Danny Scheinerman
Oral Exam Syllabus

1 Combinatorics and Graph Theory

1.1 Combinatorics

- Enumeration: Bijections, generating functions, binomial and multinomial coeeficients, recurrence relations, inclusion exclusion, Stirling's formula, Bell numbers
- Set systems: Sperner's Lemma, Erdos-Ko-Rado, LYM Inequality, statement of Kruskal-Katona
- Linear Programming: weak duality, strong duality, integer/binary linear programming
- Probabilistic method: Linearity of expectation, Markov's inequality, Chebyshev's inequality, applications to graph theory
- Combinatorial Geometry: Hellys theorem, Caratheodorys theorem, Baranys theorem, Borsuk-Ulam

1.2 Graph Theory

- Matching: Hall's theorm, Konig's theorem, Tutte's Theorem
- Connectivity and Algorithms: Hall's theorem algorithm, Konig's theorem, Tutte's theorem, Prim's algorithm, Kruska'ls algorithm, Dijkstra's algorithm, max-flow-min-cut
- Applications of probabalistic methods to random graphs
- Planarity: Euler's theorm, K_5 and $K_{3,3}$ are nonplanar, statement of Kuratowski's theorem
- Ramsey Theory: Van der Waerden's theorem, statement of Hales-Jewett
- Extremal: Turan's theorem, statement of Regularity Lemma, triangle removal lemma, Roth's theorem

2 Cryptography

- Chapters 7-11 of Introduction to Modern Cryptography by Lubell and Katz
- RSA, ElGamal, DIffie-Hellman key Exchange, Elliptic Curve basics, Discrete Log
- Pollards $p-1$ method, Pollard's Rho method, Baby-Step/Giant-Step algorithm, Discrete Logs via Index Calculus