

**CODING THEORY, MATH 567
FINAL (TAKE HOME EXAM)
DUE: THURSDAY, APRIL 24, 5PM**

You are only allowed to work by yourself. You may use the book, a calculator or other literature (include your source in that case). Problems with a \star are bonus problems. All *parts* will have equal weight in the grading (for example 1(a) gives the same number of points and problem 4).

- (1) We study the Hamming code $L = \mathcal{H}_q(r)$. This is an $[n, n - r, 3]$ code over the field \mathbb{F}_q where $n = (q^r - 1)/(q - 1)$. Let us consider first the case $q = 5$ and $r = 2$. So L is a $[6, 4, 3]$ code.
- (a) Write down a 2×6 parity check matrix for $L = \mathcal{H}_5(2)$. Also write down a 4×6 generator matrix for L .
- (b) Show that the weight enumerator $W_{L^\perp}(s)$ for L^\perp is equal to $1 + 24s^5$. (For example, by listing all codewords of L^\perp).
- (c) Use the MacWilliams identity to find the weight enumerator $W_L(s)$ of L .

We go back to the general situation. Let $L = \mathcal{H}_q(r)$ where q and r are arbitrary.

- \star (d) Prove that the weight enumerator $W_{L^\perp}(s)$ of the dual code is equal to

$$1 + (q^r - 1)s^{q^{r-1}}$$

- (e) Use (d) to write down a formula for $W_L(s)$, the weight enumerator of L .
- (2) Suppose that $n \geq 5$ is a positive integer and assume that a perfect binary 2-error correcting code of length n exists.
- (a) How many codewords would such a perfect binary 2-error correcting code of length n have? Prove that $n^2 + n + 2$ must be a power of 2.
- (b) Assume that C is a perfect 2-error correcting code binary code of length $n = 90$. Assume that C contains the zero word. Let

$$W_C(s) = A_0 + A_1s + \cdots + A_{90}s^{90}$$

be the weight enumerator of C . Explain why $A_0 = 1$ and that $A_1 = A_2 = A_3 = A_4 = 0$ and $A_0 + A_1 + \cdots + A_{90} = 2^{78}$.

- (c) Deduce that $A_5 = 11748$ by counting words of weight 3.
 *(d) Finally, deduce a contradiction by counting words of weight 4 and 5. This shows that no 2-error correcting perfect code of length 90 exists.

- (3) (a) Show that

$$A_q(2n, 2d) \geq A_q(n, d) \cdot A_q(n, 2d).$$

(Hint: use the $(u, u + v)$ construction.)

- (b) If $\frac{2}{3}n < k \leq n$, show that

$$A_2(n, k) = 2.$$

(c) Show that if n is divisible by 3, then $A_2(n, \frac{2}{3}n) = 4$.

- (4) Suppose that $1 \leq i_1 < i_2 < \cdots < i_j \leq r$. What is the weight of the codeword in the Reed-Muller code $\mathcal{R}(r, m)$ corresponding to the monomial

$$x_{i_1} x_{i_2} \cdots x_{i_j}?$$

- (5) Suppose that L is a q -ary $[n, k]$ -code with generator matrix G . Let $W_L(s)$ be the weight enumerator of L . Let S be the sum of all the weights of all codewords.

- (a) Express S in terms of the weight enumerator $W_L(s)$ (Hint: think of the derivative $W'_L(s)$).
 (b) If G does not have any zero columns, show that

$$S = n(q - 1)q^{k-1}.$$