

abstract

COMPUTER SCIENCE/DISCRETE MATH II

Topic:

Speaker:

Affiliation:

Date:

Time/Room:

Moran, Naor and Segev have asked what is the minimal $r = r(n, k)$ for which there exists an (n, k) -monotone encoding of length r , i.e., a monotone injective function from subsets of size up to k of $\{1, 2, \dots, n\}$ to r bits. Monotone encodings are relevant to the study of tamper-proof data structures and arise also in the design of broadcast schemes in certain communication networks.

To answer this question, we develop a relaxation of k -superimposed families which we call α -fraction k -multi-user tracing $((k, \alpha)$ -FUT families). We show that $r(n, k) = \Theta(k \log(n/k))$ by proving tight asymptotic lower and upper bounds on the size of (k, α) -FUT families and by constructing an (n, k) -monotone encoding of length $O(k \log(n/k))$. We also present an explicit construction of an $(n, 2)$ -monotone encoding of length $2 \log n + O(1)$, which is optimal up to an additive constant.

Joint work with Noga Alon.