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).

(a) $2048 = 2^{n-k} = 2^{11} = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} = 1 + 23 + 253 + 1771$

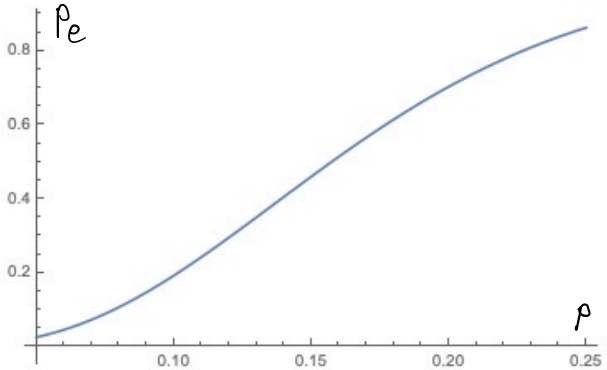
(b) Let z be a vector of the lowest weight in some coset A of G_{23}. For any $y \in A$ we have $d(y, G_{23}) = |z|$.
Indeed, by definition $d(y, G_{23}) \le |z|$ since $y + z \in G_{23}$.
If this inequality is strict then there is a vector $z' \in A$ such that $|z'| < |z|$, contradicting our assumption.
Moreover, none of the vectors z, z' of weight $1 \le w \le 3$ are in the same coset since $z + z' \in G_{23}$, but $|z + z'| \le 6$ while the smallest nonzero weight of the codevectors is 7. Thus, every coset contains exactly one vector from the set $\{x \in \mathbb{F}_2^n, 0 \le |x| \le 3\}$, and there are no other cosets because of (a).

(c) Using (b), the probability of <u>correct</u> decoding is

$$P_c = \sum_{i=0}^{3} \binom{n}{i} p^i (1-p)^{n-i}$$

and $P_e = 1 - P_c$.

[with sufficiently many trials the simulation results fit this curve exactly.]



Note that P_e changes from small to large once the most probable number of errors pn becomes larger than 3, or $p = \frac{3}{23} \approx 0.13\ldots$

Problem 2 (30pt). Consider a binary linear code C of length $n = 2^m - 1$, where $m \geq 5$ is an integer. Let α be a primitive element of $F = \mathbb{F}_{2^m}$. Let $c = (c_0, c_1, \ldots, c_{n-1}) \in C$ 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 $d \geq 7$ 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 $c(x)$.)

(a) $$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \ldots & \alpha^{n-1} \\ 1 & \alpha^3 & \alpha^{2\cdot 3} & \ldots & \alpha^{(n-1)\cdot 3} \\ 1 & \alpha^5 & \alpha^{2\cdot 5} & \ldots & \alpha^{(n-1)\cdot 5} \end{bmatrix}$$

(b) We obtain for free that $c(\alpha^{2i}) = 0$ once $c(\alpha^i) = 0$, so we can add 3 more rows to the matrix H in part (a). Now every 6 columns of this new matrix form a Vandermonde determinant, and thus are linearly independent, so distance $d(C) \geq 7$.

As for the dimension, we note that $\dim C = n - |Z|$, where $Z := \{ i \in \{0, 1, \ldots, n-1\} : c(\alpha^i) = 0 \}$ for every codeword $c \in C$ is the set of zeros of the code C.

This is the case because a codeword can be written as

(Z) $$c(x) = \left[\prod_{z \in Z} (x - z) \right] a(x), \quad a(x) \in \mathbb{F}_2[x], \ \deg a(x) \leq n - 1 - |Z|$$

Thus, $\dim(C) = \#$ of coeff's of $a(x) \} = \dim_{\mathbb{F}_2} \langle g(x) \rangle$, where $\langle g(x) \rangle$ is

the ideal in $\mathbb{F}_2[x]/(x^n-1)$ generated by $g(x)$}. Thus knowing the complete set of zeros is equivalent to knowing the dimension of C.

We observe that

If $c(\alpha^i)=0$ then $c(\alpha^{i\cdot 2^j})=0$, $j=0,1,\dots,m-1$. (1)

It remains to show that the sets

$$\{\alpha,\alpha^2,\dots,\alpha^{2^{m-1}}\},\ \{\alpha^3,\alpha^{2\cdot 3},\dots,\alpha^{2^{m-1}\cdot 3}\},\ \{\alpha^5,\alpha^{2\cdot 5},\dots,\alpha^{2^{m-1}\cdot 5}\} \quad (2)$$

are of size m. If not, then $\alpha^{i\cdot 2^j}=\alpha^i$ for some j, $1\le j\le m-1$

or, writing the exponents in the binary form

$$(0\,0\dots 0***),\quad (***)\in\{001,011,101\}$$

a cyclic shift of this expansion to the left closes earlier than after m shifts. This is clearly not possible, so (1) is true.

Note that if $\alpha^{i\cdot 2^j}=\alpha^i$ for $j<m-1$ (and thus for $j\mid m$), then the check $(\alpha^i,\alpha^{i\cdot 2},\dots,\alpha^{i\cdot 2^{m-1}})$ contributes only m/j linearly independent rows to H.

We also need to show that the sets in (2) are disjoint

Assume the contrary, for instance that

$$\alpha^{2^i}=\alpha^{2^j\cdot 3}\quad \text{for some } i,j\in\{0,\dots,m-1\}$$

If true, this would imply that $\alpha^{2^j\cdot 3-2^i}=1$

meaning that

$$3\cdot 2^j-2^i=\ell\cdot(2^m-1)\quad \text{for } -2\le\ell\le 2$$

Checking $i,j=0,1$, we see that this equality cannot hold.

For $\min(i,j)\ge 2$ the left-hand side is a multiple of 4 and the right-hand side is not, giving a contradiction.

Thus every codeword has $3m$ zeros, or $\deg\left(\prod_{z\in Z}(x-z)\right)=3m$,

$\dim(C) = n - 3m.$

by formula $(\mathcal{Z})$ above.

(c) The errors are in locations 50, 12, and 5.

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 $J := 1^{2n} = (\underbrace{11\ldots1}_{2n})$ 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 $X^T A X = (s+t) d_{ST}$.

(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

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

(e) Prove that $Y^T A Y \le \lambda \|Y\|^2$, 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.

(a) The adjacency matrix of G has the form

$$A = \begin{bmatrix} 0 & B \\ B^T & 0 \end{bmatrix} \quad \begin{matrix} + \\ - \end{matrix}$$

A is $|V| \times |V|$

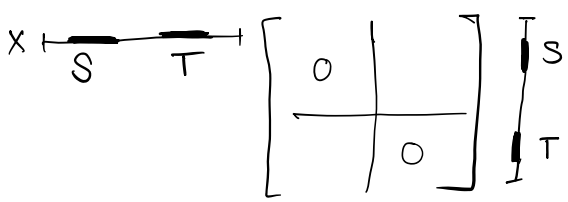
where B describes the connections from the rows in L to the columns in R.

Every row in B contains Δ ones, and thus

$$AJ = \Delta J, \quad \text{where } J = (1, 1, \ldots, 1) \in \mathbb{R}^{2|V|}$$

Similarly, $AK = -\Delta K$.

(b) The claim is obvious from the figure



Because XAX^T counts the number of edges leaving S, headed to T, and the number of edges leaving T, headed to S. This number equals $d_{ST}(s+t)$.

(c) $(Y, J) = (X, J) - \frac{s+t}{2n}(J, J) - \frac{s-t}{2n}(J, K) = (s+t) - (s+t) - 0 = 0.$

$(Y, K) = (X, K) - \frac{s+t}{2n}(J, K) - \frac{s-t}{2n}(K, K) = (s-t) - 0 - (s-t) = 0$

(d) $$X^T A X = X^T A \left(Y + \frac{s+t}{2n} J + \frac{s-t}{2n} K\right) = X^T \left(AY + \frac{s+t}{2n} \Delta J - \frac{s-t}{2n} \Delta K\right)$$

$$= \left(Y^T + \frac{s+t}{2n} J^T + \frac{s-t}{2n} K^T\right)\left(AY + \frac{s+t}{2n} \Delta J - \frac{s-t}{2n} \Delta K\right)$$

$$= Y^T AY + \frac{(s+t)^2}{2n} \Delta - \frac{(s-t)^2}{2n} \Delta = Y^T AY + \frac{2st\Delta}{n}$$

(e) Since $Y \perp J$ and $Y \perp K$,

$$Y^T AY \le Y^T \lambda Y = \lambda \|Y\|^2 \quad \text{(Rayleigh inequality)}$$

$$\|Y\|^2 = (Y,Y) = \left(X - \frac{s+t}{2n} J - \frac{s-t}{2n} K,\ X - \frac{s+t}{2n} J - \frac{s-t}{2n} K\right)$$

$$= (X,X) + \left(\frac{s+t}{2n}\right)^2 \cdot 2n + \left(\frac{s-t}{2n}\right)^2 \cdot 2n - 2\,\frac{s+t}{2n}(X,J) - 2\,\frac{s-t}{2n}(X,K)$$

$$= s+t + \frac{(s+t)^2}{2n} + \frac{(s-t)^2}{2n} - \frac{(s+t)^2}{n} - \frac{(s-t)^2}{n} = s+t - \frac{s^2+t^2}{n}.$$

(f) Collecting the results, we obtain the claimed inequality.

$$(s+t)\, d_{ST} = X^T A X \le \lambda\left(s+t - \frac{s^2+t^2}{n}\right) + \frac{2st\Delta}{n}$$

This claim is known as (the bipartite version of) the expander mixing lemma. See the survey of

S. Hoory, N. Linial, and A. Wigderson
Expander graphs and their applications
(Bulletin of the AMS)

for more information

Problem 4. (20pt) Let C and $C^\perp$ be a pair of mutually dual binary linear codes. Let $(A_0, \ldots, A_n)$ be the weight distribution of the code C and let $(A_0^\perp, \ldots, A_n^\perp)$ 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 $\frac{n}{2}$.

(a) We did this calculation in class, Lec. 13:

$$\hat{\mathbb{1}}_{C^\perp}(y) = \frac{1}{|C|} \mathbb{1}_C(y)$$

(b) We compute

$$\hat{f}(y) = \frac{1}{2^n} \sum_{x \in \mathbb{F}_2^n} (-1)^{\sum x_i y_i} z^{\sum x_i} = \frac{1}{2^n} \sum_{x_1=0}^{1} \sum_{x_2=0}^{1} \cdots \sum_{x_n=0}^{1} \prod_{i=1}^{n} (-1)^{x_i y_i} z^{x_i}$$

$$= \frac{1}{2^n} \prod_{i=1}^{n} \sum_{x=0}^{1} (-1)^{x \cdot y_i} z^x = \frac{1}{2^n} \prod_{i=1}^{n} \left(1 + (-1)^{y_i} z\right) = \frac{1}{2^n} (1+z)^{n-|y|} (1-z)^{|y|}.$$

(c) By Parseval $\langle f, \mathbb{1}_{C^\perp} \rangle = \sum_y \hat{f}(y) \hat{\mathbb{1}}_{C^\perp}(y)$

$$\frac{1}{2^n} \sum_{x \in C^\perp} z^{|x|} = \frac{1}{2^n |C|} \sum_{y \in C} (1+z)^{n-|y|} (1-z)^{|y|}$$

Collecting the terms according to their Hamming weights

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

The claimed equality is obtained by exchanging the roles of C and $C^\perp$.

(d) From the lectures we know that for $w = 0, 1, \ldots, n$

$$A_w^\perp = \frac{1}{|C|} \sum_{i=0}^{n} A_i K_w(i)$$

and thus $\sum_{w=0}^{n} A_w^\perp z^w = \frac{1}{|C|} \sum_{i=0}^{n} A_i \sum_{w=0}^{n} K_w(i) z^w$

Now the claimed equality is obvious from Eq. (1).

(e) We note that $\sum_{x \in C} |x| = \sum_{w=1}^{n} w A_w$. Now the claim

upon applying $\frac{d}{dz}$ to both sides of (1) and substituting $z=1$:

$$\sum_{w\geq 1} w A_w^{\perp} z^{w-1} = \frac{1}{|C|}\sum_{w\geq 0} w\left[(n-w)(1+z)^{n-w-1}(1-z)^{w} - w(1-z)^{w-1}(1+z)^{n-w}\right]$$

$$\Sigma w A_w = \frac{1}{|C|}\left[n\cdot 2^{n-1} - A_1\cdot 2^{n-1}\right]$$

Exchanging the roles of C and $C^{\perp}$:

$$\frac{1}{|C|}\sum_{w\geq 1} w A_w = \frac{2^n}{|C||C^{\perp}|}\left[\frac{n}{2} - \frac{A_1^{\perp}}{2}\right] = \frac{n}{2} - \frac{A_1^{\perp}}{2} = \frac{n}{2} \text{ if } A_1^{\perp} = 0.$$