Final Exam 2ITX0 Applied Logic

January 23, 2020, 9:00 - 12:00

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. The problems have to be answered on the provided ANS answer forms.

Problem 1.

(5p) Two propositional formulas A, B are given for which we want to prove B always implies A, that is, $B \to A$ is a tautology. 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 seven clauses

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

(5p) **a.** Is a resolution step possible on (1) and (5)? If so, give the resulting clause.

(15p) **b.** Establish whether this CNF is satisfiable by DPLL; start by case analysis on p. Indicate for every step the number of the clause that is used. If the formula is satisfiable, give the resulting satisfying assignment.

Problem 3.

(10p) The Tseitin transformation of the formula

$$(r \to t) \leftrightarrow ((p \land \neg q) \lor (r \to (s \land t)))$$

is a CNF. Establish the number of clauses that it has; motivate your answer.

Problem 4.

An information source produces symbols from the set $\{ Y, Z \}$, independently distributed with probabilities $\Pr(Y) = 0.3$ and $\Pr(Z) = 0.7$.

(3p) **a.** Calculate the entropy of this source, measured in bits. Show your calculation, and round your answer to two decimal places.

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

(5p) **b.** Using Huffman's algorithm, construct a prefix-free binary encoding for this source that encodes *triplets* of symbols (see table below). Give the encoding tree and label the nodes with their probability and a sequence number in the order of creation.

triplet	YYY	YYZ	YZY	YZZ	ZYY	ZYZ	ZZY	ZZZ
probability	0.027	0.063	0.063	0.147	0.063	0.147	0.147	0.343

(3p) **c.** What is the average number of bits per symbol of your encoding in 4.b? Show your calculation.

(2p) **d.** Why must that number of 4.c be ≤ 1?

(2p) **e.** How does the number of 4.c relate to the entropy of 4.a and why is that so?

Problem 5.

Consider the decimal code that encodes 4 digits $s = s_1 s_2 s_3 s_4$ into the 8-digit codeword sp with 4 check digits $p = p_1 p_2 p_3 p_4$ given by $s_1 \oplus s_2 \oplus p_1 = 0$, $s_3 \oplus s_4 \oplus p_2 = 0$, $s_1 \oplus s_3 \oplus p_3 = 0$, $s_2 \oplus s_4 \oplus p_4 = 0$, where $\oplus$ is addition modulo 10 (retaining only the rightmost digit of the regular addition). Thus, message 4575 is encoded as 45751890. This is best viewed in a tabular form:

$$
\begin{array}{c|c||c}
s_1 & s_2 & p_1 \\
\hline
s_3 & s_4 & p_2 \\
\hline\hline
p_3 & p_4 &
\end{array}
\qquad
\begin{array}{c|c||c}
4 & 5 & 1 \\
\hline
7 & 5 & 8 \\
\hline\hline
9 & 0 &
\end{array}
$$

(5p) **a.** What is the smallest positive number of digit errors that is *not detectable* when using this encoding? Also give an example.

(5p) **b.** Using this encoding, word 38519724 was received. Assuming that at most one digit was in error, which (4-digit) message was sent?

Problem 6.

You have a 6-digit decimal security code $d_1d_2d_3d_4d_5d_6$. As a backup, you want give each of three friends some information (a 'share') such that:

- From the information of the three friends together you (and they) can reconstruct the security code.
- No single friend, or two friends together, can do better than trying all possible 6-digit codes.

(5p) **a.** Explain why giving friend i ($1 \leq i \leq 3$) digits d_{2i-1} and d_{2i} is not a good idea.

(5p) **b.** Explain how to give out shares securely, and why that works.

Problem 7.

(10p) Prove

$$\{a > 0\}\ a := b;\ \text{if } a < b \text{ then } b := a \text{ else } a := 2b\ \{a = 2b\}.$$

Problem 8.

We want to prove partial correctness of

$$\begin{array}{l} \{a = 0 \wedge b = B \wedge c \geq 0\} \\ \text{while } a \neq c \text{ do} \\ \qquad \langle a := a + 1;\ b := b + 2 \rangle \\ \{b = 2c + B\} \end{array}$$

(5p) **a.** Give the involved invariant.

(15p) **b.** Give the full proof using this invariant and rules for wp.