Bernd Finkbeiner Date: May 17, 2011

Automata, Games and Verification: Lecture 6

---

7 McNaughton's Theorem (Cont'd)

Lemma 1 *For every semi-deterministic Büchi automaton $\mathcal{A}$ there exists a deterministic Muller automaton $\mathcal{A}'$ with $\mathcal{L}(\mathcal{A}) = \mathcal{L}(\mathcal{A}')$.*

Proof:

Let $\mathcal{A} = (N \uplus D, I, T, F)$, $d = |D|$, and let D be ordered by $<$. We construct the DMA $(S', \{s'_0\}, T', \mathcal{F})$:

- $S' = 2^N \times \{0, \ldots, 2d\} \to D \cup \{\llcorner\!\lrcorner\}$
- $s'_0 = (\{N \cap I\}, (d_1, d_2, \ldots, d_n, \llcorner\!\lrcorner, \ldots, \llcorner\!\lrcorner))$,
  where $d_i < d_{i+1}, \{d_1, \ldots, d_n\} = D \cap I\}$.
- $T' = \{((N_1, f_1), \sigma, (N_2, f_2)) \mid N_2 = pr_3(T \cap N_1 \times \{\sigma\} \times N)$
  $D' = pr_3(T \cap N_1 \times \{\sigma\} \times D)$
  $g_1 : n \mapsto d_2 \in D \Leftrightarrow f_1 : n \mapsto d_1 \in D \wedge d_1 \to^\sigma d_2$
  g_2: insort the elements of D' in the empty slots of g_1 (using $<$)
  f_2: delete every recurrance (leaving an *empty* slot)
- $\mathcal{F} = \{F' \subseteq S' \mid \exists i \in 1, \ldots, 2d$ s.t.
  $f(i) \neq \llcorner\!\lrcorner$ for all $(N', f) \in F'$ and
  $f(i) \in F$ for some $(N', f) \in F'\}$.

$\mathcal{L}(\mathcal{A}) \subseteq \mathcal{L}(\mathcal{A}')$:
If $\alpha \in \mathcal{L}(\mathcal{A})$, $\mathcal{A}$ has an accepting run $r = n_0 \ldots n_{j-1} d_j d_{j+1} d_{j+2} \ldots$
where $n_k \in N$ for $k < j$ and $d_k \in D$ for $k \geq j$.
Consider the run $r' = (N_0, f_0), (N_1, f_1), \ldots$ of $\mathcal{A}'$ on α.

- $n_k \in N_k$ for all $k < j$,
- for all $k \geq j$, $d_k = f_k(i)$ for some $i \leq 2d$,
- these i's are non-increasing, and hence stabilize eventually.
- for this stable i,
  $f(i) \neq \llcorner\!\lrcorner$ for all $(N', f) \in In(r')$ and $f(i) \in F$ for some $(N', f) \in In(r')$.
- $In(r') \in \mathcal{F}$.

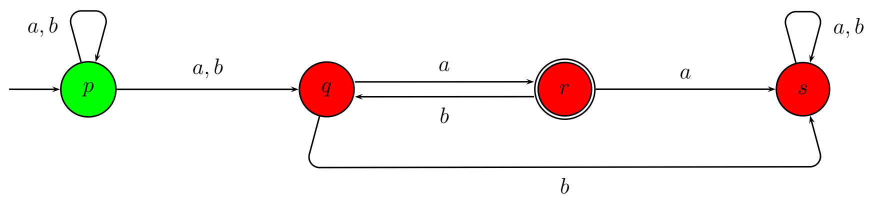
$\mathcal{L}(\mathcal{A}') \subseteq \mathcal{L}(\mathcal{A})$:
For $\alpha \in \mathcal{L}(\mathcal{A}')$, $\mathcal{A}'$ has an accepting run $r' = (N_0, f_0), (N_1, f_1), \ldots$.

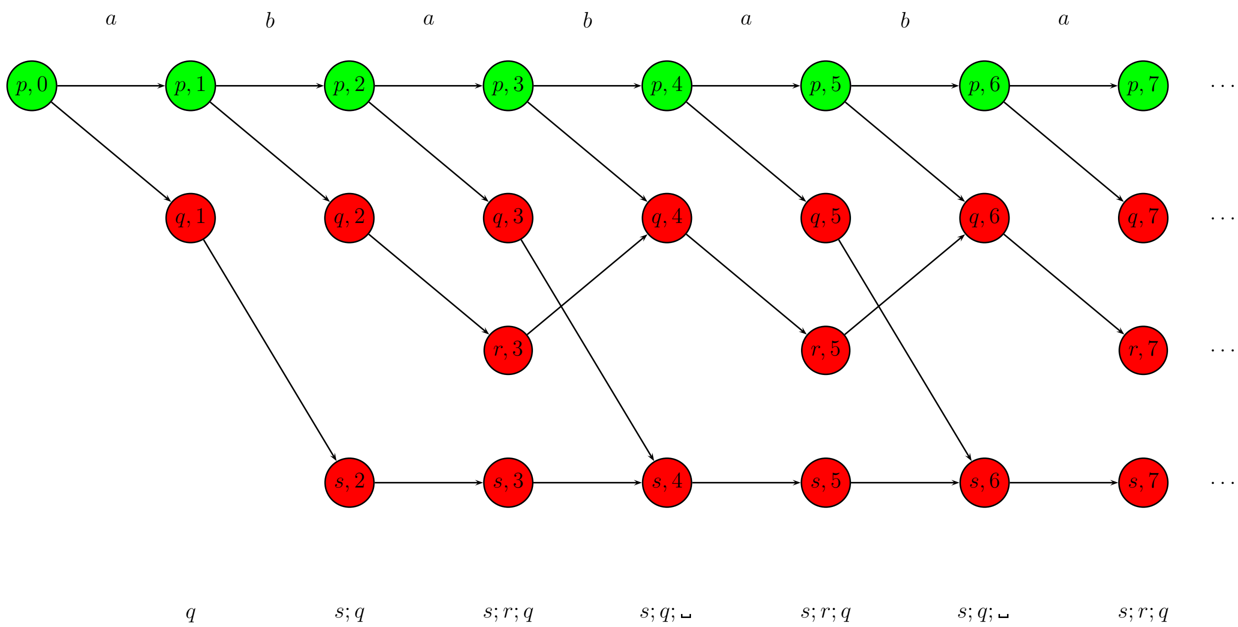
- We pick an i and an accepting set $F' \in \mathcal{F}$ s.t.
  $f(i) \neq \llcorner\!\lrcorner$ for all $(N', f) \in F'$ and $f(i) \in F$ for some $(N', f) \in F'$.

- We pick a $j \in \omega$ such that $f_n(i) \neq \textvisiblespace$ for all $n > j$.
- There is a run $r = s_0 s_1 \ldots s_j f_{j+1}(i) f_{j+2}(i) f_{j+3}(i) \ldots$ of $\mathcal{A}$ for α.
- r is accepting.

■

Example:





8 Linear-Time Temporal Logic (LTL)

1977: Amir Pnueli, *The temporal logic of programs* (Turing award 1996)

Syntax:

- Given a set of atomic propositions AP.
- Any atomic proposition $p \in AP$ is an LTL formula

- If φ, ψ are LTL formulars then so are
  - $\neg\varphi,\ \varphi \wedge \phi$,
  - $\bigcirc\varphi,\ \varphi\,\mathcal{U}\,\psi$

Abbreviations:
$\Diamond\varphi \ \equiv \ \mathit{true}\,\mathcal{U}\,\varphi$;
$\Box\,\varphi \ \equiv \ \neg(\Diamond\neg\varphi)$;
$\varphi\,\mathcal{W}\,\psi \ \equiv \ (\varphi\,\mathcal{U}\,\psi) \vee \Box\varphi$;

The *temporal operators:*

$\bigcirc$	X	Next
$\Box$	G	Always
$\Diamond$	F	Eventually
$\mathcal{U}$		Until
$\mathcal{W}$		Weak Until

Semantics: LTL formulas are interpreted over ω-words over 2^{AP}.
Notation: $\alpha, i \vDash \varphi$, where $\alpha \in (2^{AP})^{\omega}, i \in \omega$.

- $\alpha, i \vDash p$ if $p \in \alpha(i)$;
- $\alpha, i \vDash \neg\varphi$ if $\alpha, i \nvDash \varphi$;
- $\alpha, i \vDash \varphi \wedge \psi$ if $\alpha, i \vDash \varphi$ and $\alpha, i \vDash \psi$;
- $\alpha, i \vDash \bigcirc\varphi$ if $\alpha, i+1 \vDash \varphi$
  $\alpha, i \vDash \varphi\,\mathcal{U}\,\psi$ if there is some $j \geq i$ s.t. $\alpha, j \vDash \psi$ and for all $i \leq k < j$: $\alpha, k \vDash \varphi$

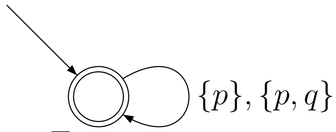
Abbreviation: $\alpha \vDash \varphi \ \equiv \ \alpha, 0 \vDash \varphi$

Definition 1

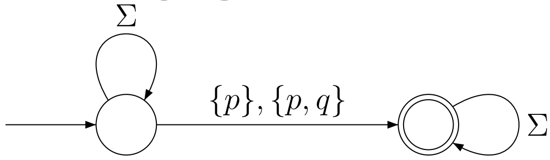
- *models*(φ)=$\{\alpha \in (2^{AP})^{w} \mid \alpha \vDash \varphi\}$
- *an LTL formula φ is* satisfiable *if models*$(\varphi) \neq \emptyset$
- *an LTL formula φ is* valid *if models*$(\varphi) = (2^{AP})^{\omega}$

Example: LTL formulas with $AP = \{p, q\}$:

- Safety: $\Box p$



- Guarantee: $\Diamond p$



There are Büchi recognizable languages that are not LTL-definable.
Example: $(\emptyset\emptyset)^*\{p\}^\omega$

Definition 2 *A language* $L \subseteq \Sigma^\omega$ *is* non-counting *iff*
$\exists n_0 \in \omega \ . \ \forall n \geq n_0 \ . \ \forall u, v \in \Sigma^*, \gamma \in \Sigma^\omega \ .$
$uv^n\gamma \in L \ \Leftrightarrow \ uv^{n+1}\gamma \in L$

Example: $L = (\emptyset\emptyset)^*\{p\}^\omega$ is counting. For every $\emptyset^n\{p\}^\omega \in L$, $\emptyset^{n+1}\{p\}^\omega \notin L$.

Theorem 1 *For every LTL-formula φ, models(φ) is non-counting.*

Proof:

Structural induction on φ:

- $\varphi = p$: choose $n_0 = 1$.
- $\varphi = \varphi_1 \wedge \varphi_2$: By IH, φ_1 defines non-counting language with threshold $n_0' \in \omega$, φ_2 with n_0''; choose $n_0 = \max(n_0', n_0'')$;
- $\varphi = \neg\varphi_1$: choose $n_0 = n_0'$.
- $\varphi = \bigcirc\varphi_1$: choose $n_0 = n_0' + 1$.
  - We show for $n \geq n_0$: $uv^n\gamma \models \bigcirc\varphi \ \Leftrightarrow \ uv^{n+1}\gamma \models \bigcirc\varphi$.
  - Case $u \neq \epsilon$, i.e., $u = au'$ for some $a \in \Sigma, u' \in \Sigma^*$:
    $au'v^n\gamma \models \bigcirc\varphi$
    iff $u'v^n\gamma \models \varphi$
    iff $u'v^{n+1}\gamma \models \varphi$ (IH)
    iff $au'v^{n+1}\gamma \models \bigcirc\varphi$.
  - Case $u = \epsilon, v = av'$ for some $a \in \Sigma, v' \in \Sigma^*$:
    $(av')^n\gamma \models \bigcirc\varphi$
    iff $(av')(av')^{n-1}\gamma \models \bigcirc\varphi$
    iff $v'(av')^{n-1}\gamma \models \varphi$
    iff $v'(av')^n\gamma \models \varphi$ (IH)
    iff $(av')^{n+1}\gamma \models \bigcirc\varphi$.

- $\varphi = \varphi_1 \mathcal{U}\ \varphi_2$: choose $n_0 = \max(n_0', n_0'') + 1$.
  Claim: for $n \geq n_0$: $uv^n\gamma \models \varphi_1 \mathcal{U}\ \varphi_2 \ \Rightarrow\ uv^{n+1}\gamma \models \varphi_1 \mathcal{U}\ \varphi_2$.
  - $uv^n\gamma \models \varphi_1 \mathcal{U}\ \varphi_2 \ \Rightarrow\ \exists j\ .\ uv^n\gamma, j \models \varphi_2$ and $\forall i < j\ .\ uv^n\gamma, i \models \varphi_1$.
  - Let j be the least such index.
  - Case $j \leq |u|$:
    by IH, $uv^{n+1}\gamma, j \models \varphi_2$ and for all $i < j\ .\ uv^{n+1}\gamma, i \models \varphi_1$;
  - Case $j > |u|$:
    $uv^{n+1}\gamma, j + |v| \models \varphi_2$ (because $uv^{n+1}\gamma$ has the same suffix from position $j + |v|$ as uv^{n+1} from position j);
    for all $|u| + |v| \leq i < j + |v|\ .\ uv^{n+1}\gamma, i \models \varphi_1$ (again, because the suffix is the same);
    By (IH), for all $i < |u|+|v|, i < j\ .\ uvv^n\gamma, i \models \varphi_1$, because $uvv^{n-1}\gamma, i \models \varphi_1$.

  Claim: for $n \geq n_0$: $uv^{n+1}\gamma \models \varphi_1 \mathcal{U}\ \varphi_2 \ \Rightarrow\ uv^n\gamma \models \varphi_1 \mathcal{U}\ \varphi_2$
  - $uv^{n+1}\gamma \models \varphi_1 \mathcal{U}\ \varphi_2 \ \Rightarrow\ \exists j\ .\ uv^{n+1}\gamma, j \models \varphi_2$ and $\forall i < j\ .\ uv^{n+1}\gamma, i \models \varphi_1$.
  - Case $j \leq |u| + |v|$:
    by IH, $uvv^{n-1}, j \models \varphi_2$ and for all $i < j\ .\ uvv^{n-1}, i \models \varphi_1$;
  - Case $j > |u| + |v|$:
    $uv^n\gamma, j - |v| \models \varphi_2$;
    for all $|u| + |v| \leq i < j\ .\ uv^n\gamma, i \models \varphi_1$;
    By (IH), for all $i < |u| + |v|\ .\ uvv^{n-1}\gamma, i \models \varphi_1$, because $uvv^n\gamma, i \models \varphi_1$.

■

9 Quantified Propositional Temporal Logic (QPTL)

Syntax: LTL formula | $\varphi \wedge \varphi$ | $\neg\varphi$ | $\exists p.\ \varphi$

Semantics:

$\alpha, i \models \exists q.\varphi$ iff there is an α' with
$\alpha'(j) \cap (AP \setminus \{q\}) = \alpha(j) \cap (AP \setminus \{q\})$ for all $j \in \omega$,
s.t. $\alpha', i \models \varphi$.