

# On conflict-driven reasoning

Maria Paola Bonacina

**Visiting:** Computer Science Laboratory, SRI International, Menlo Park, CA, USA

**Affiliation:** Dipartimento di Informatica, Università degli Studi di Verona,  
Verona, Italy, EU

19 May 2017

Conflict-driven reasoning

Conflict-driven reasoning in SAT: CDCL

Conflict-driven reasoning in SMT: MCSAT

Conflict-driven reasoning in theory combination: CDSAT

# Automated reasoning and formal methods

- ▶ Automated formal methods generate reasoning problems
  - ▶ Prove conjectures
  - ▶ Find solutions of sets of constraints
- ▶ Formal method tools incorporate/invoke reasoning engines
- ▶ Logic is the calculus of computation
- ▶ Machines reasoning about machines

# Conflict-driven reasoning: what is a conflict?

- ▶ **Conflict**: between constraints to be satisfied and a candidate partial model
- ▶ Methods that build a candidate partial model: **model-based reasoning**

# Model-based reasoning

- ▶ A reasoning method is **model-based** if it works with a candidate (partial) model of a set of clauses
- ▶ The state of the derivation includes a representation of the current candidate model
- ▶ **Inferences** transform the candidate **model**
- ▶ The candidate **model** drives the **inferences**

# Conflict-driven reasoning

- ▶ **Conflict**: one of the clauses is false in the current candidate model
- ▶ A model-based reasoning method is **conflict-driven** if inferences
  - ▶ **Explain** the conflict
  - ▶ **Solve** the conflict repairing the model

# Conflict-driven propositional reasoning: CDCL

- ▶ SAT: satisfiability of a set of clauses in propositional logic
- ▶ **Conflict-Driven Clause Learning** (CDCL) procedure  
[Marques-Silva, Sakallah: ICCAD 1996, IEEE Trans. on Computers 1999], [Moskewicz, Madigan, Zhao, Zhang, Malik: DAC 2001]  
[Marques-Silva, Lynce, Malik: SAT Handbook 2009]
- ▶ CDCL is **conflict-driven SAT-solving**

# A taste of CDCL: decide and propagate

$$\{\neg a \vee b, \neg c \vee d, \neg e \vee \neg f, f \vee \neg e \vee \neg b\} \subseteq S$$

1. **Decide:**  $a$  is true; **Propagate:**  $b$  must be true
  2. **Decide:**  $c$  is true; **Propagate:**  $d$  must be true
  3. **Decide:**  $e$  is true; **Propagate:**  $\neg f$  must be true
- ▶ Trail  $M = a, b, c, d, e, \neg f$
  - ▶ **Conflict:**  $f \vee \neg e \vee \neg b$  is false



# A taste of CDCL: explain, learn, backjump

$$\{\neg a \vee b, \neg c \vee d, \neg e \vee \neg f, f \vee \neg e \vee \neg b\} \subseteq S$$

$$M = a, b, c, d, e, \neg f$$

1. Conflict:  $f \vee \neg e \vee \neg b$
2. Explain by resolving  $f \vee \neg e \vee \neg b$  with  $\neg e \vee \neg f$ :  $\neg e \vee \neg b$
3. Learn  $\neg e \vee \neg b$ : no model with  $e$  and  $b$  true
4. Backjump to earliest state with  $\neg b$  false and  $\neg e$  unassigned:  
 $M = a, b, \neg e$
5. Continue until it finds a satisfying assignment (model) or none can be found (conflict at level 0)

# Conflict-driven reasoning in fragments of arithmetic

- ▶  $\mathcal{T}$ -satisfiability procedure: decides satisfiability of a set of ground literals in theory  $\mathcal{T}$
- ▶ Conflict-driven  $\mathcal{T}$ -satisfiability procedures for fragments of arithmetic, e.g.:
  - ▶ Linear rational arithmetic [McMillan, Kuehlmann, Sagiv: CAV 2009], [Korovin, Tsiskaridze, Voronkov: CP 2009], [Cotton: FORMATS 2010]
  - ▶ Linear integer arithmetic [Jovanović, de Moura: CADE 2011]
  - ▶ Non-linear arithmetic [Jovanović, de Moura: IJCAR 2012]
  - ▶ Floating-point binary arithmetic [Haller, Griggio, Brain, Kroening: FMCAD 2012]

# First-order assignments

- ▶ CDCL: the trail is a sequence of literals
- ▶ Example:  $M = a, b, \neg e$
- ▶ Equivalently:  $M = a \leftarrow true, b \leftarrow true, e \leftarrow false$
- ▶ Conflict-driven  $\mathcal{T}$ -satisfiability procedures for fragments of arithmetic: assignments to first-order variables
- ▶ Example:  $M = x \leftarrow 3, y \leftarrow -2, z \leftarrow 0$

# Conflict-driven theory reasoning for SMT: MCSAT

- ▶  $\mathcal{T}$ -decision procedure: decides satisfiability of a quantifier-free formula in theory  $\mathcal{T}$
- ▶ MCSAT (Model-constructing satisfiability) is a framework for conflict-driven  $\mathcal{T}$ -decision procedures:
  - ▶ One generic theory [de Moura, Jovanović: VMCAI 2013]
  - ▶ Equality + linear rational arithmetic [Jovanović, Barrett, de Moura: FMCAD 2013]
  - ▶ Non-linear integer arithmetic [Jovanović: VMCAI 2017]
  - ▶ Bit-vectors [Zeljić, Wintersteiger, Rümmer: SAT 2016]  
[Graham-Lengrand, Jovanović: SMT 2017]

# Model-constructing satisfiability: MCSAT

- ▶ CDCL-based SAT-solver + conflict-driven  $\mathcal{T}$ -satisfiability procedure: cooperate on the same level
- ▶ Trail  $M$ : **both**  $L$  (means  $L \leftarrow true$ ) and  $x \leftarrow 3$
- ▶ Any  $\mathcal{T}$  equipped with an **inference system** to **explain** theory conflicts
- ▶ Such inferences may introduce **new atoms**
- ▶ Beyond input literals: finite basis for termination
- ▶ MCSAT lifts CDCL to SMT

## Example of theory explanation (equality)

$$F = \{\dots, v \simeq f(a), w \simeq f(b), \dots\}$$

$$M = \dots a \leftarrow \alpha, b \leftarrow \alpha, w \leftarrow \beta_1, v \leftarrow \beta_2, \dots$$

Conflict!

Explain by  $a \simeq b \supset f(a) \simeq f(b)$   
(instance of substitutivity)

# Example of theory explanation (arithmetic) I

$$F = \{x \geq 2, \neg(x \geq 1) \vee y \geq 1, x^2 + y^2 \leq 1 \vee xy > 1\}$$

- ▶  $M = \emptyset$
- ▶ Boolean Propagation:  $M = x \geq 2$
- ▶ Theory Propagation:  $M = x \geq 2, x \geq 1$
- ▶ Boolean Propagation:  $M = x \geq 2, x \geq 1, y \geq 1$
- ▶ Boolean Decision:  $M = x \geq 2, x \geq 1, y \geq 1, x^2 + y^2 \leq 1$
- ▶ Semantic Decision:  
 $M = x \geq 2, x \geq 1, y \geq 1, x^2 + y^2 \leq 1, x \leftarrow 2$
- ▶ Conflict!: no value for  $y$  such that  $4 + y^2 \leq 1$

## Example of theory explanation (arithmetic) II

$$F = \{x \geq 2, \neg(x \geq 1) \vee y \geq 1, x^2 + y^2 \leq 1 \vee xy > 1\}$$

- ▶ Assume we learn  $x \neq 2$ :

$$M = x \geq 2, x \geq 1, y \geq 1, x^2 + y^2 \leq 1, x \neq 2$$

- ▶ Semantic Decision:

$$M = x \geq 2, x \geq 1, y \geq 1, x^2 + y^2 \leq 1, x \neq 2, x \leftarrow 3$$

- ▶ Another conflict!
- ▶ We do not want to learn  $x \neq 2, x \neq 3, x \neq 4 \dots$  !



## Example of theory explanation (arithmetic) III

$$F = \{x \geq 2, \neg(x \geq 1) \vee y \geq 1, x^2 + y^2 \leq 1 \vee xy > 1\}$$

- ▶ Solution: **theory explanation** by **interpolation**
- ▶  $x^2 + y^2 \leq 1$  implies  $-1 \leq x \wedge x \leq 1$  which is inconsistent with  $x = 2$
- ▶ Learn  $\neg(x^2 + y^2 \leq 1) \vee x \leq 1$
- ▶ Undo  $x \leftarrow 2$  and propagate  $x \leq 1$
- ▶  $M = x \geq 2, x \geq 1, y \geq 1, x^2 + y^2 \leq 1, x \leq 1$

## Example of theory explanation (arithmetic) IV

$$F = \{x \geq 2, \neg(x \geq 1) \vee y \geq 1, x^2 + y^2 \leq 1 \vee xy > 1\}$$

- ▶  $M = x \geq 2, x \geq 1, y \geq 1, x^2 + y^2 \leq 1, x \leq 1$
- ▶ Theory conflict:  $x \geq 2$  and  $x \leq 1$
- ▶ Conflict clause:  $\neg(x \geq 2) \vee \neg(x \leq 1)$
- ▶ Boolean Explanation (by resolution):  $\neg(x^2 + y^2 \leq 1) \vee x \leq 1$   
and  $\neg(x \geq 2) \vee \neg(x \leq 1)$  yield  $\neg(x^2 + y^2 \leq 1) \vee \neg(x \geq 2)$
- ▶ Boolean Explanation (by resolution):  
 $\neg(x^2 + y^2 \leq 1) \vee \neg(x \geq 2)$  and  $x \geq 2$  yield  $\neg(x^2 + y^2 \leq 1)$
- ▶  $M = x \geq 2, x \geq 1, y \geq 1, \neg(x^2 + y^2 \leq 1)$

# Conflict-driven multi-theory reasoning: CDSAT

- ▶ CDSAT (Conflict-driven satisfiability) is a framework for conflict-driven  $\mathcal{T}$ -decision procedures, where  $\mathcal{T}$  is a generic combination of theories  $\mathcal{T}_1, \dots, \mathcal{T}_n$
- ▶ Disjoint theories: share sorts,  $\simeq$ , uninterpreted constants
- ▶ Propositional logic is one of them
- ▶ CDSAT combines inference systems  $\mathcal{I}_1, \dots, \mathcal{I}_n$  for  $\mathcal{T}_1, \dots, \mathcal{T}_n$
- ▶ CDSAT generalizes MCSAT
- ▶ CDSAT generalizes equality sharing (aka Nelson-Oppen)

[Bonacina, Graham-Lengrand, Shankar: CADE 2017]

# Conflict-driven satisfiability: CDSAT

- ▶ Trail  $M$ : sequence of assignments (e.g.,  $L \leftarrow true, x \leftarrow 3$ )
- ▶ **CDSAT** defines the division of labor among the  $\mathcal{I}_1, \dots, \mathcal{I}_n$ : each has its **view** of the trail, knows which terms it can assign, features its inference rules that may introduce **new atoms**
- ▶ Global finite basis for termination
- ▶ **Satisfiability modulo assignment (SMA)**: decide the  $\mathcal{T}$ -satisfiability of a quantifier-free formula modulo an initial assignment of values to free first-order variables

# Example in a combination of theories

$$P = \{f(\text{select}(\text{store}(a, i, v), j)) \simeq w, f(u) \simeq w - 2, i \simeq j, u \simeq v\}$$

- ▶ Combination of
  - ▶ Equality (EUF)
  - ▶ Linear rational arithmetic (LRA)
  - ▶ Arrays (Arr)
- ▶ **Theory modules**  $\mathcal{I}_{EUF}$ ,  $\mathcal{I}_{LRA}$ , and  $\mathcal{I}_{Arr}$

## Example (continued)

- ▶ LRA has sorts  $\{prop, Q\}$ ;  $\simeq$  on each sort;  $0, 1: Q$ ;  
 $+: Q \times Q \rightarrow Q$ ;  $c \cdot: Q \rightarrow Q$  for all rational number  $c$
- ▶ Arr has sorts  $\{prop, V, I, A\}$ ;  $\simeq$  on each sort;  
 $select: A \times I \rightarrow V$ ;  $store: A \times I \times V \rightarrow A$
- ▶ EUF has sorts  $\{prop, Q, V\}$ ;  $\simeq$  on each sort;  $f: V \rightarrow Q$

# Example of CDSAT derivation I

$$P = \{f(\text{select}(\text{store}(a, i, v), j)) \simeq w, f(u) \simeq w - 2, i \simeq j, u \simeq v\}$$

- ▶ **Decisions:**  $u \leftarrow \alpha, v \leftarrow \alpha$
- ▶ **Decisions:**  $\text{select}(\text{store}(a, i, v), j) \leftarrow \alpha, w \leftarrow 0$
- ▶ **Decisions:**  $f(\text{select}(\text{store}(a, i, v), j)) \leftarrow 0, f(u) \leftarrow -2$
- ▶ **Deductions:**  $u \simeq \text{select}(\text{store}(a, i, v), j),$   
 $f(u) \not\simeq f(\text{select}(\text{store}(a, i, v), j))$
- ▶ **Conflict:** the last two yield  $\perp$  in  $\mathcal{I}_{EUF}$
- ▶ **Backjump:** flips  $f(u) \not\simeq f(\text{select}(\text{store}(a, i, v), j))$  and clears the trail saving  $u \simeq \text{select}(\text{store}(a, i, v), j)$  and its justification

## Example of CDSAT derivation II

$$P = \{f(\text{select}(\text{store}(a, i, v), j)) \simeq w, f(u) \simeq w - 2, i \simeq j, u \simeq v\}$$

- ▶ Decisions:  $u \leftarrow \alpha, v \leftarrow \alpha, \text{select}(\text{store}(a, i, v), j) \leftarrow \alpha$
- ▶ Deduction:  $u \simeq \text{select}(\text{store}(a, i, v), j)$
- ▶ Deduction:  $f(u) \simeq f(\text{select}(\text{store}(a, i, v), j))$
- ▶ Deductions:  $f(u) \simeq w, w - 2 \simeq w$  by transitivity of equality
- ▶ Conflict:  $w - 2 \simeq w$  yields  $\perp$  in  $\mathcal{I}_{LRA}$
- ▶ Conflict:  $f(u) \simeq w, f(u) \simeq w - 2$
- ▶ Conflict:  $f(u) \simeq f(\text{select}(\text{store}(a, i, v), j)),$   
 $f(\text{select}(\text{store}(a, i, v), j)) \simeq w, f(u) \simeq w - 2$
- ▶ Conflict:  $u \simeq \text{select}(\text{store}(a, i, v), j),$   
 $f(\text{select}(\text{store}(a, i, v), j)) \simeq w, f(u) \simeq w - 2$



## Example of CDSAT derivation III

$$P = \{f(\text{select}(\text{store}(a, i, v), j)) \simeq w, f(u) \simeq w - 2, i \simeq j, u \simeq v\}$$

- ▶ **Backjump:** flips  $u \simeq \text{select}(\text{store}(a, i, v), j)$  and jumps back to level 0
- ▶ **Deduction:**  $u \not\simeq \text{select}(\text{store}(a, i, v), j)$
- ▶ **Decisions:**  $u \leftarrow \alpha, v \leftarrow \alpha, \text{select}(\text{store}(a, i, v), j) \leftarrow \beta$
- ▶ **Deduction:**  $v \not\simeq \text{select}(\text{store}(a, i, v), j)$
- ▶ **Conflict:**  $i \simeq j, v \not\simeq \text{select}(\text{store}(a, i, v), j)$  yield  $\perp$  in  $\mathcal{I}_{Arr}$

## Example of CDSAT derivation IV

$$P = \{f(\text{select}(\text{store}(a, i, v), j)) \simeq w, f(u) \simeq w - 2, i \simeq j, u \simeq v\}$$

- ▶ Deduction:  $u \not\simeq \text{select}(\text{store}(a, i, v), j)$
- ▶ **Backjump**: flips  $v \not\simeq \text{select}(\text{store}(a, i, v), j)$  and jumps back to level 0
- ▶ **Deduction**:  $v \simeq \text{select}(\text{store}(a, i, v), j)$
- ▶ **Conflict**:  $u \simeq v$ ,  $u \not\simeq \text{select}(\text{store}(a, i, v), j)$ , and  $v \simeq \text{select}(\text{store}(a, i, v), j)$  yield  $\perp$
- ▶ **Conflict** at level 0:  $P$  is unsatisfiable

# Summary

- ▶ Emergence of a general paradigm of conflict-driven reasoning
- ▶ CDCL: conflict-driven SAT-solving
- ▶ Conflict-driven  $\mathcal{T}$ -satisfiability procedures in arithmetic
- ▶ MCSAT: conflict-driven SMT-solving
- ▶ CDSAT: conflict-driven combination of theories and SMA-solving
- ▶ SGGs: conflict-driven theorem proving in first-order logic  
[Bonacina, Plaisted: JAR 2016, 2017]