

The Pseudo-random world

Taoyang Wu

February 23, 2007

Pseudorandomness is an important concept and has important applications in mathematics and computer science. In this talk we are going to focus on two topics: pseudo-random sets and expanders.

The idea of pseudo-random sets was used by Green and Tao to solve the famous conjecture that the primes contains arbitrary long arithmetic progressions. In other words, for each natural number n , there exists a sequence $a, a+b, a+2b, a+3b, \dots, a+nb$ such that all items in this sequence are primes.

On the other hand, expanders is a key concept in the proof of $SL=L$ by Reingold and a combinatorial proof of PCP, probabilistic checkable proof, by Dinur.

The talk is rather informal and I would like to give a personal view on the following two problems: what is pseudorandomness and why it is so useful.