

Information Theory [MA5103]

Homework 7

1. Suppose we have an (n, k) *cyclic* code C over a field. A linear code C is defined to be a cyclic code if $c = (c_0, c_1, \dots, c_{n-1}) \in C$ implies that its right shift $c^R = (c_{n-1}, c_0, \dots, c_{n-2}) \in C$. Also, for c we define its generating function $c(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1}$ and identify it as the code c .
 - (a) Prove that $p(x)c(x) \bmod x^n - 1$ is a code for any polynomial $p(x)$.
 - (b) Let $g(x)$ be a generating function of the least degree, which is called *generator polynomial*. Prove that if $p(x) \bmod x^n - 1$ is a code then $g(x)$ divides $p(x)$.
 - (c) Prove that $k = n - \deg(g(x))$.
2. Construct $[2^m - 1, 2^m - 1 - m, 3]$ Hamming codes for $m \in \mathbb{N} \setminus \{1\}$ by defining parity check matrices whose entries are in $GF(2)$.
3. We construct cyclic $[2^m - 1, 2^m - 1 - m, 3]$ Hamming codes for $m \in \mathbb{N} \setminus \{1\}$ by using a primitive root $\alpha \in GF(2^m)$; a vector $c = (c_0, c_1, \dots, c_{n-1}) \in GF(2)^n$ is a code if $c_0 + c_1\alpha + \dots + c_{n-1}\alpha^{n-1} = 0$. Here, $n = 2^m - 1$.
 - (a) Prove that this is a cyclic code.
 - (b) Prove that the minimal polynomial of α is a generator of this code.
 - (c) Prove that the minimum distance of this code is 3.
 - (d) What is the “parity check matrix” in this construction?
4. Let C be an (n, k) MDS (linear) code over a field \mathbb{F} . Take any subset of k coordinate positions: $I \subseteq \{0, 1, \dots, n-1\}$ and any set of k elements from \mathbb{F} : $\{\alpha_i : i \in I\}$. Then, there exists a unique codeword c such that $c_i = \alpha_i$ for all $i \in I$. Hint: define proper projections and use linear algebra knowledge.
5. * Let α be an n th primitive root of unity with $n = 2^m - 1$ in $GF(2^m)$. We define an (n, k) *Reed-Solomon code* in such a way that $c = (c_0, c_1, \dots, c_{n-1})$ is a code if $\sum_{i=0}^{n-1} c_i \alpha^{ij} = 0$ for $j = 1, 2, \dots, r$ where $r = n - k$. Prove that these codewords have one-to-one correspondence with polynomials of degree $\leq k - 1$ such that $c_i = \alpha^{-i(r+1)}p(\alpha^{-i})$.

*If we have time.