

Contents

Preface	ix
1. BASICS	1
1 Lattices	1
1.1 Determinant	6
1.2 Successive minima	7
1.3 Minkowski's theorems	11
2 Computational problems	14
2.1 Complexity Theory	15
2.2 Some lattice problems	17
2.3 Hardness of approximation	19
3 Notes	21
2. APPROXIMATION ALGORITHMS	23
1 Solving SVP in dimension 2	24
1.1 Reduced basis	24
1.2 Gauss' algorithm	27
1.3 Running time analysis	30
2 Approximating SVP in dimension n	32
2.1 Reduced basis	32
2.2 The LLL basis reduction algorithm	34
2.3 Running time analysis	36
3 Approximating CVP in dimension n	40
4 Notes	42
3. CLOSEST VECTOR PROBLEM	45
1 Decision versus Search	46
2 NP-completeness	48

3	SVP is not harder than CVP	52
	3.1 Deterministic reduction	53
	3.2 Randomized Reduction	56
4	Inapproximability of CVP	58
	4.1 Polylogarithmic factor	58
	4.2 Larger factors	61
5	CVP with preprocessing	64
6	Notes	67
4.	SHORTEST VECTOR PROBLEM	69
	1 Kannan's homogenization technique	70
	2 The Ajtai-Micciancio embedding	77
	3 NP-hardness of SVP	83
	3.1 Hardness under randomized reductions	83
	3.2 Hardness under nonuniform reductions	85
	3.3 Hardness under deterministic reductions	86
	4 Notes	87
5.	SPHERE PACKINGS	91
	1 Packing Points in Small Spheres	94
	2 The Exponential Sphere Packing	96
	2.1 The Schnorr-Adleman prime number lattice	97
	2.2 Finding clusters	99
	2.3 Some additional properties	104
	3 Integer Lattices	105
	4 Deterministic construction	108
	5 Notes	110
6.	LOW-DEGREE HYPERGRAPHS	111
	1 Sauer's Lemma	112
	2 Weak probabilistic construction	114
	2.1 The exponential bound	115
	2.2 Well spread hypergraphs	118
	2.3 Proof of the weak theorem	121
	3 Strong probabilistic construction	122
	4 Notes	124
7.	BASIS REDUCTION PROBLEMS	125
	1 Successive minima and Minkowski's reduction	125

<i>Contents</i>	vii
2 Orthogonality defect and KZ reduction	131
3 Small rectangles and the covering radius	136
4 Notes	141
8. CRYPTOGRAPHIC FUNCTIONS	143
1 General techniques	146
1.1 Lattices, sublattices and groups	147
1.2 Discrepancy	153
1.3 Statistical distance	157
2 Collision resistant hash functions	161
2.1 The construction	162
2.2 Collision resistance	164
2.3 The iterative step	168
2.4 Almost perfect lattices	182
3 Encryption Functions	184
3.1 The GGH scheme	185
3.2 The HNF technique	187
3.3 The Ajtai-Dwork cryptosystem	189
3.4 NTRU	191
4 Notes	194
9. INTERACTIVE PROOF SYSTEMS	195
1 Closest vector problem	198
1.1 Proof of the soundness claim	201
1.2 Conclusion	204
2 Shortest vector problem	204
3 Treating other norms	206
4 What does it mean?	208
5 Notes	210
Index	219