Combinations of theories and the Bernays-Schönfinkel-Ramsey class

Pascal Fontaine

Loria

Verify'07

July 15-16

Bremen, Germany

Outline

Introduction

Formal development frameworks (e.g. B, TLA$^+$,...)

- generate a lot of proof obligations
- on expressive languages (for instance, set theory)

Validation platforms

- automation (for simple proofs)
- interactive tools (for difficult proofs)

SMT solvers?

Introduction

Formal development frameworks (e.g. B, TLA$^+$,. . .)

- generate a lot of proof obligations
- on expressive languages (for instance, set theory)

Validation platforms

- automation (for simple proofs)
- interactive tools (for difficult proofs)

SMT solvers?

SMT solvers expressivity

SMT solvers: incremental approach to raise expressivity

- SAT solvers

$$\neg\big[\,(p \Rightarrow q) \Rightarrow \big[\,(\neg p \Rightarrow q) \Rightarrow q\big]\big]$$

- Congruence closure (uninterpreted symbols + equality)

$$a = b \wedge \big[f(a) \neq f(b) \vee (p(a) \wedge \neg p(b))\big]$$

- Some arithmetic

$$a \leq b \wedge b \leq a + x \wedge x = 0 \wedge \big[f(a) \neq f(b) \vee (p(a) \wedge \neg p(b+x))\big]$$

- ... (Combination of theories)
- Sets

$$a \leq b \wedge b \leq a + x \wedge x = 0 \wedge f(a) \in (A \cap B) \wedge \big[f(a) \in A \setminus B \vee f(b) \notin B\big]$$

Bernays-Schönfinkel-Ramsey (BSR) theories

BSR class:

- decidable
- conjunction of $\exists^*\forall^*\varphi$ formulas
- φ quantifier-free, function-free
- $=$, predicates, constants, and Boolean connectives allowed

Examples :

- $\forall x, y. p(x, y) \equiv p(y, x)$
- $a \neq b \wedge a \neq c \wedge b \neq c \wedge \forall x. x = a \vee x = b \vee x = c$

Goal

Combining BSR (decidable) theories with other theories
Using linear arithmetic, uninterpreted symbols,... and predicates defined by a BSR theory

SMT solvers expressivity

SMT solvers: incremental approach to raise expressivity

- SAT solvers

$$\neg\big[\,(p \Rightarrow q) \Rightarrow \big[\,(\neg p \Rightarrow q) \Rightarrow q\big]\big]$$

- Congruence closure (uninterpreted symbols + equality)

$$a = b \wedge \big[f(a) \neq f(b) \vee (p(a) \wedge \neg p(b))\big]$$

- Some arithmetic

$$a \leq b \wedge b \leq a + x \wedge x = 0 \wedge \big[f(a) \neq f(b) \vee (p(a) \wedge \neg p(b + x))\big]$$

- ... (Combination of theories)
- Sets, relations, ...

$$a \leq b \wedge b \leq a + x \wedge x = 0 \wedge f(a) \in (A \cap B) \wedge \big[f(a) \in A \setminus B \vee f(b) \notin B\big]$$

Outline

1 Introduction

2 Combining BSR theories

- Combining disjoint decision procedures
- Combining non-stably infinite theories
- BSR theories and cardinalities

3 Conclusion

Combining disjoint decision procedures (1)

A combination of disjoint languages:

$$L = \{x \leq y,\, y \leq x + f(x),\, P(h(x) - h(y)),\, \neg P(0),\, f(x) = 0\}$$

uninterpreted symbols (P, f, h), and arithmetic ($+$, $-$, $\leq$, 0).

Combination of disjoint decision procedures

Combination of the empty theory and theory for linear arithmetic (both stably-infinite)

Separation using new variables:

$$\begin{array}{lcl} L_1 & = & \{x \leq y,\, y \leq x + v_1,\, v_1 = 0,\, v_2 = v_3 - v_4,\, v_5 = 0\} \\ L_2 & = & \{P(v_2),\, \neg P(v_5),\, v_1 = f(x),\, v_3 = h(x),\, v_4 = h(y)\}. \end{array}$$

L and $L_1 \cup L2$ both satisfiable or both unsatisfiable.

Combining disjoint decision procedures (2)

Cooperation by exchanging equalities:

$$\begin{aligned} L_1 &= \{x \le y,\, y \le x + v_1,\, v_1 = 0,\, v_2 = v_3 - v_4,\, v_5 = 0\} \\ L_2 &= \{P(v_2),\, \neg P(v_5),\, v_1 = f(x),\, v_3 = h(x),\, v_4 = h(y)\} \end{aligned}$$

From L_1, $x = y$:

$$\begin{aligned} L_1 &= \{x \le y,\, y \le x + v_1,\, v_1 = 0,\, v_2 = v_3 - v_4,\, v_5 = 0\} \\ L_2' &= \{P(v_2),\, \neg P(v_5),\, v_1 = f(x),\, v_3 = h(x),\, v_4 = h(y),\, x = y\} \end{aligned}$$

From L_2', $v_3 = v_4$:

$$\begin{aligned} L_1' &= \{x \le y,\, y \le x + v_1,\, v_1 = 0,\, v_2 = v_3 - v_4,\, v_5 = 0,\, v_3 = v_4\} \\ L_2' &= \{P(v_2),\, \neg P(v_5),\, v_1 = f(x),\, v_3 = h(x),\, v_4 = h(y),\, x = y\} \end{aligned}$$

From L_1', $v_2 = v_5$:

$$\begin{aligned} L_1' &= \{x \le y,\, y \le x + v_1,\, v_1 = 0,\, v_2 = v_3 - v_4,\, v_5 = 0,\, v_3 = v_4\} \\ L_2'' &= \{P(v_2),\, \neg P(v_5),\, v_1 = f(x),\, v_3 = h(x),\, v_4 = h(y),\, x = y,\, v_2 = v_5\} \end{aligned}$$

L_2'' is unsatisfiable.

Combining disjoint decision procedures (2)

Cooperation by exchanging equalities:

$$\begin{aligned} L_1 &= \{x \leq y,\, y \leq x + v_1,\, v_1 = 0, v_2 = v_3 - v_4,\, v_5 = 0\} \\ L_2 &= \{P(v_2),\, \neg P(v_5),\, v_1 = f(x),\, v_3 = h(x),\, v_4 = h(y)\} \end{aligned}$$

From L_1, $x = y$:

$$\begin{aligned} L_1 &= \{x \leq y,\, y \leq x + v_1,\, v_1 = 0,\, v_2 = v_3 - v_4,\, v_5 = 0\} \\ L_2' &= \{P(v_2),\, \neg P(v_5),\, v_1 = f(x),\, v_3 = h(x),\, v_4 = h(y),\, x = y\} \end{aligned}$$

From L_2', $v_3 = v_4$:

$$\begin{aligned} L_1' &= \{x \leq y,\, y \leq x + v_1,\, v_1 = 0,\, v_2 = v_3 - v_4,\, v_5 = 0, v_3 = v_4\} \\ L_2' &= \{P(v_2),\, \neg P(v_5),\, v_1 = f(x),\, v_3 = h(x),\, v_4 = h(y),\, x = y\} \end{aligned}$$

From L_1', $v_2 = v_5$:

$$\begin{aligned} L_1' &= \{x \leq y,\, y \leq x + v_1,\, v_1 = 0,\, v_2 = v_3 - v_4,\, v_5 = 0, v_3 = v_4\} \\ L_2'' &= \{P(v_2),\, \neg P(v_5),\, v_1 = f(x),\, v_3 = h(x),\, v_4 = h(y),\, x = y, v_2 = v_5\} \end{aligned}$$

L_2'' is unsatisfiable.

Combining disjoint decision procedures (2)

Cooperation by exchanging equalities:

$$\begin{aligned} L_1 &= \{x \le y,\ y \le x + v_1,\ v_1 = 0, v_2 = v_3 - v_4,\ v_5 = 0\} \\ L_2 &= \{P(v_2),\ \neg P(v_5),\ v_1 = f(x),\ v_3 = h(x),\ v_4 = h(y)\} \end{aligned}$$

From L_1, $x = y$:

$$\begin{aligned} L_1 &= \{x \le y, y \le x + v_1,\ v_1 = 0,\ v_2 = v_3 - v_4,\ v_5 = 0\} \\ L_2' &= \{P(v_2),\ \neg P(v_5),\ v_1 = f(x),\ v_3 = h(x),\ v_4 = h(y),\ x = y\} \end{aligned}$$

From L_2', $v_3 = v_4$:

$$\begin{aligned} L_1' &= \{x \le y, y \le x + v_1,\ v_1 = 0,\ v_2 = v_3 - v_4,\ v_5 = 0, v_3 = v_4\} \\ L_2' &= \{P(v_2),\ \neg P(v_5),\ v_1 = f(x),\ v_3 = h(x),\ v_4 = h(y),\ x = y\} \end{aligned}$$

From L_1', $v_2 = v_5$:

$$\begin{aligned} L_1' &= \{x \le y, y \le x + v_1,\ v_1 = 0,\ v_2 = v_3 - v_4,\ v_5 = 0, v_3 = v_4\} \\ L_2'' &= \{P(v_2),\ \neg P(v_5),\ v_1 = f(x),\ v_3 = h(x),\ v_4 = h(y),\ x = y, v_2 = v_5\} \end{aligned}$$

L_2'' is unsatisfiable.

Combining disjoint decision procedures (2)

Cooperation by exchanging equalities:

$$\begin{array}{rcl} L_1 & = & \{x \leq y, y \leq x + v_1, v_1 = 0, v_2 = v_3 - v_4, v_5 = 0\} \\ L_2 & = & \{P(v_2), \neg P(v_5), v_1 = f(x), v_3 = h(x), v_4 = h(y)\} \end{array}$$

From L_1, $x = y$:

$$\begin{array}{rcl} L_1 & = & \{x \leq y, y \leq x + v_1, v_1 = 0, v_2 = v_3 - v_4, v_5 = 0\} \\ L_2' & = & \{P(v_2), \neg P(v_5), v_1 = f(x), v_3 = h(x), v_4 = h(y), x = y\} \end{array}$$

From L_2', $v_3 = v_4$:

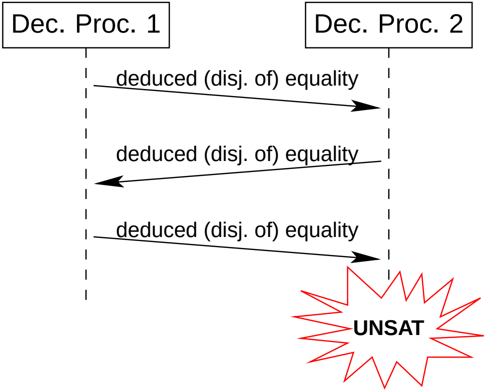
$$\begin{array}{rcl} L_1' & = & \{x \leq y, y \leq x + v_1, v_1 = 0, v_2 = v_3 - v_4, v_5 = 0, v_3 = v_4\} \\ L_2' & = & \{P(v_2), \neg P(v_5), v_1 = f(x), v_3 = h(x), v_4 = h(y), x = y\} \end{array}$$

From L_1', $v_2 = v_5$:

$$\begin{array}{rcl} L_1' & = & \{x \leq y, y \leq x + v_1, v_1 = 0, v_2 = v_3 - v_4, v_5 = 0, v_3 = v_4\} \\ L_2'' & = & \{P(v_2), \neg P(v_5), v_1 = f(x), v_3 = h(x), v_4 = h(y), x = y, v_2 = v_5\} \end{array}$$

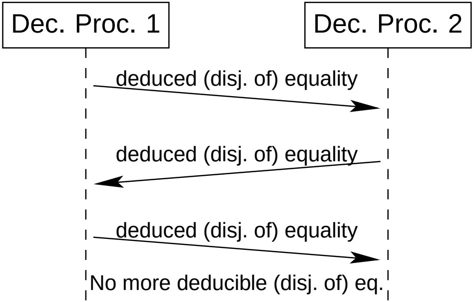
L_2'' is unsatisfiable.

Combining disj. DPs : "unsatisfiable" scenario



OK : every deduced fact is a consequence of the original set of formulas

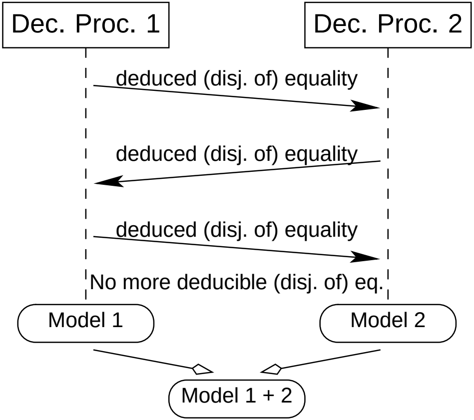
Combining disj. DPs : “satisfiable” scenario



Really SAT?

- all disjunctions of equalities propagated
- models agree on cardinalities

Combining disj. DPs : "satisfiable" scenario



Really SAT?

- all disjunctions of equalities propagated
- **models agree on cardinalities**

Ensuring agreement on cardinalities?

Different frameworks (and capabilities)

- Nelson-Oppen:
  requirement on theories: stably infinite (not suitable for BSR)
  if satisfiable, there is an infinite model (FOL theories $\Rightarrow \aleph_0$)
- Combining with the empty theory (and some others):
  the empty theory does not constraint much the cardinalities
- BSR theory and theory with only finite models:
  check every finite model against BSR theory

We show:

- possible to know exactly accepted cardinalities for BSR theory
- thus, combination possible if other theory can say if it accepts given cardinality

BSR theories and cardinalities

Well-known result:

Finite model property

If a BSR theory has a model, it has a finite model
Size: at most the number of ground terms k

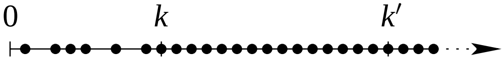
Simple property

- If it has a model with cardinality j, it has a model for every j' such that $k \leq j' \leq j$

BSR theories and cardinalities (2)

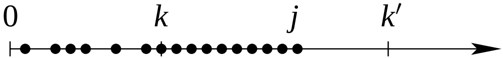
Two scenarios for a given BSR theory

- has infinite model, and accepts models for every cardinality $\geq k$



  Combination? Check if other theory accepts model greater than k

- has no infinite model, and accepts a finite number of cardinalities, all cardinalities between k and the max j being accepted



  Combination? Finite number of cardinalities to check

How to know which scenario occurs?
Does a BSR theory has an infinite model?

BSR theories and cardinalities (3)

Theorem

A BSR-theory has an infinite model if and only if it has a finite model with some (see paper) symmetry properties

Checking if such a finite model exists is decidable

From set (or relation) operators to BSR

For instance:

$$a = b \wedge (\{f(a)\} \cup E) \subseteq A \wedge f(b) \notin C \wedge A \cup B = C \cap D$$

becomes

$$a = b \wedge \forall x[(x = f(a) \vee E(x)) \Rightarrow A(x)] \wedge \neg C(f(b)) \\ \wedge \forall x.\ [A(x) \vee B(x)] \equiv [C(x) \wedge D(x)]$$

with separation variables:

$$a = b \wedge y = f(a) \wedge z = f(b) \wedge \\ \forall x[(x = y \vee E(x)) \Rightarrow A(x)] \wedge \neg C(z) \wedge \forall x.\ [A(x) \vee B(x)] \equiv [C(x) \wedge D(x)]$$

Finally: combination of a BSR theory with empty theory

From set (or relation) operators to BSR

For instance:

$$a = b \wedge (\{f(a)\} \cup E) \subseteq A \wedge f(b) \notin C \wedge A \cup B = C \cap D$$

becomes

$$a = b \wedge \forall x[(x = f(a) \vee E(x)) \Rightarrow A(x)] \wedge \neg C(f(b))$$
$$\wedge \forall x.\ [A(x) \vee B(x)] \equiv [C(x) \wedge D(x)]$$

with separation variables:

$$a = b \wedge y = f(a) \wedge z = f(b) \wedge$$
$$\forall x[(x = y \vee E(x)) \Rightarrow A(x)] \wedge \neg C(z) \wedge \forall x.\ [A(x) \vee B(x)] \equiv [C(x) \wedge D(x)]$$

Finally: combination of a BSR theory with empty theory

Outline

Conclusion

- BSR theory has an infinite model? decidable
- decidability result on combining BSR theories
- removing strong requirements from previous combination frameworks
  - BSR + theories with infinite models
  - BSR + linear arithmetic + uninterpreted symbols + arrays +...
- Adding set (relation,...) operators to language of SMT solvers
- First prototype for the combination with the empty theory
- Future work: the general case *in practice*, proof reconstruction (w.i.p.)