Name: MNR:

SKZ:

Question 1: **(15 points)**

Construct the Büchi Automaton for the (already negated) formula

$$\mathbf{F}\,(a \wedge \mathbf{X} b)$$

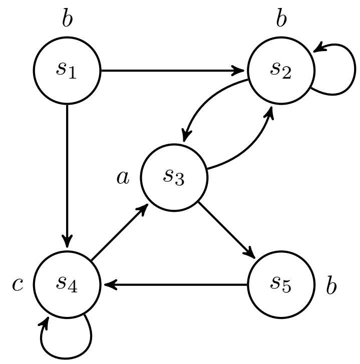
- Follow the construction steps presented in the lecture!
- For the **U** operator, you can use the one-step rule presented on slide 72.

Question 2: **(15 points)**

Perform CTL model checking on the following Kripke structure for the formula

$$\varphi = \mathbf{E}\,((\mathbf{EG}\,b)\ \mathbf{U}\,(\mathbf{EX}\,a))$$

a) To this end, draw a table with the set of satisfying states for each subformula of φ.



For example, the following tableaux is constructed for the formula $\mathbf{E}\,a\,\mathbf{U}\,b$.

Formula	State(s)
a	s_3
b	$s_1,\ s_2,\ s_5$
$\mathbf{E}\,a\,\mathbf{U}\,b$	s_1, s_2, s_3, s_5

b) Give the intermediate sets used in the fixpoint computations of $\mathbf{EG}\,b$ (the version of the algorithm that does not use SCCs) and $\mathbf{E}\,((\mathbf{EG}\,b)\ \mathbf{U}\,(\mathbf{EX}\,a))$.

Question 3: **(20 points)**

Let $K = (S, s_0, R, AP, L)$ be a *finite* Kripke structure with $AP = \{i, a, b, c\}$, and let s_0 be the only state labeled with "i". Express the following specifications about K in terms of $\mathsf{CTL}^\star$. Where possible, provide an LTL or CTL formula.

(a) From every state in K, it is *possible* to return to the initial state (which is labeled i) via a state labeled a again.

(b) All paths starting at the initial state lead to a cycle that does not contain a state labeled a *unless* the cycle includes a state labeled b.

(c) Whenever a state labeled with a is reached, a state labeled with b will be reached at a *strictly later* point.

(d) Whenever a path reaches a state labeled with a, it will eventually reach a state labeled with c, but not before it reaches a state labeled with b.

(e) Whenever a state labeled with a is reached, a state labeled with b will be reached in at least one but at most three additional steps.

Question 4: **(20 points)**

Are the following statements true/false? Mark the corresponding column in the table below.

(a) Fairness conditions cannot be directly expressed in CTL*.

(b) Every CTL formula has an equivalent CTL formula containing only **EG**, **AX**, and **EU**.

(c) For the boolean formula $(x_1 \Rightarrow y_1) \vee \cdots \vee (x_n \Rightarrow y_n)$, one can find an order on the variables $x_1, \ldots, x_n, y_1, \ldots, y_n$, so that the ROBDD that encodes the formula is linear in the size of n.

(d) Let $A \wedge B$ be unsatisfiable, and let I_1 and I_2 be interpolants for A and B. Then $I_1 \oplus I_2$ is also an interpolant for A and B (where $\oplus$ represents exclusive-or).

(e) Every trace that is a counterexample to a liveness property is lasso-shaped (i.e., has the form $s_0, \ldots, s_{\ell-1}, (s_\ell, \ldots, s_k)^\omega$).

(f) For every safety property $\varphi = \mathbf{AG}p$ there exists a Kripke structure $\mathcal{M}$ with n states such that the reachability diameter is n.

(g) There is a non-empty Kripke structure $\mathcal{M}$ that satisfies $(\mathbf{AG}\,\mathbf{EF}p) \wedge (\mathbf{EF}\,\mathbf{AG}\neg p)$.

(h) There are propositional logic formulas φ for which the Tseitin transformation yields an equisatisfiable formula ψ in conjunctive normal form (CNF) that is exponentially smaller (in terms of the number of clauses) than the smallest formula in CNF that is logically equivalent to φ.

(i) If a given transition system is safe (i.e., property P holds), then the IC3 model checking algorithm always computes the logically weakest inductive invariant that proves that P holds.

(j) Given n Büchi automata $\mathcal{B}_1, \ldots \mathcal{B}_n$, the number of states of the asynchronous product $\mathcal{B}_1 \parallel \cdots \parallel \mathcal{B}_n$ is polynomial in n.

Question	**True**	**False**
(a)		
(b)		
(c)		
(d)		
(e)		
(f)		
(g)		
(h)		
(i)		
(j)		

Question 5: **(10 points)**

Let G_i be a frame and s be a state in the IC3 algorithm such that the following holds (i.e., s is unreachable from G_i):

$$G_i(V) \wedge \neg s(V) \wedge T(V, V') \Rightarrow \neg s(V')$$

Let $c(V')$ be an interpolant for the following pair of formulas:

$$\langle \quad G_0(V') \vee (G_i(V) \wedge \neg s(V) \wedge T(V, V')) \quad , \quad s(V') \quad \rangle$$

(where $I \equiv G_0$ is the set of initial states).

Prove that c satisfies initiation and consecution!