Proof-of-work Certificates for High Complexity Mathematical Computations

Erich Kaltofen - NCSU and Duke University

Computations done by high-power cloud servers such as a Google data center can yield outputs that are easy to verify, such as the factors of an integer, but outputs can also be non-trivial to certify quickly, such as the determinant of a high-dimensional sparse matrix like the Macaulay matrix or the summation of a very large number of consecutive prime numbers.

Interactive proof protocols speed the complexity of the output verification by interaction between the high-power prover and the verifier, in fact, a polynomial-time verifier can certify all computational problems of PSPACE. The interaction can be removed to yield a proof-of-work certificate whose correctness is based on cryptographic assumptions on what the prover cannot ever compute. I will give a selection of certificates, among them our certificate for sum-of-squares proofs of inequalities and a version of the Goldwasser-Kalai-Rothblum [2008] protocol on the example of the summation of exponentially many consecutive prime numbers.