CS:4980 Topics in Computer Science II

Introduction to Automated Reasoning

Combining Theory Solvers with SAT solvers

Cesare Tinelli

Spring 2024

The University of Iowa

Credits

These slides are based on slides originally developed by **Cesare Tinelli** at the University of Iowa, and by **Clark Barrett**, **Caroline Trippel**, and **Andrew (Haoze) Wu** at Stanford University. Adapted by permission.

Checking the satisfiability of quantifier-free formulas

Theory solvers check the satisfiability of conjunctions of literals

What if we have formulas with disjunctions, like this $\mathcal{T}_{EUF}$-formula?

$$g(a) \doteq c \;\land\; (f(g(a)) \not\doteq f(c) \;\lor\; g(a) \doteq d) \;\land\; c \not\doteq d$$

What about arbitrary Boolean combinations of literals?

Checking the satisfiability of quantifier-free formulas

Theory solvers check the satisfiability of conjunctions of literals

What if we have formulas with disjunctions, like this $\mathcal{T}_{EUF}$-formula?

$$g(a) \doteq c \;\wedge\; (f(g(a)) \not\doteq f(c) \;\vee\; g(a) \doteq d) \;\wedge\; c \not\doteq d$$

What about arbitrary Boolean combinations of literals?

Checking the satisfiability of quantifier-free formulas

Theory solvers check the satisfiability of conjunctions of literals

What if we have formulas with disjunctions, like this $\mathcal{T}_{EUF}$-formula?

$$g(a) \doteq c \;\wedge\; (f(g(a)) \not\doteq f(c) \;\vee\; g(a) \doteq d) \;\wedge\; c \not\doteq d$$

What about arbitrary Boolean combinations of literals?

Checking the satisfiability of quantifier-free formulas

Theorem 1

For all theories $\mathcal{T}$, the $\mathcal{T}$-satisfiability of quantifier-free formulas is decidable iff the $\mathcal{T}$-satisfiability of conjunctions/sets of literals is decidable.

Proof.

Convert the formula to DNF and check if any of its disjuncts is $\mathcal{T}$-satisfiable. □

Problem: the DNF conversion is very inefficient! (formula size can explode exponentially)

A better solution: exploit propositional satisfiability technology to deal with the Boolean structure

Checking the satisfiability of quantifier-free formulas

Theorem 1

For all theories $\mathcal{T}$, the $\mathcal{T}$-satisfiability of quantifier-free formulas is decidable iff the $\mathcal{T}$-satisfiability of conjunctions/sets of literals is decidable.

Proof.

Convert the formula to DNF and check if any of its disjuncts is $\mathcal{T}$-satisfiable. □

Problem: the DNF conversion is very inefficient! (formula size can explode exponentially)

A better solution: exploit propositional satisfiability technology to deal with the Boolean structure

Checking the satisfiability of quantifier-free formulas

Theorem 1

For all theories $\mathcal{T}$, the $\mathcal{T}$-satisfiability of quantifier-free formulas is decidable iff the $\mathcal{T}$-satisfiability of conjunctions/sets of literals is decidable.

Proof.

Convert the formula to DNF and check if any of its disjuncts is $\mathcal{T}$-satisfiable. □

Problem: the DNF conversion is very inefficient! (formula size can explode exponentially)

A better solution: exploit propositional satisfiability technology to deal with the Boolean structure

Checking the satisfiability of quantifier-free formulas

Theorem 1
For all theories $\mathcal{T}$, the $\mathcal{T}$-satisfiability of quantifier-free formulas is decidable iff the $\mathcal{T}$-satisfiability of conjunctions/sets of literals is decidable.

Proof.
Convert the formula to DNF and check if any of its disjuncts is $\mathcal{T}$-satisfiable. □

Problem: the DNF conversion is very inefficient! (formula size can explode exponentially)

A better solution: exploit propositional satisfiability technology to deal with the Boolean structure

Lifting SAT Technology to SMT

Two main approaches:

1. *Eager*

   - translate into an equisatisfiable propositional formula
   - feed it to any SAT solver

Notable systems: UCLID

2. *Lazy*

   - abstract the input formula to a propositional one
   - feed it to a (CDCL-based) SAT solver
   - use a theory decision procedure to refine the formula and guide the SAT solver

Notable systems: Bitwuzla, cvc5, MathSAT, Yices, Z3

Lifting SAT Technology to SMT

Two main approaches:

1. *Eager*
   - translate into an equisatisfiable propositional formula
   - feed it to any SAT solver

Notable systems: UCLID

2. *Lazy*
   - abstract the input formula to a propositional one
   - feed it to a (CDCL-based) SAT solver
   - use a theory decision procedure to refine the formula and guide the SAT solver

Notable systems: Bitwuzla, cvc5, MathSAT, Yices, Z3

Lazy Approach for SMT

Given a quantifier-free Σ-formula φ, for each atomic formula α in φ, we associate a unique propositional variable $e(\alpha)$

The *Boolean skeleton* of a formula φ is a propositional logic formula, where each atomic formula α in φ is replaced with $e(\alpha)$

Example:

$$\varphi := \underbrace{x < 0}_{p_1} \vee (\underbrace{x + y < 1}_{p_2} \wedge \neg(\underbrace{x < 0}_{p_1})) \Rightarrow \underbrace{y < 0}_{p_3}$$

Boolean skeleton of φ : $p_1 \vee (p_2 \wedge \neg p_1) \Rightarrow p_3$

with $e := \{ (x < 0) \mapsto p_1,\ (x + y < 1) \mapsto p_2,\ (y < 0) \mapsto p_3 \}$

Lazy Approach for SMT

Given a quantifier-free Σ-formula φ, for each atomic formula α in φ, we associate a unique propositional variable $e(\alpha)$

The *Boolean skeleton* of a formula φ is a propositional logic formula, where each atomic formula α in φ is replaced with $e(\alpha)$

Example:

$$\varphi := \underbrace{x < 0}_{p_1} \vee (\underbrace{x + y < 1}_{p_2} \wedge \neg(\underbrace{x < 0}_{p_1})) \Rightarrow \underbrace{y < 0}_{p_3}$$

Boolean skeleton of φ : $\quad p_1 \vee (p_2 \wedge \neg p_1) \Rightarrow p_3$

with $e := \{ (x < 0) \mapsto p_1,\ (x + y < 1) \mapsto p_2,\ (y < 0) \mapsto p_3 \}$

(Very) Lazy Approach for SMT – Example

$$g(a) \doteq c \;\wedge\; (f(g(a)) \mathrel{\dot{\neq}} f(c) \;\vee\; g(a) \doteq d) \;\wedge\; c \mathrel{\dot{\neq}} d$$

Simplest setting:

- Off-line SAT solver
- Non-incremental *theory solver* for conjunctions of equalities and disequalities
- Theory atoms (e.g., $g(a) \doteq c$) *abstracted* to propositional atoms (e.g., 1)

(Very) Lazy Approach for SMT – Example

$$g(a) \doteq c \;\wedge\; (f(g(a)) \not\doteq f(c) \vee g(a) \doteq d) \;\wedge\; c \not\doteq d$$

Simplest setting:

- Off-line SAT solver
- Non-incremental *theory solver* for conjunctions of equalities and disequalities
- Theory atoms (e.g., $g(a) \doteq c$) *abstracted* to propositional atoms (e.g., 1)

(Very) Lazy Approach for SMT – Example

Notation: $\bar{p}$ stands for $\neg p$

$$\underbrace{g(a) \doteq c}_{1} \quad \wedge \quad \underbrace{f(g(a)) \not\doteq f(c)}_{\bar{2}} \vee \underbrace{g(a) \doteq d}_{3} \quad \wedge \quad \underbrace{c \not\doteq d}_{\bar{4}}$$

(Very) Lazy Approach for SMT – Example

Notation: $\bar{p}$ stands for $\neg p$

$$\underbrace{g(a) \doteq c}_{1} \quad \wedge \quad \underbrace{f(g(a)) \mathrel{\dot{\neq}} f(c)}_{\bar{2}} \vee \underbrace{g(a) \doteq d}_{3} \quad \wedge \quad \underbrace{c \mathrel{\dot{\neq}} d}_{\bar{4}}$$

- Send $\{1,\ \bar{2} \vee 3,\ \bar{4}\}$ to SAT solver
- SAT solver returns model $\{1,\ \bar{2},\ \bar{4}\}$
- Theory solver finds (concretization of) $\{1,\ \bar{2},\ \bar{4}\}$ unsat in $\mathcal{T}_{EUF}$ (meaning that $\bar{1} \vee 2 \vee 4$ is valid in $\mathcal{T}_{EUF}$)
- Send $\{1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4\}$ to SAT solver
- SAT solver returns model $\{1,\ 3,\ \bar{4}\}$
- Theory solver finds $\{1,\ 3,\ \bar{4}\}$ unsat
- Send $\{1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4,\ \bar{1} \vee \bar{3} \vee 4\}$ to SAT solver
- SAT solver finds $\{1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4,\ \bar{1} \vee \bar{3} \vee 4\}$ unsat

(Very) Lazy Approach for SMT – Example

Notation: $\bar{p}$ stands for $\neg p$

$$\underbrace{g(a) \doteq c}_{1} \;\wedge\; \underbrace{f(g(a)) \not\doteq f(c)}_{\bar{2}} \vee \underbrace{g(a) \doteq d}_{3} \;\wedge\; \underbrace{c \not\doteq d}_{\bar{4}}$$

- Send $\{1,\ \bar{2} \vee 3,\ \bar{4}\}$ to SAT solver
- SAT solver returns model $\{1,\ \bar{2},\ \bar{4}\}$
- Theory solver finds (concretization of) $\{1,\ \bar{2},\ \bar{4}\}$ unsat in $\mathcal{T}_{EUF}$ (meaning that $\bar{1} \vee 2 \vee 4$ is valid in $\mathcal{T}_{EUF}$)
- Send $\{1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4\}$ to SAT solver
- SAT solver returns model $\{1,\ 3,\ \bar{4}\}$
- Theory solver finds $\{1,\ 3,\ \bar{4}\}$ unsat
- Send $\{1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4,\ \bar{1} \vee \bar{3} \vee 4\}$ to SAT solver
- SAT solver finds $\{1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4,\ \bar{1} \vee \bar{3} \vee 4\}$ unsat

(Very) Lazy Approach for SMT – Example

Notation: $\bar{p}$ stands for $\neg p$

$$\underbrace{g(a) \doteq c}_{1} \;\wedge\; \underbrace{f(g(a)) \not\doteq f(c)}_{\bar{2}} \vee \underbrace{g(a) \doteq d}_{3} \;\wedge\; \underbrace{c \not\doteq d}_{\bar{4}}$$

- Send $\{1,\ \bar{2} \vee 3,\ \bar{4}\}$ to SAT solver
- SAT solver returns model $\{1,\ \bar{2},\ \bar{4}\}$
- Theory solver finds (concretization of) $\{1,\ \bar{2},\ \bar{4}\}$ unsat in $\mathcal{T}_{EUF}$ (meaning that $\bar{1} \vee 2 \vee 4$ is valid in $\mathcal{T}_{EUF}$)
- Send $\{1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4\}$ to SAT solver
- SAT solver returns model $\{1,\ 3,\ \bar{4}\}$
- Theory solver finds $\{1,\ 3,\ \bar{4}\}$ unsat
- Send $\{1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4,\ \bar{1} \vee \bar{3} \vee 4\}$ to SAT solver
- SAT solver finds $\{1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4,\ \bar{1} \vee \bar{3} \vee 4\}$ unsat

(Very) Lazy Approach for SMT – Example

Notation: $\bar{p}$ stands for $\neg p$

$$\underbrace{g(a) \doteq c}_{1} \quad \wedge \quad \underbrace{f(g(a)) \not\doteq f(c)}_{\bar{2}} \vee \underbrace{g(a) \doteq d}_{3} \quad \wedge \quad \underbrace{c \not\doteq d}_{\bar{4}}$$

- Send $\{1,\ \bar{2} \vee 3,\ \bar{4}\}$ to SAT solver
- SAT solver returns model $\{1,\ \bar{2},\ \bar{4}\}$
- Theory solver finds (concretization of) $\{1,\ \bar{2},\ \bar{4}\}$ unsat in $\mathcal{T}_{EUF}$
  (meaning that $\bar{1} \vee 2 \vee 4$ is valid in $\mathcal{T}_{EUF}$)
- Send $\{1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4\}$ to SAT solver
- SAT solver returns model $\{1,\ 3,\ \bar{4}\}$
- Theory solver finds $\{1,\ 3,\ \bar{4}\}$ unsat
- Send $\{1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4,\ \bar{1} \vee \bar{3} \vee 4\}$ to SAT solver
- SAT solver finds $\{1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4,\ \bar{1} \vee \bar{3} \vee 4\}$ unsat

(Very) Lazy Approach for SMT – Example

Notation: $\bar{p}$ stands for $\neg p$

$$\underbrace{g(a) \doteq c}_{1} \quad \wedge \quad \underbrace{f(g(a)) \mathrel{\dot{\neq}} f(c)}_{\bar{2}} \vee \underbrace{g(a) \doteq d}_{3} \quad \wedge \quad \underbrace{c \mathrel{\dot{\neq}} d}_{\bar{4}}$$

- Send $\{1,\ \bar{2} \vee 3,\ \bar{4}\}$ to SAT solver
- SAT solver returns model $\{1,\ \bar{2},\ \bar{4}\}$
- Theory solver finds (concretization of) $\{1,\ \bar{2},\ \bar{4}\}$ unsat in $\mathcal{T}_{EUF}$ (meaning that $\bar{1} \vee 2 \vee 4$ is valid in $\mathcal{T}_{EUF}$)
- Send $\{1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4\}$ to SAT solver
- SAT solver returns model $\{1,\ 3,\ \bar{4}\}$
- Theory solver finds $\{1,\ 3,\ \bar{4}\}$ unsat
- Send $\{1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4,\ \bar{1} \vee \bar{3} \vee 4\}$ to SAT solver
- SAT solver finds $\{1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4,\ \bar{1} \vee \bar{3} \vee 4\}$ unsat

(Very) Lazy Approach for SMT – Example

Notation: $\bar{p}$ stands for $\neg p$

$$\underbrace{g(a) \doteq c}_{1} \quad \wedge \quad \underbrace{f(g(a)) \not\doteq f(c)}_{\bar{2}} \vee \underbrace{g(a) \doteq d}_{3} \quad \wedge \quad \underbrace{c \not\doteq d}_{\bar{4}}$$

- Send $\{1,\ \bar{2} \vee 3,\ \bar{4}\}$ to SAT solver
- SAT solver returns model $\{1,\ \bar{2},\ \bar{4}\}$
- Theory solver finds (concretization of) $\{1,\ \bar{2},\ \bar{4}\}$ unsat in $\mathcal{T}_{EUF}$ (meaning that $\bar{1} \vee 2 \vee 4$ is valid in $\mathcal{T}_{EUF}$)
- Send $\{1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4\}$ to SAT solver
- SAT solver returns model $\{1,\ 3,\ \bar{4}\}$
- Theory solver finds $\{1,\ 3,\ \bar{4}\}$ unsat
- Send $\{1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4,\ \bar{1} \vee \bar{3} \vee 4\}$ to SAT solver
- SAT solver finds $\{1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4,\ \bar{1} \vee \bar{3} \vee 4\}$ unsat

(Very) Lazy Approach for SMT – Example

Notation: $\bar{p}$ stands for $\neg p$

$$\underbrace{g(a) \doteq c}_{1} \;\wedge\; \underbrace{f(g(a)) \not\doteq f(c)}_{\bar{2}} \vee \underbrace{g(a) \doteq d}_{3} \;\wedge\; \underbrace{c \not\doteq d}_{\bar{4}}$$

- Send $\{1,\ \bar{2} \vee 3,\ \bar{4}\}$ to SAT solver
- SAT solver returns model $\{1,\ \bar{2},\ \bar{4}\}$
- Theory solver finds (concretization of) $\{1,\ \bar{2},\ \bar{4}\}$ unsat in $\mathcal{T}_{EUF}$ (meaning that $\bar{1} \vee 2 \vee 4$ is valid in $\mathcal{T}_{EUF}$)
- Send $\{1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4\}$ to SAT solver
- SAT solver returns model $\{1,\ 3,\ \bar{4}\}$
- Theory solver finds $\{1,\ 3,\ \bar{4}\}$ unsat
- Send $\{1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4,\ \bar{1} \vee \bar{3} \vee 4\}$ to SAT solver
- SAT solver finds $\{1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4,\ \bar{1} \vee \bar{3} \vee 4\}$ unsat

(Very) Lazy Approach for SMT – Example

Notation: $\bar{p}$ stands for $\neg p$

$$\underbrace{g(a) \doteq c}_{1} \quad \wedge \quad \underbrace{f(g(a)) \not\doteq f(c)}_{\bar{2}} \vee \underbrace{g(a) \doteq d}_{3} \quad \wedge \quad \underbrace{c \not\doteq d}_{\bar{4}}$$

- Send $\{1,\ \bar{2} \vee 3,\ \bar{4}\}$ to SAT solver
- SAT solver returns model $\{1,\ \bar{2},\ \bar{4}\}$
- Theory solver finds (concretization of) $\{1,\ \bar{2},\ \bar{4}\}$ unsat in $\mathcal{T}_{EUF}$ (meaning that $\bar{1} \vee 2 \vee 4$ is valid in $\mathcal{T}_{EUF}$)
- Send $\{1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4\}$ to SAT solver
- SAT solver returns model $\{1,\ 3,\ \bar{4}\}$
- Theory solver finds $\{1,\ 3,\ \bar{4}\}$ unsat
- Send $\{1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4,\ \bar{1} \vee \bar{3} \vee 4\}$ to SAT solver
- SAT solver finds $\{1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4,\ \bar{1} \vee \bar{3} \vee 4\}$ unsat

(Very) Lazy Approach for SMT – Example

Notation: $\bar{p}$ stands for $\neg p$

$$\underbrace{g(a) \doteq c}_{1} \;\wedge\; \underbrace{f(g(a)) \not\doteq f(c)}_{\bar{2}} \vee \underbrace{g(a) \doteq d}_{3} \;\wedge\; \underbrace{c \not\doteq d}_{\bar{4}}$$

- Send $\{1,\ \bar{2} \vee 3,\ \bar{4}\}$ to SAT solver
- SAT solver returns model $\{1,\ \bar{2},\ \bar{4}\}$
- Theory solver finds (concretization of) $\{1,\ \bar{2},\ \bar{4}\}$ unsat in $\mathcal{T}_{EUF}$ (meaning that $\bar{1} \vee 2 \vee 4$ is valid in $\mathcal{T}_{EUF}$)
- Send $\{1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4\}$ to SAT solver
- SAT solver returns model $\{1,\ 3,\ \bar{4}\}$
- Theory solver finds $\{1,\ 3,\ \bar{4}\}$ unsat
- Send $\{1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4,\ \bar{1} \vee \bar{3} \vee 4\}$ to SAT solver
- SAT solver finds $\{1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4,\ \bar{1} \vee \bar{3} \vee 4\}$ unsat

Done! The original formula is unsatisfiable in $\mathcal{T}_{EUF}$

Eager Approach for SMT – Example

$$f(b) \doteq a \quad \vee \quad f(a) \not\doteq a$$

Step 1: Eliminate all function applications (Ackermann's encoding)

- introduce a constant symbol f_x to replace function application $f(x)$
- for each pair of introduced variables f_x, f_y, add the formula $x \doteq y \Rightarrow f_x \doteq f_y$

$$f(b) \Rightarrow f_b \qquad f(a) \Rightarrow f_a$$

$$(f_b \doteq a \;\vee\; f_a \not\doteq a) \;\wedge\; (a \doteq b \Rightarrow f_a \doteq f_b)$$

Now, atomic formulas are equalities between constants/variables

Eager Approach for SMT – Example

$$f(b) \doteq a \quad \vee \quad f(a) \not\doteq a$$

Step 1: Eliminate all function applications (Ackermann's encoding)

- introduce a constant symbol f_x to replace function application $f(x)$
- for each pair of introduced variables f_x, f_y, add the formula $x \doteq y \Rightarrow f_x \doteq f_y$

$$f(b) \Rightarrow f_b \qquad f(a) \Rightarrow f_a$$

$$(f_b \doteq a \ \vee \ f_a \not\doteq a) \ \wedge \ (a \doteq b \Rightarrow f_a \doteq f_b)$$

Now, atomic formulas are equalities between constants/variables

Eager Approach for SMT – Example

$$f(b) \doteq a \;\vee\; f(a) \not\doteq a$$

Step 1: Eliminate all function applications (Ackermann's encoding)

- introduce a constant symbol f_x to replace function application $f(x)$
- for each pair of introduced variables f_x, f_y, add the formula $x \doteq y \Rightarrow f_x \doteq f_y$

$$f(b) \Rightarrow f_b \qquad f(a) \Rightarrow f_a$$

$$(f_b \doteq a \;\vee\; f_a \not\doteq a) \;\wedge\; (a \doteq b \Rightarrow f_a \doteq f_b)$$

Now, atomic formulas are equalities between constants/variables

Eager Approach for SMT – Example

Rename f_b as c and f_a as d:

$$(f_b \doteq a \ \vee \ f_a \not\doteq a) \ \wedge \ (a \doteq b \Rightarrow f_a \doteq f_b)$$

becomes

$$(c \doteq a \ \vee \ d \not\doteq a) \ \wedge \ (a \doteq b \Rightarrow d \doteq c)$$

Step 2: Eliminate all equalities

- replace each pair of constants x, y with a unique propositional variable $p_{x,y}$
- add facts about reflexivity, symmetry, transitivity

$$\begin{gathered}(p_{c,a} \ \vee \ \neg p_{d,a}) \ \wedge \ (p_{a,b} \Rightarrow p_{d,c}) \\ \wedge \ p_{a,a} \wedge p_{b,b} \wedge p_{c,c} \wedge p_{d,d} \wedge \ (p_{a,b} \Leftrightarrow p_{b,a}) \wedge (p_{a,c} \Leftrightarrow p_{c,a}) \wedge (p_{a,d} \Leftrightarrow p_{d,a}) \wedge \cdots \\ \wedge \ ((p_{a,b} \wedge p_{b,c}) \Rightarrow p_{a,c}) \wedge ((p_{a,c} \wedge p_{c,d}) \Rightarrow p_{a,d}) \wedge \cdots\end{gathered}$$

The resulting propositional formula is equisatisfiable with the original T_{EUF}-formula

Note: Not all the transitivity cases are needed

Eager Approach for SMT – Example

Rename f_b as c and f_a as d:

$$(f_b \doteq a \ \vee \ f_a \not\doteq a) \ \wedge \ (a \doteq b \Rightarrow f_a \doteq f_b)$$

becomes

$$(c \doteq a \ \vee \ d \not\doteq a) \ \wedge \ (a \doteq b \Rightarrow d \doteq c)$$

Step 2: Eliminate all equalities

- replace each pair of constants x, y with a unique propositional variable $p_{x,y}$
- add facts about reflexivity, symmetry, transitivity

$$(p_{c,a} \ \vee \ \neg p_{d,a}) \ \wedge \ (p_{a,b} \Rightarrow p_{d,c})$$

$$\wedge \ p_{a,a} \wedge p_{b,b} \wedge p_{c,c} \wedge p_{d,d} \wedge \ (p_{a,b} \Leftrightarrow p_{b,a}) \wedge (p_{a,c} \Leftrightarrow p_{c,a}) \wedge (p_{a,d} \Leftrightarrow p_{d,a}) \wedge \cdots$$

$$\wedge \ ((p_{a,b} \wedge p_{b,c}) \Rightarrow p_{a,c}) \wedge ((p_{a,c} \wedge p_{c,d}) \Rightarrow p_{a,d}) \wedge \cdots$$

The resulting propositional formula is equisatisfiable with the original T_{EUF}-formula

Note: Not all the transitivity cases are needed

Eager Approach for SMT – Example

Rename f_b as c and f_a as d:

$$(f_b \doteq a \ \vee \ f_a \not\doteq a) \ \wedge \ (a \doteq b \Rightarrow f_a \doteq f_b)$$

becomes

$$(c \doteq a \ \vee \ d \not\doteq a) \ \wedge \ (a \doteq b \Rightarrow d \doteq c)$$

Step 2: Eliminate all equalities

- replace each pair of constants x, y with a unique propositional variable $p_{x,y}$
- add facts about reflexivity, symmetry, transitivity

$$\begin{gathered}(p_{c,a} \ \vee \ \neg p_{d,a}) \ \wedge \ (p_{a,b} \Rightarrow p_{d,c}) \\ \wedge \ p_{a,a} \wedge p_{b,b} \wedge p_{c,c} \wedge p_{d,d} \wedge \ (p_{a,b} \Leftrightarrow p_{b,a}) \wedge (p_{a,c} \Leftrightarrow p_{c,a}) \wedge (p_{a,d} \Leftrightarrow p_{d,a}) \wedge \cdots \\ \wedge \ ((p_{a,b} \wedge p_{b,c}) \Rightarrow p_{a,c}) \wedge ((p_{a,c} \wedge p_{c,d}) \Rightarrow p_{a,d}) \wedge \cdots\end{gathered}$$

The resulting propositional formula is equisatisfiable with the original T_{EUF}-formula

Note: Not all the transitivity cases are needed

Eager Approach for SMT – Example

Rename f_b as c and f_a as d:

$$(f_b \doteq a \ \vee \ f_a \not\doteq a) \ \wedge \ (a \doteq b \Rightarrow f_a \doteq f_b)$$

becomes

$$(c \doteq a \ \vee \ d \not\doteq a) \ \wedge \ (a \doteq b \Rightarrow d \doteq c)$$

Step 2: Eliminate all equalities

- replace each pair of constants x, y with a unique propositional variable $p_{x,y}$
- add facts about reflexivity, symmetry, transitivity

$$\begin{gathered}(p_{c,a} \ \vee \ \neg p_{d,a}) \ \wedge \ (p_{a,b} \Rightarrow p_{d,c}) \\ \wedge \ p_{a,a} \wedge p_{b,b} \wedge p_{c,c} \wedge p_{d,d} \wedge \ (p_{a,b} \Leftrightarrow p_{b,a}) \wedge (p_{a,c} \Leftrightarrow p_{c,a}) \wedge (p_{a,d} \Leftrightarrow p_{d,a}) \wedge \cdots \\ \wedge ((p_{a,b} \wedge p_{b,c}) \Rightarrow p_{a,c}) \wedge ((p_{a,c} \wedge p_{c,d}) \Rightarrow p_{a,d}) \wedge \cdots\end{gathered}$$

The resulting propositional formula is equisatisfiable with the original T_{EUF}-formula

Note: Not all the transitivity cases are needed

Discussion: eager vs. lazy approach

Eager

- translate into an equisatisfiable propositional formula
- feed it to any SAT solver

Lazy

- abstract the input formula to a propositional one
- feed it to a (CDCL-based) SAT solver
- use a theory decision procedure to refine the formula and guide the SAT solver

What are the pros and cons of the two approaches?

Discussion: eager vs. lazy approach

Eager

- translate into an equisatisfiable propositional formula
- feed it to any SAT solver

Lazy

- abstract the input formula to a propositional one
- feed it to a (CDCL-based) SAT solver
- use a theory decision procedure to refine the formula and guide the SAT solver

What are the pros and cons of the two approaches?

Pros and cons: eager vs. lazy approach

Eager

- Can always use the best SAT solver off the shelf
- Requires care in encoding
- Tends not to scale well

Lazy

- Theory-specific reasoning
- Designing new theory solvers can be challenging
- Might require extension of a SAT solver for more efficiency interplay with theory solver
- Scales much better

Lazy Approach – Enhancements

Several enhancements are possible to increase efficiency:

- Check $\mathcal{T}$-satisfiability only of full propositional model

  Check $\mathcal{T}$-satisfiability of partial assignment M as it grows

- If M is $\mathcal{T}$-unsatisfiable, add $\neg M$ as a clause

  If M is $\mathcal{T}$-unsatisfiable, identify a $\mathcal{T}$-unsatisfiable subset M_0 of M and add $\neg M_0$ as a clause

- If M is $\mathcal{T}$-unsatisfiable, add clause and restart

  If M is $\mathcal{T}$-unsatisfiable, backtrack to some point where the assignment was still $\mathcal{T}$-satisfiable

Lazy Approach – Enhancements

Several enhancements are possible to increase efficiency:

- Check $\mathcal{T}$-satisfiability only of full propositional model

  Check $\mathcal{T}$-satisfiability of partial assignment M as it grows

- If M is $\mathcal{T}$-unsatisfiable, add $\neg M$ as a clause

  If M is $\mathcal{T}$-unsatisfiable, identify a $\mathcal{T}$-unsatisfiable subset M_0 of M and add $\neg M_0$ as a clause

- If M is $\mathcal{T}$-unsatisfiable, add clause and restart

  If M is $\mathcal{T}$-unsatisfiable, backtrack to some point where the assignment was still $\mathcal{T}$-satisfiable

Lazy Approach – Enhancements

Several enhancements are possible to increase efficiency:

- Check $\mathcal{T}$-satisfiability only of full propositional model

  Check $\mathcal{T}$-satisfiability of partial assignment M as it grows

- If M is $\mathcal{T}$-unsatisfiable, add $\neg M$ as a clause

  If M is $\mathcal{T}$-unsatisfiable, identify a $\mathcal{T}$-unsatisfiable subset M_0 of M and add $\neg M_0$ as a clause

- If M is $\mathcal{T}$-unsatisfiable, add clause and restart

  If M is $\mathcal{T}$-unsatisfiable, backtrack to some point where the assignment was still $\mathcal{T}$-satisfiable

Lazy Approach – Enhancements

Several enhancements are possible to increase efficiency:

- Check $\mathcal{T}$-satisfiability only of full propositional model

  Check $\mathcal{T}$-satisfiability of partial assignment M as it grows

- If M is $\mathcal{T}$-unsatisfiable, add $\neg M$ as a clause

  If M is $\mathcal{T}$-unsatisfiable, identify a $\mathcal{T}$-unsatisfiable subset M_0 of M and add $\neg M_0$ as a clause

- If M is $\mathcal{T}$-unsatisfiable, add clause and restart

  If M is $\mathcal{T}$-unsatisfiable, backtrack to some point where the assignment was still $\mathcal{T}$-satisfiable

Lazy Approach – Enhancements

Several enhancements are possible to increase efficiency:

- Check $\mathcal{T}$-satisfiability only of full propositional model

  Check $\mathcal{T}$-satisfiability of partial assignment M as it grows

- If M is $\mathcal{T}$-unsatisfiable, add $\neg M$ as a clause

  If M is $\mathcal{T}$-unsatisfiable, identify a $\mathcal{T}$-unsatisfiable subset M_0 of M and add $\neg M_0$ as a clause

- If M is $\mathcal{T}$-unsatisfiable, add clause and restart

  If M is $\mathcal{T}$-unsatisfiable, backtrack to some point where the assignment was still $\mathcal{T}$-satisfiable

Lazy Approach – Enhancements

Several enhancements are possible to increase efficiency:

- Check $\mathcal{T}$-satisfiability only of full propositional model

  Check $\mathcal{T}$-satisfiability of partial assignment M as it grows

- If M is $\mathcal{T}$-unsatisfiable, add $\neg M$ as a clause

  If M is $\mathcal{T}$-unsatisfiable, identify a $\mathcal{T}$-unsatisfiable subset M_0 of M and add $\neg M_0$ as a clause

- If M is $\mathcal{T}$-unsatisfiable, add clause and restart

  If M is $\mathcal{T}$-unsatisfiable, backtrack to some point where the assignment was still $\mathcal{T}$-satisfiable

Lazy Approach – Main Benefits

Every tool does what it is good at:

- SAT solver takes care of Boolean information
- Theory solver takes care of theory information

The theory solver works only with conjunctions of literals

Modular approach:

- SAT and theory solvers communicate via a simple API
- SMT for a new theory only requires new theory solver
- An off-the-shelf SAT solver can be embedded in a lazy SMT system with low effort

Lazy Approach – Main Benefits

Every tool does what it is good at:

- SAT solver takes care of Boolean information
- Theory solver takes care of theory information

The theory solver works only with conjunctions of literals

Modular approach:

- SAT and theory solvers communicate via a simple API
- SMT for a new theory only requires new theory solver
- An off-the-shelf SAT solver can be embedded in a lazy SMT system with low effort

Lazy Approach – Main Benefits

Every tool does what it is good at:

- SAT solver takes care of Boolean information
- Theory solver takes care of theory information

The theory solver works only with conjunctions of literals

Modular approach:

- SAT and theory solvers communicate via a simple API
- SMT for a new theory only requires new theory solver
- An off-the-shelf SAT solver can be embedded in a lazy SMT system with low effort

An Abstract Framework for Lazy SMT

Several variants and enhancements of lazy SMT solvers exist

They can be modeled a satisfiability proof system like those for Abstract DPLL and Abstract CDCL

Review: Abstract DPLL

States:

$$\textsc{unsat} \qquad \langle M, \Delta \rangle$$

where

- M is a *sequence of literals* and *decision points* ($\bullet$) denoting a partial variable assignment
- Δ is a *set of clauses* denoting a CNF formula

Review: Abstract DPLL

States:

$$\textsc{unsat} \qquad \langle M, \Delta \rangle$$

where

- M is a *sequence of literals* and *decision points* ($\bullet$) denoting a partial variable assignment
- Δ is a *set of clauses* denoting a CNF formula

Note: When convenient, we treat M as a set

Provided M contains no complementary literals it determines the assignment

$$v_M(p) = \begin{cases} \text{true} & \text{if } p \in M \\ \text{false} & \text{if } \neg p \in M \\ \text{undef} & \text{otherwise} \end{cases}$$

Review: Abstract DPLL

States:

$$\textsf{UNSAT} \qquad \langle M, \Delta \rangle$$

where

- M is a *sequence of literals* and *decision points* ($\bullet$) denoting a partial variable assignment
- Δ is a *set of clauses* denoting a CNF formula

Notation: If $M = M_0 \bullet M_1 \bullet \cdots \bullet M_n$ where each M_i contains no decision points

- M_i is *decision level i* of M
- $M^{[i]}$ denotes the subsequence $M_0 \bullet \cdots \bullet M_i$, from decision level 0 through decision level i

Review: Abstract DPLL

States:

UNSAT $\quad \langle M, \Delta \rangle$

Initial state:

- $\langle \epsilon, \Delta_0 \rangle$ where ϵ is the empty assignment and Δ_0 is to be checked for satisfiability

Review: Abstract DPLL

States:

$\textsc{unsat}$ $\quad\quad$ $\langle M, \Delta \rangle$

Initial state:

- $\langle \epsilon, \Delta_0 \rangle$ where ϵ is the empty assignment and Δ_0 is to be checked for satisfiability

Expected final states:

- $\textsc{unsat}$ if Δ_0 is unsatisfiable
- $\langle M, \Delta_n \rangle$ otherwise, where Δ_n is equisatisfiable with Δ_0 and satisfied by M

Review: Abstract CDCL

States:

$$\text{UNSAT} \qquad \langle M, \Delta, C \rangle$$

where

- M and Δ are as in Abstract DPLL
- C is either $\texttt{no}$ or a *conflict clause*

Initial state:

- $\langle \epsilon, \Delta_0, \texttt{no} \rangle$, where Δ_0 is to be checked for satisfiability

Expected final states:

- UNSAT if Δ_0 is unsatisfiable
- $\langle M, \Delta_n, \texttt{no} \rangle$ otherwise, where Δ_n is equisatisfiable with Δ_0 and satisfied by M

Review: Abstract CDCL

States:

$$\text{UNSAT} \qquad \langle M, \Delta, C \rangle$$

where

- M and Δ are as in Abstract DPLL
- C is either $\texttt{no}$ or a *conflict clause*

Initial state:

- $\langle \epsilon, \Delta_0, \texttt{no} \rangle$, where Δ_0 is to be checked for satisfiability

Expected final states:

- UNSAT if Δ_0 is unsatisfiable
- $\langle M, \Delta_n, \texttt{no} \rangle$ otherwise, where Δ_n is equisatisfiable with Δ_0 and satisfied by M

Review: Abstract CDCL

States:

$$\textsc{unsat} \qquad \langle M, \Delta, C \rangle$$

where

- M and Δ are as in Abstract DPLL
- C is either $\mathtt{no}$ or a *conflict clause*

Initial state:

- $\langle \epsilon, \Delta_0, \mathtt{no} \rangle$, where Δ_0 is to be checked for satisfiability

Expected final states:

- $\textsc{unsat}$ if Δ_0 is unsatisfiable
- $\langle M, \Delta_n, \mathtt{no} \rangle$ otherwise, where Δ_n is equisatisfiable with Δ_0 and satisfied by M

Review: CDCL proof rules

$$\textsc{Propagate}\ \frac{\{l_1,\ldots,l_n,l\}\in\Delta \qquad \bar{l}_1,\ldots,\bar{l}_n\in \mathsf{M} \qquad l,\bar{l}\notin \mathsf{M}}{\mathsf{M} := \mathsf{M}\, l}$$

$$\textsc{Decide}\ \frac{l\in \mathtt{Lits}(\Delta) \qquad l,\bar{l}\notin \mathsf{M}}{\mathsf{M} := \mathsf{M}\bullet l}$$

$$\textsc{Explain}\ \frac{\mathsf{C}=\{l\}\cup C' \quad \{l_1,\ldots,l_n,\bar{l}\}\in\Delta \quad \bar{l}_1,\ldots,\bar{l}_n,\bar{l}\in \mathsf{M} \quad \bar{l}_1,\ldots,\bar{l}_n \prec_{\mathsf{M}} \bar{l}}{\mathsf{C} := \{l_1,\ldots,l_n\}\cup C'}$$

$$\textsc{Fail}\ \frac{\mathsf{C}\neq \mathtt{no} \qquad \bullet\notin \mathsf{M}}{\mathsf{UNSAT}}$$

$$\textsc{Backjump}\ \frac{\mathsf{C}=D \quad D=\{l_1,\ldots,l_n,l\} \quad \mathtt{lev}(\bar{l}_1),\ldots,\mathtt{lev}(\bar{l}_n)\leq i<\mathtt{lev}(\bar{l})}{\mathsf{M} := \mathsf{M}^{[i]}\, l \qquad \mathsf{C} := \mathtt{no} \qquad \Delta := \Delta\cup\{D\}}$$

$$\textsc{Restart}\ \frac{}{\mathsf{M} := \mathsf{M}^{[0]} \qquad \mathsf{C} := \mathtt{no}}$$

$$\textsc{Conflict}\ \frac{\mathsf{C}=\mathtt{no} \qquad \{l_1,\ldots,l_n\}\in\Delta \qquad \bar{l}_1,\ldots,\bar{l}_n\in \mathsf{M}}{\mathsf{C} := \{l_1,\ldots,l_n\}}$$

$$\textsc{Learn}\ \frac{D \text{ is a clause} \qquad \Delta\models D \qquad D\notin\Delta}{\Delta := \Delta\cup\{D\}}$$

$$\textsc{Forget}\ \frac{\mathsf{C}=\mathtt{no} \qquad \Delta=\Delta'\cup\{C\} \qquad \Delta'\models C}{\Delta := \Delta'}$$

We are going to extend this abstract framework to lazy SMT

Review: CDCL proof rules

$$\textsc{Propagate}\ \frac{\{l_1,\ldots,l_n,l\}\in\Delta \qquad \bar{l}_1,\ldots,\bar{l}_n\in \mathsf{M} \qquad l,\bar{l}\notin \mathsf{M}}{\mathsf{M} := \mathsf{M}\, l}$$

$$\textsc{Decide}\ \frac{l\in \mathtt{Lits}(\Delta) \qquad l,\bar{l}\notin \mathsf{M}}{\mathsf{M} := \mathsf{M}\bullet l}$$

$$\textsc{Explain}\ \frac{\mathsf{C}=\{l\}\cup C' \quad \{l_1,\ldots,l_n,\bar{l}\}\in\Delta \quad \bar{l}_1,\ldots,\bar{l}_n,\bar{l}\in \mathsf{M} \quad \bar{l}_1,\ldots,\bar{l}_n \prec_{\mathsf{M}} \bar{l}}{\mathsf{C} := \{l_1,\ldots,l_n\}\cup C'}$$

$$\textsc{Fail}\ \frac{\mathsf{C}\neq \mathtt{no} \qquad \bullet\notin \mathsf{M}}{\mathsf{UNSAT}}$$

$$\textsc{Backjump}\ \frac{\mathsf{C}=D \quad D=\{l_1,\ldots,l_n,l\} \quad \mathtt{lev}(\bar{l}_1),\ldots,\mathtt{lev}(\bar{l}_n)\leq i<\mathtt{lev}(\bar{l})}{\mathsf{M} := \mathsf{M}^{[i]}\, l \qquad \mathsf{C} := \mathtt{no} \qquad \Delta := \Delta\cup\{D\}}$$

$$\textsc{Restart}\ \frac{}{\mathsf{M} := \mathsf{M}^{[0]} \qquad C := \mathtt{no}}$$

$$\textsc{Conflict}\ \frac{\mathsf{C}=\mathtt{no} \qquad \{l_1,\ldots,l_n\}\in\Delta \qquad \bar{l}_1,\ldots,\bar{l}_n\in \mathsf{M}}{\mathsf{C} := \{l_1,\ldots,l_n\}}$$

$$\textsc{Learn}\ \frac{D \text{ is a clause} \qquad \Delta\models D \qquad D\notin\Delta}{\Delta := \Delta\cup\{D\}}$$

$$\textsc{Forget}\ \frac{\mathsf{C}=\mathtt{no} \qquad \Delta=\Delta'\cup\{C\} \qquad \Delta'\models C}{\Delta := \Delta'}$$

We are going to extend this abstract framework to lazy SMT

From SAT to SMT

Same state components and transitions as in Abstract CDCL except that

- Δ contains quantifier-free clauses in some theory $\mathcal{T}$
- M is a sequence of theory literals (i.e., atomic formulas or their negations) and decision points
- CDCL Rules operate on the Boolean skeleton of Δ,
  given by a mapping from theory literals to propositional literals
- The proofs system is augmented with SMT-specific rules based on $\models_{\mathcal{T}}$:
  $\mathcal{T}$-**Conflict**, $\mathcal{T}$-**Propagate** and $\mathcal{T}$-**Explain**
- We assume an oracle, the theory solver, for $\models_{\mathcal{T}}$ over theory literals
- Invariant: either $C \neq \mathtt{no}$ or $\Delta \models_{\mathcal{T}} C$ and $M \models_p \neg C$ (with $\models_p$ propositional entailment)

From SAT to SMT

Same state components and transitions as in Abstract CDCL except that

- Δ contains quantifier-free clauses in some theory $\mathcal{T}$

- M is a sequence of theory literals (i.e., atomic formulas or their negations) and decision points

- CDCL Rules operate on the Boolean skeleton of Δ,
  given by a mapping from theory literals to propositional literals

- The proofs system is augmented with SMT-specific rules based on $\models_{\mathcal{T}}$:
  $\mathcal{T}$-**Conflict**, $\mathcal{T}$-**Propagate** and $\mathcal{T}$-**Explain**

- We assume an oracle, the theory solver, for $\models_{\mathcal{T}}$ over theory literals

- Invariant: either $C \neq \mathrm{no}$ or $\Delta \models_{\mathcal{T}} C$ and $M \models_p \neg C$ (with $\models_p$ propositional entailment)

From SAT to SMT

Same state components and transitions as in Abstract CDCL except that

- Δ contains quantifier-free clauses in some theory $\mathcal{T}$
- M is a sequence of theory literals (i.e., atomic formulas or their negations) and decision points
- CDCL Rules operate on the Boolean skeleton of Δ,
  given by a mapping from theory literals to propositional literals
- The proofs system is augmented with SMT-specific rules based on $\models_{\mathcal{T}}$:
  $\mathcal{T}$-**Conflict**, $\mathcal{T}$-**Propagate** and $\mathcal{T}$-**Explain**
- We assume an oracle, the theory solver, for $\models_{\mathcal{T}}$ over theory literals
- Invariant: either $C \neq \mathrm{no}$ or $\Delta \models_{\mathcal{T}} C$ and $M \models_p \neg C$ (with $\models_p$ propositional entailment)

From SAT to SMT

Same state components and transitions as in Abstract CDCL except that

- Δ contains quantifier-free clauses in some theory $\mathcal{T}$
- M is a sequence of theory literals (i.e., atomic formulas or their negations) and decision points
- CDCL Rules operate on the Boolean skeleton of Δ,
  given by a mapping from theory literals to propositional literals
- The proofs system is augmented with SMT-specific rules based on $\models_{\mathcal{T}}$:
  $\mathcal{T}$-**Conflict**, $\mathcal{T}$-**Propagate** and $\mathcal{T}$-**Explain**
- We assume an oracle, the theory solver, for $\models_{\mathcal{T}}$ over theory literals
- Invariant: either $\mathsf{C} \neq \mathsf{no}$ or $\Delta \models_{\mathcal{T}} \mathsf{C}$ and $\mathsf{M} \models_{p} \neg\mathsf{C}$ (with $\models_{p}$ propositional entailment)

From SAT to SMT

Same state components and transitions as in Abstract CDCL except that

- Δ contains quantifier-free clauses in some theory $\mathcal{T}$
- M is a sequence of theory literals (i.e., atomic formulas or their negations) and decision points
- CDCL Rules operate on the Boolean skeleton of Δ,
  given by a mapping from theory literals to propositional literals
- The proofs system is augmented with SMT-specific rules based on $\models_{\mathcal{T}}$:
  $\mathcal{T}$-**Conflict**, $\mathcal{T}$-**Propagate** and $\mathcal{T}$-**Explain**
- We assume an oracle, the theory solver, for $\models_{\mathcal{T}}$ over theory literals
- Invariant: either $C \neq \text{no}$ or $\Delta \models_{\mathcal{T}} C$ and $M \models_p \neg C$ (with $\models_p$ propositional entailment)

From SAT to SMT

Same state components and transitions as in Abstract CDCL except that

- Δ contains quantifier-free clauses in some theory $\mathcal{T}$
- M is a sequence of theory literals (i.e., atomic formulas or their negations) and decision points
- CDCL Rules operate on the Boolean skeleton of Δ,
  given by a mapping from theory literals to propositional literals
- The proofs system is augmented with SMT-specific rules based on $\models_{\mathcal{T}}$:
  $\mathcal{T}$-**Conflict**, $\mathcal{T}$-**Propagate** and $\mathcal{T}$-**Explain**
- We assume an oracle, the theory solver, for $\models_{\mathcal{T}}$ over theory literals
- Invariant: either $C \neq \mathtt{no}$ or $\Delta \models_{\mathcal{T}} C$ and $M \models_p \neg C$ (with $\models_p$ propositional entailment)

From SAT to SMT

Same state components and transitions as in Abstract CDCL except that

- Δ contains quantifier-free clauses in some theory $\mathcal{T}$
- M is a sequence of theory literals (i.e., atomic formulas or their negations) and decision points
- CDCL Rules operate on the Boolean skeleton of Δ,
  given by a mapping from theory literals to propositional literals
- The proofs system is augmented with SMT-specific rules based on $\models_{\mathcal{T}}$:
  $\mathcal{T}$-**Conflict**, $\mathcal{T}$-**Propagate** and $\mathcal{T}$-**Explain**
- We assume an oracle, the theory solver, for $\models_{\mathcal{T}}$ over theory literals
- Invariant: either $\mathsf{C} \neq \mathtt{no}$ or $\Delta \models_{\mathcal{T}} \mathsf{C}$ and $\mathsf{M} \models_{\mathrm{p}} \neg\mathsf{C}$ (with $\models_{\mathrm{p}}$ propositional entailment)

SMT-level Rules

At SAT level:

$$\textsc{Conflict}\ \frac{\mathsf{C} = \texttt{no} \qquad \{l_1, \ldots, l_n\} \in \Delta \qquad \overline{l}_1, \ldots, \overline{l}_n \in \mathsf{M}}{\mathsf{C} := \{l_1, \ldots, l_n\}}$$

At SMT level:

$$\mathcal{T}\textsc{-Conflict}\ \frac{\mathsf{C} = \texttt{no} \qquad \overline{l}_1 \wedge \cdots \wedge \overline{l}_n \models_{\mathcal{T}} \bot \qquad \overline{l}_1, \ldots, \overline{l}_n \in \mathsf{M}}{\mathsf{C} := \{l_1, \ldots, l_n\}}$$

If a set of literals in M are unsatisfiable in $\mathcal{T}$, make their negation a conflict clause

SMT-level Rules

At SAT level:

$$\textsc{Propagate}\ \frac{\{l_1, \ldots, l_n, l\} \in \Delta \qquad \overline{l}_1, \ldots, \overline{l}_n \in \mathsf{M} \qquad l, \overline{l} \notin \mathsf{M}}{\mathsf{M} := \mathsf{M}\ l}$$

At SMT level:

$$\mathcal{T}\text{-}\textsc{Propagate}\ \frac{l \in \mathtt{Lits}(\Delta) \qquad \mathsf{M} \models_{\mathcal{T}} l \qquad l, \overline{l} \notin \mathsf{M}}{\mathsf{M} := \mathsf{M}\ l}$$

If M entails some literal l in $\mathcal{T}$, extend it with l

SMT-level Rules

At SAT level:

$$\textsc{Explain}\ \frac{\mathsf{C} = \{l\} \cup C' \quad \{l_1, \ldots, l_n, \overline{l}\} \in \Delta \quad \overline{l}_1, \ldots, \overline{l}_n, \overline{l} \in \mathsf{M} \quad \overline{l}_1, \ldots, \overline{l}_n \prec_{\mathsf{M}} \overline{l}}{\mathsf{C} := \{l_1, \ldots, l_n\} \cup C'}$$

At SMT level:

$$\mathcal{T}\text{-}\textsc{Explain}\ \frac{\mathsf{C} = \{l\} \cup D \quad \overline{l}_1 \wedge \cdots \wedge \overline{l}_n \models_{\mathcal{T}} \overline{l} \quad \overline{l}_1, \ldots, \overline{l}_n \prec_{\mathsf{M}} \overline{l}}{\mathsf{C} := \{l_1, \cdots, l_n\} \cup D}$$

If the complement $\overline{l}$ of a literal in the conflict clause is entailed in $\mathcal{T}$ by some literals $\overline{l}_1, \ldots, \overline{l}_n$ at lower decision levels, derive a new conflict clause by resolution with $\{l_1, \ldots, l_n, \overline{l}\}$

CDCL Modulo Theories proof rules

$$\textsc{Decide}\ \frac{l \in \mathtt{Lits}(\Delta) \qquad l, \bar{l} \notin M}{M := M \bullet l}$$

$$\textsc{Fail}\ \frac{C \neq \mathtt{no} \qquad \bullet \notin M}{\mathsf{UNSAT}}$$

$$\textsc{Restart}\ \frac{}{M := M^{[0]} \qquad C := \mathtt{no}}$$

$$\textsc{Learn}\ \frac{D \text{ is a clause} \qquad \Delta \models D \qquad D \notin \Delta}{\Delta := \Delta \cup \{D\}}$$

$$\textsc{Forget}\ \frac{C = \mathtt{no} \qquad \Delta = \Delta' \cup \{C\} \qquad \Delta' \models C}{\Delta := \Delta'}$$

$$\mathcal{T}\text{-}\textsc{Propagate}\ \frac{l \in \mathtt{Lits}(\Delta) \qquad M \models_{\mathcal{T}} l \qquad l, \bar{l} \notin M}{M := M\, l}$$

$$\mathcal{T}\text{-}\textsc{Conflict}\ \frac{C = \mathtt{no} \qquad \bar{l}_1 \wedge \cdots \wedge \bar{l}_n \models_{\mathcal{T}} \bot \qquad \bar{l}_1, \ldots, \bar{l}_n \in M}{C := \{l_1, \ldots, l_n\}}$$

$$\mathcal{T}\text{-}\textsc{Explain}\ \frac{C = \{l\} \cup D \qquad \bar{l}_1 \wedge \cdots \wedge \bar{l}_n \models_{\mathcal{T}} \bar{l} \qquad \bar{l}_1, \ldots, \bar{l}_n \prec_M \bar{l}}{C := \{l_1, \cdots, l_n\} \cup D}$$

$$\textsc{Propagate}\ \frac{\{l_1, \ldots, l_n, l\} \in \Delta \qquad \bar{l}_1, \ldots, \bar{l}_n \in M \qquad l, \bar{l} \notin M}{M := M\, l}$$

$$\textsc{Explain}\ \frac{C = \{l\} \cup C' \quad \{l_1, \ldots, l_n, \bar{l}\} \in \Delta \quad \bar{l}_1, \ldots, \bar{l}_n, \bar{l} \in M \quad \bar{l}_1, \ldots, \bar{l}_n \prec_M \bar{l}}{C := \{l_1, \ldots, l_n\} \cup C'}$$

$$\textsc{Backjump}\ \frac{C = D \quad D = \{l_1, \ldots, l_n, l\} \quad \mathtt{lev}(\bar{l}_1), \ldots, \mathtt{lev}(\bar{l}_n) \leq i < \mathtt{lev}(\bar{l})}{M := M^{[i]} l \qquad C := \mathtt{no} \qquad \Delta := \Delta \cup \{D\}}$$

$$\textsc{Conflict}\ \frac{C = \mathtt{no} \qquad \{l_1, \ldots, l_n\} \in \Delta \qquad \bar{l}_1, \ldots, \bar{l}_n \in M}{C := \{l_1, \ldots, l_n\}}$$

Modeling the Very Lazy Theory Approach

$\mathcal{T}$-**Conflict** is enough to model the naive integration of SAT solvers and theory solvers seen in the earlier EUF example

$$\underbrace{g(a) \doteq c}_{1} \;\wedge\; \underbrace{f(g(a)) \neq f(c)}_{\overline{2}} \vee \underbrace{g(a) \doteq d}_{3} \;\wedge\; \underbrace{c \neq d}_{\overline{4}}$$

M	Δ	C	rule
	$1,\ \overline{2} \vee 3,\ \overline{4}$	no	
$1\ \overline{4}$	$1,\ \overline{2} \vee 3,\ \overline{4}$	no	by Propagate$^+$
$1\ \overline{4} \bullet \overline{2}$	$1,\ \overline{2} \vee 3,\ \overline{4}$	no	by Decide
$1\ \overline{4} \bullet \overline{2}$	$1,\ \overline{2} \vee 3,\ \overline{4}$	$\overline{1} \vee 2 \vee 4$	by $\mathcal{T}$-Conflict
$1\ \overline{4} \bullet \overline{2}$	$1,\ \overline{2} \vee 3,\ \overline{4},\ \overline{1} \vee 2 \vee 4$	$\overline{1} \vee 2 \vee 4$	by Learn
$1\ \overline{4}$	$1,\ \overline{2} \vee 3,\ \overline{4},\ \overline{1} \vee 2 \vee 4$	no	by Restart
$1\ \overline{4}\ 2\ 3$	$1,\ \overline{2} \vee 3,\ \overline{4},\ \overline{1} \vee 2 \vee 4$	no	by Propagate$^+$
$1\ \overline{4}\ 2\ 3$	$1,\ \overline{2} \vee 3,\ \overline{4},\ \overline{1} \vee 2 \vee 4$	$\overline{1} \vee \overline{3} \vee 4$	by $\mathcal{T}$-Conflict
$1\ \overline{4}\ 2\ 3$	$1,\ \overline{2} \vee 3,\ \overline{4},\ \overline{1} \vee 2 \vee 4,\ \overline{1} \vee \overline{3} \vee 4$	no	by Learn
	$\vdots$		
	UNSAT		by Fail

Modeling the Very Lazy Theory Approach

$$\underbrace{g(a) \doteq c}_{1} \quad \wedge \quad \underbrace{f(g(a)) \not\doteq f(c)}_{\bar{2}} \vee \underbrace{g(a) \doteq d}_{3} \quad \wedge \quad \underbrace{c \not\doteq d}_{\bar{4}}$$

M	Δ	C	rule
	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	
$1\ \bar{4}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by Propagate$^+$
$1\ \bar{4} \bullet \bar{2}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by Decide
$1\ \bar{4} \bullet \bar{2}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	$\bar{1} \vee 2 \vee 4$	by $\mathcal{T}$-Conflict
$1\ \bar{4} \bullet \bar{2}$	$1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4$	$\bar{1} \vee 2 \vee 4$	by Learn
$1\ \bar{4}$	$1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4$	no	by Restart
$1\ \bar{4}\ 2\ 3$	$1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4$	no	by Propagate$^+$
$1\ \bar{4}\ 2\ 3$	$1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4$	$\bar{1} \vee \bar{3} \vee 4$	by $\mathcal{T}$-Conflict
$1\ \bar{4}\ 2\ 3$	$1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4,\ \bar{1} \vee \bar{3} \vee 4$	no	by Learn
	⋮		
	UNSAT		by Fail

Modeling the Very Lazy Theory Approach

$$\underbrace{g(a) \doteq c}_{1} \quad \wedge \quad \underbrace{f(g(a)) \not\doteq f(c)}_{\bar{2}} \vee \underbrace{g(a) \doteq d}_{3} \quad \wedge \quad \underbrace{c \not\doteq d}_{\bar{4}}$$

M	Δ	C	rule
	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	
$1\ \bar{4}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by PROPAGATE$^+$
$1\ \bar{4} \bullet \bar{2}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by DECIDE
$1\ \bar{4} \bullet \bar{2}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	$\bar{1} \vee 2 \vee 4$	by $\mathcal{T}$-CONFLICT
$1\ \bar{4} \bullet \bar{2}$	$1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4$	$\bar{1} \vee 2 \vee 4$	by LEARN
$1\ \bar{4}$	$1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4$	no	by RESTART
$1\ \bar{4}\ 2\ 3$	$1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4$	no	by PROPAGATE$^+$
$1\ \bar{4}\ 2\ 3$	$1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4$	$\bar{1} \vee \bar{3} \vee 4$	by $\mathcal{T}$-CONFLICT
$1\ \bar{4}\ 2\ 3$	$1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4,\ \bar{1} \vee \bar{3} \vee 4$	no	by LEARN
	⋮		
	UNSAT		by FAIL

Modeling the Very Lazy Theory Approach

$$\underbrace{g(a) \doteq c}_{1} \quad \wedge \quad \underbrace{f(g(a)) \not\doteq f(c)}_{\overline{2}} \vee \underbrace{g(a) \doteq d}_{3} \quad \wedge \quad \underbrace{c \not\doteq d}_{\overline{4}}$$

M	Δ	C	rule
	$1,\ \overline{2} \vee 3,\ \overline{4}$	no	
$1\ \overline{4}$	$1,\ \overline{2} \vee 3,\ \overline{4}$	no	by PROPAGATE^{+}
$1\ \overline{4} \bullet \overline{2}$	$1,\ \overline{2} \vee 3,\ \overline{4}$	no	by DECIDE
$1\ \overline{4} \bullet \overline{2}$	$1,\ \overline{2} \vee 3,\ \overline{4}$	$\overline{1} \vee 2 \vee 4$	by $\mathcal{T}$-CONFLICT
$1\ \overline{4} \bullet \overline{2}$	$1,\ \overline{2} \vee 3,\ \overline{4},\ \overline{1} \vee 2 \vee 4$	$\overline{1} \vee 2 \vee 4$	by LEARN
$1\ \overline{4}$	$1,\ \overline{2} \vee 3,\ \overline{4},\ \overline{1} \vee 2 \vee 4$	no	by RESTART
$1\ \overline{4}\ 2\ 3$	$1,\ \overline{2} \vee 3,\ \overline{4},\ \overline{1} \vee 2 \vee 4$	no	by PROPAGATE^{+}
$1\ \overline{4}\ 2\ 3$	$1,\ \overline{2} \vee 3,\ \overline{4},\ \overline{1} \vee 2 \vee 4$	$\overline{1} \vee \overline{3} \vee 4$	by $\mathcal{T}$-CONFLICT
$1\ \overline{4}\ 2\ 3$	$1,\ \overline{2} \vee 3,\ \overline{4},\ \overline{1} \vee 2 \vee 4,\ \overline{1} \vee \overline{3} \vee 4$	no	by LEARN
	⋮		
	UNSAT		by FAIL

Modeling the Very Lazy Theory Approach

$$\underbrace{g(a) \doteq c}_{1} \quad \wedge \quad \underbrace{f(g(a)) \not\doteq f(c)}_{\overline{2}} \vee \underbrace{g(a) \doteq d}_{3} \quad \wedge \quad \underbrace{c \not\doteq d}_{\overline{4}}$$

M	Δ	C	rule
	$1,\ \overline{2} \vee 3,\ \overline{4}$	no	
$1\ \overline{4}$	$1,\ \overline{2} \vee 3,\ \overline{4}$	no	by PROPAGATE$^+$
$1\ \overline{4} \bullet \overline{2}$	$1,\ \overline{2} \vee 3,\ \overline{4}$	no	by DECIDE
$1\ \overline{4} \bullet \overline{2}$	$1,\ \overline{2} \vee 3,\ \overline{4}$	$\overline{1} \vee 2 \vee 4$	by $\mathcal{T}$-CONFLICT
$1\ \overline{4} \bullet \overline{2}$	$1,\ \overline{2} \vee 3,\ \overline{4},\ \overline{1} \vee 2 \vee 4$	$\overline{1} \vee 2 \vee 4$	by LEARN
$1\ \overline{4}$	$1,\ \overline{2} \vee 3,\ \overline{4},\ \overline{1} \vee 2 \vee 4$	no	by RESTART
$1\ \overline{4}\ 2\ 3$	$1,\ \overline{2} \vee 3,\ \overline{4},\ \overline{1} \vee 2 \vee 4$	no	by PROPAGATE$^+$
$1\ \overline{4}\ 2\ 3$	$1,\ \overline{2} \vee 3,\ \overline{4},\ \overline{1} \vee 2 \vee 4$	$\overline{1} \vee \overline{3} \vee 4$	by $\mathcal{T}$-CONFLICT
$1\ \overline{4}\ 2\ 3$	$1,\ \overline{2} \vee 3,\ \overline{4},\ \overline{1} \vee 2 \vee 4,\ \overline{1} \vee \overline{3} \vee 4$	no	by LEARN
	⋮		
	UNSAT		by FAIL

Modeling the Very Lazy Theory Approach

$$\underbrace{g(a) \doteq c}_{1} \quad\wedge\quad \underbrace{f(g(a)) \not\doteq f(c)}_{\bar{2}} \vee \underbrace{g(a) \doteq d}_{3} \quad\wedge\quad \underbrace{c \not\doteq d}_{\bar{4}}$$

M	Δ	C	rule
	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	
$1\ \bar{4}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by **Propagate**$^+$
$1\ \bar{4} \bullet \bar{2}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by **Decide**
$1\ \bar{4} \bullet \bar{2}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	$\bar{1} \vee 2 \vee 4$	by $\mathcal{T}$-**Conflict**
$1\ \bar{4} \bullet \bar{2}$	$1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4$	$\bar{1} \vee 2 \vee 4$	by **Learn**
$1\ \bar{4}$	$1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4$	no	by **Restart**
$1\ \bar{4}\ \bar{2}\ 3$	$1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4$	no	by **Propagate**$^+$
$1\ \bar{4}\ \bar{2}\ 3$	$1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4$	$\bar{1} \vee \bar{3} \vee 4$	by $\mathcal{T}$-**Conflict**
$1\ \bar{4}\ \bar{2}\ 3$	$1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4,\ \bar{1} \vee \bar{3} \vee 4$	no	by **Learn**
	⋮		
	UNSAT		by **Fail**

Modeling the Very Lazy Theory Approach

$$\underbrace{g(a) \doteq c}_{1} \quad \wedge \quad \underbrace{f(g(a)) \not\doteq f(c)}_{\overline{2}} \vee \underbrace{g(a) \doteq d}_{3} \quad \wedge \quad \underbrace{c \not\doteq d}_{\overline{4}}$$

M	Δ	C	rule
	$1,\ \overline{2} \vee 3,\ \overline{4}$	no	
$1\ \overline{4}$	$1,\ \overline{2} \vee 3,\ \overline{4}$	no	by Propagate$^+$
$1\ \overline{4} \bullet \overline{2}$	$1,\ \overline{2} \vee 3,\ \overline{4}$	no	by Decide
$1\ \overline{4} \bullet \overline{2}$	$1,\ \overline{2} \vee 3,\ \overline{4}$	$\overline{1} \vee 2 \vee 4$	by $\mathcal{T}$-Conflict
$1\ \overline{4} \bullet \overline{2}$	$1,\ \overline{2} \vee 3,\ \overline{4},\ \overline{1} \vee 2 \vee 4$	$\overline{1} \vee 2 \vee 4$	by Learn
$1\ \overline{4}$	$1,\ \overline{2} \vee 3,\ \overline{4},\ \overline{1} \vee 2 \vee 4$	no	by Restart
$1\ \overline{4}\ 2\ 3$	$1,\ \overline{2} \vee 3,\ \overline{4},\ \overline{1} \vee 2 \vee 4$	no	by Propagate$^+$
$1\ \overline{4}\ 2\ 3$	$1,\ \overline{2} \vee 3,\ \overline{4},\ \overline{1} \vee 2 \vee 4$	$\overline{1} \vee \overline{3} \vee 4$	by $\mathcal{T}$-Conflict
$1\ \overline{4}\ 2\ 3$	$1,\ \overline{2} \vee 3,\ \overline{4},\ \overline{1} \vee 2 \vee 4,\ \overline{1} \vee \overline{3} \vee 4$	no	by Learn
	$\vdots$		
	UNSAT		by Fail

Modeling the Very Lazy Theory Approach

$$\underbrace{g(a) \doteq c}_{1} \quad \wedge \quad \underbrace{f(g(a)) \not\doteq f(c)}_{\bar{2}} \vee \underbrace{g(a) \doteq d}_{3} \quad \wedge \quad \underbrace{c \not\doteq d}_{\bar{4}}$$

M	Δ	C	rule
	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	
$1\ \bar{4}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by **Propagate**$^+$
$1\ \bar{4} \bullet \bar{2}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by **Decide**
$1\ \bar{4} \bullet \bar{2}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	$\bar{1} \vee 2 \vee 4$	by $\mathcal{T}$-**Conflict**
$1\ \bar{4} \bullet \bar{2}$	$1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4$	$\bar{1} \vee 2 \vee 4$	by **Learn**
$1\ \bar{4}$	$1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4$	no	by **Restart**
$1\ \bar{4}\ \bar{2}\ 3$	$1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4$	no	by **Propagate**$^+$
$1\ \bar{4}\ \bar{2}\ 3$	$1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4$	$\bar{1} \vee \bar{3} \vee 4$	by $\mathcal{T}$-**Conflict**
$1\ \bar{4}\ \bar{2}\ 3$	$1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4,\ \bar{1} \vee \bar{3} \vee 4$	no	by **Learn**
	⋮		
	UNSAT		by **Fail**

Modeling the Very Lazy Theory Approach

$$\underbrace{g(a) \doteq c}_{1} \quad \wedge \quad \underbrace{f(g(a)) \not\doteq f(c)}_{\overline{2}} \vee \underbrace{g(a) \doteq d}_{3} \quad \wedge \quad \underbrace{c \not\doteq d}_{\overline{4}}$$

M	Δ	C	rule
	$1,\ \overline{2} \vee 3,\ \overline{4}$	no	
$1\ \overline{4}$	$1,\ \overline{2} \vee 3,\ \overline{4}$	no	by PROPAGATE^{+}
$1\ \overline{4} \bullet \overline{2}$	$1,\ \overline{2} \vee 3,\ \overline{4}$	no	by DECIDE
$1\ \overline{4} \bullet \overline{2}$	$1,\ \overline{2} \vee 3,\ \overline{4}$	$\overline{1} \vee 2 \vee 4$	by $\mathcal{T}$-CONFLICT
$1\ \overline{4} \bullet \overline{2}$	$1,\ \overline{2} \vee 3,\ \overline{4},\ \overline{1} \vee 2 \vee 4$	$\overline{1} \vee 2 \vee 4$	by LEARN
$1\ \overline{4}$	$1,\ \overline{2} \vee 3,\ \overline{4},\ \overline{1} \vee 2 \vee 4$	no	by RESTART
$1\ \overline{4}\ 2\ 3$	$1,\ \overline{2} \vee 3,\ \overline{4},\ \overline{1} \vee 2 \vee 4$	no	by PROPAGATE^{+}
$1\ \overline{4}\ 2\ 3$	$1,\ \overline{2} \vee 3,\ \overline{4},\ \overline{1} \vee 2 \vee 4$	$\overline{1} \vee \overline{3} \vee 4$	by $\mathcal{T}$-CONFLICT
$1\ \overline{4}\ 2\ 3$	$1,\ \overline{2} \vee 3,\ \overline{4},\ \overline{1} \vee 2 \vee 4,\ \overline{1} \vee \overline{3} \vee 4$	no	by LEARN
	⋮		
	UNSAT		by FAIL

Modeling the Very Lazy Theory Approach

$$\underbrace{g(a) \doteq c}_{1} \quad \wedge \quad \underbrace{f(g(a)) \not\doteq f(c)}_{\bar{2}} \vee \underbrace{g(a) \doteq d}_{3} \quad \wedge \quad \underbrace{c \not\doteq d}_{\bar{4}}$$

M	Δ	C	rule
	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	
$1\ \bar{4}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by Propagate$^+$
$1\ \bar{4} \bullet \bar{2}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by Decide
$1\ \bar{4} \bullet \bar{2}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	$\bar{1} \vee 2 \vee 4$	by $\mathcal{T}$-Conflict
$1\ \bar{4} \bullet \bar{2}$	$1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4$	$\bar{1} \vee 2 \vee 4$	by Learn
$1\ \bar{4}$	$1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4$	no	by Restart
$1\ \bar{4}\ 2\ 3$	$1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4$	no	by Propagate$^+$
$1\ \bar{4}\ 2\ 3$	$1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4$	$\bar{1} \vee \bar{3} \vee 4$	by $\mathcal{T}$-Conflict
$1\ \bar{4}\ 2\ 3$	$1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4,\ \bar{1} \vee \bar{3} \vee 4$	no	by Learn
	⋮		
	UNSAT		by Fail

Modeling the Very Lazy Theory Approach

$$\underbrace{g(a) \doteq c}_{1} \quad\wedge\quad \underbrace{f(g(a)) \not\doteq f(c)}_{\bar{2}} \vee \underbrace{g(a) \doteq d}_{3} \quad\wedge\quad \underbrace{c \not\doteq d}_{\bar{4}}$$

M	Δ	C	rule
	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	
$1\ \bar{4}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by **Propagate**$^+$
$1\ \bar{4} \bullet \bar{2}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by **Decide**
$1\ \bar{4} \bullet \bar{2}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	$\bar{1} \vee 2 \vee 4$	by $\mathcal{T}$-**Conflict**
$1\ \bar{4} \bullet \bar{2}$	$1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4$	$\bar{1} \vee 2 \vee 4$	by **Learn**
$1\ \bar{4}$	$1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4$	no	by **Restart**
$1\ \bar{4}\ 2\ 3$	$1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4$	no	by **Propagate**$^+$
$1\ \bar{4}\ 2\ 3$	$1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4$	$\bar{1} \vee \bar{3} \vee 4$	by $\mathcal{T}$-**Conflict**
$1\ \bar{4}\ 2\ 3$	$1,\ \bar{2} \vee 3,\ \bar{4},\ \bar{1} \vee 2 \vee 4,\ \bar{1} \vee \bar{3} \vee 4$	no	by **Learn**
	$\vdots$		
	UNSAT		by **Fail**

A Better Lazy Approach

The very lazy approach can be improved considerably with

- an *on-line* SAT engine that accept new input clauses on the fly
- an *incremental and explicating $\mathcal{T}$-solver* that can

A Better Lazy Approach

The very lazy approach can be improved considerably with

- an *on-line* SAT engine that accept new input clauses on the fly
- an *incremental and explicating* $\mathcal{T}$-solver that can
    1. check the $\mathcal{T}$-satisfiability of M as it is extended and
    2. identify a small $\mathcal{T}$-unsatisfiable subset of M once M becomes $\mathcal{T}$-unsatisfiable

A Better Lazy Approach

The very lazy approach can be improved considerably with

- an *on-line* SAT engine that accept new input clauses on the fly
- an *incremental and explicating* $\mathcal{T}$-solver that can
  1. check the $\mathcal{T}$-satisfiability of M as it is extended and
  2. identify a small $\mathcal{T}$-unsatisfiable subset of M once M becomes $\mathcal{T}$-unsatisfiable

A Better Lazy Approach

The very lazy approach can be improved considerably with

- an *on-line* SAT engine that accept new input clauses on the fly
- an *incremental and explicating* $\mathcal{T}$-solver that can
  1. check the $\mathcal{T}$-satisfiability of M as it is extended and
  2. identify a small $\mathcal{T}$-unsatisfiable subset of M once M becomes $\mathcal{T}$-unsatisfiable

A Better Lazy Approach

$$\underbrace{g(a) \doteq c}_{1} \quad \wedge \quad \underbrace{f(g(a)) \not\doteq f(c)}_{\bar{2}} \vee \underbrace{g(a) \doteq d}_{3} \quad \wedge \quad \underbrace{c \not\doteq d}_{\bar{4}}$$

M	Δ	C	rule
	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	
$1\ \bar{4}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by PROPAGATE$^+$
$1\ \bar{4} \bullet \bar{2}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by DECIDE
$1\ \bar{4} \bullet \bar{2}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	$\bar{1} \vee 2$	by $\mathcal{T}$-CONFLICT
$1\ \bar{4}\ 2$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by BACKJUMP
$1\ \bar{4}\ 2\ 3$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by PROPAGATE
$1\ \bar{4}\ 2\ 3$	$1,\ \bar{2} \vee 3,\ \bar{4}$	$\bar{1} \vee \bar{3} \vee 4$	by $\mathcal{T}$-CONFLICT
UNSAT			by FAIL

A Better Lazy Approach

$$\underbrace{g(a) \doteq c}_{1} \quad \wedge \quad \underbrace{f(g(a)) \not\doteq f(c)}_{\bar{2}} \vee \underbrace{g(a) \doteq d}_{3} \quad \wedge \quad \underbrace{c \not\doteq d}_{\bar{4}}$$

M	Δ	C	rule
	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	
$1\ \bar{4}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by PROPAGATE$^+$
$1\ \bar{4} \bullet \bar{2}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by DECIDE
$1\ \bar{4} \bullet \bar{2}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	$\bar{1} \vee 2$	by $\mathcal{T}$-CONFLICT
$1\ \bar{4}\ 2$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by BACKJUMP
$1\ \bar{4}\ 2\ 3$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by PROPAGATE
$1\ \bar{4}\ 2\ 3$	$1,\ \bar{2} \vee 3,\ \bar{4}$	$\bar{1} \vee \bar{3} \vee 4$	by $\mathcal{T}$-CONFLICT
UNSAT			by FAIL

A Better Lazy Approach

$$\underbrace{g(a) \doteq c}_{1} \quad \land \quad \underbrace{f(g(a)) \not\doteq f(c)}_{\bar{2}} \lor \underbrace{g(a) \doteq d}_{3} \quad \land \quad \underbrace{c \not\doteq d}_{\bar{4}}$$

M	Δ	C	rule
	$1,\ \bar{2} \lor 3,\ \bar{4}$	no	
$1\ \bar{4}$	$1,\ \bar{2} \lor 3,\ \bar{4}$	no	by **Propagate**$^+$
$1\ \bar{4} \bullet \bar{2}$	$1,\ \bar{2} \lor 3,\ \bar{4}$	no	by **Decide**
$1\ \bar{4} \bullet \bar{2}$	$1,\ \bar{2} \lor 3,\ \bar{4}$	$\bar{1} \lor 2$	by $\mathcal{T}$-**Conflict**
$1\ \bar{4}\ 2$	$1,\ \bar{2} \lor 3,\ \bar{4}$	no	by **Backjump**
$1\ \bar{4}\ 2\ 3$	$1,\ \bar{2} \lor 3,\ \bar{4}$	no	by **Propagate**
$1\ \bar{4}\ 2\ 3$	$1,\ \bar{2} \lor 3,\ \bar{4}$	$\bar{1} \lor \bar{3} \lor 4$	by $\mathcal{T}$-**Conflict**
UNSAT			by **Fail**

A Better Lazy Approach

$$\underbrace{g(a) \doteq c}_{1} \quad \wedge \quad \underbrace{f(g(a)) \not\doteq f(c)}_{\bar{2}} \vee \underbrace{g(a) \doteq d}_{3} \quad \wedge \quad \underbrace{c \not\doteq d}_{\bar{4}}$$

M	Δ	C	rule
	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	
$1\ \bar{4}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by **Propagate**$^+$
$1\ \bar{4} \bullet \bar{2}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by **Decide**
$1\ \bar{4} \bullet \bar{2}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	$\bar{1} \vee 2$	by $\mathcal{T}$-**Conflict**
$1\ \bar{4}\ 2$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by **Backjump**
$1\ \bar{4}\ 2\ 3$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by **Propagate**
$1\ \bar{4}\ 2\ 3$	$1,\ \bar{2} \vee 3,\ \bar{4}$	$\bar{1} \vee \bar{3} \vee 4$	by $\mathcal{T}$-**Conflict**
UNSAT			by **Fail**

A Better Lazy Approach

$$\underbrace{g(a) \doteq c}_{1} \quad \wedge \quad \underbrace{f(g(a)) \not\doteq f(c)}_{\bar{2}} \vee \underbrace{g(a) \doteq d}_{3} \quad \wedge \quad \underbrace{c \not\doteq d}_{\bar{4}}$$

M	Δ	C	rule
	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	
$1\ \bar{4}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by **Propagate**$^+$
$1\ \bar{4} \bullet \bar{2}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by **Decide**
$1\ \bar{4} \bullet \bar{2}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	$\bar{1} \vee 2$	by $\mathcal{T}$-**Conflict**
$1\ \bar{4}\ 2$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by **Backjump**
$1\ \bar{4}\ 2\ 3$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by **Propagate**
$1\ \bar{4}\ 2\ 3$	$1,\ \bar{2} \vee 3,\ \bar{4}$	$\bar{1} \vee \bar{3} \vee 4$	by $\mathcal{T}$-**Conflict**
UNSAT			by **Fail**

A Better Lazy Approach

$$\underbrace{g(a) \doteq c}_{1} \quad \wedge \quad \underbrace{f(g(a)) \not\doteq f(c)}_{\bar{2}} \vee \underbrace{g(a) \doteq d}_{3} \quad \wedge \quad \underbrace{c \not\doteq d}_{\bar{4}}$$

M	Δ	C	rule
	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	
$1\ \bar{4}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by **Propagate**$^{+}$
$1\ \bar{4} \bullet \bar{2}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by **Decide**
$1\ \bar{4} \bullet \bar{2}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	$\bar{1} \vee 2$	by $\mathcal{T}$-**Conflict**
$1\ \bar{4}\ 2$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by **Backjump**
$1\ \bar{4}\ 2\ 3$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by **Propagate**
$1\ \bar{4}\ 2\ 3$	$1,\ \bar{2} \vee 3,\ \bar{4}$	$\bar{1} \vee \bar{3} \vee 4$	by $\mathcal{T}$-**Conflict**
UNSAT			by **Fail**

A Better Lazy Approach

$$\underbrace{g(a) \doteq c}_{1} \quad \wedge \quad \underbrace{f(g(a)) \not\doteq f(c)}_{\bar{2}} \vee \underbrace{g(a) \doteq d}_{3} \quad \wedge \quad \underbrace{c \not\doteq d}_{\bar{4}}$$

M	Δ	C	rule
	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	
$1\ \bar{4}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by **Propagate**$^+$
$1\ \bar{4} \bullet \bar{2}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by **Decide**
$1\ \bar{4} \bullet \bar{2}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	$\bar{1} \vee 2$	by $\mathcal{T}$-**Conflict**
$1\ \bar{4}\ 2$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by **Backjump**
$1\ \bar{4}\ 2\ 3$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by **Propagate**
$1\ \bar{4}\ 2\ 3$	$1,\ \bar{2} \vee 3,\ \bar{4}$	$\bar{1} \vee \bar{3} \vee 4$	by $\mathcal{T}$-**Conflict**
UNSAT			by **Fail**

A Better Lazy Approach

$$\underbrace{g(a) \doteq c}_{1} \quad \wedge \quad \underbrace{f(g(a)) \not\doteq f(c)}_{\bar{2}} \vee \underbrace{g(a) \doteq d}_{3} \quad \wedge \quad \underbrace{c \not\doteq d}_{\bar{4}}$$

M	Δ	C	rule
	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	
$1\ \bar{4}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by Propagate^{+}
$1\ \bar{4} \bullet \bar{2}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by Decide
$1\ \bar{4} \bullet \bar{2}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	$\bar{1} \vee 2$	by $\mathcal{T}$-Conflict
$1\ \bar{4}\ 2$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by Backjump
$1\ \bar{4}\ 2\ 3$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by Propagate
$1\ \bar{4}\ 2\ 3$	$1,\ \bar{2} \vee 3,\ \bar{4}$	$\bar{1} \vee \bar{3} \vee 4$	by $\mathcal{T}$-Conflict
UNSAT			by Fail

A Better Lazy Approach

$$\underbrace{g(a) \doteq c}_{1} \quad \wedge \quad \underbrace{f(g(a)) \not\doteq f(c)}_{\bar{2}} \vee \underbrace{g(a) \doteq d}_{3} \quad \wedge \quad \underbrace{c \not\doteq d}_{\bar{4}}$$

M	Δ	C	rule
	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	
$1\ \bar{4}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by **Propagate**$^{+}$
$1\ \bar{4} \bullet \bar{2}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by **Decide**
$1\ \bar{4} \bullet \bar{2}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	$\bar{1} \vee 2$	by **$\mathcal{T}$-Conflict**
$1\ \bar{4}\ 2$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by **Backjump**
$1\ \bar{4}\ 2\ 3$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by **Propagate**
$1\ \bar{4}\ 2\ 3$	$1,\ \bar{2} \vee 3,\ \bar{4}$	$\bar{1} \vee \bar{3} \vee 4$	by **$\mathcal{T}$-Conflict**
UNSAT			by **Fail**

Lazy Approach – Strategies

Ignoring **Restart** (for simplicity), a common strategy is to apply the rules using the following priorities:

1. If a clause is (propositionally) falsified by the current assignment M, apply **Conflict**
2. If M is $\mathcal{T}$-unsatisfiable, apply $\mathcal{T}$**-Conflict**
3. Apply **Fail** or **Explain**+**Learn**+**Backjump** as appropriate
4. Apply **Propagate**
5. Apply **Decide**

Depending on the cost of checking the $\mathcal{T}$-satisfiability of M,
Step (2) can be applied with lower frequency or priority

Lazy Approach – Strategies

Ignoring **Restart** (for simplicity), a common strategy is to apply the rules using the following priorities:

1. If a clause is (propositionally) falsified by the current assignment M, apply **Conflict**
2. If M is $\mathcal{T}$-unsatisfiable, apply $\mathcal{T}$**-Conflict**
3. Apply **Fail** or **Explain**+**Learn**+**Backjump** as appropriate
4. Apply **Propagate**
5. Apply **Decide**

Depending on the cost of checking the $\mathcal{T}$-satisfiability of M,
Step (2) can be applied with lower frequency or priority

Theory Propagation

With $\mathcal{T}$-**Conflict** as the only theory rule, the theory solver is used just to validate the choices of the SAT engine

With $\mathcal{T}$-**Propagate** and $\mathcal{T}$-**Explain**, it can also be used to guide the engine's search

$$\mathcal{T}\text{-}\textbf{Propagate}\ \frac{l \in \mathtt{Lits}(\Delta) \qquad \mathsf{M} \models_{\mathcal{T}} l \qquad l, \bar{l} \notin \mathsf{M}}{\mathsf{M} := \mathsf{M}\ l}$$

$$\mathcal{T}\text{-}\textbf{Explain}\ \frac{\mathsf{C} = \{l\} \cup D \qquad \bar{l}_1 \wedge \cdots \wedge \bar{l}_n \models_{\mathcal{T}} \bar{l} \qquad \bar{l}_1, \ldots, \bar{l}_n \prec_{\mathsf{M}} \bar{l}}{\mathsf{C} := \{l_1, \cdots, l_n\} \cup D}$$

Theory Propagation

With $\mathcal{T}$-**Conflict** as the only theory rule, the theory solver is used just to validate the choices of the SAT engine

With $\mathcal{T}$-**Propagate** and $\mathcal{T}$-**Explain**, it can also be used to guide the engine's search

$$\mathcal{T}\text{-}\textbf{Propagate}\ \frac{l \in \texttt{Lits}(\Delta) \qquad \mathsf{M} \models_{\mathcal{T}} l \qquad l, \bar{l} \notin \mathsf{M}}{\mathsf{M} := \mathsf{M}\ l}$$

$$\mathcal{T}\text{-}\textbf{Explain}\ \frac{\mathsf{C} = \{l\} \cup D \qquad \bar{l}_1 \wedge \cdots \wedge \bar{l}_n \models_{\mathcal{T}} \bar{l} \qquad \bar{l}_1, \ldots, \bar{l}_n \prec_{\mathsf{M}} \bar{l}}{\mathsf{C} := \{l_1, \cdots, l_n\} \cup D}$$

Theory Propagation Example

$$\underbrace{g(a) \doteq c}_{1} \quad \wedge \quad \underbrace{f(g(a)) \not\doteq f(c)}_{\bar{2}} \vee \underbrace{g(a) \doteq d}_{3} \quad \wedge \quad \underbrace{c \not\doteq d}_{\bar{4}}$$

M	Δ	C	rule
	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	
$1\ \bar{4}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by Propagate^{+}
$1\ \bar{4}\ 2$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by $\mathcal{T}$-Propagate (as $1 \models_{\mathcal{T}} 2$)
$1\ \bar{4}\ 2\ \bar{3}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by $\mathcal{T}$-Propagate (as $1,\ \bar{4} \models_{\mathcal{T}} \bar{3}$)
$1\ \bar{4}\ 2\ \bar{3}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	$\bar{2} \vee 3$	by Conflict
UNSAT			by Fail

$\mathcal{T}$-propagation eliminates search altogether in this case!
No applications of **Decide** are needed

Theory Propagation Example

$$\underbrace{g(a) \doteq c}_{1} \quad \wedge \quad \underbrace{f(g(a)) \not\doteq f(c)}_{\overline{2}} \vee \underbrace{g(a) \doteq d}_{3} \quad \wedge \quad \underbrace{c \not\doteq d}_{\overline{4}}$$

M	Δ	C	rule
	$1,\ \overline{2} \vee 3,\ \overline{4}$	no	
$1\ \overline{4}$	$1,\ \overline{2} \vee 3,\ \overline{4}$	no	by PROPAGATE$^+$
$1\ \overline{4}\ 2$	$1,\ \overline{2} \vee 3,\ \overline{4}$	no	by $\mathcal{T}$-PROPAGATE (as $1 \models_{\mathcal{T}} 2$)
$1\ \overline{4}\ 2\ \overline{3}$	$1,\ \overline{2} \vee 3,\ \overline{4}$	no	by $\mathcal{T}$-PROPAGATE (as $1,\ \overline{4} \models_{\mathcal{T}} \overline{3}$)
$1\ \overline{4}\ 2\ \overline{3}$	$1,\ \overline{2} \vee 3,\ \overline{4}$	$\overline{2} \vee 3$	by CONFLICT
UNSAT			by FAIL

$\mathcal{T}$-propagation eliminates search altogether in this case!
No applications of **DECIDE** are needed

Theory Propagation Example

$$\underbrace{g(a) \doteq c}_{1} \;\wedge\; \underbrace{f(g(a)) \not\doteq f(c)}_{\overline{2}} \vee \underbrace{g(a) \doteq d}_{3} \;\wedge\; \underbrace{c \not\doteq d}_{\overline{4}}$$

M	Δ	C	rule
	$1,\ \overline{2} \vee 3,\ \overline{4}$	no	
$1\ \overline{4}$	$1,\ \overline{2} \vee 3,\ \overline{4}$	no	by **Propagate**$^+$
$1\ \overline{4}\ 2$	$1,\ \overline{2} \vee 3,\ \overline{4}$	no	by $\mathcal{T}$-**Propagate** (as $1 \models_{\mathcal{T}} 2$)
$1\ \overline{4}\ 2\ \overline{3}$	$1,\ \overline{2} \vee 3,\ \overline{4}$	no	by $\mathcal{T}$-**Propagate** (as $1,\ \overline{4} \models_{\mathcal{T}} \overline{3}$)
$1\ \overline{4}\ 2\ \overline{3}$	$1,\ \overline{2} \vee 3,\ \overline{4}$	$\overline{2} \vee 3$	by **Conflict**
UNSAT			by **Fail**

$\mathcal{T}$-propagation eliminates search altogether in this case!
No applications of **Decide** are needed

Theory Propagation Example

$$\underbrace{g(a) \doteq c}_{1} \quad \wedge \quad \underbrace{f(g(a)) \not\doteq f(c)}_{\bar{2}} \vee \underbrace{g(a) \doteq d}_{3} \quad \wedge \quad \underbrace{c \not\doteq d}_{\bar{4}}$$

M	Δ	C	rule
	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	
$1\ \bar{4}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by **Propagate**$^{+}$
$1\ \bar{4}\ 2$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by $\mathcal{T}$-**Propagate** (as $1 \models_{\mathcal{T}} 2$)
$1\ \bar{4}\ 2\ \bar{3}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by $\mathcal{T}$-**Propagate** (as $1,\ \bar{4} \models_{\mathcal{T}} \bar{3}$)
$1\ \bar{4}\ 2\ \bar{3}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	$\bar{2} \vee 3$	by **Conflict**
UNSAT			by **Fail**

$\mathcal{T}$-propagation eliminates search altogether in this case!
No applications of **Decide** are needed

Theory Propagation Example

$$\underbrace{g(a) \doteq c}_{1} \quad \land \quad \underbrace{f(g(a)) \not\doteq f(c)}_{\bar{2}} \lor \underbrace{g(a) \doteq d}_{3} \quad \land \quad \underbrace{c \not\doteq d}_{\bar{4}}$$

M	Δ	C	rule
	$1,\ \bar{2} \lor 3,\ \bar{4}$	no	
$1\ \bar{4}$	$1,\ \bar{2} \lor 3,\ \bar{4}$	no	by **Propagate**$^{+}$
$1\ \bar{4}\ 2$	$1,\ \bar{2} \lor 3,\ \bar{4}$	no	by $\mathcal{T}$-**Propagate** (as $1 \models_{\mathcal{T}} 2$)
$1\ \bar{4}\ 2\ \bar{3}$	$1,\ \bar{2} \lor 3,\ \bar{4}$	no	by $\mathcal{T}$-**Propagate** (as $1,\ \bar{4} \models_{\mathcal{T}} \bar{3}$)
$1\ \bar{4}\ 2\ \bar{3}$	$1,\ \bar{2} \lor 3,\ \bar{4}$	$\bar{2} \lor 3$	by **Conflict**
UNSAT			by **Fail**

$\mathcal{T}$-propagation eliminates search altogether in this case!
No applications of **Decide** are needed

Theory Propagation Example

$$\underbrace{g(a) \doteq c}_{1} \;\wedge\; \underbrace{f(g(a)) \not\doteq f(c)}_{\overline{2}} \vee \underbrace{g(a) \doteq d}_{3} \;\wedge\; \underbrace{c \not\doteq d}_{\overline{4}}$$

M	Δ	C	rule
	$1,\ \overline{2} \vee 3,\ \overline{4}$	no	
$1\ \overline{4}$	$1,\ \overline{2} \vee 3,\ \overline{4}$	no	by **Propagate**$^+$
$1\ \overline{4}\ 2$	$1,\ \overline{2} \vee 3,\ \overline{4}$	no	by $\mathcal{T}$-**Propagate** (as $1 \models_{\mathcal{T}} 2$)
$1\ \overline{4}\ 2\ \overline{3}$	$1,\ \overline{2} \vee 3,\ \overline{4}$	no	by $\mathcal{T}$-**Propagate** (as $1,\ \overline{4} \models_{\mathcal{T}} \overline{3}$)
$1\ \overline{4}\ 2\ \overline{3}$	$1,\ \overline{2} \vee 3,\ \overline{4}$	$\overline{2} \vee 3$	by **Conflict**
UNSAT			by **Fail**

$\mathcal{T}$-propagation eliminates search altogether in this case!
No applications of **Decide** are needed

Theory Propagation Example

$$\underbrace{g(a) \doteq c}_{1} \quad \wedge \quad \underbrace{f(g(a)) \not\doteq f(c)}_{\bar{2}} \vee \underbrace{g(a) \doteq d}_{3} \quad \wedge \quad \underbrace{c \not\doteq d}_{\bar{4}}$$

M	Δ	C	rule	
	$1,\ \bar{2} \vee 3,\ \bar{4}$	no		
$1\ \bar{4}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by **Propagate**$^{+}$	
$1\ \bar{4}\ 2$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by $\mathcal{T}$-**Propagate**	(as $1 \models_{\mathcal{T}} 2$)
$1\ \bar{4}\ 2\ \bar{3}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	no	by $\mathcal{T}$-**Propagate**	(as $1,\ \bar{4} \models_{\mathcal{T}} \bar{3}$)
$1\ \bar{4}\ 2\ \bar{3}$	$1,\ \bar{2} \vee 3,\ \bar{4}$	$\bar{2} \vee 3$	by **Conflict**	
UNSAT			by **Fail**	

$\mathcal{T}$-propagation eliminates search altogether in this case!
No applications of **Decide** are needed

Theory Propagation Example

$$\underbrace{g(a) \doteq c}_{1} \quad \wedge \quad \underbrace{f(g(a)) \not\doteq f(c)}_{\overline{2}} \vee \underbrace{g(a) \doteq d}_{3} \quad \wedge \quad \underbrace{c \not\doteq d}_{\overline{4}}$$

M	Δ	C	rule
	$1,\ \overline{2} \vee 3,\ \overline{4}$	no	
$1\ \overline{4}$	$1,\ \overline{2} \vee 3,\ \overline{4}$	no	by **Propagate**$^+$
$1\ \overline{4}\ 2$	$1,\ \overline{2} \vee 3,\ \overline{4}$	no	by $\mathcal{T}$-**Propagate** (as $1 \models_{\mathcal{T}} 2$)
$1\ \overline{4}\ 2\ \overline{3}$	$1,\ \overline{2} \vee 3,\ \overline{4}$	no	by $\mathcal{T}$-**Propagate** (as $1,\ \overline{4} \models_{\mathcal{T}} \overline{3}$)
$1\ \overline{4}\ 2\ \overline{3}$	$1,\ \overline{2} \vee 3,\ \overline{4}$	$\overline{2} \vee 3$	by **Conflict**
UNSAT			by **Fail**

$\mathcal{T}$-propagation eliminates search altogether in this case!
No applications of **Decide** are needed

Theory Propagation Features

- With *exhaustive* theory propagation, every assignment M is $\mathcal{T}$-satisfiable
(since $M\,l$ is $\mathcal{T}$-unsatisfiable iff $M \models_{\mathcal{T}} \bar{l}$)

- For theory propagation to be effective in practice, it needs specialized theory solvers

- For some theories, e.g., difference logic, detecting $\mathcal{T}$-entailed literals is cheap and so exhaustive theory propagation is extremely effective

- For others, e.g., the theory of equality, detecting $\mathcal{T}$-entailed equalities is cheap but detecting $\mathcal{T}$-entailed disequalities is quite expensive

- If $\mathcal{T}$-**Propagate** is not applied exhaustively, $\mathcal{T}$-**Conflict** is needed to repair $\mathcal{T}$-unsatisfiable assignments

Theory Propagation Features

- With *exhaustive* theory propagation, every assignment M is $\mathcal{T}$-satisfiable
  (since $M\ l$ is $\mathcal{T}$-unsatisfiable iff $M \models_{\mathcal{T}} \bar{l}$)

- For theory propagation to be effective in practice, it needs specialized theory solvers

- For some theories, e.g., difference logic, detecting $\mathcal{T}$-entailed literals is cheap and so exhaustive theory propagation is extremely effective

- For others, e.g., the theory of equality, detecting $\mathcal{T}$-entailed equalities is cheap but detecting $\mathcal{T}$-entailed disequalities is quite expensive

- If $\mathcal{T}$-**Propagate** is not applied exhaustively, $\mathcal{T}$-**Conflict** is needed to repair $\mathcal{T}$-unsatisfiable assignments

Theory Propagation Features

- With *exhaustive* theory propagation, every assignment M is $\mathcal{T}$-satisfiable
  (since $M\,l$ is $\mathcal{T}$-unsatisfiable iff $M \models_{\mathcal{T}} \bar{l}$)

- For theory propagation to be effective in practice, it needs specialized theory solvers

- For some theories, e.g., difference logic, detecting $\mathcal{T}$-entailed literals is cheap and so exhaustive theory propagation is extremely effective

- For others, e.g., the theory of equality, detecting $\mathcal{T}$-entailed equalities is cheap but detecting $\mathcal{T}$-entailed disequalities is quite expensive

- If $\mathcal{T}$-Propagate is not applied exhaustively, $\mathcal{T}$-Conflict is needed to repair $\mathcal{T}$-unsatisfiable assignments

Theory Propagation Features

- With *exhaustive* theory propagation, every assignment M is $\mathcal{T}$-satisfiable
  (since $M\,l$ is $\mathcal{T}$-unsatisfiable iff $M \models_{\mathcal{T}} \bar{l}$)
- For theory propagation to be effective in practice, it needs specialized theory solvers
- For some theories, e.g., difference logic, detecting $\mathcal{T}$-entailed literals is cheap and so exhaustive theory propagation is extremely effective
- For others, e.g., the theory of equality, detecting $\mathcal{T}$-entailed equalities is cheap but detecting $\mathcal{T}$-entailed disequalities is quite expensive
- If $\mathcal{T}$-Propagate is not applied exhaustively, $\mathcal{T}$-Conflict is needed to repair $\mathcal{T}$-unsatisfiable assignments

Theory Propagation Features

- With *exhaustive* theory propagation, every assignment M is $\mathcal{T}$-satisfiable (since $M\,l$ is $\mathcal{T}$-unsatisfiable iff $M \models_{\mathcal{T}} \bar{l}$)
- For theory propagation to be effective in practice, it needs specialized theory solvers
- For some theories, e.g., difference logic, detecting $\mathcal{T}$-entailed literals is cheap and so exhaustive theory propagation is extremely effective
- For others, e.g., the theory of equality, detecting $\mathcal{T}$-entailed equalities is cheap but detecting $\mathcal{T}$-entailed disequalities is quite expensive
- If $\mathcal{T}$-**Propagate** is not applied exhaustively, $\mathcal{T}$-**Conflict** is needed to repair $\mathcal{T}$-unsatisfiable assignments

Theory Propagation Exercise

$$\underbrace{a \doteq b}_{1} \quad \wedge \quad \underbrace{a \doteq c}_{2} \vee \underbrace{c \doteq b}_{3} \quad \wedge \quad \underbrace{a \not\doteq b}_{\bar{1}} \vee \underbrace{f(a) \not\doteq f(c)}_{\bar{4}} \quad \wedge \quad \underbrace{c \not\doteq b}_{\bar{3}} \vee \underbrace{g(a) \doteq g(c)}_{5}$$

$$\Delta_0 \;:=\; 1,\; 2 \vee 3,\; \bar{1} \vee \bar{4},\; \bar{3} \vee 5$$

Theory Propagation Exercise

Scenario 1: propagating only $\mathcal{T}$-entailed equalities (no disequalities)

$$\underbrace{a \doteq b}_{1} \quad \wedge \quad \underbrace{a \doteq c}_{2} \vee \underbrace{c \doteq b}_{3} \quad \wedge \quad \underbrace{a \not\doteq b}_{\bar{1}} \vee \underbrace{f(a) \not\doteq f(c)}_{\bar{4}} \quad \wedge \quad \underbrace{c \not\doteq b}_{\bar{3}} \vee \underbrace{g(a) \doteq g(c)}_{5}$$

$$\Delta_0 \ := \ 1, \ 2 \vee 3, \ \bar{1} \vee \bar{4}, \ \bar{3} \vee 5$$

Theory Propagation Exercise

Scenario 1: propagating only $\mathcal{T}$-entailed equalities (no disequalities)

$$\underbrace{a \doteq b}_{1} \quad\wedge\quad \underbrace{a \doteq c}_{2} \vee \underbrace{c \doteq b}_{3} \quad\wedge\quad \underbrace{a \not\doteq b}_{\overline{1}} \vee \underbrace{f(a) \not\doteq f(c)}_{\overline{4}} \quad\wedge\quad \underbrace{c \not\doteq b}_{\overline{3}} \vee \underbrace{g(a) \doteq g(c)}_{5}$$

$$\Delta_0 \;:=\; 1,\;\; 2 \vee 3,\;\; \overline{1} \vee \overline{4},\;\; \overline{3} \vee 5$$

M	Δ	C	rule
	Δ_0	no	
$1\ \overline{4}$	Δ_0	no	by PROPAGATE$^+$
$1\ \overline{4}\ \bullet\ 2$	Δ_0	no	by DECIDE
$1\ \overline{4}\ \bullet\ 2$	Δ_0	$\overline{2} \vee 4$	by $\mathcal{T}$-CONFLICT (as $2, \overline{4} \models_{\mathcal{T}} \bot$)
$1\ \overline{4}\ \overline{2}$	$\Delta_0,\ \overline{2} \vee 4$	no	by BACKJUMP
$1\ \overline{4}\ \overline{2}\ 3$	$\Delta_0,\ \overline{2} \vee 4$	no	by PROPAGATE
$1\ \overline{4}\ \overline{2}\ 3$	$\Delta_0,\ \overline{2} \vee 4$	$\overline{1} \vee \overline{3} \vee 4$	by $\mathcal{T}$-CONFLICT (as $1, \overline{3}, \overline{4} \models_{\mathcal{T}} \bot$)
UNSAT			by FAIL

Theory Propagation Exercise

Scenario 2: propagating $\mathcal{T}$-entailed equalities and disequalities

$$\underbrace{a \doteq b}_{1} \quad \wedge \quad \underbrace{a \doteq c}_{2} \vee \underbrace{c \doteq b}_{3} \quad \wedge \quad \underbrace{a \not\doteq b}_{\bar{1}} \vee \underbrace{f(a) \not\doteq f(c)}_{\bar{4}} \quad \wedge \quad \underbrace{c \not\doteq b}_{\bar{3}} \vee \underbrace{g(a) \doteq g(c)}_{5}$$

$$\Delta_0 \ := \ 1, \ 2 \vee 3, \ \bar{1} \vee \bar{4}, \ \bar{3} \vee 5$$

Theory Propagation Exercise

Scenario 2: propagating $\mathcal{T}$-entailed equalities and disequalities

$$\underbrace{a \doteq b}_{1} \quad \wedge \quad \underbrace{a \doteq c}_{2} \vee \underbrace{c \doteq b}_{3} \quad \wedge \quad \underbrace{a \not\doteq b}_{\bar{1}} \vee \underbrace{f(a) \not\doteq f(c)}_{\bar{4}} \quad \wedge \quad \underbrace{c \not\doteq b}_{\bar{3}} \vee \underbrace{g(a) \doteq g(c)}_{5}$$

$$\Delta_0 \;:=\; 1,\;\; 2 \vee 3,\;\; \bar{1} \vee \bar{4},\;\; \bar{3} \vee 5$$

M	Δ	C	rule
	Δ_0	no	
$1\ \bar{4}$	Δ_0	no	by **Propagate**$^+$
$1\ \bar{4}\ \bar{2}$	$\Delta_0,\ \bar{2} \vee 4$	no	by $\mathcal{T}$-**Propagate** (as $1, \bar{4} \models_{\mathcal{T}} \bar{2}$)
$1\ \bar{4}\ \bar{2}\ 3$	$\Delta_0,\ \bar{2} \vee 4$	no	by **Propagate**
$1\ \bar{4}\ \bar{2}\ 3$	$\Delta_0,\ \bar{2} \vee 4$	$\bar{1} \vee \bar{3} \vee 4$	by $\mathcal{T}$-**Conflict** (as $1, 3, \bar{4} \models_{\mathcal{T}} \bot$)
UNSAT			by **Fail**

Modeling Modern Lazy SMT Solvers

At the core, current lazy SMT solvers are implementations of the proof system with rules:

(1) **Propagate**, **Decide**, **Conflict**, **Explain**, **Backjump**, **Fail**

(2) $\mathcal{T}$-**Conflict**, $\mathcal{T}$-**Propagate**, $\mathcal{T}$-**Explain**

(3) **Learn**, **Forget**, **Restart**

Basic CDCL Modulo Theories $\stackrel{\text{def}}{=}$ (1) + (2)

CDCL Modulo Theories $\stackrel{\text{def}}{=}$ (1) + (2) + (3)

Modeling Modern Lazy SMT Solvers

At the core, current lazy SMT solvers are implementations of the proof system with rules:

(1) **Propagate**, **Decide**, **Conflict**, **Explain**, **Backjump**, **Fail**

(2) $\mathcal{T}$-**Conflict**, $\mathcal{T}$-**Propagate**, $\mathcal{T}$-**Explain**

(3) **Learn**, **Forget**, **Restart**

Basic CDCL Modulo Theories $\stackrel{\text{def}}{=}$ (1) + (2)

CDCL Modulo Theories $\stackrel{\text{def}}{=}$ (1) + (2) + (3)

Correctness

Irreducible state: state to which no Basic CDCL Modulo Theories rules apply (updated terminology)
Execution: a (single-branch) derivation tree starting with $M = \emptyset$ and $C = \texttt{no}$
Exhausted execution: execution ending in an irreducible state

Theorem 2 (Strong Termination)

Every execution in which (i) LEARN/FORGET are applied only finitely many times and (ii) RESTART is applied with increased periodicity is finite.

Correctness

Irreducible state: state to which no Basic CDCL Modulo Theories rules apply (updated terminology)
Execution: a (single-branch) derivation tree starting with $\mathtt{M} = \emptyset$ and $\mathtt{C} = \mathtt{no}$
Exhausted execution: execution ending in an irreducible state

Theorem 2 (Strong Termination)

Every execution in which (i) **Learn**/**Forget** *are applied only finitely many times and (ii)* **Restart** *is applied with increased periodicity is finite.*

Correctness

Irreducible state: state to which no Basic CDCL Modulo Theories rules apply (updated terminology)
Execution: a (single-branch) derivation tree starting with $M = \emptyset$ and $C = \texttt{no}$
Exhausted execution: execution ending in an irreducible state

Theorem 2 (Strong Termination)

Every execution in which (i) LEARN/FORGET are applied only finitely many times and (ii) RESTART is applied with increased periodicity is finite.

Lemma 3

Every exhausted execution ends with either $C = no$ or UNSAT.

Correctness

Irreducible state: state to which no Basic CDCL Modulo Theories rules apply (updated terminology)
Execution: a (single-branch) derivation tree starting with $\mathsf{M} = \emptyset$ and $\mathsf{C} = \mathtt{no}$
Exhausted execution: execution ending in an irreducible state

Theorem 2 (Strong Termination)

Every execution in which (i) LEARN/FORGET are applied only finitely many times and (ii) RESTART is applied with increased periodicity is finite.

Theorem 3 (Refutation Soundness)

For every exhausted execution starting with $\Delta = \Delta_0$ and ending with UNSAT, the clause set Δ_0 is $\mathcal{T}$-unsatisfiable.

Correctness

Irreducible state: state to which no Basic CDCL Modulo Theories rules apply (updated terminology)
Execution: a (single-branch) derivation tree starting with $\mathsf{M} = \emptyset$ and $\mathsf{C} = \mathtt{no}$
Exhausted execution: execution ending in an irreducible state

Theorem 2 (Strong Termination)

Every execution in which (i) **Learn/Forget** *are applied only finitely many times and (ii)* **Restart** *is applied with increased periodicity is finite.*

Theorem 3 (Refutation Soundness)

For every exhausted execution starting with $\Delta = \Delta_0$ and ending with UNSAT, *the clause set Δ_0 is $\mathcal{T}$-unsatisfiable.*

Theorem 4 (Refutation Completeness)

For every exhausted execution starting with $\Delta = \Delta_0$ and ending with $\mathsf{C} = no$, the clause set Δ_0 is $\mathcal{T}$-satisfiable; specifically, M is $\mathcal{T}$-satisfiable and $\mathsf{M} \models_{\mathrm{p}} \Delta_0$.

CDCL($\mathcal{T}$) Architecture

The approach formalized so far can be implemented with a simple architecture originally named DPLL($\mathcal{T}$) but currently known as *CDCL($\mathcal{T}$)*

$$\text{CDCL}(\mathcal{T}) \;=\; \text{CDCL}(X) \text{ engine} \;+\; \mathcal{T}\text{-solver}$$

CDCL($\mathcal{T}$) Architecture

The approach formalized so far can be implemented with a simple architecture originally named DPLL($\mathcal{T}$) but currently known as *CDCL($\mathcal{T}$)*

$$\text{CDCL}(\mathcal{T}) \;=\; \text{CDCL}(X)\text{ engine} \;+\; \mathcal{T}\text{-solver}$$

CDCL(X):

- Very similar to a SAT solver, enumerates Boolean models
- Not allowed: pure literal rule (and other SAT specific optimizations)
- Required: incremental addition of clauses
- Desirable: partial model detection

CDCL($\mathcal{T}$) Architecture

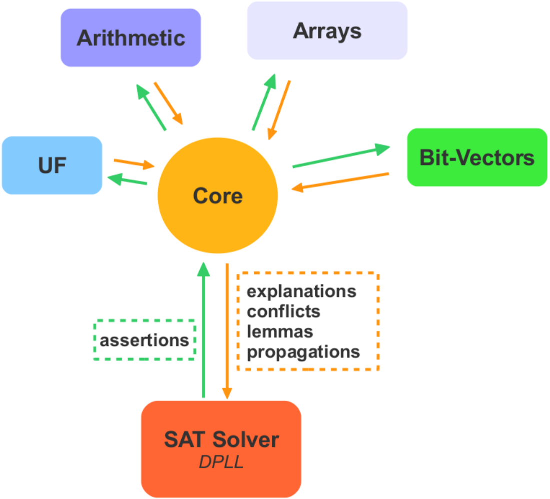
The approach formalized so far can be implemented with a simple architecture originally named DPLL($\mathcal{T}$) but currently known as *CDCL($\mathcal{T}$)*

$$\text{CDCL}(\mathcal{T}) \;=\; \text{CDCL}(X) \text{ engine} \;+\; \mathcal{T}\text{-solver}$$

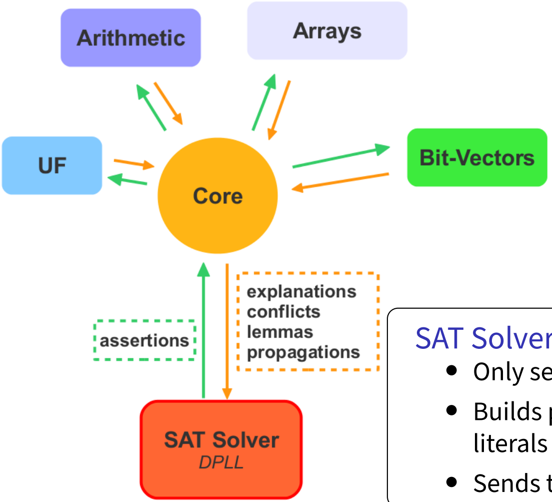
$\mathcal{T}$-solver:

- Checks the $\mathcal{T}$-satisfiability of conjunctions of literals
- Computes theory propagations
- Produces explanations of $\mathcal{T}$-unsatisfiability/propagation
- Must be incremental and backtrackable

Typical SMT solver architecture



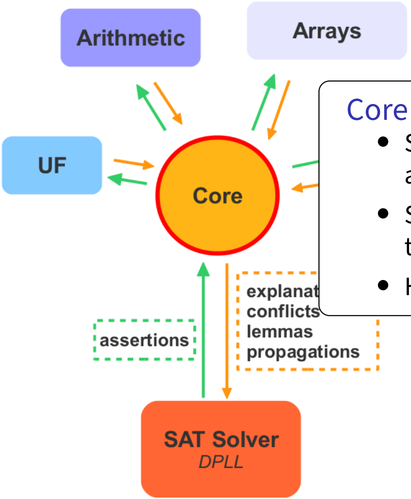
Typical SMT solver architecture



SAT Solver

- Only sees *Boolean skeleton* of problem
- Builds partial model by assigning truth values to literals
- Sends these literals to the core as *assertions*

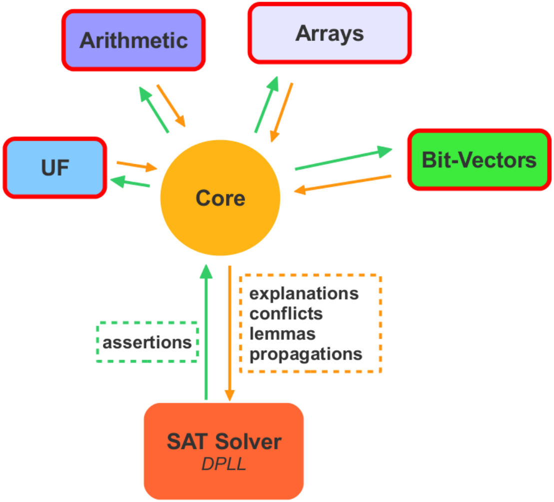
Typical SMT solver architecture



Core

- Sends each assertion to the appropriate theory
- Sends deduced literals to other theories/SAT solver
- Handles *theory combination*

Typical SMT solver architecture



Theory Solvers

- Check $\mathcal{T}$-satisfiability of sets of theory literals
- Incremental
- Backtrackable
- Conflict Generation
- Theory Propagation