El trabajo

Symbolic Model Checking withouth BDDs

Autores:

- Armin Biere[1]
- Alessandro Cimatti[2]
- Edmund Clarke[1]
- Yunshan Zhu[1]

[1] Departamento de Computación de la Universidad de Carnegie Mellon

[2] Instituto de Investigación Científica y Tecnológica de Provo, Italia

Contexto

Model checking verifica sistemas reactivos dado sistemas de transición que los representen y una especificación (usualmente en lógicas temporales).

Symbolic model checking usa una representación canónica (en particular, OBDDs) de los sistemas de transición y de las fórmulas a chequear.

Puede manejar hasta el orden de 10^{20} estados; para sistemas más complejos, el cómputo se vuelve intratable.

Motivación

Los OBDDs son muy sensibles al ordenamiento de las variables y en el peor caso su tamaño no es polinomial en la cantidad de variables.

En este trabajo presentan un una técnica basada en SAT para model checking simbólico. La idea es considerar contraejemplos de un cierto tamaño y generar una fórmula proposicional que sea satisfacible si y sólo si existe tal contraejemplo.

La ventaja es que la reducción se puede hacer en tiempo polinomial y no requiere la construcción del autómata completo. El método propuesto es muy rápido , dada la naturaleza depth-first de SAT, y además encuentra contraejemplos de longitud mínima.

Definiciones

Definición 1: Una estructura de Kripke es una tupla $M = (S, I, T, \ell)$ con un conjunto finito de estados S, un conjunto de estados iniciales $I \subseteq S$, una relación de transición $T \subseteq S \times S$, y un etiquetado de estados $\ell : S \to \mathcal{P}(A)$ de proposiciones atómicas A.

Aclaraciones:

- Usamos una codificación binaria de las variables.
- $f_I(s) \iff s \in I$.
- $f_p(s) \iff p \in \ell(s)$.
- $(s, t) \in T \iff s \to t$.
- $\pi = (s_0, s_1, \ldots)$ definimos $\pi_i = s_i$ y $\pi^i = (s_i, s_{i+1}, \ldots)$.

Definiciones...

Definición 2 (Semántica): Dada una estructura de Kripke M, un camino π en M, f una fórmula de LTL. Entonces $\pi \models f$ (f es válido a lo largo de π) se define:

- $\pi \models p \iff p \in \ell(\pi_0)$
- $\pi \models \neg p \iff p \notin \ell(\pi_0)$
- $\pi \models f \wedge g \iff \pi \models f$ y $\pi \models g$
- $\pi \models f \vee g \iff \pi \models f$ o $\pi \models g$
- $\pi \models \mathbf{G}f \iff \forall i, \pi^i \models f$
- $\pi \models \mathbf{F}f \iff \exists i, \pi^i \models f$
- $\pi \models \mathbf{X}f \iff \pi^1 \models f$
- $\pi \models f\ \mathbf{U}\ g \iff \exists i, (\pi^i \models g$ y $\forall j < i, \pi^j \models f)$
- $\pi \models f\ \mathbf{R}\ g \iff \forall i, (\pi^i \models g$ o $\exists j < i, \pi^j \models f)$

Definiciones... (cont.)

Definición 3 (Validez): Una fórmula LTL f es universalmente válida en una estructura de Kripke M $(M \models \mathbf{A}f) \iff \pi \models f$ para todos los caminos π en M con $\pi_0 \in I$. Una fórmula LTL f es existencialmente válida en una estructura de Kripke M $(M \models \mathbf{E}f) \iff \pi \models f$ para algún camino π en M con $\pi_0 \in I$.

Proposición 4: $M \models \mathbf{A}f \iff M \not\models \mathbf{E}\neg f$

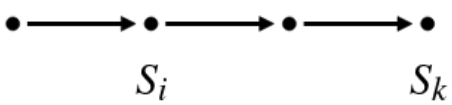
Reducimos la búsqueda de un contraejemplo de $\mathbf{A}f$ a la búsqueda de una traza que satisfaga $\neg f$.

La idea básica del bounded model checking es considerar sólo un prefijo finito de un camino que sea solución al problema de model checking existencial.

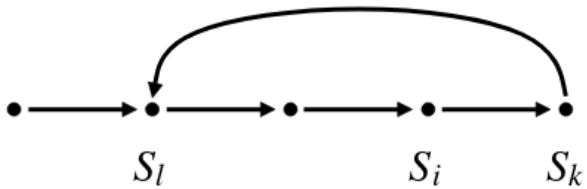
Loops

Que consideremos sólo prefijos finitos no quiere decir que consideremos sólo caminos finitos.

Un prefijo finito puede representar un camino infinito si el prefijo contiene un loop.

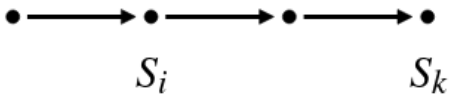


(a) no loop

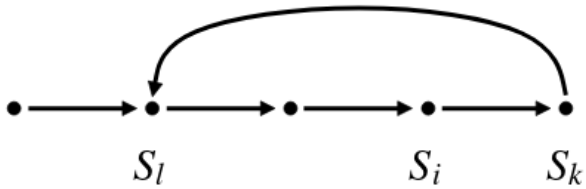


(b) (k,l)-loop

Loops



(a) no loop



(b) (k, l)-loop

Definición 5: Para $l \leqslant k$ llamamos a un camino π un (k, l)-loop si $\pi_k \rightarrow \pi_l$ y $\pi = uv^\omega$ con $u = (\pi_0, ..., \pi_{l-1})$ y $v = (\pi_l, ..., \pi_k)$. Llamamos a π simplemente un k-loop si hay un $l \in \mathbb{N}$ tal que $l \leqslant k$ para el cual π es un (k, l)-loop.

Definición 6 (Semántica acotada para trazas con loop): Sea $k \in \mathbb{N}$, π un k-loop y f una fórmula LTL. $\pi \models_k f \iff \pi \models f$.

Loops

Definición 7 (Semántica acotada para trazas sin loops): Sea $k \in \mathbb{N}$, π una traza que no es un k-loop y f una fórmula LTL.
$\pi \models_k f \iff \pi \models_k^0 f$

- $\pi \models_k^i p \iff p \in \ell(\pi_i)$
- $\pi \models_k^i \neg p \iff p \notin \ell(\pi_i)$
- $\pi \models_k^i f \wedge g \iff \pi \models_k^i f$ y $\pi \models_k^i g$
- $\pi \models_k^i f \vee g \iff \pi \models_k^i f$ o $\pi \models_k^i g$
- $\pi \models_k^i \mathbf{G} f \iff \mathit{False}$
- $\pi \models_k^i \mathbf{F} f \iff \exists i \leqslant \boldsymbol{j} \leqslant k, \pi \models_k^j f$
- $\pi \models_k^i \mathbf{X} f \iff i < k$ y $\pi \models_k^{i+1} f$
- $\pi \models_k^i f \mathbf{U} g \iff \exists i \leqslant \boldsymbol{j} \leqslant k, [\pi \models_k^j g$ y $\forall i \leqslant \boldsymbol{n} < j, \pi \models_k^n f]$
- $\pi \models_k^i f \mathbf{R} g \iff \exists i \leqslant \boldsymbol{j} \leqslant k, [\pi \models_k^j f$ y $\forall i \leqslant \boldsymbol{n} < j, \pi \models_k^n g]$

Todo anda

Lema 8 (Correctitud): Sea f una fórmula LTL, $k \in \mathbb{N}$ y π un camino. $\pi \models_k f \implies \pi \models f$.

Lema 9 (Completitud para existenciales): Sea f una fórmula LTL, M estructura de Kripke. $M \models \mathbf{E}f \implies \exists k \in \mathbb{N} / \ M \models_k \mathbf{E}f$.

Teorema 10 (Correctitud y completitud para existenciales): Sea f una fórmula LTL, M estructura de Kripke.
$M \models \mathbf{E}f \iff \exists k \in \mathbb{N} / \ M \models_k \mathbf{E}f$.

Construyendo la fórmula

Dada una estructura de Kripke M, una fórmula LTL f y una cota $k \in \mathbb{N}$ construiremos la fórmula proposicional $[\![M, f]\!]_k$. Las variables $s_0, ..., s_k$ de $[\![M, f]\!]_k$ representarán la secuencia de estados de un camino π. Cada s_i es un vector de variables de estado.

La fórmula $[\![M, f]\!]_k$ representa esencialmente restricciones sobre $s_0, ..., s_k$ / $[\![M, f]\!]_k$ es satisfacible $\iff M \models_k \mathbf{E}f$.

El tamaño de $[\![M, f]\!]_k$ es polinomial en el tamaño de f, cuadrática en k y lineal en el tamaño de las fórmulas proposicionales para T, I y $p \in A$.

Construyendo la fórmula (cont.)

Definición 11 (Desarrollando la condición de transición):
Dada una estructura de Kripke M y una cota $k \in \mathbb{N}$:

$$[\![M]\!]_k := I(s_0) \wedge \bigwedge_{i=0}^{k-1} T(s_i, s_{i+1})$$

Traduciendo las fórmulas LTL cuando no hay loop

Definición 12 (Traduciendo una fórmula LTL sin un loop):
Dada una fórmula LTL f y $k, i \in \mathbb{N} / \ i \leqslant k$.

- $[\![p]\!]_k^i := p(s_i)$
- $[\![\neg p]\!]_k^i := \neg p(s_i)$
- $[\![f \wedge g]\!]_k^i := [\![f]\!]_k^i \wedge [\![g]\!]_k^i$
- $[\![f \vee g]\!]_k^i := [\![f]\!]_k^i \vee [\![g]\!]_k^i$
- $[\![\mathbf{G} f]\!]_k^i := \mathit{False}$
- $[\![\mathbf{F} f]\!]_k^i := \bigvee_{j=i}^{k} [\![f]\!]_k^j$
- $[\![\mathbf{X} f]\!]_k^i :=$ if $i < k$ then $[\![f]\!]_k^{i+1}$ else False
- $[\![f \ \mathbf{U} \ g]\!]_k^i := \bigvee_{j=i}^{k} \left([\![g]\!]_k^j \wedge \bigwedge_{n=i}^{j-1} [\![f]\!]_k^n \right)$
- $[\![f \ \mathbf{R} \ g]\!]_k^i := \bigvee_{j=i}^{k} \left([\![f]\!]_k^j \wedge \bigwedge_{n=i}^{j} [\![g]\!]_k^n \right)$

Traduciendo las fórmulas LTL cuando hay loop

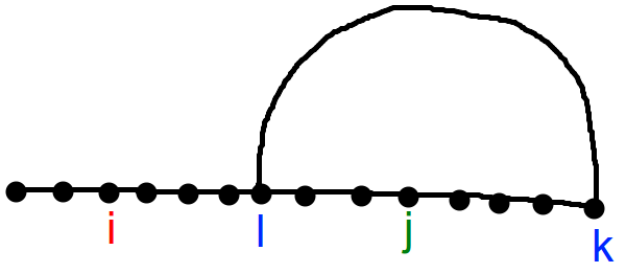
Definición 13 (Sucesor en un loop): Sea $k, l, i, \in \mathbb{N}$, con $l, i \leqslant k$. Definimos el sucesor $succ(i)$ de i en un (k, l)-loop como $succ(i) = i + 1$ para $i < k$ y $succ(k) = l$.

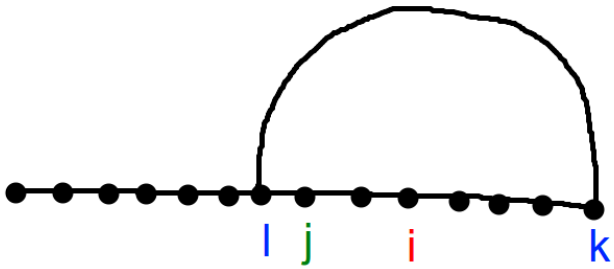
Definición 14: Dada una fórmula LTL f y $k, l, i \in \mathbb{N} / \ l, i \leqslant k$.

- ${}_l[\![p]\!]^i_k := p(s_i)$
- ${}_l[\![\neg p]\!]^i_k := \neg p(s_i)$
- ${}_l[\![f \wedge g]\!]^i_k := {}_l[\![f]\!]^i_k \wedge {}_l[\![g]\!]^i_k$
- ${}_l[\![f \vee g]\!]^i_k := {}_l[\![f]\!]^i_k \vee {}_l[\![g]\!]^i_k$
- ${}_l[\![\mathbf{G}f]\!]^i_k := \bigwedge_{j=min(i,l)}^{k} {}_l[\![f]\!]^j_k$
- ${}_l[\![\mathbf{F}f]\!]^i_k := \bigvee_{j=min(i,l)}^{k} {}_l[\![f]\!]^j_k$
- ${}_l[\![\mathbf{X}f]\!]^i_k := {}_l[\![f]\!]^{succ(i)}_k$

Traduciendo las fórmulas LTL cuando hay loop (caso f **U** g)

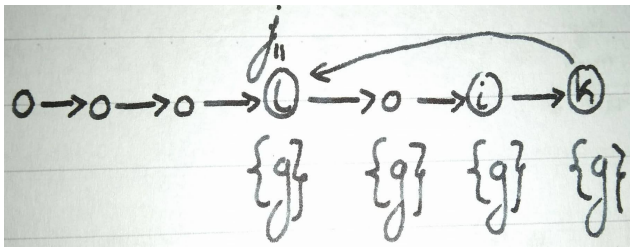
$$
{}_l[\![f \ \mathbf{U} \ g]\!]^i_k := \bigvee_{j=i}^{k} \left({}_l[\![g]\!]^j_k \wedge \bigwedge_{n=i}^{j-1} {}_l[\![f]\!]^n_k \right) \vee \bigvee_{j=l}^{i-1} \left({}_l[\![g]\!]^j_k \wedge \bigwedge_{n=i}^{k} {}_l[\![f]\!]^n_k \wedge \bigwedge_{n=l}^{j-1} {}_l[\![f]\!]^n_k \right)
$$



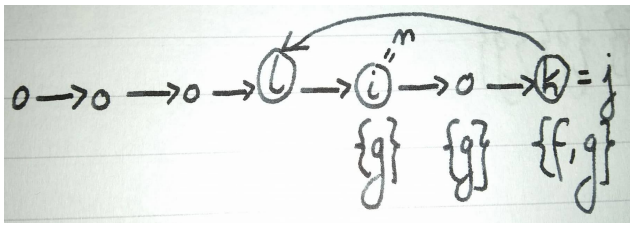


Traduciendo las fórmulas LTL cuando hay loop (caso $f\ \mathbf{R}\ g$)

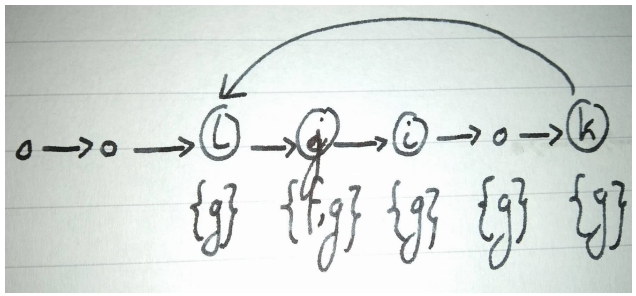
$$_l[\![f\ \mathbf{R}\ g]\!]^i_k := \bigwedge_{j=min(i,l)}^{k} {}_l[\![g]\!]^j_k \vee$$



$$\bigvee_{j=i}^{k} \left({}_l[\![f]\!]^j_k \wedge \bigwedge_{n=i}^{j} {}_l[\![g]\!]^n_k \right) \vee$$



$$\bigvee_{j=l}^{i-1} \left({}_l[\![f]\!]^j_k \wedge \bigwedge_{n=i}^{k} {}_l[\![g]\!]^n_k \wedge \bigwedge_{n=l}^{j} {}_l[\![g]\!]^n_k \right)$$



Terminando la construcción de la fórmula

Definición 15 (Condición de ciclo): Dados $k, l \in \mathbb{N} / \ l \leqslant k$.

$${}_lL_k := T(s_k, s_l),\ L_k := \bigvee_{l=0}^{k} {}_lL_k.$$

Terminando la construcción de la fórmula (cont.)

Definición 16 (Traducción general): Sea f una fórmula LTL, M una estructura de Kripke y $k \in \mathbb{N}$.

$$[\![M, f]\!]_k := [\![M]\!]_k \wedge \left(\left(\neg L_k \wedge [\![f]\!]_k^0 \right) \vee \bigvee_{l=0}^{k} \left({}_l L_k \wedge {}_l[\![f]\!]_k^0 \right) \right)$$

Teorema 17 (Correctitud del algoritmo): $[\![M, f]\!]_k$ es satisfacible $\iff$ $M \models_k \mathbf{E} f$.

Corolario 17.1 (Correctitud v2 del algoritmo): $M \models \mathbf{A} \neg f \iff \forall k \in \mathbb{N}, [\![M, f]\!]_k$ es insatisfacible.

Cotas

Teorema 18: Dada una fórmula LTL f y una estructura de Kripke M, sea $|M|$ la cantidad de estados de M.
$M \models \mathbf{E}f \iff \exists k \leqslant M \cdot 2^{|f|} / \ M \models_k \mathbf{E}f$.

Definición 19 (Diámetro del bucle): Decimos que una estructura de Kripke M tiene forma de lazo si existen $u, v \in \mathbb{N}$ tal que para todo camino p que empieza en un estado inicial, $p = u_p v_p^\omega$, donde u_p y v_p son secuencias de longitud finita de largo menor a u y v respectivamente. En tal caso se define el diámetro del bucle de M como (u, v).

Teorema 20: Dada una fórmula LTL f y una estructura de Kripke M con forma de lazo, sea (u, v) el diámetro del bucle de M.
$M \models \mathbf{E}f \iff \exists k \leqslant u + v / \ M \models_k \mathbf{E}f$.

Resultados

	SMV_1		SMV_2		SATO -g5		SATO -g50		PROVE	
bit	sec	MB	sec	MB	sec	MB	sec	MB	sec	MB
0	919	13	25	79	0	0	0	1	0	1
1	1978	13	25	79	0	0	0	1	0	1
2	2916	13	26	80	0	0	0	2	0	1
3	4744	13	27	82	0	0	0	3	1	2
4	6580	15	33	92	2	0	3	4	1	2
5	10803	25	67	102	12	0	36	7	1	2
6	43983	73	258	172	55	0	208	10	2	2
7	>17h		1741	492	209	0	642	13	7	3
8				>1GB	473	0	1198	16	29	3
9					856	1	2413	20	58	3
10					1837	1	2055	20	91	3
11					2367	1	1667	19	125	3
12					3830	1	976	17	156	4
13					5128	1	4363	25	186	4
14					4752	1	2170	23	226	4
15					4449	1	6847	31	183	5
sum	71923		2202		23970		22578		1066	

Table 1. 16x16 bit sequential shift and add multiplier with overflow flag and 16 output bits (sec = seconds, MB = Mega Byte).

Resultados

	SMV_1		SMV_2		SATO		PROVE	
cells	sec	MB	sec	MB	sec	MB	sec	MB
4	799	11	14	44	0	1	0	2
5	1661	14	24	57	0	1	0	2
6	3155	21	40	76	0	1	0	2
7	5622	38	74	137	0	1	0	2
8	9449	73	118	217	0	1	0	2
9	segmentation		172	220	0	1	1	2
10	fault		244	702	0	1	0	3
11			413	702	0	1	0	3
12			719	702	0	2	1	3
13			843	702	0	2	1	3
14			1060	702	0	2	1	3
15			1429	702	0	2	1	3

Table 4. Counterexample for liveness in a buggy DME (sec = seconds, MB = Mega Bytes).

¿Preguntas?