Final Exam 2ITX0 Applied Logic

April 15, 2021, 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.**

Problem 1.

(5 points) Three propositional formulas A, B, C are given for which we want to prove that if both A and B hold, then also C holds. Explain how this can be done by a SAT solver, in particular, give the formula on which the SAT solver has to be applied.

Problem 2.

Consider the CNF consisting of the following six clauses

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

(a) (10 points) Prove that this CNF is unsatisfiable by doing resolution. Indicate for every step the number of the clause that is used.

(b) (10 points) Prove that this CNF is unsatisfiable by DPLL; start by case analysis on p. Indicate for every step the number of the clause that is used.

Problem 3.

(10 points) Determine the number of clauses that occur in the Tseitin transformation of the formula

$$(r \leftrightarrow t) \wedge ((p \rightarrow \neg q) \vee ((s \leftrightarrow u) \vee (r \wedge t))).$$

Only the number (with motivation and calculation) is sufficient, you do not need to give the resulting CNF.

Problem 4.

Consider the following memoryless information source M (motion).

message	*north*	*east*	*south*	*west*	*halted*
probability	0.3	0.1	0.3	0.1	0.2

The following table shows an encoding E_1 of source M.

message	encoding
north	000
east	001
south	010
west	011
halted	1

(a) (1 point) How many bits per message are needed in a *fixed-length* encoding of this information source?

(b) (2 points) Using E_1, you receive 01011011100 . . . (the remaining bits are not yet available). What is the information you can extract from the received bits about the message sequence that was sent?

(c) (2 points) Encoding E_1 is not a fixed-length encoding. Why can every sequence of encoded messages be uniquely decoded anyways?

(d) (2 points) How many bits per message does encoding E_1 use *on average* when encoding source M?

(e) (4 points) What would the average number of bits per message be under a Huffman encoding? Show how you obtained this encoding (clearly indicate the steps) and its average number of bits per message.

(f) (2 points) Estimate the least number of bits per message that a lossless encoding needs, *on average*. Motivate your answer.

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.

We want to transmit k-bit messages, for some fixed integer $k \geq 1$, over a (noisy) binary symmetric channel. Consider message $s = s_1 s_2 \dots s_k$ and define (parity bit) $p = (s_1 + s_2 + \cdots + s_k) \bmod 2$; that is $p = 0$ if s has an even number of 1's, and $p = 1$ if s has an odd number of 1's. We now encode message s as $sssppp$; that is, three copies of s followed by two copies of p.

(a) (1 point) Write down the four codewords for $k = 2$

(b) (1 point) What is the rate of this encoding for $k = 2$?

(c) (1 point) What is the rate of this encoding in general, as function of k?

(d) (1 point) For $k = 2$, you receive the following 16 bits (spaces are for readability only)

11 11 10 11 11 10 11 10

What is the most likely message that was sent?

(e) (4 points) What is the smallest positive number b_d of bit errors per message that is *not detectable* when using this encoding? Explain your answer. Also give a concrete example where b_d bit errors are not detectable.

(f) (4 points) What is the smallest positive number b_c of bit errors per message that is *not correctable with certainty* when using this encoding? Explain your answer. Also give a concrete example where b_c bit errors are not correctable with certainty.

Problem 6.

You have a 64-bit security key $b_1 b_2 \dots b_{64}$ for your password file. As a backup, you want to distribute the information in that key among four friends. Each friend receives a so-called 'share' in the form of a bit sequence, such that:

- From the shares of the four friends together, the security key can be reconstructed.
- With three or fewer of the shares, an enemy can do no better than trying all possible 64-bit keys, that is, no information about the security key can be obtained.

(a) (5 points) Explain quantitatively why giving friend i ($1 \leq i \leq 4$) bits $b_{16(i-1)+1} b_{16(i-1)+2} \dots b_{16(i-1)+16}$ of the key is not a good idea.

(b) (5 points) Explain how to create shares securely, and why that works.

Problem 7.

(10 points) Compute

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

Problem 8.

We want to prove partial correctness of

$$\begin{array}{l}\{a = A \wedge b = B \wedge c = C \wedge a \leq c\}\\ \text{while } a \neq c \text{ do}\\ \qquad \langle b := b + b;\ a := a + 1\rangle\\ \{b = B * 2^{C-A}\}\end{array}$$

a. (5 points) Give the involved invariant.
b. (15 points) Give the full proof using this invariant and rules for wp.