ETH Zürich, D-INFK
HS 2024, 29. November 2024

Prof. Ueli Maurer
Giovanni Deligios, Dr. Karen Klein

Diskrete Mathematik

Exercise 11

Exercise 11.4 gives **bonus points**, which can increase the final grade. 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 course website: `https://crypto.ethz.ch/teaching/DM24/`.

11.1 Error-Correcting Codes ($\star\,\star$)

Let $\mathcal{C} \subseteq \mathrm{GF}(q)^n$ 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

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

a) Prove that $\mathcal{C}$ is t-error correcting.

b) Is it possible that there exists a codeword $c \in \mathcal{C}$ such that up to $t + 1$ *arbitrary* errors can be corrected?

11.2 Proof Systems ($\star\,\star$)

a) 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.

b) 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.*

11.3 Diffie-Hellman Proof System ($\star\,\star$)

Alice and Bob execute the Diffie-Hellman protocol, using a cyclic group $G = \langle g \rangle$ of order n. Consider the set of statements $\mathcal{S} = G^3$ and the truth function τ defined as follows:

$$\tau\big(y_A, y_B, k_{AB}\big) = 1 \quad \overset{\text{def}}{\iff} \quad \begin{array}{l} k_{AB} \text{ is the secret key resulting from} \\ \text{exchanging the public keys } y_A \text{ and } y_B. \end{array}$$

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.

11.4 Combining Proof Systems ($\star$) *(8 Points)*

Let

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

be a complete and sound proof system.

a) Define $\mathcal{P}'$ and ϕ' so that

$$\Sigma' = (\mathcal{S} \times \mathcal{S} \times \mathcal{S}, \mathcal{P}', \tau', \phi')$$

is a complete and sound proof system (and prove it!), where

$$\tau'\big((s_1, s_2, s_3)\big) = 1 \iff \text{at least 2 among } \tau(s_1), \tau(s_2), \tau(s_3) \text{ are equal to } 1.$$

b) Let

$$\overline{\Sigma} = \big(\mathcal{S}^2, \overline{\mathcal{P}}, \overline{\tau}, \overline{\phi}\big)$$

be a complete and sound proof system with

$$\begin{array}{l} \overline{\tau}\big((s_1, s_2)\big) = 1 \iff \text{exactly 1 of the statements is true in } \Sigma, \\ \qquad\qquad\qquad\qquad \text{that is, } \tau(s_1) = 1 \text{ or } \tau(s_2) = 1, \text{but not both.} \end{array} \tag{1}$$

Define $\mathcal{P}^*$ and ϕ^* so that $\Sigma^* = (\mathcal{S}, \mathcal{P}^*, \tau^*, \phi^*)$ is a complete and sound proof system (and prove it!), where

$$\tau^*(s) = 1 \iff \tau(s) = 0.$$

11.5 Homer's Birthday ($\star\,\star$)

Homer wants to organize a birthday party. He would like to invite as many friends as possible. The problem is that everything is always so difficult...

Homer wants to invite Abe. But if Abe comes, then Barney comes as well. This is not a problem yet, but if Barney comes, then Carl has to come too. And if Carl comes, Disco Stu also certainly arrives. However, if both Barney and Disco Stu come, then Carl surely doesn't come. Finally, if Disco Stu comes, then at least one of Abe and Barney comes.

Homer does not know whether anyone would eventually come to the party. Perhaps it would be better to simply go to Moe's right away?

a) Formalize the above conditions, using propositional formulas. Argue (intuitively) whether Homer should buy beer and donuts for the party or go straight to Moe's.

b) Using the following derivation rules, derive formally the answer to Subtask a).

$$\begin{aligned}
\{F \to G, G \to H\} &\vdash_{R_1} F \to H \\
\{F \to G, F \to \neg G\} &\vdash_{R_2} \neg F \\
\{F \to (G \vee H), G \to H\} &\vdash_{R_3} F \to H \\
\{F \to G\} &\vdash_{R_4} F \to (G \wedge F) \\
\{F \to G, \neg G\} &\vdash_{R_5} \neg F
\end{aligned}$$

11.6 Models and Satisfiability ($\star$)

a) Determine the sets of models of the formulas F and G. Then, decide whether F and G are equivalent or if one is a consequence of the other.

$$F = (\neg A \vee B) \wedge (B \to (\neg C \wedge \neg A)) \wedge (A \vee C) \qquad G = \neg(A \to B) \vee (C \to A)$$

b) Prove or disprove: Two formulas of propositional logic that have no common atomic formulas are not equivalent.

c) Prove or disprove: If F_1 and F_2 are formulas such that F_1 and $F_1 \to F_2$ are satisfiable, then F_2 is also satisfiable.

11.7 Satisfiability ($\star$)

For each set of formulas, either find a model or show that it is unsatisfiable.

a) $M = \{\neg A,\ B \wedge C,\ \neg A \to \neg C\}$

b) $N = \{A_1 \vee A_2,\ \neg A_2 \vee A_3,\ \neg A_3 \vee A_4,\ \ldots\}$

Due by 5. December 2024.
Exercise 11.4 is graded.