ETH Zürich, D-INFK
HS 2024, 6. December 2024

Prof. Ueli Maurer
Giovanni Deligios, Dr. Karen Klein

Diskrete Mathematik

Solution 11

11.1 Error-Correcting Codes

a) Let $c_1, c_2 \in \mathcal{C}$ with $c_1 \neq c_2$ be arbitrary. Since $\mathcal{C}$ forms a group, we know that $c = c_1 + (-c_2) \in \mathcal{C}$. We have

$$d(c_1, c_2) = \mathsf{hw}(c_1 + (-c_2)) = \mathsf{hw}(c) \geq 2t + 1.$$

In the first step, we have used that two codewords differ at a position if and only if the difference of their values at this position is non-zero. In the last step, we have used the assumption from above, together with the fact that $c_1 \neq c_2$ implies $c \neq 0^n$.
Thus, we have $d_{\mathsf{min}}(\mathcal{C}) \geq 2t + 1$, which implies by Theorem 5.41 that $\mathcal{C}$ is t-error correcting.

b) Let $c \in \mathcal{C}$ be arbitrary. Moreover, let $c_{\mathsf{min}} \in \mathcal{C} \setminus \{0^n\}$ be such that $\mathsf{hw}(c_{\mathsf{min}}) = 2t + 1$. Since $\mathcal{C}$ forms a group, we have $c + c_{\mathsf{min}} \in \mathcal{C}$. Observe that

$$d(c, c + c_{\mathsf{min}}) = \mathsf{hw}(c_{\mathsf{min}}) = 2t + 1.$$

Thus, c and $c + c_{\mathsf{min}}$ differ on exactly $2t + 1 = (t + 1) + t$ positions. We can therefore change the first $t + 1$ of these positions of c to the ones of $c + c_{\mathsf{min}}$ to obtain a word w with $d(c, w) = t + 1$ and $d(c + c_{\mathsf{min}}, w) = t$. This word w cannot be error-corrected. Since $c \in \mathcal{C}$ was arbitrary, there exists no codeword such that up to $t + 1$ arbitrary errors can be corrected.

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

a) We prove the claim constructively. Let $\mathcal{S}$ and $\mathcal{P}$ be non-empty sets and let $\phi : \mathcal{S} \times \mathcal{P} \to \{0, 1\}$ be an arbitrary function. Consider the function $\tau : \mathcal{S} \to \{0, 1\}$ defined by

$$\tau(s) = 1 \quad \overset{\text{def}}{\iff} \quad \text{there exists } p \in \mathcal{P} \text{ such that } \phi(s, p) = 1.$$

The proof system $\Pi = (\mathcal{S}, \mathcal{P}, \tau, \phi)$ is sound: For any $s \in \mathcal{S}$ and any $p \in \mathcal{P}$ with $\phi(s, p) = 1$, the definition of τ implies that $\tau(s) = 1$. Moreover, Π is complete: For any $s \in \mathcal{S}$ with $\tau(s) = 1$, the definition of τ implies that there exists $p \in \mathcal{P}$ such that $\phi(s, p) = 1$.
It is left to show that τ is unique. Consider any function $\tau' : \mathcal{S} \to \{0, 1\}$ such that $\tau \neq \tau'$. This is implies that $\tau(s) \neq \tau'(s)$ for some $s \in \mathcal{S}$. Case distinction:

- $\tau(s) = 0$ and $\tau'(s) = 1$. By definition of τ, $\tau(s) = 0$ implies there exists no $p \in \mathcal{P}$ such that $\phi(s, p) = 1$. But since $\tau'(s) = 1$, the proof system $(\mathcal{S}, \mathcal{P}, \tau', \phi)$ cannot be complete.
- $\tau(s) = 1$ and $\tau'(s) = 0$. By definition of τ, $\tau(s) = 1$ implies there exists $p \in \mathcal{P}$ such that $\phi(s, p) = 1$. But since $\tau'(s) = 0$, the proof system $(\mathcal{S}, \mathcal{P}, \tau', \phi)$ cannot be sound.

b)

(i) We prove the claim indirectly. Assume that neither Π_1 nor Π_2 is sound. Then there exist $s_1 \in \mathcal{S}_1$ and $p_1 \in \mathcal{P}_1$ such that $\tau_1(s_1) = 0$ and $\phi_1(s_1, p_1) = 1$, and there exist $s_2 \in \mathcal{S}_2$ and $p_2 \in \mathcal{P}_2$ such that $\tau_2(s_2) = 0$ and $\phi_2(s_2, p_2) = 1$. Thus, we have $\tau_3(s_1, s_2) = 0$ but $\phi_3((s_1, s_2), (p_1, p_2)) = 1$. Hence, Π_3 is not sound.

(ii) We disprove the claim by giving a counterexample. Let $\mathcal{S}_1 = \mathcal{S}_2 = \{0\}$ and $\mathcal{P}_1 = \mathcal{P}_2 = \{0\}$. We define $\tau_1(0) = 0$, $\phi_1(0, 0) = 0$, $\tau_2(0) = 1$, and $\phi_2(0, 0) = 0$. Clearly $\Pi_1 = (\mathcal{S}_1, \mathcal{P}_1, \tau_1, \phi_1)$ is complete. However, $\tau_3(0, 0) = 1$ since $\tau_2(0) = 1$, but $\phi_3((0, 0), (p_1, p_2)) = 0$ for all $(p_1, p_2) \in \mathcal{P}_1 \times \mathcal{P}_2 = \{(0, 0)\}$. Thus, Π_3 is not complete.

11.3 Diffie-Hellman Proof System

A proof of a statement (y_A, y_B, k_{AB}) will be the discrete logarithm x_A of y_A. Formally, $\mathcal{P} = \mathbb{Z}_n$ and $\phi\big((y_A, y_B, k_{AB}), x_A\big) = 1$ if and only if $g^{x_A} = y_A$ and $y_B^{x_A} = k_{AB}$.

Completeness: Assume $\tau\big((y_A, y_B, k_{AB})\big) = 1$. There exist unique $x_A, x_B \in \mathbb{Z}_n$ (the secret keys chosen by Alice and Bob) such that $g^{x_A} = y_A$ and $g^{x_B} = y_B$. Since the statement is true, we also have $k_{AB} = g^{x_A x_B} = y_B^{x_A}$. Hence, for this x_A we have $\phi\big((y_A, y_B, k_{AB}), x_A\big) = 1$.

Soundness: Assume $\phi\big((y_A, y_B, k_{AB}), x'_A\big) = 1$. Let $x_B \in \mathbb{Z}_n$ be (unique) such that $g^{x_B} = y_B$. The verification ϕ guarantees that $k_{AB} = y_B^{x'_A} = g^{x'_A x_B}$ and $g^{x'_A} = y_A$ and $x'_A \in \mathbb{Z}_n$. Hence, k_{AB} is the secret key resulting from the Diffie-Hellman protocol where Alice chooses x'_A and Bob chooses x_B.

11.4 Combining Proof Systems

a) Let $\mathcal{P}' = \{1, 2, 3\} \times \{1, 2, 3\} \times \mathcal{P} \times \mathcal{P}$ and let

$$\phi'\big((s_1, s_2, s_3), (i, j, p, p')\big) = 1 \iff i \neq j \text{ and } \phi(s_i, p) = 1 \text{ and } \phi(s_j, p') = 1.$$

To prove completeness, suppose that $\tau'(s_1, s_2, s_3) = 1$. This means that at least two s_i, s_j out of s_1, s_2, s_3 are true. By completeness of Σ there exist p and p' in $\mathcal{P}$ such that $\phi(s_i, p) = \phi(s_j, p') = 1$. This means that, with the given definition of ϕ', the 4-tuple (i, j, p, p') is a valid proof for (s_1, s_2, s_3) in Σ'.

To prove soundness, suppose that for some $(s_1, s_2, s_3) \in \mathcal{S}^3$ and some $(i, j, p, p') \in \mathcal{P}'$ we have

$$\phi'\big((s_1, s_2, s_3), (i, j, p, p')\big) = 1.$$

Then, by soundness of Σ, since $\phi(s_i, p) = 1$ and $\phi(s_j, p') = 1$ we get that s_i and s_j are true in Σ, which means that, since $i \neq j$, at least two out of s_1, s_2, s_3 are true in Σ, and by definition of τ' the statement (s_1, s_2, s_3) is true in Σ'.

b) If there are no true statements in Σ, then the solution is trivial: simply define a proof set $\mathcal{P}^*$ with a single element, and the verification function ϕ^* evaluates to true for each statement in $\mathcal{S}$ and the only proof in $\mathcal{P}^*$. Therefore, we can assume that $\mathcal{S}$ contains at least one true statement. Let $\mathcal{P}^* = \mathcal{S} \times \mathcal{P} \times \overline{\mathcal{P}}$ and let

$$\phi^*\big(s, (s', p', \overline{p})\big) = 1 \iff \phi(s', p') = 1 \text{ and } \text{ and } \overline{\phi}\big((s', s), \overline{p}\big) = 1.$$

To prove completeness of Σ^*, suppose that $\tau^*(s) = 1$ which means $\tau(s) = 0$. By assumption, there exists an element $s' \in \mathcal{S}$ with $\tau(s) = 1$. By completeness of Σ we can find a proof $p' \in \mathcal{P}$ such that $\phi(s', p') = 1$. Furthermore, since $\tau(s) = 0$, this means that $\overline{\tau}(s', s) = 1$, because only s' is true in Σ. By completeness of $\overline{\Sigma}$ we find a proof $\overline{p}$ with $\overline{\phi}((s', s), \overline{p}) = 1$. Therefore $(s', p', \overline{p})$ is a valid proof of s in Σ^* with the above definition of ϕ^*. To prove soundness of Σ^*, suppose that $\phi^*\big(s, (s', p', \overline{p})\big) = 1$. This means 1) $\overline{\phi}((s', s), \overline{p}) = 1$, which by soundness of $\overline{\Sigma}$ this means that exactly one among s', s is true in Σ and 2) $\phi(s', p') = 1$, which by soundness of Σ implies that $\tau(s') = 1$. These two facts together imply that s is false in Σ. Therefore $\tau^*(s) = 1$.

11.5 Homer's Birthday

a) Let A be the proposition "Abe comes to the party", etc. The conditions given in the exercise correspond to the following implications:

$$\begin{aligned} A &\rightarrow B && (1)\\ B &\rightarrow C && (2)\\ C &\rightarrow D && (3)\\ (B \wedge D) &\rightarrow \neg C && (4)\\ D &\rightarrow (A \vee B) && (5) \end{aligned}$$

We show that no one would arrive at the party and, hence, Homer eventually ends up at Moe's whether he organizes it or not. For each person, consider what happens when he comes to the party:

i. *A is true.* In this case, B is true by formula (1), C is true by formula (2), D is true by formula (3) and $\neg C$ is true by formula (4), which is a contradiction with C. Hence, A is false.

ii. *B is true.* In this case, again, C is true by formula (2), D is true by formula (3) and $\neg C$ is true by formula (4), which is a contradiction with C. Hence, B is false.

iii. *C is true.* In this case, D is true by formula (3) and $A \vee B$ is true by formula (5). But both the assumption that A is true and the assumption that B is true lead to a contradiction, as shown in cases i. and ii. Hence, $A \vee B$ also leads to a contradiction and C is false.

iv. *D is true.* In this case, $A \vee B$ is true by formula (5). By the same argument as above, D is false.

Overall, we can conclude that no one can come to the party. That is, all the formulas are true only if A, B, C and D are all false.

b) We now formally derive $\neg A$, $\neg B$, $\neg C$ and $\neg D$, using given derivation rules:

$$
\begin{array}{lll}
\{(5)\,,(1)\} & \vdash_{R_3} & D \to B \qquad (6)\\
\{(6)\,,(2)\} & \vdash_{R_1} & D \to C \qquad (7)\\
\{(6)\} & \vdash_{R_4} & D \to (B \wedge D) \qquad (8)\\
\{(8)\,,(4)\} & \vdash_{R_1} & D \to \neg C \qquad (9)\\
\{(7)\,,(9)\} & \vdash_{R_2} & \neg D \qquad (10)\\
\{(3)\,,(10)\} & \vdash_{R_5} & \neg C \qquad (11)\\
\{(2)\,,(11)\} & \vdash_{R_5} & \neg B \qquad (12)\\
\{(1)\,,(12)\} & \vdash_{R_5} & \neg A \qquad (13)
\end{array}
$$

11.6 Models and Satisfiability

a) Consider the function table of F:

A	B	C	$\neg A \vee B$	$\neg C \wedge \neg A$	$B \to (\neg C \wedge \neg A)$	$A \vee C$	F
0	0	0	1	1	1	0	0
0	0	1	1	0	1	1	1
0	1	0	1	1	1	0	0
0	1	1	1	0	0	1	0
1	0	0	0	0	1	1	0
1	0	1	0	0	1	1	0
1	1	0	1	0	0	1	0
1	1	1	1	0	0	1	0

The set of models for F contains all truth assignments $\mathcal{A}$, such that $\mathcal{A}(A) = \mathcal{A}(B) = 0$ and $\mathcal{A}(C) = 1$.

Consider now the function table of G:

A	B	C	$\neg(A \to B)$	$C \to A$	G
0	0	0	0	1	1
0	0	1	0	0	0
0	1	0	0	1	1
0	1	1	0	0	0
1	0	0	1	1	1
1	0	1	1	1	1
1	1	0	0	1	1
1	1	1	0	1	1

The set of models for G contains all truth assignments $\mathcal{A}$, such that $\mathcal{A}(A) = 1$ and all truth assignments $\mathcal{A}$, such that $\mathcal{A}(C) = 0$.

The formulas are not equivalent, since the sets are not the same. G is not the consequence of F, because the set of models for F is not a subset of the set of models for G. Similarly F is not a consequence of G.

b) The statement is false. A counterexample is $F = A \vee \neg A$ and $G = B \vee \neg B$. Of course, F and G have no common atomic formulas. However, by Lemma 6.1 11), $A \vee \neg A \equiv \top \equiv B \vee \neg B$.

c) The statement is false. A counterexample in propositional logic is $F_1 = A$ and $F_2 = A \wedge \neg A$. F_1 and $F_1 \rightarrow F_2$ are both satisfiable ($F_1 \rightarrow F_2$ is true for all interpretations $\mathcal{A}$ that assign $\mathcal{A}(F_1) = 0$). However, F_2 is clearly not satisfiable.

11.7 Satisfiability

a) The set M is not satisfiable. To show this, assume that $\mathcal{A}$ is a model for M. Since $\neg A \in M$, we have $\mathcal{A}(\neg A) = 1$ and thus $\mathcal{A}(A) = 0$. Moreover, we have $B \wedge C \in M$, and therefore $\mathcal{A}(B \wedge C) = 1$, which implies that $\mathcal{A}(C) = 1$.

Since $\neg A \rightarrow \neg C \in M$, we also have $\mathcal{A}(\neg A \rightarrow \neg C) = 1$, so $\mathcal{A}(\neg\neg A \vee \neg C) = \mathcal{A}(A \vee \neg C) = 1$, which implies $\mathcal{A}(A) = 1$ or $\mathcal{A}(C) = 0$. This is a contradiction to $\mathcal{A}(A) = 0$ and $\mathcal{A}(C) = 1$.

b) A model for N is, for example, the truth assignment $\mathcal{A} : \{A_1, A_2, \ldots\} \rightarrow \{0, 1\}$ that assigns $\mathcal{A}(A_1) = 1$ and $\mathcal{A}(A_i) = 0$ for $i > 1$. (One could interpret the statement A_i as "i is less or equal to 1", for $i \in \mathbb{N}$.)