Combinations of theories and the Bernays-Schönfinkel-Ramsey class

Pascal Fontaine

Verify’07
July 15-16
Bremen, Germany
Outline

1. Introduction
2. Combining BSR theories
3. Conclusion
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
  \[ \neg \left[ (p \Rightarrow q) \Rightarrow \left[ (\neg p \Rightarrow q) \Rightarrow q \right] \right] \]

- Congruence closure (uninterpreted symbols + equality)
  \[ a = b \land \left[ f(a) \neq f(b) \lor (p(a) \land \neg p(b)) \right] \]

- Some arithmetic
  \[ a \leq b \land b \leq a + x \land x = 0 \land \left[ f(a) \neq f(b) \lor (p(a) \land \neg p(b + x)) \right] \]

- … (Combination of theories)

- Sets
  \[ a \leq b \land b \leq a + x \land x = 0 \land f(a) \in (A \cap B) \land \left[ f(a) \in A \setminus B \lor f(b) \notin B \right] \]
Bernays-Schönfinkel-Ramsey (BSR) theories

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

Examples:
- $\forall x, y. p(x, y) \equiv p(y, x)$
- $a \neq b \land a \neq c \land b \neq c \land \forall x. x = a \lor x = b \lor x = c$

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

\[ \neg \left[ (p \Rightarrow q) \Rightarrow \left[ (\neg p \Rightarrow q) \Rightarrow q \right] \right] \]

- Congruence closure (uninterpreted symbols + equality)

\[ a = b \land \left[ f(a) \neq f(b) \lor (p(a) \land \neg p(b)) \right] \]

- Some arithmetic

\[ a \leq b \land b \leq a + x \land x = 0 \land \left[ f(a) \neq f(b) \lor (p(a) \land \neg p(b + x)) \right] \]

- ... (Combination of theories)

- Sets, relations, ...

\[ a \leq b \land b \leq a + x \land x = 0 \land f(a) \in (A \cap B) \land \left[ f(a) \in A \setminus B \lor f(b) \notin B \right] \]
Combining BSR theories

Outline

1. Introduction

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

3. Conclusion
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:

\[ L_1 = \{ x \leq y, \ y \leq x + v_1, \ v_1 = 0, \ v_2 = v_3 - v_4, \ v_5 = 0 \} \]

\[ L_2 = \{ P(v_2), \ \neg P(v_5), \ v_1 = f(x), \ v_3 = h(x), \ v_4 = h(y) \}. \]

\(L\) and \(L_1 \cup L_2\) both satisfiable or both unsatisfiable.
Combining disjoint decision procedures (2)

Cooperation by exchanging equalities:

\[ L_1 = \{ x \leq y, y \leq x + v_1, v_1 = 0, v_2 = v_3 - v_4, v_5 = 0 \} \]
\[ L_2 = \{ P(v_2), \neg P(v_5), v_1 = f(x), v_3 = h(x), v_4 = h(y) \} \]

From \( L_1, x = y \):
\[ L_1' = \{ x \leq y, y \leq x + v_1, v_1 = 0, v_2 = v_3 - v_4, v_5 = 0 \} \]
\[ L_2' = \{ P(v_2), \neg P(v_5), v_1 = f(x), v_3 = h(x), v_4 = h(y), x = y \} \]

From \( L_2', v_3 = v_4 \):
\[ L_1' = \{ x \leq y, y \leq x + v_1, v_1 = 0, v_2 = v_3 - v_4, v_5 = 0, v_3 = v_4 \} \]
\[ L_2' = \{ P(v_2), \neg P(v_5), v_1 = f(x), v_3 = h(x), v_4 = h(y), x = y \} \]

From \( L_1', v_2 = v_5 \):
\[ L_1'' = \{ x \leq y, y \leq x + v_1, v_1 = 0, v_2 = v_3 - v_4, v_5 = 0, v_3 = v_4 \} \]
\[ L_2'' = \{ P(v_2), \neg P(v_5), v_1 = f(x), v_3 = h(x), v_4 = h(y), x = y, v_2 = v_5 \} \]

\( L_2'' \) is unsatisfiable.
Combining disjoint decision procedures (2)

Cooperation by exchanging equalities:

\[ L_1 = \{ x \leq y, y \leq x + v_1, v_1 = 0, v_2 = v_3 - v_4, v_5 = 0 \} \]
\[ L_2 = \{ P(v_2), \neg P(v_5), v_1 = f(x), v_3 = h(x), v_4 = h(y) \} \]

From \( L_1, x = y \):

\[ L_1' = \{ x \leq y, y \leq x + v_1, v_1 = 0, v_2 = v_3 - v_4, v_5 = 0 \} \]
\[ L_2' = \{ P(v_2), \neg P(v_5), v_1 = f(x), v_3 = h(x), v_4 = h(y), x = y \} \]

From \( L_2', v_3 = v_4 \):

\[ L_1' = \{ x \leq y, y \leq x + v_1, v_1 = 0, v_2 = v_3 - v_4, v_5 = 0, v_3 = v_4 \} \]
\[ L_2' = \{ P(v_2), \neg P(v_5), v_1 = f(x), v_3 = h(x), v_4 = h(y), x = y \} \]

From \( L_1', v_2 = v_5 \):

\[ L_1'' = \{ x \leq y, y \leq x + v_1, v_1 = 0, v_2 = v_3 - v_4, v_5 = 0, v_3 = v_4 \} \]
\[ L_2'' = \{ P(v_2), \neg P(v_5), v_1 = f(x), v_3 = h(x), v_4 = h(y), x = y, v_2 = v_5 \} \]

\( L_2'' \) is unsatisfiable.
Combining disjoint decision procedures (2)

Cooperation by exchanging equalities:

\[
L_1 = \{ x \leq y, y \leq x + v_1, v_1 = 0, v_2 = v_3 - v_4, v_5 = 0 \}
\]
\[
L_2 = \{ P(v_2), \neg P(v_5), v_1 = f(x), v_3 = h(x), v_4 = h(y) \}
\]

From \( L_1 \), \( x = y \):

\[
L'_{1} = \{ x \leq y, y \leq x + v_1, v_1 = 0, v_2 = v_3 - v_4, v_5 = 0 \}
\]
\[
L'_{2} = \{ P(v_2), \neg P(v_5), v_1 = f(x), v_3 = h(x), v_4 = h(y), x = y \}
\]

From \( L'_2 \), \( v_3 = v_4 \):

\[
L''_{1} = \{ x \leq y, y \leq x + v_1, v_1 = 0, v_2 = v_3 - v_4, v_5 = 0, v_3 = v_4 \}
\]
\[
L''_{2} = \{ P(v_2), \neg P(v_5), v_1 = f(x), v_3 = h(x), v_4 = h(y), x = y \}
\]

From \( L'_1 \), \( v_2 = v_5 \):

\[
L'_{1} = \{ x \leq y, y \leq x + v_1, v_1 = 0, v_2 = v_3 - v_4, v_5 = 0, v_3 = v_4 \}
\]
\[
L'_{2} = \{ P(v_2), \neg P(v_5), v_1 = f(x), v_3 = h(x), v_4 = h(y), x = y, v_2 = v_5 \}
\]

\( L''_{2} \) is unsatisfiable.
Combining disjoint decision procedures (2)

Cooperation by exchanging equalities:

\[ L_1 = \{ x \leq y, y \leq x + v_1, v_1 = 0, v_2 = v_3 - v_4, v_5 = 0 \} \]
\[ L_2 = \{ P(v_2), \neg P(v_5), v_1 = f(x), v_3 = h(x), v_4 = h(y) \} \]

From \( L_1 \), \( x = y \):

\[ L_1' = \{ x \leq y, y \leq x + v_1, v_1 = 0, v_2 = v_3 - v_4, v_5 = 0 \} \]
\[ L_2' = \{ P(v_2), \neg P(v_5), v_1 = f(x), v_3 = h(x), v_4 = h(y), x = y \} \]

From \( L_2' \), \( v_3 = v_4 \):

\[ L_1' = \{ x \leq y, y \leq x + v_1, v_1 = 0, v_2 = v_3 - v_4, v_5 = 0, v_3 = v_4 \} \]
\[ L_2' = \{ P(v_2), \neg P(v_5), v_1 = f(x), v_3 = h(x), v_4 = h(y), x = y \} \]

From \( L_1' \), \( v_2 = v_5 \):

\[ L_1' = \{ x \leq y, y \leq x + v_1, v_1 = 0, v_2 = v_3 - v_4, v_5 = 0, v_3 = v_4 \} \]
\[ L_2'' = \{ P(v_2), \neg P(v_5), v_1 = f(x), v_3 = h(x), v_4 = h(y), x = y, v_2 = v_5 \} \]

\( L_2'' \) is unsatisfiable.
Combining disjoint decision procedures

Combining disjoint DPs: "unsatisfiable" scenario

Dec. Proc. 1

\[ \text{deduced (disj. of) equality} \]

Dec. Proc. 2

\[ \text{deduced (disj. of) equality} \]

\[ \text{deduced (disj. of) equality} \]

\[ \text{UNSAT} \]

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

Combining disjoint decision procedures

Combining disj. DPs: “satisfiable” scenario

Dec. Proc. 1

\[\text{deduced (disj. of) equality}\]

Dec. Proc. 2

\[\text{deduced (disj. of) equality}\]

Really SAT?

- all disjunctions of equalities propagated
- models agree on cardinalities

No more deducible (disj. of) eq.
Combining disjoint decision procedures

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 $k \leq j' \leq j$
Two scenarios for a given BSR theory

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

\[
\begin{array}{ccc}
0 & k & k' \\
\vdots & \ddots & \ddots & \ddots
\end{array}
\]

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

\[
\begin{array}{ccc}
0 & k & j & k' \\
\vdots & \ddots & \ddots & \ddots & \ddots
\end{array}
\]

Combination? Finite number of cardinalities to check

How to know which scenario occurs?

Does a BSR theory has an infinite model?
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
Combining BSR theories and cardinalities

From set (or relation) operators to BSR

For instance:

\[ a = b \land (\{f(a)\} \cup E) \subseteq A \land f(b) \notin C \land A \cup B = C \cap D \]

becomes

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

with separation variables:

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

Finally: combination of a BSR theory with empty theory
For instance:

\[ a = b \land (\{f(a)\} \cup E) \subseteq A \land f(b) \notin C \land A \cup B = C \cap D \]

becomes

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

with separation variables:

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

Finally: combination of a BSR theory with empty theory
Outline

1. Introduction
2. Combining BSR theories
3. 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 +... Addiing 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.)