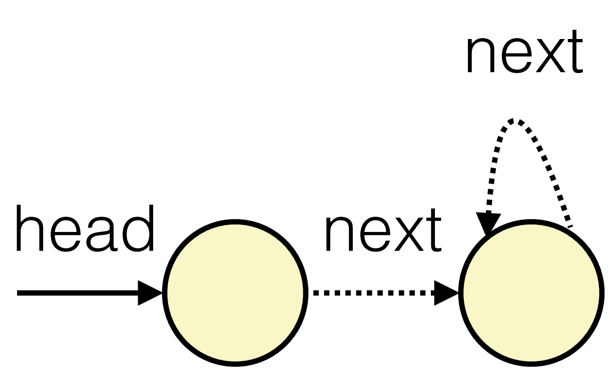
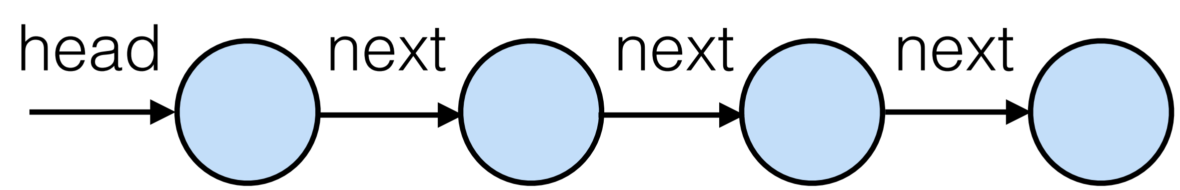
Related Work

Abstract



Concrete



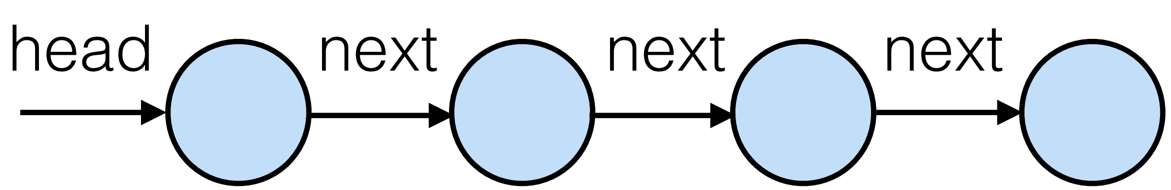
reachability $\Rightarrow$ reachability

Related Work

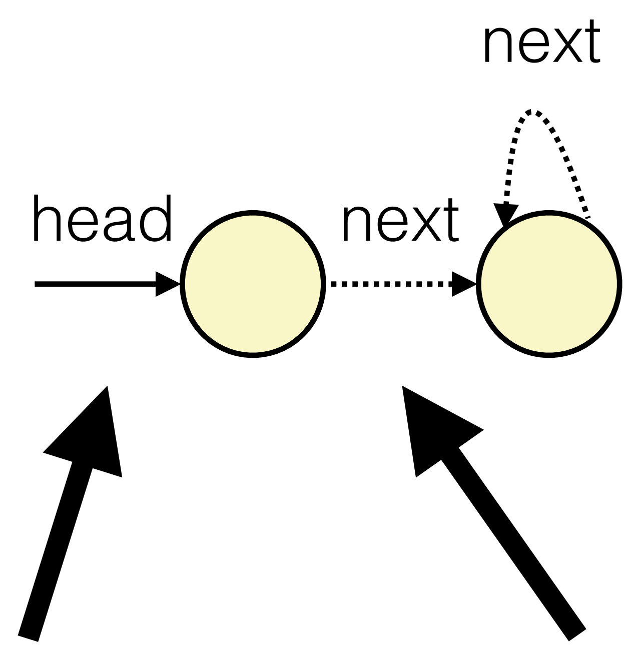
Paper	Query lang.	Abstractions	Updates
3-valued logic	FO(TC)	possible edge	yes
Canonical Graph Shapes	???	Local FOL	no
Modal logic Graph Abstr.	Modal logic	Multiplicities	yes

Parametric Shape Analysis

Concrete



Abstract

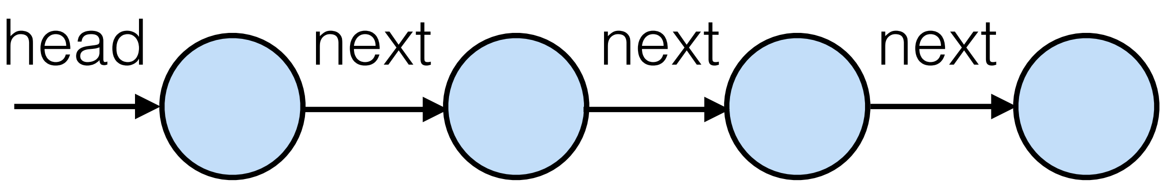


Edge *does* exist

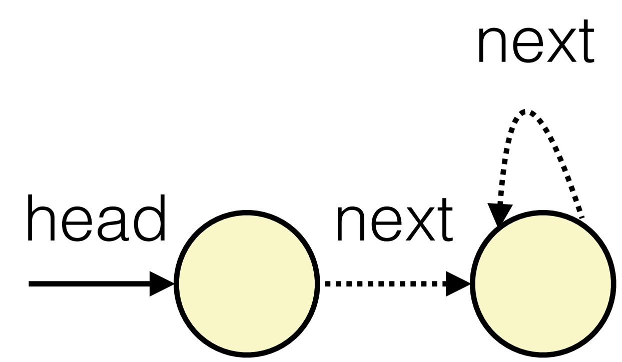
Edge *may* exist

Parametric Shape Analysis

Concrete



Abstract

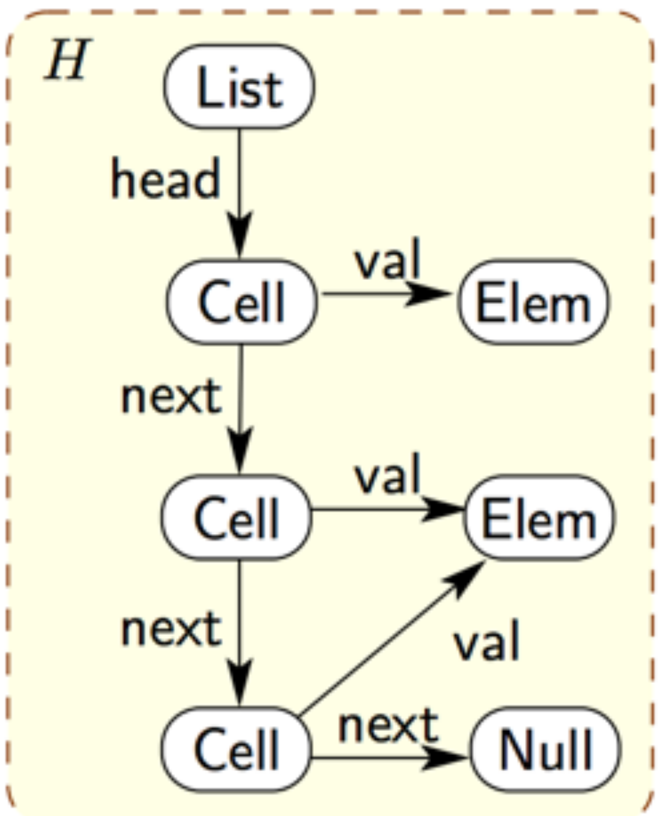


Any property in FO(TC) that holds in the abstract graph, also holds in the concrete graph

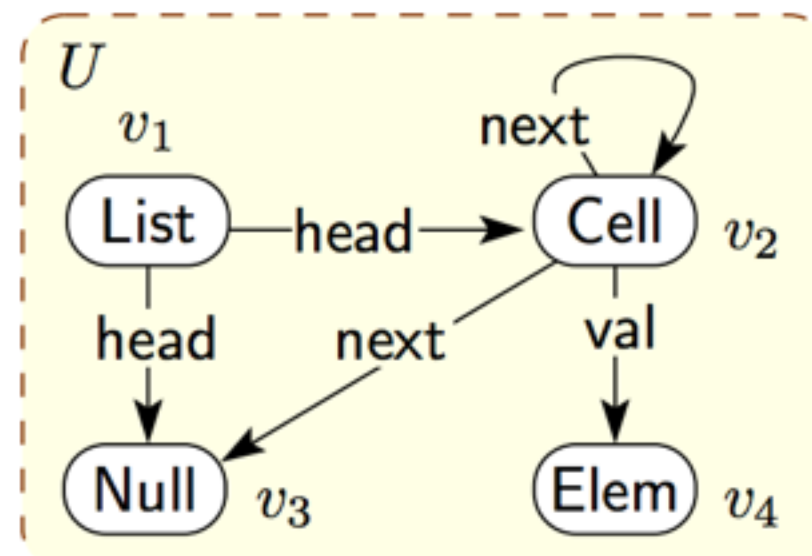
Canonical Graph Shapes

x — y

f(x) — f(y)



Graph Morphism



Concrete

Abstract

Canonical Graph Shapes

“The notion of graph typing is rather weak: the existence of a morphism from a would-be instance graph to a would-be type graph can only forbid but never enforce the presence of certain edges in the instance.”

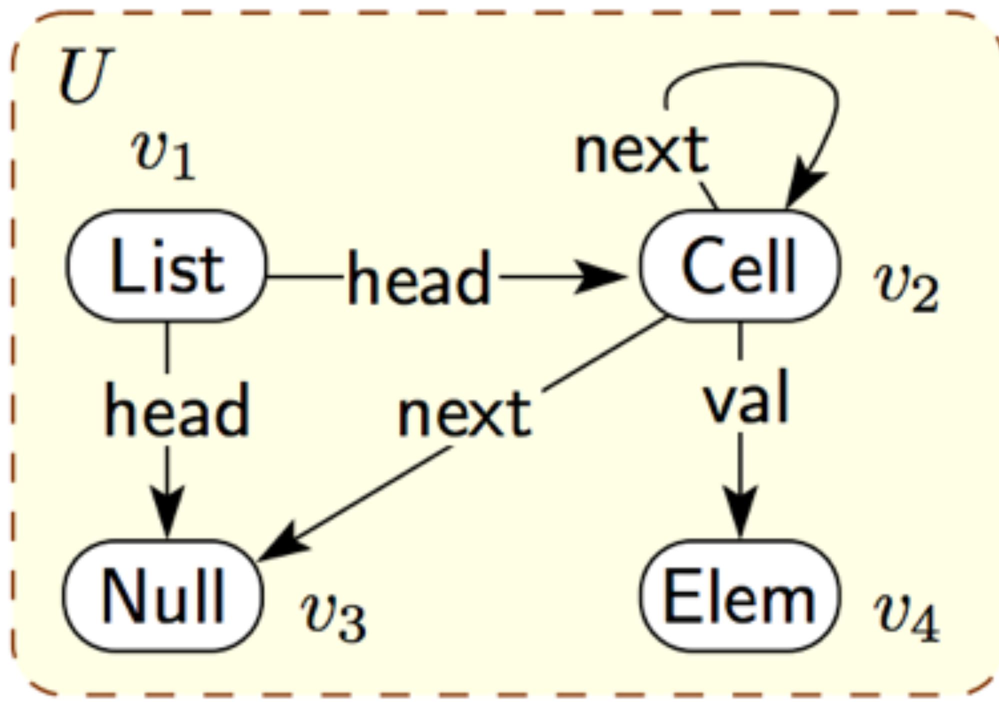
Canonical Graph Shapes

Local Shape Logic

$$\xi ::= v \ \mid \ \xrightarrow{a} v \ \mid \ \xleftarrow{a} v \ \mid \ \overset{a}{-} \ .$$
$$\phi ::= \mathbf{tt} \ \mid \ {}^{\mu}[\xi] \ \mid \ \neg\phi \ \mid \ \phi \vee \phi \ \mid \ \forall_v \phi \ .$$

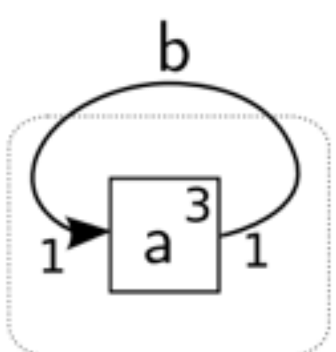
- Only ever talk about 2 nodes at a time
- Constraints given as multiplicities

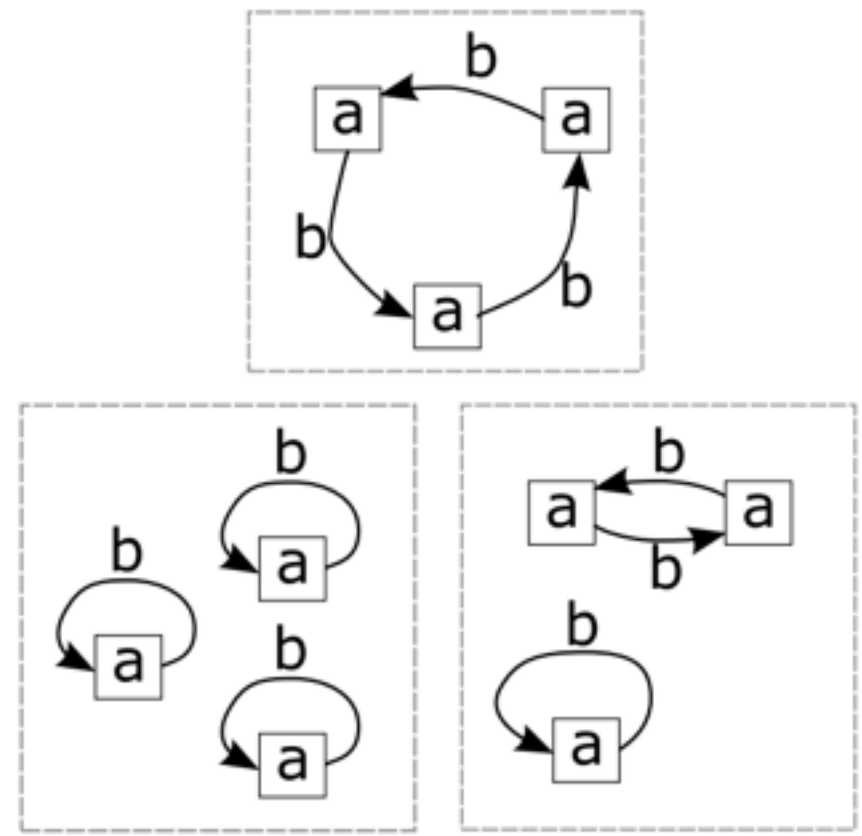
Canonical Graph Shapes



$$
\begin{array}{ll}
(1') & \forall_{v_1}({}^{\uparrow}[\underline{\mathsf{List}}] \wedge (({}^{\mathbf{1}}[\xrightarrow{\mathsf{head}} v_2] \wedge {}^{\mathbf{0}}[\xrightarrow{\mathsf{head}} v_3]) \vee ({}^{\mathbf{0}}[\xrightarrow{\mathsf{head}} v_2] \wedge {}^{\mathbf{1}}[\xrightarrow{\mathsf{head}} v_3]))) \\
(2') & {}^{\mathbf{1}}[v_3] \wedge \forall_{v_3} {}^{\uparrow}[\underline{\mathsf{Null}}] \\
(3') & \forall_{v_2}(({}^{\mathbf{1}}[\xrightarrow{\mathsf{next}} v_2] \wedge {}^{\mathbf{0}}[\xrightarrow{\mathsf{next}} v_3]) \vee ({}^{\mathbf{0}}[\xrightarrow{\mathsf{next}} v_2] \wedge {}^{\mathbf{1}}[\xrightarrow{\mathsf{next}} v_3])) \\
(4') & \forall_{v_2}(({}^{\mathbf{1}}[\xleftarrow{\mathsf{head}} v_1] \wedge {}^{\mathbf{0}}[\xleftarrow{\mathsf{next}} v_2]) \vee ({}^{\mathbf{0}}[\xleftarrow{\mathsf{head}} v_1] \wedge {}^{\mathbf{1}}[\xleftarrow{\mathsf{next}} v_2])) \\
(5') & \exists_{v_4} {}^{\mathbf{0}}[\xleftarrow{\mathsf{val}} v_2]
\end{array}
$$

Modal Logic Graph Abstraction

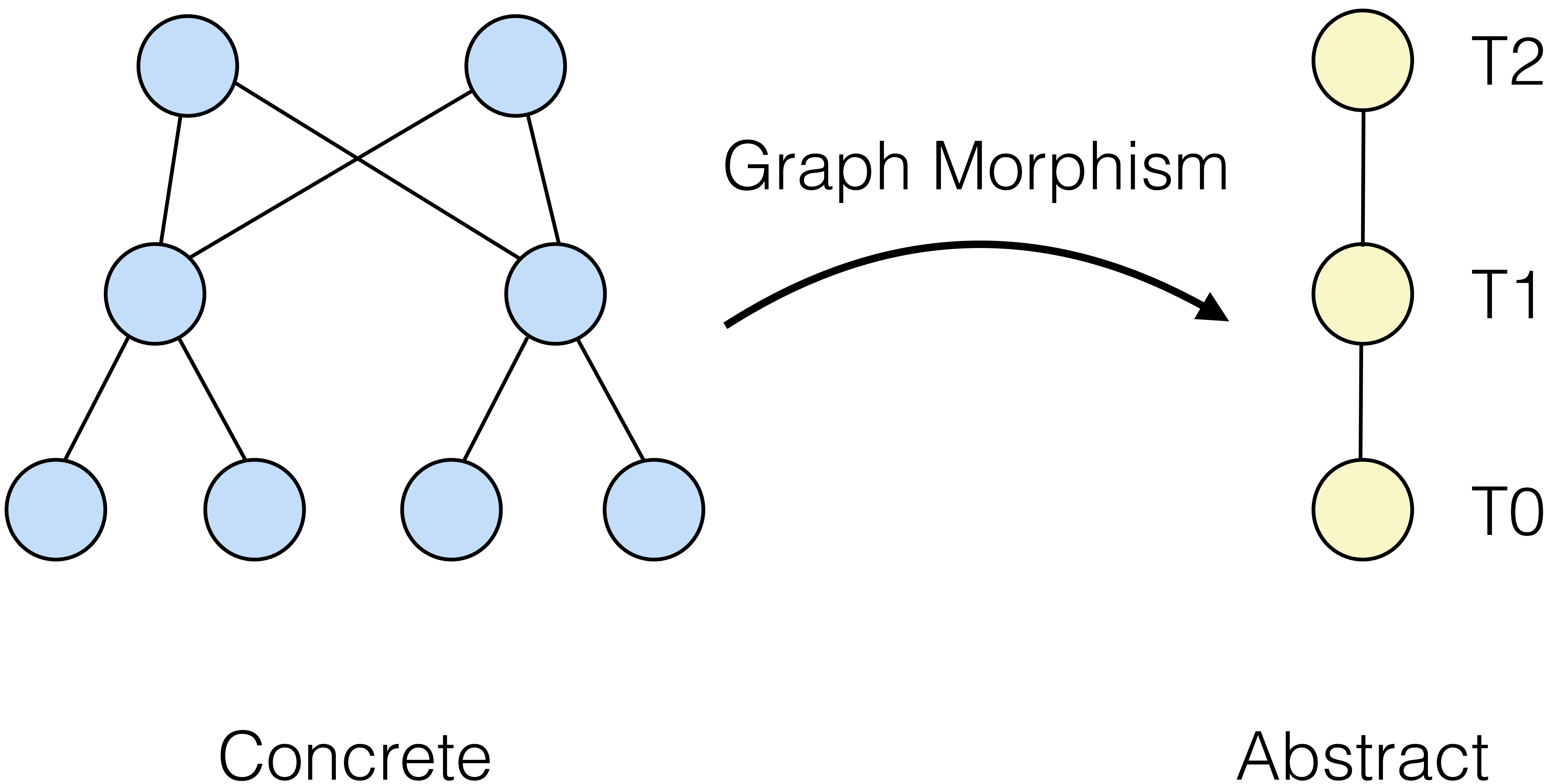




Abstract

Concrete

Abstract Topology

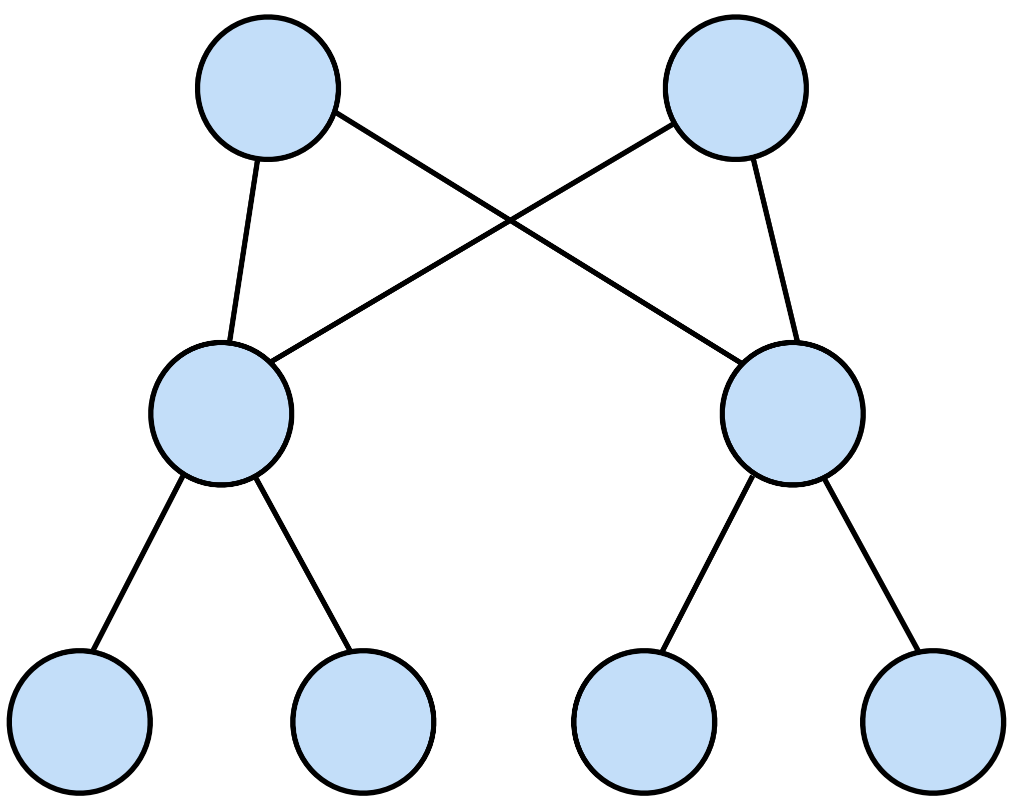


Abstract Topology

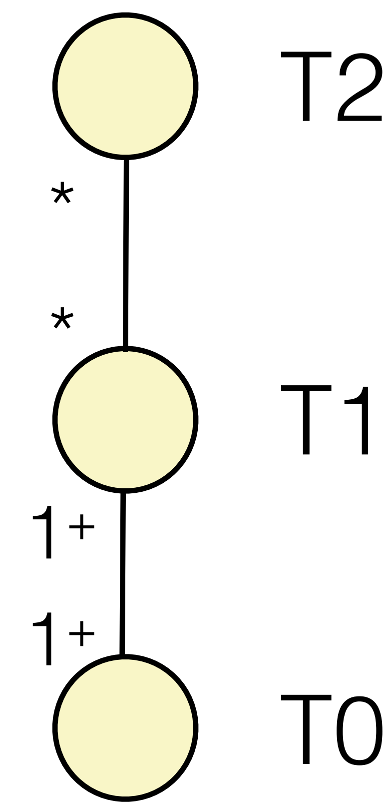
0	Zero
1	One
0^+	Zero or more
1^+	One or more
*	All/any number

Multiplicities

Abstract Topology

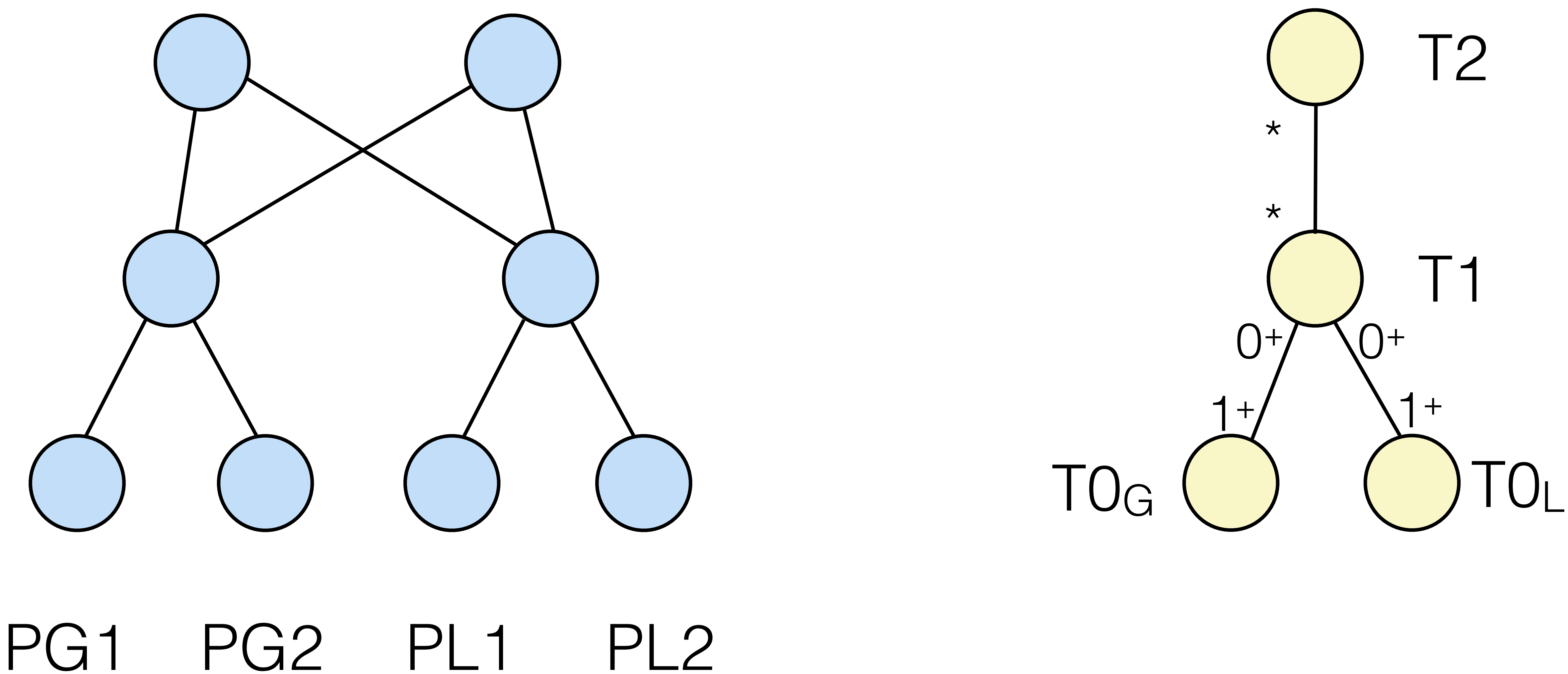


Concrete

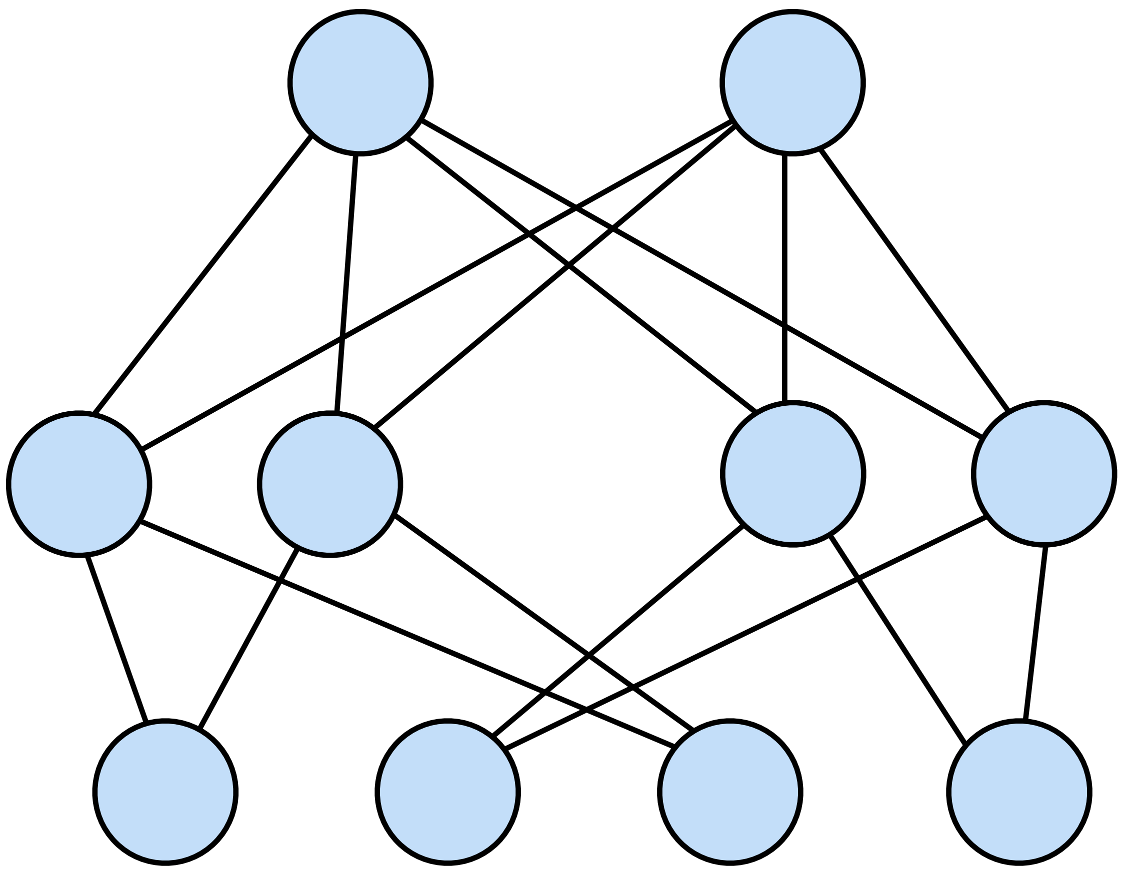


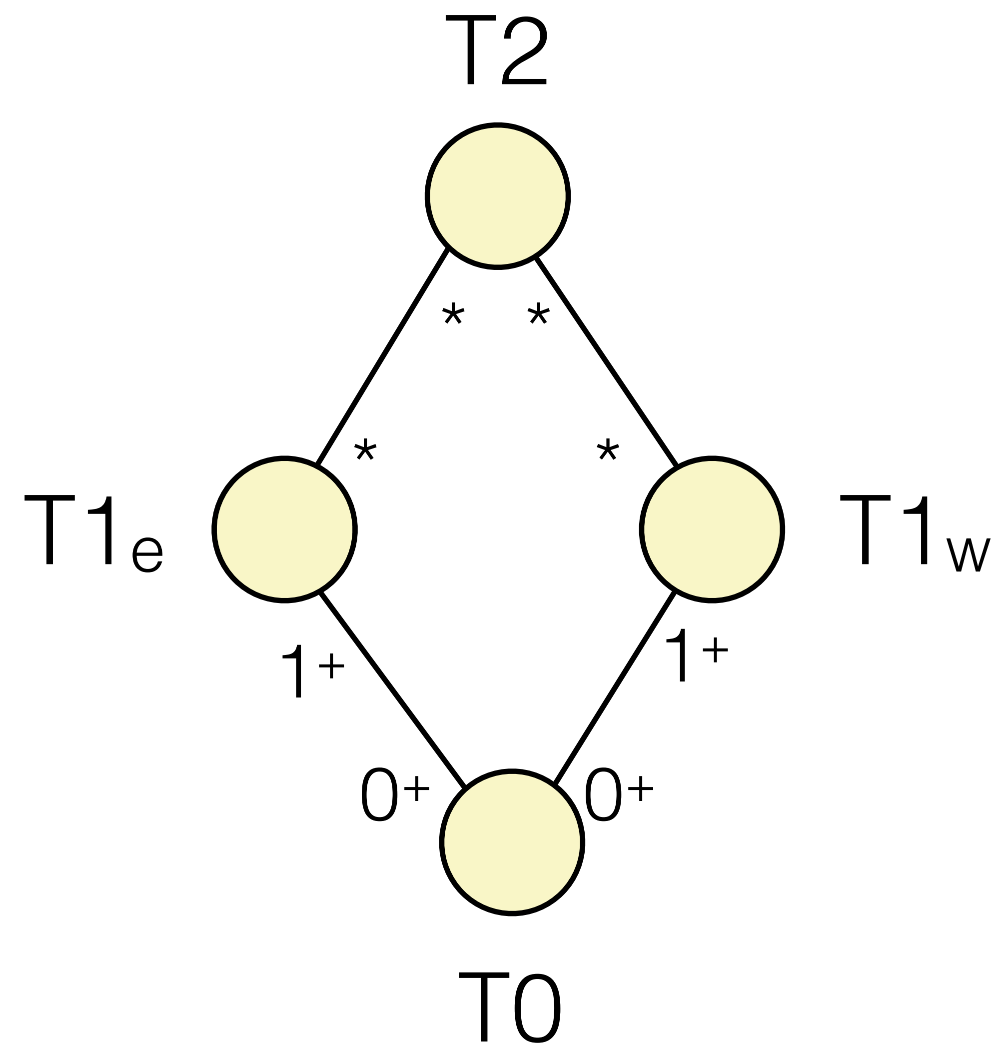
Abstract

Abstract Topology

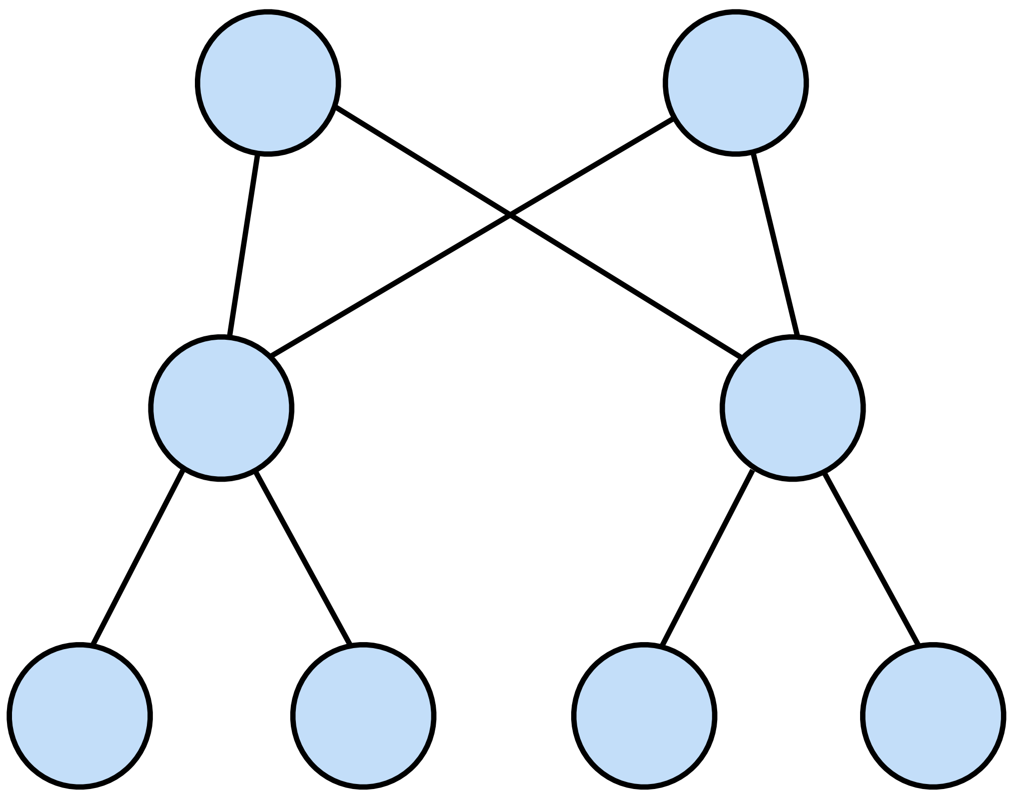


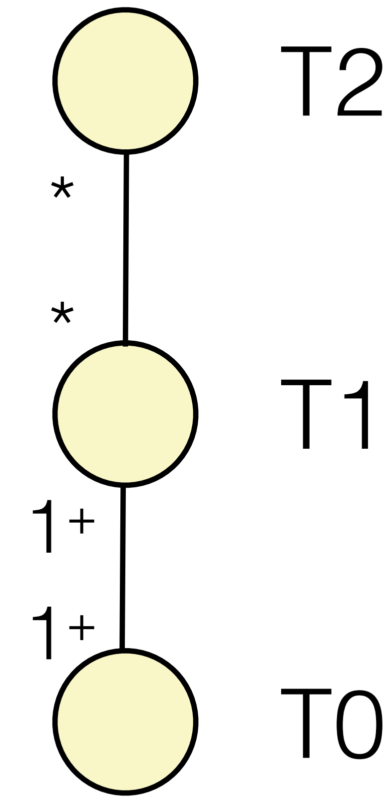
Abstract Topology





Reachability

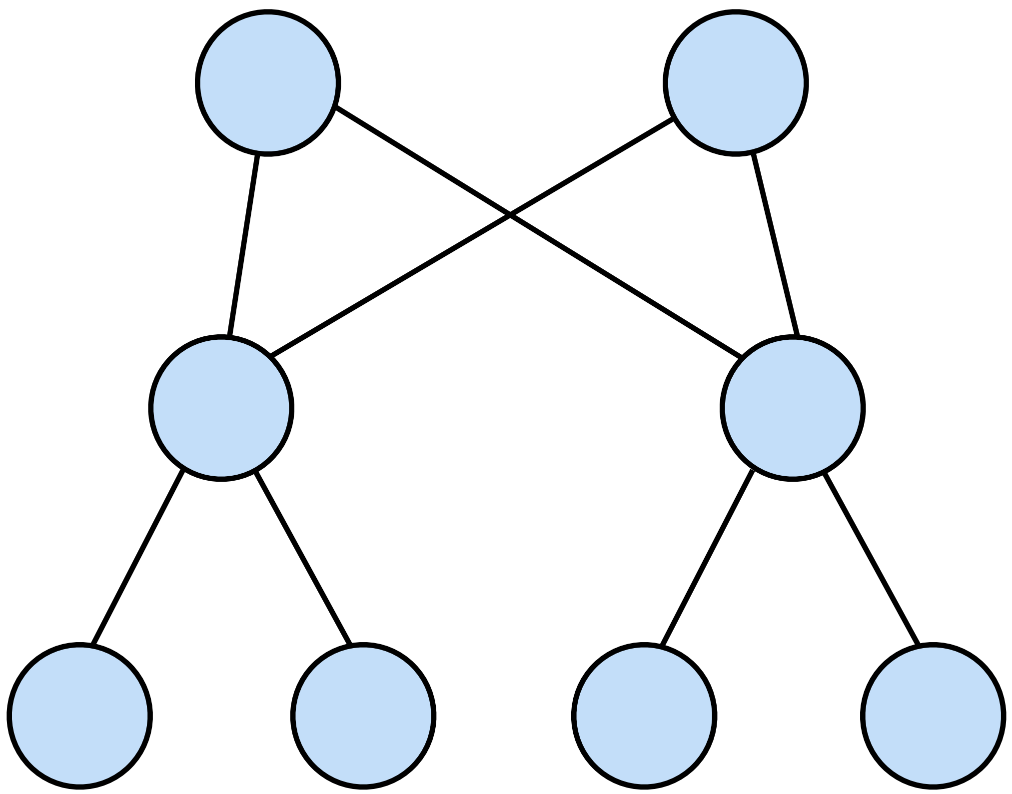


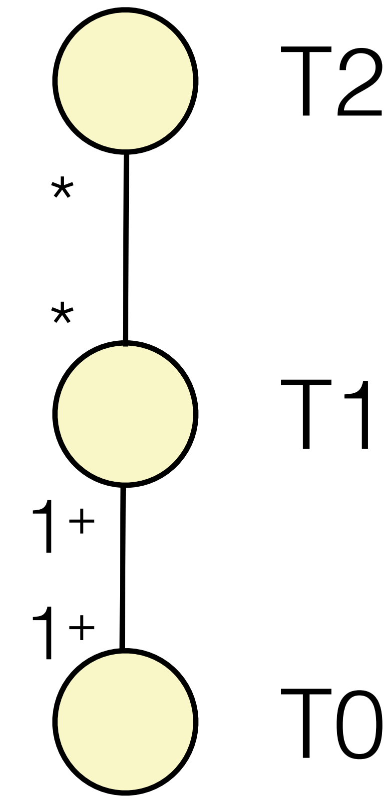


Reachability Query

If I start from some node in T0, which/how many nodes are reachable in T2, T1, T0?

Reachability

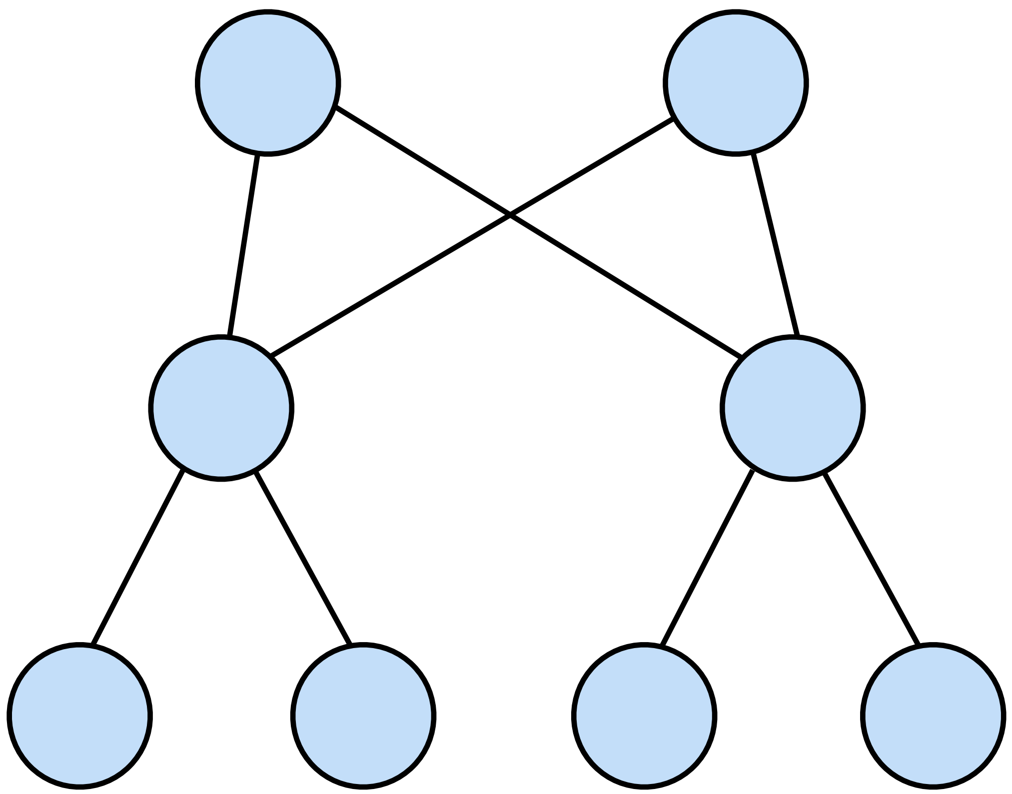


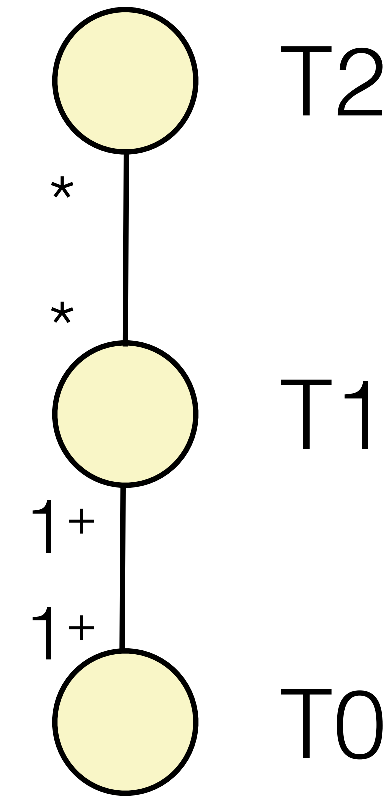


Idea

Abstract the reachable nodes as (None | Some | All)

Reachability

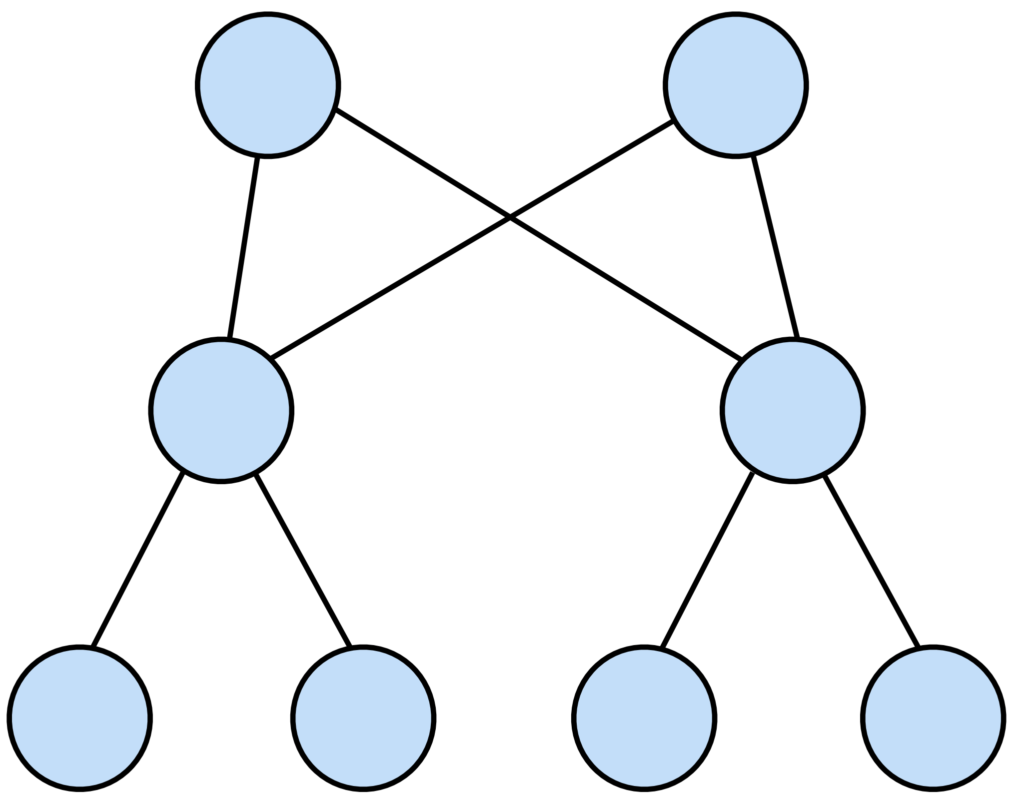


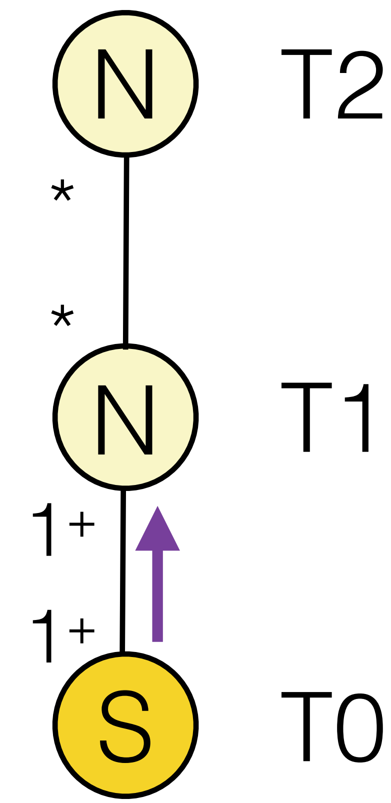


Define max operator

	N	S	A
N	N	S	A
S	S	S	A
A	A	A	A

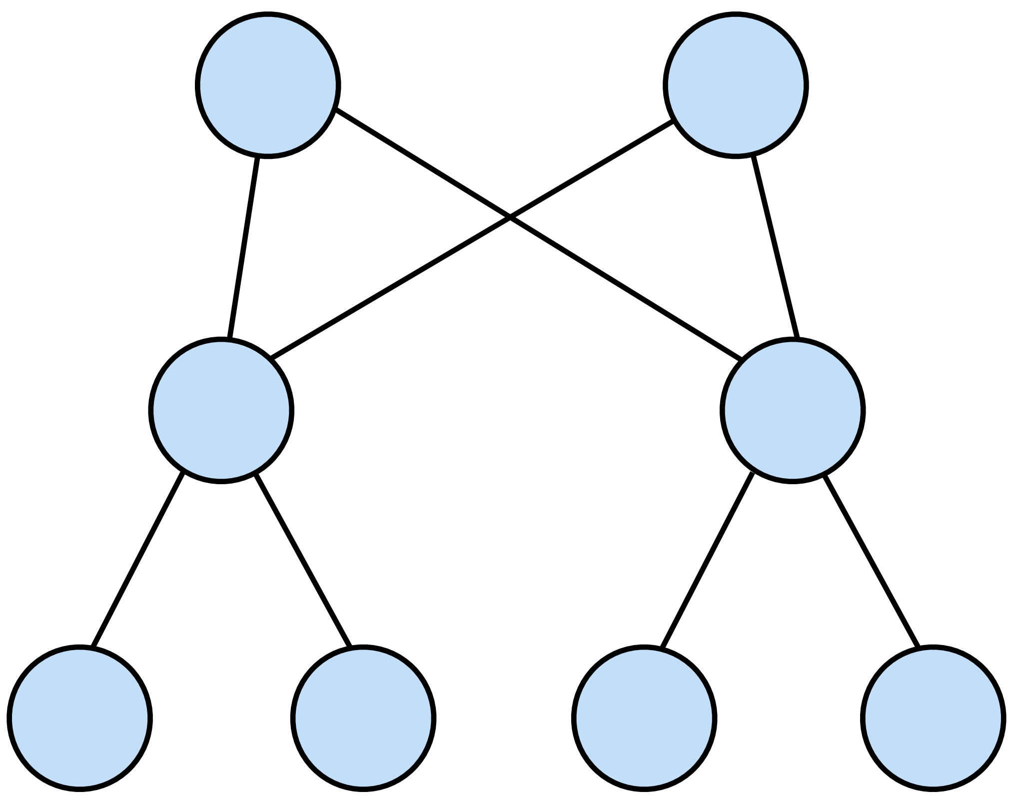
Reachability - Example 1

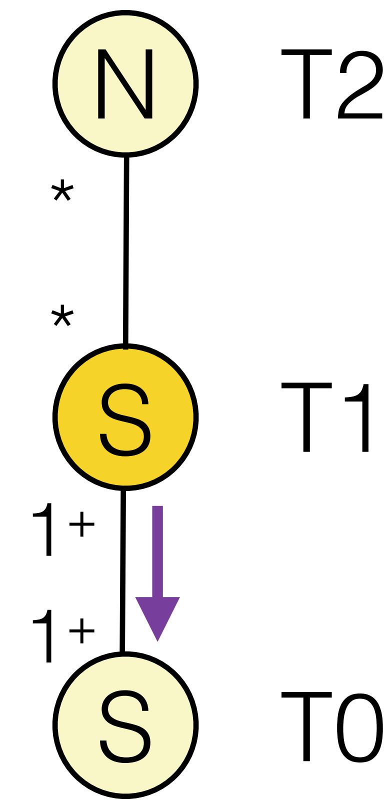




Start from *some* arbitrary node in T0

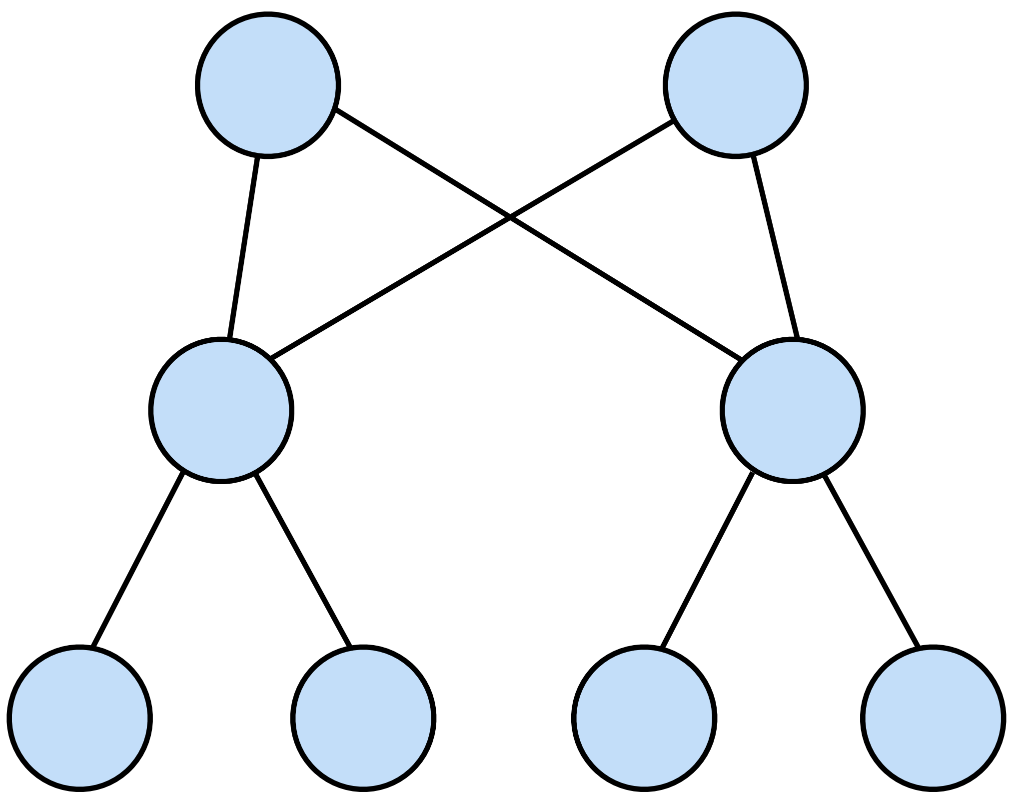
Reachability - Example 1

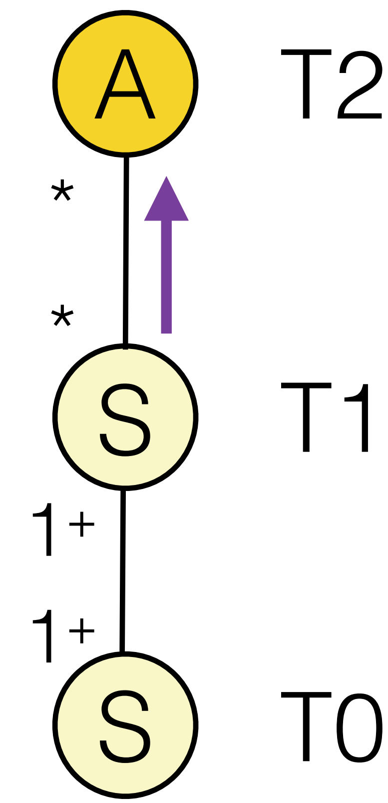




Start from *some* arbitrary node in T0

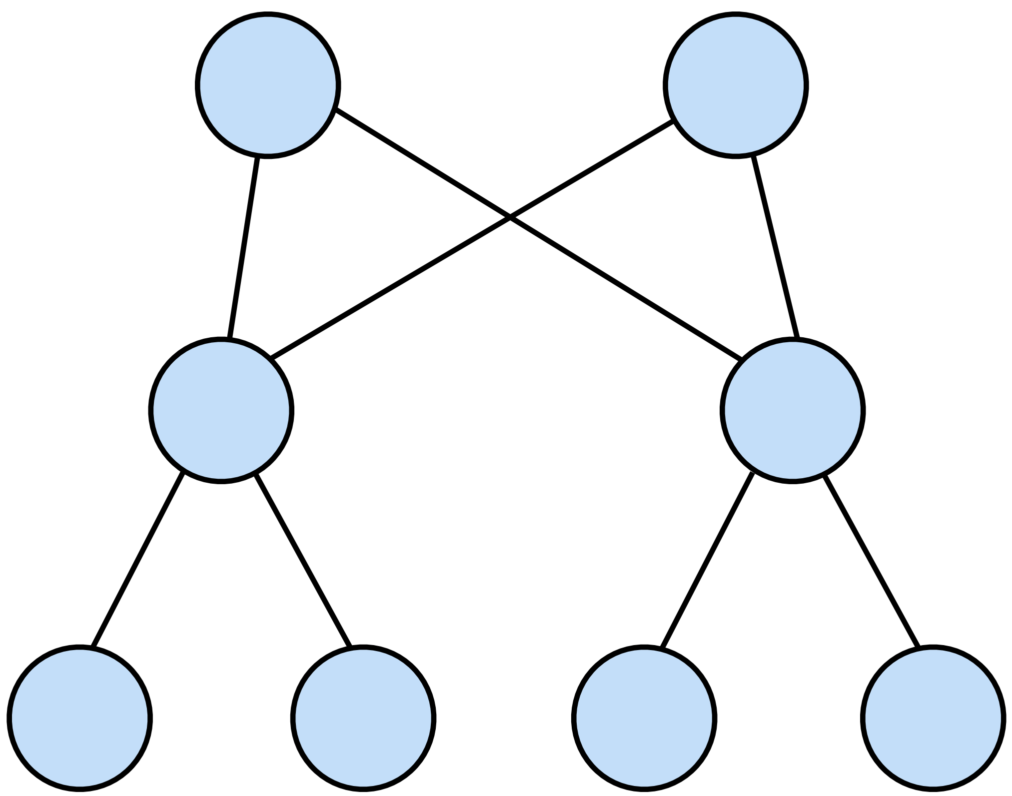
Reachability - Example 1

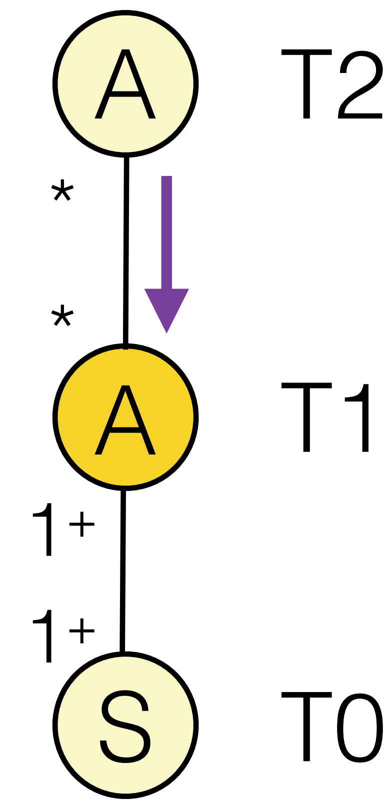




Start from *some* arbitrary node in T0

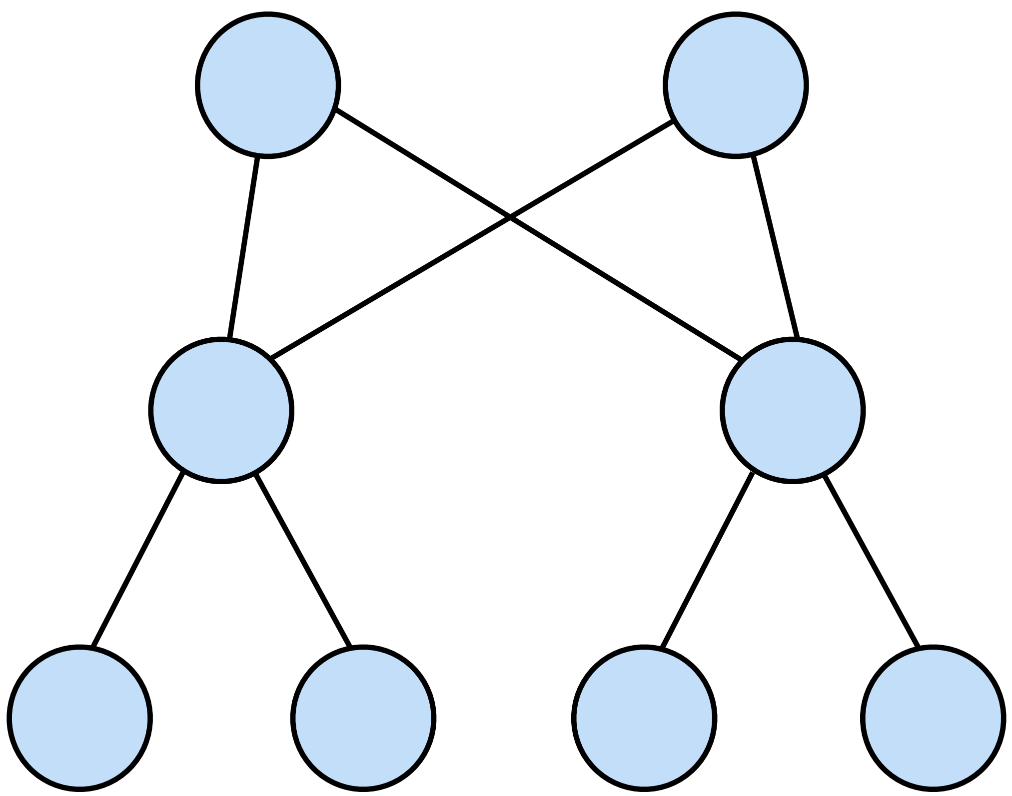
Reachability - Example 1

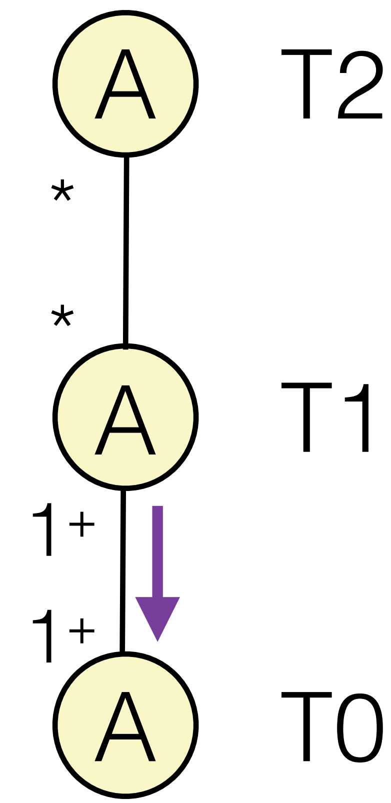




Start from *some* arbitrary node in T0

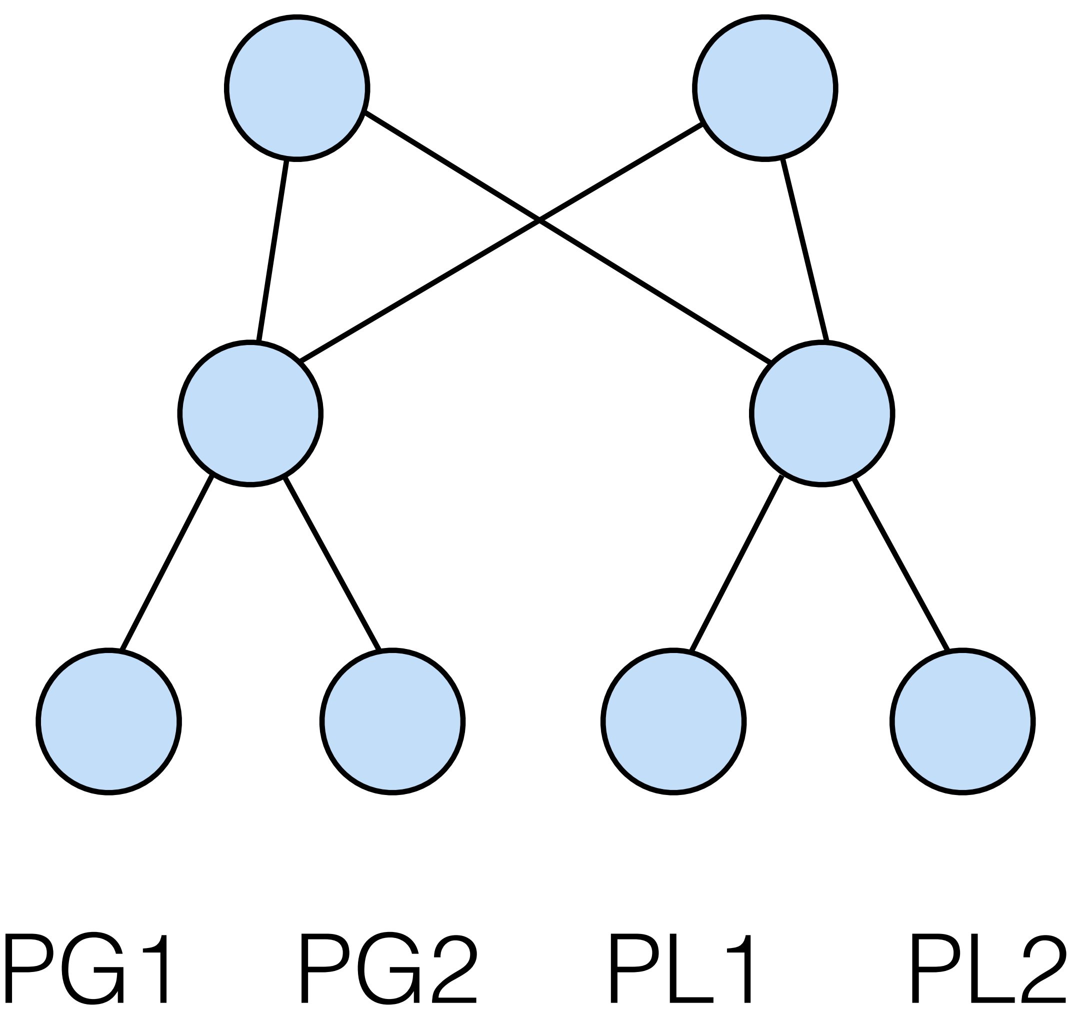
Reachability - Example 1

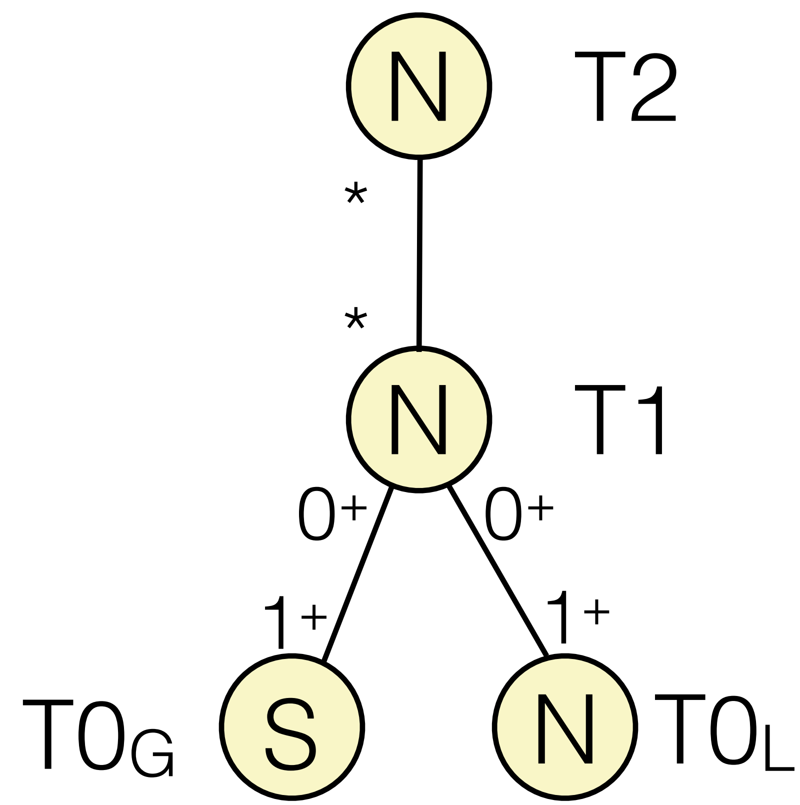




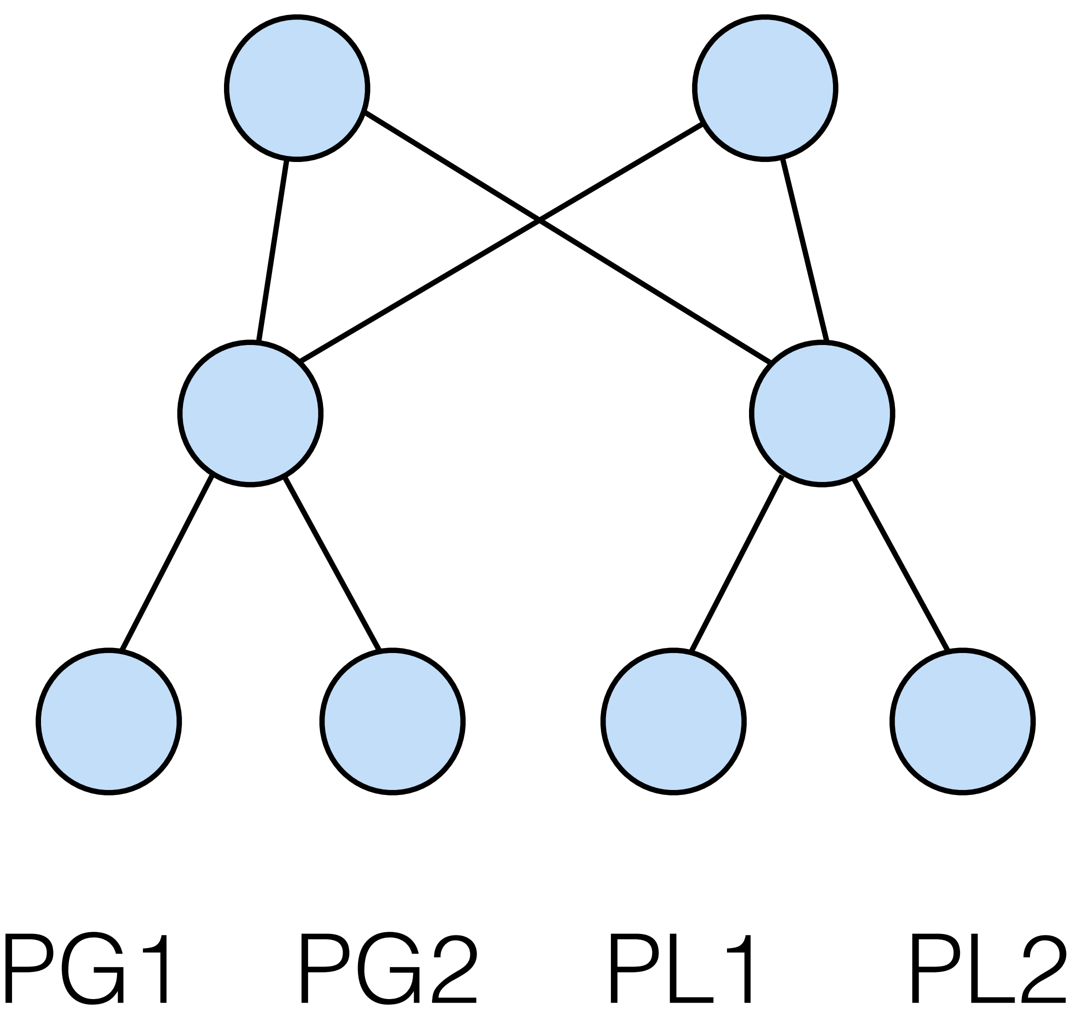
Start from *some* arbitrary node in T0

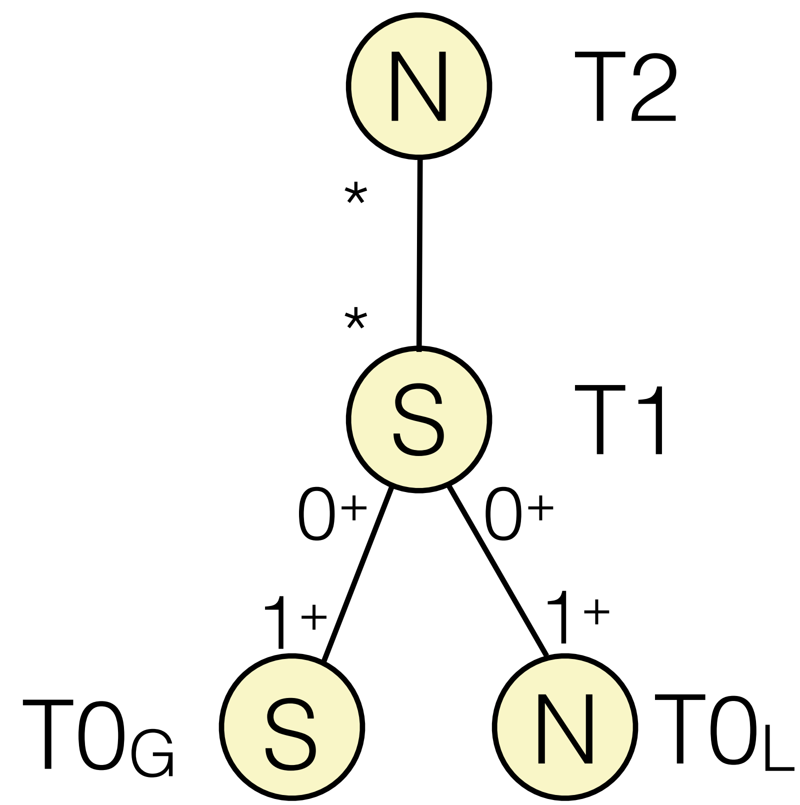
Reachability - Example 2



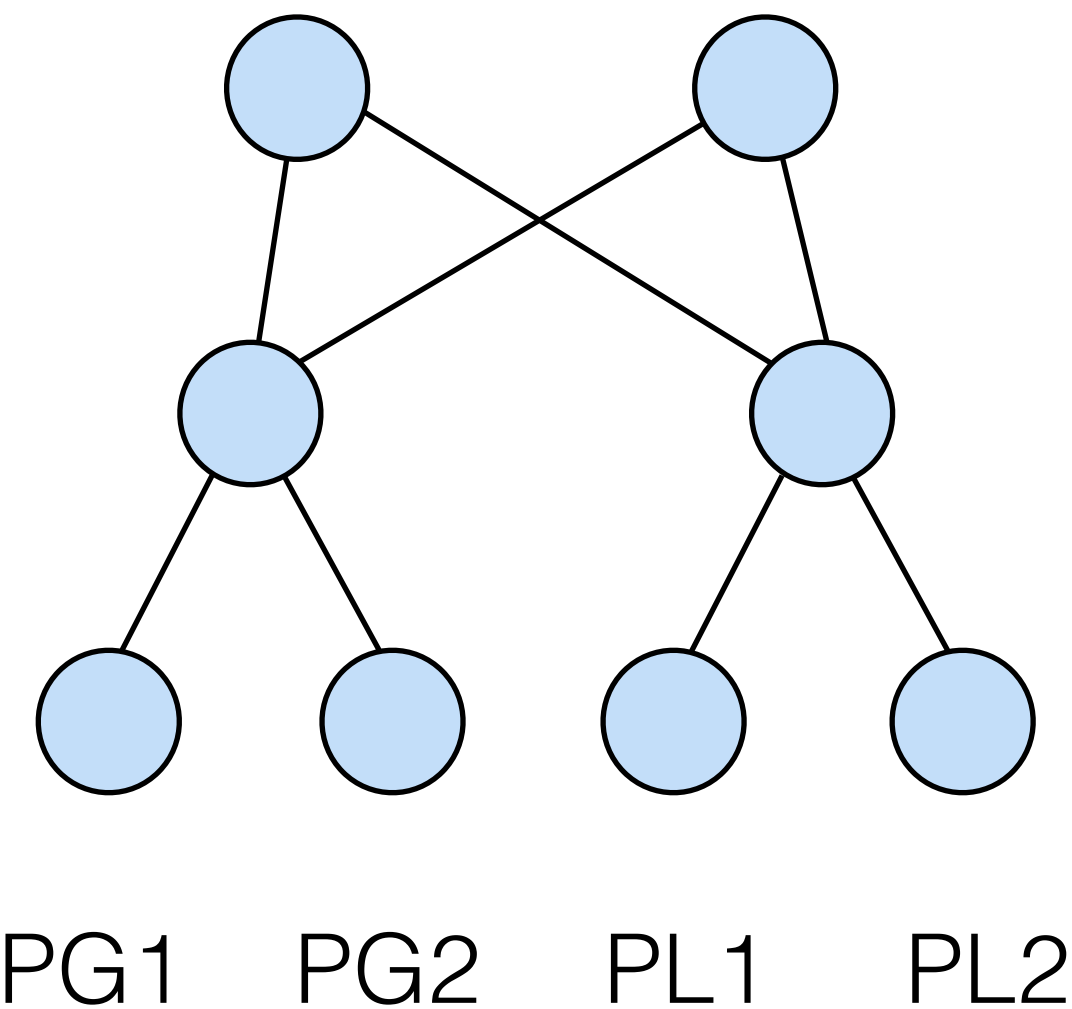


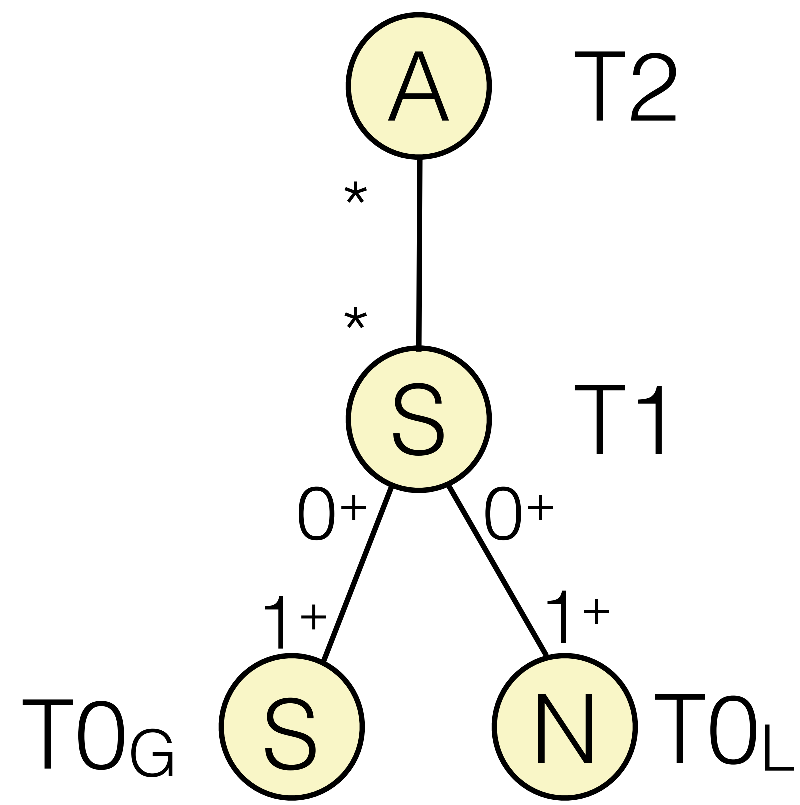
Reachability - Example 2



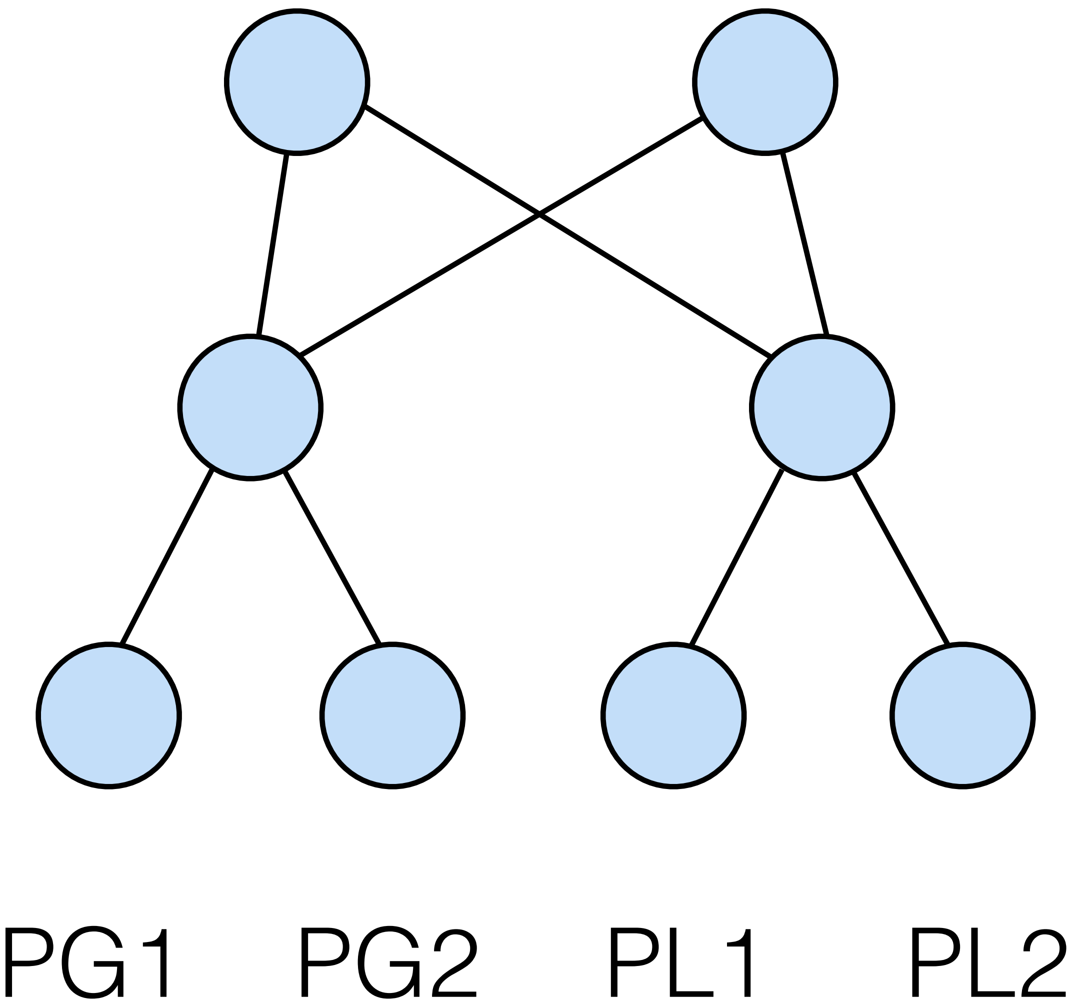


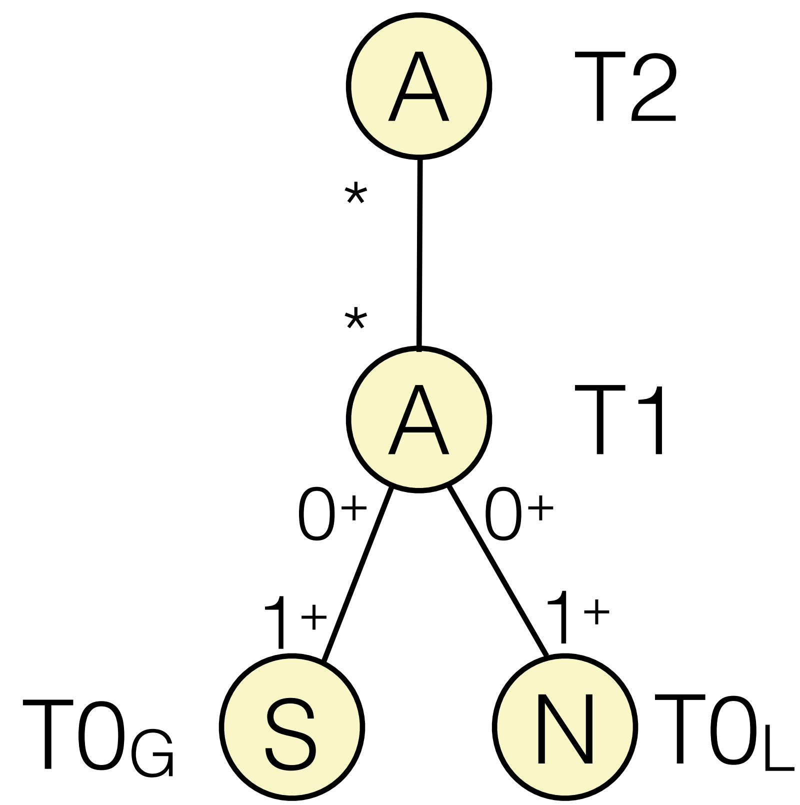
Reachability - Example 2



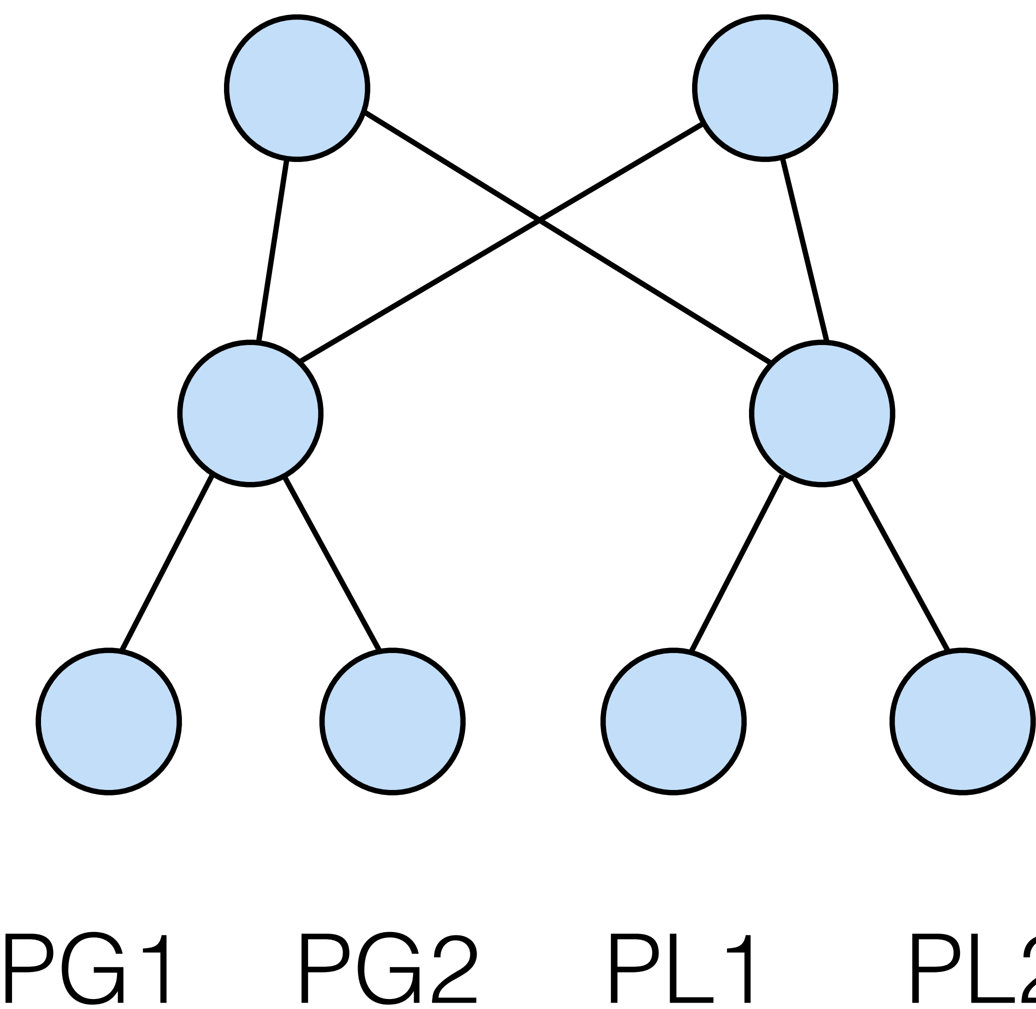


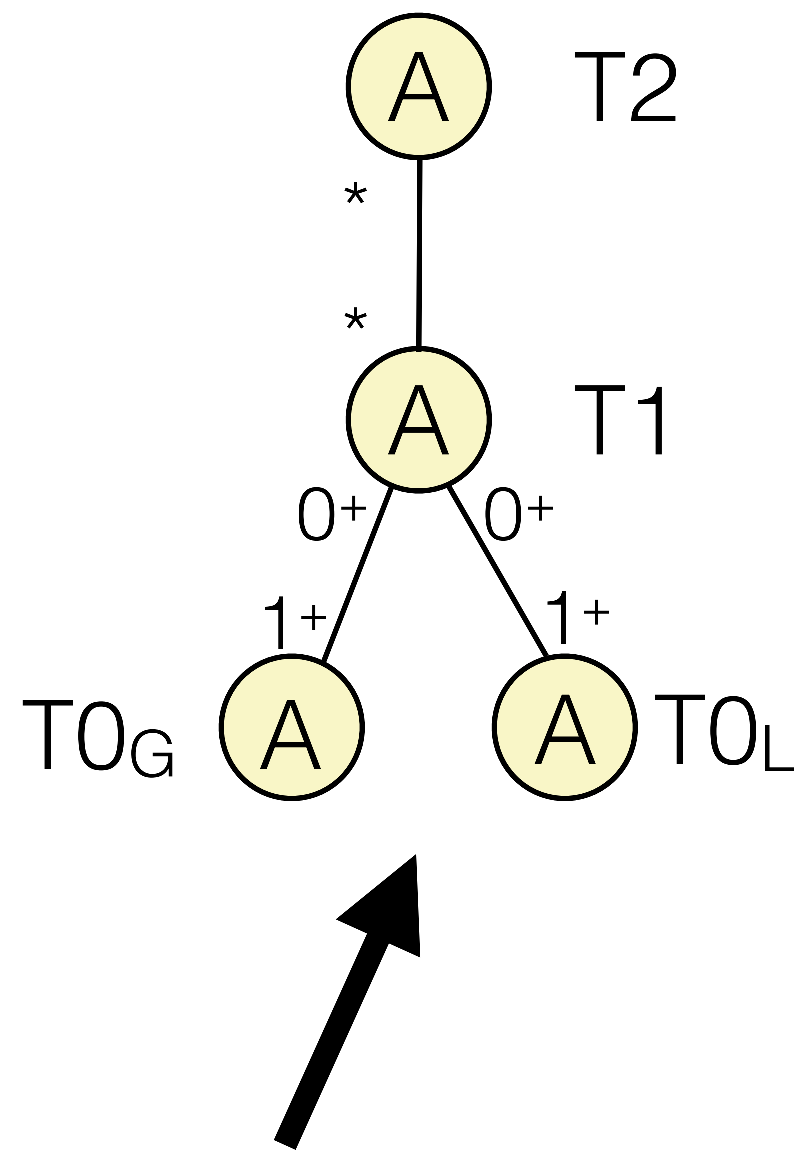
Reachability - Example 2





Reachability - Example 2





Outgoing edge information not enough

Abstract Topology

	0	1	0^+	1^+	*
N	N	N	N	N	N
S	N	S	N	S	A
A	N	S	N	S	A

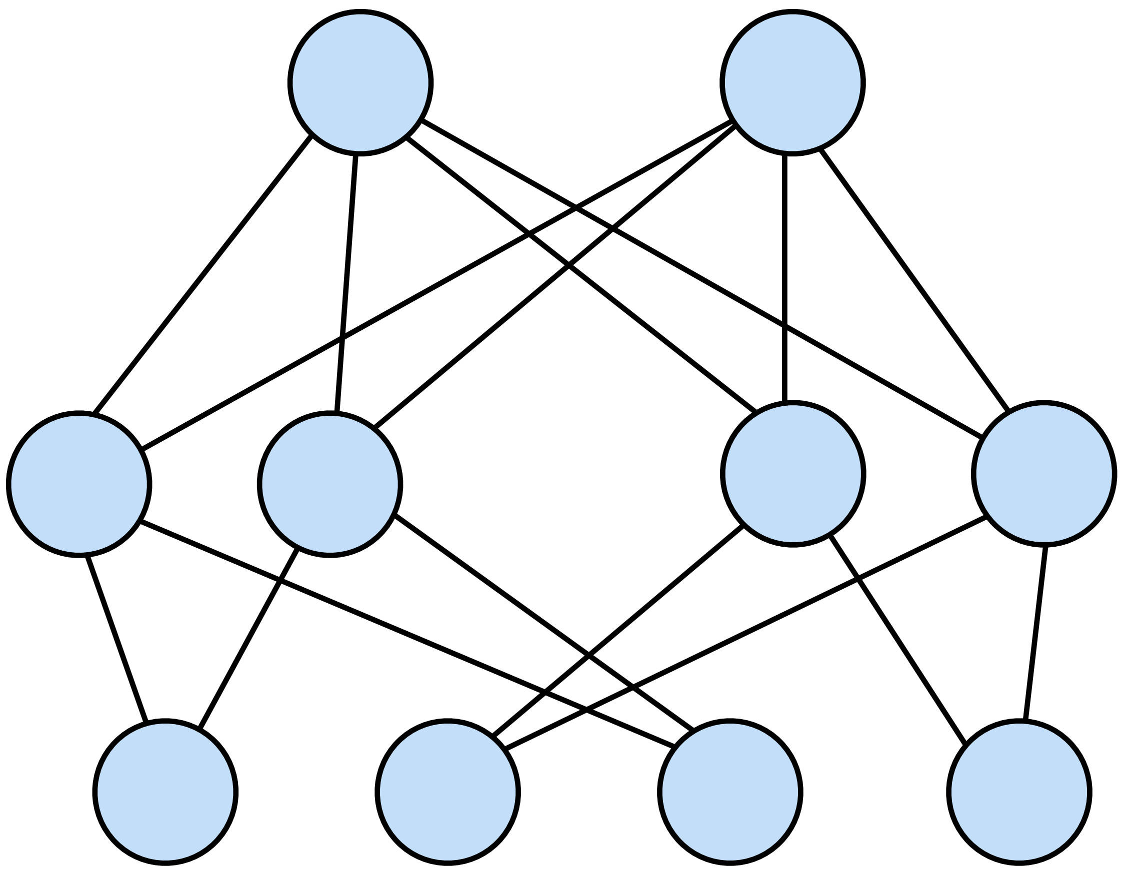
	0	1	0^+	1^+	*
N	N	N	N	N	N
S	N	S	N	S	A
A	N	**A**	N	**A**	A

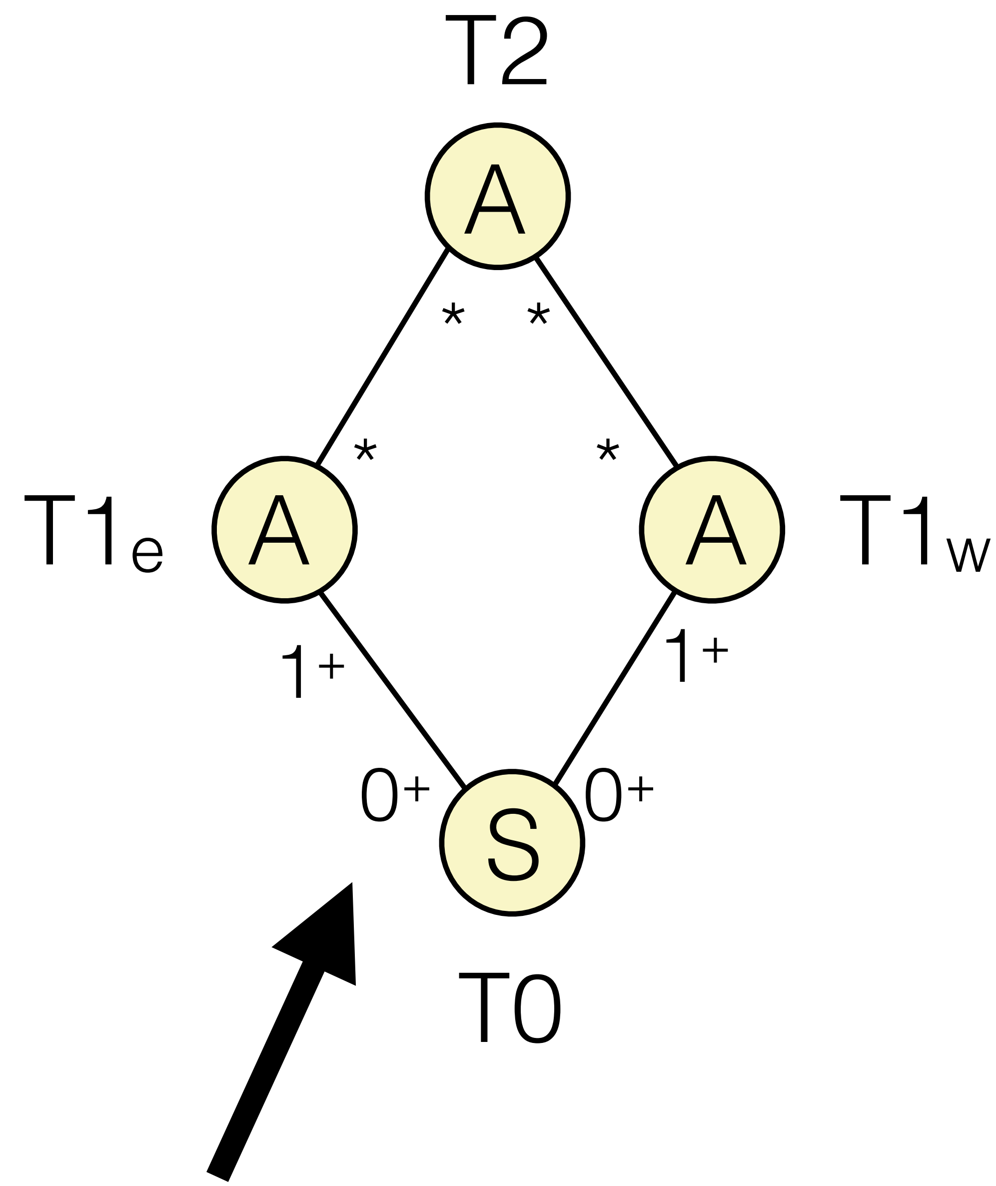
Outgoing production

Max → Current Value

Incoming production

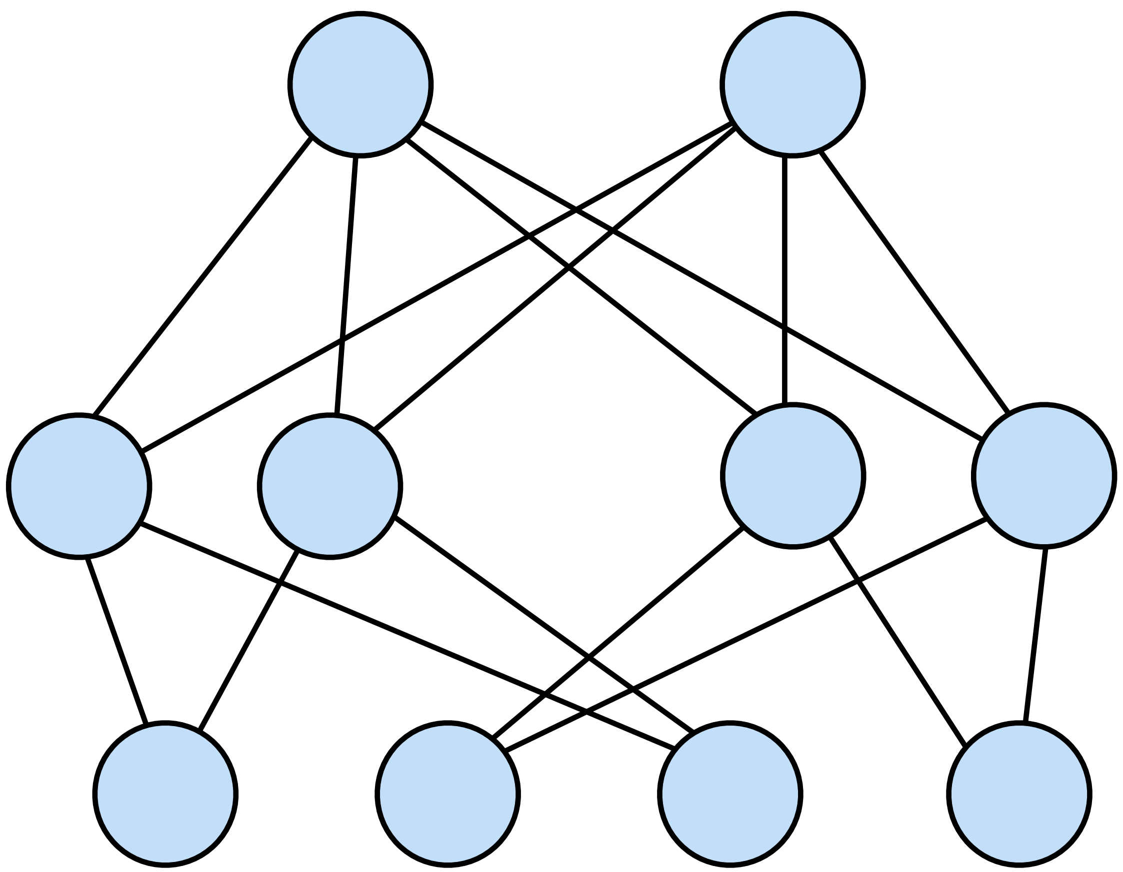
Reachability — Issue

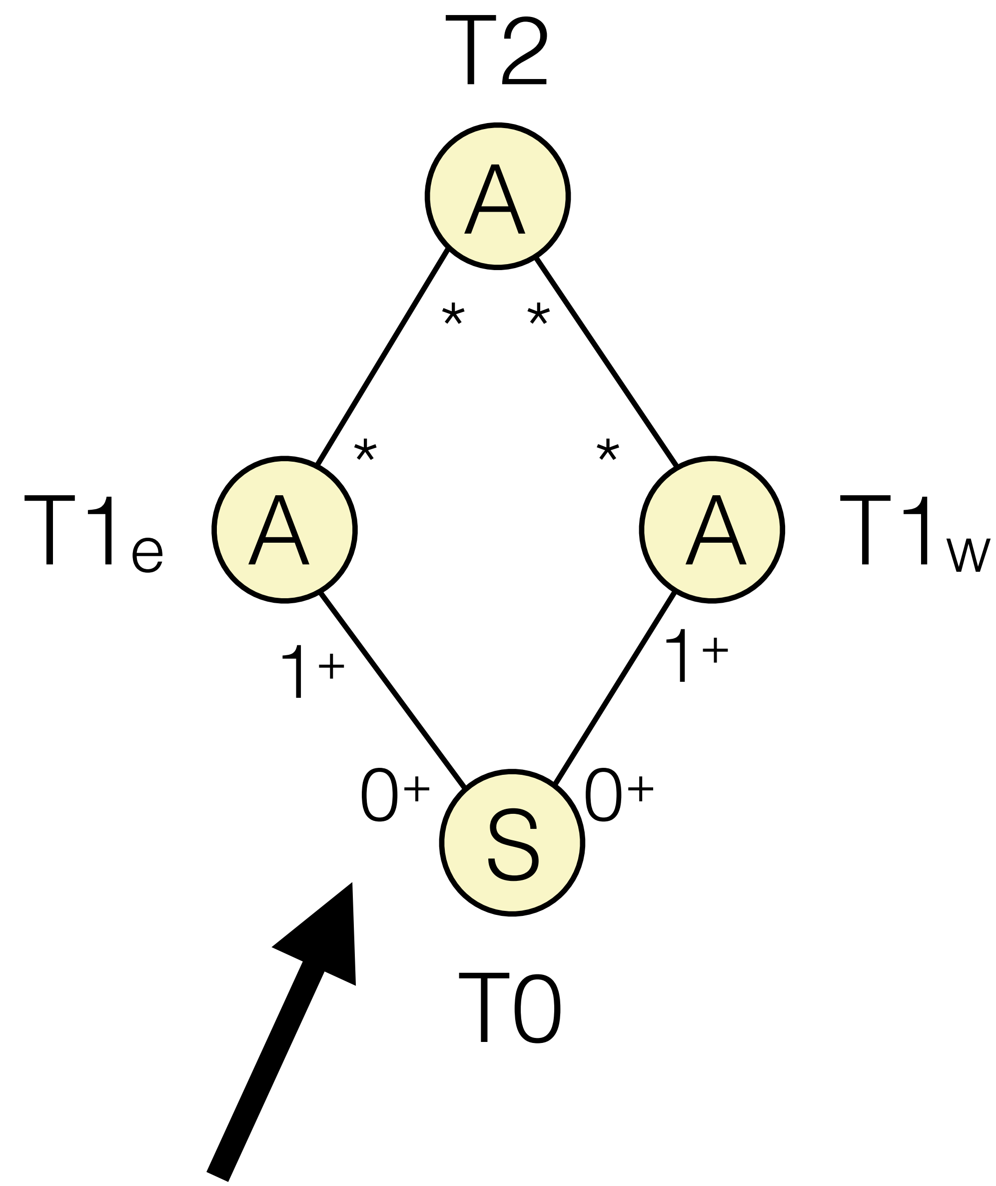




Not strong enough
Implicit disjunction

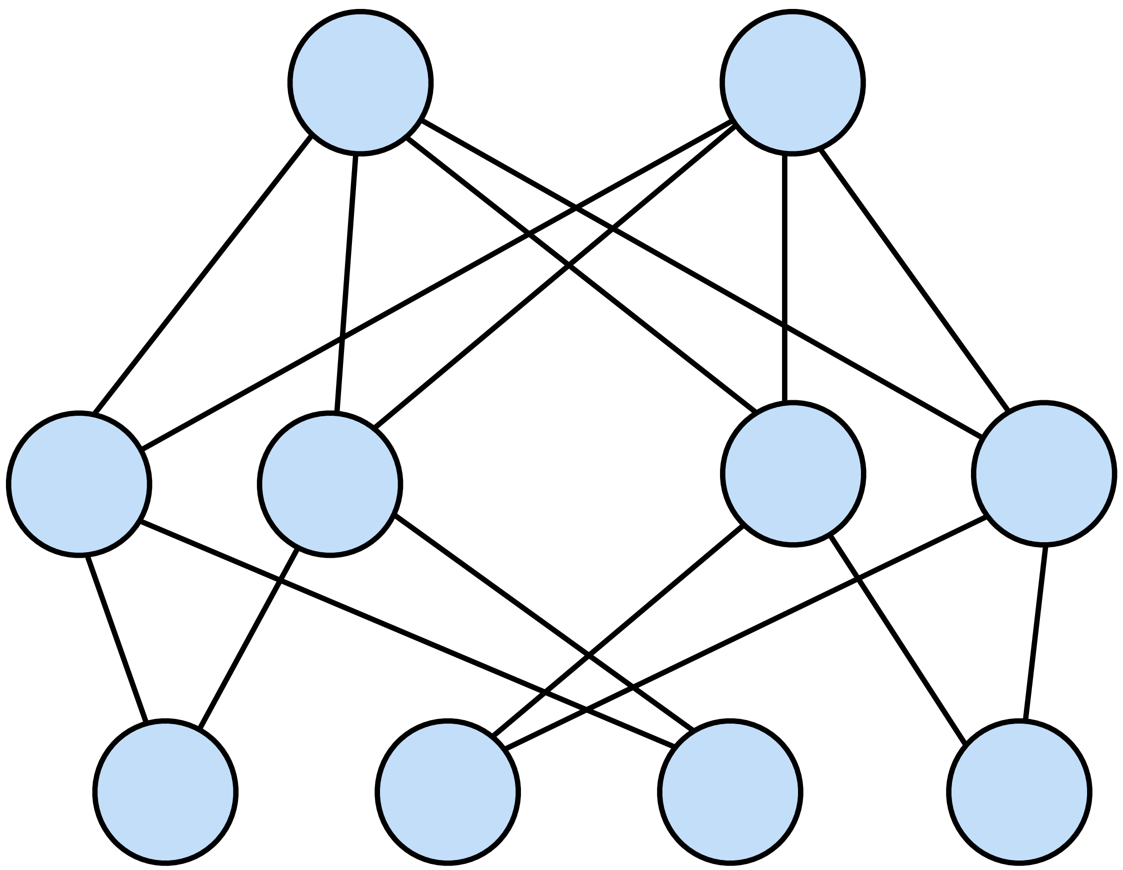
Reachability — Issue

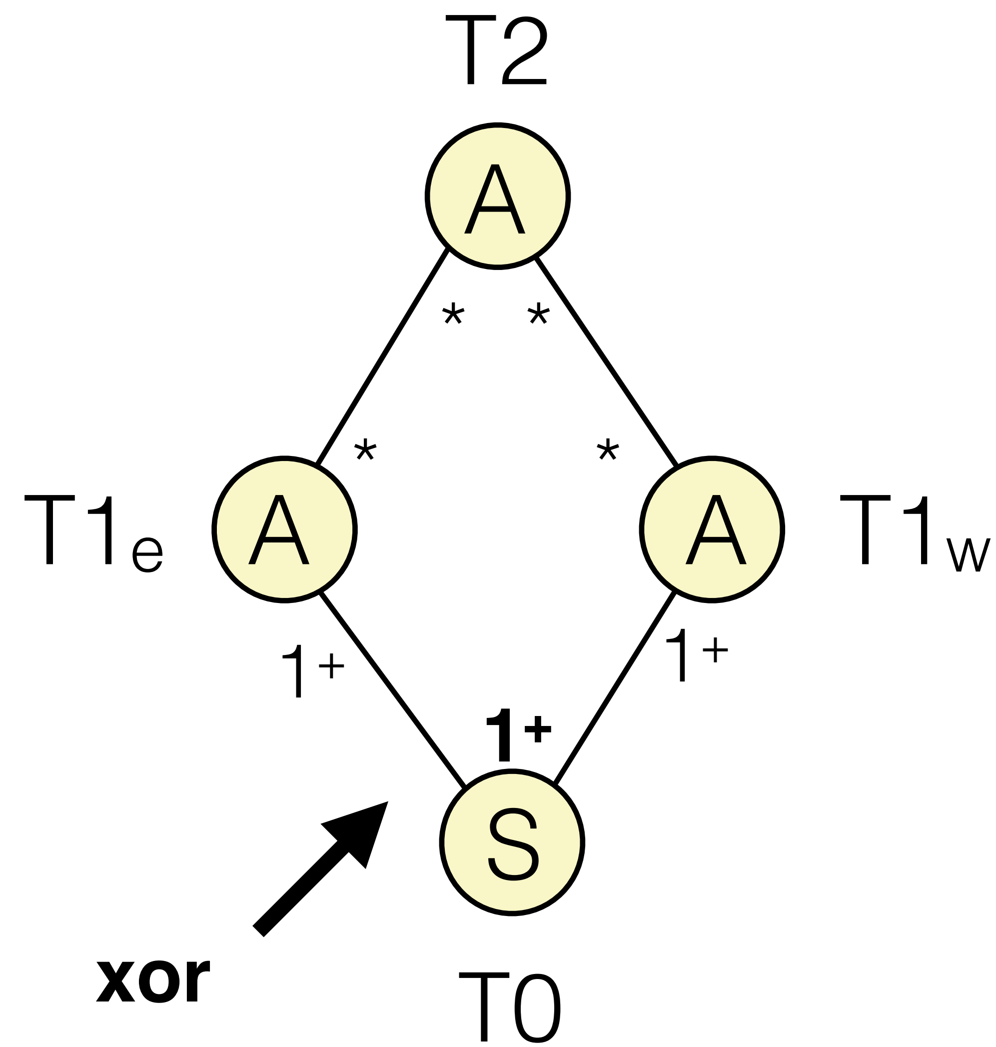




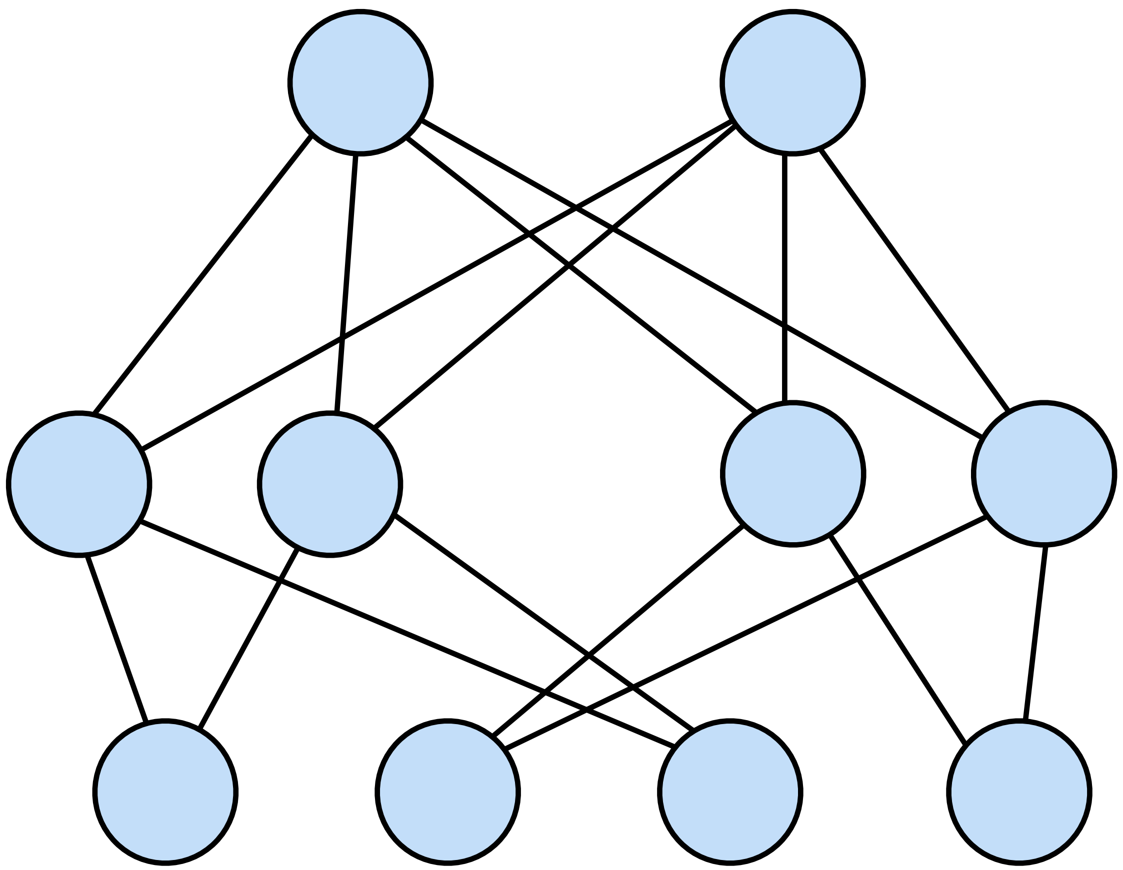
$$\forall\, T0,\ {}^{1}[\longleftarrow T1_e] \vee {}^{1}[\longleftarrow T1_w]$$

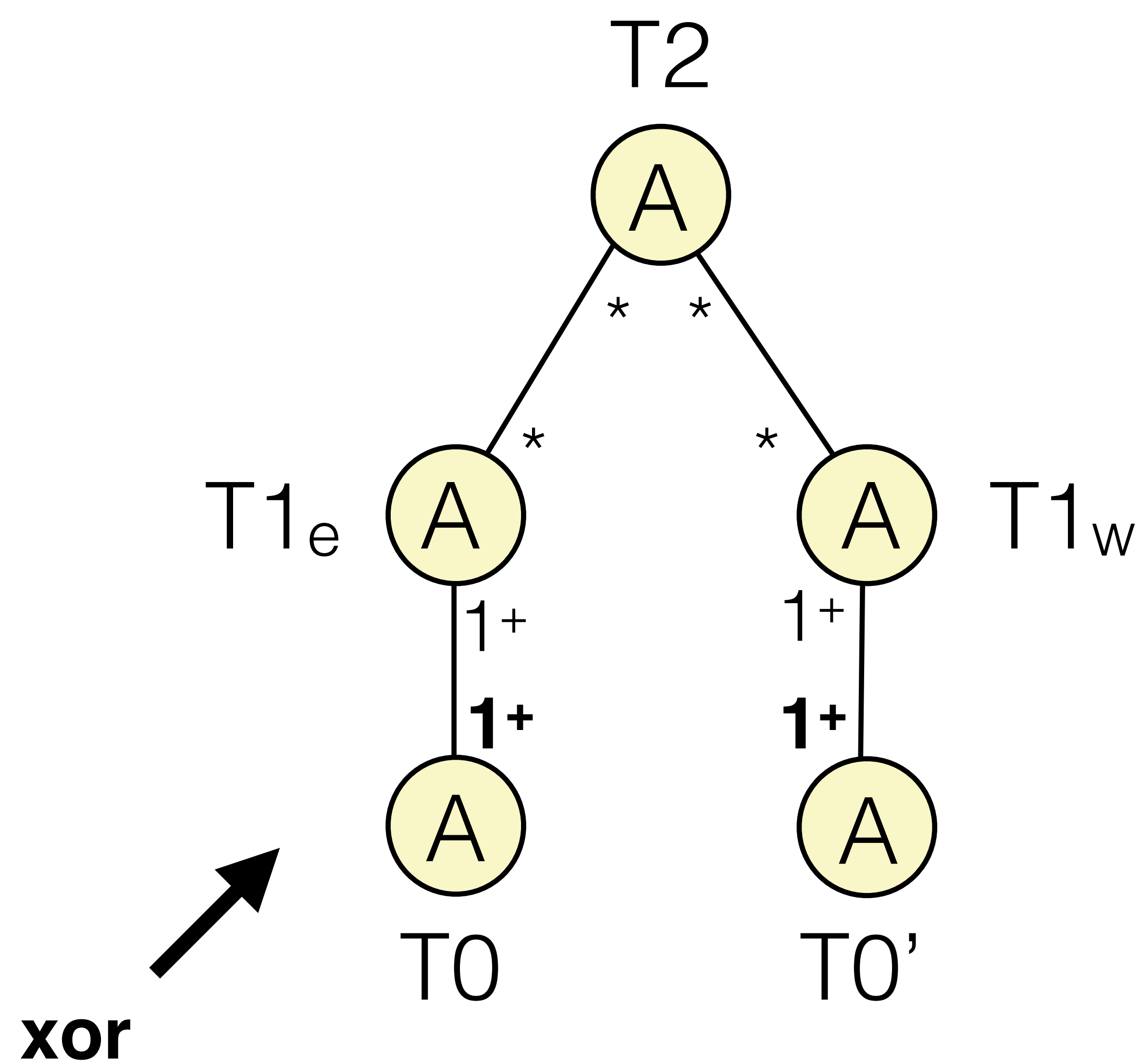
Reachability — Solution?



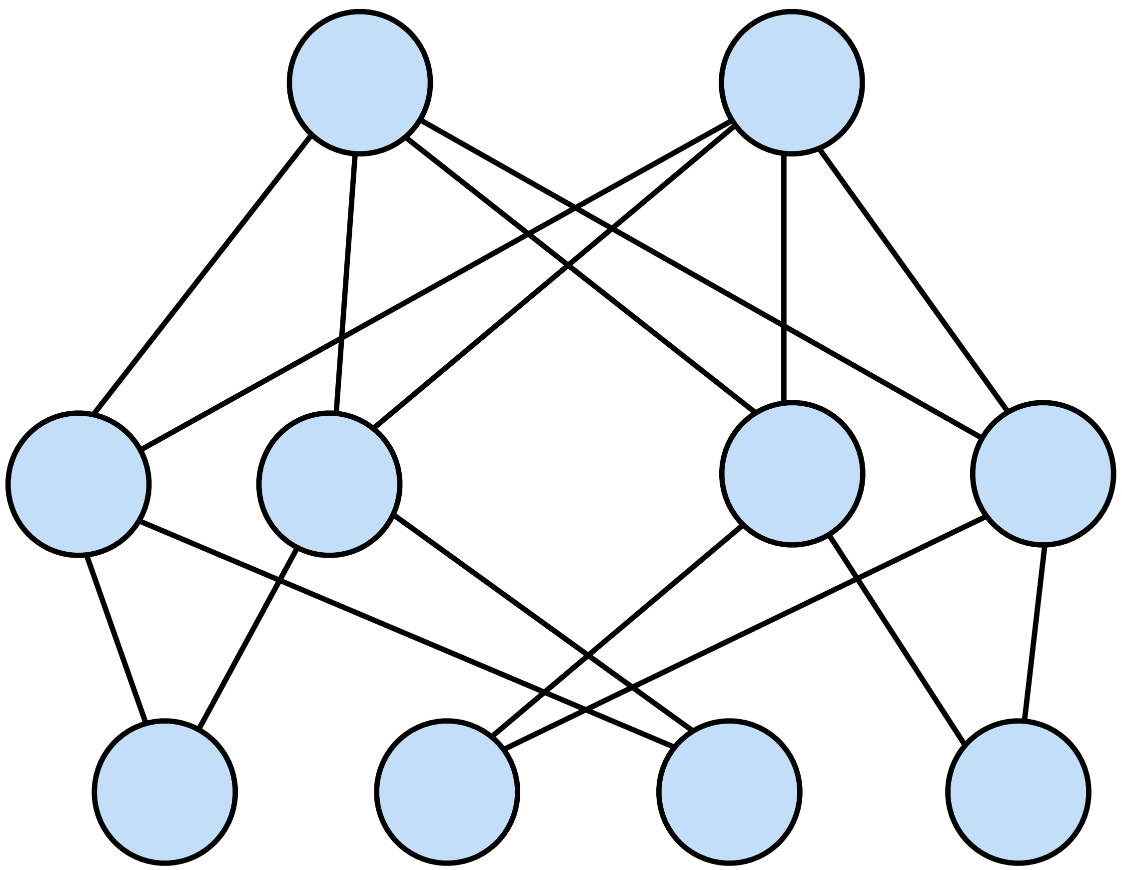


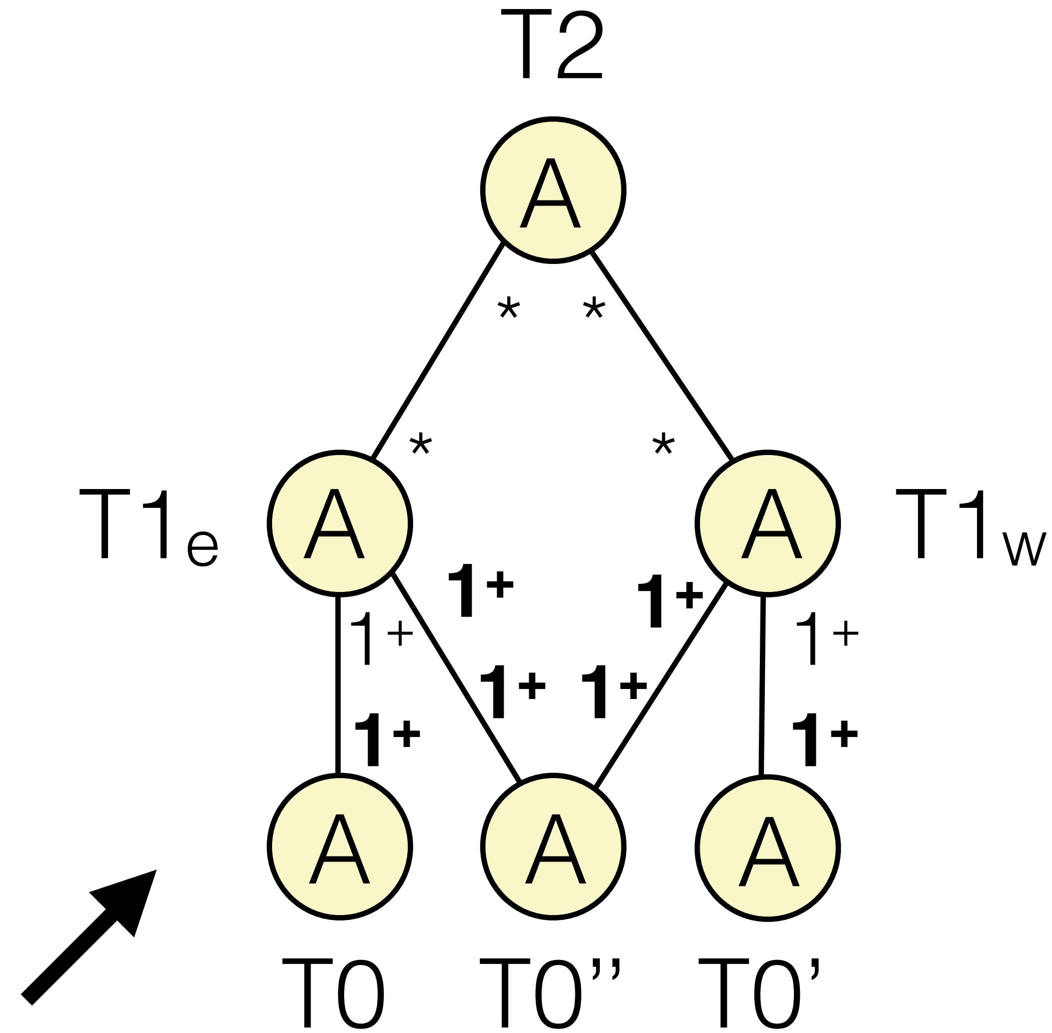
Reachability — Solution?





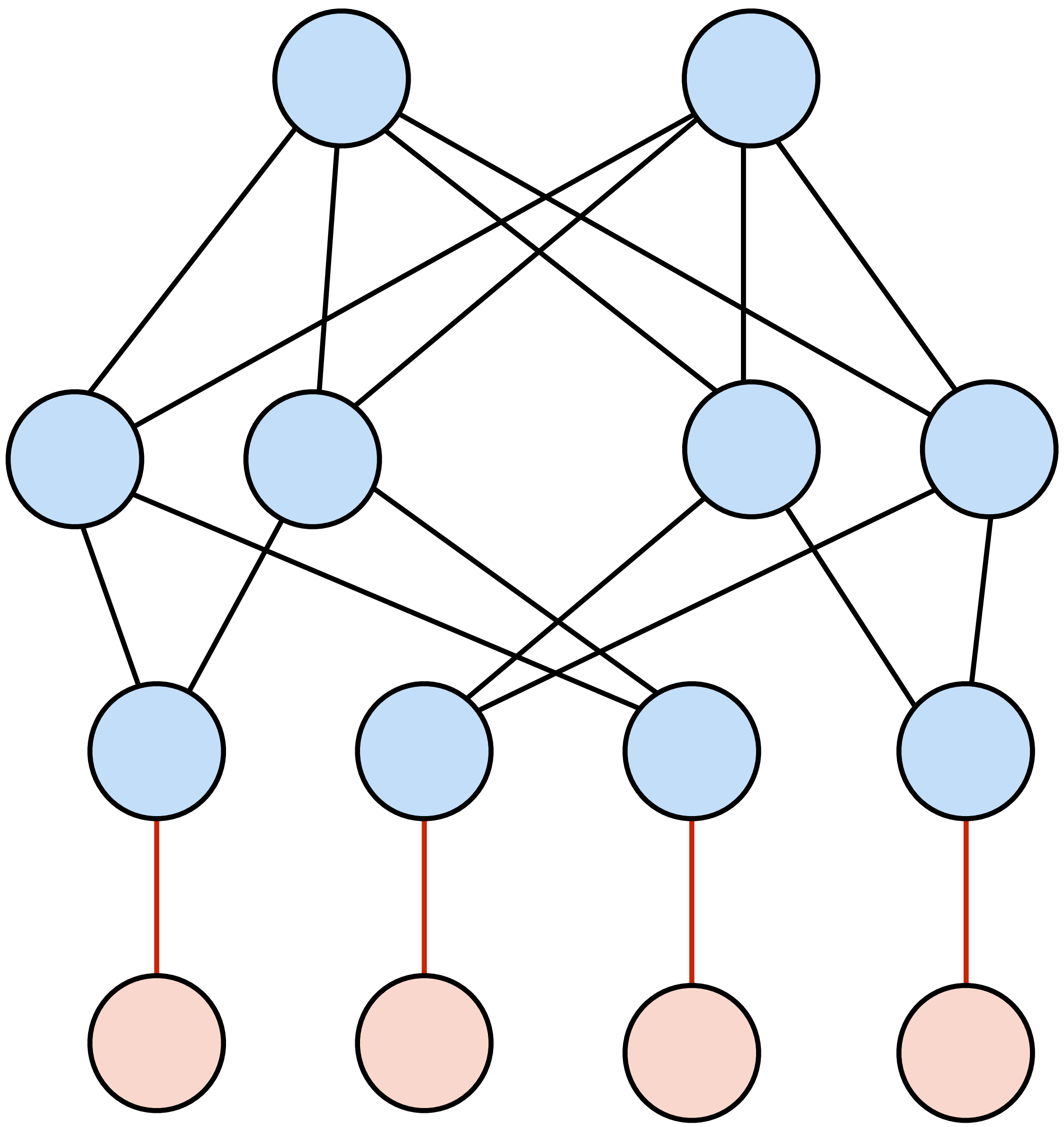
Reachability — Solution?

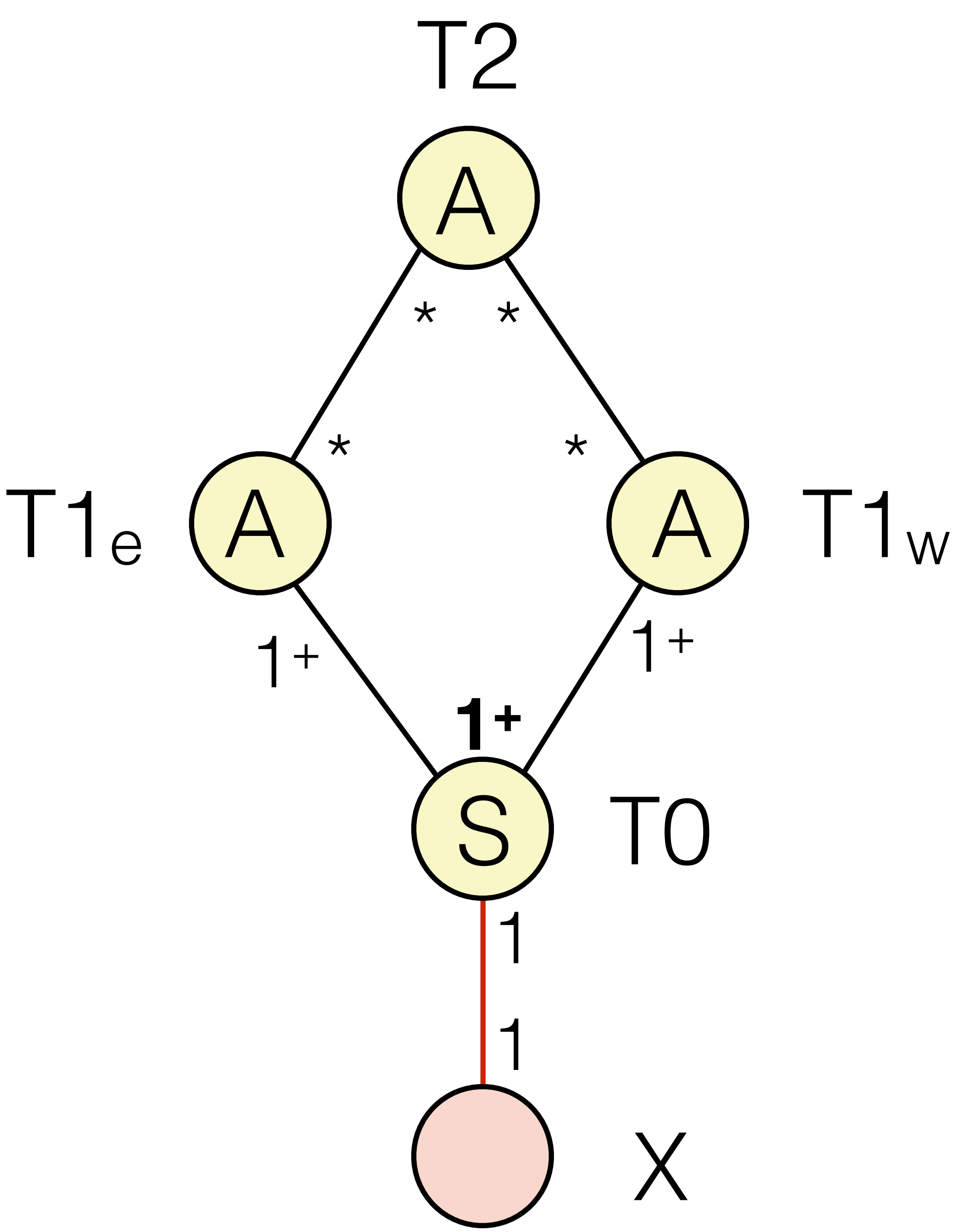




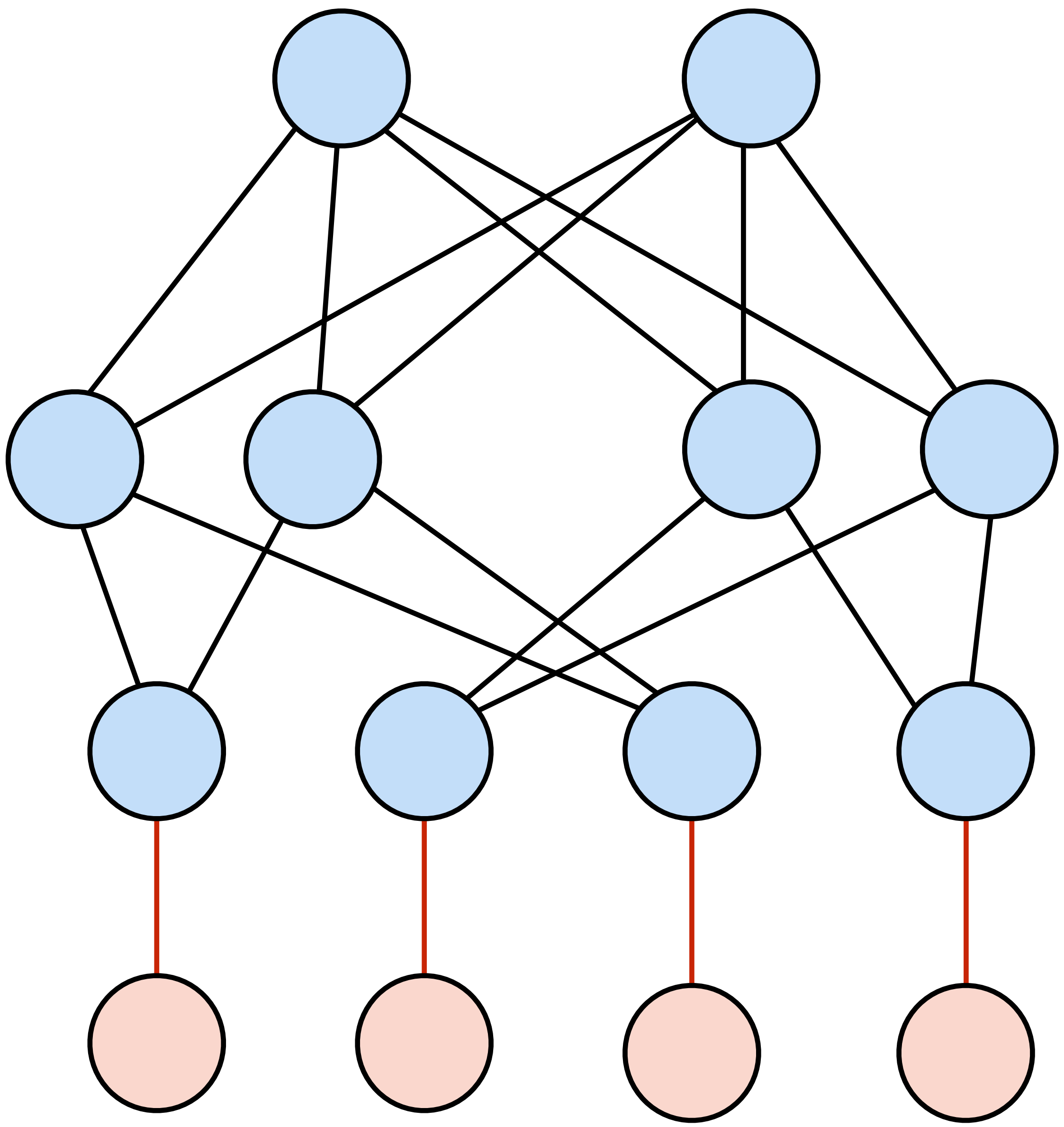
or

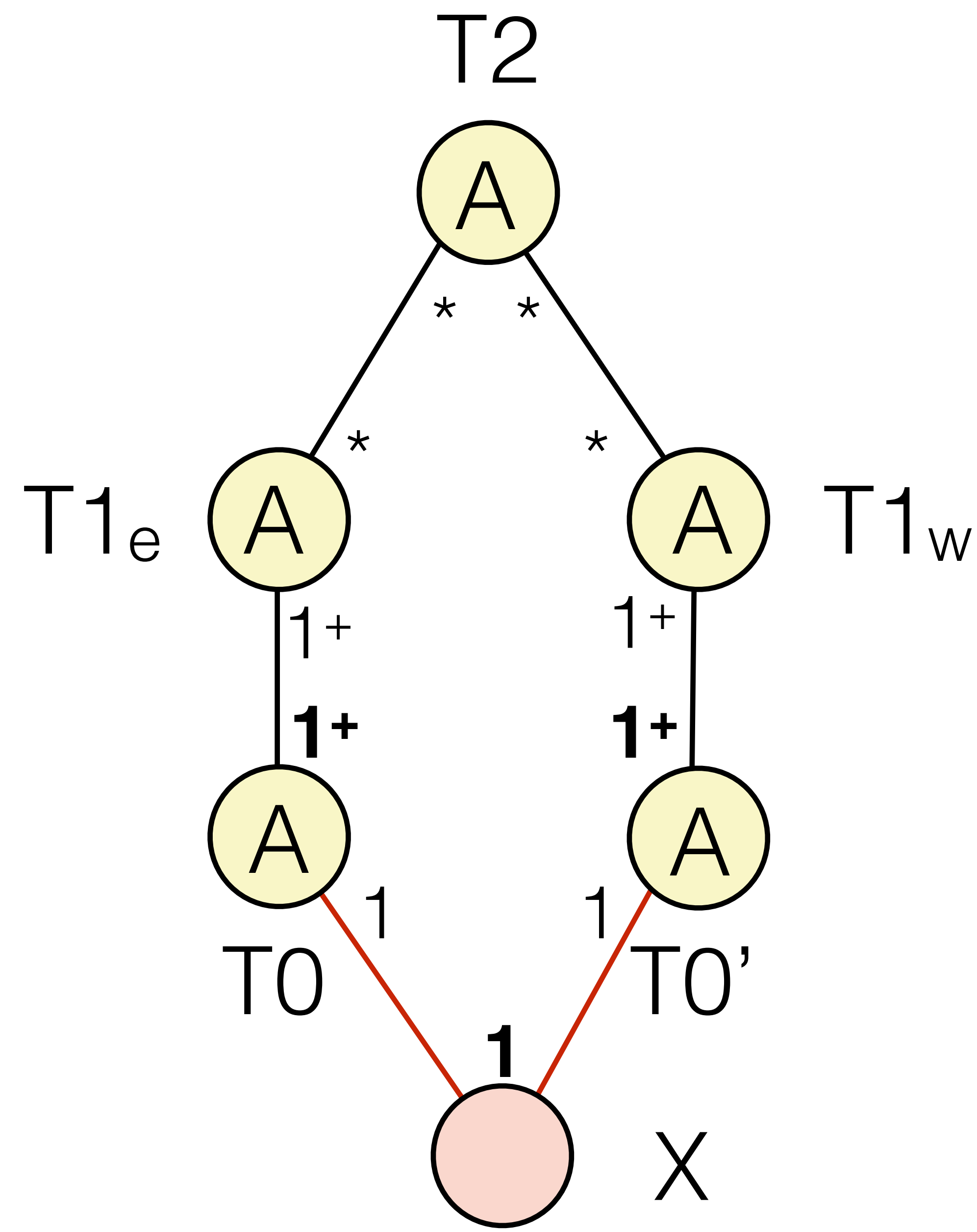
Reachability — Solution?



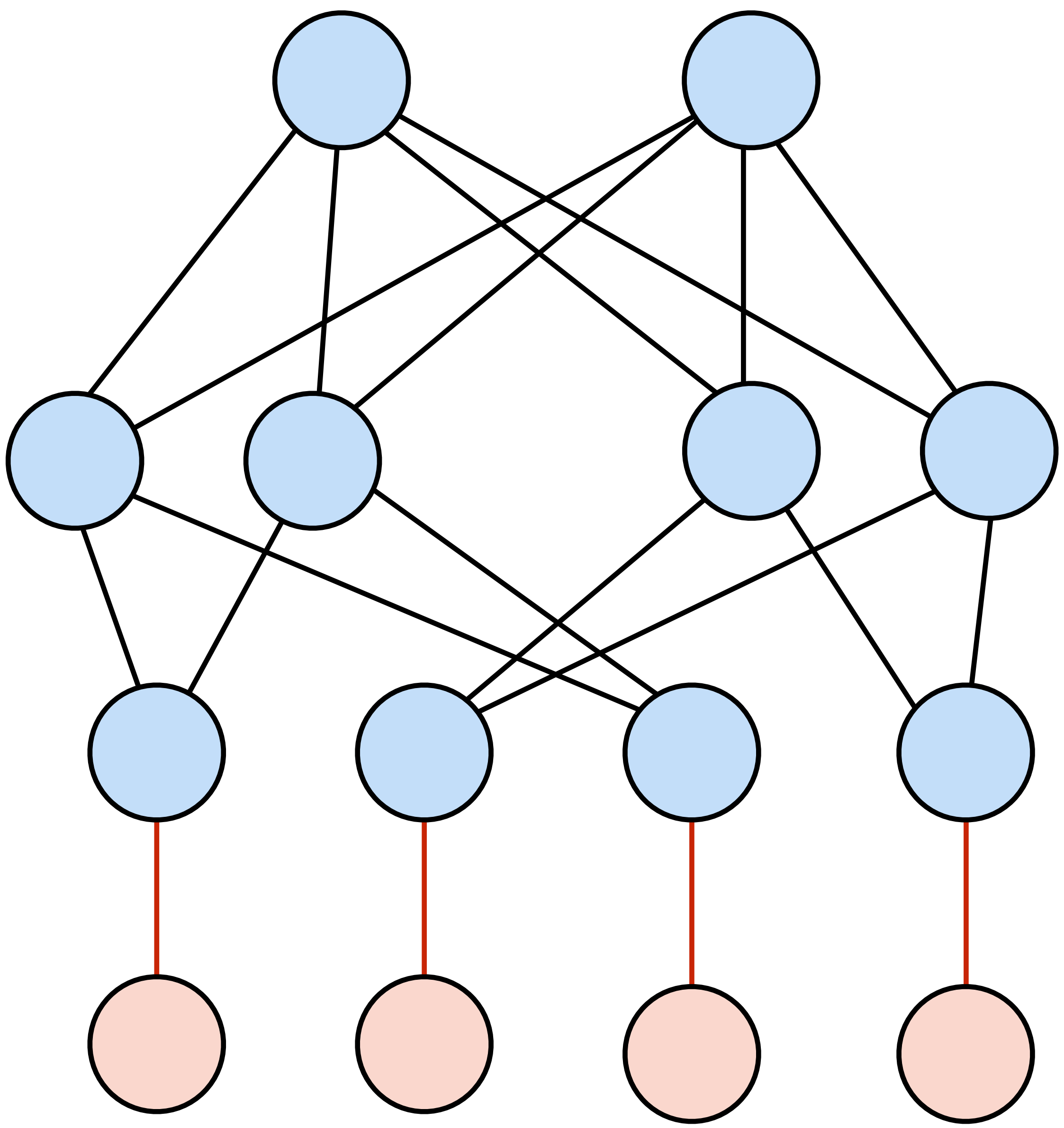


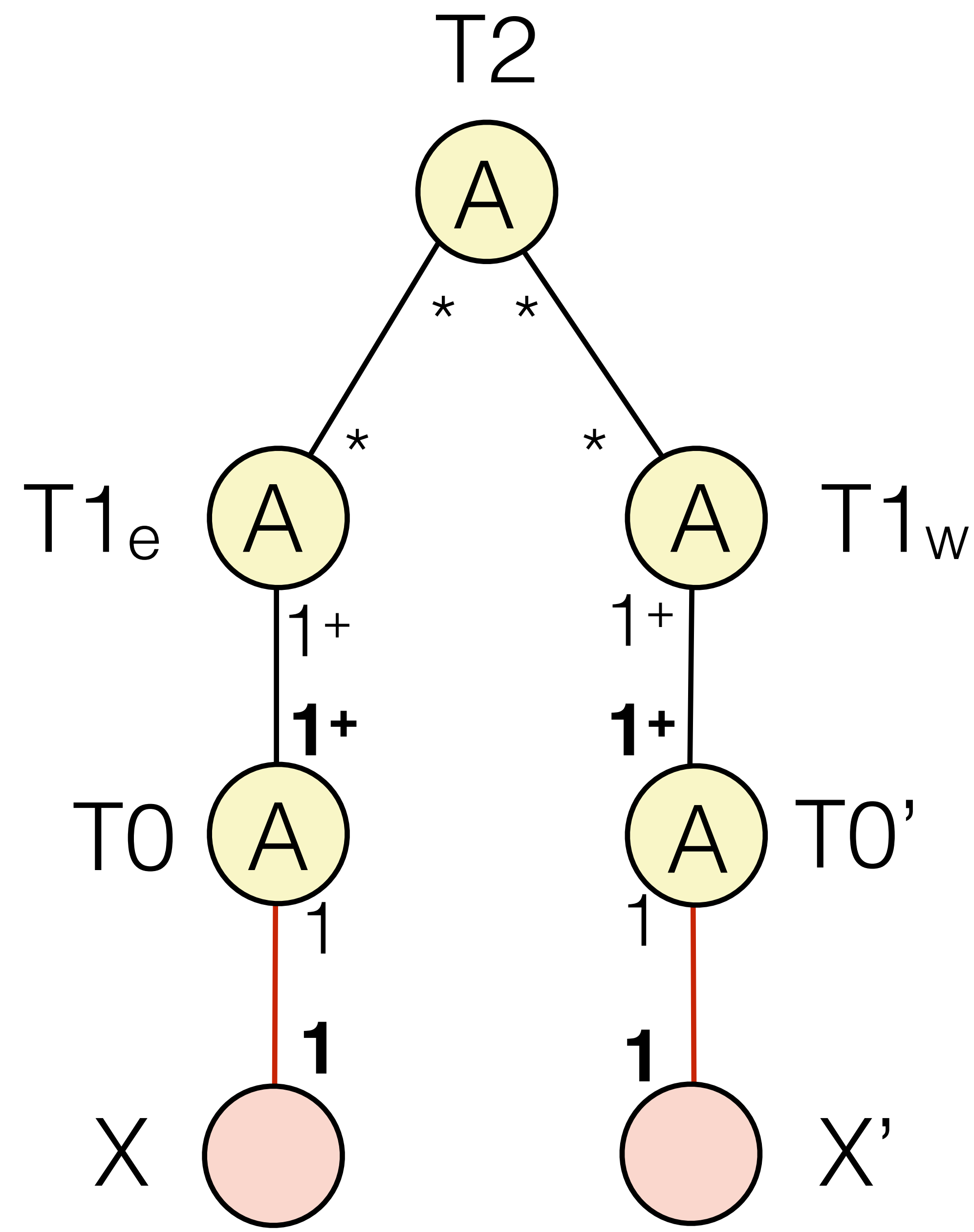
Reachability — Solution?



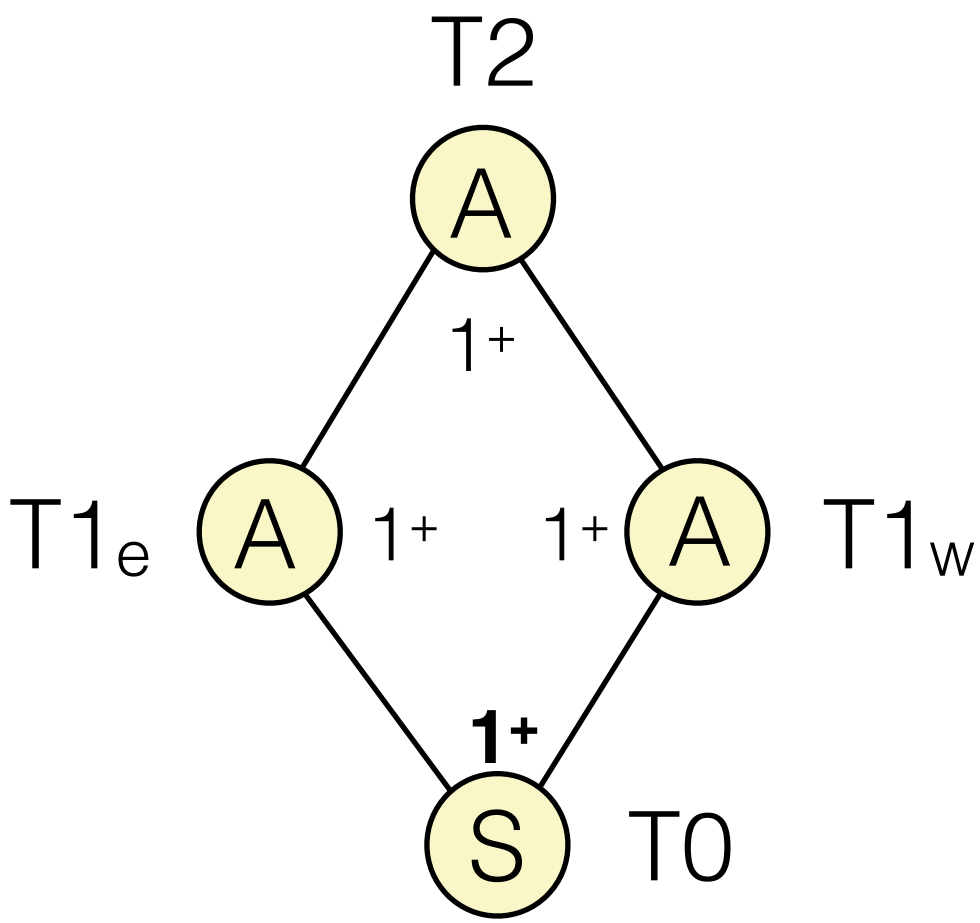


Reachability — Solution?





Reachability — Solution?



Dominators

Fixpoint computation

$$\mathrm{Dom}(n_o) = \{n_o\}$$

$$\mathrm{Dom}(n) = \left(\bigcap_{p \in \mathrm{preds}(n)} \mathrm{Dom}(p) \right) \bigcup \{n\}$$