2017 Knuth prize is Awarded to Oded Goldreich

June 13, 2017

The 2017 Donald E. Knuth Prize will be awarded to Oded Goldreich of the Weizmann Institute of Science for fundamental and lasting contributions to theoretical computer science in many areas including cryptography, randomness, probabilistically checkable proofs, inapproximability, property testing as well as complexity theory in general. Goldreich has, in addition to his outstanding research contributions, advanced these fields through many survey articles and several first class textbooks. He has contributed eminent results, new basic definitions and pointed to new directions of research. Goldreich has been one of the driving forces for the theoretical computer science community for three decades.

Goldreich's work within cryptography has addressed several fundamental issues. While still being a post-doc, jointly with Goldwasser and Micali, Goldreich formulated the concept of a pseudorandom function. Such a function, while being efficiently computable, cannot be distinguished from a truly random function by an efficient computation that only has access to the function as a black box. Not only did this paper formulate this notion but also demonstrated how this could be achieved based on the existence of a pseudorandom generator, an equally basic but simpler notion.

Goldreich, in two distinct papers, both joint with Micali and Wigderson, provided additional corner-stones for cryptography. The first paper demonstrated that the fundamental notion of zero-knowledge which is the basis for the establishment of secure cryptographic protocols, could be applied in a much more general setting than known previously. This paper showed that all languages in NP have zero knowledge interactive proofs. In addition, it also showed that zero knowledge interactive proofs extend to some languages not known to be in NP (i.e., the graph non-isomorphism problem). The second paper showed the enormous power of secure multi-party computation and established that any efficiently computable function could be evaluated in a secure way given an honest majority and the existence of a trapdoor function.

The Goldreich-Levin hard-core predicate is a diamond of complexity theory. It provides a predicate that can be used to extract random-looking bits from any one-way function and is the starting point of many constructions based on general one-way functions. It also gives the first example of an efficiently list-decodable code and its influence stretches far beyond cryptography.

While property testing existed prior to the work of Goldreich, Goldwasser

and Ron, their paper introduced property testing of combinatorial objects and turned a collection of results into a well defined research area, giving the appropriate definitions, deriving basic result and pointing towards a rich area of problems. On a similar note, Goldreich's work with Bellare and Sudan significantly advanced the technology of creating probabilistically checkable proofs and hence inapproximability result. This work also introduced the long code which has been instrumental in later developments.

The textbooks and the many surveys written by Goldreich have been highly influential in educating the next generation of computer scientists. The two-volume textbook on "Foundations of Cryptography" fulfills the promise of its title and indeed has inspired many to work in this field. The forthcoming textbook on property testing is likely to similarly strengthen and accelerate the development of that field.

Goldreich received his PhD at the Technion in 1983. He was a post-doc at MIT (1983-86), held a faculty position at the Technion (1983-1994) and since 1994 he has been a Full Professor at the Weizmann Institute of Science. He has held visiting positions at several institutes.

Prize Committee: Allan Borodin, Chair (University of Toronto), Avrim Blum (Carnegie Mellon University), Shafi Goldwasser (MIT and Weizmann Institute), Johan Håstad (KTH - Royal Institute of Technology), Satish Rao (University of California, Berkeley), and Shanghua Teng (University of Southern California).