6.0/4.0 VU Formale Methoden der Informatik (185.291)
16 March 2018

Kennz. (study id)	Matrikelnummer (student id)	Nachname (surname)	Vorname (first name)

1.) Consider the following problem:

> **EXACT HITTING SET (EHS)**
>
> INSTANCE: A collection $\mathcal{C}$ of sets of elements.
>
> QUESTION: Does there exist a set S of elements, such that for each $C \in \mathcal{C}$, $|S \cap C| = 1$, i.e. each set in $\mathcal{C}$ contains exactly one element from S?

Example: Consider $\mathcal{C} = \{\{a, b, d\}, \{b, c\}, \{c, d\}\}$. $S = \{a, c\}$ witnesses that $\mathcal{C}$ is a positive instance of **EHS**. On the other hand, $\mathcal{C}' = \{\{a, b, d\}, \{a, b, c\}, \{c, d\}\}$ is a negative instance.

By providing a suitable reduction from the **1-IN-3-SAT** problem, prove that **EXACT-HITTING-SET** is an NP-hard problem. Argue formally that your reduction is correct.

Recall that **1-IN-3-SAT** is defined as follows:

> **1-IN-3-SAT**
>
> INSTANCE: Boolean formula φ in 3-CNF.
>
> QUESTION: Does there exists a satisfying truth assignment T on φ, such that in each clause of φ, exactly one literal is true in T?

Hint: For each variable v in φ, use two elements v and $\neg v$ in your definition of $\mathcal{C}$.

(15 points)

2.) (a) Show that $b[j] \doteq f \rightarrow b\langle j \triangleleft f\rangle \doteq b$ is $\mathcal{T}_A^{=}$-valid.

Besides the equality axioms, you have the following ones for the arrays.

i. $\forall a, i, j\ \big(i \doteq j \rightarrow a[i] \doteq a[j]\big)$ (array congruence)

ii. $\forall a, v, i, j\ \big(i \doteq j \rightarrow a\langle i \triangleleft v\rangle[j] \doteq v\big)$ (read-over-write 1)

iii. $\forall a, v, i, j\ \big(i \neq j \rightarrow a\langle i \triangleleft v\rangle[j] \doteq a[j]\big)$ (read-over-write 2)

iv. $\forall a, b\, \big(\forall j\ \big(a[j] \doteq b[j]\big) \leftrightarrow a \doteq b\big)$ (extensionality)

(12 points)

(b) Consider the clauses $C_1, \ldots, C_6$ in `dimacs` format (in this order, shown in the box; recall that `0` indicates the end of a clause) which are given as input to a SAT solver.

- Apply CDCL using the convention that if a variable is assigned as a decision, then it is assigned 'true'. Select variables as decisions in *increasing* order of their respective integer IDs in the `dimacs` format, starting with variable `1`.
- When the *first* conflict occurs, draw the complete implication graph, mark the first UIP, give the derivation of the learned asserting clause that corresponds to the first UIP, and stop CDCL. You do *not* have to solve the formula!

```
-1 4 0
-4 5 0
-2 -4 6 0
-3 -6 7 0
-7 9 0
-5 -6 -7 -9 0
```

(3 points)

3.) Show that the following correctness assertion is true with respect to total correctness. Describe the function computed by the program if we consider k as its input and m as its output.

Hints: Use the formula $m^2 \le k < n^2 \land 0 \le m < n \le k+1$ as loop invariant. Depending on how you choose the variant, use one of the following annotation rules:

$\mathsf{while}\ e\ \mathsf{do} \cdots \mathsf{od} \mapsto \{\, Inv \,\}\mathsf{while}\ e\ \mathsf{do}\ \{\, Inv \land e \land t{=}t_0 \,\} \cdots \{\, Inv \land 0{\le}t{<}t_0 \,\}\mathsf{od}\{\, Inv \land \neg e \,\}$

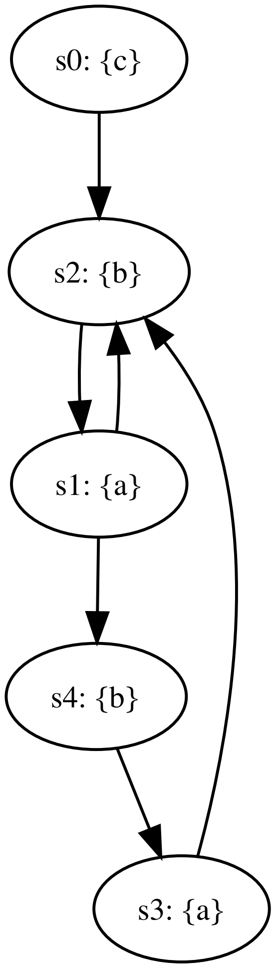
$\mathsf{while}\ e\ \mathsf{do} \cdots \mathsf{od} \mapsto \{\, Inv \,\}\mathsf{while}\ e\ \mathsf{do}\ \{\, Inv \land e \land t{=}t_0 \,\} \cdots \{\, Inv \land (e \to 0{\le}t{<}t_0) \,\}\mathsf{od}\{\, Inv \land \neg e \,\}$

$\{\, F\colon k \ge 0 \,\}$
$m := 0;$
$n := k + 1;$
while $m + 1 \ne n$ do
    $l := (m+n)/2;$
    if $l^2 \le k$ then
        $m := l$
    else
        $n := l$
    fi
od
$\{\, G\colon m^2 \le k < (m+1)^2 \,\}$

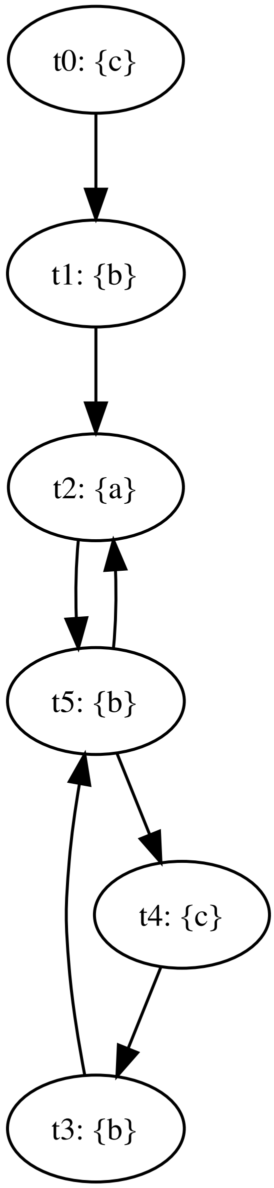
(15 points)

4.) (a) Provide a non-empty simulation relation H that witnesses $M_1 \leq M_2$, where M_1 and M_2 are shown below. The initial state of M_1 is s_0, the initial state of M_2 is t_0:

Kripke structure M_1:

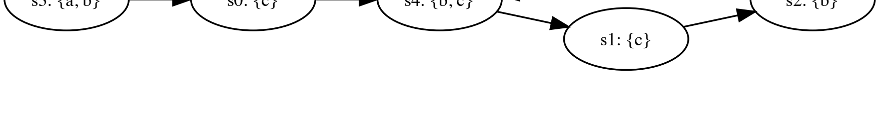


Kripke structure M_2:



(4 points)

(b) Consider the following Kripke structure M:



For each of the following formulae φ,

i. check the respective box if the formula is in CTL, LTL, and/or CTL*, and
ii. list the states s_i on which the formula φ holds; i.e. for which states s_i do we have $M, s_i \models \varphi$?

φ	CTL	LTL	CTL*	States s_i
$\mathbf{F}(a \wedge b)$	☐	☐	☐	
$\mathbf{AX}(b)$	☐	☐	☐	
$\mathbf{AX}(b \wedge c)$	☐	☐	☐	
$\mathbf{EF}(c)$	☐	☐	☐	
$\mathbf{E}[(a \wedge b)\ \mathbf{U}\ (b)]$	☐	☐	☐	

(5 points)

(c) **LTL tautologies**

Prove or disprove the following LTL formulas:

i. $(\neg \mathbf{G} q) \rightarrow (p\ \mathbf{U}\ \neg q)$
ii. $(\mathbf{GF} p) \rightarrow (\mathbf{FG} p)$
iii. $\mathbf{FX} p \rightarrow \mathbf{XF} p$

(6 points)