2018 Knuth Prize is Awarded to Johan Håstad

August 6, 2018

The 2018 Donald E. Knuth Prize will be awarded to Johan Håstad of KTH Royal Institute of Technology for his long and sustained record of milestone breakthroughs at the foundations of computer science, with huge impact on many areas including optimization, cryptography, parallel computing, and complexity theory. Håstad's multiple seminal works have not only resolved longstanding deepest problems central to circuit lower bounds, pseudorandom generation, and approximability, but also introduced transformative techniques that have fundamentally influenced much of the subsequent work in these areas.

Håstad's Ph.D. thesis — the winner of the 1986 ACM Doctoral Dissertation Award — was not just deep, but also truly beautiful. With his elegant *switching lemma*, he obtained an almost-optimal exponential lower bound on the size of constant-depth Boolean circuits for the parity function that — as Andrew Yao's earlier exponential-size bound showed — had tremendous consequence to structural complexity theory. The importance of this work for circuit complexity can be hardly overestimated and goes well beyond this concrete result, as recognized by the 1994 Gödel Prize. Both sets of ideas, sophisticated use of probabilistic methods as well as the power of random restrictions, have shaped the landscape in many other areas, from parallel complexity to learnability.

Håstad's body of work in probabilistically checkable proofs (PCP) and approximability of optimization problems has transformed the field. In the mid-1990s, he published two landmark papers, "Clique is Hard to Approximate Within $n^{1-\epsilon}$ and "Some Optimal Inapproximability Results," the latter of which was recognized by his second Gödel Prize (2011). As complexity-theoretical breakthroughs, Håstad constructed almost optimal PCPs, where optimality holds with respect to parameters such as amortized free-bit complexity and total number of queries. He then established optimal "approximation resistance" of various constraint satisfaction problems namely that one cannot do better in terms of worst-case performance ratio than the basic input-oblivious algorithm that simply picks a random assignment to the variables. These PCPs led to optimal inapproximability results for MaxClique, MaxLin2, and Max3SAT as well as to the best known hardness results for approximating other optimization problems such as maxCUT. His proofs introduced a treasure trove of ideas — particular the Fourier analytic techniques— that has influenced nearly all subsequent work in hardness of approximation.

Håstad's joint paper with Russell Impagliazzo, Leonid Levin, and Michael

Luby, “A Pseudorandom Generator from any One-way Function” is a gem in complexity theory and cryptography. The result established by this paper is of lasting importance, since it relates two fundamental concepts which are central to cryptography and to complexity theory at large. On the one hand, pseudorandom generation — with numerous applications in cryptography from encryption to authentication — captures the efficient deterministic construction of sequences, that are “effectively” random in any polynomial-time computation, from shorter uniformly distributed sequences. On the other hand, one-way functions — whose existence is the most basic assumption in modern cryptography — formulate the notion of a process that is easy to effect, but hard to reverse in the average-case sense. Håstad’s joint paper provided the ultimate result by proving that pseudorandom generators exist if and only if one-way functions exist. Thus, two fundamental phenomena in their most general and “pure” form — i.e., computational difficulty and pseudorandomness generation — are proved to be equivalent.

Johan Håstad received his BS in Mathematics from Stockholm University in 1981, his MS in Mathematics from Uppsala University in 1984, and his PhD in Mathematics from MIT in 1986. He is currently a professor the Royal Institute of Technology in Stockholm, Sweden.

2018 Knuth Prize Committee: Allan Borodin, (U. of Toronto), Alan Frieze (CMU), Avrim Blum (TTIC), Shafi Goldwasser (UC Berkeley), Noam Nisan (Hebrew U.) and Shang-Hua Teng (USC, Chair).