

## 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 2 message symbols 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  $(f_0, f_1, \dots, f_{k-1})$  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  $f_{k-1} = 0$ .]

**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.

**Exercise 6 (Secret sharing).** Throughout, we let  $\mathcal{C}$  be a binary linear code of length  $n$ . We say that a codeword  $v'$  covers a codeword  $v$  if the non-zero components of  $v$  are a subset of the non-zero components of  $v'$ . A non-zero codeword  $v$  is said to be minimal if it covers no other codeword.

1. Let  $v'$  be a non-zero non-minimal codeword of  $\mathcal{C}$ . Argue that  $v'$  covers some minimal codeword which we denote as  $v(1)$ .
2. Argue that  $v' - v(1)$  is another codeword with weight strictly less than  $v'$ .
3. Deduce that  $v' - v(1) - v(2) - \dots - v(s) = 0$  for some minimal codewords  $v(1), \dots, v(s)$ .
4. Secret sharing: Let  $\mathcal{C}$  be an  $[n, k]$  binary linear code. An information set  $\mathcal{I}$  is a set of  $k$  components whose values entirely specify any codeword (for instance, for an MDS code, any  $k$  components is an information set). Show that there always exists an information set that contains the first component, unless all codewords have their first component equal to zero.

5. Pick  $v_1 \in \{0, 1\}$  uniformly at random, this will be our “secret”. Assign uniformly random values from  $\{0, 1\}$  to all  $k - 1$  components  $v_j, j \in \mathcal{I} \setminus \{1\}$ , independently of  $v_1$ . From  $\{v_j, j \in \mathcal{I}\}$  compute the full codeword  $v = v_1, v_2, \dots, v_n$ . Distribute digits  $v_2, v_3, \dots, v_n$  to  $n - 1$  distinct persons.

We now provide secrecy analysis for this scheme and analyze the sets of persons that are able to recover the secret  $v_1$ .

- (a) A set of  $t$  persons, with combined knowledge of  $v_{j_1}, v_{j_2}, \dots, v_{j_t}$ , represents a *critical set* if they can recover the secret  $v_1$  without error, but any proper subset of these persons recovers the value of  $v_1$  only with probability  $1/2$ . Show that if a set of  $t$  persons, with combined knowledge of  $v_{j_1}, v_{j_2}, \dots, v_{j_t}$ , represents a *critical set*, then

$$v_1 = v_{j_1} + \dots + v_{j_t} \pmod{2}.$$

Hint: consider the parity check matrix representation of  $\mathcal{C}$

- (b) Deduce that the codeword with zeros everywhere except at positions 1 and  $\{j_i, i = 1, \dots, t\}$  belongs to the dual code  $\mathcal{C}^\perp$  of  $\mathcal{C}$ .
- (c) Deduce that any critical set of persons corresponds to a minimal codeword in  $\mathcal{C}^\perp$  whose first component is a 1, and such that the persons indices correspond to the components of the non-zero entries of the codeword, after the first component.
- (d) We now illustrate the secret sharing scheme through an example. Consider the code whose parity-check matrix is

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

It can be checked that positions 1,2,4 form an information set. Fix the first digit of a codeword,  $v_1$ , our secret, then choose the second and fourth positions uniformly at random, and compute the full codeword  $v$ . Give the digits in positions 2,3,4, and 5 to Alice, Bob, Carol, and David, respectively. What are the critical sets that can recover the secret  $v_1$ ?