Chapter 9

Review

The final exam focuses on the part after midterm exam. The codes in this part are all linear codes, so we need some facts and results for linear codes, such as:

- Definition of linear codes;
- the parameters of linear codes;
- the minimum weight of linear code: \( \text{wt}(C) = d(C) \);
- generator matrix \( G \) and the standard form for generator matrix;
- dual codes (self-dual code and self orthogonal codes);
- parity-check matrix \( H \), the standard form and the relation between standard generator matrices and standard parity-check matrices;
- \( C^\perp = \{ x \in F_q^n \mid Gx^t = 0 \} \) and \( C = \{ x \in F_q^n \mid Hx^t = 0 \} \).
- calculate minimum distance from a parity-check matrix.

Chapter 4. Hamming codes

- **Definition 4.1**: the definition of Hamming codes;
- **Remark 3) after the definition**: An easy way to write down a PCM (parity-check matrix) for a Hamming code [ref. to Examples 4.1, 4.2; Problem 2 in Assignment 4; Problem 5 1) in Assignment 3];
• **Theorem 4.1**: $\text{Ham}(r, q)$ is a perfect $[\frac{q^r - 1}{q - 1}, \frac{q^r - 1}{q - 1} - r, 3]$ linear code;

• Hamming size: $A_q(\frac{q^r - 1}{q - 1}, 3) = q^{n-r} = q^{\frac{q^r - 1}{q - 1} - r}$ [ref. to Problem 5 2) in Assignment 3];

• decoding with a $q$-ary Hamming code [ref. to Examples 4.3, 4.4, 4.5; Problem 2 in Assignment 4].

### Chapter 5. Golay codes

• **Property of perfect codes**: If $C$ is a perfect $q$-ary $(n, M, 2t+1)$-code, then we have $\bigcup_{x \in C} S(x, t) = F_q^n$, here the union is a disjoint union.

• **Definitions and properties of $G_{23}$ and $G_{24}$**: Propositions 5.2, 5.4, [ref. to Problems 3,4,5 in Assignment 4];

• We do not need the ternary case in the final exam, but you should know how to check parameters satisfy the perfect code’s condition, i.e., the equation (1.1) in chapter 1 holds.

### Chapter 6. Finite fields

• **Some definitions**: degree of polynomials, irreducible polynomials, division rule, greatest common divisor, least common multiple. [ref. to Problem 6 in Assignment 4];

• Linear factor and irreducibility of 2nd and 3rd degree polynomials: Lemma 6.3 and Corollary 6.4 [ref. to Problem 7 in Assignment 4];

• The quotient ring (or field) $F_q[x]/f(x)$;

• Uniqueness of finite field of order $q$: Theorem 6.2;

• **Primitive elements and the order of nonzero elements**: Definitions 6.9, 6.10; Lemma 6.11, Theorem 6.3 [ref. to Examples 6.5, 6.6, 6.7; Problem 1 in Assignment 5];
• Minimal polynomials: Definitions 6.12; Theorems 6.4, 6.5; corollary 6.13 [ref. to Examples 6.5, 6.6, 6.7; Problem 1 in Assignment 5];

• Cyclotomic cosets and minimal polynomials of $\alpha^i$: Definitions 6.14; Theorem 6.6 [ref. to Examples 6.9, 6.10; Problem 2 in Assignment 5];

• Factorization: Theorem 6.7 and Corollary 6.15 [ref. to Example 6.11; Problem 3 in Assignment 5];

Chapter 7. Cyclic codes

• Definition of cyclic codes;

• One to one correspondence between $F_q^n$ and $F_q[x]/(x^n - 1)$;

• Properties of cyclic codes: Theorems 7.1, 7.2, 7.3; the generator polynomials of cyclic codes [ref. to Problem 5, 6, 7 in Assignment 5];

• The quotient ring (or field) $F_q[x]/f(x)$;

• Cyclic generator matrix and cyclic parity-check matrix: they are given by generator polynomial and check polynomial; Theorems 7.4, 7.5, 7.6 [ref. to Problem 4 in Assignment 5];

• Cyclic binary Hamming codes: Theorem 7.7 [ref. to Example 7.4].

Chapter 8. BCH codes

• Primitive BCH codes: focus on the primitive case; Lemma 8.3 [ref. to Examples 8.1];

• Minimum distance of primitive BCH codes: Theorem 8.2: the code with design distance $d$ has minimum distance at least $d$ [ref. to Example 8.2];

• Decoding of BCH codes: [ref. to Examples 8.3, 8.4, 8.5].

Note: For Lemmas, Theorems and Propositions, you do not need to know the details of proof, but you should be familiar with the results and use them to solve problems and prove some statements.