Shamir's scheme is the only strongly multiplicative LSSS with maximal adversary

Abspoel, M.A.

Mathematisch Instituut, Universiteit Leiden

Shamir's scheme is the only strongly multiplicative LSSS with maximal adversary

Master's thesis of:
Mark A. Abspoel

Thesis advisors:
prof.dr. Ronald Cramer
Diego Mirandola, MSc

Date of defense: 15 September 2016

Abstract

We consider linear secret sharing schemes (LSSS) over a finite field K with the shares in K. An LSSS with t-adversary and n players is strongly multiplicative if it has $(n-t)$-product reconstruction. It is well-known that for strongly multiplicative LSSS with the secret in K it holds that $t \leq \frac{n-1}{3}$. This bound is sharp, as equality can be attained using Shamir's scheme. We show that in fact Shamir's scheme is the only strongly multiplicative LSSS with maximal adversary t.

We generalize this result to strongly multiplicative LSSS with the secret in an extension field L over K of finite degree k. We show that it holds that $t \leq \frac{n-2k+1}{3}$, and that equality can be attained using an extension of Shamir's scheme, where we take the evaluation point of the secret in L. We also show that this scheme is the only one that attains maximal t.

We build on earlier work by Mirandola and Zémor from 2015, who showed a coding-theoretic version of Vosper's theorem, a classical result from additive combinatorics. This theorem states in particular that a linear MDS code C of length n is Reed-Solomon if the dimension of its Schur square C^{*2} satisfies $2 < \dim C^{*2} = 2\dim C - 1 < n - 1$. We discuss whether this theorem also applies to non-MDS linear codes, and in doing so we provide a slight generalization of the theorem. We also prove that non-MDS codes C exist with $\dim C^{*2} = 2\dim C - 1$ and with C of arbitrary codimension, using the amalgamated direct sum of codes.

As a second coding-theoretic application of the analogue of Vosper's theorem, we show an implication for error-correcting pairs. It was shown by Márquez-Corbella and Pellikaan in 2016 that existence of a t-error correcting pair for an MDS code C implies that C is Reed-Solomon. They gave two separate proofs. Besides their original proof, they gave a second proof that indirectly uses the analogue of Vosper's theorem. We show an alternative proof directly from this theorem.

1 Introduction

Secret sharing is the dispersal of secret information over n players, such that each player gets a *share* of the information, and together they can use their shares to reconstruct the secret. The canonical example is Shamir's secret sharing scheme [Sha79], which works as follows.

Let K be a publicly-known finite field, and suppose a *dealer* holds a secret element $s \in K$. To share the secret among $n \leq |K|$ players numbered by $1, \ldots, n$, the dealer selects a uniformly random polynomial $f \in K[X]$ of degree $\leq t$ such that $f(0) = s$, and gives each player i a share $x_i = f(i)$. The scheme offers $(t+1)$-reconstruction, which means that a coalition of $\geq t+1$ players can reconstruct s with their shares. To accomplish this, they use Lagrange interpolation to find f, and thus the secret $s = f(0)$. It also offers t-privacy: given at most t shares they jointly do not give information about s. To see this, fix shares $x_{p_1}, \ldots, x_{p_t}$ for players $p_1, \ldots, p_t$, respectively. For every $s' \in K$ there exists a polynomial f' of degree at most t that runs through the points (p_j, x_{p_j}) for $j = 1, \ldots, t$ and $(0, s')$, and in fact the number of such polynomials f' is the same for every $s' \in K$.

We can describe this secret sharing scheme with the following set.

$$C := \left\{ (s, x_1, \ldots, x_n) \in K^{n+1} \;\middle|\; (x_1, \ldots, x_n) \text{ is a vector of shares for the secret } s \right\} \quad (1)$$

We have that $C \subseteq K^{n+1}$ is a subset, and in fact for Shamir's scheme it is closed under K-linear combinations. This makes it a linear code of length $n+1$, i.e a K-vector

subspace of the $(n+1)$-dimensional vector space K^{n+1}. Secret sharing schemes for which C is linear are called linear secret sharing schemes (LSSS).

For Shamir's scheme, the code C is called a Reed-Solomon code. Let $K[X]_{\leq t}$ denote the set of all polynomials in $K[X]$ of degree at most t, and for a polynomial $f \in K[X]_{\leq t}$ define $f(\infty)$ to be the coefficient of X^t. Reed-Solomon codes are those of the following form

$$\left\{(y_0 f(\alpha_0), \ldots, y_n f(\alpha_n)) \in K^{n+1} \;\middle|\; f \in K[X]_{\leq t}\right\}$$

for non-zero $y_0, \ldots, y_n \in K$ and distinct $\alpha_0, \ldots, \alpha_n \in K \cup \{\infty\}$.

Shamir's scheme is an example of a linear secret sharing scheme (LSSS), where the elements of C in Equation (1) form a K-vector space. Since the players can reconstruct the secret, we may also view such a scheme as a K-linear map $\psi : C' \to K$, where C' is the projection of C onto its last n coordinates. The secret sharing scheme having r-reconstruction if equivalent to ψ being r-wise determined. The latter means that for every set of coordinates $\{b_1, \ldots, b_r\} \subseteq \{1, \ldots, n\}$ of size $|B| = r$ we have that $\psi(\mathbf{x}) = 0$ for every $\mathbf{x} = (x_1, \ldots, x_n) \in C'$ with $(x_{b_1}, \ldots, x_{b_r}) = (0, \ldots, 0)$.

Arithmetic secret sharing schemes are LSSS with multiplicative properties. These properties enable the construction of secure multi-party computation (MPC) protocols. In MPC, n players each hold pieces of input data for a function, and they wish to compute the output of this function while keeping the inputs private.

For $\mathbf{x} = (x_1, \ldots, x_n), \mathbf{y} = (y_1, \ldots, y_n) \in K^n$ denote the coordinate-wise product by $\mathbf{x} * \mathbf{y} = (x_1 y_1, \ldots, x_n y_n)$. For a K-vector subspace $C \subseteq K^n$ let $C^{*2} := K\langle \mathbf{x} * \mathbf{y} \;\middle|\; \mathbf{x}, \mathbf{y} \in C \rangle$ be the K-linear span of the coordinate-wise products of all pairs of vectors in C. For $B \subseteq \{1, \ldots, n\}$ a set of coordinates, write $\pi_B : K^n \to K^{|B|}$ for the projection map, and for a vector $\mathbf{x} \in K^n$ denote its image under π_B by $\mathbf{x}_B := \pi_B(\mathbf{x})$.

Definition 1.1. Let n, t, r be integers with $1 \leq t < r \leq n$, K be a finite field, and A be a finite-dimensional non-trivial K-algebra. An $(n, t, 2, r)$-*arithmetic secret sharing scheme* (C, ψ) of A over K is a K-vector subspace $C \subseteq K^n$ and a surjective K-linear map $\psi : C \to A$, such that we have:

- (t-*privacy*) For each set of coordinates $B \subseteq \{1, \ldots, n\}$ of size $|B| = t$, and for each $s \in A$ and $\mathbf{y} \in \pi_B(C)$, there is some $\mathbf{x} \in C$ with $\psi(\mathbf{x}) = s$ and $\mathbf{x}_B = \mathbf{y}$.
- ($(2, r)$-*multiplicativity*) There is a unique K-linear map $\overline{\psi} : C^{*2} \to A$ such that:
  1. For each $\mathbf{x}, \mathbf{y} \in C$ we have $\overline{\psi}(\mathbf{x} * \mathbf{y}) = \psi(\mathbf{x}) \cdot \psi(\mathbf{y})$.
  2. $\overline{\psi}$ is r-wise determined

Given an $(n, t, 2, r)$-arithmetic secret sharing scheme for K over K, one can construct an MPC protocol secure against a passive adversary, where the players follow the protocol correctly and the adversary can only observe, and not change, the data accessible by up to t players. Let $f : K^n \to K^n$ be any function, and suppose each player p_i holds input x_i to the function, and wishes to learn the output y_i, where $(y_1, \ldots, y_n) = f(x_1, \ldots, x_n)$. Assume each pair of players have a private communication channel. It is now possible to construct a protocol that allows each player to learn their desired output, and such that any adversary that can see the inputs and outputs x_i, y_i of up to t players, learns nothing other than what can be computed from just these values [CDN15].

Secret sharing with an arithmetic secret sharing works as follows. When a dealer wants to share a secret $s \in A$ in this arithmetic secret sharing scheme, he or she selects a

uniformly random preimage $\mathbf{x}$ from $\psi^{-1}(s)$, and distribute each coordinate x_i to player i. We see that this scheme offers t-privacy as follows. Fix t shares $(y_{p_i})_{i=1}^t$ for players $p_1, \ldots, p_t$. Then for every secret $s \in A$ there is at least one matching codeword $\mathbf{x} \in C$ with $\mathbf{x}_B = (y_b)_{b \in B}$ and $\psi(\mathbf{x}) = s$. In particular by linearity of ψ the number of such matching codewords is the same for each $s \in A$. $\overline{\psi}$ being r-wise determined ensures that given r coordinates of a vector $\mathbf{x} \in C^{*d}$ its image under $\overline{\psi}$ is uniquely determined. If $\mathbf{y} \in C^{*d}$ is any vector with $\mathbf{x}_B = \mathbf{y}_B$, then $\overline{\psi}(\mathbf{y} - \mathbf{x}) = 0$ so $\overline{\psi}(\mathbf{x}) = \overline{\psi}(\mathbf{y})$.

Shamir's scheme as defined above gives an $(n, t, 2, n)$-arithmetic secret sharing scheme if $t < \frac{n}{2}$. Let $s, s' \in K$ be secrets with associated polynomials $f, g \in K[X]_{\leq t}, f(0) = s, g(0) = s'$, and $x_i = f(i), y_i = g(i)$ be the corresponding shares. We have $(2t+1)$-reconstruction for the product ss', since fg is a polynomial of degree at most $2t$. By linearity this guarantees $(2, 2t+1)$-multiplicativity.

As in Equation (1), for an arithmetic secret sharing scheme (C, ψ) we have a K-vector subspace

$$\widetilde{C} := \left\{ (\psi(\mathbf{x}), \mathbf{x}) \;\middle|\; \mathbf{x} \in C \right\} \subseteq A \times K^n$$

Recall that for $A = K$ we had that Shamir's scheme was given by a Reed-Solomon code. We will phrase this more precisely in the context of arithmetic secret sharing schemes.

Definition 1.2. Let K be a finite field. We say an arithmetic secret sharing scheme (C, ψ) for K over K is *given by Shamir's scheme* if $\widetilde{C}$ is a Reed-Solomon code.

The older notion of a strongly multiplicative LSSS (see e.g. [CDM00]) is equivalent to an $(n, t, 2, r)$-arithmetic secret sharing scheme with $r \leq n - t$. This condition enables the construction of an MPC protocol robust against *active* adversaries, i.e. adversaries that can fully control the behaviour of up to t players, including changing the data sent by these players. In this protocol, an adversary is detected with probability 1 if they try to cheat.

It is easy to see that if $r \leq n - t$, we have

$$t \leq \frac{n-1}{3}.$$

If there is $(2, n-t)$-multiplicativity and t-privacy, we can show there is also $(1, n-2t)$-multiplicativity, as follows. Let $B \subseteq \{1, \ldots, n\}$ be a set of coordinates of size $|B| = n - 2t$. If $\mathbf{x} \in C$ with $\mathbf{x}_B = \mathbf{0}$, by t-privacy there is some $\mathbf{y} \in C$ with $\psi(\mathbf{y}) = 1$ and such that $\mathbf{y}$ has t zeroes in coordinates in the complement of B. Then $\mathbf{x} * \mathbf{y}$ has $n - t$ zeroes, so $0 = \overline{\psi}(\mathbf{x} * \mathbf{y}) = \psi(\mathbf{x})\psi(\mathbf{y}) = \psi(\mathbf{x})$. This shows B is a reconstructing set for (C, ψ), and thus we have shown $(1, n-2t)$-multiplicativity. It then follows that $t < n - 2t$, hence $t \leq \frac{n-1}{3}$.

It is well-known that we can get equality in this bound using Shamir's scheme. Our main result is that the converse holds has well, specifically that $(n, t, 2, n-t)$-arithmetic secret sharing schemes of K over K that have a maximal adversary parameter t must be given by Shamir's scheme.

Theorem 1.3. *Let $t \geq 1$ be an integer. Then any $(3t+1, t, 2, 2t+1)$-arithmetic secret sharing scheme of K over K is given by Shamir's scheme.*

Let $K \subseteq L$ be an extension of finite fields of degree k. If we now regard an arithmetic secret sharing scheme of L over K, a similar claim holds. In Shamir's scheme we can also take the evaluation point of the secret in L [Che+08]. This scheme has t-privacy and $(t+k)$-reconstruction, so it is no longer threshold if $k > 1$. The associated vector

space $\widetilde{C} \subseteq L \times K^n$ is not a linear code in the proper sense. We can still realize it as what we call an *extension field Reed-Solomon code*, that is $\widetilde{C}$ is of the form

$$\left\{(y_0 f(\alpha_0), y_1 f(\alpha_1), \ldots, y_n f(\alpha_n)) \;\middle|\; f \in K[X]_{<k+t}\right\}$$

where we allow y_0, α_0 to lie in the extension field L, and the other $y_i, \alpha_i \in K$ as before.

Definition 1.4. Let $K \subseteq L$ be an extension of finite fields. We say an arithmetic secret sharing scheme (C, ψ) for L over K is given by Shamir's scheme if $\widetilde{C}$ is extension field Reed-Solomon.

For $(n, t, 2, n-t)$-arithmetic secret sharing schemes of L over K, we will show that

$$t \leq \frac{n - 2k + 1}{3} \tag{2}$$

Shamir's scheme is the only arithmetic secret sharing scheme that attains equality in this bound.

Theorem 1.5. *Let $t \geq 1$ be an integer, and let $K \subseteq L$ be an extension of finite fields of degree k. Then any $(3t + 2k - 1, t, 2, 2t + 2k - 1)$-arithmetic secret sharing scheme for L over K is given by Shamir's scheme.*

To prove these results, we use a theorem inspired by the field of additive combinatorics. Additive combinatorics is a relatively modern field that takes ideas from number theory, harmonic analysis, ergodic theory and combinatorics. Recently various applications of additive combinatorics to cryptography have surfaced, which is interesting given that they come from a different background than the fields with more established applications to cryptography like for instance elliptic curves, coding theory and lattices.

A concise definition of the field of additive combinatorics can be hard to capture [Gre09]. Generally, additive combinatorics studies the additive structure of sets. The central objects of interest are *additive sets* (A, Z), where $A \subseteq Z$ is a finite non-empty subset of an abelian group Z. Additive sets are in general not additively closed – in fact, it is this lack of algebraic structure that is central in the study of these objects. Often, this additive set is referred to as simply A; Z is known as the *ambient group*.

Additive sets in the same ambient group can be added together and subtracted from each other. If $A, B \subseteq Z$ are additive sets (i.e. finite non-empty subsets), then their sumset and difference set are, respectively,

$$A + B := \{a + b \;|\; a \in A,\, b \in B\} \quad \text{and} \quad A - B := \{a - b \;|\; a \in A,\, b \in B\}$$

One can study the cardinalities of these constructions. For example, trivial estimates include $\max\{|A|, |B|\} \leq |A + B| \leq |A||B|$. Sets with a small *doubling constant* $\frac{|A+A|}{|A|}$ have different structural properties from those with large doubling constants. Note that $1 \leq \frac{|A+A|}{|A|}$, with equality if and only if A is a subgroup.

Generally, one does not assume special structural properties about the additive sets other than their additive structure (for example, when regarding subsets A of the integers $\mathbb{Z}$, one would not generally make statements about the number of odd or prime integers contained in A), but specific ambient groups may be considered. For example, the following theorem known as the Cauchy-Davenport inequality is one of the classical cornerstones of additive combinatorics, and concerns the cyclic group $\mathbb{Z}_p$ $(= \mathbb{Z}/p\mathbb{Z})$ as ambient group:

Theorem 1.6 (Cauchy-Davenport inequality)**.** *Let p be a prime, and let $A, B \subseteq \mathbb{Z}_p$ be two additive sets. Then*

$$|A + B| \geq \min\{p, |A| + |B| - 1\}$$

The name stems from the original discovery by Cauchy in 1813 [Cau13], and the later rediscovery by Davenport in 1935 [Dav35]. A partial converse of this theorem is Vosper's theorem [Vos56b], which examines the subsets that satisfy equality in the theorem. In this thesis, we will examine a linear version of Vosper's theorem and its applications to cryptography.

Applications of additive combinatorics to cryptography come from various directions. Often a construction is proven secure for certain asymptotic bounds on the parameters. For instance, Aggarwal, Dodis and Lovett published an efficient construction for non-malleable codes in the split-state model, where the size of the encoded message is $\tilde{O}((k + \log 1/\varepsilon)^7)$ for a message of k bits and ε-non malleability [ADL14]. They prove correctness using a result by Sanders [San10], that proves a weakened version of the Polynomial Freiman-Ruzsa conjecture [TV09, Conjecture 5.34]. Should the Polynomial Freiman-Ruzsa conjecture hold, then their construction is secure for an encoding of size $\tilde{O}((k + \log 1/\varepsilon)^2)$. Lipmaa used a result by Elkin [Elk11] on progression-free sets to prove secure parameters for their novel construction of a non-interactive zero knowledge scheme [Lip12]. See [Bib13] for an overview on the use of additive combinatorics in cryptography and theoretical computer science.

One can also use additive combinatorics to prove structural results. One approach is to apply the proof techniques used in additive combinatorics to derive claims for structures other than additive sets. This thesis will examine a result by Mirandola and Zémor, who obtained an analogue of Vosper's theorem for linear codes [MZ15]. We will apply this result to cryptography, in particular to arithmetic secret sharing schemes as we have seen, and also to error correcting pairs.

Let $\mathbf{x} \in K^{n+1}$ be a vector. We define its *weight* $w(\mathbf{x})$ as the number of non-zero coordinates, thus we have $0 \leq w(\mathbf{x}) \leq n + 1$. The minimum distance for a linear code C is the minimum weight of its non-zero vectors $\mathrm{d}_{\min}(C) = \min_{\mathbf{x} \in C \setminus \{\mathbf{0}\}} w(\mathbf{x})$. We recall the Singleton bound [Sin64], which states that for a linear code C of length ℓ we have

$$\dim C + \mathrm{d}_{\min}(C) \leq \ell + 1$$

Linear codes that satisfy equality in this bound are called *maximum distance separable*, or MDS for short. Examples of MDS codes are Reed-Solomon codes, the $[n, 1]$-repeated code $C = \{(x, \ldots, x) \subseteq K^n \mid x \in K\}$ and the trivial code K^n. In general, linear MDS codes of length n and dimension k correspond to n-arcs in the projective space $\mathbb{P}^{k-1}(K)$ [BTB88].

Error-correcting pairs were introduced independently by Pellikaan [Pel92] and Kötter [Köt92], and provide a condition for the existence of an efficient decoding algorithm. In [MP16], Márquez-Corbella and Pellikaan gave two separate proofs, an independent one and one based on [MZ15], that the existence of a t-error correcting pair for an MDS code C implies that C is a Reed-Solomon code. We present a more straightforward version of their second proof, which exposes the underlying theorem of [MZ15] more clearly.

This thesis is organized as follows. Section 2 introduces the concepts and notation we will use in the thesis, most notably general coding theory, the product of codes,

and Reed-Solomon codes. In Section 3 we give a general definition of arithmetic secret sharing schemes using a *codex*, and we shall derive some of its coding-theoretic properties.

Section 4 introduces the linear version of Vosper's theorem, that pertains to linear MDS codes. We reflect on the necessity of the MDS condition, and prove that there exist non-MDS codes which satisfy the dimension constraint in the theorem using the amalgamated direct sum construction. In Section 5 we give an implication for error-correcting pairs.

In Section 6 we will prove our main results Theorems 1.3 and 1.5. Section 7 discusses a further generalization to generalized codes, in which every coordinate (not just the secret) is in some extension field of the base field over which the code is defined. We conclude with a discussion of the achieved results and possible further work in Section 8.

2 Notation and preliminaries

Let $\mathbb{F}_q$ denote the finite field with q elements. For a positive integer n, we write the direct sum of n copies of $\mathbb{F}_q$ as $\mathbb{F}_q^n$. It is a vector space over $\mathbb{F}_q$ of dimension n. We write $\mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$.

For a positive integer n we will write $[n] := \{1, 2, \ldots, n\}$. Vectors, and hence codewords, are denoted in boldface, e.g. $\mathbf{x}$. Unless otherwise specified, we will index coordinates by elements from $[n]$, and we use the convention of referring to a vector's coordinates by subscript indices, so $\mathbf{x} = (x_1, \ldots, x_n)$.

The *support* of a vector $\mathbf{x}$ is the set of coordinates on which it has a non-zero entry, i.e. $\operatorname{supp}(\mathbf{x}) := \{i \mid x_i \neq 0\} \subseteq [n]$. The weight $w(\mathbf{x})$ of a vector is the cardinality of its support, i.e. the number of non-zero coordinates. The support of a set of vectors S is the union of the support of its codewords; S is said to have *full support* if $\operatorname{supp}(S) = \bigcup_{\mathbf{x}\in S} \operatorname{supp}(\mathbf{x}) = [n]$.

A *linear code* C of length n is a finite-dimensional $\mathbb{F}_q$-vector subspace of $\mathbb{F}_q^n$. We will call its elements *codewords*. The *dimension* of C as an $\mathbb{F}_q$-vector space is denoted $\dim_{\mathbb{F}_q}(C)$. We will omit the field $\mathbb{F}_q$ in this expression when it is obvious. The *minimum distance* $\mathrm{d}_{\min}(C)$ is the minimum weight of all non-zero codewords in C, or $n+1$ if $C = \{0\}$. Since C is a linear space, the zero vector $\mathbf{0} = (0, \ldots, 0)$ is always in C.

Since linear codes are just finite-dimensional vector spaces, they also have bases. It is customary to write codewords as $1 \times n$ row vectors. Then, if $\{\mathbf{g}_1, \ldots, \mathbf{g}_k\}$ are row vectors that form a basis for the linear code $C \subseteq \mathbb{F}_q^n$, then the $k \times n$ matrix

$$\begin{pmatrix} \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_k \end{pmatrix}$$

is called a *generator matrix* for C. We have $C = \{\mathbf{x}C \mid x \in \mathbb{F}_q^k\}$.

Every code $C \subseteq \mathbb{F}_q^n$ also has a dual code $C^\perp \subseteq \mathbb{F}_q^n$ with respect to the standard inner product $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^n x_i y_i$. That is,

$$C^\perp := \left\{ \mathbf{y} \in \mathbb{F}_q^n \;\middle|\; \langle \mathbf{x}, \mathbf{y} \rangle = 0 \text{ for each } \mathbf{x} \in C \right\}.$$

A code C is *self-dual* if $C = C^\perp$. The dual distance of C is defined as $\mathrm{d}^\perp(C) := \mathrm{d}_{\min}(C^\perp)$.

We recall the definition of MDS codes from the introduction. In particular a linear MDS code has full support. We have the following equivalences for MDS codes.

Proposition 2.1. *Let $C \subseteq \mathbb{F}_q^n$ be a linear code. Then the following are equivalent:*

1. *C is MDS*
2. *If G is a generator matrix for C, then every set of $\dim C$ columns of G are linearly independent*
3. *Every systematic generator matrix for C has all rows of weight $n + 1 - \dim C$*

Proof. For the equivalence of 1 and 2, see [LX04, Theorem 5.4.5]. For the equivalence of 1 and 3, see [MZ15, Lemma 4]. □

Sometimes we wish to lower the length of the code by excluding some of its coordinates. The following notation can be convenient:

Notation. Suppose $C \subseteq \mathbb{F}_q^n$ is a code, and $I \subseteq [n]$ is a set of coordinates. Then we write $C_I := \pi_I(C)$ for the image of C under the projection map

$$\begin{aligned} \pi_I : \mathbb{F}_q^n &\to \mathbb{F}_q^{|I|} \\ (x_i)_{i=1}^n &\mapsto (x_i)_{i \in I} \end{aligned}$$

This process is known as *puncturing* and we will call C_I a *punctured code*. If $x \in C$ we will write $\mathbf{x}_I := \pi_I(\mathbf{x})$ for its image in C_I.

Note that the notation for the coordinate sets of punctured codes varies throughout the literature, where sometimes the coordinates specified are those that are omitted. We see the punctured code as a projection, and find the chosen notation more suitable for this purpose.

2.1 Reed-Solomon codes

A special subclass of MDS codes are the Reed-Solomon codes.

Definition 2.2. Let $\alpha_1, \ldots, \alpha_n$ be distinct elements of $\mathbb{F}_q \cup \{\infty\}$, and write $\boldsymbol{\alpha} := (\alpha_1, \ldots, \alpha_n)$. Let $\mathbf{y} = (y_1, \ldots, y_n) \in \left(\mathbb{F}_q^*\right)^n$. We denote by $\mathbb{F}_q[X]_{<k}$ the set of all polynomials in X with coefficients in $\mathbb{F}_q$ and degree strictly less than k. For $f \in \mathbb{F}_q[X]_{<k}$ define $f(\infty)$ as the coefficient of X^{k-1}. We write

$$C_k(\boldsymbol{\alpha}, \mathbf{y}) := \left\{ (y_1 f(\alpha_1), \ldots, y_n f(\alpha_n)) \;\middle|\; f \in \mathbb{F}_q[X]_{<k} \right\}$$

A *(generalized) Reed-Solomon code* is a linear code C of the form $C = C_k(\boldsymbol{\alpha}, \mathbf{y})$. We call $\boldsymbol{\alpha}$ an *evaluation point sequence* of C and $\mathbf{y}$ a *scaling vector*.

The nomenclature of Reed-Solomon codes varies throughout the literature. The "generalized" part of the term usually signifies the inclusion of a scaling vector, but it may also refer to allowing an evaluation point at infinity. We will not make these distinctions in this thesis, and will just refer to them as Reed-Solomon codes. Note that we require $n \leq q + 1$, since the α_i are all distinct.

If we let $\mathrm{ev}_{\boldsymbol{\alpha},\mathbf{y}}$ denote the evaluation map sending a polynomial f to the vector $(y_i f(\alpha_i))_i$, Reed-Solomon codes can be seen as the image of $\mathrm{ev}_{\boldsymbol{\alpha},\mathbf{y}}$ on the set of polynomials $\mathbb{F}_q[X]_{<k}$. This set is an $\mathbb{F}_q$-vector space of dimension k. Since a non-zero polynomial of degree $< k$ has at most $k - 1$ roots, we have that $w(\mathrm{ev}_{\boldsymbol{\alpha},\mathbf{y}}(f)) \geq n - (k - 1)$ for non-zero f, so $\mathrm{d}_{\min}(C) = n + 1 - k$. This shows all Reed-Solomon codes are MDS.

Reed-Solomon codes have a generator matrix which is a Vandermonde matrix, except for the column associated to the evaluation point ∞, and except for scaling of the columns. We will abuse notation, and still refer to matrices of this form as Vandermonde matrices. If we suppose $\alpha_1 = \infty$ and $y_1 = \cdots = y_n = 1$, then the following is a generator matrix for C:

$$\begin{pmatrix} 0 & 1 & 1 & \dots & 1 \\ 0 & \alpha_2 & \alpha_3 & \dots & \alpha_n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \alpha_2^{k-2} & \alpha_3^{k-2} & \dots & \alpha_n^{k-2} \\ 1 & \alpha_2^{k-1} & \alpha_3^{k-1} & \dots & \alpha_n^{k-1} \end{pmatrix}$$

For a given Reed-Solomon code C, its evaluation point sequence is not unique. In 1987, Arne Dür showed in [Dür87] that for a given Reed-Solomon code C, we have that its set of evaluation point sequences is an orbit of the action of the general linear group

$$\mathrm{GL}(2, \mathbb{F}_q) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d, \in \mathbb{F}_q;\ ad - bc \neq 0 \right\}$$

on $(\mathbb{F}_q \cup \{\infty\})^n$. Here, the evaluation points are interpreted as elements of the projective line $\mathbb{F}_q \cup \{\infty\} = (\mathbb{F}_q \cup \{\infty\})$. An element $f \in \mathrm{GL}(2, \mathbb{F}_q)$ acts on an evaluation point $z \in \mathbb{F}_q \cup \{\infty\}$ as

$$f = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : z \mapsto \frac{az + b}{cz + d}$$

and its acts coordinate-wise on evaluation point sequences $\boldsymbol{\alpha}$. Since the action of $f \in \mathrm{GL}(2, \mathbb{F}_q)$ is invariant under multiplication by a scalar $\lambda \in \mathbb{F}_q^*$, we can also identify such a transformation by an element $\bar{f}$ of the projective linear group $\mathrm{PGL}(2, \mathbb{F}_q)$, i.e. $\mathrm{GL}(2, \mathbb{F}_q)$ modulo equivalence under scalar multiplication. We note that this group is triply transitive (see e.g. [Dür87]).

Theorem 2.3. *Let $2 \leq k \leq n-2$ and K be a finite field. Then $C_k(\boldsymbol{\alpha}, \mathbf{y}) = C_k(\boldsymbol{\beta}, \mathbf{v})$ for $\boldsymbol{\alpha}, \boldsymbol{\beta} \in (K \cup \{\infty\})^n$ and $\mathbf{y}, \mathbf{v} \in (K^*)^n$ if and only if there are some $f = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2, K)$ and $\lambda \in K^*$ such that for each i we have*

$$\begin{aligned} \beta_i &= f(\alpha_i) \\ v_i &= \lambda \theta(f, \alpha_i)^{k-1} y_i \end{aligned}$$

where θ is given by

$$\theta(f, z) = \begin{cases} cz + d & \text{if } z \in K \text{ and } cz + d \neq 0 \\ \frac{ad-bc}{-c} & \text{if } z \in K \text{ and } cz + d = 0 \\ c & \text{if } z = \infty \text{ and } c \neq 0 \\ a & \text{if } z = \infty \text{ and } c = 0 \end{cases}.$$

Proof. See [Dür87]. □

If $C \subseteq K^n$ is a linear code, and $K \subseteq L$ is an extension of finite fields, we may take the L-linear span $L\langle C\rangle := L\langle \mathbf{x} \mid \mathbf{x} \in C\rangle$. The result is a linear code of length n over L. This construction is also known as an *extension of scalars*, and it is equivalent to taking the tensor product $C \otimes_K L$. The following two lemmas give results on taking the extension of scalars of Reed-Solomon codes.

Lemma 2.4. *Let $K \subseteq L$ be an extension of finite fields. Let $C \subseteq K^n$ be a linear code, and $L\langle C\rangle$ its L-linear span. If $L\langle C\rangle$ is Reed-Solomon, and if it has a generator matrix with entries in the base field K, then C is also Reed-Solomon, and it has an evaluation point sequence $\boldsymbol{\alpha} \in (K \cup \{\infty\})^n$. Furthermore, if $D \subseteq L^n$ is any code which shares some evaluation point sequence with $L\langle C\rangle$, then $\boldsymbol{\alpha}$ is also an evaluation point sequence for D.*

Proof. The proof of the first claim can be found in [MP16, Proposition C.3]. Suppose $D \subseteq L^n$ is any linear code which shares an evaluation point sequence with $L\langle C\rangle$, i.e. we have for some $\boldsymbol{\beta} \in (L \cup \{\infty\})^n, \mathbf{x}, \mathbf{x}' \in (L^*)^n$ that

$$L\langle C\rangle = C_k(\boldsymbol{\beta}, \mathbf{x}) = C_k(\boldsymbol{\alpha}, \mathbf{x}'),\ D = C_{k'}(\boldsymbol{\beta}, \mathbf{y})$$

then there exists some $\phi \in \mathrm{GL}(2, L)$ such that $\phi(\alpha_i) = \beta_i$ for all i. It follows that $D = C_{k'}(\boldsymbol{\alpha}, \mathbf{y}')$. □

Lemma 2.5. *Let $C \subseteq K^n$ be a Reed-Solomon code, and suppose $\alpha \in K^n$ is an evaluation point sequence for C. Then $C^\perp$ is also a Reed-Solomon code which has α as an evaluation point sequence.*

Proof. See e.g. [JX16, Lemma 2.2]. □

2.2 The product of codes

Let $C, D \subseteq \mathbb{F}_q^n$ be codes. Suppose $\mathbf{x} = (x_1, \ldots, x_n) \in C, \mathbf{y} = (y_1, \ldots, y_n) \in D$. Then we may form a coordinate-wise product

$$\mathbf{x} * \mathbf{y} = (x_1 y_1, \ldots, x_n y_n)$$

Taking the span of all such products, we obtain a new linear code $C * D \subseteq \mathbb{F}_q^n$. This construction is sometimes also known as the *Schur product* of codes.

If $\{\mathbf{g}_1, \ldots, \mathbf{g}_k\}$ is a basis for C and $\{\mathbf{h}_1, \ldots, \mathbf{h}_l\}$ is a basis for D, then

$$C * D = \mathrm{span}\langle \mathbf{g}_i * \mathbf{h}_j \rangle$$

It follows that $\dim C * D \leq \dim C \dim D$. Note that the set $\{\mathbf{g}_i * \mathbf{h}_j\}_{i,j}$ is not a basis in general as it may be linearly dependent.

The following is an analogue of Theorem 1.6 for linear codes:

Lemma 2.6. *Let $C, D \subseteq \mathbb{F}_q^n$ be linear codes of full support, and suppose at least one of them is MDS. Then*

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

Proof. See [Ran15]. □

For an MDS code $C \subseteq \mathbb{F}_q^n$ of dimension $\leq \frac{n}{2}$, the lemma implies that

$$\dim C^{*2} \geq 2 \dim C - 1.$$

The codes that provide equality in this bound, i.e. that have $\dim C^{*2} = 2 \dim C - 1$ are of particular interest to us. We shall introduce terminology and shall refer to these codes as having a *small square*. In particular, if C is a self-dual MDS code then it satisfies this condition. Also, all Reed-Solomon codes have a small square. In fact, they are the only MDS codes that have a small square, which as we will see later is precisely the statement of Corollary 4.7.

3 Secret sharing

As we have seen in the introduction, secret sharing is the dispersal of secret information into multiple shares, such that the original secret can be reconstructed from these shares. There are various ways to formally define secret sharing. We will now give a general definition of arithmetic secret sharing schemes using a codex [Cra11; CCX12]. The notion of a codex is somewhat technical, but it applies well to arithmetic secret sharing. Recently, other applications of codices have surfaced, e.g. to local decoding of Reed-Muller codes [CXY16]. The definitions of secret sharing schemes in this section are taken from [CDN15, Chapters 11–12], and they can be found in more detail there. In this section K, is a (not necessarily finite) field.

Definition 3.1. Let A be a K-algebra of finite dimension, and let $C \subseteq K^n$ be a linear code with $\psi : C \to A$ a K-linear map. Let $B \subseteq [n]$ be a set of coordinates.

We say B is a *privacy set for* (C, ψ) if the map

$$\begin{aligned} \pi_{\psi,B} : C &\to A \times C_B \\ \mathbf{x} &\mapsto (\psi(\mathbf{x}), \pi_B(\mathbf{x})) \end{aligned}$$

is surjective.

We say B is a *reconstructing set for* (C, ψ) if for each $\mathbf{z} \in C$ with $\mathbf{z}_B = \mathbf{0}$ we have that $\psi(\mathbf{z}) = 0$.

Remark 3.2. By linearity, B being a privacy set is equivalent to the condition that for any $s \in A$ there is some $\mathbf{x} \in C$ with $\mathbf{x}_B = \mathbf{0}$ and $\psi(\mathbf{x}) = s$. B being a privacy set guarantees that for $\mathbf{x} \in C$ the image $\psi(\mathbf{x})$ is independent from the B-coordinates $\mathbf{x}_B$.

B being a reconstructing set means that for a codeword $\mathbf{x} \in C$, the B-coordinates fully determine $\psi(\mathbf{x})$: if $\mathbf{z}, \mathbf{z}' \in C$ with $\mathbf{z}_B = \mathbf{z}'_B$ then $\pi_B(\mathbf{z} - \mathbf{z}') = \mathbf{0}$, hence $\psi(\mathbf{z} - \mathbf{z}') = 0$ and therefore $\psi(\mathbf{z}) = \psi(\mathbf{z}')$.

Write $C_{\mathbf{0}\downarrow B} := C \cap \ker \pi_B$. Then B is a reconstructing set for (C, ψ) if and only if $C_{\mathbf{0}\downarrow B} \subseteq \ker \psi$, and B is a privacy set for (C, ψ) if and only if $\psi(C_{\mathbf{0}\downarrow B}) = L$.

Definition 3.3. Let A be a K-algebra, and let $d \geq 1$ and $1 \leq r \leq n$ be integers. Suppose $C \subseteq K^n$ is a linear code, and let $\psi : C \to A$ be a K-linear map. Then (C, ψ) is said to have (d, r)-*multiplicativity* if there is a unique K-linear map $\overline{\psi} : C^{*d} \to A$ such that:

1. for all $\mathbf{x}_1, \ldots, \mathbf{x}_d \in C$ we have $\overline{\psi}(\mathbf{x}_1 * \ldots * \mathbf{x}_d) = \psi(\mathbf{x}_1) \cdots \psi(\mathbf{x}_d)$.
2. $\overline{\psi}$ is r-wise determined, all sets $B \subseteq [n]$ of size $|B| = r$ are reconstructing sets for $(C^{*d}, \overline{\psi})$.

Note that (d, r)-multiplicativity implies $(\leq d, \geq r)$-multiplicativity under the condition that A is a unital algebra and that ψ is surjective.

Proposition 3.4. *Let A be a unital K-algebra, $C \subseteq K^n$ a linear code, and $\psi : C \to A$ a surjective K-linear map. Suppose we have integers $1 \leq d' \leq d$ and $1 \leq r \leq r' \leq n$. If (C, ψ) has (d, r)-multiplicativity then it also has (d', r')-multiplicativity.*

Proof. Suppose $d = d'$. Directly from the definition it follows that a map $\overline{\psi} : C \to A$ that is r-wise determined is also r'-wise determined, hence (d, r')-multiplicativity is evident.

We now prove the statement for $(d', r') = (d - 1, r)$; the full claim then follows by induction. Let $\overline{\psi}$ as in Definition 3.3. ψ is surjective, hence pick $\mathbf{x}_d \in C$ with $\psi(\mathbf{x}_d) = 1$. Define a K-linear map $\overline{\vartheta} : C^{*d-1} \to A$ as

$$\overline{\vartheta}(\mathbf{x}_1 * \ldots * \mathbf{x}_{d-1}) := \overline{\psi}(\mathbf{x}_1 * \ldots * \mathbf{x}_{d-1} * \mathbf{x}_d) = \psi(\mathbf{x}_1) \cdots \psi(\mathbf{x}_{d-1}) \cdot 1.$$

If $B \subseteq [n]$ is of size $|B| = r$ and $\mathbf{x} \in C^{*d-1}$ is such that $\mathbf{x}_B = 0$, then $\overline{\vartheta}(\mathbf{x}) = \overline{\psi}(\mathbf{x} * \mathbf{x}_d) = 0$, since $(\mathbf{x} * \mathbf{x}_d)_B = \mathbf{0}$. Uniqueness of $\overline{\vartheta}$ follows from condition 1. □

Definition 3.5. Let A be a K-algebra, and let $0 \leq t < n$ be integers. Suppose $C \subseteq K^n$ is a linear code, and let $\psi : C \to A$ be a K-linear map. If $t = 0$, then (C, ψ) is 0-disconnected by default. If $t > 0$, (C, ψ) is t-disconnected if for each $B \subseteq [n]$ of size $|B| = t$ we have that B is a privacy set. If additionally $C_B = K^t$, we say there is t-disconnection with uniformity.

We can now define a codex.

Definition 3.6. Let A be a finite-dimensional non-trivial 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 K is a pair (C, ψ) where $C \subseteq K^n$ is a K-linear subspace and $\psi : C \to A$ is a K-linear map such that

1. ψ is surjective
2. (C, ψ) has (d, r)-multiplicativity
3. (C, ψ) has t-disconnection

An arithmetic secret sharing scheme is defined as a codex with some restrictions.

Definition 3.7. Let $d \geq 2, t \geq 1$ be integers and let A be a finite-dimensional non-trivial $\mathbb{F}_q$-algebra. An *arithmetic secret sharing scheme* is an (n, t, d, r)-codex for A over $\mathbb{F}_q$.

A is called the *secret space* and $\mathbb{F}_q$ the *share space* of the scheme. When a dealer wants to share a secret $s \in A$ in this arithmetic secret sharing scheme, he or she selects a uniformly random preimage $\mathbf{x}$ from $\psi^{-1}(s)$, and distributes each coordinate x_i to player i. A coalition $B \subseteq [n]$ of size $|B| \geq r$ can reconstruct the secret: since we have $(1, r)$-multiplicativity by Proposition 3.4 there is a unique K-linear map $\overline{\psi} : C \to A$ compatible with ψ that is r-wise determined. Therefore, given any r coordinates $\mathbf{y} \in K^r$, such that are there is at least one codeword $\mathbf{x} \in C$ with $\mathbf{x}_B = \mathbf{y}$, the secret $\psi(\mathbf{x})$ is well-defined.

Privacy is guaranteed by t-disconnection property, since given a coalition $B \subseteq [n]$ of size $|B| = t$ and coordinates $(y_b)_{b \in B}$ there is for every secret $s \in A$ at least one matching codeword $\mathbf{x} \in C$ with $\mathbf{x}_B = (y_b)_{b \in B}$ and $\psi(\mathbf{x}) = s$. In particular by linearity of ψ the number of such matching codewords is the same for each $s \in A$.

Since a codex is defined in terms of (d, r)-multiplicativity, the reconstruction parameter r is linked to the power of the code d. Taking Proposition 3.4 into account, if $d > 1$ it sometimes makes sense to see C as having different reconstruction parameters $r_{d'}$ for every power $1 \leq d' \leq d$ such that C also has $(d', r_{d'})$-multiplicativity. We shall later see an example of this, when determining whether C is an MDS code or not. We have the following lemma for these parameters.

Lemma 3.8. *Suppose we are given an (n, t, d, r)-codex for A over K with $d \geq 2$. Then it is also an $(n, t, d-1, r-t)$-codex.*

Proof. Let (C, ψ) be the (n, t, d, r)-codex. We want to show $(d-1, r-t)$-multiplicativity. From Proposition 3.4 we know (C, ψ) has $(d-1, r)$-multiplicativity, so we may write $\overline{\vartheta} : C^{*d-1} \to A$ for the unique r-wise determined K-linear map from Definition 3.3. We will show $\overline{\vartheta}$ is $(r-t)$-wise determined.

Suppose $B \subseteq [n]$ is any coordinate set of size $|B| = r - t$, and take an arbitrary $\mathbf{x} \in C^{*d-1}$ with $\mathbf{x}_B = \mathbf{0}$. Write $\overline{\psi} : C^{*d} \to A$ for the unique K-linear map from the definition of (d, r)-multiplicativity. Let $B' \subseteq [n] \setminus B$ be any subset of coordinates of size $|B'| = t$. By t-disconnection there is some $\mathbf{y} \in C$ with $\mathbf{y}_{B'} = \mathbf{0}$ and $\psi(\mathbf{y}) = 1$. Taking the product $\mathbf{x} * \mathbf{y}$ we see $(\mathbf{x} * \mathbf{y})_{B \cup B'} = \mathbf{0}$, so

$$0 = \overline{\psi}(\mathbf{x} * \mathbf{y}) = \overline{\vartheta}(\mathbf{x})\psi(\mathbf{y}) = \overline{\vartheta}(\mathbf{x})$$

□

In fact, if A is a K-algebra of dimension $k > 1$ which does not have zero-divisors, we can do even better. We use the following lemma, which gives information on sets which are neither privacy nor reconstructing.

Lemma 3.9. *Let A be a K-algebra of finite K-dimension k, and suppose $C \subseteq K^n$ is a linear code, and $\psi : C \to A$ is a K-linear map such that (C, ψ) has t-disconnection. Let r be an integer with $t \leq r < t + k$. Then any coordinate set $B \subseteq [n]$ of size $|B| = r$ is not a reconstructing set for (C, ψ).*

Proof. Recall the notation $C_{\mathbf{0}\downarrow B} = C \cap \ker \pi_B$ from Remark 3.2. Pick a subset $B' \subseteq B$ of size $|B'| = t$. Since there is t-privacy, B' is a privacy set, so $\psi(C_{\mathbf{0}\downarrow B'}) = A$.

We have that the projection of $C_{\mathbf{0}\downarrow B'}$ onto the coordinate set $B \setminus B'$ is the K-linear map

$$\pi_{B \setminus B'}\big|_{C_{\mathbf{0}\downarrow B'}} : C_{\mathbf{0}\downarrow B'} \to \pi_{B \setminus B'}(C_{\mathbf{0}\downarrow B'})$$

which is a surjective map with kernel $C_{\mathbf{0}\downarrow B}$. The dimension of its image at most $|B| - |B'| = r - t < k$. Write $V := C_{\mathbf{0}\downarrow B}, W := C_{\mathbf{0}\downarrow B'}$, so $\dim W - \dim V < k$.

We have $V \subset W$, and $\psi : W \to L$ is a surjective K-linear map. Recall B is a reconstructing set iff $\psi(V) = 0$. Since V, W are finite-dimensional K-vector spaces, we may take the orthogonal complement $V^\perp$ in W. We have $\psi(W) = \psi(V) + \psi(V^\perp) = L$, and $\dim V^\perp = \dim W - \dim V < k$ hence $\dim \psi(V^\perp) < k$ and since we have $\dim \psi(W) = k$ we must have $\psi(V) \neq 0$, which shows B is not a reconstructing set. □

Lemma 3.10. *Let A be a non-trivial K-algebra with $k := \dim_K < \infty$ which does not have zero-divisors. Suppose we are given an (n, t, d, r)-codex for A over K with $d \geq 2$. Then it is also an $(n, t, d-1, r-t-k+1)$-codex.*

Proof. Let (C, ψ) be the (n, t, d, r)-codex. We want to show $(d-1, r-t-k+1)$-multiplicativity. From Proposition 3.4 we know (C, ψ) has $(d-1, r)$-multiplicativity, so we may write $\overline{\vartheta} : C^{*d-1} \to A$ for the unique r-wise determined K-linear map from Definition 3.3. We will show $\overline{\vartheta}$ is $(r-t-k+1)$-wise determined.

Suppose $B \subseteq [n]$ is any coordinate set of size $|B| = r-t-k+1$, and take an arbitrary $\mathbf{x} \in C^{*d-1}$ with $\mathbf{x}_B = \mathbf{0}$. Write $\overline{\psi} : C^{*d} \to A$ for the unique K-linear map from the definition of (d, r)-multiplicativity. Let $B' \subseteq [n] \setminus B$ be any subset of coordinates of size $|B'| = t + k - 1$. By Lemma 3.9 we have that $\psi(C_{\mathbf{0}\downarrow B'}) \neq 0$, hence pick $\mathbf{y} \in C_{\mathbf{0}\downarrow B'}$ with $\psi(\mathbf{y}) = s \neq 0$. Then $\pi_{B \cup B'}(\mathbf{x} * \mathbf{y}) = \mathbf{0}$, hence $0 = \overline{\psi}(\mathbf{x} * \mathbf{y}) = \overline{\vartheta}(\mathbf{x})\psi(\mathbf{y})$, and since $\psi(\mathbf{y}) \neq 0$ and A does not have zero-divisors, we have $\psi(\mathbf{x}) = 0$. □

We can also define a codex in terms of a "generalized code". The following proposition gives the equivalence.

Proposition 3.11. *Let A be a non-trivial K-algebra of finite dimension. Let n, t, d, r be integers with $d \geq 1$ and $0 \leq t < r \leq n$.*

Suppose (C, ψ) is an (n, t, d, r)-codex for A over K. Then there is a K-vector subspace $\widetilde{C} \subseteq A \times K^n$ with coordinates indexed by $\{0, 1, \ldots, n\}$, given by

$$\widetilde{C} := \big\{(\psi(\mathbf{x}), \mathbf{x}) \;\big|\; \mathbf{x} \in C\big\}$$

such that:

1. $\pi_0(\widetilde{C}) = A$
2. *If $t > 0$, then for each subset of coordinates $B \subseteq [n]$ of size $|B| = t$ and for each $a \in A$ there is some $\widetilde{\mathbf{x}} \in \widetilde{C}$ with $\widetilde{\mathbf{x}}_B = \mathbf{0}$ and $\widetilde{x}_0 = a$.*
3. *For each subset of coordinates $B \subseteq [n]$ of size $|B| = r$ and for each $\mathbf{z} \in \widetilde{C}^{*d}$ with $\mathbf{z}_B = \mathbf{0}$, it holds that $\widetilde{z}_0 = 0$.*

Conversely, given such a K-vector subspace $\widetilde{C} \subseteq A \times K^n$ of the form $\widetilde{C} = \{(\psi(\mathbf{x}), \mathbf{x}) \mid \mathbf{x} \in C\}$ for a K-linear map $\psi : C \to A$ and a code $C \subseteq K^n$ that satisfies the three conditions, we have that (C, ψ) is an (n, t, d, r)-codex.

Proof. The forward direction follows directly from the definitions of a codex. For the converse, see [CDN15]. □

The object $\widetilde{C} \subseteq A \times K^n$ is generally not a code, since the first coordinate does not reside in the field K. However, some terminology from coding theory still applies, and we will refer to $\widetilde{C}$ as a *generalized code*, i.e. a K-linear subspace of a product of K-algebras indexed by $0, 1, \ldots, n$, so that we still have some sense of coordinates. Since it is a vector space, the K-dimension $\dim_K \widetilde{C}$ is well-defined. Because of property 3, ψ is surjective, hence we have

$$\dim_K \widetilde{C} = \dim_K C \tag{3}$$

Since Proposition 3.11 gives an equivalent definition of a codex in terms of a generalized code, we will abuse notation slightly and we will also refer to $\widetilde{C} \subseteq A \times K^n$ as a codex. Of particular interest will be codices where A is a finite extension field of the finite base field K.

One other case of a generalized code that will be relevant later, is what we will call an *extension field code*.

Definition 3.12. Let K be a finite field, and let n be an integer. For each $i = 1, \ldots, n$, let $K(\eta_i)$ be a finite field extension of K. An *extension field code* is a K-linear subspace $C \subseteq \bigoplus_{i=1}^{n} K(\eta_i)$.

An example of an extension field code, we define an extension field Reed-Solomon code.

Definition 3.13. Let K be a finite field and let $C \subseteq \bigoplus_{i=1}^{n} K(\eta_i)$ be an extension field code. We say C is *extension field Reed-Solomon* if it is of the form

$$C = C_k(\boldsymbol{\alpha}, \mathbf{y}) = \{(y_1 f(\alpha_1), \ldots, y_n f(\alpha_n)) \mid f \in K[X]_{<k}\}$$

for a positive integer $k < n$, and for each i we have $\alpha_i \in K(\eta_i) \cup \{\infty\}, y_i \in K(\eta_i)^*$ such that the α_i are all distinct in compositum $K(\eta_1, \ldots, \eta_n) \cup \{\infty\}$.

The parameters r and t of an (n, t, d, r)-arithmetic secret sharing scheme (C, ψ) over $\mathbb{F}_q$ are closely related to the dimensions $\dim C^{*k}, k \geq 1$ of C and its powers as an $\mathbb{F}_q$-vector space. This allows us to use theory for the dimensions of these (product) spaces as a way to deduce claims on the parameters.

Lemma 3.14. *Let (C, ψ) be an (n, t, d, r)-arithmetic secret sharing scheme for A over $\mathbb{F}_q$. Then*

$$\dim C \geq t + \dim A \tag{4}$$

$$\dim C^{*d} \leq r \tag{5}$$

Proof. Suppose $l := \dim C$. Let G be a generator matrix for C. After possibly renumbering coordinates, we may suppose G is in systematic form $G = (I\ X)$. We project C down onto the first t coordinates, which is generated by either a part of I if $t \leq l$, or by I and a part of X if $t \geq l$. By t-disconnection we have that

$$\pi_{\psi,[l]} : C \to A \times \pi_{[t]}(C)$$

is a surjective K-linear map, hence

$$l = \dim C \geq \dim A + \dim \pi_{[t]}(C) = \dim A + \min\{t, l\} > \min\{t, l\}$$

which leads to a contradiction if $\min\{t, l\} = l$. Therefore $t < l$ and $l \geq \dim A + t$.

For Equation (5), suppose that $\dim C^{*d} > r$. In a similar manner as before, we look at the generator matrix G of C^{*d} in systematic form $(I\ X)$, possibly after renumbering coordinates. Since A is non-trivial and ψ is surjective, we have that the unique linear map $\overline{\psi} : C^{*d} \to A$ satisfying Definition 3.5 is non-zero, hence there is at least one basis vector, say $\mathbf{g}_{r+1}$, whose image satisfies $\overline{\psi}(\mathbf{g}_{r+1}) \neq 0$. Now, projecting $\mathbf{g}_{r+1}$ onto the first $[r]$ coordinates we get $\pi_{[r]}(\mathbf{g}_{r+1}) = \mathbf{0}$ yet $\overline{\psi}(\mathbf{g}_{r+1}) \neq 0$, contradicting that $\overline{\psi}$ is r-wise determined. □

The condition of a codex $\widetilde{C} \subseteq K \times K^n$ being MDS can be phrased in terms of its parameters.

Proposition 3.15. *Let (C, ψ) be an $(n, t, 1, t+1)$-codex for K over K. Then $\widetilde{C}$ is an MDS code. In particular, so is C. Conversely, given an MDS code $\widetilde{C}$ of dimension $t+1$, $\widetilde{C}$ is a codex in the sense of Proposition 3.11.*

Proof. $\dim C = t+1$ by Lemma 3.14.

Let $G = (I\ A)$ be a systematic generator matrix of $\widetilde{C}$, where $\mathbf{a}_1, \ldots, \mathbf{a}_{t+1} \in K^{n-t}$ are the rows of A. We want to show that A does not contain any zero entries; then G satisfies condition 3 of Proposition 2.1 and it follows that it is MDS. The first row of G is of the form

$$\mathbf{g}_1 = (1, 0, 0, \ldots, 0, \mathbf{a}_1)$$

Since ψ is $(t+1)$-wise determined, if any entry in $\mathbf{a}_1$ would be 0, then $g_{11} = 0$, which is not the case. Hence $w(\mathbf{g}_1) = 1 + n - t$.

For $i > 1$ we have the i-th row of G of the form

$$\mathbf{g}_i = (0, \ldots, 1, \ldots, 0, \mathbf{a}_i)$$

Suppose one entry of $\mathbf{a}_i$ is zero, say at C-coordinate $j \in [n]$. Let $B := \{1, 2, \ldots, i-1, i+1, \ldots, t-1, t, j\}$. Since we have t-disconnection, we know that there is an $\mathbf{x} \in C$ with $\psi(\mathbf{x}) = 1$ and $\mathbf{x}_B = \mathbf{0}$.

We may write $\mathbf{x} = c_1(\mathbf{g}_1)_{[n]} + \cdots + c_{t+1}(\mathbf{g}_{t+1})_{[n]}$. Since $\psi(\mathbf{x}) = 1$ we have $c_1 = 1$. We know $g_{1j} \neq 0$ and $g_{ij} = 0$, so we need $c_m \neq 0$ for some index $m \in [t] \setminus \{j\}$. But since $x_m = 0$, we also need $c_m = 0$, leading to a contradiction. Hence each entry of $\mathbf{a}_i$ non-zero, hence C is MDS by Proposition 2.1. Since $\dim C = \dim \widetilde{C}$, the projection C is also MDS.

Conversely, suppose we are given an MDS code $\widetilde{C} \subseteq K^{n+1}$ indexed by $0, 1, \ldots, n$ of dimension $t+1 \leq n$, then it satisfies the conditions of Proposition 3.11. Condition 1 follows since an MDS code has full support. Conditions 2 and 3 follow from the minimum distance of C being $\mathrm{d}_{\min}(C) = n + 2 - (t+1) = n + 1 - t$ – so a codeword $\mathbf{x} \in C$ that has $\geq t+1$ zeroes must be the zero vector $\mathbf{0}$. □

Theorem 3.16. *Let $K \subseteq L$ be an extension of finite fields of degree k. Suppose we have an $(n, t, 2, n-t)$-arithmetic secret sharing scheme for L over K. Then we have*

$$t \leq \frac{n - 2k + 1}{3}$$

Proof. Let (C, ψ) denote the secret sharing scheme with $\overline{\psi} : C^{*2} \to L$ the K-linear map for $(2, n-t)$-multiplicativity. Let $B \subseteq [n]$ be a set of size $n - 2t - k + 1$. We will show B is a reconstructing set.

Let $\mathbf{x} \in C$ with $\mathbf{x}_B = \mathbf{0}$. Pick $B' \subseteq [n] \setminus B$ of size $t + k - 1$. By Lemma 3.9 we have that $\psi(C_{\mathbf{0}\downarrow B'}) \neq 0$, hence pick $\mathbf{y} \in C_{\mathbf{0}\downarrow B'}$ with $\psi(\mathbf{y}) = s \neq 0$. Then $\pi_{B \cup B'}(\mathbf{x} * \mathbf{y}) = \mathbf{0}$, hence $0 = \overline{\psi}(\mathbf{x} * \mathbf{y}) = \psi(\mathbf{x})\psi(\mathbf{y})$, and since $\psi(\mathbf{y}) \neq 0$ we have $\psi(\mathbf{x}) = 0$.

So ψ is $(n-2t-k+1)$-wise determined, and since $t + k \leq n - 2t - k + 1$ by Lemma 3.14 we have

$$3t \leq n - 2k + 1$$

□

4 Vosper's theorem for codes

Vosper's theorem gives a partial converse of Theorem 1.6, saying the subsets that satisfy equality in the theorem are what are called *arithmetic progressions*:

Definition 4.1. Let a, d be elements of an abelian group Z, and let k be a positive integer. An *arithmetic progression* in Z of length k is a set

$$\{a, a+d, a+2d, \ldots, a+(k-1)d\}$$

Here d is called the *step* of the progression.

Theorem 4.2 (Vosper's theorem)**.** *Let p be a prime, and let A, B be subsets of the abelian group $\mathbb{Z}_p$, with $|A|, |B| \geq 2$ and $|A+B| \leq p-2$. Then $|A+B| = |A| + |B| - 1$ if and only if A and B are arithmetic progressions with the same step.*

There are several known ways to prove the theorem. Vosper originally proved the theorem [Vos56b] using another transform called the Davenport transform. Later he published an addendum giving a simpler proof based on the e-transform [Vos56a]. In 2006, Rødseth gave an even shorter proof of the theorem [Rød06] using the Davenport transform.

In 2015, Bachoc, Serra and Zémor proved a linear version of Vosper's theorem in the setting of field extensions [BSZ15]. Also in 2015, Mirandola and Zémor published a linear version of Vosper's theorem applied to linear codes [MZ15]. We will focus on the latter result. Here, the role of arithmetic progressions in the classical setting is taken on by Reed-Solomon codes.

Theorem 4.3. *Let $C, D \subseteq \mathbb{F}_q^n$ be MDS codes, with $\dim C, \dim D \geq 2$ and $\dim C * D \leq n-2$. If*

$$\dim C * D = \dim C + \dim D - 1$$

then C and D are Reed-Solomon codes with a common evaluation point sequence.

Proof. See [MZ15]. □

Remark 4.4. The *common* evaluation point sequence in the theorem refers to that there is some $\boldsymbol{\alpha} \in (\mathbb{F}_q \cup \{\infty\})^n$ that is an evaluation point sequence for both C and D. By Theorem 2.3 this means that also for every $\boldsymbol{\beta} \in (\mathbb{F}_q \cup \{\infty\})^n$ that is an evaluation point sequence for C, we have that $\boldsymbol{\beta}$ is an evaluation point sequence for D, and vice versa.

Note that while Theorem 4.2 concerns arbitrary subsets of $\mathbb{Z}_p$, Theorem 4.3 is restricted to the subclass of MDS codes, but it does not put restrictions on the ambient space.

Using the proofs in [MZ15], the restriction of the codes being MDS is hard to remove. We can slightly generalize Theorem 4.3 by relaxing the Reed-Solomon condition to include codes with non-distinct evaluation point sequences. The proof of Theorem 4.3 relies on [MZ15, Lemma 26], which also holds in the following form (with the MDS condition removed):

Lemma 4.5. *Let $C, D \subseteq \mathbb{F}_q^n$ be full-support codes of dimension k and l, respectively, with*

$$\dim C * D = k + l - 1$$

Let $I \subseteq [n]$ be a coordinate set with $|I| \geq k + l - 1$ such that projecting C, D on it does not change the dimension, i.e.

$$\dim C_I = \dim C = k$$
$$\dim D_I = \dim D = l$$

If C_I, D_I are Reed-Solomon codes with a common evaluation point sequence then C, D are Reed-Solomon codes with a common evaluation point sequence.

Proof. The proof from [MZ15, Lemma 26] works – the MDS condition there is not needed and is replaced by the condition that puncturing does not change the dimension. □

The following theorem then gives a slight generalization of Theorem 4.3:

Theorem 4.6. *Let $C, D \subseteq \mathbb{F}_q^n$ be full-support codes of dimension k and ℓ, respectively, with $k, \ell \geq 2$. Let $I \subseteq [n]$ be a coordinate set such that $|I| \geq k + \ell + 1$ and assume that the punctured codes $C_I, D_I \subseteq F^{|I|}$ are MDS and of dimension k and l, respectively. If furthermore*

$$n - 2 \geq \dim C * D = k + \ell - 1$$

then C and D are Reed-Solomon codes (allowing repeated coordinates, though at least $|I|$ distinct coordinates) with a common evaluation point sequence.

Proof. We apply Theorem 4.3 to C_I, D_I. Then we use Lemma 4.5. □

The case for $C = D$ in Theorem 4.3 is interesting in its own right. In Section 6 we will mostly use this restriction of the theorem:

Corollary 4.7. *Let $C \subseteq \mathbb{F}_q^n$ be a linear MDS code, with $\dim C \leq \frac{n-1}{2}$. Then C is Reed-Solomon if and only if C has a small square, i.e. $\dim C^{*2} = 2 \dim C - 1$.*

Remark 4.8. Note that if $\dim C \geq \frac{n+1}{2}$, then by Lemma 2.6 we have that C^{*2} is the full space, hence $\dim C^{*2}$ does not yield information about whether C is Reed-Solomon. However, by Lemma 2.5 we can apply Corollary 4.7 to $C^\perp$. In the remaining case, where C is an MDS code of dimension $\dim C = \frac{n}{2}$ and C has a small square, C is actually not necessarily Reed-Solomon, see [MZ15, Remark 28].

A natural question would be to ask whether there can be non-MDS codes with a small square. The answer is affirmative. We can prove the following result.

Theorem 4.9. *For any finite field $\mathbb{F}_q$ and integer $\ell \geq 1$ there exists a code $C \subseteq \mathbb{F}_q^n$, for some integer n (which in general depends on ℓ), such that:*

1. *C has a small square*
2. *C is not MDS*
3. *C^{*2} has codimension ℓ, i.e. $\dim C^{*2} = n - \ell$*

To prove this, we use the amalgamated direct sum (cf. [Coh+97, p. 89]) of two linear codes.

Definition 4.10. Let C, D be linear codes over a finite field $\mathbb{F}_q$ whose support includes the last, respectively first, coordinate. Then their *amalgamated direct sum* (ADS) is

$$C \dot{\oplus} D = \{(\mathbf{x}, a, \mathbf{y}) \mid a \in \mathbb{F}_q,\ (\mathbf{x}, a) \in C,\ (a, \mathbf{y}) \in D\}$$

Proposition 4.11. *We have:*

$$\begin{aligned} \operatorname{length}(C \dot{\oplus} D) &= \operatorname{length}(C) + \operatorname{length}(D) - 1 \\ \dim(C \dot{\oplus} D) &= \dim(C) + \dim(D) - 1 \qquad (6) \\ \min\{\mathrm{d}_{\min}(C), \mathrm{d}_{\min}(D)\} \leq \mathrm{d}_{\min}(C \dot{\oplus} D) &\leq \mathrm{d}_{\min}(C) + \mathrm{d}_{\min}(D) - 1 \qquad (7) \end{aligned}$$

Proof. The first equation is trivial. Equation (6) follows by looking at the linear map $C \oplus D \to \mathbb{F}_q$ that sends $(\mathbf{x}, \mathbf{y})$ to $x_{n_C} - y_1$, where $n_C = \text{length}(C)$ is the index of the last coordinate in C. Its kernel is $C \dot{\oplus} D$, and if the last and first coordinates are in their respective supports, then the image has dimension 1.

We see that Equation (7) holds by noting that if $(\mathbf{x}, a, \mathbf{y}) \in C \dot{\oplus} D$ is a non-zero codeword of minimum weight, then assuming without loss of generality that $(\mathbf{x}, a) \neq \mathbf{0}$, we have $w(\mathbf{x}, a, \mathbf{y}) \geq w(\mathbf{x}, a) \geq \mathrm{d}_{\min}(C)$. It is sharp in the general case: if $(\mathbf{x}, 0) \in C$ is a non-zero codeword of minimal weight then $(\mathbf{x}, 0, 0) \in C \dot{\oplus} D$ is a codeword of the same weight.

For the upper bound, take $(\mathbf{x}, a) \in C$ and $(b, \mathbf{y}) \in D$ of minimal weight. If $a = 0$ then $(\mathbf{x}, a, 0) \in C \dot{\oplus} D$ so the upper bound is satisfied, and similarly for $b = 0$. If $a \neq 0 \neq b$ then $ab^{-1}(b, \mathbf{y}) = (a, ab^{-1}\mathbf{y})$ is a codeword of identical weight to $(b, \mathbf{y})$, so $w(\mathbf{x}, a, ab^{-1}\mathbf{y}) = w(\mathbf{x}, a) + w(b, \mathbf{y}) - 1 = \mathrm{d}_{\min}(C) + \mathrm{d}_{\min}(D) - 1$. In particular, the bound is sharp if a, b are never zero for non-zero codewords. □

Remark 4.12. This also shows that if $\mathrm{d}_{\min}(C) \leq \mathrm{d}_{\min}(D)$ and $(\mathbf{x}, 0) \in C$ is a codeword of minimal weight then $\mathrm{d}_{\min}(C \dot{\oplus} D) = \mathrm{d}_{\min}(C)$. If C is MDS then we can always guarantee such a codeword. In particular $C \dot{\oplus} D$ is never MDS, except in the case where both C and D are the trivial spaces $\mathbb{F}_q^{\dim(C)}, \mathbb{F}_q^{\dim(D)}$, respectively.

Suppose $C \dot{\oplus} D$ is MDS. Then each collection of $\dim C + \dim D - 1$ columns of its generator matrix (see (8) below) must be linearly independent by Proposition 2.1. So this must also hold for collections of columns of the generator matrices of C and D. Hence C and D must also be MDS. Consider the Singleton bound for $C \dot{\oplus} D$, then

$$\dim(C) + \dim(D) - 1 + \mathrm{d}_{\min}(C) = \text{length}(C) + 1 + \dim(D) - 1 = \text{length}(C) + \dim(D)$$

which would be equal to $\text{length}(C) + \text{length}(D) - 1 + 1$ so $\dim(D) = \text{length}(D)$. This implies $1 = \mathrm{d}_{\min}(D) \geq \mathrm{d}_{\min}(C)$, hence $\mathrm{d}_{\min}(C) = 1$, so C and D are both trivial.

For codes that have a small square we can give precise expressions for the dimension of the square of their amalgamated direct sums.

Proposition 4.13. *Let C, D be two linear codes with a small square. Then $C \dot{\oplus} D$ (assuming it is defined) also has a small square.*

Proof. Without loss of generality, assume C has generator matrix $(A \ I)$ and D has generator matrix $(I \ B)$. Here I denotes an identity matrix of suitable size. Let k_C, k_D denote the respective dimensions. Then $C \dot{\oplus} D$ has generator matrix

$$\begin{pmatrix} \boxed{\text{A}} & \begin{matrix} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & & & & & \\ 0 & \dots & 0 & 1 & 0 & 0 & 0 & \boxed{\text{B}} \\ & & & & 1 & & & \\ & & & & & \ddots & & \\ & & & & & & 1 & \end{matrix} \end{pmatrix} \tag{8}$$

where we note the k_C-th row contains both the last row of A and the first row of B.

Taking the square we get a code that is generated by the coordinate-wise products of pairs of rows and therefore has the following "generator matrix" – in the sense that

the rows span the code but are not in general linearly independent:

$$\begin{pmatrix} * & I & * \\ A\dot{*}A & O & O \\ O & O & B\dot{*}B \end{pmatrix}$$

Here O denotes a zero matrix of suitable size, and we take $A\dot{*}A$ to mean the $k(k-1)$ coordinate-wise products of *distinct* rows of A. Since C has a small square we know that its square, which has unreduced generator matrix

$$\begin{pmatrix} * & I \\ A\dot{*}A & O \end{pmatrix}$$

must satisfy $\operatorname{rank} A\dot{*}A = k_C - 1$, and an analogous constraint holds for B. We conclude that

$$\dim\left(\left(C\dot{\oplus}D\right)^{*2}\right) = (k_C + k_D - 1) + (k_C - 1) + (k_D - 1) = 2\left(k_C + k_D\right) - 1.$$

□

Proof of Theorem 4.9. If C is a $[2k, k]$ code with a small square, then its square has codimension 1. Such is the case, for example, for a self-dual code that has a row of weight $k+1$ in its systematic generator matrix, because then A has a row of non-zeroes in the notation of the previous proposition, hence $\operatorname{rank} A\dot{*}A \geq k-1$, but since C is self-dual we have $(1, \ldots, 1) \in (C^{*2})^{\perp}$, so $\dim C^{*2} \leq 2k-1$. We can also take C to be a Reed-Solomon code, which is guaranteed to exist for any $\mathbb{F}_q, k$.

Taking two such codes C, D of respective dimensions k_C, k_D we have that their amalgamated direct sum $C\dot{\oplus}D$ (if it is defined) has a small square, hence has a square of dimension $2(k_C + k_D - 1) - 1 = n - 2$ (where $n = n_C + n_D - 1 = 2k_C + 2k_D - 1$), so its square has codimension 2. We can repeat this construction: if for each $1 \leq i \leq \ell$ we have C_i a linear $[2k_i, k_i]$ code with a small square with both first and last coordinate in its support (unless $i = 1, \ell$ then we only need the last, respectively first, coordinate in its support), then

$$C_1\dot{\oplus}C_2\dot{\oplus}\ldots\dot{\oplus}C_\ell = (\ldots((C_1\dot{\oplus}C_2)\dot{\oplus}C_3)\dot{\oplus}\ldots)\dot{\oplus}C_\ell$$

is a non-MDS code with a small square with its square of codimension ℓ. □

5 Implications for error-correcting pairs

In this section, we give an application of Theorem 4.3 for error correcting pairs. This notion was introduced independently by Pellikaan [Pel92] and Kötter [Köt92], and provides a condition for the existence of an efficient decoding algorithm. More precisely, if a code has a t-error correcting pair then there is a decoding algorithm with complexity $\mathcal{O}(n^3)$ that corrects up to t errors for a code of length n.

Márquez-Corbella and Pellikaan showed in [MP16] that the existence of a t-error correcting pair for an MDS code C implies that C is a Reed-Solomon code. They gave two separate proofs. Besides their original proof, they gave a second proof that uses critical pairs of the Product Singleton bound from [MZ15]. We will present a more straightforward proof which uses Theorem 4.3 directly.

The definition of an error correcting pair is somewhat technical. We will not use it directly, but instead refer to two results from [Pel96]. We present it for sake of completeness.

Definition 5.1. Let $C \subseteq \mathbb{F}_q^n$ be a code, and let t be an integer. Suppose $A, B \subseteq \mathbb{F}_{q^k}^n$ are codes over a finite extension field of $\mathbb{F}_q$. Then (A, B) is a t-error correcting pair for C if the following four properties hold:

1. $(A * B) \perp C$
2. $\dim A > t$
3. $\mathrm{d}^{\perp}(B) > t$
4. $\mathrm{d}_{\min}(A) + \mathrm{d}_{\min}(C) > n$

The result from [MP16] is the following:

Theorem 5.2. *Let $2 \leq t < \frac{n}{2}$ be an integer. Let $C \subseteq \mathbb{F}_q^n$ be an MDS code of dimension $n-2t$ that has a t-error correcting pair (A, B) over a finite extension $\mathbb{F}_{q^k}$. Then A, B, C are Reed-Solomon codes with a common evaluation point sequence.*

For the proof, we use two results from [Pel96]:

Proposition 5.3. *If $C \subseteq \mathbb{F}_q^n$ is an MDS code of dimension $n - 2t$, and (A, B) is a t-error correcting pair for C, then A is an MDS code of dimension $t + 1$.*

Proof. [Pel96, Proposition 2.5] □

Proposition 5.4. *If $C \subseteq \mathbb{F}_q^n$ has a t-error correcting pair (A, B) over $\mathbb{F}_{q^k}$ and $q^k > \max_{1 \leq i \leq t} \binom{n}{i}$, there exists a subcode $B_t \subseteq B$ which is MDS and of dimension t, such that (A, B_t) is a t-error correcting pair for C.*

Proof. [Pel96, Corollary 5.4] □

We can now prove the theorem.

Proof of Theorem 5.2. By Propositions 5.3 and 5.4, A is an MDS code of dimension $t+1$ and there is an MDS subcode $B_t \subseteq B$ of dimension t, passing to a larger extension field if necessary. By Lemma 2.6 we get

$$2t \leq \dim A * B_t \leq \dim A * B \leq \dim(\mathbb{F}_{q^k} \otimes C)^{\perp} = 2t$$

hence $A * B_t = A * B = (\mathbb{F}_{q^k} \otimes C)^{\perp}$. Applying Theorem 4.3 we get that $A, B,$ and $(\mathbb{F}_{q^k} \otimes C)^{\perp}$ are Reed-Solomon codes with a common evaluation point sequence, and we also see $B = B_t$. The result now follows from Lemmas 2.4 and 2.5.

□

6 Implications for secret sharing

In this section, we will prove our main results Theorem 1.3 and Theorem 1.5, using Theorem 4.3. In fact, we will be mostly using Corollary 4.7 which looks at the square of codes (i.e. $C = D$ in Theorem 4.3). We will now prove Theorem 1.3.

We recall Theorem 1.3:

Theorem 1.3. *Let $t \geq 1$ be an integer. Then any $(3t + 1, t, 2, 2t + 1)$-arithmetic secret sharing scheme of K over K is given by Shamir's scheme.*

Proof. Let (C, ψ) denote the arithmetic secret sharing scheme. By Lemma 3.8 it has $(1, t+1)$-multiplicativity, so by Proposition 3.15 $\widetilde{C}$ must be MDS of dimension $t+1$.

Using Lemma 3.14 and Lemma 2.6 we have

$$2t + 1 = 2 \dim \widetilde{C} - 1 \leq \dim \widetilde{C}^{*2} \leq 2t + 1$$

and thus we have equality everywhere. Since $\dim \widetilde{C} = t+1 \leq \frac{3t+1}{2}$ we apply Corollary 4.7 and conclude that $\widetilde{C}$ is Reed-Solomon. □

We will now consider arithmetic secret sharing schemes where the secret lies in some finite extension field L of the base field K. First we show that in this case we have the bound of Equation (2).

Lemma 6.1. *Let $K \subseteq L$ be an extension of finite fields of degree k. Suppose we have an $(n, t, 2, n-t)$-arithmetic secret sharing scheme for L over K. Then we have*

$$t \leq \frac{n - 2k + 1}{3}$$

Proof. We use Lemma 3.10 and observe the arithmetic secret sharing also has parameters $(n, t, 1, n - 2t - k + 1)$. By Lemma 3.14 we have

$$t + k \leq n - t - k + 1$$

and the bound follows. □

The remainder of this section will be dedicated to proving Theorem 1.5. Recall that this theorem states that $(n, t, 2, n-t)$-arithmetic secret sharing schemes for L over K that have maximal adversary t must be given by Shamir's scheme.

We will use the equivalence of codices from Proposition 3.11 and observe that for $C \subseteq L \times K^n$ we can take the L-linear span of C. We have seen this construction before in Section 2.1. The result is a linear code $L\langle C \rangle$ over L of length $n+1$.

Lemma 6.2. *Suppose*

$$S = \{(\psi(\mathbf{g}_1), \mathbf{g}_1), \ldots, (\psi(\mathbf{g}_l), \mathbf{g}_l)\}$$

is a K-basis of a codex $C \subseteq L \times K^n$, where $\psi : K^n \to L$ is a K-linear map, $\mathbf{g}_i \in K^n$ for indices i. Then S is an L-basis of $L\langle C \rangle$. In particular, $\dim_K C = \dim_L L\langle C \rangle$.

Proof. By definition, the L-linear span of S is $L\langle C \rangle$. Suppose

$$c_1(\psi(\mathbf{g}_1), \mathbf{g}_1) + \cdots + c_l(\psi(\mathbf{g}_l), \mathbf{g}_l) = (0, \mathbf{0})$$

inside L^{n+1} for $c_1, \cdots c_l \in L$. Since

$$0 = c_1\psi(\mathbf{g}_1) + \cdots + c_l\psi(\mathbf{g}_l) = \psi(c_1\mathbf{g}_1 + \cdots + c_l\mathbf{g}_l)$$

and ψ is a K-linear map, we observe that S is linearly independent over L if and only if $\mathbf{g}_1, \ldots, \mathbf{g}_l$ are; that is, it suffices to look at the last n coordinates.

We know L is a vector space over K, say with basis $\{\alpha_j\}_{j \in J}$. Looking now at the coefficients for the basis vector α_j of $c_1\mathbf{g}_1 + \cdots + c_l\mathbf{g}_l = 0$ we get

$$c_{1j}\mathbf{g}_1 + \cdots + c_{lj}\mathbf{g}_l = 0$$

where $\sum_j c_{ij}\alpha_j = c_i$ for all i. This is a K-linear combination, hence by linear independence over K we conclude that $c_{ij} = 0$ for all i, j and so S is linearly independent over L. □

Corollary 6.3. *Let $C \subseteq L \times K^n$ be a codex, and write $D := L\langle C\rangle$. Then $\dim_L D^{*2} = \dim_K C^{*2}$.*

Proof. Suppose

$$S = \{(\psi(\mathbf{g}_1), \mathbf{g}_1), \ldots, (\psi(\mathbf{g}_l), \mathbf{g}_l)\}$$

is a K-basis of C. Then we construct C^{*2} as

$$C^{*2} = K\left\langle (\psi(\mathbf{g}_i)\,\psi(\mathbf{g}_j), \mathbf{g}_i * \mathbf{g}_j)\right\rangle = K\left\langle (\psi(\mathbf{g}_i * \mathbf{g}_j), \mathbf{g}_i * \mathbf{g}_j)\right\rangle$$

and we apply the lemma. □

Lemma 6.4. *Let (C, ψ) be an (n, t, d, r)-codex for L over K, and let $\phi : L\langle C\rangle \to L$ be the L-linear extension of ψ. Then $(L\langle C\rangle, \phi)$ is also an (n, t, d, r)-codex.*

Proof. Clearly, ϕ is surjective. Write $\overline{\psi} : C^{*d} \to L$ for the unique K-linear map for (d, r)-multiplicativity. We linearly extend this map to $\overline{\phi} : L\langle C\rangle^{*d} \to L$, so that for $\mathbf{x}_1, \ldots, \mathbf{x}_d \in L\langle C\rangle$ it holds that $\overline{\phi}(\mathbf{x}_1 * \ldots \mathbf{x}_d) = \phi(\mathbf{x}_1) \cdots \phi(\mathbf{x}_d)$. We show $\overline{\phi}$ is r-wise determined. Let B be a reconstructing set for $(C^{*d}, \overline{\psi})$. Let $\mathbf{x} \in L\langle C\rangle^{*d}$ with $\mathbf{x}_B = \mathbf{0}$, and let $\mathbf{g}_1, \ldots, \mathbf{g}_\ell$ be a K-basis for C^{*d}, and hence an L-basis for $L\langle C\rangle^{*d}$. We may write $\mathbf{x} = c_1\mathbf{g}_1 + \cdots + c_\ell\mathbf{g}_\ell$, for $c_1, \ldots, c_\ell \in L$. If $\{\alpha_1, \ldots, \alpha_k\}$ is a basis of L as a K-vector space, then we see there are $c_{ij} \in L$ for $i = 1, \ldots, \ell$ and $j = 1, \ldots, k$ such that

$$\overline{\phi}(\mathbf{x}) = \overline{\phi}\left(\sum_{i=1}^{\ell}\sum_{j=1}^{k} c_{ij}\alpha_j\mathbf{g}_i\right) = \sum_{j=1}^{k}\alpha_j\overline{\psi}\left(\sum_{i=1}^{\ell} c_{ij}\mathbf{g}_i\right)$$

Since $\mathbf{x}_B = \mathbf{0}$ we have for all j that $\pi_B(\sum_{i=1}^{\ell} c_{ij}\mathbf{g}_i) = \mathbf{0}$ hence $\overline{\phi}(\mathbf{x}) = 0$. Hence B is a reconstructing set of $(L\langle C\rangle^{*d}, \overline{\phi})$.

That a privacy set for (C, ψ) is also a privacy set for $(L\langle C\rangle, \phi)$ is immediate using the condition in Remark 3.2. This shows that $(L\langle C\rangle, \phi)$ has t-disconnection. □

Lemma 6.5. *Let $C \subseteq K^n$ be a linear code, A be a finite-dimensional non-trivial K-algebra, and $\psi : C \to A$ be a surjective K-linear map. Let $B \subseteq [n]$ be a set which is not reconstructing for (C, ψ). Then B is a privacy set for $L\langle C\rangle$.*

Proof. Since B is not reconstructing, we have that $\psi(C_{\mathbf{0}\downarrow B}) \neq 0$. So let $s \in L$ be non-zero and in the image of $\psi(C_{\mathbf{0}\downarrow B})$, say $\psi(\mathbf{x}) = s \neq 0$ for some $\mathbf{x} \in C_{\mathbf{0}\downarrow B}$. Take $\lambda \in L$. $L\langle C\rangle$ is an L-vector space, hence $\lambda\mathbf{x} \in L\langle C\rangle$, but also $\lambda\mathbf{x} \in L\langle C\rangle_{\mathbf{0}\downarrow B}$ since $(\lambda\mathbf{x})_B = \mathbf{0}$. So $\psi\left(L\langle C\rangle_{\mathbf{0}\downarrow B}\right) \supseteq \psi\left(L\langle\mathbf{x}\rangle\right) = L\langle s\rangle = L$, hence B is a privacy set for $L\langle C\rangle$. □

Lemma 6.6. *Let G be a generator matrix for a Reed-Solomon code $C \subseteq K^n$. If $I \subseteq [n]$ is a subset of coordinates such that the projection C_I is of full dimension, i.e. $\dim_K C_I = \dim_K C$, and the I-indexed columns of G form a Vandermonde matrix G_I, then G is a Vandermonde matrix.*

Proof. Write $k := \dim C$, and let $\mathbf{g}_1, \ldots, \mathbf{g}_k$ denote the rows of G. If $k \leq 2$ then C is Reed-Solomon by default, so assume $k > 2$. Since C is Reed-Solomon, codewords $\mathbf{x} \in C$ correspond uniquely to polynomials $f \in K[X]_{<k}$. By Lagrange interpolation we can uniquely determine the polynomial f given $k = |I|$ points, and since G_I is Vandermonde we have that $f_i = X^{i-1}$ corresponds to row $\mathbf{g}_i$. It follows that G is also Vandermonde. □

Lemma 6.7. *Let $K \subseteq L$ be an extension of fields. Let $C \subseteq L \times K^n$ be a codex over K. Suppose $L\langle C\rangle \subseteq L^{n+1}$ is a Reed-Solomon code. Then C is extension field Reed-Solomon.*

Proof. Write $D := L\langle C\rangle$. Puncturing C, D by deleting the zeroth coordinate, we get codes C', D' with

$$\dim_K C' = \dim_K C = \dim_L D = \dim_L D'.$$

Since D is MDS, so is $D' = L\langle C'\rangle$, hence so is C' (as is easily seen from the definition of minimum distance and the Singleton bound). Thus C' also has a small square, and therefore must be Reed-Solomon.

Let G' be a generator matrix for C' with entries in K. Since a generator matrix for C' is also one for D', we know that D' is a Reed-Solomon code with some evaluation point sequence $(\alpha_1, \ldots, \alpha_n) \in K^n$. By Lemma 6.6 then D has a generator matrix of the form

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & g_n \\ g_0\alpha_0 & g_1\alpha_1 & \cdots & g_n\alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ g_0\alpha_0^{d-1} & g_1\alpha_1^{d-1} & \cdots & g_n\alpha_n^{d-1} \end{pmatrix}$$

Now, since the last n columns all have entries in K, we know G must also be a (generalized, the first column having entries in L) generator matrix of C, showing that C is of the desired form. □

We now use the above results to prove Theorem 1.5.

Theorem 1.5. *Let $t \geq 1$ be an integer, and let $K \subseteq L$ be an extension of finite fields of degree k. Then any $(3t + 2k - 1, t, 2, 2t + 2k - 1)$-arithmetic secret sharing scheme for L over K is given by Shamir's scheme.*

Proof. Let (C, ψ) be the arithmetic secret sharing scheme, and consider the K-vector space $\widetilde{C}$ from Proposition 3.11. First we show $L\langle\widetilde{C}\rangle$ is MDS. By Lemma 3.9 all coordinate sets of size $\leq t + k - 1$ are not reconstructing sets of C, hence by Lemma 6.5 they are privacy sets of $L\langle C\rangle$. Therefore $L\langle C\rangle$ has $(t + k - 1)$-privacy. Since by Lemma 6.4 we have $(2, 2t + 2k - 1)$-multiplicativity for $L\langle C\rangle$, it follows from Lemma 3.8 that $L\langle C\rangle$ has $(t + k)$-reconstruction, which implies $L\langle\widetilde{C}\rangle$ is MDS by Proposition 3.15 and $\dim L\langle\widetilde{C}\rangle = t + k$.

Using Equation (3) and applying Lemma 6.2 and Corollary 6.3 we get

$$\dim_K(C) = \dim_K(\widetilde{C}) = \dim_L(L\langle\widetilde{C}\rangle)$$
$$\dim_K(C^{*2}) = \dim_K(\widetilde{C}^{*2}) = \dim_L(L\langle\widetilde{C}\rangle^{*2})$$

This implies that $L\langle\widetilde{C}\rangle$ has a small square, so since it is MDS and $\dim L\langle\widetilde{C}\rangle = t+k < \frac{3t+2k-1}{2}$ we have that $L\langle\widetilde{C}\rangle$ is Reed-Solomon. We apply Lemma 6.7 and conclude that $\widetilde{C}$ is extension field Reed-Solomon. □

7 Generalizing to extension field codes

Rather than just regarding codices $C \subseteq \mathbb{F}_{q^k} \times \mathbb{F}_q^n$, we can consider arbitrary extension field codes where each coordinate is in some extension field of a finite base field K. We

can ask the same question as in the previous section: if $L\langle C\rangle$ is Reed-Solomon – or equivalently, an MDS code with a small square – does it follow that C is extension field Reed-Solomon?

To answer this question, we first note that we can have multiple linearly independent basis vectors in one coordinate, so $\dim_K C$ could be strictly larger than $\dim_L L\langle C\rangle$. For example, if the degree $[K(\eta_1) : K]$ is strictly larger than 1 we could have

$$C = K\langle (1, 0, \ldots, 0), (\eta_1, 0, \ldots, 0)\rangle$$

which has K-dimension 2, but $\dim_L L\langle C\rangle = 1$. To prevent this, we will assume that the dimension does not decrease when passing from C to $L\langle C\rangle$, i.e. $\dim_K C = \dim_L L\langle C\rangle$.

We can apply the puncturing argument from Lemma 6.7 given a few more assumptions. First, we will establish some intermediate lemmas.

Notation. In the remainder of this section, we will sometimes abuse notation slightly and whenever we write that an evaluation point α_i is in some field F, we will also allow it to be equal to ∞, and we assume that a scaling vector coordinate is never 0.

Lemma 7.1. *Let $C \subseteq K^n$ be a Reed-Solomon code of dimension $2 \leq k \leq n-2$. Given three arbitrary coordinates $J = \{j_1, j_2, j_3\}$, C has a unique evaluation point sequence $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in (K \cup \{\infty\})^n$ such that $\boldsymbol{\alpha}_J = (0, 1, \infty)$. Furthermore, the associated scaling vector $\mathbf{g} = (g_1, \ldots, g_n) \in (K^*)^n$ is unique up to a scalar multiple $(\lambda g_1, \ldots, \lambda g_n)$ for some $\lambda \in K^*$.*

Proof. Let $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n)$ be an evaluation point sequence for C. By Theorem 2.3 $\boldsymbol{\alpha} \in (K \cup \{\infty\})^n$ is also an evaluation point sequence for $\boldsymbol{\beta}$ if and only if there is some $f \in \mathrm{GL}(2, K)$ such that $f(\beta_i) = \alpha_i$ for all i.

By invariance under scalar multiplication, such transformations f correspond bijectively to the elements of $\mathrm{PGL}(2, K)$. Since this group is 3-transitive, there is $\bar{f} \in \mathrm{PGL}(2, K)$ mapping each $\beta_i \mapsto \alpha_i$, and in fact this $\bar{f}$ is unique (see e.g. [Uen05, Lemma 2.2]). If $(\beta_1, \beta_2, \beta_3) = (0, 1, \infty)$ then $\bar{f}$ must be the identity, hence $\alpha_i = \beta_i$ for all i. Since $cz + d = 1$, hence $\theta(f, z) = 1$, uniqueness of the scaling vector up to a scalar multiple also follows from Theorem 2.3. □

Lemma 7.2. *Let C be an extension field code of K on n coordinates, such that $L\langle C\rangle$ is Reed-Solomon and $\dim_K C = \dim_L L\langle C\rangle$. Let $I \subseteq [n]$ be a subset of coordinates of cardinality $|I| \geq 2 \dim_K C - 1$, and define $F := K(\bigcup_{i \in I} \eta_i)$ to be the compositum of the fields associated to the coordinates in I.*

Then there is an evaluation point sequence $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in (L \cup \{\infty\})^n$ and a scaling vector $\mathbf{g} = (g_1, \ldots, g_n) \in (L^*)^n$ for $L\langle C\rangle$ such that

$$\alpha_i, g_i \in \begin{cases} F & \text{for } i \in I \\ F(\eta_i) & \text{for } i \notin I \end{cases}$$

Furthermore, given the constraint that $\boldsymbol{\alpha}_J = (0, 1, \infty)$ on three distinguished coordinates $J \subseteq I$, $\boldsymbol{\alpha}$ is unique and $\mathbf{g}$ is unique up to a scalar multiple.

Proof. First, we observe that $F\langle C_I\rangle$ is an MDS code of dimension equal to $\dim_L L\langle C\rangle$: if $\{\mathbf{g}_1, \ldots, \mathbf{g}_k\}$ is a K-basis for C, then it is also an L-basis for $L\langle C\rangle$ by the assumption that the dimension does not decrease when passing to $L\langle C\rangle$. Then $\{(\mathbf{g}_1)_I, \ldots, (\mathbf{g}_k)_I\}$ is an F-basis for $F\langle C_I\rangle$. Since it is also an L-basis for the MDS code $L\langle C_I\rangle$, every k columns of its associated matrix are linearly independent.

From this we conclude that since

$$\begin{aligned} 2\dim_L L\langle C\rangle - 1 = \dim_L L\langle C\rangle^{*2} &\geq \dim_F F\langle C_I\rangle^{*2} \\ &\geq \min\{|I|, 2\dim_F F\langle C_I\rangle + 1\} = 2\dim_L L\langle C\rangle - 1 \end{aligned}$$

that $F\langle C_I\rangle$ is a Reed-Solomon code. Let $\boldsymbol{\beta} \in (F \cup \{\infty\})^{|I|}, \mathbf{y} \in (F^*)^{|I|}$ be the unique evaluation point sequence and scaling vector, respectively, for C_I for which $\boldsymbol{\beta}_J = (0, 1\infty)$ for some distinguished coordinates J. Since $L\langle C\rangle$ is Reed-Solomon, it also has a unique evaluation point sequence $\boldsymbol{\alpha}$ and scaling vector $\mathbf{g}$ for which $\boldsymbol{\alpha}_J = (0, 1, \infty)$. Because $L\langle F\langle C_I\rangle\rangle = L\langle C_I\rangle = (L\langle C\rangle)_I$ these vectors must be equal on the I-coordinates, we have $\alpha_i, g_i \in F$.

Picking any coordinate $i \notin I$, we can now choose to project on $I \cup \{i\}$, and get a Reed-Solomon code $F(\eta_i)\langle C_{I\cup\{i\}}\rangle$. In a similar fashion, we may conclude that $\alpha_i, g_i \in F(\eta_i)$. □

If we take two partially overlapping coordinate sets I, I' in Lemma 7.2, we can "glue" the corresponding evaluation point sequences and scaling vectors. Suppose $I, I' \subseteq [n]$ are subsets of coordinates as in Lemma 7.2, and let F, F' be their associated compositas. If $|I \cap I'| \geq 3$ then we get an evaluation point sequence $\boldsymbol{\alpha} \in (L \cup \{\infty\})^n$ and scaling vector $\mathbf{g} \in (L^*)^n$ with:

$$\alpha_i, g_i \in \begin{cases} F \cap F' & \text{for } i \in I \cap I' \\ (F \cap F')(\eta_i) & \text{for } i \notin I \cap I' \end{cases}$$

Using this method we get the following result.

Theorem 7.3. *Let C be an extension field code of K on n coordinates, such that $L\langle C\rangle$ is Reed-Solomon and $\dim_K C = \dim_L L\langle C\rangle$. Suppose at least three coordinates are in the base field K, and that we have t sets of coordinates $I_1, \ldots, I_t$, all of cardinality $|I_s| \geq 2\dim_K C - 4$ such that the intersection of the associated compositas for these coordinates is K. That is, let $F_s := K(\bigcup_{j\in I_s} \eta_j)$ be the compositum of all $K(\eta_j)$ with $j \in I_s$, and suppose that the intersection of fields $F_1 \cap F_2 \cap \cdots \cap F_t = K$.*

Then C is extension field Reed-Solomon:

$$C = \left\{(g_1 f(\alpha_1), \ldots, g_n f(\alpha_n)) \;\middle|\; f \in K[X]_{<k}\right\}$$

with for each i: $g_i, \alpha_i \in K(\eta_i)$.

Proof. Let $J \subseteq [n]$ be 3 coordinates j which have $\eta_j \in K$. Then, we can apply Lemma 7.2 to each of the sets $J \cup I_s$ for $s = 1, \ldots, t$ to get a unique evaluation point sequence $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ and scaling vector $\mathbf{g} = (g_1, \ldots, g_n)$ for $L\langle C\rangle$, which must satisfy, for each s:

$$\alpha_i, g_i \in \begin{cases} F_s & \text{for } i \in I_s \\ F_s(\eta_i) & \text{for } i \notin I_s \end{cases}$$

and thus each $\alpha_i, g_i \in (F_1 \cap \cdots \cap F_t)(\eta_i)$. □

8 Discussion

We have proved that Shamir's scheme is the only $(n, t, 2, n-t)$-arithmetic secret sharing scheme for a finite field K over K with a maximal adversary t. For a finite extension field L over K, we have shown that for an $(n, t, 2, n-t)$-arithmetic secret sharing scheme of L over L, we have

$$t \leq \frac{n-2k+1}{3} \tag{9}$$

and that such a scheme with t maximal must also be given by Shamir's scheme. While this bound holds for arithmetic secret sharing schemes for a field extension, the best known bound for arithmetic secret sharing schemes for an arbitrary K-algebra A is

$$t \leq \frac{n-k+1}{3}$$

It is conjectured in [Cas16] that this bound is not sharp, and that Equation (9) should hold. It would be interesting to investigate this further, and try to close the gap between the bounds.

To show our results, we used a linear version of Vosper's theorem, that transposes a classical result from additive combinatorics to the setting of coding theory. A natural avenue of further exploration would be to try to transpose other results from additive combinatorics to coding theory or other settings. Various results have already been achieved, for instance in [Lec14], [BL15], [MZ15].

Some results in this thesis might also be improved upon. The puncturing argument of Lemma 6.7 works well for the case of a codex of $\mathbb{F}_{q^k}/\mathbb{F}_q$, but has limitations in the general extension field case of Section 7. Perhaps another approach could lead to a stronger statement, e.g. one that is comparable to Theorem 1.5.

References

[ADL14] Divesh Aggarwal, Yevgeniy Dodis, and Shachar Lovett. "Non-malleable Codes from Additive Combinatorics". In: *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*. STOC '14. New York, New York: ACM, 2014, pp. 774–783. ISBN: 978-1-4503-2710-7. DOI: 10.1145/2591796.2591804.

[Bib13] Khodakhast Bibak. "Additive Combinatorics: With a View Towards Computer Science and Cryptography—An Exposition". In: *Number Theory and Related Fields: In Memory of Alf van der Poorten*. Ed. by M. Jonathan Borwein, Igor Shparlinski, and Wadim Zudilin. New York, NY: Springer New York, 2013, pp. 99–128. ISBN: 978-1-4614-6642-0. DOI: 10.1007/978-1-4614-6642-0_4.

[BL15] Vincent Beck and Cédric Lecouvey. *Additive combinatorics methods in associative algebras*. 2015.

[BSZ15] Christine Bachoc, Oriol Serra, and Gilles Zemor. "An analogue of Vosper's Theorem for Extension Fields". In: (2015).

[BTB88] A. A. Bruen, J. A. Thas, and A. Blokhuis. "On M.D.S. codes, arcs in PG(n, q) with q even, and a solution of three fundamental problems of B. Segre". In: *Inventiones mathematicae* 92.3 (1988), pp. 441–459. ISSN: 1432-1297. DOI: 10.1007/BF01393742.

[Cas16] Ignacio Cascudo. "Secret Sharing Schemes with Algebraic Properties and Applications". In: *Pursuit of the Universal: 12th Conference on Computability in Europe, CiE 2016, Paris, France, June 27 - July 1, 2016, Proceedings*. Ed. by Arnold Beckmann, Laurent Bienvenu, and Nataša Jonoska. Cham: Springer International Publishing, 2016, pp. 68–77. ISBN: 978-3-319-40189-8. DOI: 10.1007/978-3-319-40189-8_7.

[Cau13] A. Cauchy. "Recherches sur les nombres". In: *Journal de l'École polytechnique* 9 (1813), pp. 99–116.

[CCX12] Ignacio Cascudo, Ronald Cramer, and Chaoping Xing. "The arithmetic codex". In: *2012 IEEE Information Theory Workshop*. Institute of Electrical & Electronics Engineers (IEEE), Sept. 2012. DOI: 10.1109/itw.2012.6404767.

[CDM00] Ronald Cramer, Ivan Damgård, and Ueli Maurer. "General Secure Multiparty Computation from Any Linear Secret-sharing Scheme". In: *Proceedings of the 19th International Conference on Theory and Application of Cryptographic Techniques*. EUROCRYPT'00. Bruges, Belgium: Springer-Verlag, 2000, pp. 316–334. ISBN: 3-540-67517-5.

[CDN15] Ronald Cramer, Ivan Bjerre Damgård, and Jesper Buus Nielsen. *Secure Multiparty Computation and Secret Sharing*. Cambridge New York: Cambridge University Press, 2015. ISBN: 978-1107043053.

[Che+08] Hao Chen et al. "Strongly Multiplicative Ramp Schemes from High Degree Rational Points on Curves". In: *Advances in Cryptology – EUROCRYPT 2008: 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13-17, 2008. Proceedings*. Ed. by Nigel Smart. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 451–470. ISBN: 978-3-540-78967-3. DOI: 10.1007/978-3-540-78967-3_26.

[Coh+97] G. Cohen et al. *Covering codes*. Amsterdam New York: Elsevier, 1997. ISBN: 9780444825117.

[Cra11] Ronald Cramer. "The Arithmetic Codex: Theory and Applications". In: *Advances in Cryptology – EUROCRYPT 2011: 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings*. Ed. by Kenneth G. Paterson. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 1–1. ISBN: 978-3-642-20465-4. DOI: 10.1007/978-3-642-20465-4_1.

[CXY16] Ronald Cramer, Chaoping Xing, and Chen Yuan. *On Multi-Point Local Decoding of Reed-Muller Codes*. 2016.

[Dav35] H. Davenport. "On the addition of residue classes". In: *Journal of the London Mathematical Society* 1 (1935), pp. 30–32.

[Dür87] Arne Dür. "The automorphism groups of Reed-Solomon codes". In: *Journal of Combinatorial Theory, Series A* 44.1 (Jan. 1987), pp. 69–82. DOI: 10.1016/0097-3165(87)90060-4.

[Elk11] Michael Elkin. "An improved construction of progression-free sets". In: *Isr. J. Math.* 184.1 (July 2011), pp. 93–128. DOI: 10.1007/s11856-011-0061-1.

[Gre09] Ben Green. "Book Review - Additive Combinatorics by Terence C. Tao and Van H. Vu". In: *Bulletin (New Series) of the American Mathematical Society* 46.3 (July 2009), pp. 489–497.

[JX16] Lingfei Jin and Chaoping Xing. *New MDS Self-Dual Codes from Generalized Reed-Solomon Codes*. 2016.

[Köt92] R. Kötter. "A unified description of an error locating procedure for linear codes". In: *Proceedings of Algebraic and Combinatorial Coding Theory* (1992), pp. 113–117.

[Lec14] Cédric Lecouvey. "Plünnecke and Kneser type theorems for dimension estimates". In: *Combinatorica* 34.3 (2014), pp. 331–358. ISSN: 1439-6912. DOI: 10.1007/s00493-014-2874-0.

[Lip12] Helger Lipmaa. "Progression-Free Sets and Sublinear Pairing-Based Non-Interactive Zero-Knowledge Arguments". In: *Theory of Cryptography: 9th Theory of Cryptography Conference, TCC 2012, Taormina, Sicily, Italy, March 19-21, 2012. Proceedings*. Ed. by Ronald Cramer. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 169–189. ISBN: 978-3-642-28914-9. DOI: 10.1007/978-3-642-28914-9_10.

[LX04] San Ling and Chaoping Xing. *Coding Theory: A First Course*. Cambridge University Press, 2004. ISBN: 978-0521529235.

[MP16] Irene Márquez-Corbella and Ruud Pellikaan. "A characterization of {MDS} codes that have an error correcting pair". In: *Finite Fields and Their Applications* 40 (2016), pp. 224–245. ISSN: 1071-5797. DOI: http://dx.doi.org/10.1016/j.ffa.2016.04.004.

[MZ15] D. Mirandola and G. Zémor. "Critical Pairs for the Product Singleton Bound". In: *IEEE Transactions on Information Theory* 61.9 (Sept. 2015), pp. 4928–4937. ISSN: 0018-9448. DOI: 10.1109/TIT.2015.2450207.

[Pel92] Ruud Pellikaan. "On decoding by error location and dependent sets of error positions". In: *Discrete Mathematics* 106-107 (Sept. 1992), pp. 369–381. DOI: 10.1016/0012-365x(92)90567-y.

[Pel96] Ruud Pellikaan. "Shanghai Conference Issue on Designs, Codes, and Finite Geometries, Part I On the existence of error-correcting pairs". In: *Journal of Statistical Planning and Inference* 51.2 (1996), pp. 229–242. ISSN: 0378-3758. DOI: http://dx.doi.org/10.1016/0378-3758(95)00088-7.

[Ran15] Hugues Randriambololona. "On products and powers of linear codes under componentwise multiplication". In: *Proc. 14th International Conference on Arithmetic, Geometry, Cryptography, and Coding Theory (AGCT-14), Luminy, France*. 2015, pp. 3–7.

[Rød06] Ø. J. Rødseth. "Sumsets mod p". In: *Trans. R. Norw. Soc. Sci. Lett.* 4 (2006), pp. 1–10.

[San10] Tom Sanders. "On the Bogolyubov-Ruzsa lemma". In: (2010). DOI: 10.2140/apde.2012.5.627.

[Sha79] Adi Shamir. "How to Share a Secret". In: *Commun. ACM* 22.11 (Nov. 1979), pp. 612–613. ISSN: 0001-0782. DOI: 10.1145/359168.359176.

[Sin64] R. Singleton. "Maximum distance q-nary codes". In: *IEEE Trans. Inform. Theory* 10.2 (Apr. 1964), pp. 116–118. DOI: 10.1109/tit.1964.1053661.

[TV09] Terence Tao and Van H. Vu. *Additive Combinatorics (Cambridge Studies in Advanced Mathematics)*. 1st ed. Cambridge University Press, Dec. 2009. ISBN: 9780521136563.

[Uen05] Kenji Ueno. *An introduction to algebraic geometry*. Providence, RI: American Mathematical Society, 2005. ISBN: 978-0821811443.

[Vos56a] A. G. Vosper. "Addendum to "The Critical Pairs of Subsets of a Group of Prime Order"". In: *Journal of the London Mathematical Society* s1-31.3 (July 1956), pp. 280–282. DOI: 10.1112/jlms/s1-31.3.280.

[Vos56b] A. G. Vosper. "The Critical Pairs of Subsets of a Group of Prime Order". In: *Journal of the London Mathematical Society* s1-31.2 (Apr. 1956), pp. 200–205. DOI: 10.1112/jlms/s1-31.2.200.