Midterm Exam of Error-Correcting Codes

Nov. 11, 2021

1. (a) (4%) Determine whether X^7+1 is irreducible over $GF(2)$ or not.
   (b) (4%) Determine whether $X^4+X^3+X^2+X+1$ is irreducible over $GF(2)$ or not.
   (c) (4%) Let α be a primitive element of $GF(64)$ with $1+\alpha+\alpha^6=0$. Determine whether X^2+X+1 is irreducible over $GF(4)$ or not.

2. Consider a primitive element of the finite field $GF(2^6)$ for which $1+\alpha+\alpha^6=0$.
   (a) (4%) Find all the field elements of $GF(2^6)$ of order 9.
   (b) (4%) Express α^{15} in polynomial form.
   (b) (4%) Find the binary minimal polynomial of α^9.

3. Let α a primitive element in $GF(2^{11})$.
   (a) (4%) Show all the conjugates of α over $GF(2)$.
   (b) (4%) Find an element in $GF(2^{11})$ which is a primitive $23rd$ root of unity.
   (c) (4%) Find the BCH bound of the binary cyclic code for which its generator polynomial is the minimal polynomial of α.

4. Consider an (n,k) binary BCH code with error-correcting capability t.
   (a) (4%) Let $n=63$ and $k=18$. Please find its t.
   (b) (4%) Let $n=127$ and $t=9$. Please find its k.

5. (a) (5%) Let $g(X)=(1+X)(1+X+X^4)$ be the generator polynomial of an $(15,10)$ binary cyclic code C. Find a generator matrix of C.
   (b) (5%) Find a parity check matrix of C.
   (c) (5%) Use $g(X)$ to systematically encode the message $u(X)=1+X^3$ into a codeword of C.

6. (8%) State and prove the Singleton bound.

7. (10%) Prove that the Reed-Solomon code defined by $C=\{\bar{a}=A(\alpha^i), i=0,1,...,n-1\}$, where $\deg A(X)<k$, is an (n,k) cyclic code with $n-k$ consecutive roots.

8. (8%) Let $g(X)$ be the generator polynomial of an (n,k) cyclic code C. Suppose C is interleaved to a depth of λ. Prove that the interleaved code C^λ is also cyclic and its generator polynomial is $g(X^\lambda)$.

9. (a) (5%) Describe the procedure of syndrome decoding for an (n,k) binary cyclic code C.
   (b) (5%) Show that for this cyclic code C all the polynomials in the same coset have the same syndrome.

10. (10%) For $i=1,2$, let C_i be a binary (n,k_i,d_i) linear code with generator matrix G_i. Assume $d_2>d_1$, we can construct a binary linear code of length $2n$: $C=(C_1|C_1+C_2)$ $=\{(\overline{u}|\overline{u}+\overline{v}):\overline{u}\in C_1,\overline{v}\in C_2\}$. Prove that the minimum distance of C is $\min\{2d_1,d_2\}$.