Wigderson@Fields: Randomness, Pseudorandomness and Derandomization

September-14-10
2:57 PM

Problem $x \in [2^n, 2^{n+1}]$ is it prime?

1975 efficient probabalistic algorithm.

2002 efficient deterministic algorithm.

Problem Find a prime between 2^n & 2^{n+1}.

only probabilistically easy.

Polynomial Identities To check if a polynomial in many variables, given perhaps as a product, is zero, feed in random numbers. Without randomization we don't know how to do it.

Problem Find all large ($>\epsilon$) Fourier Coeffs of a function $f: (\mathbb{Z}/2)^n \to \mathbb{C}$.

Problem Estimate the volume of a convex $K \subset \mathbb{R}^d$ ($d >> 1$) given by a set of inequalities.

Meta-Theorem If there are natural hard problems, then randomness can be efficiently eliminated.