ETH Zürich, D-INFK
HS 2017, 27. November 2017

Prof. Ueli Maurer
Marta Mularczyk

# Diskrete Mathematik

# Exercise 11

### 11.1 Error-correcting codes ($\star\star$)

Let $C \subseteq G^n$ be an error-correcting code over a group $G$, with the additional assumption that $C$ with component-wise addition is a group. (In fact, many error-correcting codes have such property, for example the codes obtained by polynomial interpolation, described in Theorem 5.42.) Let the Hamming weight of a codeword in $C$ be defined as the number of positions different than $0$. Show that the minimum distance of $C$ is equal to the minimum Hamming weight among all codewords in $C \setminus \{0^n\}$.

### 11.2 Proof system ($\star\star$)

Let $e = 10$ and let $X$ be the set of natural numbers smaller than $10^9$. Consider the following statement: for a given set $A \subseteq X$ and value $t \in X$, there exists a subset $B$ of $A$ such that the sum of values in $B$, each increased or decreased by at most $e$, is equal to $t$.

For example, for $t = 159283701$ and $A = \{314, 159265358, 9, 79323, 84626433, 8327, 9502, 8841, 971693993, 751\}$, the statement is true: $159283701 = (159265358+1)+(9-3)+(9502-1)+(8841+2)$.

Let $\mathcal{S} = \mathcal{P} = \{0,1\}^*$. Propose functions $\tau$ and $\phi$, such that $\Pi = (\mathcal{S}, \mathcal{P}, \tau, \phi)$ is a complete and sound proof system for statements described above. (For an example of how to describe such functions, see Example 6.1 and Example 6.3.)

Write down the proof for $A$ and $t$ given in the example above. Your proof should be efficient for such cases: for the given $A$ and $t$ above, it should not be longer than $64$ bits.

### 11.3 Formulas of propositional logic *(11 Points)*

**a)** ($\star$) For the formulas $F$ and $G$, determine the set of all its models. Moreover, decide whether the formulas are equivalent or if one follows from the other.

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

*(5 Points)*

**b)** ($\star\star$) Prove that $F$ is a logical consequence of $G$ (i.e., $G \models F$) if and only if $F \wedge G$ is equivalent to $G$ (i.e., $F \wedge G \equiv G$). *(4 Points)*

**c)** ($\star\star$) Prove or disprove: two formulas of propositional logic that have no common atomic formulas are not equivalent. *(2 Points)*

### 11.4 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...

First of all, Homer wants to invite Abe. But Abe comes only under the condition that Barney comes as well. This in itself is not a problem, but if Barney comes, then Carl has to come as well. But when Carl comes, Disco Stu also certainly arrives. However, if both Barney and Disco Stu come to the party, then Carl surely does not come. Finally, Disco Stu comes only if 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)** ($\star\star$) Formalize the above conditions, using propositional formulas. Argue (intuitively) whether Homer should buy beer and donuts for the party or go strait to Moe's.

**b)** ($\star\star\star$) Use the following derivation rules, in order to formally derive the answer to Subtask a).

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

**Due on 4. December 2017.**
**Exercise 11.3 will be corrected.**