Logikseminariet Stockholm–Uppsala

Michael O. Rabin
Harvard University

Randomness and Non-Transferable, Non-Publishable Proofs

The past three decades saw the introduction of surprising new modes of proof from theoretical computer science into mathematics. The randomized primality test establishes the primality of a large integer by employing a small number of coin tosses. Zero Knowledge Proofs enable a Prover to convince a Verifier that he the Prover knows the solution for a mathematical problem without revealing anything about the solution itself. The method of Probabilistically Checkable Proofs allows the re-writing of any proof into a form that enables a Verifier to check the proof by looking at as few as 20 bits of the text of the proof. All these methods employ randomization and yield proofs of a radically novel nature. Computers are employed to establish difficult mathematical results. We shall explain these new notions of proof and discuss their meaning and implications. The talk will be self-contained.

Onsdag 13 september kl. 10.00–11.45,
sal 14 (**Gradängsalen**), hus 5,
Kräftriket, Stockholm.

http://www.math.su.se/~jesper/seminarier/