Interpolant Strength Revisited

Georg Weissenbacher

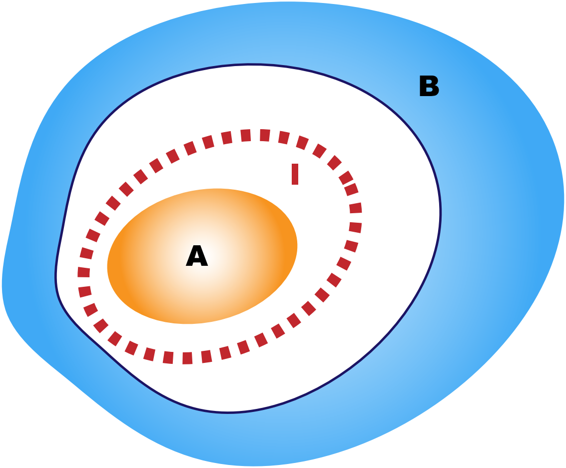
SAT'12, Trento

TECHNISCHE UNIVERSITÄT WIEN
Vienna University of Technology

What is a Craig Interpolant?

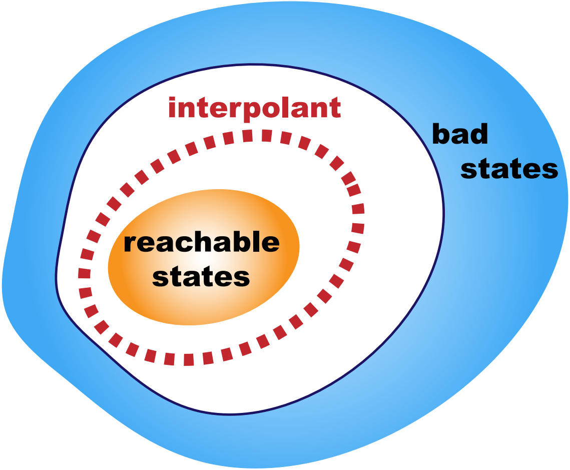
Craig-Robinson interpolant for inconsistent (first-order) conjunction $A \wedge B$:

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



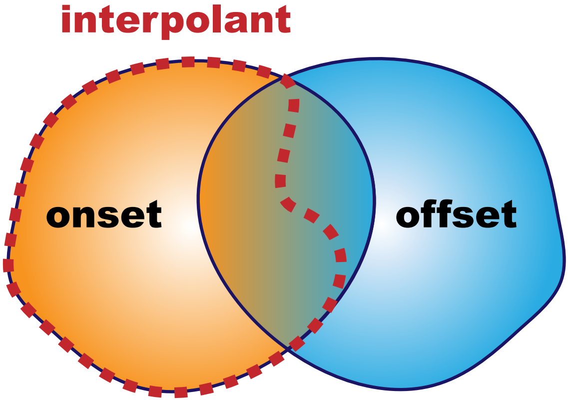
Interpolants in Verification (e.g. McMillan CAV'03)

- approximate image computation
- Interpolant *separates* "good states" from "bad states"



Interpolants in Synthesis (Jiang, Lin, Hung ICCAD'09)

- Given: circuit specification R : Inputs $\times$ Output $\rightarrow \mathbb{B}$
- Wanted: functional implementation I : Inputs $\rightarrow \mathbb{B}$
- Interpolant *separates* "onset" from "offset"



Existing Propositional Interpolation Techniques

- Extract interpolants from resolution proofs
- One interpolant per proof:
  - Proof determines resulting interpolant

proof $\rightarrow$  $\rightarrow$ interpolant

- Do not allow for variation of resulting interpolant!

Outline

- Background
  - Pudlák's Interpolation System
- Interpolation for Propositional Hyper-Resolution Proofs
  - Novel Interpolation Rules (enable *Variation*)
  - "Merge-Free" Resolution Chains
- Labelled Interpolation and Hyper-Resolution
- First-Order Logic Derivations and Interpolation for Hyper-Resolution

Resolution for CNF Formulas

- CNF formula: A conjunction of clauses

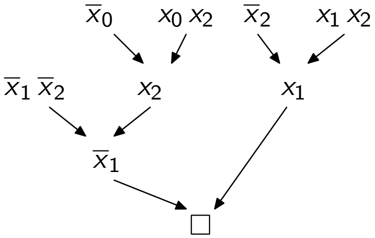
$$\bigwedge_i \bigvee_j \ell_{i,j}\,, \qquad \ell_{i,j} \in \{x, \overline{x} \mid x \in \text{Variables}\}$$

e.g.,

$$(\overline{x}_1 \vee \overline{x}_2) \wedge \overline{x}_0 \wedge (x_0 \vee x_2) \wedge \overline{x}_2 \wedge (x_1 \vee x_2)$$

- Resolution proofs

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



Interpolants as Separators (Pudlák JSL'97)

$$\underbrace{(\overline{x}_1 \vee \overline{x}_2) \wedge \overline{x}_0 \wedge (x_0 \vee x_2)}_{A} \quad \wedge \quad \underbrace{\overline{x}_2 \wedge (x_1 \vee x_2)}_{B}$$

$$\underbrace{(\overline{x}_1 \vee \overline{x}_2) \wedge \overline{x}_0 \wedge (x_0 \vee x_2)}_{A} \quad \wedge \quad \underbrace{\overline{x}_2 \wedge (x_1 \vee x_2)}_{B}$$

Interpolants as Separators (Pudlák JSL'97)

$$\underbrace{(\overline{x}_1 \vee \overline{x}_2) \wedge \overline{x}_0 \wedge (x_0 \vee x_2)}_{A} \quad \wedge \quad \underbrace{\overline{x}_2 \wedge (x_1 \vee x_2)}_{B}$$

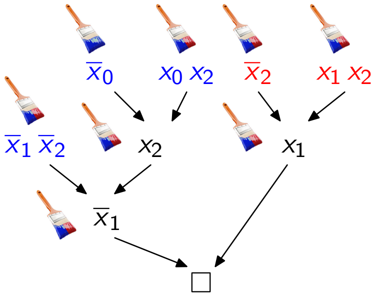
$$A \Rightarrow \overline{x}_1 \qquad B \Rightarrow x_1 \qquad x_1 \in \mathrm{Var}(A) \cap \mathrm{Var}(B)$$

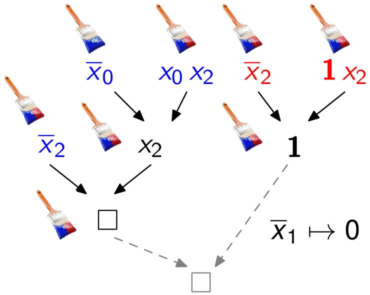
$$\underbrace{(\overline{x}_1 \vee \overline{x}_2) \wedge \overline{x}_0 \wedge (x_0 \vee x_2)}_{A} \quad \wedge \quad \underbrace{\overline{x}_2 \wedge (x_1 \vee x_2)}_{B}$$

$$A \Rightarrow \overline{x}_1 \qquad B \Rightarrow x_1 \qquad x_1 \in \mathrm{Var}(A) \cap \mathrm{Var}(B)$$

I is *false*	$(\overline{x}_1 \mapsto 0)$	$\longrightarrow$	$(A \wedge I)$	unsatisfiable
I is *true*	$(\overline{x}_1 \mapsto 1)$	$\longrightarrow$	$(B \wedge \neg I)$	unsatisfiable

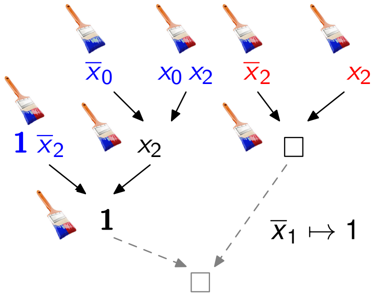
Interpolants *separate* Resolution Proofs (Pudlák JSL'97)



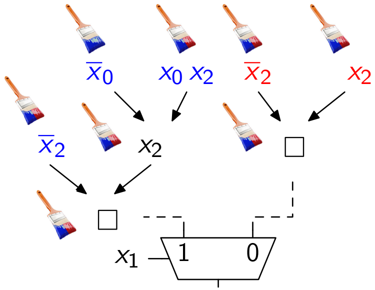


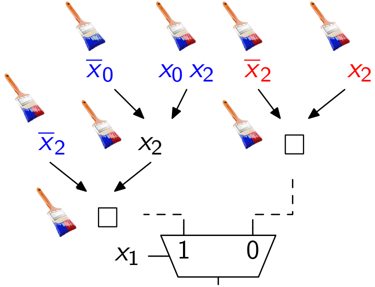
$\overline{x}_0$
$x_0\ x_2$
$\overline{x}_2$
1 x_2
$\overline{x}_2$
x_2
1
□
$\overline{x}_1 \mapsto 0$
□

Interpolants *separate* Resolution Proofs (Pudlák JSL'97)



Interpolants *separate* Resolution Proofs (Pudlák JSL'97)

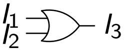


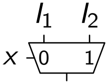


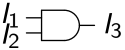
- Annotate *each clause C* in proof with *partial interpolant* I_C
  - $A \wedge \neg I_C \Rightarrow C \setminus \{\ell \in C \mid \ell$ is $\}$
  - $B \wedge \quad I_C \Rightarrow C \setminus \{\ell \in C \mid \ell$ is $\}$
  - $\mathrm{Var}(I_C) \subseteq \mathrm{Var}(A) \cap \mathrm{Var}(B)$

- Base case (initial vertices):
  - If $C \in A$: $I \stackrel{\text{def}}{=} 0$
  - If $C \in B$: $I \stackrel{\text{def}}{=} 1$
- Induction step (internal vertices):

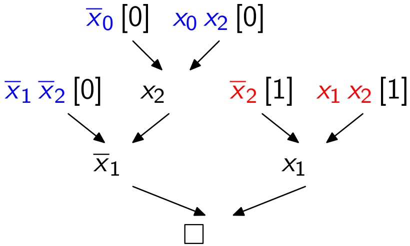
$$\frac{C_1 \vee x \quad [I_1] \qquad C_2 \vee \overline{x} \quad [I_2]}{C_1 \vee C_2 \quad [I_3]}$$

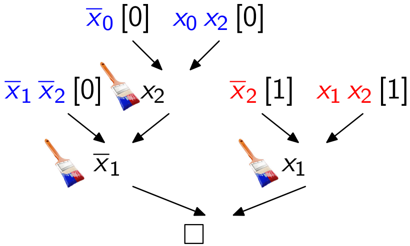
if x is  $I_3 \stackrel{\text{def}}{=} I_1 \vee I_2$ 

if x is  $I_3 \stackrel{\text{def}}{=} (x \vee I_1) \wedge (I_2 \vee \overline{x})$ 

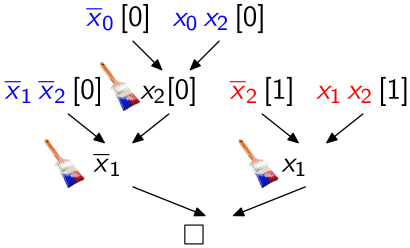
if x is  $I_3 \stackrel{\text{def}}{=} I_1 \wedge I_2$ 

Pudlák's Interpolation System (Pudlák JSL'97)

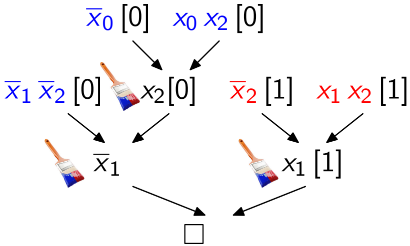




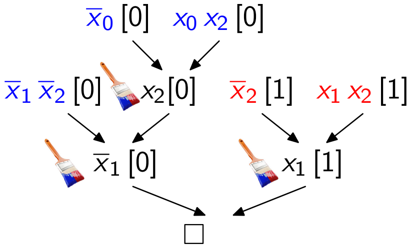
$\overline{x}_0$ [0]
$x_0\ x_2$ [0]
$\overline{x}_1\ \overline{x}_2$ [0]
x_2
$\overline{x}_2$ [1]
$x_1\ x_2$ [1]
$\overline{x}_1$
x_1
$\square$


$\overline{x}_0$ [0]
$x_0\ x_2$ [0]
$\overline{x}_1\ \overline{x}_2$ [0]
x_2[0]
$\overline{x}_2$ [1]
$x_1\ x_2$ [1]
$\overline{x}_1$
x_1
$\square$

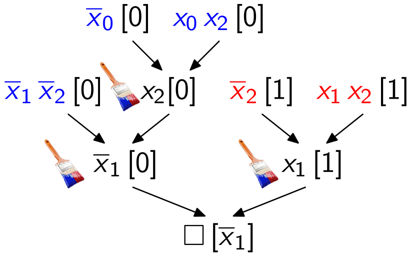
- $0 \vee 0 = 0$



- $0 \vee 0 = 0$
- $(x_2 \vee 1) \wedge (\overline{x}_2 \vee 1) = 1$



- $0 \vee 0 = 0$
- $(x_2 \vee 1) \wedge (\overline{x}_2 \vee 1) = 1$
- $(x_2 \vee 0) \wedge (\overline{x}_2 \vee 0) = 0$

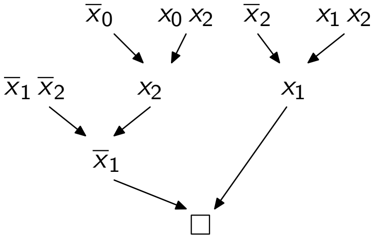


- $0 \vee 0 = 0$
- $(x_2 \vee 1) \wedge (\overline{x}_2 \vee 1) = 1$
- $(x_2 \vee 0) \wedge (\overline{x}_2 \vee 0) = 0$
- $\underline{(x_1 \vee 1) \wedge (\overline{x}_1 \vee 0) = \overline{x}_1}$

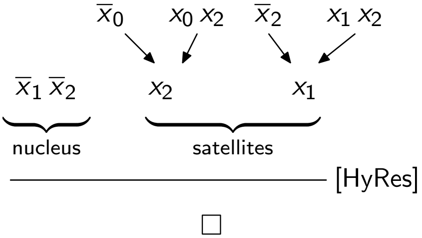
Outline

- Background
  - Pudlák's Interpolation System
- **Interpolation for Propositional Hyper-Resolution Proofs**
  - Novel Interpolation Rules (enable *Variation*)
  - "Merge-Free" Resolution Chains
- Labelled Interpolation and Hyper-Resolution
- First-Order Logic Derivations and Interpolation for Hyper-Resolution

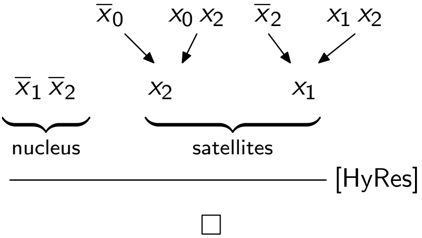
Hyper-Resolution (Robinson JACM'65)



Hyper-Resolution (Robinson JACM'65)

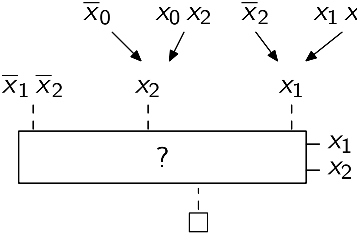


Hyper-Resolution (Robinson JACM'65)



$$\frac{\overbrace{(C_1 \vee x_1) \quad \cdots \quad (C_n \vee x_n)}^{\text{satellites}} \qquad \overbrace{(\overline{x}_1 \vee \cdots \vee \overline{x}_n \vee D)}^{\text{nucleus}}}{\bigvee_{i=1}^{n} C_i \vee D} \quad \text{[HyRes]}$$

- condensation of a derivation consisting of several resolutions



$$\frac{\overbrace{(C_1 \vee x_1) \quad \cdots \quad (C_n \vee x_n)}^{\text{satellites}} \qquad \overbrace{(\overline{x}_1 \vee \cdots \vee \overline{x}_n \vee D)}^{\text{nucleus}}}{\bigvee_{i=1}^{n} C_i \vee D} \text{ [HyRes]}$$

- condensation of a derivation consisting of several resolutions

Interpolation for Hyper-Resolution Steps

$$\frac{(C_1 \vee x_1) \quad [I_1] \quad \cdots \quad (C_n \vee x_n) \quad [I_n] \qquad (\overline{x}_1 \vee \cdots \vee \overline{x}_n \vee D) \quad [I_{n+1}]}{\bigvee_{i=1}^{n} C_i \vee D \quad [I]}$$

if $x_1, \ldots, x_n$ are  $\quad I \stackrel{\text{def}}{=} \bigwedge_{i=1}^{n} (x_i \vee I_i) \wedge \left(I_{n+1} \vee \bigvee_{i=1}^{n} \overline{x}_i\right)$

$$\frac{(C_1 \vee x_1) \quad [I_1] \quad \cdots \quad (C_n \vee x_n) \quad [I_n] \qquad (\overline{x}_1 \vee \cdots \vee \overline{x}_n \vee D) \quad [I_{n+1}]}{\bigvee_{i=1}^{n} C_i \vee D \quad [I]}$$

if $x_1, \ldots, x_n$ are  $\quad I \stackrel{\text{def}}{=} \bigvee_{i=1}^{n+1} I_i$

if $x_1, \ldots, x_n$ are  $\quad I \stackrel{\text{def}}{=} \bigwedge_{i=1}^{n}(x_i \vee I_i) \wedge \left(I_{n+1} \vee \bigvee_{i=1}^{n} \overline{x}_i\right)$

if $x_1, \ldots, x_n$ are  $\quad I \stackrel{\text{def}}{=} \bigwedge_{i=1}^{n+1} I_i$

$$\frac{(C_1 \vee x_1) \quad [I_1] \quad \cdots \quad (C_n \vee x_n) \quad [I_n] \qquad (\overline{x}_1 \vee \cdots \vee \overline{x}_n \vee D) \quad [I_{n+1}]}{\bigvee_{i=1}^{n} C_i \vee D \quad [I]}$$

if $x_1, \ldots, x_n$ are  $I \stackrel{\text{def}}{=} \bigvee_{i=1}^{n+1} I_i$

if $x_1, \ldots, x_n$ are  $I \stackrel{\text{def}}{=} \bigwedge_{i=1}^{n}(x_i \vee I_i) \wedge \left(I_{n+1} \vee \bigvee_{i=1}^{n} \overline{x}_i\right)$

if $x_1, \ldots, x_n$ are  $I \stackrel{\text{def}}{=} \bigwedge_{i=1}^{n+1} I_i$

not total!

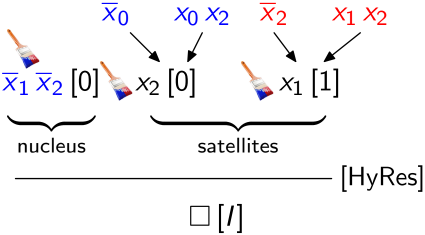
Interpolation for Hyper-Resolution: Example Revisited

$\overline{x}_0$ $\quad x_0\, x_2$ $\quad \overline{x}_2$ $\quad x_1\, x_2$

$$\underbrace{\overline{x}_1\, \overline{x}_2\ [0]}_{\text{nucleus}}\quad \underbrace{x_2\ [0] \qquad x_1\ [1]}_{\text{satellites}}$$

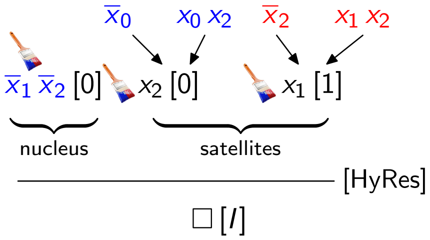
$$\frac{\qquad\qquad\qquad\qquad}{\square\ [I]}\ [\text{HyRes}]$$

if $x_1, \ldots, x_n$ are $\quad I \stackrel{\text{def}}{=} \bigwedge_{i=1}^{n}(x_i \vee I_i) \wedge \left(I_{n+1} \vee \bigvee_{i=1}^{n} \overline{x}_i\right)$



if $x_1, \ldots, x_n$ are  $\quad I \stackrel{\text{def}}{=} \bigwedge_{i=1}^{n}(x_i \vee I_i) \wedge \left(I_{n+1} \vee \bigvee_{i=1}^{n} \overline{x}_i\right)$

- $I \stackrel{\text{def}}{=} (x_1 \vee 1) \wedge (x_2 \vee 0) \wedge (\overline{x}_1 \vee \overline{x}_2 \vee 0) \quad \equiv \quad \underline{x_2 \wedge (\overline{x}_1 \vee \overline{x}_2)}$



if $x_1, \ldots, x_n$ are $\quad I \stackrel{\text{def}}{=} \bigwedge_{i=1}^{n}(x_i \vee I_i) \wedge \left(I_{n+1} \vee \bigvee_{i=1}^{n} \overline{x}_i\right)$

- $I \stackrel{\text{def}}{=} (x_1 \vee 1) \wedge (x_2 \vee 0) \wedge (\overline{x}_1 \vee \overline{x}_2 \vee 0) \quad \equiv \quad \underline{x_2 \wedge (\overline{x}_1 \vee \overline{x}_2)}$
- *I implies* $\overline{x}_1$ but is *not equivalent* (try $x_1 = x_2 = 0$)

Interpolation for Hyper-Resolution Steps

$$\frac{(C_1 \vee x_1) \quad [I_1] \quad \cdots \quad (C_n \vee x_n) \quad [I_n] \qquad (\overline{x}_1 \vee \cdots \vee \overline{x}_n \vee D) \quad [I_{n+1}]}{\bigvee_{i=1}^{n} C_i \vee D \quad [I]}$$

if $x_1, \ldots, x_n$ are  $I \stackrel{\text{def}}{=} \begin{cases} \bigwedge_{i=1}^{n}(x_i \vee I_i) \wedge \left(I_{n+1} \vee \bigvee_{i=1}^{n} \overline{x}_i\right) \\ \textit{or} \\ \bigvee_{i=1}^{n}(\overline{x}_i \wedge I_i) \vee \left(I_{n+1} \wedge \bigwedge_{i=1}^{n} x_i\right) \end{cases}$

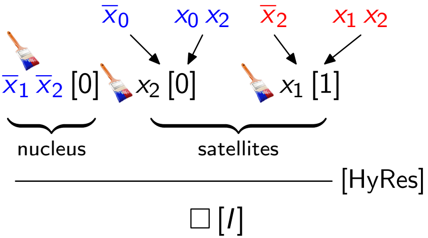
$$\frac{(C_1 \vee x_1) \quad [I_1] \quad \cdots \quad (C_n \vee x_n) \quad [I_n] \qquad (\overline{x}_1 \vee \cdots \vee \overline{x}_n \vee D) \quad [I_{n+1}]}{\bigvee_{i=1}^{n} C_i \vee D \quad [I]}$$

if $x_1, \ldots, x_n$ are  $I \stackrel{\text{def}}{=} \bigvee_{i=1}^{n+1} I_i$

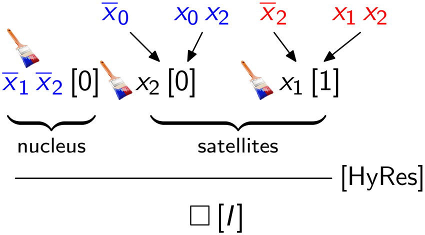
if $x_1, \ldots, x_n$ are  $I \stackrel{\text{def}}{=} \begin{cases} \bigwedge_{i=1}^{n}(x_i \vee I_i) \wedge \left(I_{n+1} \vee \bigvee_{i=1}^{n} \overline{x}_i\right) \\ \textit{or} \\ \bigvee_{i=1}^{n}(\overline{x}_i \wedge I_i) \vee \left(I_{n+1} \wedge \bigwedge_{i=1}^{n} x_i\right) \end{cases}$

if $x_1, \ldots, x_n$ are  $I \stackrel{\text{def}}{=} \bigwedge_{i=1}^{n+1} I_i$

Interpolation for Hyper-Resolution: Example Revisited (Again)



if $x_1, \ldots, x_n$ are $\quad I \stackrel{\text{def}}{=} \bigvee_{i=1}^{n} (\overline{x}_i \wedge I_i) \vee \left(I_{n+1} \wedge \bigwedge_{i=1}^{n} x_i\right)$



if $x_1, \ldots, x_n$ are $\quad I \stackrel{\text{def}}{=} \bigvee_{i=1}^{n}(\overline{x}_i \wedge I_i) \vee \left(I_{n+1} \wedge \bigwedge_{i=1}^{n} x_i\right)$

- $I \stackrel{\text{def}}{=} (\overline{x}_1 \wedge 1) \vee (\overline{x}_2 \wedge 0) \wedge (x_1 \wedge x_2 \wedge 0) \quad \equiv \quad \overline{x}_1$

- Base case (initial vertices):
  - If $C \in A$: $I \stackrel{\text{def}}{=} 0$
  - If $C \in B$: $I \stackrel{\text{def}}{=} 1$
- Induction step (internal vertices):

$$\frac{(C_1 \vee x_1) \quad [I_1] \quad \cdots \quad (C_n \vee x_n) \quad [I_n] \qquad (\overline{x}_1 \vee \cdots \vee \overline{x}_n \vee D) \quad [I_{n+1}]}{\bigvee_{i=1}^{n} C_i \vee D \quad [I]}$$

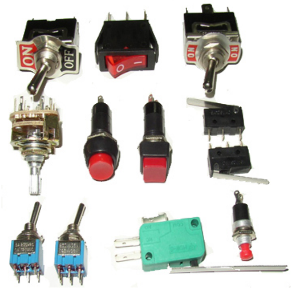
if $x_1, \ldots, x_n$ are  $I \stackrel{\text{def}}{=} \bigvee_{i=1}^{n+1} I_i$

if $x_1, \ldots, x_n$ are  $I \stackrel{\text{def}}{=} \begin{cases} \bigwedge_{i=1}^{n}(x_i \vee I_i) \wedge \left(I_{n+1} \vee \bigvee_{i=1}^{n} \overline{x}_i\right) \\ \text{or} \\ \bigvee_{i=1}^{n}(\overline{x}_i \wedge I_i) \vee \left(I_{n+1} \wedge \bigwedge_{i=1}^{n} x_i\right) \end{cases}$

if $x_1, \ldots, x_n$ are  $I \stackrel{\text{def}}{=} \bigwedge_{i=1}^{n+1} I_i$

Parametrised Interpolation System

+



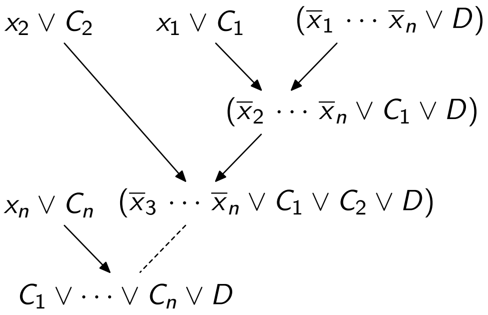
- Interpolation for Hyper-Resolution provides us with a choice for each *inner* node of the proof

+

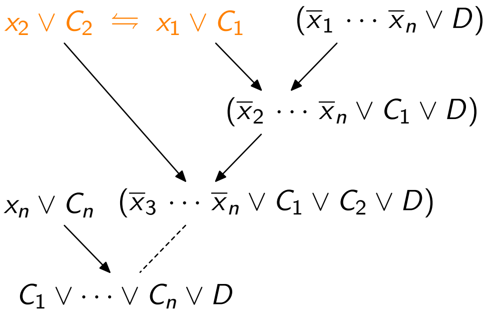
- Interpolation for Hyper-Resolution provides us with a choice for each *inner* node of the proof
- Moreover: Choice determines *strength* of interpolant

$$\bigwedge_{i=1}^{n}(x_i \vee I_i) \wedge \left(I_{n+1} \vee \bigvee_{i=1}^{n} \overline{x}_i\right)$$
$$\Downarrow$$
$$\bigvee_{i=1}^{n}(\overline{x}_i \wedge I_i) \vee \left(I_{n+1} \wedge \bigwedge_{i=1}^{n} x_i\right)$$

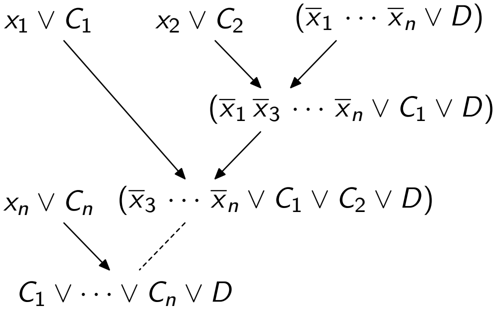
Hyper-Resolution Steps as Chains



Hyper-Resolution Steps as Chains

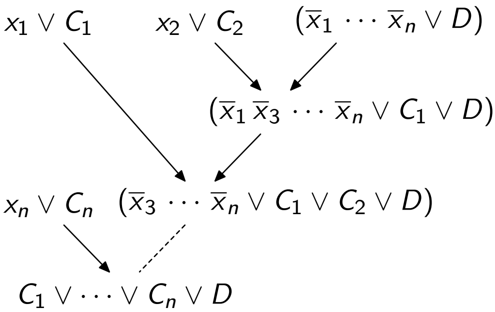


- May swap resolution steps if "merge-free" ($\overline{x}_2 \notin C_1$, $\overline{x}_1 \notin C_2$)



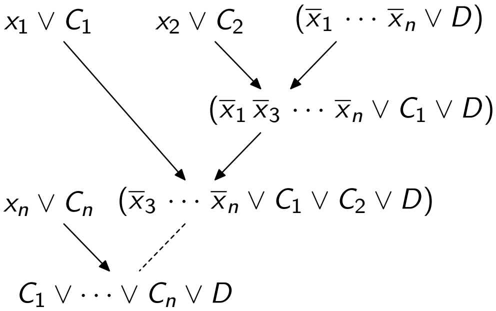
- May swap resolution steps if “merge-free” ($\overline{x}_2 \notin C_1$, $\overline{x}_1 \notin C_2$)

Hyper-Resolution Steps as Chains

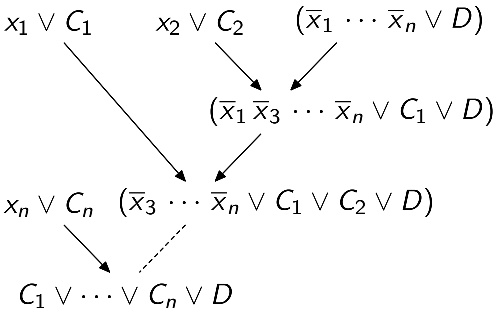


- May swap resolution steps if "merge-free" ($\overline{x}_2 \notin C_1$, $\overline{x}_1 \notin C_2$)
    - Swapping affects *interpolant strength* [D'Silva et al. VMCAI'10]

Hyper-Resolution Steps as Chains



- May swap resolution steps if "merge-free" ($\overline{x}_2 \notin C_1$, $\overline{x}_1 \notin C_2$)
  - Swapping affects *interpolant strength* [D'Silva et al. VMCAI'10]
- If all steps can be swapped: *strongly* merge free



- May swap resolution steps if "merge-free" ($\overline{x}_2 \notin C_1$, $\overline{x}_1 \notin C_2$)
  - Swapping affects *interpolant strength* [D'Silva et al. VMCAI'10]
- If all steps can be swapped: *strongly* merge free
  - Strongly merge-free chains correspond to hyper-resolution (sufficient but not necessary condition)

Completeness of Interpolation System: Splitting Chains

- pivots in chains may not be *uniformly* labelled
- can be resolved by *splitting* hyper-resolution step
  - at most one step for each of { , , }

$$\frac{(x_1 \vee C_1)\ (x_2 \vee C_2)\ (x_3 \vee C_3)\ (x_4 \vee C_4) \quad (\overline{x}_1 \vee \overline{x}_2 \vee \overline{x}_3 \vee \overline{x}_4 \vee D)}{C_1 \vee C_2 \vee C_3 \vee C_4 \vee D}$$

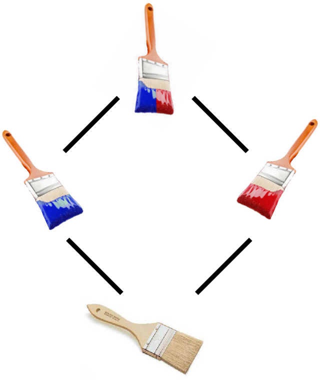
$$\rightsquigarrow$$

$$\frac{(x_2 \vee C_2)\ (x_4 \vee C_4) \qquad \dfrac{(x_1 \vee C_1)\ (x_3 \vee C_3) \quad (\overline{x}_1 \vee \overline{x}_2 \vee \overline{x}_3 \vee \overline{x}_4 \vee D)}{(\overline{x}_2 \vee \overline{x}_4 \vee C_1 \vee C_3 \vee D)}\ [\text{-HyRes}]}{C_1 \vee C_2 \vee C_3 \vee C_4 \vee D}\ [\text{-HyRes}]$$

Outline

- Background
  - Pudlák's Interpolation System
- Interpolation for Propositional Hyper-Resolution Proofs
  - Novel Interpolation Rules (enable *Variation*)
  - "Merge-Free" Resolution Chains
- **Labelled Interpolation and Hyper-Resolution**
- First-Order Logic Derivations and Interpolation for Hyper-Resolution

- Colouring scheme can be relaxed!



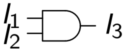
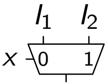
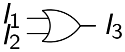
(colour lattice)

-  $\sqcup$  $=$ 

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 $\in$ {  ,  ,  }

Strength of Interpolants (Using Labelled Interpolation)

	A-local	*A*/*B*-shared	*B*-local	
strongest				
				⇓
⇓				
				⇓
weakest				

Elimination of Non-Essential Literals (Using Labelled Interpolation)

- Enables elimination of *non-essential* literals

A-clause	B-clause
	

$$\frac{(x_1 \vee C_1)\quad [I_1] \qquad (x_2 \vee C_2)\quad [I_2] \qquad (\overline{x}_1 \vee \overline{x}_2 \vee D)\quad [I_3]}{(C_1 \vee C_2 \vee D) \quad [(x_1 \vee I_1) \wedge (x_2 \vee I_2) \wedge (\overline{x}_1 \vee \overline{x}_2 \vee I_3)]}$$

⇝ relabel

$$\frac{(x_1 \vee C_1)\quad [I_1] \qquad (x_2 \vee C_2)\quad [I_2] \qquad (\overline{x}_1 \vee \overline{x}_2 \vee D)\quad [I_3]}{(C_1 \vee C_2 \vee D) \quad [I_1 \vee I_2 \vee I_3]}$$

Labelled Interpolation System for Hyper-Resolution

- 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):

$$\frac{(C_1 \vee x_1) \quad [I_1] \quad \cdots \quad (C_n \vee x_n) \quad [I_n] \qquad (\overline{x}_1 \vee \cdots \vee \overline{x}_n \vee D) \quad [I_{n+1}]}{\bigvee_{i=1}^{n} C_i \vee D \quad [I]}$$

if $\bigwedge_{i=1}^{n} L(x_i) \sqcup L(\overline{x}_i) =$  $\quad I \stackrel{\text{def}}{=} \bigvee_{i=1}^{n+1} I_i$

if $\bigwedge_{i=1}^{n} L(x_i) \sqcup L(\overline{x}_i) =$  $\quad I \stackrel{\text{def}}{=} \begin{cases} \bigwedge_{i=1}^{n}(x_i \vee I_i) \wedge \left(I_{n+1} \vee \bigvee_{i=1}^{n} \overline{x}_i\right) \\ \textit{or} \\ \bigvee_{i=1}^{n}(\overline{x}_i \wedge I_i) \vee \left(I_{n+1} \wedge \bigwedge_{i=1}^{n} x_i\right) \end{cases}$

if $\bigwedge_{i=1}^{n} L(x_i) \sqcup L(\overline{x}_i) =$  $\quad I \stackrel{\text{def}}{=} \bigwedge_{i=1}^{n+1} I_i$

- Complete lattices induced by point-wise extension of:
  - Labelling function *L* : *Nodes* $\rightarrow \{$ , ,  $\}$ for initial nodes
  - Choice χ : *Nodes* $\rightarrow \{1, 2\}$ of interpolation rule for internal nodes
- Enables
  - systematic variable of *strength* (using *L*, χ)
  - elimination of *non-essential* literals (using *L*)
- Choice and labelling functions for hyper-resolution are *orthogonal*

Outline

- Background
  - Pudlák's Interpolation System
- Interpolation for Propositional Hyper-Resolution Proofs
  - Novel Interpolation Rules (enable *Variation*)
  - “Merge-Free” Resolution Chains
- Labelled Interpolation and Hyper-Resolution
- **First-Order Logic Derivations & Interpolation f. Hyper-Resolution**

Hyper-Resolution Proofs from First-Order Derivations

$$\dfrac{\dfrac{\dfrac{y = x}{y \leq x} \qquad \dfrac{y \neq 0 \qquad \dfrac{z = y\&(y-1)}{z \leq y - 1}}{z < y}}{z < x} \qquad x = z}{\textbf{false}}$$

$\rightsquigarrow$ extract

$$\dfrac{(y = x) \quad (y \neq 0) \quad (z = y\&(y-1)) \quad \overbrace{\left(\overline{(y = x)} \vee \overline{(y \neq 0)} \vee \overline{(z = y\&(y-1))} \vee (z < x)\right)}^{\text{tautology}}}{z < x}$$

- Extract propositional hyper-resolution proofs from FOL derivations
  - Treat *closed/ground* FOL formulae as propositional atoms
- Colouring conditions impose restrictions on proof structure
  - c.f. [Jhala & McMillan TACAS'06] and [Kovács & Voronkov CADE'09]

Conclusion

- Generalises *labelled interpolation systems* to *hyper-resolution*
- Subsumes
  - existing propositional interpolation systems (Huang/Krajíček/Pudlák, McMillan)
  - first-order interpolation systems of [Kovács & Voronkov CADE'09] and [Weissenbacher 2010]

  and relates them in logical strength
- Enables systematic modulation of interpolants
  - variation of logical strength
  - elimination of non-essential literals