On w-Automata and Temporal Logic

S. Safra — Weizmann Inst.

M.Y. Vardi — IBM Almaden

Temporal Logic

TL : A logic for specifying ongoing computations.

◇ P : Eventually P will hold.

□ P : Henceforth P will hold

○ P : In the next moment P will hold.

Examples

□ (Requested → ◇ Granted) : Every request is eventually granted.

□ ◇ Requested → □ ◇ Granted : Every persistent request is eventually granted

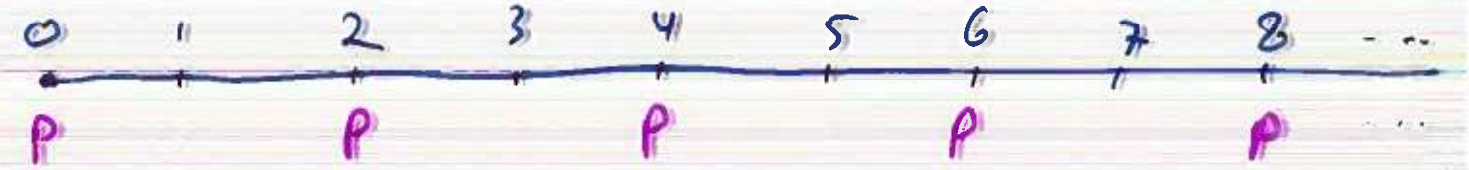
WEAKNESS

TL is not expressive enough for compositional verification.

EXAMPLE

The following is not expressible in TL:

"P holds in every even moment"



Extended Temporal Logic

Prop : a set of atomic propositions

- If $p \in Prop$, then p is a formula.
- If ψ_1 and ψ_2 are formulas, then $\sim\psi_1$ and $\psi_1 \wedge \psi_2$ are formulas.
- If $\psi_1, \ldots, \psi_m$ are formulas, $\Sigma = \{a_1, \ldots, a_n\}$ is an alphabet, and $L \subseteq \Sigma^\omega$ is an ω-regular language, then $L(\psi_1, \ldots, \psi_m)$ is a formula.

Semantics

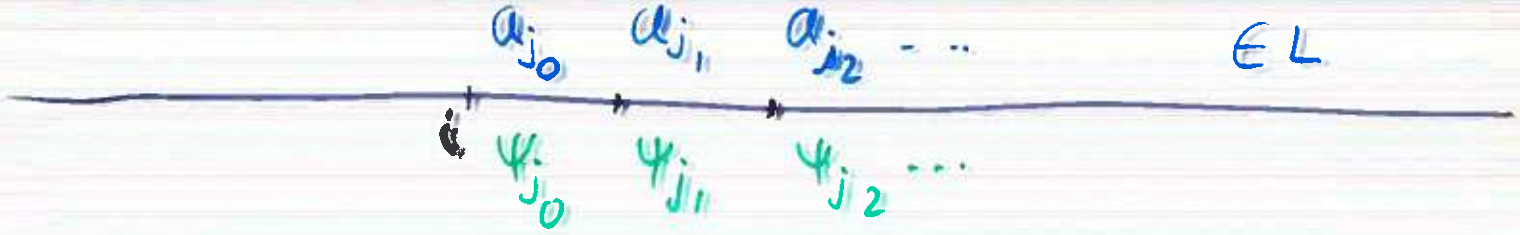
Computation - an infinite sequence of truth assignments: $\sigma : \omega \to 2^{Prop}$.

$\sigma, i \models \varphi$: φ holds at point i of σ.

- $\sigma, i \models P$ if $P \in \sigma(i)$.
- $\sigma, i \models \Psi_1 \wedge \Psi_2$ if $\sigma, i \models \Psi_1$ and $\sigma, i \models \Psi_2$.
- $\sigma, i \models \neg \Psi$ if $\sigma, i \not\models \Psi$.
- $\sigma, i \models L(\Psi_1, \dots, \Psi_m)$ if $\exists\, w \in L$, $w(k) = a_{j_k}$, such that $\sigma, i+k \models \Psi_{j_k}$ for all $k \geq 0$.

Example: $\Sigma = \{a\}$, $L = \Sigma^{\omega}$

$L(\Psi) \equiv \Box \Psi$


α_{j_0}
α_{j_1}
α_{j_2} ...
$\in L$
ψ_{j_0}
ψ_{j_1}
ψ_{j_2} ...

Automata

Table: $T = (\Sigma, S, S_0, \rho)$

Σ - alphabet

S - state set

$S_0 \subseteq S$ - initial state set

$\rho : S \times \Sigma \to 2^S$ - transition function

Word: $w = a_0 a_1 a_2 \cdots$

Run: $r = \eta_0 \eta_1 \eta_2 \cdots$

$\eta_0 \in S_0, \quad \eta_{i+1} \in \rho(\eta_i, a_i)$

$\lim(r)$: states that occur i.o. in r

Acceptance condition: $C \subseteq 2^S$

Acceptance: $\lim(r) \in C$

ACCEPTANCE CONDITIONS

Büchi: $F \subseteq S$

F visited infinitely often.

Street: $\{(L_i, U_i)\}$ $\quad L_i, U_i \subseteq S$

L_i visited infinitely often $\Rightarrow$

U_i visited infinitely often.

Acceptance Formulas

ω-Automaton: $A = (T, C)$ accepts $L_\omega(A)$

ω-regular: $L = L_\omega(A)$

- View C as a set of truth assignments on S; express C by a Boolean formula on S. E.g., $\neg\wedge\wedge(t \vee u) \to \{\{t\}, \{u\}, \{t,u\}\}$

Emerson-Lei automata: $A = (T, f)$

- Büchi formula: $f = \bigvee F$, $F \subseteq S$

L ω-regular $\to$ L accepted by Büchi automata

- streett formula: $f = \bigwedge_i (\bigvee L_i \to \bigvee U_i)$, $L_i, U_i \subseteq S$

L ω-regular $\to$ L accepted by deter. streett automaton

$ETL \rightsquigarrow ETL_B, ETL_S, ETL_{EL}$

Nonemptiness

A nonempty $\iff$ $L_\omega(A) \neq \emptyset$

Testing nonemptiness:

- Büchi automata : NL-complete.
- streett automata : P-complete.
- EL automata : NP-complete

Testing satisfiability for ETL:

- ETL_B : PSPACE-complete.
- ETL_S : ?
- ETL_{EL} : ?

SUCCINCTNESS

Upper Bounds (easy)

EL $\xrightarrow{exp}$ Büchi

Consequently:

EL $\xrightarrow{exp}$ Streett Streett $\xrightarrow{exp}$ Büchi

Lower Bounds

EL $\xrightarrow{exp}$ Streett Street $\xrightarrow{exp}$ Büchi

EL $\xrightarrow{\ell + P}$ STREET

$\Sigma = \{0, 1\}$

$\Sigma^\omega = (\Sigma^m)^\omega$

$L_m = \{w \in \Sigma^\omega : w = uv^\omega,\ u \in (\Sigma^m)^*, v \in \Sigma^m\}$

L_m consists of almost always identical m-words.

- L_m is accepted by an EL aut. with $O(m)$ states.
- L_m is not accepted by a streett aut. with $< 2^m$ states.

STREETT $\xrightarrow{\text{exp}}$ BÜCHI

$\Sigma = \{0, 1, 2\}$

Let $u \in \Sigma^m$: $u = a_0 \dots a_{m-1}$

i 0-active in $u \equiv a_i = 0$

i 1-active in $u \equiv a_i = 1$

$\Sigma^\omega = (\Sigma^m)^\omega$

Let $w = u_0 u_1 u_2 \dots$, $u_i \in \Sigma^m$

i 0-active in $w \equiv i$ 0-active in u_i, i

i 1-active in $w \equiv i$ 1-active in u_i, i

$$L_m = \{ w \in \Sigma^\omega : i \text{ 0-active} \Leftrightarrow i \text{ 1-active} \}_{0 \le i \le m-1}$$

- L_m is accepted by a Streett aut. with $O(m)$ states.
- L_m is not accepted by a Büchi aut. with $< 2^m$ states.

Complementation

$A \longrightarrow \bar{A}$

$\Sigma^\omega - L_\omega(A) = L(\bar{A})$

Known: Büchi complementation: $2^{O(n \log n)}$ Tight

Easy ub: EL comp.: $2^{2^{O(n)}}$

New lb: EL comp.: $2^{2^{O(n)}}$

New ub (hard): Streett comp.: $2^{O(n^5)}$

This suggests:

- ETL_S - feasible
- ETL_{EL} - infeasible

Buchi Complementation

$\Delta = \{0, 1\}$ $\quad \Sigma = \{0, 1, 2\}$

Let $w = u_0 2 u_1 2 u_2 \ldots$, $u_i \in \Delta^n$

w is an n-counter if

$$u_{i+1} = u_i + 1 \pmod{2^n}$$

$$L_n = \{ w \in (\Delta^n 2)^\omega : w \text{ is an } n\text{-counter} \}$$

- $\overline{L_n}$ is accepted by a Büchi aut. with $O(n)$ states.
- L_n is not accepted by an EL automaton with $< 2^n$ states.

EL Complementation

$\Delta = \{0, 1\}$, $\Sigma = \{0, 1, 2, 3\}$

n-number: $u \in \Delta^n$

Indexed 2^n-number: $v \in (\Delta^n 2 \Delta)^{2^n}$

$$v = u_0 2 i_0 \, u_1 2 i_1 \ldots u_{2^n-1} 2 i_{2^n-1}$$

$$u_j = j$$

$$val(v) = i_0 \ldots i_{2^n-1}$$

Let $w = v_0 3 v_1 3 v_2 3 \ldots$, v_i indexed 2^n-number

w is a 2^n-counter if

$$val(u_{i+1}) = val(u_i) + 1 \pmod{2^{2^n}} \text{ for all } i > i_0.$$

$L_n = \{w : w \text{ is a } 2^n\text{-counter}\}$

- $\overline{L_n}$ is accepted by an EL aut. with $O(n)$ states.
- L_n is not accepted by an EL aut. with $< 2^{2^n}$ states.

ETL

- ETL_B – PSPACE-complete
- ETL_S – PSPACE-complete
- ETL_{EL} – EXPSPACE-complete

But practically:

- ETL_B – time $2^{O(n \log n)}$
- ETL_S – time $2^{O(n^5)}$

History Graphs

$T = (\Sigma, S, S_0, \rho)$

Define $\rho : 2^S \times \Sigma^* \to 2^S$

$\rho(V, \lambda) = V$, $\rho(V, wa) = \{t : t \in \rho(\eta, a), \eta \in \rho(V, w)\}$

History graph for T: $G = (V, E)$

$V \subseteq S$, $E : V^2 \to 2^{2^S}$

G corresponds to $w \in \Sigma^*$:

- $\rho(V, w) = V$
- $H \in E(\eta, t)$ iff there is a run of T from η to t visiting precisely the states in H.

- G corresponds to $w \in \Sigma^\omega$:

  There exists a sequence $0 < i_0 < i_1 < i_2 \ldots$ such that $V = \rho(s_0, w[0, i_0])$ and G corresponds to $w[i_j, i_{j+1}]$ for all $j \geq 0$

- G idempotent:

  if $H_1 \in E(r, r)$ and $H_2 \in E(r, t)$,

  then $H_1 \cup H_2 \in E(r, t)$

- G non accepting wrt C if $E(r, r) \cap C = \emptyset$

  for all $r \in V$.

Lemma

- Each $w \in \Sigma^\omega$ has a corresponding idempotent history graph.
- w not accepted by $A = (T, C)$ if it has a corresponding non accepting i.p. h.g.

History Graphs for Streett Automata

$$A = (T, f), \quad f = \bigwedge_{i=1}^{k} (VL_i \to VU_i)$$

$$\Delta = \{1, \ldots, k\}$$

- **Pair assignment for V:**

  $\alpha : V \to \Delta^*$ assigns to every state a sequence of distinct pair indices

- **Pair assignment for h.g. $G = (V, E)$:**

  if $\alpha(n) = i_1, \ldots, i_\ell$ and $H \in E(n, n)$, then $\exists j$, $1 \le j \le \ell$, such that $H \cap L_{i_j} \neq \emptyset$ and $H \cap U_{i_{j'}} = \emptyset$ for all $j' \le j$.

Lemma. An idempotent history graph is non accepting iff it has a pair assignment.

PAIR GRAPHS

$\Delta' = \{1, \ldots, k+1\}$

Pair graphs: $G = (V, F)$

$V \subseteq S$, $F : V^3 \to 2^{(\Delta')^2}$

$|G| = O(n^s)$

Definitions

- A pair graph G and a pair assignment α
  - corresponds to $w \in \Sigma^*$.
  - corresponds to $w \in \Sigma^\omega$.
  - idempotent.
  - nonaccepting.

Lemma. w not accepted by A iff

there is a pair assignment α and a nonaccepting idempotent pair graph G that corresponds to w.

Construction. • Guess G and α.
• Check conditions.

Determinization

Büchi : $2^{O(n \log n)}$ (Safra)

EL : $2^{2^{O(n)}}$

Streett : ???