ETH Zürich, D-INFK
HS 2020, 27. November 2020

Prof. Ueli Maurer
David Lanzenberger

Diskrete Mathematik

Exercise 12

Exercise 12.2 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/DM20/`.

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

Alice and Bob execute the Diffie-Hellman protocol, using a cyclic group $G = \langle g \rangle$ of order n. Consider the set of statements $\mathcal{S} = \{(y_A, y_B, k_{AB}) \mid y_A, y_B, k_{AB} \in G\}$ and the truth function τ defined as follows: $\tau\big((y_A, y_B, k_{AB})\big) = 1$ if k_{AB} is the secret key resulting from exchanging the public keys y_A and y_B. Define $\mathcal{P}$ and ϕ, such that $\Pi = (\mathcal{S}, \mathcal{P}, \tau, \phi)$ is a complete and sound proof system. Justify your answer.

12.2 A Special Calculus for Propositional Logic ($\star$) *(8 Points)*

Consider the calculus consisting of the following four derivation rules:

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

a) Is the calculus sound? No justification is needed.

b) Formally derive $A \to C$ from $\{A \to B, B \to C\}$ in the calculus.

12.3 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 the 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.

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

12.5 CNF and DNF ($\star$)

a) Let $F = (\neg(A \to C)) \leftrightarrow (A \to B)$. Using the method of function tables, construct a formula in CNF that is equivalent to F and a formula in DNF that is equivalent to F.

b) Let $G = (A \wedge \neg B) \vee (\neg A \wedge (C \wedge D))$. Using the equivalences from Lemma 6.1, construct a formula in CNF that is equivalent to G. In each step write which equivalence you use.

12.6 Satisfiability ($\star\ \star$)

Let $n > 0$ be arbitrary, and let $F_1, \ldots, F_n$ and $G_1, \ldots, G_{n+1}$ be any formulas (of any logic). Prove that if the following formula H is satisfiable, then $G_1 \vee \cdots \vee G_{n+1}$ is also satisfiable.

$$H = (G_1 \vee F_1) \wedge \Big((G_2 \vee \neg F_1 \vee F_2) \wedge (G_3 \vee \neg F_2 \vee F_3) \wedge \cdots \wedge (G_n \vee \neg F_{n-1} \vee F_n) \Big) \wedge (G_{n+1} \vee \neg F_n)$$

Hint. Use Definition 6.10.

Due by 8. December 2020.
Exercise 12.2 is graded.