CS 510/08

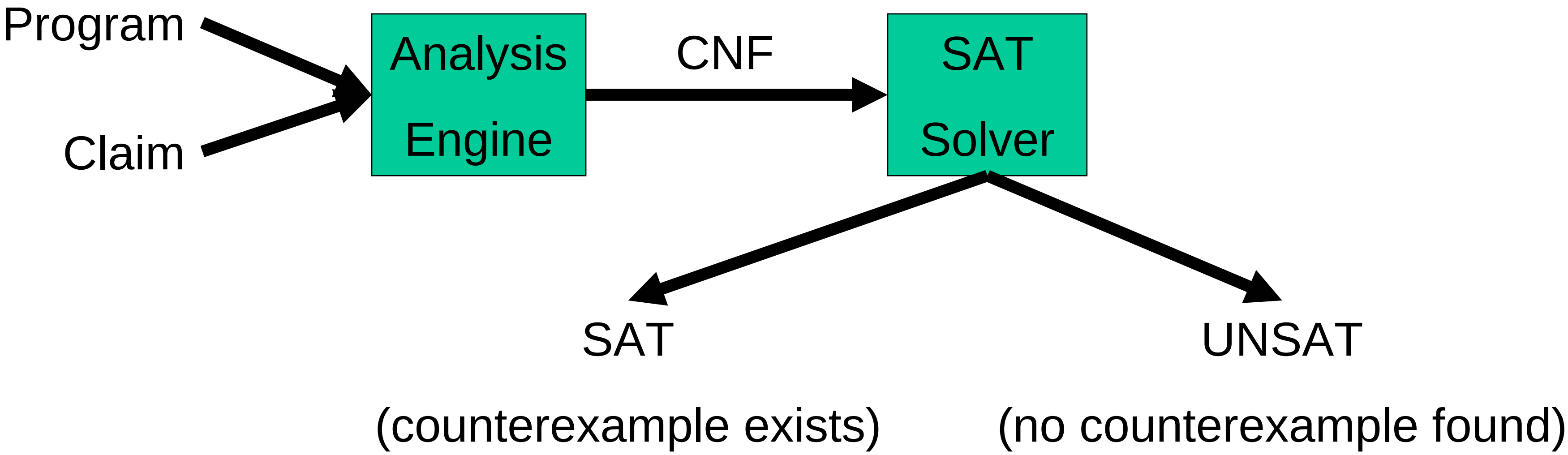
Model Checking Java Programs (Java PathFinder)

Slides partially compiled from the NASA JavaPathFinder project and E. Clarke's course material

Java PathFinder

- JPF is an explicit state software model checker for Java bytecode
  - JPF is a Java virtual machine that executes your program not just once (like a normal VM), but theoretically in all possible ways, checking for property violations like deadlocks or unhandled exceptions along all potential execution paths.

Symbolic Model Checking



Explicit State Model Checking

- The program is indeed executing
  - jpf <your class> <parameters>
    - Very similar to "java <your class> <parameters>
  - Execute in a way that all possible scenarios are explored
    - Thread interleaving
    - Undeterministic values (random values)
  - Concrete input is provided
  - A state is indeed a concrete state, consisting of
    - Concrete values in heap/stack memory

JPF Status

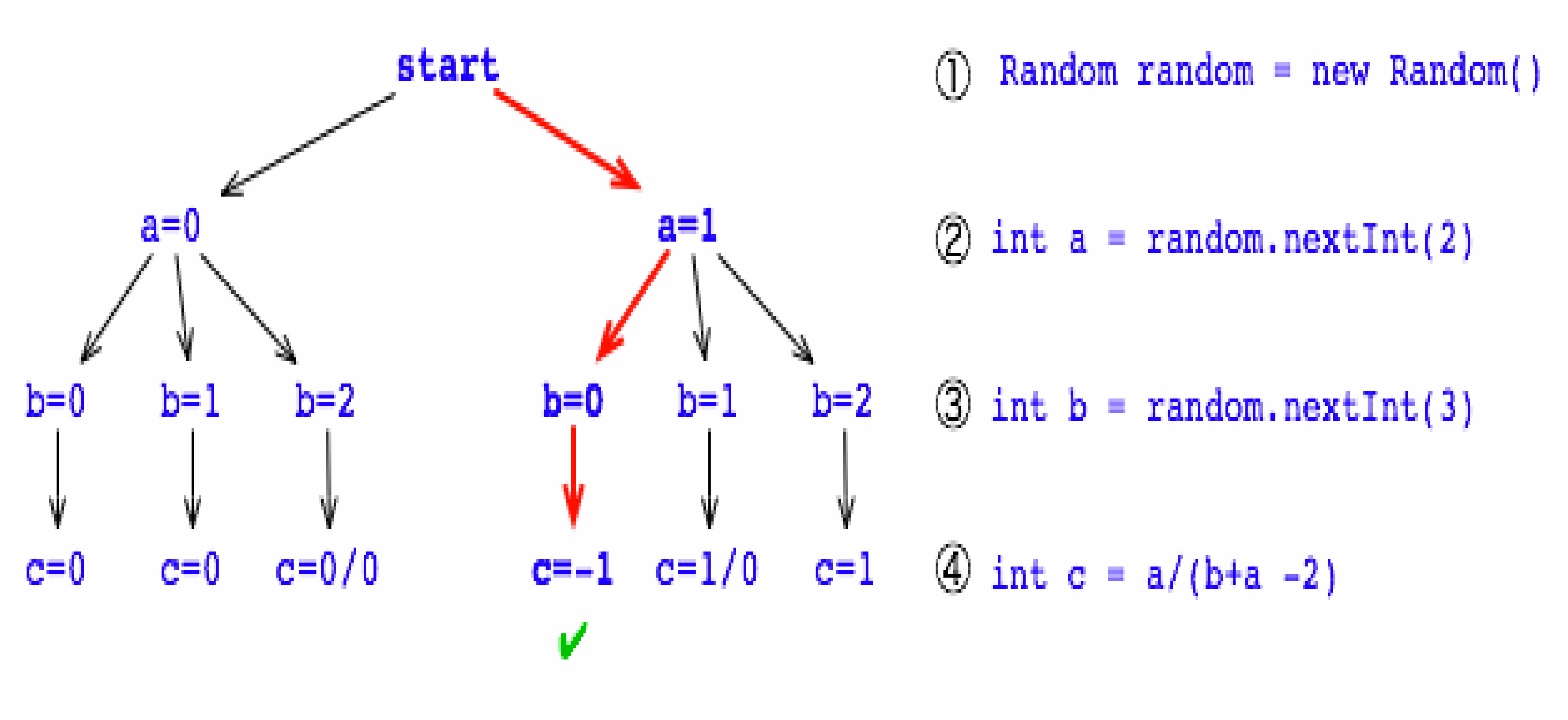
- developed at the Robust Software Engineering Group at NASA Ames Research Center
- currently in it's fourth development cycle
  - v1: Spin/Promela translator - 1999
  - v2: backtrackable, state matching JVM - 2000
  - v3: extension infrastructure (listeners, MJI) - 2004
  - v4: symbolic execution, choice generators - 4Q 2005
- open sourced since 04/2005 under NOSA 1.3 license: <javapathfinder.sourceforge.net>
- it's a first: no NASA system development hosted on public site before
- 11100 downloads since publication 04/2005

An Example

```
import java.util.Random;

public class Rand {
     public static void main (String[] args) {
          Random random = new Random(42);        //  (1)

          int a = random.nextInt(2);             //  (2)
          System.out.println("a=" + a);

          //... lots of code here

          int b = random.nextInt(3);             //  (3)
          System.out.println("  b=" + b);

          int c = a/(b+a -2);                    //  (4)
          System.out.println("    c=" + c);
     }
}
```

```
> java Rand
a=1
  b=0
    c=-1
>
```

An Example (cont.)

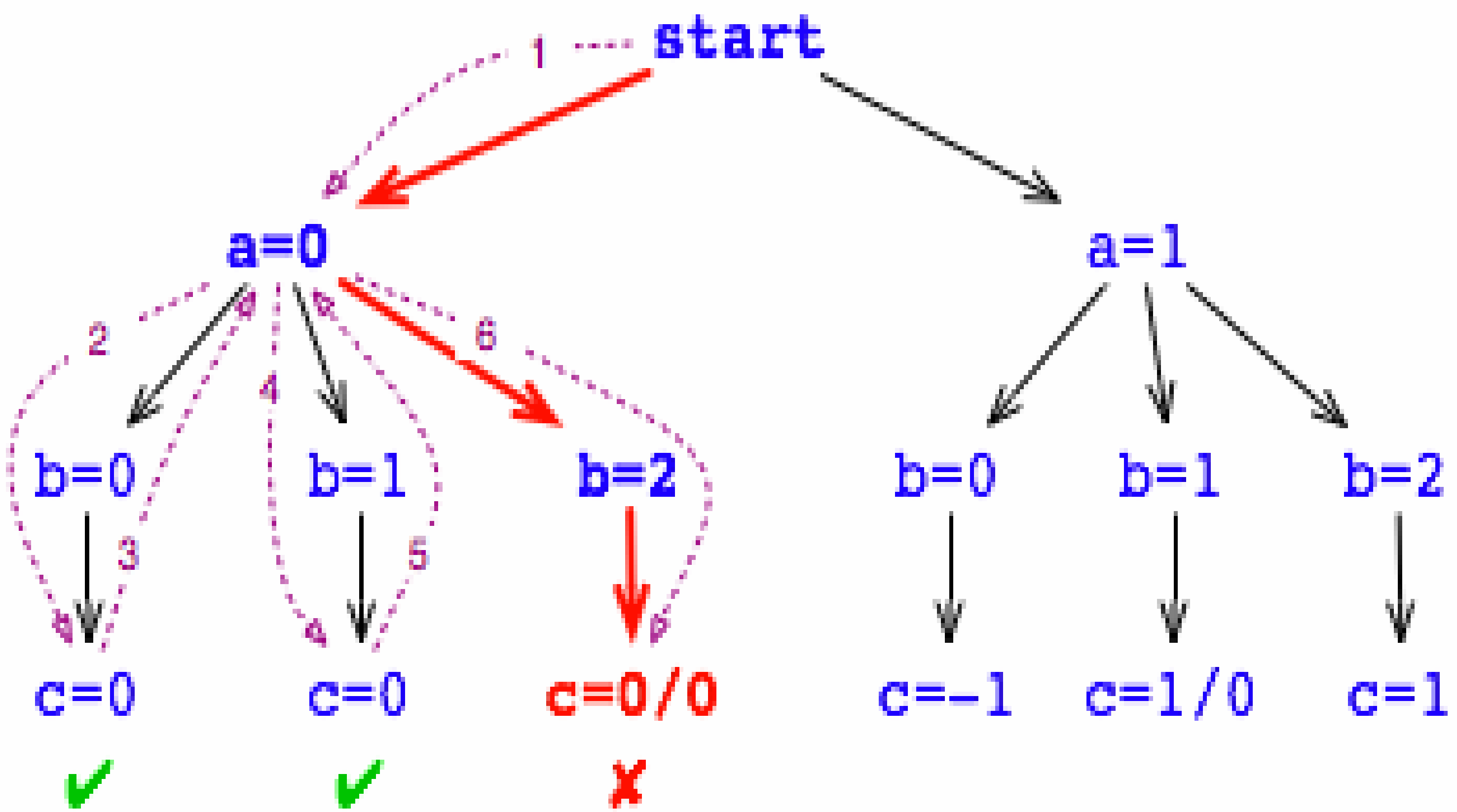


- **One execution corresponds to one path.**

```
> bin/jpf Rand
```

```
JavaPathfinder v4.1 - (C) 1999-2007 RIACS/NASA Ames Research Center
====================================================== system under test
application: /Users/pcmehlitz/tmp/Rand.java

====================================================== search started: 5/23/07 11:48 PM
a=1
  b=0
    c=-1

====================================================== results
no errors detected

====================================================== search finished: 5/23/07 11:48 PM
>
```

```
> bin/jpf +vm.enumerate_random=true Rand
JavaPathfinder v4.1 - (C) 1999-2007 RIACS/NASA Ames Research Center
====================================================== system under test
application: /Users/pcmehlitz/tmp/Rand.java

====================================================== search started: 5/23/07 11:49 PM
a=0
  b=0
    c=0
  b=1
    c=0
  b=2

====================================================== error #1
gov.nasa.jpf.jvm.NoUncaughtExceptionsProperty
java.lang.ArithmeticException: division by zero
        at Rand.main(Rand.java:15)
....
>
```



- **JPF explores multiple possible executions GIVEN THE SAME CONCRETE INPUT**

Another Example

```
public class Racer implements Runnable {

     int d = 42;

     public void run () {
          doSomething(1000);                    // (1)
          d = 0;                                // (2)
     }

     public static void main (String[] args){
          Racer racer = new Racer();
          Thread t = new Thread(racer);
          t.start();

          doSomething(1000);                    // (3)
          int c = 420 / racer.d;                // (4)
          System.out.println(c);
     }

     static void doSomething (int n) {
          // not very interesting..
          try { Thread.sleep(n); } catch (InterruptedException ix) {}
     }
}
```

```
> bin/jpf Racer
JavaPathfinder v4.1 - (C) 1999-2007 RIACS/NASA Ames Research Center
==================================================== system under
application: /Users/pcmehlitz/tmp/Racer.java

==================================================== search starte
10
10

==================================================== error #1
gov.nasa.jpf.jvm.NoUncaughtExceptionsProperty
java.lang.ArithmeticException: division by zero
        at Racer.main(Racer.java:20)

==================================================== trace #1
---------------------------------------------------- transition #0 thread: 0
gov.nasa.jpf.jvm.choice.ThreadChoiceFromSet {>main}
      [282 insn w/o sources]
  Racer.java:15                  : Racer racer = new Racer();
  Racer.java:1                   : public class Racer implements Runnable {
      [1 insn w/o sources]
  Racer.java:3                   : int d = 42;
  Racer.java:15                  : Racer racer = new Racer();
  Racer.java:16                  : Thread t = new Thread(racer);
      [51 insn w/o sources]
  Racer.java:16                  : Thread t = new Thread(racer);
  Racer.java:17                  : t.start();
---------------------------------------------------- transition #1 thread: 0
```

```
------------------------------------------------------ transition #1 thread: 0
gov.nasa.jpf.jvm.choice.ThreadChoiceFromSet {>main,Thread-0}
  Racer.java:17                  : t.start();
  Racer.java:19                  : doSomething(1000);                    // (3)
  Racer.java:6                   : try { Thread.sleep(n); } catch (InterruptedException ix) {}
      [2 insn w/o sources]
  Racer.java:6                   : try { Thread.sleep(n); } catch (InterruptedException ix) {}
  Racer.java:7                   : }
  Racer.java:20                  : int c = 420 / racer.d;                // (4)
------------------------------------------------------ transition #2 thread: 1
gov.nasa.jpf.jvm.choice.ThreadChoiceFromSet {main,>Thread-0}
  Racer.java:10                  : doSomething(1000);                    // (1)
  Racer.java:6                   : try { Thread.sleep(n); } catch (InterruptedException ix) {}
      [2 insn w/o sources]
  Racer.java:6                   : try { Thread.sleep(n); } catch (InterruptedException ix) {}
  Racer.java:7                   : }
  Racer.java:11                  : d = 0;                                // (2)
------------------------------------------------------ transition #3 thread: 1
gov.nasa.jpf.jvm.choice.ThreadChoiceFromSet {main,>Thread-0}
  Racer.java:11                  : d = 0;                                // (2)
  Racer.java:12                  : }
------------------------------------------------------ transition #4 thread: 0
gov.nasa.jpf.jvm.choice.ThreadChoiceFromSet {>main}
  Racer.java:20                  : int c = 420 / racer.d;                // (4)

====================================================== search finished: 5/24/07 12:32 AM
>
```

Two Essential Capabilities

- Backtracking
  - Means that JPF can restore previous execution states, to see if there are unexplored choices left.
    - While this is theoretically can be achieved by re-executing the program from the beginning, backtracking is a much more efficient mechanism if state storage is optimized.
- State matching
  - JPF checks every new state if it already has seen an equal one, in which case there is no use to continue along the current execution path, and JPF can backtrack to the nearest non-explored non-deterministic choice
    - Head and thread-stack snapshots.

The Challenge

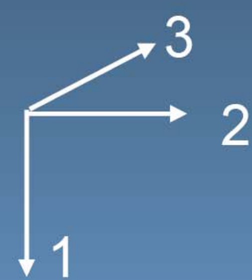
```
int   x,  y,  r;
int  *p, *q, *z;
int **a;

thread_1(void)        /* initialize p, q, and r */
{
    p = &x;
    q = &y;
    z = &r;
}
thread_2(void)        /* swap contents of x and y */
{
    r = *p;
    *p = *q;
    *q = r;
}
thread_3(void)        /* access z via a and p */
{
    a = &p;
    *a = z;
    **a = 12;
}
```

3 asynchronous threads
accessing shared data
3 statements each
how many test runs are needed to
check that no data corruption can occur?

The Challenge (cont.)

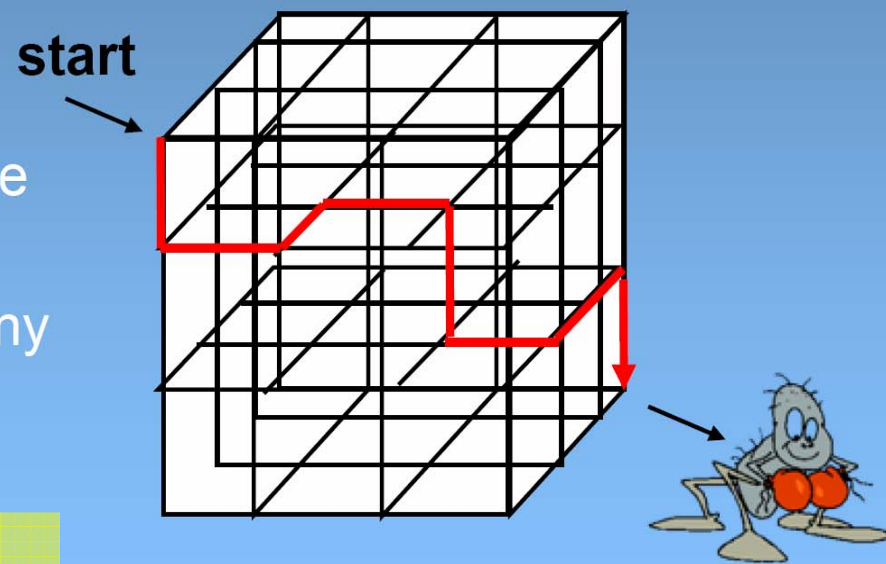
cs 510 Software Engineering

- the number of possible thread interleavings is...



$$\frac{9!}{6!.3!} \cdot \frac{6!}{3!.3!} \cdot \frac{3!}{3!} =$$ 1,680 possible executions

placing 3 sets of 3 tokens in 9 slots



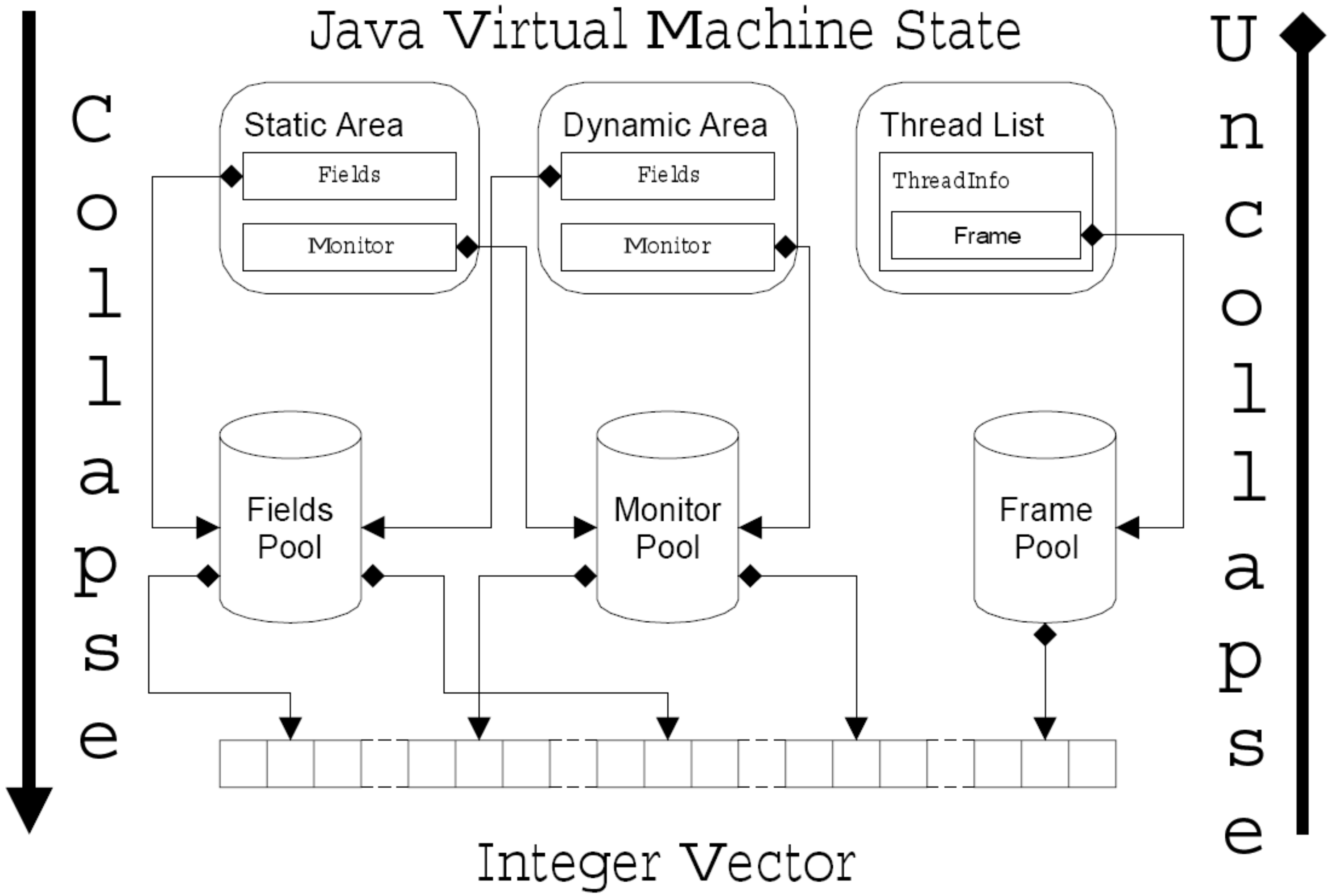
- are all these executions okay?
- can we check them all? should we check them all?
- in classic system testing, how many would normally be checked?

State Explosion!!

JPF's Solution

- Configurable search strategy
  - Directing the search so that defects can be found quicker
    - A debugging tool instead of a "proof" system.
  - User can easily develop his/her own strategy
- Reducing state storage
  - State collapsing
    - Premise: only a tiny part of the state is changed upon each transaction. (e.g. a single stack frame)
    - Dividing a state into components, use hashtable to index a specific value for a component.

Solution- State Collapsing



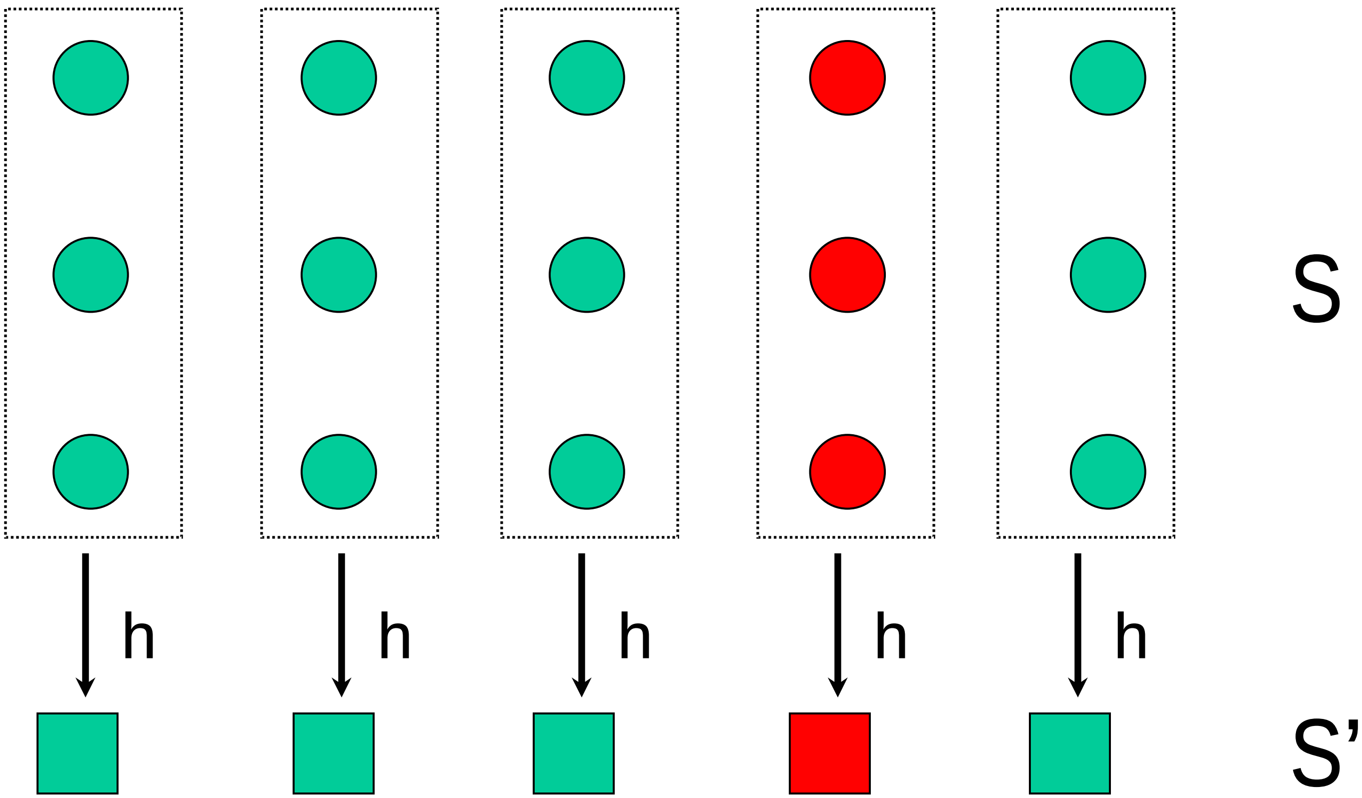
Solution (3) – State Reduction

- Orthogonal (our focus)
  - **State Abstraction**
  - **Partial Order Reduction**
- JPF specific
  - **Host VM Execution**
    - Delegate execution to the underlying host VM (no state tracking).
  - **Heuristic Choice Generators**

Abstraction

- Eliminate details irrelevant to the property
- Obtain simple finite models sufficient to verify the property
  - E.g., Infinite state $ #Finite state approximation
- Disadvantage
  - Loss of Precision: False positives/negatives

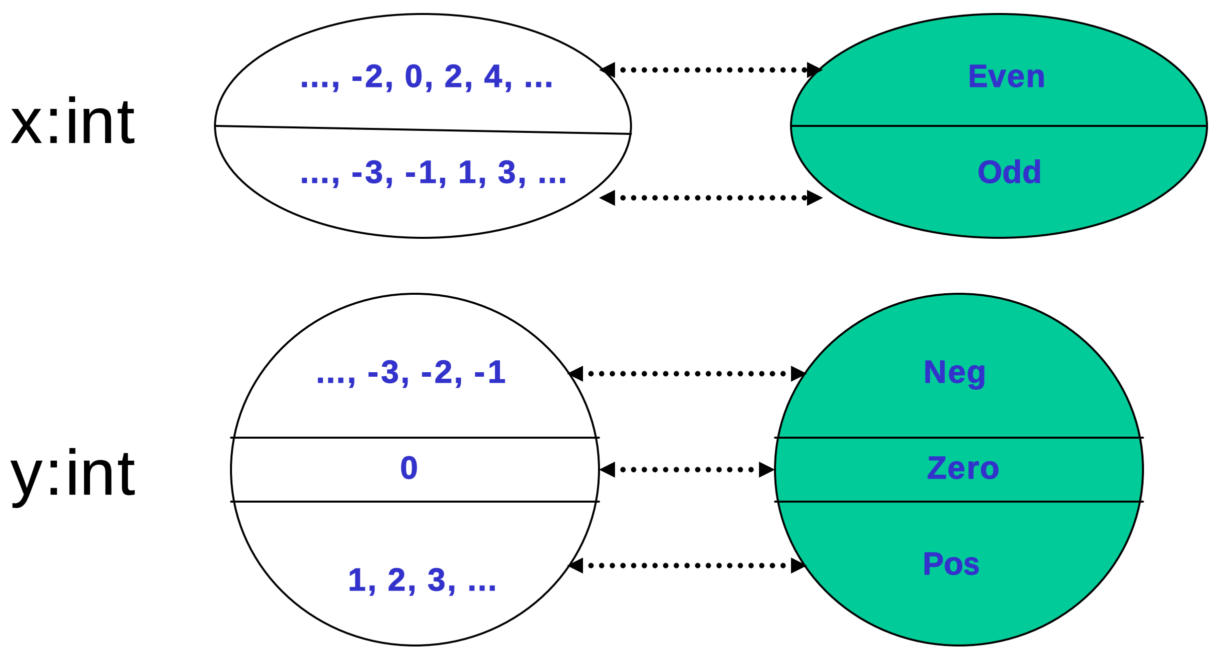
Data Abstraction



Abstraction Function h : from S to S'

Data Abstraction Example

- Abstraction proceeds component-wise, where variables are components



Data Abstraction Example

- Partition concrete variables into visible(V) and invisible(I) variables.
- The abstract model consists of V variables. I variables are existentially quantified out.
- The abstraction function maps each state to its projection over V.

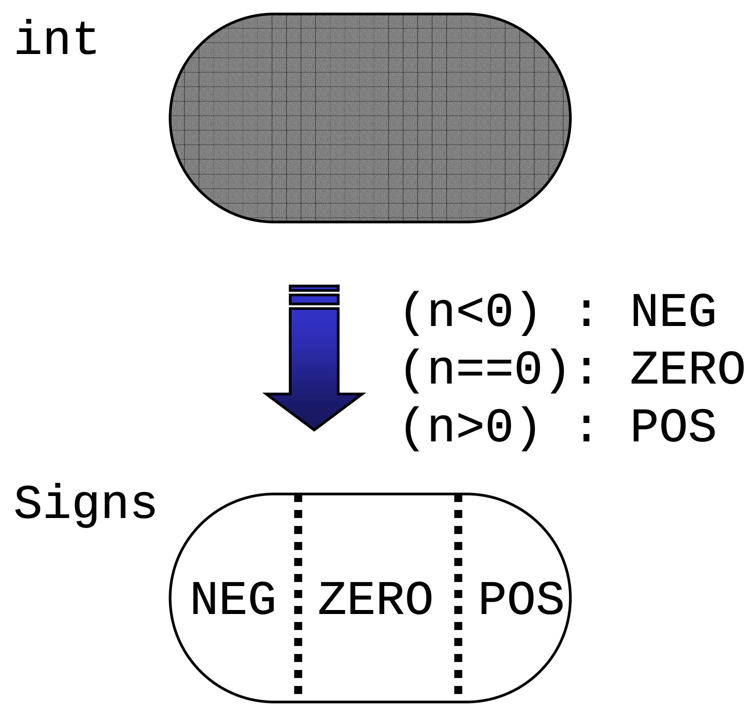
Data Type Abstraction

Code

```
int x = 0;
if (x == 0)
  x = x + 1;
```

```
Signs x = ZERO;
if (Signs.eq(x,ZERO))
  x = Signs.add(x,POS);
```

Abstract Data domain



How do we Abstract Behaviors?

- Abstract domain *A*
  - Abstract concrete values to those in *A*
- Then compute transitions in the abstract domain
  - Over-approximations: Add extra behaviors
  - Under-approximations: Remove actual behaviors

Guarantees from Abstraction

Assume M' is an abstraction of M

- Strong Preservation:
  - P holds in M' iff P holds in M
- Weak Preservation:
  - P holds in M' implies P holds in M

Discussion of Abstraction

- Formalizing Abstraction/Refinement
  - Homomorphic Abstractions
  - Abstract Interpretation Theory
- Applications
  - Software – e.g., Predicate Abstraction

Building an Abstraction

- Computing Abstract Domain
- Computing Abstract Transitions

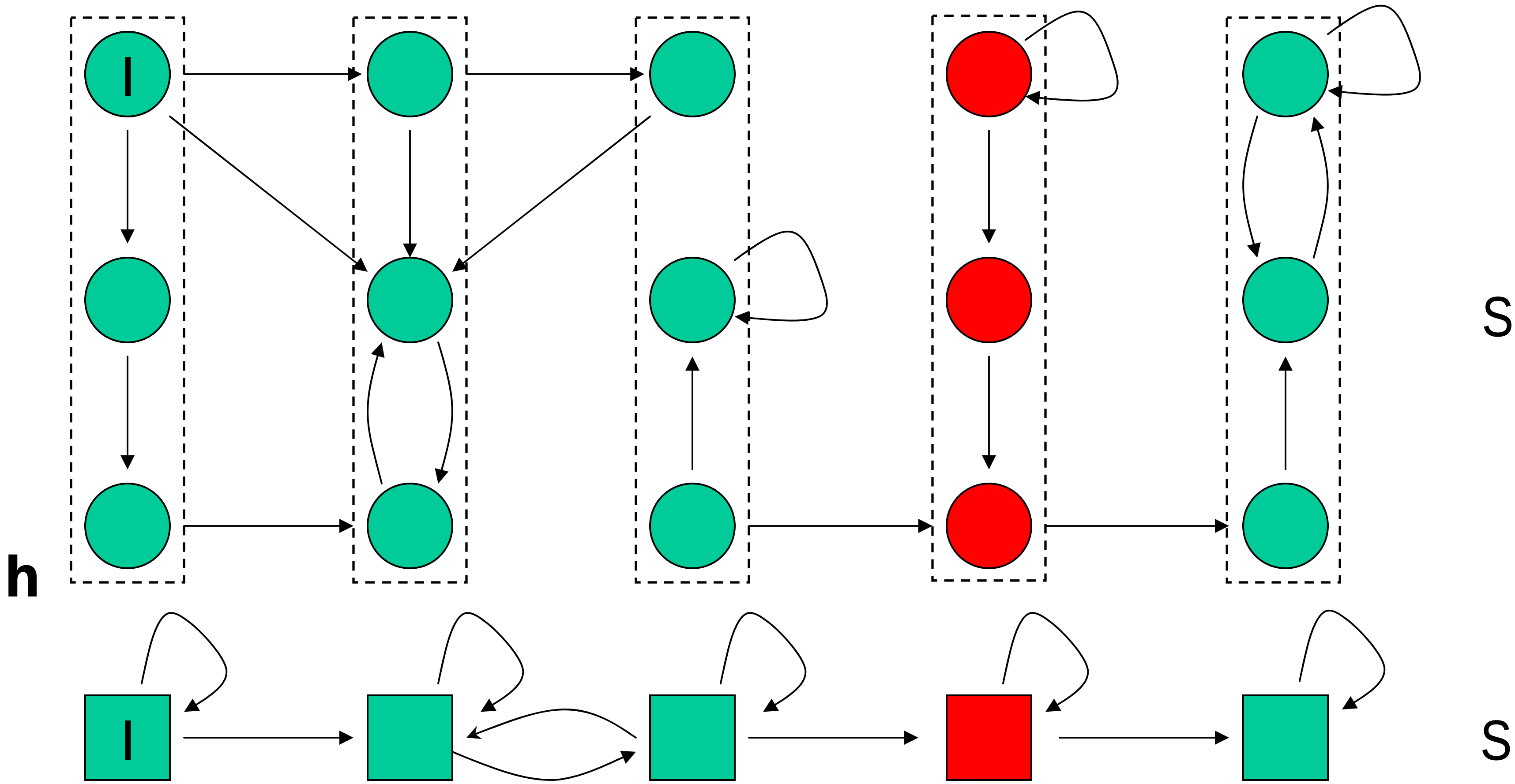
Homomorphisms

- Clarke et. al.- '94, '00
- Concrete States S, Abstract states S'
- Abstraction function (Homomorphism)
  - h: S $ S'
  - Induces a partition on S equal to size of S'

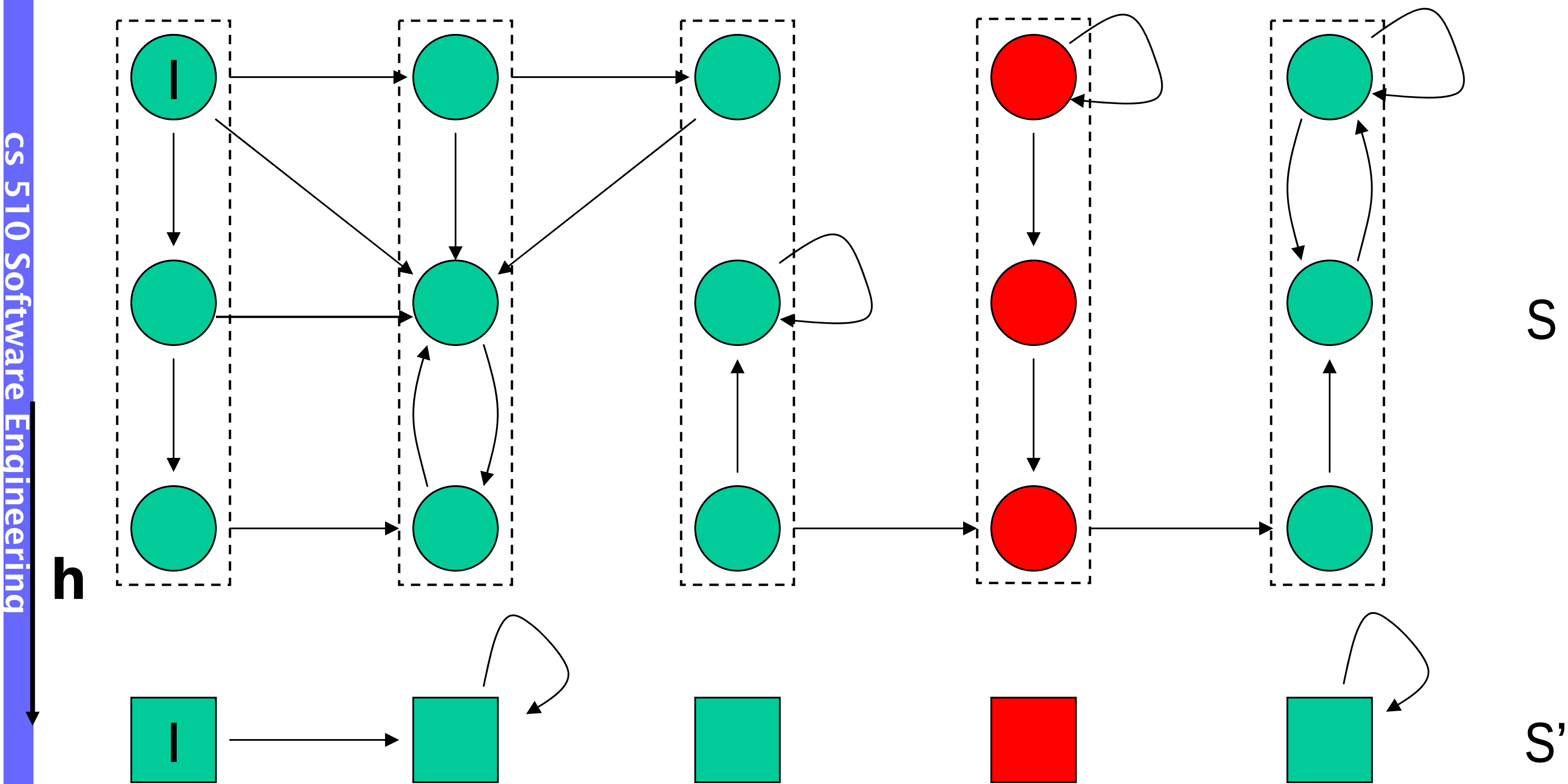
Existential/Universal Abstractions

- Existential
  - Make a transition from an abstract state if **at least one** corresponding concrete state has the transition.
  - Abstract model M' simulates concrete model M
- Universal
  - Make a transition from an abstract state if **all** the corresponding concrete states have the transition.

Existential Abstraction (Over-approximation)

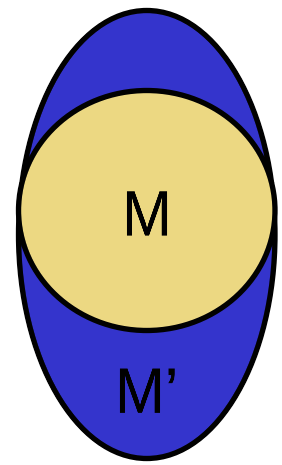


Universal Abstraction (Under-Approximation)



Guarantees from Exist. Abstraction

- Let φ be a *hold-for-all-paths* property
- M' existentially abstracts M, so M ` M'



- Preservation Theorem

$$M' \models \varphi \rightarrow M \models \varphi$$

- Converse does not hold

$$M' \not\models \varphi \not\rightarrow M \not\models \varphi$$

- $M' \not\models \varphi$: counterexample may be spurious

Guarantees from Univ. Abstraction

- Let φ be a existential-quantified property and M simulates M’

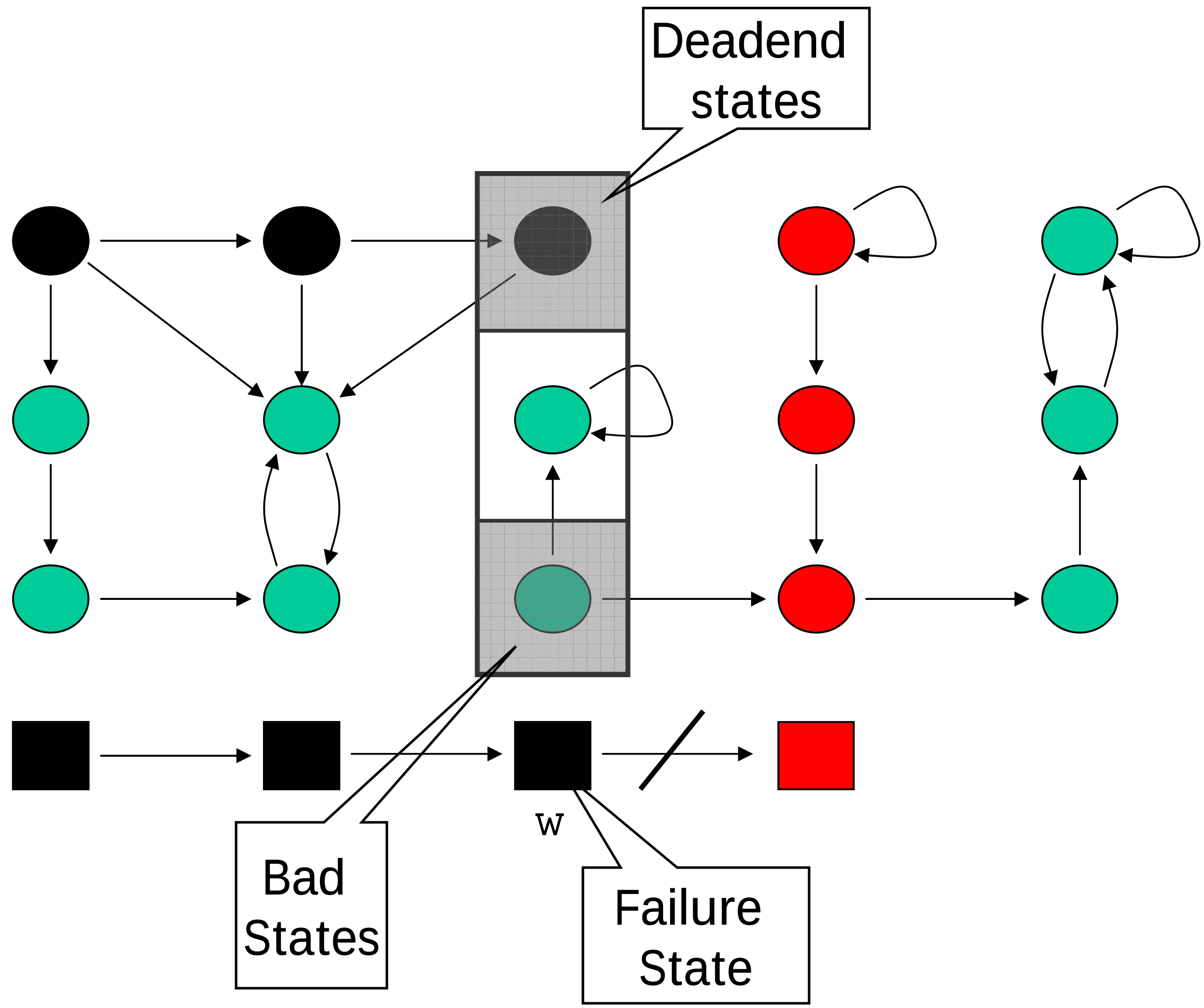
- **Preservation Theorem**

$$M' \; 5 \; \varphi \;\rightarrow\; M \; 5 \; \varphi$$

- Converse does not hold

$$M \nvDash \varphi \;\not\rightarrow\; M' \nvDash \varphi$$

Why spurious counterexample?

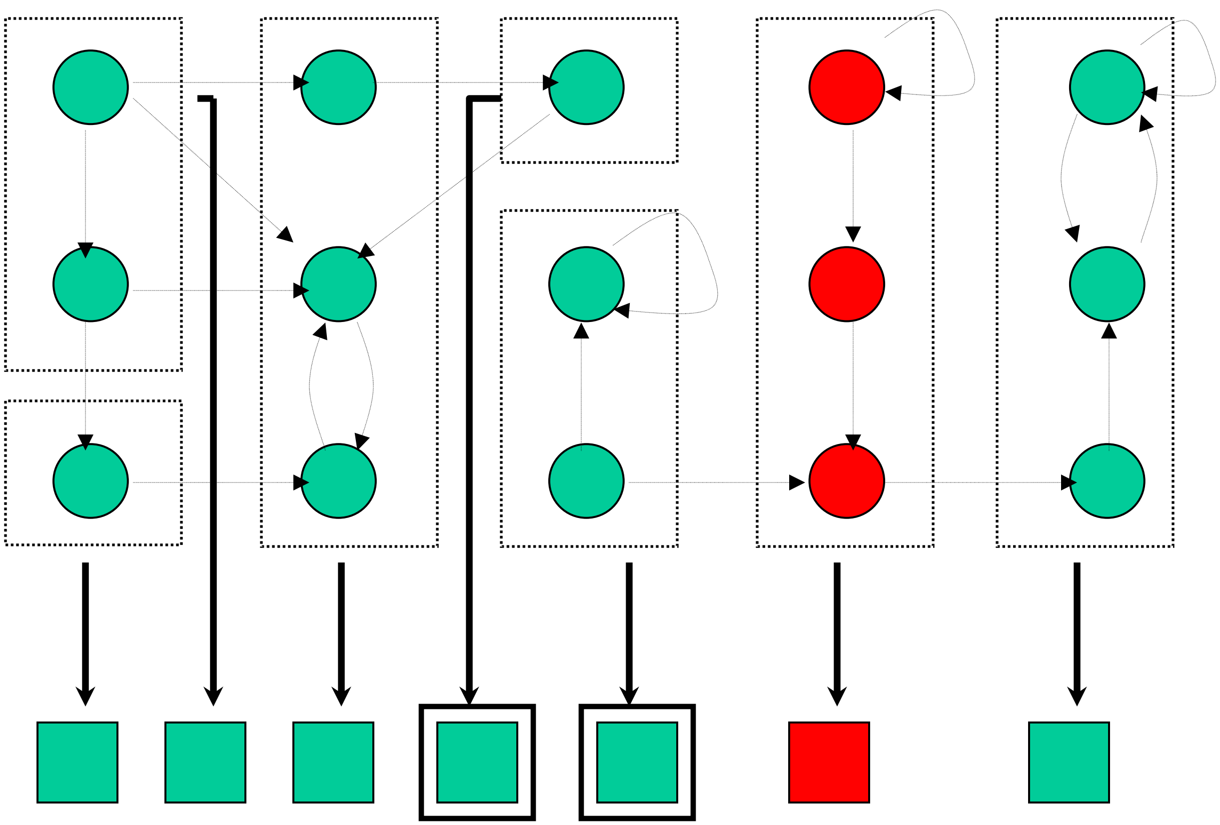


Refinement

- Problem: Deadend and Bad States are in the same abstract state.
- Solution: Refine abstraction function.
- The sets of Deadend and Bad states should be separated into different abstract states.

Refinement

h’

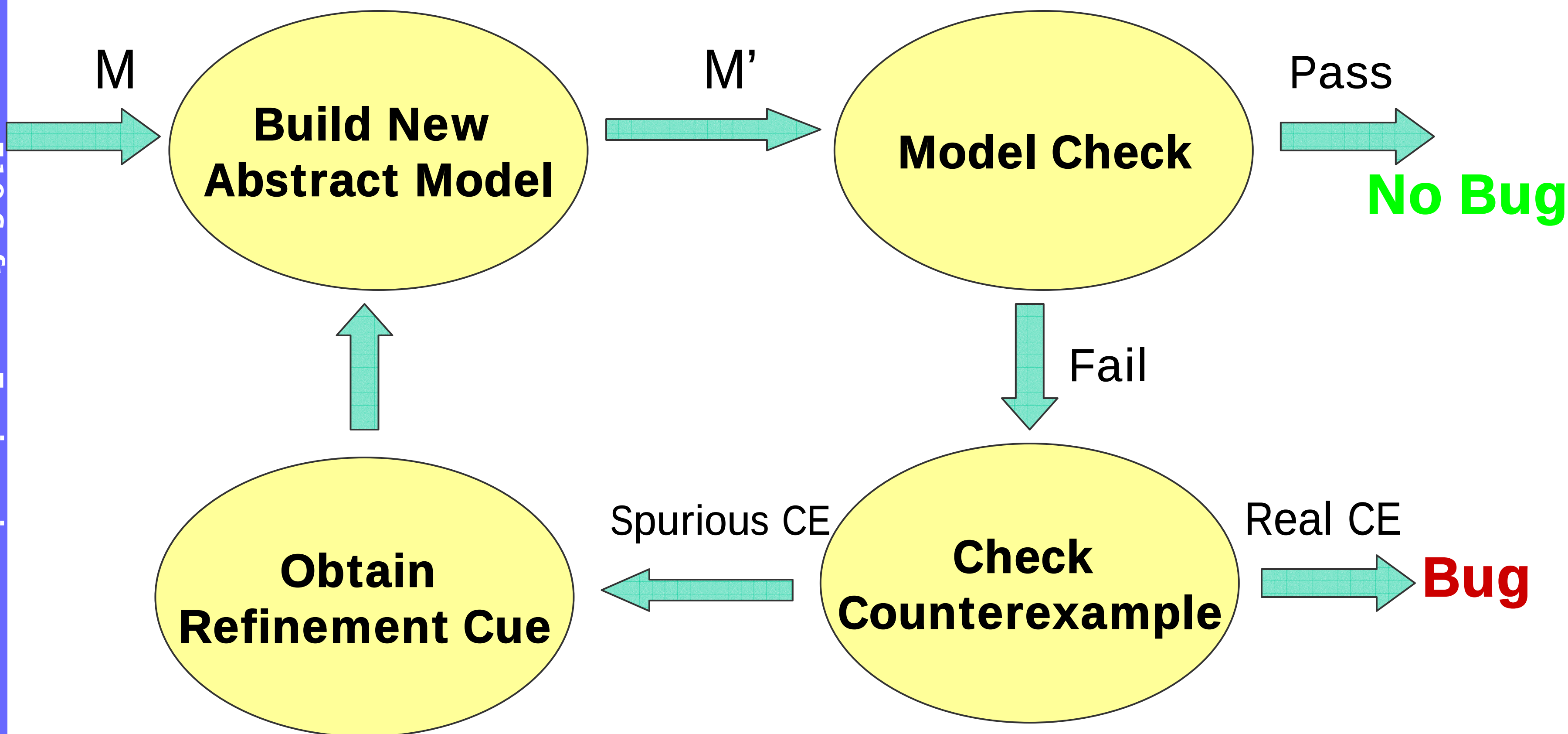


Refinement : h’

Automated Abstraction/Refinement

- Good abstractions are hard to obtain
  - Automate both Abstraction and Refinement processes
- Counterexample-Guided AR (CEGAR)
  - Build an abstract model M'
  - Model check property P, M' ¶ P?
  - If M' ¶ P, then M ¶ P by Preservation Theorem
  - Otherwise, check if Counterexample (CE) is spurious
  - Refine abstract state space using CE analysis results
  - Repeat

Counterexample-Guided Abstraction-Refinement (CEGAR)



Predicate Abstraction

- Extract a finite state model from an infinite state system
- Used to prove assertions or safety properties
- Successfully applied for verification of C programs
  - SLAM (used in windows device driver verification)
  - MAGIC, BLAST, F-Soft

Example for Predicate Abstraction

```
int main() {
  int i;

  i=0;

  while(even(i))
    i++;
}
```

+

$p_1 \Leftrightarrow i=0$
$p_2 \Leftrightarrow \text{even}(i)$

=

```
void main() {
  bool p1, p2;

  p1=TRUE;
  p2=TRUE;

  while(p2)
  {
    p1=p1?FALSE:nondet();
    p2=!p2;
  }
}
```

C program **Predicates** **Boolean program**

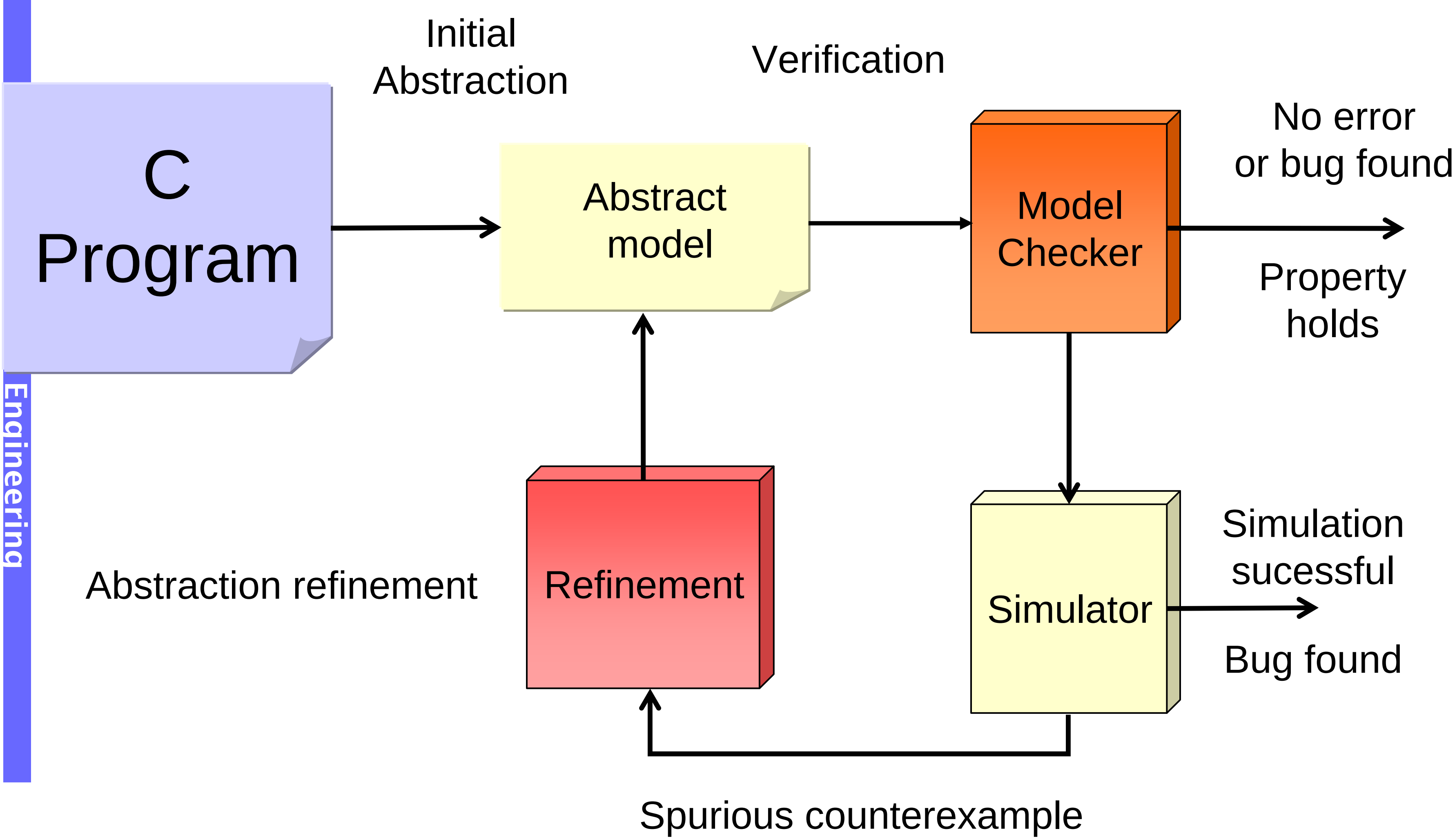
[Graf, Saidi '97]

[Ball, Rajamani '01]

Computing Predicate Abstraction

- How to get predicates for checking a given property?
- How do we compute the abstraction?
- Predicate Abstraction is an over-approximation
  - How to refine coarse abstractions

Counterexample Guided Abstraction Refinement loop



Abstraction

```
x = ctr;
y = ctr + 1;
if (x = i-1){
  if (y != i){
    ERROR:
  }
}
```

C program

Abstract

```
skip;
skip;
if (*){
  if (*){
    ERROR:
  }
}
```

No predicates available currently

Checking the abstract model

Is ERROR reachable?

```
1: skip;
2: skip;
3: if (*){
4:   if (*){
        ERROR:
     }
   }
```

yes

Abstract model has a path leading to error state

Does this correspond to a real bug?

```
1: skip;
2: skip;
3: if (*){
4:   if (*){
       ERROR:
     }
   }
```

```
1: x = ctr;
2: y = ctr + 1;
3: assume(x == i-1)
4: assume (y != i)
```

Concrete trace

Check using a SAT solver

Not possible

Refinement

```
1: x = ctr;
2: y = ctr + 1;
3: assume(x == i-1)
4: assume (y != i)
```

Spurious Counterexample

```
1: skip;
2: skip;
3: if (*){
4:   if (*){
          ERROR:
     }
   }
```

Initial abstraction

Refinement

```
1: x = ctr;
2: y = ctr + 1;
3: assume(x == i-1)
4: assume (y != i)
```

```
1: skip;
2: skip;
3: if (*){
4:   if (b0){
         ERROR:
     }
   }
```

boolean b0 : y != i

Refinement

```
1: x = ctr;
2: y = ctr + 1;
3: assume(x == i-1)
4: assume (y != i)
```

```
1: skip;
2: skip;
3: if (b1){
4:   if (b0){
        ERROR:
     }
   }
```

boolean b0 : y != i

boolean b1 : x== i-1

Refinement

Weakest precondition of y != i

ctr + 1 ! = i

```
1: x = ctr;
2: y = ctr + 1;
3: assume(x == i-1)
4: assume (y != i)
```

```
1: skip;
2: b0 = b2;
3: if (b1){
4:   if (b0){
        ERROR:
     }
   }
```

boolean b0 : y != i

boolean b1 : x== i-1

Refinement

boolean b2 : ctr + 1 ! = i

boolean b3: ctr == i -1

```
x = ctr;
y = ctr + 1;
assume(x == i-1)
assume (y != i)
```

```
b1 = b3;
b0 = b2;
if (b1){
  if (b0){
      ERROR:
  }
}
```

boolean b0 : y != i

boolean b1 : x== i-1

Refinement

boolean b2 : ctr + 1 ! = i

boolean b3: ctr == i -1

What about initial values of b2 and b3?

are mutually exclusive.

b2 =1, b3 = 0

b2 =0 , b3 = 1

```
b1 = b3;
b0 = b2;
if (b1){
  if (b0){
     ERROR:
   }
 }
```

So system is safe!

boolean b0 : y != i

boolean b1 : x== i-1

Tools for Predicate Abstraction of C

- SLAM at Microsoft
  - Used for verifying correct sequencing of function calls in windows device drivers
- MAGIC at CMU
  - Allows verification of concurrent C programs
  - Found bugs in MicroC OS
- BLAST at Berkeley
  - Lazy abstraction, interpolation
- SATABS at CMU
  - Computes predicate abstraction using SAT
  - Can handle pointer arithmetic, bit-vectors
- F-Soft at NEC Labs
  - Localization, register sharing