

1046-05-1085

Venkatesan Guruswami*, venkat@cs.washington.edu. *Coding theory and Pseudorandomness.*

There is a rich interplay between coding theory and computational complexity theory that has enriched both disciplines over the years. In particular, error-correcting codes have been instrumental in several advances in the subject of pseudorandomness, leading to explicit constructions of objects (such as expander graphs, randomness extractors, pseudorandom generators, etc.) with desirable properties similar to those achieved by random objects.

This talk will survey some recently discovered interconnections between coding theory and pseudorandomness, including the construction of lossless expanders from a variant of Reed-Solomon codes, and the construction of Euclidean sections and compressed sensing matrices from expander codes. We will also mention some coding-theoretic challenges for derandomization, resolving which will lead to explicit codes with important properties. (Received September 14, 2008)