Telecom ParisTech
Teacher: Aslan Tchamkerten

Telecom 202b, Coding Theory
October 2021

ASSIGNMENT 3

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

Exercise 2. Show that a Reed-Solomon code with 1 message symbol and n codeword symbols is an n times repetition code.

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) $\alpha_1 = 0$, $\alpha_2 = 1$, $\alpha_3 = x$, $\alpha_4 = x + 1$.

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 $f_{k-1} = 0$.]

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.