Expanders, Psuedorandomness, Derandomization

Part I – Introduction

Introducing some of the key players

1. Resilient functions.
2. Deterministic extractors:
   (a) For oblivious and non-oblivious bit-fixing sources.
   (b) For two independent sources (and Ramsey graphs).
   (c) For affine sources.
3. Seeded extractors.

Deterministic amplification

1. A review of probabilistic inequalities, Markov, Chebychev, Chernoff.
2. Deterministic amplification by bounded independence.
3. Deterministic amplification by expander walks.
4. Deterministic amplification by extractors and dispersers.
5. (-) Approximating frequency moments efficiently in small space.

Small bias with respect to linear tests

1. The Fourier Transform.
2. (-) Back again to resilient functions.
3. ε-bias sets (and almost balanced binary error correcting codes).
4. Almost k–wise independence
5. (-) Testing linearity

AC^0

1. Parity is hard for AC^0.
2. Average-case hardness for AC^0.
3. Polylog-wise independence fools AC^0.

Error-correcting codes and seeded extractors

1. A review of error-correcting codes and list-decoding.
2. Strong extractors and list-decoding.
3. Trevisan's extractor.

Part II – Two-source extractors

Two-soucres extractors

1. Non-malleable extractors.
2. The Chattopadhyay-Zuckerman construction.

Part III – The Hardness vs. Randomness Paradigm

The Paradigm

1. Pseudorandom generators.
2. The "Hardness vs. Randomness" paradigm and the Nisan-Wigderson PRG.

Hardness implies de-randomization

1. A review of error-correcting codes and local-decoding.
2. List-decoding RS codes.
3. The STV Worst-case to average-case reduction.
4. If E does not have sub-exponential circuits then $\mathsf{BPP} = \mathsf{P}$.

De-randomization implies hardness

1. Karp-lipton theorems, $\mathsf{PSPACE} \subseteq \mathsf{P/poly}$ implies $\mathsf{PSPACE} = \mathsf{MA}$.
2. $\mathsf{NEXP} \subseteq \mathsf{P/poly}$ implies $\mathsf{NEXP} = \mathsf{MA}$ (IKW).
3. Derandomizing PIT means proving circuit lower bounds (IK).

Part IV – Advanced topics

The many ways a graph can be expander

1. Combinatorial and algebraic expansion.
2. Ramanujan graphs and the LPS construction.
3. The zig-zag construction.
4. Better combinatorial expansion: explicit expanders with the unique neighbor property.

Better list-decodable codes and extractors

1. Parvaresh-Vardy codes
2. The Guruswami-Umans-Vadhan extractor.
3. The Dvir-Wigderson merger.