

# Refinement Strategies for Verification Methods Based on Datapath Abstraction

Zaher S. Andraus, Mark H. Liffiton, & Karem A. Sakallah  
University of Michigan



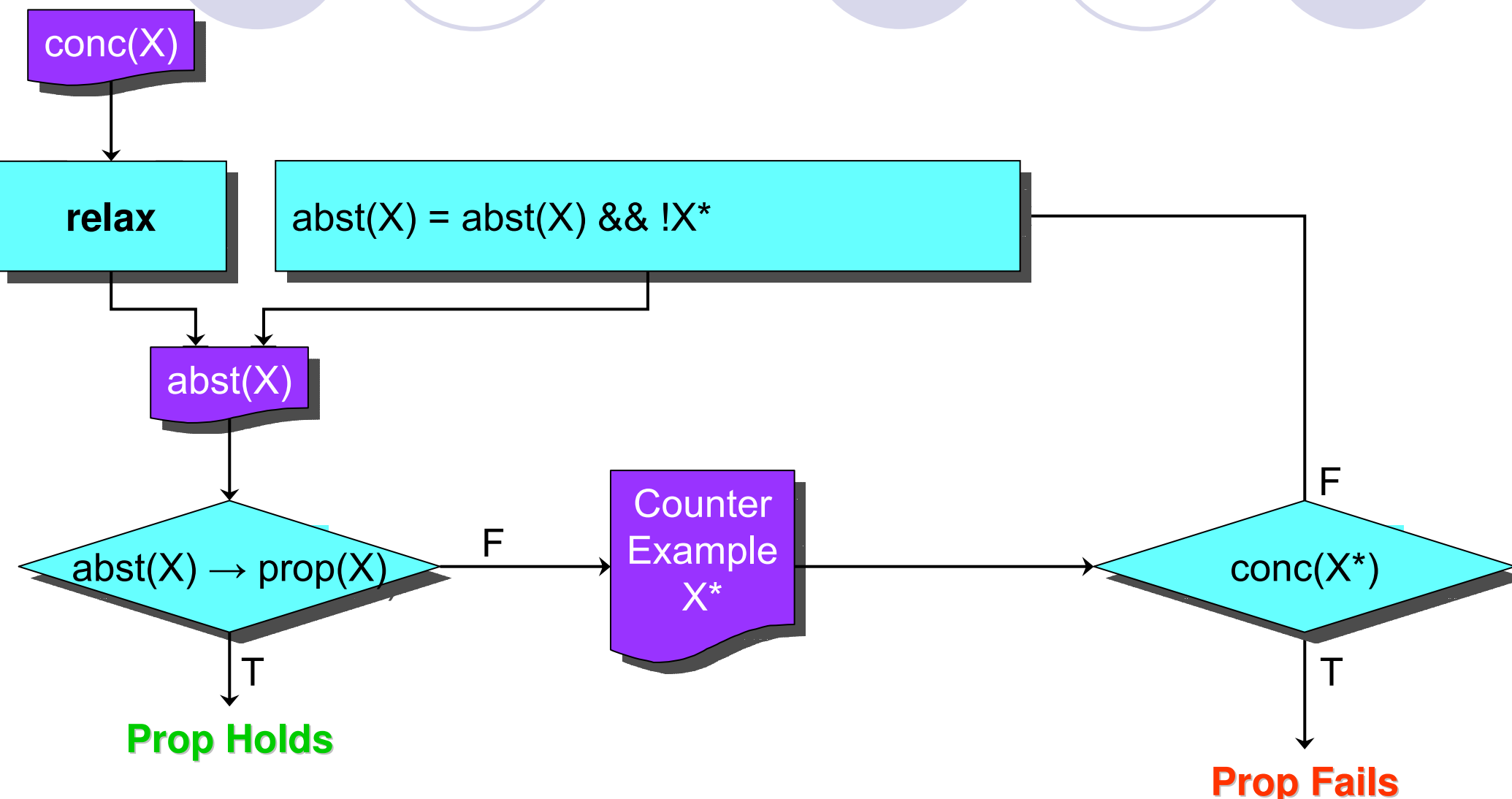
ASP-DAC 2006  
Yokohama, Japan  
January 25, 2006



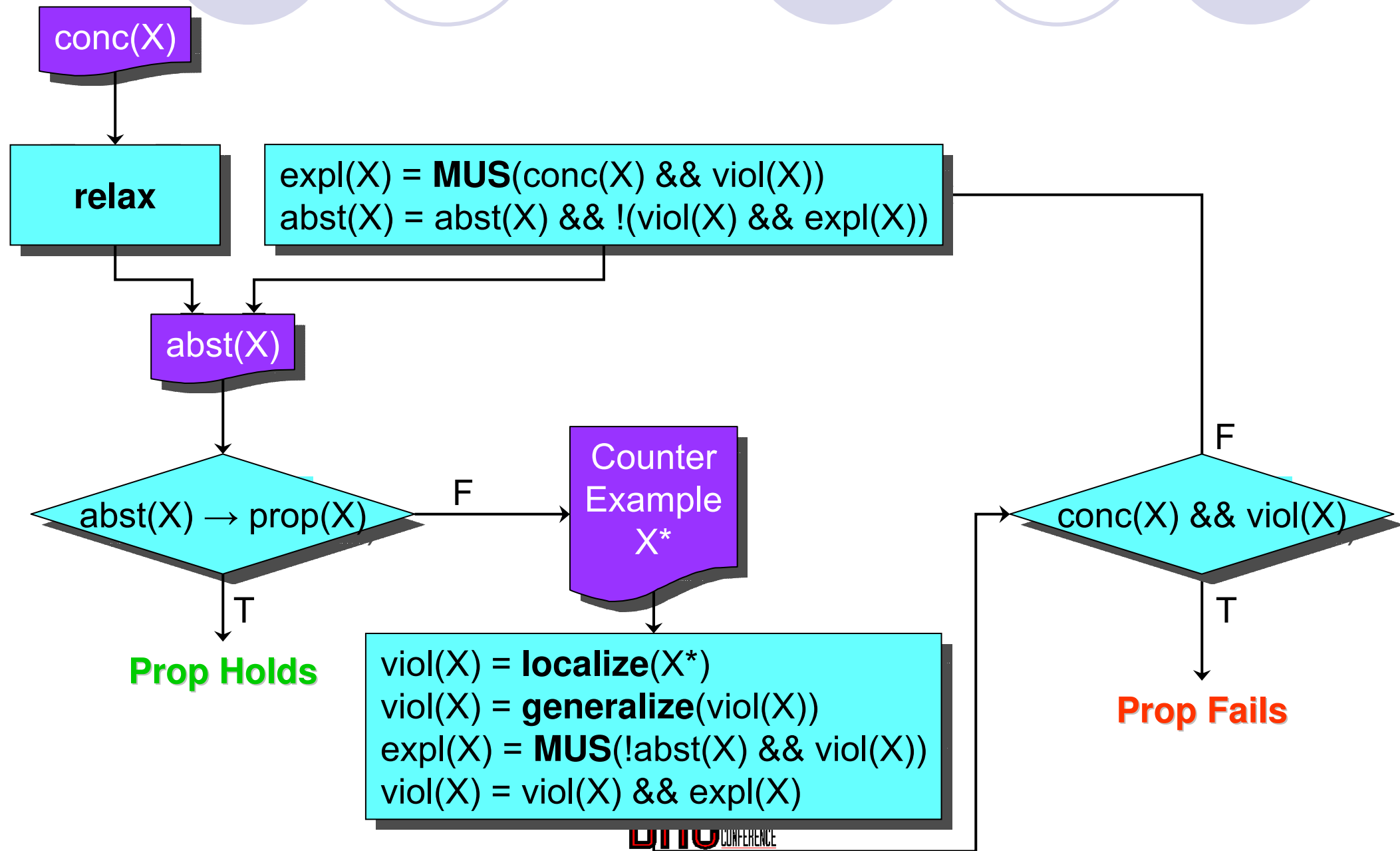
# REVEAL

- Formal equivalence verification of Verilog designs
- Based on automatic *datapath abstraction & refinement*
- Leverages recent advances in *scalable automated reasoning methods*
- Suitable for verification of (control logic of) pipelined microprocessors against their ISA specs
- Extensible (through suitable definition of “equivalence”) to other high-performance microarchitectures

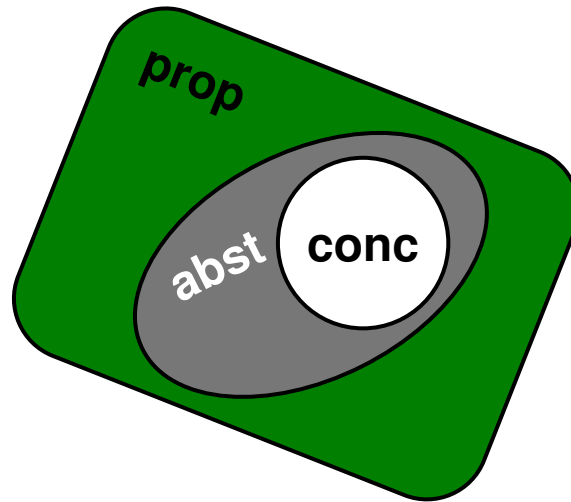
# Basic CEGAR



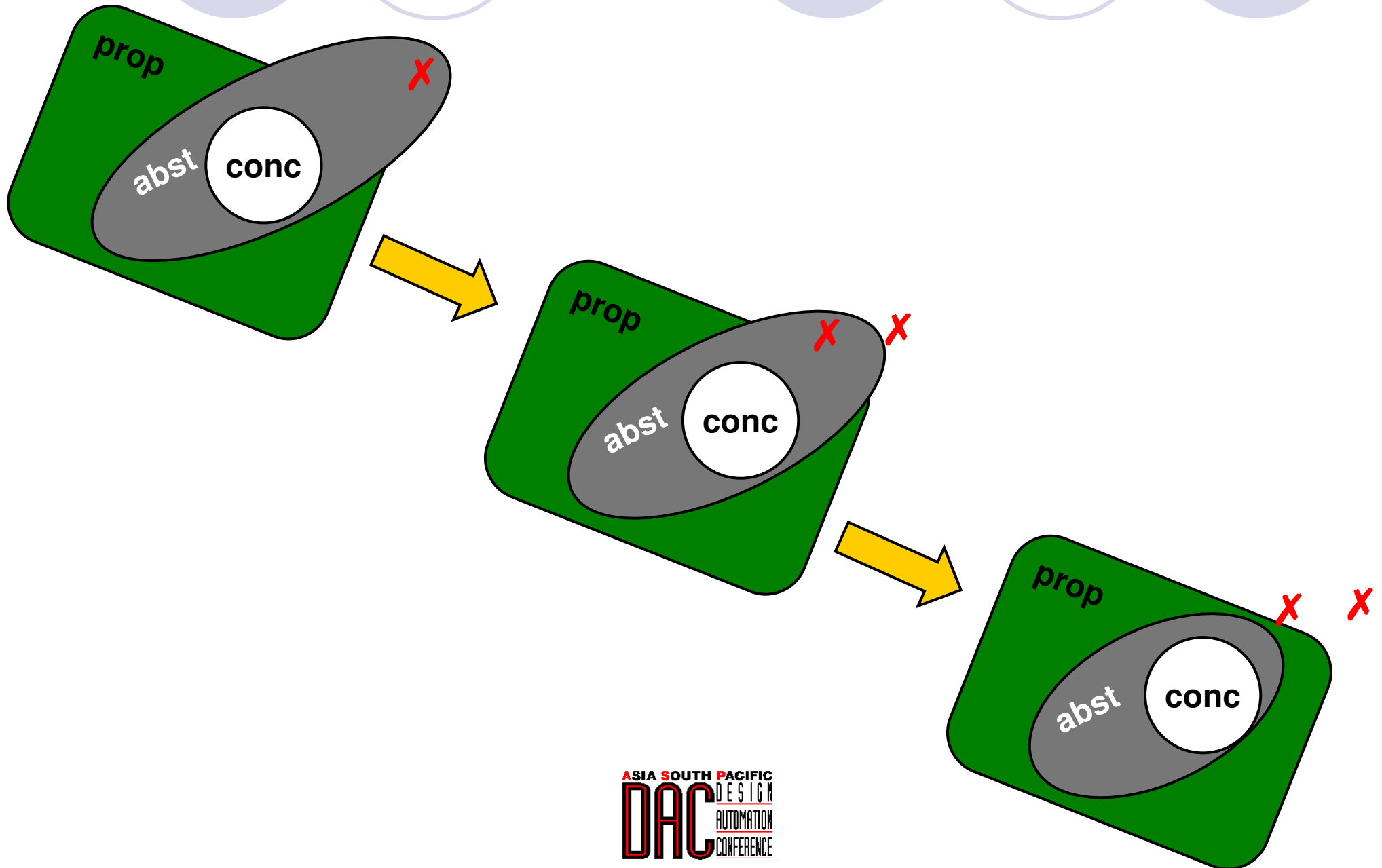
# CEGAR with Enhanced Refinement



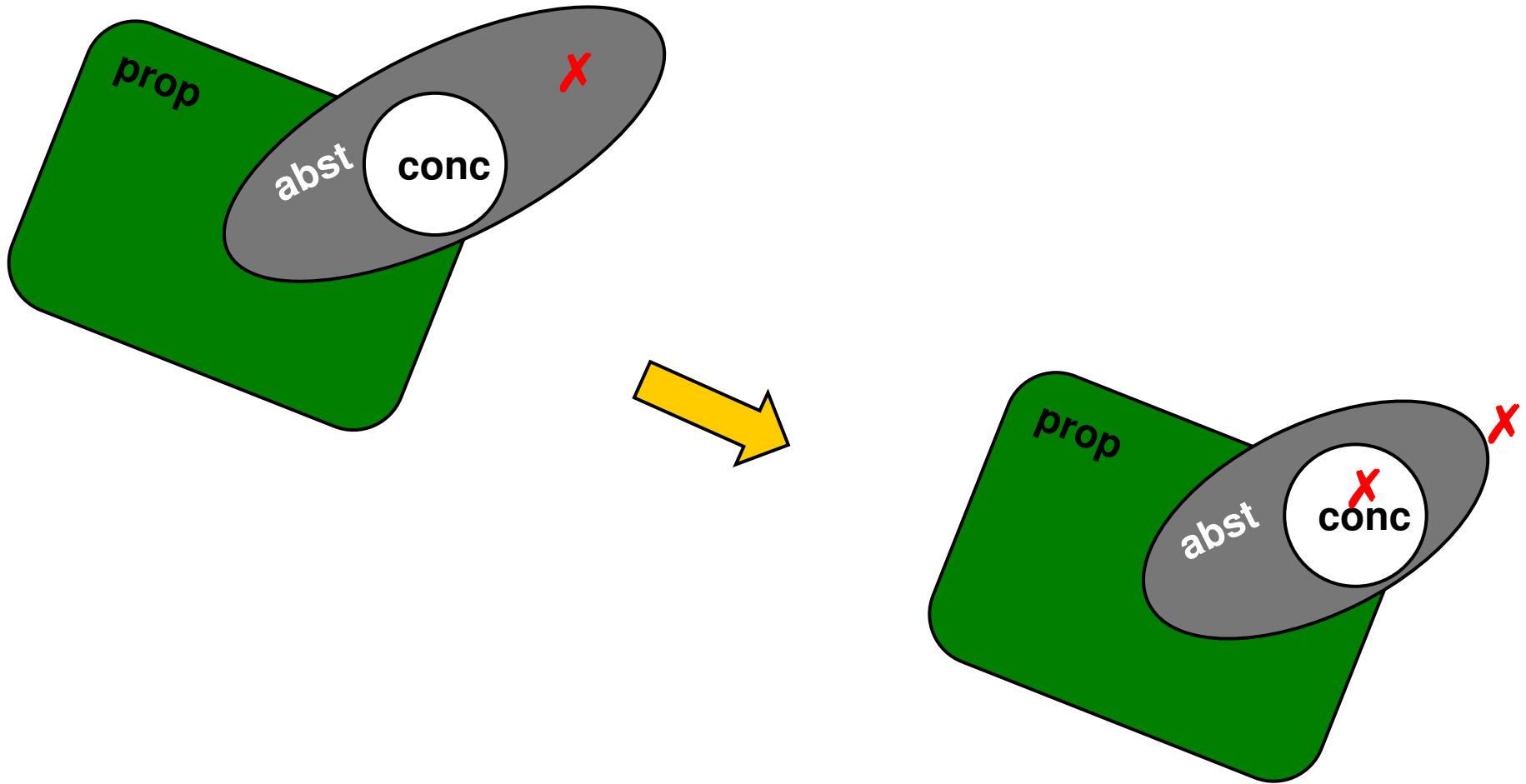
# Property Satisfied by Abstract Model



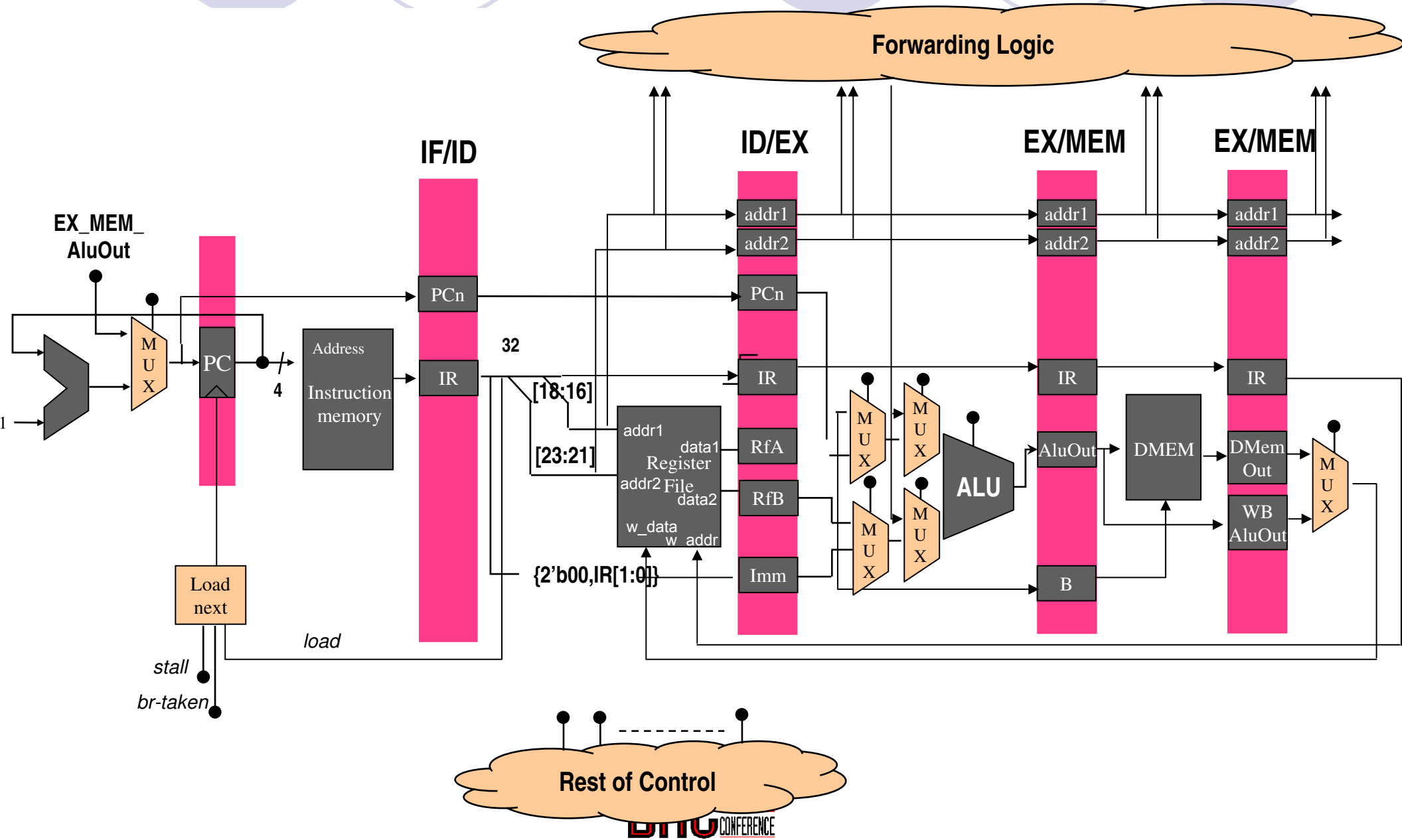
# Property Violated by Abstract Model but Satisfied by Concrete Model



# Property Violated by both Abstract and Concrete Models

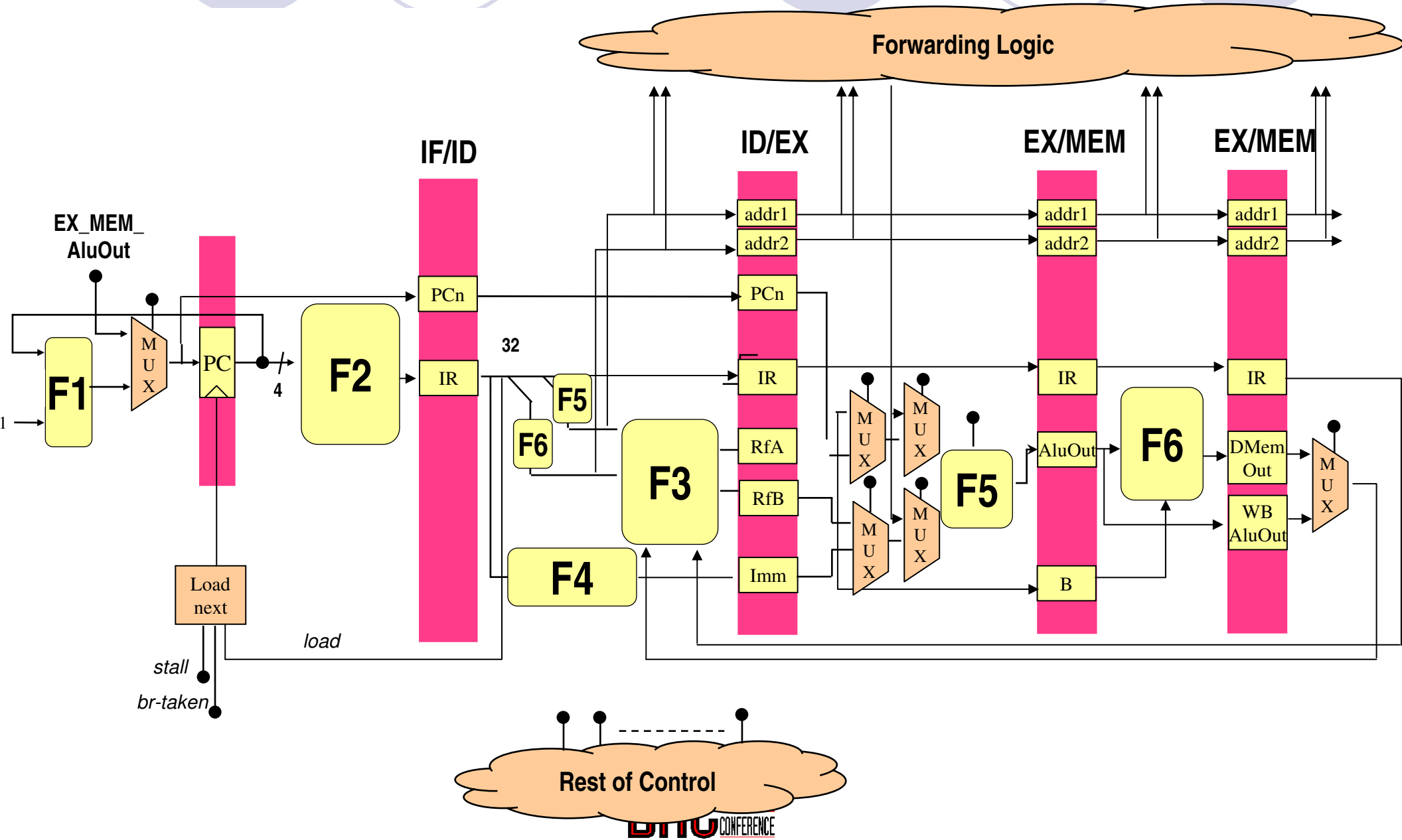


# Datapath Abstraction





# Datapath Abstraction



# Running Example

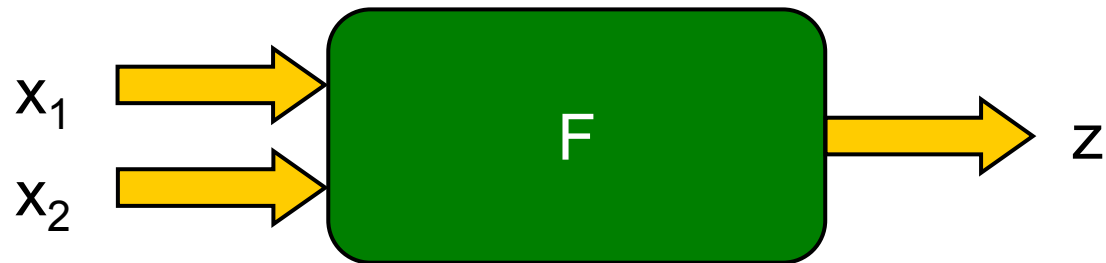
```
module example();  
  wire [3:0] a, b;  
  wire m = a[3]; // msb  
  wire l = a[0]; // lsb  
  wire c = m? a >> 1 : a;  
  wire d = l? b >> 2 : c;  
  wire e = m? a : a >> 1;  
  wire f = l? {2'b00, b[3:2]} : e;  
  wire p = !(a == 0) || (d == f);  
endmodule;
```

```
conc( a,b,c,d,e,f,l,m,p ) =  
  ( m = a[3] ) ^  
  ( l = a[0] ) ^  
  ( m ^ ( c = a >> 1 ) v ~m ^ ( c = a ) ) ^  
  ( l ^ ( d = b >> 2 ) v ~l ^ ( d = c ) ) ^  
  ( m ^ ( e = a ) v ~m ^ ( e = a >> 1 ) ) ^  
  ( l ^ ( f = { 2'b00, b[3:2] } ) v ~l ^ ( f = e ) ) ^  
  ( p = ~( a = 0 ) v ( d = f ) )
```

# Running Example

$$\begin{aligned} \text{conc}(a,b,c,d,e,f,l,m,p) = & \\ & (m = a[3]) \wedge \\ & (l = a[0]) \wedge \\ & (m \wedge (c = a \gg 1) \vee \neg m \wedge (c = a)) \wedge \\ & (l \wedge (d = b \gg 2) \vee \neg l \wedge (d = c)) \wedge \\ & (m \wedge (e = a) \vee \neg m \wedge (e = a \gg 1)) \wedge \\ & (l \wedge (f = \{2'b00, b[3:2]\}) \vee \neg l \wedge (f = e)) \wedge \\ & (p = \neg(a = 0) \vee (d = f)) \end{aligned}$$
$$\begin{aligned} \text{abst}(a,b,c,d,e,f,l,m,s,t,u,p,\text{zero}) = & \\ & (m = \text{EX1}(a)) \wedge \\ & (l = \text{EX2}(a)) \wedge \\ & (s = \text{SR1}(a, \text{succ}(\text{zero}))) \wedge \\ & (t = \text{SR2}(b, \text{succ}(\text{succ}(\text{zero})))) \wedge \\ & (u = \text{CT1}(\text{zero}, \text{EX3}(b))) \wedge \\ & (c = \text{ite}(m,s,a)) \wedge \\ & (d = \text{ite}(l,t,c)) \wedge \\ & (e = \text{ite}(m,a,s)) \wedge \\ & (f = \text{ite}(l,u,e)) \wedge \\ & (p = \neg(a = 0) \vee (d = f)) \wedge \\ & \text{Functional Consistency Constraints} \end{aligned}$$

# Functional Consistency



$$(y_1 = x_1) \wedge (y_2 = x_2) \rightarrow F(y_1, y_2) = F(x_1, x_2)$$

# 1<sup>st</sup> Iteration: Counterexample

$$\begin{aligned} \text{abst}(a,b,c,d,e,f,l,m,s,t,u,p,\text{zero}) = & \\ (m = \text{EX1}(a)) \wedge & \\ (l = \text{EX2}(a)) \wedge & \\ (s = \text{SR1}(a, \text{succ}(\text{zero}))) \wedge & \\ (t = \text{SR2}(b, \text{succ}(\text{succ}(\text{zero})))) \wedge & \\ (u = \text{CT1}(\text{zero}, \text{EX3}(b))) \wedge & \\ (c = \text{ite}(m,s,a)) \wedge & \\ (d = \text{ite}(l,t,c)) \wedge & \\ (e = \text{ite}(m,a,s)) \wedge & \\ (f = \text{ite}(l,u,e)) \wedge & \\ (p = \neg(a = 0) \vee (d = f)) \wedge & \end{aligned}$$

Functional Consistency Constraints

$$\begin{aligned} \text{abst}(a,b,c,d,e,f,l,m,s,t,u,p,\text{zero}) = & \\ (1 = \text{EX1}(0)) \wedge & \\ (1 = \text{EX2}(0)) \wedge & \\ (16 = \text{SR1}(0, \text{succ}(\text{zero}))) \wedge & \\ (20 = \text{SR2}(8, \text{succ}(\text{succ}(\text{zero})))) \wedge & \\ (12 = \text{CT1}(\text{zero}, \text{EX3}(8))) \wedge & \\ (16 = \text{ite}(1,16,0)) \wedge & \\ (20 = \text{ite}(1,20,16)) \wedge & \\ (0 = \text{ite}(1,0,16)) \wedge & \\ (12 = \text{ite}(1,12,0)) \wedge & \\ (0 = \neg(0 = 0) \vee (20 = 12)) \wedge & \end{aligned}$$

Functional Consistency Constraints

# 1<sup>st</sup> Iteration: Localize Counterexample

$\text{abst}(a,b,c,d,e,f,l,m,s,t,u,p,\text{zero}) =$   
 $(m = \text{EX1}(a)) \wedge$   
 $(l = \text{EX2}(a)) \wedge$   
 $(s = \text{SR1}(a, \text{succ}(\text{zero}))) \wedge$   
 $(t = \text{SR2}(b, \text{succ}(\text{succ}(\text{zero})))) \wedge$   
 $(u = \text{CT1}(\text{zero}, \text{EX3}(b))) \wedge$   
 $(c = \text{ite}(m,s,a)) \wedge$   
 $(d = \text{ite}(l,t,c)) \wedge$   
 $(e = \text{ite}(m,a,s)) \wedge$   
 $(f = \text{ite}(l,u,e)) \wedge$   
 $(p = \neg(a = 0) \vee (d = f)) \wedge$   
Functional Consistency Constraints

$\text{abst}(a,b,c,d,e,f,l,m,s,t,u,p,\text{zero}) =$   
 $(1 = \text{EX1}(0)) \wedge$   
 $(1 = \text{EX2}(0)) \wedge$   
 $(16 = \text{SR1}(0, \text{succ}(\text{zero}))) \wedge$   
 $(20 = \text{SR2}(8, \text{succ}(\text{succ}(\text{zero})))) \wedge$   
 $(12 = \text{CT1}(\text{zero}, \text{EX3}(8))) \wedge$   
 $(16 = \text{ite}(1,16,0)) \wedge$   
 $(20 = \text{ite}(1,20,16)) \wedge$   
 $(0 = \text{ite}(1,0,16)) \wedge$   
 $(12 = \text{ite}(1,12,0)) \wedge$   
 $(0 = \neg(0 = 0) \vee (20 = 12)) \wedge$   
Functional Consistency Constraints

# 1<sup>st</sup> Iteration: Generalize Counterexample

$\text{abst}(a, b, c, d, e, f, l, m, s, t, u, p, \text{zero}) =$   
 $(m = \text{EX1}(a)) \wedge$   
 $(l = \text{EX2}(a)) \wedge$   
 $(s = \text{SR1}(a, \text{succ}(\text{zero}))) \wedge$   
 $(t = \text{SR2}(b, \text{succ}(\text{succ}(\text{zero})))) \wedge$   
 $(u = \text{CT1}(\text{zero}, \text{EX3}(b))) \wedge$   
 $(c = \text{ite}(m, s, a)) \wedge$   
 $(d = \text{ite}(l, t, c)) \wedge$   
 $(e = \text{ite}(m, a, s)) \wedge$   
 $(f = \text{ite}(l, u, e)) \wedge$   
 $(p = \neg(a = 0) \vee (d = f)) \wedge$

Functional Consistency Constraints

$(a = 0) \wedge$   
 $(l = 1) \wedge$   
 $(t \neq u)$

# 1<sup>st</sup> Iteration: Minimal Abstract Explanation

$$\begin{aligned} \text{abst}(a,b,c,d,e,f,l,m,s,t,u,p,\text{zero}) = & \\ & (m = \text{EX1}(a)) \wedge \\ & (l = \text{EX2}(a)) \wedge \\ & (s = \text{SR1}(a, \text{succ}(\text{zero}))) \wedge \\ & (t = \text{SR2}(b, \text{succ}(\text{succ}(\text{zero})))) \wedge \\ & (u = \text{CT1}(\text{zero}, \text{EX3}(b))) \wedge \\ & (c = \text{ite}(m,s,a)) \wedge \\ & (d = \text{ite}(l,t,c)) \wedge \\ & (e = \text{ite}(m,a,s)) \wedge \\ & (f = \text{ite}(l,u,e)) \wedge \\ & (p = \neg(a = 0) \vee (d = f)) \wedge \end{aligned}$$

Functional Consistency Constraints

$$\begin{aligned} & (a = 0) \wedge \\ & (l = 1) \wedge \\ & (t \neq u) \end{aligned}$$



# 1<sup>st</sup> Iteration: Minimal Concrete Explanations

$\text{conc}(a, b, c, d, e, f, l, m, p) =$

$(m = a[3]) \wedge$

$(l = a[0]) \wedge$

$(m \wedge (c = a \gg 1) \vee \neg m \wedge (c = a)) \wedge$

$(l \wedge (d = b \gg 2) \vee \neg l \wedge (d = c)) \wedge$

$(m \wedge (e = a) \vee \neg m \wedge (e = a \gg 1)) \wedge$

$(l \wedge (f = \{2'b00, b[3:2]\}) \vee \neg l \wedge (f = e)) \wedge$

$(p = \neg(a = 0) \vee (d = f))$

$\text{viol}_1 = (a = 0) \wedge (a[0] = 1)$

$\text{viol}_2 = b \gg 2 \neq \{2'b00, b[3:2]\}$

## 2<sup>nd</sup> Iteration: Counterexample

$\text{abst}(a,b,c,d,e,f,l,m,s,t,u,p,\text{zero}) =$   
 $(m = \text{EX1}(a)) \wedge$   
 $(l = \text{EX2}(a)) \wedge$   
 $(s = \text{SR1}(a, \text{succ}(\text{zero}))) \wedge$   
 $(t = \text{SR2}(b, \text{succ}(\text{succ}(\text{zero})))) \wedge$   
 $(u = \text{CT1}(\text{zero}, \text{EX3}(b))) \wedge$   
 $(c = \text{ite}(m,s,a)) \wedge$   
 $(d = \text{ite}(l,t,c)) \wedge$   
 $(e = \text{ite}(m,a,s)) \wedge$   
 $(f = \text{ite}(l,u,e)) \wedge$   
 $(p = \neg(a = 0) \vee (d = f)) \wedge$   
 $\neg((a = 0) \wedge (l = 1)) \wedge \neg(t \neq u)$

Functional Consistency Constraints

$\text{abst}(a,b,c,d,e,f,l,m,s,t,u,p,\text{zero}) =$   
 $(1 = \text{EX1}(0)) \wedge$   
 $(0 = \text{EX2}(0)) \wedge$   
 $(8 = \text{SR1}(0, \text{succ}(\text{zero}))) \wedge$   
 $(3 = \text{SR2}(16, \text{succ}(\text{succ}(\text{zero})))) \wedge$   
 $(3 = \text{CT1}(\text{zero}, \text{EX3}(16))) \wedge$   
 $(8 = \text{ite}(1,8,0)) \wedge$   
 $(8 = \text{ite}(0,3,8)) \wedge$   
 $(0 = \text{ite}(1,0,8)) \wedge$   
 $(0 = \text{ite}(0,3,0)) \wedge$   
 $(0 = \neg(0 = 0) \vee (8 = 0)) \wedge$   
 $\neg((0 = 0) \wedge (0 = 1)) \wedge \neg(3 \neq 3)$

Functional Consistency Constraints

## 2<sup>nd</sup> Iteration: Localize Counterexample

$\text{abst}(a,b,c,d,e,f,l,m,s,t,u,p,\text{zero}) =$   
 $(m = \text{EX1}(a)) \wedge$   
 $(l = \text{EX2}(a)) \wedge$   
 $(s = \text{SR1}(a, \text{succ}(\text{zero}))) \wedge$   
 $(t = \text{SR2}(b, \text{succ}(\text{succ}(\text{zero})))) \wedge$   
 $(u = \text{CT1}(\text{zero}, \text{EX3}(b))) \wedge$   
 $(c = \text{ite}(m,s,a)) \wedge$   
 $(d = \text{ite}(l,t,c)) \wedge$   
 $(e = \text{ite}(m,a,s)) \wedge$   
 $(f = \text{ite}(l,u,e)) \wedge$   
 $(p = \neg(a = 0) \vee (d = f)) \wedge$   
 $\neg((a = 0) \wedge (l = 1)) \wedge \neg(t \neq u)$

Functional Consistency Constraints

$\text{abst}(a,b,c,d,e,f,l,m,s,t,u,p,\text{zero}) =$   
 $(1 = \text{EX1}(0)) \wedge$   
 $(0 = \text{EX2}(0)) \wedge$   
 $(8 = \text{SR1}(0, \text{succ}(\text{zero}))) \wedge$   
 $(3 = \text{SR2}(16, \text{succ}(\text{succ}(\text{zero})))) \wedge$   
 $(3 = \text{CT1}(\text{zero}, \text{EX3}(16))) \wedge$   
 $(8 = \text{ite}(1,8,0)) \wedge$   
 $(8 = \text{ite}(0,3,8)) \wedge$   
 $(0 = \text{ite}(1,0,8)) \wedge$   
 $(0 = \text{ite}(0,3,0)) \wedge$   
 $(0 = \neg(0 = 0) \vee (8 = 0)) \wedge$   
 $\neg((0 = 0) \wedge (0 = 1)) \wedge \neg(3 \neq 3)$

Functional Consistency Constraints

## 2<sup>nd</sup> Iteration: Generalize Counterexample

$\text{abst}(a,b,c,d,e,f,l,m,s,t,u,p,\text{zero}) =$   
 $(m = \text{EX1}(a)) \wedge$   
 $(l = \text{EX2}(a)) \wedge$   
 $(s = \text{SR1}(a, \text{succ}(\text{zero}))) \wedge$   
 $(t = \text{SR2}(b, \text{succ}(\text{succ}(\text{zero})))) \wedge$   
 $(u = \text{CT1}(\text{zero}, \text{EX3}(b))) \wedge$   
 $(c = \text{ite}(m,s,a)) \wedge$   
 $(d = \text{ite}(l,t,c)) \wedge$   
 $(e = \text{ite}(m,a,s)) \wedge$   
 $(f = \text{ite}(l,u,e)) \wedge$   
 $(p = \neg(a = 0) \vee (d = f)) \wedge$   
 $\neg((a = 0) \wedge (l = 1)) \wedge \neg(t \neq u)$

Functional Consistency Constraints

$(a = 0) \wedge$   
 $(l = 0) \wedge$   
 $(m = 1) \wedge$   
 $(t = u) \wedge$   
 $(a \neq s)$

## 2<sup>nd</sup> Iteration: Minimal Abstract Explanation

$\text{abst}(a,b,c,d,e,f,l,m,s,t,u,p,\text{zero}) =$   
 $(m = \text{EX1}(a)) \wedge$   
 $(l = \text{EX2}(a)) \wedge$   
 $(s = \text{SR1}(a, \text{succ}(\text{zero}))) \wedge$   
 $(t = \text{SR2}(b, \text{succ}(\text{succ}(\text{zero})))) \wedge$   
 $(u = \text{CT1}(\text{zero}, \text{EX3}(b))) \wedge$   
 $(c = \text{ite}(m,s,a)) \wedge$   
 $(d = \text{ite}(l,t,c)) \wedge$   
 $(e = \text{ite}(m,a,s)) \wedge$   
 $(f = \text{ite}(l,u,e)) \wedge$   
 $(p = \neg(a = 0) \vee (d = f)) \wedge$   
 $\neg((a = 0) \wedge (l = 1)) \wedge \neg(t \neq u)$

Functional Consistency Constraints

$(a = 0) \wedge$   
 $(l = 0) \wedge$   
 $(t = u) \wedge$   
 $(a \neq s)$

## 2<sup>nd</sup> Iteration: Minimal Concrete Explanations

$\text{conc}(a,b,c,d,e,f,l,m,p) =$

$(m = a[3]) \wedge$

$(l = a[0]) \wedge$

$(m \wedge (c = a \gg 1) \vee \neg m \wedge (c = a)) \wedge$

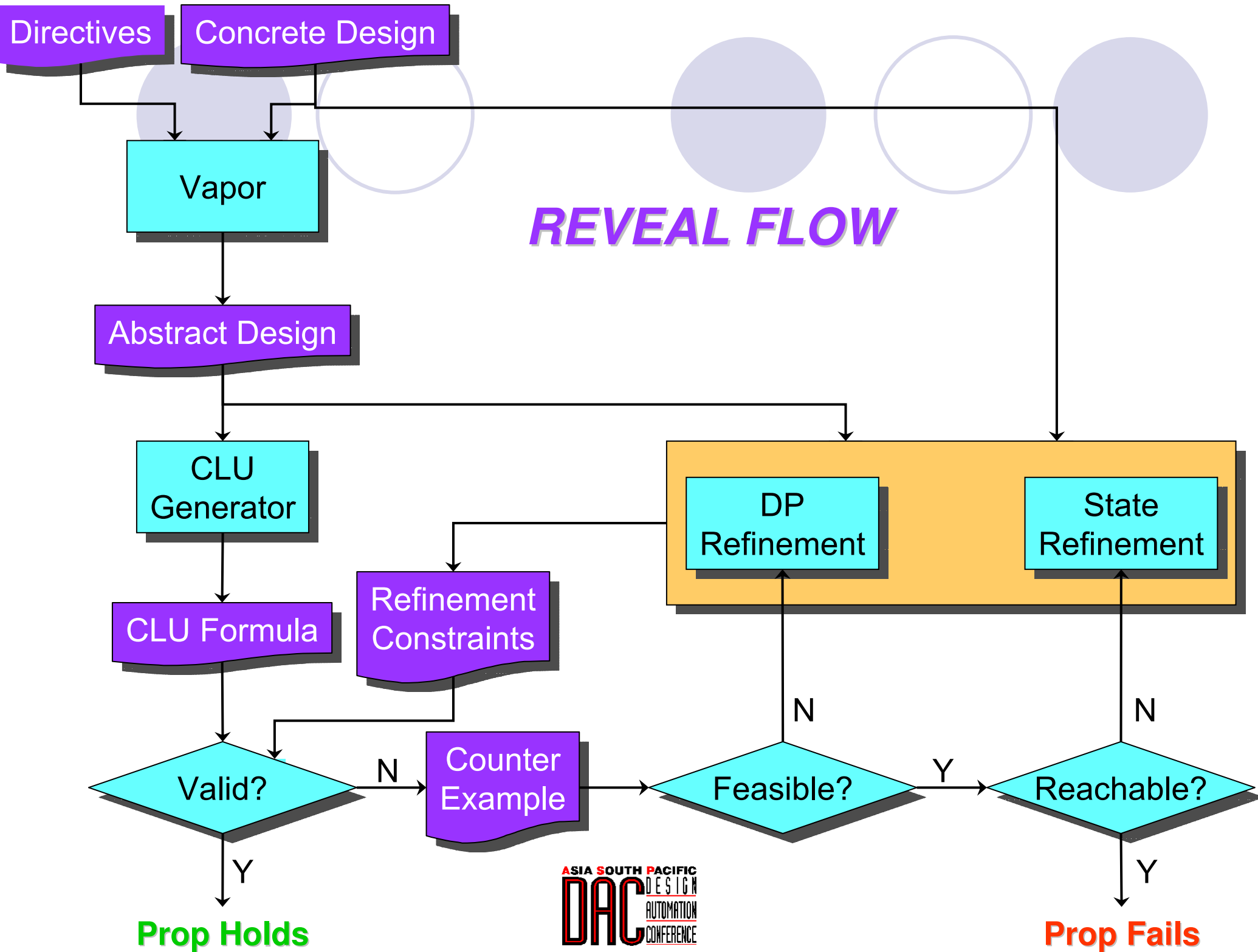
$(l \wedge (d = b \gg 2) \vee \neg l \wedge (d = c)) \wedge$

$(m \wedge (e = a) \vee \neg m \wedge (e = a \gg 1)) \wedge$

$(l \wedge (f = \{2'b00, b[3:2]\}) \vee \neg l \wedge (f = e)) \wedge$

$(p = \neg(a = 0) \vee (d = f))$

$\text{viol}_3 = (a = 0) \wedge (a \neq a \gg 1)$



**REVEAL FLOW**

**Prop Holds**

**Prop Fails**

# Preliminary Evaluation: Benchmarks

Module	Source	Lines	Latches
DLX	VIS	686	396
Risc16f84	OpenCores	1719	8312
SimplePipeline	UM	148	1597
SimpleCorr	UM	86	5



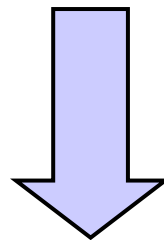
# Preliminary Evaluation: Verification Results

Module	Test	Result	CE Length	Run Time (s)	Refinement Iterations
DLX	1	BUG	11	19.13	2
	2	VALID	-	20.91	2
Risc16f84	1	BUG	4	0.31	1
	2	BUG	4	36.52	2
	3	VALID	-	9.3	1
SimplePipeline	1	VALID	-	3.2	2
SimpleCorr	1	VALID	-	2.7	4

# Other Refinement Strategies

- Bit Slicing: admit “mistake” and blast terms back to bits
- Find multiple explanations of the violation from the abstract model
- Generalize (and store) inferred “facts”:

$$\text{Viol} = \neg[\text{CT2}(\text{zero}, \text{EX4}(\text{pc})) = \text{EX4}(\text{pc})]$$



$$\text{Viol}' = \neg[\forall T \cdot \text{CT2}(\text{zero}, T) = T]$$

# Extensions: Apply on Real-World Examples

- Broader category of pipelines and architectures
  - Out-of-Order Execution
  - Superscalar / VLIW
  - External and Internal Exceptions (Interrupts)
  - Speculation
  - Hierarchical Memory
- Other abstraction schemes to prevent blow-up of CLU formulas
  - Predicate abstraction
  - Temporal abstraction