



# 目 次

<b>第 1 章 機械モデルと模倣</b> .....	1
P. van Emde Boas : 足立 暁生	
1. 序 論 .....	3
1.1 計算量理論の不変量 .....	3
1.2 機械モデルの形式化 .....	6
2. 逐次計算機械モデル .....	16
2.1 Turing 機 械 .....	16
2.2 レジスタ機械 .....	22
2.3 記憶装置変更機械 .....	31
2.4 回路と非一様モデル .....	34
3. 第 2 種機械クラス .....	37
3.1 PSPACE と推移閉包 .....	38
3.2 交 替 モ デ ル .....	41
3.3 莫大な量のデータを単位時間で処理する逐次処理機械 .....	44
3.4 真の並列性をもつ機械 .....	47
4. 第 2 種機械クラス以外の並列機械モデル .....	52
4.1 弱い並列機械 .....	52
4.2 第 2 種機械クラスに属するモデルより強力なモデル .....	54
謝 辞 .....	59
文 献 .....	60
<b>第 2 章 計算量のクラスのカatalog</b> .....	65
D. S. Johnson : 五十嵐善英	
1. 序 論 .....	67
1.1 問題と問題例 .....	67
1.2 問題の解き方 .....	69
1.3 機 械 モ デ ル .....	70
1.4 資 源 の 制 限 .....	73
1.5 最初の例：クラス P (とクラス FP) .....	74
1.6 還 元 .....	75
1.7 完 全 性 .....	76

1.8	相対的な世界	78
1.9	カタログの構成	79
2.	手に負えそうもない問題	80
2.1	クラス NP, NP 完全問題, 構造的な結果	80
2.2	co-NP, $NP \cap co-NP$ , 非決定性還元	86
2.3	NP 困難, NP 容易, NP 等価問題 (クラス $F\Delta_2^P$ )	87
2.4	NP と $\Delta_2^P$ の間: クラス $D^P$ と Boole 階層	89
2.5	多項式階層	91
2.6	PSPACE とその部分クラス	94
3.	手に負えないことが確かな問題	97
3.1	クラス EXPTIME とその変形	97
3.2	クラス NEXPTIME	98
3.3	NEXPTIME を越えるもの	99
4.	カウントによるクラス	101
4.1	カウンティング Turing 機械とクラス #P	101
4.2	曖昧でない Turing 機械とクラス FUP と UP	105
4.3	ランダム Turing 機械とクラス R, co-R, ZPP	107
4.4	ランダム化還元と NP	111
4.5	確率的 Turing 機械およびクラス PP と BPP	113
4.6	推計 Turing 機械, 対話証明, それらが定義するクラス	114
5.	P の 内 部	118
5.1	準線形の領域限定で定義されるクラス, POLYLOG-SPACE, L, NL, SC	118
5.2	並列計算とクラス NC, RNC	122
5.3	NC の 内 部	127
5.4	$NC^1$ の 内 部	130
6.	新しい発展, 表, 図	135
6.1	新しい発展	135
6.2	表 と 図	136
	文 献	143

**第3章 機械モデルと独立な計算量理論** ..... 153

J. I. Seiferas: 渡辺 治

1.	序 論	155
2.	単純 Turing 機械と領域計算量	156
3.	再帰, 水増し可能性, そして計算量の確定性に関する定理	158
4.	ギャップならびに任意のスピードアップに関する定理	164
5.	帰納的スピードアップに関する定理	169
6.	STM に関する基本定理	172

7. 機械モデルからの独立性 .....	173
謝 辞 .....	181
文 献 .....	182
<b>第4章 Kolmogorov 記述量とその応用</b> .....	<b>185</b>
M. Li and P. M. B. Vitányi : 渡辺 治	
1. 序 論 .....	187
1.1 発見者たち .....	193
2. Kolmogorov 記述量の数学理論 .....	195
2.1 圧縮不可能性 .....	199
2.2 自己分離型記述法 .....	201
2.3 $K$ の大きさに関する考察 .....	203
2.4 無限長のランダム列 .....	205
2.5 $K$ のアルゴリズム的性質 .....	207
2.6 情 報 .....	209
2.7 自己分離型 Kolmogorov 記述量 .....	210
2.8 確 率 論 .....	212
2.9 先験的確率：Solomonoff-Levin 分布 .....	214
3. 圧縮可能性の応用 .....	216
3.1 Gödel の定理の1つの解釈 .....	216
3.2 理論形成における帰納的推論 .....	217
3.3 Rissanen の最小記述長原理 .....	219
3.4 Valiant の学習モデルにおける学習可能性 .....	221
3.5 計算可能な実数の非ランダム性 .....	222
3.6 知 恵 の 数 $\Omega$ .....	222
4. 数学への応用例：弱い素数定理 .....	225
5. 圧縮不可能性の応用：下界の証明 .....	226
5.1 下界証明の3つの例 .....	227
5.2 下界：テープ数の比較 .....	230
5.3 下界：多ヘッド vs. 少ヘッド .....	233
5.4 下界：並列計算と分岐プログラム .....	235
5.5 下界：表検索における時間とプログラムサイズのトレードオフ .....	236
5.6 下界：超集積回路 .....	237
5.7 下界：確率的アルゴリズム .....	238
5.8 下界：形式言語理論 .....	239
5.9 下界：どの方法を使うか .....	241
5.10 下界：未解決問題 .....	242

6. 資源限定 Kolmogorov 記述量とその応用	242
6.1 ポテンシャル	243
6.2 論理の深さ	244
6.3 一般化された Kolmogorov 記述量	246
6.4 一般化された Kolmogorov 記述量の構造的証明への応用	248
6.5 時間限定 Kolmogorov 記述量と言語の圧縮について	250
6.6 Kolmogorov ランダム還元	254
7. 結 論	255
謝 辞	256
文 献	256

**第5章 文字列中のパターン照合のためのアルゴリズム** ..... 263

A. V. Aho : 仙波 一郎

1. 序 論	265
2. パターンの記法	266
2.1 正規表現	267
2.2 正規表現記法の拡張	267
2.3 後退参照付き正規表現	268
3. キーワードの照合	270
3.1 素朴なアルゴリズム	270
3.2 Karp-Rabin アルゴリズム	271
3.3 Knuth-Morris-Pratt アルゴリズム	272
3.4 Boyer-Moore アルゴリズム	275
3.5 平均的な性能	278
3.6 理論的考察	279
4. キーワードの集合の照合	280
4.1 Aho-Corasick アルゴリズム	280
4.2 Commentz-Walter アルゴリズム	284
5. 正規表現の照合	287
5.1 正規表現に対する非決定性アルゴリズム	288
5.2 正規表現を認識する決定性アルゴリズム	291
6. 関 連 問 題	294
6.1 後退参照付き正規表現の照合問題	294
6.2 繰り返されたパターンと回文の発見	295
6.3 近似的文字列照合	296
6.4 ドントケア (don't care) 記号を含む文字列照合	299
7. 結 論	299
謝 辞	300

文 献 .....	300
-----------	-----

## 第6章 データ構造 .....305

K. Mehlhorn and A. Tsakalidis : 浅野 孝夫

1. 序 論 .....	307
2. 辞書問題 .....	309
2.1 比較に基づくデータ構造 .....	310
2.2 表現に基づくデータ構造 .....	316
3. 重み付き辞書問題と自己組織データ構造 .....	324
4. 残 存 性 .....	328
5. ユニオン-スプリット-ファインド問題 .....	329
5.1 ユニオン-ファインド問題 .....	329
5.2 区間スプリット-ファインド問題 .....	331
5.3 区間ユニオン-スプリット-ファインド問題 .....	331
6. 優先順位付きキュー .....	331
7. 最近共通祖先問題 .....	333
8. 選 択 問 題 .....	335
9. 併 合 問 題 .....	337
10. 動的化技法 .....	338
文 献 .....	339

## 第7章 計算幾何学 .....347

F. F. Yao : 浅野 哲夫

1. 序 論 .....	349
2. 技法とパラダイム .....	349
2.1 分割統治法 .....	349
2.2 走 査 法 .....	350
2.3 幾何学的変換 .....	350
2.4 領 域 法 .....	350
2.5 分割質問法 .....	350
2.6 多次元探索 .....	351
2.7 ランダムサンプリング .....	351
2.8 下 界 .....	351
3. 凸 包 .....	352
3.1 平面上の集合の凸包 .....	353
3.2 下 界 .....	354
3.3 高次元における凸包 .....	354

3.4 関 連 問 題 .....	355
4. Voronoi 図 .....	356
4.1 準 備 .....	357
4.2 構 成 法 .....	358
4.3 一般化された Voronoi 図 .....	359
5. 近 接 問 題 .....	361
5.1 最近点および最近点对 .....	361
5.2 Euclid 最小全域木 .....	362
5.3 Euclid 最小マッチング .....	363
5.4 Euclid 行商人問題 .....	363
5.5 最 大 空 円 .....	364
5.6 クラスタリング問題 .....	364
5.7 最 大 距 離 .....	364
6. 線 形 計 画 法 .....	365
6.1 2次元での線形計画問題 .....	365
6.2 3次元以上への一般化 .....	366
6.3 応 用 .....	367
6.4 注 釈 .....	368
7. 三角形分割と分解 .....	369
7.1 単純な多角形の三角形分割 .....	369
7.2 多角形の分割 .....	370
7.3 多角形の被覆 .....	370
8. 平面点位置決定 .....	371
9. 多 次 元 木 .....	373
9.1 区 分 木 .....	373
9.2 ヒープ探索木 .....	374
9.3 $k$ - $d$ 木 .....	375
9.4 領 域 木 .....	375
10. 領 域 探 索 .....	375
10.1 直交領域探索 .....	376
10.2 半空間領域探索 .....	377
10.3 領域探索問題の下界 .....	378
11. 可視部分の計算 .....	379
11.1 線 分 の 交 差 .....	380
11.2 隠 面 除 去 .....	380
11.3 可 視 グ ラ フ .....	381
12. 組合せ幾何学 .....	382
12.1 アレンジメント .....	382
12.2 Davenport-Schinzel 列 .....	382

12.3	2等分と $k$ 集合	383
12.4	$\lambda$ 行列と他のタイプ	383
13.	その他のトピック	384
13.1	有限精度幾何学	384
13.2	ランダムサンプリング	384
14.	結 論	385
文 献		386

## 第8章 ロボティクスにおけるアルゴリズム的な動作計画 ..... 395

J. T. Schwartz and M. Sharir : 林 朗

1.	序 論	397
2.	動作計画問題とは	399
3.	静的な既知環境における動作計画	402
3.1	動作計画問題の一般解	405
3.2	計算量の下界	408
3.3	投 影 法	409
3.4	レトラクト法および関連する手法	412
3.5	その他の手法	415
4.	動作計画問題の変形	419
4.1	最適計画問題	419
4.2	適応性のある動作計画および探検的動作計画	422
4.3	障害物が動くときの動作計画	423
4.4	その他の種々の変形	423
4.5	一般的タスク計画	424
5.	動作計画に関連する, 計算幾何学の成果	425
5.1	交差の検出	425
5.2	一般化 Voronoi 図	426
5.3	Davenport-Schinkel 列	426
謝 辞		429
文 献		429

## 第9章 アルゴリズムとデータ構造の平均計算量解析 ..... 435

J. S. Vitter and Ph. Flajolet : 平田 富夫

1.	序 論	437
2.	組合せ的数え上げ	440
2.1	概 要	440
2.2	通常母関数	442



2.3	指数型母関数 .....	445
2.4	母関数から数え上げへ .....	447
3.	漸 近 法 .....	449
3.1	概 説 .....	449
3.2	特異点解析 .....	450
3.3	鞍 部 点 法 .....	454
3.4	Mellin 変 換 .....	456
3.5	極限確率分布 .....	457
4.	整列アルゴリズム .....	460
4.1	反 転 .....	460
4.2	挿入整列法 .....	463
4.3	Shell 整列法 .....	463
4.4	バブル整列法 .....	468
4.5	クイック整列法 .....	470
4.6	基数交換整列法 .....	471
4.7	選択整列法とヒープ整列法 .....	471
4.8	併合整列法 .....	472
5.	木の再帰的分解とアルゴリズム .....	473
5.1	2分木と平面木 .....	473
5.2	2分探索木 .....	480
5.3	基数交換トライ .....	486
5.4	デジタル探索木 .....	489
6.	ハッシュ法とアドレス計算技法 .....	490
6.1	バケットアルゴリズムと連鎖法 .....	491
6.2	開アドレス方式によるハッシュ法 .....	503
7.	動的アルゴリズム .....	507
7.1	総合コストと履歴モデル .....	507
7.2	動的データ構造のサイズ .....	509
7.3	Set-Union-Find アルゴリズム .....	512
謝 辞	.....	515
文 献	.....	516

**第 10 章 グラフアルゴリズム .....** 521  
 J. van Leeuwen : 斎藤 明

1.	序 論 .....	523
2.	グラフの表現 .....	523
2.1	グラフの描画 .....	524
2.2	計算機におけるグラフの表現 .....	528

2.3	横断によるグラフ上の探索	535
2.4	推移的簡約と推移的閉包	536
2.5	一般グラフの生成	540
2.6	グラフの種々のクラスについて	542
3.	グラフの基本構造に関するアルゴリズム	548
3.1	連結度	548
3.2	最小全域木	552
3.3	最短路	554
3.4	道と閉路	558
3.5	グラフの分解	568
3.6	同形判定問題	572
4.	グラフに関する組合せ最適化問題	577
4.1	最大マッチング	577
4.2	最大マッチングを求めるアルゴリズム	581
4.3	最大フロー	586
4.4	最大フローを求めるアルゴリズム	591
4.5	フローに関連したその他の問題	600
文 献		610

## 第 11 章 代数的計算量理論 ..... 629

V. Strassen: 町田 元

1.	序 論	631
2.	加 法 鎖	633
3.	計 算 列	634
4.	代 入	634
5.	超 越 次 数	636
6.	幾 何 的 次 数	637
7.	導 関 数	639
8.	分 岐	641
9.	計算量のクラス	644
10.	行列の乗算と双 1 次計算量	646
11.	退化と漸近的スペクトラム	648
12.	階数と境界階数に対する下界	652
12.1	代 数	652
12.2	特殊なフォーマットをもつ双線形写像	653
12.3	典型的階数と境界階数	654
13.	Fourier 変換	655
14.	完 全 問 題	656

15. 結 論 .....659  
 文 献 .....660

**第 12 章 数論アルゴリズム** .....667

A. K. Lenstra and H. W. Lenstra, Jr. : 寺田 文行

1. 序 論 .....669  
 2. 基 本 事 項 .....671  
   2.1 滑 ら か さ .....671  
   2.2 楕 円 曲 線 .....671  
   2.3 類 群 .....675  
   2.4 連立方程式の解法 .....677  
 3. 有限 Abel 群に関するアルゴリズム .....679  
   3.1 は じ め に .....679  
   3.2 指数時間アルゴリズム .....680  
   3.3 位数が滑らかな群 .....682  
   3.4 準指数アルゴリズム .....683  
 4. 整 数 の 分 解 .....690  
   4.1 は じ め に .....690  
   4.2 楕円曲線を用いた整数の分解 .....691  
   4.3 滑らかさテストに頼る方法 .....693  
   4.4 2次ふるい法 .....696  
   4.5 3次ふるい法 .....698  
 5. 素 数 性 判 定 .....699  
   5.1 概 説 .....699  
   5.2 いくつかの古典的手法 .....700  
   5.3 楕円曲線を用いる素数判定 .....702  
 謝 辞 .....706  
 文 献 .....706

**第 13 章 暗 号** .....711

R. L. Rivest : 西村 和夫

1. 序 論 .....713  
 2. 基 礎 .....713  
   2.1 使い捨て乱数方式 .....714  
   2.2 データ暗号化規格 (DES) .....715  
 3. 暗号学の目的と道具 .....717  
 4. 数学的な準備 .....718

5.	暗号における計算量理論の基礎	720
5.1	チェックサムと1方向性関数	720
5.2	落とし戸関数	721
5.3	1方向性述語と落とし戸述語	722
5.4	計算量理論的に妥当な仮定	722
6.	プライバシー	723
6.1	秘密鍵暗号系	723
6.2	決定性の公開鍵暗号	724
6.3	確率的な公開鍵暗号化	727
6.4	暗号演算子の合成と多重暗号化	731
7.	乱数列または擬似乱数列の生成とその関数	732
7.1	乱数ビット列の生成	732
7.2	擬似乱数ビット列または擬似乱数列の生成	733
8.	デジタル署名	736
8.1	署名方式の安全性の証明	738
8.2	確率的署名方式	739
9.	2者間のプロトコル	740
9.1	例	740
9.2	零知識プロトコル	742
10.	多者間のプロトコル	744
10.1	例	744
10.2	多者間のピンポンプロトコル	745
10.3	ほとんどの者が正直である場合の多者間のプロトコル	746
11.	暗号と計算量理論	746
謝	辞	747
文	献	748

## 第14章 有限関数の複雑さ 755

R. B. Boppana and M. Sipser : 西野 哲朗

1.	序 論	757
1.1	簡単な歴史	757
2.	一般の回路	758
2.1	Boole回路とTuring機械	759
2.2	非明示的な下界	761
2.3	明示的な下界	762
3.	深さ限定回路	763
3.1	定義	763
3.2	制 約	764

3.3	Hastad のスイッチング補題	765
3.4	パリティ関数に対する下界	769
3.5	深さの階層	770
3.6	単調深さ限定回路	771
3.7	確率的深さ限定回路	771
3.8	$\text{MOD}_p$ ゲートを含む回路に対する Razborov-Smolensky の下界	772
3.9	応用	774
4.	単調回路	778
4.1	背景	778
4.2	単調回路サイズに対する Razborov の下界	779
4.3	クリーク関数に対する下界	781
4.4	多項式下界	784
5.	論理式	785
5.1	単調論理式サイズに対する Karchmer-Wigderson の下界	785
5.2	連結度関数に対する下界	787
5.3	非単調論理式	790
5.4	対称関数	793
6.	分岐プログラム	794
6.1	領域計算量との関係	795
6.2	サイズの限界	796
7.	結論	797
謝辞		798
文献		798

## 第 15 章 通信ネットワーク .....803

N. Pippenger : 丸岡 章

1.	序論	805
1.1	通信ネットワークと計算	805
1.2	演算の形態	805
2.	通信の問題	807
2.1	接続の問題	807
2.2	一般化された接続問題	810
2.3	シフト, マージ, 分類のネットワーク	813
2.4	他の問題	815
3.	Ajtai, Komlós と Szemerédi の定理	818
3.1	定理の応用	818
3.2	近似分類ネットワーク	820
3.3	レジスタの移動	821

3.4 ネットワークの構成 .....	825
3.5 局所的な議論 .....	826
3.6 全体的な議論 .....	827
謝 辞 .....	829
文 献 .....	829
<b>第 16 章 VLSI 理 論</b> .....	833
Th. Lengauer : 浅田 邦博	
1. 序 論 .....	835
2. VLSI 計算量の尺度 .....	837
3. VLSI モデル .....	840
4. 基本的下界論 .....	842
5. 幾何学的分割定理 .....	843
6. Boole 述語関数の通信量 .....	844
7. 多出力 Boole 関数の通信量 .....	851
8. VLSI チップのスイッチングエネルギーの下界 .....	854
9. VLSI チップの $AT^2$ 計算量の上界 .....	858
謝 辞 .....	861
文 献 .....	862
<b>第 17 章 共有メモリ機械のための並列アルゴリズム</b> .....	865
R. M. Karp and V. Ramachandran : 岩野 和生	
1. 序 論 .....	867
2. 効率の良い PRAM アルゴリズム .....	869
2.1 PRAM モデルと効率の良いアルゴリズムや最適なアルゴリズムの概念 .....	869
2.2 基本となる PRAM のテクニック .....	871
2.3 効率の良いグラフアルゴリズム .....	878
2.4 ソート, マージ, 選択 .....	883
2.5 さらなる話題 .....	891
3. 並列計算のモデル .....	892
3.1 PRAM モデル間の関係 .....	892
3.2 PRAM の下界 .....	893
3.3 回 路 .....	895
3.4 回路と PRAM の関係 .....	897
3.5 交替 Turing 機械 .....	899
3.6 ベクトル機械 .....	902
3.7 ランダム計算複雑度のクラス .....	903

3.8	算 術 モ デ ル	903
3.9	並 列 計 算 原 理	904
4.	NC アルゴリズムと P 完全問題	905
4.1	は じ め に	905
4.2	算術操作のための NC 回路	906
4.3	式の評価のための回路	910
4.4	Boole 行列の乗算と推移的閉包	911
4.5	行 列 の 乗 算	912
4.6	直線的なプログラムの動的な評価	914
4.7	極大独立集合問題	916
4.8	応 用	918
4.9	ランダム NC アルゴリズム	921
4.10	さらなる結果	924
4.11	P 完 全 問 題	925
4.12	未解決の問題	928
5.	結 論	929
謝	辞	930
文	献	931

## 第 18 章 汎用並列アーキテクチャ ..... 941

L. G. Valiant : 中野 秀男

1.	序 論	943
2.	いくつかのネットワーク	944
2.1	序 論	944
2.2	ハイパーキューブの族	945
2.3	特別な応用	947
3.	経 路 選 択	948
3.1	並列通信方式	948
3.2	有向バタフライに対する証明	951
3.3	待ち行列制御規則に対する不変性	954
3.4	検 査 能 力	955
3.5	道 の 長 さ	956
3.6	長さの制約されたバッファ	956
4.	普 遍 性	957
4.1	汎用並列計算	957
4.2	PRAM モデル	958
4.3	シミュレーション	959
4.4	結 論	966

謝 辭 .....	966
文 獻 .....	966
索 引 .....	971