

Model Based Theory Combination

SMT 2007

Leonardo de Moura and Nikolaj Bjørner

{leonardo, nbjorner}@microsoft.com.

Microsoft Research

Combination of Theories

- ▶ In practice, we need a combination of theories.

- ▶ Examples:

- ▶ $x + 2 = y \Rightarrow f(\text{read}(\text{write}(a, x, 3), y - 2)) = f(y - x + 1)$

- ▶ $f(f(x) - f(y)) \neq f(z), x + z \leq y \leq x \Rightarrow z < 0$

- ▶ Given

$$\Sigma = \Sigma_1 \cup \Sigma_2$$

$$\mathcal{T}_1, \mathcal{T}_2 : \text{theories over } \Sigma_1, \Sigma_2$$

$$\mathcal{T} = DC(\mathcal{T}_1 \cup \mathcal{T}_2)$$

- ▶ Is \mathcal{T} consistent?

- ▶ Given satisfiability procedures for conjunction of literals of \mathcal{T}_1 and \mathcal{T}_2 , how to decide the satisfiability of \mathcal{T} ?

Nelson-Oppen Combination

- ▶ Let \mathcal{T}_1 and \mathcal{T}_2 be consistent, stably infinite theories over disjoint (countable) signatures. Assume satisfiability of conjunction of literals can be decided in $O(T_1(n))$ and $O(T_2(n))$ time respectively.

Then,

1. The combined theory \mathcal{T} is consistent and stably infinite.
2. **Non-deterministic NO**: Satisfiability of quantifier free conjunction of literals in \mathcal{T} can be decided in $O(2^{n^2} \times (T_1(n) + T_2(n)))$.
3. **Deterministic NO**: If \mathcal{T}_1 and \mathcal{T}_2 are convex, then so is \mathcal{T} and satisfiability in \mathcal{T} is in $O(n^4 \times (T_1(n) + T_2(n)))$.

Nelson-Oppen Combination Procedure

- ▶ The combination procedure:

Initial State: ϕ is a conjunction of literals over $\Sigma_1 \cup \Sigma_2$.

Purification: Preserving satisfiability transform ϕ into $\phi_1 \wedge \phi_2$,
such that, $\phi_i \in \Sigma_i$.

Interaction: Guess a partition of $\mathcal{V}(\phi_1) \cap \mathcal{V}(\phi_2)$ into disjoint subsets. Express it as conjunction of literals ψ .

Example. The partition $\{x_1\}, \{x_2, x_3\}, \{x_4\}$ is represented as $x_1 \neq x_2, x_1 \neq x_4, x_2 \neq x_4, x_2 = x_3$.

Component Procedures : Use individual procedures to decide whether $\phi_i \wedge \psi$ is satisfiable.

Return: If both return yes, return yes. No, otherwise.

Convexity

- ▶ A theory \mathcal{T} is *convex* iff
 - for all finite sets Γ of literals and
 - for all non-empty disjunctions $\bigvee_{i \in I} x_i = y_i$ of variables,
 $\Gamma \models_{\mathcal{T}} \bigvee_{i \in I} x_i = y_i$ iff $\Gamma \models_{\mathcal{T}} x_i = y_i$ for some $i \in I$.
- ▶ For convex theories, instead of *guessing*, one can *deduce* the equalities to be shared.
- ▶ Key idea: propagate $x \simeq y$ to Γ_2 whenever $\mathcal{T}_1 \cup \Gamma_1 \models x \simeq y$, and vice-versa.
- ▶ Sharing equalities is sufficient:
 - Theory \mathcal{T}_1 can assume that $x^{M_2} \neq y^{M_2}$ whenever $x \simeq y$ is not implied by \mathcal{T}_2 and vice versa.

Combining theories in practice

- ▶ *Propagate all implied equalities.*
 - ▶ Deterministic Nelson-Oppen.
 - ▶ Complete only for convex theories.
 - ▶ It may be expensive for some theories.
- ▶ *Delayed Theory Combination.*
 - ▶ Nondeterministic Nelson-Oppen.
 - ▶ Create set of interface equalities ($x = y$) between shared variables.
 - ▶ Use SAT solver to guess the partition.
 - ▶ Disadvantage: the number of additional equality literals is quadratic in the number of shared variables.

Model based theory combination

- ▶ Common to these methods is that they are *pessimistic* about which equalities are propagated.

- ▶ *Model-based Theory Combination*

- ▶ *Optimistic approach.*

- ▶ Use a candidate model M_i for one of the theories \mathcal{T}_i and propagate all equalities implied by the candidate model, hedging that other theories will agree.

if $M_i \models \mathcal{T}_i \cup \Gamma_i \cup \{u = v\}$ **then** propagate $u = v$.

- ▶ If not, use backtracking to fix the model.
 - ▶ It is cheaper to enumerate equalities that are implied in a particular model than of all models.

Model based theory combination: Example

$$x = f(y - 1), f(x) \neq f(y), 0 \leq x \leq 1, 0 \leq y \leq 1$$

Purifying

Model based theory combination: Example

$$x = f(z), f(x) \neq f(y), 0 \leq x \leq 1, 0 \leq y \leq 1, z = y - 1$$

Model based theory combination: Example

$\mathcal{T}_{\mathcal{E}}$			$\mathcal{T}_{\mathcal{A}}$	
Literals	Eq. Classes	Model	Literals	Model
$x = f(z)$	$\{x, f(z)\}$	$x^{\mathcal{E}} = *_1$	$0 \leq x \leq 1$	$x^{\mathcal{A}} = 0$
$f(x) \neq f(y)$	$\{y\}$	$y^{\mathcal{E}} = *_2$	$0 \leq y \leq 1$	$y^{\mathcal{A}} = 0$
	$\{z\}$	$z^{\mathcal{E}} = *_3$	$z = y - 1$	$z^{\mathcal{A}} = -1$
	$\{f(x)\}$	$f^{\mathcal{E}} = \{*_1 \mapsto *_4,$ $*_2 \mapsto *_5,$ $*_3 \mapsto *_1,$ $else \mapsto *_6\}$		
	$\{f(y)\}$			

Assume $x = y$

Model based theory combination: Example

$\mathcal{T}_{\mathcal{E}}$			$\mathcal{T}_{\mathcal{A}}$	
Literals	Eq. Classes	Model	Literals	Model
$x = f(z)$	$\{x, y, f(z)\}$	$x^{\mathcal{E}} = *_1$	$0 \leq x \leq 1$	$x^{\mathcal{A}} = 0$
$f(x) \neq f(y)$	$\{z\}$	$y^{\mathcal{E}} = *_1$	$0 \leq y \leq 1$	$y^{\mathcal{A}} = 0$
$x = y$	$\{f(x), f(y)\}$	$z^{\mathcal{E}} = *_2$	$z = y - 1$	$z^{\mathcal{A}} = -1$
		$f^{\mathcal{E}} = \{*_1 \mapsto *_3,$	$x = y$	
		$*_2 \mapsto *_1,$		
		$else \mapsto *_4\}$		

Unsatisfiable

Model based theory combination: Example

\mathcal{T}_E			\mathcal{T}_A	
Literals	Eq. Classes	Model	Literals	Model
$x = f(z)$	$\{x, f(z)\}$	$x^E = *_1$	$0 \leq x \leq 1$	$x^A = 0$
$f(x) \neq f(y)$	$\{y\}$	$y^E = *_2$	$0 \leq y \leq 1$	$y^A = 0$
$x \neq y$	$\{z\}$	$z^E = *_3$	$z = y - 1$	$z^A = -1$
	$\{f(x)\}$	$f^E = \{*_1 \mapsto *_4,$	$x \neq y$	
	$\{f(y)\}$	$*_2 \mapsto *_5,$		
		$*_3 \mapsto *_1,$		
		$else \mapsto *_6\}$		

Backtrack, and assert $x \neq y$.

\mathcal{T}_A model need to be fixed.

Model based theory combination: Example

$\mathcal{T}_{\mathcal{E}}$			$\mathcal{T}_{\mathcal{A}}$	
Literals	Eq. Classes	Model	Literals	Model
$x = f(z)$	$\{x, f(z)\}$	$x^{\mathcal{E}} = *_1$	$0 \leq x \leq 1$	$x^{\mathcal{A}} = 0$
$f(x) \neq f(y)$	$\{y\}$	$y^{\mathcal{E}} = *_2$	$0 \leq y \leq 1$	$y^{\mathcal{A}} = 1$
$x \neq y$	$\{z\}$	$z^{\mathcal{E}} = *_3$	$z = y - 1$	$z^{\mathcal{A}} = 0$
	$\{f(x)\}$	$f^{\mathcal{E}} = \{*_1 \mapsto *_4,$	$x \neq y$	
	$\{f(y)\}$	$*_2 \mapsto *_5,$		
		$*_3 \mapsto *_1,$		
		$else \mapsto *_6\}$		

Assume $x = z$

Model based theory combination: Example

\mathcal{T}_E			\mathcal{T}_A	
Literals	Eq. Classes	Model	Literals	Model
$x = f(z)$	$\{x, z, f(x), f(z)\}$	$x^E = *_1$	$0 \leq x \leq 1$	$x^A = 0$
$f(x) \neq f(y)$	$\{y\}$	$y^E = *_2$	$0 \leq y \leq 1$	$y^A = 1$
$x \neq y$	$\{f(y)\}$	$z^E = *_1$	$z = y - 1$	$z^A = 0$
$x = z$		$f^E = \{*_1 \mapsto *_1,$ $*_2 \mapsto *_3,$ $else \mapsto *_4\}$	$x \neq y$	
			$x = z$	

Satisfiable

Model based theory combination: Example

$\mathcal{T}_{\mathcal{E}}$			$\mathcal{T}_{\mathcal{A}}$	
Literals	Eq. Classes	Model	Literals	Model
$x = f(z)$	$\{x, z, f(x), f(z)\}$	$x^{\mathcal{E}} = *_1$	$0 \leq x \leq 1$	$x^{\mathcal{A}} = 0$
$f(x) \neq f(y)$	$\{y\}$	$y^{\mathcal{E}} = *_2$	$0 \leq y \leq 1$	$y^{\mathcal{A}} = 1$
$x \neq y$	$\{f(y)\}$	$z^{\mathcal{E}} = *_1$	$z = y - 1$	$z^{\mathcal{A}} = 0$
$x = z$		$f^{\mathcal{E}} = \{*_1 \mapsto *_1,$ $*_2 \mapsto *_3,$ $\text{else} \mapsto *_4\}$	$x \neq y$ $x = z$	

Let h be the bijection between $S_{\mathcal{E}}$ and $S_{\mathcal{A}}$.

$$h = \{*_1 \mapsto 0, *_2 \mapsto 1, *_3 \mapsto -1, *_4 \mapsto 2, \dots\}$$

Model based theory combination: Example

$\mathcal{T}_{\mathcal{E}}$		$\mathcal{T}_{\mathcal{A}}$	
Literals	Model	Literals	Model
$x = f(z)$	$x^{\mathcal{E}} = *_1$	$0 \leq x \leq 1$	$x^{\mathcal{A}} = 0$
$f(x) \neq f(y)$	$y^{\mathcal{E}} = *_2$	$0 \leq y \leq 1$	$y^{\mathcal{A}} = 1$
$x \neq y$	$z^{\mathcal{E}} = *_1$	$z = y - 1$	$z^{\mathcal{A}} = 0$
$x = z$	$f^{\mathcal{E}} = \{*_1 \mapsto *_1,$ $*_2 \mapsto *_3,$ $else \mapsto *_4\}$	$x \neq y$	$f^{\mathcal{A}} = \{0 \mapsto 0$ $1 \mapsto -1$ $else \mapsto 2\}$

Extending \mathcal{A} using h .

$$h = \{*_1 \mapsto 0, *_2 \mapsto 1, *_3 \mapsto -1, *_4 \mapsto 2, \dots\}$$

Simplex: a model base theory solver

- ▶ Tableau: \mathcal{B} and \mathcal{N} denote the set of basic and nonbasic variables.

$$x_i = \sum_{x_j \in \mathcal{N}} a_{ij} x_j \quad x_i \in \mathcal{B},$$

- ▶ Solver stores upper and lower bounds l_i and u_i , and a mapping β that assigns a value $\beta(x_i)$ to every variable.
- ▶ The bounds on nonbasic variables are always satisfied by β , that is, the following invariant is maintained

$$\forall x_j \in \mathcal{N}, \quad l_j \leq \beta(x_j) \leq u_j.$$

- ▶ Bounds constraints for basic variables are not necessarily satisfied by β , but pivoting steps can be used to fix bounds violations.

Simplex: a model based theory solver

- ▶ The current model for the simplex solver is given by β .
- ▶ *Bound propagation*
 - ▶ *Equations + Bounds* can be used to derive *new bounds*.
 - ▶ Example: $x = y - z, y \leq 2, z \geq 3 \rightsquigarrow x \leq -1$.

Opportunistic equality propagation

- ▶ Efficient (and incomplete) methods for propagating equalities.
- ▶ Notation
 - ▶ A variable x_i is *fixed* iff $l_i = u_i$.
 - ▶ A linear polynomial $\sum_{x_j \in \mathcal{V}} a_{ij} x_j$ is fixed iff x_j is fixed or $a_{ij} = 0$.
 - ▶ Given a linear polynomial $P = \sum_{x_j \in \mathcal{V}} a_{ij} x_j$:
 $\beta(P)$ denotes $\sum_{x_j \in \mathcal{V}} a_{ij} \beta(x_j)$.

Opportunistic equality propagation

- ▶ Equality propagation in arithmetic:

FixedEq

$$l_i \leq x_i \leq u_i, \quad l_j \leq x_j \leq u_j \implies x_i = x_j \quad \text{if} \quad l_i = u_i = l_j = u_j$$

EqRow

$$x_i = x_j + P \implies x_i = x_j \quad \text{if} \quad P \text{ is fixed, and } \beta(P) = 0$$

EqOffsetRows

$$\begin{array}{l} x_i = x_k + P_1 \\ x_j = x_k + P_2 \end{array} \implies x_i = x_j \quad \text{if} \quad \left\{ \begin{array}{l} P_1 \text{ and } P_2 \text{ are fixed, and} \\ \beta(P_1) = \beta(P_2) \end{array} \right.$$

EqRows

$$\begin{array}{l} x_i = P + P_1 \\ x_j = P + P_2 \end{array} \implies x_i = x_j \quad \text{if} \quad \left\{ \begin{array}{l} P_1 \text{ and } P_2 \text{ are fixed, and} \\ \beta(P_1) = \beta(P_2) \end{array} \right.$$

Opportunistic theory/equality propagation

- ▶ These rules can miss some implied equalities.
- ▶ Example: $z = w$ is detected, but $x = y$ is not because w is not a fixed variable.

$$x = y + w + s$$

$$z = w + s$$

$$0 \leq z$$

$$w \leq 0$$

$$0 \leq s \leq 0$$

- ▶ Remark: bound propagation can be used imply the bound $0 \leq w$, making w a fixed variable.

Model mutation

- ▶ Sometimes $x^M = y^M$ by accident.
- ▶ *Model mutation*: diversify the current model.
- ▶ For a Simplex based procedure, *freedom intervals* \rightsquigarrow model mutation without pivoting.

Ackermann's reduction

- ▶ *Ackermann's reduction* is used to remove uninterpreted functions.
 - ▶ For each application $f(\vec{a})$ in ϕ create a fresh variable $f_{\vec{a}}$.
 - ▶ For each pair of applications $f(\vec{a}), f(\vec{c})$ in ϕ add the clause $\vec{a} \neq \vec{c} \vee f_{\vec{a}} = f_{\vec{c}}$.
 - ▶ Replace $f(\vec{a})$ with $f_{\vec{a}}$ in ϕ .
- ▶ It is used in some SMT solvers to reduce $\mathcal{T}_{\mathcal{L}\mathcal{A}} \cup \mathcal{T}_{\mathcal{E}}$ to $\mathcal{T}_{\mathcal{L}\mathcal{A}}$.
- ▶ *Main problem: quadratic number of new clauses.*
- ▶ It is also problematic to use this approach in the context of *several theories* and when combining SMT solvers with *quantifier instantiation*.

Ackermann's reduction

- ▶ Congruence closure based algorithms miss the following inference rule

$$f(\bar{n}) \neq f(\bar{m}) \implies \bigvee n_i \neq m_i$$

- ▶ Following simple formula takes $\mathcal{O}(2^N)$ time to be solved using SAT + Congruence closure.

$$\bigwedge_{i=1}^N (p_i \vee x_i = v_0), (\neg p_i \vee x_i = v_1), (p_i \vee y_i = v_0), (\neg p_i \vee y_i = v_1),$$
$$f(x_N, \dots, f(x_2, x_1) \dots) \neq f(y_N, \dots, f(y_2, y_1) \dots)$$

- ▶ It can be solved in polynomial time with Ackermann's reduction.
- ▶ A similar behavior is also observed in several pipeline verification problems.

Dynamic Ackermann's reduction

- ▶ This performance problem reflects a limitation in the current congruence closure algorithms used in SMT solvers.
- ▶ It is not related with the theory combination problem.
- ▶ *Dynamic Ackermannization*: clauses corresponding to Ackermann's reduction are added when a congruence rule participates in a conflict.

	CC		Ack		Dyn Ack	
	conflicts	time (s)	conflicts	time (s)	conflicts	time (s)
c10bi	217232	143.87	6880	6.09	5885	1.75
f10id	> 8752181	> 1800	22038	16.20	21220	7.20

Experimental Results

	#	MathSAT	MathSAT-dtc	Yices	Z3
EufLaArithmetic	52	1851.50 (11)	785.87 (1)	10.45	17.34
Hash	199	520.90	19.39	11.48	6.54
Wisa	256	886.36 (1)	6916.18	4.37	2.78
RandomCoupled	400	517.05	518.15	9516.11 (51)	56.16
RandomDecoupled	500	11989.60 (1)	97.07	19362.40 (51)	41.95
Simple	98	1366.33	7053.98 (29)	2328.63 (53)	1.00
Ackermann	99	228.49 (82)	344.00 (82)	2.99	1.72
Total	1604	17360.23 (95)	15734.64 (112)	31236.43 (155)	127.49

Experimental Results (cont.)

	Z3-dtc	Z3-dtc*	Z3-ack	Z3-neq	Z3-ndack	Z3
EufLaArithmetic	796.71 (11)	2830.38 (4)	1094.47 (1)	786.15	11.56	17.34
Hash	310.10	305.75	23.68	5.89	6.02	6.54
Wisa	364.71	385.06	12.31	4.89	2.40	2.78
RandomCoupled	8122.45 (166)	12451.82 (103)	101.24	56.45	56.65	56.16
RandomDecoupled	12421.30 (85)	15316.60 (71)	56.54	51.23	48.39	41.95
Simple	7.26	7.34	33.89	0.45	1.00	1.00
Ackermann	728.22 (77)	733.58 (77)	37.99	1.74	874.21 (77)	1.72
Total	22750.75 (339)	32030.53 (255)	1360.12 (1)	906.78	1000.23 (77)	127.49

Conclusion

- ▶ New theory combination method.
- ▶ Solves a number of practical deficiencies with other known solutions to integrating theories.
- ▶ Optimizations:
 - ▶ Opportunistic equality propagation.
 - ▶ Model mutation.
- ▶ Dynamic Ackermannization copes with limitations in the current congruence closure algorithms.
- ▶ We are experimenting with a model-based array theory.