はじめに

なぜランダム性か？

計算機科学者はなぜランダムを研究し，利用すべきなのか？　コンピュータの動作原理は，乱数が持つ予想困難性とは対極に位置しているように見える．むしろ乱数を利用することは逆効果で，効率的にコンピュータを利用するにはどうしたらよいのかという困難な問題に対して，徒（いたずら）に複雑な要因を加えているように思える．

科学は過去 100 年にわたって，自然現象のモデル化とその解析においてランダム性は本質的に必要なものとして受容してきた．物理学を例にとると，Newton の法則は，宇宙は決定論的であり，十分に大きいコンピュータがあれば適当な初期条件から将来の惑星の位置を特定することができる，ということを我々に教えてくれる．一方で，量子力学の発展は，これとは異なる見方を暗示している．宇宙は依然として物理法則に従っているが，その法則の根源は確率的である．現代量子力学に対する Einstein の批判の言葉「神はサイコロを振らない」は有名だが，素粒子物理における多数の支持を受けている理論はランダムな挙動や統計的な法則に基づいている．他の科学分野でも，遺伝学や生物学における進化論から自由市場経済における価格変動のモデル化まで，多岐にわたってランダム性は重要な役割を果たしている．

計算機科学も決して例外ではない．高度な理論が必要な確率的検査可能証明の概念からパソコンのイーサネットカードの実設計まで，ランダム性と確

率的手法は現代の計算機科学において主要な役割を果たしている．ここ 20 年，確率論を計算機科学に導入する事例が急増している．計算機科学を広範かつより高度な応用に適用できるように，より高度でより洗練された確率的技法が開発されてきている．本書では，計算機科学に関連するランダム性の基本的手法である乱択アルゴリズムや，アルゴリズムの確率的解析について学習する．

乱択アルゴリズム

乱択アルゴリズムは計算の実行中にランダムな選択をするアルゴリズムである．現実には，乱択アルゴリズムは乱数生成器が生成した値を利用して，複数ある次の実行手順候補の中から一つを決定する．例えば，イーサネットカード中に実装されているプロトコルは，共有されているイーサネット通信媒体に次はいつアクセスするのかを，乱数を用いて決定している．ランダム性は対称性を破るのに有効であり，異なる複数のカードが媒体に対する同時アクセスを繰り返すことを防ぐのに役立っている．モンテカルロシミュレーションを含む乱択アルゴリズムで広く利用されている応用の一つに，暗号利用における素数判定がある．上記の応用やその他の多くの応用において，乱択アルゴリズムは既知の決定的な解法よりも非常に効率的である．さらに，多くの場合，乱択アルゴリズムは単純であり，実装が容易である．

これらの長所に対して短所もある．アルゴリズム出力はある確率で誤る可能性がある．すなわち，効率性はある確率で保証されるにすぎない．誤る可能性のあるアルゴリズムを設計することは奇妙かもしれないが，誤り確率が十分に小さいならば，速度やメモリ効率を改善することを考慮すると十分価値があるだろう．

アルゴリズムの確率的解析

計算量理論を用いると，問題の計算複雑さに応じた分類，特に平易な問題と困難な問題との区別を考えることができる．例えば，計算量理論は巡回セールスマン問題が NP 困難であることを示してくれる．このことから巡回セールスマン問題の例題を都市数の準指数時間で解くアルゴリズムは存在しないように思える．古典的な最悪時間計算量理論の困った点は，それが難しい問題として分類されるにもかかわらず，現実的には容易に解けることがあると

いうことである．確率的解析は，この現象について理論的な説明を与えてくれる．これらの問題は特異な入力の集合に対しては困難かもしれないが，たいていの入力（特に，現実的な応用で現れるような入力）に対して容易に解ける．より正確に言うと，ありうるすべての入力の集合を表す何らかの確率分布に従ってランダムに入力が選択されるとき，解きやすい例題が与えられやすく，解きにくい例題は相対的に小さい確率でしか現れない．アルゴリズムの確率的解析は，妥当に定義された確率空間から入力が抽出されるときにアルゴリズムがどのように動作するかを調べる手法である．すでに見たように，NP 困難問題でさえほとんどすべての入力に対して極めて効率的なアルゴリズムが存在しうるのである．

本書の構成

この教科書は計算機科学や応用数学分野の高学年の学部生あるいは修士学生に向けた 1～2 学期分の講義用に構成されている．トップクラスの多くの大学では，乱択手法や確率的技法の学習は，理論系大学院生向けの先端的セミナでの話題から，学部高学年や初年度の修士学生へ向けた通常のコースでの話題となってきている．乱択手法や確率的技法についての研究用の高度ですばらしい書籍は数多く存在するが，入門書に対する要求も高い．本書がこの要求を満足するものと我々は期待している．

本教科書はブラウン大学およびハーバード大学での「計算機科学における確率的手法」という近年の講義（講義番号 CS 155 および CS 233）を発展させたものである．これらの講義，そして本書において強調したいことは，確率的手法や枠組みについてであり，個々の応用についてではない．本書の各章はそのような手法や技法をそれぞれ一つに絞って書かれている．乱択アルゴリズムの解析やランダムな入力に対するアルゴリズムの確率的解析をもとにした事例を通じて，各技法を理解しやすいように配慮してある．ネットワーク分野の興隆を反映して，多くの事例は（著者の趣味でもあるが）ネットワークに関連したものになっている．

本書は 14 章で構成されている．大きく二つに分けて考えることもでき，前半（第 1 章から第 7 章）は我々が基本的な素材と考えているもので構成されている．本書を講義に使う講師が学生に仮定すべきことは，計算機科学科の標

準的な講義「離散数学」で教えるような確率論の初歩の知識だけである．第 1 章から第 3 章では興味深い応用を導入しつつ確率論の基礎の復習を行う．ランダム標本抽出，期待値，Markov の不等式，分散，Chebyshev の不等式などについてである．前述の「離散数学」の講義において確率論の基礎知識を十分に教えているならば，これらの章の内容は簡単に教える程度でよい．しかしながら，これらの章は乱択アルゴリズムの概念やアルゴリズムの確率的解析の導入部分であり，本書を通して用いられるいくつかの例題を含んでいるため，読み飛ばしてしまうことは勧められない．

第 4 章から第 7 章はより先進的な話題である Chernoff 上界，ボールとビンのモデル，確率的手法，Markov 連鎖についてである．これらの章で扱っている素材は前の章よりも難易度が高くなっている．特に難しい節については * 印を付けてある（よって，講師は飛ばすことを考えてもよい）．最初の 7 章で扱う基本的素材は，講義の進め方に応じて，四半期あるいは半期を賄う内容量と考えている．

本書の後半（第 8 章から第 14 章）は補足的な先進的素材であり，必要に応じて基本講義内で教えることもできるし，先進的な別の講義で教えてもよい．これらの章はほぼ自己完結する形で書かれており，講師が講義計画に応じて選択することができる．連続確率とエントロピーの章は基本講義に組み込むのに最適である．連続確率への入門（第 8 章）では，一様分布と指数分布に限定し，待ち行列理論についての例題を与えている．エントロピー（第 9 章）では，ランダム性をいかに測るかを検討し，乱数抽出，圧縮，符号の文脈において自然な形でエントロピーが現れることを見る．

第 10 章と第 11 章は，それぞれモンテカルロ法とカップリングについて扱う．これらの章は互いに関連しているので一緒に教えることが望ましい．マルチンゲールについての第 12 章では，非独立な確率変数を扱う重要な問題について触れる．同テーマは異なる形で，第 13 章へと引き続き，対独立性と脱乱択化へと展開する．最後に均等配分の章（第 14 章）では，著者の関心に近い話題に触れ，第 5 章で行ったボールとビンの問題の解析と関連付ける．

話題の順番は，特に本書の前半部分では，アルゴリズム系の教養における相対的な重要性に基づいている．例えば，Chernoff 上界の研究は Markov 連鎖のような基本的な確率概念よりも優先される．しかしながら，本書を利用する講師が異なる順番で各章を教えることは，選択肢としてあってもよい．例

えば，一般的な確率過程をより強調する講義の場合，Markov 連鎖（第 7 章）を第 1〜3 章の直後に教え，続いてボールとビン，ランダムグラフ（第 5 章，ただし Hamilton 閉路は省略してもよい）を教えてもよい．確率的手法を扱っている第 6 章は飛ばすことも可能で，代わりに連続確率と Poisson 過程（第 8 章）へと繋いでもよい．しかしながら，Chernoff 上界に関する第 4 章の材料は，残りの話題のたいていの部分で必須である．

著者はこの本での素材を，ほんの少しの例外を除いて，厳密な数学的解析に基づく方法と技法だけに限定することにした．本書のすべての主張には完全な証明が与えられている．明白なことだが，非常に役に立っている多くの確率的手法はこの範疇に属さない．例えば，モンテカルロ法の重要分野で多用される現実的な解法は，その効果や効率を厳密な数学的解析によって示すよりも，むしろ計算機実験によって例証された発見的手法である．発見的手法の長所と短所を理解し適切に応用するためには，基礎となる確率論と厳密な技法をしっかり把握することこそが必須であるという考え方を，本書を通じて訴えたい．学生の皆が講義終了時までにこの考え方の良さを理解してくれることを期待する．

謝辞

まず，本書で扱っているすばらしい素材を生み出してくれた多くの確率論研究者と計算機科学者に感謝したい．原論文を数多く引用することに本書のページを割く方針はとらない．代わりに，本書で触れた話題についての高度な議論やバックグラウンドを与えてくれる数多くの書籍を参考文献として記載することにする．

本書はブラウン大学での講義 CS 155 およびハーバード大学での講義 CS 223 を受講した学生やティーチングアシスタントからの意見やフィードバックに負っているところが大きい．特に本書の初校を読んでコメントしてくれた Aris Anagnostopoulos，Eden Hochbaum，Rob Hunter，Adam Kirsch に感謝したい．

2003 年の秋学期にバークレーでの講義 CS 174 で本書の草稿を利用してくれた Dick Karp に特に感謝したい．彼のコメントや訂正は草稿を改善するのに最も貢献した．2004 年の春学期にバークレーでの講義 CS 174 で教鞭をとっ

た Peter Bartlett からも多くの訂正や有益なコメントをいただいた．

原稿の各部分を注意深く読み，多くの誤りを指摘してくれ，内容や表現において重要な改良方法を提案してくれた同僚 Artur Czumaj，Alan Frieze，Claire Kenyon，Joe Marks，Salil Vadhan，Eric Vigoda，そして出版社の校正刷りを読んでくれた匿名の校閲者にも感謝したい．

また，Rajeev Motwani と Prabhakar Raghavan には，彼らのすばらしい書籍 *Randomized Algorithms* から一部の練習問題を利用することに同意してくれたことに感謝したい．

Cambridge University Press の Lauren Cowles には，原稿の準備と整備にあたり構成上の補助や助言をしてくれたことに感謝したい．

本書を書き上げるにあたり，NSF ITR Grant no. CCR-0121154 から援助を受けた．

訳者まえがき

情報処理技術の基礎として，アルゴリズムやデータ構造が一般教養として教育されている．一方で，ランダム性を利用した乱択アルゴリズム技術の進展により，アルゴリズムやデータ構造を基礎に置くネットワーク技術などの諸分野も，同様に進展を見せている．そういった諸分野を学習するにあたり，乱択アルゴリズムやその確率的解析技術が必要不可欠な状況になってきている．もちろん，従来からも確率・統計が一般教養科目の一つとして教えられてはいるが，進展する応用分野との乖離は大きくなるばかりである．そのため，進展する諸応用分野と確率・統計とを橋渡しするために，乱択アルゴリズムを前提とした確率的解析技術をまとめて提供することが教育上求められている．このような状況の初期において，Rajeev Motwani と Prabhakar Raghavan による画期的な成書 *Randomized Algorithms* が書かれたが，乱択アルゴリズムの重要性がプログラム開発を実際に行う現場には十分に認知されていなかったためか，邦訳の出版には至らなかった．その後 10 年が経過し，乱択アルゴリズムを前提とした確率的解析の重要性がさらに高まっている中にあって，ネットワークアルゴリズム理論分野の第一級の研究者である Michael Mitzenmacher と Eli Upfal によって *Probability and Computing* が書き上げられた．本書はその邦訳である．

本書の構成については，著者による序文にもあるので省略し，訳出に関して若干触れる．まず，学術上の人名に関しては英文のままとした．これはカタカナ表記が正しい発音と一致しないことによる．関連文献を人名で調べた

い場合にも英文表記であったほうが有用であろう．また，専門用語で邦訳が定着していないものについては，なるべく邦訳をあてることを心掛けた．これは学問領域の発展度と邦訳定着率は相関するという訳者の信念によることもあるが，初学者への配慮でもある．英文と邦訳の併記という方法も可能であろうが，原書ページ数からして少なくない分量であるため，不必要なページ数の増加を避けることを優先させた．

最後に本書の翻訳の機会を与えてくださった共立出版の石井徹也氏に深く感謝している．そして，東京工業大学の渡辺治氏および渡辺研究室の学生諸氏，同じく東京工業大学の岡本吉央氏，大阪府立大学の西村治道氏よりいただいた有益なコメントに感謝している．とりわけ，岡本吉央氏には専門用語の適切な邦訳に関しての貴重な意見をいただき感謝している．

2009 年 3 月

訳者