The Arduous Road of Modelling

Excerpts from Records of an Enjoyable Co-operation of Nearly 20 Years

Helmut Jürgensen
The University of Western Ontario
London, Canada

Plan of the Talk

- Some history and why working with John was a pleasure
- Some scientific background
- The struggle to get things right
- Lessons

Details, in particular those concerning modelling, will be given in the printed version of this talk.

Some History

- 1971 – First encounter in Haifa.
- 1976 – My first ever trip to North America, visiting Gabriel Thierrin in London: Talks at Purdue, Penn State, and also Waterloo. The latter on *Enumeration of Semigroups.*
- Many other meetings. For instance in Vic-sur-Cère with Eilenberg, Schützenberger and many others. Notably: John's visit to Darmstadt in the early eighties and his eventful railway journey to Austria.
- 1982 – My sabbatical at Western and Waterloo: Working with Karel Culik, Jozsef Gruska, David Matthews, Arto Salomaa, Gabriel Thierrin, Derick Wood, and John. John had his usual job as chair. We looked at syntactic monoids of languages with certain solvable groups as their maximal subgroups and did not get very far.

- 1983 – We moved to London.
- John returned to circuit theory in the early eighties. 1986 he suggested to look at recent work by Courtois, David and their students on circuit testing.

This started our intense co-operation with regular meetings in Waterloo and London.

- About 1986–1999: Circuit testing: Modelling the concepts and process; proving empirical claims.
- About 2000–2007: Software verification: Modelling trace assertions and establishing the related proof systems.

1996–2007: I held a second position 1n Potsdam, Germany. I commuted across the ocean. This slowed us down – I apologize.

Background on Circuit Testing

- Given: A circuit A to be tested (CUT) and the specification of the "good" circuit A_0.
- Question: Is A functionally equivalent to A_0?
- Method: Send an input sequence (sequence of "test patterns" or "test") to A and A_0, observe and compare the behaviours of A and A_0.
- Problem: Keep the test short. In general this is a hopeless task! It is NP-complete with the number of states being more than 10^{12}.
- Test for likely faults only: "Fault model" – a small finite set of automata
- One tests only for faults in the model, but may detect many other faults. Fault coverage extends beyond the fault model.

Here is a figure from the papers we started with. It looks as cryptic as the paper itself was. It concerns the testing of a memory.

The figure shows the Markov chain for testing for a pattern-sensitive fault of the type $\uparrow j \Rightarrow \uparrow i$ in a memory. Under some 'environment' conditions, writing a 1 into memory cell j which contains 0, causes the contents of cell i to change to 1.

The main claim: *Many faults may need a more than linear deterministic test length – but may need only a linear random test length.*

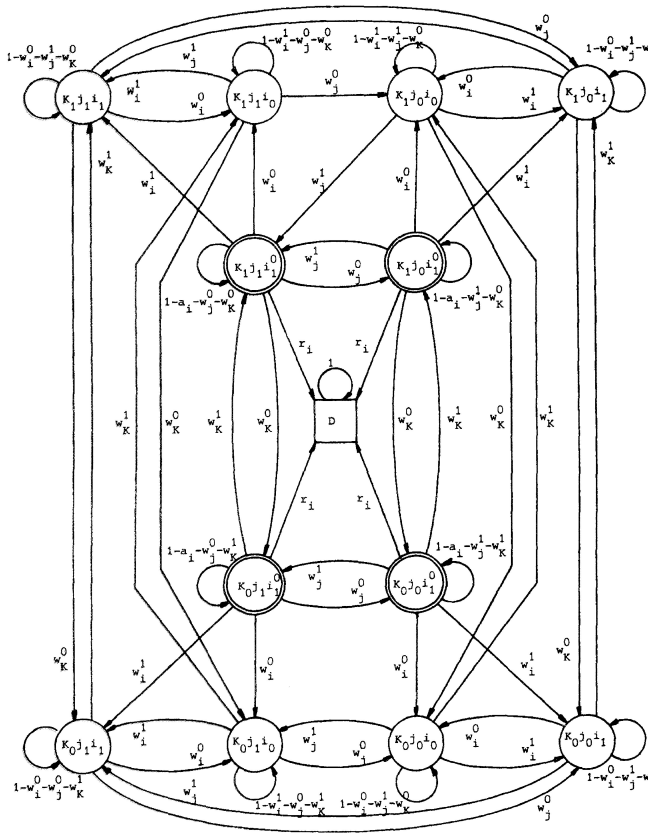


Fig. 4. Markov chain for the active PSF's: $\uparrow j \Rightarrow \uparrow i$ when $K = 1$.

The original goals:

- A comprehensive theory of circuit testing.
- Explain and prove the difference between deterministic and random testing.

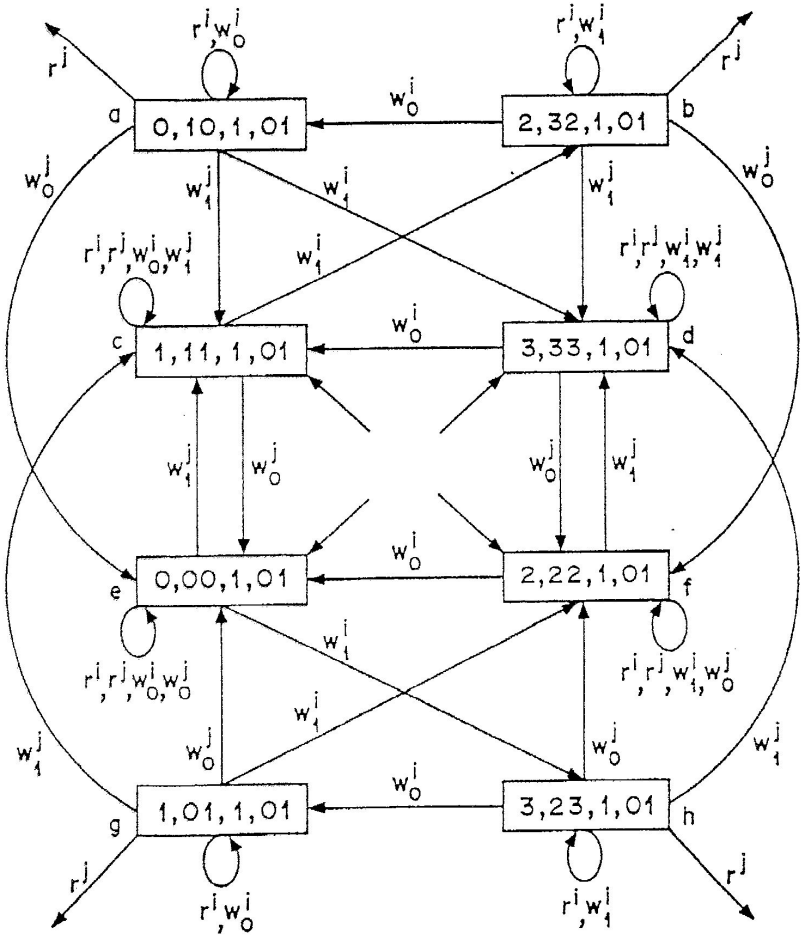
Narrowed to: Sequential circuits; then random-access memories (RAMs); then just understand the engineering papers at hand.

The tasks:

- Translate the engineering terminology: fault; single fault; multiple fault; pattern-sensitive fault; fault model; deterministic test; random test; fault coverage; fault diagnosis; fault detection; etc.
- Model the testing process.
- Formulate and prove the conjectures.

Our first model, presented in 1987 at the 2nd Canadian Test Workshop in Winnipeg, did all this, but was not correct and too complicated.

- The good and faulty circuits are semi-automata.
- Single and multiple faults discussed superficially.
- Fault schema: ND-automaton to simulate all potential behaviours. Initial states ignored.
- Observer: ND-automaton modelling potential observations – using knowledge set and knowledge acquisition function. Probabilities added for random testing.



Our second model, presented in 1988 as a pair of papers at a conference in Salgótarján and at the 3rd Canadian Test Workshop in Halifax:

- Fixes the flaws and simplifies the Winnipeg model.
- Generalizes Hennie's work on diagnostic automaton experiments (1960s).
- The good machine is a Mealy automaton A_0; the fault model is a finite set of Mealy automata A_i; the CUT is not considered.
- The observer is a deterministic semi-automaton constructed as a "kind of" direct product of all possible initialized versions of A_0 and the A_i.
- Diagnosis goals are expressed as partitions of a set related to the states of the observer.
- Test sequences are words accepted for a given diagnosis goal.
- By adding probabilities, one gets a model for diagnosis with random test sequences.

This model was published – finally – in 1992 in JETTA (for abritrary sequential machines).

Further events:

- 1988 and 1990: John and I organize the 3rd and 5th Canadian Test Workshops in Halifax and Ottawa.
- 1990: Bruce Cockburn and John publish proofs of bounds for deterministic test lengths for RAMs. There are faults which require greater than linear test lengths.

  Founding of the Maveric group.  `http://maveric.uwaterloo.ca`
- 1991: We start working on the notion of multiple faults.
- 1992: We prove – with René David – the conjecture about random testing: For a large class of memory faults the random test length is $O(n/\varepsilon)$, while some of these require a non-linear deterministic test length (JETTA 1997).
- 1992–1996: Several papers on the rôle of automata in circuit testing, mostly with some polishing refinements and simplifications.

Fault composition:

- "A multiple fault is the presence of several single faults". Here "fault" means "physical fault". For example: i-stuck-at-0 and $\uparrow j \Rightarrow \uparrow i$. What happens?
- A new automaton composition operation $\diamond$ is needed to model the co-existence of faults. The operation must be consistent with the physical phenomena.
- Automaton model: e.g. Mealy automata.
- Generic conditions: The set of faults in a fault model is a semilattice (with zero – the zero element represents all faults which are not in the model).
- Specific physical conditions: Equations describing the composition of automata in the fault model.

- Thatte-Abraham model: stuck-at, transition, and coupling faults.
- Component automaton: Mealy automaton with "product-structured" state set. Composition of component automata as operation on state components.
- The composition of Thatte-Abraham faults satisfies the generic and special physical conditions.
- The composition of component automata must take the physical assumptions into account. This leads to several semilattice structures (JETTA 1996, Salomaa-Festschrift 1999).

When combined with the observer construction, one has a comprehensive model for RAM testing which is purely automaton theoretic.

Software testing:

- 2000–2006: Formulating a rigorous model for software testing using Parnas's trace assertions.
- Start: Puzzled by the literature.
- Method: Use the axiomatic techniques of circuit testing.
- Publications: IJFCS 1996 and 1997.

Lessons:

- The formal definitions of terms must express precisely the essential properties of their technical counterparts. By proving "trivial" statements one can and should check whether the definitions are "correct" and complete.

  We struggled with the notion of "multiple fault" for quite some time.

- Keep the model simple (Occam's razor): It should not require complicated constructs if the technical process itself can be explained without them.

  The concepts of "knowledge set" and "knowledge acquisition function" in our Winnipeg model seemed natural, but actually led to unnecessary complications. The later version of the "observer" is far simpler intuitively and mathematically.

- Separate the concepts!

  Separating generic and physical conditions on fault composition resulted in significant simplifications of the model.

- One needs to convince the practitioners in their terms of the model being adequate, complete, and useful. One needs to convince the mathematicians (or the grant selection committee) of the work being worth anything at all.

  A very good paper may end up being rejected several times by both scientific communities, but for different reasons. Convincing requires exceptionally careful writing.

  Experience: People in the field don't understand why the work is useful; theoreticians consider it trivial.

- As to careful writing: We discussed every single comma.

  We are both meticulous and wrote the papers word-by-word, symbol-by-symbol during our meetings.

- Profound research takes time. The new NSERC procedures still pretend to favour research programmes, but they really support short-term projects, and thus destroy the research culture in Canada.

  Given the new procedures, one might not even consider proposing a long-term project like ours. Funding, if provided at all, would be far too unstable.

A more specific set of "lessons" will be given in the full printed paper.

The reward?

After one has established a beautiful model with proofs, one can be sure a referee will say "it's fine that you proved all this! Where are the simulations or experiments to corroborate it?"

Less cynically:

Our joint work over nearly 20 years was challenging, successful, and most enjoyable. I have learnt much from this co-operation. I am sure our work will have a long-term impact and I am proud of it.

Thank you, John!