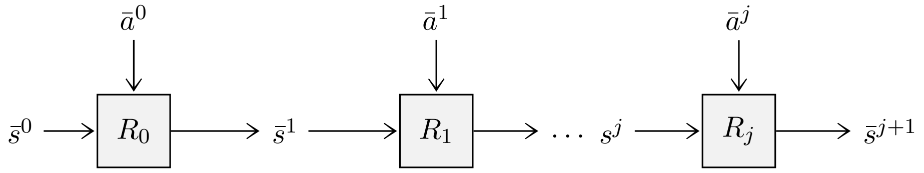
Exercises 2

Exercise 1 (Traces)**.** Recall formulas T_j defined in the lecture that are true if and only if there exist a trace of length j starting from initial state that satisfies error formula E, where $FV(E) \subseteq \{s_1, \ldots, s_n\}$.

$\bar{s}^i$ denotes state variables in step i.

$\bar{a}^i$ denotes inputs in step i.



$$T_j \quad \equiv \quad Init[\bar{s} := \bar{s}^0] \ \wedge \ \left(\bigwedge_{i=0}^{j-1} R_i \right) \ \wedge \ E[\bar{s} := \bar{s}^j]$$

where R_i is our transition formula, with variables renamed:

$$R_i \ \equiv \ R[(\bar{s}, \bar{a}, \bar{x}, \bar{s}') := (\bar{s}^i, \bar{a}^i, \bar{x}^i, \bar{s}^{i+1})]$$

1. In this system (which has n Boolean variables), give a simple upper bound on the longest trace from the initial state that does not contain any repeated states.

   Let the set of error states be $S_E = \{\bar{v} \mid [\bar{s} \to \bar{v}] \models E\}$.

2. Use T_j and similar formulas to find quantified Boolean formulas F (QBF, with quantification only over propositional variables) whose free variables are $s_1, \ldots, s_n$ and such that the set

   $$\{\bar{v} \mid [\bar{v} \mapsto \bar{s}] \models F\}$$

   is one of the following (write the form of the formula for each of the sets):

   - states that can be reached in exactly k steps, $(\bar{r}^k)[Init]$
   - states that can be reached in at most k steps, $(\bigcup_{i=0}^{k} \bar{r}^i)[\textsf{Init}]$
   - all reachable states $(\bigcup_{i=0}^{\infty} \bar{r}^i)[\textsf{Init}]$

- states that can reach error state in k steps, $(\bar{r}^{-1})^k[S_E]$
- states that can reach error state in at most k steps, $(\bigcup_{i=0}^{k}(\bar{r}^{-1})^i)[S_E]$
- all stuck states in the system, $\{\bar{v} \mid \neg\exists\bar{v}'.(\bar{v},\bar{v}') \in \bar{r}\}$

3. Write QBF formulas without free variables that express the following:
   - no error state is reachable from the initial state
   - no stuck state is reachable from the initial state
   - every state in the system is reachable in k or fewer steps
   - there exists an infinite trace of the system (for some behavior of the environment given by the values of $\bar{a}$ in every step).

Exercise 2 (Tseytin Transformation)**.** The Tseytin transformation of a propositional formula ϕ is a formula in Conjunctive Normal Form (CNF) produced the following way: Recursively for each subformula ϕ_k of ϕ looking like $x_i \circ x_j$, create a new variable y_k and a new assignement $y_k \leftrightarrow x_i \circ x_j$ (for $\circ \in \{\vee, \wedge, \rightarrow\}$ and similarly for negation). Replace ϕ_k by y_k in ϕ and continue until ϕ is reduced to a single variable. Take the conjunction of that variable with all created assignements. For example,

$$\neg(a \wedge b) \rightarrow c$$

becomes

$$(y_1 \leftrightarrow (a \wedge b)) \wedge (y_2 \leftrightarrow \neg y_1) \wedge (y_3 \leftrightarrow y_2 \rightarrow c) \wedge y_3$$

Any expression of the type $y_k \leftrightarrow x_i \circ x_j$ can then also be equivalently expressed in CNF.

A formula can always be transformed into an equivalent one in conjunctive normal form without adding new variables, but doing so may require exponential increase in size. The Tseytin transform is guaranteed to increase the size of any formula by only a constant factor.

1. Compute the Tseytin transformation of $\neg(((a \vee \neg b) \wedge \neg(b \rightarrow c)) \rightarrow a)$.
2. Prove that on all inputs, a formula and its Tseytin transform are always equisatisfiable (one is satisfiable if and only if the other is), but not necessarily equivalent.
3. Prove that if Tseytin's transform of $\neg F$ is unsatisfiable, then F is a valid formula.
4. given n the size of an original formula, give the assymptotic size of its Tseytin transformation, in "Big O" notation.

Exercise 3 (SAT solving)**.** Prove the validity of the formula

$$((a \lor \neg b) \land \neg(b \to c)) \to a$$

by first using the Tseytin's transformation you have computed in the first question of Exercise 2, and then following by a resolution proof on clauses to obtain an empty clause.

Exercise 4 (First-order structures)**.** Consider a first-order language (signature) $\mathcal{L} = \{L, B, T\}$ with one relation symbol, L, of arity two, and constants, B, T. Consider the following formulas in the language $\mathcal{L}$:

$$\begin{array}{rl} \mathsf{Min}: & \forall x. L(B, x) \\ \mathsf{Max}: & \forall x. L(x, T) \\ \mathsf{Tot}: & \forall x. \forall y. (L(x, y) \lor L(y, x)) \\ \mathsf{Tra}: & \forall x. \forall y. \forall z.\ ((L(x, y) \land L(y, z)) \to L(x, z)) \end{array}$$

Let $S = \{\mathsf{Min}, \mathsf{Max}, \mathsf{Tot}, \mathsf{Tra}\}$.

1. Let $D = \{b, u, t\}$ be a set of three elements. List all possible FOL structures (D, α) of language $\mathcal{L}$ in which the set of formulas S is true and where $\alpha(B) = b$ and $\alpha(T) = t$. For each structure, show the two-dimensional table of the form:

L	b	u	t
b			
u			
t			

   filled with 0 and 1 where 1 indicates the relation holds and 0 that it does not hold. Explain why these are the only structures with the required property. For each structure, indicate whether L satisfies the axioms of a partial order (reflexivity, symmetry, transitivity).

2. Now consider an extended language $\mathcal{L}' = \mathcal{L} \cup \{E\}$ where E is a binary relation symbol. We will define a new structure α' that also defines E. In each of the structures identified in Q1, give a table for E such additionally the following formula is true:

$$\mathsf{Both}: \ \forall x. \forall y. \, (E(x, y) \leftrightarrow (L(x, y) \land L(y, x)))$$

   In each case, check whether the relation given by $\alpha'(E)$ is an equivalence relation (i.e., it is reflexive, symmetric, and transitive). Let $S' = S \cup \{\mathsf{Both}\}$.

3. Does there exist a structure α' (with arbitrary domain) that makes S' true such that the relation $\alpha'(E)$ is *not* an equivalence relation?

4. (Intentionally open ended) Can you use structure α' with any domain D that satisfies S' to define a new structure α_1 that also satisfies S', that has a possibly different domain D_1 but with size no larger than D, and where $\alpha_1(L)$ is a partial order relation?