Complete Instantiation for Quantified Formulas in SMT
CAV 2009

Yeting Ge
New York University

Leonardo de Moura
Microsoft Research
a > 3, (a = b ∨ a = b + 1), f(a) = 0, f(b) = 1
Many Applications

- Dynamic symbolic execution (DART)
- Extended static checking
- Test-case generation
- Bounded model checking (BMC)
- Equivalence checking
- ...

Complete Instantiation – CAV 2009
A theory $T$ is a set of sentences.

$F$ is satisfiable modulo $T$ iff $T \cup F$ is satisfiable.
Array Theory:
\[ \forall a, i, v: \text{read(write}(a, i, v), i) = v \]
\[ \forall a, i, v: i = j \lor \text{read(write}(a, i, v), j) = \text{read}(a, j) \]

- Linear Arithmetic
- Bit-vectors
- Inductive datatypes
- ...

Complete Instantiation – CAV 2009
\( a > 3, (a = b \lor a = b + 1), f(a) = 0, f(b) = 1 \)

<table>
<thead>
<tr>
<th>Symbols</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>f, g, h</td>
<td>Uninterpreted functions</td>
</tr>
<tr>
<td>a, b, c</td>
<td>Uninterpreted constants</td>
</tr>
<tr>
<td>+, -, &lt;, ≤, 0, 1, ...</td>
<td>Interpreted symbols</td>
</tr>
</tbody>
</table>
a > 3, (a = b ∨ a = b + 1), f(a) = 0, f(b) = 1

Model/Structure:

a → 4
b → 3
f → { 4 → 0, 3 → 1, ... }
$$a > 3, (a = b \lor a = b + 1), f(a) = 0, f(b) = 1$$

Model $M$:
- $M(a) = 4$
- $M(b) = 3$
- $M(f) = \{ 4 \rightarrow 0, 3 \rightarrow 1, \ldots \}$
Many SMT Solvers:
- Barcelogic, Beaver, Boolector,
- CVC3, MathSAT, OpenSMT,
- Sateen, Yices, Z3, ...

They are very efficient for quantifier-free formulas.
Many applications need quantifiers

Modeling the runtime

\( \forall h, o, f: \)
\[
\text{IsHeap}(h) \land o \neq \text{null} \land \text{read}(h, o, \text{alloc}) = t
\]
\[\Rightarrow\]
\[
\text{read}(h, o, f) = \text{null} \lor \text{read}(h, \text{read}(h, o, f), \text{alloc}) = t
\]
Many applications need quantifiers

- Modeling the runtime
- User provided assertions

\forall \ i, j: i \leq j \Rightarrow \text{read}(a, i) \leq \text{read}(b, j)
Many applications need **quantifiers**

- Modeling the runtime
- User provided assertions
- Unsupported theories

\[ \forall x: p(x,x) \]
\[ \forall x,y,z: p(x,y), p(y,z) \implies p(x,z) \]
\[ \forall x,y: p(x,y), p(y,x) \implies x = y \]
Many applications need **quantifiers**

- Modeling the runtime
- User provided assertions
- Unsupported theories
- Solver must be fast in satisfiable instances.

**We want to find bugs!**
Many Approaches

- Superposition Calculus + SMT.
- Instantiation Based Methods
  - Implemented on top of “regular” SMT solvers.
  - Heuristic quantifier instantiation (E-Matching).
  - Complete quantifier instantiation.

*Complete Instantiation – CAV 2009*
Instantiation Based Methods: Related work

- Bernays-Schönfinkel class.
- Stratified Many-Sorted Logic.
- **Array Property Fragment**.
- Local theory extensions.
∀x₁, x₂: ¬p(x₁, x₂) ∨ f(x₁) = f(x₂) + 1,
p(a,b), a < b + 1
Simplifying Assumption: CNF

\[ \neg p(x_1, x_2) \lor f(x_1) = f(x_2) + 1, \]
\[ p(a,b), a < b + 1 \]
Variables appear only as arguments of uninterpreted symbols.

\[
f(g(x_1) + a) < g(x_1) \lor h(f(x_1), x_2) = 0
\]

\[
f(x_1 + x_2) \leq f(x_1) + f(x_2)
\]
Given a set of formulas $F$, build an equisatisfiable set of quantifier-free formulas $F^*$

“Domain” of $f$ is the set of ground terms $A_f$

$t \in A_f$ if there is a ground term $f(t)$

Suppose
1. We have a clause $C[f(x)]$ containing $f(x)$.
2. We have $f(t)$.

$\rightarrow$

Instantiate $x$ with $t$: $C[f(t)]$. 
Example

\begin{align*}
F & \quad F^* \\
g(x_1, x_2) &= 0 \lor h(x_2) = 0, \\
g(f(x_1), b) + 1 &\leq f(x_1), \\
h(c) &= 1, \\
f(a) &= 0
\end{align*}
$g(x_1, x_2) = 0 \lor h(x_2) = 0,$
$g(f(x_1), b) + 1 \leq f(x_1),$
$h(c) = 1,$
$f(a) = 0$

Copy quantifier-free formulas

“Domains”:

$A_f: \{ a \}$
$A_g: \{ \}$
$A_h: \{ c \}$

Complete Instantiation – CAV 2009
Example

\[ g(x_1, x_2) = 0 \lor h(x_2) = 0, \]
\[ g(f(x_1), b) + 1 \leq f(x_1), \]
\[ h(c) = 1, \]
\[ f(a) = 0 \]

<table>
<thead>
<tr>
<th><strong>F</strong></th>
<th><strong>F</strong>*</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ g(x_1, x_2) = 0 \lor h(x_2) = 0, ]</td>
<td>[ h(c) = 1, ]</td>
</tr>
<tr>
<td>[ g(f(x_1), b) + 1 \leq f(x_1), ]</td>
<td>[ f(a) = 0, ]</td>
</tr>
<tr>
<td>[ h(c) = 1, ]</td>
<td>[ ]</td>
</tr>
<tr>
<td>[ f(a) = 0 ]</td>
<td>[ ]</td>
</tr>
</tbody>
</table>

“Domains”:

| \(A_f\) | \{a\} |
| \(A_g\) | \{\} |
| \(A_h\) | \{c\} |
Example

\[ g(x_1, x_2) = 0 \lor h(x_2) = 0, \]
\[ g(f(x_1), b) + 1 \leq f(x_1), \]
\[ h(c) = 1, \]
\[ f(a) = 0 \]

\[ F^* \]
\[ h(c) = 1, \]
\[ f(a) = 0, \]
\[ g(f(a), b) + 1 \leq f(a) \]

“Domains”:
\[ A_f : \{ a \} \]
\[ A_g : \{ [f(a), b] \} \]
\[ A_h : \{ c \} \]
Example

\[
g(x_1, x_2) = 0 \lor h(x_2) = 0, \quad g(f(x_1), b) + 1 \leq f(x_1),
\]
\[
h(c) = 1, \quad f(a) = 0
\]

“Domains”:
\[
A_f : \{ a \}
\]
\[
A_g : \{ [f(a), b] \}
\]
\[
A_h : \{ c \}
\]
Example

F
\[ g(x_1, x_2) = 0 \lor h(x_2) = 0, \]
\[ g(f(x_1), b) + 1 \leq f(x_1), \]
\[ h(c) = 1, \]
\[ f(a) = 0 \]

F*
\[ h(c) = 1, \]
\[ f(a) = 0, \]
\[ g(f(a), b) + 1 \leq f(a), \]
\[ g(f(a), b) = 0 \lor h(b) = 0 \]

“Domains”:
\[ A_f : \{ a \} \]
\[ A_g : \{ [f(a), b] \} \]
\[ A_h : \{ c, b \} \]
Example

\[ g(x_1, x_2) = 0 \lor h(x_2) = 0, \]
\[ g(f(x_1), b) + 1 \leq f(x_1), \]
\[ h(c) = 1, \]
\[ f(a) = 0 \]

\[ F^* \]
\[ h(c) = 1, \]
\[ f(a) = 0, \]
\[ g(f(a), b) + 1 \leq f(a), \]
\[ g(f(a), b) = 0 \lor h(b) = 0 \]

“Domains”:
\[ A_f : \{ a \} \]
\[ A_g : \{ [f(a), b] \} \]
\[ A_h : \{ c, b \} \]
Example

**F**

\[ g(x_1, x_2) = 0 \lor h(x_2) = 0, \]
\[ g(f(x_1), b) + 1 \leq f(x_1), \]
\[ h(c) = 1, \]
\[ f(a) = 0 \]

**F**

\[ h(c) = 1, \]
\[ f(a) = 0, \]
\[ g(f(a), b) + 1 \leq f(a), \]
\[ g(f(a), b) = 0 \lor h(b) = 0, \]
\[ g(f(a), c) = 0 \lor h(c) = 0 \]

“Domains”:

- \( A_f : \{ a \} \)
- \( A_g : \{ [f(a), b], [f(a), c] \} \)
- \( A_h : \{ c, b \} \)
Example

\[ g(x_1, x_2) = 0 \lor h(x_2) = 0, \]
\[ g(f(x_1), b) + 1 \leq f(x_1), \]
\[ h(c) = 1, \]
\[ f(a) = 0 \]

\[ F \]

\[ F^* \]
\[ h(c) = 1, \]
\[ f(a) = 0, \]
\[ g(f(a), b) + 1 \leq f(a), \]
\[ g(f(a), b) = 0 \lor h(b) = 0, \]
\[ g(f(a), c) = 0 \lor h(c) = 0 \]

\[ M \]
\[ a \rightarrow 2, b \rightarrow 2, c \rightarrow 3 \]
\[ f \rightarrow \{ 2 \rightarrow 0, \ldots \} \]
\[ h \rightarrow \{ 2 \rightarrow 0, 3 \rightarrow 1, \ldots \} \]
\[ g \rightarrow \{ [0,2] \rightarrow -1, [0,3] \rightarrow 0, \ldots \} \]
Given a model $M$ for $F^*$, 
Build a model $M^\pi$ for $F$

Define a projection function $\pi_f$ s.t. 
range of $\pi_f$ is $M(A_f)$, and 
$\pi_f(v) = v$ if $v \in M(A_f)$

Then, 
$M^\pi(f)(v) = M(f)(\pi_f(v))$
Basic Idea (cont.)

\[ M(A_f) \xrightarrow{\pi_f} M(f) \]

\[ M(f) \]

\[ M(f(A_f)) \]

\[ M(\pi(f)) \]

\[ M(A_f) \xrightarrow{\pi_f} M(A_f) \xrightarrow{M(f)} M(f(A_f)) \]

Complete Instantiation – CAV 2009
Given a model $M$ for $F^*$, build a model $M^\pi$ for $F$

In our example, we have: $h(b)$ and $h(c)$

$\rightarrow A_h = \{ b, c \}$, and $M(A_h) = \{ 2, 3 \}$

$\pi_h = \{ 2 \rightarrow 2, 3 \rightarrow 3, \text{else} \rightarrow 3 \}$

$M(h)$

$\{ 2 \rightarrow 0, 3 \rightarrow 1, \ldots \}$

$M^\pi(h)$

$\{ 2 \rightarrow 0, 3 \rightarrow 1, \text{else} \rightarrow 1 \}$

$M^\pi(h) = \lambda x. \text{if}(x=2, 0, 1)$
Example

**F**
- $g(x_1, x_2) = 0 \lor h(x_2) = 0$
- $g(f(x_1), b) + 1 \leq f(x_1)$
- $h(c) = 1$
- $f(a) = 0$

**F*\**
- $h(c) = 1$
- $f(a) = 0$
- $g(f(a), b) + 1 \leq f(a)$
- $g(f(a), b) = 0 \lor h(b) = 0$
- $g(f(a), c) = 0 \lor h(c) = 0$

**M**
- $a \rightarrow 2$, $b \rightarrow 2$, $c \rightarrow 3$
- $f \rightarrow \lambda x. 2$
- $h \rightarrow \lambda x. \text{if}(x=2, 0, 1)$
- $g \rightarrow \lambda x,y. \text{if}(x=0 \land y=2, -1, 0)$

**M**\(\pi\)
- $a \rightarrow 2$, $b \rightarrow 2$, $c \rightarrow 3$
- $f \rightarrow \{ 2 \rightarrow 0, \ldots \}$
- $h \rightarrow \{ 2 \rightarrow 0, 3 \rightarrow 1, \ldots \}$
- $g \rightarrow \{ [0,2] \rightarrow -1, [0,3] \rightarrow 0, \ldots \}$
Example: Model Checking

\( M^\pi \)

\( a \rightarrow 2, b \rightarrow 2, c \rightarrow 3 \)
\( f \rightarrow \lambda x. \ 2 \)
\( h \rightarrow \lambda x. \ \text{if}(x=2, \ 0, \ 1) \)
\( g \rightarrow \lambda x,y \. \ \text{if}(x=0 \land y=2, -1, 0) \)

Does \( M^\pi \) satisfies?

\( \forall x_1, x_2 : g(x_1, x_2) = 0 \lor h(x_2) = 0 \)

\( \forall x_1, x_2 : \text{if}(x_1=0 \land x_2=2, -1, 0) = 0 \lor \text{if}(x_2=2, 0, 1) = 0 \) is valid

\( \exists x_1, x_2 : \text{if}(x_1=0 \land x_2=2, -1, 0) \neq 0 \land \text{if}(x_2=2, 0, 1) \neq 0 \) is unsat

\( \text{if}(s_1=0 \land s_2=2, -1, 0) \neq 0 \land \text{if}(s_2=2, 0, 1) \neq 0 \) is unsat
Suppose $M^\pi$ does not satisfy $C[f(x)]$.

Then for some value $v$, $M^\pi\{x \rightarrow v\}$ falsifies $C[f(x)]$.

$M^\pi\{x \rightarrow \pi_f(v)\}$ also falsifies $C[f(x)]$.

But, there is a term $t \in A_f$ s.t. $M(t) = \pi_f(v)$
Moreover, we instantiated $C[f(x)]$ with $t$.

So, $M$ must not satisfy $C[f(t)]$.
Contradiction: $M$ is a model for $F^*$. 

*Complete Instantiation – CAV 2009*
Refinement 1: Lazy construction

- $F^*$ may be very big (or infinite).
- Lazy-construction
  - Build $F^*$ incrementally, $F^*$ is the limit of the sequence $F^0 \subseteq F^1 \subseteq \ldots \subseteq F^k \subseteq \ldots$
  - If $F^k$ is unsat then $F$ is unsat.
  - If $F^k$ is sat, then build (candidate) $M^\pi$
  - If $M^\pi$ satisfies all quantifiers in $F$ then return sat.
Refinement 2: Model-based instantiation

Suppose $M^\pi$ does not satisfy a clause $C[f(x)]$ in $F$.

Add an instance $C[f(t)]$ which “blocks” this spurious model. Issue: how to find $t$?

Use model checking, and the “inverse” mapping $\pi_f^{-1}$ from values to terms (in $A_f$).

$$\pi_f^{-1}(v) = t \quad \text{if} \quad M^\pi(t) = \pi_f(v)$$
Model-based instantiation: Example

\[ \forall x_1: f(x_1) < 0, \]
\[ f(a) = 1, \quad f(b) = -1 \]
\[ f(a) < 0 \]

unsat

Model Checking \[ \forall x_1: f(x_1) < 0 \]
not \[ f(s_1 = 2, 1, -1) < 0 \]

\[ s_1 \rightarrow 2 \]
\[ \pi_f^{-1}(2) = a \]
Is our procedure refutationally complete?

FOL Compactness

A set of sentences is unsatisfiable iff it contains an unsatisfiable finite subset.

A theory $T$ is a set of sentences, then apply compactness to $F^* \cup T$
Infinite $F^*$: Example

$F$

$\forall x_1: f(x_1) < f(f(x_1)),$
$\forall x_1: f(x_1) < a,$
$1 < f(0).$

$F^*$

$f(0) < f(f(0)),$  $f(f(0)) < f(f(f(0))),$  ...
$f(0) < a,$  $f(f(0)) < a,$  ...
$1 < f(0)$

Unsatisfiable

Every finite subset of $F^*$ is satisfiable.
Infinite $F^*$: What is wrong?

- Theory of linear arithmetic $T_Z$ is the set of all first-order sentences that are true in the standard structure $Z$.
- $T_Z$ has non-standard models.
- $F$ and $F^*$ are satisfiable in a non-standard model.

Alternative: a theory is a class of structures.
- Compactness does not hold.
- $F$ and $F^*$ are still equisatisfiable.
Given a clause $C_k[x_1, \ldots, x_n]$

Let

$S_{k,i}$ be the set of ground terms used to instantiate $x_i$ in clause $C_k[x_1, \ldots, x_n]$

How to characterize $S_{k,i}$?

<table>
<thead>
<tr>
<th>$F$</th>
<th>(\Delta_F)</th>
</tr>
</thead>
<tbody>
<tr>
<td>j-th argument of $f$ in $C_k$</td>
<td>system of set constraints</td>
</tr>
<tr>
<td>a ground term $t$</td>
<td>$t \in A_{f,j}$</td>
</tr>
<tr>
<td>$t[x_1, \ldots, x_n]$</td>
<td>$t[S_{k,1}, \ldots, S_{k,n}] \subseteq A_{f,j}$</td>
</tr>
<tr>
<td>$x_i$</td>
<td>$S_{k,i} = A_{f,j}$</td>
</tr>
</tbody>
</table>
\[ \Delta_F: \text{Example} \]

**F**

- \( g(x_1, x_2) = 0 \lor h(x_2) = 0 \),
- \( g(f(x_1), b) + 1 \leq f(x_1) \),
- \( h(c) = 1 \),
- \( f(a) = 0 \)

**\( \Delta_F \)**

- \( S_{1,1} = A_{g,1} \), \( S_{1,2} = A_{g,2} \), \( S_{1,2} = A_{h,1} \)
- \( S_{2,1} = A_{f,1} \), \( f(S_{2,1}) \subseteq A_{g,1} \), \( b \in A_{g,2} \)
- \( c \in A_{h,1} \)
- \( a \in A_{f,1} \)

**\( \Delta_F \): least solution**

- \( S_{1,1} = \{ f(a) \} \), \( S_{1,2} = \{ b, c \} \)
- \( S_{2,1} = \{ a \} \)

Use \( \Delta_F \) to generate \( F^* \)
$\Delta_F$ is **stratified** then the least solution (and F*) is finite.

<table>
<thead>
<tr>
<th>t[S_{k,1}, ..., S_{k,n}] \subseteq A_{f,j}</th>
<th>level(S_{k,i}) &lt; level(A_{f,j})</th>
</tr>
</thead>
<tbody>
<tr>
<td>$S_{k,i} = A_{f,j}$</td>
<td>level(S_{k,i}) = level(A_{f,j})</td>
</tr>
</tbody>
</table>

New decidable fragment: NEXPTIME-Hard.

The least solution of $\Delta_F$ is exponential in the worst case.

$a \in S_1$, $b \in S_1$, $f_1(S_1, S_1) \subseteq S_2$, ..., $f_n(S_n, S_n) \subseteq S_{n+1}$

F* can be doubly exponential in the size of F.
### Arithmetical literals: $\pi_f$ must be monotonic.

<table>
<thead>
<tr>
<th>Literal of $C_k$</th>
<th>$\Delta_F$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\neg(x_i \leq x_j)$</td>
<td>$S_{k,i} = S_{k,j}$</td>
</tr>
<tr>
<td>$\neg(x_i \leq t), \neg(t \leq x_i)$</td>
<td>$t \in S_{k,i}$</td>
</tr>
<tr>
<td>$x_i = t$</td>
<td>${t+1, t-1} \subseteq S_{k,i}$</td>
</tr>
</tbody>
</table>

### Offsets:

<table>
<thead>
<tr>
<th>$j$-th argument of $f$ in $C_k$</th>
<th>$\Delta_F$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_i + r$</td>
<td>$S_{k,i}+r \subseteq A_{f,j}$</td>
</tr>
<tr>
<td></td>
<td>$A_{f,j}+(-r) \subseteq S_{k,i}$</td>
</tr>
</tbody>
</table>
Extensions: Example

Shifting

\neg (0 \leq x_1) \lor \neg (x_1 \leq n) \lor f(x_1) = g(x_1 + 2)
More Extensions

- Many-sorted logic
- Pseudo-Macros

\[ 0 \leq g(x_1) \lor f(g(x_1)) = x_1, \]
\[ 0 \leq g(x_1) \lor h(g(x_1)) = 2x_1, \]
\[ g(a) < 0 \]
SMT solvers usually return *unsat* or *unknown* for quantified SMT formulas.

Z3 was the only SMT-solver in SMT-COMP’08 to correctly answer satisfiable quantified formulas.

New decidable fragments.

Model-based instantiation and Model checking.

Conditions for refutationally complete procedures.

Future work: more efficient model checking techniques.

Thank you!