Towards an interpolating DPLL($\Gamma+\mathcal{T}$)

Maria Paola Bonacina

Dipartimento di Informatica
Università degli Studi di Verona
Verona, Italy

November 4, 2011

What is interpolation?

Interpolant I of (A, B) in theory $\mathcal{T}$: $A \vdash_{\mathcal{T}} B$

- Implied by A and implies B: $A \vdash_{\mathcal{T}} I$ and $I \vdash_{\mathcal{T}} B$
- *Uninterpreted* symbols in I *common* to A and B
- *Interpreted* symbols *allowed* (if $\mathcal{T}$ not empty)

Reverse interpolant I of (A, B): $A, B \vdash_{\mathcal{T}} \bot$

- Implied by A and inconsistent with B: $A \vdash_{\mathcal{T}} I$ and $B, I \vdash_{\mathcal{T}} \bot$

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

Uninterpreted symbols

- *A-local* (*B-local*): in A (B) and not in B (A)
- *Global*: in both

Thus, term/atom/literal/clause:

- *A-local*: all uninterpreted symbols in A + at least one A-local
- *B-local*: all uninterpreted symbols in B + at least one B-local
- *Global*: all uninterpreted symbols are global
- Otherwise: *AB-mixed*

Sample application: Automated invariant generation

- Loop: $\{pre\}$ `while C do T` $\{post\}$
- Invariant I made of symbols *common* to *pre* and *post*

- A: unfolding of the loop k times
- B: post-condition violated
- If post-condition satisfied after k iterations: $A, B \vdash \bot$
- (Reverse) interpolant of (A, B): candidate invariant

Improving the state of the art in interpolation

- *Generality*: interpolants for more logics, theories, inference systems
- *Quality*: better interpolants; stronger? weaker? shorter?

First direction: interpolation for DPLL($\Gamma+\mathcal{T}$)

What is DPLL($\Gamma+\mathcal{T}$)

- DPLL($\Gamma+\mathcal{T}$): SMT-solver with superposition (Γ) integrated
- Fully automated treatment of quantifiers
- $\mathcal{T}$-satisfiability of $S = \mathcal{R} \cup P$
- $\mathcal{R}$: non-ground clauses without $\mathcal{T}$-symbols;
  P: ground clauses with $\mathcal{T}$-symbols
- Γ: non-ground clauses + ground unit $\mathcal{R}$-clauses
- DPLL($\mathcal{T}$): all ground clauses

Two approaches to interpolation

- Building interpolation into the decision procedure (e.g., congruence closure, arrays)
- Inductive approach:
  - Given refutation build interpolant by structural induction
  - Good for generic inference systems

Both needed for DPLL($\Gamma+\mathcal{T}$)

Inductive approach

- Attach a *partial interpolant* to every clause in the refutation
- Partial interpolant of $\square$ is interpolant
- Every inference: Partial interpolant of conclusion built from partial interpolants of premises

Partial interpolant

- C occurs in a refutation of $A \cup B$
- $A \wedge B \vdash C$
- $A \wedge \neg C \vdash \neg B \vee C$
- Interpolant of $A \wedge \neg C$ and $\neg B \vee C$
- Reverse interpolant of $A \wedge \neg C$ and $B \wedge \neg C$
- Change of partition unless C is global
- Use *projections*

Projections

C: disjunction (conjunction) of literals

- $C|_A$: A-local (and global literals) of C
- $C|_B$: B-local and global literals of C
- $\bot$ ($\top$) if empty

If clause C has no AB-mixed literals: $C = C|_A \vee C|_B$

Partial interpolant

- Clause C in refutation of $A \cup B$
- *Partial interpolant* $PI(C)$: interpolant of
  $A \wedge \neg(C|_A)$ and
  $B \wedge \neg(C|_B)$
- If C is $\square$: $PI(C)$ interpolant of (A, B)
- Requirements:
  - $A \wedge \neg(C|_A) \vdash PI(C)$
  - $B \wedge \neg(C|_B) \wedge PI(C) \vdash \bot$
  - $PI(C)$ global

Interpolation system

- Define *interpolation system*:
  For every inference rule: how it builds partial interpolant of conclusion from partial interpolants of premises
- Prove *complete*:
  Show that these formulæ are indeed partial interpolants

Interpolating system for DPLL($\Gamma+\mathcal{T}$)

Interpolating systems for:

1. DPLL
2. Equality sharing
3. DPLL($\mathcal{T}$)
4. Γ: superposition
5. DPLL($\Gamma+\mathcal{T}$)

Propositional interpolation systems

- Propositional resolution
- DPLL: generates proof by resolution
- Input literals are either *A-local* or *B-local* or *global*
- Literals in proof are input literals
- *No AB-mixed* literals
- Case analysis on literal resolved upon

Interpolation system for resolution

C clause in ground Γ-refutation of $A \cup B$:

- $C \in A$: $PI(C) = \bot$
- $C \in B$: $PI(C) = \top$
- $C \vee D$ resolvent of $p_1 : C \vee L$ and $p_2 : D \vee \neg L$:
  - L is A-local: $PI(C \vee D) = PI(p_1) \vee PI(p_2)$
  - L is B-local: $PI(C \vee D) = PI(p_1) \wedge PI(p_2)$
  - L is global: $PI(C \vee D) = (L \vee PI(p_1)) \wedge (\neg L \vee PI(p_2))$

Equality changes the picture ...

- What if *AB-mixed equation* $t_a \simeq t_b$ is derived?
- *Congruence closure*:
  t_a: representative of congruence class of A-local terms
  t_b: representative of congruence class of B-local terms
  Merge: one of them should become global
- *Rewriting*:
  t_a (t_b): A-local (B-local) ground term in normal form
  $t_a \succ t_b$: replace t_a with t_b everywhere
  t_b should become global!
- A-local/B-local/global change dynamically!

Equality-interpolating theories

$\mathcal{T}$ equality-interpolating:

If $A \cup B \models_{\mathcal{T}} t_a \simeq t_b$ then
$A \cup B \models_{\mathcal{T}} t_a \simeq t \wedge t_b \simeq t$ for some global ground term t

Congruence closure: t representative of new congruence class

Separating ordering

Ordering $\succ$ on terms and literals:
separating if $t \succ s$ whenever s is global and t is not

Rewriting: t_a and t_b rewritten to t

Lemma: Separating ordering implies *no AB-mixed literals* in ground Γ-proof trees

Connecting equality-interpolating and separating ordering

Theorem: The quantifier-free fragment of the theory of equality is *equality-interpolating*

If $A \cup B \models t_a \simeq t_b$ then
$A \cup B \cup \{t_a \not\simeq t_b\} \vdash \bot$ by Γ with *separating ordering*
valley proof $t_a \stackrel{*}{\rightarrow} t \stackrel{*}{\leftarrow} t_b$ with no AB-mixed equations
t must be global

Other equality-interpolating theories: *lists*; *linear inequalities* in *rational* arithmetic

Equality sharing aka Nelson-Oppen scheme

- $\mathcal{T}$-satisfiability procedure for $\mathcal{T} = \bigcup_{i=1}^{n} \mathcal{T}_i$ from $\mathcal{T}_i$-satisfiability procedure $\mathcal{Q}_i$
- In DPLL($\Gamma+\mathcal{T}$): Model-based theory combination

For interpolation:

- All $\mathcal{T}_i$'s equality-interpolating (equality is the common ground)
- All $\mathcal{Q}_i$'s generate proofs and $\mathcal{T}_i$-interpolants
- Propagated equalities: between shared constants; between ground uninterpreted terms

Interpolation in equality sharing

- $A \cup B$ set of ground $\mathcal{T}$-literals (unit $\mathcal{T}$-clauses)
- Each $\mathcal{Q}_i$ 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
- $A' = A_i \cup K|_A$ and $B' = B_i \cup K|_B$
- *Theory-specific partial interpolant* $PI^i_{(A',B')}(C)$ of propagated equation C:
  $\mathcal{T}_i$-interpolant of $(A' \wedge \neg(C|_A), B' \wedge \neg(C|_B))$

The EQSH interpolation system

C unit clause in refutation $A_i \cup B_i \cup K \vdash_{\mathcal{T}_i} \bot$

- $C \in A$: $PI(C) = \bot$
- $C \in B$: $PI(C) = \top$
- C derived as $A_i \cup B_i \cup K \vdash_{\mathcal{T}_i} C$:
  $PI(C) = (PI^i_{(A',B')}(C) \vee \bigvee_{L \in A'} PI(L)) \wedge \bigwedge_{L \in B'} PI(L)$

If $K = \emptyset$ (e.g., only one theory, or C does not depend on propagated equations) $PI(C) = PI^i_{(A',B')}(C)$

Interpolation in DPLL($\mathcal{T}$)

- $A \cup B$ set of ground $\mathcal{T}$-clauses
- DPLL($\mathcal{T}$)-refutation: propositional resolution + $\mathcal{T}$-lemmas
- C is $\mathcal{T}$-lemma means $\neg C$ is $\mathcal{T}$-unsat
- No AB-mixed literals: $\neg C = (\neg C)|_A \wedge (\neg C)|_B$
- $(\neg C)|_A \wedge (\neg C)|_B$ 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

Interpolation system for DPLL($\mathcal{T}$)

Add one case to interpolation system for propositional resolution:

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

Interpolation system GΓI: superposition

C clause in ground Γ-refutation of $A \cup B$:

- $c\colon C \vee l[r] \vee D$ generated from $p_1\colon C \vee s \simeq r$ and $p_2\colon D \vee l[s]$
  - $s \simeq r$ A-local: $PI(c) = PI(p_1) \vee PI(p_2)$
  - $s \simeq r$ B-local: $PI(c) = PI(p_1) \wedge PI(p_2)$
  - $s \simeq r$, $l[s]$ global: $PI(c) = (s \simeq r \vee PI(p_1)) \wedge (l[s] \vee PI(p_2))$
  - $s \simeq r$ global, $l[s]$ not:
    $PI(c) = (s \simeq r \vee PI(p_1)) \wedge (s \not\simeq r \vee PI(p_2))$
- Superposition into equational literal and Simplification: same

Completeness

Theorem: If the ordering is separating, GΓI is a *complete* interpolation system for ground Γ-refutations.

The proof shows that the partial interpolants built by GΓI satisfy the properties of partial interpolants.

Interpolation in DPLL($\Gamma+\mathcal{T}$)

- Hypothetical clauses: $H \rhd C$
- H: conjunction of ground literals assigned in DPLL($\mathcal{T}$)
- If Γ infers C from $C_1, \ldots, C_m, L_{m+1}, \ldots, L_k$,
  infer $H \rhd C$ from $H_1 \rhd C_1, \ldots, H_m \rhd C_m, L_{m+1}, \ldots, L_k$,
  where $H = H_1 \cup \ldots H_m \cup \{L_{m+1}, \ldots, L_k\}$
- $H \rhd C$ means $\neg H \vee C$: hypotheses are carried along
- Discharged if Γ generates $H \rhd \Box$: conflict clause $\neg H$
- DPLL($\Gamma+\mathcal{T}$)-refutation: DPLL($\mathcal{T}$)-refutation + Γ-subproof

Interpolation system for DPLL($\Gamma+\mathcal{T}$)

Add one case to interpolation system for DPLL($\mathcal{T}$):

- Hypothetical clause $H \rhd C$ inferred by Γ from $H_1 \rhd C_1, \ldots, H_m \rhd C_m$ and $L_{m+1}, \ldots, L_k$:
  partial interpolant produced by interpolation system for Γ for Γ-inference inferring C from $C_1, \ldots, C_m, L_{m+1}, \ldots, L_k$

Completeness follows from that of the interpolation systems for Γ and DPLL($\mathcal{T}$)

Current work: beyond ground problems

- Substitutions: L global but $L\sigma$ not necessarily
- Separating ordering not enough to avoid AB-mixed literals
- Introduction of quantifiers: $\exists$ for A-local terms and $\forall$ for B-local terms
- Provisional partial interpolants + introduction of quantifiers

Summary of contributions

- Unified framework of definitions for interpolation
- Survey of interpolation systems for DPLL, equality sharing and DPLL($\mathcal{T}$), *reconstructing proofs* and including *model based theory combination*
- Interpolation and equality: connecting *equality-interpolating theory* and *separating ordering*
- A first *complete* interpolation system for *ground* Γ-refutations
- Interpolation system for general Γ-refutations: in progress
- Putting all together: interpolation system for DPLL($\Gamma+\mathcal{T}$)

Acknowledgements

- Joint work with Moa Johansson
- Building on work by (in reverse chronological order):
  - Georg Weissenbacher
  - Vijay D'Silva
  - Madan Musuvathi
  - Greta Yorsh
  - Ken McMillan
  - ... ...

Thank you!