

Prefácio

Este texto consiste das notas para um curso apresentado no 26º Colóquio Brasileiro de Matemática no IMPA, Rio de Janeiro, em julho de 2007.

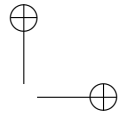
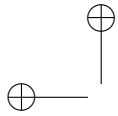
O objetivo do curso “Introdução aos Algoritmos Randomizados” é apresentar a pesquisadores e estudantes da área de ciência da computação as técnicas fundamentais para o desenvolvimento de algoritmos randomizados (também chamados probabilísticos, por alguns autores). O curso tem caráter introdutório: não são assumidos conhecimentos avançados de probabilidade ou de algoritmos. Os conceitos teóricos que se fazem necessários são apresentados no próprio texto, em geral acompanhando os próprios problemas e algoritmos que os demandam. Ao completar este curso, o aluno terá travado contato com o instrumental básico dessa área e com um elenco representativo de algoritmos randomizados — e, em alguns casos, também determinísticos — para diversos problemas combinatórios. Este curso introdutório corresponde a tema de iniciação científica, tem um número mínimo de pré-requisitos, estimula o aluno à investigação científica e ainda não é oferecido regularmente nos currículos das universidades brasileiras.

O projeto para este curso a quatro autores nasceu da tese de doutorado de Vinícius, defendida no Programa de Engenharia de Sistemas e Computação (PESC) da COPPE/UFRJ em março de 2006. Durante a escrita dessa tese, realizada sob a orientação de Celina, foram criados vários algoritmos, entre determinísticos e randomizados, para um problema de teoria dos grafos. Alguns desses algoritmos foram desenvolvidos em co-autoria com Guilherme, que fez seu mestrado em estruturas de dados cinéticas (determinísticas e rando-

mizadas) também no PESC e orientado por Celina. Guilherme faz doutorado em geometria computacional na Universidade de Maryland. Manoel veio da Universidade Federal de Pernambuco participar como membro da banca da tese de doutorado de Vinícius, tendo naquela ocasião manifestado interesse em voltar ao tema que apresentara no Colóquio de 1989 para discutir o algoritmo randomizado de Rabin. Vinícius é, desde abril de 2006, pós-doutor junto ao PESC, onde lecionou uma versão preliminar destas notas.

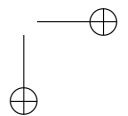
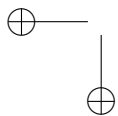
Agradecemos ao comitê organizador do Colóquio Brasileiro de Matemática pela oportunidade de apresentar este curso. Agradecemos também à CAPES, ao CNPq e à FAPERJ pelo apoio concedido na forma de bolsas de doutorado, pós-doutorado, pesquisa e auxílios para viagens. Agradecemos a Antonio Carlos Rodrigues Monteiro e Raphael Carlos Santos Machado pelas atentas correções e sugestões de melhorias. Finalmente, agradecemos a Luiz Henrique de Figueiredo pelo cuidadoso trabalho de diagramação.

Celina, Guilherme, Manoel e Vinícius.
Rio de Janeiro, 30 de abril de 2007.



Conteúdo

1	Randomizados?	1
1.1	Probabilidade básica	4
1.1.1	Axiomas e definições	4
1.2	Variáveis aleatórias e esperança	8
1.2.1	Linearidade da esperança	9
1.2.2	Limites de cauda	10
1.2.3	Algumas variáveis aleatórias importantes	11
1.3	Monte Carlo e Las Vegas	13
1.3.1	Monte Carlo	14
1.3.2	Las Vegas	21
1.3.3	Certeza ou desempenho?	23
1.4	Classes de complexidade	27
1.5	Exercícios	29
1.6	Notas bibliográficas	30
2	Paradigmas combinatórios e análise probabilística	31
2.1	Paradigmas combinatórios	32
2.1.1	O modelo de bolas-e-latas	32
2.1.2	O colecionador de cupons	34
2.2	Análise probabilística de algoritmos	37
2.2.1	Quick Sort	38
2.2.2	Quick Sort Randomizado	42
2.2.3	Bucket Sort	43
2.3	Exercícios	44
2.4	Notas bibliográficas	47



3	Primalidade	49
3.1	Aritmética modular	50
3.2	Maior divisor comum	53
3.3	Teorema Fundamental da Aritmética	57
3.4	O Pequeno Teorema de Fermat	59
3.5	Teorema Chinês do Resto	62
3.6	Geradores para \mathbb{Z}_n^*	65
3.7	Pseudoprimos	69
3.8	A exponenciação é rápida em \mathbb{Z}_n	75
3.9	Quase decidindo primalidade em tempo polinomial	80
3.10	A importância de números primos grandes: o RSA	82
3.11	Exercícios	84
3.12	Notas bibliográficas	85
4	Geometria Computacional	87
4.1	Programação linear	88
4.2	Funções hash	93
4.3	Par de pontos mais próximos	96
4.4	Exercícios	102
4.5	Notas bibliográficas	103
5	O Método Probabilístico	105
5.1	Provas de existência	105
5.1.1	O método da probabilidade positiva	106
5.1.2	O método da esperança	108
5.2	De-randomização	110
5.2.1	O método das esperanças condicionais	111
5.3	Exercícios	114
5.4	Notas bibliográficas	115
	Bibliografia	117