Interpolant Strength

V. D'Silva, D. Kroening, M. Purandare, G. Weissenbacher

University of Oxford and ETH Zurich

VMCAI, Madrid, 18th of January, 2010

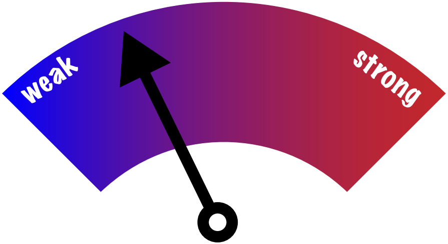
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Verification with Model Checking And Interpolation

- Craig-interpolation commonly applied in model checking
  - used to compute approximate images
- Strongest interpolant not necessarily the best one
  - Coarse approximations can lead to faster convergence
- Range of interpolants exists
  - but existing interpolation systems can only generate one

Outline

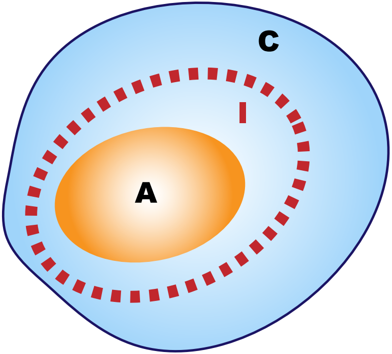
- Background
  - What is a Craig interpolant?
  - Interpolant-based model checking
  - Interpolation for propositional logic
- A novel, more general interpolation system
- Interpolant strength



What is a Craig interpolant?

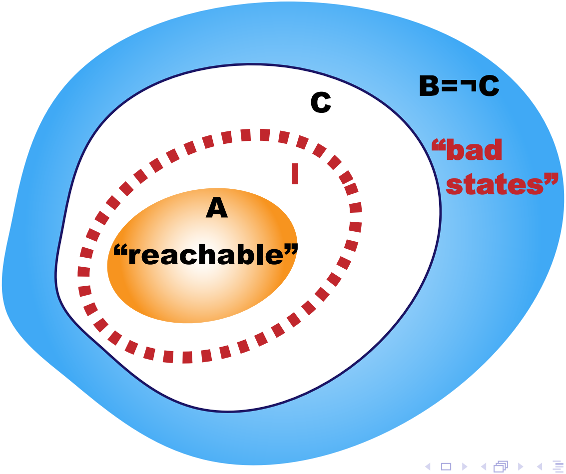
"Traditional" definition [William Craig, 57]:

- $A \Rightarrow I \Rightarrow C$
- all non-logical symbols in I occur in A *as well as* in C

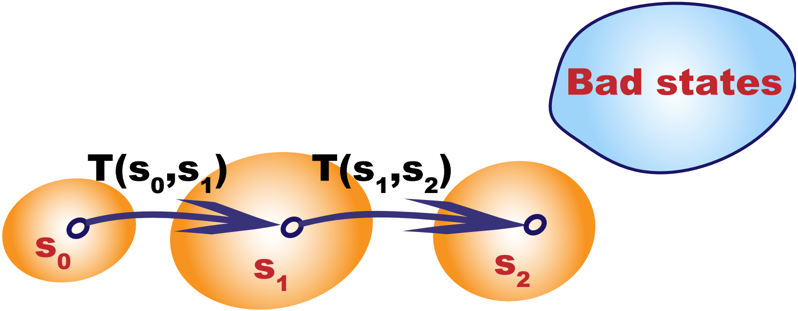


Common definition for automated verification:

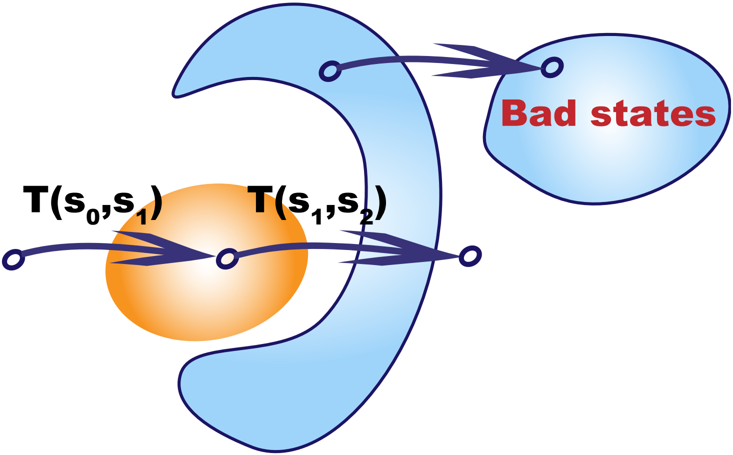
- $A \Rightarrow I$ and $I \wedge B$ inconsistent
- all non-logical symbols in I occur in A *as well as* in B

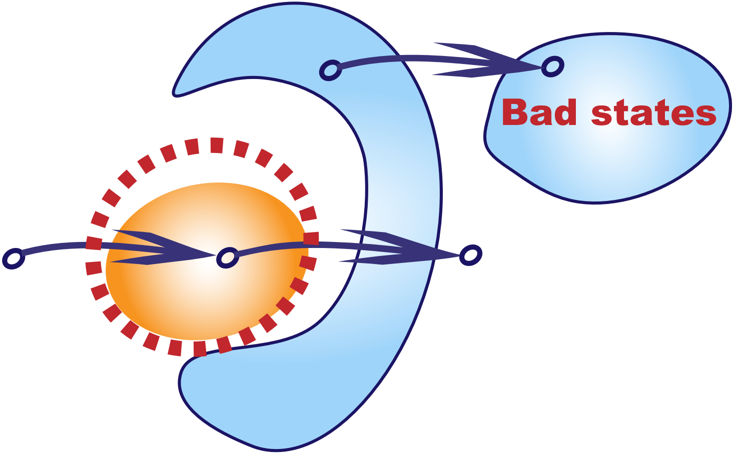


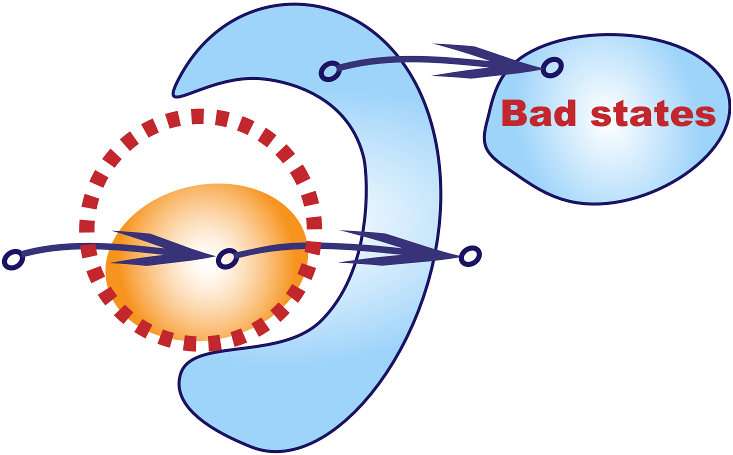
Bounded Model Checking

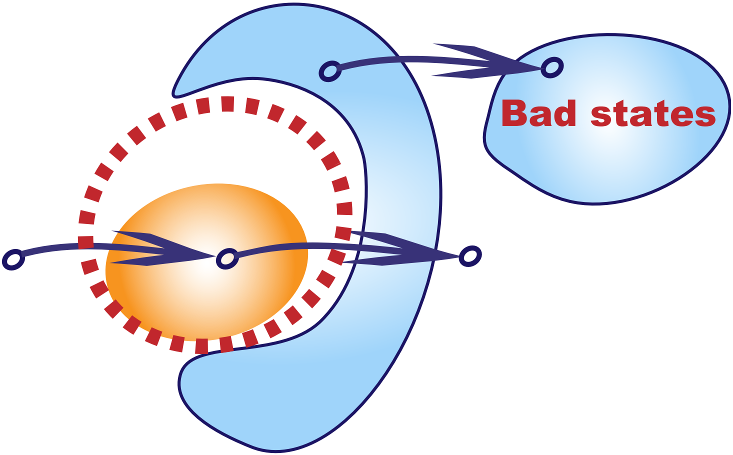


Interpolant-based Model Checking

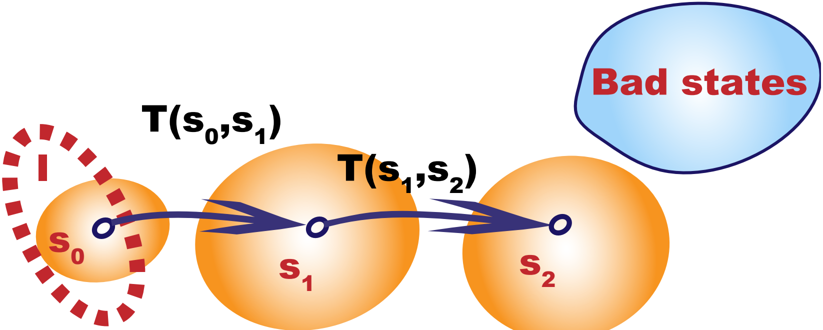



Bad states


Bad states


Bad states

Interpolant-based Model Checking: Iteration



- $x_0 = 0$
- $T(x_i, x_{i+1}) \equiv (x_{i+1} := x_i + 2)$
- Property: $x \neq 7$

$s_0 \cup I$	Strongest	Intermediate Interpolant	Weakest
$\{0\}$	$x_i = 2$	$x_i\%2 = 0$	$(x_i + 2) \neq 7$
$\{0, 2\}$	$x_i \in \{2, 4\}$	$x_i\%2 = 0$	$\ldots$
$\{0, 2, 4\}$	$x_i \in \{2, 4, 6\}$	$x_i\%2 = 0$	$\ldots$
$\{0, 2, 4, \ldots\}$	$x_i \in \{2, 4, 6, \ldots\}$	$x_i\%2 = 0$	$\ldots$

- Strongest interpolant delays convergence
- Weakest interpolant results in spurious counterexample

- CNF formula: A conjunction of clauses

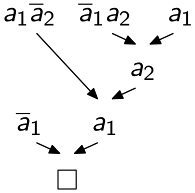
$$\bigwedge_i \bigvee_j \ell_{i,j}\,, \qquad \ell_{i,j} \in \{a, \overline{a} \mid a \in \text{Variables}\}$$

e.g.,

$$\overline{a}_1 \wedge (a_1 \vee \overline{a}_2) \wedge (\overline{a}_1 \vee a_2) \wedge a_1$$

- Resolution proofs

$$\frac{(C \vee a) \qquad (D \vee \overline{a})}{C \vee D} \quad \text{[Res]}$$



Resolution for CNF Formulas

- CNF formula: A conjunction of clauses

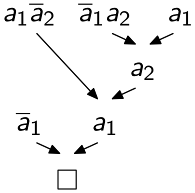
$$\bigwedge_i \bigvee_j \ell_{i,j}\,, \qquad \ell_{i,j} \in \{a, \overline{a} \mid a \in \text{Variables}\}$$

e.g.,

$$\overline{a}_1 \wedge (a_1 \vee \overline{a}_2) \wedge (\overline{a}_1 \vee a_2) \wedge a_1$$

- Resolution proofs

$$\frac{(C \vee a) \qquad (D \vee \overline{a})}{C \vee D} \quad [\text{Res}]$$

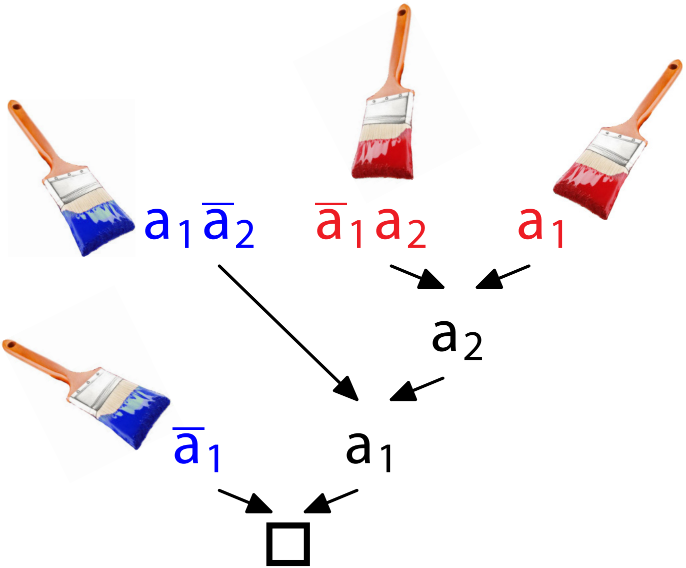


- Naturally generated by modern SAT solvers

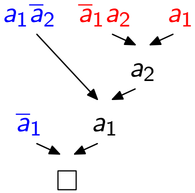
Colouring Formulas

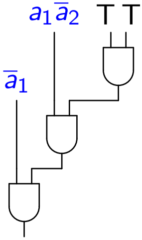
$A \equiv \overline{a}_1 \wedge (a_1 \vee \overline{a}_2)$ $B \equiv (\overline{a}_1 \vee a_2) \wedge a_1$

Interpolants from Resolution Proofs



- Interpolant I is a circuit following the structure of the proof
- In our example, I is
  - T if input values make $\overline{a}_1 \wedge (a_1 \vee \overline{a}_2)$ true
  - F if input values make $(\overline{a}_1 \vee a_2) \wedge a_1$ true





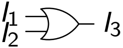
McMillan's Interpolation System

Annotate each clause C in the proof with a *partial interpolant* I

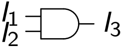
- Base case (initial clause C):
  -  $I =$ "keep all literals $\ell \in C$ s.t. $\mathrm{var}(\ell) \in \mathrm{Var}(B)$"
  -  $I = \mathrm{T}$
- Induction step (internal clauses C_1, C_2):

$$\frac{C_1 \vee a \quad [I_1] \qquad C_2 \vee \overline{a} \quad [I_2]}{C_1 \vee C_2 \quad [I_3]}$$

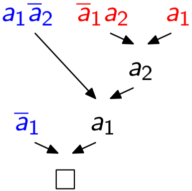
if $a \notin \mathrm{Var}(B)$, $\quad I_3 \stackrel{\text{def}}{=} I_1 \vee I_2$

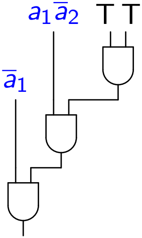


if $a \in \mathrm{Var}(B)$, $\quad I_3 \stackrel{\text{def}}{=} I_1 \wedge I_2$



Interpolants from Proofs: Example Revisited





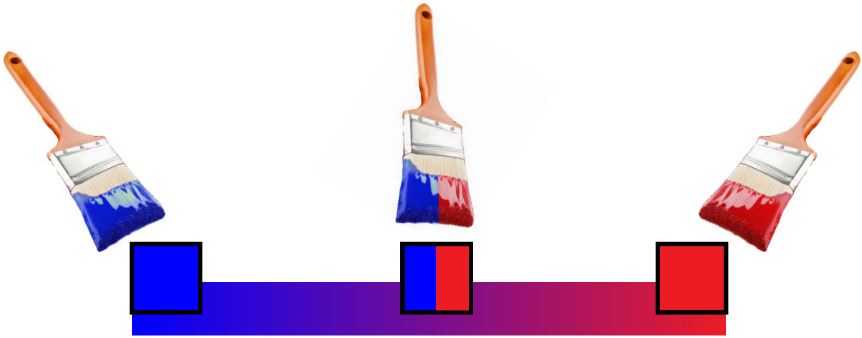
- I is $(\overline{a}_1 \wedge \overline{a_2})$, the strongest possible interpolant
- All interpolants form a lattice.

$$\overline{a}_1 \vee \overline{a}_2$$

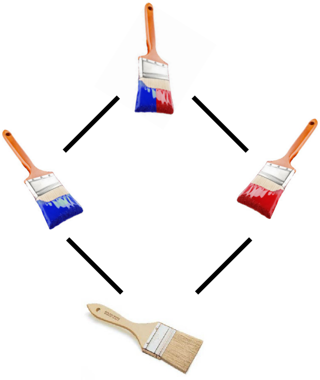
$$\overline{a}_1 \qquad\qquad \overline{a}_2$$

$$\overline{a}_1 \wedge \overline{a}_2$$

- Existing interpolation systems unnecessarily restrict *artistic freedom*



Lattice of Colours, Join

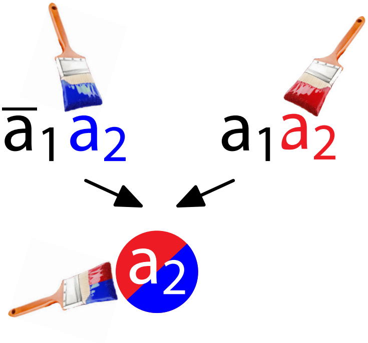


(colour lattice)

Locality Preserving Colouring

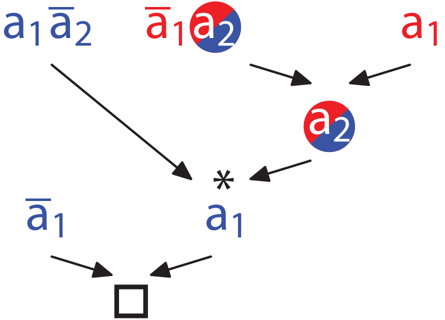
Each literal ℓ in each clause coloured separately!

- Literals from $A \setminus B$ must be coloured 
- Literals from $B \setminus A$ must be coloured 
- Literals from A and B: Any colour $\in$ {  ,  ,  }



$\bar{a}_1 a_2$
$a_1 a_2$
a_2

Example: Coloured Proof



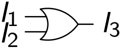
- $L(\overline{a}_2, u) \sqcup L(a_2, v) =$ 

Labelled Interpolation System

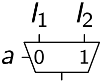
- Base case (initial vertices):
  - If $C \in$ A: $I \stackrel{\text{def}}{=}$ “all literals $\ell \in C$ s.t. $L(\ell, v) =$  ”
  - If $C \in$ B: $I \stackrel{\text{def}}{=} \neg($ “all literals $\ell \in C$ s.t. $L(\ell, v) =$  ”)
- Induction step (internal vertices):

$$\frac{C_1 \vee a \quad [I_1] \qquad C_2 \vee \bar{a} \quad [I_2]}{C_1 \vee C_2 \quad [I_3]}$$

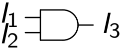
if $L(a) \sqcup L(\bar{a}) =$  $I_3 \stackrel{\text{def}}{=} I_1 \vee I_2$



if $L(a) \sqcup L(\bar{a}) =$  $I_3 \stackrel{\text{def}}{=} (a \vee I_1) \wedge (I_2 \vee \bar{a})$



if $L(a) \sqcup L(\bar{a}) =$  $I_3 \stackrel{\text{def}}{=} I_1 \wedge I_2$



Theorem. *For any* (A, B)*-refutation* R *and locality preserving colouring* L*,* $\text{ITP}(L, R)$ *is an interpolant for* (A, B)*.*

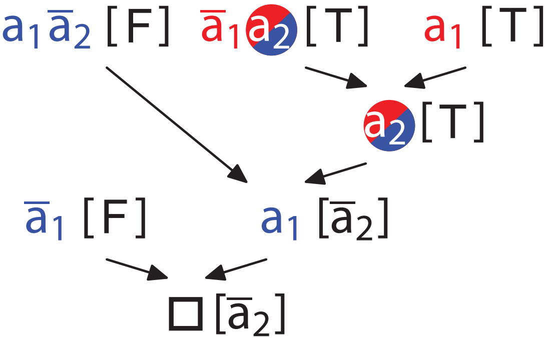
Proof: Minor adaptation of [Yorsh and Musuvathi, CADE '05]:

Invariant:

$$A \wedge (\neg C|_A) \vdash I$$

$$B \wedge (\neg C|_B) \vdash \neg I$$

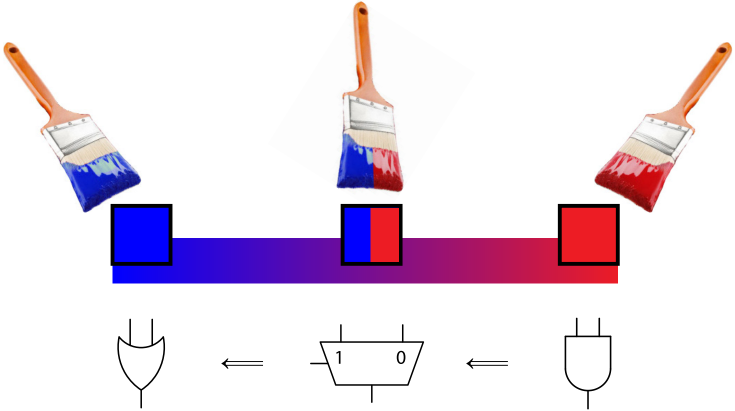
$$\mathrm{Var}(I) \subseteq \mathrm{Var}(A) \cap \mathrm{Var}(B)$$



- Interpolant $\overline{a_2}$ cannot be obtained with existing systems!
- Also, $\overline{a_2}$ is implied by $\overline{a}_1 \wedge \overline{a}_2$.

Strength of Interpolants

$$I_1 \vee I_2 \Longleftarrow (a \vee I_1) \wedge (I_2 \vee \overline{a}) \Longleftarrow I_1 \wedge I_2$$



Theorem: Strength of Interpolants

- min and max for colours
- Lift $\Leftarrow$, min and max pointwise to colouring functions

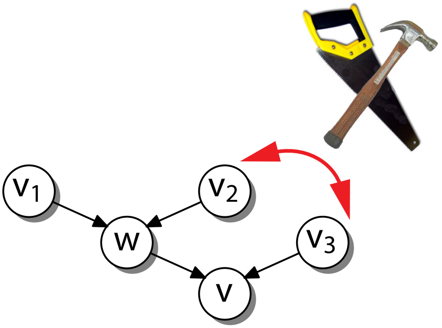
Theorem. *Let R be an* (A, B)*-refutation and* $\mathbb{L}_R$ *be the set of locality preserving colourings over R. The structure* $(\mathbb{L}_R, \Leftarrow, \max, \min)$ *is a complete lattice.*

Strength of Interpolants (continued)

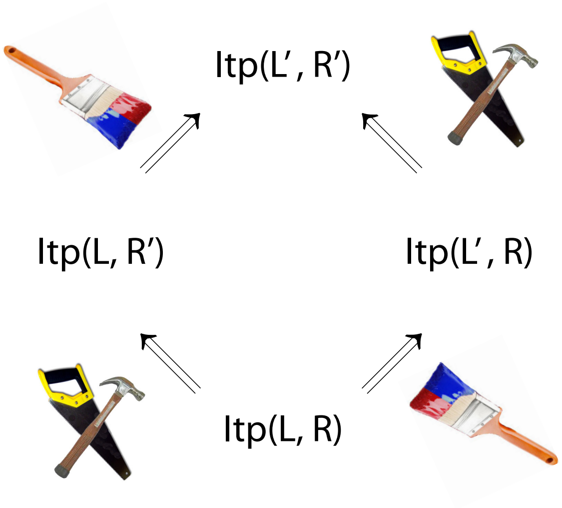
	A-local	*A*/*B*-shared	*B*-local	
strongest				(McMillan)
		 . . . 		
⇓				(Huang, Krajíček, Pudlák)
		 . . . 		
weakest				(“inverse” McMillan)

Restructuring Proofs

- Change strength of interpolant by swapping nodes in proof
- Informally introduced in [Jhala and McMillan, LMCS 07]



- Labelling and restructuring are orthogonal techniques!



- Labelled interpolation systems
  - generalise existing interpolation systems for propositional logic
  - constitute a dial for tuning interpolant strength
- All proofs available in ETH Technical Report 652
- Vijay D'Silva, ESOP 2010:

  Propositional Interpolation and
  Abstract Interpretation

  - Interpolation systems, clauses and interpolants form abstract domains.
  - Existing systems as optimal abstractions of the colouring system.
- Future work
  - Empirical analysis of effect of interpolant strength