abstract

Video of this lecture

COMPUTER SCIENCE/DISCRETE MATH II

Topic:

Speaker:

Affiliation:

Date:

Time/Room:

An epsilon-biased set X in {0,1}^n is a set so that for every non-empty set T in [n] the following holds. The random bit B(T) obtained by selecting at random a vector x in X, and computing the mod-2 sum of its T-coordinates, has bias at most epsilon. Such sets may be viewed as generating matrices of binary error correcting codes of distance (1/2 - epsilon), as well as pseudorandom sets in the sense that all their nontrivial Fourier coefficients are at most epsilon in absolute value. Determining the smallest size of such an epsilon-biased sets X, and explicitly constructing them has a long history.

We shall survey three constructions of epsilon-bias sets, each is better in some range of parameters. The first construction is by Alon, Goldreich, Hastad and Peralta and gives an explicit epsilon-biased set X of size at most order (n/eps)^2. The second construction, of Alon, Bruck, Naor, Naor and Roth, gives a set X of size at most roughly n/eps^3. The third construction is by Ben-Aroya and Ta-Shma and gives roughly (n/eps^2)^{5/4} for epsilon at least n^{-0.5} (which is better than previous constructions for eps = 1/n, for example). The last two constructions (can) use algebraic-geometric codes. If time permits, we shall discuss the connection to algebraic geometry codes in more detail.