Trip report E.W.Dijkstra, Newcastle-upon-Tyne, 6-10 Sep. 1982

The yearly Joint International Seminar on the Teaching of Computing Science — sponsored by IBM UK Ltd and organized by The University of Newcastle-upon-Tyne — was this time devoted to the topic "Formal Specification".

I arrived in Newcastle earlier than usual. I used to take the plane from Amsterdam on Monday afternoon, but British Caledonian had moved that flight to the evening. I found that flight too late, so I took the morning flight. I left Nuenen at 8:15 .

I also returned earlier than usual. Instead of returning as usual on Friday evening I changed my reservation to the morning flight so as to be able to attend a discussion on Friday afternoon at the University where earlier that week one of my mathematical colleagues had launched such a violent attack on a text written by my assistent that some action from my side seemed necessary before I would be off to Danmark next Sunday. As expected, the man's "criticism" was unsubstantial: like so many more traditional mathematicians he was just unaware of the rigour with which computing science has by now separated logic from philosophy.

I shall deal with the speakers in alphabetic order.

The lecture by J.-R. Abrial "Specification and Construction of Parallel Processes" I missed as a result of my early departure, something I regretted very much since I had never heard him.

R.M.Burstall devoted three lectures on "Specifications using an Algebraic Approach." He was much clearer than I remember from earlier occasions, yet hardly changed my attitude: I am still unconvinced, yet I gladly give him the benefit of the doubt.

D.I. Good's first lecture was on "Specification and Mechanical Proof of a Distributed System in Gypsy". It had the charm of reporting on work actually done. He presented his achievement with just pride and great honesty, not hiding the fact that so far the economics of his approach left something to be desired. I was sorry to miss his second lecture "Reusable Problem Domain Theories"; I quote from his abstract "In our experience with specifying and proving several real programs of considerable size, we have found that the dominant cost comes from what essentially amounts to building an effective theory of the problem domain."

J.J. Horning gave one lecture on "Some Notes on Putting Formal Specifications to Productive Use", in which he closely followed the paper he wrote with John V. Guttag and Jeanette Wing. As a result I liked the lecture as little as the paper, which had already given rise to extensive correspondence and a long discussion between the two of us on Monday afternoon. He then gave two lectures on "Notes on the Design of the "Larch" Family of Languages", of which I missed the last one, what I regretted since the one I could attend — though largely on plans and intentions — contained more meat than the first one.

C.B. Jones gave three lectures — titled "The Rigorous Method", "Meta IV", and "An Application" respectively —. With him I can never escape the feeling that his VDL past still shows itself and that his formalism should be redesigned for the sake of effectiveness. The issue of "bias" was explained very clearly.

P.M. Melliar-Smith gave three lectures, all of which I could attend: "The Formal Specification and Mechanical Specification of SIFT: A Fault-Tolerant Flight Control System", "A System for Formal Specification and Mechanical Specification" and "The Specification and Verification of Asynchronous Distributed Systems". They were all three very informative.

What is here euphemistically referred to as "flight control" concerns the problem of using electronics to make planes with mechanically unstable wings fly, which for the sake of reliability has to be approached by a bunch of machines working in parallel. Two operating systems have been designed for that task and the comparison between the two was illuminating. The one had been designed in the traditional way for a configuration with special-purpose hardware for the voting procedure, the other with the intention of proving its correctness for a configuration without special hardware for voting: the one had required 4000 statements and its correctness could not be established, while the other -in which Melliar-Smith had been involved- required eventually only 250 statements. A nice confirmation! (And, please, remember that in a binary world a factor of 16 corresponds to 4 orders of magnitude!)

In his second lecture he explained quite convincingly why they had built their own deduction system. Instead of being confined to those tasks for which a decision procedure was available, the theorem provers hanging around -at SRI- were based on heuristics inspired by Artificial Intelligence, a "sophistication" which had made them useless. I quote:

"A drawback to heuristic theorem-proving attempts is that successful proof depends upon intimate knowledge of the heuristics employed. One must understand how very subtle changes in specification structure, even those that preserve semantic equivalence, can affect the direction and final outcome of the proof attempt. Lemma form becomes as important as content."

So much for Artificial Intelligence.

In his third talk he described how they intend to use temporal logic. It was very clear, but much less convincing; presumably contrary to his intentions he gave more food to my suspicion that temporal logic's hidden quantifications embody a methodological mistake.

P. Mosses gave two lectures of which, after having heard the first, I skipped the second one.

R. Nakajima from Kyoto University had planned to give two lectures on "Use of Formal Specifications in a Modular Programming System". After a vain attempt of explaining the Iota system —using the most obscure graphics I had seen for a long time— he gave his perception of the Japanese "5th generation computer". That was very funny and very illuminating. He described it primarily as a bureaucratic monstrum out of touch with reality. Its major impact seemed to be that now all research proposals had to be rewritten so as to make them look like "FGC proposals". In this respect it looks as if Japan is creating its own Ada, adding, as it is, to its society a next layer of dishonesty.

On Thursday evening, at the closing dinner at Durham Castle, W.M.Turski gave a nice after-dinner speech, in which he redressed the balance and put the supposed virtues of formal -if not formalistic- treatment in proper perspective.

* * *

Jim Horning and I enjoyed the privilege of staying at Hotel Randell. After our return from the closing dinner, Jim was tired and went to bed. Till then, Brian and I had not had the time to talk in peace; he described to me the highlights of the project he had been working on for the last nine months -and about which he could now talk freely-. It sounded fascinating; that last night at Hotel Randell I had a short sleep.

I did not join the excursion on Wednesday afternoon: fearing to be otherwise occupied during the weekend, I spent that afternoon preparing the after-dinner speech I would have to deliver the next week in Copenhagen. I did join all other social events: on Monday evening the "At Home" organized by Harry Whitfield and his wife, on Tuesday evening dinner and Northumberland folk music at Close House, on Wednesday evening an informal gathering, and on Thursday the closing dinner. That day F.L. Bauer had come from Munich, having some business to conduct with me and a few others. That had to be squeezed in as well. In retrospect I realize that I have hardly spoken to the general English colleague: my time has been fully occupied by those present whom I know very well.

Plataanstraat 5
5671 AL NUENEN
The Netherlands

17 September 1982
prof. dr. Edsger W. Dijkstra
Burroughs Research Fellow