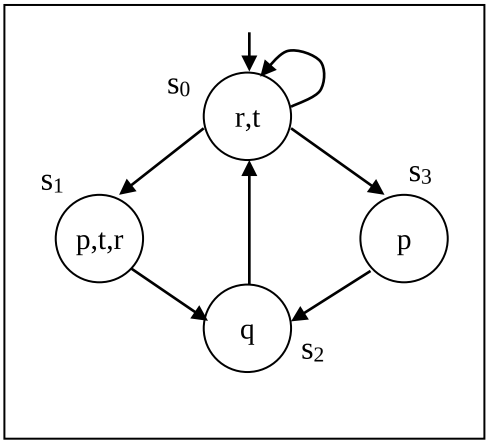
FORMAL METHODS **Module 1**

Exercises

1) Given a transition system $M = (S, S_0, L, R)$ (in the figure),
   a) complete the specification of M by substituting "..." with right symbols from figure;
   b) represent the model in symbolic form, e.g.
      transition $< s_2, s_0>$ in symbolic form $R_{2,0} \equiv \neg p \wedge q \wedge \neg r \wedge \neg t \wedge \neg p' \wedge \neg q' \wedge r' \wedge t'$
   c) draw a computation tree of M up to 4 levels starting from s_0.



$S = \{ s_0, \ \ldots \ , s_3\}$
$S_0 = \{ s_0\}$
L : $l(s_0) = \{r\}$,
$l(s_1) = \{p, t, r\}$
$l(s_2) = \{...\}$
$l(s_3) = \{...\}$
$R = \{..., < s_2, s_0>, ...\}$

2) Check the satisfiability of following CTL formulas for the transition system M defined above

   a) $M, s_0 \models EF(q)$
   b) $M, s_0 \models EG(r)$
   c) $M, s_2 \models AG(r)$
   d) $M, s_2 \models \neg EX(r)$
   e) $M, s_0 \models A((t \vee p)\ U\ q)$
   f) $M, s_0 \models E(r \dashrightarrow (t \wedge \neg q))$

   NB! " -->" denotes temporal "leads to" operator not implication.

3. Given a symbolic state: $\varphi \equiv \neg x_1 \wedge x_2$
   and symbolic transition relation $R \equiv \neg(x_1 \Rightarrow x_2) \wedge \neg x_1' \wedge x_2'$,
   find symbolic pre-image $EX(\varphi) \equiv \exists V' (R \wedge \varphi [V' / V])$ using $\exists$-quantifier elimination.

   Solution:
   1. We substitute variables V in φ with their primed counterparts
      $\varphi [V' / V] \equiv \neg x_1 \wedge x_2 [x'_1/ x_1, x'_2/ x_2] \equiv \neg x'_1 \wedge x'_2$
   2. Rewrite symbolic definition of $EX(\varphi) \equiv \exists V' (R \wedge \varphi [V' / V])$ by substituting $\varphi [V'/V]$
      and R, i.e.

$EX(\varphi) \equiv \exists V' (R \wedge \varphi[V' / V]) \equiv \exists x'_1, x'_2 (\neg(x_1 \Rightarrow x_2) \wedge \neg x_1' \wedge x_2' \wedge \neg x'_1 \wedge x'_2$

3. Simplification:
   a. the formula of previous step has sub-formula $\neg x'_1 \wedge x'_2$ twice. We remove duplication and get
   b. substitute implication using equivalence ($a \Rightarrow b \equiv \neg a \vee b$)
      $\equiv \exists x'_1, x'_2 (\neg(\neg x_1 \vee x_2) \wedge \neg x'_1 \wedge x'_2$ (by De'Morgan's law)
      $\equiv \exists x'_1, x'_2 (\neg\neg x_1 \wedge \neg x_2) \wedge \neg x'_1 \wedge x'_2$ (by $\neg\neg$ law)
      $\equiv \exists x'_1, x'_2 (x_1 \wedge \neg x_2) \wedge \neg x'_1 \wedge x'_2$

4. $\exists$ elimination (starting from innermost bound variable x'_2)

$\equiv \exists x'_1 (((x_1 \wedge \neg x_2) \wedge \neg x'_1 \wedge x'_2)[false/x'_2] \vee (x_1 \wedge \neg x_2) \wedge \neg x'_1 \wedge x'_2)[true/x'_2])$

$\equiv \exists x'_1 (((x_1 \wedge \neg x_2) \wedge \neg x'_1 \wedge false) \vee (x_1 \wedge \neg x_2) \wedge \neg x'_1 \wedge true)$

$\equiv \exists x'_1 (x_1 \wedge \neg x_2 \wedge \neg x'_1)$

Then eliminate $\exists x'_1$:

$\equiv (x_1 \wedge \neg x_2 \wedge \neg x'_1)[false/x'_1] \vee (x_1 \wedge \neg x_2 \wedge \neg x'_1)[true/x'_1]$

$\equiv (x_1 \wedge \neg x_2 \wedge \neg false) \vee (x_1 \wedge \neg x_2 \wedge \neg true)$

$\equiv (x_1 \wedge \neg x_2 \wedge true) \vee (x_1 \wedge \neg x_2 \wedge false)$

$\equiv (x_1 \wedge \neg x_2) \vee false$

$\equiv x_1 \wedge \neg x_2$

Answer: $EX(\varphi) \equiv x_1 \wedge \neg x_2$