Refinement Strategies for Verification Methods Based on Datapath Abstraction

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

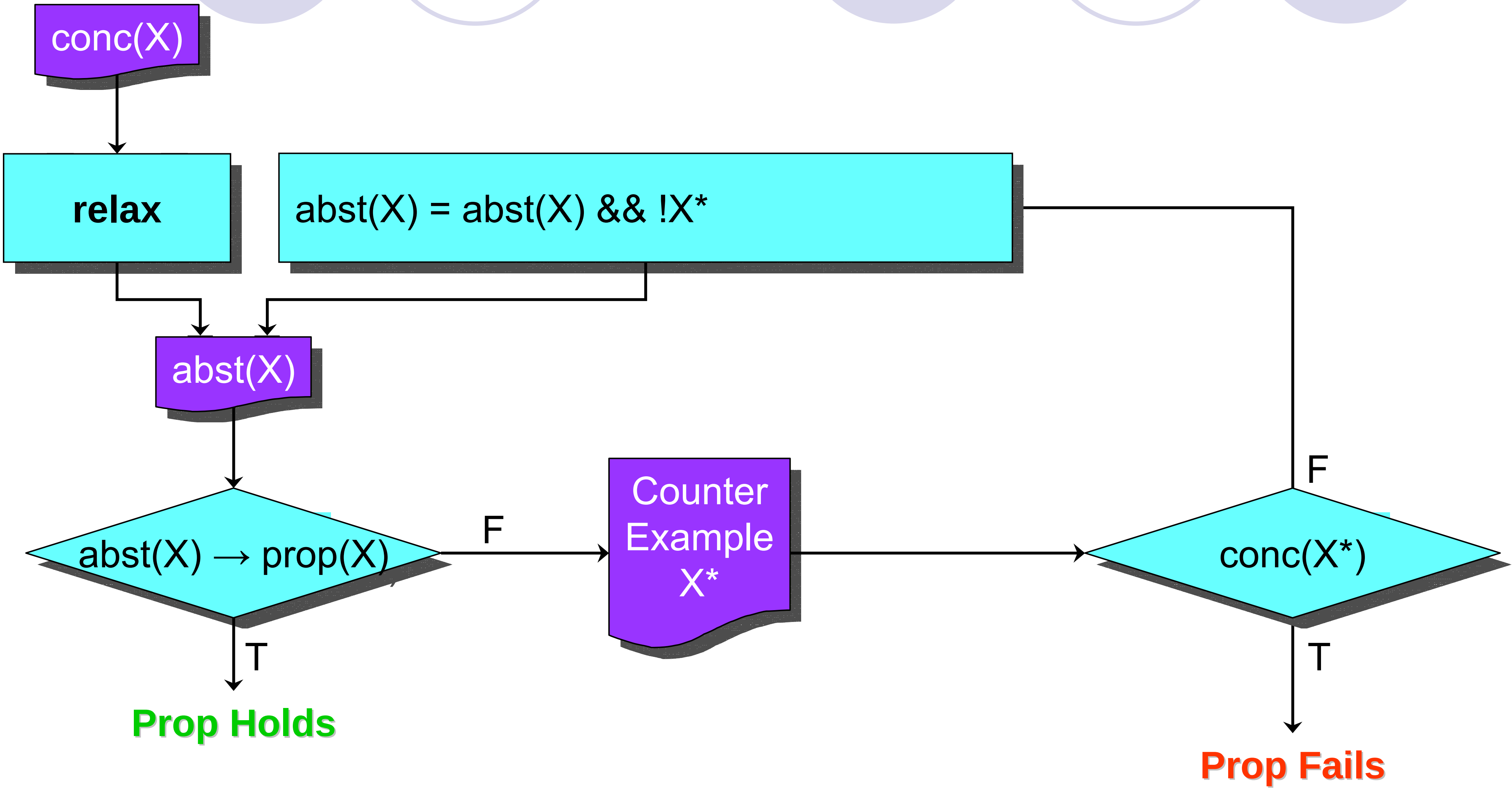
ASIA SOUTH PACIFIC DAC DESIGN AUTOMATION CONFERENCE

ASP-DAC 2006
Yokohama, Japan
January 25, 2006

REVEAL

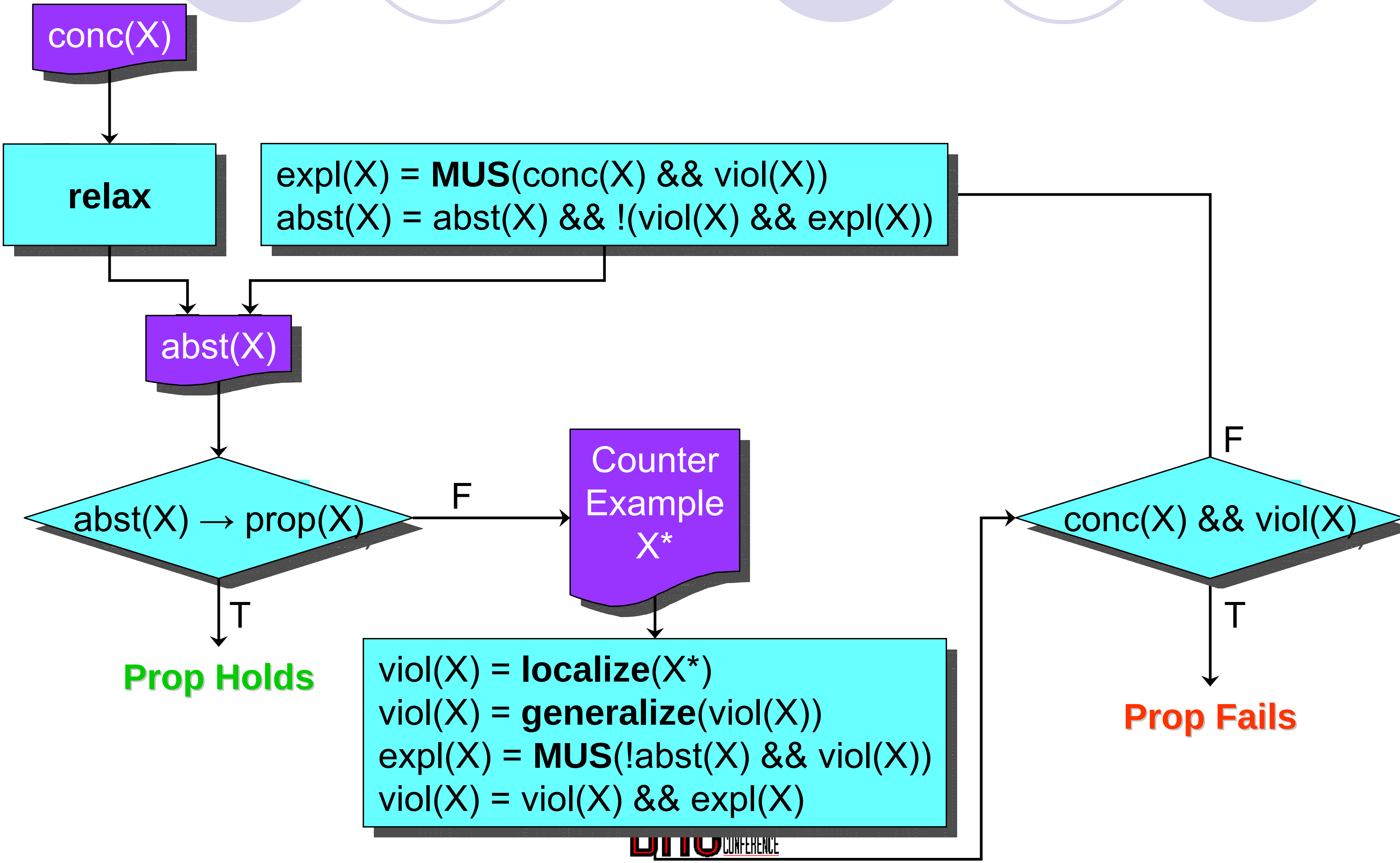
- Formal equivalence verification of Verilog designs
- Based on automatic *datapath abstraction & refinement*
- Leverages recent advances in *scalable automated reasoning methods*
- Suitable for verification of (control logic of) pipelined microprocessors against their ISA specs
- Extensible (through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

Basic CEGAR

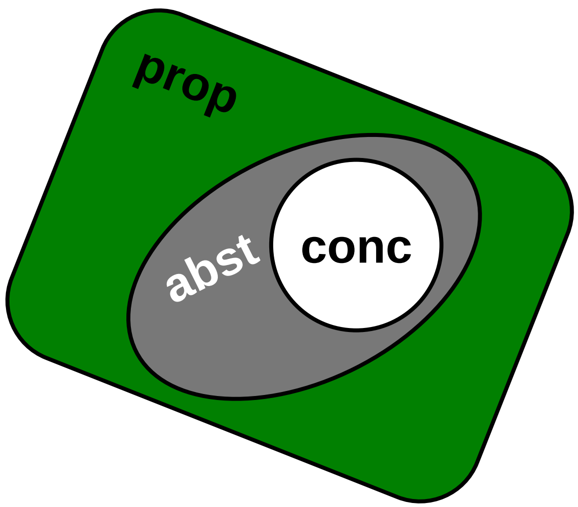


conc(X)
relax
abst(X) = abst(X) && !X*
abst(X)
abst(X) → prop(X)
F
Counter Example X*
F
conc(X*)
T
T
Prop Holds
Prop Fails

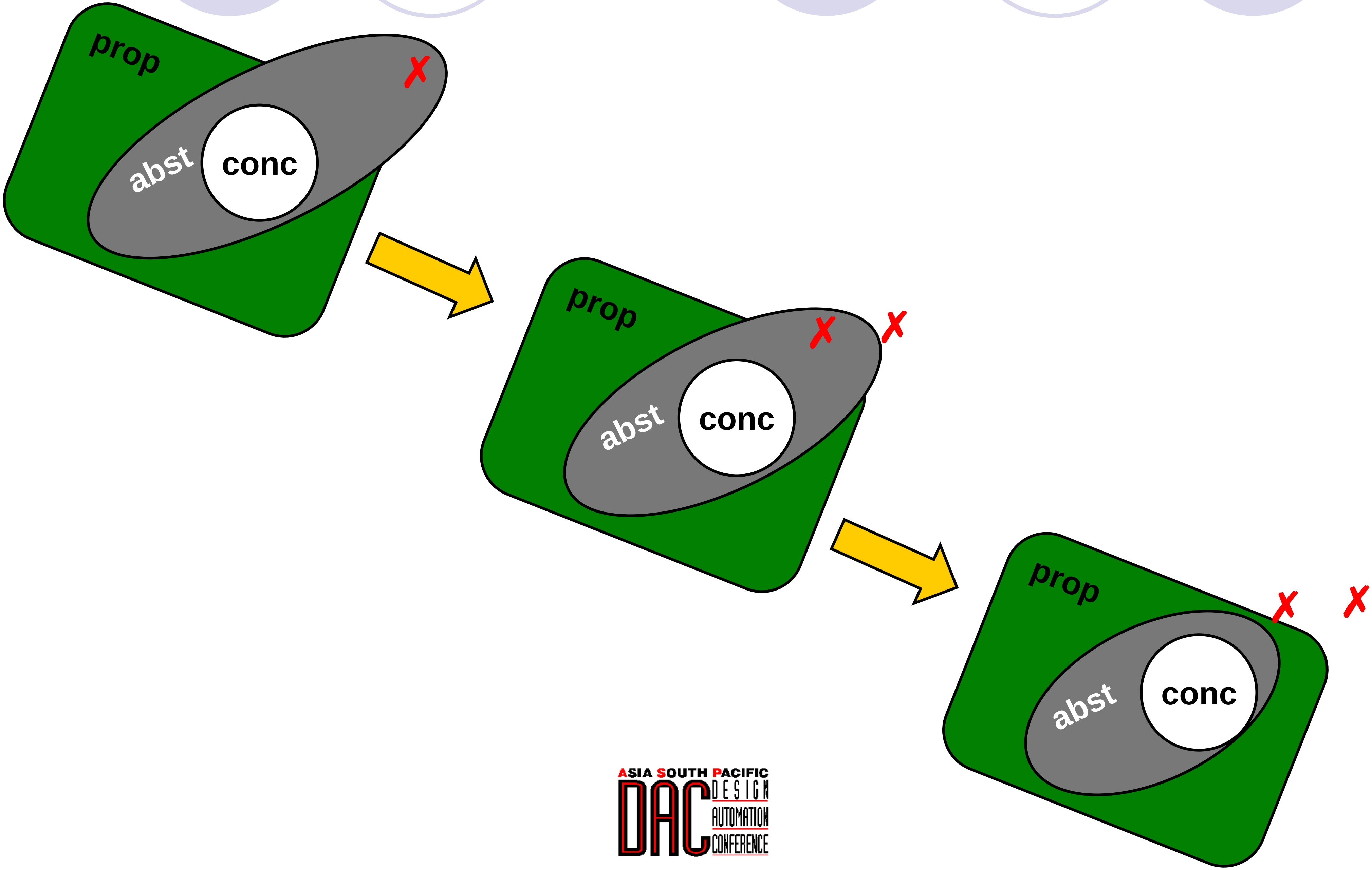
CEGAR with Enhanced Refinement



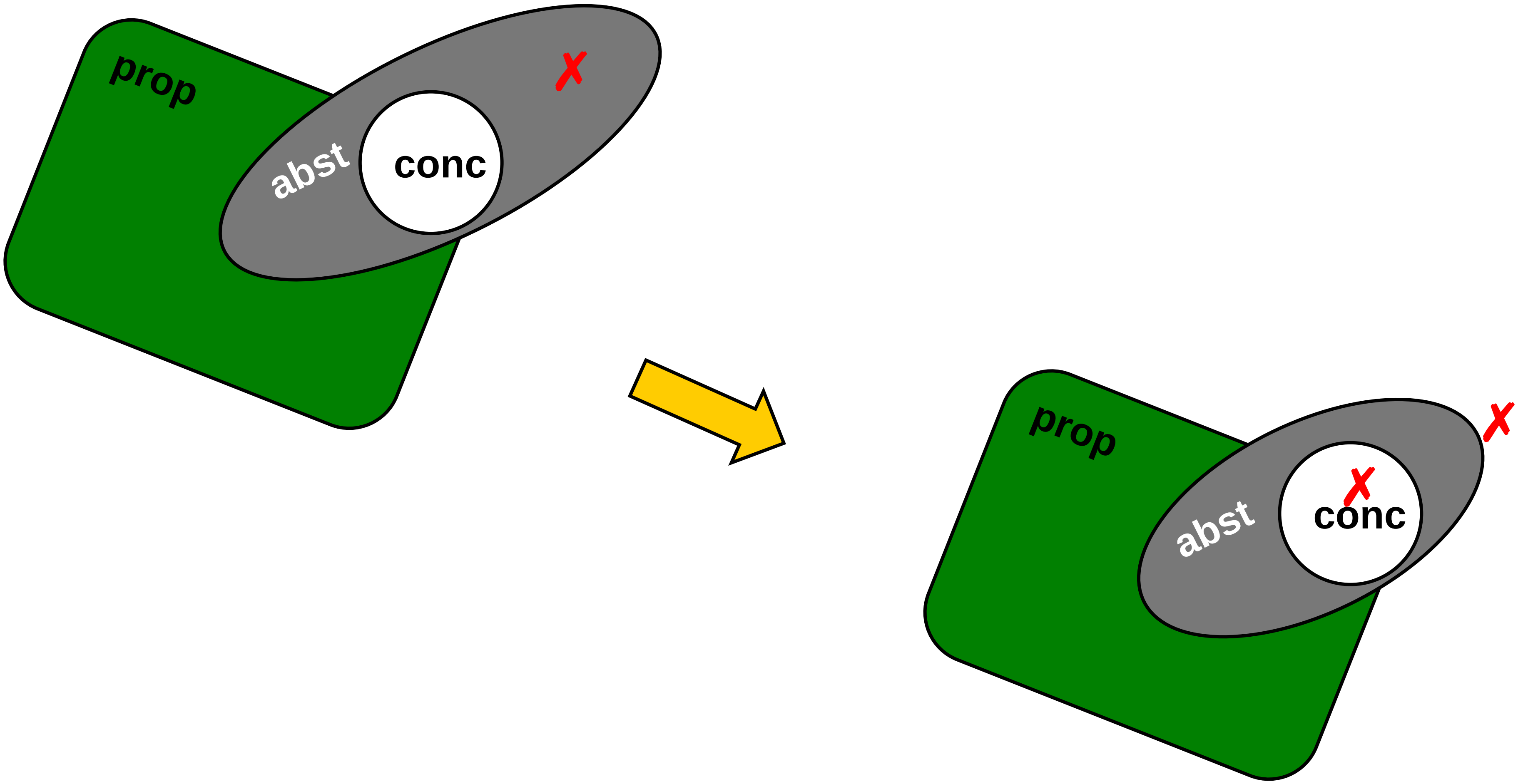
Property Satisfied by Abstract Model



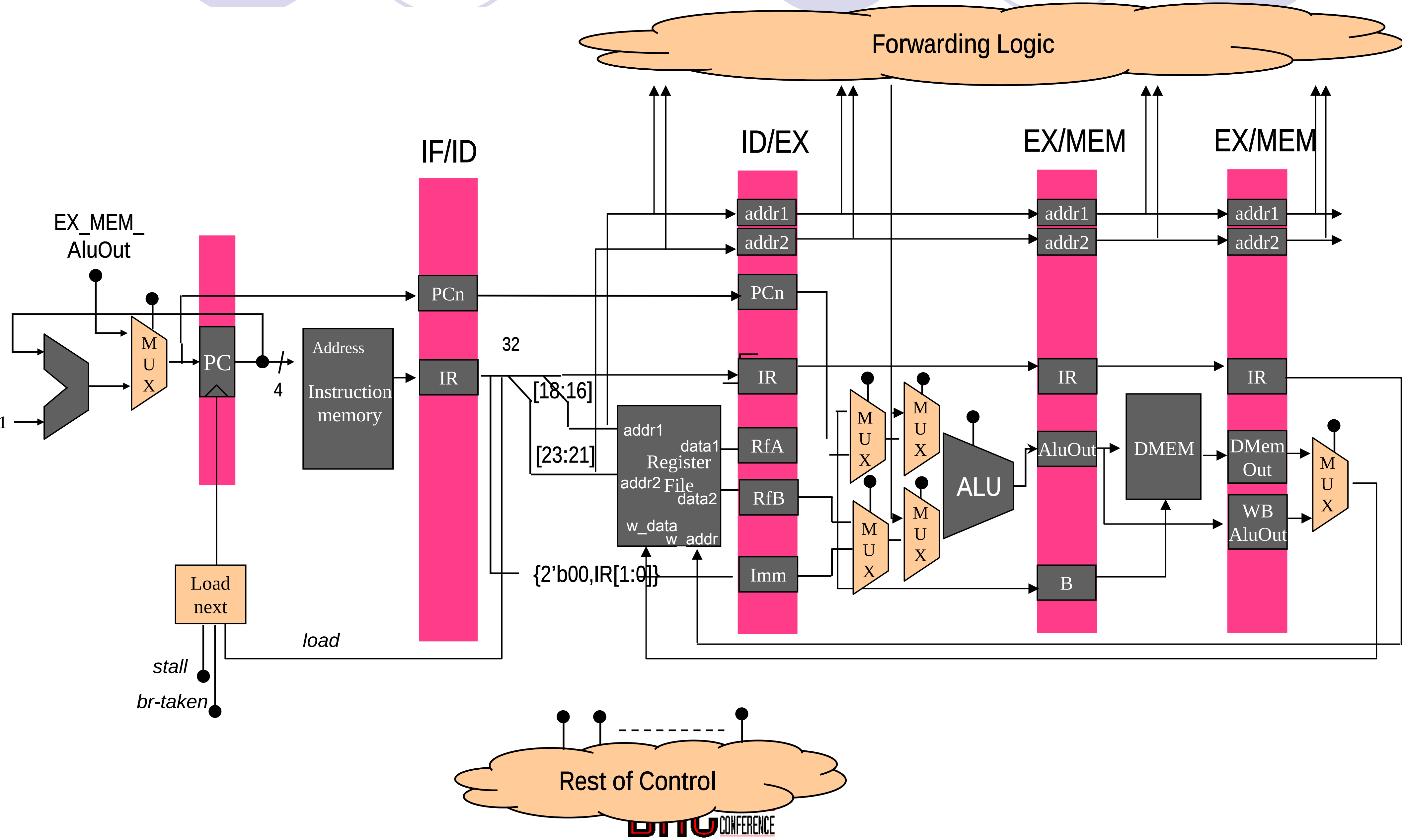
Property Violated by Abstract Model but Satisfied by Concrete Model



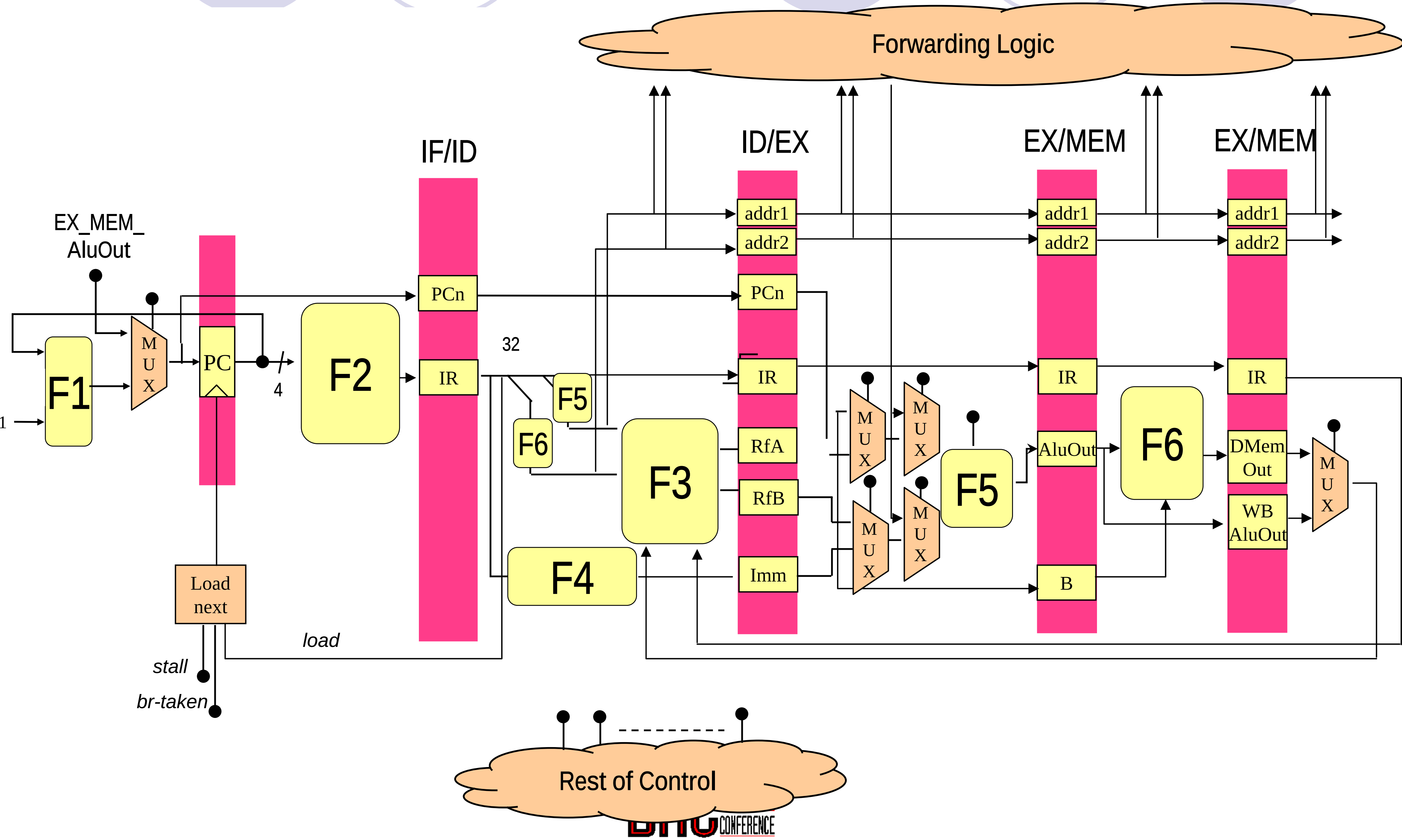
Property Violated by both Abstract and Concrete Models



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;
```

$$
\begin{aligned}
&conc(a,b,c,d,e,f,l,m,p) = \\
&\quad (m = a[3]) \wedge \\
&\quad (l = a[0]) \wedge \\
&\quad (m \wedge (c = a \gg 1) \vee \neg m \wedge (c = a)) \wedge \\
&\quad (l \wedge (d = b \gg 2) \vee \neg l \wedge (d = c)) \wedge \\
&\quad (m \wedge (e = a) \vee \neg m \wedge (e = a \gg 1)) \wedge \\
&\quad (l \wedge (f = \{2'b00, b[3:2]\}) \vee \neg l \wedge (f = e)) \wedge \\
&\quad (p = \neg(a = 0) \vee (d = f))
\end{aligned}
$$

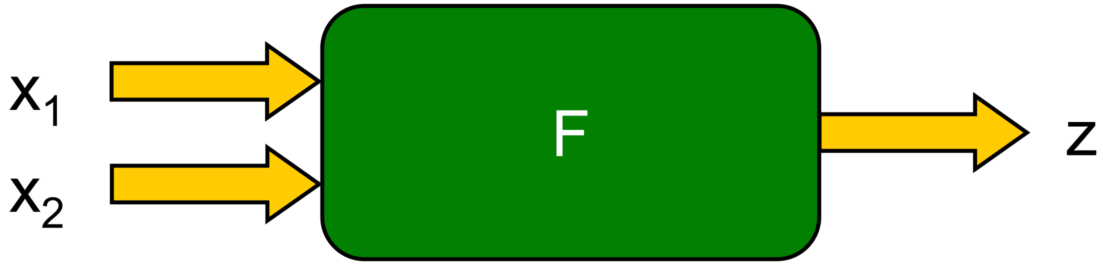
Running Example

$$\begin{aligned}
&conc(a,b,c,d,e,f,l,m,p) = \\
&\quad (m = a[3]) \wedge \\
&\quad (l = a[0]) \wedge \\
&\quad (m \wedge (c = a \gg 1) \vee \neg m \wedge (c = a)) \wedge \\
&\quad (l \wedge (d = b \gg 2) \vee \neg l \wedge (d = c)) \wedge \\
&\quad (m \wedge (e = a) \vee \neg m \wedge (e = a \gg 1)) \wedge \\
&\quad (l \wedge (f = \{2'b00, b[3:2]\}) \vee \neg l \wedge (f = e)) \wedge \\
&\quad (p = \neg(a = 0) \vee (d = f))
\end{aligned}$$

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

Functional Consistency Constraints

Functional Consistency



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

1^{st} Iteration: Counterexample

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

Functional Consistency Constraints

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

Functional Consistency Constraints

1^{st} Iteration: Localize Counterexample

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

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

1^{st} Iteration: Generalize Counterexample

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

Functional Consistency Constraints

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

1^{st} Iteration: Minimal Abstract Explanation

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

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

1^{st} Iteration: Minimal Concrete Explanations

$$
\begin{aligned}
&\mathrm{conc}(a,b,c,d,e,f,l,m,p) = \\
&\quad (m = a[3]) \wedge \\
&\quad (l = a[0]) \wedge \\
&\quad (m \wedge (c = a \gg 1) \vee \neg m \wedge (c = a)) \wedge \\
&\quad (l \wedge (d = b \gg 2) \vee \neg l \wedge (d = c)) \wedge \\
&\quad (m \wedge (e = a) \vee \neg m \wedge (e = a \gg 1)) \wedge \\
&\quad (l \wedge (f = \{2'b00, b[3:2]\}) \vee \neg l \wedge (f = e)) \wedge \\
&\quad (p = \neg(a = 0) \vee (d = f))
\end{aligned}
$$

$$
\begin{aligned}
\mathrm{viol}_1 &= (a = 0) \wedge (a[0] = 1) \\
\mathrm{viol}_2 &= b \gg 2 \neq \{2'b00, b[3:2]\}
\end{aligned}
$$

2^{nd} Iteration: Counterexample

$\text{abst}(a,b,c,d,e,f,l,m,s,t,u,p,zero) =$

$(m = EX1(a)) \wedge$

$(l = EX2(a)) \wedge$

$(s = SR1(a,\mathbf{succ}(zero))) \wedge$

$(t = SR2(b,\mathbf{succ}(\mathbf{succ}(zero)))) \wedge$

$(u = CT1(zero,EX3(b))) \wedge$

$(c = \mathbf{ite}(m,s,a)) \wedge$

$(d = \mathbf{ite}(l,t,c)) \wedge$

$(e = \mathbf{ite}(m,a,s)) \wedge$

$(f = \mathbf{ite}(l,u,e)) \wedge$

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

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

Functional Consistency Constraints

$\text{abst}(a,b,c,d,e,f,l,m,s,t,u,p,zero) =$

$(1 = EX1(0)) \wedge$

$(0 = EX2(0)) \wedge$

$(8 = SR1(0,\mathbf{succ}(zero))) \wedge$

$(3 = SR2(16,\mathbf{succ}(\mathbf{succ}(zero)))) \wedge$

$(3 = CT1(zero,EX3(16))) \wedge$

$(8 = \mathbf{ite}(1,8,0)) \wedge$

$(8 = \mathbf{ite}(0,3,8)) \wedge$

$(0 = \mathbf{ite}(1,0,8)) \wedge$

$(0 = \mathbf{ite}(0,3,0)) \wedge$

$(0 = \neg(0 = 0) \vee (8 = 0)) \wedge$

$\neg((0 = 0) \wedge (0 = 1)) \wedge \neg(3 \neq 3)$

Functional Consistency Constraints

2^{nd} Iteration: Localize Counterexample

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

Functional Consistency Constraints

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

Functional Consistency Constraints

2^{nd} Iteration: Generalize Counterexample

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

Functional Consistency Constraints

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

2^{nd} Iteration: Minimal Abstract Explanation

$\mathrm{abst}(a,b,c,d,e,f,l,m,s,t,u,p,zero) =$

$(m = EX1(a)) \wedge$

$(l = EX2(a)) \wedge$

$(s = SR1(a, \mathbf{succ}(zero))) \wedge$

$(t = SR2(b, \mathbf{succ}(\mathbf{succ}(zero)))) \wedge$

$(u = CT1(zero, EX3(b))) \wedge$

$(c = \mathbf{ite}(m,s,a)) \wedge$

$(d = \mathbf{ite}(l,t,c)) \wedge$

$(e = \mathbf{ite}(m,a,s)) \wedge$

$(f = \mathbf{ite}(l,u,e)) \wedge$

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

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

Functional Consistency Constraints

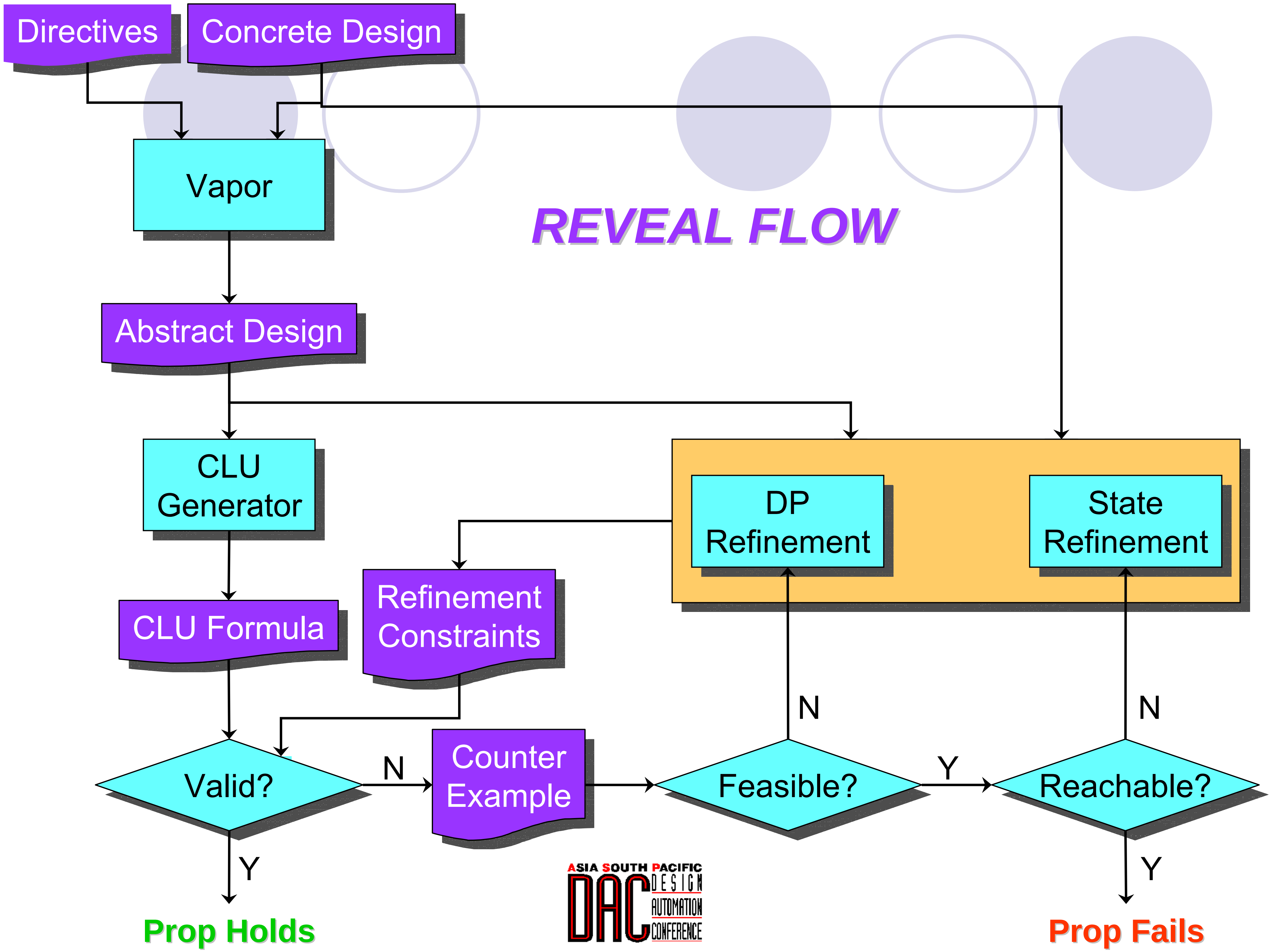
$(a = 0) \wedge$
$(l = 0) \wedge$
$(t = u) \wedge$
$(a \neq s)$

SOUTH PACIFIC DESIGN AUTOMATION CONFERENCE

2^{nd} Iteration: Minimal Concrete Explanations

$$
\begin{aligned}
&\mathrm{conc}(a,b,c,d,e,f,l,m,p) = \\
&\quad (m = a[3]) \wedge \\
&\quad (l = a[0]) \wedge \\
&\quad (m \wedge (c = a \gg 1) \vee \neg m \wedge (c = a)) \wedge \\
&\quad (l \wedge (d = b \gg 2) \vee \neg l \wedge (d = c)) \wedge \\
&\quad (m \wedge (e = a) \vee \neg m \wedge (e = a \gg 1)) \wedge \\
&\quad (l \wedge (f = \{2'b00, b[3:2]\}) \vee \neg l \wedge (f = e)) \wedge \\
&\quad (p = \neg(a = 0) \vee (d = f))
\end{aligned}
$$

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



REVEAL FLOW
Directives
Concrete Design
Vapor
Abstract Design
CLU Generator
CLU Formula
Refinement Constraints
DP Refinement
State Refinement
Valid?
N
Counter Example
Feasible?
Y
Reachable?
N
N
Y
Y
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”:

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

$$\Downarrow$$

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

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