Constraint-Based Verification

Carl Pixley
Advanced Technology Group
Synopsys, Inc.

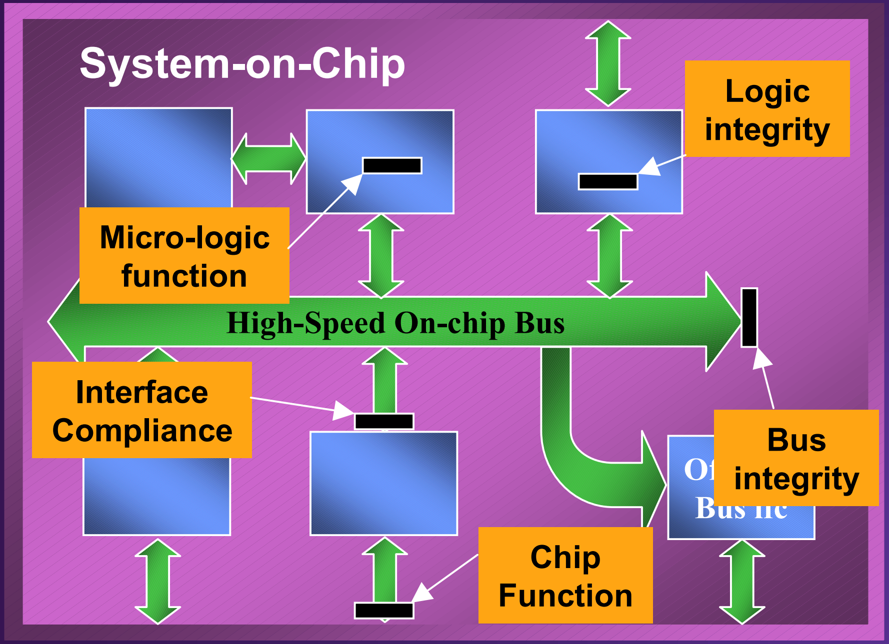
John Havlicek, Ken Albin
Motorola Inc., Austin

What is Constraint-Based Verification?

- Designers define constraints involving the inputs of their designs.
- They can immediately simulate their designs with constraints ONLY and debug wave forms. No testbench program is needed.
- Constraints and design mature incrementally.
- During integration constraints become monitors automatically. (Flipping) This supports assume/guarantee reasoning.

Constraint / Assertion-Based Methodology

Assertions (e.g., OVA, CBV) Verification



System-on-Chip

Logic integrity

Micro-logic function

High-Speed On-chip Bus

Interface Compliance

Bus integrity

Of

Bus Ifc

Chip Function

Use of Assertions

- Checking results
- Stimulus generation (Constraint assertions like SimGen)
- Proving correctness
- Measuring coverage
- Verification IP reuse

Reuse of Assertions Among Simulation, Semi-Formal, and Formal Verification

Constraint Examples

"Inputs 0, 1 & 2 are 0-1-hot"

`In0 + In1 + In2 <= 1;`

"A transaction start can only be asserted when the address state machine is in the idle state."

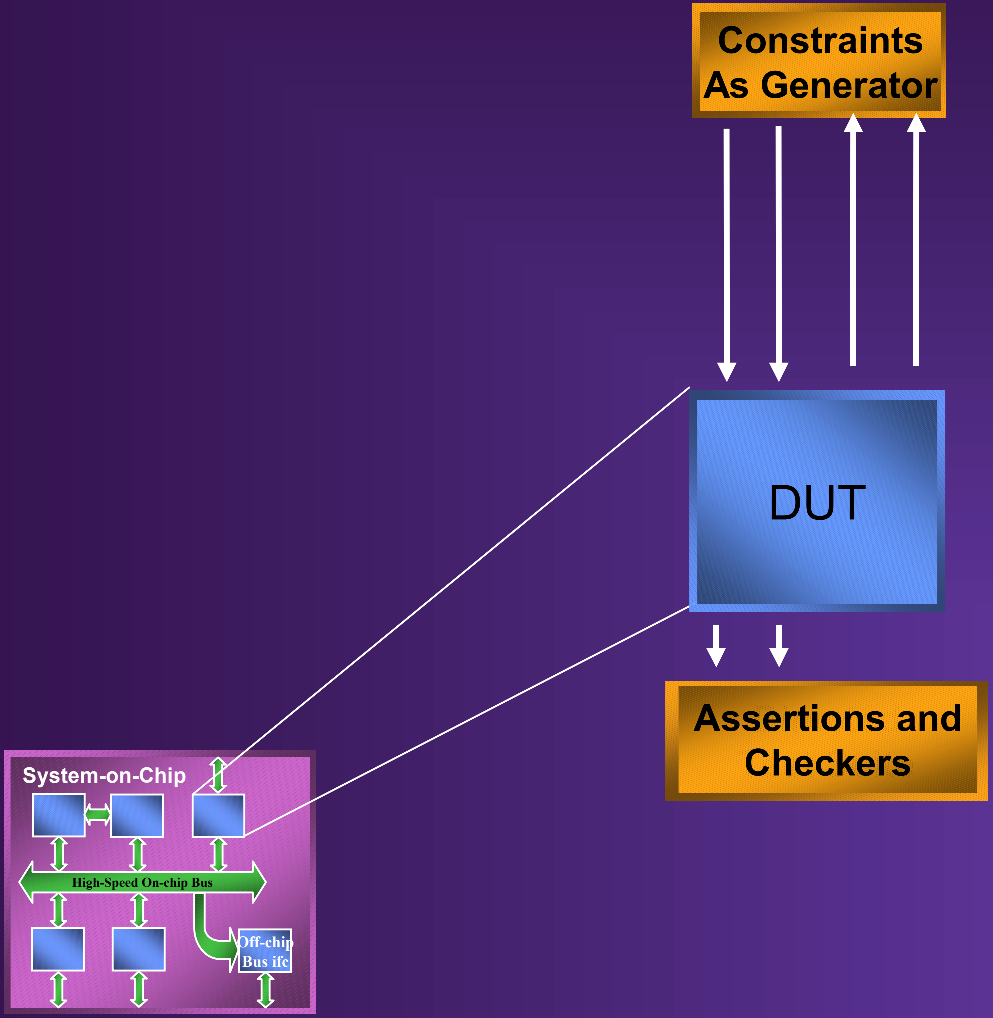
`` ts -> (addr_state = `ADDR_IDLE)); ``

Constraints are just Verilog formulas. This is **not** the CBV language. It works fine with OVA or Verilog.

Generation

In0 + In1 + In2 <= 1;

ts -> (addr_state = `ADDR_IDLE));

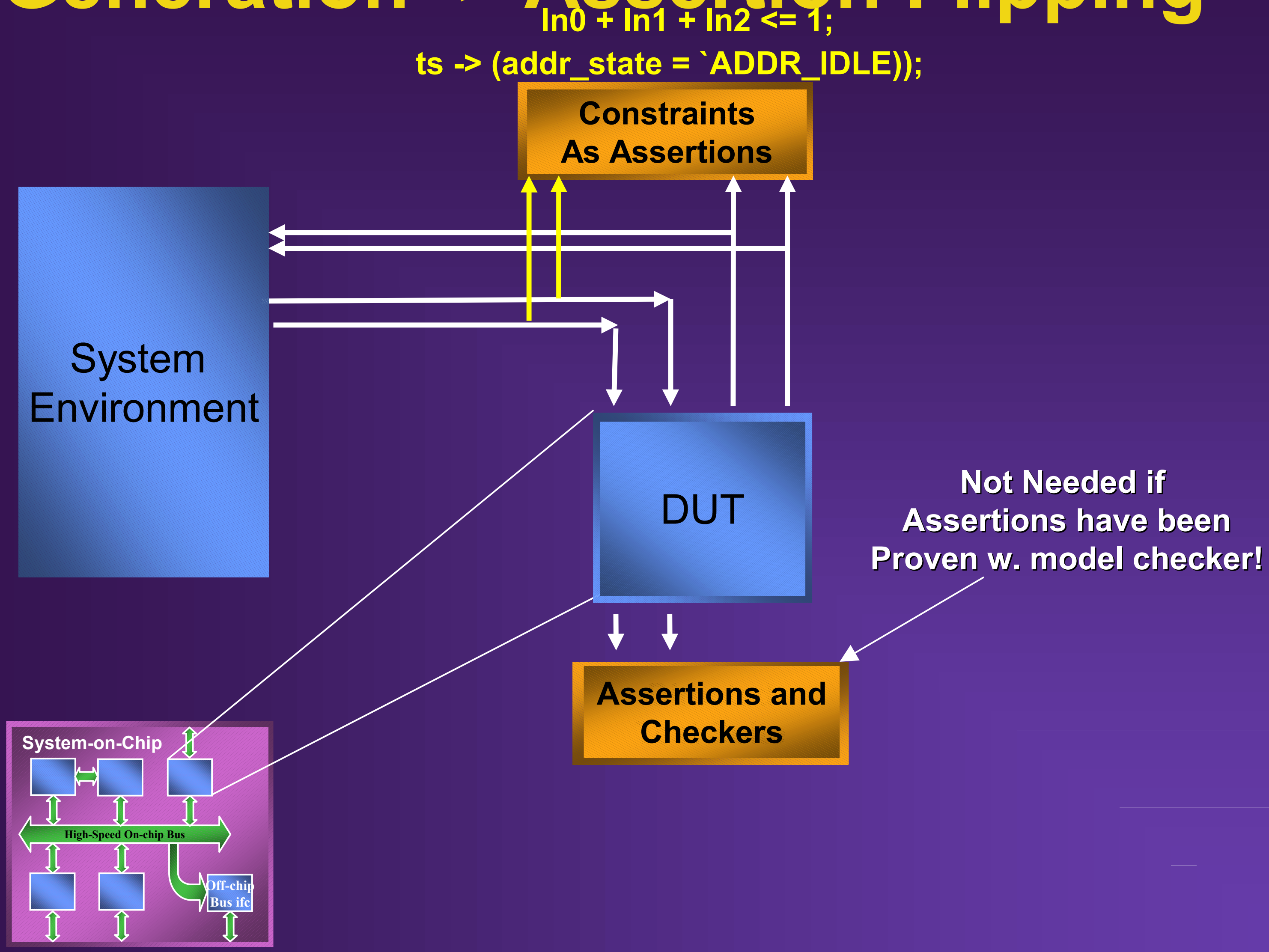


Constraints As Generator

DUT

Assertions and Checkers

Generation -> Assertion Flipping



In0 + In1 + In2 <= 1;

ts -> (addr_state = `ADDR_IDLE));

Constraints As Assertions

System Environment

DUT

Not Needed if Assertions have been Proven w. model checker!

Assertions and Checkers

Constraint-Based Verification

- **Enables early, more extensive use of assertion–based simulation at the unit level by designers!**
  - -- by lowering the effort to animate a design block and
  - by incrementally refining the logic and constraints

Constraint-Based Verification

- **Design Manager:**

"My proposal is for designers to test their logic before releasing it to the verification team. This will guarantee that we're not fighting careless/silly errors when the blocks are integrated in a system environment.

There are two reasons why I would like to follow the CBV [*SimGen*] route: 1) all the support you and your group have provided this past year and a half, and 2) I believe it would be easier for designers to use this tool than trying to learn the [conventional directed-random simulation] environment along with C++ and everything else."

Constraint-Based Verification

Low-effort, early animation of design blocks. The cost of getting started is low.

Designers don't have to write an elaborate test-bench to begin animating and debugging a block.

Because the development of environments for designs is incremental, the cost of developing constraint-based environments is amortized over time.

Constraint-Based Verification

Constraint-based verification integrates well with other, existing simulation approaches.

It can be integrated incrementally into a verification flow.

Constraints can be developed to monitor inputs in a directed or directed random approach. As constraints mature, they become simulation drivers (E.g., Automotive at Motorola).

Simulation & Formal methodology

Constraints can be used both in simulation and formal verification (model checking).

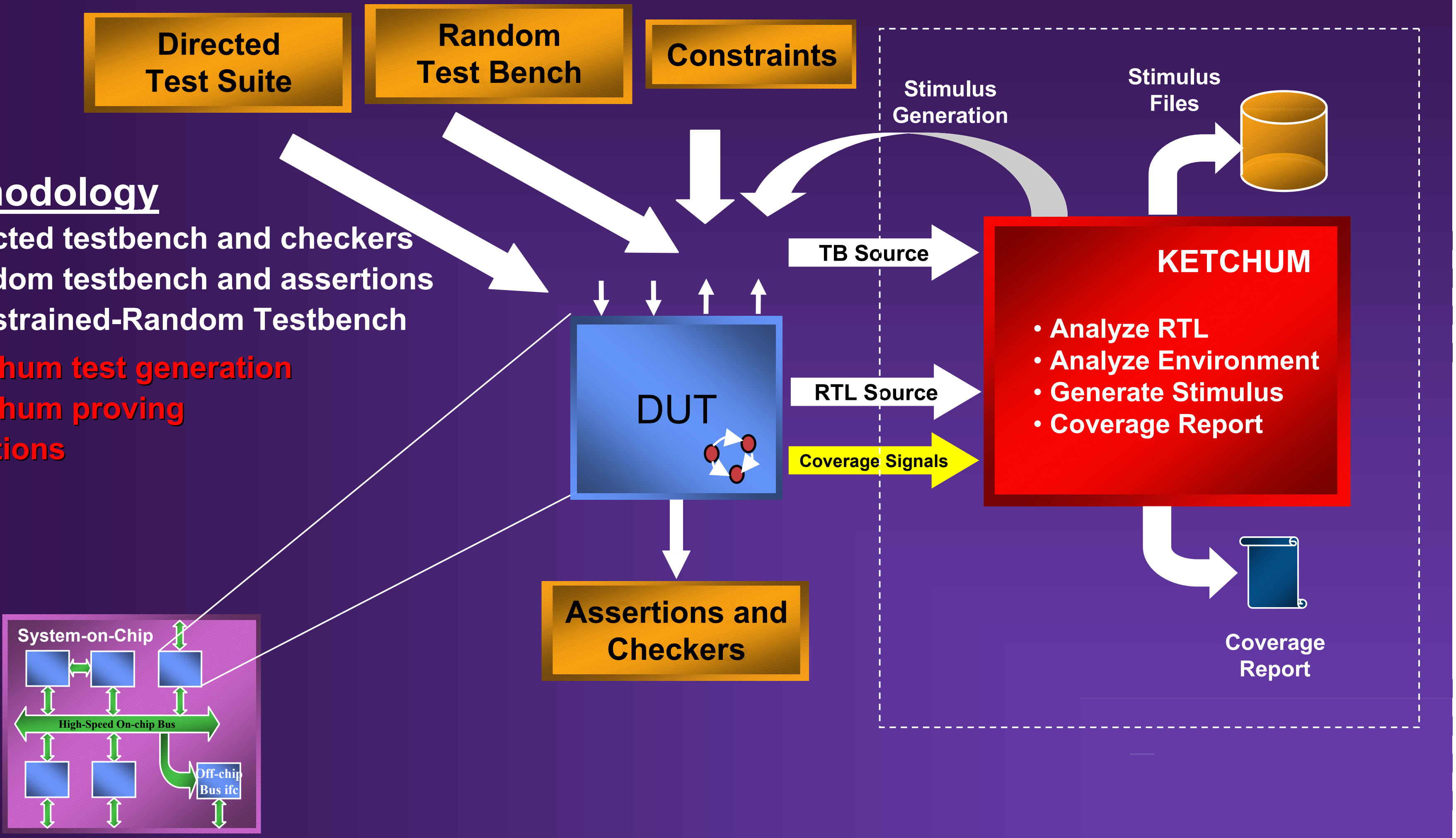
Constraint-based verification reinforces assertion-based verification (e.g., OVA – because constraints ARE assertions.

Constraint-based simulation is unexpectedly effective in finding corner cases. (See slides below.)

Ketchum Simulation & Formal Verification

Methodology

- Directed testbench and checkers
- Random testbench and assertions
- Constrained-Random Testbench
- Ketchum test generation
- Ketchum proving assertions



Constraint-Based Verification

Reuse of constraint verification IP at the SoC level

1. Constraints can be used with model checking as environments.
2. Constraint-based generators can be easily converted into checkers during system integration.

Constraint-Based Verification

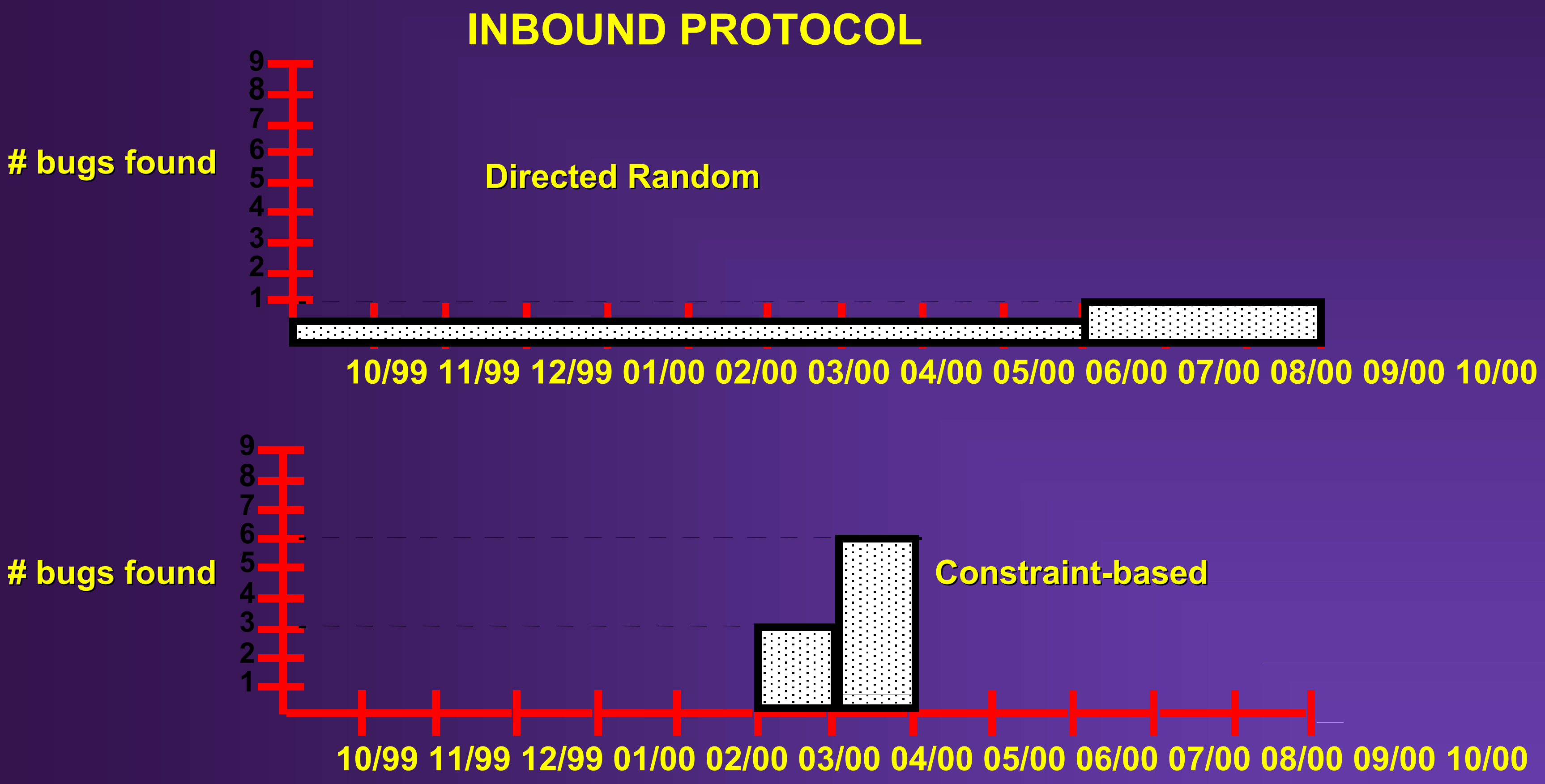
Constraint-based verification simulates **corner cases** of designs more effectively than other methods.

Constraint-based simulation **finds bugs earlier!**

Another **PPC** Design Manager:

> “The kind of bugs [CBV/SimGen user] has found in my logic are difficult to find in simulation. I do not believe we can guarantee a high quality first tapeout without [t]his work.”

Directed-Random vs. Constrained-Random

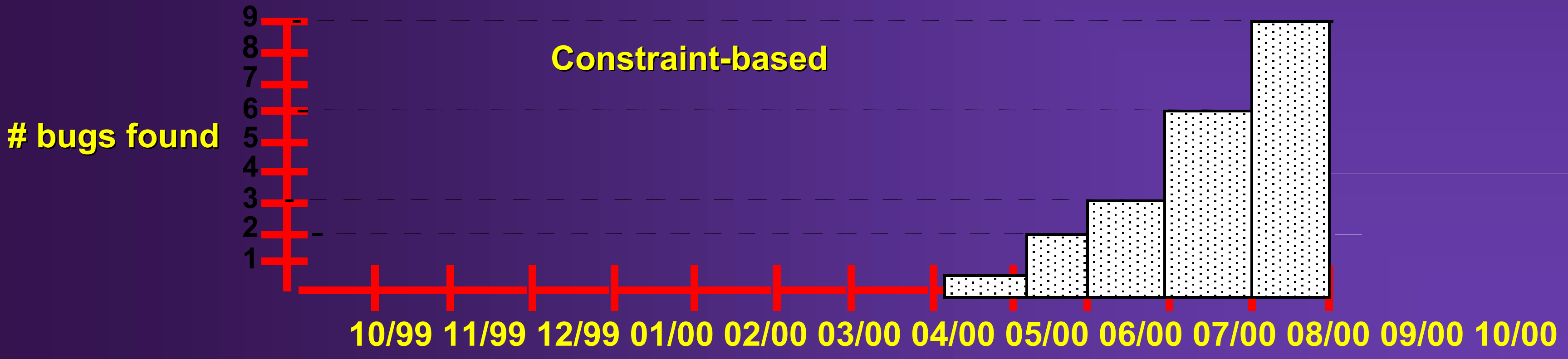


INBOUND PROTOCOL

Constrained-random vs. directed random

OUTBOUND - LOGIC LAYER


Directed Random


Constraint-based

Benefits

. Constraint-based verification can be put in the hands of designers at the module, block and unit levels of design. This implies a much broader user-base for formal and simulation tools.

. Verification checkers are left all over the design to locate and isolate problems near the bug site.

. Constraints formally document interfaces to DUVs in a machine-readable way.

Observation

- **Complex** temporal assertions (checkers) CANNOT be easily reused as stimulus generators.

Constraint Example

Request

Req_id[0;1]

Req_type[0:2]

Req_prior[0:1]

XYZ

Response

Resp_id[0:1]

Resp_type[0:1]

Assume: A request may be given only if its identifier is not equal to the identifier of any active transaction.

Constraint Example

```
module xyz;

function activate(id[0:1])[0:0]   = request  &
   (req_id == id) ;

function deactivate(id[0:1])[0:0] = response
   & (resp_id == id) ;

function active_next(id[0:1])[0:0] =

     (deactivate(id) ? 1'b0       :

      activate(id)   ? 1'b1       :

                       active[id]) ;
```

Constraint-based Verification

```
var active[0:3] =
      {active_next(0),
        active_next(1),
        active_next(2),
        active_next(3),
          } ;
constraint(request ? ~active[req_id] : 1'b1) ;
```

Constraint-based Verification

- User provides constraints as Boolean expressions involving state and inputs.
- User provides biasing for each variable.
- SimGen generates input vectors to simulator on each clock cycle by solving constraints -- all together.
- SimGen is non-backtracking!
- SimGen is constant cost for each cycle. The cost is linear data structures representing constraints (e.g. BDDs).

SimGen technical issues

- Keeping BDD size low
- Automatic identification of special constraints that can be handled separately
- Constraint fracturing
- Variable ordering
- Constraint prioritization
- Run-time constraint solving (e.g., Shimizu/Dill)

Summary

- Provides early/easy animation of DUVs by designers -- without checkers, without stimulus driver programs, ….
- Provides robust stimulus to exercise corner cases of design
- Inputs can be “weighted” to bias simulation
- Stimulus generation and checkers are dual concepts.
- Incrementally integrates into existing simulation environment.

Summary (cont.)

- Constraint-based verification is a sales opportunity.
- Constraint-Based Verification works with both simulation (VCS & Vera), formal tools (Ketchum) and OVA.
- Constraints can be used by designers directly and incrementally – broader market.
- Constraint-based verification finds bugs faster than other methods.

References

- [0] J. Yuan, K. Shultz, C. Pixley, H. Miller, “SimGen: A Tool for Automatically Generating Simulation Environments from Constraints”, ITC Workshop on Microprocessor Test and Verification, October 22-23, 1998
- [1] J. Yuan, K. Shultz, C. Pixley, H. Miller, A. Aziz, “Modeling Design Constraints and Biasing in Simulation Using BDDs”, ICCAD 1999
- [2] James H. Kukula and Thomas R. Shiple, "Building Circuits from Relations" CAV 2000
- [3] K. Shimizu, D. L. Dill, and A. J. Hu. "Monitor-Based Formal Specification of PCI", FMCAD 2000, Austin, Texas.
- [4] K. Shimizu, D. L. Dill, C-T. Chou, "A Specification Methodology by a Collection of Compact Properties as Applied to the Intel Itanium Processor Bus Protocol", CHARME 2001, Livingston, Scotland.
- [5] Matt Kaufmann, A. Martin, C. Pixley, “Design Constraints in Symbolic Model Checking”, CAV 1998: 477-487

End of Talk

Common User Assertion Examples

- One-hot buses
- Full and parallel case synthesis pragmas
- Array accesses
- Bus contention
- Valid data not lost in stalled pipelines
- Low priority events eventually processed
- Requests handled within spec’d window
- Packet Valid signal asserted correctly