COMP60332

Two hours

Examination definition sheet is available on pages 6 to 10 of this examination paper.

UNIVERSITY OF MANCHESTER
SCHOOL OF COMPUTER SCIENCE

Automated Reasoning and Verification

Date: Friday 27th May 2016

Time: 14:00 - 16:00

Please answer any THREE Questions from the FOUR Questions provided

Use a SEPARATE answerbook for each QUESTION.

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, structural CNF transformation, propositional redundancy elimination)

   (a) i. Define when an ordering is well-founded. (2 marks)

   ii. Write down two main properties preserved by the lexicographic combination of orderings. (2 marks)

   iii. Consider natural numbers $(\mathbb{N}, >)$. How the following triples are related in the lexicographic combination $>^3$? (2 marks)

   $$(3,10,5),\ (4,2,1),\ (0,1,5),\ (1,1,0)$$

   iv. How many triples are smaller than $(0,1,0)$ in $>^3$? (1 mark)

   v. Is $>^3$ a well-founded ordering ? Explain your answer. (1 mark)

   (b) Transform the following formula $(p \to \neg q) \to (\neg p \wedge q)$ into clausal normal form using the structural clausal form transformation. (6 marks)

   (c) Explain how validity and equivalence of propositional formulas can be expressed in terms of satisfiability. (2 marks)

   (d) Briefly describe propositional tautology elimination and subsumption elimination. Use examples to illustrate these notions. (4 marks)

2. (Formalisation in propositional logic, DPLL, LTL)

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

   i. $X = 1$
   ii. $X \geq 2$
   iii. $X \neq Y$

   (6 marks)

   (b) Check whether the following set of clauses is satisfiable using the propositional DPLL procedure. Make literal decisions in the following sequence:

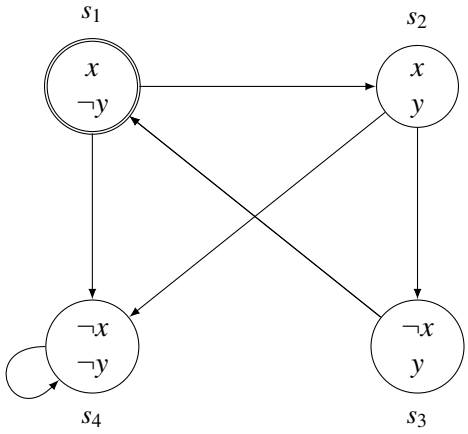
   $$\neg t^d \ldots \neg s^d \ldots v^d \ldots$$

   Apply backjumping (BJ) whenever possible. Explain the backjumping step and how a lemma can be generated based on the conflict analysis.

$\|\|$
$s \vee \neg q \vee u$
$t \vee q$
$\neg v \vee \neg q \vee m$
$t \vee \neg m \vee \neg v$

   (10 marks)

   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. $\Diamond(y \wedge \bigcirc \neg y)$
   ii. $\Diamond \Box(x \wedge y)$
   iii. $\Box(x \rightarrow \neg y)$
   iv. $\Box\Diamond y \wedge \Box\Diamond \neg y$

   (4 marks)

3. (Translation from English to first-order logic, transform to clause form, unification, validity and resolution, Herbrand interpretations)

   (a) Let $P(x)$ represent 'x is at the party',
   $F(x,y)$ represent 'x is a friend of y'
   Express each of the following sentences as a first-order formula. (4 marks)

   i. Everyone at the party has a friend at the party.

   ii. No one at the party is friends with everyone at the party.

   (b) The transformation of a first-order formula into clausal form as described in class involves four steps.

   i. State what are the four steps and in which order are they applied. (2 marks)

   ii. The result of the transformation to clausal form is not unique. State **one** reason why, and state why it does not matter that the clausal form is unique. (2 marks)

   (c) Use the resolution method to determine whether the following formula is valid or not valid: (3 marks)

$$\forall x \exists y P(x,y) \rightarrow \forall x P(x, f(x)).$$

   (d) Apply the unification algorithm based on the $\Rightarrow_U$-rules to unify the following two atoms. In each step say which rules are applied and apply the rules exhaustively. Give the most general unifier and the unified atom, if they exists.

$$Q(x, g(y), h(z)) \qquad Q(y, g(z), h(x))$$

   Here, x, y, z denote variables.
   Note that the $\Rightarrow_U$-rules are given at the end of the exam paper. (5 marks)

   (e) Let the signature Σ consist of two constants a and b, and one binary predicate symbol R. Consider the folowing Herbrand interpretation:

$$I = \{R(a,a), R(a,b)\}.$$

   Determine if the following clauses hold in I. Briefly explain your answers. (4 marks)

   i. $I \models \neg R(a,b) \vee R(a,a)$

   ii. $I \models \neg R(b,a) \vee R(b,b)$

   iii. $I \models \neg R(x,y) \vee R(y,y)$

   iv. $I \models \neg R(x,y) \vee R(x,x)$

4. (Model construction, orderings, ordered resolution with selection, redundancy)

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

   1. $A_2 \vee A_3 \vee A_2$
   2. $\neg A_4 \vee A_0 \vee A_3 \vee A_1$
   3. A_0
   4. $\neg A_0 \vee A_3 \vee A_4$
   5. $A_1 \vee A_2$
   6. $\neg A_3 \vee A_0$

   i. Let the ordering on atoms be defined by $A_1 \succ A_2 \succ A_4 \succ A_3 \succ A_0$. Sort the clauses in N with respect to $\succ_C$. (2 marks)

   ii. Construct the candidate model $I_N^{\succ}$ for N as described in lectures. (4 marks)

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

   (b) (Ordered resolution, redundancy) Let $\succ$ be a total and well-founded ordering on ground atoms such that

   $$Q(1,1) \succ Q(1,0) \succ Q(0,1) \succ Q(0,0) \succ H(1) \succ H(0) \succ P.$$

   0 and 1 are regarded as constants. Let N be the following set of clauses.

   1. $\neg H(0)$
   2. $H(1)$
   3. $P \vee Q(x,y) \vee H(x)$
   4. $\neg P \vee Q(x,y) \vee \neg H(x)$
   5. $\neg Q(x,y) \vee H(x) \vee H(y)$

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

   ii. Use ordered resolution $Res^{\succ}$ with redundancy elimination, where $\succ$ is an atom ordering defined as above (no literal is selected), to either derive the empty clause or obtain a set of clauses that is saturated up to redundancy.

   A. In your derivation indicate the maximal literals in every clause and justify each step. (5 marks)

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

   (c) Give **one** advantage of ordered resolution over unordered resolution (i.e., no ordering and also no selection function is used). Briefly illustrate your answer by using the derivation you gave in answer the previous question 4(b)ii. (You may, if you wish, give a different, small example to illustrate your answer.) (3 marks)

Examination definition sheet

Structural transformation. Lemma: $F[G]$ is satisfiable $\Leftrightarrow F[n_G] \wedge (n_G \leftrightarrow G)$ is satisfiable. provided n_G is a (fresh) propositional variable not occurring in $F[G]$. n_G can be seen as a name for G. *Structural CNF Transformation:* introduce names recursively for every non-literal subformula in the original formula.

DPLL rules.

Unit Propagate (UP):

$$U \parallel S, \;\; \Rightarrow_{\mathrm{UP}} \;\; U\ell \parallel S \qquad \text{if} \begin{cases} I_U \models \neg C, \text{ for } C \vee \ell \in S \\ \ell \text{ is undefined in } I_U \end{cases}$$

Decide (D):

$$U \parallel S \;\; \Rightarrow_D \;\; U\ell^d \parallel S \qquad \text{if} \begin{cases} \ell \text{ is undefined in } I_U \end{cases}$$

Backtrack (B)

$$U\ell^d V \parallel S \;\; \Rightarrow_B \;\; U\overline{\ell} \parallel S \qquad \text{if} \begin{cases} I_{U\ell^d V} \models \neg C, \text{ for } C \in S, \\ V \text{ contains no decision literals} \end{cases}$$

Unsat ($\bot$)

$$U \parallel S \;\; \Rightarrow_\bot \;\; \bot \parallel S \qquad \text{if} \begin{cases} I_U \models \neg C, \text{ for } C \in S, \\ U \text{ contains no decision literals} \end{cases}$$

Backjumping (BJ)

$$U\ell^d V \parallel S \;\; \Rightarrow_{BJ} \;\; Ue \parallel S \qquad \text{if} \begin{cases} I_{U\ell^d V} \models \neg C, \text{ for } C \in S, \\ U \wedge S \models e, \\ \text{e is undefined in } U. \end{cases}$$

Lemma Learning (LL):

$$U \parallel S \;\; \Rightarrow_{LL} \;\; U \parallel S \cup \{C\} \qquad \text{if} \begin{cases} S \models C \\ C \text{ is set-reduced} \end{cases}$$

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