Theory of Computing: A Scientific Perspective (Extended Abstract)*

Oded Goldreich[†] Avi Wigderson[‡]

August 2, 1997

Theory of Computation (TOC) seeks to understand computational phenomena, be it natural, man-made or imaginative. TOC is an independent scientific discipline of fundamental importance. Its intrinsic goals (those which were achieved, those which are yet to be achieved, and those which are yet to be defined) transcend the immediate applicability to engineering and technology.

Research in TOC has been extremely successful and productive in the few decades of its existence, with continuously growing momentum. This research has revolutionized the understanding of computation and has deep scientific and philosophical consequences which will be *further* recognized in the future. Moreover, this research and its dissemination through education and interaction was responsible for enormous technological progress.

Much of the full version of our manuscript [2] is devoted to substantiating the strong statements made above. Here, due to space limitations, we merely list a few of the fundamental achievements of TOC.

- Revolutionizing the perception of knowledge and information, stressing that different representations of the same information may not be computationally equivalent. Consequently, TOC has emphasized the importance of data representation, and developed efficient methods for its organization and manipulation,

- Revolutionizing the approach to problem-solving via the explicit introduction of the concept of an algorithm and measures for its efficiency, and the development of general techniques for the design of algorithms.

- Initiating the study of computational intractability. This study led to an understanding of the intrinsic difficulty of many basic problems in computer science as well as in other sciences: Showing that these problems are, in some form, NP-Complete is taken as strong evidence to their intrinsic complexity and thus a concept of TOC came to play a fundamental role in diverse scientific disciplines. Furthermore, TOC was able to utilize computational intractability; this is what Modern Cryptography is all about (cf., [1]). Computational intractability was shown to be necessary and sufficient for a variety of natural cryptographic tasks such as encryption and signatures.

- Revolutionizing the understanding and usage of randomness. In particular, randomness is used as a powerful tool in the design of algorithms. A computational theory of randomness

[*] A preliminary version of the full paper is available from `http://theory.lcs.mit.edu/~oded/toc-sp.html`.

[†] Department of Computer Science and Applied Mathematics, Weizmann Institute of Science, Rehovot, ISRAEL. E-mail: `oded@wisdom.weizmann.ac.il`

[‡] Institute for Computer Science, Hebrew University, Givat Ram, Jerusalem, ISRAEL. E-mail: `avi@cs.huji.ac.il`

has been developed reshaping the understanding of this fundamental concept and yielding a sound notion of a pseudorandom generator. The introduction of randomness into the domain of proofs has revolutionized the latter notion leading to fundamental and useful concepts such as interactive proofs, zero-knowledge proofs and probabilistically checkable proofs.

- Initiating the study of parallel and distributive systems. The study of parallel algorithms resulted in amazing ways to get around "inherently sequential" tasks. The study of distributed environments resulted in models and methods of coordination of multiple agents under various circumstances including unreliable communication and faulty/malicious agents.
- Introducing novel conceptual frameworks and conventions in the analysis of phenomena and algorithms; including the asymptotic analysis, the worse-case (or adversarial) approach, competitive analysis and so on. Structure is typically revealed when adopting these frameworks, whereas it is obscured by unjustified assumptions on "typical behavior" of a phenomena which is not well-understood.

We stress that the achievements mentioned above are more or less equally spread over the last 30 years, and many are very recent. Indeed, the rate of progress done by TOC in these years is astonishing and there is no inherent reason for this progress to stop.

The success of TOC is directly correlated to the extremely high quality and creativity of researchers in TOC, to their independence, and to the fundamental (and exciting) nature of the questions TOC addresses. In order for the Theory of Computing to prosper in the future it is essential that TOC attracts the same calibre of researchers, that Theoretical Computer Scientists concentrate their research efforts in Theory of Computing and that they enjoy the freedom to do so. Free pursuit of their research interests may well lead individual scientists to work closely with/in application areas. Indeed, our field has already an admirable tradition where many TOC leaders (undirected and un-forced) chose to redirect part of their research so as to strongly influence application areas as well as other sciences. Yet, decisions taken by individual scientists following their own understanding of the discipline differ drastically from attempts to direct the whole discipline towards directions which are not intrinsic to it. Thus we completely reject the opinion, which has been spreading in our community in the last few years, that the prosperity of TOC depends on service to other disciplines and immediate applicability to the current technological development.

We claim that these dangerous feelings within the TOC community, leading to the willingness to dictate non-intrinsic directions to its researchers, are not the outcome of external pressures alone. They also result from two internal sources, which have to be recognized, understood and then counteracted.

The first source is a deep (but unjustified) feeling of frustration among some members of the TOC community. The frustration is due to unrealistic expectations by which the TOC community should have been able to gain by now an almost full understanding of the nature of efficient computation. The unrealistic nature of these expectations stems from the un-imagined (by the founders of the field) depth, richness and difficulty of central TOC questions, revealed in the last 20 years. It is not surprising that while these facts generated frustrations in a young, inexperienced field like ours, the same facts generated increasing respect and appreciation for TOC in Mathematics and other more mature sciences. What should be concluded from our short history is positive: our deep unsolved problems, the understanding and techniques we gathered so far, and the continuous introduction of the computational point of view to more diverse natural and artificial phenomena, offer a great agenda of research in TOC for the 21st century.

The second source of internal problems is the lack of a "leadership group", deeply convinced of the importance of the discipline, which is willing and able to oppose pressures from the outside, as well as further this conviction to the junior TOC generations. Again, some of this stems from TOC being a young, politically inexperienced field, pampered for a long time due to practical interest in computer science. Thus our leaders have chosen to concentrate on research (with phenomenal success), but have neglected to ensure the same atmosphere of (economic and spiritual) freedom for the younger generations. This can be remedied, by a great public relations offensive of our leaders on the funding agencies and the university administrations as well as the general scientific community. We strongly feel that it is nearly trivial to "sell" TOC as a remarkable, continuous success story, whose future findings are even likely to exceed the past ones both in intrinsic scientific interest as well as influence on technology and other sciences. We recognize that doing this requires sacrifice of time and effort from our leaders, and call upon them to take on this important chore, just as their peers in other sciences like Physics and Biology have been doing for decades. The fact that our research needs are negligible compared to the needs of these other sciences (and even to those of experimental computer science) should help these efforts considerably.

It is clear that despite the measures suggested above, which will hopefully improve the funding and job situation in TOC, we have reached the end of the era of exponential growth and unlimited support. Thus, it is more crucial than ever that TOC continues to attract the best students to its ranks. We believe again that this is an easy task, achieved via the teaching of the great achievements of TOC research and its even greater challenges. Likewise, it is crucial that TOC sustains the complete academic freedom that enabled past success.

To summarize, TOC is a relatively new scientific discipline of fundamental importance, which has been extremely successful and is still far from achieving its intrinsic goals. The intellectual challenges of TOC are gigantic and of the greatest importance. It is thus essential that this discipline be given a high priority, both inside computer science and among the sciences. It is up to us to ensure this, via education of the world outside TOC on our achievements, and via continuous research of the same quality on our scientific agenda.

References

[1] O. Goldreich. On the Foundations of Modern Cryptography. In the proceedings of *Crypto97*, Springer LNCS, Vol. 1294, pp. 46–74. Also available from `http://theory.lcs.mit.edu/~oded/tfoc.html`.

[2] O. Goldreich and A. Wigderson. Theory of Computing: A Scientific Perspective. Available from `http://theory.lcs.mit.edu/~oded/toc-sp.html`. May 1996.