Proof-producing decision procedures and their combination

Silvio Ranise, Christophe Ringeissen, Duc-Khanh Tran

LORIA — Nancy

The Combination Problem

Verification conditions typically are in combination of many data-structures/theories

- arithmetic
- arrays
- lists
- Bit vectors
- uninterpreted function symbols
- ...

Proof-Producing decision procedures to improve the efficiency of SMT provers
➨ *small conflict sets* allow us to have a better pruning of Boolean assignments

Conflict Sets

A conflict set is an unsatisfiable set of literals
A conflict set CS is *minimal* if there no $CS' \subset CS$ such that CS' is a conflict set

An explanation for $x = y$ is a satisfiable set of literals wich entails $x = y$.
An explanation EX for $x = y$ is *minimal* if there is no $EX' \subset EX$ such that EX' is an explanation for $x = y$

Remark: an explanation EX is minimal for $x = y$ iff $EX \cup \{x \neq y\}$ is a minimal conflict set

Problems:

- How to design decision procedures computing a *small* conflict set in case of unsatisfiability?
- How to design decision procedures computing *small* explanations for entailed equalities in case of satisfiability?

Outline

- Encoding proofs in explanation graphs
- Explaining Congruence Closure ($\mathcal{E}$)
- Explaining Gauss Elimination ($\mathcal{LA}$)
- Explaining in the combination $\mathcal{E} \cup \mathcal{LA}$
- Understanding the explanation result: introduction of *quasi-conflict sets*, computation of *minimal* quasi-conflict sets
- a uniform way to explain the Congruence Closure method and the Nelson-Oppen combination method

Explanation Graphs: an Intuition

A labelled graph whose vertices are variables to encode the entailment of equalities between variables (also called **elementary equalities**)

Labels provide explanations

Key observation: the entailment of elementary equalities is crucial both for the Congruence Closure method and the Nelson-Oppen combination method

Explanation Graphs: Example of Congruence Closure

Init $\Omega; E; G \vdash$

$\Omega; E; Insert(G, z = z', \{z = t, z' = t\})$

if $\begin{cases} z = t, z' = t \in \Omega \\ z \neq z', (z, z') \notin CP(G) \end{cases}$

Ins $\Omega; E \cup \{x = x'\}; G \vdash$

$\Omega; E; Insert(G, x = x', \{x = x'\})$

if $x \neq x', (x, x') \notin CP(G)$

Explaining Congruence Closure (continued)

Skip $\quad \Omega; E \cup \{x = x'\}; G \vdash$

$\Omega; E; G$

if $x = x'$ or $(x, x') \in CP(G)$

Cong $\quad \Omega; E; G \vdash$

$$\Omega; E; Insert(G, z = z', \{z = f(y_1, \ldots, y_n), z' = f(y'_1, \ldots, y'_n)\} \cup \bigcup_{j \in J} \{y_j = y'_j\})$$

if
$$\begin{cases} z = f(y_1, \ldots, y_n), z' = f(y'_1, \ldots, y'_n) \in \Omega \\ z \neq z', (z, z') \notin CP(G) \\ I, J \text{ is a partition of } \{1, \ldots, n\} \text{ such that } J \neq \emptyset \text{ and} \\ (\forall i \in I : y_i = y'_i), (\forall j \in J : (y_j, y'_j) \in CP(G)) \end{cases}$$

Explanation Graphs: Formal Definition

Definition 1 *Let φ be a set of literals, $G = (V, E)$ be an acyclic unoriented graph, and $<$ be an ordering relation on E. G is an* explanation graph *of φ w.r.t. $<$ if (i) V is the set of constants occurring in φ, (ii) there exists a labelling function $\mathcal{L}_G$ with domain E and codomain $\mathbf{2}^{\varphi} \cup \mathbf{2}^{CP(G)}$, (iii) the following properties are satisfied for any $v_1 = v_2 \in E$:*

(iii.a) $\mathcal{L}_G(v_1 = v_2)$ is satisfiable and $\mathcal{L}_G(v_1 = v_2) \models v_1 = v_2$,

(iii.b) for each $v_1' = v_2'$ in $\mathcal{L}_G(v_1 = v_2) \backslash \varphi$ we have that $e < (v_1 = v_2)$, for any e in $ElemPath(G, v_1', v_2')$.

An explanation graph is said edge-minimal *if all its edges are minimally explained.*

Explaining Gauss Elimination

Key idea: Use of labelled equalities. If $\ell_1 : t_1 = 0$ and $\ell_2 : t_2 = 0$ are linearly combined so to obtain $t_1 + c * t_2 = 0$, then its label will be the expression $\ell_1 + c * \ell_2$.

Lemma 1 *Given the unsatisfiable set of k equalities $l_1 : e_1, l_2 : e_2, \ldots, l_k : e_k$, let $l'_1 : e'_1, l'_2 : e'_2, \ldots, l'_k : e'_k$ be the set of equalities obtained after running* GA. *If the equality $l'_h : e'_h$ for $h \in \{1, ..., k\}$ is unsatisfiable (i.e. e'_h is of the form $0 = c$ and $c \neq 0$ or $s = 0$ and s is a fresh variable), then the set $CS := \{e_i | l_i : e_i$ s.t. l_i occurs in $l'_h\}$ is a minimal conflict set.*

A similar lemma for the explanation of an elementary equality (after back-substitution).

➨ possible construction of an edge-minimal explanation graph in case of satisfiability

Combining Conflict Sets

- Adapt the Nelson-Oppen combination method
- Use of an explanation graph to store entailed elementary equalities
- Return more than true or false...

Combination Algorithm

$\mathsf{Unsat}_{=1}$ $\quad \Gamma_1; \Delta_V; G; \Gamma_2 \vdash$

$$false\{(CS_{T_1}(\Gamma_1 \cup Eq(G)) \cap \Gamma_1, CS_{T_1}(\Gamma_1 \cup Eq(G)) \backslash \Gamma_1, G)\}$$

if $\Gamma_1 \cup Eq(G)$ is T_1-unsatisfiable

$\mathsf{Unsat}_{\neq}$ $\quad \Gamma_1; \Delta_V; G; \Gamma_2 \vdash$

$$false\{(\{x \neq y\}, \{x = y\}, G)\}$$

if $(x, y) \in CP(G)$ and $x \neq y \in \Delta_V$

$\mathsf{Deduction}_1$ $\quad \Gamma_1; \Delta_V; G; \Gamma_2 \vdash$

$$\Gamma_1; \Delta_V; G', \Gamma_2$$

$$\text{if } \begin{cases} \Gamma_1 \cup Eq(G) \text{ is } T_1\text{-satisfiable} \\ T_1 \cup (\Gamma_1 \cup Eq(G)) \models x = y \\ (x, y) \notin CP(G) \\ G' = Insert(G, x = y, EX_{T_1}^{x=y}(\Gamma_1 \cup Eq(G))) \end{cases}$$

Interest of this Combination Algorithm

- What is the result (ψ, E, G) computed by the combination algorithm?
- Does it lead to a *small* conflict set?
- This combination algorithm is not well-suited for $\mathcal{E}$, since the Congruence Closure does not return minimal explanations...

Quasi-Conflict Sets

Definition 2 *Let φ be an unsatisfiable set of literals, ψ be a satisfiable (strict) subset of φ, G be a explanation graph of φ w.r.t. some $<$, and E be a set of equalities. The triplet (ψ, E, G) is a* quasi-conflict set *of φ w.r.t. $<$ if $E \subseteq CP(G)$ and $\psi \cup E$ is unsatisfiable. The triplet (ψ, E, G) is a* minimal quasi-conflict set *if there is no smaller quasi-conflict set (ψ', E', G') of φ w.r.t. $<$.*

Ordering on quasi-conflict sets:

$(\psi', E', G') \preceq (\psi, E, G)$ if $\psi' \subseteq \psi$, $E' \subseteq E$ and $G' \sqsubseteq G$

Ordering on labelled graphs:

$G' \sqsubseteq G$ if $Edge(G') \subseteq Edge(G)$ and
$\forall e \in Edge(G'),\ \mathcal{L}_{G'}(e) \subseteq \mathcal{L}_G(e)$.

How to Get Minimal Quasi-Conflict Sets

Theorem 1 *Let (ψ, E, G) be a quasi-conflict set of φ such that $\psi \cup E$ is a minimal conflict set. If all edges of $G_{|E}$ are minimally explained then $(\psi, E, G_{|E})$ is a minimal quasi-conflict set of φ.*

Notation: $G_{|E}$ denotes the subgraph of G which allows us to explain elementary equalities in E.

Minimal Quasi-Conflict Sets for the Theory of Equality

Corollary 1 *Let Ω be a set of $\mathcal{E}$-literals in flat solved form, let E be a set of elementary equalities and let Δ_V be a set elementary disequalities. Consider $\varphi = (\Omega \cup E \cup \Delta_V)$ and $G = CC(\Omega, E)$ be the edge-minimal complete explanation graph of $\Omega \cup E$ computed by the Congruence Closure algorithm with Explanation. If there exist x, y such that $x \neq y \in \Delta_V$ and $(x, y) \in CP(G)$, then φ is unsatisfiable and $(\{x \neq y\}, \{x = y\}, G_{|\{x=y\}})$ is a* **minimal quasi-conflict set** *of φ. Otherwise, φ is satisfiable.*

Minimal Quasi-Conflict Sets for the Union of Theories

Corollary 2 *Let T_1 and T_2 be two disjoint convex and stably infinite theories such that for each $i = 1, 2$, a T_i-satisfiability procedure is known. Let Ω_i be a set of T_i-equalities in solved form for $i = 1, 2$, let E be a set of elementary equalities and let Δ_V be a set of elementary disequalities. Consider $\varphi = (\Omega_1 \cup \Omega_2 \cup \Delta_V \cup E)$ and cf be a final configuration obtained by the repeated application of combination rules of on the initial configuration $\Omega_1; \Delta_V; UF^{Var(\varphi)}(E); \Omega_2$.*

- *If cf is of the form $false\{(\Omega', E', G)\}$, then φ is $T_1 \cup T_2$-unsatisfiable. Furthermore, $(\Omega', E', G_{|E'})$ is a quasi-conflict set of φ, which is minimal if $\Omega' \cup E'$ is a minimal conflict set and if all edges of $G_{|E'}$ are minimally explained.*
- *Otherwise, φ is $T_1 \cup T_2$-satisfiable.*

Small Explanation Engines: a Better Interface

A better result requires a better interface using quasi-conflict sets instead of conflict sets!

Basic idea: component decision procedures should return quasi-conflict sets instead of conflict sets, and in any case **edge-minimal** explanation graphs

More precisely:

- If UNSAT, then return (ψ, E, G) such that ... and G is **edge-minimal**
- If SAT, then return (ψ, E, G) such that G is an **edge-minimal** explanation graph storing more entailed elementary equalities, if possible.

Small Explanation Engines: Formal Definition

Definition 3 *Let T be a theory. A* small explanation engine (resp. small flat explanation engine) for T *is a computable function μEX such that: given a set Ω of T-equalities in solved form (resp. a set T-equalities in flat solved form) and a set E of elementary equalities, $\mu EX(\Omega, E)$ returns a triplet (Ω', E', G) satisfying the following properties:*

- $\Omega' \subseteq \Omega$,
- E' *is a set of elementary equalities,*
- G *is an* **edge-minimal** *explanation graph of $\Omega \cup E$,*
- *if $\Omega \cup E$ is T-unsatisfiable, then $\Omega' \cup E'$ is a* **minimal** *conflict set and $E' \subseteq CP(G)$,*
- *if $\Omega \cup E$ is T-satisfiable, then $\Omega' = \emptyset$, $E' \supseteq E$, $E' \backslash E \subseteq CP(G)$, and ($E' = E$ iff E is complete for $\Omega \cup E$ modulo T).*

Remark: $\Omega \cup E$ is T-satisfiable iff $\Omega' = \emptyset$.

Small Explanation Engine: Examples

Theory $\mathcal{E}$:

Function $\mu EX_{\mathcal{E}}(\Omega, E)$

$G := CC(\Omega, E)$

Return $(\emptyset, Eq(G), G)$

Theory $T = \mathcal{LA}$:

Function $\mu EX_T(\Omega, E)$

$G := UF^{Var(\Omega)}(E)$

If $\Omega \cup E$ is T-unsatisfiable **Then**

$\Omega' := CS_T(\Omega \cup E) \cap \Omega$

$E' := CS_T(\Omega \cup E) \backslash \Omega$

Else

If $(\exists x = y : (x, y) \notin CP(G) \ \wedge \ T \models \Omega \cup E \Rightarrow x = y)$ **Then**

$G := Insert(G, x = y, EX_T^{x=y}(\Omega \cup E))$

$E' := E \cup \{x = y\}$

Else $E' := E$

Return (Ω', E', G)

Combination Algorithm: New Interface

$\mathsf{Unsat}_{=1}$ $\quad \Omega_1; \Delta_V; G; \Omega_2 \vdash$

$$false\{(\Omega_1', E_1', G')\}$$

$$\text{if } \begin{cases} \mu EX_1(\Omega_1, Eq(G)) = (\Omega_1', E_1', G_1) \\ \Omega_1' \neq \emptyset \\ G' = Merge(G, G_1) \end{cases}$$

$\mathsf{Unsat}_{\neq}$ $\quad \Omega_1; \Delta_V; G; \Omega_2 \vdash$

$$false\{(\{x \neq y\}, \{x = y\}, G)\}$$

$$\text{if } (x, y) \in CP(G) \text{ and } x \neq y \in \Delta_V$$

$\mathsf{Deduction}_1$ $\quad \Omega_1; \Delta_V; G; \Omega_2 \vdash$

$$\Omega_1; \Delta_V; G'; \Omega_2$$

$$\text{if } \begin{cases} \mu EX_1(\Omega_1, Eq(G)) = (\emptyset, E_1, G_1) \\ G' = Merge(G, G_1) \\ G' \neq G \end{cases}$$

Main Result I

Theorem 2 *Let T_1 and T_2 be two disjoint convex and stably infinite theories such that for each $i = 1, 2$, a small explanation engine for T_i is known. Let Ω_i be a set of T_i-equalities in solved form for $i = 1, 2$, let E be a set of elementary equalities and let Δ_V be a set of elementary disequalities. Consider $\varphi = (\Omega_1 \cup \Omega_2 \cup \Delta_V \cup E)$ and cf be a final configuration obtained by the repeated application of the* improved combination rules *of on the initial configuration $\Omega_1; \Delta_V; UF^{Var(\varphi)}(E); \Omega_2$.*

- *If cf is of the form $false\{(\Omega', E', G)\}$, then φ is $T_1 \cup T_2$-unsatisfiable. Furthermore, $\Omega' \cup E'$ is a minimal conflict set and $(\Omega', E', G_{|E'})$ is a* **minimal quasi-conflict set***.*
- *Otherwise, cf is of the form $\Omega_1; \Delta_V; G; \Omega_2$ and φ is $T_1 \cup T_2$-satisfiable. Furthermore, G is complete for φ modulo $T_1 \cup T_2$.*

Main Result II

Corollary 3 (Modular construction of small explanation engines) *Let T_1 and T_2 be two signature-disjoint, convex, and stably infinite theories such that for each $i = 1, 2$, a small flat explanation engine for T_i is known. Then, the* improved combination algorithm *provides a small flat explanation engine for $T_1 \cup T_2$.*

Design of Decision Procedures

- Combining with non stably infinite theories: application to data-structures
  ➨ Ranise, Ringeissen, Zarba (FroCoS'05)
- Combining with superposition-based decision procedures
  ➨ Ranise, Ringeissen, Tran (ICTAC'05)
- SMT($T_1 \cup T_2$)
  ➨ Cimatti, ..., Ranise, ... (CAV'05)

Implementation of Decision Procedures

A new version of haRVey by Pascal Fontaine (LORIA)

- SAT solver instead of BDDs: zChaff, MiniSAT
- A better implementation of the combination of the theory of equality and linear arithmetic on rationals and integers
- A parser for SMT-LIB
- *dynamic theories*: a way to handle sets, relations, arrays, ..., thanks to Congruence Closure (and instantiation)