On the P vs. BPP problem

Part I – Local list decoding

Local unique decoding for Reed-Muller codes.

List decoding

1. The Johnson's bound
2. Reed-Solomon code (Sudan), and,
3. Hadamard code (The Goldreich-Levin Theorem)

Local list decoding

1. Reed-Muller codes (STV)
2. Concatenated codes.

Part II – The Hardness vs. Randomness Paradigm

Hardness implies de-randomization

1. The "Hardness vs. Randomness" paradigm and the Nisan-Wigderson PRG.
2. The STV Worst-case to average-case reduction.
3. 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 III – Advanced Topics (we will do only a few of the topics below)

Natural proofs

Randomness extractors

1. Extractors
2. Another look at reconstruction PRGs
3. Trevisan's extractor.
4. The Shaltiel-Umans extractor.
5. The Guruswami-Umans-Vadhan extractor.

Algebraic Nisan-Wigderson

PIT and factoring