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 \( A_i, i = 0, \ldots, n \) 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 \( E \subset \{1, 2, \ldots, n\} \). Let \( C(E) \) be a linear code obtained by taking all codewords of \( C \) of the form \( c = (c_i, i = 1, \ldots, n) \), where \( c_i = 0 \) for all \( i \in E^c \) (zeros outside \( E \)). Show that for all \( w = 0, 1, \ldots, n \)
\[
\sum_{i=0}^{n} A_i \binom{n-i}{n-w} = \sum_{E: |E| = w} |C(E)|,
\]
where on the right we sum the cardinalities of the codes \( C(E) \) over all \( w \)-subsets of \( \{1, \ldots, n\} \). 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 \( \text{dim}(C(E)) = w - \text{rk}(H(E)) \), where \( \text{rk}(\cdot) \) is the rank of the argument (mod 2).

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

(d)* Prove that (a)-(c) imply that
\[
\sum_{i=0}^{n-u} A_i^+ \binom{n-i}{u} = 2^{n-k-u} \sum_{i=0}^{u} A_i \binom{n-i}{n-u}.
\]

**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 \( D \) for which \( H \) is a parity-check matrix. Let \( A_w \) be a random number of vectors of Hamming weight \( w \) in \( D \).

(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 \( EA_w = 2^{k-n} \binom{n}{w} \), \( w \geq 1 \).

(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 \( C \) spanned by the rows of \( G \) (its dimension may be \( k \) or less). Let \( A_w \) be a random number of vectors of Hamming weight \( w \) in \( C \). Prove the following three equalities
\[
\begin{align*}
(1) \quad EA_0 &= 1 + \frac{2^k - 1}{2^n}; \\
(2) \quad EA_w &= \binom{n}{w} \frac{2^k - 1}{2^n}, \quad w \geq 1 \\
(3) \quad EA_w^2 &= EA_w + \frac{(2^k - 1)(2^k - 2)}{2^{2n}} \binom{n}{w}^2.
\end{align*}
\]