Release Operator

$\varphi_1 R \varphi_2 := \neg((\neg\varphi_1) U (\neg\varphi_2))$ defined from U

$\equiv (\neg\varphi_1 \wedge \neg\neg\varphi_2) W (\neg\neg\varphi_1 \wedge \neg\neg\varphi_2)$

$\equiv (\neg\varphi_1 \wedge \varphi_2) W (\varphi_1 \wedge \varphi_2)$

We prove its semantics, for all paths $\pi = \pi[0]\pi[1]\pi[2]\dots$

$\pi \models \varphi_1 R \varphi_2 \iff$

$\iff \pi \models \neg((\neg\varphi_1) U (\neg\varphi_2))$

$\iff \pi \not\models (\neg\varphi_1) U (\neg\varphi_2)$

$\iff$ NOT$(\pi \models (\neg\varphi_1) U (\neg\varphi_2))$

$\iff$ NOT $\exists i \geq 0 : (\underbrace{\pi^{\geq i} \models \neg\varphi_2}_{\pi^{\geq i} \not\models \varphi_2}$ AND $\forall 0 \leq j < i : \underbrace{\pi^{\geq j} \models \neg\varphi_1}_{\pi^{\geq j} \not\models \varphi_1})$

$\iff \forall i \geq 0 : (\pi^{\geq i} \models \varphi_2$ OR **NOT** $\forall 0 \leq j < i : \pi^{\geq j} \not\models \varphi_1)$

$\iff \forall i \geq 0 : ((\forall 0 \leq j < i : \pi^{\geq j} \not\models \varphi_1) \rightarrow \pi^{\geq i} \models \varphi_2)$

φ_2 must hold for as long as φ_1 is false <u>and</u> also for the first time step in which φ_1 is true

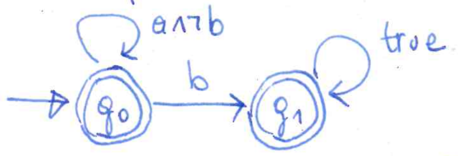
$\iff \forall i \geq 0 : ((\pi^{\geq i} \models \varphi_1$ AND $\forall 0 \leq j < i : \pi^{\geq j} \not\models \varphi_1) \Rightarrow \pi^{\geq j} \models \varphi_2)$

AND $($**NOT** $(\underbrace{\exists i \geq 0 : \pi^{\geq i} \models \varphi_1}_{\forall i \geq 0 : \pi^{\geq i} \not\models \varphi_1}) \Rightarrow \forall i \geq 0 : \pi^{\geq i} \models \varphi_2)$

03-02-2026

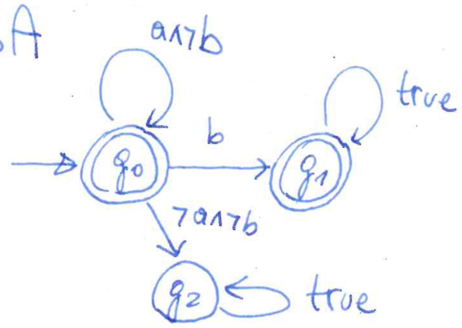
Lecture-6-LTL-model-checking

NBA for $a \mathsf{W} b$

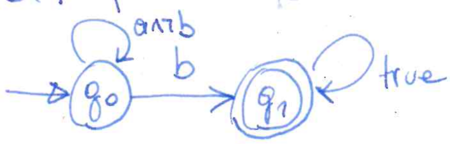


incomplete, since $\xrightarrow{\neg a \wedge \neg b}$ missing in q_0

DBA complete

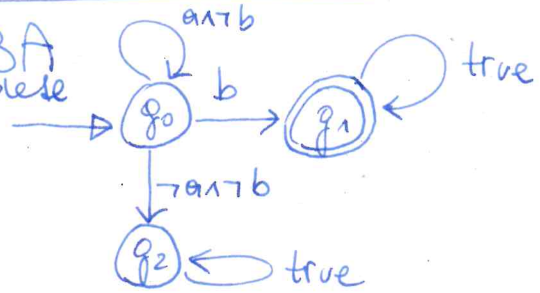


NBA for $a \mathsf{U} b$



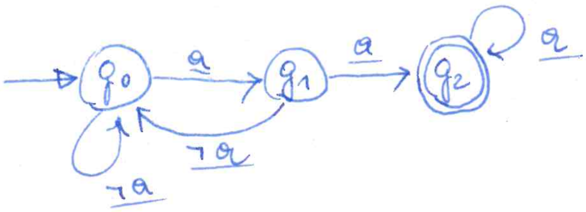
incomplete

DBA complete

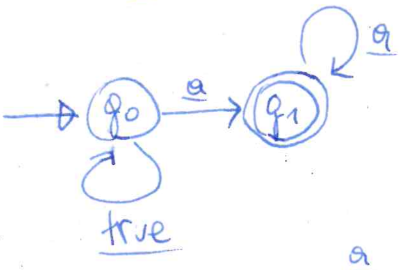


Büchi

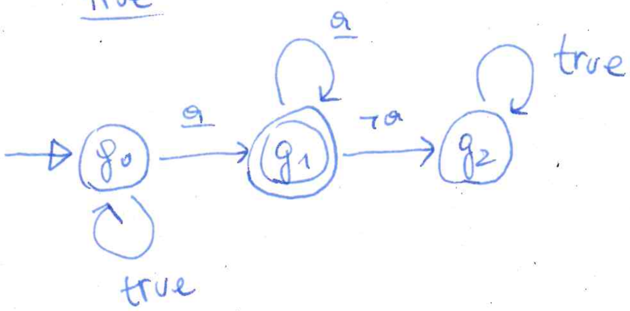
Roger's automaton for $\Diamond \Box a$ (eventually always a)



incomplete, because no $\xrightarrow{\neg a}$ transition from q_2, but deterministic



incomplete, but not deterministic because $q_0 \xrightarrow{\{a\}} \begin{cases} q_0 \\ q_1 \end{cases}$ are possible transitions



Complete, but also not deterministic because $q_0 \xrightarrow{\{a\}} \begin{cases} q_0 \\ q_1 \end{cases}$

LTL-Model checking algorithm

CTL

$TS = \langle S, Act, \rightarrow, I, AP, L \rangle$

$TS \not\models \Phi$

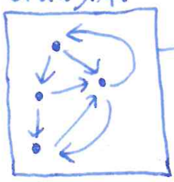
$I \ni s \not\models \Phi$

$\pi \not\models \Phi$

path

behaviour transition system

by MODELLING



Φ conjunction of several requirements

$\Box\Diamond c \vee \Diamond\neg d$

or $U ob$

...

specification

MC

$\times$ + counterexample trace

$\checkmark$ $TS \models \Phi$

$$\begin{aligned}
TS \models \Phi &\iff Traces(TS) \subseteq Words(\Phi) \\
&\iff Traces(TS) \cap (2^{AP})^{\omega} \setminus Words(\Phi) = \emptyset \\
&\iff Traces(TS) \cap Words(\neg\Phi) = \emptyset \\
&\iff Traces(TS) \cap \mathcal{L}_\omega(\mathcal{A}_{\neg\Phi}) = \emptyset \quad [\mathcal{L}_\omega(\mathcal{G}_{\neg\Phi})] \\
&\iff \mathcal{L}_\omega(TS \otimes \mathcal{A}_{\neg\Phi}) = \emptyset \\
&\iff TS \otimes \mathcal{A}_{\neg\Phi} \models \Diamond\Box\neg F
\end{aligned}$$

Basic LTL-model checking algorithm (Vardi, Wolper 1986)

System → Model of System → Transition system TS

Negation of Property → LTL-formula $\neg\Phi$ → Generalized Büchi automaton $\mathcal{G}_{\neg\Phi}$ → Büchi automaton $\mathcal{A}_{\neg\Phi}$

Transition system TS + Büchi automaton $\mathcal{A}_{\neg\Phi}$ → Product transition system $TS \otimes \mathcal{A}_{\neg\Phi}$

$TS \otimes \mathcal{A}_{\neg\Phi} \models \Diamond\Box\neg F$?

"eventually forever in <u>not</u>-final states"

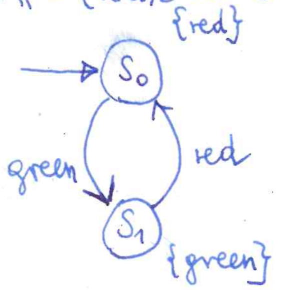
yes → $\checkmark$ Property satisfied! $TS \models \Phi$

no → Property violated! + trace/path witness

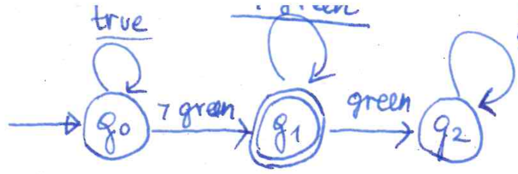
check whether there is a reachable final state on every cycle of $TS \otimes \mathcal{A}_{\neg\Phi}$

Complexity: $O(|TS| \cdot 2^{|\Phi|})$ PSPACE-Complete

$AP = \{red, green\}$



TrLight



$\mathcal{A}_{\bar{P}}$

NBA for $\Diamond\Box\neg green$

Example

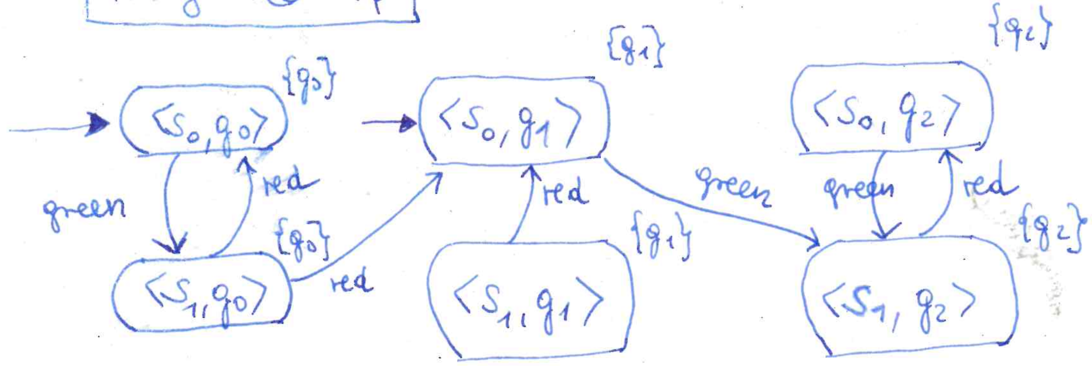
$$\mathcal{L}_\omega(\mathcal{A}_{\bar{P}}) = \{A_0A_1\ldots \in (2^{AP})^\omega \mid \overset{\infty}{\forall} j\geq 0.\ green \notin A_j\}$$
$$= 2^{AP} \setminus \{A_0A_1\ldots \in (2^{AP})^\omega \mid \overset{\infty}{\exists} j\geq 0.\ green \in A_j\}$$
$$= 2^{AP} \setminus P = \bar{P}$$

We want to check the property P "infinitely often green".
Its complement is the property "eventually always not green"
$\bar{P} = (2^{AP})^\omega \setminus P$ $\Diamond\Box\neg green$

$$\left.\begin{aligned}
TrLight \models P &\iff Traces(TrLight) \subseteq P \\
&\iff Traces(TrLight) \cap \underbrace{(2^{AP}\setminus P)}_{\bar{P} = \mathcal{L}_\omega(\mathcal{A}_{\bar{P}})} = \emptyset \\
&\iff Traces(TrLight) \cap \mathcal{L}_\omega(\mathcal{A}_{\bar{P}}) = \emptyset \\
&\iff TrLight \otimes \mathcal{A}_{\bar{P}} \models \Diamond\Box\neg q_1
\end{aligned}\right\} (*)$$

product of LTS with NBA

$TrLight \otimes \mathcal{A}_{\bar{P}}$



$TrLight = \langle S, Act, \rightarrow, I, AP, L\rangle$ $S = \{s_0, s_1\}$, $Act = \{green, red\}$, $I = \{s_0\}$

$\mathcal{A}_{\bar{P}} = \langle Q, 2^{AP}, \delta, Q_0, F\rangle$ $Q = \{q_0, q_1, q_2\}$, $Q_0 = \{q_0\}$, $F = \{q_1\}$

$TrLight \otimes \mathcal{A}_{\bar{P}} = \langle S\times Q, Act, \rightarrow', I', AP', L'\rangle$

where $\rightarrow'$ is defined via: $\dfrac{s \xrightarrow{\alpha} t \quad q \xrightarrow{L(t)} p}{\langle s,q\rangle \xrightarrow{\alpha}' \langle t,p\rangle}$

$I' = \{\langle \tilde{s}_0, q\rangle \mid \tilde{s}_0 \in I \text{ and } \exists q_0 \in Q_0.\ q_0 \xrightarrow{L(\tilde{s}_0)} q\} = \{\langle s_0, q_0\rangle, \langle s_0, q_1\rangle\}$

$AP' = Q$

$L'(\langle s,q\rangle) = \{q\}$

(*) $TrLight \otimes \mathcal{A} \models \Diamond\Box\neg q_1$ "eventually forever" $\neg q_1$

$\iff TrLight \models P$ "infinitely often green"

φ an LTL-formula.

G_φ is constructed such that it accepts all words $\sigma = A_0 A_1 A_2 \ldots \in Word(\varphi)$.

Hereby a word $\sigma = A_0 A_1 A_2 \ldots$ will be accepted by a run $\bar{\sigma} = B_0 B_1 B_2 \ldots$ with states $B_i \supseteq A_i$ where B_i a maximal subset of subformulas or negated subformulas of φ such that: $\varphi \in B_i \iff A_i A_{i+1} A_{i+2} \ldots \models \varphi$

Ex. $\varphi = a \, U (\neg a \wedge b) \qquad \sigma = \{a\}\{a,b\}\{b\}\ldots$

$$B_i \subseteq \underbrace{\{a, b, \neg a, \neg a \wedge b, \varphi\}}_{\text{subformulas of } \varphi} \cup \underbrace{\{\neg a, \neg b, \neg(\neg a \wedge b), \neg\varphi\}}_{\text{negated subformulas of } \varphi}$$

$$B_0 = \{a, \neg b, \neg(\neg a \wedge b), \varphi\}$$
$$B_1 = \{a, b, \neg(\neg a \wedge b), \varphi\}$$
$$B_3 = \{b, \neg a, \neg a \wedge b, \varphi\}$$

The semantics of the next-step operator relies on a non-local condition and will be encoded in the transition relation.

The meaning of the until-operator is split according to the expansion law into local conditions (encoded in the states) and a next-step condition (encoded in transitions).

$(\varphi_1 U \varphi_2 \equiv \varphi_2 \vee (\varphi_1 \wedge \bigcirc(\varphi_1 U \varphi_2))$

Closure of an LTL-formula φ:

closure$(\varphi) := \{\psi \mid \psi$ is subformula of φ, or a negation of a subformula of $\varphi\}$
where we identify $\neg\neg\psi$ with ψ

example: closure$(\underbrace{a \, U (\neg a \wedge b)}_{=:\varphi}) = \{a, b, \neg a, \neg b, \neg a \wedge b, \neg(\neg a \wedge b), \varphi, \neg\varphi\}$

$|\text{closure}(\varphi)| \in O(|\varphi|)$

Elementary Sets of formulas:

$B \subseteq$ closure(φ) is elementary if B is consistent w.r.t. prop. logic,
maximal,
locally consistent w.r.t. Until

B is consistent w.r.t. prop. logic:

$$\left.\begin{array}{l} \varphi_1 \wedge \varphi_2 \in B \iff \varphi_1 \in B \text{ and } \varphi_2 \in B \\ \psi \in B \implies \neg\psi \notin B \\ \text{true} \in \text{closure}(\varphi) \implies \text{true} \in B \end{array}\right\} \text{ for all } \varphi_1 \wedge \varphi_2, \psi \in B$$

B is locally consistent w.r.t. Until-operator:

$$\left.\begin{array}{l} \varphi_2 \in B \implies \varphi_1 U \varphi_2 \in B \\ \varphi_1 U \varphi_2 \in B \text{ and } \varphi_2 \notin B \implies \varphi_1 \in B \end{array}\right\} \text{ for all } \varphi_1 U \varphi_2 \in \text{closure}(\varphi)$$

B is maximal:

$$\left.\psi \notin B \implies \neg\psi \in B \quad \right\} \text{ for all } \psi \in \text{closure}(\varphi).$$

Local consistency condition for the until operator is due to:

$$\varphi_1 U \varphi_2 \equiv \varphi_2 \vee (\varphi_1 \wedge \bigcirc(\varphi_1 U \varphi_2)).$$

Maximality and consistency imply:

$$\psi \in B \iff \neg\psi \notin B.$$

$$\varphi_1, \varphi_2 \notin B \implies \varphi_1 U \varphi_2 \notin B$$

Thm. For every LTL-formula φ over AP there exists a GNBA G_φ over 2^{AP} such that

(a) $Words(\varphi) = \mathcal{L}_\omega(G_\varphi)$

(b) G_φ can be constructed in time $2^{O(|\varphi|)}$

(c) The number of accepting sets of G_φ is bounded above by $O(|\varphi|)$.

Proof. $G_\varphi = (Q, 2^{AP}, \delta, Q_0, \mathcal{F})$

where $Q := \{B \subseteq closure(\varphi) / B \text{ is elementary}\}$

$Q_0 := \{B \in Q / \varphi \in B\}$

$\mathcal{F} := \{F_{\varphi_1 U \varphi_2} / \varphi_1 U \varphi_2 \in closure(\varphi)\}$

where $F_{\varphi_1 U \varphi_2} = \{B \in Q / \varphi_1 U \varphi_2 \notin B \text{ or } \varphi_2 \in B\}$

$\delta : Q \times 2^{AP} \to 2^Q$

$$\langle B, A\rangle \longmapsto \delta(B,A) := \begin{cases} \emptyset & \dots \text{ if } A \neq B \cap AP \\ \{B' \dots & \text{if } A = B \cap AP \\ \text{where } B' \text{ is elementary such that} & \\ \text{(i) } (O\psi \in B \Leftrightarrow \psi \in B') \text{ for all } O\psi \in closure(\varphi) & \\ \text{(ii) for every } \varphi_1 U \varphi_2 \in closure(\varphi) & \\ \quad \varphi_1 U \varphi_2 \in B \Updownarrow \varphi_2 \in B \vee (\varphi_1 \in B \wedge \varphi_1 U \varphi_2 \in B') & (*) \end{cases}$$

$= \{B' \in Q / (*)\}$

$\varphi_1 U \varphi_2 \equiv \varphi_2 \vee (\varphi_1 \wedge O(\varphi_1 U \varphi_2))$

For the definition of $F_{\varphi_1 U \varphi_2} = \{B \in Q / \varphi_1 U \varphi_2 \notin B \text{ or } \varphi_2 \in B\}$ note:

$\overset{\infty}{\exists} j \geq 0 : B_j \in \underbrace{F_{\varphi_1 U \varphi_2}}_{= \{B \in Q / \varphi_1 U \varphi_2 \notin B \text{ or } \varphi_2 \in B\}} \Longleftrightarrow \neg \overset{\infty}{\forall} j \geq 0 : B_j \in \underbrace{Q \setminus F_{\varphi_1 U \varphi_2}}_{= \{B \in Q / \varphi_1 U \varphi_2 \in B \text{ and } \varphi_2 \notin B\}}$

$G_{\circ a} = \langle Q, 2^{AP}, \delta, Q_0, \mathcal{F} \rangle \quad \mathcal{F} \in 2^{2^{AP}}$

Example. GNBA for $\varphi = \circ a \quad AP = \{a\}$.

nondet.

generalized Büchi-automaton

acceptance condition $\mathcal{F} \in 2^{(2^{AP})}$: traces must visit every subset of states in $\mathcal{F}$ infinitely often

($\mathcal{F}$ can be empty) → then all traces are accepting

$closure(\circ a) = \{a, \neg a, \circ a, \neg \circ a\}$

subformulas + negation, identify $\neg\neg\Phi$ with Φ

$Q = \{B \subseteq closure(\circ a) \mid B \text{ is elementary}\} = \{B_1, B_2, B_3, B_4\}$

max. consistent

loc. consistent w.r.t. U

$B_1 = \{a, \circ a\} \quad B_2 = \{a, \neg\circ a\}$

$B_3 = \{\neg a, \circ a\} \quad B_4 = \{\neg a, \neg\circ a\}$

$\mathcal{F} = \{F_{\varphi_1 U \varphi_2} \mid \varphi_1 U \varphi_2 \in closure(\varphi)\} = \emptyset$

hence all traces are accepting.

B consistent w.r.t. prop. logic

$\varphi_1 \wedge \varphi_2 \in B \Leftrightarrow \varphi_1 \in B$ and $\varphi_2 \in B$

$\psi \in B \Rightarrow \neg\psi \notin B$

$true \in closure(\varphi) \Rightarrow true \in B$

for all $\varphi_1 \wedge \varphi_2, \psi \in B$

B locally consistent w.r.t. U

$\varphi_2 \in B \Rightarrow \varphi_1 U \varphi_2 \in B$

$\varphi_1 U \varphi_2 \in B$ and $\varphi_2 \notin B \Rightarrow \varphi_1 \in B$

for all $\varphi_1 U \varphi_2 \in closure(\varphi)$

B is maximal:

$\psi \notin B \Rightarrow \neg\psi \in B$ for all $\psi \in closure(\varphi)$.

$\delta : Q \times 2^{AP} \to 2^Q$

$\langle q, A \rangle \mapsto \delta(q, A)$

e.g.

$\delta(B_2, \{a\})$

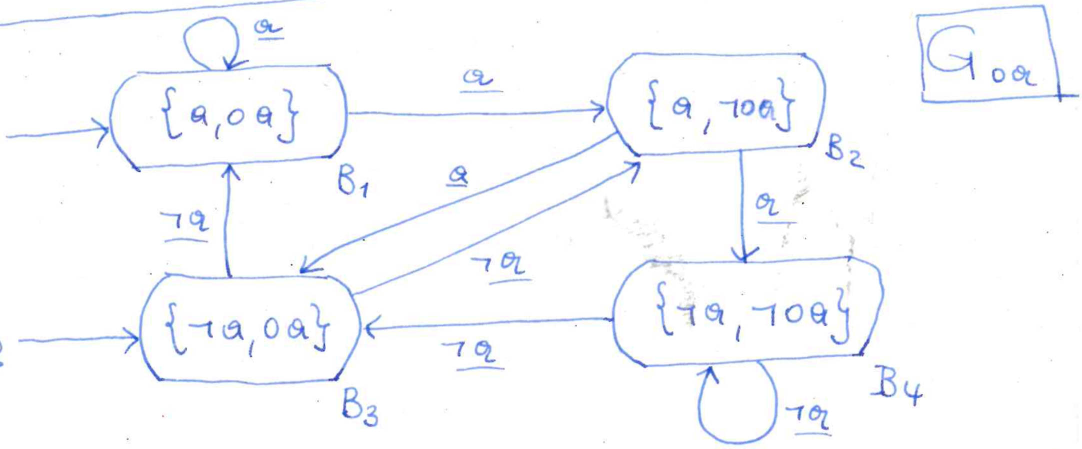
$= \{B_2^- \mid \circ\psi \in B_2 \Leftrightarrow \psi \in B_2^-$ for all $\psi \in cl(\varphi)\}$

$= \{B_2^- \mid \circ a \in B_2 \Leftrightarrow a \in B_2^-\}$

$= \{B_2^- \mid a \notin B_2^-\}$

$= \{B_2^- \mid \neg a \in B_2^-\}$

$= \{B_3, B_4\}$



$\sigma = \neg a \; a \; \neg a \; a \; \neg a \; \neg a \; \neg a \; a \; a \; a \; \neg a \ldots \in AP^\omega$

run of $\sigma = B_3 \; B_2 \; B_3 \; B_2 \; B_4 \; B_4 \; B_3 \; B_1 \; B_1 \; B_2 \ldots \in Q^\omega$

$\sigma = \neg a \; \neg a \; a \; a \ldots$

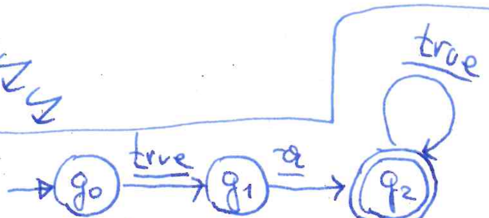
runs: B_1 ↯

$B_3 \; B_1$ ↯

$B_3 \; B_2$ ↯

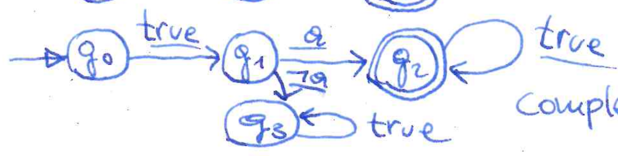
DBA

A 3-state NBA for $\circ a$ is:



incomplete

4-state NBA/DBA for $\circ a$ is:



complete

Example 2 $\varphi = a \,\mathsf{U}\, b$ $AP = \{a, b\}$

$\mathrm{closure}(\varphi) = \{a, b, \neg a, \neg b, a \,\mathsf{U}\, b, \neg(a \,\mathsf{U}\, b)\}$

$Q := \{B \subseteq \mathrm{closure}(\varphi) \,/\, B \text{ is elementary}\} = \{B_1, B_2, B_3, B_4, B_5\}$

$B_1 = \{a, b, \varphi\}$ $B_4 = \{a, \neg b, \neg\varphi\}$

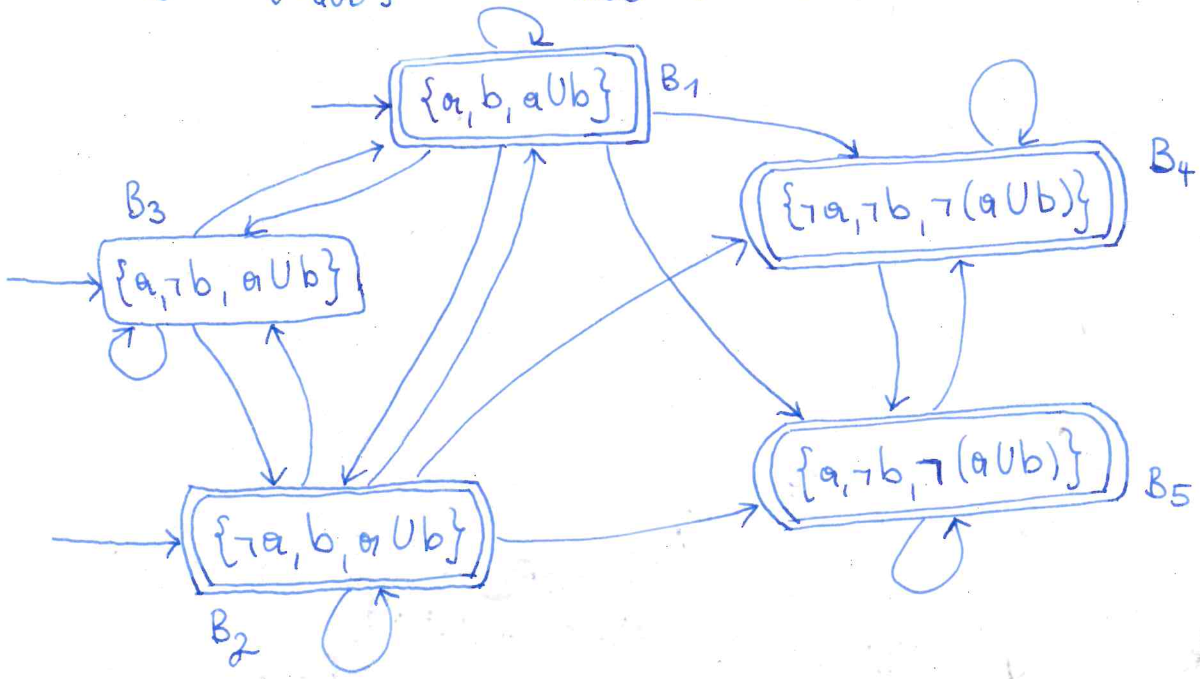
$B_2 = \{\neg a, b, \varphi\}$ $B_5 = \{\neg a, \neg b, \neg\varphi\}$

$B_3 = \{a, \neg b, \varphi\}$

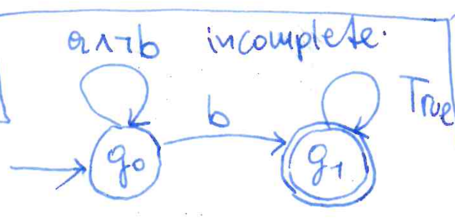
note that $\{\neg a, \neg b, \varphi\}$ and $\{\neg a, b, \neg\varphi\}$, $\{a, b, \neg\varphi\}$ are <u>not</u> locally consistent, hence not elementary.

$Q_0 := \{B \in Q \mid \varphi = a \,\mathsf{U}\, b \in B\} = \{B_1, B_2, B_3\}$

$\mathcal{F} := \{F_{a\mathsf{U}b}\}$ where $F_{a\mathsf{U}b} = \{B \in Q \mid a \,\mathsf{U}\, b \notin B \text{ or } b \in B\} = \{B_1, B_2, B_4, B_5\}$



A 2-state NBA for $\varphi = a \,\mathsf{U}\, b$ is:



is not a DBA, because $\xrightarrow{\neg a \wedge \neg b}$ transition is missing in q_0