Journal of Universal Computer Science, vol. 2, no. 5 (1996), 242-244
submitted: 13/5/96, accepted: 13/5/96, appeared: 28/5/96 © Springer Pub. Co.

THE FINITE, THE UNBOUNDED AND THE INFINITE [1]

Cristian Calude
Computer Science Department, The University of Auckland, Private Bag 92019,
Auckland, New Zealand; email: cristian@cs.auckland.ac.nz.

This issue of *J. UCS* is devoted to the proceedings of the Summer School "Chaitin Complexity and Applications" organised by the *Black Sea University,*[2] and the *Centre for Discrete Mathematics and Theoretical Computer Science,*[3] in Mangalia,[4] Romania, from June 27 to July 6.[5] We have grouped the following ten papers under the title[6] of these introductory notes.

The School has focused on basic results of AIT[7] and their relevance for understanding the limits of classical/constructive/finite precision mathematics and of mathematical foundations of cryptography. Applications to computer algebra and efficient Lisp programming, as well as a sketch of a quantum information theory have been also presented.

Three people are universally credited with co-discovering some of the basic ideas of AIT: G. Chaitin, A. Kolmogorov and R. Solomonoff.[8] Chaitin has contributed the largest body of work to AIT and continues to be very active at the present time; the School was very fortunate to have him as a *key-note* speaker.

[1] C. Calude (ed.). *The Finite, the Unbounded and the Infinite, Proceedings of the Summer School "Chaitin Complexity and Applications",* Mangalia, Romania, 27 June – 6 July, 1995.

[2] The BSU is a multinational institution (a NGO) aimed at a non-formal education relating to the key issues of the Black Sea Region. Established in 1992, the University offers postgraduate short-term courses targeted at the specific needs of the region, particularly with regard to the shared concerns with the culture, economy and ecology of the Black Sea countries. The BSU organizes every year several summer courses in Mangalia, from ecology to economy, through applied or theoretical sciences.

[3] The Centre for Discrete Mathematics and Theoretical Computer Science, CDMTCS, which is a joint venture involving the Computer Science and Mathematics Departments of the Universities of Auckland and Waikato, New Zealand, was founded in 1995 to support basic research on the interface between mathematics and computing. More details and up-to-date information can be found at the url `http://www.cs.auckland.ac.nz/CDMTCS/index.html`.

[4] Mangalia is a small Romanian city offering a delightful sea shore—the sun shines and the sea sings its waves—, large orchards, vineyards, and many beautiful traces of ancient civilizations (Hellenic, Roman, Byzantine, Ottoman). It dates back to the 6th c.BC, when it was a Doric colony called Callatis.

[5] A presentation of this event, by F. Geurts, has appeared in the *EATCS Bull.* 57(1995), 276; more details, including some pictures are available from the url `http://www.cs.auckland.ac.nz/CDMTCS/docs/chaitin.html`.

[6] Suggested by George Markowsky.

[7] AIT stands for *A*lgorithmic *I*nformation *T*heory. The *information* part of the name comes from Shannon's information theory, that first proposed a quantitative measure of the amount of information; the *algorithmic* part of the name comes from the fact that algorithms (programs) are used for measuring information content.

[8] Some authors use instead of AIT the name *Kolmogorov complexity*; we find this tendency both unfair and unfortunate.

*

The first four papers deal with the basics of AIT; three papers are focussing on applications; two contributions discuss Chaitin ToyLisp, and the last paper presents some current open problems in AIT. Another contribution of the School, namely two proofs for the fact that the *program-size complexity computes the halting problem*, has appeared in a note jointly written by G. Chaitin, A. Arslanov and C. Calude in the *EATCS Bull.* 57 (1995), 198-200.

The first contribution is an elementary, gentle presentation of AIT titled *Introduction to Algorithmic Information Theory* is written by George Markowsky. The presentation usesa a “real” programming language, Logo[9] (more exactly, WinLogo).

Greg Chaitin contribution explores the limits of mathematics and his results enhance and strengthen Gödel’s incompleteness theorems, which many regard as the most fundamental to the foundations of mathematics.[10] Chaitin’s new definition of a self-delimiting universal Turing machine, that is easy to program and runs very quickly, provides a new foundation for AIT. Previously, AIT had an abstract mathematical quality; now it is possible to write down executable programs that embody the proofs of the main theorems. In Chaitin’s words, *AIT goes from dealing with remote idealized mythical objects to being a theory about practical down-to-earth gadgets that one can actually play with and use.* The reader can play with the new software in Java from the url `http://www.research.ibm.com/people/c/chaitin/`.

A note written by C. Calude and C. Grozea offers a new and simpler proof of Kraft-Chaitin inequality, one of the most important technical tools used in AIT.

The fundamental atoms processed by quantum computation (based upon a model of universal quantum computer whose elementary unit is a two-port interferometer capable of arbitrary $U(2)$ transformations) are the quantum bits, which are analyzed from the AIT point of view in the paper *Quantum algorithmic information theory*, by Karl Svozil.

The next two papers are very challenging. The conclusion reached by Helmut Jürgensen and Lynda Robbins in their paper *Towards foundations of cryptography* is: *there is no perfect secrecy!*. By addressing the question *Is finite precision arithmetic useful for physics?* Françoise Chaitin-Chatelin is discussing some examples, drawn from numerical analysis, which illustrate the subtle interplay between the discrete and the continuous in solving equations from physics.

Doru Ştefănescu, in *Polynomials, constructivity and randomness*, presents some effective characterizations of prime elements in a polynomial ring and polynomial factorization techniques. The possibility of an effective version of Hilbert’s irreducibility theorem and the probabilistic techniques of Berlekamp are also discussed.

Two papers, *Chaitin’s ToyLisp on a connex machine*, by Gheorghe Ştefan and Mihaela Maliţa, and *Toy Lisp interpreter on a connex machine*, by Bogdan

[9] Logo is actually LISP dressed up so it can be seen out on the street!

[10] The significance of these theorems go beyond mathematics; for example, they are very central in the philosophy of consciousness as discussed by Roger Penrose books *The Emperor’s New Mind* and *The Shadows of the Mind* (Oxford University Press, 1990, 1995).

Mîţu and Corina Mîţu, are discussing a new model of universal computation (the connex machine) and an efficient implementation of Chaitin's ToyLisp on this machine.

*

I would like to thank:

– all invited lecturers for their superb contributions,
– Professor Mircea Maliţa, the driving force of the BSU, and his team, for the effort put in organising the School,
– Professors Michael Detlefsen and Hermann Maurer, for suggesting *J. UCS* as a vehicle for the proceedings of the School,
– the CDMTCS for its support,
– and, least but not last, the wonderful audience, for the receptivity and interest (some students, e.g. A. Arslanov, C. Grozea, have already started to publish in AIT).