On products of linear error correcting codes

Mirandola, D.

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

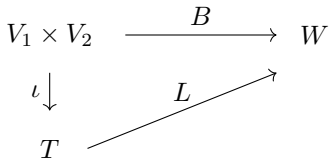
In this section we refresh some basic notions from the theory of bilinear forms and establish a correspondence between bilinear forms and tensor products that will be useful in the future. Most of the material can be found in textbooks like [45].

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

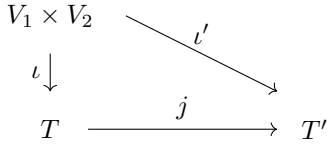
$$B(v_1, \cdot)\colon \begin{array}{ccc} V_2 & \longrightarrow & W \\ y & \longmapsto & B(v_1, y) \end{array} \qquad B(\cdot, v_2)\colon \begin{array}{ccc} V_1 & \longrightarrow & W \\ x & \longmapsto & B(x, v_2) \end{array}$$

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 $\mathbb{F}$.