CMSC818K/ENEE729A. Home assignment 2. **Instructor: A. Barg**

Date due Oct. 22, 2020, 8:00pm.

Please submit your work as a **single PDF file** to ELMS/Canvas under the Assignments tab

- Papers submitted as multiple pictures of individual pages are difficult for grading and **will not be accepted**.
- Justification of solutions is required.
- Each problem is worth 10 points. A subset of problems will be graded.

Problem 1. (In this problem you will learn a new method of proving results that rely on random choice from finite sets)

Below we use the notation V_w for the volume of the ball in the q-ary Hamming space Q^n, $V_w = \sum_{i=0}^{w} \binom{n}{i}(q-1)^i$.

We a constructing a random code of size M. Let d be the target value of the code's distance. Our goal is to estimate M from below as a function of d. The GV bound suggests that there may exist codes of size $M > q^n/V_{d-1}$ (we have proved this for linear codes over fields). Let us show that even if Q is not a field, and so our codes are not linear, it is still possible to prove the GV bound by random choice (up to a constant multiplier).

Call a point in the code *good* if its distance to any other code point is $\ge d$. Call an ordered set of M points in Q^n *good* if all of its points are good.

(a) Estimate from above the number of bad choices for the ith code point if all the other $M-1$ points are fixed.

(b) Estimate from above the number of choices for the remaining $M-1$ points, and derive an upper bound on the number of codes of size M in which the ith point is bad.

(c) Estimate from above the number of bad codes of size M. If this bound is less than the total number of codes of size M, i.e., q^{nM}, there exists a good code. This gives a bound on M in terms of d, but the result is a far cry from GV (you should get for M the inequality $M(M-1)V_{d-1} < q^n$, bad.)

(d) Show that the average number of bad points in the code is $\le M(M-1)V_{d-1}/q^n$ and argue that there is a code, denote it A, with at most than many bad points. Choose M such that the average number of bad points $\le M/2$, and discard them from the code A. The remaining code is good, and its size $M > q^n/4V_{d-1}$. This is where we wanted to be.

Problem 2. (Exercises for finite fields; please justify all answers)

(a) How many zeros does the polynomial x^4+x^3+1 have in $\mathbb{F}_{16}$? The same question about x^4+x^2+x. Please justify your answers without substituting all the elements of $\mathbb{F}_{16}$ into the polynomials.

(b) In the lectures we constructed $\mathbb{F}_{16}$ using the powers $\alpha^0, \alpha^1 \dots, \alpha^{14}$ of a root α of the polynomial x^4+x+1. Now construct the finite field $\mathbb{F}_{16}$ by adding to $\mathbb{F}_2$ a root ξ of the polynomial x^4+x^3+1, and express every nonzero element $\alpha^j, 0 \le j \le 14$ as a power of ξ.

(c) Consider the polynomial $f(x) = x^4+x^3+x^2+x+1$. Is $f(x)$ irreducible over $\mathbb{F}_2$? Is $f(x)$ primitive over $\mathbb{F}_2$? Add to $\mathbb{F}_2$ the roots of $f(x)$ and prove that in this way we obtain the field $\mathbb{F}_{16}$.

Let $\xi \in \mathbb{F}_{16}$ be a root of $f(x)$, i.e., $f(\xi) = 0$. Show that $1+\xi$ is a primitive element in $\mathbb{F}_{16}$ (the easiest is to express $1+\xi$ as some power of α from part (b)).

(d) Prove that $\mathbb{F}_{p^l}$ is a subfield of $\mathbb{F}_{p^m}$ if and only if l divides m. Thus, $\mathbb{F}_4$ is a subfield of $\mathbb{F}_{16}$ and $\mathbb{F}_8$ is not, but both $\mathbb{F}_4$ and $\mathbb{F}_8$ are subfields in $\mathbb{F}_{64}$. Take a primitive polynomial of degree 6 over $\mathbb{F}_2$ (google for the tables, or construct yourself) and let α be its root. Identify the elements of $\mathbb{F}_4$ and $\mathbb{F}_8$ in terms of the powers of α. In particular, you will obtain that $\mathbb{F}_4 = \{0, 1, \alpha^i, \alpha^j\}$ for some i, j. Show that $\alpha^i + \alpha^j \in \mathbb{F}_4$.

Problem 3. (Computers OK, but justification required. In each of (a),(b),(c) explain why your result is correct.)

(a) Is 2 is a primitive element of the field $F := \mathbb{F}_{13}$?

(b) Write out a parity-check matrix of the $[n = 12, k = 8]$ RS code C over F (explain how you obtained it).

(c) Suppose that a codeword $c \in C$ was transmitted over the channel, and the received vector is

$$y = (2, 0, 10, 3, 10, 2, 4, 12, 0, 8, 9, 6).$$

Is y a codeword of the code C? Perform the steps of the Berlekamp-Welch algorithm to recover the transmitted vector c. Once you have found c, explain why this is a correct answer.

You will use some software, I advise GAP (www.gap-system.org). It knows quite a bit about finite fields and codes. Here is a little example:

```
gap> LoadPackage("guava", "2.1");
gap> x:=Indeterminate(GF(13),"x");;
gap> C:=ReedSolomonCode(12,5);
a cyclic [12,8,5]3..4 Reed-Solomon code over GF(13)
gap> GeneratorMat(C);
```

(answer not shown)

At this point GAP knows that C is a Reed-Solomon code and can compute a lot about it.

Problem 4. (Cyclic RS codes)

(a) Let $F = \mathbb{F}_q$ be a finite field with primitive element α. Let $\Omega = (\alpha^i, i = 0, 1, \ldots, q-2)$ be the set of nonzero elements of F. Define an $[n = q-1, k]$ RS code C as a set of evaluations of the polynomials $f(x) \in F[x]$ of degree $\le k-1$. Prove directly that the code is cyclic, i.e., that if $c = (c_0, c_1, \ldots, c_{n-1}) \in C$ is a codeword, then any cyclic shift of c, e.g., $(c_{n-1}, c_0, c_1, \ldots, c_{n-2})$ is also a codeword in C.

(b) (using the notation from part (a)). We will think of the codewords of an $[n = q-1, k]$ code as polynomials of the form

$$c(x) = \sum_{i=0}^{n-1} c_i x^i, \quad \text{where } c_i \in F.$$

Consider the polynomial $g(x) = (x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{d-1})$. Let us form a code

$$D = \{a(x)g(x) \bmod (x^n - 1),\ 0 \le \deg(a(x)) \le k-1\},$$

where $a(x)$ runs over all the polynomials over F with degrees from 0 to $k-1$. What are the dimension and distance of the code D? (If this looks difficult, read Roth's book [R] Sec. 8.1).

(c) Show that all the coefficients of the polynomial $g(x)$ are nonzero (do *not* attempt to multiply out!).

(d) Now let $F = \mathbb{F}_{16}$ and let $d = 13$. What are the parameters $[n, k]$ of the code D constructed as in part (b)? Write out a generator matrix of the code.