The most important questions of life are, for the most part, really only problems of probability. Strictly speaking one may even say that nearly all our knowledge is problematical; and in the small number of things which we are able to know with certainty, even in the mathematical sciences themselves, induction and analogy, the principal means for discovering truth, are based on probabilities, so that the entire system of human knowledge is connected with this theory.


## Contents

1 Lecture 1, January 3, 2011. Overview and basic concepts
   1.1 Three problems ............................................. 4
   1.2 Basic concepts ............................................. 4

2 Lecture 2, January 5, 2011. Fundamental inequalities, the probabilistic method
   2.1 Application: the probabilistic method ..................................................... 7
   2.2 Chernoff bound for uniform Bernoulli rvs (symmetric random walk) .............. 8
   2.3 Application: set discrepancy ................................................................. 9

3 Lecture 3, January 10, 2011. Overview of applications, Shannon’s coding theorem
   3.1 Shannon’s coding theorem ................................................................. 10

4 Lecture 4, January 12, 2011. Variance, Chebyshev inequality, pairwise independence, hashing
   4.1 Pairwise independence and the second-moment inequality ............................ 13
   4.2 Hash functions ............................................. 13

5 Lecture 5, January 19, 2011. Applications of pairwise (or nearly so) independence
   5.1 Cuckoo Hashing ............................................. 15
   5.2 Improvement to the proof of Shannon’s coding theorem, using linear codes ........ 16
   5.3 Concentration of the number of prime factors: Turan’s proof of a theorem of Hardy and Ramanujan ................................................................. 17

6 Lecture 6, January 24, 2011. Limited linear independence, limited statistical independence, and error correcting codes
   6.1 Statistically independent uniform rvs from linear independence ...................... 18
   6.2 Proof of Thm 16 Part 1: Upper bound on the size of $k$-wise independent sample spaces .... 20

7 Lecture 7, January 26, 2011. Lower bound on $k$-wise indep. sample spaces; applications of $k$-wise independence
   7.1 Proof of Thm 16 Part 2: Lower bound on the size of $k$-wise independent sample spaces .... 22
   7.2 More applications of $k$-wise independence: unique-solving languages in NP ........ 23
# Lecture 8, January 31, 2011. More applications of $k$-wise independence: MIS and derandomization

8.1 Parallel complexity classes ................................................. 24
8.2 Maximal Independent Set .................................................. 24

# Lecture 9, February 2, 2011. Finish MIS; General Chernoff Bd

9.1 Derandomization .............................................................. 26
9.2 General Chernoff bound. Moment generating function ................. 27
9.3 Johnson-Lindenstrauss embedding ......................................... 28

# Lecture 10, February 7, 2011. Johnson-Lindenstrauss embedding $L_2 \rightarrow L_2$

10.1 Normed spaces ............................................................... 29
10.2 The JL method .............................................................. 30
10.3 A related method ............................................................ 31

# Lecture 11, February 9, 2011. Bourgain embedding $X \rightarrow L_{p_r}, p \geq 1$

11.1 Embedding into $L_1$ .......................................................... 34
11.2 Embedding into any $L_{p_r}, p \geq 1$ ......................................... 36


12.1 Sampling a random factored integer $\leq n$ .............................. 37
12.2 The Lovász local lemma ..................................................... 37

# Lecture 13, February 16, 2011. Cont.: Lovasz local lemma

13.1 Proof ......................................................................... 38
13.2 Ramsey numbers ............................................................ 39
13.3 Application: Better $R(k, k)$ lower bound ............................... 40

# Lecture 14, February 23, 2011. Cont.: Lovasz local lemma

14.1 Application: van der Waerden lower bound ........................... 40
14.2 Algorithms based on random processes, IV: Branching Processes .... 41
14.3 Algorithms based on random processes, IV: branching processes. Moser-Tardos algorithm for the local lemma ........................................... 42

# Lecture 15, February 28, 2011. Cont.: MT algorithm for the local lemma

15.1 Algorithms based on random processes, IV: branching processes. Game tree evaluation – upper bound ................................................. 44


16.1 Game tree evaluation: randomized algorithm ........................... 45
16.2 Randomized and distributional complexity: von Neumann - Yao .......... 45
16.3 Algorithms based on random processes, IV: branching processes. Game tree evaluation – lower bound ................................................. 45