ETH Zürich, D-INFK
HS 2020, 9. December 2020

Prof. Ueli Maurer
David Lanzenberger

# Diskrete Mathematik

# Solution 12

### 12.1 Proof Systems ($\star\star$)

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

### 12.2 A Special Calculus for Propositional Logic

**a)** The calculus is sound.

**b)** We now formally derive $A \to C$ from $\{A \to B, B \to C\}$, using the given derivation rules.

$$\begin{array}{rll}
\varnothing & \vdash_{R_2} & (B \to C) \to (A \to (B \to C)) \\
\{(B \to C) \to (A \to (B \to C)), B \to C\} & \vdash_{R_1} & A \to (B \to C) \\
\varnothing & \vdash_{R_4} & (A \to (B \to C)) \to ((A \to B) \to (A \to C)) \\
\{(A \to (B \to C)) \to ((A \to B) \to (A \to C)), A \to (B \to C)\} & \vdash_{R_1} & (A \to B) \to (A \to C) \\
\{(A \to B) \to (A \to C), A \to B\} & \vdash_{R_1} & A \to C
\end{array}$$

### 12.3 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 $F_1 \to F_2$ are both satisfiable ($F_1 \to F_2$ is true for all interpretations $\mathcal{A}$ that assign $\mathcal{A}(F_1) = 0$). However, $F_2$ is clearly not satisfiable.

### 12.4 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 $\neg A \to \neg C \in M$, we also have $\mathcal{A}(\neg A \to \neg C) = 1$, 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 $\mathcal{A} : \{A_1, A_2, \ldots\} \to \{0, 1\}$ 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 $i \in \mathbb{N}$.)

### 12.5 Normal Forms

**a)** The function table of $F = (\neg(A \to C)) \leftrightarrow (A \to B)$ is

| $A$ | $B$ | $C$ | $(\neg(A \to C))$ | $(A \to B)$ | $F$ |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 1 | 0 |
| 0 | 0 | 1 | 0 | 1 | 0 |
| 0 | 1 | 0 | 0 | 1 | 0 |
| 0 | 1 | 1 | 0 | 1 | 0 |
| 1 | 0 | 0 | 1 | 0 | 0 |
| 1 | 0 | 1 | 0 | 0 | 1 |
| 1 | 1 | 0 | 1 | 1 | 1 |
| 1 | 1 | 1 | 0 | 1 | 0 |

Using the technique from the proof of Theorem 6.6, we can find an equivalent formula in CNF:

$$(A \vee B \vee C) \wedge (A \vee B \vee \neg C) \wedge (A \vee \neg B \vee C) \wedge (A \vee \neg B \vee \neg C) \wedge (\neg A \vee B \vee C) \wedge (\neg A \vee \neg B \vee \neg C)$$

and an equivalent formula in DNF:

$$(A \wedge \neg B \wedge C) \vee (A \wedge B \wedge \neg C)$$

**b)** $(A \wedge \neg B) \vee (\neg A \wedge (C \wedge D))$

$$\begin{aligned}
&\equiv \big((A \wedge \neg B) \vee \neg A\big) \wedge \big((A \wedge \neg B) \vee (C \wedge D)\big) && \mid 6) \\
&\equiv \big(\neg A \vee (A \wedge \neg B)\big) \wedge \big((A \wedge \neg B) \vee (C \wedge D)\big) && \mid 2) \\
&\equiv \big((\neg A \vee A) \wedge (\neg A \vee \neg B)\big) \wedge \big((A \wedge \neg B) \vee (C \wedge D)\big) && \mid 6) \\
&\equiv \big((\neg A \vee A) \wedge (\neg A \vee \neg B)\big) \wedge \big(((A \wedge \neg B) \vee C) \wedge ((A \wedge \neg B) \vee D)\big) && \mid 6) \\
&\equiv \big((\neg A \vee A) \wedge (\neg A \vee \neg B)\big) \wedge \big((C \vee (A \wedge \neg B)) \wedge (D \vee (A \wedge \neg B))\big) && \mid 2), 2) \\
&\equiv (\neg A \vee A) \wedge (\neg A \vee \neg B) \wedge (C \vee A) \wedge (C \vee \neg B) \wedge (D \vee A) \wedge (D \vee \neg B) && \mid 6), 6)
\end{aligned}$$

This formula is in CNF. Using equivalences 2), 11), 2) and 9), one can find a simpler formula equivalent to $G$, also in CNF:

$$(\neg A \vee \neg B) \wedge (C \vee A) \wedge (C \vee \neg B) \wedge (D \vee A) \wedge (D \vee \neg B).$$

### 12.6 Satisfiability

Assume that $H$ is satisfiable and let $\mathcal{A}$ be a model for $H$. We have (1) $\mathcal{A}(G_1 \vee F_1) = 1$, (2) $\mathcal{A}(G_{n+1} \vee \neg F_n) = 1$ and (3) $\mathcal{A}(G_{i+1} \vee \neg F_i \vee F_{i+1}) = 1$ for all $1 \leq i \leq n-1$.

Since $\mathcal{A}$ is suitable for $H$, it is also suitable for $G_1 \vee \cdots \vee G_{n+1}$. Assume towards a contradiction that $\mathcal{A}(G_1 \vee \cdots \vee G_{n+1}) = 0$. Then $\mathcal{A}(G_1) = \cdots = \mathcal{A}(G_{n+1}) = 0$. We show by induction that $\mathcal{A}(F_i) = 1$ for all $1 \leq i \leq n$. For the base case $i = 1$, (1) and $\mathcal{A}(G_1) = 0$ imply that $\mathcal{A}(F_1) = 1$. Now assume $\mathcal{A}(F_i) = 1$ for some $1 \leq i \leq n-1$. Then $\mathcal{A}(\neg F_i) = 0$, and since also $\mathcal{A}(G_{i+1}) = 0$, we have, $\mathcal{A}(F_{i+1}) = 1$ by (3).

Therefore, $\mathcal{A}(F_n) = 1$, so $\mathcal{A}(G_{n+1} \vee \neg F_n) = 0$, which is a contradiction with (2).