Final Exam 2ITX0 Applied Logic

April 17, 2020, 18:00 - 21:00

This examination consists of 8 problems for which the indicated number of points can be obtained. The grade is the obtained number of points divided by 10. **You must explain all your answers.**

After finishing your work you have to take scans/pictures and upload them in the ANS system, no later than 21:30. Please use names showing the numbers of corresponding problems. Please also include your student pass (on an unwritten part of your paper) in one of your pictures.

On Friday, April 24, some additional skype meetings will be hold with a part of the participants of this examination; if you are selected you may expect a request for such a meeting by email on Friday, April 24, between 9:00 and 10:00.

Problem 1.

(10 points) Present a formula in proposition logic on ten boolean variables $p_1, p_2, \ldots, p_{10}$, in logic notation, expressing that exactly one of the ten variables $p_1, p_2, \ldots, p_{10}$ has the value false. Here you may use the standard notation $\bigwedge_{P(i,j)}$ for conjunction over all i, j satisfying some property $P(i, j)$.

Problem 2.

(15 points) Consider the CNF consisting of the following eight clauses

(1)	$\neg p \vee t$	(5)	$p \vee \neg r \vee s$
(2)	$\neg q \vee r$	(6)	$\neg q \vee s \vee \neg t$
(3)	$p \vee q \vee s$	(7)	$r \vee \neg s \vee \neg t$
(4)	$\neg r \vee \neg s$	(8)	$\neg p \vee q \vee s$

Establish whether this CNF is satisfiable by DPLL; start by case analysis on r. Indicate for every step the number of the clause that is used. If the formula is satisfiable, give the resulting satisfying assignment.

Problem 3.

(10 points) Give the Tseitin transformation of the formula

$$(p \to q) \vee (\neg r \to (p \wedge q));$$

make clear what are the names of the subformulas that you introduce.

Problem 4.

Consider the following memoryless information source W (weather).

message	*sunny*	*overcast*	*rain*	*hail*	*snow*
probability	0.3	0.3	0.2	0.1	0.1

The following table shows an encoding E_1 of source W.

message	encoding
sunny	0
overcast	10
rain	110
hail	1110
snow	1111

(a) (2 points)

How many bits per message are needed in a *fixed-length* encoding of this information source?

(b) (3 points)

Encoding E_1 is not a fixed-length encoding. Why can every sequence of encoded messages be uniquely decoded anyways? Using E_1, you receive 110001110; what message sequence was sent?

(c) (3 points)

How many bits per message does encoding E_1 use *on average* when encoding source W?

(d) (4 points)

As you know, Huffman's algorithm offers some freedom, and it can produce many different encodings that all have the same efficiency. Can the encoding under **c** have resulted from applying Huffman's algorithm? What would the average number of bits per message be under a Huffman encoding?

(e) (3 points)

Is it possible to find an encoding that, *on average*, uses strictly *less* than 2.2 bits per message?

The following binary logarithms are given:

p	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9
$-\log_2 p$	3.32	2.32	1.74	1.32	1.00	0.737	0.515	0.322	0.152

Problem 5.

Consider the following binary encoding for eight messages.

message	encoding
000	0000000
001	1101001
010	1100110
011	0001111
100	1011010
101	0110011
110	0111100
111	1010101

(a) (2 points)

What is the rate of this encoding?

(b) (4 points)

What is the smallest positive number b_d of bit errors that is *not detectable* when using this encoding? Also give a concrete example where b_d bit errors are not detectable.

(c) (4 points)

What is the smallest positive number b_c of bit errors that is *not correctable with certainty* when using this encoding? Also give a concrete example where b_c bit errors are not correctable with certainty.

Problem 6.

You have a 24-bit security key $b_1 b_2 \dots b_{24}$. To communicate it securely, you want give each of four couriers some information (a 'share') such that:

- From the information of the four couriers together the recipient can reconstruct the security key.
- Intercepting three or fewer couriers, an enemy can do no better than trying all possible 24-bit keys, that is, the enemy has not obtained any information about the security key.

(a) (5 points)

Explain why giving courier i ($1 \leq i \leq 4$) bits $b_{6i-5} b_{6i-4} \dots b_{6i}$ is not a good idea.

(b) (5 points)

Explain how to give out shares securely, and why that works.

Problem 7.

(10 points) Compute

$$wp(c := a;\ \text{if } a < b \text{ then } \langle b := a; c := b\rangle, a + b = c).$$

Problem 8.

For a given value $k \geq 0$ we want to compute 2^k, using the invariant $b = 2^{k-a}$. The following incomplete Hoare triple is given:

$\{k \geq 0\}$
a := ?; b := ?;
while $a \neq 0$ do
$\quad\quad \langle a := a - 1;\ b :=?\rangle$
$\{b = 2^k\}$

(**a**) (5 points)

Replace the three question marks '?' by expressions only using $0, 1, a, b, k, +$ such that the program is correct with respect to the given pre- and postcondition.

(**b**) (15 points)

Give the full proof (of partial correctness) using the given invariant and rules for wp.