CQC class, Home assignment 1. Date due April 1, 2022, 11:59pm EDT.

Instructors: `Victor Albert and Alexander Barg`

Please submit your work as a **single PDF file** to ELMS (under the "Assignments" tab)

- Papers submitted as multiple separate files (pictures of individual pages) are difficult for grading and **will not be accepted**.
- Justification of solutions is required.
- Please note the clickable links in the assignment.

Problem 1 (20pt). The binary Golay code G_{23} has length $n = 23$, dimension 12, and distance 7.

(a) Prove that G_{23} meets the sphere packing bound with equality.

(b) Suppose that we perform the nearest neighbor decoding of G_{23}, i.e., given a vector $y \in \mathbb{F}_2^{23}$, find $c \in G_{23}$ that satisfies $d(c, y) \le d(c', y)$ for all $c' \in G_{23}$. Prove that this codeword c equals $y + x$, where x is the vector of the smallest Hamming weight in the coset of G_{23} in $\mathbb{F}_2^{23}$ that contains y.

(c) Suppose that the code is used on the binary symmetric channel BSC(p) with error probability p. Based on parts (a), (b), give an expression for the probability P_e that the described decoding procedure results in an error. Plot $P_e(p)$ for $p \in [0.05, 0.25]$.

(d) Now perform a computer experiment to check your calculation in (c). Namely, choose a random codeword c in G_{23} and flip each bit independently with probability p. Note whether the obtained vector y is decoded to c or not. Repeat this experiment many times, and plot the probability of decoding error in the same plot as in part (c).

Problem 2 (30pt). Consider a binary linear code C of length $n = 2^m - 1$, where $m \ge 5$ is an integer. Let α be a primitive element of $F = \mathbb{F}_{2^m}$. Let $c = (c_0, c_1, \dots, c_{n-1}) \in C$ be a codeword, which we will also write as a polynomial $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$.

(a) From now on, C is a primitive narrow-sense BCH code of length n. Specifically, we will assume that every codeword $c \in C$ satisfies $c(\alpha^i) = 0, i = 1, 3, 5$. What is the parity-check matrix of the code C, written in terms of the powers of α?

(b) Prove that the distance of C is $d \ge 7$ and the dimension is $n - 3m$.

(c) Take $m = 6$, so the above construction yields a $[63, 45, 7]$ BCH code C. Assume that the primitive element α of $\mathbb{F}_{2^6}$ satisfies the relation $\alpha^6 = \alpha^4 + \alpha^3 + \alpha + 1$. A codeword $c(x)$ of the code C was received with errors, and the received vector has the (polynomial) form

$$Y(x) = x^{62}+x^{60}+x^{57}+x^{56}+x^{54}+x^{53}+x^{51}+x^{49}+x^{47}+x^{45}+x^{43}+x^{36}+x^{35}+x^{34}+x^{32}+x^{29}+x^{12}+x^{5}$$

The Peterson-Gorenstein-Zierler decoder is a procedure that corrects up to 3 errors (up to $(d-1)/2$ errors in general). A description of the procedure is posted on the class page. Please program this procedure and correct the errors in the vector $Y(x)$ to recover $c(x)$. You will need software that can handle finite fields, such as GAP or Sagemath. Please submit the program, with a description of the decoding steps, and the correct codeword $c(x)$ as your answers. (No credit for submitting only $c(x)$.)

Problem 3 (20pt). Given a bipartite regular graph $G(V = L \cup R, E)$ with left and right degrees Δ and $|L| = |R| = n$. Denote by A the $2n \times 2n$ adjacency matrix of G with columns and rows indexed by $v \in V$, and let λ be its second eigenvalue.

Let $S \subset L$ and $T \subset R$ with $s = |S|$ and $t = |T|$. Let $\deg_T(v)$ be the number of edges that connect a vertex $v \in L$ with T and let $\deg_S(v)$ be number of edges that connect a vertex $v \in R$ with S. Define the average degree

$$d_{ST} = \frac{\sum_{v\in S} \deg_T(v) + \sum_{v\in T} \deg_S(v)}{s+t}.$$

(a) Argue that $J := 1^{2n} = (\underbrace{11\dots1}_{2n})$ and $K := (1^n, -1^n)$ are eigenvectors of A.

(b) Let $X = \mathbb{1}_{S\cup T}$ be the indicator function of the set $S \cup T$ in V, viewed as a $2n$-dimensional binary vector. Prove that $X^T AX = (s+t)d_{ST}$.

(c) Define the vector $Y = X - \frac{s+t}{2n}J - \frac{s-t}{2n}K$. Prove that $\langle Y, J\rangle = \langle Y, K\rangle = 0$.

(d) Using (a) and the expression for X in part (c), show that

$$X^T AX = 2\frac{st}{n}\Delta + Y^T AY.$$

(e) Prove that $Y^T AY \le \lambda\|Y\|^2$, where λ is the 2nd eigenvalue of G and $\|Y\|^2 = \langle Y, Y\rangle$. Show that that

$$\|Y\|^2 = s + t - \frac{s^2+t^2}{n}.$$

(f) Combining the results in (b)-(e), deduce the bipartite version of the expander mixing lemma:

$$d_{ST} \le \frac{2st}{s+t}\frac{\Delta}{n} + \lambda - \frac{\lambda}{n}\frac{s^2+t^2}{s+t}.$$

This completes the proof of the lower bound on the distance of expander codes in Lec. 12.

Problem 4. (20pt) Let C and $C^\perp$ be a pair of mutually dual binary linear codes. Let $(A_0, \dots, A_n)$ be the weight distribution of the code C and let $(A_0^\perp, \dots, A_n^\perp)$ be the weight distribution of the code $C^\perp$.

(a) Compute the Fourier expansion of the function $\mathbb{1}_{C^\perp}$.

(b) Compute the Fourier expansion of the function $f(x) = z^{\sum_{i=1}^n x_i}$, where $x \in \{0,1\}^n$ and z is a formal variable.

(c) Use the Parseval identity to prove the *MacWilliams theorem*, i.e., the equality

$$\sum_{i=0}^n A_i z^i = \frac{1}{|C^\perp|}\sum_{i=0}^n A_i^\perp (1-z)^i(1+z)^{n-i}.$$

(d) Use the first lemma in Lec.13 to show that the Krawtchouk polynomials satisfy the following:

$$\sum_{i=0}^n K_i(k)z^i = (1-z)^k(1+z)^{n-k}.$$

(this expression is called the *generating function* of the numbers $K_i(k)$).

(e) Define the average weight of the codewords in C as $\sum_{x\in C}\frac{|x|}{|C|}$. Using the result in Part (c), show that, as long as $d^\perp > 1$, it equals $\frac{n}{2}$.