A Brief History of Formal Methods

Cliff Jones
Newcastle University

Lille 2018-02-07

Formal Methods (big subject)

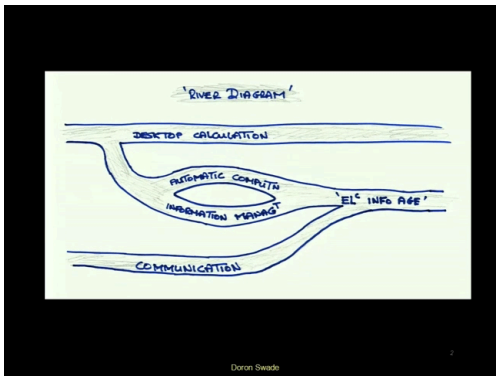
- semantics of programming languages
- verifying/developing programs
- computer assisted reasoning
- …
- complexity
- AI
- Petri Nets
- Nivat

Formal methods: split of talk

- describing programming languages
  - semantics
  - “different approaches” interacted
  - (limited?) impact
- early researchers reasoned about programs
  - (based on [Jones03])
  - search has been for “tractability”
  - later move to use in development process
  - impact

Doron Swade’s “avoid the grand narrative”

- semantics of programming languages
  - interplay **
- verifying/developing programs



“On the fact that the Atlantic has two sides”

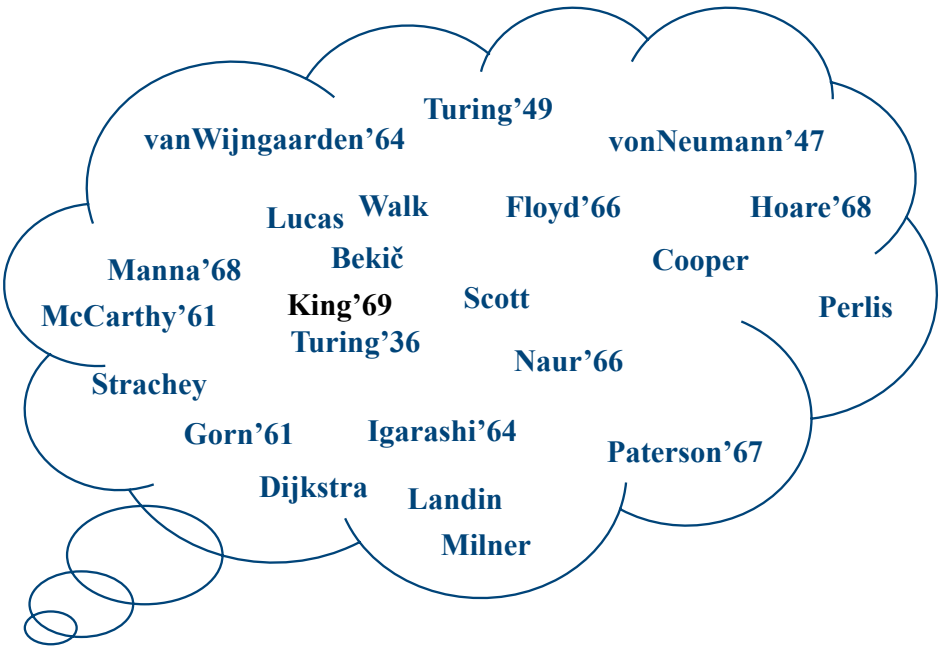
- (I love Edsger’s title - but …)
- interesting difference of emphasis (formal)
  - US tends to focus on “complexity”
  - Europeans on “formal methods”
- many of US FM folk have spent EU time
  - Dana Scott, John Reynolds, …
  - Boyer-Moore theorem prover
- J’s explanation??

Emphasis is on applicability: “theoreticians” who really programmed

- Dijkstra: ALGOL 60, THE
- Hoare: at English Electric
- Milner
- Burstall
- …

HLLs
(High-Level programming Languages)

- thousands of HLLs!
  - Jean Sammet gave up at 500
  - Landin's "next 700 PLs"
  - web site gave up at 8512
- panel at MFPS-XX (2004)
  - Scott, Reynolds, McCarthy, Jones!
  - Vaughan Pratt's (2 part) question



Influence?

People involved in semantics

Operational	Axiomatic	Denotational
McCarthy	Hoare	Landin
Elgot	Apt	Strachey
Vienna Lab		Scott
Plotkin		Plotkin
		Vienna Lab
		etc.
	9	

What constitutes semantics? (of HLLs)

- "ability to reason about programs"?
- Semiotics C. S. Peirce/Charles Morris
  - Heinz Zemanek (u.a.) applied to HLLs
- syntax: form
  - solved 1960
- semantics: meaning
  - harder!
- pragmatics: intent

Why formal semantics?

- precise
- divides problem (cf. Fetzer)
  - use by writers of compilers for $\mathcal{L}$
  - use by those programming in $\mathcal{L}$
  - cf. Boyer/Moore “stack”

Such formal semantics are difficult

- scale
  - toy language vs. ALGOL 60 vs. PL/I (or Ada, …)
- precise yet permissive!
  - non-determinism is hard!
    - bad examples (even in Pascal)
  - crucial for concurrency

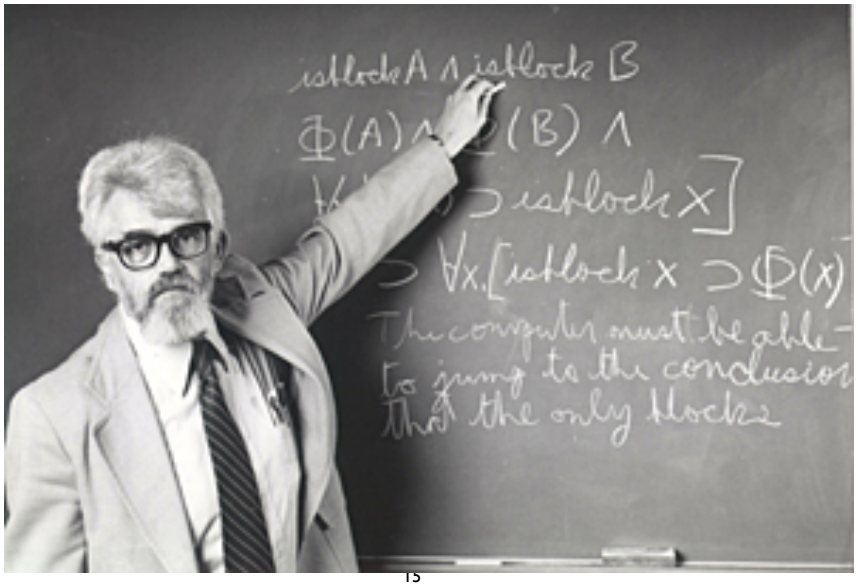
Some key meeting(place)s

- FLDL Baden-bei-Wien 1964
- MTOC IBM Yorktown 1968
- IFIP Working Groups
  - WG 2.2 (especially April 1969)
  - WG 2.1
  - WG 2.3
- HOPL conferences
  - 1981, 1996, …

Semantics: Equivalences

- study of program schemata
  - Luckham, Park, Patterson
- disagreement at MTOC (1968)
  - re Floyd/Manna
  - McCarthy vs. Patterson
- come back to … (CKAs)

John McCarthy
1927-2011



Semantics: Operational (a)

- Program + State -> State
- "abstract interpreter" McCarthy
  - Baden-bei-Wien 1964 FLDL conference
  - "Micro-ALGOL" - interesting choice of subset
  - + abstract syntax concept
- Vienna Definition Language (VDL) 1964-68
  - PL/I huge language
  - many new concepts (including concurrency)
  - "grand state"
- Plotkin's SOS (concurrency)

IBM Lab Vienna

Semantics: Operational (b)

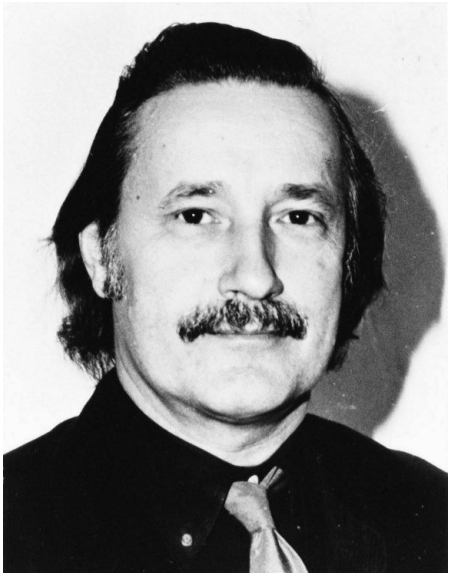
- VDL “abstract interpreter”
  - like a “non-deterministic function”
  - “grand state”
  - Program + Env + State -> Env + State
  - but (far) worse
  - attempts to use in proofs: Lucas/Jones/Henhapl
- Plotkin’s SOS (concurrency)
  - small state
  - inference rules (logic of extended judgements)
  - copes neatly with non-determinacy

Gordon Plotkin (b. 1946)

Semantics: Denotational (a)

- simple case: Program -> (State -> State)
  - “homomorphic rule”
  - higher level of reasoning
- Stachey/Landin already at FLDL
  - lack of model for untyped Lambda Calculus
  - Scott to Oxford late 1968
  - deBakker/Scott ms presented in IBM Vienna Lab August 1968

Strachey/Landin/Scott



Semantics: Denotational (b)

- Oxford
  - Scott's first stay "most exciting term" (not achieved later)
  - foundations (after "OWHY" paper) - cf. Scott 2016
  - "continuations"
- Vienna Development Method (VDM)
  - language definition aspect ("exit concept")
- power domains for concurrency

“avoid the grand narrative”

- OS/DS interplay
  - small state
  - environments
    - Id -> (Loc | FnDen)
  - jumps

Semantics: Axiomatic

- Floyd/Hoare axioms - interesting path
  - FLDL comment
  - series of drafts
  - 1968 paper “An axiomatic basis …”
  - link to OS by Peter Lauer (Vienna to Hoare in Belfast)
  - CKAs (cf. ACM video)
  - (see later for program development)
- question: ability to handle difficult HLL concepts
  - Hoare/Wirth Pascal “axioms”

Semantics: a key trend

- McCarthy 1964 (and 1962)
  - VDL seen as Baroque
  - ALGOL 60 description as rebuttal
  - Vienna proof attempts (de Bakker comment!)
- we were all seduced by denotational semantics
  - Oxford
  - VDM
  - Plotkin's contributions to domain theory
- recent return to (S)OS
  - see Plotkin + Jones "contexts"

"Exegesis" (4 ALGOL descriptions)

- ALGOL 60 = good choice
- TR available CS-TR-1498
  - a version will be in HaPoP-16 proceedings
- four "complete" descriptions of ALGOL 60
  - Lauer VDL (operational) description
  - Allen/Chapman/Jones "functional semantics"
  - Mosses (Oxford) "denotational semantics"
  - Henhapl/Jones VDM (denotational)
- fair amount of history (context etc.)

“Exegesis” - topics for each approach

- syntactic issues
  - including “context conditions” (van Wijngaarden)
- semantic approach
- grand/small state
  - separation of “environment”
  - handling local naming (and dreaded “own” vars)
- jumps (“goto”)
  - continuations
  - exit mechanism
- (not) concurrency

Controversy

- Peter Naur’s 1982 attack in BIT
  - republished in his 2004 book
  - argues against formalism
  - (we remained on good terms)
  - comment from other Dane!

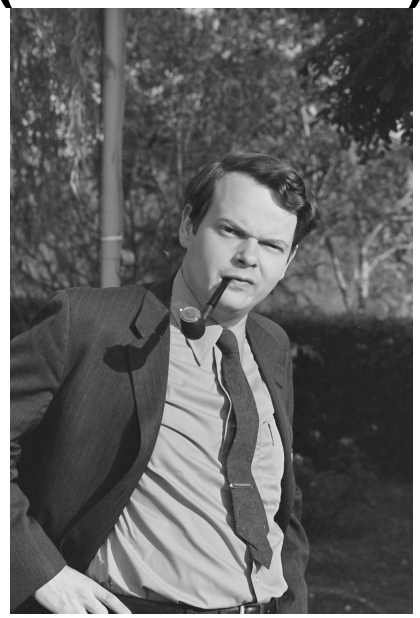
“Semantic Challenges” CS-TR-1516

- mainly (S)OS
  - denotational runs into problems
  - axiomatic: SL, R/G
- ALGOL-like blocks, functions, procedures
  - parameter passing modes
- non-determinism
  - concurrency (the biggie!)
    - also separate paper (for a *Festschrift*) expands on

Impact(?) of formal semantics

- Turing Language (Holt)
- (S)ML
- Ada?
  - requirements
  - Véronique Donzeau-Gouge
- Modula-II standard
- John Reynolds “… midwives/morticians …”
  - = main impact should be language design

John Reynolds (1935-2013)



Some resources re semantics

- my web site for copies of key documents
  - http://homepages.cs.ncl.ac.uk/cliff.jones/semantics-library/
- Strachey's 100th birth anniversary
  - videos: https://www.cs.ox.ac.uk/strachey100/
- Hoare interview for ACM
  - https://amturing.acm.org/interviews/hoare_4622167.cfm

Troy Astarte's forthcoming thesis

- available late 2018
- formal semantics of HLLs
- technical material in the two TRs
- much more historical
- archive research
- careful interviews with key players