COMP 60332

Two hours

Examination definition sheet is available at the back of the examination.

UNIVERSITY OF MANCHESTER
SCHOOL OF COMPUTER SCIENCE

Automated Reasoning and Verification

Date: Wednesday 30th May 2018

Time: 09:45 - 11:45

Please answer any THREE Questions from the FOUR Questions provided.

Use a SEPARATE answerbook for each QUESTION.

Each Question is worth 20 marks.

This is a CLOSED book examination

The use of electronic calculators is NOT permitted

[PTO]

Answer any *three* of the four questions

Note that a definition sheet is included at the back of the exam paper.

1. (Orderings, CNF transformation, propositional resolution, formalisation in propositional logic)

   (a) i. Define when an ordering $(X, \succ)$ is well-founded. (1 mark)

   ii. Consider an ordering $a \succ b \succ c$ on a set $X = \{a, b, c\}$ and its multi-set extension $\succ_{\text{mul}}$. Determine how the following multi-sets are compared in $\succ_{\text{mul}}$:

   $$\{c, c, b, b\};\ \{a, c\};\ \{a, a\};\ \{a, b, c\};\ \{a, b\};\ \emptyset$$

   (1 mark)

   iii. Write down two main properties of orderings preserved by the multi-set extensions. (2 marks)

   iv. Does the following statement hold true for every well-founded ordering: "There are only finite number of elements smaller than any given element."? Explain your answer. (2 marks)

   (b) What are two main differences between structural CNF transformation and syntactic CNF transformation (based on equivalence rules)? (2 marks)

   (c) Propositional resolution.

   i. Write down inference rules of the propositional resolution calculus ($\mathbb{BR}$). (2 marks)

   ii. Define when an inference rule is sound. (1 mark)

   iii. Show that the propositional resolution calculus is sound. (3 marks)

   (d) Consider n workers and k jobs, assume $n > 0, k > 0$. Write down a propositional formula which is satisfiable if and only if it is possible to assign jobs to workers such that the following conditions are satisfied: i) all jobs are assigned to workers, ii) each worker is assigned at most one job, iii) a job is assigned to at most two workers. (6 marks)

2. (Representing arithmetic relations using propositional logic, DPLL, LTL, 1-induction)

   (a) Consider non-negative integers of a bit-width n in binary notation. Represent the following relations using propositional logic:

   i. $X \neq 2$
   ii. $X \geq 2$
   iii. $X \neq Y$
   iv. $2X = Y$

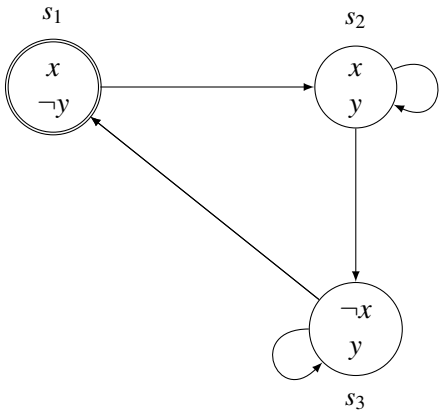
   In the last problem the relation is assumed to be false when an overflow occurs. (5 marks)

   (b) i) Define the Horn fragment of propositional logic. Which DPLL rule alone is a decision procedure for the Horn fragment ? (2 marks)

   ii) Consider a set of clauses over n variables. How many steps of unit propagation are possible at most, without applications of other rules of the DPLL algorithm? Briefly explain your answer. (2 marks)

   iii) What are two main optimisations applied to the DPLL algorithm. Briefly describe them. (3 marks)

   (c) Consider a transition system with the following state transition graph.



   Which of the following formulas are true on some path starting from the initial state? If a formula is true on a path draw one such path.

   i. $\Diamond \Box x$
   ii. $\Box(y \rightarrow \Diamond \neg y)$
   iii. $x \, \mathbf{U} \, \Box \neg x$
   iv. $\Box \Diamond y \wedge \Box \Diamond \neg y$ (4 marks)

   (d) Consider a transition system $\mathbb{S}$ represented by propositional formulas $I(\bar{x}), \mathcal{T}(\bar{x}, \bar{x}')$. Consider a set of unsafe states represented by a propositional formula $Unsafe(\bar{x})$ and safe states by $Safe(\bar{x}) \equiv \neg Unsafe(\bar{x})$. Write down formulas representing i) the base case and ii) the inductive case of the 1-induction algorithm for checking that the unsafe states are not reachable in $\mathbb{S}$. (4 marks)

3. (Translation from English to first-order logic, semantic equivalences, unification, validity & resolution, Herbrand interpretations)

   (a) Let G be the following first-order formula.

$$\forall x\big[\big(B(x) \wedge W(jk,x)\big) \rightarrow \forall z\big(F(z,jk) \rightarrow R(z,x)\big)\big]$$

   Suppose the non-logical symbols in the formula have the following interpretation.

$B(x)$	means that x is a book
$W(x,y)$	means that x writes y
$F(x,y)$	means that x is a fan of y
$R(x,y)$	means that x reads y
jk	represents JK Rowling (the author of the Harry Potter books)

   i) Express the formula G in idiomatic English without using variables. (2 marks)

   ii) Transform the negation $\neg G$ of the formula into negation normal form (i.e., push negation inwards as far as possible using semantic equivalences of first-order logic). (3 marks)

   iii) Express the formula obtained in 3(a)ii in idiomatic English without using variables. (1 mark)

   (b) Use our unification algorithm based on the $\Rightarrow_U$-rules to unify the following two atomic formulae, if that is possible. Give the most general unifier, if there is one. (Note that the $\Rightarrow_U$-rules are given at the end of the exam paper.)

$$P(x,g(f(a)),f(x)) \qquad P(f(a),y,y)$$

   x, y denote variables. (4 marks)

   (c) Use resolution to show: (6 marks)

   i) $\forall x P(x,f(x)) \rightarrow \forall x \exists y P(x,y)$ is valid, but

   ii) $\forall x \exists y P(x,y) \rightarrow \forall x P(x,f(x))$ is not valid.

   (d) For each of the following statements state whether it is true or false. Give an explanation if the statement is true. Give a counter-example if the statement is false. (4 marks)

   i) Not every Herbrand model of $P(f(f(a)))$ is a model of the set

$$N = \{\ P(f(a)) \wedge \neg P(a),\ \neg P(x) \vee P(f(f(x)))\ \}.$$

   ii) The following set N has infinitely many Herbrand models.

$$N = \{\ P(b),\ \neg P(x) \vee \neg P(g(x)\ \}$$

4. (Bookwork, orderings, model construction, ordered resolution, redundancy)

   (a) Give a brief explanation of **two** of the following. (4 marks)

   i) term
   ii) Skolemisation
   iii) selection function
   iv) exception clause

   (b) Let N be the following set of ground clauses.

$$
\begin{array}{ll}
1. & A_1 \vee A_3 \\
2. & \neg A_4 \vee A_5 \vee A_5 \\
3. & A_4 \vee \neg A_1 \\
4. & A_1 \vee A_5 \vee A_4 \vee A_1 \\
5. & \neg A_2 \vee A_5
\end{array}
$$

   Assume the ordering on the atoms is defined by

$$A_2 \succ A_5 \succ A_4 \succ A_1 \succ A_3.$$

   i) Sort the clauses in N with respect to the extension $\succ_C$ of the ordering $\succ$ to clauses. (Note that $\succ_C$ is defined at the end of the exam paper.) (2 marks)

   ii) Construct the candidate model $I_N^{\succ}$ as described in lectures for the set N above (and nothing else). (3 marks)

   iii) Is the obtained candidate model $I_N^{\succ}$ a model of N? Say why, or why not. (1 mark)

   (c) Let $\succ$ be a total and well-founded ordering on ground atoms such that:

   $(*)$ if the atom A contains more symbols than B, then $A \succ B$.

   Let N be the following set of clauses.

$$
\begin{array}{ll}
1. & P(x_1,x_2) \vee Q(x_1,x_1,x_2) \vee S(x_1) \\
2. & \neg Q(x_3,x_3,x_4) \vee S(x_4) \\
3. & \neg Q(x_5,x_6,x_6) \vee \neg S(x_5) \\
4. & P(x_7,x_7) \vee \neg R \vee \neg Q(x_7,x_7,x_8) \\
5. & \neg P(x_9, f(b))
\end{array}
$$

   i) For each clause state which literals are strictly maximal in it relative to the ordering $\succ$ given in $(*)$. (2 marks)

   ii) Use ordered resolution $Res^{\succ}$, where $\succ$ is an atom ordering defined in $(*)$ (no literal is selected), to either derive the empty clause or obtain a saturated set of clauses. In your derivation indicate the maximal literals in every clause and justify each step. (5 marks)

   iii) In your derivation also indicate which of the clauses (if any) are redundant in the derivation, and why. (3 marks)

Examination definition sheet

LTL semantics.

Let $\pi = s_0, s_1, s_2 \ldots$ be a sequence of states and F be an LTL formula. F is true on π, denoted by $\pi \models F$, defined by induction on F as follows. For all $i = 0, 1, \ldots$ denote by π_i the sequence of states $s_i, s_{i+1}, s_{i+2} \ldots$ (note that $\pi_0 = \pi$).

- $\pi \models \top$ and $\pi \not\models \bot$.
- $\pi \models p$ if $s_0 \models p$.
- $\pi \models F_1 \wedge \ldots \wedge F_n$ if for all $j = 1, \ldots, n$ we have $\pi \models F_j$;
- $\pi \models F_1 \vee \ldots \vee F_n$ if for some $j = 1, \ldots, n$ we have $\pi \models F_j$.
- $\pi \models \neg F$ if $\pi \not\models F$.
- $\pi \models F \rightarrow G$ if either $\pi \not\models F$ or $\pi \models G$;
- $\pi \models F \leftrightarrow G$ if either both $\pi \not\models F$ and $\pi \not\models G$ or both $\pi \models F$ and $\pi \models G$.
- $\pi \models \bigcirc F$ if $\pi_1 \models F$;
- $\pi \models \Diamond F$ if for some $i = 0, 1, \ldots$ we have $\pi_i \models F$;
- $\pi \models \Box F$ if for all $i = 0, 1, \ldots$ we have $\pi_i \models F$.
- $\pi \models F \,\mathbf{U}\, G$ if for some $k = 0, 1, \ldots$ we have $\pi_k \models G$ and $\pi_0 \models F, \ldots, \pi_{k-1} \models F$.

Two LTL formulas F and G are called equivalent, denoted $F \equiv G$, if for every path π we have $\pi \models F$ if and only if $\pi \models G$.

Herbrand models. The *Herbrand universe* T_Σ (over Σ) is the set of all ground terms over Σ.

A *Herbrand interpretation* I (over Σ) is a set of ground atoms over Σ.

Truth in I of *ground formulae* is defined inductively by:

$$\begin{aligned} I &\models \top && I \not\models \bot \\ I &\models A \text{ iff } A \in I, \text{ for any ground atom } A \\ I &\models \neg F \text{ iff } I \not\models F \\ I &\models F \wedge G \text{ iff } I \models F \text{ and } I \models G \\ I &\models F \vee G \text{ iff } I \models F \text{ or } I \models G \end{aligned}$$

Truth in I of any *quantifier-free formula* F with free variables $x_1, \ldots, x_n$ is defined by:

$$I \models F(x_1, \ldots, x_n) \text{ iff } I \models F(t_1, \ldots, t_n), \text{ for every } t_i \in \mathrm{T}_\Sigma$$

Truth in I of any *set N of clauses* is defined by:

$$I \models N \quad \text{iff} \quad I \models C, \text{ for each } C \in N$$

Construction of candidate models. Let $N, \succ$ be given.

For all ground clauses C over the given signature, the sets I_C and Δ_C are inductively defined with respect to the clause ordering $\succ$ by:

$$I_C := \bigcup_{C \succ D} \Delta_D$$

$$\Delta_C := \begin{cases} \{A\}, & \text{if } C \in N,\ C = C' \vee A,\ A \succ C' \text{ and} \\ & I_C \not\models C \\ \emptyset, & \text{otherwise} \end{cases}$$

We say that C *produces* A, if $\Delta_C = \{A\}$.

The *candidate model* for N (wrt. $\succ$) is given as

$$I_N^{\succ} := \bigcup_{C \in N} \Delta_C.$$

We also simply write I_N, or I, for $I_N^{\succ}$, if $\succ$ is either irrelevant or known from the context.

Orderings. Let $(X, \succ)$ be an ordering. The *multi-set extension* $\succ_{\text{mul}}$ of $\succ$ to (finite) multi-sets over X is defined by

$$\begin{aligned} S_1 \succ_{\text{mul}} S_2 \text{ iff } & S_1 \neq S_2 \text{ and} \\ & \forall x \in X, \text{ if } S_2(x) > S_1(x) \text{ then} \\ & \quad \exists y \in X : \; y \succ x \text{ and } S_1(y) > S_2(y) \end{aligned}$$

Suppose $\succ$ is a total and well-founded ordering on ground atoms. $\succ_L$ denotes the *ordering on ground literals* and is defined by:

$$\begin{array}{lll} [\neg]A & \succ_L & [\neg]B, \quad \text{if } A \succ B \\ \neg A & \succ_L & A \end{array}$$

$\succ_C$ denotes the *ordering on ground clauses* and is defined by the multi-set extension of $\succ_L$, i.e. $\succ_C = (\succ_L)_{\text{mul}}$.

Maximal literals. Let $\succ$ be a total and well-founded ordering on ground atoms.

A ground literal L is called *[strictly] maximal* wrt. a ground clause C iff

$$\text{for all } L' \text{ in } C: \quad L \succeq L' \quad [L \succ L'].$$

A non-ground literal L is *[strictly] maximal* wrt. a (ground or non-ground) clause C iff there exists a ground substitution σ such that

$$\text{for all } L' \text{ in } C: \quad L\sigma \succeq L'\sigma \quad [L\sigma \succ L'\sigma].$$

If L is [strictly] maximal wrt. a clause C then we say that L is *[strictly] maximal in* $L \vee C$.

The $\Rightarrow_U$-rules of the unification algorithm.

Orientation:	$t \doteq x, E$	$\Rightarrow_U$	$x \doteq t, E$ if $t \notin \mathcal{X}$
Trivial:	$t \doteq t, E$	$\Rightarrow_U$	E
Disagreement/Clash:	$f(\ldots) \doteq g(\ldots), E$	$\Rightarrow_U$	$\bot$
Decomposition:	$f(s_1, \ldots, s_n) \doteq f(t_1, \ldots, t_n), E$	$\Rightarrow_U$	$s_1 \doteq t_1, \ldots, s_n \doteq t_n, E$
Occur-check:	$x \doteq t, E$	$\Rightarrow_U$	$\bot$ if $x \in var(t), x \neq t$
Substitution:	$x \doteq t, E$	$\Rightarrow_U$	$x \doteq t, E\{x/t\}$ if $x \in var(E), x \notin var(t)$

Ordered resolution with selection calculus $Res^{\succ}_{S}$. Let $\succ$ be an atom ordering and S a selection function.

Ordered resolution with selection rule:

$$\frac{C \vee A \qquad \neg B \vee D}{(C \vee D)\sigma}$$

provided $\sigma = \mathrm{mgu}(A, B)$ and

(i) $A\sigma$ strictly maximal wrt. $C\sigma$;

(ii) nothing is selected in C by S;

(iii) either $\neg B$ is selected,
or else nothing is selected in $\neg B \vee D$ and $\neg B\sigma$ is maximal wrt. $D\sigma$.

Ordered factoring rule:

$$\frac{C \vee A \vee B}{(C \vee A)\sigma}$$

provided $\sigma = \mathrm{mgu}(A, B)$ and

(i) $A\sigma$ is maximal wrt. $C\sigma$ and

(ii) nothing is selected in C.

Redundancy. Let N be a set of ground clauses and C a ground clause. C is called *redundant* wrt. N, if there exist $C_1, \ldots, C_n \in N$, $n \geq 0$, such that

(i) all $C_i \prec C$, and

(ii) $C_1, \ldots, C_n \models C$.

A general clause is *redundant* wrt. N if each ground instance $C\sigma$ of C either belongs to $G_\Sigma(N)$ or is redundant wrt. $G_\Sigma(N)$.

N is called *saturated up to redundancy* (wrt. $Res^{\succ}_{S}$) iff every conclusion of an $Res^{\succ}_{S}$-inference with non-redundant clauses in N is in N or is redundant (i.e.

$$Res^{\succ}_{S}(N \setminus Red(N)) \subseteq N \cup Red(N),$$

where $Red(N)$ denotes the set of clauses redundant wrt. N).

END OF EXAMINATION