Symbolic model checking

Why?
Saves us from constructing a model's state space explicitly. Effective "cure" for state space explosion problem.

How?
Sets of states and the transition relation are represented by formulas. Set operations are defined in terms of formula manipulations.

Data structures
ROBDDs - allow for efficient storage and manipulation of logic formulas.

Representing Models Symbolically

- A system state represents an interpretation (truth assignment) for a set of propositional variables $V$.
- Formulas represent sets of states that satisfy it
  - False - $\emptyset$, True - $S$
  - $a$ - set of states in which $a$ is true - ($\{s_0, s_1\}$)
  - $b$ - set of states in which $b$ is true - ($\{s_1, s_2\}$)
  - $a \lor b = \{s_0, s_1\} \cup \{s_1, s_2\} = \{s_0, s_1, s_2\}$
- State transitions are described by relations over two sets of variables, $V$ (source state) and $V'$ (destination state)
  - Trans. from $s_2$ to $s_3$ is described by $(\neg a \land b \land \neg a' \land \neg b')$.
  - Trans. from $s_0$ to $s_1$ and $s_2$, and from $s_1$ to $s_2$ and to itself is described by $(a \land b')$.
  - Relation $R$ is described by $(a \land b') \lor (\neg a \land b \land \neg a' \land \neg b')$.
Model Checking using Sets of States

Computing $||\varphi||$

- $\varphi$ is $\top$ : return $S$
- $\varphi$ is $\bot$ : return $\emptyset$
- $\varphi$ is atomic : return $\{s \in S \mid \varphi \in L(s)\}$
- $\varphi$ is $\neg \varphi_1$ : return $S \setminus ||\varphi_1||$
- $\varphi$ is $\varphi_1 \land \varphi_2$ : return $||\varphi_1|| \cap ||\varphi_2||$
- $\varphi$ is $\varphi_1 \lor \varphi_2$ : return $||\varphi_1|| \cup ||\varphi_2||$
- $\varphi$ is $AX \varphi_1$ : return $||\neg EX \neg \varphi||$
- $\varphi$ is $EX \varphi_1$ : return $SAT_{EX}(\varphi_1)$
- $\varphi$ is $EU \varphi_1$ : return $SAT_{EU}(\varphi_1)$
- $\varphi$ is $EG \varphi_1$ : return $SAT_{EG}(\varphi_1)$

Model Checking on Sets of States, Cont’d

function $SAT_{EX}(\varphi)$:
return $\{s_0 \in S \mid s_0 \rightarrow s_1 \text{ for some } s_1 \in ||\varphi||\}$

function $SAT_{EG}(\varphi)$
$X := \emptyset; Y := S$;
repeat
$X := Y$
$Y := ||\varphi|| \cap SAT_{EX}(X)$
until $X = Y$
return $Y$
Model Checking on Sets of States, Cont’d

function $\text{SAT}_{EU}(\varphi, \psi)$
/* compute set of states satisfying $E[\varphi U \psi]$ */
$X := \emptyset$; $Y := \emptyset$
repeat
    $X := Y$
    $Y := ||\psi|| \cup (||\varphi|| \cap \text{SAT}_{EX}(X))$
until $X = Y$
return $Y$

Example: $M, s_2 \models E[a U \neg b]$)

1. Model

2. $\neg b$

3. $\neg b \lor (a \land \text{EX}[a U \neg b])$

4. $\neg b \lor (a \land \text{EX}[a U \neg b]) \lor (a \land \text{EX EX}[a U \neg b])$
**Lattice Theory**

Def: A lattice is a partial order \((L, \leq)\) for which a unique greatest lower bound and a unique least upper bound exist for each pair of elements. These are known as **join** \((a \sqcup b)\) and **meet** \((a \sqcap b)\).

Examples:

(a) \((\text{Bool, } \Rightarrow)\); (b) \((\text{Nat, } \leq)\); (c) A non-lattice; (d) \((2^{\{a,b,c\}}, \subseteq)\)

\(\top\) (top) = \(\sqcup L\)

\(\bot\) (bottom) = \(\sqcap L\)

---

**Properties of Lattices**

**monotonicity**

\[ a \leq a' \land b \leq b' \Rightarrow a \sqcap b \leq a' \sqcap b' \]

\[ a \leq a' \land b \leq b' \Rightarrow a \sqcup b \leq a' \sqcup b' \]

**idempotence**

\[ a \sqcup a = a \]

\[ a \sqcap a = a \]

**commutativity**

\[ a \sqcup b = b \sqcup a \]

\[ a \sqcap b = b \sqcap a \]

**associativity**

\[ a \sqcup (b \sqcup c) = (a \sqcup b) \sqcup c \]

\[ a \sqcap (b \sqcap c) = (a \sqcap b) \sqcap c \]

**absorption**

\[ a \sqcup (a \sqcap b) = a \]

\[ a \sqcap (a \sqcup b) = a \]

In general, a function \(F : L \rightarrow L\) is monotone if

\[ \forall x, y \in L : x \leq y \Rightarrow F(x) \leq F(y). \]
Monotone Functions and Fixpoints

$S$ — set of states, $F : P(S) \rightarrow P(S)$ — function on the powerset of $S$.

1. $F$ is monotone if $\forall X, Y \subseteq S \cdot X \subseteq Y$ implies $F(X) \subseteq F(Y)$
2. $X \subseteq S$ is a fixpoint of $F$ if $X = F(X)$

Examples:
1. $S = \{s_0, s_1\}$, $F(Y) = Y \cup \{s_0\}$
   Is $F$ monotone?

   What are fixpoints of $F$?

2. $G(Y) = \begin{cases} \{s_1\} & \text{if } Y = s_0 \\ \{s_0\} & \text{else} \end{cases}$
   Is $G$ monotone?

   What are fixpoints of $G$?

Fixpoints (Cont’d)

Greatest fixpoint:

$Y = F(Y) \land \forall X \cdot X = F(X) \Rightarrow X \subseteq Y$

Computing greatest fixpoint:

$\top \supseteq F(\top) \supseteq F(F(\top)) \supseteq \ldots \supseteq F^i(\top) = F^{i+1}(\top)$

Least fixpoint:

$Y = F(Y) \land \forall X = F(X) \Rightarrow Y \subseteq X$

Computing least fixpoint:

$\bot \subseteq F(\bot) \subseteq F(F(\bot)) \subseteq \ldots \subseteq F^i(\bot) = F^{i+1}(\bot)$

$F^i(X)$ means "$F$ applied $i$ times".
Fixpoints (Cont’d)

Can a monotone function have several fixpoints?
If \( F \) is a monotone function, is \( \text{lfp}(F) = \text{gfp}(F) \)? (or \( \mu X. F(X) = \nu X. F(X) \))

Fixpoints (Cont’d)

Exercises:
Let \( H_1, H_2, H_3 : P(\{1, \ldots, 10\}) \rightarrow P(\{1, \ldots, 10\}) \). Let \( \forall Y \subseteq \{1, \ldots, 10\} \).
Which of the functions are monotone:
- \( H_1(Y) = Y - \{1, 4, 7\} \)
- \( H_2(Y) = \{2, 5, 9\} - Y \)
- \( H_3(Y) = \{1, 2, 3, 4, 5\} \cap (\{2, 4, 8\} \cup Y) \)
What are greatest and least fixpoints of \( H_3 \)?

Theorem (Knaster-Tarski)

Let \( (L, \leq) \) be a lattice, \( F : L \rightarrow L \) be a monotone function. Then,
\[ \mu X. F(X) = F^{n+1}(\bot) \quad \text{and} \quad \nu X. F(X) = F^{n+1}(\top), \]
where \( n = \text{height}(L) \).

Proof:
1. \( \bot \subseteq F^1(\bot) \subseteq F^2(\bot) \subseteq \ldots \subseteq F^i(\bot) \forall i \geq 1 \).
   \( F^1(\bot) \) needs to contain at least one element. \( F^2 \) at least two. Thus, \( F^{n+1} \)
   should contain \( n + 2 \) elements. This cannot happen since \( L \) has only \( n + 1 \)
   unique elements.
2. Suppose \( X \) is another fixpoint. We should show that \( F^{n+1}(\bot) \subseteq X \).
   The proof goes by induction:
   (a). \( \bot \subseteq X \)
   (b). \( F(\bot) \subseteq F(X) = X \) since \( F \) is monotone.
   Thus, \( F^i(\bot) \subseteq X \forall i \geq 0 \), including the \( i \) which is \( n + 1 \).
Symbolic Calculation of $EXb$ for System on Slide 97

Symbolic representation of the transition relation is:

$$R = (a \land b') \lor (\neg a \land b \land \neg a' \land \neg b')$$

Symbolic computation using pre-image on Slide 107.

$$\begin{align*}
||EXb|| & = pre(b, R) \\
& = \exists a', b' \cdot R \land b' \\
& = \exists a', b' \cdot ((a \land b') \lor (\neg a \land b \land \neg a' \land \neg b')) \land b' \\
& = \exists a', b' \cdot ((a \land b') \lor ((\neg a \land b \land \neg a' \land \neg b')) \land b') \\
& = \exists a', b' \cdot (a \land b') \lor f \\
& = \exists a', b' \cdot (a \land b') \\
& = \exists b' \cdot (a \land b') \\
& = (a \land t) \lor (a \land f) \\
& = a
\end{align*}$$

That is, $||EXb||$ is true in a state $s$ iff $s \models a$. 

Theorem: $pre$ and $img$ (post) are monotone.
Proof

1. Monotonicity. Take $X, Y \subseteq S$, $X \subseteq Y$.
   We need to show $G(X) \subseteq G(Y)$
   
   $$G(X) = ||\psi|| \cup (||\phi|| \cap ||EXX||)$$
   $$\subseteq ||\psi|| \cup (||\phi|| \cap ||EXY||)$$
   $$= G(Y)$$

2. Show that
   $$\forall X \subseteq S \cdot G(X) = X \Rightarrow X \supseteq ||E[\phi U \psi]|$$
   Proof is by induction on the length of prefix of the path along which $\phi U \psi$ is satisfied: there is a path $s_0, s_1, \ldots$ and $j \geq 0$ s.t. $s_j \models \psi \land \forall l < i, s_l \models \phi$.
   If this length is 0, then it can be computed by $G^1(\emptyset) = ||\psi||$
   Inductive hypothesis: $G^{i+1}$ computes $E[\phi U \psi]$ for length up to $i$.
   Inductive case: Consider the path $s_0, s_1, \ldots$. For state $s_1$, inductive hypothesis holds. Since $(s_0, s_1) \in R, s_0 \models \phi$ and $s_0 \models EX(G^{i+1}(\emptyset))$, thus, $s_0 \in G^{i+2}$. 

Correctness Arguments: SAT$_{EU}$

Intuition: least fixpoint - finite number of iterations

$$E[\phi U \psi] = \psi \lor (\phi \land EXE[\phi U \psi])$$ or

$$||E[\phi U \psi]|| = ||\psi|| \cup (||\phi|| \cap ||EXE[\phi U \psi]||)$$

So, $||E[\phi U \psi]||$ is a fixpoint of

$$G(X) = ||\psi|| \cup (||\phi|| \cap ||EXX||)$$

Theorem: For $G$ as defined above and $n = |S|,$

1. $G$ is monotone
2. $||E[\phi U \psi]|| = \mu X \cdot G(X)$
Symbolic Model-Checking Algorithm on BDDs

**Procedure** $MC(p)$

**Case**

- $p \in A$ : return $Build("p")$
- $p = \neg \phi$ : return $Apply("\neg", MC(\phi))$
- $p = \phi \land \psi$ : return $Apply("\land", MC(\phi), MC(\psi))$
- $p = \phi \lor \psi$ : return $Apply("\lor", MC(\phi), MC(\psi))$
- $p = EX \phi$ : return $existQuantify(V',$
  
  $Apply("\land", R, Prime(MC(\phi)))$)
- $p = AX \phi$ : return $Apply("\neg", MC(EX \neg \phi))$
- $p = E[\phi U \psi]$ : $Q_0 = Build(\bot)$
  
  $Q_{i+1} = Apply("\lor", Q_i, Apply("\lor", MC(\psi),$
  
  $Apply("\land", MC(\phi), MC(EX Q_i))))$
  
  return $Q_n$ when $Q_n = Q_{n+1}$
- $p = EG \phi$ : $Q_0 = Build(\top)$
  
  $Q_{i+1} = Apply("\land", MC(\phi), MC(EX Q_i)))$
  
  return $Q_n$ when $Q_n = Q_{n+1}$

**Correctness Arguments: SAT$_{EG}$**

Intuition: greatest fixpoint: infinite number of iterations

$EG \phi = \phi \land EX EG \phi$ or $||EG \phi|| = ||\psi|| \cap \{s \mid \exists s' s \rightarrow s' \land s' \in ||EG \phi||\}$

So, $||EG \phi||$ is a fixpoint of $F(X) = ||\phi|| \cap ||EX X||$

Theorem: Let $F$ be defined above and $n = |S|$.

1. $F$ is monotone
2. $||EG \phi|| = vX.F(X)$

Proof:

1. Monotonicity. Obvious because of monotonicity of EX.
2. Show that

   $\forall X \subseteq S \cdot F(X) = X \Rightarrow X \subseteq ||EG \phi||$

So, take an element $s \in X$ and show that it is in $||EG \phi||$.

Take $s_0 \in X$. $F(X) = ||\phi|| \cap EX X$, so clearly, $||\phi||(s_0)$ holds.

By mathematical induction, construct a path $s_0, s_1, \ldots$ such that $||\phi||(s_i)$ holds.

So, $s_0 \in ||EG \phi||$.

**Symbolic Model-Checking Algorithm on BDDs**

---


Symbolic Fairness

- Let \( C = \{\psi_1, \psi_2, \ldots, \psi_k\} \) be fairness constraints.

- Recall, we only need to know how to compute \( ||E_C G \phi|| \)

- A set \( Z = ||E_C G \phi|| \) if it is the largest set such that
  1. \( Z \subseteq ||\phi|| \)
  2. for all fairness constraints \( \psi_i \), and all states \( s \in Z \), there exists a path of length one or more to a state in \( ||\psi_i|| \), going only through states in \( ||\phi|| \).

- Symbolically
  - \( \nu Z \cdot \phi \land \bigwedge_{i=1}^k EX E[\phi U (Z \land \psi_i)] \)
  - BTW: formula not expressible in CTL
  - Note: \( EU \) recomputed at each iteration of \( EG \)
  - Complexity: square in \(|S|\)
Witnesses and Counterexamples

• Witness for $\|EX\varphi\|(s)$
  – $s_1$ is a witness iff it is in $img(\{s\}, R) \cap \|\varphi'\|

• Witness for $\|E[qU\psi]\|(s_0)$
  – From the algorithm: $s \in Q_i$ iff there exists a path of at most $i$ steps from $s$
    to a state in $\|\psi\|$, going only through states in $\|\varphi\|$.
  – Find the smallest $i$ such that $s_0 \in Q_i$
  – Let $s_1$ be a witness to $\|EX Q_{i-1}\|(s_0)$, $s_2$ a witness to $\|EX Q_{i-2}\|(s_1)$,
    etc.
  – $s_0, s_1, s_2, \ldots$ is the witness for $EU$

Witnesses and Counterexamples (Cont’d)

• Witness for $\|EG\varphi\|(s)$
  – Need to find a looping path from $s$, going through states in $\|\varphi\|$.
  – $\|\varphi \land EXE[\varphi U(\varphi \land \{s\})]\|(s)$ means – there exists a path from $s$ to
    itself going only through states in $\|\varphi\|$.
  – If $\|\varphi \land EXE[\varphi U(\varphi \land \{s\})]\|(s)$ holds, then apply algorithm for $EU$
  – Otherwise,
    * find a witness $s_1$ for $\|\varphi \land EXEG\varphi\|(s)$
    * repeat from $s_1$
  – Why does this terminate?