

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 $f_0 + f_1x$ with $f_0, f_1 \in \mathbb{F}_4$. Thus the mapping between information symbols and codewords is given by

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

The full mapping is thus

0	0	→	(0	0	0	0)	x	0	→	(x	x	x	x)
0	1	→	(0	1	x	$x + 1$)	x	1	→	(x	$x + 1$	0	1)
0	x	→	(0	x	$x + 1$	1)	x	x	→	(x	0	1	$x + 1$)
0	$x + 1$	→	(0	$x + 1$	1	x)	x	$x + 1$	→	(x	1	$x + 1$	0)
1	0	→	(1	1	1	1)	$x + 1$	0	→	($x + 1$	$x + 1$	$x + 1$	$x + 1$)
1	1	→	(1	0	$x + 1$	x)	$x + 1$	1	→	($x + 1$	x	1	0)
1	x	→	(1	$x + 1$	x	0)	$x + 1$	x	→	($x + 1$	1	0	x)
1	$x + 1$	→	(1	x	0	$x + 1$)	$x + 1$	$x + 1$	→	($x + 1$	0	x	1)

□

Exercise 4. Consider the following mapping from $(\mathbb{F}_q)^k$ to $(\mathbb{F}_q)^{k+1}$. Let $(f_0, f_1, \dots, f_{k-1})$ be any k -tuple over \mathbb{F}_q , and define the polynomial $f(x) = f_0 + f_1x + \dots + f_{k-1}x^{k-1}$ of degree less than k . Map $(f_0, f_1, \dots, f_{k-1})$ 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). □