Ideal-Theoretic Explanation of Capacity-Achieving Decoding

Siddharth Bhandari
Tata Institute of Fundamental Research, Mumbai, India

Prahladh Harsha
Tata Institute of Fundamental Research, Mumbai, India

Mrinal Kumar
Department of Computer Science and Engineering, IIT Bombay, India

Madhu Sudan
School of Engineering and Applied Sciences, Harvard University, Cambridge, MA, USA

Abstract

In this work, we present an abstract framework for some algebraic error-correcting codes with the aim of capturing codes that are list-decodable to capacity, along with their decoding algorithm. In the polynomial ideal framework, a code is specified by some ideals in a polynomial ring, messages are polynomials and their encoding is the residue modulo the ideals. We present an alternate way of viewing this class of codes in terms of linear operators, and show that this alternate view makes their algorithmic list-decodability amenable to analysis.

Our framework leads to a new class of codes that we call *affine Folded Reed-Solomon codes* (which are themselves a special case of the broader class we explore). These codes are common generalizations of the well-studied Folded Reed-Solomon codes and Univariate Multiplicity codes, while also capturing the less-studied Additive Folded Reed-Solomon codes as well as a large family of codes that were not previously known/studied.

More significantly our framework also captures the algorithmic list-decodability of the constituent codes. Specifically, we present a unified view of the decoding algorithm for ideal-theoretic codes and show that the decodability reduces to the analysis of the distance of some related codes. We show that good bounds on this distance lead to capacity-achieving performance of the underlying code, providing a unifying explanation of known capacity-achieving results. In the specific case of affine Folded Reed-Solomon codes, our framework shows that they are list-decodable up to capacity (for appropriate setting of the parameters), thereby unifying the previous results for Folded Reed-Solomon, Multiplicity and Additive Folded Reed-Solomon codes.

2012 ACM Subject Classification Mathematics of computing → Coding theory

Keywords and phrases List Decodability, List Decoding Capacity, Polynomial Ideal Codes, Multiplicity Codes, Folded Reed-Solomon Codes

Digital Object Identifier 10.4230/LIPIcs.APPROX/RANDOM.2021.56

Category RANDOM

Related Version *Full Version*: `https://arxiv.org/abs/2103.07930`
Full Version: `https://eccc.weizmann.ac.il/report/2021/036/`

Funding *Siddharth Bhandari & Prahladh Harsha:* Research supported by the Department of Atomic Energy, Government of India, under project 12-R&D-TFR-5.01-0500 and in part by the Google PhD and Swarnajayanti Fellowships.
Madhu Sudan: Supported in part by a Simons Investigator Award and NSF Award CCF 1715187.

Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2021).
Editors: Mary Wootters and Laura Sanità; Article No. 56; pp. 56:1–56:21
Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

1 Introduction

Reed-Solomon codes are obtained by evaluations of polynomial of degree less than k at n distinct points in a finite field $\mathbb{F}$. Folded-Reed-Solomon (FRS) codes are obtained by evaluating a polynomial at sn (carefully chosen) points that are grouped into n bundles of size s each, and then viewing the resulting sn evaluations as n elements of $\mathbb{F}^s$. Multiplicity codes are obtained by evaluating the polynomial, and $s-1$ of its derivatives and again viewing the resulting sn evaluations as n elements of $\mathbb{F}^s$.

This "bundling" (or folding, as it is called for FRS codes) in FRS codes and Multiplicity codes may be viewed at best as a harmless operation – it does not hurt the rate and (relative) distance of a code which is already optimal in these parameters. But far from merely being harmless, in the context algorithmic list-decoding, bundling has led to remarkable improvements and to two of the very few explicit capacity achieving codes in the literature. Indeed the only other codes that achieve list-decoding capacity algorithmically and do not use one of the above codes as an ingredient are the Folded Algebraic-Geometric codes, which also use bundling. Despite this central role, the bundling operation is not well-understood algebraically. Indeed it seems like an "adhoc" operation rather than a principled one. Unearthing what bundling is and understanding when and why it turns out to be so powerful is the primary goal of this work, and we make some progress towards this.

Turning to the algorithms for list-decoding the above codes close to capacity, there are two significantly different ones in the literature. A (later) algorithm due to Guruswami and Wang [6][1] which seems more generalizable, and the original algorithm of Guruswami and Rudra [3] which is significantly more challenging to apply to multiplicity codes (see [9]). In both cases, while the algorithm for FRS works in all (reasonable) settings, the algorithms for multiplicity codes only work when the characteristic of the field is larger than the degrees of the polynomials in question. Looking more closely at FRS codes, part of the careful choice of bundling in FRS codes is to pick each bundle to be a geometric progression. If one were to switch this to an arithmetic progression, then one would get a less-studied family codes called the Additive-FRS. It turns out the Additive-FRS codes are also known to be list-decodable to capacity but only via the original algorithm. Thus, the short summary of algorithmic list-decoding is that there is no short summary! Algorithms tend to work but we need to choose carefully and read the fine print.

The goal of this paper is to provide a unifying algebraic framework that (a) captures bundling algebraically, (b) captures most of the algorithmic success also algebraically, leaving well-defined parts for combinatorial analysis and (c) leads to new codes that also achieve capacity. In this work we use basic notions from linear algebra and polynomial rings to present a unifying definition (see Definitions 3.1 and 4.4) that captures the codes very generally, and also the decoding ability (see Theorem 1.1). We elaborate on these below.

Polynomial ideal codes

Our starting point is what we term "polynomial ideal codes". A *polynomial ideal code* over a finite field $\mathbb{F}$ and parameters k, s is specified by n pairwise relatively prime monic polynomials $E_0(X), \ldots, E_{n-1}(X) \in \mathbb{F}[X]$of degree equal to s.[2] The encoding maps a message $p \in \mathbb{F}^k$

[1] We note that the Guruswami-Wang algorithm is inspired by an idea due to Vadhan [12, Theorem 5.24] that shows that it suffices to interpolate a polynomial Q which is linear in the y-variables. However, the algorithm from [12] is not applicable to our setting since it uses polynomial factorization as well as analysis tools that are specific to Reed-Solomon codes. The further simplifications developed in [6] are key to the applicability in our setting.

[2] Here $\mathbb{F}[X]$ refers to the ring of univariate polynomials in the variable X over the field $\mathbb{F}$ while $\mathbb{F}_{<k}[X]$ refers to the vector-space of polynomials in $\mathbb{F}[X]$ of degree strictly less than k.

(interpreted as a polynomial of degree less than k) to n symbols as follows:

$$\begin{aligned} \mathbb{F}_{<k}[X] &\longrightarrow (\mathbb{F}_{<s}[X])^n \\ p(X) &\longmapsto (p(X) \pmod{E_i(X)})_{i=0}^{n-1} \end{aligned}$$

The codes described above, Reed-Solomon, FRS, Multiplicity and Additive-FRS, are all examples of polynomial ideal codes. For Reed-Solomon codes, this is folklore knowledge: the evaluation point a_i corresponds to going mod $E_i(X) = (X - a_i)$. For any bundling of the Reed-Solomon codes this follows by taking product of the corresponding polynomials. For multiplicity codes of order s, the evaluation of a polynomial and its derivatives at a_i corresponds to going modulo $E_i(X) = (X - a_i)^s$.

The abstraction of polynomial ideal codes is not new to this work. Indeed Guruswami, Sahai and Sudan [4, Appendix A] already proposed these codes as a good abstraction of algebraic codes. Their framework is even more general, in particular they even consider non-polynomial ideals such as in $\mathbb{Z}$. They suggest algorithmic possibilities but do not flesh out the details. In this work we show that polynomial ideal codes, as we define them, are indeed list-decodable up to the Johnson radius. We note that the proof involves some steps not indicated in the previous work but for the most part this confirms the previous thinking.

The abstraction above also captures "bundling" (or folding) nicely - we get them by choosing $E_i(X)$ to be a product of some $E_{ij}(X)$. But the above abstraction thus far fails to capture the capacity-achieving aspects of the codes (i.e., the benefits of this bundling) and the decoding algorithms. This leads us to the two main *novel* steps of this paper:

- We present an alternate viewpoint of polynomial ideal *codes* in terms of *linear operators*.
- We abstract the Guruswami-Wang linear-algebraic list-decoding *algorithm* in terms of *linear operators*.

The two sets of "linear operators", in the codes and in the decoding algorithm, are not the same. But the linearity of both allows them to interact nicely with each other. We elaborate further below after introducing them.

Linear operator codes

In this work, a linear operator is an $\mathbb{F}$-linear function $L : \mathbb{F}[X] \to \mathbb{F}[X]$. A *linear operator code* is characterized by a family of linear operators $\mathcal{L} = (L_0, \ldots, L_{s-1})$, a set $A = \{a_0, \ldots, a_{n-1}\} \subseteq \mathbb{F}$ of evaluation points and k a degree parameter such that $k \leq s \cdot n$. The corresponding linear operator code, denoted by $LO_k^A(\mathcal{L})$, is given as follows:

$$\begin{aligned} \mathbb{F}_{<k}[X] &\longrightarrow (\mathbb{F}^s)^n \\ p(X) &\longmapsto (\mathcal{L}(p)(a_i))_{i=0}^{n-1} \end{aligned}$$

Linear operator codes easily capture polynomial ideal codes. For instance, the multiplicity codes are linear operator codes wherein the linear operators are the successive derivative operators. But they are also too general – even if we restrict the operators to map $\mathbb{F}_{<k}[X]$ to itself, an operator allows k^2 degrees of freedom.

We narrow this broad family by looking subfamilies of linear operators and codes. The specific subfamily we turn are what we call "ideal linear operators". We say that linear operators $L_0, \ldots, L_{s-1}$ are *ideal linear operators* with respect to a set A of evaluation points if for every $a \in A$, the vector space

$$I^a(\mathcal{L}) = \{p \in \mathbb{F}[X] \mid \mathcal{L}(p)(a) = \bar{0}\}$$

is an ideal. (When the set of evaluation points is clear from context, we drop the phrase "with respect to A".) Linear operator codes corresponding to ideal linear operators are called *ideal linear operator codes* (see Definitions 4.1 and 4.4 for precise definitions).

It is not hard to see that a family of linear operators $\mathcal{L} = (L_0, \ldots, L_{s-1})$ has the ideal property if is satisfies the following *linearly-extendibility* property: There exists a matrix $M(X) \in \mathbb{F}[X]^{s\times s}$ such that for all $p \in \mathbb{F}[X]$ we have

$$\mathcal{L}(X \cdot p(X)) = M(X) \cdot \mathcal{L}(p(X)).$$

This motivates yet another class of linear operators and code: We say that an operator family $\mathcal{L}$ is a *linearly-extendible linear operator* if such a matrix $M(X)$ exists and the resulting code is said to be a *linearly-extendible linear operator code* (see Definitions 4.2 and 4.4 for precise definitions).

It turns out that these three definitions of codes – polynomial ideal codes, ideal linear operator codes and linearly-extendible linear operator codes – are equivalent (see Propositions 4.6 and 4.8 and Corollary 4.9). And while the notion of polynomial ideal codes captures the codes mentioned thus far naturally, the equivalent notion of linearly-extendible codes provides a path to understanding the applicability of the linear-algebraic list-decoding algorithm of Guruswami and Wang.

While it is not the case that every linearly-extendible linear operator code (and thus every polynomial ideal code) is amenable to this list-decoding algorithm, it turns out that one can extract a nice sufficient condition on the linear-extendibility for the algorithm to be well-defined. This allows us to turn the question of list-decodability into a quantitative one – how many errors can be corrected. And the linear operator framework now converts this question into analyzing the rank of an associated matrix.

The sufficient condition we extract is the following: we say that an operator $L : \mathbb{F}[X] \to \mathbb{F}[X]$ is degree-preserving if $\deg_X(Lf) \leq \deg_X(f)$ for all $f \in \mathbb{F}[X]$. Observe that any degree-preserving linear operator when restricted to $\mathbb{F}_{<k}[X]$ can be represented by an upper-triangular matrix in $\mathbb{F}^{k\times k}$. A family of linear operators obtained by repeated iteration, $\mathcal{L} = (I = L^0, L = L^1, L^2, \ldots, L^{s-1})$ is called an *iterative* family. We associate with any degree-preserving family $\mathcal{L} = (L_0, \ldots, L_{s-1})$ of linear operators a simple matrix in $\mathbb{F}^{s\times k}$ called $\mathrm{Diag}(\mathcal{L})$, whose ith row is the diagonal of L_i and consider the code in $\mathbb{F}^k$ generated by $\mathrm{Diag}(\mathcal{L})$.

The following theorem now shows that for any degree-preserving iterative linearly-extendible operator codes, lower bound on the distance of $\mathrm{Diag}(\mathcal{L})$ yields an upper bound on the list size obtained by the Guruswami-Wang algorithm, even when the number of errors approaches $(1 - \text{rate})$ of the code.

▶ **Theorem 1.1.** *Suppose $L : \mathbb{F}[X] \to \mathbb{F}[X]$ is a degree-preserving linear operator and A a set of evaluation points such that for $\mathcal{L} = (L^0, L^1, \ldots, L^{s-1})$ the corresponding code $\mathcal{C}$ is a linearly-extendible linear operator code. Furthermore, if the matrix $\mathrm{Diag}(\mathcal{L}) \in \mathbb{F}^{s\times k}$ formed by stacking the diagonals of the s linear operators as the rows is the generator matrix of a code with distance $1 - \frac{\ell}{k}$, then, $\mathcal{C}$ is list-decodable up to the distance $1 - \frac{k}{(s-m+1)n} - \frac{1}{m}$ with list size q^ℓ for any $1 \leq m \leq s$.*

We remark that our actual theorem is more general (see Theorem 5.2) where we further separate the role of linear operators used to build the code, from those that seed the decoding algorithm. But it immediately implies Theorem 1.1 above, which in turn already suffices to capture the capacity achieving decodability of FRS, multiplicity and additive-FRS codes. Regarding the aspect of the need to lower bound the distance of the code generated by

$Diag(\mathcal{L})$, to bound the list size of the codes, we stress that for each of these codes the lower bound on the distance follows from fairly simple arguments. Indeed the generality of the arguments allows us to capture broader families of codes uniformly, as described next.

A Common Generalization

Our framework leads very naturally to a *new* class of codes that we call the *Affine Folded Reed-Solomon* (Affine-FRS) codes: these are codes defined by ideals of the form $\prod_{i=0}^{s-1}(X - \ell^{(i)}(a))$ where $\ell(z) = \alpha z + \beta$ is any linear form and $\ell^{(i)}(z) = \underbrace{\ell(\ell \ldots \ell(z) \ldots)}_{i \text{ times}}$. These codes generalize all the previously considered codes: The case $\ell(z) = \gamma z$ are the FRS codes, the case $\ell(z) = z$ are the Multiplicity codes, and the case $\ell(z) = z + \beta$ are the Additive FRS codes!

▶ **Theorem 1.2** (Informal statement – see Theorem A.8). *Let ℓ be any linear form such that either $\operatorname{ord}(\ell) \geq k$ or $(\operatorname{char}(\mathbb{F}) \geq k$ and $\beta \neq 0)$* [3]*. Then the Affine-FRS codes corresponding to the linear form ℓ are list-decodable up to capacity.*

Previously, even for the special case of the Additive FRS codes, list-decodability close to capacity was only achieved by the more involved algorithm of Guruswami & Rudra [3] and Kopparty [9] (see paragraph on Additive Folding and Footnote 4 in [2, Section III]). (A similar approach can be extended to cover the case of $\operatorname{ord}(\ell) \geq k$ in Theorem 1.2: however, it seems difficult to do so for the case when $\operatorname{ord}(\ell)$ is small.)

Thus, our Affine-FRS codes lead to the first common abstraction of the three codes as well as the first common algorithm for solving the list-decoding problem for these codes. (Furthermore, this algorithm is linear-algebraic.)‘ Arguably thus, even if the Affine-FRS codes had been studied previously, it is not clear that the ability to decode them for every choice of $\ell(z)$ would be obvious.

Organization

The rest of the paper is organized as follows. We begin with some preliminaries in Section 2. We then formally define polynomial ideal codes and linear operator codes in Sections 3 and 4 respectively. In Section 5, we discuss list-decoding algorithms for polynomial ideal codes. We first present the list-decoding algorithm for *all* polynomial ideal codes up to the Johnson radius in Section 5.1 and then the list-decoding algorithm beyond the Johnson radius for special families of linear operator codes in Section 5.2. Finally, we conclude by demonstrating how these results can be used to show that several well-known families of codes (Folded Reed-Solomon, multiplicity, additive Folded Reed-Solomon codes) as well as their common generalization affine folded Reed-Solomon achieve list-decoding capacity in Appendix A.

Throughout the paper, we skip the proofs of various claims due to space constraints. We refer the interested reader to the full version of the paper [1] for the complete proofs.

2 Notations and Preliminaries

We start with some notations that we follow in the rest of this paper.

- For a natural number n, $[n]$ denotes the set $\{0, 1, \ldots, n-1\}$.
- $\mathbb{F}$ denotes a field.

[3] $\operatorname{ord}(\ell)$ refers to the smallest positive integer u such that $\ell^{(u)}(z) = z$.

- For $a, b, i, j \in \mathbb{Z}$, where $a, b, i, j \geq 0$ the bivariate monomial X^iY^j is said to have (a, b)-weighted degree at most d if $ai + bj \leq d$. $N(a, b)$ denotes the number of bivariate monomials of $(1, a)$-weighted degree at most b.
- For $a, b \in \mathbb{Z}$, a bivariate polynomial $Q(X, Y)$ is said to have (a, b)-weighted degree at most d, if it is supported on monomials of (a, b)-weighted degree at most d.
- We say that a function $f(n) : \mathbb{N} \to \mathbb{N}$ is $\mathsf{poly}(n)$, if there are constants $c, n_0 \in \mathbb{N}$ such that for all $n \geq n_0$, $f(n) \leq n^c$.
- $\mathbb{F}[X]$ is the ring of univariate polynomials with coefficients in $\mathbb{F}$, and for every $k \in \mathbb{N}$, $\mathbb{F}_{<k}[X]$ denotes the set of polynomials in $\mathbb{F}[X]$ of degree strictly less than k.
- For a multivariate polynomial $f(X_0, X_1, \ldots, X_{n-1}) \in \mathbb{F}[X_0, X_1, \ldots, X_{n-1}]$, $\deg_{X_i}(f)$ denotes the degree of f, when viewing it as a univariate in X_i, with coefficients in the polynomial ring on the remaining variables over the field $\mathbb{F}$.

Estimates on $N(a, b)$

We rely on the following simple lemma to estimate the number of bivariate monomials with $(1, a)$-weighted degree at most b. See the full version [1] for the proof.

▶ **Lemma 2.1.** *For every $a, b \in \mathbb{N}$, let $N(a, b)$ denote the number of bivariate monomials with $(1, a)$-weighted degree at most b. Then, the following are true.*

1. $N(a - 1, b) \geq b^2/2a$.
2. *For every $\eta \in \mathbb{N}$, if a divides b, then*

$$N(a, b) - N(a, b - a\eta) - \eta(b - a\eta + 1) = a\eta(\eta + 1)/2\,.$$

Johnson radius

▶ **Theorem 2.2** (List decoding up to Johnson radius). *Let $q \in \mathbb{N}$ be a natural number. Any code with block length n and relative distance δ over an alphabet of size q is (combinatorially) list decodable from $(1 - \sqrt{(1 - \delta)})$ fraction of errors with list size at most $n^2q\delta$.*

We have the following bound for codes, referred to popularly as the *Singleton bound* [11], though the bound appears earlier in the works of Joshi [7] and Komamiya [8].

▶ **Theorem 2.3** (Komamiya-Joshi-Singleton bound). *The rate R and the relative distance δ of a code satisfy $R + \delta \leq 1 + o(1)$.*

In particular, for codes which lie on the Komamiya-Joshi-Singleton bound, we have that they are combinatorially list decodable from $1 - \sqrt{R} - o(1)$ fraction errors with polynomial list size.

List-decoding upto capacity

▶ **Definition 2.4** (List-decoding Capacity). *Consider a family of codes $\mathcal{C} = \{C_1, \ldots, C_n, \ldots\}$ where C_n has rate ρ_n and block length n with alphabet Σ_n. Then, $\mathcal{C}$ is said to achieve list-decoding capacity if $\forall \varepsilon > 0$ there exists an n_0 such that $\forall n \geq n_0$ and all received words $w \in \Sigma^n$, there exists at most a polynomial number of codewords $c \in C_n$ such that $\delta(c, w) \leq (1 - \rho_n(1 + \varepsilon))$.*

Further, if there exists an efficient algorithm for finding all these codewords, then, $\mathcal{C}$ is said to achieve list-decoding capacity efficiently. Ideally, we want to keep Σ_n as small as possible.

Chinese remainder theorem

We also rely on the following version of the Chinese Remainder Theorem for the polynomial ring.

▶ **Theorem 2.5.** *Let $E_0(X), E_1(X), \ldots, E_{s-1}(X)$ be univariate polynomials of degree equal to d over a field $\mathbb{F}$ such that for every distinct $i, j \in [s]$, E_i and E_j are relatively prime. Then, for every s-tuple of polynomials $(r_0(X), \ldots, r_{s-1}(X)) \in \mathbb{F}[X]^s$ such that each r_i is of degree strictly less than d (or zero), there is a unique polynomial $p(X) \in \mathbb{F}[X]$ of degree at most $d^s - 1$ such that for all $i \in [s]$,*

$$p(X) = r_i(X) \mod E_i(X)\,.$$

Polynomial ideals

▶ **Definition 2.6.** *A subset $I \subseteq \mathbb{F}[X]$ of polynomials is said to be an ideal if the following are true.*

- $0 \in I$.
- *For all $p(X), q(X) \in I$, $p + q \in I$.*
- *For every $p(X) \in I$ and $q(X) \in \mathbb{F}[X]$, $p(X) \cdot q(X) \in I$.*

For the univariate polynomial ring $\mathbb{F}[X]$, we also know that every ideal I is principal, i.e. there exists a polynomial $p(X) \in I$ such that

$$I = \{p(X)q(X) : q(X) \in \mathbb{F}[X]\}\,.$$

3 Polynomial ideal codes

In this section, we discuss polynomial ideal codes in more detail, and see how this framework captures some of the well studied families of algebraic error correcting codes.

We start with the formal definition of polynomial ideal codes.

▶ **Definition 3.1** (polynomial ideal codes)**.** *Given a field $\mathbb{F}$, parameters s, k and n satisfying $k < s \cdot n$, the polynomial ideal code is specified by a family of n polynomials $E_0, \ldots, E_{n-1}$ in the ring $\mathbb{F}[X]$ of univariate polynomials over the field $\mathbb{F}$ satisfying the following properties.*

1. *For all $i \in [n]$, polynomial E_i has degree exactly s.*
2. *The E_i's are* monic *polynomials.*
3. *The polynomials E_i's are pairwise relatively prime.*

The encoding of the polynomial ideal code maps is as follows:

$$\mathbb{F}_{<k}[X] \longrightarrow (\mathbb{F}_{<s}[X])^n$$
$$p(X) \longmapsto (p(X) \pmod{E_i(X)})_{i=0}^{n-1}$$

As is clear from the definition, polynomial ideal codes are linear over $\mathbb{F}$ and have rate k/sn and relative distance $(1 - (k-1)/sn)$. Since the sum of rate and relative distance satisfy the Komamiya-Joshi-Singleton bound, these codes are maximal-distance separable (MDS) codes.

We note that in general, E_i's need not have the same degree, but for notational convenience, we work in the setting when each of them is of degree equal to s. We also note that these codes continue to be well defined even if the E_i's are not relatively prime. In this case, the condition, $k < s \cdot n$ is replaced by k being less than the degree of the lowest common multiple of $E_0, E_1, \ldots, E_{n-1}$. However, the distance of the code suffers in this case, and such codes need not approach the Komamiya-Joshi-Singleton bound. We now observe that some of the standard and well studied family of algebraic error correcting codes are in fact instances of polynomial ideal codes for appropriate choice of $E_0, E_1, \ldots, E_{n-1}$.

3.1 Some well known codes via polynomial ideals

The message space for all these codes is identified with univariate polynomials of degree at most $k-1$ in $\mathbb{F}[X]$. We assume that the underlying field $\mathbb{F}$ is of size at least n for this discussion, else, we work over a large enough extension of $\mathbb{F}$.

Reed-Solomon Codes

Let $a_0, a_1, \ldots, a_{n-1}$ be n distinct elements of $\mathbb{F}$. In a Reed-Solomon code, we encode a message polynomial $p(X) \in \mathbb{F}[X]_{<k}$ by its evaluation on $a_0, a_1, \ldots, a_{n-1}$. To view these as a polynomial ideal code, observe that $p(a_i) = p(X) \mod (X - a_i)$. Thus, we can set the polynomials $E_i(X)$ in Definition 3.1 to be equal to $(X - a_i)$ for each $i \in [n]$. Thus, $s = 1$. Clearly, the E_i's are relatively prime since $a_0, a_1, \ldots, a_{n-1}$ are distinct.

Folded Reed-Solomon Codes [3]

Let $\gamma \in \mathbb{F}_q^*$ be an element of multiplicative order at least s, i.e. $\gamma^0, \gamma, \ldots, \gamma^{s-1}$ are all distinct field elements. Further, let the set of evaluation points be $A = \{a_0, \ldots, a_{n-1}\}$ such that for any two distinct i and j the sets $\left\{a_i, a_i\gamma, \ldots, a_i\gamma^{s-1}\right\}$ and $\left\{a_j, a_j\gamma, \ldots, a_j\gamma^{s-1}\right\}$ are disjoint. In a Folded Reed-Solomon code, with block length n and folding parameter s is defined by the following encoding function.

$$p(X) \longmapsto \left(p(a_i), p(a_i\gamma^1), \ldots, p(a_i\gamma^{(s-1)})\right)_{i=0}^{n-1}$$

Thus, these are codes over the alphabet $\mathbb{F}^s$.

To view these as polynomial ideal codes, we set $E_i(X) = \prod_{j=0}^{s-1}(X - a_i\gamma^j)$. Clearly, each such E_i is a polynomial of degree equal to s, and since for any two distinct i and j the sets $\left\{a_i, a_i\gamma, \ldots, a_i\gamma^{s-1}\right\}$ and $\left\{a_j, a_j\gamma, \ldots, a_j\gamma^{s-1}\right\}$ are disjoint, the polynomials $E_0, E_1, \ldots, E_{n-1}$ are all relatively prime.

To see the equivalence between these two viewpoints observe that $p(a_i\gamma^j) = p(X) \mod (X - a_i\gamma^j)$. Moreover, $(X - a_i\gamma^j)$ are all relatively prime as j varies in $[s]$ for every $i \in [n]$. Thus, by the Chinese Remainder Theorem over $\mathbb{F}[X]$, there is a bijection between remainders of a polynomial modulo $\{(X - a_i\gamma^j) : j \in [s]\}$ and the remainder modulo the product $E_i = \prod_{j\in[s]}(X - a_i\gamma^j)$ of these polynomials.

Additive Folded Reed-Solomon Codes [3]

Additive Folded Reed-Solomon codes are a variant of the Folded Reed-Solomon codes defined above. Let $\mathbb{F}_q$ have characteristic at least s and let $\beta \in \mathbb{F}_q^*$. Further, let the set of evaluation points be $A = \{a_0, \ldots, a_{n-1}\}$ where $a_i - a_j \notin \{0, \beta, 2\beta, \ldots, (s-1)\beta\}$ for distinct i and j. Here, s denotes the folding parameter. The encoding is defined as follows.

$$p(X) \longmapsto (p(a_i), p(a_i + \beta), \ldots, p(a_i + \beta(s-1)))_{i=0}^{n-1}$$

Thus, these are also codes over the alphabet $\mathbb{F}^s$.

To view these as polynomial ideal codes, we set $E_i(X) = \prod_{j=0}^{s-1}(X - a_i + \beta j)$. Clearly, each such E_i is a polynomial of degree equal to s, and since $a_i - a_j \notin \{0, \beta, 2\beta, \ldots, (s-1)\beta\}$ for distinct i and j, the polynomials $E_0, E_1, \ldots, E_{n-1}$ are all relatively prime.

To see the equivalence between the two definitions, the argument is again identical to that for Folded Reed-Solomon codes discussed earlier in this section. We just observe $(X - a_i + \beta j)$ are all relatively prime j varies in $[s]$ for every $i \in [n]$, and thus by the Chinese Remainder

Theorem over $\mathbb{F}[X]$, there is a bijection between remainders of a polynomial modulo $\{(X - a_i + \beta j) : j \in [s]\}$ and the remainder modulo the product $E_i = \prod_{j\in[s]}(X - a_i + \beta j)$ of these polynomials.

Univariate Multiplicity Codes [10]

Univariate multiplicity codes, or simply multiplicity codes are a variant of Reed-Solomon, where in addition to the evaluation of the message polynomial at every a_i, we also give the evaluation of its derivatives of up to order $s-1$. While they can be defined over all fields, for the exposition in this paper, we consider these codes over fields $\mathbb{F}$ of characteristic at least sn. Moreover, we also work with the standard derivatives (from analysis), as opposed to Hasse derivatives which is typically the convention in coding theoretic context. Let $a_0, a_1, \ldots, a_{n-1} \in \mathbb{F}$ be distinct field elements.

The encoding is defined as follows.

$$p(X) \longmapsto \left(p(a_i), \frac{\partial p}{\partial X}(a_i), \ldots, \frac{\partial^{s-1} p}{\partial X^{s-1}}(a_i)\right)_{i=0}^{n-1}$$

Here, $\frac{\partial^j p}{\partial X^{j-1}}$ denotes the (standard) jth order derivative of p with respect to X.

To view these as polynomial ideal codes, we set $E_i(X) = (X - a_i)^s$. Clearly, each such E_i is a polynomial of degree equal to s, and since a_i's are all distinct, these polynomials $E_0, E_1, \ldots, E_{n-1}$ are all relatively prime.

The equivalence of these two definitions follows from an application of Taylor's theorem to univariate polynomials, which says the following.

$$\begin{aligned} p(X) &= p(a_i + X - a_i) \\ &= p(a_i) + (X - a_i)\frac{\partial p}{\partial X}(a_i) + \cdots + \frac{1}{(s-1)!}(X - a_i)^{s-1}\frac{\partial^{s-1} p}{\partial X^{s-1}}(a_i) + (X - a_i)^s \cdot q(X) \end{aligned}$$

for some polynomial $q(X) \in \mathbb{F}[X]$. Thus,

$$p(X) \mod (X - a_i)^s = p(a_i) + (X - a_i)\frac{\partial p}{\partial X}(a_i) + \cdots + \frac{1}{(s-1)!}(X - a_i)^{s-1}\frac{\partial^{s-1} p}{\partial X^{s-1}}(a_i).$$

Therefore, $p(X) \mod (X - a_i)^s$ we can *read* off the evaluations of the derivatives of p of order up to $s-1$ at a_i by explicitly writing $p(X) \mod (X - a_i)^s$ as a polynomial in $(X - a_i)$ (via interpolation for instance), and reading off the various coefficients. Similarly, using the above expression, given the evaluation of all the derivatives of order up to $s-1$ of p at a_i, we can also reconstruct $p(X) \mod (X - a_i)^s$.

Affine Folded Reed-Solomon Codes

We now describe a common generalization of the codes defined above, which we call Affine Folded Reed-Solomon Codes. Fix integers k, n, q with $n \leq q$. Let $\alpha \in \mathbb{F}_q^*$ and $\beta \in \mathbb{F}_q$ such that the multiplicative order of α is u. Further, define $\ell(X) = \alpha X + \beta$ and

$$\ell^{(i)}(X) = \underbrace{\ell(\ell \ldots \ell(X))}_{i \text{ times}} = \alpha^i X + \beta \cdot \sum_{j=0}^{i-1} \alpha^j = \alpha_i X + \beta_i.$$

In fact, if $\alpha \neq 1$, i.e, $u > 1$ then, $\beta_u = \beta \cdot \sum_{j=0}^{u-1} \alpha^j = 0$ and hence $\ell^{(u)}(X) = \ell^{(0)}(X)$. Let $\mathrm{ord}(\ell)$ denote the smallest positive integer t such that $\ell^{(t)}(X) = X$. The message space of the Affine Folded Reed-Solomon code of degree k with block length n and folding parameter s is polynomials of degree at most $k-1$ over $\mathbb{F}[X]$, i.e., $\mathbb{F}_{<k}[X]$ where $\mathbb{F} = \mathbb{F}_q$. Let the set of evaluation points be $A = \{a_0, \ldots, a_{n-1}\}$ such that for distinct i, j the sets $\left\{\ell^{(0)}(a_i), \ldots, \ell^{(s-1)}(a_i)\right\}$ and $\left\{\ell^{(0)}(a_j), \ldots, \ell^{(s-1)}(a_j)\right\}$ are disjoint.

The encoding function of Affine Folded Reed-Solomon Codes is given as: (Recall that $t = \operatorname{ord}(\ell)$; let $s = v \cdot t + r$ where $r < t$.)

$$p(X) \longmapsto \begin{pmatrix} p(\ell^{(0)}(a_i)) & \frac{\partial p}{\partial X}(\ell^{(0)}(a_i)) & \ldots & \frac{\partial^{v-1} p}{\partial X^{v-1}}(\ell^{(0)}(a_i)) & \frac{\partial^{v} p}{\partial X^{v}}(\ell^{(0)}(a_i)) \\ \vdots & \vdots & \ldots & \vdots & \vdots \\ \vdots & \vdots & \ldots & \vdots & \frac{\partial^{v} p}{\partial X^{v}}(\ell^{(r-1)}(a_i)) \\ p(\ell^{(t-1)}(a_i)) & \frac{\partial p}{\partial X}(\ell^{(t-1)}(a_i)) & \ldots & \frac{\partial^{v-1} p}{\partial X^{v-1}}(\ell^{(t-1)}(a_i)) & \end{pmatrix}_{i=0}^{n-1}.$$

Thus, these are also codes over the alphabet $\mathbb{F}^s$.

To view these as polynomial ideal codes we set

$$E_i(X) = \prod_{j=0}^{s-1}(X - \alpha_j a_i - \beta_j) = \prod_{j=0}^{r-1}(X - \ell^{(j)}(a_i))^{v+1} \cdot \prod_{j=r}^{t-1}(X - \ell^{(j)}(a_i))^{v}.$$

For the choice of A as above, the polynomials $E_i = E(X, a_i)$ are pairwise co-prime. Similar to the previous cases of Folded/Additive Reed-Solomon and Multiplicy codes we have a bijection between the remainders of a polynomial modulo E_i and the encoding of the polynomial at a_i.

3.2 An alternate definition

We now discuss an alternate definition of polynomial ideal codes; the advantage being that this definition ties together the polynomials $E_0, E_1, \ldots, E_{n-1}$ into a single bivariate polynomial. This would be useful later on when we discuss the connection between polynomial ideal codes and linear operator codes.

▶ **Definition 3.2** (polynomial ideal codes (in terms of bivariate polynomials)). *Given a field $\mathbb{F}$, parameters s, k and n satisfying $k < s \cdot n$, the polynomial ideal code is specified by a bivariate polynomial $E(X, Y)$ over the field $\mathbb{F}$ and a set of n field elements $a_0, a_1 \ldots, a_{n-1}$ in $\mathbb{F}$ satisfying the following properties.*

1. $\deg_X E(X, Y) = s$.
2. *$E(X, Y)$ is a* monic *polynomial in the variable X.*
3. *The polynomials $E(X, a_i)$'s are pairwise relatively prime.*

Since E is monic and has (exact) degree s in the variable X, any polynomial $p \in \mathbb{F}[X]$ has the following unique representation.

$$p(X) = Q^{(p)}(X, Y) \cdot E(X, Y) + R^{(p)}(X, Y) \qquad \textit{where } \deg_X(R^{(p)}(X, Y)) < s.$$

The encoding of the polynomial ideal code maps is as follows:

$$\begin{aligned} \mathbb{F}_{<k}[X] &\longrightarrow (\mathbb{F}_{<s}[X])^n \\ p(X) &\longmapsto \left(R^{(p)}(X, a_i)\right)_{i=0}^{n-1}. \end{aligned}$$

The equivalence of Definitions 3.1 and 3.2 is not hard to see. We summarize this in the simple observation below.

▶ **Observation 3.3.** *Definitions 3.1 and 3.2 are equivalent.*

Proof. Given a code as per Definition 3.1, we can view this as a code according to Definition 3.2 by picking n distinct $a_0, a_1, \ldots, a_{n-1} \in \mathbb{F}$ (or in a large enough extension of $\mathbb{F}$ of size at least n) and use standard Lagrange interpolation to find a bivariate polynomial $E(X, Y)$ such that for every $i \in [n]$,

$$E(X, a_i) = E_i\,.$$

More precisely, we define $E(X, Y)$ as follows.

$$E(X,Y) := \sum_{i\in[n]} \left(\prod_{j\in[n]\setminus\{i\}} \frac{(Y-a_j)}{(a_j-a_i)} \right) \cdot E_i(X)\,.$$

Clearly, $E(X, a_i)$'s are relatively prime, and their degree in X equals s and $E(X, Y)$ is monic in X. The equivalence of the encoding function also follows immediately from the definitions.

The other direction is even simpler. Given a code as per Definition 3.2, we can view this as a code as per Definition 3.1 by just setting $E_i(X)$ to be equal to $E(X, a_i)$ for every $i \in [n]$. The condition on the degree of E_i and their relative primality follows immediately from the fact that $E(X, Y)$ is monic in X of degree s, and $E(X, a_i)$'s are relatively prime. Once again, the encoding map can be seen to be equivalent in both the cases. ◀

From Observation 3.3 and the discussion in Section 3.1, the Reed-Solomon codes, Folded Reed-Solomon codes, Additive Folded Reed-Solomon codes and Multiplicity codes can also be viewed as polynomial ideal codes as per Definition 3.2.

- **Reed-Solomon codes**: We take $E(X, Y)$ to be equal to $(X - Y)$, the set of points $a_0, \ldots, a_{n-1}$ remain the same.
- **Folded Reed-Solomon codes**: We take $E(X, Y) = \prod_{j\in[s]}(X - \gamma^j Y)$ and the set of evaluation points $a_0, \ldots, a_{n-1}$ are set as before, and $\gamma \in \mathbb{F}^*$ is an element of high enough order.
- **Additive Folded Reed-Solomon codes**: We take $E(X, Y) = \prod_{j\in[s]}(X - Y + \beta j)$ and the set of evaluation points $a_0, \ldots, a_{n-1}$ are set as before. Recall that $\mathbb{F}$ is taken to be a field of characteristic at least s for these codes.
- **Multiplicity codes**: We take $E(X, Y)$ to be equal to $(X - Y)^s$, the set of points $a_0, \ldots, a_{n-1}$ are distinct.
- **Affine Folded Reed-Solomon codes:** We take $E(X, Y) = \prod_{i=0}^{s-1}(X - \ell^{(i)}(Y))$ where $\ell(Y) = \alpha Y + \beta$ with $\alpha \in \mathbb{F}_q^*$ and $\beta \in \mathbb{F}_q$. Recall that the set of evaluation points $A = \{a_0, \ldots, a_{n-1}\}$ is such that for distinct i, j the sets $\left\{\ell^{(0)}(a_i), \ldots, \ell^{(s-1)}(a_i)\right\}$ and $\left\{\ell^{(0)}(a_j), \ldots, \ell^{(s-1)}(a_j)\right\}$ are disjoint.

It follows immediately from these definitions that all the desired properties in Definition 3.2 are indeed satisfied. We skip the remaining details.

4 Linear operator codes

In this section, we give an alternate viewpoint of polynomial ideal codes in terms of codes defined based on linear operators on the ring of polynomials.

▶ **Definition 4.1** (linear operators). *Let $\mathcal{L} = (L_0, \ldots, L_{s-1})$ be a of s linear operators where each $L_i : \mathbb{F}[X] \to \mathbb{F}[X]$ is a $\mathbb{F}$-linear operator over the ring $\mathbb{F}$. For any $f \in \mathbb{F}[X]$, it will be convenient to denote by $\mathcal{L}(f)$ the (row) vector $(L_0(f), \ldots, L_{s-1}(f)) \in \mathbb{F}[X]^s$.*

Given any such family $\mathcal{L}$ and element $a \in \mathbb{F}$, define

$$I^a(\mathcal{L}) = \{p(X) \in \mathbb{F}[X] \mid \mathcal{L}(p)(a) = \bar{0}\}.$$

If the family $\mathcal{L}$ of linear operators family and the set of field elements $A \subseteq \mathbb{F}$ further satisfy the property that $I^a(\mathcal{L})$ is an ideal for each $a \in A$, we refer to the family $\mathcal{L}$ as an ideal family of linear operators *with respect to A.*

In this case, since $\mathbb{F}[X]$ is a principal ideal domain, for each $a \in A$, $I^a(\mathcal{L}) = \langle E^a(\mathcal{L})(X)\rangle$ for some monic polynomial $E^a(\mathcal{L}) \in F[X]$.

We now define a special condition on the family of linear operators $\mathcal{L}$ which will help us capture when $I^a(\mathcal{L})$ forms an ideal.

▶ **Definition 4.2** (linearly-extendible linear operators). *The family $\mathcal{L}$ of linear operators is said to be* linearly-extendible *if there exists a matrix $M(X) \in \mathbb{F}[X]^{s\times s}$ such that for all $p \in F[X]$ we have*

$$\mathcal{L}(X \cdot p(X)) = M(X) \cdot \mathcal{L}(p(X)). \tag{1}$$

We give two examples to illustrate the definition:

- Let $L_0(f(X)) = f(X)$ and $L_1(f(X)) = f'(X)$ where f' is the formal derivative of f. Then, by the product rule $L_1(Xf(X)) = X \cdot f'(X) + f(X)$. Hence, in this case $M(X) = \left(\begin{smallmatrix} X & 0 \\ 1 & X \end{smallmatrix}\right)$.
- Let $L_0(f(X)) = f(X)$ and $L_1(f(X)) = f(\gamma X)$ where $\gamma \in \mathbb{F}_q$ is non-zero. Then, we have $L_1(Xf(X)) = \gamma X f(\gamma X)$. Hence, in this case $M(X) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & \gamma X \end{smallmatrix}\right)$.

▶ **Observation 4.3.** *Suppose $\mathcal{L}$ is linearly-extendible and $M(X)$ is the corresponding matrix from Equation* (1).

- *For any $j \geq 0$ we have $\mathcal{L}(X^j \cdot p(X)) = (M(X))^j \cdot \mathcal{L}(p(X))$. Thus, by linearity we have that for any $q \in \mathbb{F}[X]$:*

  $$\mathcal{L}(q(X) \cdot p(X)) = q(M(X)) \cdot \mathcal{L}(p(X)).$$

  For instance if $q(X) = X^j$ then $\mathcal{L}(X^j \cdot p(X)) = (M(X))^j \cdot \mathcal{L}(p(X))$.
- *The family $\mathcal{L}$ is completely specified by $\mathcal{L}(1)$ and $M(X)$. In other words, $\mathcal{L}(p(X)) = p(M(X)) \cdot \mathcal{L}(1)$.*
- *For every set A of evaluation points, $\mathcal{L}$ is an ideal family of linear operators with respect to A. This is because if at a point a we have $\mathcal{L}(p)(a) = 0$ then $\mathcal{L}(Xp)(a) = (M(X) \cdot \mathcal{L}(p(X)))(a) = M(X = a) \cdot \mathcal{L}(p)(a) = 0$. This means that if $p(X) \in I^a(\mathcal{L})$ then $Xp(X) \in I^a(\mathcal{L})$, and hence by linearity for any $q(X) \in \mathbb{F}[X]$ we have $q(X) \cdot p(X) \in I^a(\mathcal{L})$.*

▶ **Definition 4.4** (linear operator codes). *Let $\mathcal{L} = (L_0, \ldots, L_{s-1})$ be a family of linear operators, $A = \{a_1, \ldots, a_n\} \subseteq \mathbb{F}$ be a set of evaluation points and k a degree parameter such that $k \leq s \cdot n$. Then the linear operator code generated by $\mathcal{L}$ and A, denoted by $LO_k^A(\mathcal{L})$, is given as follows:*

$$\begin{aligned} \mathbb{F}_{<k}[X] &\longrightarrow (\mathbb{F}^s)^n \\ p(X) &\longmapsto (\mathcal{L}(p)(a_i))_{i=1}^n . \end{aligned}$$

- *If $\mathcal{L}$ is an ideal family of linear operators with respect to A where the polynomials $E_i := E^{a_i}(\mathcal{L})$, which are the monic generator polynomials for the ideals $I^{a_i}(\mathcal{L})$, further satisfy the following:*
  1. *For all $i \in [n]$, polynomial E_i has degree exactly s.*
  2. *The polynomials E_i's are pairwise relatively prime.*

Then the linear operator code is said to be an ideal linear operator code *and denoted by* $ILO_k^A(\mathcal{L})$.

- *If the ideal linear operator code* $ILO_k^A(\mathcal{L})$ *further satisfies that* $\mathcal{L}$ *is linearly-extendible, then the ideal linear operator code is said to be a* linearly-extendible linear operator code*, denoted by* $LELO_k^A(\mathcal{L})$.

▶ Remark 4.5. The rate of the $LO_k^A(\mathcal{L})$ code is k/sn. Further, if the the code is an ideal linear operator code, i.e., $ILO_k^A(\mathcal{L})$, then its distance is $1 - \frac{k-1}{sn}$. Hence, $ILO_k^A(\mathcal{L})$ is an MDS code.

▶ **Proposition 4.6.** *Any polynomial ideal code is a linearly-extendible linear operator code.*

See the full version [1] for a proof.

▶ Remark 4.7. (degree preserving) If the bivariate polynomial $E(X,Y)$ has total degree s, then, the linear operator in the $LELO$ code obtained above has the property that $\deg_X L_i(X^j) \leq j$: in fact, $\deg_X L_i(X^j) \leq j - i$.

▶ **Proposition 4.8.** *Any ideal linear operator code is a polynomial ideal code.*

Proof. Consider an ideal linear operator code $ILO_k^A(\mathcal{L})$. For any polynomial $p(X) \in \mathbb{F}[X]$ and a point $a_i \in A$, giving $\mathcal{L}(p(X))(a)$ is equivalent to giving $p(X) \mod \langle E_i \rangle$ where $\langle E_i \rangle = I^{a_i}(\mathcal{L})$. However, the E_is readily satisfy Definition 3.1. ◀

Now, we state a corollary which further corroborates the notion of linear-extendibility.

▶ **Corollary 4.9** (Equivalence of ILO and $LELO$)**.** *From Propositions 4.6 and 4.8 it follows that every ideal linear operator code is also a linearly-extendible linear operator code.*

Below we state some well known codes in their linear operator descriptions (a more formal treatment is given in *Appendix A*):

- **Reed-Solomon Codes**: Let $A = \{a_0, \ldots, a_{n-1}\}$ be distinct elements in $\mathbb{F}_q$ These are $LELO_{\mathcal{L},A}$ where $\mathcal{L} = (I)$. That is the encoding of the message polynomial $p(X) \in \mathbb{F}_{<k}[X]$ at a point a is $L(f(X))(a) = f(a)$.
- **Folded Reed-Solomon Codes**: Let $\gamma \in F_q^*$ with multiplicative order at least s. $FRS[k,n]$ with folding parameter s are linearly-extendible linear operator codes $LELO_{\mathcal{L},A}$ where:
  - $\mathcal{L} = (L_0, \ldots, L_{s-1})$ with $L_1(f(X)) = f(\gamma Y)$ for $f(X) \in \mathbb{F}_q[X]$ and $L_i = L_1^i$ for $i \in \{0, 1, \ldots, s-1\}$.
  - For the above family of operators $M(X)$ is given by $M(X)_{ij} = \gamma^i X \cdot \mathbb{I}[i = j]$ for $i, j \in [s]$.
  - The set of evaluation points is $A = \{a_0, \ldots, a_{n-1}\}$ where for any two distinct i and j the sets $\{a_i, a_i\gamma, \ldots, a_i\gamma^{s-1}\}$ and $\{a_j, a_j\gamma, \ldots, a_j\gamma^{s-1}\}$ are disjoint.
- **Multiplicity Codes**: Then, $MULT[k,n]$ codes of order s are linearly-extendible linear operator codes $LELO_{\mathcal{L},A}$ where:
  - $\mathcal{L} = (L_0, \ldots, L_{s-1})$ with $L_1(f(X)) = \frac{\partial f(X)}{\partial X}$ for $f(X) \in \mathbb{F}_q[X]$ and $L_i = L_1^i$ for $i \in \{0, 1, \ldots, s-1\}$.
  - For the above family of operators $M(X)$ is given by $M(X)_{ij} = X \cdot \mathbb{I}[i = j] + i \cdot \mathbb{I}[i-1 = j]$ for $i, j \in [s]$.
  - The set of evaluation points is $A = \{a_0, \ldots, a_{n-1}\}$ where a_is are all distinct.
- **Additive Folded Reed-Solomon Codes**: Let $\beta \in \mathbb{F}_q$ be a non-zero element and the characteristic of $\mathbb{F}_q$ be at least s. Then, Additive-FRS$[k,n]$ codes with folding parameter s are linearly-extendible linear operator codes $LELO_{\mathcal{L},A}$ where:

  - $\mathcal{L} = (L_0, \dots, L_{s-1})$ with $L_1(f(X)) = f(X + \beta)$ for $f(X) \in \mathbb{F}_q[X]$ and $L_i = L_1^i$ for $i \in \{0, 1, \dots, s-1\}$.
  - For the above family of operators $M(X)$ is given by $M(X)_{ij} = (X + i\beta) \cdot \mathbb{I}[i = j]$ for $i, j \in [s]$.
  - The set of evaluation points is $A = \{a_0, \dots, a_{n-1}\}$ where $a_i - a_j \notin \{0, \beta, 2\beta, \dots, (s-1)\beta\}$ for distinct i and j.
- **Affine Folded Reed-Solomon Codes:** Let $\alpha \in \mathbb{F}_q^*$ and $\beta \in \mathbb{F}_q$. Further, let $\ell(X) = \alpha X + \beta$ with $\mathrm{ord}(\ell) = u$. Then Affine-FRS$[k, n]$ codes with folding parameter s are linearly-extendible codes $LELO_{\mathcal{L},A}$ described below. (See Observation A.7 for more details.)

  Define $D_1 : \mathbb{F}[X] \to \mathbb{F}[X]$ as $D_1(f(X)) = \frac{\partial f(X)}{\partial X}$ and $S_1 : \mathbb{F}[X] \to \mathbb{F}[X]$ as $S_1(f(X)) = f(\ell(X))$. Further, for $i \geq 0$ let $D_i = D_1^i$ and $S_i = S_1^i$. Recall, that the order of α is u. For any integer $r \in [s]$ let $r = r_1 u + r_0$, with $r_0 < u$, be the unique representation of r.
  - Define $L_r : \mathbb{F}[X] \to \mathbb{F}[X]$ as $L_r(f(X)) = S_{r_0}(D_{r_1} f(X))$. Set $\mathcal{L} = (L_0, \dots, L_{s-1})$. Clearly, $\mathcal{L}$ is a family of linear operators.
  - $L_r(Xf) = S_{r_0}(D_{r_1} f) = S_{r_0}(r_1 \cdot D_{r_1 - 1} f + X \cdot D_{r_1} f) = r_1 \cdot L_{r-u} f + S_{r_0}(X) \cdot L_r f$: hence, $\mathcal{L}$ is a set of linearly-extendible linear operators.
  - The set of evaluation points $A = \{a_0, \dots, a_{n-1}\}$ is such that for distinct i, j the sets $\left\{\ell^{(0)}(a_i), \dots, \ell^{(s-1)}(a_i)\right\}$ and $\left\{\ell^{(0)}(a_j), \dots, \ell^{(s-1)}(a_j)\right\}$ are disjoint.

5 List-decoding of polynomial ideal codes

In this section, we discuss the list-decoding of polynomial ideal codes.

5.1 List-decoding up to to the Johnson radius

We first observe that polynomial ideal codes are list decodable in polynomial time, up to the Johnson radius.

▶ **Theorem 5.1.** *Let $k, s, n \in \mathbb{N}$ be such that $k < sn$ and $s < k - 1$. Let $E_0(X), E_1(X), \dots, E_{n-1}(X) \in \mathbb{F}[X]$ be relatively prime monic polynomials of degree equal to s each. Let $\mathrm{Enc} : \mathbb{F}_{<k}[X] \longrightarrow (\mathbb{F}_{<s}[X])^n$ be the encoding function defined as*

$$p(X) \longmapsto (p(X) \pmod{E_i(X)})_{i=0}^{n-1} .$$

Then, there is an algorithm, which takes as input a received word $\mathbf{c} = (\mathbf{c}_0, \mathbf{c}_1, \dots, \mathbf{c}_n) \in \mathbb{F}_{<s}[X]^n$ and for every $\varepsilon > 0$ outputs all polynomials $f \in \mathbb{F}_{<k}[X]$ such that $\mathrm{Enc}(f)$ and $\mathbf{c}$ agree on at least $(k/sn)^{1/2} + \varepsilon$ fraction of coordinates in time $\mathsf{poly}(n, 1/\varepsilon)$.

Observe that the rate of this code is k/sn and distance is $1 - (k-1)/sn$, and thus Theorem 5.1 gives us an algorithmic analog of Theorem 2.2 for these codes.

The list decoding algorithm for polynomial ideal codes is an (almost immediate) extension of an algorithm of Guruswami, Sahai and Sudan [4] for list decoding codes based on Chinese Remainder Theorem to this setting. This algorithm, in turn, relies on ideas in an earlier algorithm of Guruswami and Sudan [5] for list decoding Reed-Solomon codes up to the Johnson radius.

As noted in the introduction, most of the ideas for the proof of Theorem 5.1 were already there in the work of Guruswami, Sahai and Sudan [4] and all we do in this section is to flush out some of the details. Due to space constraints, we refer the interested reader to full version [1] for details.

5.2 List-decoding beyond the Johnson radius

In this section, we use the linear operator viewpoint of polynomial ideal codes to study their list-decodability beyond the Johnson radius. We show that if the family of linear operators $\mathcal{L}$ and the evaluation points satisfy some further properties, then the linear operator code is list-decodable all the way up to the distance of the code.

Let $\mathcal{G} = (G_0, \ldots, G_{m-1})$ and $\mathcal{T} = (T_0, T_1, \ldots, T_{r-1})$ be two families of linear operators such that $G_i : \mathbb{F}[X] \to \mathbb{F}[X]$ and $\mathcal{T}$ is a linearly-extendible family of linear operators. We say that the pair $(\mathcal{T}, \mathcal{G})$ *list-composes* in terms of $\mathcal{L}$ at the set of evaluation points A if we have the following. For every linear operator $G \in \mathcal{G}$ and field element $a \in A$, there exists a linear function $h_{G,a} : \mathbb{F}^s \to \mathbb{F}^r$ such that for every polynomial $f \in \mathbb{F}[X]$ we have

$$\mathcal{T}(G(f))(a) = h_{G,a}(\mathcal{L}(f)(a)).$$

▶ **Theorem 5.2.** *If $LO_k^A(\mathcal{L})$ is a linear operator code and there exists two families of linear operators $\mathcal{G} = (G_0, \ldots, G_{m-1})$ and $\mathcal{T} = (T_0, \ldots, T_{r-1})$ such that*

1. *$(\mathcal{T}, A)$ forms a linearly-extendible linear operator code $LELO^A_{k+nr/m}(\mathcal{T})$*
2. *The pair $(\mathcal{T}, \mathcal{G})$ list-composes in terms of $\mathcal{L}$ at the set of evaluation points*
3. *$\mathcal{G}$ is degree-preserving*
4. $\mathrm{Diag}(\mathcal{G}) \in \mathbb{F}^{|\mathcal{G}| \times k}$ *is the generator matrix of a code with distance $k - \ell$.*

Then, $LO_k^A(\mathcal{L})$ is list-decodable up to the distance $1 - \frac{k}{rn} - \frac{1}{m}$ with list size q^ℓ.

This theorem clearly implies Theorem 1.1. We refer the interested reader to the full version of the paper [1] for the proof.

References

1 Siddharth Bhandari, Prahladh Harsha, Mrinal Kumar, and Madhu Sudan. Ideal-theoretic explanation of capacity-achieving decoding. (manuscript). arXiv:2103.07930, eccc:2021/TR21-036.

2 Venkatesan Guruswami. Linear-algebraic list decoding of folded Reed-Solomon codes. In *Proc. 26th IEEE Conf. on Comput. Complexity*, pages 77–85, 2011. doi:10.1109/CCC.2011.22.

3 Venkatesan Guruswami and Atri Rudra. Explicit codes achieving list decoding capacity: Error-correction with optimal redundancy. *IEEE Trans. Inform. Theory*, 54(1):135–150, 2008. (Preliminary version in *38th STOC*, 2006). eccc:2005/TR05-133, doi:10.1109/TIT.2007.911222.

4 Venkatesan Guruswami, Amit Sahai, and Madhu Sudan. "Soft-decision" decoding of Chinese Remainder Codes. In *Proc. 41st IEEE Symp. on Foundations of Comp. Science (FOCS)*, pages 159–168, 2000. doi:10.1109/SFCS.2000.892076.

5 Venkatesan Guruswami and Madhu Sudan. Improved decoding of Reed-Solomon and algebraic-geometry codes. *IEEE Trans. Inform. Theory*, 45(6):1757–1767, 1999. (Preliminary version in *39th FOCS*, 1998). eccc:1998/TR98-043, doi:10.1109/18.782097.

6 Venkatesan Guruswami and Carol Wang. Linear-algebraic list decoding for variants of Reed-Solomon codes. *IEEE Trans. Inform. Theory*, 59(6):3257–3268, 2013. (Preliminary version in *26th IEEE Conference on Computational Complexity*, 2011 and *15th RANDOM*, 2011). eccc:2012/TR12-073, doi:10.1109/TIT.2013.2246813.

7 Durga Datt Joshi. A note on upper bounds for minimum distance codes. *Information and Control*, 1(3):289–295, 1958. doi:10.1016/S0019-9958(58)80006-6.

8 Yasuo Komamiya. Application of logical mathematics to information theory. *Proc. 3rd Japan. Nat. Cong. Appl. Math*, 437, 1953.

9 Swastik Kopparty. List-decoding multiplicity codes. *Theory of Computing*, 11:149–182, 2015. eccc:2012/TR12-044, doi:10.4086/toc.2015.v011a005.

10 Swastik Kopparty, Shubhangi Saraf, and Sergey Yekhanin. High-rate codes with sublinear-time decoding. *J. ACM*, 61(5):28:1–28:20, 2014. (Preliminary version in *43rd STOC*, 2011). `eccc:2010/TR10-148`, `doi:10.1145/2629416`.

11 Richard Collom Singleton. Maximum distance q-nary codes. *IEEE Trans. Inform. Theory*, 10(2):116–118, 1964. `doi:10.1109/TIT.1964.1053661`.

12 Salil P. Vadhan. Pseudorandomness. *Found. Trends Theor. Comput. Sci.*, 7(1-3):1–336, 2012. `doi:10.1561/0400000010`.

A Example of Codes Achieving List-Decoding Capacity

In this section we will use Theorem 5.2 to (re)prove the list-decoding capacity of the Folded Reed-Solomon codes, multiplicity codes and additive Folded Reed-Solomon codes. We then introduce a common generalization of all these codes, which we refer to as affine Folded Reed-Solomon codes and prove the list-decoding up to capacity of these codes.

A.1 Folded Reed-Solomon (FRS) Codes

Fix integers k, n, q with $n \leq q$. Fix $\gamma \in \mathbb{F}_q^*$ of multiplicative order at least s. The message space of the $FRS_s^\gamma[k,n]$ code with folding parameter s is polynomials of degree at most $k-1$ over $\mathbb{F}[X]$, i.e., $\mathbb{F}_{<k}[X]$ where $\mathbb{F} = \mathbb{F}_q$. Then, FRS codes are linearly-extendible linear operator codes $LELO_{\mathcal{L},A}$ where:

- $\mathcal{L} = (L_0, \ldots, L_{s-1})$ with $L_1(f(X)) = f(\gamma X)$ for $f(X) \in \mathbb{F}_q[X]$ and $L_i = L_1^i$ for $i \in \{0, 1, \ldots, s-1\}$.
- For the above family of operators $M(X)$ is given by $M(X)_{ij} = \gamma^i X \cdot \mathbb{I}[i = j]$ for $i, j \in [s]$.
- The set of evaluation points is $A = \{a_0, \ldots, a_{n-1}\}$ where for any two distinct i and j the sets $\left\{a_i, a_i\gamma, \ldots, a_i\gamma^{s-1}\right\}$ and $\left\{a_j, a_j\gamma, \ldots, a_j\gamma^{s-1}\right\}$ are disjoint.

▶ Remark A.1.

1. Recall that the bivariate polynomial $E(X,Y)$ corresponding to the polynomial ideal code representation is $E(X,Y) = \prod_{i=0}^{s-1}(X - \gamma^i Y)$.
2. For the choice of A as above, the rate of the code is $\frac{k}{sn}$ and its distance is $1 - \frac{k-1}{sn}$ as the polynomials $E_i = E(X, a_i)$ are pairwise co-prime.

▶ **Theorem A.2** ([6]). *Let $\gamma \in \mathbb{F}_q^*$ be an element of order at least k. Further, let $A = \{a_0, \ldots, a_{n-1}\}$ be a set of evaluation points where for any two distinct i and j the sets $\left\{a_i, a_i\gamma, \ldots, a_i\gamma^{s-1}\right\}$ and $\left\{a_j, a_j\gamma, \ldots, a_j\gamma^{s-1}\right\}$ are disjoint. For every $\varepsilon > 0$ there exists s large enough ($s \geq \Omega(1/\varepsilon^2)$) such that $FRS_s^\gamma[k,n]$ at the set of evaluation points A can be efficiently list-decoded up to distance $1 - \frac{k}{sn} - \varepsilon$.*

Proof. We will prove this by applying Theorem 5.2. Set $\mathcal{G} = (L_0, \ldots, L_{m-1})$ for some integer $m < s$ to be set later and $\mathcal{T} = (T_0, \ldots, T_{r-1})$ with $r = s - m + 1$ and $T_i = L_i$.

Theorem 5.2-Item 1: Clearly, $(\mathcal{T}, A)$ forms a linearly-extendible linear operator code $LELO^A_{k+nr/m}(\mathcal{T})$ which is $FRS_r^\gamma[k + nr/m, n]$ at the set of evaluation points A.

Theorem 5.2-Item 2: For all $G_i \in \mathcal{G}$, $T_j \in \mathcal{T}$ and $a \in A$, we have that for every polynomial $f \in \mathbb{F}[X]$: $T_j(G_i(f))(a) = L_{i+j}(f)(a)$. Notice that $L_{i+j} \in \mathcal{L}$ as $i + j \leq s - 1$.

Theorem 5.2-Item 3: $G_i(x^j) = \gamma^{ij} y^j$, and hence $\mathcal{G}$ is degree preserving.

Theorem 5.2-Item 4: The matrix $\mathrm{Diag}(\mathcal{G})$ is given by $\mathrm{Diag}(\mathcal{G})_{ij} = \gamma^{ij}$ for $i \in [m]$ and $j \in [k]$. Hence, as long as γ has order at least k this is the generator matrix of $RS[m-1, k]$ and hence its distance is $k - m + 1$.

Thus $FRS_s^\gamma[k,n]$ can be efficiently list-decoded up to distance $1 - \frac{k-1}{rn} - \frac{1}{m}$ with list size q^{m-1}. By choosing a large enough m and s we can ensure that $1 - \frac{k-1}{rn} - \frac{1}{m} > 1 - \frac{k}{sn} - \varepsilon$. ◀

A.2 Multiplicity ($MULT$) Codes

Fix integers k, n, q with $n \leq q$. The message space of the $MULT_s[k, n]$ code of order s is polynomials of degree at most $k-1$ over $\mathbb{F}[X]$, i.e., $\mathbb{F}_{<k}[X]$ where $\mathbb{F} = \mathbb{F}_q$. Then, $MULT_s[k, n]$ codes are linearly-extendible linear operator codes $LELO_{\mathcal{L},A}$ where:

- $\mathcal{L} = (L_0, \ldots, L_{s-1})$ with $L_1(f(X)) = \frac{\partial f(X)}{\partial X}$ for $f(X) \in \mathbb{F}_q[X]$ and $L_i = L_1^i$ for $i \in \{0, 1, \ldots, s-1\}$.
- For the above family of operators $M(X)$ is given by $M(X)_{ij} = X \cdot \mathbb{I}[i = j] + i \cdot \mathbb{I}[i - 1 = j]$ for $i, j \in [s]$.
- The set of evaluation points is $A = \{a_0, \ldots, a_{n-1}\}$ where a_is are all distinct.

▶ Remark A.3.

1. Recall that the bivariate polynomial $E(X, Y)$ corresponding to the polynomial ideal code representation is $E(X, Y) = (X - Y)^s$.
2. For the choice of A as above, $MULT_s[k, n]$ is a code with rate $\frac{k}{sn}$ and distance $1 - \frac{k-1}{sn}$ as the polynomials $E_i = E(X, a_i)$ are pairwise co-prime.

▶ **Theorem A.4** ([6]). *Let the characteristic of $\mathbb{F}_q$ be at least $\max(s, k)$. Further, let the set of evaluation points be $A = \{a_0, \ldots, a_{n-1}\}$ where a_is are all distinct. Then, for every $\varepsilon > 0$ there exists s large enough ($s \geq \Omega(1/\varepsilon^2)$) such that $MULT_s[k, n]$ can be efficiently list-decoded up to distance $1 - \frac{k}{sn} - \varepsilon$.*

Proof. We will again appeal to Theorem 5.2. Set $\mathcal{G} = (G_0, \ldots, G_{m-1})$ where $G_i = \frac{X^i}{i!} \cdot L_i$ for $i \in \{0, 1, \ldots, m-1\}$ for some integer $m < s$ to be set later and $\mathcal{T} = (T_0, \ldots, T_{r-1})$ with $r = s - m + 1$ and $T_i = L_i$.

Theorem 5.2-Item 1: Clearly, $(\mathcal{T}, A)$ forms a linearly-extendible linear operator code $LELO^A_{k+nr/m}(\mathcal{T})$ which is $MULT_r[k + nr/m, n]$ of order r at the set of evaluation points A.

Theorem 5.2-Item 2: For all $G_i \in \mathcal{G}$, $T_j \in \mathcal{T}$ and $a \in A$, we have that for every polynomial $f \in \mathbb{F}[X]$:

$$T_j(G_i(f))(a) = (\sum_{b=0}^{j} \binom{j}{b}\binom{i}{b} \cdot (b!/i!) \cdot X^{i-b} L_{i+b}(f))(a).$$

Notice that the above expression only involves L_is where $i < s$.

Theorem 5.2-Item 3: $G_i(X^j) = \binom{j}{i} \cdot X^j$, and hence $\mathcal{G}$ is degree preserving.

Theorem 5.2-Item 4: The matrix $\text{Diag}(\mathcal{G})$ is given by $\text{Diag}(\mathcal{G})_{ij} = \binom{j}{i}$ for $i \in [m]$ and $j \in [k]$. This matrix can be transformed via elementary row operations to a $RS[m, k]$ generator matrix with points of evaluations as $0, 1, \ldots, k-1$; thus, as long as the characteristic of $\mathbb{F}_q$ is at least k we have that the distance of $\text{Diag}(\mathcal{G})$ is $k - m + 1$.

Thus $MULT_s[k, n]$ can be efficiently list-decoded up to distance $1 - \frac{k-1}{rn} - \frac{1}{m}$ with list size q^{m-1}. By choosing a large enough m and s we can ensure that $1 - \frac{k-1}{rn} - \frac{1}{m} > 1 - \frac{k}{sn} - \varepsilon$. ◀

A.3 Additive Folded Reed-Solomon (Additive-FRS) Codes

Fix integers k, n, q with $n \leq q$. Let $\beta \in \mathbb{F}_q$ be a non-zero element and characteristic of $\mathbb{F}_q$ is at least s. The message space of the Additive-FRS$^\beta_s[k, n]$ code with folding parameter s is polynomials of degree at most $k - 1$ over $\mathbb{F}[X]$, i.e., $\mathbb{F}_{<k}[X]$ where $\mathbb{F} = \mathbb{F}_q$. Then, Additive-FRS$^\beta_s[k, n]$ codes are linearly-extendible linear operator codes $LELO_{\mathcal{L},A}$ where:

- $\mathcal{L} = (L_0, \ldots, L_{s-1})$ with $L_1(f(X)) = f(X + \beta)$ for $f(X) \in \mathbb{F}_q[X]$ and $L_i = L_1^i$ for $i \in \{0, 1, \ldots, s-1\}$.

- For the above family of operators $M(X)$ is given by $M(X)_{ij} = (X + i\beta) \cdot \mathbb{I}[i = j]$ for $i, j \in [s]$.
- The set of evaluation points is $A = \{a_0, \ldots, a_{n-1}\}$ where $a_i - a_j \notin \{0, \beta, 2\beta, \ldots, (s-1)\beta\}$ for distinct i and j.

▶ Remark A.5.

1. Recall that the bivariate polynomial $E(X, Y)$ corresponding to the polynomial ideal code representation is $E(X, Y) = \prod_{i=0}^{s-1}(X - Y - i\beta)$.
2. For the choice of A as above, Additive-FRS$_s^\beta[k, n]$ is a code with rate $\frac{k}{sn}$ and distance $1 - \frac{k-1}{sn}$ as the polynomials $E_i = E(X, a_i)$ are pairwise co-prime.

▶ **Theorem A.6.** *Let the characteristic of $\mathbb{F}_q$ be at least $\max(s, k)$ and $\beta \in \mathbb{F}_q$ be a non-zero element. Further, let the set of evaluation points $A = \{a_0, \ldots, a_{n-1}\}$ be such that $a_i - a_j \notin \{0, \beta, 2\beta, \ldots, (s-1)\beta\}$ for distinct i and j. Then, for every $\varepsilon > 0$ there exists s large enough ($s \geq \Omega(1/\varepsilon^2)$) such that Additive-FRS$_s^\beta[k, n]$ over the set of evaluation points A can be efficiently list-decoded up to distance $1 - \frac{k}{sn} - \varepsilon$.*

Proof. We will again appeal to Theorem 5.2. To define $\mathcal{G} = (G_0, \ldots, G_{m-1})$ for some integer $m < s$, we need the following definitions. Let $B \in \mathbb{F}_q^{m \times m}$ be a matrix where $B_{ij} = (j)^i$ for $i, j \in [m]$, i.e, the transpose of the Vandermonde matrix at the points $\{0, 1, \ldots, m-1\}$: these points are distinct since the characteristic of the field is at least k. Further, let $\mathbf{b}_i \in \mathbb{F}_q^m$ be a vector such that $B\mathbf{b}_i = e_i$ for $i \in [m]$ where e_is are the standard basis vectors: $\mathbf{b}_i$s exist because B is full rank. Now, define $G_i = X^i \cdot \sum_{c=0}^{m-1} \mathbf{b}_i(c) L_c$ for $i \in [m]$. Set $\mathcal{T} = (T_0, \ldots, T_{r-1})$ with $r = s - m + 1$ and $T_i = L_i$.

Theorem 5.2-Item 1: Clearly, $(\mathcal{T}, A)$ forms a linearly-extendible linear operator code $LELO_{k+nr/m}^A(\mathcal{T})$ which is Additive-FRS$_r^\beta[k + nr/m, n]$ with folding parameter r at the set of evaluation points A.

Theorem 5.2-Item 2: For all $G_i \in \mathcal{G}$, $T_j \in \mathcal{T}$ and $a \in A$, we have that for every polynomial $f \in \mathbb{F}[X]$:

$$\begin{aligned} T_j(G_i(f))(a) &= T_j\left(X^i \cdot \sum_{c=0}^{m-1} \mathbf{b}_i(c) L_c\right)(a) \\ &= \left((X + j\beta)^i \cdot \sum_{c=0}^{m-1} \mathbf{b}_i(c) L_{c+j}\right)(a). \end{aligned}$$

Notice that the above expression only involves L_is where $i < s$. Theorem 5.2-Item 3:

$$\begin{aligned} G_i(X^j) &= X^i \cdot \sum_{c=0}^{m-1} \mathbf{b}_i(c) L_c(X^j) \\ &= X^i \cdot \sum_{c=0}^{m-1} \mathbf{b}_i(c)(X + c\beta)^j \\ &= X^i \cdot \sum_{c=0}^{m-1} \mathbf{b}_i(c) \sum_{h \leq j} \binom{j}{h} X^h \cdot (c\beta)^{j-h} \\ &= X^i \cdot \left(\binom{j}{i}\beta^i X^{j-i} + \sum_{h \leq j-m} \alpha_h X^h\right) \end{aligned}$$

(this is because $B\mathbf{b}_i = e_i$ which means that for $h > j - m$ we have $\sum_{c=0}^{m-1} \mathbf{b}_i(c) \cdot (c)^{j-h} = \mathbb{I}[j - h = i]$; α_h are field constants)

$$= \binom{j}{i} \beta^{i-1} X^j + \dots,$$

and hence $\mathcal{G}$ is degree preserving.

Theorem 5.2-Item 4: By the above, the matrix $\mathrm{Diag}(\mathcal{G})$ is given by $\mathrm{Diag}(\mathcal{G})_{ij} = \binom{j}{i}\beta^i$ for $i \in [m]$ and $j \in [k]$. Up to scaling this is the same code as $\mathrm{Diag}(\mathcal{G})$ in Theorem A.4: and hence, if the characteristic of the field is at least k then its distance is $k - m + 1$.

Thus Additive-$\mathrm{FRS}_s^\beta[k, n]$ can be efficiently list-decoded up to distance $1 - \frac{k-1}{rn} - \frac{1}{m}$ with list size q^{m-1}. By choosing a large enough m and s we can ensure that $1 - \frac{k-1}{rn} - \frac{1}{m} > 1 - \frac{k}{sn} - \varepsilon$. ◀

A.4 Affine Folded Reed-Solomon (Affine-FRS) Codes

We first recall the defintion of Affine-FRS codes. Fix integers k, n, q with $n \leq q$. Let $\alpha \in \mathbb{F}_q^*$ and $\beta \in \mathbb{F}_q$ such that the multiplicative order of α is u. Further, define $\ell(X) = \alpha X + \beta$ and

$$\ell^{(i)}(X) = \underbrace{\ell(\ell \dots \ell(X))}_{i \text{ times}} = \alpha^i X + \beta \cdot \sum_{j=0}^{i-1} \alpha^j = \alpha_i X + \beta_i.$$

In fact, if $\alpha \neq 1$, i.e, $u > 1$ then, $\ell^{(u)}(X) = \ell^{(0)}(X)$. Let $\mathrm{ord}(\ell)$ denote the smallest positive integer t such that $\ell^{(t)}(z) = z$. The message space of the Affine-$\mathrm{FRS}_s^{\alpha,\beta}[k, n]$ code with folding parameter s is polynomials of degree at most $k - 1$ over $\mathbb{F}[X]$, i.e., $\mathbb{F}_{<k}[X]$ where $\mathbb{F} = \mathbb{F}_q$. Let the set of evaluation points be $A = \{a_0, \dots, a_{n-1}\}$ such that for distinct i, j the sets $\left\{\ell^{(0)}(a_i), \dots, \ell^{(s-1)}(a_i)\right\}$ and $\left\{\ell^{(0)}(a_j), \dots, \ell^{(s-1)}(a_j)\right\}$ are disjoint. Then, Affine-$\mathrm{FRS}_s^{\alpha,\beta}[k, n]$ codes are polynomial ideal codes where:

- The bivariate polynomial $E(X, Y)$ corresponding to the polynomial ideal code representation is $E(X, Y) = \prod_{i=0}^{s-1}(X - \alpha_i Y - \beta_i)$.
- For the choice of A as above, Affine-$\mathrm{FRS}_s^{\alpha,\beta}[k, n]$ is a code with rate $\frac{k}{sn}$ and distance $1 - \frac{k-1}{sn}$ as the polynomials $E_i = E(X, a_i)$ are pairwise co-prime.

We will now recall the description of Affine-FRS codes in terms of linear operators which will be helpful while list-decoding. Define $D_1 : \mathbb{F}[X] \to \mathbb{F}[X]$ as $D_1(f(X)) = \frac{\partial f(X)}{\partial X}$ and $S_1 : \mathbb{F}[X] \to \mathbb{F}[X]$ as $S_1(f(X)) = f(\ell(X))$. Further, for $i \geq 0$ let $D_i = D_1^i$ and $S_i = S_1^i$. Recall, that the order of α is u. For any integer $r \in [s]$ let $r = r_1 u + r_0$, with $r_0 < u$, be the unique representation of r. Then, define $L_r : \mathbb{F}[X] \to \mathbb{F}[X]$ as $L_r(f(X)) = S_{r_0}(D_{r_1} f(X))$. Set $\mathcal{L} = (L_0, \dots, L_{s-1})$. Clearly, $\mathcal{L}$ is a family of linear operators. Further, $L_r(Xf) = S_{r_0}(D_{r_1} Xf) = S_{r_0}(r_1 \cdot D_{r_1 - 1} f + X \cdot D_{r_1} f) = r_1 \cdot L_{r-u} f + S_{r_0}(X) \cdot L_r f$: hence, $\mathcal{L}$ is a set of linearly-extendible linear operators.

▶ **Observation A.7.** *If $u > 1$ then at an evaluation point $a \in F_q$ the following pieces of information are the same:*

- $f(X) \mod \prod_{i=0}^{s-1}(X - \alpha_i a - \beta_i)$
- $\mathcal{L}(f)(a)$.

Hence, if $u > 1$, then, Affine-$\mathrm{FRS}_s^{\alpha,\beta}[k, n]$ at the points of evaluation A is $LELO_{\mathcal{L},A}$.

▶ **Theorem A.8.** *For every $\varepsilon > 0$, there exists a large enough s such that the follow holds. Let $\mathbb{F}_q$ be a field, k a parameter and $\ell(X) = \alpha \cdot X + \beta$ such that $\alpha \in \mathbb{F}_q^*$ and $\beta \in \mathbb{F}_q$. Furthermore, let the evaluation points $A = \{a_0, \dots, a_{n-1}\}$ be such that for distinct i, j the sets $\left\{\ell^{(0)}(a_i), \dots, \ell^{(s-1)}(a_i)\right\}$ and $\left\{\ell^{(0)}(a_j), \dots, \ell^{(s-1)}(a_j)\right\}$ are disjoint. Then, if either:*

- $\mathrm{ord}(\ell) \geq k$ *or*
- $\mathrm{char}(\mathbb{F}_q) > k$ *and* $\beta \neq 0$

holds, Affine-FRS$_s^{\alpha,\beta}[k,n]$ *over the set of evaluation points* A *can be efficiently list-decoded up to distance* $1 - \frac{k}{sn} - \varepsilon$.

Proof. We will again appeal to Theorem 5.2. Let u be the multiplicative order of α. Let $v = \lfloor s/u \rfloor$.

Case $\mathrm{ord}(\ell) \geq k$. This means that $u \geq k$. This is similar to decoding FRS codes. We skip the details.

Henceforth, we assume that $\mathrm{char}(\mathbb{F}_q) \geq k$ *and* $\beta \neq 0$.

Case $u = 1$. This is the same case as for Additive-FRS codes. Thus, by Theorem A.6 we are done.

Case $u > 1$ and $v \geq \sqrt{s}$. (This case is similar to $MULT_v[k,n]$.)

Define $\mathcal{G} = (G_0, \ldots, G_{m-1})$ for some integer $m < s$, as $G_i(f) = (X^i/i!) \cdot D_i f$. Let $r = (v-m)u$ and set $\mathcal{T} = \{L_0, L_1, \ldots, L_{r-1}\}$.

Theorem 5.2-Item 1: Clearly, $(\mathcal{T}, A)$ forms a linearly-extendible linear operator code $LELO^A_{k+nr/m}(\mathcal{T})$ which is Affine-FRS$_r^{\alpha,\beta}[k+nr/m, n]$ at the set of evaluation points A.

Theorem 5.2-Item 2: For all $G_i \in \mathcal{G}$, $T_j \in \mathcal{T}$ and $a \in A$ we have that for every polynomial $f \in \mathbb{F}[X]$:

$$\begin{aligned} T_j(G_i(f))(a) &= \left(S_{j_0} D_{j_1}\left(\frac{X^i}{i!} \cdot D_i(f)\right)\right)(a) \\ &= \left(S_{j_0} \sum_{b=0}^{j_1} \binom{j_1}{b}\binom{i}{b} \cdot (b!/i!) \cdot X^{i-b} D_{i+b}(f)\right)(a) \\ &= \left(\sum_{b=0}^{j_1} \binom{j_1}{b}\binom{i}{b} \cdot (b!/i!) \cdot (S_{j_0} X^{i-b}) \cdot L_{j_0+(i+b)u}(f)\right)(a). \end{aligned}$$

Notice that the above expression only involves L_is where $i < s$.

Theorem 5.2-Items 3 and 4: are identical to the corresponding items in Theorem A.4.

Thus Affine-FRS$_s^{\beta}[k,n]$ can be efficiently list-decoded up to distance $1 - \frac{k-1}{rn} - \frac{1}{m}$ with list size q^{m-1}. By choosing a large enough m and s we can ensure that $1 - \frac{k-1}{rn} - \frac{1}{m} > 1 - \frac{k}{sn} - \varepsilon$.

Case $u > \sqrt{s}$. (This case is similar to Additive-FRS$_u^{\beta}[k,n]$.) As in Theorem A.6, to define $\mathcal{G} = (G_0, \ldots, G_{m-1})$ for some integer $m < u$, we need the following definitions. Let $B \in \mathbb{F}_q^{m \times m}$ be a matrix where $B_{ij} = (\beta(\alpha^j - 1)/(\alpha^j))^i$ for $i, j \in [m]$, i.e, the transpose of the Vandermonde matrix at the points $\{\beta(\alpha^j - 1)/(\alpha^j) \mid j \in [m]\}$: these points are distinct since the order of u is at least m. Further, let $\mathbf{b}_i \in \mathbb{F}_q^m$ be a vector such that $B\mathbf{b}_i = e_i$ for $i \in [m]$ where e_is are the standard basis vectors: $\mathbf{b}_i$s exist because B is full rank.

Define $\mathcal{G} = (G_0, \ldots, G_{m-1})$ for some integer $m < s$, as $G_i = X^i \cdot \sum_{c=0}^{m-1} b_i(c) S_c$. Let $r = s - m + 1$ and set $\mathcal{T} = \{L_0, \ldots, L_{r-1}\}$.

Theorem 5.2-Item 1: Clearly, $(\mathcal{T}, A)$ forms a linearly-extendible linear operator code $LELO^A_{k+nr/m}(\mathcal{T})$ which is Affine-FRS$_r^{\alpha,\beta}[k+nr/m, n]$ at the set of evaluation points A.

Theorem 5.2-Item 2: For all $G_i \in \mathcal{G}$, $T_j \in \mathcal{T}$ and $a \in A$ we have that for every polynomial $f \in \mathbb{F}[X]$:

$$\begin{aligned}
T_j(G_i(f))(a) &= \left(S_{j_0} D_{j_1}\left(X^i \cdot \sum_{c=0}^{m-1} b_i(c) S_c f\right)\right)(a) \\
&= \left(S_{j_0} \sum_{b=0}^{j_1} \binom{j_1}{b}\binom{i}{b} \cdot (b!) \cdot X^{i-b} D_b \left(\sum_{c=0}^{m-1} b_i(c) S_c f\right)\right)(a) \\
&= \left(S_{j_0} \sum_{b=0}^{j_1} \binom{j_1}{b}\binom{i}{b} \cdot (b!) \cdot X^{i-b} \left(\sum_{c=0}^{m-1} (b_i(c)\alpha_c^b) S_c D_b f\right)\right)(a) \\
&= \left(S_{j_0} \sum_{b=0}^{j_1} \binom{j_1}{b}\binom{i}{b} \cdot (b!) \cdot X^{i-b} \left(\sum_{c=0}^{m-1} (b_i(c)\alpha_c^b) L_{bu+c} f\right)\right)(a).
\end{aligned}$$

Notice that the above expression only involves L_is where $i < s$.

Theorem 5.2-Items 3 and 4: follow almost identically to the corresponding items in Theorem A.6.

Thus Affine-FRS$_s^\beta[k, n]$ can be efficiently list-decoded up to distance $1 - \frac{k-1}{rn} - \frac{1}{m}$ with list size q^{m-1}. By choosing a large enough m and s we can ensure that $1 - \frac{k-1}{rn} - \frac{1}{m} > 1 - \frac{k}{sn} - \varepsilon$. ◀