On interpolation in decision procedures

Maria Paola Bonacina

(Joint work with Moa Johansson)

Dipartimento di Informatica
Università degli Studi di Verona
Verona, Italy

July 5, 2011
Motivation

Interpolation for propositional resolution

Interpolation and equality

Interpolation in decision procedures

Current work: beyond ground problems
What is interpolation?

- Formulae $A$ and $B$ such that $A \vdash B$: interpolant $I$ lies *between* $A$ and $B$
- Derivability: $A \vdash I$ and $I \vdash B$
- Signature: $I$ made of symbols *common* to $A$ and $B$

- *Craig’s Interpolation Lemma*: interpolants exist for closed formulæ
- Clausal theorem proving: *sets of clauses*
Refutational theorem proving: reverse interpolant

- Formulae $A$ and $B$ inconsistent: $A, B \vdash \bot$
- Then $A \vdash I$ and $B, I \vdash \bot$
- $I$ made of symbols common to $A$ and $B$

Reverse interpolant of $(A, B)$: interpolant of $(A, \neg B)$

Reasoning modulo theories: $\vdash_T$

$T$-symbols regarded as *common*
Example in propositional logic

\[ A = \{ a \lor e, \neg a \lor b, \neg a \lor c \} \quad B = \{ \neg b \lor \neg c \lor d, \neg d, \neg e \} \]

* a \lor e resolves with \neg e to yield a
Example in propositional logic

\[ A = \{a \lor e, \neg a \lor b, \neg a \lor c\} \quad B = \{\neg b \lor \neg c \lor d, \neg d, \neg e\} \]

- \(a \lor e\) resolves with \(\neg e\) to yield \(a\)
- \(a\) resolves with \(\neg a \lor c\) to yield \(c\)
Example in propositional logic

\[ A = \{ a \lor e, \neg a \lor b, \neg a \lor c \} \quad B = \{ \neg b \lor \neg c \lor d, \neg d, \neg e \} \]

- $a \lor e$ resolves with $\neg e$ to yield $a$
- $a$ resolves with $\neg a \lor c$ to yield $c$
- $a$ resolves with $\neg a \lor b$ to yield $b$
Example in propositional logic

\[ A = \{ a \lor e, \neg a \lor b, \neg a \lor c \} \quad B = \{ \neg b \lor \neg c \lor d, \neg d, \neg e \} \]

- \( a \lor e \) resolves with \( \neg e \) to yield \( a \)
- \( a \) resolves with \( \neg a \lor c \) to yield \( c \)
- \( a \) resolves with \( \neg a \lor b \) to yield \( b \)
- \( b \) resolves with \( \neg b \lor \neg c \lor d \) to yield \( \neg c \lor d \)
- \( c \) resolves with \( \neg c \lor d \) to yield \( d \)
Example in propositional logic

\[ A = \{ a \lor e, \neg a \lor b, \neg a \lor c \} \quad B = \{ \neg b \lor \neg c \lor d, \neg d, \neg e \} \]

- \( a \lor e \) resolves with \( \neg e \) to yield \( a \)
- \( a \) resolves with \( \neg a \lor c \) to yield \( c \)
- \( a \) resolves with \( \neg a \lor b \) to yield \( b \)
- \( b \) resolves with \( \neg b \lor \neg c \lor d \) to yield \( \neg c \lor d \)
- \( c \) resolves with \( \neg c \lor d \) to yield \( d \)
- \( d \) resolves with \( \neg d \) to yield \( \Box \)
Example in propositional logic

\[ A = \{a \lor e, \neg a \lor b, \neg a \lor c\} \quad B = \{\neg b \lor \neg c \lor d, \neg d, \neg e\} \]

- \( a \lor e \) resolves with \( \neg e \) to yield \( a \)
- \( a \) resolves with \( \neg a \lor c \) to yield \( c \)
- \( a \) resolves with \( \neg a \lor b \) to yield \( b \)
- \( b \) resolves with \( \neg b \lor \neg c \lor d \) to yield \( \neg c \lor d \)
- \( c \) resolves with \( \neg c \lor d \) to yield \( d \)
- \( d \) resolves with \( \neg d \) to yield \( \Box \)
- Interpolant \( I: e \lor (c \land b) \)
Example in combination of theories I

\[ A = \{ f(x_1) + x_2 \simeq x_3, \ f(y_1) + y_2 \simeq y_3, \ y_1 \leq x_1 \} \]
\[ B = \{ x_2 \simeq g(b), \ y_2 \simeq g(b), \ x_1 \leq y_1, \ x_3 < y_3 \} \]

After separation:

\[ A_{EUF} = \{ a_1 \simeq f(x_1), \ a_2 \simeq f(y_1) \} \]
\[ A_{LI} = \{ a_1 + x_2 \simeq x_3, \ a_2 + y_2 \simeq y_3, \ y_1 \leq x_1 \} \]
\[ B_{EUF} = \{ x_2 \simeq g(b), \ y_2 \simeq g(b) \} \]
\[ B_{LI} = \{ x_1 \leq y_1, \ x_3 < y_3 \} \]
Example in combination of theories II

- $y_1 \leq x_1$ with $x_1 \leq y_1$ yield $x_1 \simeq y_1$
Example in combination of theories II

- $y_1 \leq x_1$ with $x_1 \leq y_1$ yield $x_1 \simeq y_1$
- $x_1 \simeq y_1$ with $a_1 \simeq f(x_1)$ and $a_2 \simeq f(y_1)$ yield $a_1 \simeq a_2$
Example in combination of theories II

- $y_1 \leq x_1$ with $x_1 \leq y_1$ yield $x_1 \simeq y_1$
- $x_1 \simeq y_1$ with $a_1 \simeq f(x_1)$ and $a_2 \simeq f(y_1)$ yield $a_1 \simeq a_2$
- $x_2 \simeq g(b)$ with $y_2 \simeq g(b)$ yield $x_2 \simeq y_2$
Example in combination of theories II

- $y_1 \leq x_1$ with $x_1 \leq y_1$ yield $x_1 \simeq y_1$
- $x_1 \simeq y_1$ with $a_1 \simeq f(x_1)$ and $a_2 \simeq f(y_1)$ yield $a_1 \simeq a_2$
- $x_2 \simeq g(b)$ with $y_2 \simeq g(b)$ yield $x_2 \simeq y_2$
- $a_1 \simeq a_2$, $x_2 \simeq y_2$ with $a_1 + x_2 \simeq x_3$, $a_2 + y_2 \simeq y_3$ yield $x_3 \simeq y_3$
Example in combination of theories II

- \( y_1 \leq x_1 \) with \( x_1 \leq y_1 \) yield \( x_1 \simeq y_1 \)
- \( x_1 \simeq y_1 \) with \( a_1 \simeq f(x_1) \) and \( a_2 \simeq f(y_1) \) yield \( a_1 \simeq a_2 \)
- \( x_2 \simeq g(b) \) with \( y_2 \simeq g(b) \) yield \( x_2 \simeq y_2 \)
- \( a_1 \simeq a_2, \ x_2 \simeq y_2 \) with \( a_1 + x_2 \simeq x_3, \ a_2 + y_2 \simeq y_3 \) yield \( x_3 \simeq y_3 \)
- \( x_3 \simeq y_3 \) and \( x_3 < y_3 \) yields \( \square \)
Example in combination of theories II

- $y_1 \leq x_1$ with $x_1 \leq y_1$ yield $x_1 \simeq y_1$
- $x_1 \simeq y_1$ with $a_1 \simeq f(x_1)$ and $a_2 \simeq f(y_1)$ yield $a_1 \simeq a_2$
- $x_2 \simeq g(b)$ with $y_2 \simeq g(b)$ yield $x_2 \simeq y_2$
- $a_1 \simeq a_2$, $x_2 \simeq y_2$ with $a_1 + x_2 \simeq x_3$, $a_2 + y_2 \simeq y_3$ yield $x_3 \simeq y_3$
- $x_3 \simeq y_3$ and $x_3 < y_3$ yields $\Box$
- Interpolant $I$: $y_1 < x_1 \lor x_2 - y_2 \simeq x_3 - y_3$
Why interpolation?

- Interpolant is a formula \textit{in between} formulæ.
- Formulæ represent program states that satisfy them.
- Interpolant gives information on \textit{intermediate} states.
Image computation in model checking

- Program as *transition system*
- Forward reachability: computing *images*
- Backward reachability: computing *pre-images*
- Interpolant: *over-approximation* of an image/pre-image
Abstraction refinement in software model checking

Interpolant $I$ of $F = A \cup B$: add literals of $I$: exclude trace $T$
Automated invariant generation

- Loop: \( \text{pre while } C \text{ do } T \text{ post} \)
  - \( \forall s. \text{pre}[s] \supset I(s) \)
  - \( \forall s, s'. I(s) \land C[s] \land T[s, s'] \supset I(s') \)
  - \( \forall s. I(s) \land \neg C[s] \supset \text{post}(s) \)

- Invariant \( I \) made of symbols \textit{common} to \textit{pre} and \textit{post}

- \( A \): \( k \)-unfolding of loop; \( B \): post-condition violated

- \( A, B \vdash \bot \)

- Interpolant of \((A, B)\): candidate invariant
Basic notions for interpolation: Colors

Non-variable symbol:
- *A-colored*: occurs in $A$ and not in $B$
- *B-colored*: occurs in $B$ and not in $A$
- *Transparent*: occurs in both

Ground term/literal/clause:
- All transparent symbols: *transparent*
- *A-colored* (at least one) and transparent symbols: *A-colored*
- *B-colored* (at least one) and transparent symbols: *B-colored*
- Otherwise: *AB-mixed*
Projections

\( C \): disjunction (conjunction) of literals

**Symmetric projections:**

- \( C|_A \): \( A \)-colored and transparent literals
- \( C|_B \): \( B \)-colored and transparent literals
- \( C|_T \): transparent literals
- \( \bot \) (\( \top \)) if empty

**Asymmetric projections:**

- \( C \setminus B = C|_A \setminus C|_T \) (\( A \)-colored only)
- \( C \downarrow_B = C|_B \) (transparent go with \( B \)-colored)
Partial interpolant

- Clause $C$ in refutation of $A \cup B$
- Partial interpolant $PI(C)$: interpolant of $A \land \neg (C|_A)$ and $B \land \neg (C|_B)$
- If $C$ is $\square$: $PI(C)$ interpolant of $(A, B)$
- Requirements:
  - $A \land \neg (C|_A) \vdash PI(C)$
  - $B \land \neg (C|_B) \land PI(C) \vdash \bot$
  - $PI(C)$ transparent
Given: proof (refutation) of $A \cup B$ ($A$ and $B$ sets of clauses)

**Interpolation system**: extracts interpolant of ($A$, $B$)

**How?** Attaching $Pl(C)$ to each clause $C$ in proof

$Pl(\square)$ is interpolant of ($A$, $B$)

**Complete** interpolation system
Why interpolation for propositional resolution?

- Propositional logic
- Davis-Putnam-Logemann-Loveland procedure (DPLL)
- Decision procedure: candidate model $M$
  model found: return $sat$;
  failure: return $unsat$
- Generated proofs: by resolution
DPLL as transition system

State of derivation: $M \parallel F$ or $M \parallel F \parallel C$

- **Decide**: guess $L$ is true, add it to $M$ (*decided literals*)
- **UnitPropagate**: propagate consequences (*implied literals*)
- **Conflict**: detect $L_1 \lor \ldots \lor L_n$ all false
- **Explain**: resolve *conflict clause with justification*
- **Learn**: may learn conflict clause
- **Backjump**: undo at least one decision
- **Unsat**: conflict clause is $\square$ (nothing else to try)
Proof produced by DPLL

- Resolution steps in *Explain* transitions
- Between conflict clauses and justifications
- Justifications are either input clauses or learnt clauses (former conflict clauses)
- Clauses involved: input clauses and conflict clauses
Propositional interpolation systems

- Literals in proof are input literals
- Input literals are either $A$-colored or $B$-colored or transparent
- No $AB$-mixed literals
The HKPYM interpolation system

C clause in refutation of $A \cup B$ by propositional resolution:

- $C \in A$: $PI(C) = \bot$
- $C \in B$: $PI(C) = \top$
- $C \lor D$ propositional resolvent of $p_1: C \lor L$ and $p_2: D \lor \neg L$:
  - $L$ A-colored: $PI(C \lor D) = PI(p_1) \lor PI(p_2)$
  - $L$ B-colored: $PI(C \lor D) = PI(p_1) \land PI(p_2)$
  - $L$ transparent: $PI(C \lor D) = (L \lor PI(p_1)) \land (\neg L \lor PI(p_2))$

Symmetric projections
Example with HKPYM

\[ A = \{ a \lor e, \neg a \lor b, \neg a \lor c \} \quad B = \{ \neg b \lor \neg c \lor d, \neg d, \neg e \} \]

▷ \( a \lor e \ \bot \) resolves with \( \neg e \ \top \) to yield \( a \ [e] \):  
e is transparent: \[ (e \lor \bot) \land (\neg e \lor \top) \] = \[ e \]
Example with HKPYM

\[ A = \{a \lor e, \neg a \lor b, \neg a \lor c\} \quad B = \{\neg b \lor \neg c \lor d, \neg d, \neg e\} \]

- \(a \lor e [\bot]\) resolves with \(\neg e [\top]\) to yield \(a [e]\):
  - \(e\) is transparent: \([e \lor \bot] \land (\neg e \lor \top) = [e]\)
- \(a [e]\) resolves with \(\neg a \lor c [\bot]\) to yield \(c [e]\):
  - \(a\) is \(A\)-colored: \([e \lor \bot] = [e]\)
Example with HKPYM

$$A = \{ a \lor e, \neg a \lor b, \neg a \lor c \} \quad B = \{ \neg b \lor \neg c \lor d, \neg d, \neg e \}$$

- $a \lor e [\bot]$ resolves with $\neg e [\top]$ to yield $a [e]$: $e$ is transparent: $[(e \lor \bot) \land (\neg e \lor \top)] = [e]$.
- $a [e]$ resolves with $\neg a \lor c [\bot]$ to yield $c [e]$: $a$ is $A$-colored: $[e \lor \bot] = [e]$.
- $a [e]$ resolves with $\neg a \lor b [\bot]$ to yield $b [e]$: $a$ is $A$-colored: $[e \lor \bot] = [e]$.
Example with HKPYM

\[ A = \{a \lor e, \neg a \lor b, \neg a \lor c\} \quad B = \{\neg b \lor \neg c \lor d, \neg d, \neg e\} \]

- \( a \lor e \ [\bot] \) resolves with \( \neg e \ [\top] \) to yield \( a \ [e] \):
  - \( e \) is transparent: \([ (e \lor \bot) \land (\neg e \lor \top) ] = [e] \)
- \( a \ [e] \) resolves with \( \neg a \lor c \ [\bot] \) to yield \( c \ [e] \):
  - \( a \) is \( A \)-colored: \([ e \lor \bot ] = [e] \)
- \( a \ [e] \) resolves with \( \neg a \lor b \ [\bot] \) to yield \( b \ [e] \):
  - \( a \) is \( A \)-colored: \([ e \lor \bot ] = [e] \)
- \( b \ [e] \) resolves with \( \neg b \lor \neg c \lor d \ [\top] \) to yield \( \neg c \lor d \ [b \lor e] \):
  - \( b \) is transparent: \([ (b \lor e) \land (\neg b \lor \top) ] = [b \lor e] \)
Example with HKPYM

\[ A = \{a \lor e, \neg a \lor b, \neg a \lor c\} \quad B = \{\neg b \lor \neg c \lor d, \neg d, \neg e\} \]

- \(a \lor e\) [\(\bot\)] resolves with \(\neg e\) [\(\top\)] to yield \(a\) [\(e\)]:
  - \(e\) is transparent: \([e \lor \bot] \land (\neg e \lor \top) = [e]\)
- \(a\) [\(e\)] resolves with \(\neg a \lor c\) [\(\bot\)] to yield \(c\) [\(e\)]:
  - \(a\) is \(A\)-colored: \([e \lor \bot] = [e]\)
- \(a\) [\(e\)] resolves with \(\neg a \lor b\) [\(\bot\)] to yield \(b\) [\(e\)]:
  - \(a\) is \(A\)-colored: \([e \lor \bot] = [e]\)
- \(b\) [\(e\)] resolves with \(\neg b \lor \neg c \lor d\) [\(\top\)] to yield \(\neg c \lor d\) [\(b \lor e\)]:
  - \(b\) is transparent: \([(b \lor e) \land (\neg b \lor \top)] = [b \lor e]\)
- \(c\) [\(e\)] resolves with \(\neg c \lor d\) [\(b \lor e\)] to yield \(d\) [\(e \lor (c \land b)\)]:
  - \(c\) is transparent: \([(c \lor e) \land (\neg c \lor b \lor e)] = [e \lor (c \land b)]\)
Example with HKPYM

\[ A = \{ a \lor e, \neg a \lor b, \neg a \lor c \} \quad B = \{ \neg b \lor \neg c \lor d, \neg d, \neg e \} \]

- \( a \lor e \) [\( \bot \)] resolves with \( \neg e \) [\( \top \)] to yield \( a \) [\( e \)]:
  - \( e \) is transparent: \([ (e \lor \bot) \land (\neg e \lor \top) ] = [e] \)
- \( a \) [\( e \)] resolves with \( \neg a \lor c \) [\( \bot \)] to yield \( c \) [\( e \)]:
  - \( a \) is \( A \)-colored: \([ e \lor \bot ] = [e] \)
- \( a \) [\( e \)] resolves with \( \neg a \lor b \) [\( \bot \)] to yield \( b \) [\( e \)]:
  - \( a \) is \( A \)-colored: \([ e \lor \bot ] = [e] \)
- \( b \) [\( e \)] resolves with \( \neg b \lor \neg c \lor d \) [\( \top \)] to yield \( \neg c \lor d \) [\( b \lor e \)]:
  - \( b \) is transparent: \([ (b \lor e) \land (\neg b \lor \top) ] = [b \lor e] \)
- \( c \) [\( e \)] resolves with \( \neg c \lor d \) [\( b \lor e \)] to yield \( d \) [\( e \lor (c \land b) \)]:
  - \( c \) is transparent: \([ (c \lor e) \land (\neg c \lor b \lor e) ] = [e \lor (c \land b)] \)
- \( d \) [\( e \lor (c \land b) \)] resolves with \( \neg d \) [\( \top \)] to yield \( \Box \) [\( e \lor (c \land b) \)]:
  - \( d \) is \( B \)-colored: \([ (e \lor (c \land b)) \land \top ] = [e \lor (c \land b)] \)
The MM interpolation system

C clause in refutation of $A \cup B$ by propositional resolution:

- $C \in A$: $PI(C) = C|_T$
- $C \in B$: $PI(C) = T$
- $C \lor D$ propositional resolvent of $p_1: C \lor L$ and $p_2: D \lor \neg L$:
  - $L$ A-colored: $PI(C \lor D) = PI(p_1) \lor PI(p_2)$
  - $L$ B-colored or transparent: $PI(C \lor D) = PI(p_1) \land PI(p_2)$

Asymmetric projections
Example with MM

\[ A = \{ a \lor e, \neg a \lor b, \neg a \lor c \} \quad B = \{ \neg b \lor \neg c \lor d, \neg d, \neg e \} \]

- \( a \lor e \) \( [e] \) resolves with \( \neg e \) \( [\top] \) to yield \( a \) \( [e] \): 
  - e is transparent: \( [e \land \top] = [e] \)
Example with MM

\[ A = \{a \lor e, \neg a \lor b, \neg a \lor c\} \quad B = \{\neg b \lor \neg c \lor d, \neg d, \neg e\} \]

- \(a \lor e\) [e] resolves with \(\neg e\) [\(\top\)] to yield \(a\) [e]:
  - e is transparent: \([e \land \top] = [e]\)

- \(a\) [e] resolves with \(\neg a \lor c\) [c] to yield \(c\) [e \(\lor\) c]:
  - a is \(A\)-colored: \([e \lor c]\)
Example with MM

\[ A = \{ a \lor e, \neg a \lor b, \neg a \lor c \} \quad B = \{ \neg b \lor \neg c \lor d, \neg d, \neg e \} \]

\[
\begin{align*}
&\quad \quad a \lor e \ [e] \text{ resolves with } \neg e \ [\top] \text{ to yield } a \ [e]: \\
&\text{e is transparent: } [e \land \top] = [e]
\end{align*}
\]

\[
\begin{align*}
&\quad \quad a \ [e] \text{ resolves with } \neg a \lor c \ [c] \text{ to yield } c \ [e \lor c]: \\
&\text{a is A-colored: } [e \lor c]
\end{align*}
\]

\[
\begin{align*}
&\quad \quad a \ [e] \text{ resolves with } \neg a \lor b \ [b] \text{ to yield } b \ [e \lor b]: \\
&\text{a is A-colored: } [e \lor b]
\end{align*}
\]
Example with MM

\[ A = \{a \lor e, \neg a \lor b, \neg a \lor c\} \quad B = \{\neg b \lor \neg c \lor d, \neg d, \neg e\} \]

- \(a \lor e\) [e] resolves with \(\neg e\) [\(\top\)] to yield \(a\) [e]:
  - e is transparent: \([e \land \top] = [e]\)
- \(a\) [e] resolves with \(\neg a \lor c\) [c] to yield \(c\) [e \lor c]:
  - a is A-colored: \([e \lor c]\)
- \(a\) [e] resolves with \(\neg a \lor b\) [b] to yield \(b\) [e \lor b]:
  - a is A-colored: \([e \lor b]\)
- \(b\) [e \lor b] resolves with \(\neg b \lor \neg c \lor d\) [\(\top\)] to yield \(\neg c \lor d\) [e \lor b]:
  - b is transparent: \([(e \lor b) \land \top] = [e \lor b]\)
Example with MM

\[ A = \{ a \lor e, \neg a \lor b, \neg a \lor c \} \quad B = \{ \neg b \lor \neg c \lor d, \neg d, \neg e \} \]

- \( a \lor e \) [e] resolves with \( \neg e \) [\( \top \)] to yield \( a \) [e]:
  - \( e \) is transparent: \([ e \land \top ] = [ e ]\)
- \( a \) [e] resolves with \( \neg a \lor c \) [c] to yield \( c \) [\( e \land c \)]:
  - \( a \) is \( A \)-colored: \([ e \lor c ]\)
- \( a \) [e] resolves with \( \neg a \lor b \) [b] to yield \( b \) [\( e \land b \)]:
  - \( a \) is \( A \)-colored: \([ e \lor b ]\)
- \( b \) [\( e \land b \)] resolves with \( \neg b \lor \neg c \lor d \) [\( \top \)] to yield \( \neg c \lor d \) [\( e \land b \)]:
  - \( b \) is transparent: \([ (e \land b) \land \top ] = [ e \land b ]\)
- \( c \) [\( e \land c \)] resolves with \( \neg c \lor d \) [\( e \land b \)] to yield \( d \) [\( e \land (c \land b) \)]:
  - \( c \) is transparent: \([ (e \land c) \land (e \land b)] = [ e \land (c \land b) ]\)
Example with MM

\[ A = \{ a \lor e, \neg a \lor b, \neg a \lor c \} \quad B = \{ \neg b \lor \neg c \lor d, \neg d, \neg e \} \]

- \( a \lor e \) [e] resolves with \( \neg e \) [\( \top \)] to yield \( a \) [e]:
  - \( e \) is transparent: \( [e \land \top] = [e] \)
- \( a \) [e] resolves with \( \neg a \lor c \) [c] to yield \( c \) [e \lor c]:
  - \( a \) is \( A \)-colored: \( [e \lor c] \)
- \( a \) [e] resolves with \( \neg a \lor b \) [b] to yield \( b \) [e \lor b]:
  - \( a \) is \( A \)-colored: \( [e \lor b] \)
- \( b \) [e \lor b] resolves with \( \neg b \lor \neg c \lor d \) [\( \top \)] to yield \( \neg c \lor d \) [e \lor b]:
  - \( b \) is transparent: \( [(e \lor b) \land \top] = [e \lor b] \)
- \( c \) [e \lor c] resolves with \( \neg c \lor d \) [e \lor b] to yield \( d \) [e \lor (c \land b)]:
  - \( c \) is transparent: \( [(e \lor c) \land (e \lor b)] = [e \lor (c \land b)] \)
- \( d \) [e \lor (c \land b)] resolves with \( \neg d \) [\( \top \)] to yield \( \square \) [e \lor (c \land b)]:
  - \( d \) is \( B \)-colored: \( [(e \lor (c \land b)) \land \top] = [e \lor (c \land b)] \)
Equality changes the picture ...

- Propositional logic: what is *transparent* remains *transparent*
- Equality: what if *AB-mixed equation* $t_a \simeq t_b$ is derived?
  - $t_a$: $A$-colored ground term; $t_b$: $B$-colored ground term
- *Congruence closure*: $t_a$ and $t_b$ representatives of singly-colored classes: merge: one of them should become transparent
- *Rewriting*: $t_a \succ t_b$ and $t_b$ in normal form:
  - $t_b$ should become transparent
- *$A$-colored/$B$-colored/transparent change dynamically!*
Equality-interpolating theories

- $\mathcal{T}$: theory
- $A$ and $B$: $\mathcal{T}$-formulæ or sets of $\mathcal{T}$-clauses
- if $A \land B \models_{\mathcal{T}} t_a \simeq t_b$:
  
  $$A \land B \models_{\mathcal{T}} t_a \simeq t \land t_b \simeq t$$
  
  for transparent ground term $t$

Congruence closure: $t$ representative of the new congruence class
Separating ordering

Ordering $\succ$ on terms and literals: 

- *separating* if $t \succ s$ whenever $s$ is transparent and $t$ is not

Rewriting: $t_a$ and $t_b$ rewritten to $t$
Separating implies colorable

- **Colorable proof**: no $AB$-mixed literals
- **Lemma**: Separating ordering $\Rightarrow$ all ground proofs by resolution and rewriting colorable
- **Intuition**: if $s \simeq r$ and $l[s]$ not $AB$-mixed and $s \succ r$, then $l[r]$ not $AB$-mixed
EUF is equality-interpolating

- Equational proofs: chains $s \leftrightarrow t$; valley proofs $s \leftrightarrow o \leftrightarrow t$
- **Theorem**: The quantifier-free fragment of the theory of equality is equality-interpolating
- **Intuition**: $A \land B \models t_a \simeq t_b \Rightarrow A \cup B \cup \{t_a \not\simeq t_b\} \vdash \bot$ by ground completion + separating ordering; colorable valley proof $t_a \rightarrow t \leftarrow t_b$ with $t$ transparent.

Other equality-interpolating theories: *linear inequalities, lists*
Equality sharing aka Nelson-Oppen scheme

$\mathcal{T}$-satisfiability procedure for $\mathcal{T} = \bigcup_{i=1}^{n} \mathcal{T}_i$

- **Disjoint**: only shared symbol is $\simeq$
- **Stably infinite**: every $\mathcal{T}_i$-sat ground formula has $\mathcal{T}_i$-model of infinite cardinality
- Equipped with $\mathcal{T}_i$-satisfiability procedure $\mathcal{Q}_i$
- **New**: Equality-interpolating + $\mathcal{Q}_i$ generates proofs and $\mathcal{T}_i$-interpolants

- Mixed terms *separated* by introducing new constants
- Each $\mathcal{Q}_i$ propagates all entailed (disjunctions of) equalities between shared constants
Model-based theory combination

A variant of equality sharing:

- Each $Q_i$ builds candidate $\mathcal{T}_i$-model $M_i$;
- $Q_i$ propagates equalities between ground terms true in $M_i$;
- They are guesses: if not entailed undo by backtracking;
- Suitable for backtracking based engine DPLL: DPLL($\mathcal{T}$)

What follows works also for model-based theory combination
Interpolation in equality sharing

- $A \cup B$ set of ground $T$-literals (unit $T$-clauses)
- Each $Q_i$ deals with $A_i \cup B_i \cup K$: interpolation wrt partition $(A', B')$ of $A_i \cup B_i \cup K$
- Equality-interpolating: $K$ contains no $AB$-mixed equations
- $A' = A_i \cup K|_A$
  $B' = B_i \cup K|_B$
- *Theory-specific partial interpolant* $PI^i_{(A', B')}(C)$ of propagated equation $C$:
  $T_i$-interpolant of $(A' \land \neg(C|_A), B' \land \neg(C|_B))$
Example with theory-specific partial interpolants

- $y_1 \leq x_1$ with $x_1 \leq y_1$ yield $x_1 \simeq y_1 \ [y_1 \leq x_1]$

$L_1$-interpolant of $(y_1 \leq x_1, \ x_1 \leq y_1 \land x_1 \not\simeq y_1)$
Example with theory-specific partial interpolants

- \( y_1 \leq x_1 \) with \( x_1 \leq y_1 \) yield \( x_1 \simeq y_1 \ [y_1 \leq x_1] \)
  \( LI \)-interpolant of \((y_1 \leq x_1, x_1 \leq y_1 \land x_1 \not\simeq y_1)\)

- \( x_1 \simeq y_1 \) with \( a_1 \simeq f(x_1), a_2 \simeq f(y_1) \) yield \( a_1 \simeq a_2 \ [x_1 \not\simeq y_1] \)
  \( EUF \)-interpolant of \(\{a_1 \simeq f(x_1), a_2 \simeq f(y_1), a_1 \not\simeq a_2\}, \{x_1 \simeq y_1\}\)
Example with theory-specific partial interpolants

- \( y_1 \leq x_1 \) with \( x_1 \leq y_1 \) yield \( x_1 \simeq y_1 \) \([y_1 \leq x_1]\)
  \(LI\)-interpolant of \((y_1 \leq x_1, x_1 \leq y_1 \land x_1 \not\simeq y_1)\)

- \( x_1 \simeq y_1 \) with \( a_1 \simeq f(x_1), a_2 \simeq f(y_1) \) yield \( a_1 \simeq a_2 \) \([x_1 \not\simeq y_1]\)
  \(EUF\)-interpolant of \((\{a_1 \simeq f(x_1), a_2 \simeq f(y_1), a_1 \not\simeq a_2\}, \{x_1 \simeq y_1\})\)

- \( x_2 \simeq g(b) \) with \( y_2 \simeq g(b) \) yield \( x_2 \simeq y_2 \) \([\top]\)
  \(EUF\)-interpolant of \((\{\top\}, \{x_2 \simeq g(b), y_2 \simeq g(b), x_2 \not\simeq y_2\})\)
  \(K = \{x_1 \simeq y_1, a_1 \simeq a_2, x_2 \simeq y_2\}\) (propagated equalities)
Example with theory-specific partial interpolants

- \( y_1 \leq x_1 \) with \( x_1 \leq y_1 \) yield \( x_1 \simeq y_1 \) \([y_1 \leq x_1]\)

  *LI*-interpolant of \((y_1 \leq x_1, x_1 \leq y_1 \land x_1 \not\simeq y_1)\)

- \( x_1 \simeq y_1 \) with \( a_1 \simeq f(x_1), a_2 \simeq f(y_1) \) yield \( a_1 \simeq a_2 \) \([x_1 \not\simeq y_1]\)

  *EUF*-interpolant of \(\{a_1 \simeq f(x_1), a_2 \simeq f(y_1), a_1 \not\simeq a_2\}\), \(\{x_1 \simeq y_1\}\)

- \( x_2 \simeq g(b) \) with \( y_2 \simeq g(b) \) yield \( x_2 \simeq y_2 \) \([\top]\)

  *EUF*-interpolant of \(\{\top\}, \{x_2 \simeq g(b), y_2 \simeq g(b), x_2 \not\simeq y_2\}\)

  \(K = \{x_1 \simeq y_1, a_1 \simeq a_2, x_2 \simeq y_2\}\) (propagated equalities)

- \( a_1 \simeq a_2, x_2 \simeq y_2 \) with \( a_1 + x_2 \simeq x_3, a_2 + y_2 \simeq y_3 \) yield \( x_3 \simeq y_3 \)

- \( x_3 \simeq y_3 \) and \( x_3 < y_3 \) yields □ \([x_2 - y_2 \simeq x_3 - y_3]\)

  *LI*-interpolant of

  \(\{a_1 + x_2 \simeq x_3, a_2 + y_2 \simeq y_3, a_1 \simeq a_2\}\), \(\{x_3 < y_3, x_2 \simeq y_2\}\)
The EQSH interpolation system

- C unit clause in refutation $A_i \cup B_i \cup K \vdash_{\mathcal{I}_i} \bot$
  - $C \in A$: $PL(C) = \bot$
  - $C \in B$: $PL(C) = \top$
  - C derived as $A_i \cup B_i \cup K \vdash_{\mathcal{I}_i} C$:
    $$PL(C) = (PL_{(A',B')}^i(C) \lor \bigvee_{L \in A'} PL(L)) \land \bigwedge_{L \in B'} PL(L)$$

- $L \in A'$: input $A$-literals + $A$-colored propagated equations
- $L \in B'$: input $B$-literals + $B$-colored/transparent propagated equations (if asymmetric)
- $PL(C) = PL_{(A',B')}^i(C)$ if $C$ does not depend on propagated equations
Example with partial interpolants by EQSH

- $y_1 \leq x_1$ with $x_1 \leq y_1$ yield $x_1 \simeq y_1 [y_1 \leq x_1]$

$$PL(x_1 \simeq y_1) = PL^L(x_1 \simeq y_1) = y_1 \leq x_1$$
Example with partial interpolants by EQSH

- $y_1 \leq x_1$ with $x_1 \leq y_1$ yield $x_1 \simeq y_1$ [$y_1 \leq x_1$]
  \[
  PL(x_1 \simeq y_1) = PL^L(x_1 \simeq y_1) = y_1 \leq x_1
  \]

- $x_1 \simeq y_1$ with $a_1 \simeq f(x_1)$, $a_2 \simeq f(y_1)$ yield $a_1 \simeq a_2$ [$y_1 < x_1$]
  \[
  PL(a_1 \simeq a_2) = PL^{\text{EUF}}(a_1 \simeq a_2) \land PL(x_1 \simeq y_1) = \left( x_1 \not\simeq y_1 \land y_1 \leq x_1 \right) = y_1 < x_1
  \]
Example with partial interpolants by EQSH

$y_1 \leq x_1$ with $x_1 \leq y_1$ yield $x_1 \simeq y_1 [y_1 \leq x_1]$

$PI(x_1 \simeq y_1) = PI^{LI}(x_1 \simeq y_1) = y_1 \leq x_1$

$x_1 \simeq y_1$ with $a_1 \simeq f(x_1)$, $a_2 \simeq f(y_1)$ yield $a_1 \simeq a_2 [y_1 < x_1]$

$PI(a_1 \simeq a_2) = PI^{EUF}(a_1 \simeq a_2) \land PI(x_1 \simeq y_1) = (x_1 \not\simeq y_1 \land y_1 \leq x_1) = y_1 < x_1$

$x_2 \simeq g(b)$ with $y_2 \simeq g(b)$ yield $x_2 \simeq y_2 [\top]$

$PI(x_2 \simeq y_2) = PI^{EUF}(x_2 \simeq y_2) = \top$
Example with partial interpolants by EQSH

- $y_1 \leq x_1$ with $x_1 \leq y_1$ yield $x_1 \simeq y_1$ $[y_1 \leq x_1]$
  \[PI(x_1 \simeq y_1) = PL^L(x_1 \simeq y_1) = y_1 \leq x_1\]

- $x_1 \simeq y_1$ with $a_1 \simeq f(x_1)$, $a_2 \simeq f(y_1)$ yield $a_1 \simeq a_2$ $[y_1 < x_1]$
  \[PI(a_1 \simeq a_2) = PL^{EUF}(a_1 \simeq a_2) \land PI(x_1 \simeq y_1) = (x_1 \not\simeq y_1 \land y_1 \leq x_1) = y_1 < x_1\]

- $x_2 \simeq g(b)$ with $y_2 \simeq g(b)$ yield $x_2 \simeq y_2$ $[\top]$
  \[PI(x_2 \simeq y_2) = PL^{EUF}(x_2 \simeq y_2) = \top\]

- $a_1 \simeq a_2$, $x_2 \simeq y_2$ with $a_1 + x_2 \simeq x_3$, $a_2 + y_2 \simeq y_3$ yield $x_3 \simeq y_3$

- $x_3 \simeq y_3$ and $x_3 < y_3$ yields $\Box [y_1 < x_1 \lor x_2 - y_2 \simeq x_3 - y_3]$
  \[PI(\Box) = (PL^L(\Box) \lor PI(a_1 \simeq a_2)) \land PI(x_2 \simeq y_2) = (x_2 - y_2 \simeq x_3 - y_3 \lor y_1 < x_1)\]
DPLL(\(\mathcal{T}\)) as transition system

State of derivation: \(M \parallel F\) or \(M \parallel F \parallel C\)

- **\(\mathcal{T}\)-Propagate**: add to \(M\) an \(L\) that is \(\mathcal{T}\)-consequence of \(L_1, \ldots, L_n \in M\)
  
  **\(\mathcal{T}\)-lemma**: \(\neg L_1 \lor \ldots \lor \neg L_n \lor L\) *(justification)*

- **\(\mathcal{T}\)-Conflict**: detect that \(L_1, \ldots, L_n\) in \(M\) are \(\mathcal{T}\)-inconsistent
  
  **\(\mathcal{T}\)-conflict clause**: \(\neg L_1 \lor \ldots \lor \neg L_n\)

For model-based theory combination:

- **PropagateEq**: add to \(M\) ground \(s \simeq t\) true in \(\mathcal{T}_i\)-model
Interpolation in DPLL(\(\mathcal{T}\))

- \(A \cup B\) set of ground \(\mathcal{T}\)-clauses
- DPLL(\(\mathcal{T}\))-refutation of \(A \cup B\): propositional resolution + \(\mathcal{T}\)-conflict clauses + \(\mathcal{T}\)-lemmas
- \(C = \neg\ L_1 \lor \ldots \lor \neg\ L_n\) \(\mathcal{T}\)-conflict clause, because \(\neg\ C = L_1 \land \ldots \land L_n\) is \(\mathcal{T}\)-unsat
- \(C = \neg\ L_1 \lor \ldots \lor \neg\ L_n \lor L\) \(\mathcal{T}\)-lemma, means \(\neg\ C = L_1 \land \ldots \land L_n \land \neg L\) is \(\mathcal{T}\)-unsat
- \((\neg C)|_A \land (\neg C)|_B\) is \(\mathcal{T}\)-unsat
- The \(\mathcal{T}\)-interpolant of \(((\neg C)|_A, (\neg C)|_B)\) computed by EQSH provides partial interpolant of \(C\) in DPLL(\(\mathcal{T}\))-refutation
HKPYM–T and MM–T interpolation systems

Add one case to either HKPYM or MM:

- $C$ is $\mathcal{T}$-conflict clause or $\mathcal{T}$-lemma:
  
  $PI(C)$ is $\mathcal{T}$-interpolant of $((\neg C)|_A, (\neg C)|_B)$ extracted by EQSH from $\neg C \vdash_\mathcal{T} \bot$
Summary of contributions

Survey of the state of the art in ground interpolation:

- Definitions and terminology: towards standardization
- Interpolation systems HKPYM and MM
- Interpolation and equality: connecting \textit{equality-interpolating theory} and \textit{separating ordering}
- Interpolation system EQSH for equality sharing/model based theory combination
- Interpolation systems HKPYM–T and MM–T for DPLL($\mathcal{T}$)

References: in the article in the TABLEAUX proceedings
Current work: beyond ground problems

- Interpolation system for a superposition based engine $\Gamma$
  - Ground proofs
  - Non-ground proofs: investigating restrictions
- Interpolation system for $\text{DPLL}(\Gamma + T)$

Maria Paola Bonacina and Moa Johansson.
Towards interpolation in an SMT solver with integrated superposition.
Workshop on Satisfiability Modulo Theories (SMT), Snowbird, July 2011.
Summary

- Symbolic Execution: computing pre-conditions, post-conditions
- Model Checking: computing images, pre-images
- Theorem Proving: computing interpolants
- Theorem proving *is* artificial intelligence
- Theorem proving for program checking *is* artificial intelligence
Thanks

- To the PC of TABLEAUX
- To the PC of FTP
- To the local organizers and
- Thank you all for being here!