Model checking — Endterm

- You have **120 minutes** to complete the exam.
- Answers must be written in a **separate booklet**. Do not answer on the exam.
- Please let us know if you need more paper.
- Write your name and Matrikelnummer on every sheet.
- Write with a non-erasable **pen**. Do not use red or green.
- You are not allowed to use auxiliary means other than pen and paper.
- You can obtain **40 points (plus 4 bonus points)**. You need **17 points** to pass.

Question 1: LTL and Büchi automata (2 + 2 + 2 + 3 = 9 points)

Consider the following LTL formulae over the set of atomic propositions $AP = \{p, q\}$:

$$\phi_1 = \mathbf{FG}(p \mathbin{\mathbf{U}} q) \qquad \phi_2 = \mathbf{FG}(\neg p \to q) \qquad \phi_3 = \mathbf{G}(\neg p \lor (p \mathbin{\mathbf{R}} q))$$

(a) Is there a word satisfying ϕ_1 but not ϕ_2? If so, exhibit such a word and if not, briefly explain why it does not exist.

(b) Is there a word satisfying ϕ_2 but not ϕ_1? If so, exhibit such a word and if not, briefly explain why it does not exist.

(c) Is there a word satisfying all three formulae? If so, exhibit such a word and if not, briefly explain why it does not exist.

(d) Give a Büchi automaton accepting exactly the words satisfying ϕ_1. Make sure it accepts the following words: $\{p, q\}^\omega, \{p\}\{q\}^\omega$ and rejects the following words: $\emptyset^\omega, \{p\}^\omega$.

Question 2: CTL (1 + 1 + 1 + 1 = 4 points)

Consider the CTL formulas $\mathbf{EF}p, \mathbf{EFAG}p, \mathbf{AGEF}p, \mathbf{AGAF}p, \mathbf{AG}p$ over $AP = \{p\}$. Draw:

(a) a Kripke structure $\mathcal{K}_1$ satisfying $\mathbf{EF}p$ but not $\mathbf{EFAG}p$;

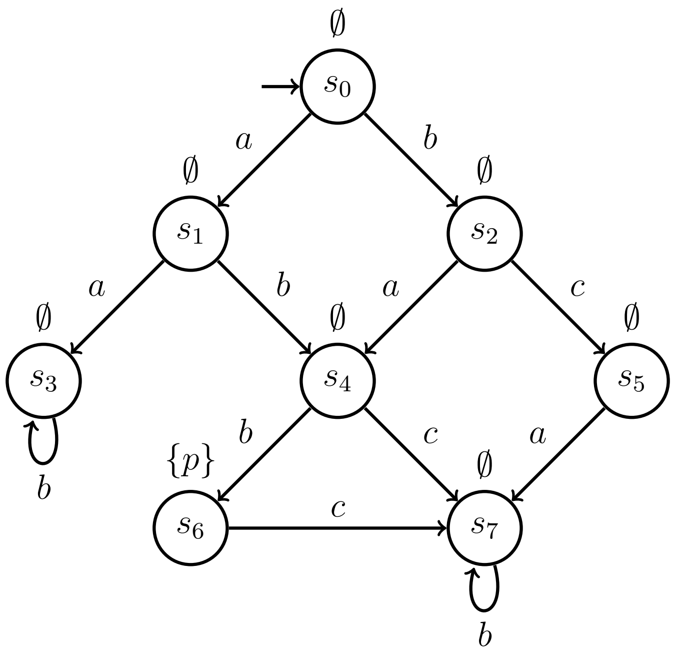
(b) a Kripke structure $\mathcal{K}_2$ satisfying $\mathbf{EFAG}p$ but not $\mathbf{AGEF}p$;

(c) a Kripke structure $\mathcal{K}_3$ satisfying $\mathbf{AGEF}p$ but not $\mathbf{AGAF}p$;

(d) a Kripke structure $\mathcal{K}_4$ satisfying $\mathbf{AGAF}p$ but not $\mathbf{AG}p$.

Question 3: Partial order reduction **$(1+1+1+1+1=5$ points)**

Consider the labelled Kripke structure $\mathcal{K} = (S, A, \rightarrow, r, AP, \nu)$ where $S = \{s_0, \ldots, s_7\}$, $A = \{a, b, c\}$ (A is the set of actions), $r = s_0$, $AP = \{p\}$, and $\rightarrow$ and ν are graphically represented below. Observe that p holds only at state s_6 and nowhere else.



(a) Give the largest relation $I \subseteq A \times A$ satisfying the three properties of an independence relation (irreflexivity, symmetry, and the "diamond property") and explain why it is the largest.

(b) Give the largest invisibility set $U \subseteq A$.

(c) Does $red(s_0) = \{a\}$ satisfy condition C_1 (see below) for I and U? Justify your answer.

(d) Does $red(s_4) = \{b\}$ satisfy all of C_0–C_3 (see below) for I and U? Justify your answer.

(e) Does $red(s_2) = \{a\}$ satisfy all of C_0–C_3 (see below) for I and U? Justify your answer.

Recall that the conditions C_0–C_3 for $red(s)$ are:

- C_0: $red(s) = \emptyset$ iff $en(s) = \emptyset$.
- C_1: Every path starting at s satisfies: no action dependent on some action in $red(s)$ can be executed without an action from $red(s)$ occurring first.
- C_2: If $red(s) \neq en(s)$, then all actions in $red(s)$ are invisible.
- C_3: For all cycles in the reduced Kripke structure the following holds: if $a \in en(s)$ for some state s in the cycle, then $a \in red(s')$ for some (possibly other) state s' in the cycle.

Question 4: Binary decision diagrams (4 points)

Assume that you are given a Kripke structure with states $S = \{s_0, s_1, \ldots, s_7\}$.

(a) Compute a multi-BDD representing the two subsets of states $P = \{s_0, s_1, s_3, s_5, s_7\}$ and $Q = \{s_0, s_2, s_6, s_7\}$. Encode each state of S using three bits in the obvious way:

$$s_0 \mapsto 000, s_1 \mapsto 001, \ldots, s_7 \mapsto 111.$$

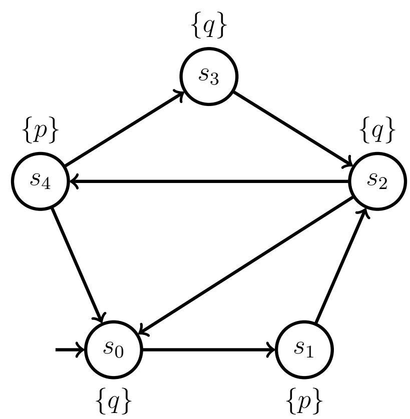
Use the ordering $b_0 < b_1 < b_2$ where b_0 is the most significant bit and b_2 is the least significant bit of the binary encoding.

(b) **2 bonus points:** Compute a BDD node for the set $P \cap Q$ using the BDD intersection algorithm (see below). Show the recursion tree.

> Recall the BDD intersection algorithm. Let B and C be two nodes of a multi-BDD. The node for the intersection of B and C is computed as follows:
>
> - If B and C are equal, then return B.
> - If B or C are the 1 leaf, then return the other BDD.
> - If B or C are the 0 leaf, then return 0.
> - Otherwise, compare the two variables labelling of B and C, and let x be the smaller among the two (or the one labelling both).
> - If B is labelled by x, then let B_1 and B_0 be the children of B; otherwise, let $B_1 := B$ and $B_0 := B$. Define C_1 and C_0 analogously.
> - Apply the strategy recursively to the pairs B_1, C_1 and B_0, C_0, yielding BDD nodes E and F. If $E = F$, return E, otherwise return $mk(x, E, F)$.

Question 5: Abstraction refinement (2 + 1 + 2 = 5 points)

Consider the Kripke structure $\mathcal{K} = (S, \rightarrow, r, AP, \nu)$ where $S = \{s_0, s_1, s_2, s_3, s_4\}$, $r = s_0$, $AP = \{p, q\}$, and $\rightarrow$ and ν are graphically represented as follows:



Let $\approx$ be the equivalence relation over S given by $s \approx t$ iff $\nu(s) = \nu(t)$.

(a) Construct the Kripke structure $\mathcal{K}'$ obtained by abstracting S with respect to $\approx$.

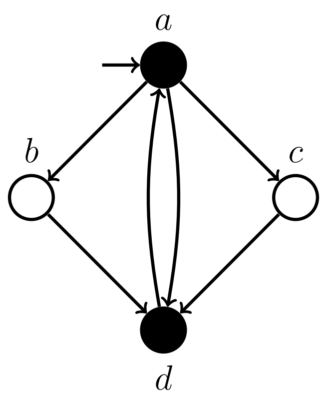
(b) Give a counterexample showing that $\mathcal{K}'$ does not satisfy $\mathbf{GF}p$.

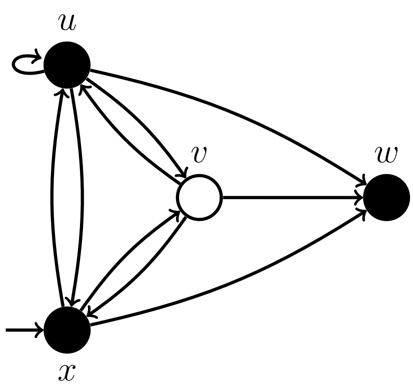
(c) Following the procedure seen in class, use the counterexample to refine $\mathcal{K}'$ into a Kripke structure $\mathcal{K}''$.

(d) **2 bonus points**: Keep refining the abstraction until you prove that $\mathcal{K}$ satisfies $\mathbf{GF}p$.

Question 6: Simulations and bisimulations (2 + 2+ 2 = 6 points)

Consider the two following Kripke structures $\mathcal{K}_1$ (left) and $\mathcal{K}_2$ (right) over $AP = \{p\}$. States coloured black satisfy proposition p and others do not.





(a) Does $\mathcal{K}_2$ simulate $\mathcal{K}_1$? If your answer is *yes*, then give a simulation relation, and if it is *no*, then explain why no simulation relation exists.

(b) Does $\mathcal{K}_1$ simulate $\mathcal{K}_2$? If your answer is *yes*, then give a simulation relation, and if it is *no*, then explain why no simulation relation exists.

(c) Define what is a bisimulation. Give a Kripke structure $\mathcal{K}_3$ bisimilar to $\mathcal{K}_2$ but with fewer states than $\mathcal{K}_2$.

Question 7: Pushdown systems (3 + 3 + 1 = 7 points)

Consider the following recursive program with a global boolean variable `x`:

```
           boolean x;

           procedure foo;                     procedure bar;
f0:          x := not x;          b0:           if x then
                                                  call foo;
f1:          if x then                          endif;
               call foo;
             else                 b1:           return;
               call bar;
             endif;

f2:          return;
```

(a) Model the program, where the value of `x` is not initialized, with a pushdown system $\mathcal{P} = (P, \Gamma, \Delta)$. Give explicit enumerations of the set of control states P, the stack alphabet Γ, and the set of rules Δ.
Hint: Δ contains 10 rules.

(b) Let E be the set of all configurations of $\mathcal{P}$ with empty stack. Give a $\mathcal{P}$-automaton recognizing the language E. Use the saturation rule to compute a $\mathcal{P}$-automaton recognizing the language $pre^*(E)$. For each transition added by the saturation rule, briefly explain how it is generated.
Hint: The $\mathcal{P}$-automaton for $pre^*(E)$ should have 10 transitions.

(c) Is there any configuration of $P \times \Gamma^*$ from which it is impossible to reach a configuration with empty stack? Briefly justify your answer.