Formal Methods in Software Development

Eager SMT Solving (Equality Logic, Bit-blasting)

Mădălina Erașcu

West University of Timișoara
Faculty of Mathematics and Informatics
Department of Computer Science

Based on slides of the lecture Satisfiability Checking (Erika Ábrahám), RTWH Aachen

WS 2019/2020

Outline

Outline

SMT solving

- We want to extend propositional logic with theories.

SMT solving

- We want to extend propositional logic with theories.
- For satisfiability checking, SAT-solving will be extended to SAT-modulo-theories (SMT) solving.

SMT solving

- We want to extend propositional logic with theories.
- For satisfiability checking, SAT-solving will be extended to SAT-modulo-theories (SMT) solving.
- SMT-LIB: language, benchmarks, tutorials, ...
- SMT-COMP: performance and capabilities of tools
- SMT Workshop: held annually

Eager SMT solving

- How can such an extension to SMT solving look like?

Eager SMT solving

- How can such an extension to SMT solving look like?
- We will see two basically different approaches:
  - Eager SMT solving transforms logical formulas over some theories into satisfiability-equivalent propositional logic formulas and applies SAT solving. ("Eager" means theory first)
  - Lazy SMT solving uses a SAT solver to find solutions for the Boolean skeleton of the formula, and a theory solver to check satisfiability in the underlying theory. ("Lazy" means theory later)

Eager SMT solving

- How can such an extension to SMT solving look like?
- We will see two basically different approaches:
  - Eager SMT solving transforms logical formulas over some theories into satisfiability-equivalent propositional logic formulas and applies SAT solving. ("Eager" means theory first)
  - Lazy SMT solving uses a SAT solver to find solutions for the Boolean skeleton of the formula, and a theory solver to check satisfiability in the underlying theory. ("Lazy" means theory later)
- Today we will have a closer look at the eager approach.

Eager vs. Lazy SMT Solving

Theories for Eager SMT Solving

Theories for Eager SMT Solving

- All NP-complete problems can be transformed to equivalent propositional SAT problems (with polynomial effort).
- However, this is not always effective in praxis (the transformation would sometimes solve the hardest part of the problem).

Theories for Eager SMT Solving

- All NP-complete problems can be transformed to equivalent propositional SAT problems (with polynomial effort).
- However, this is not always effective in praxis (the transformation would sometimes solve the hardest part of the problem).
- Some well-suited theories for eager SMT solving:
  - Equalities and uninterpreted functions
  - Finite-precision bit-vector arithmetic
  - Quantifier-free linear integer arithemtic (QF_LIA)
  - Restricted λ-calculus (e.g., arrays)
  - ...

Theories for Eager SMT Solving

- All NP-complete problems can be transformed to equivalent propositional SAT problems (with polynomial effort).
- However, this is not always effective in praxis (the transformation would sometimes solve the hardest part of the problem).
- Some well-suited theories for eager SMT solving:
  - Equalities and uninterpreted functions
  - Finite-precision bit-vector arithmetic
  - Quantifier-free linear integer arithemtic (QF_LIA)
  - Restricted λ-calculus (e.g., arrays)
  - ...
  - Combinations of the above theories

Some Eager SMT Solver Implementations

- UCLID: Proof-based abstraction-refinement [Bryant et al., TACAS'07]
- STP: Solver for linear modular arithmetic to simplify the formula [Ganesh&Dill, CAV'07]
- Spear: Automatic parameter tuning for SAT [Hutter et al., FMCAD'07]
- Boolector: Rewrites, underapproximation, efficient SAT engine [Brummayer&Biere, TACAS'09]
- Beaver: Equality/constant propagation, logic optimization, special rules for non-linear operations [Jha et al., CAV'09]
- SONOLAR: Non-linear arithmetic [Brummayer et al., SMT'08]
- SWORD: Fixed-size bit-vectors [Jung et al, SMTCOMP'09]
- Layered eager approaches embedded in the lazy DPLL(T) framework: CVC3 [Barrett et al.], MathSAT [Bruttomesso et al.], Z3 [de Moura et al.]

Excursion: SMT-LIB Format

- `http://smtlib.cs.uiowa.edu`
- SMT-LIB is an international initiative aimed at facilitating research and development in Satisfiability Modulo Theories (SMT). Since its inception in 2003, the initiative has pursued these aims by focusing on the following concrete goals.
  - Provide standard rigorous descriptions of background theories used in SMT systems.
  - Develop and promote common input and output languages for SMT solvers.
  - Connect developers, researchers and users of SMT, and develop a community around it.
  - Establish and make available to the research community a large library of benchmarks for SMT solvers.
  - Collect and promote software tools useful to the SMT community.

Excursion: SMT-LIB Format (cont'd)

```
(declare-fun f (Int) Int)
(declare-fun a () Int) ; a is a constant
(declare-const b Int) ; syntax sugar for (declare-fun b () Int)
(assert (> a 20))
(assert (> b a))
(assert (= (f 10) 1))
(check-sat)
(get-model)
```

Use a SMT solver for checking the satisfiability, for example Z3 `https://rise4fun.com/z3/`.

Outline

Equality logic with uninterpreted functions

We extend propositional logic with

- equalities and
- uninterpreted functions (UFs).

Equality logic with uninterpreted functions

We extend propositional logic with

- equalities and
- uninterpreted functions (UFs).

Syntax:

- variables x over an arbitrary domain D,
- constants c from the same domain D,
- function symbols F for functions of the type $D^n \rightarrow D$, and
- equality as predicate symbol.

Equality logic with uninterpreted functions

We extend propositional logic with

- equalities and
- uninterpreted functions (UFs).

Syntax:

- variables x over an arbitrary domain D,
- constants c from the same domain D,
- function symbols F for functions of the type $D^n \to D$, and
- equality as predicate symbol.

$$
\begin{array}{llllllll}
\textit{Terms:} & t & := & c & \mid & x & \mid & F(t, \ldots, t) \\
\textit{Formulas:} & \varphi & := & t = t & \mid & (\varphi \land \varphi) & \mid & (\neg \varphi)
\end{array}
$$

Equality logic with uninterpreted functions

We extend propositional logic with

- equalities and
- uninterpreted functions (UFs).

Syntax:

- variables x over an arbitrary domain D,
- constants c from the same domain D,
- function symbols F for functions of the type $D^n \to D$, and
- equality as predicate symbol.

$$\begin{array}{llllllll} \textit{Terms:} & t & := & c & \mid & x & \mid & F(t,\dots,t) \\ \textit{Formulas:} & \varphi & := & t = t & \mid & (\varphi \land \varphi) & \mid & (\neg\varphi) \end{array}$$

Semantics: straightforward

Motivation

- Equality logic and propositional logic are both NP-complete.
- Thus they model the same decision problems.

Motivation

- Equality logic and propositional logic are both NP-complete.
- Thus they model the same decision problems.
- Why to study both?

Motivation

- Equality logic and propositional logic are both NP-complete.
- Thus they model the same decision problems.
- Why to study both?
  - Convenience of modeling
  - Efficiency

Equality logic with uninterpreted functions

Notation and assumptions:

- Formula with equalities: φ^E
- Formula with equalities and uninterpreted functions: φ^{UF}
- Same simplifications for parentheses as for propositional logic.
- Input formulas are in NNF.
- Input formulas are checked for satisfiability.

Removing constants

Theorem

There is an algorithm that generates for an input formula φ^{UF} an equisatisfiable output formula $\varphi^{UF'}$ without constants, in polynomial time.

Algorithm: Exercise

In the following we assume that the formulas do not contain constants.

Outline

Motivation

- Replacing functions by uninterpreted functions in a given formula is a common technique to make reasoning easier.
- It makes the formula weaker: $\models \varphi^{UF} \rightarrow \varphi$
- Ignore the semantics of the function, but:

Motivation

- Replacing functions by uninterpreted functions in a given formula is a common technique to make reasoning easier.
- It makes the formula weaker: $\models \varphi^{UF} \rightarrow \varphi$
- Ignore the semantics of the function, but:
  - Functional congruence: Instances of the same function return the same value for equal arguments.

From uninterpreted functions to equality logic

We lead back the problems of equality logic with uninterpreted functions to those of equality logic without uninterpreted functions.

Two possible reductions:

- Ackermann's reduction
- Bryant's reduction

Outline

1. Eager SMT Solving
2. Excursion: SMT-LIB Format
3. Eager SMT Solving for Equality Logic with Uninterpreted Functions
   - Equality Logic with Uninterpreted Functions
   - Eager SMT Solving for Uninterpreted Functions
     - Ackermann's reduction
     - Bryant's reduction
   - Eager SMT Solving for Equality Logic
     - Equality Graphs
4. Eager SMT Solving for Finite-precision Bit-vector Arithmetic

Ackermann's reduction

Given an input formula φ^{UF} of equality logic with uninterpreted functions, transform the formula to a satisfiability-equivalent equality logic formula φ^{E} of the form

$$\varphi^{E} := \varphi_{flat} \land \varphi_{cong},$$

where φ_{flat} is a flattening of φ^{UF}, and φ_{cong} is a conjunction of constraints for functional congruence.

For validity-equivalence check

$$\varphi^{E} := \varphi_{cong} \rightarrow \varphi_{flat}.$$

Ackermann's reduction

- Input: φ^{UF} with m instances of an uninterpreted function F.
- Output: satisfiability-equivalent φ^{E} without any occurrences of F.

Algorithm

Ackermann's reduction

- Input: φ^{UF} with m instances of an uninterpreted function F.
- Output: satisfiability-equivalent φ^{E} without any occurrences of F.

Algorithm

1. Assign indices to the F-instances.
2. $\varphi_{flat} := \mathcal{T}(\varphi^{UF})$ where $\mathcal{T}$ replaces each occurrence F_i of F by a fresh Boolean variable f_i.
3. $\varphi_{cong} := \bigwedge_{i=1}^{m-1} \bigwedge_{j=i+1}^{m} (\mathcal{T}(arg(F_i)) = \mathcal{T}(arg(F_j))) \rightarrow f_i = f_j$
4. Return $\varphi_{flat} \wedge \varphi_{cong}$.

Ackermann's reduction: Example

$$\varphi^{UF} \quad := \quad (x_1 \neq x_2) \vee (F(x_1) = F(x_2)) \vee (F(x_1) \neq F(x_3))$$

Ackermann's reduction: Example

$$\begin{aligned} \varphi^{UF} &:= (x_1 \neq x_2) \vee (F(x_1) = F(x_2)) \vee (F(x_1) \neq F(x_3)) \\ \varphi_{flat} &:= \end{aligned}$$

Ackermann's reduction: Example

$$\varphi^{UF} \quad := \quad (x_1 \neq x_2) \vee (F(x_1) = F(x_2)) \vee (F(x_1) \neq F(x_3))$$
$$\varphi_{flat} \quad := \quad (x_1 \neq x_2) \vee (f_1 = f_2) \vee (f_1 \neq f_3)$$

Ackermann's reduction: Example

$$
\begin{aligned}
\varphi^{UF} &:= (x_1 \neq x_2) \vee (F(x_1) = F(x_2)) \vee (F(x_1) \neq F(x_3)) \\
\varphi_{flat} &:= (x_1 \neq x_2) \vee (f_1 = f_2) \vee (f_1 \neq f_3) \\
\varphi_{cong} &:=
\end{aligned}
$$

Ackermann's reduction: Example

$$
\begin{array}{lcl}
\varphi^{UF} & := & (x_1 \neq x_2) \vee (F(x_1) = F(x_2)) \vee (F(x_1) \neq F(x_3)) \\
\varphi_{flat} & := & (x_1 \neq x_2) \vee (f_1 = f_2) \vee (f_1 \neq f_3) \\
\varphi_{cong} & := & ((x_1 = x_2) \quad \rightarrow \quad (f_1 = f_2)) \wedge \\
 & & ((x_1 = x_3) \quad \rightarrow \quad (f_1 = f_3)) \wedge \\
 & & ((x_2 = x_3) \quad \rightarrow \quad (f_2 = f_3))
\end{array}
$$

Ackermann's reduction: Example

$$
\begin{array}{lll}
\varphi^{UF} & := & (x_1 \neq x_2) \vee (F(x_1) = F(x_2)) \vee (F(x_1) \neq F(x_3)) \\
\varphi_{flat} & := & (x_1 \neq x_2) \vee (f_1 = f_2) \vee (f_1 \neq f_3) \\
\varphi_{cong} & := & ((x_1 = x_2) \quad \rightarrow \quad (f_1 = f_2)) \wedge \\
 & & ((x_1 = x_3) \quad \rightarrow \quad (f_1 = f_3)) \wedge \\
 & & ((x_2 = x_3) \quad \rightarrow \quad (f_2 = f_3)) \\
\varphi^{E} & := &
\end{array}
$$

Ackermann's reduction: Example

$$
\begin{array}{lcl}
\varphi^{UF} & := & (x_1 \neq x_2) \vee (F(x_1) = F(x_2)) \vee (F(x_1) \neq F(x_3)) \\
\varphi_{flat} & := & (x_1 \neq x_2) \vee (f_1 = f_2) \vee (f_1 \neq f_3) \\
\varphi_{cong} & := & ((x_1 = x_2) \quad \rightarrow \quad (f_1 = f_2)) \wedge \\
 & & ((x_1 = x_3) \quad \rightarrow \quad (f_1 = f_3)) \wedge \\
 & & ((x_2 = x_3) \quad \rightarrow \quad (f_2 = f_3)) \\
\varphi^{E} & := & \varphi_{flat} \wedge \varphi_{cong}
\end{array}
$$

Ackermann's reduction: Example

Check if the following programs are equivalent.

- ```
  int power3 (int in){
      int out = in;
      for (int i=0; i<2; i++)
          out = out * in;
      return out;
  }
  ```
- ```
  int power3_b (int in){
      return ((in * in) * in);
  }
  ```

Ackermann's reduction: Example

Check if the following programs are equivalent.

- ```
  int power3 (int in){
      int out = in;
      for (int i=0; i<2; i++)
          out = out * in;
      return out;
  }
  ```
- ```
  int power3_b (int in){
      return ((in * in) * in);
  }
  ```

- $\varphi_1 \ := \ out_0 = in \wedge out_1 = out_0 * in \wedge out_2 = out_1 * in$
- $\varphi_2 \ := \ out_b = (in * in) * in$
- Equivalence check: $\varphi_3 \ := \ (\varphi_1 \wedge \varphi_2) \rightarrow (out_2 = out_b)$

Ackermann's reduction: Example

$$\begin{aligned}\varphi_3 \quad := \quad & (out_0 = in \wedge out_1 = out_0 * in \wedge \\ & out_2 = out_1 * in \wedge out_b = (in * in) * in) \rightarrow \\ & (out_2 = out_b)\end{aligned}$$

Ackermann's reduction: Example

$$\begin{aligned}\varphi_3 \quad := \quad & (out_0 = in \wedge out_1 = out_0 * in \wedge \\ & out_2 = out_1 * in \wedge out_b = (in * in) * in) \rightarrow \\ & (out_2 = out_b)\end{aligned}$$

Motivation for using uninterpreted functions: computational; deciding formulas with multiplication over, for example, 32-bit variables is notoriously hard. Replacing the multiplication symbol with uninterpreted functions can solve the problem.

Ackermann's reduction: Example

$$\begin{aligned}\varphi_3 \quad := \quad & (out_0 = in \land out_1 = out_0 * in \land \\ & out_2 = out_1 * in \land out_b = (in * in) * in) \rightarrow \\ & (out_2 = out_b)\end{aligned}$$

Motivation for using uninterpreted functions: computational; deciding formulas with multiplication over, for example, 32-bit variables is notoriously hard. Replacing the multiplication symbol with uninterpreted functions can solve the problem.

$$\begin{aligned}\varphi^{UF} \quad := \quad & (out_0 = in \land out_1 = G(out_0, in) \land \\ & out_2 = G(out_1, in) \land out_b = G(G(in, in), in)) \rightarrow \\ & (out_2 = out_b)\end{aligned}$$

Ackermann's reduction: Example

$$\varphi^{UF} := (out_0 = in \wedge out_1 = G(out_0, in) \wedge out_2 = G(out_1, in) \wedge out_b = G(G(in, in), in)) \rightarrow (out_2 = out_b)$$

Ackermann's reduction: Example

$$\varphi^{UF} := (out_0 = in \wedge out_1 = G(out_0, in) \wedge out_2 = G(out_1, in) \wedge out_b = G(G(in, in), in)) \rightarrow (out_2 = out_b)$$

$$\varphi_{flat} := (out_0 = in \wedge out_1 = G_1 \wedge out_2 = G_2 \wedge out_b = G_4) \rightarrow (out_2 = out_b)$$

$$\begin{aligned}
\varphi_{cong} := \; & ((out_0 = out_1 \wedge in = in) & \rightarrow & \quad G_1 = G_2)\wedge \\
& ((out_0 = in \wedge in = in) & \rightarrow & \quad G_1 = G_3)\wedge \\
& ((out_0 = G_3 \wedge in = in) & \rightarrow & \quad G_1 = G_4)\wedge \\
& ((out_1 = in \wedge in = in & \rightarrow & \quad G_2 = G_3)\wedge \\
& ((out_1 = G_3 \wedge in = in) & \rightarrow & \quad G_2 = G_4)\wedge \\
& ((in = G_3 \wedge in = in) & \rightarrow & \quad G_3 = G_4)
\end{aligned}$$

Check if $\varphi_{cong} \Rightarrow \varphi_{flat}$ is valid.

Outline

1 Eager SMT Solving

2 Excursion: SMT-LIB Format

3 Eager SMT Solving for Equality Logic with Uninterpreted Functions
- Equality Logic with Uninterpreted Functions
- Eager SMT Solving for Uninterpreted Functions
  - Ackermann's reduction
  - Bryant's reduction
- Eager SMT Solving for Equality Logic
  - Equality Graphs

4 Eager SMT Solving for Finite-precision Bit-vector Arithmetic

Bryant's reduction

- Case expression:

$$
\begin{array}{rcllcl}
F_i^* & = & case & x_1 = x_i & : & f_1 \\
 & & & x_2 = x_i & : & f_2 \\
 & & & \ldots & & \\
 & & & x_{i-1} = x_i & : & f_{i-1} \\
 & & & true & : & f_i
\end{array}
$$

where x_i is the argument $arg(F_i)$ of F_i for all i.

- Semantics:

$$
\bigvee_{j=1}^{i} \left(\left(\bigwedge_{k=1}^{j-1} (x_k \neq x_i) \right) \wedge (x_j = x_i) \wedge (F_i^* = f_j) \right)
$$

Bryant's reduction

- Input: φ^{UF} with m instances of an uninterpreted function F.
- Output: satisfiability-equivalent φ^{E} without any occurrences of F.

Algorithm

Bryant's reduction

- Input: φ^{UF} with m instances of an uninterpreted function F.
- Output: satisfiability-equivalent φ^{E} without any occurrences of F.

Algorithm

1. Assign indices to the F-instances.
2. Return $\mathcal{T}^*(\varphi^{UF})$ where $\mathcal{T}^*$ replaces each $F_i(arg(F_i))$ by

$$
\begin{array}{lll}
\textit{case} & \mathcal{T}^*(arg(F_1)) = \mathcal{T}^*(arg(F_i)) & : \; f_1 \\
& \ldots & \\
& \mathcal{T}^*(arg(F_{i-1})) = \mathcal{T}^*(arg(F_i)) & : \; f_{i-1} \\
& \textit{true} & : \; f_i
\end{array}
$$

Bryant's reduction: Example

- ```
  int power3 (int in){
     int out = in;
     for (int i=0; i<2; i++)
        out = out * in;
     return out;
  }
  ```
- ```
  int power3_b (int in){
     return ((in * in) * in);
  }
  ```

Bryant's reduction: Example

- ```
  int power3 (int in){
     int out = in;
     for (int i=0; i<2; i++)
        out = out * in;
     return out;
  }
  ```
- ```
  int power3_b (int in){
     return ((in * in) * in);
  }
  ```

- $\varphi_1 \;:=\; out_0 = in \wedge out_1 = out_0 * in \wedge out_2 = out_1 * in$
- $\varphi_2 \;:=\; out_b = (in * in) * in$
- $\varphi_3 \;:=\; (\varphi_1 \wedge \varphi_2) \rightarrow (out_2 = out_b)$

Bryant's reduction: Example

$$
\begin{aligned}
\varphi_3 \quad := \quad & (out_0 = in \wedge out_1 = out_0 * in \wedge \\
& out_2 = out_1 * in \wedge out_b = (in * in) * in) \rightarrow \\
& (out_2 = out_b)
\end{aligned}
$$

Bryant's reduction: Example

$$
\begin{aligned}
\varphi_3 \quad := \quad & (out_0 = in \wedge out_1 = out_0 * in \wedge \\
& out_2 = out_1 * in \wedge out_b = (in * in) * in) \rightarrow \\
& (out_2 = out_b)
\end{aligned}
$$

$$
\begin{aligned}
\varphi^{UF} \quad := \quad & (out_0 = in \wedge out_1 = G(out_0, in) \wedge \\
& out_2 = G(out_1, in) \wedge out_b = G(G(in, in), in)) \rightarrow \\
& (out_2 = out_b)
\end{aligned}
$$

Bryant's reduction: Example

$$\varphi^{UF} := (out_0 = in \land out_1 = G(out_0, in) \land out_2 = G(out_1, in) \land out_b = G(G(in, in), in)) \to (out_2 = out_b)$$

Bryant's reduction: Example

$$
\begin{array}{rcl}
\varphi^{UF} & := & (out_0 = in \wedge out_1 = G(out_0, in) \wedge out_2 = G(out_1, in) \wedge \\
 & & out_b = G(G(in, in), in)) \rightarrow (out_2 = out_b) \\
\varphi^{E} & := & (out_0 = in \wedge out_1 = G_1^* \wedge out_2 = G_2^* \wedge \\
 & & out_b = G_4^*) \rightarrow (out_2 = out_b) \text{ with}
\end{array}
$$

$$
\begin{array}{rcllcl}
G_1^* & = & & & & g_1 \\
G_2^* & = & case & out_0 = out_1 \wedge in = in & : & g_1 \\
 & & & true & : & g_2 \\
G_3^* & = & case & out_0 = in \wedge in = in & : & g_1 \\
 & & & out_1 = in \wedge in = in & : & g_2 \\
 & & & true & : & g_3 \\
G_4^* & = & case & out_0 = G_3^* \wedge in = in & : & g_1 \\
 & & & out_1 = G_3^* \wedge in = in & : & g_2 \\
 & & & in = G_3^* \wedge in = in & : & g_3 \\
 & & & true & : & g_4
\end{array}
$$

Outline

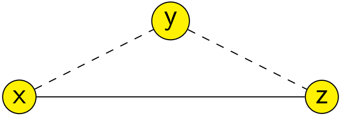
E-graphs

$$\varphi^E : x = y \land y = z \land z \neq x$$

- The equality predicates: $\{x = y, y = z, z \neq x\}$
- Break into two sets:

$$E_= = \{x = y, y = z\}, \quad E_{\neq} = \{z \neq x\}$$

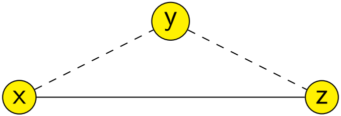
- The equality graph (E-graph) $G^E(\varphi^E) = \langle V, E_=, E_{\neq} \rangle$



The E-graph and Boolean structure in φ^E

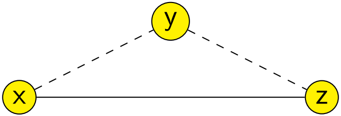
$$\begin{array}{lll} \varphi_1^E: & x = y \wedge y = z \wedge z \neq x & \text{unsatisfiable} \\ \varphi_2^E: & (x = y \wedge y = z) \vee z \neq x & \text{satisfiable!} \end{array}$$

Their E-graph is the same:



$\Longrightarrow$ The graph $G^E(\varphi^E)$ represents an abstraction of φ^E.
It ignores the Boolean structure of φ^E.

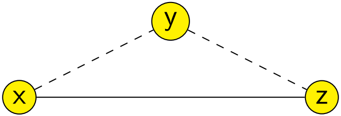
Equality and disequality paths



Definition (Equality Path)

A path that uses $E_=$ edges is an *equality path*. We write $x =^* z$.

Equality and disequality paths



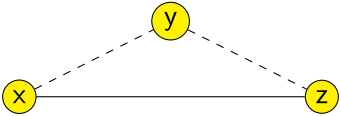
Definition (Equality Path)

A path that uses $E_=$ edges is an *equality path*. We write $x =^* z$.

Definition (Disequality Path)

A path that uses edges from $E_=$ and exactly one edge from $E_{\neq}$ is a *disequality path*. We write $x \neq^* z$.

Contradictory cycles



Definition (Contradictory Cycle)

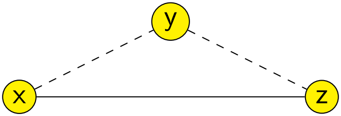
A cycle with one disequality edge is a *contradictory cycle*.

Theorem

For every two nodes x, y on a contradictory cycle the following holds:

- $x =^* y$
- $x \neq^* y$

Contradictory cycles



Definition

A subgraph of E is called *satisfiable* iff the conjunction of the predicates represented by its edges is satisfiable.

Theorem

A subgraph is unsatisfiable iff it contains a contradictory cycle.

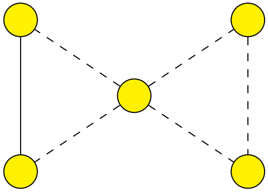
Simple cycles

Question: What is a simple cycle?

Simple cycles

Question: What is a simple cycle?

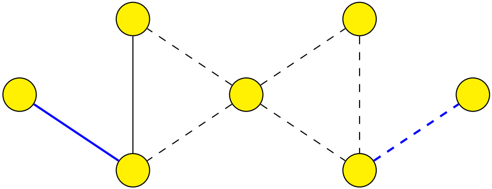
A cycle is simple if it is represented by a path in which none of the vertices is repeated, other than the starting and ending vertices.



Theorem

Every contradictory cycle is either simple, or contains a simple contradictory cycle.

Simplifying the E-graph of φ^E



Let S be the set of edges that are not part of any contradictory cycle.

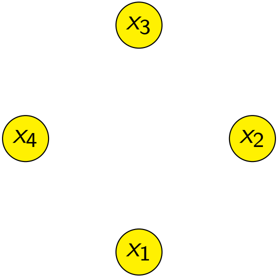
Theorem

Replacing

- *all equations in φ^E that correspond to solid edges in S with false, and*
- *all equations in φ^E that correspond to dashed edges in S with true*

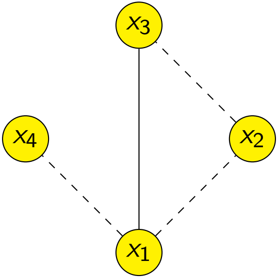
preserves satisfiability.

Simplifying the E-graph: Example



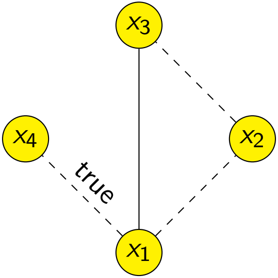
- $$\begin{aligned}&(x_1 = x_2 \quad \vee \quad x_1 = x_4) \quad \wedge \\ &(x_1 \neq x_3 \quad \vee \quad x_2 = x_3)\end{aligned}$$

Simplifying the E-graph: Example



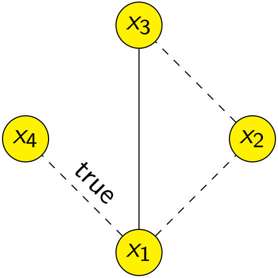
- $(x_1 = x_2 \quad \vee \quad x_1 = x_4) \quad \wedge$
  $(x_1 \neq x_3 \quad \vee \quad x_2 = x_3)$

Simplifying the E-graph: Example



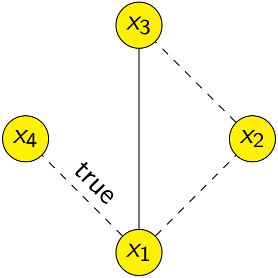
- $$\begin{array}{l}(x_1 = x_2 \quad \vee \quad x_1 = x_4) \quad \wedge \\ (x_1 \neq x_3 \quad \vee \quad x_2 = x_3)\end{array}$$

Simplifying the E-graph: Example



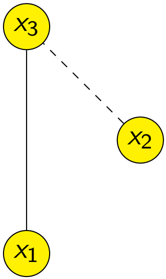
- $$(x_1 = x_2 \quad \vee \quad x_1 = x_4) \quad \wedge$$
  $$(x_1 \neq x_3 \quad \vee \quad x_2 = x_3)$$
- $$(x_1 = x_2 \quad \vee \quad \text{true} \quad) \quad \wedge$$
  $$(x_1 \neq x_3 \quad \vee \quad x_2 = x_3)$$

Simplifying the E-graph: Example



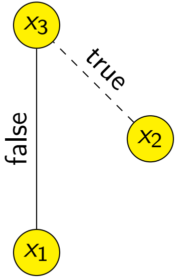
- $(x_1 = x_2 \quad \vee \quad x_1 = x_4) \quad \wedge$
  $(x_1 \neq x_3 \quad \vee \quad x_2 = x_3)$
- $(x_1 = x_2 \quad \vee \quad \text{true} \quad) \quad \wedge$
  $(x_1 \neq x_3 \quad \vee \quad x_2 = x_3)$
- $(x_1 \neq x_3 \quad \vee \quad x_2 = x_3)$

Simplifying the E-graph: Example



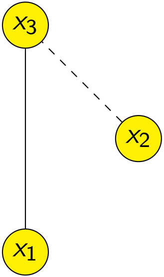
- $$\begin{array}{lllll}(x_1 = x_2 & \vee & x_1 = x_4) & \wedge \\ (x_1 \neq x_3 & \vee & x_2 = x_3) & \end{array}$$
- $$\begin{array}{lllll}(x_1 = x_2 & \vee & \text{true} \quad) & \wedge \\ (x_1 \neq x_3 & \vee & x_2 = x_3) & \end{array}$$
- $(x_1 \neq x_3 \quad \vee \quad x_2 = x_3)$

Simplifying the E-graph: Example



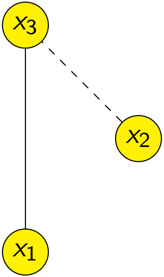
- $(x_1 = x_2 \quad \vee \quad x_1 = x_4) \quad \wedge$
  $(x_1 \neq x_3 \quad \vee \quad x_2 = x_3)$
- $(x_1 = x_2 \quad \vee \quad \text{true} \quad) \quad \wedge$
  $(x_1 \neq x_3 \quad \vee \quad x_2 = x_3)$
- $(x_1 \neq x_3 \quad \vee \quad x_2 = x_3)$

Simplifying the E-graph: Example



- $$\begin{array}{lcll} (x_1 = x_2 & \vee & x_1 = x_4) & \wedge \\ (x_1 \neq x_3 & \vee & x_2 = x_3) & \end{array}$$
- $$\begin{array}{lcll} (x_1 = x_2 & \vee & \text{true} \;) & \wedge \\ (x_1 \neq x_3 & \vee & x_2 = x_3) & \end{array}$$
- $(x_1 \neq x_3 \quad \vee \quad x_2 = x_3)$
- $\neg\text{false} \vee \text{true}$

Simplifying the E-graph: Example



- $(x_1 = x_2 \lor x_1 = x_4) \land$
  $(x_1 \neq x_3 \lor x_2 = x_3)$
- $(x_1 = x_2 \lor \text{true}) \land$
  $(x_1 \neq x_3 \lor x_2 = x_3)$
- $(x_1 \neq x_3 \lor x_2 = x_3)$
- $\neg\text{false} \lor \text{true}$
- $\rightarrow$ Satisfiable!

Outline

Finite-precision bit-vector arithmetic

"Bit blasting":

- Model bit-level operations (functions and predicates) by Boolean circuits
- Use Tseitin's encoding to generate propositional SAT encoding
- Use a SAT solver to check satisfiability
- Convert back the propositional solution to the theory

Effective solution for many applications.

- Example: Bounded model checking for C programs (CBMC) [Clarke, Kroening, Lerda, TACAS'04]

No further details in the FMSD course.