Computing Beyond Algorithmics

Cristian S. Calude
University of Auckland, New Zealand
www.cs.auckland.ac.nz/˜cristian

March 18, 2005

1 If acquiring knowledge seems expensive, try ignorance![1]

2 Understanding computation

Fingers, tally sticks, and the abacus were the first tools to carry out simple computations. The mechanical systems invented by Leibniz were capable of fairly large multiplications. More recently, Turing machines were invented to mimic the computation done by a human being. For over seventy years the Turing machine model of computation has defined what it means to "compute" a (mathematical) function and to "generate/verify" a (mathematical) proof; the foundations of the modern theory of computing are based on it.

The truth of mathematical statements is as objective and independent of the physical reality as Plato or Gödel believed it to be; however, the way truth is revealed to humans or machines is through the physical world, so the very existence of these statements is ultimately conditioned not only by logical restrictions, but also by the physical laws and by the resources available in the real universe (for example, according to Landauer-Lloyd limit, any computation using more then 10^{120} bits is fantasy). This is equally true for abstract computation which becomes "real" only as a physical process.

Gödel's "interesting axiom", *Die Welt ist vernünftig*[2], does not contradict Gödel's incompleteness theorem as the formal axiomatic systems *evolve* as the laws of physics evolve (at least with the change of the states of the universe).

A simple analysis shows that the physical process corresponding to a Turing computation (the running of an algorithm) is very special, namely it is *closed*: no new input is accepted once the computation has begun. Most "real" computations, from internet protocols to robots, from quantum and chemical to biological computations, to cite just a few, lie beyond the Turing model because the computing agent interacts with the environment which cannot be simulated by a Turing machine.

[1] This section is deliberately empty.

[2] The world is reasonable/rational/sensible/intelligible.

A concrete example, light computing, will be discussed laster. **The challenge is to find models of computation describing the new computing realities**.

3 Turing's barrier

Turing's Thesis, according to which every algorithm capable of effectively computing a function can be simulated by a Turing machine, defines a limit/barrier on the class of functions one can hope to compute.

This thesis was extrapolated to say that "a Turing machine can simulate any computer". This later form, to which Turing (probably) would not have subscribed, can be easily refuted by considering interactive protocols which go beyond algorithmics.

But even at the level of function computability there is an enormous interest in transgressing Turing's barrier. Why? Because **science means/is computation**[3], hence the limits of science are the limits of our computational capability.

4 A case study: computing with light

Light computing is digital computing using laser light instead of electricity, and holograms instead of silicon computer chips. Why use laser light instead of electricity? First, light travels thousands of times faster than electrons (more precisely, electronic signals) in computer chips. Secondly, light computers could be made of inexpensive plastic and glass that are easier to manufacture than the sand from which electronic computer chips are made (via a very expensive refining). Thirdly, sophisticated programs that run slowly even on today's supercomputers (for applications in weather prediction, speech recognition, high resolution graphic) could be adequately run on light computers.

A beam of light can be also used to speed-up silicon computers, and even push their capability beyond the Turing barrier. This can be obtained at a very low cost by using a normal PC augmented with a source of quantum random bits—readily achievable with the quantum mechanical random number generator *Quantis* (available as an OEM component which can be mounted on a plastic circuit board or as a PCI card). This hybrid computer, PC + Quantis, capable of supplying a (theoretically, arbitrarily) long string of quantum random bits sufficiently fast for cryptographic applications, is a (provably) better computing agent for probabilistic algorithms, and has capability beyond Turing's barrier (as quantum random bits cannot be obtained by software pseudo-random generators).

[3] Indeed, if science is a procedure for producing a set of rules for answering questions posed about the universe, then to answer a scientific question amounts to produce a computer program whose running—computation—produces the answer to the question as its output.