Craig Interpolants for QFPA

Seminar on Automated Reasoning 2010

Alen Stojanov

École Polytechnique Fédérale de Lausanne
Lausanne, Switzerland

November 19, 2010

Recap

- *Presburger arithmetic* is the first-order theory defined by the structure $\langle \mathbb{Z}, \doteq, \leq, + \rangle$:

$$\phi ::= t \doteq 0 \mid t \leq 0 \mid a|t \mid \phi \wedge \phi \mid \phi \vee \phi \mid \neg\phi \mid \exists x.\phi \mid \forall x.\phi$$

$$t ::= a \mid c \mid x \mid at + \ldots + at$$

- ϕ is a FOL formula over t and $a \in \mathbb{Z}$ is an integer constant.
- t denotes terms of linear arithmetic and for simplicity we represent it as: $t = \sum_{i \in J} a_i x_i + c$

Recap

- *Quantifier Free Presburger Arithmetics* removes the quantifiers such that:

$$\phi ::= t \doteq 0 \mid t \leq 0 \mid a|t \mid \phi \wedge \phi \mid \phi \vee \phi \mid \neg\phi$$

$$t ::= a \mid c \mid x \mid at + \ldots + at$$

- Two *QFP* formulas A and B are *inconsistent* if their conjunction is unsatisfiable

Equisatisfiable Formulas

- Let $\mathcal{V}(\phi)$ to be the set of variables occurring in a formula ϕ and for any two formulas A and B, we denote:
  - $\mathcal{L}_A = \mathcal{V}(A) \backslash \mathcal{V}(B)$ as the set of variables *local* to A
  - $\mathcal{G} = \mathcal{V}(A) \cap \mathcal{V}(B)$ as the set of variables *global* to A and B
- We also denote $A \dot{\equiv} B$ if A and B are *equisatisfiable* i.e. if existentially quantifying their respective local variables produces two logically equivalent formulas:

$$\exists \mathcal{L}_A . A \equiv \exists \mathcal{L}_B . B$$

Equisatisfiable Formulas Example

- Are the following formulas equisatisfiable:

$$A := x + y \doteq 7 \text{ and } B := y + z \doteq 21$$

Equisatisfiable Formulas Example

- Are the following formulas equisatisfiable:

$$A := x + y \doteq 7 \text{ and } B := y + z \doteq 21$$

- A and B are equisatisfiable. Consider:

$$\mathcal{L}_A = \{x\} \text{ and } \mathcal{L}_B = \{z\}$$

$$\text{if } x = 0 \text{ and } z = 14 \Rightarrow \exists \mathcal{L}_A . A \equiv \exists \mathcal{L}_B . B$$

Equisatisfiable Formulas Example

- Are the following formulas equisatisfiable:

$$A := x + y \doteq 7 \text{ and } B := y + z \doteq 21$$

- A and B are equisatisfiable. Consider:

$$\mathcal{L}_A = \{x\} \text{ and } \mathcal{L}_B = \{z\}$$

$$\text{if } x = 0 \text{ and } z = 14 \Rightarrow \exists \mathcal{L}_A.A \equiv \exists \mathcal{L}_B.B$$

- What about:

$$A := x + y \doteq 7 \wedge x \doteq 0 \text{ and } B := y + z \doteq 21 \wedge z \doteq 0$$

Tightening of inequalities

- Let's assume that for inequality $f = t \leq 0$ it is defined $g = gcd(\{|a_i| : i \in J\})$ (the greatest common divisor) of a term such that $t = \sum_{i \in J} a_i x_i + c$.
- An inequality is *tight* if g divides c i.e. $g|c$
- $\mathcal{T}(f)$ represents the *tight form* of the inequalities f.
- Every f can be represented into $\mathcal{T}(f)$ by replacing c with $g\lceil \frac{c}{g} \rceil$

Homogenization

A formula $F(\sigma)$ is called σ-homogenized if all occurrences of σ have unit coefficients. For $Q(x)$ over x, this can be achieved by:

1. Compute least common multiple $l = lcm(\{|a_i| : i \in J\})$
2. Multiply each term of $Q(x)$, having multiple of ax, by $\frac{l}{a}$, such that all coefficients of $Q(x)$ will become either l or $-l$. (for divisibility constraints $d|t$ multiply both d and t by $\frac{l}{a}$).
3. Replace each lx with new variable σ and conjoin the results with new constraint $l|\sigma$.

σ is a fresh variable, and $F(\sigma)$ is equisatisfiable with $Q(x)$.

Exact Projection

Exact projection: $proj(Q(x), x)$ produces equisatisfiable formula, eliminating x from x-homogenized $Q(x)$. We handle two cases:

1. $Q(x)$ contains one equality eq: Because of homogenization $eq := x \doteq t$, we can drop eq and obtain $Q'(x) = [x/t]Q(x)$.
2. $Q(x)$ does not contains any equality: Compute $Q'(x)$ by removing all inequalities over x and compute $l = lcm\{d : d$ is a periodicity of some divisibility constraints containing $x\}$. Eliminate x by replacing $Q'(x)$ with $\exists i \in \{0, \ldots, l\}.Q'(i)$.

Denote $proj(Q, V)$ if $proj(Q(x), x)$ has been applied to all $x \in V$.

Exact Projection Example

Project $Q(x) := 6|3x - 2y - 2$ over x, using exact projection.

Exact Projection Example

Project $Q(x) := 6|3x - 2y - 2$ over x, using exact projection.

1. By x-homogenization, $Q(x) := 6|3x - 2y - 2$ becomes:

$$Q'(\sigma) := 6|\sigma - 2y - 2 \wedge 3|\sigma$$

Exact Projection Example

Project $Q(x) := 6|3x - 2y - 2$ over x, using exact projection.

1. By x-homogenization, $Q(x) := 6|3x - 2y - 2$ becomes:

$$Q'(\sigma) := 6|\sigma - 2y - 2 \wedge 3|\sigma$$

2. By exact projection we have:

$$\exists i \in \{0, \ldots, 6\}.6|i - 2y - 2 \wedge 3|i$$

Definition

- A *(Craig) Interpolant* for two inconsistent quantifier-free formulas (A, B) is a formula I such that:

Definition

- A *(Craig) Interpolant* for two inconsistent quantifier-free formulas (A, B) is a formula I such that:
  1. $A \models I$

Definition

- A *(Craig) Interpolant* for two inconsistent quantifier-free formulas (A, B) is a formula I such that:
  1. $A \models I$
  2. $(B, I) \models \perp$

Definition

- A *(Craig) Interpolant* for two inconsistent quantifier-free formulas (A, B) is a formula I such that:
  1. $A \models I$
  2. $(B, I) \models \perp$
  3. $\mathcal{V}(I) \subseteq \mathcal{G}$

Definition

- A *(Craig) Interpolant* for two inconsistent quantifier-free formulas (A, B) is a formula I such that:
  1. $A \models I$
  2. $(B, I) \models \perp$
  3. $\mathcal{V}(I) \subseteq \mathcal{G}$
- Let A and B be the (inconsistent) formulas $x = y + 1 \wedge z = y$ and $x = y$, respectively. What is the Craig Interpolant of these formulas?

Definition

- A *(Craig) Interpolant* for two inconsistent quantifier-free formulas (A, B) is a formula I such that:
  1. $A \models I$
  2. $(B, I) \models \perp$
  3. $\mathcal{V}(I) \subseteq \mathcal{G}$
- Let A and B be the (inconsistent) formulas $x = y + 1 \wedge z = y$ and $x = y$, respectively. What is the Craig Interpolant of these formulas?
- An example of an interpolant I for A and B is $x = y + 1$.

Use the *Omega Test - W. Pugh algorithm* to eliminate equalities from constraints:

- Each divisibility constraint $d|t$ represent as $d\sigma + t \doteq 0$, such that σ is a fresh variable. We now have system of equalities only.
- Remove equality $ax + t \doteq 0$ immediately if a is an unit coefficient. by replacing $x \doteq -t$.
- Use "symmetric" modulo function $a \widehat{mod} b = a - b\lfloor \frac{a}{b} + \frac{1}{2} \rfloor$ and replace every equality $ax + t \doteq 0$ by:

$$(a \widehat{mod} m)x + (t \widehat{mod} m) \doteq m\sigma$$

where $m = |a| + 1$ and σ is a fresh variable.

- Since $a \widehat{\bmod} m = -sign(a)$, x can be eliminated since it already has unit coefficient.
- We denote the elimination of all equalities in ϕ as $elim(\phi)$.
- Note: Omega Test algorithm will immediately return $\perp$ if it encounters unsatisfiable equality.

Partial Equality Interpolant

A *partial equality interpolant* for (A, B) is a conjunction of linear equalities ϕ^A such that:

1. $A \models \phi^A$
2. $(B, \phi^A) \models \phi$
3. if ϕ contains an unsatisfiable equality, then $\mathcal{V}(\phi^A) \subseteq \mathcal{G}$.

Denote $(A, B) \vdash \phi[\phi^A]$, if we can derive interpolant ϕ^A from (A, B)

Elimination Rules

Derive an interpolant from a proof of inconsistency of the linear equality formulas. Hypothesis rule:

$$\textsc{HypEq}\ \frac{}{(A, B) \vdash (A \wedge B)[A]}$$

Eliminate constraints and finally calculate the interpolant:

$$\textsc{ElimEq}\ \frac{(A, B) \vdash \quad A \wedge B\ \ [A]}{(A, B) \vdash \mathit{elim}(A \wedge B)[\mathit{proj}(A, \mathcal{L}_A)]}$$

Equality and Divisibility Constraints Interpolation Example

- Find interpolant for $A := (6|3z - 2y - 2)$ and $B := (6x - y \doteq 0)$

Equality and Divisibility Constraints Interpolation Example

- Find interpolant for $A := (6|3z - 2y - 2)$ and $B := (6x - y \doteq 0)$
- By *elim*$(A \wedge B)$, the conjunction $6|x + 3z - 2y - 2 = 0 \wedge 6x - y = 0$ becomes:

$$6\sigma - 12x - 3 = 0$$

Equality and Divisibility Constraints Interpolation Example

- Find interpolant for $A := (6|3z - 2y - 2)$ and $B := (6x - y \doteq 0)$
- By $elim(A \wedge B)$, the conjunction $6|x + 3z - 2y - 2 = 0 \wedge 6x - y = 0$ becomes:

$$6\sigma - 12x - 3 = 0$$

- Putting it all together:

$$\textsc{ElimEq}\ \frac{(A, B) \vdash 6\sigma + 3z - 2y - 2 = 0 \wedge 6x - y = 0[6|3z - 2y - 2]}{(A, B) \vdash 6\sigma - 12x - 3 = 0[\exists i \in \{0, \ldots, 6\}.(6|i - 2y - 2) \wedge (3|i)]}$$

Elimination by Tightening

- Adopt Fourier-Motzkin Elimination (FME) into *Omega Test*.Consider the following inequalities:

$$ax + t_1 \leq 0 \text{ and } -bx + t_2 \leq 0$$

- Equivalently we can define upper and lower bounds of x:

$$at_2 \leq abx \leq -bt_1$$

- FME removes variable x by tightening:

$$\mathcal{T}(at_2 + bt_1 \leq 0)$$

Elimination by Tightening cont.

- Although $\mathcal{T}(at_2 + bt_1 \leq 0)$ is implied by $at_2 \leq abx \leq -bt_1$, it is not generally vise versa, thus the two inequalities are **not equisatisfiable** and the projection is *inexact projection*.
- If $-bt_1 - at_2 < ab$ (the bounds distance is smaller than ab), solution to the following inequality is not guaranteed:

$$\mathcal{T}(-ab + 1 \leq at_2 + bt_1 \leq 0)$$

- Solution is only a "thin" part of polyhedron, and it has to be checked.

Strongest Convex Projection

- **Definition**. For lower and upper bounds $ax + t_1 \leq 0$ and $-bx + t_2 \leq 0$, let $t' \leq 0$ be the tight form of $at_2 + bt_1 \leq 0$, and let $m \geq 0$. Inequality $t' + m \leq 0$ is the strongest convex projection of these bounds if there is no integer i such that:

$$(at_2 \leq abx \leq -bt_1) \models (t' + i \leq 0) \models (t' + m \leq 0)$$

Strongest Convex Projection Cont.

The inequality $\mathcal{T}(-ab + 1 \leq at_2 + bt_1 \leq 0)$ represents a constraint which can be written in the form: $-c' \leq t' \leq 0$, and can be represented as the quantifier-free formula:

$$\exists i \in \{-c', \ldots, 0\}.t' \doteq 0$$

This equality conjoined with the upper and lower bounds can be checked for feasible solution in the thin polyhedron.

Strongest Convex Projection Example

Calculate the Strongest Convex Projection of the following inequalities: $x + 3y - 2 \leq 0$ and $-3y + 1 \leq 0$

Strongest Convex Projection Example

Calculate the Strongest Convex Projection of the following inequalities: $x + 3y - 2 \leq 0$ and $-3y + 1 \leq 0$

- The "thin" part is represented by $-8 \leq 6x - 3 \leq 0$

Strongest Convex Projection Example

Calculate the Strongest Convex Projection of the following inequalities: $x + 3y - 2 \leq 0$ and $-3y + 1 \leq 0$

- The "thin" part is represented by $-8 \leq 6x - 3 \leq 0$
- $\mathcal{T}(-8 \leq 6x - 3 \leq 0)$ results in $6x = 0$.

Strongest Convex Projection Example

Calculate the Strongest Convex Projection of the following inequalities: $x + 3y - 2 \leq 0$ and $-3y + 1 \leq 0$

- The "thin" part is represented by $-8 \leq 6x - 3 \leq 0$
- $\mathcal{T}(-8 \leq 6x - 3 \leq 0)$ results in $6x = 0$.
- Replacing x in the upper and lower bounds leads to: $3y \leq 0$ and $-3y + 3 \leq 0$

Strongest Convex Projection Example

Calculate the Strongest Convex Projection of the following inequalities: $x + 3y - 2 \leq 0$ and $-3y + 1 \leq 0$

- The "thin" part is represented by $-8 \leq 6x - 3 \leq 0$
- $\mathcal{T}(-8 \leq 6x - 3 \leq 0)$ results in $6x = 0$.
- Replacing x in the upper and lower bounds leads to: $3y \leq 0$ and $-3y + 3 \leq 0$
- Finally since $3y \leq 0$ and $-3y + 3 \leq 0$ are parallel, the strongest convex projection is $6x + 1 \leq 0$

Partial Inequality Interpolant

A *partial inequality interpolant* for (A, B) is an inequality $t^A \leq 0$ such that:

1. $A \models t^A \leq 0$
2. $B \models t - t^A \leq 0$
3. $\mathcal{V}(t^A \leq 0) \subseteq \mathcal{V}(A)$ and $\mathcal{V}(t - t^A) \subseteq \mathcal{V}(B)$

Denote $(A, B) \vdash t \leq 0[I \leq 0]$, if we can derive interpolant $I \leq 0$ from (A, B)

Inequality Constraints Interpolation

Hypothesis rule:

$$\textsc{HypIn}\ \frac{}{(A,B) \vdash t \leq 0[\mathcal{X}(t \leq 0)]}\ (t \leq 0) \in (A,B)$$

where $\mathcal{X}(t \leq 0)$ is $t \leq 0$, if $t \leq 0 \in A$, and $0 \leq 0$ otherwise.

$$\textsc{Proj}\ \frac{\begin{array}{ll}(A,B) \vdash & ax + t_1 \leq 0[t_1' \leq 0] \\ (A,B) \vdash & -bx + t_2 \leq 0[t_2' \leq 0]\end{array}}{(A,B) \vdash \mathcal{T}(at_2 + bt_1 \leq 0)[\mathcal{T}(at_2' + bt_1' + m \leq 0)]}\ a,b \in \mathbb{N}_{\geq 1}$$

m is either $m = 0$ or the strongest convex projection.

Combining the Two Methods

Let's assume that we have two inconsistent formulas A and B such that E_A and E_B are conjunctions of equalities of A and B respectively. In order to calculate the interpolant of (A, B) we distinguish two cases:

1. If there is one unsatisfiable equality in E_A or E_B, then the interpolant is calculated by $proj(E_A, \mathcal{L}(E_A))$, disregarding the inequalities.
2. Otherwise, all the equalities and divisibility constraints are removed by the previously defined rules, and new pair (A', B') is computed containing only inequalities, and an interpolant of only inequalities can be calculated.

Combining the Two Methods

$A' \wedge B'$ is equisatisfiable to $A \wedge B$, but not equivalent, thus the interpolant of (A', B') can contain variables which are not contained into (A, B). If we denote $\phi\{x \leftarrow t_u\}$ the result of substituting x with every term t_u. we can formalize the rule:

$$\textsc{Comb}\ \frac{(A', B') \vdash \bot\ [t'' \leq 0]}{(A, B) \vdash \bot\ [proj(t' \leq 0 \wedge E_A, \mathcal{L}_A)]} \qquad \begin{array}{l} t'' \doteq t'\{x \leftarrow t_u\} \\ (A, B) \vdash t \leq 0[t' \leq 0] \end{array}$$

- The method first eliminates equalities and divisibility constraints from the system and then projects inequalities using an extension of the Fourier-Motzkin variable elimination.
- It permits combination of equalities, inequalities and divisibility properties.
- As such, it is able to improve the automatic model checking based on counterexample-guided abstraction refinement.