Formal techniques for software and hardware verification

Lecturers:

Vladimir Zakharov

Vladislav Podymov

e-mail:

valdus@yandex.ru

2020, fall semester

Seminar 3

CTL

BDD

Model checking for CTL: tableaux-based algorithm, symbolic algorithm

Exercise 1

Suggest a ctl-formula corresponding to the following sentence:

1. No matter how the computer operates, if it is on, then it can be turned off

   on is a proposition "the computer is on"

2. If I want to quit, I can do it next day

   w is a proposition "today I want to quit"

   q is a proposition "today I quit"

3. If I fail the course, I will be expelled next day

   f is a proposition "today I failed the course"

   e is a proposition "I am to be expelled today"

Exercise 1

Suggest a ctl-formula corresponding to the following sentence:

4. Any received request will eventually be processed

   r is a proposition "a request is received"

   p is a proposition "a request is processsed"

5. The system can reach a state in which the process P takes the resource r and never releases it

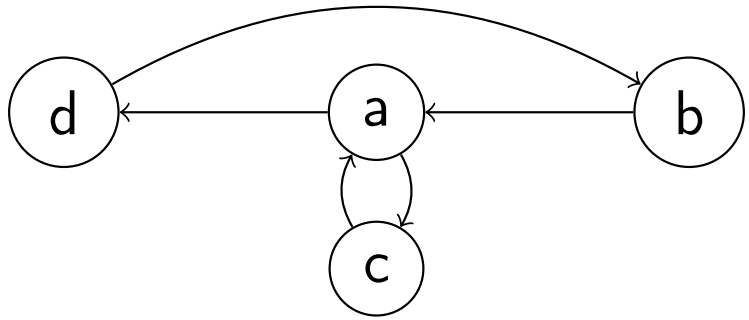
   t is a proposition "r is taken by P"

6. If the computer is broken, it remains broken forever.

   b is a proposition "the computer is broken"

Exercise 2

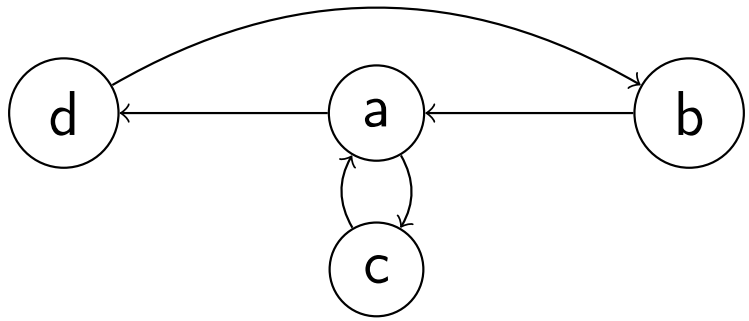
Which states of the following Kripke structure satisfy the given formula?



1. **EX**d
2. **AX**d
3. **EF**b
4. **AF**b
5. **EG**b
6. **EG**$\neg b$

Exercise 2

Which states of the following Kripke structure satisfy the given formula?



7. $\mathbf{AGAF}a$
8. $\mathbf{E}(c\mathbf{U}\neg c)$
9. $\mathbf{A}(\neg c\mathbf{UEF}c)$
10. $\mathbf{A}(b\mathbf{UA}(a\mathbf{U}d))$

Exercise 3

Consider the following implication:

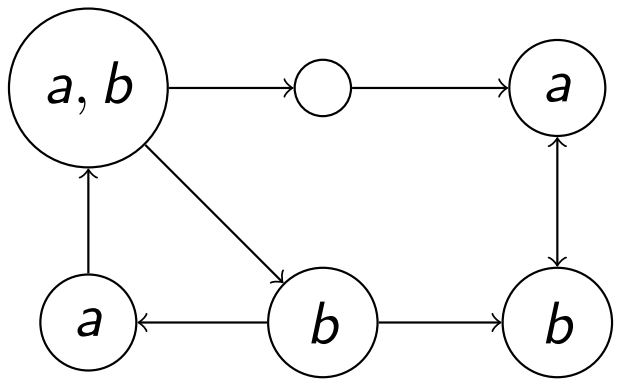
$$\text{if } M, s \models \varphi, \text{ then } M, s \models \psi$$

Does the implication hold for any Kripke structure M, any state s of M, and the following formulae φ, ψ?

1. $\varphi = \mathbf{AFAG}p$, $\psi = \mathbf{AFG}p$
2. $\varphi = \mathbf{AFG}p$, $\psi = \mathbf{AFAG}p$
3. $\varphi = \mathbf{AFEG}p$, $\psi = \mathbf{AFG}p$
4. $\varphi = \mathbf{AFG}p$, $\psi = \mathbf{AFEG}p$
5. $\varphi = \mathbf{AGAF}p$, $\psi = \mathbf{AGF}p$
6. $\varphi = \mathbf{AGF}p$, $\psi = \mathbf{AGAF}p$
7. $\varphi = \mathbf{AGEF}p$, $\psi = \mathbf{AGF}p$
8. $\varphi = \mathbf{AGF}p$, $\psi = \mathbf{AGEF}p$

Exercise 4

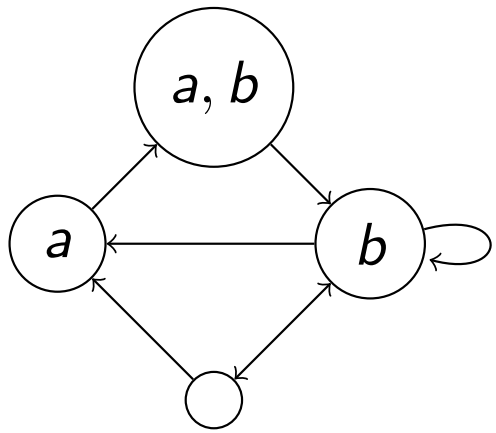
Using the tableau-based model checking algorithm, compute the set of all states satisfying the given formula



AG$(a \vee b)$

Exercise 4

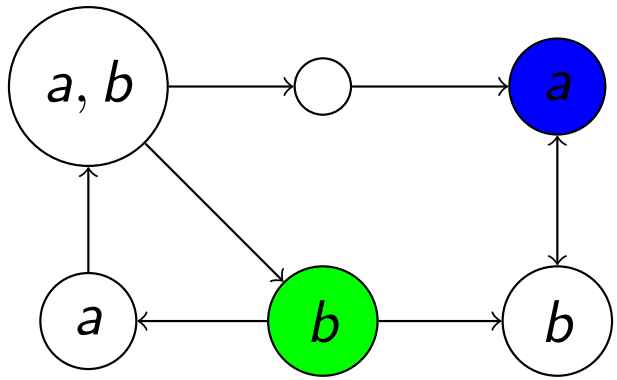
Using the tableau-based model checking algorithm, compute the set of all states satisfying the following formula



1. **EGEXAX**b
2. **A**(**EXAX**b**U**a)

Exercise 5

Using the tableau-based model checking algorithm, compute the set of all states of a **fair** Kripke structure satisfying the following formula



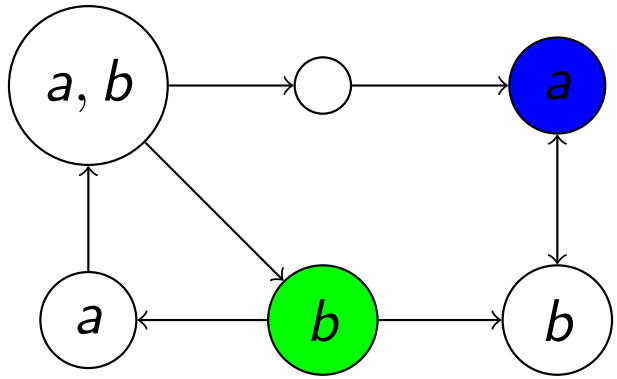
- **AGAF**$(a \,\&\, b)$
- **AFAG**$(a \rightarrow \mathbf{AX}\neg a)$

Fairness constraints:

- $\emptyset$

Exercise 5

Using the tableau-based model checking algorithm, compute the set of all states of a **fair** Kripke structure satisfying the following formula



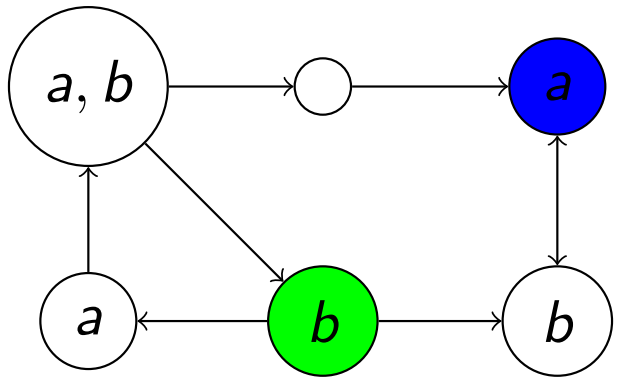
- **AGAF**$(a \,\&\, b)$
- **AFAG**$(a \rightarrow \mathbf{AX}\neg a)$

Fairness constraints:

- $\{\{$ $\}\}$
- $\{\{$ $\}\}$

Exercise 5

Using the tableau-based model checking algorithm, compute the set of all states of a **fair** Kripke structure satisfying the following formula



- $\mathbf{AGAF}(a \,\&\, b)$
- $\mathbf{AFAG}(a \rightarrow \mathbf{AX}\neg a)$

Fairness constraints:

- $\{\{$●, ●$\}\}$
- $\{\{$●$\}, \{$●$\}\}$

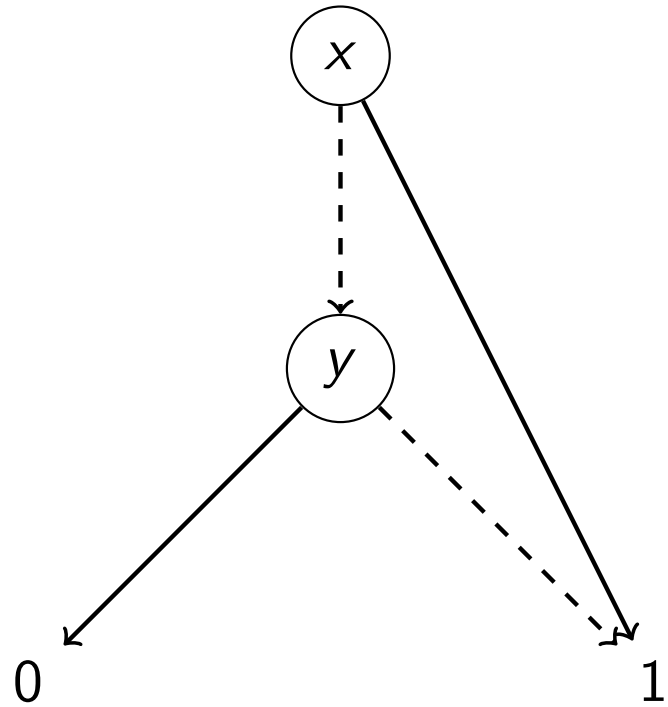
Exercise 6

Implement the given formula as a ROBDD for the given variable ordering

1. $x \rightarrow y$
   - $x \prec y$
   - $y \prec x$
2. $x \,\&\, y \vee x \,\&\, z \vee y \,\&\, z$
   - $x \prec y \prec z$
3. $x \,\&(y \oplus z) \vee \neg x \,\&(\neg y \oplus \neg z)$
   - $x \prec y \prec z$
4. $(x \rightarrow y) \oplus ((y \rightarrow \neg z) \rightarrow x \,\&\, y)$
   - $x \prec y \prec z$
   - $z \prec y \prec x$
5. $x \,\&\, x' \vee y \,\&\, y' \vee z \,\&\, z'$
   - $x \prec y \prec z \prec x' \prec y' \prec z'$
   - $x \prec x' \prec y \prec y' \prec z \prec z'$

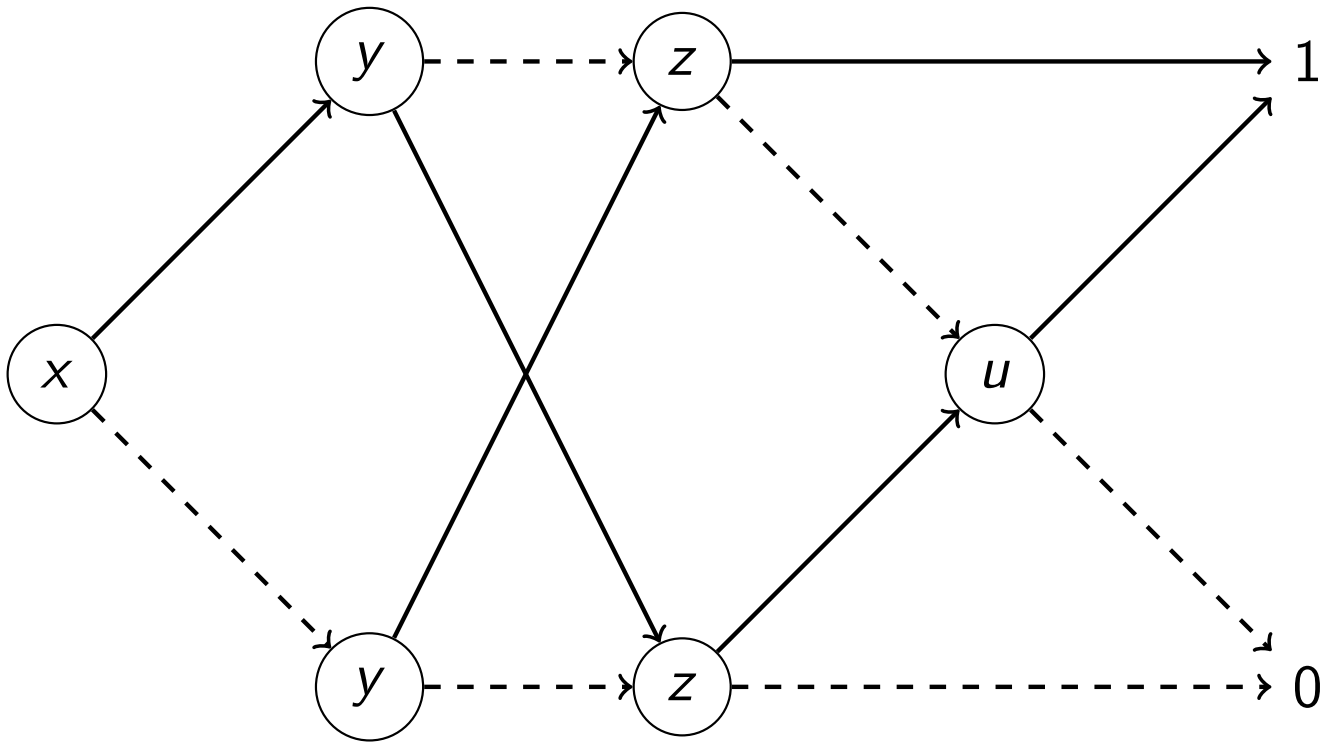
Exercise 7

Implement the following ROBDD as a disjunctive normal form



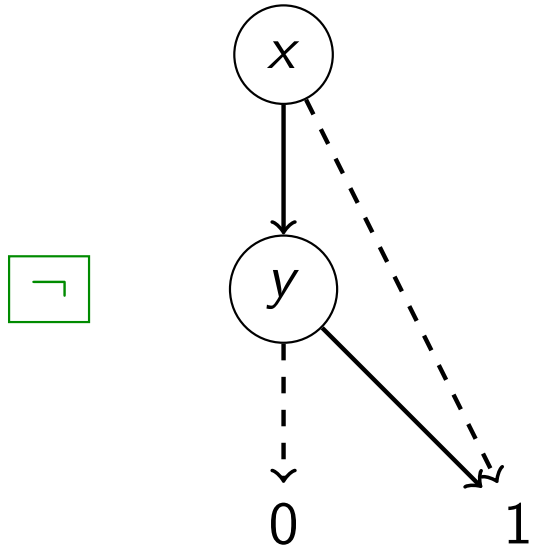
Exercise 7

Implement the following ROBDD as a disjunctive normal form



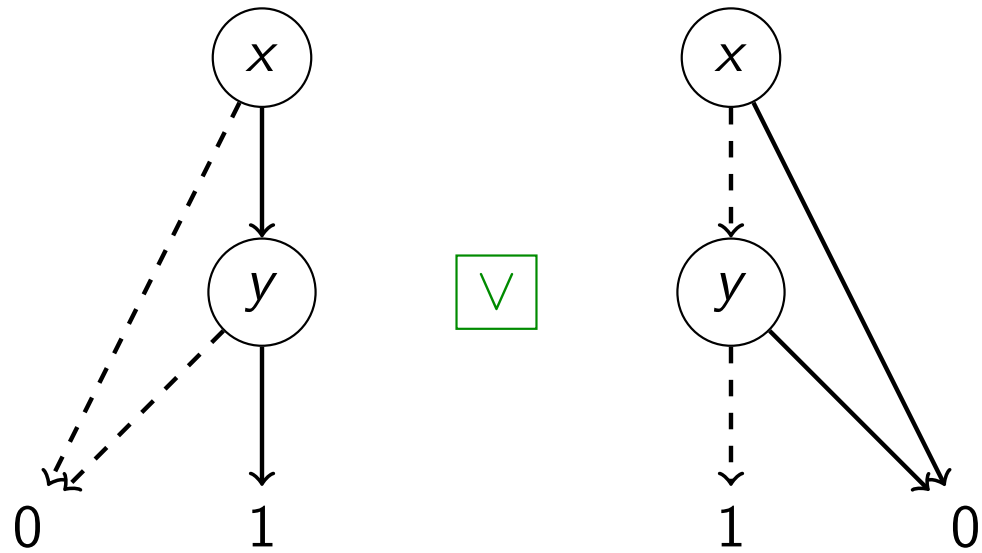
Exercise 8

Apply the given operation to the given ROBDD (or ROBDDs):



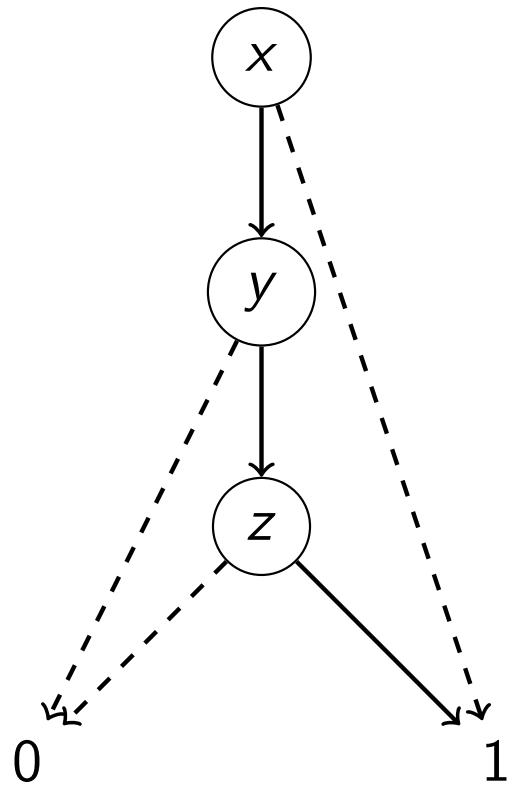
Exercise 8

Apply the given operation to the given ROBDD (or ROBDDs):

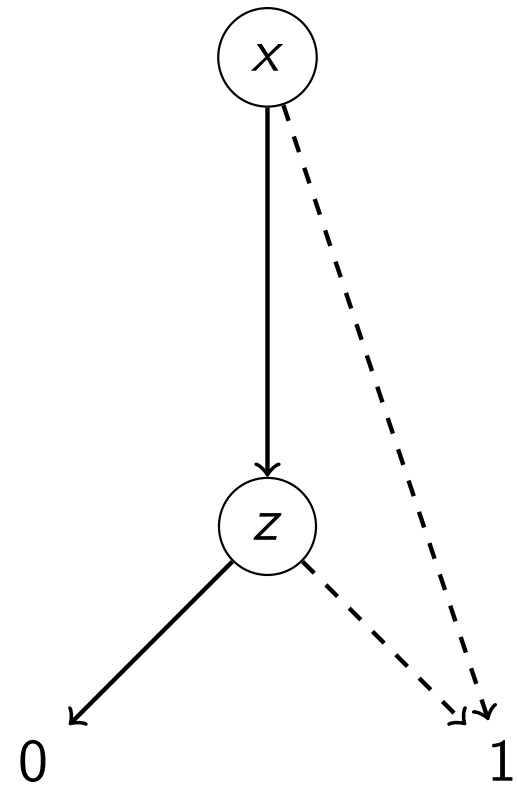


Exercise 8

Apply the given operation to the given ROBDD (or ROBDDs):



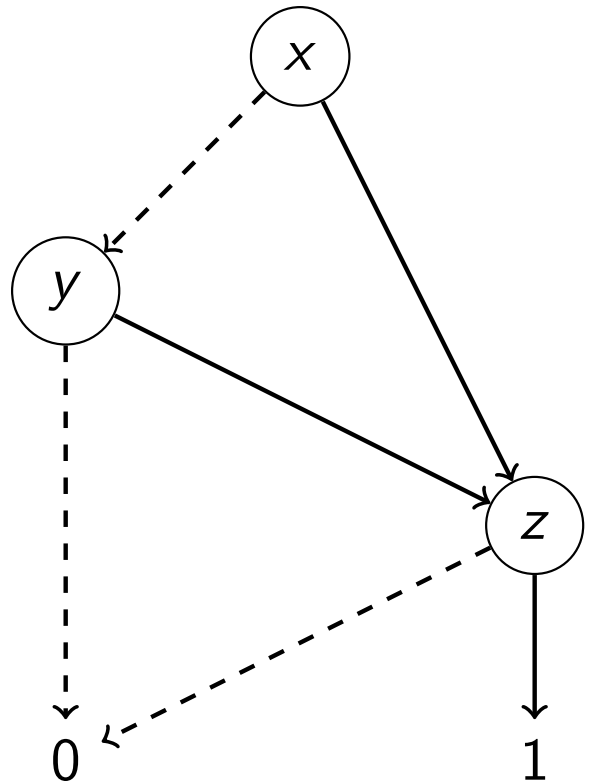
&



Exercise 8

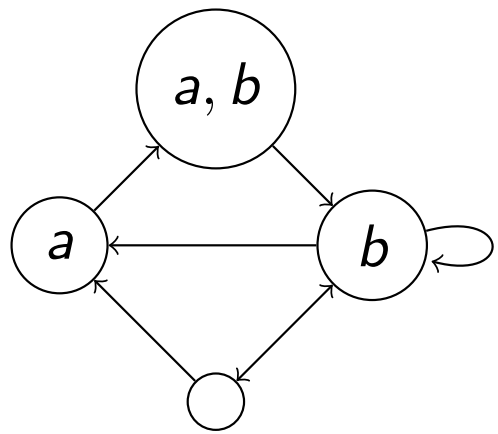
Apply the given operation to the given ROBDD (or ROBDDs):

$y \leftarrow 1$



Exercise 9

1. Construct a ROBDD representation of the following Kripke structure
2. Using the symbolic algorithm, compute the set of all states satisfying the given formula



1. **EGEXAX**b
2. **A**(**EXAX**b**U**a)