Telecom Paris ACCQ204, Coding Theory
Teacher: Aslan Tchamkerten

ASSIGNMENT 3 - SOLUTIONS

Exercise 1. Suppose we are in $\mathbb{F}_2$. Find

1. $\gcd(x^4 + x^2 + 1, x^2 + 1)$
2. $\gcd(x^6 + x^5 + x^3 + x + 1, x^4 + x^2 + 1)$
3. $\gcd(x^6 + x^5 + x^3 + x + 1, x^4 + x^3 + x + 1)$

Solution. 1. 1
2. $x^4 + x^2 + 1$
3. $x^2 + x + 1$

□

Exercise 2. Show that a Reed-Solomon code with 2 message symbols and n codeword symbols is an n times repetition code.

Solution. If we have a 2 message symbols, encoding polynomials are of degree zero (i.e., are constants) and evaluated n times. □

Exercise 3. Construct an $RS(n = 4, k = 2)$ code. For the construction you may want to consider the irreducible polynomial $X^2 + X + 1$ over $\mathbb{F}_2$ and the evaluation points (to be justified) $\alpha_1 = 0$, $\alpha_2 = 1$, $\alpha_3 = x$, $\alpha_4 = x + 1 = x^2$.

Solution. Since $n = 4$ we need a base field with (at least) 4 elements. So let's choose the base field $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1)$ whose elements are thus

$$\{0, 1, x, x + 1 = x^2\}.$$

Since $k = 2$, the message polynomials are of degree $k - 1 = 1$ and can be written as $f_0 + f_1 x$ with $f_0, f_1 \in \mathbb{F}_4$. Thus the mapping between information symbols and codewords is given by

$$(f_0, f_1) \to (f_0 + f_1\alpha_1, f_0 + f_1\alpha_2, f_0 + f_1\alpha_3, f_0 + f_1\alpha_4).$$

The full mapping is thus

$$\begin{array}{cccccc} 0 & 0 & \to & (0 & 0 & 0 & 0) \\ 0 & 1 & \to & (0 & 1 & x & x+1) \\ 0 & x & \to & (0 & x & x+1 & 1) \\ 0 & x+1 & \to & (0 & x+1 & 1 & x) \\ 1 & 0 & \to & (1 & 1 & 1 & 1) \\ 1 & 1 & \to & (1 & 0 & x+1 & x) \\ 1 & x & \to & (1 & x+1 & x & 0) \\ 1 & x+1 & \to & (1 & x & 0 & x+1) \end{array} \qquad \begin{array}{cccccc} x & 0 & \to & (x & x & x & x) \\ x & 1 & \to & (x & x+1 & 0 & 1) \\ x & x & \to & (x & 0 & 1 & x+1) \\ x & x+1 & \to & (x & 1 & x+1 & 0) \\ x+1 & 0 & \to & (x+1 & x+1 & x+1 & x+1) \\ x+1 & 1 & \to & (x+1 & x & 1 & 0) \\ x+1 & x & \to & (x+1 & 1 & 0 & x) \\ x+1 & x+1 & \to & (x+1 & 0 & x & 1) \end{array}$$

□

Exercise 4. Consider the following mapping from $(\mathbb{F}_q)^k$ to $(\mathbb{F}_q)^{k+1}$. Let $(f_0, f_1, \ldots, f_{k-1})$ be any k-tuple over $\mathbb{F}_q$, and define the polynomial $f(x) = f_0 + f_1 x + \ldots + f_{k-1}x^{k-1}$ of degree less than k. Map $(f_0, f_1, ..., f_{k-1})$ to the $(q+1)$-tuple $(\{f(\alpha_i), \alpha_i \in \mathbb{F}_q\}, f_{k-1})$—i.e., to the RS codeword corresponding to $f(x)$, plus an additional component equal to f_{k-1}.

Show that the $q^k(q+1)$-tuples generated by this mapping as the polynomial $f(z)$ ranges over all q^k polynomials over $\mathbb{F}_q$ of degree $< k$ form a linear $(n = q+1, k, d = n-k+1)$ MDS code over $\mathbb{F}_q$. [Hint:$f(x)$ has degree $< k-1$ if and only if $f_{k-1} = 0$.]

Solution. The code has length $n = q+1$. It is linear because the sum of codewords corresponding to$f(x)$ and $g(x)$ is the codeword corresponding to $f(x) + g(x)$, another polynomial of degree less than k. Its dimension is k because no polynomial other than the zero polynomial maps to the zero $(q+1)$-tuple.

To prove that the minimum weight of any nonzero codeword is $d = n - k + 1$, use the hint and consider the two possible cases for f_{k-1}:

- If $f_{k-1} \neq 0$, then deg$f(x) = k-1$. By the fundamental theorem of algebra, the RS codeword corresponding to $f(x)$ has at most $k-1$ zeroes. Moreover, the f_{k-1} component is nonzero. Thus the number of nonzero components in the code $(q+1)$-tuple is at least $q-(k-1)+1 = n-k+1$.

- If $f_{k-1} = 0$ and $f(x) = 0$, then deg$f(x) \leq k-2$. By the fundamental theorem of algebra, the RS codeword corresponding to $f(x)$ has at most $k-2$ zeroes, so the number of nonzero components in the code $(q+1)$-tuple is at least $q-(k-2) = n-k+1$.

□

Exercise 5. Suppose we want to correct bursts of errors, that is error patterns that affect a certain number of consecutive bits. Suppose we are given an $[n, k]$ RS code over $\mathbb{F}_{2^t}$. Show that this code yields a binary code which can correct any burst of $(\lfloor (n-k) \rfloor / 2 - 1)t$ bits.

Solution. Map each 2^t symbols of $\mathbb{F}_{2^t}$ into t bits. The code can correct up to $(d-1)/2$ symbol errors which translates into an error correction capability of $(\lfloor (d-1)/2 \rfloor - 1)t$ consecutive bits ($\lfloor (d-1)/2 \rfloor t$ if the burst of errors starts at the beginning of a symbol). □

Exercise 6 (Hats and Hamming)**.** A group of n students are led to the examination hall. Each student is uniformly randomly (and independently of others) adorned with a black (0) or a white (1) hat. Each student can see the color of everyone else's hat but cannot see his own hat. The professor asks the students to write a guess of the color of their own hat in a paper and return – the answer can be either *black* or *white* or they can choose to skip the guessing and write *skip*. If at least one of the students guesses a color (not everyone *skips*) and everyone who guesses a color guesses correctly, then all the students pass the exam; otherwise all of them fail. The students are not allowed to communicate once they are given their hats; their guesses or skips must be based solely on the colors of the hats they can see. However, the students can confer beforehand and devise a strategy. How can the students maximize their probability of passing the exam?

i. (Naïve strategy) Can you devise a strategy that succeeds with probability $1/2$?

Solution. One (fixed) student guesses *black* and everyone else *skips*. □

ii. (A better strategy) Consider the following strategy for $n = 3$: if a student sees that the other two students have the same color hat, he guesses the other color. If a student sees that the other two students have different colors, then he *skips*. Calculate the probability of success for this strategy.

Solution. Denoting by (a, b, c) with $a, b, c \in \{0, 1\}$, the configuration of colors of the hats of the 3 students, the proposed strategy fails if the configuration is either $(0, 0, 0)$ or $(1, 1, 1)$. Therefore, the probability of success is $3/4$. □

iii. (Generalization) Consider the following generalization of the above strategy for $n = 2^r - 1$ students. Construct the $[2^r - 1, 2^r - r - 1]_2$ Hamming code with parity check matrix H. The ith student "receives" a binary vector y of length n with the symbol corresponding to ith position erased. He constructs two copies of y, namely v_0 and v_1 and sets the ith position to 0 and 1, respectively.

(a) If $Hv_0^T \neq 0$ and $Hv_1^T \neq 0$, then he *skips*.

(b) If $Hv_0^T \neq 0$ and $Hv_1^T = 0$, then he writes 0.

(c) If $Hv_0^T = 0$ and $Hv_1^T \neq 0$, then he writes 1.

a. Show that the fourth case, namely, $Hv_0^T = 0$ and $Hv_1^T = 0$ never occurs.

Solution. This case occurs if both v_0 and v_1 are codewords, which is not possible since $d_H(v_0, v_1) = 1$ by construction and the minimum distance of the code is 3. □

b. Explain how this strategy ensures that at least one of the students guesses a color (not everyone *skips*).
Hint – The Hamming code is a perfect code.

Solution. The Hamming code is a perfect code, namely, the union of Hamming balls of radius 1 centered at codewords is $\{0, 1\}^n$. Hence, every vector of length n is at a Hamming distance less than or equal to 1 to at least one of the codewords. So there is at least one student whose v_0 or v_1 is a codeword (and hence he does not *skip*). □

c. The strategy fails if the configuration v satisfies $Hv^T = 0$; succeeds otherwise. Calculate the probability of failure.

Solution. The strategy fails if the configuration v satisfies $Hv^T = 0$. This occurs if v is one of the codewords, the probability of which is equal to

$$\frac{2^k}{2^n} = \frac{1}{2^r} = \frac{1}{n+1}.$$

□

d. Consider an alternative strategy given by

   i. If $Hv_0^T \neq 0$ and $Hv_1^T \neq 0$, then he *skips*.
   ii. If $Hv_0^T \neq 0$ and $Hv_1^T = 0$, then he writes 1.
   iii. If $Hv_0^T = 0$ and $Hv_1^T \neq 0$, then he writes 0.

   Is this better or worse than the original strategy in terms of probability of success?

   Solution. The original strategy succeeds with probability $\frac{n}{n+1}$. For this alternative strategy, the success event and failure event are interchanged compared to the original strategy and hence has probability of failure equal to $\frac{n}{n+1} > \frac{1}{n+1}$. □