Diskrete Mathematik HS2025 — Prof. Dennis HOFHEINZ

Marian DIETZ — Milan GONZALEZ-THAUVIN — Zoé REINKE

Exercise sheet 11

This is the exercise sheet number 11. The difficulty of the questions and exercises are rated from very easy (⋆) to hard (⋆ ⋆ ⋆ ⋆) . The graded exercise is Exercise 11.2 and your solution has to be uploaded on the Moodle page of the course **by 04/12/2025, 23:59**. The solution to this exercise must be your own work, you may not share your solutions with anyone else. See also the note on dishonest behavior on the Moodle page.

Exercise 11.1 Error-Correcting Codes (⋆ ⋆)

Let $n \in \mathbb{N}\backslash\{0\}$, F be a finite field and let $\mathcal{C} \subseteq F^n$ be a code that forms a group with element-wise addition (such a code is also called **linear**). Let $d(c_1, c_2)$ denote the Hamming distance between two codewords $c_1, c_2 \in \mathcal{C}$. Moreover, let $\mathsf{hw}(c)$ denote the **Hamming weight** (i.e., the number of non-zero positions) of a codeword $c \in \mathcal{C}$. Assume that there exists $t \in \mathbb{N}$ such that

$$\min_{c \in \mathcal{C}\backslash\{0^n\}} \mathsf{hw}(c) = 2t + 1.$$

1. Prove that $\mathcal{C}$ is t-error correcting.
2. Is it possible that there exists a codeword $c \in \mathcal{C}$ such that up to $t + 1$ **arbitrary** errors can be corrected?

Exercise 11.2 A new linear code (⋆ ⋆) — GRADED *(8 points)*

Please upload your solution by 04/12/2025

Like in the previous exercise, let $n \in \mathbb{N} \setminus \{0\}$, F be a finite field and let $\mathcal{C} \subseteq F^n$ be a linear code, i.e. such that $\langle \mathcal{C}; +, -, 0^n \rangle$ is a group with $+$ (resp. $-$) the element-wise addition (resp. inverse) of F and 0^n the codeword composed of n zeros. Let $d(c_1, c_2)$ denote the Hamming distance between two codewords $c_1, c_2 \in \mathcal{C}$ and let also $\mathsf{hw}(c)$ denote the Hamming weight (i.e., the number of non-zero positions) of a codeword $c \in \mathcal{C}$.

1. Show that the Hamming weight hw satisfies the triangle inequality, i.e.

$$\forall x, y \in \mathcal{C}, \mathsf{hw}(x + y) \leq \mathsf{hw}(x) + \mathsf{hw}(y)$$

2. Show that $d_{\min}(\mathcal{C}) = \min_{c \in \mathcal{C}\setminus\{0^n\}} \mathsf{hw}(c)$.
   Hint: show both inequalities in order to conclude with the equality.

3. Let $U \subseteq F^n$ and $V \subseteq F^n$ be two **linear** codes. Let $\mathcal{D} \subseteq F^{2n}$ be the linear code defined as
$$\mathcal{D} \overset{\text{def}}{=} \{(u \parallel (u+v)) \mid u \in U, v \in V\}$$
with $\parallel$ the denoting concatenation (from two words of length n, we obtain a word of length $2n$). Prove that that $d_{\min}(\mathcal{D}) = \min(2d_{\min}(U), d_{\min}(V))$.
Hint: same as above.

Exercise 11.3 Proof Systems ($\star\star$)

1. Prove or disprove the following statement: For any non-empty sets $\mathcal{S}$ and $\mathcal{P}$, and any function $\phi : \mathcal{S} \times \mathcal{P} \to \{0,1\}$, there exists a **unique** function $\tau : \mathcal{S} \to \{0,1\}$ such that $\Pi = (\mathcal{S}, \mathcal{P}, \tau, \phi)$ is a sound and complete proof system.

2. Let $\Pi_1 = (\mathcal{S}_1, \mathcal{P}_1, \tau_1, \phi_1)$ and $\Pi_2 = (\mathcal{S}_2, \mathcal{P}_2, \tau_2, \phi_2)$ be two proof systems. We combine Π_1 and Π_2 into a third proof system
$$\Pi_3 = (\mathcal{S}_1 \times \mathcal{S}_2, \mathcal{P}_1 \times \mathcal{P}_2, \tau_3, \phi_3),$$
where
$$\tau_3(s_1, s_2) = 1 \quad \overset{\text{def}}{\iff} \quad \tau_1(s_1) = 1 \text{ or } \tau_2(s_2) = 1,$$
and
$$\phi_3((s_1, s_2), (p_1, p_2)) = 1 \quad \overset{\text{def}}{\iff} \quad \phi_1(s_1, p_1) = 1 \text{ or } \phi_2(s_2, p_2) = 1.$$
Prove or disprove each of the following statements:
   (i) *If Π_3 is sound, then Π_1 or Π_2 is sound.*
   (ii) *If Π_1 or Π_2 is complete, then Π_3 is complete.*

Exercise 11.4 Diffie-Hellman Proof System ($\star\star$)

Alice and Bob execute the Diffie-Hellman protocol[1], using the cyclic group $G \overset{\text{def}}{=} \langle \mathbb{Z}_p^*; \odot_p \rangle$ with p prime and generator g [2]. Let n be the order of G (here $p-1$) and consider the set of statements $\mathcal{S} = G^3$ and the truth function τ defined as follows:

$$\tau\big(y_A, y_B, k_{AB}\big) = 1 \quad \overset{\text{def}}{\iff} \quad \begin{array}{l}\text{There exist } x_A, x_B \in \mathbb{Z}_n \text{ such that}\\ k_{AB} \text{ is the shared secret resulting from}\\ \text{exchanging the public keys } y_A \overset{\text{def}}{=} g^{x_A} \text{ and } y_B \overset{\text{def}}{=} g^{x_B}.\end{array}$$

Let $\mathcal{P} = \mathbb{Z}_n$. Define $\phi : \mathcal{S} \times \mathcal{P} \to \{0,1\}$, such that $\Pi = (\mathcal{S}, \mathcal{P}, \tau, \phi)$ is a complete and sound proof system. Prove your answer.

[1] Section 4.6 of the lecture notes but in this exercise we use groups to simplify notations. In particular, in a cyclic group G of order n with generator g, if $x \in \mathbb{Z}_n$ we will write g^x to denote the (unique) element of G equal to g^k when $k \in \mathbb{Z}$ is in the class x. In other words, **here** $\mathbb{Z}_n$ can be interpreted as the set $\{0, 1, \cdots, n-1\}$.

[2] As mentioned in Section 5.3.6, G can actually be any cyclic group for which computing $x \in \mathbb{Z}_n$ from g^x (its *discrete logarithm*) is hard.

Exercise 11.5 Yet another proof system (exam FS 2024) ($\star$)

This exercise is taken from the spring exam of 2024.
Consider the proof systems

$$\Sigma_1 = \big(\mathcal{S}_1, \mathcal{P}_1, \tau_1, \phi_1\big),$$
$$\Sigma_2 = \big(\mathcal{S}_2, \mathcal{P}_2, \tau_2, \phi_2\big).$$

Consider the new proof system derived from Σ_1 and Σ_2 as follows:

$$\Sigma = \big(\mathcal{S}_1 \times \mathcal{S}_2, \mathcal{P}_1 \times \mathcal{P}_2, \tau, \phi\big)$$

where

$$\tau(s_1, s_2) = 1 \iff \text{at least one of } \tau_1(s_1) \text{ and } \tau_2(s_2) \text{ equals } 1.$$

and

$$\phi\big((s_1, s_2), (p_1, p_2)\big) = 1 \iff \text{exactly one of } \phi_1(s_1, p_1) \text{ and } \phi_2(s_2, p_2) \text{ equals } 1.$$

1. **Prove or disprove** the following statement: if both Σ_1 and Σ_2 are sound, then Σ is sound.

2. **Prove or disprove** the following statement: if both Σ_1 and Σ_2 are complete, then Σ is complete.

Due by 04/12/2025, 23:59.
Exercise 11.2 will be graded.