SAT and SMT Solving

Sarah Winkler

SS 2018

Department of Computer Science
University of Innsbruck

Outline

Summary of Last Week

Definitions

- theory consists of
  - signature Σ: set of function and predicate symbols
  - axioms T: set of sentences in first-order logic in which only function and predicate symbols of Σ appear
- theory is stably infinite if every satisfiable quantifier-free formula has model with infinite carrier set
- theory T is convex if $F \vDash_T \bigvee_{i=1}^{n} u_i = v_i$ implies $F \vDash_T u_i = v_i$ for some $1 \leqslant i \leqslant n$ $\forall$ quantifier-free conjunction F and variables u_i, v_i

Definition

theory combination $T_1 \oplus T_2$ of two theories

- T_1 over signature Σ_1
- T_2 over signature Σ_2

has signature $\Sigma_1 \cup \Sigma_2$ and axioms $T_1 \cup T_2$

Assumptions

Nelson-Oppen Method: Nondeterministic Version

Input quantifier-free conjunction φ in theory combination $T_1 \oplus T_2$

Output satisfiable or unsatisfiable

1. purification

$$\varphi \;\approx\; \varphi_1 \wedge \varphi_2 \quad \text{for } \Sigma_1\text{-formula } \varphi_1 \text{ and } \Sigma_2\text{-formula } \varphi_2$$

2. guess and check
   - V is set of shared variables in φ_1 and φ_2
   - guess equivalence relation E on V
   - arrangement $\alpha(V, E)$ is formula

$$\bigwedge_{x \mathrel{E} y} x = y \quad \wedge \bigwedge_{\neg(x \mathrel{E} y)} x \neq y$$

   - if $\varphi_1 \wedge \alpha(V, E)$ is T_1-satisfiable and $\varphi_2 \wedge \alpha(V, E)$ is T_2-satisfiable then return satisfiable else return unsatisfiable

Nelson-Oppen Method: Deterministic Version

Input quantifier-free conjunction φ in combination $T_1 \oplus T_2$ of convex theories T_1 and T_2

Output satisfiable or unsatisfiable

1. purification $\varphi \;\approx\; \varphi_1 \wedge \varphi_2$ for Σ_1-formula φ_1 and Σ_2-formula φ_2
2. V: set of shared variables in φ_1 and φ_2
   E: already discovered equalities between variables in V
3. test satisfiability of $\varphi_1 \wedge E$ (and add implied equations)
   - if $\varphi_1 \wedge E$ is T_1-unsatisfiable then return unsatisfiable
   - else add new implied equalities to E
4. test satisfiability of $\varphi_2 \wedge E$ (and add implied equations)
   - if $\varphi_2 \wedge E$ is T_2-unsatisfiable then return unsatisfiable
   - else add new implied equalities to E
5. if E has been extended in steps 3 or 4 then go to step 2
   else return satisfiable

Outline

- Summary of Last Week
- Bounded Model Checking for Verification

Bounded Model Checking for Verification

Disastrous Software Bugs

Ariane 5 Flight 501 (1996)

- destroyed 37 seconds after launch
- software for Ariane 4 for was reused
- software error: data conversion from 64-bit floating point to 16-bit integer caused arithmetic overflow
- cost: 370 million $

http://en.wikipedia.org/wiki/Ariane_5_Flight_501

Mars Exploration Rover “Spirit” (2004)

- landed on January 4
- stopped communicating on January 21
- software error: stuck in reboot loop
- reboot failed because of flash memory failure, ultimate problem: too many files

http://en.wikipedia.org/wiki/Spirit_(rover)

Heathrow Terminal 5 Opening (2008)

- baggage system collapsed on opening day
- 42,000 bags not shipped with their owners, 500 flights cancelled
- software was tested but did not work properly with real-world load
- cost 50 million £

http://www.zdnet.com/article/it-failure-at-heathrow-t5-what-really-happened

Trading Glitch at Knight Capital (2012)

- bug in trading software resulted in 45 minutes of uncontrolled buys
- company did 11% of US trading that year
- software was run in invalid configuration
- 440 million $ lost

http://en.wikipedia.org/wiki/Knight_Capital_Group

Death in Self-Driving Car Crash (2018)

- person died in accident with Uber’s self-driving car
- victim was wrongly classified by software as non-obstacle

http://www.siliconrepublic.com/companies/uber-bug-crash

Software is Ubiquitous in Critical Systems

transport, energy, medicine, communication, finance, embedded systems, ...

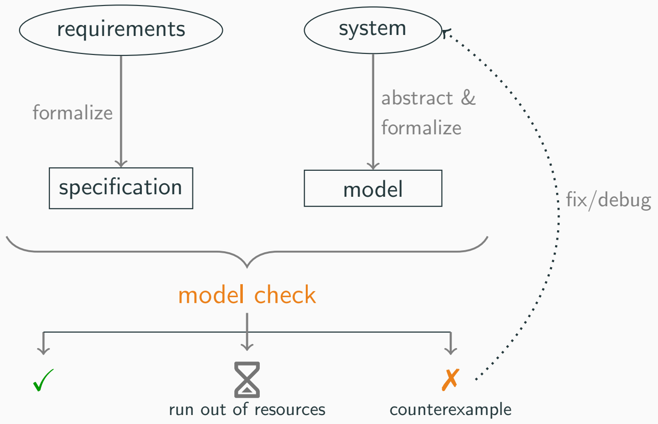
How to Ensure Correctness of Software?

- testing
  - + cheap, simple
  - − checks desired result only for given set of testcases
- verification
  - + can prove automatically that system meets specification, i.e., desired output is delivered for all inputs
  - − more costly

Model Checking

- widely used verification approach to
  - find bugs in software and hardware
  - prove correctness of models
- Turing Award 2007 for Clarke, Emerson, and Sifakis
- bounded model checking can be reduced to SAT/SMT

Model Checking: Workflow

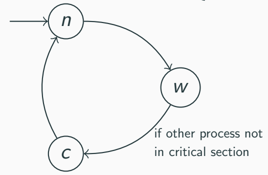


Model Checking Example: Mutex (1)

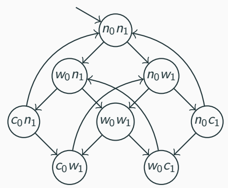
- concurrent processes P_0, P_1 share some resource, access controlled by mutex
- program run by P_0, P_1 matches pattern

```
# non-critical section
while (other process critical) :
  wait ()
# critical section
# non-critical section
```

- process can be abstracted to model $\mathcal{M} = \langle S, R\rangle$ with states $S = \{n, w, c\}$ and transitions R:



Model Checking Example: Mutex (2)



- obtain model for 2 processes by product construction: write $s_0 s_1$ for P_0 being in state s_0 and P_1 in state s_1
- desired properties:

safe: only one process is in its critical section at any time
live: whenever any process wants to enter its critical section, it will eventually be permitted to do so
non-blocking: a process can always request to enter its critical section

- how to formalize desired properties? temporal logic, e.g. LTL or CTL

safe: G $\neg(c_0 \wedge c_1)$ ✓ as $c_0 c_1$ unreachable
live: G $(w_0 \to$ F $c_0)$ ✗ e.g. 
non-blocking: AG $(n_0 \to$ EX $w_0)$ ✓

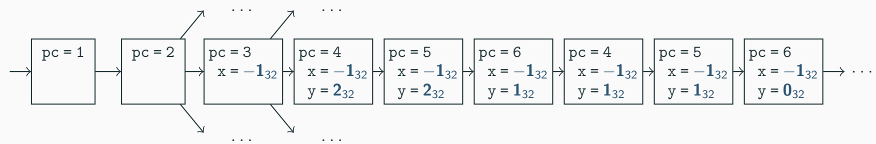
Common Kinds of Properties

- G ψ for propositional formula ψ is safety property
- G $(\psi \to$ F$\chi)$ for propositional formulas ψ,χ is liveness property

Example: Can This Program Cause An Overflow? (1)

```
1 void main() {
2   int x = -1;
3   int y = nondet_int();
4   while (y<100) {
5     y = y+x;
6   }
7 }
```

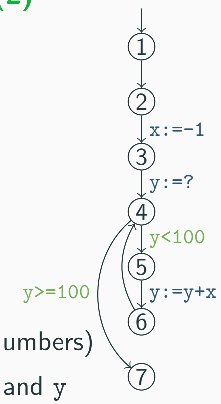
- model checking problem: addition $x + y$ in line 5 does not over/underflow
  - state of program run is assignment of x, y + value of program counter
  - property G $(\mathrm{pc} = 5 \to ((x > \mathbf{0}_{32} \wedge x + y > y) \vee (x \leqslant \mathbf{0}_{32} \wedge x + y \leqslant y)))$
- (part of) model:



- but state space is very large: $(2^{32})^2 \cdot 7$ for bit width 32
- cannot check all possible values

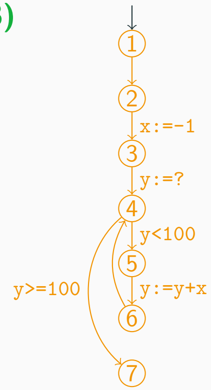
Example: Can This Program Cause An Overflow? (2)

```
1 void main() {
2   int x = -1;
3   int y = nondet_int();
4   while (y<100) {
5     y = y+x;
6   }
7 }
```



- construct program graph G
- $\{1, \dots, 7\}$ are possible values of program counter (line numbers)
- state is tuple $\langle \text{pc}, x, y \rangle$ of values of program counter, x, and y
- state of form $\langle 1, \dots, \dots \rangle$ is initial state
- examples of state transitions according to G:
  - $\langle 4, -\mathbf{1}_{32}, \mathbf{10}_{32} \rangle \to \langle 5, -\mathbf{1}_{32}, \mathbf{10}_{32} \rangle$ is possible
  - $\langle 4, -\mathbf{1}_{32}, \mathbf{101}_{32} \rangle \to \langle 7, -\mathbf{1}_{32}, \mathbf{101}_{32} \rangle$ is possible
  - $\langle 4, \mathbf{10}_{32}, \mathbf{101}_{32} \rangle \to \langle 5, \mathbf{10}_{32}, \mathbf{101}_{32} \rangle$ is not possible
  - $\langle 4, -\mathbf{1}_{32}, \mathbf{1}_{32} \rangle \to \langle 5, -\mathbf{1}_{32}, \mathbf{2}_{32} \rangle$ is not possible

Example: Can This Program Cause An Overflow? (3)



1. define predicates
   - $I(\langle pc, x, y \rangle) = (pc = 1)$ to characterize initial state
   - to characterize possible state transitions:

$$
\begin{aligned}
&T(\langle pc, x, y \rangle, \langle pc', x', y' \rangle) = \\
&\quad (pc = 1 \wedge pc' = 2) \vee (pc = 2 \wedge pc' = 3 \wedge x' = -1) \vee \\
&\quad (pc = 3 \wedge pc' = 4 \wedge x = x') \vee \\
&\quad (pc = 4 \wedge p' = 5 \wedge y < 100 \wedge x = x' \wedge y = y') \vee \\
&\quad (pc = 5 \wedge pc' = 6 \wedge y' = y + x \wedge x = x') \vee \\
&\quad (pc = 4 \wedge pc' = 7 \wedge y \geqslant 100 \wedge x = x' \wedge y = y') \vee \\
&\quad (pc = 6 \wedge pc' = 4 \wedge x = x' \wedge y = y')
\end{aligned}
$$

   - $P(\langle pc, x, y \rangle) = (pc = 5) \wedge ((x > \mathbf{0}_{32} \wedge x + y \leqslant y) \vee (x \leqslant \mathbf{0}_{32} \wedge (y + x > y)))$
2. for states $s_0, \dots, s_k$ formula φ_k expresses overflow occurring within k steps:

$$\varphi_k = I(s_0) \wedge \bigwedge_{i=0}^{k-1} T(s_i, s_{i+1}) \wedge \bigvee_{i=0}^{k} P(s_i)$$

3. if φ_k satisfiable then overflow can occur within k steps ... ask Z3

Bounded Model Checking

- find counterexamples to desired property of transition system (bugs)
- counterexamples are bounded in size

Definition (Transition System)

transition system $\mathcal{T} = (S, \to, S_0, L)$ where

- S is set of states
- $\to \subseteq S \times S$ is transition relation
- $S_0 \subseteq S$ is set of initial states
- A is a set of propositional atoms
- $L : S \to 2^A$ is labeling function associating state with subset of A

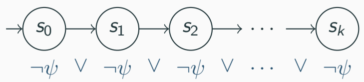
Remark

S and A may be (countably) infinite

Bounded Model Checking: Safety Properties

Idea

given transition system and property G ψ, look for counterexamples in $\leqslant k$ steps



SAT/SMT Encoding

given transition system $\mathcal{T}$ and safety property G ψ

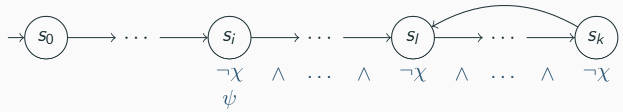
- use encoding $\langle s \rangle$ of state $s \in S$ by set of SAT/SMT variables
- use predicates
  - I for initial states such that $I(\langle s \rangle)$ is true iff $s \in S_0$
  - T for transitions such that $T(\langle s \rangle, \langle s' \rangle)$ is true iff $s \to s'$ in $\mathcal{T}$
  - P such that $P(\langle s \rangle)$ is true iff ψ holds in s
- use different fresh variables for $k + 1$ states $\langle s_0 \rangle, \dots, \langle s_k \rangle$
- check satisfiability of

$$I(\langle s_0 \rangle) \wedge \bigwedge_{i=0}^{k-1} T(\langle s_i \rangle, \langle s_{i+1} \rangle) \wedge \bigvee_{i=0}^{k} \neg P(\langle s_i \rangle)$$

Bounded Model Checking: Liveness Properties

Idea

- counterexample to liveness property $\mathsf{G}\,(\psi \to \mathsf{F}\chi)$ requires infinite path
- look for counterexamples in $\leqslant k$ steps of lasso shape:



SAT/SMT Encoding

given transition system $\mathcal{T}$ and liveness property $\mathsf{G}\,(\psi \to \mathsf{F}\chi)$

- use encoding of states, predicates I and T as for safety properties
- predicate P such that $P(\langle s\rangle)$ is true iff ψ holds in s
- predicate C such that $C(\langle s\rangle)$ is true iff χ holds in s
- check satisfiability of

$$I(\langle s_0\rangle) \wedge \bigwedge_{i=0}^{k-1} T(\langle s_i\rangle, \langle s_{i+1}\rangle) \wedge \bigvee_{i=0}^{k} \left(P(\langle s_i\rangle) \wedge \bigwedge_{j=i}^{k} \neg C(\langle s_j\rangle) \wedge \bigvee_{l=i}^{k} T(\langle s_k\rangle, \langle s_l\rangle) \right)$$

Transition System $\mathcal{T}(P)$ from Program P

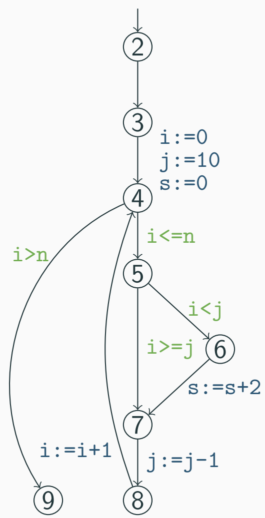
- state $\langle pc, v_0, \dots, v_n\rangle$ consists of
  - value for program counter pc, i.e. line number in P
  - assignment for variables in scope $\mathtt{v}_0, \dots, \mathtt{v}_n$
- there is step $s \to s'$ for $s = \langle pc, v_0, \dots, v_n\rangle$ and $s' = \langle pc', v_0', \dots, v_n'\rangle$ iff P admits step from s to s'
- S_0 consists of initial program states
- atom set A consists of all propositional formulas over $pc, v_0, \dots, v_n$
- labeling $L(s)$ is set of all atoms A which hold in $s = \langle pc, v_0, \dots, v_n\rangle$

Program Graph

- nodes are line numbers
- edge from line l to line l' if program counter can go from line l to l'
- two kinds of edge labels:
  - conditions for program counter to take this path
  - assignments of updated variables
- program graph is useful to derive encoding of $\mathcal{T}(P)$

Checking an Explicit Assertion

```
1  int n;
2  int main() {
3    int i, j=10, s=0;
4    for(i=0; i<=n; i++) {
5      if (i<j)
6        s = s + 2;
7      j--;
8    }
9    assert(s==n*2 || s == 0);
10 }
```



- construct program graph
- states are of form $\langle \mathrm{pc}, i, j, n, s\rangle$
- safety property to check is $\mathsf{G}\,(\mathrm{pc} = 9 \to (s = 2n \vee s = 0))$
- see `verification.py`

Software Verification Competition (SV-COMP)

- annual competition
  `https://sv-comp.sosy-lab.org/2018/`
- industrial (and crafted) benchmarks
  `https://github.com/sosy-lab/sv-benchmarks`
- many tools use SMT solvers

Common Safety Properties

- no overflow in addition: $(\mathtt{x} > 0 \wedge \mathtt{x} + \mathtt{y} \geqslant \mathtt{y}) \vee (\mathtt{x} \leqslant 0 \wedge \mathtt{x} + \mathtt{y} \leqslant \mathtt{y})$
- array accesses in bounds: $0 \leqslant \mathtt{i} < \mathit{size}(\mathtt{a})$ for all accesses a[i]
- memory safety: set predicate $\mathit{ok}(\mathit{addr})$ when memory allocated, check $\mathit{ok}(\mathtt{p})$ for every dereference $*\mathtt{p}$
- explicit assertions

Bibliography

Armin Biere, Alessandro Cimatti, Edmund M. Clarke, Ofer Strichman, and Yunshan Zhu.
Bounded Model Checking
Advances in Computers 58, pp 117–148, 2003.

Armin Biere.
Bounded Model Checking.
Chapter 14 in: Handbook of Satisfiability, IOS Press, pp. 457–481, 2009.