Class 13 Exercises

CS250/EE387, Winter 2022

In the lecture videos/notes, we saw *Folded Reed-Solomon Codes*. Recall that the guarantee of these codes was the following:

Theorem 1. *Let $\varepsilon > 0$. There is a choice of $s = O(1/\varepsilon)$ and $m = O(1/\varepsilon^2)$ so that the following holds.*

Let $\mathcal{C} \subseteq (\mathbb{F}_q^m)^N$ be a Folded RS code with folding parameter m. (So $N = n/m$, where $n \leq q$ is the length of the original RS code). Let R be the rate of $\mathcal{C}$.

The $\mathcal{C}$ is $(1 - R - \varepsilon, L)$-list-decodable, where $L = q^s$. Moreover, for any $z \in (\mathbb{F}_q^m)^N$, the list

$$\mathcal{L} = \{c \in \mathcal{C} : \delta(c, z) \leq 1 - R - \varepsilon\}$$

is contained in a subspace $V \subseteq \mathcal{C}$ of dimension at most s.

In this exercise, we'll see that actually we can improve the list size from $L = q^s$ (which is larger than N^s, since $q \geq n \geq N$) to something that doesn't depend on the length N of the code.

1. For this question, we will use the following theorem:

   Theorem 2. *Let $V \subset (\mathbb{F}_q^m)^N$ be any subspace of dimension at most s, so that for any two $c, c' \in V$, $\delta(c, c') \geq 1 - R$.*

   Let $S \subseteq [N]$ be a random set of size t. Then the probability that there exist two $c, c' \in V$ so that $c|_S = c'|_S$ is at most

   $$\mathbb{P}_S[c|_S = c'|_S] \leq R^t \left(\frac{t}{R}\right)^s.$$

   You don't need to prove the theorem (yet!), but just make sure you understand it.

   Solution

   Got it!

2. Consider the following (randomized) decoding algorithm for an FRS code of rate R.

   Given $z \in (\mathbb{F}_q^m)^N$:

   - Run the decoder from Theorem 1 to obtain a subspace $V \subseteq \mathcal{C}$ of dimension at most $s = O(1/\varepsilon)$ that contains the list $\mathcal{L} = \{c \in \mathcal{C} : \delta(c, z) \leq 1 - R - \varepsilon\}$.

- Choose $S \subseteq [N]$ of size t uniformly at random. (In more detail, we will choose t elements of $[N]$, independently with replacement, to be in S. So maybe it happens that $|S| \leq t$ if there are collisions).
- If there is a unique codeword $c \in V$ so that $c|_S = z|_S$, return c.
- Otherwise, return FAIL.

Let $c \in \mathcal{C}$ be such that $\delta(c, z) \leq 1 - R - \varepsilon$. Show that the probability that this algorithm returns c is at least

$$\Pr[\text{Alg returns } c] \geq (R+\varepsilon)^t - R^t \left(\frac{t}{R}\right)^s.$$

Solution

There are two reasons that the algorithm would fail to return c. The first is that $z|_S \neq c|_S$. Since $\delta(c, z) \leq 1 - R - \varepsilon$, the probability that

$$\Pr[z|_S = c|_S] = (R+\varepsilon)^t,$$

and so

$$\Pr[z|_S \neq c|_S] = 1 - (R+\varepsilon)^t.$$

The other bad event that could happen is that if there is some $c' \in V$ so that $c'|_S = c|_S$. By Theorem 2, the probability that this occurs is at most $R^t(t/R)^s$. By a union bound,

$$\Pr[\text{Alg returns } c] \geq 1 - (1 - (R+\varepsilon)^t) - R^t \left(\frac{t}{R}\right)^s = (R+\varepsilon)^t - R^t(t/R)^s,$$

as desired.

3. Suppose that R is some constant (like, $1/4$ or something like that), and that s is large enough and ε is small enough. Show that if $t \geq \frac{100s}{\varepsilon} \ln(s/\varepsilon)$, then

$$R^t(t/R)^s \leq \frac{1}{e}(R+\varepsilon)^t.$$

Note: It's okay to be super handwavey here. In particular, feel free to use the approximation $e^x \approx 1 + x$ for small x as though it were an equality, and feel free to make the constant "100" bigger if you like, and feel free to change $1/e$ to $1/2$ or $9/10$ or any constant in $(0, 1)$ that you like.

Solution

First we write $(R+\varepsilon)^t = R^t(1+\varepsilon/R)^t$, so we want to show that

$$(t/R)^s \leq \frac{1}{2}(1+\varepsilon/R)^t.$$

Using the approximation $1 + x \approx e^x$ for small x, we have

$$(1+\varepsilon/R)^t \approx e^{t\varepsilon/R},$$

so we want to show that

$$(t/R)^s \leq \frac{1}{e} e^{t\varepsilon/R}.$$

Taking logs of both sides, this reads

$$s \ln(t/R) \leq \frac{t\varepsilon}{R} - 1.$$

Thus, we should have

$$t \geq \frac{R(s \ln(t/R) + 1)}{\varepsilon}. \tag{1}$$

If R is a constant, then choosing $t = \Omega(s \ln(s/\varepsilon)/\varepsilon)$ will satisfy this.
(To see this, we can plug into (1):

$$\begin{aligned}
\frac{100 s \ln(s/\varepsilon)}{\varepsilon} &\geq \frac{R(s \ln(100 s \ln(s/\varepsilon)/\varepsilon) + 1)}{\varepsilon} \\
&= \frac{Rs \ln(s/\varepsilon)}{\varepsilon} + \frac{Rs \ln\ln(s/\varepsilon)}{\varepsilon} + \frac{Rs \ln(100) + 1}{\varepsilon} \\
&\Leftrightarrow \\
\frac{(100 - R) s \ln(s/\varepsilon)}{\varepsilon} &\geq \frac{Rs \ln\ln(s/\varepsilon)}{\varepsilon} + \frac{Rs \ln(100) + 1}{\varepsilon} \\
&\Leftrightarrow \\
(100 - R) \ln(s/\varepsilon) &\geq R \ln\ln(s/\varepsilon) + R \ln(100) + 1
\end{aligned}$$

which is true for large enough s and small enough ε, since the left hand is asymptotically larger than the right hand side.)

4. Use the previous two parts to show that, for any z,

$$|\mathcal{L}_z| = \left(\frac{s}{\varepsilon}\right)^{O(s/\varepsilon)} = \left(\frac{1}{\varepsilon}\right)^{O(1/\varepsilon^2)},$$

where

$$\mathcal{L}_z = \{c \in \mathcal{C} \,:\, \delta(c, z) \leq 1 - R - \varepsilon\}.$$

In particular, the FRS code $\mathcal{C}$ is actually $(1 - R - \varepsilon, (1/\varepsilon)^{O(1/\varepsilon^2)})$-list-decodable, which is asymptotically better than what Theorem 1 gives (assuming N is way way bigger than $1/\varepsilon$).

Note: As before, assume that R is some constant, like $1/4$.

Hint: Consider the expected number of codewords returned by the algorithm above. On the one hand, this is at most one. On the other hand, what do you get if you compute it another way?

Solution

Following the hint, we have

$$1 \geq \mathbb{E}[\text{num codewords returned}] \geq \sum_{c \in \mathcal{L}_z} \Pr[c \text{ is returned }],$$

where the second inequality follows from part 2. By part 3, we conclude that

$$1 \geq |\mathcal{L}_z| \cdot (1 - 1/e)(R + \varepsilon)^t,$$

where

$$t = 100s \log(s/\varepsilon)/\varepsilon.$$

Solving for $|\mathcal{L}_z|$, we have

$$|\mathcal{L}_z| \leq \frac{1}{(1 - 1/e)(R + \varepsilon)^t} = \exp(O(t)) = \exp(O(s \log(s/\varepsilon)/\varepsilon)) = (s/\varepsilon)^{O(s/\varepsilon)}.$$

Plugging in $s = O(1/\varepsilon)$ gives the result.

5. **Bonus.** Prove Theorem 2. We'll walk you through a slightly easier version:

   Theorem 3. *Let $V \subseteq \mathbb{F}_q^n$ be any subspace of dimension at most s, so that for any two $c, c' \in V$, $\delta(c, c') \geq 1 - R$.*

   Let $S \subseteq [n]$ be a random (multi-)set of size t (that is, choose t elements of n, independently with replacement). Then the probability that there exist two $c, c' \in V$ so that $c|_S = c'|_S$ is at most

   $$\Pr_S[c|_S = c'|_S] \leq R^t \left(\frac{t}{R}\right)^s =: p,$$

   where above we are defining p to be that quantity.

   (The only difference between this and Theorem 2 is that we are ignoring the folding. The folding doesn't really change the proof, it's just obnoxious to keep track of.)

   (a) Let $M \in \mathbb{F}_q^{n \times s}$ be a matrix whose columns form a basis for V. Let $S \subseteq [n]$ be as in the theorem statement. Let $M|_S$ denote M restricted to the columns in S. Explain why it is enough to show that $M|_S$ is rank s with probability at least p.

   Solution

   Let $c, c' \in V$, so we can write $c = Mx, c' = Mx'$ for some $x, x' \in \mathbb{F}^s$. If $c|_S = c'|_S$, then $(M|_S)x = (M|_S)x'$, but if $M|_S$ is full rank this implies that $x = x'$. But then $c = c'$.

   (b) Say that $S = \{i_1, i_2, \ldots, i_t\}$, and imagine choosing these indices one at a time. Say we have chosen i_1 and are about to choose i_2. Explain why the i_2'th row of M is linearly independent with the i_1'st row of M with probability at least R.

Solution

Let's call the first row that we picked $v \in \mathbb{F}^s$. Suppose towards a contradiction that the claim is false. Then there's a strictly greater than R fraction of rows of M that are linearly dependent with v. Let $x \in \mathbb{F}^s$ be any nonzero vector so that $v^T x = 0$. But then Mx has strictly greater than an R fraction of zeros, since $(Mx)_i = 0$ for any row i that's linearly dependent with v. This is a contradiction of the fact that $\delta(c, c') \geq 1 - R$ for any $c, c' \in V$, since Mx and 0 are both in V and they have distance $< 1 - R$.

(c) Continuing the line of thought above, suppose we have chosen i_1 and i_2 (and suppose that rows i_1 and i_2 span a space of dimension at most s, which will be true anyway as long as $s > 2$). Explain why the i_3'rd row of M does not lie in the span of the first two, with probability at least R.

Solution

We can use the same argument as before. Suppose towards a contradiction that the claim is false, and say that v_1, v_2 are the first two rows of M that we picked. Choose any x so that $x^T v_1 = x^T v_2 = 0$. We can do this since s_1, s_2 don't span an s-dimensional space. But then Mx has strictly more than a R fraction of zeros, and this is a contradiction of distance.

(d) Continuing further, let $2 < r \leq t$, and suppose that you have chosen $i_1, i_2, \ldots, i_{r-1}$, **and** that you still don't have a full rank set of rows. Explain why the i_r's row of M does not lie in the span of rows $i_1, \ldots, i_{r-1}$, with probability at least R.

Solution

Exactly the same argument again!

(e) Use the fact that you proved in the previous part to prove the theorem.

Hint. If we draw t rows of M and fail to get a full-rank matrix, then there are at least $t - s + 1$ rows that we drew that did not increase the dimension of the span of the rows that we have...

Hint. We have $\binom{t}{t-s+1} R^{t-s+1} \leq R^t (t/R)^s$ (why?)

Solution

Suppose that we draw t rows of M and fail to get a full-rank matrix. Following the hint, there are at least $t - s + 1$ choices of rows so that when we chose that row, we did not increase the dimension of the span of rows that we were building.
By the previous part, the probability that this happens for those $t - s + 1$ choices is at most R^{t-s+1}. We need to union bound over all possible choices of $t - s + 1$ rows, so we get

$$\Pr[M|_S \text{ not rank } s\ ] \leq \binom{t}{t-s+1} R^{t-s+1}.$$

Following this hint, this is at most the thing we want it to be. To see why, notice

that

$$\binom{t}{t-s+1}R^{t-s+1} = \binom{t}{s-1}R^{t-s+1} \leq t^{s-1}R^{t-s+1} = (t/R)^{s-1}R^t \leq (t/R)^s R^t,$$

as desired.