abstract

COMPUTER SCIENCE/DISCRETE MATH II
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

The 'method of multiplicities' (which is a variant of the polynomial method in combinatorics) is a very effective method to derive combinatorial bounds on the size of certain sets in vector spaces over finite fields. In this work we extend this method to derive tighter bounds on Kakeya sets and mergers and apply these tighter bounds to build better seeded extractor. Using our extended method we derive the following results:

1) A lower bound on the size of Kakeya sets which is tight to within a factor of 2 of the known upper bounds (previous bound were off by an exponential factor in the dimension of the space).

2) A tighter analysis of the 'Curve Merger' from [DW08] which significantly reduces its seed length and allows us to use it over smaller finite fields than before.

3) A new construction of seeded extractors (based on the improved merger analysis) that have logarithmic seed and sub-linear entropy loss. Previous constructions of extractors had either super-logarithmic seed or linear entropy loss.

One of the main ingredients in our extended method is a 'multiplicity enhanced' version of the Schwartz-Zippel lemma which allows us to apply it to polynomials of degree higher than the field size.