Temporal Logics over Mazurkiewicz Traces
A Quick Tour

Madhavan Mukund
Chennai Mathematical Institute
92 G N Chetty Rd, Chennai 600 017, India
http://www.cmi.ac.in/~madhavan

Arcachon, 23 May 2002

Motivation

- Temporal logic — convenient specification language
- Formulas interpreted over sequences
  - For concurrent systems, sets of interleaved behaviours
  - Combinatorial explosion in verification
- Can we directly reason about a single structure that describes the entire behaviour of a concurrent system?

Mazurkiewicz traces

- An alphabet with an independence relation, (Σ, I)
- Independent letters can be commuted.

  If $(a, b) \in I$, then $wabw' \sim w'abw$
- A trace is an equivalence class of words—a single concurrent behaviour with different, equivalent linearizations
- Traces faithfully model behaviour of concurrent systems with static architecture —e.g., safe Petri nets

Traces revisited

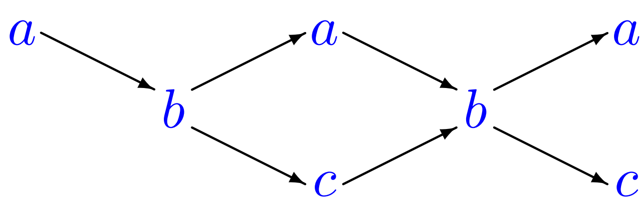
- Dependence alphabet (Σ, D): D is the complement of I

  Dependence graph; e.g., $(\Sigma, D) = a — b — c — d$

  Here, (a, c), (b, d), (a, d) are independent pairs

- A trace is a labelled partial order

  The trace $\{abacbac, abcabac, \ldots, abcabca\}$ is the (set of linearizations of the) labelled partial order



Finite and infinite traces

$$(\Sigma, D) = a \text{ — } b \text{ — } c \text{ — } d$$

Finite trace

$$\begin{tikzcd}
a \arrow[dr] & & a \arrow[dr] & & a \\
& b \arrow[ur] \arrow[dr] & & b \arrow[ur] \arrow[dr] & \\
& & c \arrow[ur] & & c
\end{tikzcd}$$

Infinite trace

$$\begin{tikzcd}
a \arrow[r] & b \arrow[r] & c \arrow[r] & b \arrow[r] & \cdots \\
d \arrow[r] & c \arrow[u] & & &
\end{tikzcd}$$

Traces as partial orders

A trace over (Σ, D) is a labelled partial order $t = (E, \leq, \lambda)$ such that

- $e \not\leq f$ and $f \not\leq e$ implies $(\lambda(e), \lambda(f)) \notin D$

  Concurrent (unordered) events correspond to independent actions

- $e \lessdot f$ implies $(\lambda(e), \lambda(f)) \in D$

  The causality order on events is generated by D

- For all $e \in E$, $\downarrow e = \{f \mid f \leq e\}$ is finite

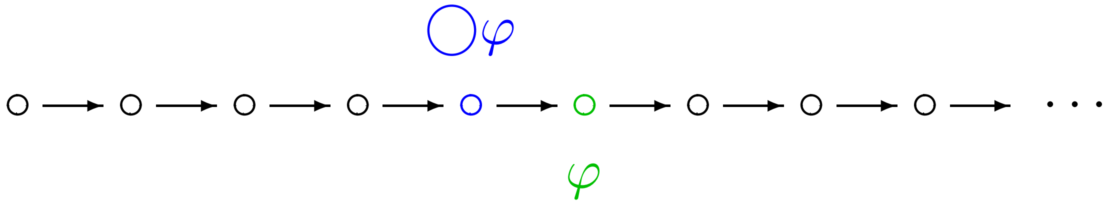
  Each event has a finite past (infinite traces are "real")

Key fact For each (Σ, D), the width of traces over (Σ, D) is bounded.

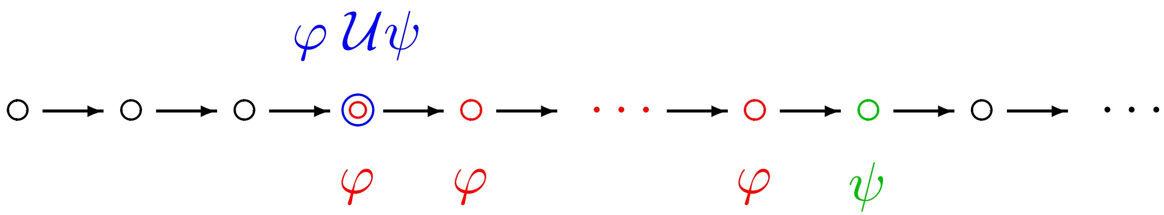
Linear-time temporal logic over sequences

- Atomic propositions, boolean connectives, temporal modalities

- Next



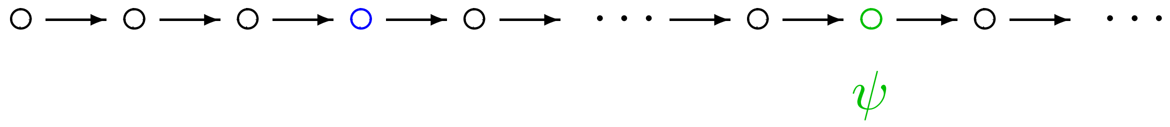
- Until



Derived modalities

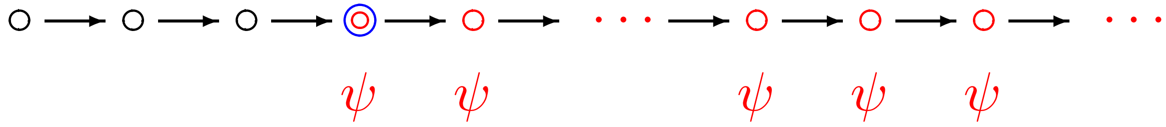
$$\Diamond\psi \equiv \top\,\mathcal{U}\psi$$

- Eventually



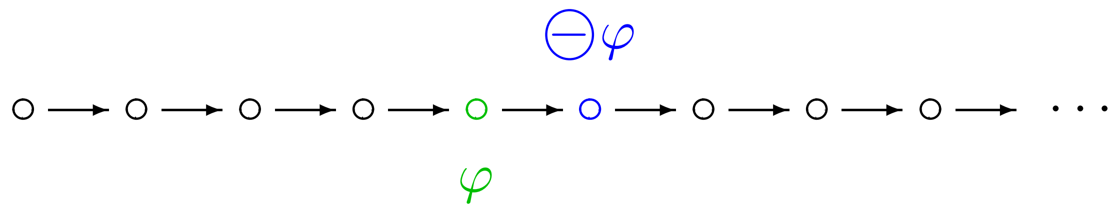
$$\Box\psi \equiv \neg\Diamond\neg\psi$$

- Henceforth

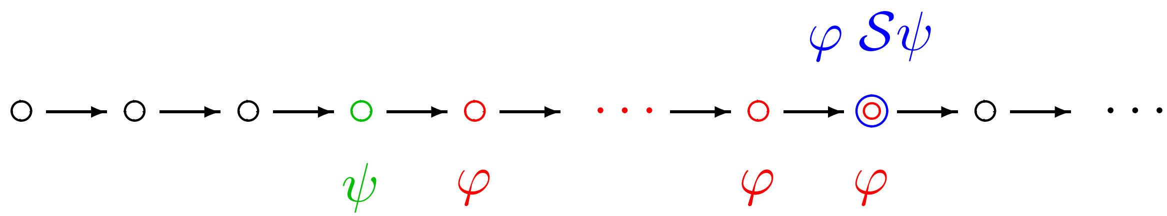


Past modalities

- Previous



- Since



- Theorem (Kamp '68)

  LTL has the same expressive power as $FO(\mathbb{N}, <)$.

- Theorem (Gabbay, Pnueli, Shelah & Stavi '80)

  LTL with only future modalities has the same expressive power as $FO(\mathbb{N}, <)$.

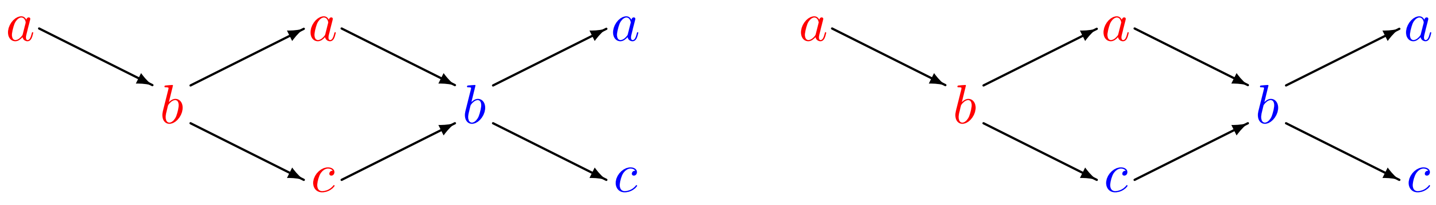
- Theorem (Sistla & Clarke '82)

  Model checking LTL is PSPACE-complete.

  – Do all sequences generated by a finite-state system S satisfy an LTL formula φ?

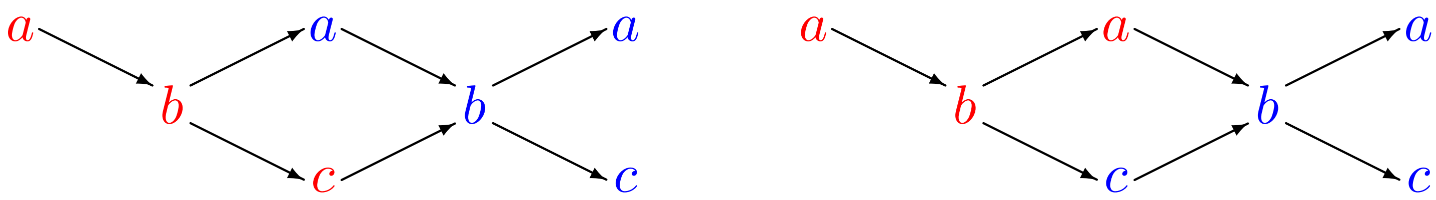
LTL over traces

- Points on a sequence $\Leftrightarrow$ prefixes of the sequence
- A prefix of a trace is a downward closed subset of events

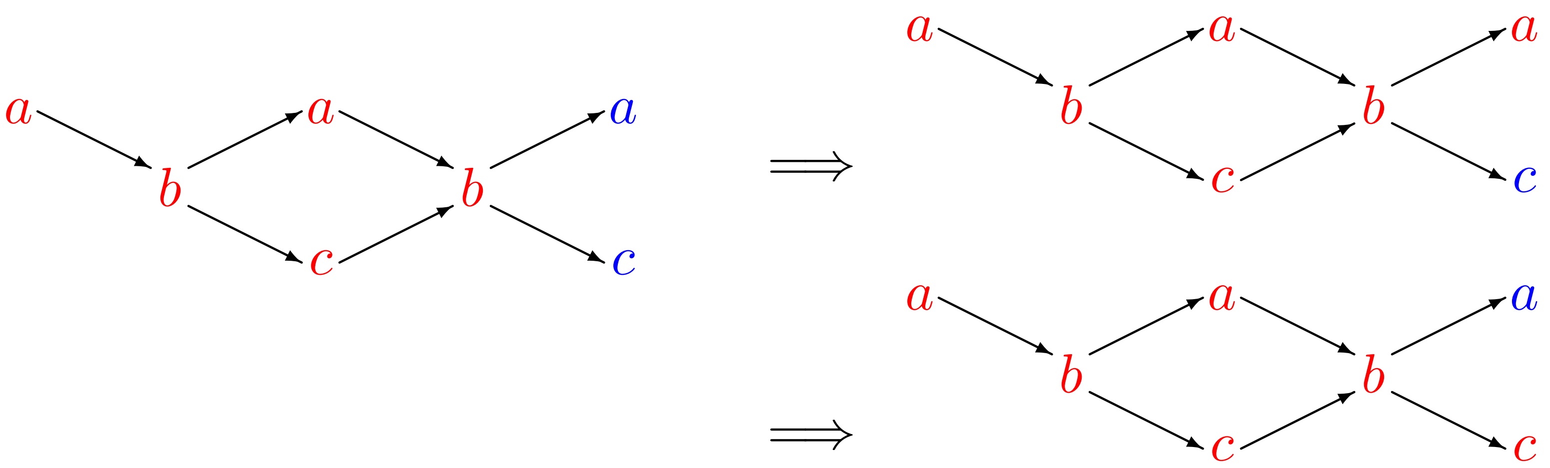


- Interpret formulas at prefixes
- Prefixes can be ordered in the obvious way—$c \preceq c'$ iff $c \subseteq c'$

- Two prefixes may be unordered



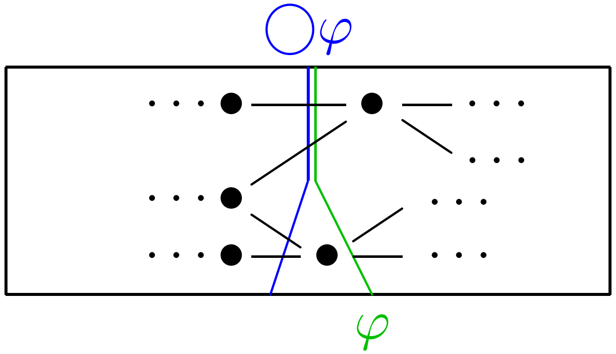
- A prefix may have more than one “next” prefix



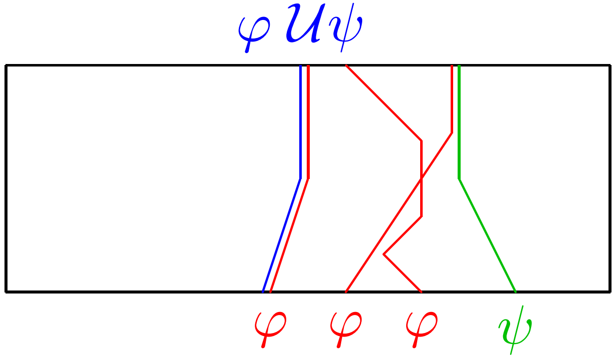
Trace modalities

For a trace $t = (E, \leq, \lambda)$ over (Σ, D), let $c \subseteq E$ be a prefix.

$t, c \models \bigcirc\varphi$ if there exists a "next" prefix $c' = c \cup \{e\}$ such that $t, c' \models \varphi$



$t, c \models \varphi\,\mathcal{U}\psi$ if $t, c' \models \psi$ for some prefix c', $c \preceq c'$, and for all c'' with $c \preceq c'' \preceq c'$, $t, c'' \models \psi$



Fix a trace alphabet (Σ, D).

- When interpreted on traces over (Σ, D), what is the expressive power of LTL($\bigcirc, \mathcal{U}$) with respect to $FO(<)$?
  - LTL($\bigcirc, \mathcal{U}$) is within $FO(<)$ because width of a trace is bounded!

- Theorem (Thiagarajan & Walukiewicz, LICS '97)

  Expressively complete, if you add past formulas $\ominus a$

  - $t, c \models \ominus a$ if c contains a maximal event labelled a

- Theorem (Diekert & Gastin, ICALP '00)

  Expressively complete with just $\bigcirc$ and $\mathcal{U}$.

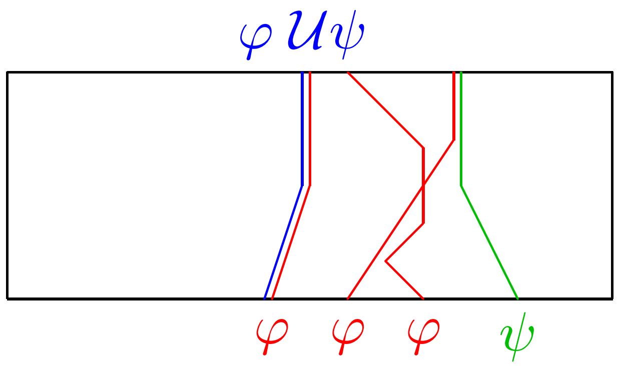
  Generalizes the GPSS '80 result from sequences to traces.

Unfortunately, . . .

- Theorem (Walukiewicz, ICALP '98)

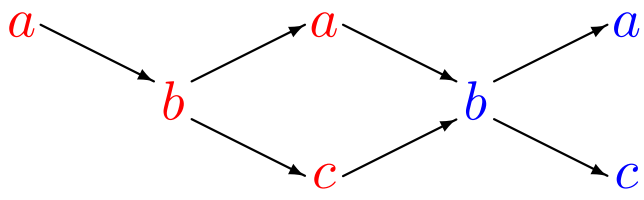
  Model checking is non elementary.

  "Too many" configurations between φ and ψ.

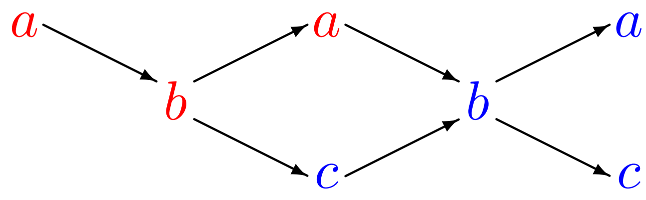


Global vs local configurations

Global configuration



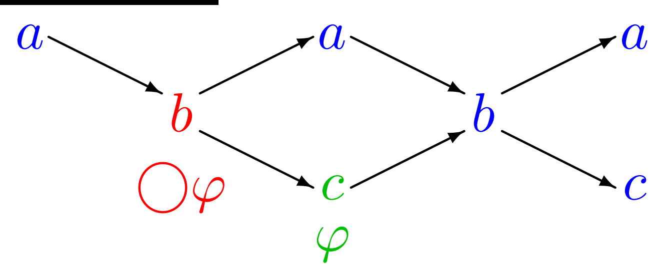
Local configuration



- Local configuration represents local history of an event.
  - Events $e \in E \quad \Leftrightarrow \quad$ Local configurations ${\downarrow}e \subseteq E$
- Variables in $FO(<)$ are interpreted as events
- Can we evaluate temporal formulas at local configurations and still be as expressive as $FO(<)$?

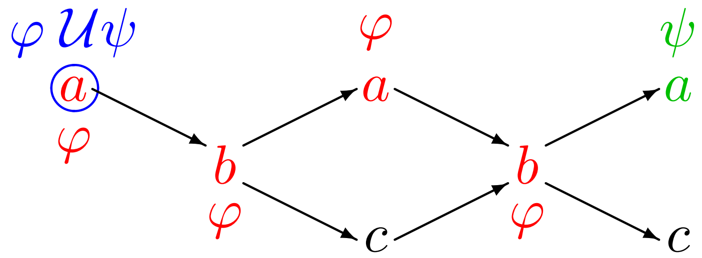
Local logics on traces

Hasse diagram provides a natural local interpretation for $\bigcirc$



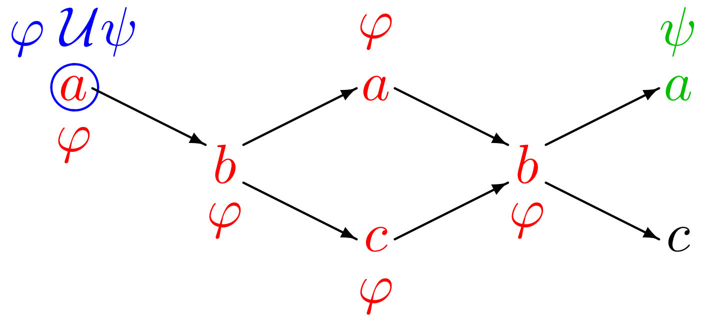
Existential until

φ holds on *some* path in the interval



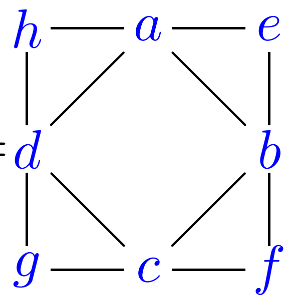
Universal until

φ holds on *every* path in the interval

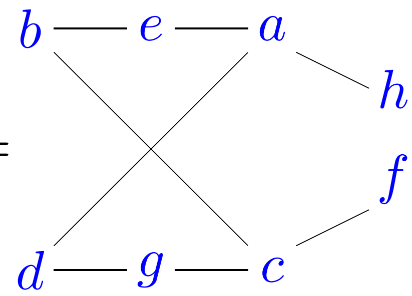


Existential until is not first-order expressible

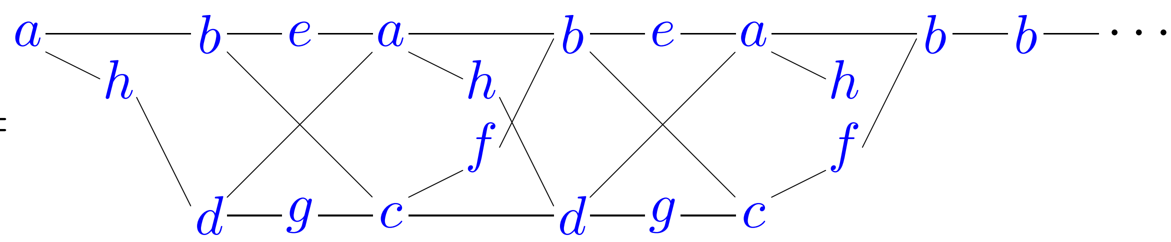
$(\Sigma, D) =$



$t =$



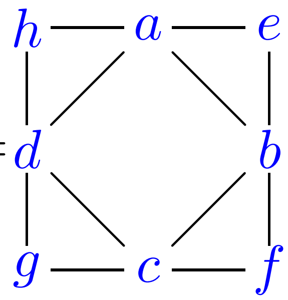
$aht^2b^\omega =$



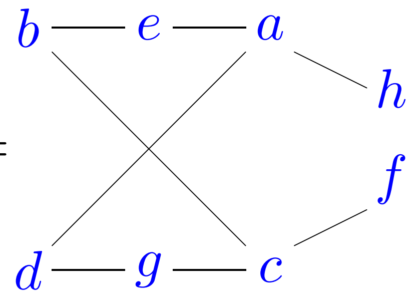
Example (independently) due to Gastin and Walukiewicz

Existential until is not first-order expressible

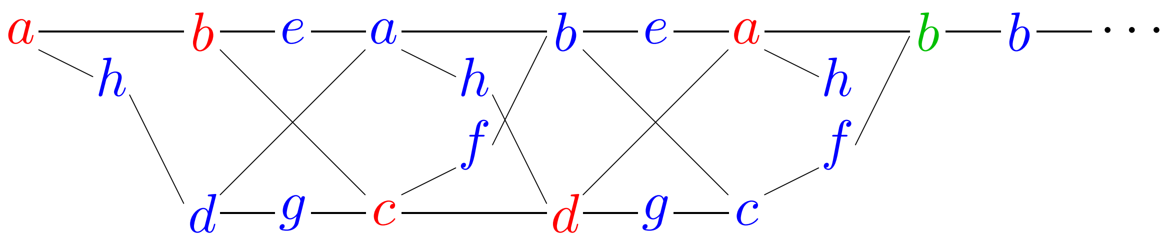
$(\Sigma, D) =$



$t =$

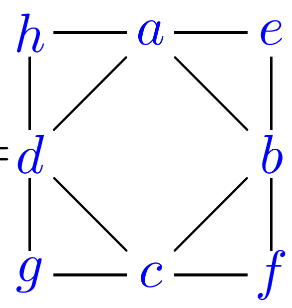


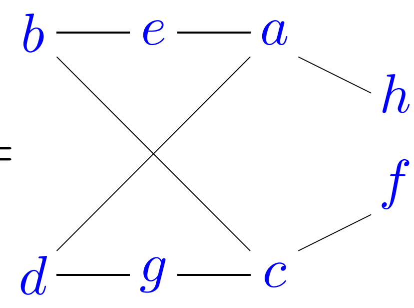
$aht^2b^\omega =$

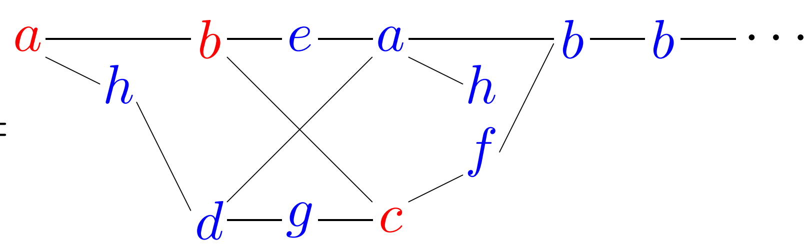


$$\varphi = a \vee b \vee c \vee d \, \mathcal{U} \square b$$

Existential until is not first-order expressible

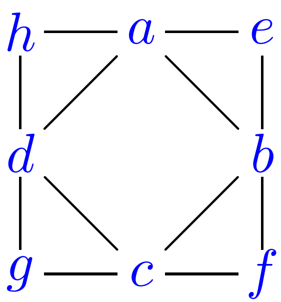
$(\Sigma, D) =$


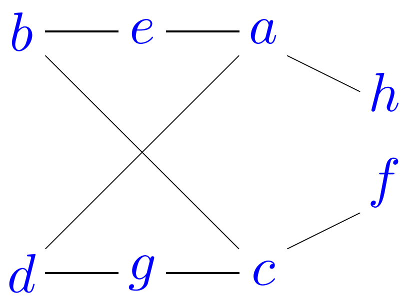
$t =$


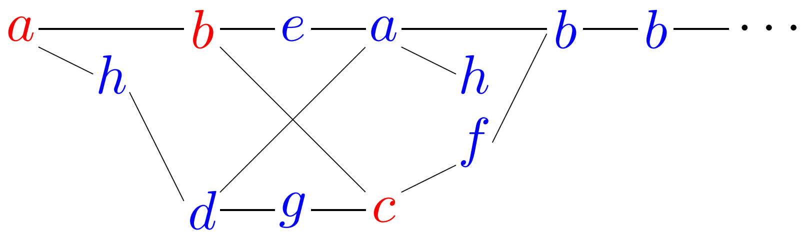
$aht^1b^\omega =$


$$\varphi = a \vee b \vee c \vee d \,\mathcal{U} \Box b$$

Existential until is not first-order expressible

$(\Sigma, D) =$ 

$t =$ 

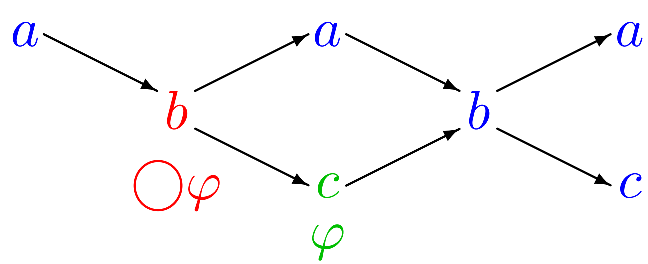
$aht^1b^\omega =$ 

$$\varphi = a \vee b \vee c \vee d \,\mathcal{U} \Box b$$

$$aht^*b^\omega \cap \mathcal{L}(\varphi) = ah(t^2)^*b^\omega$$

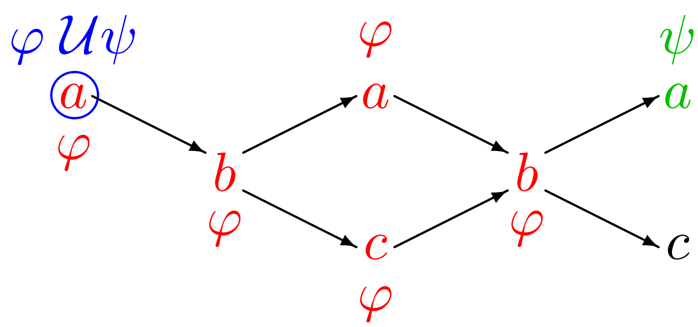
Local logics on traces

Existential $\bigcirc$

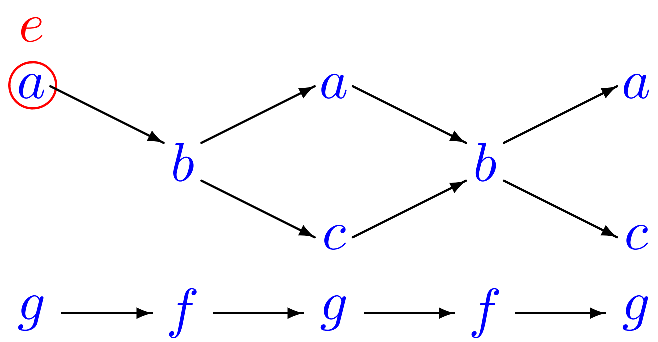


Universal until

φ holds on *every* path in the interval



- Need some way of globally combining local formulas to span disjoint components



Formula at e cannot "reach" the disconnected chain $gfgfg$

- Global formulas

Boolean combinations of $EM\varphi$, φ a local formula

$t \models EM\varphi$ if there is a minimal event e in t such that $t, e \models \varphi$

Pure future local logics are not sufficient

φ is a pure future formula if $t, e \models \varphi$ implies that $t't, e \models \varphi$ for any t', t, e

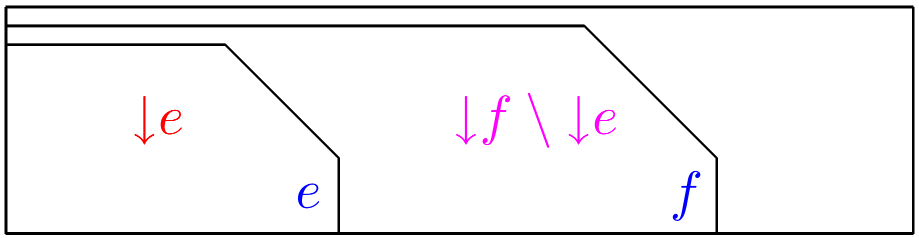
Example (Walukiewicz)

The following traces over $a — b — c — d$ cannot be distinguished by pure future local formulas

$$\begin{tikzcd}
a \arrow[r] & b \arrow[r] & c \arrow[r] & b \arrow[r] & \cdots \\
d \arrow[r] & c \arrow[u] & & &
\end{tikzcd}
\qquad
\begin{tikzcd}
d \arrow[r] & c \arrow[r] & b \arrow[r] & c \arrow[r] & \cdots \\
a \arrow[r] & b \arrow[u] & & &
\end{tikzcd}$$

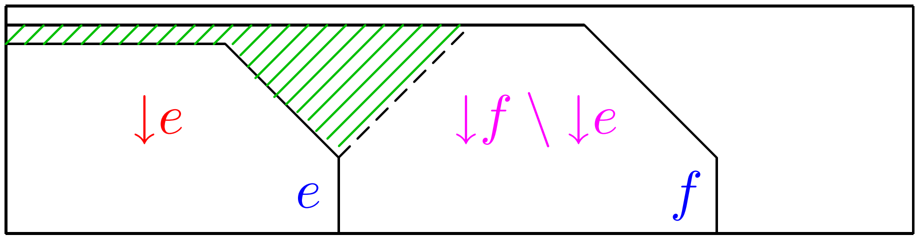
A stronger until

- For events $e \leq f$, the interval between e and f is more properly defined as $\downarrow f \setminus \downarrow e$



A stronger until

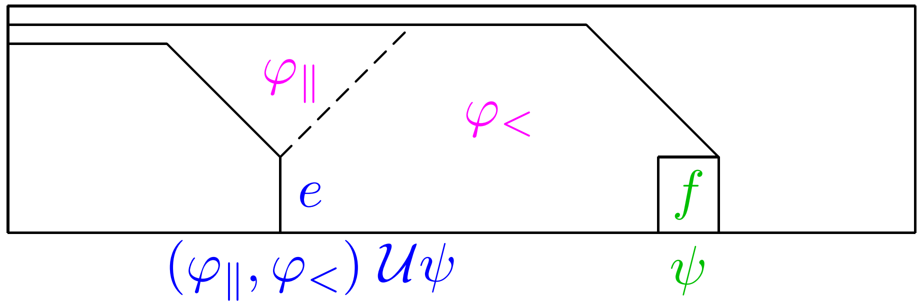
- For events $e \leq f$, the interval between e and f is more properly defined as $\downarrow f \setminus \downarrow e$



- This interval includes events that do not lie above e

- A ternary until

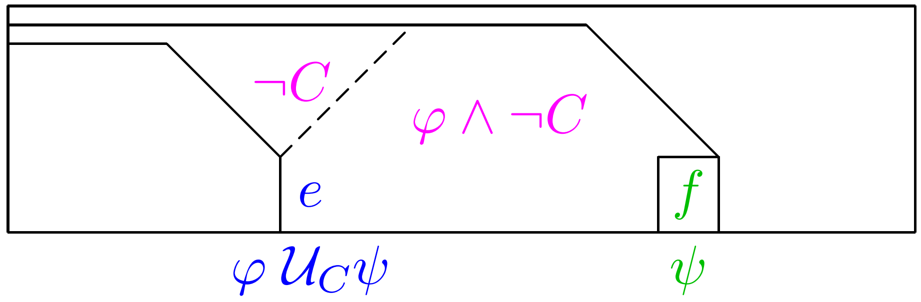
$(\varphi_{\|}, \varphi_{<})\,\mathcal{U}\psi$



- A weaker version — filtered until

$\varphi\,\mathcal{U}_C\psi$, $C \subseteq \Sigma$

  – φ holds above e and below f
  – No action from C occurs in $\downarrow f \setminus \downarrow e$



A stronger until . . .

Filtered until can distinguish these traces

$$\begin{tikzcd}
a \arrow[r] & b \arrow[r] & c \arrow[r] & b \arrow[r] & \cdots \\
d \arrow[r] & c \arrow[u] & & &
\end{tikzcd}$$

$$\begin{tikzcd}
d \arrow[r] & c \arrow[r] & b \arrow[r] & c \arrow[r] & \cdots \\
a \arrow[r] & b \arrow[u] & & &
\end{tikzcd}$$

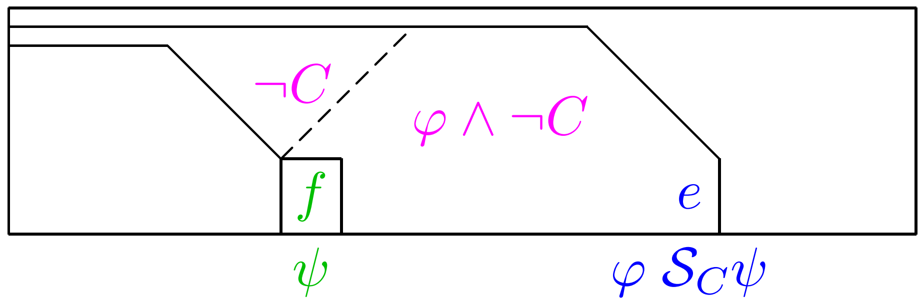
The formula $EM\,d\,\mathcal{U}_{\{a\}}c$ is true in the first trace, but not in the second.

A dual modality — filtered since

$\varphi\, \mathcal{S}_C \psi$, $C \subseteq \Sigma$

- φ holds above f and below e

- No action from C occurs in $\downarrow e \setminus \downarrow f$



Theorem (Gastin & Mukund, ICALP '02)

$LTL(\bigcirc, \ominus, \mathcal{U}_C, \mathcal{S}_C)$ has the same expressive power as $FO(<)$.

For each fixed alphabet (Σ, D), the model-checking problem is in PSPACE (and hence PSPACE-complete).

Corollary

$FO_3(<)$, FO with 3 variables, is as expressive as $FO(<)$ for traces.

Independent of the width of the trace!

Pure future modalities

Theorem (Diekert & Gastin, LPAR '01)

$LTL(\bigcirc, \mathcal{U})$, where $\mathcal{U}$ is the universal pure future local until, has the same expressive power as $FO(<)$ for cographs.

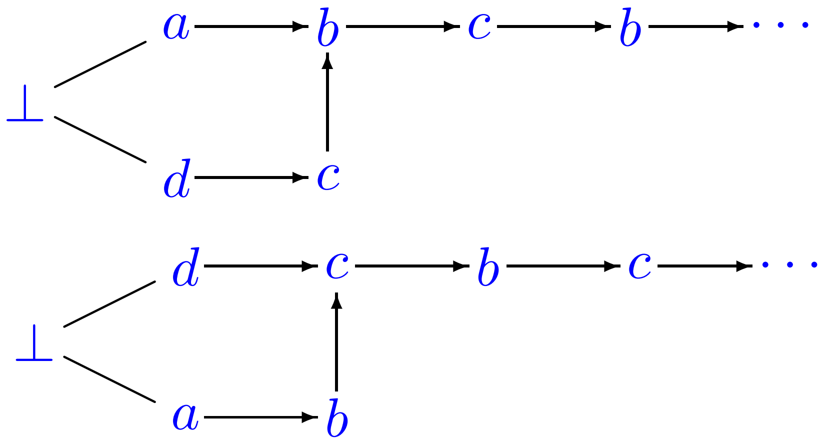
Cographs—traces where the alphabet (Σ, D) is series-parallel.

- (Σ, D) is built from singletons using
  - $\Sigma_1 \cdot \Sigma_2$ — all actions in Σ_1 are dependent on all actions Σ_2
  - $\Sigma_1 \parallel \Sigma_2$ — all actions in Σ_1 are independent of all actions Σ_2
- (Σ, D) is N-free, does not embed $a — b — c — d$.
- Traces generated by (Σ, D) are series-parallel graphs.

What if . . .

- For arbitrary alphabets, you have only $\mathcal{U}_C$, but not $\mathcal{S}_C$?

- Each trace is equipped with a special bottom element.



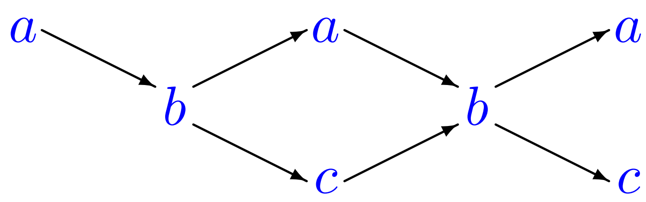
Can separate these traces using the pure future formula $\neg a\,\mathcal{U} c$ evaluated at $\perp$.

Another point of view

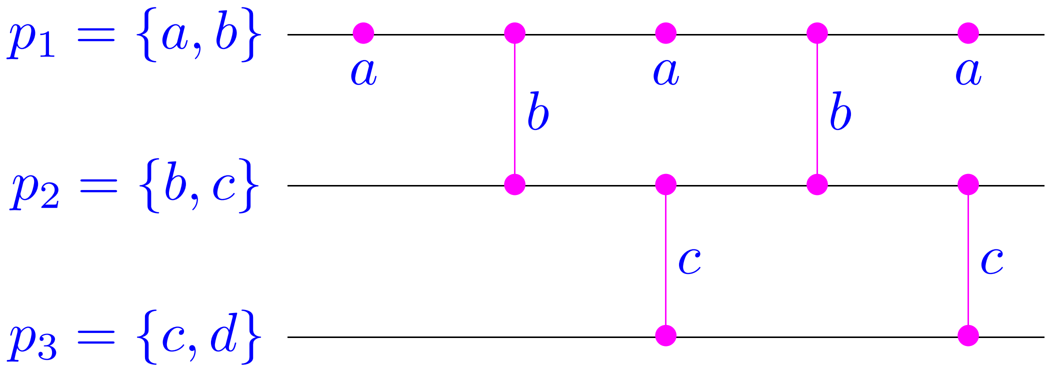
- (Σ, D) can be implemented as a distributed alphabet $(\Sigma_1, \ldots, \Sigma_n)$.
  - $\bigcup_{1 \leq i \leq n} \Sigma_i = \Sigma$
  - If $(a, b) \in D$, then for some i, $\{a, b\} \in \Sigma_i$
- Think of each i as an agent or process in a distributed system.
- Example, can implement $a — b — c — d$ with three agents.

  Distributed alphabet is $(\{a, b\}, \{b, c\}, \{c, d\})$.

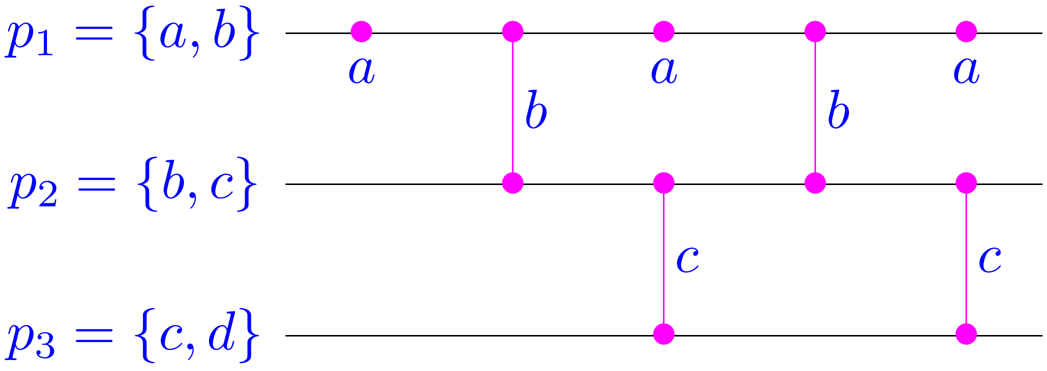
Can redraw the trace



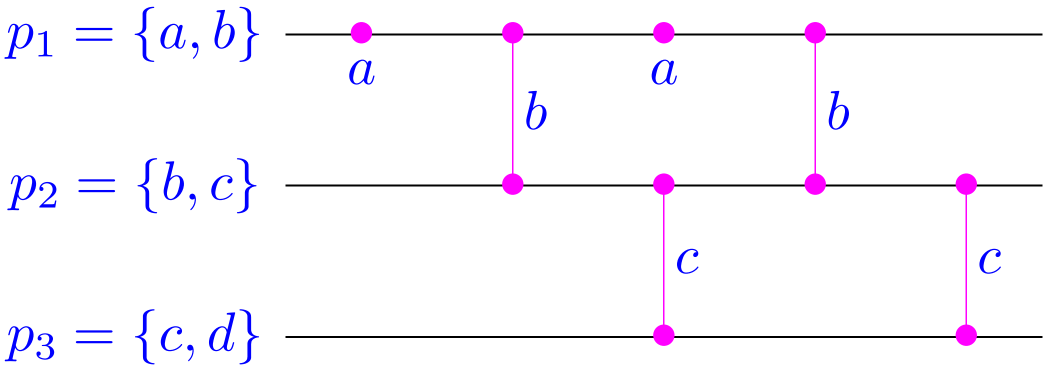
as



The view that p_3 has of

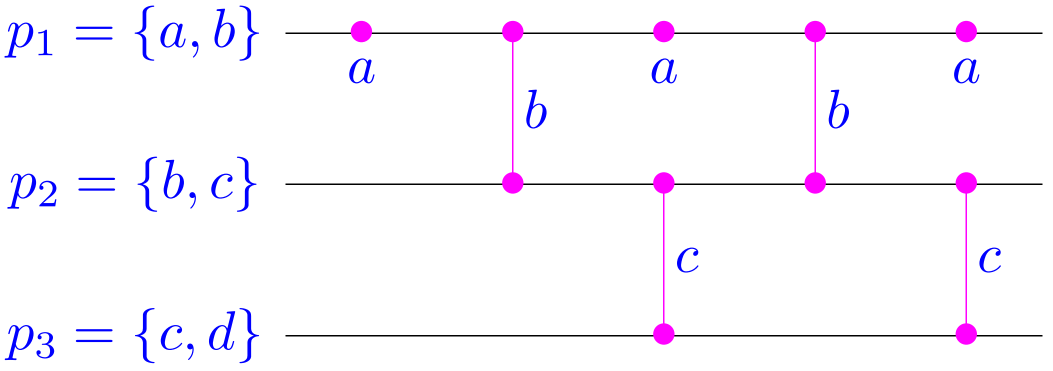


is

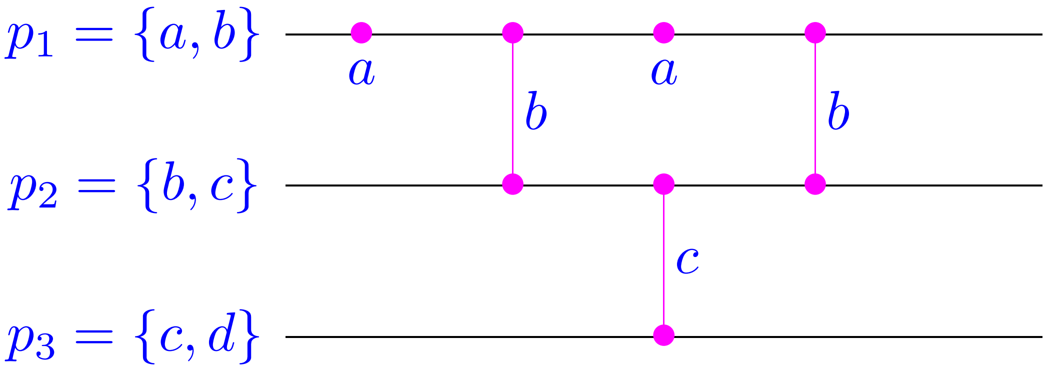


Another point of view . . .

The p_1 view of the p_3 view of



is



Another point of view . . .

- Define local modalities based on processes

(TrPTL, Thiagarajan LICS '94)

- $t, e \models \bigcirc_i \varphi$

  With respect to the maximal i-event in $\downarrow e$, the next i-event satisfies φ

- $t, e \models \varphi \, \mathcal{U}_i \psi$

  Starting with the maximal i-event in $\downarrow e$, the sequence of events along process i satisfies $\varphi \, \mathcal{U} \psi$.

- Boolean combination of assertions $EM_i \varphi$ which say that there is a minimal i-event satisfying the local formula φ.

- Is TrPTL equivalent to $FO(<)$?

  Probably not, but counterexample is elusive

- Using more explicit past assertions, it is possible to obtain a process-oriented temporal logic that is equivalent to $FO(<)$

(Adsul & Sohoni, ICALP '02)

Summary

- Temporal logics interpreted over the Hasse diagram of a trace
  - Without a special element $\perp$, to what extent are past modalities required?
  - With a special element $\perp$, are past modalities required at all?
- Temporal logics interpreted over the process view of a trace
  - Is TrPTL expressively complete?
- Not discussed at all in this talk
  - μ-calculi on traces and expressive completeness with respect to MSO (Niebert '95, Walukiewicz '01)