NTIN 100 Intro to Info Transmission and Processing summer 2018/2019

4th homework assignment - More on error correcting codes

turn in by May 15, 2019.

Problem 1. Let n be a positive integer. Consider the following code: each message is a matrix M from $GF[2]^{n\times n}$. The codeword of M consists of M together with parities of each row, each column, and the parity of the parities, i.e., a codeword is from $GF[2]^{(n+1)\times(n+1)}$. How many errors can this code correct? How do you correct the errors?

Problem 2. Consider a $(n,k,d)_q$ code.

a) What type of code do we get if we remove a given position from all the codewords.

b) What type of code do we get if we pick a position in the codewords, choose a symbol which appears most often in that position, remove all codewords which have a different symbol in that position, and remove the position from all the remaining codewords.

Problem 3. In this problem we will design CRC codes (*Cyclic Redundancy Check*). Let us pick $n < k$ and a polynomial $q(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ of degree n over $GF[2]$. CRC code of a message $m \in \{0,1\}^k$ is computed as follows: similarly to Reed-Solomon codes, let $p_m(x) = m_{k-1}x^{k-1} + m_{k-2}x^{k-2} + \cdots + m_0$, where $m = m_0 m_1 \cdots m_{k-1}$. The CRC code of message m is the polynomial $r_m(x)$ of degree at most $n-1$, the reminder after dividing $p_m(x)$ by $q(x)$ over $GF[2]$. I.e., $p_m(x) = q(x)\cdot t_m(x) + r_m(x)$. (The division of polynomials over $GF[2]$ works similarly to the division of polynomials over real numbers.) Show the following claims:

a) If $q(x)$ is such that $q(0) = 1$ then for any two messages $m, m' \in \{0,1\}^k$ of Hamming distance $\Delta_{\text{Ham}}(m,m') = 1$, $r_m(x) \neq r_{m'}(x)$. (*Hint:* Use the fact, that every polynomial can be uniquely written as a product of irreducible polynomials. An irreducible polynomial cannot be divided by any other polynomial except for 1 and itself.)

b) If $q(x)$ is such that $q(0) = 1$ then for any two messages $m, m' \in \{0,1\}^k$ which differ in multiple bits that are at most $n-2$ positions far apart, $r_m(x) \neq r_{m'}(x)$.

c) If $q(x)$ has an even number of non-zero coefficients then for any two messages $m, m' \in \{0,1\}^k$ of odd Hamming distance, $r_m(x) \neq r_{m'}(x)$. Show that such $q(x)$ is divisible by $x+1$.

d) There is a polynomial $q(x)$ such that $q(0) = 1$ and $q(x)$ does not divide any of the polynomials $x^i + 1$, where $1 \leq i \leq 2^{\frac{n}{2} - \log n}$. (*Hint:* Use the fact that the number of irreducible polynomials of degree n over $GF[2]$ is at least $\frac{1}{n}\cdot\left(2^n - 2^{(n+2)/2}\right)$.)

e) There is a polynomial $q(x)$ such that for each $k < 2^{\frac{n}{2} - 1 - \log n}$ and any two messages $m, m' \in \{0,1\}^k$ which differ in at most three bits, $r_m(x) \neq r_{m'}(x)$.

f) Use the CRC code to design a usual code which can correct at least one error. What other types of errors can the code detect?