On the heroism of really pursuing formal methods

Dino Mandrioli

Politecnico di Milano

- Thanks for the (undeserved?) invitation!
- A very informal non-technical presentation (however …)
  - (Deliberately) a somewhat provocative one
- A personal view of the state of our (not too young) discipline
  - Driven by a typical (only Italian?) analogy
- Perspectives (not advises!)

Formal methods have been around for quite a while

- The pioneering work by McCarthy, Floyd, Hoare, …
- Major technical achievements
  - More and more “powerful” methods
  - Real-life applications
  - Supporting tools
  - …
- The never ending mission to fight reluctancy, skepticism, … derision
  - The “commandments”
  - Hopes and hypes
  - “Lightweight” recipes
  - Self-criticism

  …

- But we are still here to debate about their chances to succeed
- Hard to say anything original thereabout
- However it could be interesting to exchange opinions, ideas, …
- … let me start with my own ones:
  - Mostly but not exclusively focused on FM promotion and acceptance

The title:

- Copyright by Dijkstra:
  - On the cruelty of really teaching computer science (CACM 1989)
- Whether it is a cruelty or a mission or heroism …
- … it is a fact the both topics remain hot from many and many years
- … and not by chance I “paired” them by borrowing Dijkstra’ title

The half-glass analogy:

Let’s begin with the “close to empty” view:

- FMs are still widely ignored by the community “at large” … if not disparaged (even within academia)
    - Quite unlike the swift success of many typical “novelties” or buzzwords
        - Cloud, big data, crowdsourcing, …
    - Whether deserved or not, whether lasting or not
- Among the many reasons that have been adduced for such a situation let me focus on (one of) the major one:

The (average) lack of mathematical skill necessary (?) to “really pursuing” FMs (1):

- Certainly the mathematical background typical of most (Comput*ing* science) FMs is rather different from traditional mathematics taught to students of traditional engineering fields:
  - ***Very*** roughly speaking: continuous versus discrete math
- But why?
- The case of my Politecnico (interested in sharing experiences):
  - (Besides more traditional math) our CS students must get (optional courses are not included … and not very crowded ☹):
    - 5 credits in mathematical logic and algebra
    - 5+ credits in basic theoretical CS (automata theory, computation and complexity theory, …)
    - 5 credits in formal languages and compilers
  - The average performances (and acceptance) on these topics are far from satisfactory

The (average) lack of mathematical skill necessary (?) to “really pursuing” FMs (2):

- The situation certainly does not improve outside university, mainly among not-so-young engineers, or managers … i.e., those who take strategic decisions.
- All this is rather well-known and, unfortunately, holds even more generally for the larger field of scientific and technological disciplines.
- Thus, to analyze the roots of the –not new – phenomenon, I propose a sort of “zoom out” into a wider, “sociological” perspective:

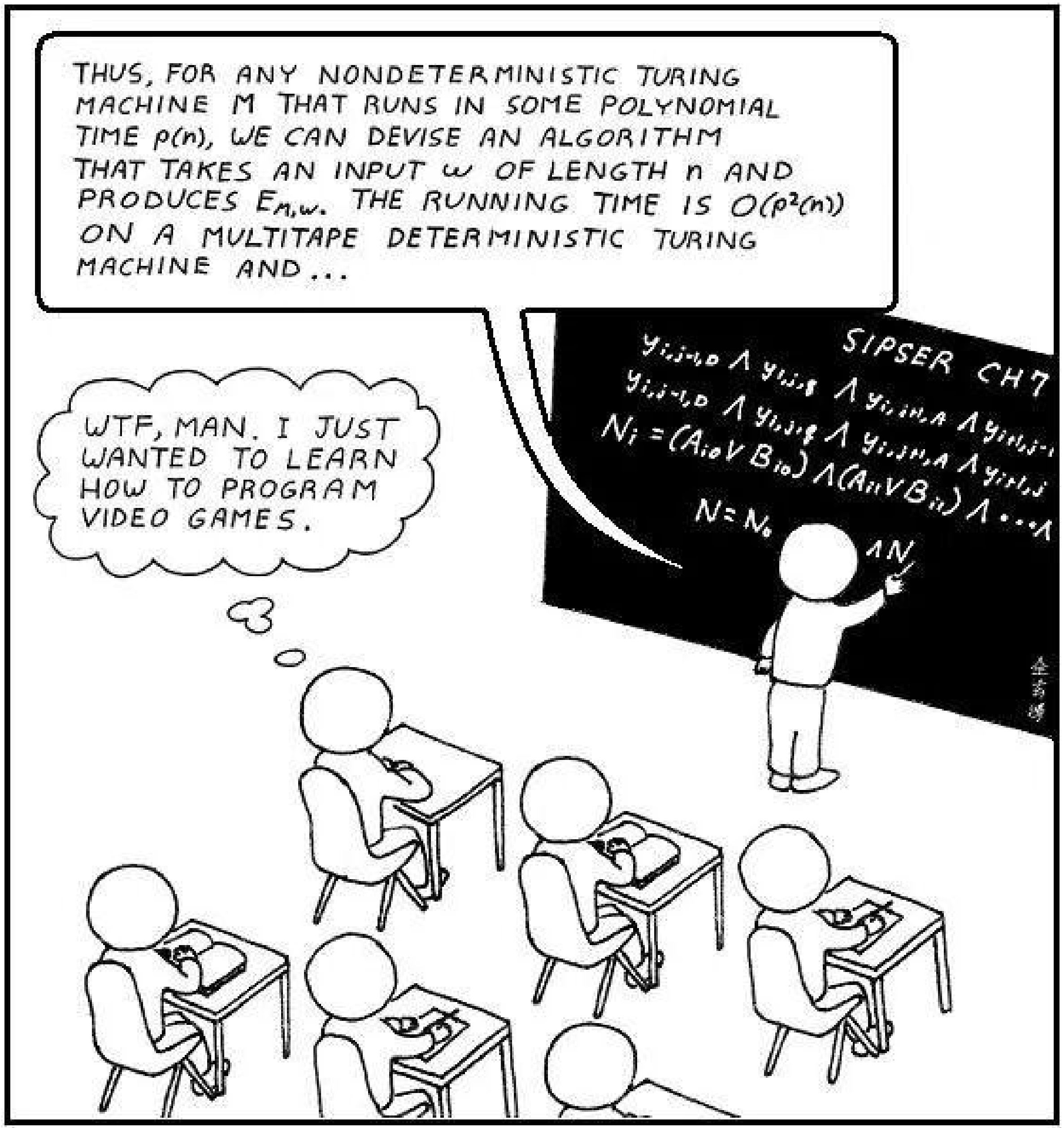
A modest and highly subjective “sociological analysis” (1):

- The “sociological laziness/impatience” towards rigorous reasoning and mathematics
- The “sociological laziness” towards rigor at all:
  - The rush to time to market
  - The “good enough” … but how good is good enough?
  - Salesmen sell “the skin of the bear before killing him” (another Italian proverb)
    - Then technicians deliver (necessarily) a product full of bugs and patches
  - Agile methods:
    - NB: nothing against agile methods, provided they are real *methods*, preferably also *formal* …

A modest and highly subjective “sociological analysis” (2):

This mentality, of course, is “mirrored” in students’ attitude:

- Their impatience to achieve immediate results…
  - From the “Hello word program” (remember Dijkstra’s paper …), to :



THUS, FOR ANY NONDETERMINISTIC TURING MACHINE M THAT RUNS IN SOME POLYNOMIAL TIME $p(n)$, WE CAN DEVISE AN ALGORITHM THAT TAKES AN INPUT w OF LENGTH n AND PRODUCES $E_{M,w}$. THE RUNNING TIME IS $O(p^2(n))$ ON A MULTITAPE DETERMINISTIC TURING MACHINE AND...
WTF, MAN. I JUST WANTED TO LEARN HOW TO PROGRAM VIDEO GAMES.
SIPSER CH7
$N_i = (A_{i0} \vee B_{i0}) \wedge (A_{i1} \vee B_{i1}) \wedge \cdots \wedge$
$N = N_0$
$\wedge N$

Semi-technical-semi-sociological note:

- SW technical peculiarities somewhat exacerbate the consequences of this sociological attitude:
  - SW is malleable
  - The borderline between design and realization (even delivery) becomes fuzzy(ier) … agile …
  - There is often a feeling of “self-learning” (learning by doing vs. learning by teaching-studying)
    - “I can do it myself; I do not need to hire a SW engineer”
    - Would you start building a two-store house (let alone a skyscraper) by assembling a bunch of bricks and some cement?

What do “we” (the academia) do in this techno-sociological context? (1) *My answer*:

- “We” help … making things worse:
  - We advocate “a sharp departure from traditional teaching”
  - We advocate learning by doing as opposed to learning by studying
    - We suggest that freshmen can be immediately involved in … producing videogames (much better than the “hello word program”!)
  - We complain that students lack “soft skills” against “hard ones”
  - We claim that the little our students need of discipline *XX* can be better taught by ourselves, the expert of discipline *YY* which uses *XX*, than by XX experts who are biased towards irrelevant technicalities.
- Personally:
  - I did and still do like “building things with my hands”; when a kid I plaid with pleasure mixing up chemical reactors from the toy box or welding electric components to build “may own radio set” … of course with no knowledge at all of the physical phenomena that were underlying my “experiments”

- A significant personal experience at a workshop on teaching (general) engineering held at the Imperial College a few years ago:
  - A poster room with “engineering artifacts” made by first year students
  - Universal complains about the lack of students’ attitude to work in teams: OK, but …
  - No complain about their attitude to develop a rigorous reasoning (?!)
    - I did not mention it because …
  - Wishes to teach less math (this came from a respected SW engineer)… and of course more ….
- Are we surprised that in this context students do not like FMs?

What do “we” (the academia) do in this techno-sociological context?(2) *My answer*:

- “We” help … making things worse:
  - We replace quality by quantity
    - In teaching
    - In research
  - The inflation of published papers
  - The inflation of bibliometric indexes
  - The hectic proliferation of publication venues and PC memberships
  - The “go/publish to conferences” syndrome (almost exclusive of CS): the typical “time to market” attitude
  - Lot of self-promotion
  - ….
- Are we surprised that (good) theoretical works (not only FMs) are overwhelmed by massively produced ones?
  - NB: I am not claiming that theoretical research does not suffer from the same defect! But it is a priori in a losing position w.r.t. other types of research.

- Another very recent personal experience:
    - Evaluating 157 project proposals by “young Italian researchers” (ERC-like)
    - Only 4 out of them could be classified as theoretical
    - Hardly one could be labeled as FMs
- Fortunately there are “voices” arguing against this habit (recently: Vardi, CACM): let’s hope they have some … impact.

What do “we” (the FMs community) do in this techno-sociological context? (3)

- Some serious mistakes have been acknowledged (and some recovery action has been taken) but they are still present and dangerous:
  - Overselling (“FMs as miracles”): hopes and hypes
  - Overlooking the difficulties of technology transfer
  - Too little attention to, and *knowledge* of, the peculiar needs of the various application fields and to the managerial and political aspects
  - Too much love for the mathematical elegance and competitive attitude in formalism promotion (“my model is better than yours”)
  - The lack of well-engineered tools
  - …

Fortunately there are also facts that can make the glass looking “not too far from full” (1)

- The number of important success stories of application of FMs to real-life (in general critical) systems is increasing
  - Success is not only “technical” (correctness, reliability, …) but often even economic
- Major companies are looking at FMs with more confidence (and less skepticism)
- Particularly relevant the case of NASA
  - The Mars mission
  - Sponsoring its own FMs conference
- In general increased hopes and expectations from several fields of “heavy” industry (railway, avionic, robotics, e-health….)
  - But careful not to go back from hopes to hypes again!

Fortunately there are also facts that can make the glass looking “not too far from full” (2)

- After all, many recipients of the Turing and other prestigious awards due their success to important results in FMs
- Various tools are now available of increasing quality and reliability (about user friendliness …)
- More integration between informal, semiformal, formal models, methods, tools, e.g.:
  - Various instances of UML “paired with” some formal machinery
- In particular …

Fortunately there are also facts that can make the glass looking “not too far from full” (3)

- … the advent and success (breakthrough?) of **Model Checking**
    - The attractiveness of the “push button” philosophy
    - More and more stories of successful applications
    - The use of “Model checking engines” (SAT, SMT solvers, …) as the internal core of sophisticated (and user friendly?) tools (more successful than previous similar attempts with more powerful theorem provers.)
    - Here again a hidden risk of transition from hopes to hypes (more later about this).

So what? How to fill up the glass? (1)

- Hard to give any original answer to this question: let’s emphasize a few strong points and a few “less shared” ones …:
- Apply incrementality: small steps in
  - Research, technology transfer, teaching, developing projects
  - Are often safer than “big jumps” with many unknown aspects
  - Obviously breakthrough ideas are welcome … if they are not the usual hypes.
- Offer much user friendliness … not only in tools
  - Which anyway are an important “atout” from many points of view, not only user friendliness

So what? How to fill up the glass? (2)

- When introducing a novel FM in an industrial environment be more a student than a teacher
  - (am I contradicting my claim against soft skills?)
- Research and technology transfer certainly benefit from each other but their integration/interaction should be managed quite carefully

A few side remarks … somewhat leading back towards empty glass

- FMs and standards: in principle FMs should be exploited in standard definition … is this happening?
    - In my experience …
    - Here the issue is eminently «political/commercial» and few of us have the power to influence «big decisions»
    - Nevertheless … perhaps the glass is not empty.
- SW is pervasive; FMs could/should be pervasive in SW engineering; both lead to a system engineering view (somebody talks abouth systems of systems ☺)
    - It is therefore appropriate to advocate interdisciplinarity …
    - Which however is «interpreted» in various ways
        - By engineers
        - By SW engineers
        - And by FM people?

Only a few words about research

- Research is and must be absolutely free
- Simply ridiculous to pretend to «address» it; just a personal impression:
- Much attention devoted to model checking (correct!)
    - Finding decidable «new» languages/models
    - Analyzing their (complexity) tractability
    - PSPACE: good enough; EXPTIME: no good. Sure?
    - From worst case to average case?
    - I share Vardi's suggestion:
        - Leave «normal theoretical approaches» or integrate/complement them with
        - «a theory of folklore and common sense»

How to conclude?

- (More than) a few years ago I concluded:
    - Be optimistic (I am never been so much)
    - Be stubbhorn (I am always been, but …)
- And now?
    - (Continue to) Be heroes (tough advise!)
    - Hard to be «superheroes» (rather we are (*if* we are) *poor* … real heores)
    - Perhaps we (better: *you*) could be *smart heroes*:
        - Diplomatic heroes
        - Politics (in a generalized sense) is always dominant
        - Pursue and support hard skills but do not forget the soft ones!
- After all: (let’s) try to remain (a little) optimistic … and to make the glass a little fuller