MAD 6607: Coding Theory

Edoardo Persichetti | Test 3

Exercise 1 Write at least one of the MacWilliams identities.

Exercise 2 Let $q = 3$ and $n = 8$.

a) Write all the cyclotomic cosets mod n over $\mathbb{F}_q$.

b) Therefore determine the multiplicative order of q mod n.

c) Factor completely[1] the polynomial $x^n - 1$ over $\mathbb{F}_q$, then use one of the irreducible factors just found (of the proper degree) to define $\mathbb{F}_{q^m}$.

d) Using the field arithmetic corresponding to this choice, find the minimal polynomials corresponding to each coset.

e) Finally, find all the primitive idempotents of R_n.

Exercise 3 Let $q = 8 = 2^3$ and $n = 9$. Consider $\mathbb{F}_q$ as defined usually[2] by $x^3 + x + 1$ and primitive element α.

a) Write all the cyclotomic cosets mod n over $\mathbb{F}_q$.

b) Therefore determine the multiplicative order of q mod n.

c) Let m be the order determined in part b), and call β an element of $\mathbb{F}_{q^m}$ of order n. What are the conjugates of β?

d) Verify that $p(x) = x^m + \alpha x + \alpha$ is irreducible over $\mathbb{F}_q$. Consequently, use $p(x)$ to define[3] $\mathbb{F}_{q^m}$ and compute[4] $Tr_{\mathbb{F}_q}(\beta)$.

e) Write a parity-check matrix H for the Hamming code H_m over $\mathbb{F}_{q^m}$.

f) Project H over $\mathbb{F}_q$. What is the dimension of the Hamming code over $\mathbb{F}_q$?

g) Calculate the minimal polynomial of the element β.

h) Finally, determine the generator polynomial of the Hamming code over $\mathbb{F}_q$ and build the associated generator matrix.

Exercise 4 Let $g(x)$ be the generator polynomial of a binary cyclic code of length n.

a) Show that, if $(x + 1) \mid g(x)$, then the code contains only codewords of even weight.

b) On the other hand, prove that, if $x + 1$ is **not** a factor, then it must contain the all-1s codeword $111\ldots1$.

[1] Down to polynomials of degree 1 and 2.

[2] It might be a good idea to write out the index table for faster computations.

[3] You don't need to write out the whole field, the first few elements will be enough for your computations.

[4] Remember that this is an element of $\mathbb{F}_q$!