UNIVERSITY OF OXFORD

EXAMINATION

COMPUTER SCIENCE

Automata, Logic and Games

Candidate Number: 39410

Hilary 2005

April 7, 2005

Question 1

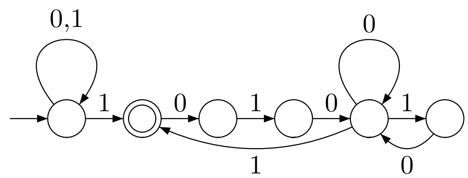
(a) $\alpha \in L$ if and only if after some position k, α does not contain any occurrence of 11 and contains infinitely many occurrences of 101.

$\alpha \in [\![(0+1)^*.L']\!]$ where L' is the language recognizing the words containing infinitely many 101 but containing no occurrence of 11.

Consider $\beta \in L'$, after each occurrence of 101 in β there must be a 0 (since 11 is not allowed). Moreover, between two occurrences of 1010, the only two possible sequences of symbols are 0 and 10, this corresponds to the regular expression $(0+10)^*$.

Therefore $L' = [\![(1010(0+10)^*)^\omega]\!]$ and $L = [\![(0+1)^* \, (1010(0+10)^*)^\omega]\!]$

The following Büchi-automaton recognizes this language:



(b) Suppose that a deterministic automaton $A = (Q, \{0,1\}, q0, \delta, F)$ recognizes L. Then δ is a function and we can extend it to a function $Q \times \{0,1\} \rightarrow Q$ returning the state reached after reading a given sequence of symbols from a given state.

A must accept $(101)^\omega$, therefore there is a word $w_1 \in \Sigma^*$ such that $\delta(q_0, w_1) \in F$, where w_1 is either $(101)^{n_1}$, $(101)^{n_1}1$ or $(101)^{n_1}10$ for some $n_1 \in \mathbb{N}$.

Again, A must accept $w_1.11(101)^\omega$ therefore, there is a word $w_2 \in \Sigma^*$ such that $\delta(q_0, w_1.11.w_2) \in F$, where w_2 is either $(101)^{n_2}$, $(101)^{n_2}1$ or $(101)^{n_2}10$ for some $n_2 \in \mathbb{N}$.

In this manner, we can create an infinite word $\alpha = w_1.11.w_2.11.\ldots.w_k.11.\ldots$ which is recognized by A since the corresponding run passes infinitely through states in F. This is a contradiction, since α contains infinitely many 11 and therefore cannot belong to L = L(A).

Question 2

We prove the result by contradiction. Suppose that $\phi(A, B)$, expressing that A and B have the same number of elements, is definable in S1S.

We define the S1S formula partition(A, B, C) stating that the sets A, B and C form a partition of ω:

$$\begin{aligned}\text{partition}(A,B,C) \quad = \quad & \forall x.(x \in A \ \vee \ x \in B \ \vee \ x \in C) \\ & \wedge \forall y. \neg \left((y \in A \ \wedge \ y \in B) \vee (y \in A \ \wedge \ y \in C) \vee (y \in B \ \wedge \ y \in C) \right)\end{aligned}$$

We define $\psi(X,Y)$ stating that after an occurrence of an element in Y there is no occurrence of an element in X:

$$\psi(X,Y) = \forall y. y \in Y \to (\forall x. x \geq y \to x \notin X)$$

We now consider the alphabet $\Sigma = \{0,1\}^3$. An infinite word α on Σ is defined by three tracks characterized by the sets A, B and C:

$$\forall x \in \omega : \alpha(x) = \begin{pmatrix} [x \in A] \\ [x \in B] \\ [x \in C] \end{pmatrix}$$

We use the following notation:

$$a = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, b = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \text{ and } c = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

Then the following formula denotes the language $L = \{a^n b^n c^\omega | n \in \mathbb{N}\}$:

$$\text{partition}(A,B,C) \wedge \psi(A,B) \wedge \psi(B,C) \wedge \psi(A,C) \wedge (\exists z. z \in C)$$

Hence L is S1S definable and therefore there is a non-deterministic Büchi automaton recognizing L (by theorem 3.3 of the the lecture's notes).

This is a contradiction since L is not regular. Indeed, suppose that a Büchi-automaton A with m states recognizes L. Take $n > m$, then $a^n b^n c^\omega \in L$. After reading the first n symbols a, the automaton has visited twice a particular state. Suppose this state has been visited after reading a^i and after reading a^j with $i < j \leq n$. We know that $a^i b^i c^\omega \in L$. Since A is in the same state after reading a^i and a^j, we also have $a^j b^i c^\omega \in L$ too. This is a contradiction since $i < j$.

Question 3

(a) Let us define the following two operators:

$$A \oplus B \triangleq (A \vee B) \wedge \neg(A \wedge B)$$

$$A \leftrightarrow B \triangleq \neg(A \oplus B)$$

Then the following formula $\phi(X,Y,Z)$ expresses that the numbers a,b and c represented respectively by the finite sets X,Y and Z are related by the equation $a + b = c$:

$$\begin{aligned} \phi(X,Y,Z) \quad &= \quad \exists R | 0 \notin R \\ &\wedge \quad \forall b.\ b \in Z \leftrightarrow [(b \in X) \oplus (b \in Y) \oplus (b \in R)] \\ &\wedge \quad \forall b.\ \mathbf{s}\, b \in R \leftrightarrow ([(b \in X) \wedge (b \in Y)] \vee [(b \in X) \wedge (b \in R)] \vee [(b \in Y) \wedge (b \in R)]) \end{aligned}$$

The first line states that there is a set R defining the value of the reminder for every step of the binary addition. $0 \notin R$ means that there is no reminder for the computation of the digit 0 of c. The second line defines how the semi-addition is done and the third line defines how the reminder is calculated at every step.

(b) For any first-order formula ψ over the structure $(\omega, +)$, we can construct an equivalent S1S formula $F(\psi)$ as follow:

Let x, y and z be first order variables, we define corresponding second order μ-calculus variables X, Y and Z. F is defined recursively as follow:

$$\begin{array}{rcl} F(\psi_1 \wedge \psi_2) & = & F(\psi_1) \wedge F(\psi_2) \\ F(\psi_1 \vee \psi_2) & = & F(\psi_1) \vee F(\psi_2) \\ F(\neg\psi) & = & \neg F(\psi) \\ F(\forall x.\psi) & = & \forall X.F(\psi) \\ F(\exists x.\psi) & = & \exists X.F(\psi) \\ F(x + y = z) & = & \phi(X, Y, Z) \\ F(x) & = & X \end{array}$$

Moreover for any constant $n \in \omega$ we define $F(n)$ as the set of numbers corresponding to the position of 1's in the binary representation of n:

$F(n) = \{k \in \mathbb{N} |$ the k^{th} binary digit in the binary representation of n is a $1\}$

A Presburger arithmetic formula $\phi(x_1, \ldots, x_n)$ can be transformed into the S1S formula $F(\phi(x_1, \ldots, x_n)) = \psi(X_1, \ldots X_n)$. From this S1S formula, we can construct the Büchi automaton A_ψ defines in slide 3-17 of the lecture's note. The language recognized by this automaton is not empty if and only if the formula ψ is satisfiable. Hence, since non-emptyness is decidable for Büchi automata (theorem 1.6), Presburger arithmetic is decidable.

(c) What we proved is that when we encode numbers into sets, we can decide whether the second-order variable X, Y and Z encode numbers satisfying the relation $x + y = z$.

But if x, y and z are first-order variables then the natural number addition $x + y = z$ on these first-order variables is not definable in S1S.

Question 4

See answer on the attached sheets.

Question 5

(a) We define the following two functions:

$$\begin{array}{rcl}\Phi(X,Z) & = & [a]((Z \vee \langle b\rangle t) \wedge X) \\ \phi(X) & = & \mu Z.\Phi(X,Z)\end{array}$$

Let us first do some preliminary computations:

– We have:

$$\begin{array}{rcl}\|\mu^0 Z.\Phi(S,Z)\|_\emptyset^T & = & \emptyset \\ \|\mu^1 Z.\Phi(S,Z)\|_\emptyset^T & = & \|[a](\underbrace{\langle b\rangle t}_{\{1\}})\|_\emptyset^T = \{2\} \\ \|\mu^2 Z.\Phi(S,Z)\|_\emptyset^T & = & \|[a](\underbrace{\{2\} \vee \{1\}}_{\{1,2\}})\|_\emptyset^T = \{1,2\} \\ \|\mu^3 Z.\Phi(S,Z)\|_\emptyset^T & = & \|[a](\{1,2\} \vee \{1\})\|_\emptyset^T = \{1,2\}\end{array}$$

therefore:

$$\|\phi(S)\|_\emptyset^T = \|\mu Z.\Phi(S,Z)\|_\emptyset^T \quad = \quad \{1,2\} \tag{1}$$

– moreover:

$$\begin{array}{rcl}\|\mu^0 Z.\Phi(\{1,2\},Z)\|_\emptyset^T & = & \emptyset \\ \|\mu^1 Z.\Phi(\{1,2\},Z)\|_\emptyset^T & = & \|[a](\{1\} \wedge \{1,2\})\|_\emptyset^T = \|[a](\{1\})\|_\emptyset^T = \{2\} \\ \|\mu^2 Z.\Phi(\{1,2\},Z)\|_\emptyset^T & = & \|[a]((\{2\} \vee \{1\}) \wedge \{1,2\})\|_\emptyset^T = \|[a](\{1,2\})\|_\emptyset^T = \{1,2\} \\ \|\mu^3 Z.\Phi(\{1,2\},Z)\|_\emptyset^T & = & \|[a]((\{1,2\} \vee \{1\}) \wedge \{1,2\})\|_\emptyset^T = \|[a](\{1,2\})\|_\emptyset^T = \{1,2\}\end{array}$$

therefore:

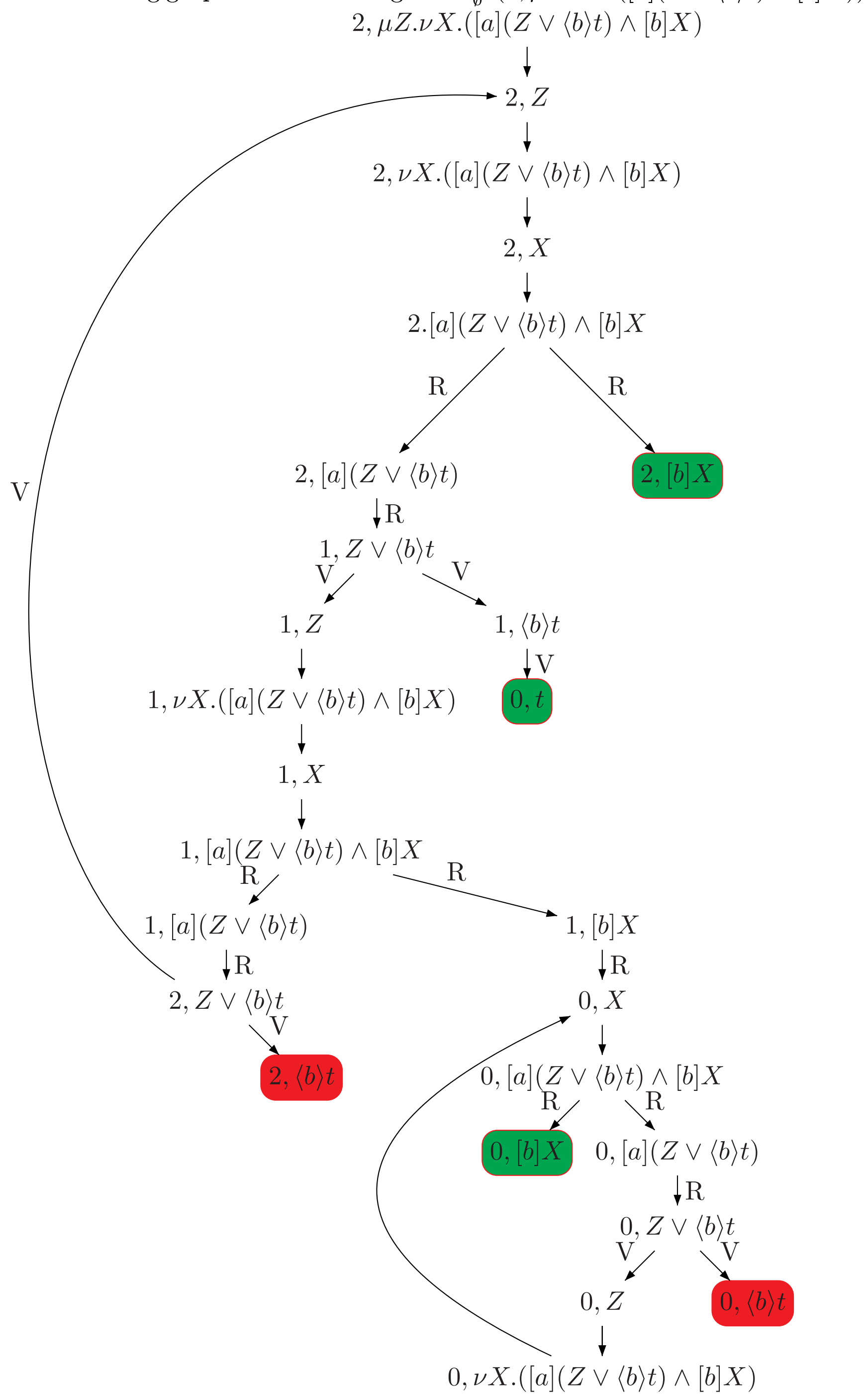
$$\|\phi(\{1,2\})\|_\emptyset^T = \|\mu Z.\Phi(\{1,2\},Z)\|_\emptyset^T = \{1,2\} \tag{2}$$

We can compute the fixpoint approximants for $\|\nu X.\phi(X)\|_\emptyset^T$:

$$\begin{array}{rcl}\|\nu^0 X.\phi(X)\|_\emptyset^T & = & S \\ \|\nu^1 X.\phi(X)\|_\emptyset^T & = & \|\phi(S)\|_\emptyset^T = \{1,2\} \quad \text{(equation 1)} \\ \|\nu^2 X.\phi(X)\|_\emptyset^T & = & \|\phi(\{1,2\})\|_\emptyset^T = \{1,2\} \quad \text{(equation 2)}\end{array}$$

Hence $\|\nu X.\phi(X)\|_\emptyset^T = \{1,2\}$.

(b) The following graph describes the game $\mathcal{G}^T_\emptyset\,(2, \mu Z.\nu X.([a](Z \vee \langle b \rangle t) \wedge [b]X))$:



The green position correspond to the verifier's winning positions, the red positions correspond to the refuter's winning position.

We recall theorem 5.2 from the notes:

Theorem 1 *1. $s \models_V^T \phi$ iff player V has as history-free winning strategy for $\mathcal{G}_V^T(s,\phi)$*

2. $s \not\models_V^T \phi$ iff player R has as history-free winning strategy for $\mathcal{G}_V^T(s,\phi)$

V has a history-free winning strategy for $\mathcal{G}_\emptyset^T(2, \mu Z.\nu X.([a](Z \vee \langle b\rangle t) \wedge [b]X))$ consisting in choosing the position "$1, \langle b\rangle t$" when the game is at position "$1, Z \vee \langle b\rangle t$". Hence $2 \models \mu Z.\nu X.([a](Z \vee \langle b\rangle t) \wedge [b]X)$.

Question 6

(a)

$$\begin{aligned}
\alpha \models \mathbf{X}\phi \to \mathbf{X}\psi &\iff (\alpha \models \mathbf{X}\phi) \Longrightarrow (\alpha \models \mathbf{X}\psi)\\
&\iff (\alpha^1 \models \phi) \Longrightarrow (\alpha^1 \models \psi)\\
&\iff \alpha^1 \models (\phi \to \psi)\\
&\iff \alpha \models \mathbf{X}(\phi \to \psi)
\end{aligned}$$

(b)

$$\begin{aligned}
\alpha \models \phi \,\mathbf{R}\, \psi &\iff \forall k \geq 0.(\alpha^k \models \psi \ \vee\ \exists i : 0 \leq i < k.\alpha^i \models \phi)\\
&\iff \left[\alpha \models \psi \ \vee\ \overbrace{\exists i : 0 \leq i < 0.\alpha^i \models \phi}^{false}\right] \qquad (k=0)\\
&\qquad \wedge \underbrace{\forall k > 0.(\alpha^k \models \psi \ \vee\ \exists i : 0 \leq i < k.\alpha^i \models \phi)}_{A}\\
&\iff \alpha \models \psi \wedge [(A \wedge \alpha \models \psi) \vee (A \wedge \alpha \not\models \psi)] \qquad (3)
\end{aligned}$$

- Since

$$\alpha \models \phi \qquad \Longrightarrow \qquad \left[\forall k > 0.\exists i : 0 \leq i < k.\alpha^i \models \phi\right] \equiv A$$

we have $(A \wedge \alpha \models \psi) \quad \equiv \quad \alpha \models \phi$.

- Moreover,

$$\begin{aligned}
A \wedge \alpha \not\models \phi &\Longrightarrow \forall k > 0.(\alpha^k \models \psi \vee \exists i : 0 < i < k.\alpha^i \models \phi)\\
&\overset{k \leftarrow k-1}{\iff} \forall k \geq 0.(\alpha^{k+1} \models \psi \vee \exists i : 0 < i < k+1.\alpha^i \models \phi)\\
&\overset{i \leftarrow i-1}{\iff} \forall k \geq 0.(\alpha^{k+1} \models \psi \vee \exists i : 0 \leq i < k.\alpha^{i+1} \models \phi)\\
&\iff \forall k \geq 0.((\alpha^1)^k \models \psi \vee \exists i : 0 \leq i < k.(\alpha^1)^i \models \phi)\\
&\overset{R\text{ def.}}{\iff} \alpha^1 \models \phi \,\mathbf{R}\, \psi\\
&\Longrightarrow \alpha \models \mathbf{X}(\phi \,\mathbf{R}\, \psi)
\end{aligned}$$

By plugging these two results into equation 3 we obtain the desired result:

$$\alpha \models \phi \ \mathbf{R} \ \psi \Longrightarrow \alpha \models \psi \wedge [\alpha \models \phi \vee \alpha \models \mathbf{X}(\phi \ \mathbf{R} \ \psi)]$$

(c) We first prove the identity f $\mathbf{R}$ $\phi = \mathbf{G}\phi$:

$$\begin{aligned} \alpha \models \mathrm{f}\ \mathbf{R}\ \phi \quad &\Longleftrightarrow \quad \forall k \geq 0.\alpha^k \models \phi \ \vee \ \exists i : 0 \leq i < k : \alpha^i \models \mathrm{f} \\ &\Longleftrightarrow \quad \forall k \geq 0.\alpha^k \models \phi \\ &\Longleftrightarrow \quad \alpha \models \mathbf{G}\phi \end{aligned}$$

Hence:

$$\begin{aligned} \mathrm{f}\ \mathbf{R}\ (\phi \wedge \mathbf{X}\phi) \rightarrow (\phi \rightarrow \mathrm{f}\ \mathbf{R}\phi) \quad &\equiv \quad \mathbf{G}(\phi \wedge \mathbf{X}\phi) \rightarrow (\phi \rightarrow \mathbf{G}\phi) \\ &\equiv \quad \mathbf{G}\phi \rightarrow (\phi \rightarrow \mathbf{G}\phi) \\ &\equiv \quad (\mathbf{G}\phi \wedge \phi) \rightarrow (\mathbf{G}\phi) \\ &\equiv \quad \mathbf{G}\phi \rightarrow (\mathbf{G}\phi) \\ &\equiv \quad \mathbf{true} \end{aligned}$$

(d) **Claim**: $\phi \ \mathbf{R} \ \psi \equiv \mathbf{G}(\neg\phi \wedge \psi) \ \vee \ (\neg\phi \wedge \psi)\mathbf{U}(\phi \wedge \psi)$

Proof: We first note that $\phi \ \mathbf{R} \ \psi \equiv [(\phi \ \mathbf{R} \ \psi) \wedge \mathbf{G}\neg\phi] \ \vee \ [(\phi \ \mathbf{R} \ \psi) \wedge \mathbf{F}\phi]$

- We have $(\phi \ \mathbf{R} \ \psi) \wedge \mathbf{G}\neg\phi \ \equiv \ \mathbf{G}(\neg\phi \wedge \psi)$, indeed:

$$\begin{aligned} \alpha \models (\phi \ \mathbf{R} \ \psi) \wedge \mathbf{G}\neg\phi \quad &\Longleftrightarrow \quad \big(\forall k \geq 0.\alpha^k \models \psi \vee \exists i : 0 \leq i < k.\alpha^i \models \phi\big) \wedge (\forall l \geq 0 : \alpha^l \models \neg\phi) \\ &\Longleftrightarrow \quad \forall k \geq 0 : (\alpha^k \models \psi \wedge \forall l \geq 0 : \alpha^l \models \neg\phi) \\ &\qquad \vee \underbrace{\big[(\exists i : 0 \leq i < k.\alpha^i \models \phi) \wedge (\forall l \geq 0 : \alpha^l \models \neg\phi)\big]}_{false} \\ &\Longleftrightarrow \quad \forall k \geq 0 : \alpha^k \models \psi \wedge \forall l \geq 0 : \alpha^l \models \neg\phi \\ &\Longleftrightarrow \quad \alpha \models \mathbf{G}(\neg\phi \wedge \psi) \end{aligned}$$

- moreover $(\phi \ \mathbf{R} \ \psi) \wedge \mathbf{F}\phi \ \equiv \ (\neg\phi \wedge \psi)\mathbf{U}(\phi \wedge \psi)$, indeed:

$$\begin{aligned} \alpha \models (\phi \ \mathbf{R} \ \psi) \wedge \mathbf{F}\phi \quad &\Longleftrightarrow \quad (\forall k \geq 0 : \alpha^k \models \psi \vee \exists i : 0 \leq i < k : \alpha^i \models \phi) \\ &\qquad \wedge(\exists i_0.\alpha^{i_0} \models \phi \wedge \forall j < i_0 : \alpha^j \models \neg\phi) \\ &\Longleftrightarrow \quad \exists i_0.\alpha^{i_0} \models \phi \wedge (\forall j < i_0 : \alpha^j \models \neg\phi) \\ &\qquad \wedge(\forall k \geq 0 : \alpha^k \models \psi \vee \exists i : 0 \leq i < k : \alpha^i \models \phi) \\ &\Longleftrightarrow \quad \exists i_0.\alpha^{i_0} \models \phi \wedge (\forall j < i_0 : \alpha^j \models \neg\phi) \\ &\qquad \wedge(\forall k < i_0 : \alpha^k \models \psi \vee \exists i : 0 \leq i < k : \alpha^i \models \phi) \\ &\qquad \wedge(\alpha^{i_0} \models \psi \vee \exists i : 0 \leq i < i_0 : \alpha^i \models \phi) \\ &\qquad \wedge(\forall k > i_0 : \alpha^k \models \psi \vee \exists i : 0 \leq i < k : \alpha^i \models \phi) \\ &\Longleftrightarrow \quad \exists i_0.\alpha^{i_0} \models \phi \wedge (\forall j < i_0 : \alpha^j \models \neg\phi) \end{aligned}$$

$$
\begin{aligned}
&& &\wedge \forall k < i_0 : \alpha^k \models \psi \\
&& &\wedge \alpha^{i_0} \models \psi \\
&& &\wedge (\forall k > i_0 : \alpha^k \models \psi \vee \exists i : 0 \leq i < k : \alpha^i \models \phi) \\
&\iff & &\exists i_0 . \alpha^{i_0} \models \phi \wedge (\forall j < i_0 : \alpha^j \models \neg\phi) \\
&& &\wedge \forall k < i_0 : \alpha^k \models \psi \\
&& &\wedge \alpha^{i_0} \models \psi \\
&& &\wedge \forall k > i_0 . \\
&& &\quad [\big(\alpha^{i_0} \models \phi \wedge \alpha^k \models \psi\big) \vee \underbrace{\big(\alpha^{i_0} \models \phi \wedge \exists i : 0 \leq i < k : \alpha^i \models \phi\big)}_{\alpha^{i_0} \models \phi}] \\
&\iff & &\exists i_0 . \alpha^{i_0} \models \phi \wedge (\forall j < i_0 : \alpha^j \models \neg\phi) \\
&& &\wedge \quad \forall k < i_0 : \alpha^k \models \psi \\
&& &\wedge \quad \alpha^{i_0} \models \psi \\
&& &\wedge \quad \underbrace{\big(\alpha^{i_0} \models \phi \wedge \forall k > i_0 . \alpha^k \models \psi\big) \vee \alpha^{i_0} \models \phi}_{\alpha^{i_0} \models \phi} \\
&\iff & &\exists i_0 . (\forall j < i_0 : \alpha^j \models \neg\phi) \wedge (\forall k < i_0 : \alpha^k \models \psi) \\
&& &\wedge \quad \alpha^{i_0} \models (\psi \wedge \phi) \\
&\iff & &\exists i_0 . \forall j < i_0 : \alpha^j \models \neg\phi \wedge \psi \\
&& &\wedge \quad \alpha^{i_0} \models (\psi \wedge \phi) \\
&\iff & &\alpha \models (\neg\phi \wedge \psi)\mathbf{U}(\phi \wedge \psi)
\end{aligned}
$$

■

Question 7

Suppose that a formula ϕ has a model. Then there is a transition system $T = \langle S, \rightarrow, \rho \rangle$ and a state $r \in S$ such that $r \models_T \phi$.

- The model T can be unwound into a tree rooted at r: the graph of the transition system is browsed from r in a breadth-first search manner, every time we reach an edge $s \rightarrow t$ where t has already been visited, we replace the edge $s \rightarrow t$ by an edge pointing to a newly created tree obtained by unwinding the LTS at state t. This process clearly removes all the cycles in the graph, hence the resulting model is a tree but possibly with an infinite depth.

  It is also obvious that s satisfies ϕ in this new model: for a given state, the possible outcomes are the same in the two models.

- We need to prove that the resulting tree has a bounded width.

  We achieve this by assuming with no proof that the small model property is true for the modal μ-calculus.

The small model property states that if a formula has a model then it has a model with finite number of states.

By unwinding the finite model, we obtain a tree model with possibly infinite depth (if there are loops in the finite model) but with a bounded width. Indeed, the unwinding process preserves the number of outgoing edges for a node: there may be infinitely many copies of a node but for all these copies, the number of outgoing edges is the same as the original node. The number of outgoing edges for a node is clearly bounded by $|S|.|\mathcal{L}|$ where $\mathcal{L}$ is the labeling set.