pdf`, 1988.

[58] Ruud Pellikaan. On decoding by error location and dependent sets of error positions. *Discrete Mathematics*, 106:369 – 381, 1992.

[59] Ruud Pellikaan. On the Efficient Decoding of Algebraic-Geometric Codes. In P. Camion, P. Charpin, and S. Harari, editors, *Eurocode '92: International Symposium on Coding Theory and Applications*, pages 231–253. Springer Vienna, Vienna, 1993.

[60] Ruud Pellikaan. On the existence of error-correcting pairs. *Journal of Statistical Planning and Inference*, 51(2):229–242, 1996.

[61] Hugues Randriambololona. Bilinear Complexity of Algebras and the Chudnovsky-Chudnovsky Interpolation Method. *J. Complex.*, 28(4):489–517, August 2012.

[62] Hugues Randriambololona. An Upper Bound of Singleton Type for Componentwise Products of Linear Codes. *IEEE Transactions on Information Theory*, 59(12):7936–7939, Dec 2013.

[63] Hugues Randriambololona. Asymptotically Good Binary Linear Codes With Asymptotically Good Self-Intersection Spans. *IEEE Transactions on Information Theory*, 59(5):3038–3045, May 2013.

[64] Hugues Randriambololona. Linear independence of rank 1 matrices and the dimension of $*$-products of codes. In *2015 IEEE International Symposium on Information Theory (ISIT)*, pages 196–200, June 2015.

[65] Hugues Randriambololona. On products and powers of linear codes under componentwise multiplication. *Contemporary Mathematics, Algorithmic Arithmetic, Geometry, and Coding Theory*, 637:3–77, 2015.

[66] Jean-Pierre Serre. *A Course in Arithmetic*. Graduate texts in mathematics. Springer, 1973.

[67] Adi Shamir. How to Share a Secret. *Commun. ACM*, 22(11):612–613, November 1979.

[68] V. M. Sidelnikov and S. O. Shestakov. On insecurity of cryptosystems based on generalized Reed-Solomon codes. *Discrete Mathematics and Applications*, 2(4):439–444, 1992.

[69] Terence Tao and Van H. Vu. *Additive Combinatorics*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2006.

[70] J. H. van Lint and R. M. Wilson. On the minimum distance of cyclic codes. *IEEE Transactions on Information Theory*, 32(1):23–40, 1986.

[71] Jacobus Hendricus van Lint. *Introduction to Coding Theory*. Graduate Texts in Mathematics. Springer Berlin Heidelberg, 2013.

[72] A. G. Vosper. The Critical Pairs of Subsets of a Group of Prime Order. *Journal of the London Mathematical Society*, s1-31(2):200–205, 1956.

[73] Christian Wieschebrink. Two NP-complete Problems in Coding Theory with an Application in Code Based Cryptography. In *2006 IEEE International Symposium on Information Theory (ISIT)*, pages 1733–1737, July 2006.

[74] S. Winograd. Some bilinear forms whose multiplicative complexity depends on the field of constants. *Mathematical systems theory*, 10(1):169–180, 1976.

Summary

The product CD of two codes C and D is defined to be the span of all elements of the form xy, where x is in C, y is in D and the product is computed componentwise. The square C^2 of a code C is naturally defined as the product of C with itself. These notions, throughout the last forty years, have appeared in many different fields, such as cryptography, complexity theory, additive combinatorics and cryptanalysis. We show three main results on such products and discuss applications to cryptography. Our methods are typically algebraic-combinatorial in nature, though sometimes probabilistic techniques will be involved.

Our first purpose is to answer the following question: does the square of a code "typically" fill the whole space? We give a positive answer, for codes of dimension k and length roughly $k^2/2$ or smaller. Moreover, the convergence speed is exponential if the difference $k(k+1)/2 - n$ is at least linear in k. The proof uses random coding and combinatorial arguments, together with algebraic tools involving the precise computation of the number of quadratic forms of a given rank, and the number of their zeros. As a consequence of this work, it is impossible to rely on random codes in situations where properties of the code square are required, as it will be the full space, hence trivial, with high probability. This impacts for instance secret sharing: it is known that linear, non-multiplicative secret sharing schemes with optimal privacy and reconstruction parameters can be constructed using random codes; however, due to our results, such schemes will most likely not be arithmetic.

Our second result characterizes Product-MDS pairs of linear codes, i.e. pairs of codes C, D whose product under coordinatewise multiplication has maximum possible minimum distance as a function of the code length and the dimensions $\dim C, \dim D$. We prove in particular, for $C = D$, that if the square of the code C has minimum distance at least 2, and (C, C) is a Product-MDS pair, then either C is a generalized Reed-Solomon code, or C is a direct sum of self-dual codes. The proof is based on new coding-theory analogues of classical theorems of additive combinatorics, namely Kneser's and Vosper's Theorems. More

recently, these techniques have been used to prove that, among all t-strongly multiplicative secret sharing schemes on n players, only Shamir's scheme can achieve the optimal $t = (n-1)/3$.

Finally, we focus on a foundational question which is novel to the best of our knowledge. Multiplicative linear secret sharing is a fundamental notion in the area of secure multiparty computation and, since recently, in the area of two-party cryptography as well. In a nutshell, this notion guarantees that "the product of two secrets is obtained as a linear function of the vector consisting of the coordinatewise product of two respective share-vectors". Suppose we abandon the linearity condition and instead require that this product is obtained by some, not-necessarily-linear "product reconstruction function". Is the resulting notion equivalent to multiplicative linear secret sharing? We show the (perhaps somewhat counter-intuitive) result that this relaxed notion is strictly more general. Concretely, fix a finite field as the base field over which linear secret sharing is considered. Then we show there exists an (exotic) linear secret sharing scheme with an unbounded number of players n such that it has t-privacy with $t = \Omega(n)$ and such that it does admit a product reconstruction function, yet this function is necessarily nonlinear. In addition, we determine the minimum number of players for which those exotic schemes exist. Our proof is based on combinatorial arguments involving quadratic forms. It extends to similar separation results for important variations, such as strongly multiplicative secret sharing.

Samenvatting

Het product CD van twee codes C en D is gedefiniëerd als het lineair opspansel van alle elementen van de vorm xy, waar x een element van C is en y een element van D, en het product componentbewijs wordt berekend. Het kwadraat C^2 van een code C is op natuurlijke wijze gedefinieerd als het product van C met zichzelf. Deze begrippen zijn de laatste veertig jaar in verscheidene vakgebieden verschenen, zoals in de cryptografie, complexiteitstheorie, additieve combinatoriek en cryptanalyse. We bewijzen drie hoofdresultaten over deze producten en bespreken toepassingen op het gebied van de cryptografie. Onze methoden zijn hoofdzakelijk algebraïsch-combinatorisch, hoewel soms gebruik wordt gemaakt van probabilistische technieken.

Ons eerste doel is om de volgende vraag te beantwoorden: vult het kwadraat van een code "normaliter" de hele ruimte op? We geven een bevestigend antwoord voor codes van dimensie k en lengte ruwweg $k^2/2$ of kleiner. Bovendien is de snelheid van convergentie exponentieel als het verschil $k(k+1)/2 - n$ op zijn minst lineair is in k. Het bewijs gebruikt random codes en combinatorische argumenten, samen met algebraïsche tools die een precieze berekening van het aantal kwadratische vormen van een gegeven rang, samen met hun aantal nulpunten, erbij betrekken. Als gevolg van dit resultaat is het niet mogelijk om random codes te gebruiken in situaties waar bepaalde eisen zijn aan het kwadraat van de code, gezien dat dit met hoge waarschijnlijkheid de hele ruimte zal zijn. Dit heeft gevolgen voor bijvoorbeeld secret sharing: het is bekend dat lineaire, niet-multiplicatieve secret-sharingschema's met optimale privacy- en reconstructieparameters geconstrueerd kunnen worden met random codes; gezien onze resultaten echter, zullen deze schema's hoogstwaarschijnlijk niet aritmetisch zijn.

Ons tweede resultaat karakteriseert product-MDS-paren van lineaire codes, dat wil zeggen paren van codes C, D wier product onder coördinaatsgewijze vermenigvuldiging een maximale minimumafstand heeft als functie van de lengte van de code en de dimensies $\dim C, \dim D$. We bewijzen in het bijzonder voor het geval $C = D$, dat als het kwadraat van de code C een minimumafstand

van op zijn minst 2 heeft, en (C, C) een product-MDS-paar is, dat C ofwel een gegeneraliseerde Reed-Solomoncode is, ofwel C een directe som is van zelfduale codes. Het bewijs is gebaseerd op nieuwe coderingstheoretische analoga van klassieke stellingen uit de additieve combinatoriek, te weten de stellingen van Kneser en Vosper. Recentelijk zijn deze technieken gebruikt om aan de tonen dat, onder alle t-sterk multiplicatieve secret-sharingschema's met n spelers, alleen Shamirs schema de optimale $t = (n-1)/3$ kan bereiken.

Tenslotte richten we ons op een fundamentele vraag die naar ons beste weten nieuw is. Multiplicatieve lineaire secret sharing is een fundamenteel begrip op het gebied van secure multiparty computation, en sinds kort ook op het gebied van twee-spelercryptografie. Kort gezegd geeft dit begrip een garantie dat "het product van twee geheimen verkregen kan worden als een lineaire functie van de vector die bestaat uit het coördinaatsgewijze product van twee respectievelijke share-vectoren". Neem nu aan dat we de conditie van lineariteit laten varen en in plaats daarvan vereisen dat dit product verkregen kan worden door een bepaalde, niet noodzakelijkerwijs lineaire, "productreconstructiefunctie". Is de resulterende notie equivalent met multiplicatieve lineaire secret sharing? We laten het (wellicht contra-intuïtieve) resultaat zien dat deze versoepelde notie een strikte veralgemenisering is. Concreet gezien, neem een eindig lichaam als basislichaam waarover lineaire secret sharing wordt beschouwd. We laten dan zien dat er een (exotisch) lineair secret-sharingschema over dit basislichaam bestaat met een onbegrensd aantal spelers n zodat het t-privacy heeft met $t = \Omega(n)$, en zodat het een productreconstructiefunctie toelaat, waar deze functie noodzakelijkerwijs niet-lineair is. Daarbovenop bepalen we het minimum aantal spelers waarvoor deze exotische schema's bestaan. Ons bewijs is gebaseerd op combinatorische argumenten die betrekking hebben op kwadratische vormen. Het heeft uitbreidingen naar onderscheidingsresultaten voor vergelijkbare versoepelde condities, zoals in het geval van sterk multiplicatieve secret sharing.

Résumé

Le produit CD de deux codes C et D est défini comme l'espace vectoriel engendré par tous les éléments de la forme xy, où x appartient à C, y appartient à D et le produit est effectué coordonnée par coordonnée. Le carré C^2 d'un code C est naturellement défini comme le produit de C par lui-même. Au cours des quarante dernières années, ces notions ont régulièrement fait des apparitions dans différents domaines, comme la cryptographie, la théorie de la complexité, la combinatoire additive et la cryptanalyse. Nous démontrons trois principaux résultats sur les produits de codes et discutons de leurs applications à la cryptographie. Nos méthodes combinent des considérations algébriques et combinatoires, mais parfois des techniques probabilistiques seront également impliquées.

Pour notre premier résultat, notre but principal est de répondre à la question suivante : le carré d'un code "typique", remplit-il l'espace tout entier ? Nous donnons une réponse affirmative, pour des codes de dimension k et de longueur qui ne dépasse pas à peu près $k^2/2$. De plus, la vitesse de convergence vers 1 de la probabilité de cet événement est exponentielle si la différence $k(k+1)/2-n$ est au moins linéaire en k. La preuve utilise du codage aléatoire et des arguments combinatoires, avec des outils algébriques qui impliquent le calcul précis du nombre de formes quadratiques de rang donné, et le nombre de leurs zéros. Comme conséquence de ce travail, il résulte qu'il est impossible de compter sur les codes aléatoires dans des situations où il est nécessaire d'exploiter des propriétés du carré d'un code, car celui-ci sera l'espace entier - donc trivial - avec grande probabilité. Ceci a un impact, par exemple, sur le partage de secret : il est connu que les schémas de partage de secret linéaires non multiplicatifs avec privacy et paramètres de reconstruction optimaux peuvent être construits en utilisant des codes aléatoires ; cependant, nos résultats démontrent que ces schémas seront très probablement non arithmétiques.

Notre deuxième résultat caractérise les paires de codes linéaires Produit-MDS, c'est-à-dire les paires de codes C, D dont le produit coordonnée par coordonnée a la distance minimale la plus grande possible, la longueur des codes et les

dimensions $\dim C, \dim D$ étant fixées. En particulier, nous prouvons que pour $C = D$, si le carré du code C a une distance minimale au moins 2 et (C, C) est une paire Produit-MDS, alors soit C est un code de Reed-Solomon généralisé, soit C est une somme directe de codes autoduaux. La preuve est basée sur des nouveaux résultats de théorie des codes, analogues aux théorèmes classiques de combinatoire additive, notamment ceux de Kneser et de Vosper. Plus récemment, ces techniques ont été utilisées pour montrer que, parmi tous les schémas t-fortement multiplicatifs de partage de secret entre n joueurs, seul le schéma de Shamir peut atteindre le $t = (n-1)/3$ optimal.

Enfin, nous nous concentrons sur une question qui à notre connaissance est nouvelle. Le partage de secret linéaire multiplicatif est une notion fondamentale dans le domaine du calcul sécurisé à plusieurs participants et, depuis peu, dans le domaine de la cryptographie à deux participants aussi. En bref, cette notion guarantit que "le produit de deux secrets est obtenu comme une fonction linéaire du vecteur qui consiste en le produit coordonnée par coordonnée des deux vecteurs de partage respectifs. Supposons que nous renoncions à la condition de linéarité afin de demander plutôt que ce produit soit obtenu par une "fonction de reconstruction du produit" pas forcément linéaire. La notion résultante, est-elle équivalente au partage de secret linéaire ? Nous démontrons le résultat (peut-être quelque peu contre-intuitif) que cette notion relaxée est strictement plus générale. Concrétement, fixons un corps fini comme corps de base sur lequel le partage de secret est défini. Alors nous montrons qu'il existe un schéma de partage de secret linéaire (exotique) avec un nombre illimité de joueurs n, muni de t-privacy avec $t = \Omega(n)$ et qui admet une fonction de reconstruction du produit: mais cette fonction est nécessairement non linéaire. En outre, nous déterminons le nombre minimum de joueurs pour lesquels ces schémas exotiques existent. Notre preuve est basée sur des arguments combinatoires qui impliquent les formes quadratiques. Elle s'étend à des résultats de séparation pour des variations importantes, tels que le partage de secret fortement multiplicatif.

Acknowledgments

In my experience as a Ph.D. candidate, I had the privilege of working with two of the highest experts in my field of interest, namely Ronald Cramer and Gilles Zémor. Ronald, your non-constant presence had the twofold effect of teaching me that a scientist needs to be independent, but at the same time can count on other scientists as sources of ideas: and you are an endless one. Gilles, during my stay in Bordeaux we regularly spent infinite hours in your office, staring at your whiteboard and working not as a supervisor with his student, but as peers. This wonderful combination of different ways to play the role of supervisor allowed me to make the best out of this experience, and I am grateful for that. On top of that, I had the pleasure to share out-of-office situations with both of you: this should be a mandatory part of your role in my opinion, thank you for doing it spontaneously.

The paternity of two thirds of the content of this thesis is shared with Ignacio Cascudo. Nacho, you were the first person who welcomed me when I arrived at CWI and the best possible co-supervisor for the first year and a half of my career. Thank you for all the mathematical discussions we had and for guiding me through my first steps as a Ph.D. candidate.

This thesis would never have existed as a concrete book without the support of my colleague and friend Gabriele Spini. Gabriele, thank you for teaching me the existence and, through your example, the meaning of the word "dependable". And congratulations for your Ph.D..

The Cryptology group at CWI was the perfect setting for these four years of hard work. I am grateful to all people who have been part of the group throughout these years and who have shared with me their knowledge, or even just a lunch. I thank also all CWI people who were present at any of my well-deserved breaks: all people I shared a coffee with, all people I played football or table-football with, all people I met at a Praethuys or at a gaming night.

Ringrazio le persone conosciute in questi anni e che, ciascuno a proprio modo, mi hanno aiutato a continuare questo difficile percorso. Un pensiero spe-

ciale è dedicato ai miei amici Alberto, Giovanni, Giuseppe, Marcello, Nicola e Samuele: la lontananza da casa è sempre stata per me un peso, il mio più profondo ringraziamento per essere stati la mia seconda famiglia. Grazie a Andrea, Emanuele, Fortunato, Luca, Marco, Rosanna e Tommaso, incontri virtuali trasformatisi in amicizie reali.

Ho la fortuna di avere in Italia una famiglia, degli amici, e una città pronti ad abbracciarmi a ogni mio ritorno e a salutarmi a ogni mia ripartenza. A tutti voi, grazie per essere un motivo per tornare. A Maddalena, grazie per esserci sempre stata per me. A Giacomino, grazie per credere in me anche più di quanto non creda io stesso. Ad Anna, scusa per essermi perso i sei anni più belli della tua vita: spero che un giorno tu possa capire quanto questa scelta sia stata difficile ma allo stesso tempo importante, e magari trarne ispirazione. A Matteo, semplicemente grazie: non c'è altro da aggiungere per chi è allo stesso tempo un cugino, un fratello e un migliore amico.

Concludo ringraziando Madre e Padre per aver sopportato la mancanza del loro unico figlio: posso solo dirvi che è stato difficile per me almeno quanto lo è stato per voi, e che sono tornato.

Curriculum Vitae

Diego Mirandola was born on the 14th of November 1988 in Verona, Italy. He grew up in the nearby town of Caldiero, and obtained his high school diploma from the "Liceo Scientifico A. Messedaglia" in 2007.

He then started his Bachelor in Mathematics at the University of Padua, Italy (Università degli Studi di Padova), obtaining the corresponding diploma in 2010. During these years, he was supported by a grant from INdAM, the Italian National Institute of High Mathematics.

That same year he was accepted in the Algant-Master program, a double-degree Erasmus Mundus project; he spent the first year (2010-2011) at the University of Stellenbosch, South Africa, and the second year (2011-2012) at the University of Bordeaux, France – then Université de Bordeaux 1. He wrote his master thesis, with title "Schur products of linear codes: a study of parameters", under the supervision of Professor Gilles Zémor from the University of Bordeaux, obtaining his master degree in 2012.

In 2012 he was awarded an ALGANT-Doc joint Ph.D. fellowship to continue his studies in Mathematics at Universiteit Leiden, the Netherlands, and Université de Bordeaux, under the supervision of Prof. Dr. Ronald Cramer and Prof. Dr. Gilles Zémor (Bordeaux), in cooperation with the Centrum Wiskunde & Informatica (CWI) of Amsterdam, the Netherlands.

Publications

I. Ignacio Cascudo, Ronald Cramer, Diego Mirandola, Carles Padró, and Chaoping Xing. On secret sharing with nonlinear product reconstruction. *SIAM Journal on Discrete Mathematics*, 29(2):1114–1131, 2015.

II. Ignacio Cascudo, Ronald Cramer, Diego Mirandola, and Gilles Zémor. Squares of Random Linear Codes. *IEEE Transactions on Information*

Theory, 61(3):1159–1173, March 2015.

III. Diego Mirandola and Gilles Zémor. Critical Pairs for the Product Singleton Bound. *IEEE Transactions on Information Theory*, 61(9):4928–4937, Sept. 2015.