Class 14 Exercises

CS250/EE387, Winter 2025

In the lecture videos/notes, we saw *Locally Correctable Codes* (LCCs). Recall the definition of an LCC:

Definition 1 (LCC)**.** *A code $\mathcal{C} \subseteq \mathbb{F}_q^n$ is a (δ, Q, γ)-LCC if there is a randomized algorithm A so that the following holds. For all $w \in \mathbb{F}_q^n$ so that $\delta(c, w) \leq \delta$ for some $c \in \mathcal{C}$, and for all $i \in [n]$, A makes Q queries to w and outputs $A^w(i)$ so that*

$$\Pr[A^w(i) = c_i] \geq 1 - \gamma,$$

where the probability is over the choice of queries.

We saw several examples of LCCs. One was Reed-Muller codes:

Definition 2 (q-ary Reed-Muller Code)**.** *The m-variate Reed-Muller code over $\mathbb{F}_q$ with degree r is given by*

$$RM_q(m, r) = \left\{ \langle f(\vec{\alpha}) \rangle_{\vec{\alpha} \in \mathbb{F}_q^m} \,:\, f \in \mathbb{F}_q[X_1, \ldots, X_m], \deg(f) \leq r \right\}.$$

For the rest of today, we will specialize to the case where $m = 2$ for simplicity.

As we saw in the videos, the RM codes that were decent LCCs had low rate. Today, we'll see one way to modify them, through a process called *lifting*, to make the rate close to 1. To motivate this, let's do a quick warm-up:

0. Consider the following property of a (possibly high-degree) polynomial $p(X, Y)$, which we'll call property $\mathcal{P}(r)$:

   Definition 3. *We say that $p(X, Y) \in \mathbb{F}_q[X, Y]$ satisfies* property $\mathcal{P}(r)$ *if for any line $\ell(T) = (aT + b, cT + d)$, the univariate polynomial $p(\ell(T))$ is equivalent to (that is, has all the same evaluations as) a polynomial of degree at most r.*

   (a) Explain why any polynomial $p(X, Y)$ with total degree at most r has property $\mathcal{P}(r)$.

   Solution

   This is because

   $$p(\ell(T)) = \sum_{i,j} p_{i,j} (aT + b)^i (cT + d)^j$$

   and we can see that the maximum power on T is the maximum $i + j$ over all (i, j)

that show up in the sum, which is at most r by the definition of total degree.

(b) Let $\mathcal{F} \subseteq \mathbb{F}_q[X, Y]$, so that every polynomial $f \in \mathcal{F}$ has property $\mathcal{P}(r)$. In the mini-lecture, we saw a proof that $RM_q(2, r)$ was an LCC (for appropriate values of q, r). Explain why the same argument works for the code

$$\mathcal{C} = \left\{ \langle f(\vec{\alpha}) \rangle_{\vec{\alpha} \in \mathbb{F}_q^2} \,:\, f \in \mathcal{F} \right\}.$$

Solution

The only property we used about RM codes was that their restriction to a line was an RS code of degree at most r. Property $\mathcal{P}(r)$ says exactly this.

(c) What might be the advantage of considering a code like $\mathcal{C}$ over $RM_q(m = 2, r)$?

Solution

By (a), such a $\mathcal{C}$ is at least as large as $RM_q(2, r)$. If it happened to be bigger, we'd have a code with the same locality properties but better rate!

For the rest of today's class, we will see how to come up with a code $\mathcal{C}$ as in part (c) above with rate way better than the corresponding Reed-Muller code! **We'll do it for the special case that q is a power of 2; $m = 2$; and $r = q - 2$.**

1. Let's start with an example. Consider the polynomial $p(X, Y) = X^2Y^2 \in \mathbb{F}_4[X, Y]$.

   (a) Is (the evaluation vector of) $p(X, Y)$ in $RM_{q=4}(m = 2, r = 2)$?

   Solution

   No, since the total degree is 4, which is larger than $r = 2$.

   (b) Show that $p(X, Y)$ has property $\mathcal{P}(2)$.
   Hint: You may use the **facts** that for any $x, y \in \mathbb{F}_4$, we have $(x + y)^2 = x^2 + y^2$, and $x^4 = x$.

   Solution

   Let $\ell(T) = (aT + b, cT + d)$. Then

   $$\begin{aligned} p(\ell(T)) &= (aT + b)^2(cT + d)^2 \\ &= (a^2T^2 + b^2)(c^2T^2 + d^2) \\ &= (ac)^2T^4 + (a^2d^2 + b^2c^2)T^2 + (db)^2 \\ &\equiv (ac)^2T + (a^2d^2 + b^2c^2)T^2 + (db)^2 \end{aligned}$$

   is equivalent to a polynomial of degree at most 2.

   (c) Reflect on the fact that this is pretty weird. Can you come up with an example like this over the real numbers?

   Solution

   Weird! (And no, you can't. Also you can't come up with one over $\mathbb{F}_p$ for prime p).

2. **From now until the end of class, let $q = 2^t$. As before, we have $m = 2$, and let's fix $r = q - 2$.**

   (a) What is the rate of $RM_q(m = 2, r = q - 2)$? (Or at least, what is its limit as q gets large?)

   Solution

   The dimension of this code is the number of monomials of total degree at most $q - 2$, which is $\sum_{j=0}^{q-2}(j + 1) = \frac{q^2}{2} + O(q)$. (This is because the number of bivariate monomials of degree exactly j is $j + 1$.)
   The length of the code is q^2, so the rate is

   $$\frac{q^2/2 + O(q)}{q^2} \to \frac{1}{2}.$$

   (b) Consider the following theorem:

Theorem 1. *Let $q = 2^t$ for some t. The the number of $f(X,Y) \in \mathbb{F}_q[X,Y]$ so that $\mathcal{P}(q-2)$ holds for $f(X,Y)$ is at least $q^{4^t-3^t-1}$.*

Assuming that theorem is true, explain why this implies the existence of a LCC $\mathcal{C}$ of length $N = q^2$ and rate that tends to 1 as $N \to \infty$, with parameters $\delta = \frac{1}{100\sqrt{N}}$, $Q = \sqrt{N}$, and $\gamma = 0.1$.

Note: In case it is helpful, $\log_3(4) \approx 1.26$.

Solution

We'll use the code $\mathcal{C}$ from exercise 0(b) above, where $\mathcal{F}$ is the set of polynomials so that $\mathcal{P}(q-2)$ holds. The rate of this code is

$$\frac{4^t - 3^t}{q^2} = \frac{q^2 - q^{\log_3(4)} - 1}{q^2} = 1 - \frac{1}{q^{2-\log_3(4)}} - q^{-2},$$

which approaches 1 as $q \to \infty$.

To see that this has the desired locality properties, we'll use the same argument we saw for RM codes. Suppose that the codeword is given by some $f \in \mathbb{F}_q[X,Y]$, and we want $f(b,d)$ for some $b, d \in \mathbb{F}$.

Choose a random line $\ell(T) = (aT + b, cT + d)$ through the point (b,d) that we are trying to correct (so $a, c \in \mathbb{F}_q^*$ are random). If there are a $\delta = 1/(100\sqrt{N}) = 1/(100q)$ fraction of errors total, than the expected number of errors on that line is $1/100$. By Markov's inequality, with probability at least $1/100$ we avoid any errors altogether, and query $q-1$ uncorrupted points of the univariate polynomial $f(\ell(T))$. Since this has degree at most $q-2$, we can recover it uniquely, and in particular we can learn

$$f(\ell(0)) = f(b,d),$$

which is what we wanted.

3. In this part, we will (mostly) prove Theorem 1.

   Say that a monomial $M_{ij}(X,Y) := X^iY^j$ is *good* if $\mathcal{P}(q-2)$ holds for $M_{ij}(X,Y)$.

   (a) Explain why, to prove Theorem 1, it is enough to show that the number of good monomials is at least $4^t - 3^t - 1$.

   Solution

   If there are M good monomials, then there are q^M polynomials we can make by taking linear combinations of them. Since Property $\mathcal{P}(q-2)$ is preserved under linear combinations, this would prove the theorem.

   (b) Let $\ell(T) = (T, aT + b)$. (We are going to restrict ourselves to lines that look like this for simplicity; the general case is basically the same). Suppose that $(i,j) \neq (q-1, q-1)$. Consider the univariate polynomial

   $$P_{ij}(T) = M_{ij}(\ell(T)).$$

Show that the coefficient on T^{q-1} in $P_{ij}(T)$ is

$$\begin{cases} \binom{j}{q-i-1} a^{q-i-1} b^{j-(q-i-1)} & j \geq q-i-1 \\ 0 & j < q-i-1 \end{cases}$$

where when we refer to an integer like $\binom{j}{q-i-1}$ as a element of $\mathbb{F}_{2^t}$, we mean $1+1+\ldots+1$ that many times.

Conclude that if $\binom{j}{q-i-1} \equiv 0 \mod 2$, then $M_{ij}(X,Y)$ is good.[1] (For the "conclude" part, you can use the fact that $1+1=0$ in $\mathbb{F}_{2^t}$; you can also use the convention that $\binom{a}{b} = 0$ if $b > a$).

Solution

We write out

$$\begin{aligned} M_{ij}(\ell(T)) &= T^i (aT+b)^j \\ &= T_i \sum_{\ell \leq j} \binom{j}{\ell} a^\ell b^{j-\ell} T^\ell \\ &= \sum_{\ell \leq j} \binom{j}{\ell} a^\ell b^{j-\ell} T^{\ell+i}. \end{aligned}$$

The only way that T^{q-1} shows up is if $\ell = q-1-i$. (For those of you rightly worried about it, notice that we'll never get T^{2q-2} since $i, j \leq q-1$, and at least one is $< q-1$. The reason to be worried about this is that $T^q \equiv T$, so $T^{2q-2} \equiv T^{q-1}$ in $\mathbb{F}_q[T]$.)

Thus, we plug in $\ell = q-1-i$ and we get

$$\binom{j}{q-1-i} a^{(q-1-i)} b^{j-(q-1-i)},$$

as desired.

Thus, if $\binom{j}{q-i-1} \equiv 0 \mod 2$, then this term vanishes in $\mathbb{F}_{2^t}$, since $1+1=0$.

(c) To finish the proof, we will use the following corollary of Lucas' theorem (which we will not prove):

Fact 2. *For an integer $m < 2^t$, let $b(m) \in \{0,1\}^t$ denote the binary expansion of m. For example if $t=3$, we have $b(5) = 101$. For a vector $v \in \{0,1\}^t$, write $\overline{v} \in \{0,1\}^t$ to denote the coordinate-wise flip of v. For example, $\overline{b(5)} = 010$.*

For two vectors $v, w \in \{0,1\}^t$, we say that v "lies in the 2-shadow of w" if $v_i = 1$ implies that $w_i = 1$. For example, $v = 100$ lies in the 2-shadow of $w = 101$, since whenever v has a 1, w also has a 1. However, $v = 110$ does not lie in the 2-shadow of $w = 101$, since $v_2 = 1$ but $w_2 = 0$.

[1] Here, you can ignore the fact that we didn't consider general lines of the form $(aT+b, cT+d)$, only lines like $(T, aT+b)$. The argument for the more general case is exactly the same, just slightly more tedious. Notice that by restricting to these simpler lines, we are only leaving out the "horizontal" lines of the form $(c, aT+b)$ for some constant c.

*With this notation, the **fact** is that, for $q = 2^t$,*

$$\binom{j}{q-i-1} \neq 0 \Leftrightarrow \overline{b(i)} \leq_2 b(j).$$

This fact may seem weird, but it is true! Convince yourself of this by example by applying it to with $j = 5$ and $i = 3$, and for $j = 5$ and $i = 4$ (and with $t = 3$ for both).

Solution

For $j = 5, i = 3$, we have

$$\binom{j}{q-1-i} = \binom{5}{4} = 5 \equiv 1 \mod 2.$$

We see that $b(5) = 101$, and $\overline{b(3)} = \overline{011} = 100$. This check out, since $100 \leq_2 101$.
For $j = 5, i = 4$, we have

$$\binom{j}{q-1-i} = \binom{5}{3} = 10 \equiv 0 \mod 2.$$

We see that $b(5) = 101$ and $\overline{b(4)} = \overline{100} = 011$. This checks out, since 011 is *not* in the 2-shadow of 101, and indeed the binomial coefficient vanishes mod 2.

(d) Show that the number of good monomials is at least $4^t - 3^t - 1$, proving the theorem.
Hint: You want to show that the number of pairs (i, j) so that $\overline{b(i)} \leq_2 b(j)$ is at most 3^t (why?). Imagine constructing a pair (i, j) with this property coordinate by coordinate. How many possibilities are there for $(\overline{b(i)}[k], b(j)[k])$ for each coordinate $k = 0, \ldots, t-1$?
Hint: If you do it in a different way than the hint above is hinting at, it might be helpful that $\sum_{s=0}^{t} \binom{t}{s} 2^s = 3^t$.

Solution

By the above, we just need to count the number of pairs (i, j) so that $\overline{(b(i))} \leq_2 b(j)$; this will bound the number of *bad* monomials. (Otherwise, the binomial coefficient will vanish and M_{ij} will be good).
If we consider writing out $b(j)$ and $\overline{b(i)}$ stacked on top of each other, there are at most three possible pairs of bits that can show up in each place: $\binom{0}{0}$, $\binom{1}{0}$, and $\binom{1}{1}$. (If the last option, $\binom{0}{1}$, shows up, that means that $\overline{b(i)}$ does not lie in the 2-shadow of $b(j)$).
Since there are 3 options for each of t places, the total number of pairs $(b(j), \overline{b(i)})$ that are bad is at most 3^t. Since there's a one-to-one mapping from $j \to b(j)$ and from $i \to \overline{b(i)}$, this means there are at most 3^t bad (i, j). We started with $q^2 - 1 = 4^t - 1$ possible monomials (remembering that we are excluding $X^{q-1}Y^{q-1}$), so that's a total of at least $4^t - 3^t - 1$ good monomials, as desired.

4. **(Bonus)** Try to use the same ideas for $r < q - 2$ and $m > 2$ to come up with an LCC with rate close to 1 and parameters $\delta = 0.01, Q = N^{0.01}, \gamma = 0.01$.

Solution

Check out https://arxiv.org/abs/1208.5413