Effectively Propositional Interpolants

Samuel Drews and Aws Albarghouthi

WISCONSIN UNIVERSITY OF WISCONSIN–MADISON

Effectively Propositional Logic (EPR)

$$\exists x_1 \ldots x_n \, \forall y_1 \ldots y_m \; \varphi$$

Quantifier-free
No function symbols

- Decidable satisfiability
- Expressive; can encode linked lists

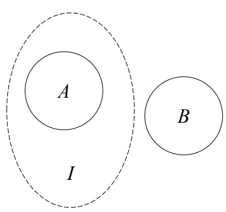
Interpolants

Given A and B such that

$A \wedge B$ is unsatisfiable

Find I such that

$A \rightarrow I$ is valid
$I \wedge B$ is unsatisfiable
I is in shared vocabulary (A, B)



Restricted Logics for Invariants

$I(\vec{x}) \wedge T(\vec{x}, \vec{x}') \rightarrow I(\vec{x}')$
is valid, or

$I(\vec{x}) \wedge T(\vec{x}, \vec{x}') \wedge \neg I(\vec{x}')$
is unsat

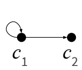
$\exists^* \forall^* \varphi$ decidable, but
$\forall^* \exists^* \varphi$ undecidable

- $\exists$-logic: $\exists^* \varphi$
- $\forall$-logic: $\forall^* \varphi$
- AF-logic: boolean combinations of $\exists$-logic and $\forall$-logic formulae

Models and Diagrams

$$\varphi = \exists a \forall b.\, p(a, b)$$

Model $m \models \varphi$

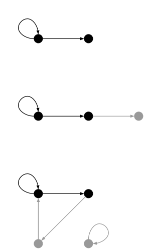


Diagram

$$diag(m) = \exists c_1, c_2 . c_1 \neq c_2 \\ \wedge\, p(c_1, c_1) \wedge \neg p(c_2, c_2) \\ \wedge\, p(c_1, c_2) \wedge \neg p(c_2, c_1)$$

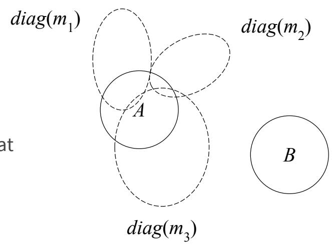
Models and Diagrams

$$diag(m) = \exists c_1, c_2 . c_1 \neq c_2 \\ \wedge\, p(c_1, c_1) \wedge \neg p(c_2, c_2) \\ \wedge\, p(c_1, c_2) \wedge \neg p(c_2, c_1)$$



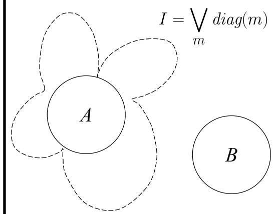
UITP: for ∃-logic

$I \leftarrow False$
while $A \wedge \neg I$ is sat
  $m \models A \wedge \neg I$
  if $diag(m) \wedge B$ is sat
    return *none*
  $I \leftarrow I \vee diag(m)$
return I

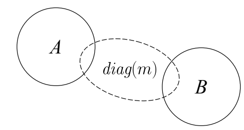


UITP: for ∃-logic

$I = \bigvee_m diag(m)$

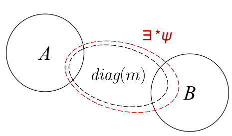


No ∃-logic interpolant



UITP Soundness

- Returning I : interpolant by construction
- Returning *none* is sound:
  $diag(m)$ is the strongest ∃-logic formula m models



UITP Termination (and Completeness)

EPR small model property:
  All EPR A have a bound k such that
  $m \models A \;\rightarrow\; \exists m'.\; m' \models A \;\wedge\; m' \subseteq m \;\wedge\; |m'| \leq k$

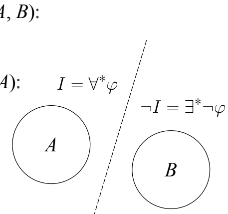
  So $m \models diag(m')$

$$A \rightarrow \bigvee_{m \models A : |m| \leq k} diag(m)$$

UITP: for ∀-logic

Suppose I is a ∀-logic interpolant for (A, B):
  $A \wedge \neg I$ unsat, $I \wedge B$ unsat

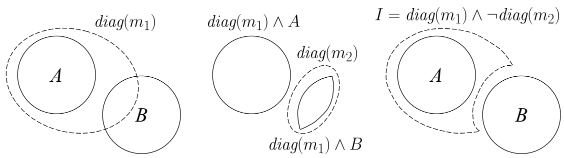
Then $\neg I$ is a ∃-logic interpolant for (B, A):
  $B \wedge \neg\neg I$ unsat, $\neg I \wedge A$ unsat



BITP: for AF-logic

UITP(A, B):	BITP(A, B):
$I \leftarrow False$	$I \leftarrow False$
while $A \wedge \neg I$ is sat	while $A \wedge \neg I$ is sat
$m \models A \wedge \neg I$	$m \models A \wedge \neg I$, $d \leftarrow diag(m)$
if $diag(m) \wedge B$ is sat	if $d \wedge B$ is sat
return *none*	$d \leftarrow d \wedge \neg \mathrm{BITP}(B \wedge d, A \wedge d)$
$I \leftarrow I \vee diag(m)$	$I \leftarrow I \vee d$
return I	return I

BITP: for AF-logic

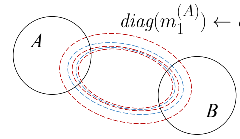


BITP Soundness and Relative Completeness

Soundness: returned I is interpolant by construction

Rel. Compl.: Existence of AF-logic interpolant → termination

$$diag(m_1^{(A)}) \leftarrow diag(m_2^{(B)}) \leftarrow diag(m_3^{(A)}) \ldots$$



$$\varphi \in \text{AF-logic}$$
$$m_i^{(A)}, m_{i+2}^{(A)} \models \varphi$$
$$\rightarrow m_{i+1}^{(B)} \models \varphi$$

Experiments

Implemented simple interpolation-based verifier, ITPV

Compared ITPV to $\text{PDR}_\forall$ on 18 benchmarks
  Average time: $\text{PDR}_\forall$ 3.9s, ITPV 8.9s

ITPV succeeded on benchmarks modified to require AF-logic

Questions?