An exposition of recent list-size bounds of FRS Codes

Abhibhav Garg[*] Prahladh Harsha[†] Mrinal Kumar[†] Ramprasad Saptharishi[†]
Ashutosh Shankar[†]

Abstract

In the last year, there have been some remarkable improvements in the combinatorial list-size bounds of Folded Reed Solomon codes and multiplicity codes. Starting from the work on Kopparty, Ron-Zewi, Saraf and Wootters [KRSW23] (and subsequent simplifications due to Tamo [Tam24]), we have had dramatic improvements in the list-size bounds of FRS codes[1] due to Srivastava [Sri25] and Chen & Zhang [CZ24]. In this note, we give a short exposition of these three results (Tamo, Srivastava and Chen-Zhang).

1 Introduction

We start by defining Folded Reed Solomon (FRS) codes and list decoding capacity. Folded Reed-Solomon codes were introduced by Krachkovsky [Kra03], and then re-discovered by Guruswami and Rudra [GR08] in the context of list-decoding. Let $\mathbb{F}_q$ be a finite field of q elements, with $q > k$.

Definition 1.1 (folded Reed-Solomon codes (FRS) [Kra03, GR08])**.** *Let $S = \{\alpha_1, \ldots, \alpha_n\}$ be a set of n distinct elements in $\mathbb{F}_q$ and let γ be a generator of $\mathbb{F}_q^*$. The* folded Reed-Solomon code *with parameters (k, S, s) is defined via the following map:*

$$\begin{aligned}\mathrm{FRS}_{k,s} \colon \mathbb{F}_q[x]^{<k} &\to (\mathbb{F}_q^s)^n \\ f(x) &\mapsto \left(\begin{bmatrix} f(\alpha_1) \\ f(\gamma\alpha_1) \\ \vdots \\ f(\gamma^{s-1}\alpha_1) \end{bmatrix}, \ldots, \begin{bmatrix} f(\alpha_n) \\ f(\gamma\alpha_n) \\ \vdots \\ f(\gamma^{s-1}\alpha_n) \end{bmatrix} \right) .\end{aligned}$$

The parameter s is also referred to as the folding parameter *of the* FRS *code.*

[*] University of Waterloo, Canada. abhibhav.garg@uwaterloo.ca. Work done when the author was visiting TIFR.

[†] Tata Institute of Fundamental Research, Mumbai, India. {prahladh,mrinal,ramprasad,ashutosh.shankar}@tifr.res.in.

[1] While all the results in this note refer to FRS codes, they extend to all affine FRS codes, which includes multiplicity codes and additive-FRS codes.

The rate *of the above code shall be donoted by R, with $R := k/ns$, and it is known that the fractional distance of the code is $1 - R$.* $\Diamond$

For the rest of the article, the set $S = \{\alpha_1, \dots, \alpha_n\}$ will be fixed and we will just refer to the FRS code as $\mathrm{FRS}_{k,s}$ code. We overload notation and use the same symbol to refer to both the polynomials (which correspond to messages) and their encodings under the above map.

List-decodability: The notion of distance between codewords would be the standard Hamming distance.

Definition 1.2 (Hamming balls)**.** *For any point $y \in \Sigma^n$ for some alphabet Σ, we denote the* Hamming ball of fractional radius ρ around y *by $B(y, \rho)$ defined as*

$$B(y, \rho) := \{x \in \Sigma^n \ : \ |\{i \in [n] \ : \ x_i \neq y_i\}| < \rho n\} \ . \qquad \Diamond$$

The primary objective in list-decodability is to understand up to what radius do Hamming balls have "few" codewords.

Definition 1.3 (List-decodability)**.** *A code $\mathcal{C} \subseteq \Sigma^n$ is said to be (ρ, L) list-decodable if for every $y \in \Sigma^n$ we have*

$$|C \cap B(y, \rho)| \leq L \ . \qquad \Diamond$$

Folded Reed-Solomon codes were shown to achieve list-decoding capacity by Guruswami and Rudra [GR08]. That is, the set of codewords in a ball of radius $1 - R - \varepsilon$ around any point in the code space is small.

Guruswami and Wang [GW13] re-proved this result in the following specific way: for FRS codes with folding parameter $O(1/\varepsilon^2)$, for any point y in the code space, they show the existence of a linear subspace $\mathcal{A} \subset \mathbb{F}_q\left[x\right]^{<k}$ with $\dim \mathcal{A} = O(1/\varepsilon)$ such that every codeword in the ball $B(y, 1 - R - \varepsilon)$ is the encoding of a polynomial in $\mathcal{A}$. This implies that the list size is at most $q^{O(1/\varepsilon)}$. Their proof of the existence of the subspace is algorithmic. We state this as a lemma below.

Lemma 1.4 (Guruswami-Wang [GW13])**.** *Let $y \in \left(\mathbb{F}_q^s\right)^n$ be a received word for a $\mathrm{FRS}_{k,s}$ code of rate $R = k/ns$. Then, for $\rho = 1 - R - \varepsilon$, if $s = \Omega(1/\varepsilon^2)$, there is an affine space $\mathcal{A}$ of dimension $O(1/\varepsilon)$ that contains all codewords in $B(y, \rho) \cap C$. Furthermore, an affine basis for $\mathcal{A}$ can be obtained in time polynomial in $n, \log q, 1/\varepsilon$ given the received word y.*

Subsequently, Kopparty, Saraf, Ron-Zewi and Wootters [KRSW23] showed that the upper bound on the list size at radius $1 - R - \varepsilon$ for such codes can be improved from polynomial $q^{O(1/\varepsilon)}$ to constant $(1/\varepsilon)^{O(1/\varepsilon)}$. A cleaner analysis of this upper bound was given by Tamo [Tam24]. These proofs were also algorithmic: they build on the previous result by taking the subspace as input and "pruning" the list size in a randomized fashion. In particular, if $\mathcal{L}$ denotes the list of codewords in the ball $B(y, 1-R-\varepsilon)$, i.e., $\mathcal{L} := B(y, 1-R-\varepsilon) \cap \mathrm{FRS}_{k,s}$, then the KRSW/Tamo improvement can be written as follows, a further simplified proof of which is presented in Section 2.

Theorem 1.5 ([KRSW23, Tam24])**.** *The size of $\mathcal{L}$ is upper-bounded by $(1/\varepsilon)^{O(1/\varepsilon)}$.*

How small can the list-size bound be? Shangguan and Tamo [ST23] generalized the classical Singleton bound to show that any code with rate R that is $(1-R-\varepsilon, L)$ list-decodable satisfies $L \geq \frac{1-R-\varepsilon}{\varepsilon}$. Very recently, Srivastava [Sri25] and Chen & Zhang [CZ24] gave dramatic improvements on this list-size to $O(1/\varepsilon)$ almost matching the generalized Singleton bound up to a constant multiplicative factor.

Theorem 1.6 ([Sri25])**.** *The size of $\mathcal{L}$ is upper-bounded by $O(1/\varepsilon^2)$.*

Theorem 1.7 ([CZ24])**.** *The size of $\mathcal{L}$ is upper-bounded by $O(1/\varepsilon)$.*

We will give simplified proofs of these improvements in Sections 4 and 5. It is to be noted that these proofs are combinatorial and algorithmizing them (efficiently; in time nearly-linear or even polynomial in the list size) remains open. The results of KRSW/Tamo also extend to list-recovery. However, as Chen-Zhang observe the dramatic improvements on list-size bounds for list-decoding FRS codes obtained by Srivastava and Chen & Zhang do not extend to list-recovery of FRS codes. We (re-)present the Chen & Zhang counterexample in Section 6.

Agreement graphs: A key ingredient we will be using in the proofs of these improvements is the notion of an agreement graph, which we define below.

Definition 1.8 (Agreement graph)**.** *For any code $\mathcal{C} \subseteq \Sigma^n$, message $y \in \Sigma^n$, and a set of distinct codewords $f_1, \ldots, f_m \in \mathcal{C}$, the* agreement graph $G(\{f_1, \ldots f_m\}, y)$ *is defined as the bipartite graph, with m vertices on the left (corresponding to the list of codewords) and n vertices on the right (corresponding to the blocks), and an edge connecting $i \in [m]$ on the left with $j \in [n]$ on the right if the encoding of f_i agrees with y at coordinate j.* ◊

All the proofs will essentially attempt to upper-bound the number of edges in any agreement graph, and thereby infer that there cannot be "too many" left-vertices (codewords) with "large degree" (agreement).

2 KRSW/Tamo's upper bound for list size

The bounds due to Kopparty, Ron-Zewi, Saraf and Wootters work for any linear code, not necessarily FRS codes and we will also state the results in that generality. Let $\mathbb{F}$ be any finite field, s a positive integer and $\mathcal{C} \subseteq (\mathbb{F}^s)^n$ be an $\mathbb{F}$-linear code over the alphabet $\mathbb{F}^s$ with block length n and fractional distance δ.

Let $y \in \left(\mathbb{F}_q^s\right)^n$ be an arbitrary point in the code space of $\mathcal{C}$. Let $\mathcal{L} := \{f_1, \ldots, f_t\} = B(y, \rho) \cap \mathcal{C}$ be the list of codewords at distance at most $\rho = \delta - \varepsilon$ from y.

Definition 2.1 (Certificates)**.** *Let $\mathcal{A}$ be an affine subspace of an $\mathbb{F}$-linear code $\mathcal{C} \subseteq (\mathbb{F}^s)^n$. A* certificate with respect to y *is a sequence of coordinates $(i_1, \ldots, i_a)$ (each $i_j \in [n]$) such that there is a unique codeword $f \in \mathcal{A}$ that agrees with y at the coordinates $i_1, \ldots, i_a$; we shall say that this is a* certificate for f*.*

We shall call such a certificate a minimal certificate *if $i_1, \ldots, i_{a'}$ is* not *a certificate for any $a' < a$.* ♢

Equivalently, if $G = G(\mathcal{L}, y)$ is the agreement graph, then a certificate for f identifies a set of right vertices with unique common neighbour being f.

Theorem 2.2 ([KRSW23, Tam24])**.** *Let $\mathcal{C} \subseteq (\mathbb{F}^s)^n$ be an $\mathbb{F}$-linear code with distance δ and $\rho = \delta - \varepsilon$ and $y \in \left(\mathbb{F}_q^s\right)^n$ an arbitrary message. Suppose $\mathcal{L} := B(y, \rho) \cap \mathcal{C}$ is contained in an affine space of dimension r.*

Then there is a probability distribution on minimal certificates with respect to y such that for any $f \in \mathcal{L}$, the set of of minimal certificates for f of length at most r has probability mass at least ε^r

In particular, the size of $\mathcal{L}$ is upper-bounded by $(1/\varepsilon^r)$.

Proof. Let $\mathcal{A}$ be the affine subspace of dimension r containing $\mathcal{L}$. The distribution on minimal certificates is the most natural one — start with $C_0 = \emptyset$ and extend it by choosing a uniformly random coordinate, one coordinate at a time, until it becomes a minimal certificate. Fix any $f \in \mathcal{L}$ for the rest of the argument. The goal is to show that the probability mass on short certificates for f is large. For a set of coordinates $S = \{i_1, \ldots, i_t\}$, we will define $\mathcal{A}(S)$ as

$$\mathcal{A}(S) := \{f \in \mathcal{A} : \ f \text{ agrees with } y \text{ at coordinate } i, \text{ for all } i \in S\} \ .$$

To begin with, $\mathcal{A}^{(0)} := \mathcal{A}$ contains f. Assume that we have constructed a partial certificate $C_j = (i_1, \ldots, i_j)$ so far with $\mathcal{A}^{(j)} := \mathcal{A}(C_j)$ being an affine space containing f. Whenever we have $\mathcal{A}^{(j)} = \mathcal{A}(C_j) \neq \{f\}$ (i.e., C_j is not yet a certificate for f), let $f' \neq f$ be any other element of $\mathcal{A}^{(j)}$. Since f' and f are distinct codewords, they agree on at most $(1 - \delta)n$ coordinates but f agrees with y on more than $(1 - \delta + \varepsilon)n$ coordinates. Hence, if i_{j+1} was chosen to be any of the coordinates where that f agrees with y but disagrees with f' on that coordinate, then we have that $\mathcal{A}^{(j+1)} := \mathcal{A}(\{i_1, \ldots, i_{j+1}\})$ continues to contain f but is a strictly smaller subspace of $\mathcal{A}^{(j)}$. Thus, with probability at least ε on the choice of $i_{j+1} \in [n]$, we have that for $C_{j+1} = (i_1, \ldots, i_{j+1})$

$$f \in \mathcal{A}^{(j+1)} \text{ and } \dim \mathcal{A}^{(j+1)} < \dim \mathcal{A}^{(j)}.$$

where $\mathcal{A}^{(j+1)} = \mathcal{A}(C_{j+1})$. Since $\dim \mathcal{A}^{(0)} \leq r$, with probability at least ε^r we get a minimal certificate for f of length at most r. □

3 Dimension of typical subspaces obtained from restrictions

In the above proof, we started with an r-dimensional space $\mathcal{A}$ that included all our codewords of interest, and we considered various subspaces $\mathcal{A}_i$ defined as

$$\mathcal{A}_i := \{f \in \mathcal{A} : \ f \text{ agrees with } y \text{ at coordinate } i\}$$

and let $r_i := \dim \mathcal{A}_i$. In the above proof, we mainly used the fact that $r_i < r$ for at least εn many choices of i. The following lemma of Guruswami and Kopparty [GK16] says that, for FRS codes, the average r_i is significantly smaller than r.

Lemma 3.1 (Guruswami and Kopparty [GK16]). *Let $y \in \left(\mathbb{F}_q^s\right)^n$ and $\mathcal{A}$ be an affine subspace of $\mathrm{FRS}_{k,s}$ of dimension r. For each $i \in [n]$, define*

$$\mathcal{A}_i = \{f \in \mathcal{A} : \ f \textit{ agrees with } y \textit{ at coordinate } i\}$$

with $r_i = \dim \mathcal{A}_i$. Then,

$$\sum_{i \in [n]} r_i \leq r \cdot \tau_r \cdot n$$

for $\tau_r = \frac{sR}{s-r+1}$ where $R = k/ns$.

In other words, $\mathbb{E}_i[r_i] \approx r \cdot R$. More precisely, if $s = \Theta(1/\varepsilon^2)$ and $r = \Theta(1/\varepsilon)$, then $\tau_r = R \cdot (1 + \Theta(\varepsilon))$.

For the sake of completeness, we add a proof of the above lemma in Appendix A. Using this lemma, we can obtain significantly better bounds on the list size for FRS codes.

4 Srivastava's improved list size bound

Srivastava's [Sri25] main theorem is the following.

Theorem 4.1 (Better list size bounds for FRS codes [Sri25]). *If y is any received word, and $\mathcal{A}$ is an affine subspace of dimension r, then for any $r \leq t \leq s$ we have*

$$\left| B\left(y, \frac{t}{t+1}\left(1 - \frac{s}{s-r+1}R\right)\right) \cap \mathcal{A} \right| \leq (t-1)r + 1.$$

Writing in terms of $\tau_r = \frac{sR}{s-r+1}$ (as in Lemma 3.1), the above can be written as

$$\left| B\left(y, \frac{t}{t+1}\left(1 - \tau_r\right)\right) \cap \mathcal{A} \right| \leq (t-1)r + 1 \ .$$

Setting parameters: For any parameter $\varepsilon > 0$, we can set $t = 2/\varepsilon$, and $s = 3/\varepsilon^2$. By Guruswami and Wang [GW13], we know that

$$B\left(y, \frac{t}{t+1}(1-\tau_t)\right) \cap \mathrm{FRS}_{k,s}$$

is contained in an affine subspace of dimension at most $r = t - 1$. Plugging these parameters in, we can check that $\rho = \frac{t}{t+1}(1-\tau_t) \geq 1 - R - \varepsilon$.

$$\begin{aligned}
\rho &= \frac{t}{t+1} \cdot \left(1 - \frac{sR}{s-t+2}\right) \\
&= \frac{(2/\varepsilon)}{(2/\varepsilon+1)} \left(1 - R \cdot \frac{3/\varepsilon^2}{3/\varepsilon^2 - 1/\varepsilon + 2}\right) \\
&= \frac{1}{(1+\frac{\varepsilon}{2})} \left(1 - R \cdot \frac{1}{1 - (\varepsilon/3) + (2/3)\varepsilon^2}\right) \\
&= (1 - \frac{\varepsilon}{2} \pm \Theta(\varepsilon^2)) \cdot \left(1 - R\left(1 + \frac{\varepsilon}{3} \pm \Theta(\varepsilon^2)\right)\right) \\
&= 1 - R - \varepsilon\left(\frac{1}{2} + \frac{R}{3}\right) \pm \Theta(\varepsilon^2) \\
&\geq 1 - R - \varepsilon\ .
\end{aligned}$$

In that case, we get that $\mathrm{FRS}_{k,s}$ codes are $(1 - R - \varepsilon, O(1/\varepsilon^2))$-list-decodable.

4.1 Proof of Theorem 4.1

The above theorem is proved by induction on the dimension r. The base case is when $r = 1$. The following bound holds for any linear code.

Lemma 4.2. *(Theorem 4.1 for $r = 1$) If y is any received word, and $\mathcal{A}$ is an affine subspace of dimension 1, then for any $t \geq 1$ we have*

$$\left|B\left(y, \frac{t}{t+1}(1-R)\right) \cap \mathcal{A}\right| \leq t\ .$$

Proof. Let $L = \left|B\left(y, \frac{t}{t+1}(1-R)\right) \cap \mathcal{A}\right|$

Suppose the affine space $\mathcal{A}$ is of form $\{f_0 + \sigma f_1 : \sigma \in \mathbb{F}_q\}$, with $f_1 \neq 0$. Let us use $S := \{i \in [n] : (\mathrm{FRS}_{k,s}(f_1))_i \neq 0\}$ to denote the support of the encoding of f_1. Note that $|S| \geq (1-R) \cdot n$.

Notice also that two distinct codewords in the list have to disagree completely on S. Hence, every right-side vertex in S has at most one outgoing edge.

We now count edges in the agreement graph, from both sides. From the codewords side, since each codeword has agreement strictly more than $n(1 - \frac{t}{t+1}(1-R))$, the number of edges is more than $Ln(1 - \frac{t}{t+1}(1-R))$.

From the locations side, each vertex in S contributes at most one edge. Each vertex outside S may contribute up to L edges. This gives the total number of edges to be at most $|S| + L(n - |S|) = Ln - (L-1)|S| \leq Ln - (L-1)(1-R)n$ using the above lower bound on $|S|$.

Combining the upper and lower bound on the number of edges,

$$Ln\left(1 - \frac{t}{t+1}(1-R)\right) < Ln - (L-1)(1-R)n$$

Rearranging and cancelling out Ln on both sides,

$$(L-1)(1-R)n < L\frac{t}{t+1}(1-R)n$$

Solving for L gives $L < t+1$. □

We now prove the main theorem.

Proof of Theorem 4.1. Let $\rho := \frac{t}{t+1}\left(1 - \tau_r\right)$ and we wish to bound the size of $B(y,\rho) \cap \mathcal{A}$.

$$L(r) := \max_{\mathcal{A}\,:\,\dim \mathcal{A} = r} \left|B(y,\rho) \cap \mathcal{A}\right| .$$

We will prove a bound on $L(r)$ by inducting on r.

Inductive claim: $L_i \leq L(r_i) \leq \sigma \cdot r_i + 1$ for a constant σ independent of r_i.

We will eventually show $\sigma = t - 1$ would be sufficient, giving us the requisite bound.

For each i, let $\mathcal{A}_i$ be the subspace of $\mathcal{A}$ corresponding to agreement at coordinate i with y. Let $r_i := \dim \mathcal{A}_i$. Let L be the number of codewords in $B(y,\rho) \cap \mathcal{A}$, and let L_i be the number of codewords in $B(y,\rho) \cap \mathcal{A}_i$. By the induction hypothesis, for every i such that $r_i < r$, we have $L_i \leq L(r_i) \leq \sigma r_i + 1$.

We count the number of edges in the agreement graph. Counting from the left, each codeword has agreement at least $(1-\rho)n$, therefore the number of edges is at least $(1-\rho)nL$. Counting from the right, coordinate i is incident to at most L_i codewords, therefore the number of edges is at most $\sum_i L_i$. Combining this, we have the inequality $\sum_i L_i \geq (1-\rho)nL$.

We cannot use induction to control the coordinates where $r_i = r$, therefore for these coordinates we use the trivial bound $L_i \leq L$. Let $\mathcal{B}$ be the set of coordinates for which this is true. We therefore have

$$\sum_{i \notin \mathcal{B}} \left(\sigma \cdot r_i + 1\right) \geq L\left((1-\rho)n - |\mathcal{B}|\right) \;.$$

Every codeword in the list agrees with y on the set $\mathcal{B}$, therefore in particular the codewords agree with each other on this set. Since any two codewords can have agreement at most Rn, we have

$|\mathcal{B}| \leq Rn$, which implies the term $((1-\rho)n - |\mathcal{B}|)$ is positive. Therefore, we can deduce

$$L \leq \frac{\sum_{i \notin \mathcal{B}} (\sigma \cdot r_i + 1)}{(1-\rho)n - |\mathcal{B}|} \ .$$

By Lemma 3.1, we have

$$\begin{aligned}
\sum_{i \in [n]} r_i = \sum_{i \notin \mathcal{B}} r_i + |\mathcal{B}| \cdot r \leq rn\tau_r \\
\implies \sum_{i \notin \mathcal{B}} (\sigma \cdot r_i + 1) &\leq \sigma \cdot rn\tau_r - \sigma \cdot r\,|\mathcal{B}| + (n - |\mathcal{B}|) \\
&= \sigma \cdot rn\tau_r + n - |\mathcal{B}|\,(\sigma \cdot r + 1) \ . \\
\implies L \leq \frac{\sigma rn\tau_r + n - |\mathcal{B}|\,(\sigma r + 1)}{(1-\rho)n - |\mathcal{B}|} \ .
\end{aligned}$$

To complete the induction, we have to show $L \leq \sigma \cdot r + 1$. From the above, it suffices to show

$$\begin{aligned}
0 &\leq ((1-\rho)n - |\mathcal{B}|) \cdot (\sigma r + 1) - (\sigma rn\tau_r + n - |\mathcal{B}|\,(\sigma r + 1)) \\
&= (1-\rho)n \cdot (\sigma r + 1) - (\sigma rn\tau_r + n) \ .
\end{aligned}$$

Indeed, using the fact that $\rho = \frac{t}{t+1} \cdot (1 - \tau_r)$, we have

$$\begin{aligned}
(1-\rho) \cdot (\sigma r + 1) - (\sigma r \cdot \tau_r + 1) &= \sigma r \cdot ((1-\rho) - \tau_r) + (1 - \rho - 1) \\
&= \sigma r \cdot ((1-\tau_r) - \rho) - \rho \\
&= \sigma r \cdot \rho \cdot \left(\frac{t+1}{t} - 1\right) - \rho \\
&= \rho \cdot \left(\frac{\sigma r}{t} - 1\right) \geq 0 \quad \text{for } \sigma = (t-1)
\end{aligned}$$

since $(t-1)r \geq t$ as $t > r \geq 2$. □

From the above proof, it feels like we could have perhaps taken $\sigma = \frac{t}{r}$, thereby getting a list size bound of $L(r) \leq \sigma r + 1 \leq t + 1$ instead of $O(tr)$. However, note that the above proof used the fact that σ was independent of r (when we bounded $\sum_{r_i < r} L(r_i)$ with $\sigma \sum r_i + (n - |\mathcal{B}|)$). Nevertheless, this perhaps suggests that there is some slack in the above analysis and one could perhaps improve the analysis to obtain a list-size bound of $O(t)$ instead of $O(tr)$.

Chen and Zhang [CZ24] (independent and parallel to Srivastava [Sri25]) obtain an $O(t)$ bound by using induction to bound the number of edges of the agreement graph rather than bounding the list size directly.

5 Further improvements on the list size due to Chen and Zhang

Theorem 5.1 (Chen and Zhang [CZ24]). *Let $y \in \left(\mathbb{F}_q^s\right)^n$ be an arbitrary received word for the* $\mathrm{FRS}_{k,s}$ *code. For any $0 \le t \le s$, we have*

$$\left| B\left(y, \frac{t}{t+1}\left(1-\tau_t\right)\right) \cap \mathrm{FRS}_{k,s} \right| \le t \ ,$$

where $\tau_t = \frac{sR}{s-t+1}$ (as in Lemma 3.1).

Setting parameters: As in the previous case, if $t = 2/\varepsilon$ and $s = 3/\varepsilon^2$ we once again have $\rho = \frac{t}{t+1}\left(1-\tau_t\right) \ge 1 - R - \varepsilon$, the above theorem shows that $\mathrm{FRS}_{k,s}$ codes are $(1-R-\varepsilon, 2/\varepsilon)$-list-decodable.

Remark. *Unlike the previous bound of Srivastava (Theorem 4.1), the above bound is oblivious of any ambient space that the codewords lie in. In particular, the above list-size bound does not rely on the fact from Guruswami and Wang [GW13] that all close-enough codewords lie in a low-dimensional affine space.* ◊

The above theorem will be proved by once again considering relevant agreement graphs and upper-bounding the number of edges in it. For a set of distinct codewords $\{f_1, \ldots, f_m\}$ and a received word $y \in \left(\mathbb{F}_q^s\right)^n$, let $G = G(\{f_1, \ldots, f_m\}, y)$ be the agreement graph. We will use E_G to denote the number of edges in G. For any subset H of left vertices in G, let E_H denote the number of edges in the induced graph $G(H, y)$.

Let n_G be the number of right vertices of G that have degree at least 1 (these are the positions where at least one of the codewords agrees with y). Similarly, for any subgraph induced by a set H of left vertices, n_H is the number of right vertices with degree at least 1 (we overload notation and use H for both the subset of vertices and the induced subgraph).

The main technical lemma of Chen and Zhang can be stated as follows.

Lemma 5.2 (Chen and Zhang [CZ24]). *Let $\mathcal{A}$ be the affine subspace spanned by $f_1, \ldots, f_m$ and suppose r be the dimension of this affine space. Then, for any agreement graph $G = G(\{f_1, \ldots, f_m\}, y)$ corresponding to a message $y \in \left(\mathbb{F}_q^s\right)^n$, we have*

$$E_G \le \frac{(m-1)k}{s-r+1} + n_G \ .$$

Recalling the parameter τ_r from Lemma 3.1, the above can be restated as saying

$$E_G \le (m-1) \cdot n \cdot \tau_r + n_G \ .$$

Before we see the proof of the above lemma, let us see how Lemma 5.2 implies Theorem 5.1.

Proof of Theorem 5.1. Assume on the contrary that there are $t+1$ distinct codewords $f_1, \dots, f_{t+1}$ that with fractional distance less than ρ from y, where $\rho = \frac{t}{t+1}(1-\tau_t) = \frac{t}{t+1} - \frac{t}{t+1}\tau_t$. Consider the agreement graph $G = G(\{f_1, \dots, f_{t+1}\}, y)$. By counting edges from the left, we have that

$$|E_G| > (1-\rho)n \cdot (t+1) = (t\tau_t + 1)n \ .$$

On the other hand, note that any set of $t+1$ codewords is contained in an affine space of dimension $r \leq t$. Thus, using Lemma 5.2 we have

$$|E_G| \leq (t+1-1) \cdot n \cdot \tau_t + n_G \leq (t\tau_t + 1) \cdot n$$

contradicting the above bound. Hence the size of the list must be at most t. □

5.1 Proof of Lemma 5.2

Recall that we have to prove that for $G = G(\{f_1, \dots, f_m\}, y)$, the number of edges $|E_G|$ is upper-bounded by

$$E_G \leq (m-1) \cdot n \cdot \tau_r + n_G \ .$$

where r is the dimension of the smallest affine space $\mathcal{A}$ containing $f_1, \dots, f_m$.

The proof is by induction on m. The case of $m = 1$ is trivial, since $E_G = n_G$ when $m = 1$.

Now suppose $m \geq 2$. Hence $r \geq 1$. We partition the set of codewords as follows. Let $f^{(0)}, f^{(1)}, \dots, f^{(r)}$ be $r+1$ codewords in the list $\{f_1, \dots, f_m\}$ such that the smallest affine space generated by $\left\{f^{(0)}, \dots, f^{(r)}\right\}$ is $\mathcal{A}$. For $i = 0, \dots, r$, let $\mathcal{A}^{(i)}$ be the smallest affine space generated by $\left\{f^{(0)}, \dots, f^{(i)}\right\}$. Observe that the affine dimension of $\mathcal{A}^{(i)}$ is i and $f^{(i)} \in \mathcal{A}^{(i)} \setminus \mathcal{A}^{(i-1)}$ where we have defined $\mathcal{A}^{(-1)} := \emptyset$. For $i = 0, \dots, r$, define

$$H'_i := \mathcal{A}^{(i)} \cap \{f_1, \dots, f_m\} \ ,$$
$$H_i := H'_i \setminus \mathcal{A}^{(i-1)} \ .$$

Clearly $(H_0, \dots, H_r)$ is a partition of $\{f_1, \dots, f_m\}$. Furthermore, $f^{(i)} \in H_i$ and hence $H_i \neq \emptyset$. Let $m_i := |H_i|$. We have $\sum m_i = m$ and each $0 \neq m_i < m$ since $m_0 = 1$ and $r \geq 1$. Let $r^{(i)}$ be the affine dimension of H_i.

We apply the inductive hypothesis on the subgraphs induced by $H_0, \dots, H_r$. The induced subgraphs are exactly the agreement graphs of the list of codewords in H_i. Therefore by induction we have

$$E_{H_i} \leq (m_i - 1) \cdot n \cdot \tau_{r^{(i)}} + n_{H_i} \leq (m_i - 1) \cdot n \cdot \tau_r + n_{H_i}.$$

The total number of edges of G is the sum of the number of edges in each induced graph, therefore

$$\begin{aligned} E_G = \sum_{i=0}^{r} E_{H_i} \leq \sum_{i=0}^{r} ((m_i - 1) \cdot n \cdot \tau_r + n_{H_i}) &= m \cdot n \cdot \tau_r - (r+1) \cdot n \cdot \tau_r + \sum_i n_{H_i} \\ &= (m-1) \cdot n \cdot \tau_r - r \cdot n \cdot \tau_r + \sum_i n_{H_i} \ . \end{aligned}$$

We now relate the quantities $\sum n_{H_i}$ with n_G.

Consider any right vertex $j \in [n]$ of G. If j has degree 0 in G, then j does not contribute to n_G or to n_{H_i} for any i.

For each $j \in [n]$ with degree at least 1 in G, let t_j be the number of i's such that there is an edge from j to H_i. Then j contributes t_j to $\sum n_{H_i}$ and 1 to n_G. Hence, we have $\sum_i n_{H_i} - n_G = \sum_j (t_j - 1)$.

Using this in the equation above gives

$$E_G \leq (m-1) \cdot n \cdot \tau_r + n_G - r \cdot n \cdot \tau_r + \sum_j (t_j - 1) \ .$$

For each such $j \in [n]$, let $\mathcal{A}_j$ be the affine subspace of $\mathcal{A}$ containing all codewords that agree with the message y at coordinate j, and let r_j be its dimension. Note by our construction of the partition $H_0, \ldots, H_r$ that any set of vectors chosen by picking at most one from each H_i are affine independent. Hence, since j has edges to t_j different H_i's, we have that $r_j \geq (t_j - 1)$.

By Lemma 3.1, we have $\sum (t_j - 1) \leq \sum r_j \leq r \cdot n \cdot \tau_r$. Combining this with the above equation, we have

$$E_G \leq (m-1) \cdot n \cdot \tau_r + n_G \ .$$

That completes the proof of Lemma 5.2. □

6 List-size lower bounds for list-recovery

Although Theorem 5.1 gives optimal bounds for list-decoding of FRS codes, Chen and Zhang also show that an exponential dependence in ε is unavoidable for the question of list-recovery. In this section we give their counter-example.

Recall that the set of evaluation points for the $\mathrm{FRS}_{k,s}$ code are $\alpha_1, \ldots, \alpha_n$, with γ being the generator of $\mathbb{F}_q^*$ used for the folding. For each $i \in [n]$, define the polynomial $Q_i(x)$ defined as

$$Q_i(x) = (x - \alpha)(x - \gamma\alpha) \cdots (x - \gamma^{s-1}\alpha).$$

The i-th symbol of the $\mathrm{FRS}_{k,s}$ encoding of a polynomial g can equivalently also be thought of as the residue $(g(x) \bmod Q_i(x))$.

Define integer parameters m, p such that $m \approx \frac{R}{\varepsilon} + 1$ and

$$p = \left\lfloor \frac{m \left\lfloor \frac{k-1}{s} \right\rfloor}{m-1} \right\rfloor = \frac{m}{m-1} \cdot \frac{k}{s} - O(1) = n(R+\varepsilon) - O(1).$$

Consider the following set of m polynomials:

$$\text{For } i = 1, \dots, m-1, \quad f_i(x) := \prod_{\substack{j \in [p] \\ j \neq i \bmod m}} Q_i(x).$$

By the choice of m and k, it follows that $\deg f_i \leq (k-1)$ for all $i \in [m]$ since each f_i is a product of at most $\frac{m-1}{m}$ of the Q_j's for $j \in [p]$.

Lemma 6.1 (List-recovery for FRS codes [CZ24])**.** *Let B be any set of ℓ distinct field elements. Consider the set of polynomials*

$$\mathcal{G} := \{\beta_1 f_1 + \dots + \beta_m f_m \ : \ \beta_i \in B\} \ .$$

Then, $|\mathcal{G}| = \ell^m$ and, for each $i \in [p]$, we have

$$\left|\left\{ (\mathrm{FRS}_{k,s}(g))_i \ : \ g \in \mathcal{G} \right\}\right| \leq \ell \ .$$

(That is, the FRS *encoding of any polynomial in $\mathcal{G}$ takes only one of ℓ possible values in the first p coordinates.)*

Since $p \approx n(R+\varepsilon)$, we have a particular instance of list-recover with each coordinate list-size bounded by ℓ, with $\ell^{R/\varepsilon}$ codewords with fractional agreement of $R + \varepsilon$.

Proof. To see that $|\mathcal{G}|$ has size ℓ^m, we observe that the polynomials $f_1, \dots, f_m$ are linearly independent. Indeed, if $c_1 f_1 + \dots + c_m f_m = 0$, with $c_1 \neq 0$ (without loss of generality), looking at the equation modulo $Q_1(x)$ yields a nonzero quantity on the left-hand side but zero on the right.

As for the second claim, let $g = \beta_1 f_1 + \cdots \beta_m f_m$. Then, observe that $(\mathrm{FRS}_{k,s}(g))_i = g \bmod Q_i(x) = \beta_{i'} \left(f_{i'}(x) \bmod Q_i(x)\right)$ where $i' \in [m]$ is the unique value such that $i' = i \bmod m$ (since all other f_j's are divisible by Q_i). As β_i's come from a set of size at most ℓ, the i-th coordinate of $\mathrm{FRS}_{k,s}(g)$ will be one of the ℓ scalings of $(f_{i'}(x) \bmod Q_i(x))$. $\square$

References

[CZ24] Yeyuan Chen and Zihan Zhang. *Explicit folded Reed-Solomon and multiplicity codes achieve relaxed generalized singleton bound*, 2024. (manuscript). arXiv:2408.15925. 1, 3, 8, 9, 12

[GK16] Venkatesan Guruswami and Swastik Kopparty. *Explicit subspace designs*. Comb., 36(2):161–185, 2016. (Preliminary version in *54th FOCS*, 2013). eccc:2013/060. 5, 13

[GR08] 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). arXiv:cs/0511072, eccc:2005/133. 1, 2

[GW13] 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:2012/073. 2, 6, 9

[Kra03] Victor Yu. Krachkovsky. *Reed-Solomon codes for correcting phased error bursts*. IEEE Trans. Inform. Theory, 49(11):2975–2984, 2003. 1

[KRSW23] Swastik Kopparty, Noga Ron-Zewi, Shubhangi Saraf, and Mary Wootters. *Improved list decoding of Folded Reed-Solomon and Multiplicity codes*. SIAM J. Comput., 52(3):794–840, 2023. (Preliminary version in *59th FOCS*, 2018). arXiv:1805.01498, eccc:2018/091. 1, 2, 3, 4

[Sri25] Shashank Srivastava. *Improved list size for folded Reed-Solomon codes*. In Yossi Azar and Debmalya Panigrahi, eds., *Proc. 36th Annual ACM-SIAM Symp. on Discrete Algorithms (SODA)*, pages 2040–2050. 2025. arXiv:2410.09031. 1, 3, 5, 8

[ST23] Chong Shangguan and Itzhak Tamo. *Generalized Singleton bound and list-decoding Reed-Solomon codes beyond the Johnson radius*. SIAM J. Comput., 52(3):684–717, 2023. (Preliminary version in *52nd STOC*, 2020). arXiv:1911.01502. 3

[Tam24] Itzhak Tamo. *Tighter list-size bounds for list-decoding and recovery of folded Reed-Solomon and multiplicity codes*. IEEE Trans. Inform. Theory, 70(12):8659–8668, 2024. arXiv:2312.17097. 1, 2, 3, 4

A Proof of the Guruswami-Kopparty lemma

For the sake of completeness, we give a proof of the Lemma 3.1 (restated below):

Lemma 3.1 (Guruswami and Kopparty [GK16]). *Let $y \in \left(\mathbb{F}_q^s\right)^n$ and $\mathcal{A}$ be an affine subspace of $\mathrm{FRS}_{k,s}$ of dimension r. For each $i \in [n]$, define*

$$\mathcal{A}_i = \{f \in \mathcal{A} : \ f \text{ agrees with } y \text{ at coordinate } i\}$$

with $r_i = \dim \mathcal{A}_i$. Then,

$$\sum_{i \in [n]} r_i \le r \cdot \tau_r \cdot n$$

for $\tau_r = \frac{sR}{s-r+1}$ where $R = k/ns$.

Proof. Let the r-dimensional affine space $\mathcal{A}$ be $f_0 + \mathbb{F}\text{-span}\{f_1, \dots, f_r\}$, where $f_1, \dots, f_r$ are linearly independent polynomials of degree less than k. The *Folded-Wronskian*, $W_\gamma(f_1, \dots, f_r)$ of these polynomials is defined as the following determinant of an $r \times r$ matrix.

$$W_\gamma(f_1, \dots, f_r) = \begin{vmatrix} f_1(x) & f_2(x) & \cdots & f_r(x) \\ f_1(\gamma x) & f_2(\gamma x) & \cdots & f_r(\gamma x) \\ \vdots & \vdots & \ddots & \vdots \\ f_1(\gamma^{r-1}x) & f_2(\gamma^{r-1}x) & \cdots & f_r(\gamma^{r-1}x) \end{vmatrix}$$

We will use $\mathcal{W}_\gamma(f_1, \dots, f_r)$ to refer to the $r \times r$ matrix above. The above polynomial has degree at most rk, and since $f_1, \dots, f_r$ are linearly independent, it is known that the Folded-Wronskian is a nonzero polynomial. We will relate the r_i's with appropriate roots of $W_\gamma(f_1, \dots, f_r)$ and their multiplicities.

Fix a coordinate $i \in [n]$ and α_i being the correspondent element of $\mathbb{F}$. The space $\mathcal{A}_i$ can be equivalently expressed as all polynomials form $f_0 + \beta_1 f_1 + \cdots + \beta_r f_r$ (where $\beta_1, \dots, \beta_r \in \mathbb{F}_q$) such that

$$\beta_1 f_1(\gamma^j \alpha_i) + \cdots + \beta_r f_r(\gamma^j \alpha_i) = (y_i)_j - f_0(\gamma^j \alpha_i) \quad \text{for } j = 0, \dots, s-1$$

In other words, $\beta_1, \dots, \beta_r$ are solutions to the linear system

$$\begin{bmatrix} f_1(\alpha_i) & \cdots & f_r(\alpha_i) \\ f_1(\gamma\alpha_i) & \cdots & f_r(\gamma\alpha_i) \\ \vdots & \ddots & \vdots \\ f_1(\gamma^{s-1}\alpha_i) & \cdots & f_r(\gamma^{s-1}\alpha_i) \end{bmatrix}_{s \times r} \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_r \end{bmatrix}_{r \times 1} = \begin{bmatrix} (y_i)_0 - f_0(\alpha_i) \\ (y_i)_1 - f_0(\gamma\alpha_i) \\ \vdots \\ (y_i)_{s-1} - f_0(\gamma^{s-1}\alpha_i) \end{bmatrix}_{s \times 1}.$$

Hence, if $\dim \mathcal{A}_i = r_i$, then the rank of the $s \times r$ matrix on the LHS is at most $r - r_i$. Furthermore, note that for any $\sigma \in \{\alpha_i, \gamma\alpha_i, \dots, \gamma^{s-r}\alpha_i\}$, the matrix $\mathcal{W}_\gamma(f_1, \dots, f_r) \mid_{x=\sigma}$ is an $r \times r$ submatrix of the above $s \times r$ matrix. Since the above $s \times r$ matrix has a rank-deficit of r_i, we have that each such σ must be a root of $W_\gamma(f_1, \dots, f_r)$ of multiplicity at least r_i. Hence,

$$\sum_{i \in [n]} r_i(s - r + 1) \leq \deg(W_\gamma(f_1, \dots, f_r)) \leq rk$$

$$\implies \sum_{i \in [n]} r_i \leq \frac{rk}{s - r + 1} = r \cdot \tau_r \cdot n. \qquad \square$$