DEMONSTRATION SESSION

ANALYZE

Rigorous verification of asynchronous circuits and systems.

Ken Stevens
Air Force Institue of Technology

Developed at the University of Calgary with financial support from Hewlett-Packard.

GENERAL APPLICATION

Unbounded delay verification for all hazard models:

- Delay-insensitive (DI)
- Quasi delay-insensitive (QDI)
- Speed-independent (SI)
- Burst-mode (BM?)

Example 1: C-Element

1. Efficient SOP C-Element does not verify under SI hazard model.
2. Efficient SOP C-Element verifies under BM hazard model.

MATHEMATICAL RIGOR

1. Only tool based on a model proven to not create false positive results. Details:
   - Bisimulation verification
   - Complete Trace verification
2. Process Logic
   - CCS (Milner's Calculus for Concurrent Systems)
   - Model Checking
   - Temporal logic (HML)

Example 2: Contrived circuit that gives false positive under AVER in burst-mode.

Example 3: Post Office SEQUENCER circuit

HIERARCHICAL

Can be used for top-down verification of systems, to the gate level.

- "Congruence" achieves hierarchical application
- Partial order for looseness of specification ("conformance")

Examples of system verification (not included in this demo:)

1. CAM (Categorical Abstract Machine)
2. Parts of the AMULET
3. Sutherland's MOVE machine (by Hans van Gageldonk)
4. Multirate FFT Chip

HIERARCHICAL (cont)

BISIMULATION CONFORMANCE FORMALIZATION

Bisimulation Conformance between implementation I and specification S is written as $I \succeq_b S$ and holds iff $\forall\, \alpha \in \text{Act}$ and $\forall\, \beta \in \overline{\mathcal{A}} \cup \{\tau\}$ and $\forall\, \gamma \in \mathcal{A}$

(i) Whenever $S \stackrel{\alpha}{\rightarrow} S'$ then
$\exists\, I'$ such that
$I \stackrel{\widehat{\alpha}}{\Rightarrow} I'$ and $I' \succeq_b S'$

(ii) Whenever $I \stackrel{\beta}{\rightarrow} I'$ then
$\exists\, S'$ such that
$S \stackrel{\widehat{\beta}}{\Rightarrow} S'$ and $I' \succeq_b S'$

(iii) Whenever $I \stackrel{\gamma}{\rightarrow} I'$ and $S \stackrel{\gamma}{\Rightarrow}$ then
$\exists\, S'$ such that
$S \stackrel{\gamma}{\Rightarrow} S'$ and $I' \succeq_b S'$

EXAMPLES FROM PROCEEDINGS

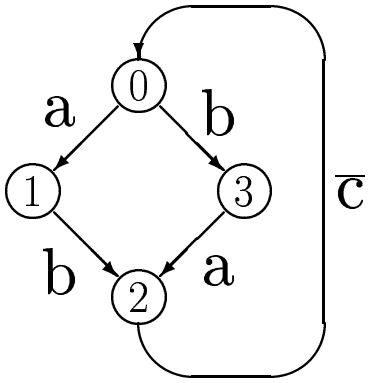
1. Simple Latch Control – page 14.
2. COP – page 119
3. Boolean function unit – page 161
4. One place buffer – page 231
5. SCSI-init-send circuit – page 245

DIRECTIONS

1. Bounded delay verification
2. Conformance not as a partial order
3. Tool improvements
   (a) Circuit generators
   (b) HDL language interfaces
   (c) Specification generators (Al's butterflies)
   (d) Efficiency
   (e) Graphical interface

EXAMPLE 1: C-ELEMENT

Specifications:

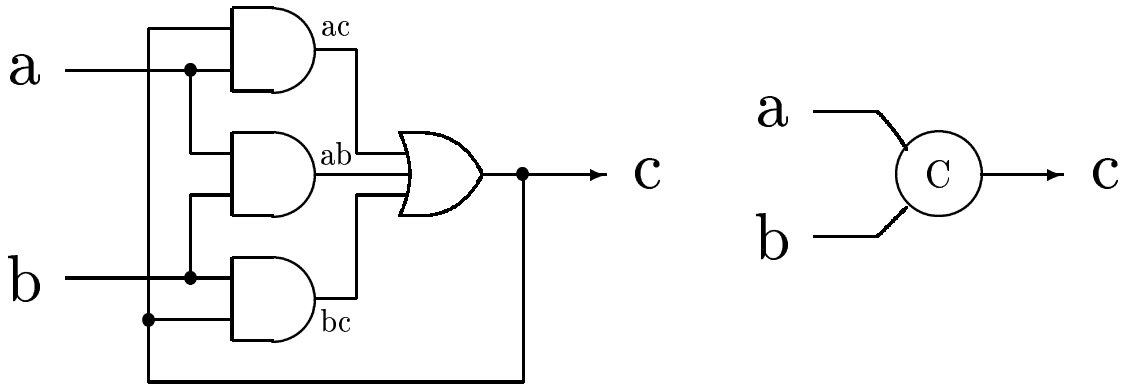


c \ ab	00	01	11	10
0	0	0	1	0
1	0	1	1	1

C-elt $\stackrel{\text{def}}{=}$ a.b.$\overline{c}$.C-elt + b.a.$\overline{c}$.C-elt

C-elt $\stackrel{\text{def}}{=}$ (a,b).$\overline{c}$.C-elt

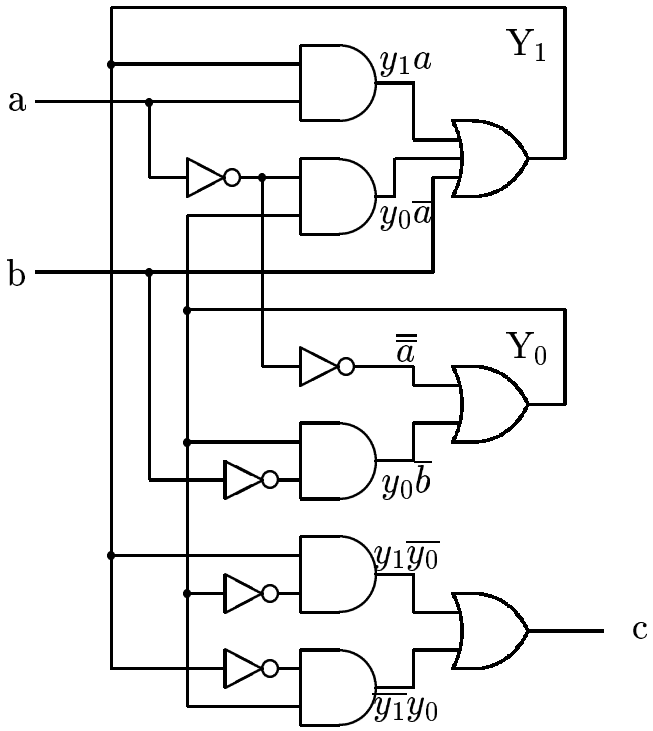
EXAMPLE 1: C-ELEMENT



$$\text{C-Imp} \stackrel{\text{def}}{=} (\text{AND2}[c/b, ac/c] \setminus \text{AND2}[ab/c] \setminus \text{AND2}[c/b, bc/c] \setminus \text{OR3}[ac/a, ab/b, bc/c, c/d] \setminus)\setminus\{ac, ab, bc\}$$

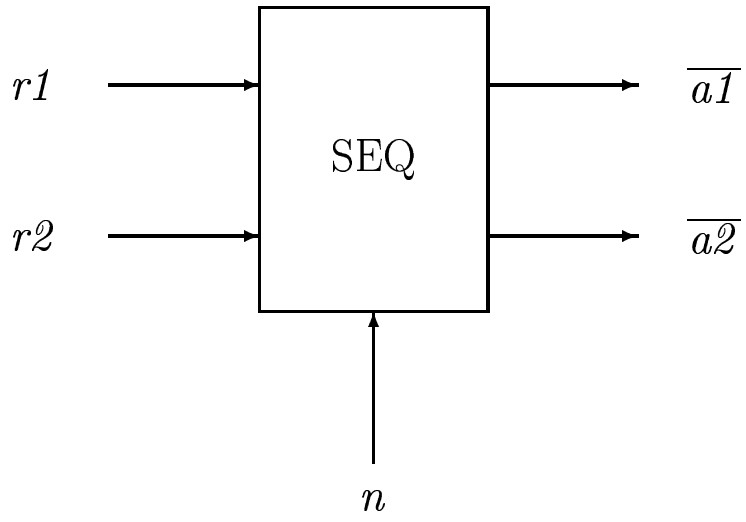
EXAMPLE 2: CONTRIVED CIRCUIT

$$\text{Spec} \stackrel{\text{def}}{=} \text{a.}\overline{\text{c}}\text{.a.}\overline{\text{c}}\text{.Spec} + \text{b.}\overline{\text{c}}\text{.b.}\overline{\text{c}}\text{.Spec}$$



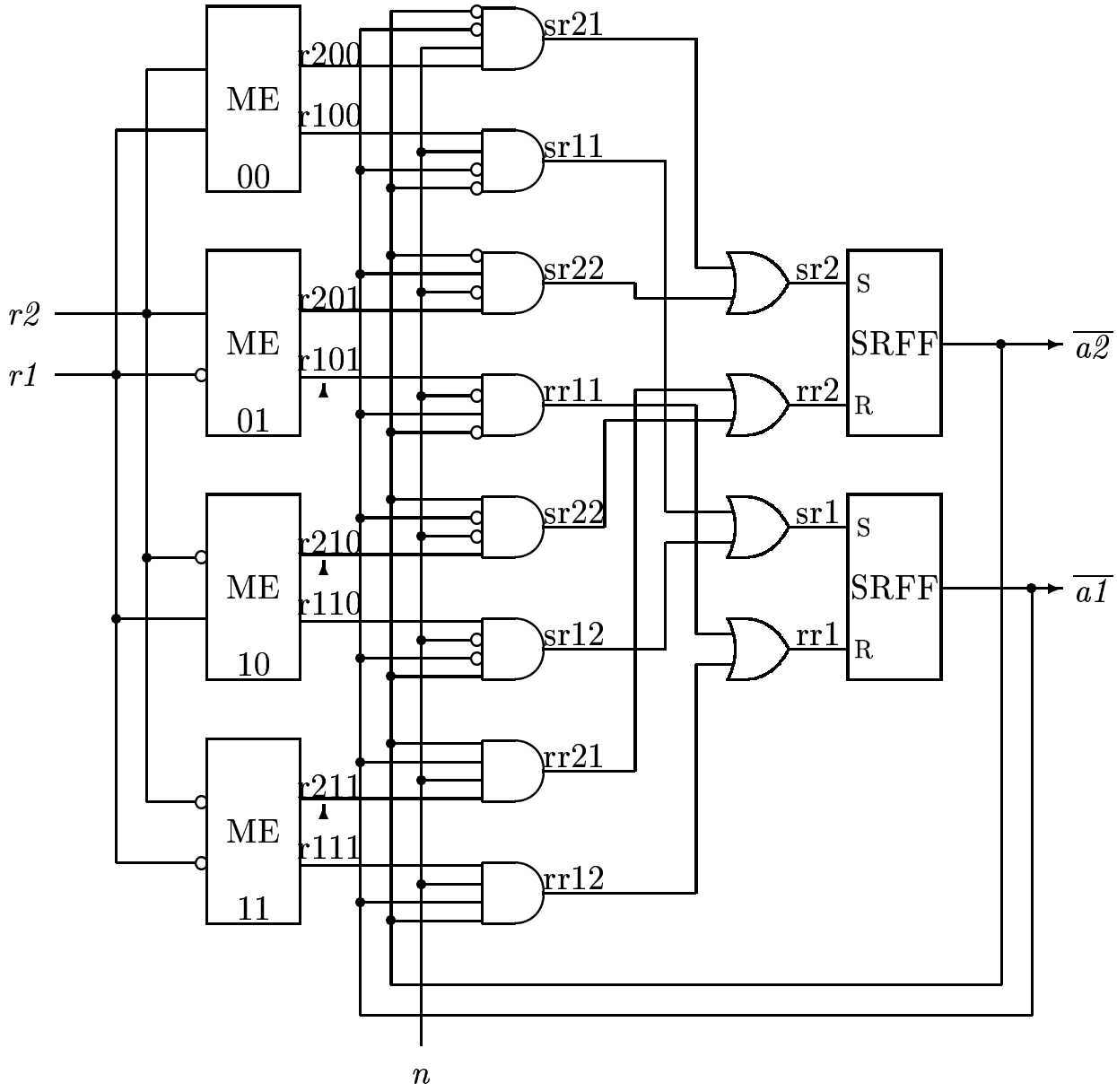
EXAMPLE 3: PO SEQUENCER

The Sequencer Module



SIfc	$\stackrel{\text{def}}{=}$	r.g1.g2.'a.'p.SIfc
SSem	$\stackrel{\text{def}}{=}$	'g1.n.'g2.p.SSem + n.'g1.'g2.p.SSem
SEQUENCER	$\stackrel{\text{def}}{=}$	(SIfc[r1/r, a1/a] | SIfc[r2/r, a2/a] | SSem) \ \{g1, g2, p}

EXAMPLE 3: PO SEQUENCER



2^{74} states; 3,664 Burst visited