CMSC818K/ENEE729A. Home assignment 1.

Date due October 1, 2020, 8:00pm Eastern Time.

Instructor: A. Barg

Please submit your work as a **single PDF file** by email to abarg@umd.edu

- 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. Exercise 4.8 in the book by Guruswami, Rudra, and Sudan, link on the class page.

Problem 2. Exercise 6.7 in the book; please use the case $q = 2$ in the statement of the exercise.

Problem 3. This problem discusses a combinatorial approach to the MacWilliams theorem. Below C is a linear $[n, k]$ code with weight distribution $A_i, i = 0, \dots, n$ and $C^{\perp}[n, n-k]$ is its dual code, G is the generator matrix of C and H is its parity-check matrix.

(a) Let $E \subset \{1, 2, \dots, n\}$. Let $C(E)$ be a linear code obtained by taking all codewords of C of the form $c = (c_i, i = 1, \dots, n)$, where $c_i = 0$ for all $i \in E^c$ (zeros outside E). Show that for all $w = 0, 1, \dots, n$

$$\sum_{i=0}^{n} A_i \binom{n-i}{n-w} = \sum_{E:|E|=w} |C(E)|,$$

where on the right we sum the cardinalities of the codes $C(E)$ over all w-subsets of $\{1, \dots, n\}$. Hint: A_i is the number of codewords of weight i, and these codewords therefore contain $n - i$ zeros. This relates these codewords to the codes $C(E)$ where E is a subset of the complement of the support of the codeword.

(b) Let $H(E)$ be the restriction of H to the columns with indices in the set E. Letting $|E| = w$, prove that $\dim(C(E)) = w - \mathrm{rk}(H(E))$, where $\mathrm{rk}(\cdot)$ is the rank of the argument (mod 2).

(c) Prove that $w - \mathrm{rk}(H(E)) = k - \mathrm{rk}(G(E^c))$ for any $E \subset \{1, 2, \dots, n\}$.

(d)* Prove that (a)-(c) imply that

$$\sum_{i=0}^{n-u} A_i^{\perp} \binom{n-i}{u} = 2^{n-k-u} \sum_{i=0}^{u} A_i \binom{n-i}{n-u}.$$

Problem 4. (a) (PARITY-CHECK ENSEMBLE.) Let H be a binary $(n-k) \times n$ matrix whose elements are independent Bernoulli random variables with $\Pr(0) = \Pr(1) = 1/2$. Consider a linear code $\mathcal{D}$ for which H is a parity-check matrix. Let $\mathcal{A}_w$ be a random number of vectors of Hamming weight w in $\mathcal{D}$.

(b1) Prove that for any nonzero vector $x \in \{0, 1\}^n$ the probability $P(Hx^t = 0) = 1/2^{n-k}$.

(b2) Prove that $EA_w = 2^{k-n}\binom{n}{w}, w \ge 1$.

(a) (GENERATOR MATRIX ENSEMBLE.) Let G be a binary $k \times n$ matrix whose elements are independent Bernoulli random variables with $\Pr(0) = \Pr(1) = 1/2$. Consider a linear code $\mathcal{C}$ spanned by the rows of G (its dimension may be k or less). Let $\mathcal{A}_w$ be a random number of vectors of Hamming weight w in $\mathcal{C}$. Prove the following three equalities

$$(1)\ \ EA_0 = 1 + \frac{2^k - 1}{2^n}; \qquad (2)\ \ EA_w = \binom{n}{w} \frac{2^k - 1}{2^n}, \quad w \ge 1$$

$$(3)\ \ EA_w^2 = EA_w + \frac{(2^k-1)(2^k-2)}{2^{2n}} \binom{n}{w}^2.$$