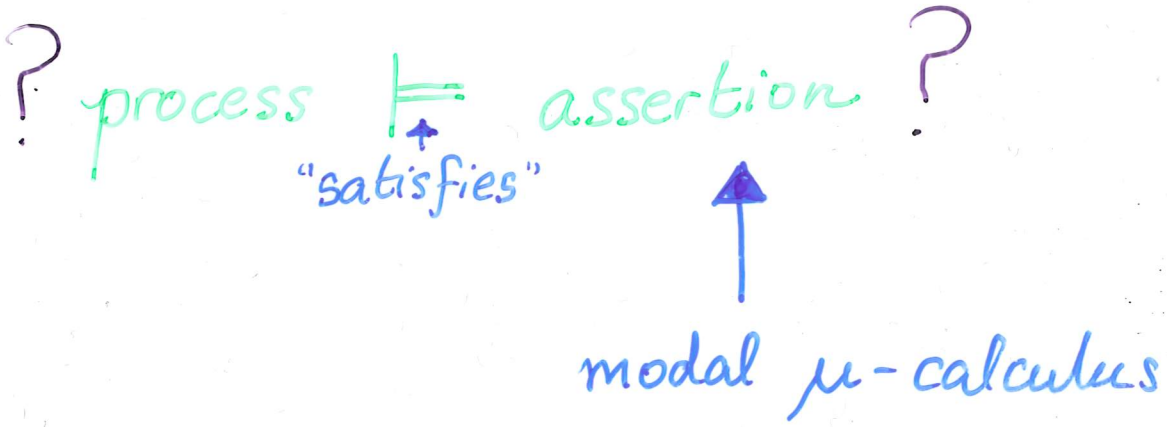
Tarski's Fixed Point Theorem and Model Checking.



Specifying the Vending Machine

$$Ven = coin.(\overline{tea}.\overline{change}.Ven + \overline{coffee}.\overline{change}.Ven)$$

$$Ven' = coin.\overline{tea}.\overline{change}.Ven' + coin.\overline{coffee}.\overline{change}.Ven'$$

$$User = \overline{coin}.coffee.change.\overline{work}$$

Expected properties

$L = \{coin, tea, coffee, change\}$

$$Sys = (Ven \mid User) \setminus L$$

* always outputs 'work'
* never deadlocks

Define

terminal = { processes that properly terminated }

$nil \mid nil$ ✓ $\qquad (a \mid \overline{b}) \setminus \{a,b\}$ ✗

⇝ Allow arbitrary sets to be defined for assertions

$$Dead = \neg terminal \wedge [-]F$$

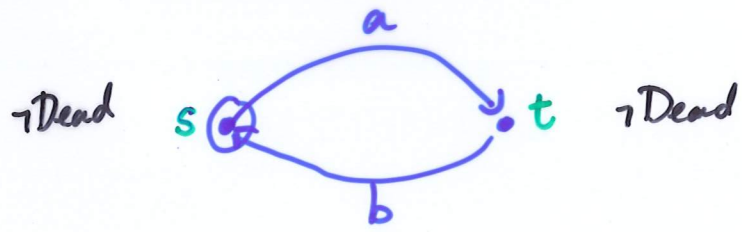
Want to express

"no deadlocked state is reachable"

Idea: 'Recursive' definition of propositions

$$? \quad X = \neg Dead \wedge [-]X \quad ?$$

But ... there are (in principle) many potential sets X that satisfy the above equation



least:

Greatest:

⟿ least & greatest fixpoints

$$\nu X.(\neg Dead \wedge [-]X)$$

Tarski's Fixed Point Theorem

Let $\varphi : \mathcal{P}(S) \to \mathcal{P}(S)$ be monotonic,

i.e., $u \subseteq u' \Rightarrow \varphi(u) \subseteq \varphi(u')$.

Then, φ has a maximum fixed point

$$M = \bigcup \{ u \subseteq S \mid u \subseteq \varphi(u) \}:$$

"u is a post-fixed pt. of φ"

(i) $M = \varphi(M)$,

(ii) $u \subseteq \varphi(u) \Rightarrow u \subseteq M$.

Dually, φ has a minimum fixed point

$$m = \bigcap \{ u \subseteq S \mid \varphi(u) \subseteq u \}:$$

"u is a pre-fixed p.t. of φ"

(i) $m = \varphi(m)$

(ii) $\varphi(u) \subseteq u \Rightarrow m \subseteq u$

Notation: $\nu X.\varphi(X)$ maximum fixed point

$\mu X.\varphi(X)$ minimum fixed point

Proof rules for maximum fixed points

$$\nu X.\varphi(X) = \varphi(\nu X.\varphi(X))$$

If $u \subseteq \varphi(u)$, then

$u \subseteq \nu X.\varphi(X)$.

Uses of Tarski's fixed point theorem:

Minimum fixed points

Inductive definitions, so syntax, operational semantics, rule based programs, model checking

Maximum fixed points

Co-inductive definitions, bisimulation, model checking.

Strong equivalence as a maximum fixed point:

$p \; \varphi(R) \; q$

iff

(i) $\forall \alpha, p'. \quad p \xrightarrow{\alpha} p' \Rightarrow$

$\exists q'. \quad q \xrightarrow{\alpha} q' \;\&\; p' \; R \; q'$

and

(ii) $\forall \alpha, q'. \quad q \xrightarrow{\alpha} q' \Rightarrow$

$\exists p'. \quad p \xrightarrow{\alpha} p' \;\&\; p' \; R \; q'.$

$R \subseteq \varphi(R)$ iff R is a strong bisim.

$$\sim \; = \bigcup \{ R \mid R \subseteq \varphi(R) \}$$

$$\sim \; = \nu X. \; \varphi(X)$$

The modal μ-calculus

Formulas:

* S for S any subset of states (or finite descriptions)

* T, F

* $A \wedge B$, $A \vee B$, $\neg A$

* $\langle a \rangle A$, $\langle - \rangle A$ (with $[a]A \equiv \neg\langle a \rangle \neg A$ and $[-]A \equiv \neg\langle - \rangle \neg A$)

* $\nu X.A$ if A is an assertion in which the variable X only occurs positively i.e. under an even number of $\neg$

Disallows $\nu X. \neg X$

Take $\boxed{\mu X.A \equiv \neg \nu X. \neg A[\neg X / X]}$

e.g. $\mu X.(\text{Dead} \vee \langle - \rangle X)$

$\equiv \neg \nu X (\neg(\text{Dead} \vee \langle - \rangle \neg X))$

equivalent to

$\neg \nu X (\neg \text{Dead} \wedge [-] X)$

Interpretation

* $s \models S$ iff $s \in S$

* $s \models T$ always

⋮

* $s \models \nu X.A$

iff $s \in \nu X.A$

iff $s \in \bigcup \{ S \subseteq \mathcal{P} \mid S \subseteq A[S/X] \}$

($\mathcal{P}$: set of states/processes)

i.e. the maximum fixpoint of the monotonic function

$$S \longmapsto A[S/X]$$

In general, if $\varphi : Pow(State) \longrightarrow Pow(State)$ and the function

$$S \longmapsto A[S/X]$$

is $\cup$-continuous

$$\mu X.A = \bigcup_{n \in \omega} \varphi^n(\emptyset) = \varphi(\emptyset) \vee \varphi(\varphi(\emptyset)) \vee \varphi\varphi\varphi(\emptyset) \vee \ldots$$

If it is $\cap$-continuous,

$$\nu X.A = \bigcap_{n \in \omega} \varphi^n(T)$$

$\rightsquigarrow$ set of all states

$$= \varphi(T) \wedge \varphi(\varphi(T)) \wedge \varphi\varphi\varphi(T) \wedge \cdots$$

In a finite-state system, φ is always $\cap$- and $\cup$-continuous.

Noting

$$\emptyset \subseteq \varphi(\emptyset) \subseteq \varphi\varphi(\emptyset) \subseteq \varphi\varphi\varphi(\emptyset) \subseteq \ldots$$

$$T \supseteq \varphi(T) \supseteq \varphi\varphi(T) \supseteq \varphi\varphi\varphi(T) \supseteq \ldots$$

by monotonicity, if the system has n states then,

$$\nu X.A = \varphi^n(T)$$

$$\mu X.A = \varphi^n(\emptyset)$$

Examples.

Consider the process

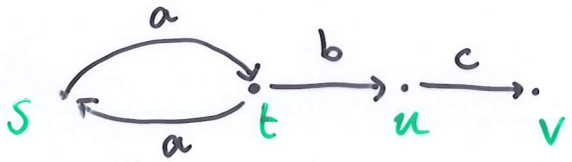
$$P \stackrel{\text{def}}{=} a.(a.P + b.c.nil)$$

$s = P$

$t = a.P + b.c.nil$

$u = c.nil$

$v = nil$



Which states satisfy: $\phi = \langle a \rangle \phi \leq \phi$

* $\mu X.\langle a \rangle X$ Least subset Y s.t. $\langle a \rangle Y \subseteq Y$

  $\phi \vee \langle a \rangle \phi \vee \langle a \rangle \langle a \rangle \phi \vee \ldots$

* $\nu X.\langle a \rangle X$ Greatest subset Y s.t. $Y \subseteq \langle a \rangle Y$

  $T \wedge \langle a \rangle T \wedge \langle a \rangle \langle a \rangle T \wedge \langle a \rangle \langle a \rangle \langle a \rangle T \wedge \ldots$

* $\mu X.[a] X$ Least subset Y s.t. $[a] Y \subseteq Y$

  $F \vee [a] F \vee [a][a] F \vee [a][a][a] F \vee \ldots$

* $\nu X.[a] X$ Greatest subset Y s.t. $Y \subseteq [a] Y$

Prop

$s \models \nu X.\ \langle a \rangle X$

in a finite-state transition system iff

$\exists$ an infinite sequence of a-transitions from s.

Proof

$$\varphi(X) \stackrel{\text{def}}{=} \langle a \rangle X$$

There is a decreasing chain

$$T \supseteq \varphi(T) \supseteq \dots \supseteq \varphi^n(T) \supseteq \dots$$

s.t.

$$\nu X.\ \langle a \rangle X = \bigcap_{n \in \omega} \varphi^n(T)$$

By induction, for all states t and $n \geq 1$

$t \models \varphi^n(T)$ iff $\exists t_1 \dots t_n$ s.t.

$$t \xrightarrow{a} t_1 \xrightarrow{a} \dots \xrightarrow{a} t_n$$

i.e. from t, there is a sequence of n a-transitions.

Assuming no. of states is k, $\nu X.\ \varphi(X) = \varphi^k(T) = \varphi^{k+1}(T)$

Hence $s \models \nu X.\ \langle a \rangle X$ iff $s \models \varphi^k(T)$

iff $\exists$ a sequence of k a-transitions from s.

Such a path must loop, so there is an infinite sequence.

CTL

$$A ::= At \mid A_0 \wedge A_1 \mid A_0 \vee A_1 \mid \neg A \mid T \mid F \mid EX A \mid EG A \mid E[A_0 \, U \, A_1]$$

A path from a state s is a maximal sequence of states

$$\pi = (\pi_0, \pi_1, \cdots, \pi_i, \cdots)$$

s.t. $s = \pi_0$ & $\pi_i \rightarrow \pi_{i+1}$, all i.

$s \models EXA$ iff Exists a path from s whose neXt state satisfies A.

$s \models EGA$ iff Exists a path from s such that Globally A on path.

$s \models E[A \, U \, B]$ iff Exists a path from s on which A Until B.

Derived assertions

$$AX\,B \equiv \neg EX \neg B$$

$$EF\,B \equiv E[T\,U\,B]$$

$$AG\,B \equiv \neg EF \neg B$$

$$AF\,B \equiv \neg EG \neg B$$

$$A[B\,U\,C] \equiv$$

$$\neg E[\neg C\,U(\neg B \wedge \neg C)] \wedge \neg EG \neg C$$