University of California, Berkeley Instructor: Venkatesan Guruswami
CS 294-226: Advances in Error-Correcting Codes Term: Fall 2022

PROBLEM SET 4
Due by 11.59pm PST Wednesday, November 30

INSTRUCTIONS

- You are allowed to collaborate with up to two students taking the class in solving problem sets. But here are some rules concerning such collaboration:

  1. You should think about each problem by yourself for at least 30 minutes before commencing any collaboration.
  2. Collaboration is defined as discussion of the lecture material and solution approaches to the problems. Please note that *you are not allowed to share any written material and you must write up solutions on your own*. You must clearly acknowledge your collaborator(s) in the write-up of your solutions.
  3. Of course, if you prefer, you can also work alone.

- Solutions typeset in LaTeX are encouraged, but not required. If you are submitting handwritten solutions, please write clearly and legibly (you might want to first write the solution sketch in rough, before transferring it to the version you turn in which should be a "finished product").
- Solutions should be turned in via gradescope.
- You may consult any of the class notes or videos that were assigned for initial preparation, and the "Essential Coding Theory" text linked from the course page. But please refrain from searching for solutions on the web. Do not hesitate to contact the instructor should you have any questions.
- Please start work on the problem set early. The problems vary in difficulty and length and it will be a good idea to give yourself enough time for the longer / trickier problems.

---

1. Let $\mathbb{F}_q$ be a finite field and let $\Sigma = \mathbb{F}_q^m$ for some positive integer m. Suppose that we have a code $C \subseteq \Sigma^N$ that is $\mathbb{F}_q$-linear, i.e., closed under $\mathbb{F}_q$-linear combinations. (Note that folded Reed-Solomon codes are an example of such codes.) Suppose that the relative distance of C is δ and for any $w \in \Sigma^N$, all codewords of C within Hamming distance (over the alphabet Σ) $(\delta - \epsilon)N$ from w are contained in a $\mathbb{F}_q$-subspace $V_w \subset C$ of dimension at most s, for some positive integer s.

   This implies that C is $(\delta - \epsilon, q^s)$-list-decodable. In this exercise, you will prove that C is in fact $(1 - \delta - \epsilon, L)$-list-decodable for

   $$L := \left(\frac{1}{1-\delta}\right)^{O\left(\frac{s(1-\delta)}{\epsilon}\log(\frac{s}{\epsilon})\right)}, \tag{1}$$

   so that when s is a constant, we get a list-size bound that is a constant independent of N, q.

   In fact, you will show the bound (1) algorithmically, by giving a randomized algorithm that, given as input w and a $\mathbb{F}_q$-basis for V_w, outputs a list of size at most L that will, with probability at least $1/2$, include *all* codewords of C within Hamming distance $(1 - \delta - \epsilon)N$ of w.

   The algorithm is very simple, and repeats the following procedure $O(L \log L)$ times to compute a list $\mathcal{L}$, for a parameter r to be worked out:

- Pick indices $i_1, i_2, \ldots, i_r \in [N]$ independently at random.
- If there is a unique $v \in V_w$ such $v_{i_j} = w_{i_j}$ for $j = 1, 2, \ldots, r$, and v is within Hamming distance $(\delta - \epsilon)N$ from w, then include v in $\mathcal{L}$.

For a specific run of the algorithm, let $H = \{v \in V_w \mid v_{i_j} = w_{i_j} \text{ for } j = 1, 2, \ldots, r\}$.

(a) Note that H is an affine $\mathbb{F}_q$-subspace of V_w. Prove that the probability that $\dim(H) > 0$ is at most

$$\binom{r}{r-s+1}(1-\delta)^{r-s+1} .$$

Hint: Consider the linear subspace $H' = \{v \in V_w \mid v_{i_j} = 0 \text{ for } j = 1, 2, \ldots, r\}$. Imagine adding the constraints $v_{i_j} = 0$ one by one to go from V_w to H'. What's the chance that a nonzero vector survives the upcoming constraint? In order for $\dim(H') > 0$, for at least $s - 1$ of the r steps, all current vectors must survive the constraint.

(b) Suppose $c \in V_w$ is within Hamming distance $(\delta - \epsilon)N$ from w. Argue that $H = \{c\}$ with probability at least

$$(1 - \delta + \epsilon)^r - (1 - \delta)^r \left(\frac{r}{1-\delta}\right)^s . \tag{2}$$

Hint: $H = \{c\}$ means $c \in H$ and $\dim(H) = 0$.

(c) For a suitable choice of $r = \Theta\left(\frac{s(1-\delta)}{\epsilon} \log(\frac{s}{\epsilon})\right)$ prove that the quantity (2) is lower bounded by $\Omega(1/L)$ for L defined in (1).

(d) Deduce the claimed list-decoding guarantee of the above algorithm.

(e) What does the list-size bound (1) translate to for the rate R folded RS codes list-decodable up to radius $1 - R - \epsilon$ from lecture?

2. In lecture, we discussed the Reed-Muller code RM$[q, m, r]$ that maps m-variate polynomials over $\mathbb{F}_q$ of total degree at most $r < q$ to its evaluations on $\mathbb{F}_q^m$. This gave an $[n, k, \geq d]_q$ code with $n = q^m$, $k = \binom{m+r}{m}$ and $d = n(1 - r/q)$.

In this problem let us focus on the case $m = 2$, i.e., bivariate polynomials.

(a) Taking $r = q(1 - \epsilon)$ for $\epsilon \to 0$, argue that RM$[q, m, r]$ can have rate approaching $1/2$.

(b) Give a q-query local correction algorithm for RM$[q, 2, r]$ that given oracle access to a string y that differs from the encoding of a degree r polynomial $f \in \mathbb{F}_q[X, Y]$ on at most $d/100$ locations, on input $a \in \mathbb{F}_q^2$, outputs $f(a)$ with probability at least $2/3$.

(c) Now modify the code RM$[q, 2, r]$ as follows: a polynomial $f \in \mathbb{F}_q[X, Y]$ of total degree at most r is encoded as $\langle f(a), \frac{\partial f}{\partial X}(a), \frac{\partial f}{\partial Y}(a)\rangle_{a \in \mathbb{F}_q^2}$. Thus we get a code of length $n = q^2$ over an alphabet of size q^3.

Prove that (i) distance of this code is at least $n(1 - r/(2q))$, and (ii) by taking $r = 2q(1 - \epsilon)$, the code can have rate approaching $2/3$.

(d) **[Not for turning in.]** One can give an $O(\sqrt{n})$-query local correction algorithm for this code as well. Can you describe how such an algorithm and its analysis might go?

3. Let p be a prime and let $1 \leq k < p$. For prime fields $\mathbb{F}_p$ and m a natural number dividing $(p - 1)$, we can also define m-folded Reed-Solomon codes based on *additive* folding, namely the map C :

$\mathbb{F}_p[X]_{<k} \to (\mathbb{F}_p^m)^N$ defined by

$$C : f(X) \mapsto \left(\begin{bmatrix} f(1) \\ f(2) \\ \vdots \\ f(m) \end{bmatrix}, \begin{bmatrix} f(m+1) \\ f(m+2) \\ \vdots \\ f(2m) \end{bmatrix}, \ldots, \begin{bmatrix} f(p-m) \\ f(p-m+1) \\ \vdots \\ f(p-1) \end{bmatrix} \right).$$

where $N \coloneqq (p-1)/m$. Our goal in this problem is to list-decode additive folded Reed-Solomon codes (additive FRS) up to capacity.

(a) Consider the map on polynomials $L : \mathbb{F}_p[X] \to \mathbb{F}_p[X]$ defined as $L(f)(X) \coloneqq X(f(X+1) - f(X))$. For any positive integer $a \leq p - m$, prove that there exists an invertible linear map $M_a : \mathbb{F}_p^m \to \mathbb{F}_p^m$ satisfying

$$M_a : \begin{bmatrix} f(a) \\ f(a+1) \\ \vdots \\ f(a+m-1) \end{bmatrix} \mapsto \begin{bmatrix} L^0(f)(a) \\ L^1(f)(a) \\ \vdots \\ L^{m-1}(f)(a) \end{bmatrix}$$

For any polynomial $f \in \mathbb{F}_p[X]$. Here, L^ℓ denotes L composed ℓ times with itself.

(b) For $i \in [N]$, define $a_i \coloneqq 1 + m(i-1)$. Consider the map $\mathcal{M} : (\mathbb{F}_p^m)^N \to (\mathbb{F}_p^m)^N$ defined as

$$\mathcal{M} : y = (y_1, \ldots, y_N) \mapsto (M_{a_1} y_1, M_{a_2} y_2, \ldots, M_{a_N} y_N)$$

Show that $\Delta(y, y') = \Delta(\mathcal{M}(y), \mathcal{M}(y'))$ for all $y, y' \in (\mathbb{F}_p^m)^N$.

(c) Consider the code $C' : \mathbb{F}_p[X]_{<k} \to (\mathbb{F}_p^m)^N$

$$C' : f(X) \mapsto \left(\begin{bmatrix} L^0(f)(1) \\ L^1(f)(1) \\ \vdots \\ L^{m-1}(f)(1) \end{bmatrix}, \begin{bmatrix} L^0(f)(m+1) \\ L^1(f)(m+1) \\ \vdots \\ L^{m-1}(f)(m+1) \end{bmatrix}, \ldots, \begin{bmatrix} L^0(f)(p-m) \\ L^1(f)(p-m) \\ \vdots \\ L^{m-1}(f)(p-m) \end{bmatrix} \right).$$

Show that $C' = \mathcal{M} \circ C$. Thus the codes C and C' are equivalent under a collection of invertible linear maps.

(d) Fix some natural number $1 \leq s < m$. For any polynomial $f \in \mathbb{F}_p[X]$, consider the vector $\mathcal{L}(f(X)) \in \mathbb{F}_p[X]^{m-s+1}$ defined as

$$\mathcal{L}(f(X)) \coloneqq \begin{bmatrix} L^0(f)(X) \\ L^1(f)(X) \\ \vdots \\ L^{m-s}(f)(X) \end{bmatrix}.$$

Show that there exists a matrix $T(X) \in \mathbb{F}_p[X]^{(m-s+1)\times(m-s+1)}$ such that $\mathcal{L}(Xf(X)) = T(X)\mathcal{L}(f(X))$.

(e) Consider some natural number D that we will choose later. Consider any received codeword $y \in (\mathbb{F}_p^m)^N$, and define $w \coloneqq \mathcal{M}(y)$. Let $w_{i,j}$ denote the j'th symbol in the i'th coordinate of w. Consider a polynomial $Q \in \mathbb{F}_p[X, Y_1, \ldots, Y_s]$ of the form

$$Q(X, Y_1, \ldots, Y_s) = A_1(X)Y_1 + \ldots + A_s(X)Y_s \tag{3}$$

where $\deg(A_\ell) \leq D$ for $\ell \leq s$. Prove that for $D = \lfloor \frac{N(m-s+1)}{s} \rfloor$, there exists a nonzero polynomial Q of the form in Equation 3 satisfying

$$\sum_{j=1}^{s} A_\ell(T)(a_i) \begin{bmatrix} w_{i,j} \\ w_{i,j+1} \\ \vdots \\ w_{i,j+m-s} \end{bmatrix} = 0$$

for all $i \in [N]$. Here, $A_\ell(T)(a_i) \in \mathbb{F}_p^{(m-s+1)\times(m-s+1)}$ denotes the matrix obtained by considering the matrix $A_\ell(T)(X) \in \mathbb{F}_p[X]^{(m-s+1)\times(m-s+1)}$, which is obtained by applying the polynomial A_ℓ on $T(X)$, and then evaluating it at $X = a_i$.

(f) Given any polynomial $f \in \mathbb{F}_p[X]_{<k}$ such that $C(f)$ and y agree on at least $\left(\frac{1}{s} + \frac{k}{N(m-s+1)}\right) N +$ 1 coordinates, show that the polynomial $R(X) := Q(X, L^0(f)(X), L^1(f)(X), \ldots, L^{s-1}(f)(X))$ is identically zero. (Hint: How does the map L change the degree of f? Thus what can the degree of R at most be? Now, what can you say about the weight of the 'codeword' $\mathcal{L}(R)(X)$ when evaluated on $X = a_1, \ldots, a_N$?)

(g) Show that the collection of polynomials $f \in \mathbb{F}_p[X]_{<k}$ satisfying the identity

$$A_1(X)L^0(f)(X) + A_2(X)L^1(f)(X) + \ldots + A_s(X)L^{s-1}(f)(X) \equiv 0 \tag{4}$$

form a vector space of dimension at most $s-1$. (Hint: What can you say about the coefficients of the k highest-degree monomials in Equation 4?)

(h) For any $\epsilon > 0$, show that by picking s and m appropriately, the code C is efficiently list-decodable up to a fraction of $1 - R - \epsilon$ errors. (i.e. is list-decodable up to capacity).

4. In this problem, we are going to show the existence of 3-query linear LDCs assuming the existence of infinitely many *Mersenne primes*. That is, in this problem, we will assume the existence of infinitely many natural numbers $t \in \mathbb{N}$ such that $2^t - 1$ is a prime number.

(a) Given a prime number p and natural number $M > p-1$, construct a collection of vectors $U = \{u_1, \ldots, u_n\} \subseteq \mathbb{F}_p^M$ and $V = \{v_1, \ldots, v_n\} \subseteq \mathbb{F}_p^M$ with $n = \binom{M}{p-1}$ such that $\langle u_i, v_j \rangle = 0$ if and only if $i = j$.

(b) Given p and M as in the previous part, consider a natural number t dividing $p-1$. Set $m := M^{\frac{p-1}{t}}$. Use the previous two parts to construct a collection of vectors $U = \{u_1, \ldots, u_n\} \subseteq \mathbb{F}_p^m$ and $V = \{v_1, \ldots, v_n\} \subseteq \mathbb{F}_p^m$ of the same size such that (1) $\langle u_i, v_j \rangle = 0$ if $i = j$ and (2) $\langle u_i, v_j \rangle^t = 1$ if $i \neq j$. (Hint: How are $\langle u^{\otimes \ell}, v^{\otimes \ell} \rangle$ and $\langle u, v \rangle$ related? Here, $u^{\otimes \ell}$ denotes the tensor product of u with itself ℓ times. Put another way, it's the vector whose entries are $\prod_{j=1}^{\ell} u_{i_j}$ for all possible tuples $(i_1, \ldots, i_\ell)$.)

(c) (Not to turn in) Show that if $2^t - 1$ is a prime number, then t must be a prime number. Give an example of when the converse is false.

(d) Throughout the rest of this problem, fix a number $t \in \mathbb{N}$ such that $p := 2^t - 1$ is a prime number and a primitive element $g \in \mathbb{F}_{2^t}^*$. Construct a polynomial $r(x) \in \mathbb{F}_{2^t}[x]$ of the form $r(x) = 1 + x^a + x^b$ for $a, b \in \mathbb{Z}/p\mathbb{Z}$ such that $r(1) \neq 0$ and $r(g^i) = 0$ for all $i \in \mathbb{Z}/p\mathbb{Z}$ satisfying $i^t \equiv 1 \pmod{p}$.

(e) For any vector $u \in (\mathbb{Z}/p\mathbb{Z})^m$, consider the function $f_u : (\mathbb{Z}/p\mathbb{Z})^m \to \mathbb{F}_{2^t}$ defined as $f_u(x) = g^{\langle u, x \rangle}$. Prove that the collection of functions $\{f_u\}_{u \in (\mathbb{Z}/p\mathbb{Z})^m}$ forms a basis of the space of functions $\{f : (\mathbb{Z}/p\mathbb{Z})^m \to \mathbb{F}_{2^t}\}$.

(f) Consider the collection of vectors $U, V \subseteq (\mathbb{Z}/p\mathbb{Z})^m$ with $|U| = |V| = n$ as in part (b). Consider the code $C : \mathbb{F}_2^n \to \mathbb{F}_{2^t}^{p^m}$ defined as $C(a_1, \ldots, a_n)_x = \sum_{i=1}^n a_i g^{\langle v_i, x\rangle}$ for $x \in (\mathbb{Z}/p\mathbb{Z})^m$. By considering the collection of queries $\{z, z + au_i, z + bu_i\}$ for $z \in (\mathbb{Z}/p\mathbb{Z})^m$, prove that C is a 3-query linear LDC with $n = \dim(C)$.

(g) Given a natural number $t \in \mathbb{N}$ such that $2^t - 1$ is a prime number, show that the construction in the previous part gives an infinite family of 3-query linear LDCs that map n-bit messages to codewords over $\mathbb{F}_{2^t}$ of blocklength at most $\exp(O(n^{1/t}))$.

(h) Assuming the existence of infinitely many natural numbers $t \in \mathbb{N}$ such that $2^t - 1$ is a prime number, show that the construction in the previous part gives an infinite family of 3-query linear LDCs that map n-bit messages to codewords over $\mathbb{F}_{2^t}$ of blocklength at most $\exp(n^{O(1/\log\log n)})$.

(i) (Optional, Extra Credit) How would you turn the 3-query linear LDC over $\mathbb{F}_{2^t}$ from the previous part into a 3-query binary linear LDC?

5. Enough algebraic problems—let us do something different which will take us back to a code we saw in the very first lecture.

   For the noise model where one bit of the codeword gets erased (and we know which location got erased), the parity check code gives a simple solution to recover the missing bit, with just one bit redundancy. Now, consider the harsher model where one bit gets *deleted* and we *don't* know the position of the missing bit. (So a codeword such as 111010 could be received as 11110.)

   (a) Suppose $C \subseteq \{0,1\}^n$ is a binary code capable of recovering from deletion of one bit. Prove that $|C| \leq O(2^n/n)$. Thus about $\log n$ bits of redundancy are needed in such a code.

   (b) For integers n, ℓ, $0 \leq \ell \leq n$, consider the code

   $$C_\ell = \{(x_1, x_2, \ldots, x_n) \in \{0,1\}^n \mid x_1 + 2x_2 + 3x_3 + \cdots + nx_n \equiv \ell \pmod{(n+1)}\},$$

   where the sum above is over integers.

   Prove that each C_ℓ is capable of correctly recovering a deleted bit in its codewords. That is, if $x \in C_\ell$ and $y \in \{0,1\}^{n-1}$ is obtained by deleting any bit of x, then x is unique codeword of C_ℓ that has y as a subsequence.

   Deduce the existence of a code of size $\geq 2^n/(n+1)$ that can correct a single deletion.

6. **[Back to algebra, but no need to turn in this problem — including it since many of you asked about AG codes]** We have mentioned objects called algebraic-geometric codes, that generalize Reed-Solomon codes and have some amazing properties, a few times in the course. The objective of this exercise is to construct one such AG code, and establish its rate vs distance trade-off.

   Let p be a prime and $q = p^2$. Consider the equation

   $$Y^p + Y = X^{p+1} \tag{5}$$

   over $\mathbb{F}_q$.

   (a) Prove that there are exactly p^3 solutions in $\mathbb{F}_q \times \mathbb{F}_q$ to (5). That is, if $S \subseteq \mathbb{F}_q^2$ is defined as

   $$S = \{(\alpha, \beta) \in \mathbb{F}_q^2 \mid \beta^p + \beta = \alpha^{p+1}\} \tag{6}$$

   then $|S| = p^3$.

(b) Prove that the polynomial $f(X,Y) = Y^p + Y - X^{p+1}$ is irreducible over $\mathbb{F}_q$.
(**Suggestion**: One approach is to use the Eisenstein criterion (feel free to look this up), considering $f(X,Y)$ as a polynomial in X with coefficients from $\mathbb{F}_q[Y]$.)

(c) Let $n = p^3$. Consider the evaluation map $\mathrm{ev} : \mathbb{F}_q[X,Y] \to \mathbb{F}_q^n$ defined by

$$\mathrm{ev}(f) = (f(\alpha,\beta) : (\alpha,\beta) \in S)$$

where S is the set defined in (6).

Argue that if $f \neq 0$ and is not divisible by $Y^p + Y - X^{p+1}$, then $\mathrm{ev}(f)$ has Hamming weight at least $n - \deg(f)(p+1)$, where $\deg(f)$ denotes the *total* degree of f.
(**Hint**: You are allowed to use ***Bézout's theorem***, which states that if $f, g \in \mathbb{F}_q[X,Y]$ are nonzero polynomials *with no common factors*, then they have at most $\deg(f)\deg(g)$ common zeroes.)

(d) For an integer parameter $\ell \geq 1$, consider the set $\mathcal{F}_\ell$ of bivariate polynomials

$$\mathcal{F}_\ell = \{f \in \mathbb{F}_q[X,Y] \mid \deg(f) \leq \ell, \deg_X(f) \leq p\}$$

where $\deg_X(f)$ denotes the degree of f in X.

Argue that $\mathcal{F}_\ell$ is an $\mathbb{F}_q$-linear space of dimension $(\ell+1)(p+1) - \frac{p(p+1)}{2}$.

(e) Consider the code $C \subseteq \mathbb{F}_q^n$ for $n = p^3$ defined by

$$C = \{\mathrm{ev}(f) \mid f \in \mathcal{F}_\ell\}\ .$$

Prove that C is a linear code with minimum distance at least $n - \ell(p+1)$.

(f) Deduce a construction of an $[n,k]_q$ code with distance $d \geq n - k + 1 - p(p-1)/2$.
(**Remark:** Reed-Solomon codes have $d = n - k + 1$, whereas these codes are off by $p(p-1)/2$ from the Singleton bound. However they are much longer than RS codes, with a block length of $n = q^{3/2}$, and the deficiency from the Singleton bound is only $o(n)$.)