Basic Course Information

Mondays 4:30-6:30, Room 301
http://www.cs.princeton.edu/courses/cs598f/

Randomized Algorithms

This course will be a seminar designed to focus on the use of randomization in the design of algorithms as well as the formal analysis of such randomized algorithms. Presentations will aim at demonstrating some of the common underlying techniques as well as looking at examples of the many different applications areas where randomization has proved to be an important tool. Techniques include random sampling, randomized incremental constructions, and randomized rounding to name a few. Problems will be drawn from domains including computational geometry, graph algorithms, parallel algorithms, approximation algorithms and online computation.

Prerequisites

The ideal prerequisites for this course will include the algorithmic experience and sophistication equivalent to cos423 (Theory of Algorithms), along with some experience with basic probability theory included in a course such as cos341 (Discrete Mathematics) or math390.

Grading

This course will be offered on the *Pass/D/Fail Only* grading system.

Seminar Format

The format of the class will be in the style of a classic graduate seminar. The majority of lectures will be student presentations based on a combination of papers selected from the literature. Occasional lectures may be given by the instructor or guests.

Required Work

Each student will be asked to give one lecture during the course. Some suggested topics with references are listed below, however students can also speak with the instructor if they wish to propose a different topic of interest. The exact content of the lecture will be left to the discretion of the presentor; papers from the literature may serve as guides, however the speakers may pick and choose as they see fit.

In addition, each student will be asked to turn in one written paper which serves as a summary or tutorial of the material which was presented in class. This paper can be turned in anytime before the dean's date.

Finally, depending on enrollment, there may be some opportunity for students to work in pairs in preparing a lecture and written assignment.

Text books

Although we will not require any text book for this seminar, four books have been placed on reserve in the Engineering Library. The book of Motwani and Raghavan [MR95] is an invaluable reference and tutorial for the current state of the field of randomized algorithms. A great many of the topics we cover are also discussed in detail in this book. The books of Feller [Fel69a, Fel69b] and Billingsley [Bil86] serve as in depth texts for an introduction to the mathematics of probability theory.

Possible Topics and Reading

This list is by no means meant to be exhaustive, rather as representative of many of the techniques and applications involving randomized algorithms. Those topics marked with a "$\star$" are ones which we particularly hope to include in this seminar.

This list is organized primiarily by application areas, although a few headers group papers based on a common technique (and there is some overlap between groupings). Presentations dates/topics will be scheduled with the instructor on a first-come, first-serve basis.

Adversaries, Lower Bounds, and Complexity

- $\star$ Yao's Minimax Principle [Yao77]
- $\star$ Online Adversary Models [RS94, BBK$^+$94]

Hashing and Fingerprinting

- Perfect Hashing [Spr77, Yao81, TY79, FK84]
- Universal Hashing [CW79, FKS84]
- Fingerprinting [Fre77, DL78, Sch80, Zip79]
- Probabilistically Checkable Proofs (PCP)

Computational Geometry

- ⋆ Random Sampling Framework of Clarkson and Shor [CS89, Cla87]
  (a general technique applying to many problems, including convex hulls, Voronoi diagrams, trapezoidal decompositions and linear programming.
- • Binary Space Partitions [PY90]
- • Trapezoidal Decompositions and Triangulations [Sei91]

  General surveys which include many of the above topics can be found in [Cla92, Mul93, Sei93].

Graph Algorithms.

- ⋆ Minimum Spanning Trees (random sampling) [KKT95]
- ⋆ Minimum Cuts (random selection) [KS96]
- • Generalizations to Matroids (generalizations of above) [Kar98, Kar93]

Online Algorithms

- ⋆ Paging, Caching and the k-server problem. [FKL$^+$91, MS91]
- • Scheduling and Load Ballancing [BFKV95, CvW94, Sga97, Sei97] (and Section 4.2 of [Sga98])
- • Robot Navigation

Randomized Rounding in Approximation Algorithms

- ⋆ Linear Programs [RT87, GW94] (also see surveys [MNR97, BV94])
- ⋆ Semi-definite Programs [GW95, KMS98] (and some of [MNR97])

Derandomization

- ⋆ [Rag88, CF90, KM97] to mention just a few (long survey in [LW95]).

Parallel and Distributed Algorithms

- ⋆ Routing [VB81, BH85, KKT91, BPSU97]
- • Maximal Independent Set [Lub86, Lub93]
- ⋆ Choice Coordination and Byzantine Agreement [Rab82, Rab83, CD89]

Number Theory

- • RSA encryption
- • Primality testing

Machine Learning

- • Probably Approximately Correct (PAC) Learning [Val84, Val85, BEHW89]

References

[BBK$^+$94] Shai Ben-David, Allan Borodin, Richard Karp, Gábor Tardos, and Avi Wigderson. On the power of randomization in online algorithms. *Algorithmica*, 11(1):2–14, 1994.

[BEHW89] Anselm Blumer, Andrzej Ehrenfeucht, David Haussler, and Manfred K. Warmuth. Learnability and the Vapnik-Chervonenkis dimension. *Journal of the ACM*, 36(4):929–965, 1989.

[BFKV95] Yair Bartal, Amos Fiat, Howard Karlof, and Rakesh Vohra. New algorithms for an ancient scheduling problem. *Journal of Computer and System Sciences*, 51(3):359–366, 1995.

[BH85] Allan Borodin and John E. Hopcroft. Routing, merging and sorting on parallel models of computation. *Journal of Computer and System Sciences*, 30(1):130–145, 1985.

[Bil86] Patrick Billingsley. *Probability and Measure*. John Wiley & Sons, New York, 1986.

[BPSU97] Allan Borodin, Prabhakar, Baruch Schieber, and Eli Upfal. How much can hardware help routing? *Journal of the ACM*, 44(5):726–741, 1997.

[BV94] D. Bertsimas and R. Vohra. Linear programming relaxations, approximation algorithms and randomization: A unified view of covering problems. Technical Report OR-285-94, Operations Research Dept, MIT, 1994.

[CD89] Benny Chor and Cynthia Dwork. Randomization in Byzantine agreement. In S. Micali, editor, *Randomness and Computing*, volume 5 of *Advances in Computing Research*, pages 443–497. JAI Press, Greenwich, CT, 1989.

[CF90] Bernard Chazelle and Joel Friedman. A deterministic view of random sampling and its use in geometry. *Combinatorica*, 10(3):229–249, 1990.

[Cla87] Kenneth Clarkson. New applications of random sampling in computational geometry. *Discrete and Computational Geometry*, 2:195–222, 1987.

[Cla92] Kenneth Clarkson. Randomized geometric algorithms. In D.-Z. Du and F. K. Hwang, editors, *Computing in Euclidean Geometry*, volume 1 of *Lecture Notes Series on Computing*, pages 117–162. World Scientific, Singapore, 1992.

[CS89] Kenneth Clarkson and Peter Shor. Applications of random sampling in computational geometry, II. *Discrete and Computational Geometry*, 4:387–421, 1989.

[CvW94] Bo Chen, André van Vliet, and Gerhard J. Woeginger. A lower bound for randomized on-line scheduling algorithms. *Information Processing Letters*, 51(5):221–230, 1994.

[CW79] J. Lawrence Carter and Mark N. Wegman. Universal classes of hash functions. *Journal of Computer and System Sciences*, 18(2):143–154, 1979.

[DL78] Richard DeMillo and Richard Lipton. A probabilistic remark on algebraic program testing. *Information Processing Letters*, 7:193–195, 1978.

[Fel69a] William Feller. *An Introduction to Probability Theory and Its Applications*, volume 1. John Wiley & Sons, New York, 1969.

[Fel69b] William Feller. *An Introduction to Probability Theory and Its Applications*, volume 2. John Wiley & Sons, New York, 1969.

[FK84] Michael L. Fredman and János Komlós. On the size of separating systems and families of perfect hash functions. *SIAM Journal on Algebraic and Discrete Methods*, 5(1):61–68, 1984.

[FKL+91] Amos Fiat, Richard M. Karp, Michael Luby, Lyle A. McGeoch, Daniel D. Sleator, and Neil E. Young. Competitive paging algorithms. *Journal of Algorithms*, 12(4):685–699, 1991.

[FKS84] Michael L. Fredman, János Komlós, and E. Szemerédi. Storing a sparse table with $O(1)$ worst case access time. *Journal of the ACM*, 31(3):538–544, 1984.

[Fre77] Rusins Freivalds. Probabilistic machines can use less running time. In B. Gilchrist, editor, *Information Processing 77, Proceedgins of IFIP Congress 77*, pages 839–842. North-Holland, Amsterdam, 1977.

[GW94] Michel X. Goemans and David P. Willaimson. New 3/4-approximation algorithms for MAX-SAT. *SIAM Journal of Discrete Mathematics*, 7(4):656–666, 1994.

[GW95] Michel X. Goemans and David P. Willaimson. Improved approximation algorithms for maximum cut and satisfiability problems using semidefinite programming. *Journal of the ACM*, 42(6):1115–1145, 1995.

[Kar93] David Karger. Random sampling in matroids, with applications to graph connectivity and minimum spanning trees. In *Proc. 34th Symp. on Foundations of Computer Science*, pages 84–93, Palo Alto, November 1993.

[Kar98] David Karger. Random sampling and greedy sparsification in matroid optimization problems. *Mathematical Programming B*, 82(1–2):41–81, 1998.

[KKT91] Christos Kaklamanis, Danny Krizanc, and Thanasis Tsantilas. Tight bounds for oblivious routing in the hypercube. *Mathematical Systems Theory*, 24(4):223–232, 1991.

[KKT95] David Karger, Philip Klein, and Robert Tarjan. A randomized linear-time algorithm to find minimum spanning trees. *Journal of the ACM*, 42(2):321–328, 1995.

[KM97] David Karger and Rajeev Motwani. Derandomization via approximation: An NC algorithm for minimum cuts. *SIAM Journal on Computing*, 26(1):255–272, 1997.

[KMS98] David Karger, Rajeev Motwani, and Madhu Sudan. Approximate graph coloring by semidefinite programming. *Journal of the ACM*, 45(2):246–265, 1998.

[KS96] David Karger and Clifford Stein. A new approach to the minimum cut problem. *Journal of the ACM*, 43(4):601–640, 1996.

[Lub86] Michael Luby. A simple parallel algorithm for the maximal independent set. *SIAM Journal on Computing*, 15(4):1036–1053, 1986.

[Lub93] Michael Luby. Removing randomness in parallel computation without a processor penalty. *Journal of Computer and System Sciences*, 47(2):250–286, 1993.

[LW95] Michael Luby and Avi Wigderson. Pairwise independence and derandomization. Technical Report TR-95-035, ICSI, Univ. of Berkeley, 1995. http://www.icsi.berkeley.edu/~luby/pair_sur.html.

[MNR97] Rajeev Motwani, Joseph Naor, and Prabhakar Raghavan. Randomized approximation algorithms in combinatorial optimization. In D. Hochbaum, editor, *Approximation Algorithms for NP-Hard Problems*, pages 447–481. PWS Publishing Company, Boston, MA, 1997.

[MR95] Rajeev Motwani and Phabhakar Raghavan. *Randomized Algorithms*. Cambridge University Press, New York, 1995.

[MS91] Lyle A. McGeoch and Daniel D. Sleator. A strongly competitive randomized paging algorithm. *Algorithmica*, 6(6):816–825, 1991.

[Mul93] Ketan Mulmuley. *Computational Geometry: An Introduction Through Randomized Algorithms*. Patience-Hall, Englewood Cliffs, NJ, 1993.

[PY90] Michael Paterson and Frances Yao. Efficient binary space partitions for hidden-surface removal and solid modeling. *Discrete and Computational Geometry*, 5:485–503, 1990.

[Rab82] Michael Rabin. The choice coordination problem. *Acta Informatica*, 17:121–134, 1982.

[Rab83] Michael Rabin. Randomized Byzantine generals. In *Proc. 24th Symp. on Foundations of Computer Science*, pages 403–409, 1983.

[Rag88] Prabhakar Raghavan. Probabilisitic construction of deterministic algorithms: Approximating packing integer programs. *Journal of Computer and System Sciences*, 37(2):130–143, 1988.

[RS94] Prabhakar Raghavan and Marc Snir. Memory versus randomization in on-line algorithms. *IBM Journal of Research and Development*, 38:683–707, 1994.

[RT87] Prabhakar Raghavan and Clark D. Thompson. Randomized rounding: A technique for provably good algorithms and algorithmic proofs. *Combinatorica*, 7:365–374, 1987.

[Sch80] Jacob T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM*, 27(4):701–717, 1980.

[Sei91] Raimond Seidel. A simple and fast incremental randomized algorithm for computing trapezoidal decompositions and for triangulating polygons. *Computational Geometry: Theory and Applications*, 1:51–64, 1991.

[Sei93] Raimond Seidel. Backwards analysis of randomized geometric algorithms. In J. Pach, editor, *New Trends in Discrete and Computational Geometry*, volume 10 of *Algorithms and Combinatorics*, pages 37–68. Springer-Verlag, 1993.

[Sei97] Steve Seiden. Randomized algorithms for that ancient scheduling problem. In *Proc. Fifth Workshop on Algorithms and Data Structures*, volume 1272 of *Lecture Notes in Computer Science*, pages 210–223, Berlin, 1997. Springer-Verlag.

[Sga97] Jirí Sgall. A lower bound for randomized on-line multiprocessor scheduling. *Information Processing Letters*, 63(1):149–175, 1997.

[Sga98] Jirí Sgall. On-line scheduling – a survey. In A. Fiat and G. Woeginger, editors, *Online Algorithms: The State of the Art*, volume 1442 of *Lecture Notes in Computer Science*, pages 196–231. Springer-Verlag, Berlin, 1998.

[Spr77] Renzo Sprugnoli. Perfect hashing functions: A single probe retrieving method for static sets. *Communications of the ACM*, 20(11):841–850, 1977.

[TY79] Robert E. Tarjan and Andrew Yao. Storing a sparse table. *Communications of the ACM*, 22(11):606–611, 1979.

[Val84] Leslie Valiant. A theory of the learnable. *Communications of the ACM*, 27(11):1134–1142, 1984.

[Val85] Leslie Valiant. Learning disjunctions of conjunctions. In *Proceedings of the Ninth International Joint Conference on Artificial Intelligence*, pages 560–566, 1985.

[VB81] Leslie Valiant and G. Brebner. Universal schemes for parallel communication. In *Proc. 13th ACM Symp. on Theory of Computing*, pages 263–277, Milwaukee, WI, May 1981.

[Yao77] Andrew Yao. Probabilistic computations: Towards a unified measure of complexity. In *Proc. 17th Symp. on Foundations of Computer Science*, pages 222–227, 1977.

[Yao81] Andrew Yao. Should tables be sorted? *Journal of the ACM*, 28(3):615–628, 1981.

[Zip79] R. E. Zippel. Probabilistic algorithms for sparse polynomials. In *Proceedings of EUROSAM 79*, volume 72 of *Lecture Notes in Computer Science*, pages 216–226. Springer-Verlag, 1979.