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

Prof. Ueli Maurer
Marta Mularczyk

Diskrete Mathematik

Solution 11

11.1 Error-correcting codes

For any two codewords $a, b \in C$, let $d(a, b)$ denote the Hamming distance between a and b and let $w(a)$ denote the Hamming weight of a.

Observe that for any $a \in C$, we have $w(a) = d(a, 0^n)$. Therefore, if there exists a non-zero codeword with Hamming weight k, then there also exists a pair of different codewords with Hamming distance k.

Moreover, for any $a, b \in C$, we have $d(a, b) = w(a \ominus b)$. Therefore, if there exists a pair of different codewords with Hamming distance k, then there also exists a non-zero codeword with Hamming weight k.

Thus, the set of Hamming weights of all non-zero codewords in C is equal to the set of Hamming distances between all pairs of different codewords in C. Hence, their minima are equal.

11.2 Proof system

We first define the function τ. Note that we can represent any number in X by a bitstring of length 30, since $\lceil \log_2(10^9) \rceil = 30$. Hence, any sequence of numbers in X can be represented by a bitstring s, such that $|s|$ is a multiple of 30. We say that a bitstring s encodes a set $A \subseteq X$ if $|s|$ is a multiple of 30 and if s represents a sequence of *unique* numbers in X (note that the empty string encodes the empty set).

Let now $\tau : \{0,1\}^* \to \{0,1\}$ be defined by $\tau(s) = 1$ if and only if the first 30 bits of s represent a number $t \in X$ and the rest of the bits encode a set $A \subseteq X$ for which there exists a $B \subseteq A$ such that the sum of values in B, each increased or decreased by at most e, is equal to t.

Let us now define the function ϕ. For given A and t, a proof will be a sequence of length $5|A|$. Namely, for each element of A, a proof will specify whether this element should be in B and, if so, what value should be added or subtracted from it. Such sequence can be represented by a bitstring in the following way.

For each element of the sequence, we will use a bitstring of length 5. A bitstring of length 5 can represent any number in $\{-15, \ldots, 15\}$ (for a given number a, the first bit is 0 if $a \geq 0$ and 1 if $a \leq 0$, while the remaining 4 bits represent $|a|$). Note that in such case 0 has two representations: 00000 and 10000. We let 10000 denote that a given element of A is not an element of B. The remaining bitstrings of length 5, uniquely representing numbers in $\{-10, \ldots, 10\}$, denote the value that should be added to a given element when computing the sum.

Hence, $\phi(s,p) = 1$ if and only if the following conditions hold:

1) s is a valid encoding of $t \in X$ and $A \subseteq X$ (which is checked the same way as in τ). Let $A = \{a_1, \ldots, a_l\}$.

2) p has length $|p| = 5l$ and represents a sequence $(e_1, \ldots, e_l)$, where $e_i \in \{-10, \ldots, 10\} \cup \{\perp\}$ for all i (by $\perp$ we denote the special symbol represented by 10000).

3) $t = \sum\limits_{\substack{i=1 \\ e_i \neq \perp}}^{l} a_i + e_i$.

With the construction steps given above, it is easy to verify that the resulting proof system $\Pi = (\mathcal{S}, \mathcal{P}, \tau, \phi)$ is sound and complete.
The example in the exercise has the following proof: the sequence to be encoded is $(\perp, 1, -3, \perp, \perp, \perp, -1, 2, \perp, \perp)$, which in the binary form is the following bitstring of length 50:

$$(10000, 00001, 10011, 10000, 10000, 10000, 10001, 00010, 10000, 10000).$$

11.3 Formulas of propositional logic

a) Consider the function table of $F = (\neg A \to B \wedge C) \leftrightarrow \neg C$:

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

(1 Point)

Each model for F must contain one of the following sets $\{\{A = 0, B = 0, C = 1\}, \{A = 1, B = 0, C = 0\}, \{A = 1, B = 1, C = 0\}\}$. *(1 Point)*

Consider now the function table of $G = (\neg A \wedge \neg B \wedge C) \vee \neg(\neg A \vee B \vee C)$:

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

(1 Point)

Each model for G must contain one of the following sets $\{\{A = 0, B = 0, C = 1\}, \{A = 1, B = 0, C = 0\}\}$.

(1 Point)

Since the set models for F contains the set of models for G, each model for G is also a model for F. Hence, F is a logical consequence of G. The formulas are not equivalent, since the sets are not the same. *(1 Point)*

b) $G \models F$ means that every truth assignment suitable for both F and G, which is a model for G, is also a model for F (see Definition 6.12). By Definition 6.16, this happens if and only if every such truth assignment is a model for $F \wedge G$. That is, $G \models F$ if and only if $G \models (F \wedge G)$. Moreover, we have $(F \wedge G) \models G$, because, by Definition 6.16, every truth assignment, which is a model for $F \wedge G$, is also a model for G. Hence, $G \models F$ if and only if $(F \wedge G) \models G$ and $G \models (F \wedge G)$, which, by Definition 6.13, means that $G \equiv (F \wedge G)$.

Warning: One generally has to prove that the implication holds in both directions: $G \models F$ implies $(F \wedge G) \equiv G$ and $(F \wedge G) \equiv G$ implies $G \models F$. In the proof above all steps hold in both directions.

c) The statement is false. In order to show this, consider the following counterexample. Let $F := A \vee \neg A$ and $G := B \vee \neg B$. Of course, F and G have no common atomic formulas. However, by Lemma 6.2 11), $A \vee \neg A \equiv \top \equiv B \vee \neg B$. *(2 Points)*

11.4 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:

$$A \rightarrow B \quad (1)$$
$$B \rightarrow C \quad (2)$$
$$C \rightarrow D \quad (3)$$
$$(B \wedge D) \rightarrow \neg C \quad (4)$$
$$D \rightarrow (A \vee B) \quad (5)$$

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:

$D \to B$	(6)	R_3 by (5) and (1)	$\neg D$	(10)	R_2 by (7) and (9)
$D \to C$	(7)	R_1 by (6) and (2)	$\neg C$	(11)	R_5 by (3) and (10)
$D \to (B \wedge D)$	(8)	R_4 by (6)	$\neg B$	(12)	R_5 by (2) and (11)
$D \to \neg C$	(9)	R_1 by (8) and (4)	$\neg A$	(13)	R_5 by (1) and (12)