BOOK REVIEWS

BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 50, Number 3, July 2013, Pages 481–487
S 0273-0979(2013)01407-1
Article electronically published on April 5, 2013

Inevitable randomness in discrete mathematics, by József Beck, University Lecture Series, 49, American Mathematical Society, Providence, RI, 2009, xiii+250 pp., ISBN 978-0-8218-4756-5, US $59.00

1. Introduction

The beauty and utility of randomness is more than matched by its mysteries. How can we tell if a putative source of randomness (such as the frequency of the emission of electrons from a decaying radioactive material) is truly random? Indeed, how does one define randomness?

Starting from the 17th century work of Pascal and Fermat, and spurred on by the 20th century axiomatic approaches of S. N. Bernstein, A. N. Kolmogorov, and R. E. von Mises,[1] we have been applying randomness with steadily increasing power and precision. More recently, theoretical computer science has helped bring the meaning of randomness to a sharper focus. But whether randomness is truly necessary in the solution of certain fundamental problems remains unknown.

József Beck's *Inevitable randomness in discrete mathematics* gives a novel point of view on these questions. To better understand the theoretical and conceptual advances Beck puts forth, let us first review how we profit from randomness in certain settings adjacent to those considered in his book. In what follows, we will sometimes refer to basic notions from algorithmic complexity. Some of the best sources for further background on complexity are [Sip92, Pap95, AB09, For09, Lip09].

2. Do we need randomness?

How quickly can we determine whether a given integer N is prime? The advent of public key cryptography in the latter half of the 20th century generated a serious need for algorithms with complexity polynomial in $\log N$.

To check the primality of N, one can of course use trial division by primes up to $\left\lfloor \sqrt{N} \right\rfloor$, but this naive method is doomed to time exponential in $\log N$. Fortunately, through some clever tricks involving square roots mod N [SS77], Solovay and Strassen found a randomized algorithm with complexity cubic in $\log N$.

2010 *Mathematics Subject Classification.* Primary 60-02, 05-02, 91A46; Secondary 05D40, 11K38.

[1] Kolmogorov's measure-theoretic approach ultimately led the way.

More precisely, recall that for any integer a and prime p, the *Legendre symbol* $\left(\frac{a}{p}\right)$ is 0, 1, or -1, according as p divides a, a is a nonzero square mod p, or a is not a square mod p. The *Jacobi symbol* $\left(\frac{a}{N}\right)$ is then defined to be $\left(\frac{a}{p_1}\right)^{e_1} \cdots \left(\frac{a}{p_k}\right)^{e_k}$, assuming $N = p_1^{e_1} \cdots p_k^{e_k}$ for distinct primes $p_1, \ldots, p_k$ and positive integers $e_1, \ldots, e_k$.

If N is prime, then it is easy to show from Fermat's Little Theorem that $\left(\frac{a}{N}\right) = a^{(N-1)/2} \bmod N$ for all a. The following classic result, discovered independently by D. H. Lehmer around 1975, provides a partial converse strong enough to enable a primality test.

Theorem 2.1 ([SS77])**.** *If N is odd and composite, then at least half the integers a in $\{1, \ldots, N\}$ satisfy $\left(\frac{a}{N}\right) \neq a^{(N-1)/2} \bmod N$.* ■

Gauss's famous Law of Quadratic Reciprocity, along with some additional basic properties of the Jacobi symbol, and the ancient trick of recursive squaring, implies that the equality $\left(\frac{a}{N}\right) \stackrel{?}{=} a^{(N-1)/2} \bmod N$ can be checked efficiently. (In particular, one *never* uses the factorization of N to compute $\left(\frac{a}{N}\right)$ in practice.) The Solovay–Strassen Primality Test, for an odd input N, then proceeds as follows: Pick a uniformly random $a \in \{1, \ldots, N\}$. Declare N to be composite if $\left(\frac{a}{N}\right) \neq a^{(N-1)/2} \bmod N$, or declare N to be *probably* prime otherwise. It is then easily checked that a declaration of compositeness is always correct, and a composite N will be declared composite with probability at least $\frac{1}{2}$. One can of course run the test k times to reduce the error probability to no worse than $\frac{1}{2^k}$.

The preceding test gives one-sided error: a declaration of compositeness is always correct, but probable primality need not mean actual primality. Based on an ingenious use of elliptic curves over finite fields, Adleman and Huang [AH92] later gave a randomized polynomial-time primality detection algorithm with one-sided error in the opposite direction: the algorithm either correctly declares primality (with probability at least $\frac{1}{2}$), or declares "possibly composite". Combining the Solovay–Strassen and Adleman–Huang primality tests, we thus obtain an efficient method to decide the primality of N: in time polynomial in $\log N$, we either get a correct answer (with probability at least $\frac{1}{2}$), or a declaration of doubt (with probability at most $\frac{1}{2}$).

From a theoretical point of view, assuming we are satisfied with the underlying source of randomness and we are willing to live with a small error probability, efficient primality detection was thus settled in the 1990s. At that time, derandomizing efficient primality testing still appeared as distant as efficient integer factorization (which still remains an open problem in early 2013). Agrawal, Kayal, and Saxena's early 21st century discovery of a *deterministic* algorithm for primality detection, with complexity $(\log N)^{7.5+o(1)}$, was then a spectacular advance [AKS02].

So we now know that randomness is not necessary for polynomial-time primality detection. However, in practice, refinements of the seminal methods of Solovay, Strassen, Adleman, Huang, and others (still using randomness) remain the methods of choice for checking primality of large integers.

Discerning whether randomness helps in other decision problems has led to deep results in complexity theory, e.g., the connections between polynomial identity testing and lower bounds for circuit complexity (see, e.g., [IW97, IK04, Koi11]). In our next setting, we will see how polynomial-time complexity is almost impossible without randomization, in certain *enumerative* problems.

3. Can randomness provably help us?

For the computation of volumes of high-dimensional polytopes, it appears that theoretical tractability hinges on the use of randomness: under certain well-known hypotheses from complexity theory, we can actually prove that randomness is needed.

More precisely, given a point set $\{a_1,\ldots,a_n\}\subset\mathbb{Z}^d$, with cardinality n, convex hull[2] P, and $n\geq d$, how quickly can one compute the standard Euclidean d-volume $\mathrm{Vol}_d(P)$? Before answering this question, let us recall some basic facts about polytopes.

First, recall that the convex hull Q of $d+1$ points in $\mathbb{R}^N$ with $\mathrm{Vol}_d(Q)>0$ is a *d-simplex*. Note also that by checking the rank of the matrix M whose columns are $a_2-a_1,\ldots,a_n-a_1$ (e.g., via a routine application of Hermite factorization [Sto00]), we can decide the inequality $\mathrm{Vol}_d(P)\stackrel{?}{>}0$ in time polynomial in $n+\sigma$, where σ is the maximum bit-size of any coordinate of any a_i. Finally, let us recall the standard computational geometry fact that computing a simplicial subdivision[3] $\{\Delta_i\}_i$ of P takes $\Theta\left(n^{\lfloor\frac{d+1}{2}\rfloor}+n\log n\right)$ arithmetic operations in the worst case [Ede87]. In summary, this means that, when $P\subset\mathbb{R}^d$, we can compute $\mathrm{Vol}_d(P)$ in time exponential in d by subdividing P and adding the volumes of the cells of the subdivision. Since the cells are simplices by construction, the volume is then simply a sum of $d\times d$ determinants (of matrices with columns of the form a_i-a_j).

Computing $\mathrm{Vol}_d(P)$ in time *polynomial* in $n+\sigma$ then turns out to be extremely difficult, if not impossible.

Theorem 3.1 ([DF88])**.** *If we define the bit-size of a point set $\{a_1,\ldots,a_n\}\subset\mathbb{Z}^d$ with convex hull P to be the sum of the bit-sizes of the coordinates of the a_i, then computing $\mathrm{Vol}_d(P)$ is $\#\mathbf{P}$-complete.* ■

$\#\mathbf{P}$ is the enumerative analogue of the complexity class **NP**. An algorithm for $\mathrm{Vol}_d(P)$ with complexity polynomial in $n+\sigma$ would thus imply $\mathbf{P}=\mathbf{NP}$—a widely doubted, but still unknown equality of complexity classes. Note that the bit-size of $\{a_1,\ldots,a_n\}$ is bounded from above by $dn\sigma$. Polynomiality in $n+\sigma$ is thus equivalent to polynomiality in the bit-size of $\{a_1,\ldots,a_n\}$ since we have assumed $n\geq d$. Note also that the bit-size of the integer $d!\mathrm{Vol}_d(P)$ is $O(d\sigma+n\log n)$ since P is certainly contained in the cube $[-2^\sigma,2^\sigma]^d$.

The discovery that randomization gives a way to circumvent the preceding complexity barrier was then another beautiful surprise from the 1990s.

Theorem 3.2 ([DFK91])**.** *There is a randomized algorithm that, given any $\delta,\varepsilon>0$, computes an approximation V of $\mathrm{Vol}_d(P)$ satisfying*

$$(1-\varepsilon)\mathrm{Vol}_d(P)\leq V\leq(1+\varepsilon)\mathrm{Vol}_d(P)$$

with probability at least $1-\delta$, using a number of bit operations polynomial in $n+\sigma+\frac{1}{\varepsilon}+\log\frac{1}{\delta}$. ■

The main result of [DFK91] is actually an efficient randomized algorithm for approximating the volume of any convex body given by a certain kind of *membership*

[2] i.e., smallest convex set containing $a_1,\ldots,a_n$

[3] i.e., a subdivision of P into a finite union of d-simplices $\bigcup_i\Delta_i$ such that the vertices of any Δ_i lie in $\{a_1,\ldots,a_n\}$ and $\Delta_i\cap\Delta_j$ is always a face of both Δ_i and Δ_j

oracle, i.e., a separate algorithm to decide whether an input point x is contained in P. Since membership in a convex hull can be decided in polynomial time via modern linear programming, the statement above thus follows via standard lattice-geometric rounding arguments. Theorem 3.2 (since improved by Lovász, Montenegro, Simonovitz, Sinclair, Vempala, and others [Sim03]) was first proved by starting with a clever reduction to another fundamental problem: efficiently simulating the uniform distribution on high-dimensional convex bodies. The key technical advance from [DFK91] was thus a subtle study of the convergence of a particular kind of random walk to the uniform distribution.

If one assumes $\mathbf{P} \neq \mathbf{NP}$, then Theorem 3.2 tells us that randomness is indeed our only hope for computing polytope volume in time polynomial in the dimension.

4. Beck's book

One can easily find many other examples (e.g., from algebraic geometry, combinatorial optimization, cryptography, and physics) of the algorithmic benefits of randomness. However, a deeper question is how randomness can help us understand or revisit non-algorithmic parts of mathematics as well. Beck goes in this direction, starting with a remarkably lucid discussion around a diverse set of examples. His ultimate goal is to support, formulate, and prove (in certain cases) a structural dichotomy for discrete systems. Briefly:

> *Discrete systems are either simple or they exhibit advanced pseudo-randomness.*

Beck calls this dichotomy the *Solid Liquid Gas (SLG) Conjecture*.

The distribution of the lower integer parts $\lfloor nx \rfloor_{n=1}^{\infty}$ mod 1, for x either a rational number or a quadratic irrational, gives a concrete example of this dichotomy: for rational x we have periodicity, but (as detailed in Chapter 5) a quadratic irrational x results in a distribution obeying a kind of Central Limit Theorem. Clarifying the SLG Conjecture, and applying it to combinatorial game theory, takes up the entire book, consisting of three parts.

Part A, spread across five chapters, shows how certain mathematical results can be reproduced, or how certain conjectures can be suggested, through simple probabilistic heuristics.

For example (see Chapter 3), if one imagines the Legendre symbols $\left(\frac{a}{p}\right)$ for $a \in \{1, \ldots, p-1\}$ to be independent and identically distributed uniform random variables taking values in $\{\pm 1\}$, one may infer (via the Central Limit Theorem) that $\sum_{a=1}^{x} \left(\frac{a}{p}\right) = O(\sqrt{x})$ (for $x \leq p$) with high probability. Considering that we can in fact prove (thanks to work of Polyá and Vinogradov around 1920) that $\sum_{a=1}^{x} \left(\frac{a}{p}\right) \leq \sqrt{p} \log p$, it is tempting to believe that our preceding heuristic has somehow been vindicated. However, proving $\sum_{a=1}^{x} \left(\frac{a}{p}\right) = x^{\frac{1}{2}+o(1)}$ remains an open problem, even for $x > p^{\varepsilon}$ and any $\varepsilon > 0$.

As another example (see Chapter 1), we can recall Cramer's famous heuristic for studying the primes: build a random set S of integers by tossing a biased coin for each integer n (starting from $n = 3$ and then proceeding in increasing order) and including n in S if one gets Heads. The coin one tosses for the integer n shows Heads with probability $\frac{1}{\log n}$ and Tails with probability $1 - \frac{1}{\log n}$. Curiously, the expectation of the cardinality $\#\{n \leq x \mid n \in S\}$ is within $O(1)$ of the classical function $\mathrm{Li}(x) :=$

$\int_2^x \frac{dt}{\log t}$, the latter being a well-known analytic approximation to the prime counting function $\pi(x)$. Furthermore, the fluctuation of $\#\{n \le x \mid n \in S\}$ about $\mathrm{Li}(x)$ is $O\left(x^{\frac{1}{2}+o(1)}\right)$, which is in harmony with the fluctuation of $\pi(x)$ about $\mathrm{Li}(x)$ predicted by the Riemann Hypothesis. (The inequality $|\pi(x) - \mathrm{Li}(x)| = O(\sqrt{x}\log x)$ is in fact equivalent to the Riemann Hypothesis, which remains unproved as of early 2013.)

Beck's other examples from Part A include the randomness of the base b digits of almost all real numbers (a classic 1909 theorem of Borel), the connections between continued fractions and ergodicity, the fluctuation of the average of value of $\#\{(x,y) \in \mathbb{Z}^2 \mid x^2 + y^2 = n\}$ about π, Erdős and Kac's 1939 Central Limit Theorem for the integer divisor function, and the assumption of randomness in the derivation of Boltzmann's Energy Law from statistical mechanics. All of Beck's examples are intriguing and quite clearly laid out.

In his discussion of Boltzmann's Energy Law, Beck uses a classical quandary to motivate a particular aspect of his main conjecture: the role of *a priori probabilities*. In particular, since completely calculating the state of, say, 10^{25} particles in a gas is infeasible, at such scales one makes an assumption that the states in an isolated system in equilibrium occur with equal probability. In other words, one assumes that the true physical behavior is consistent with assigning a priori probabilities in a judicious manner. (Just making sense of this assumption was a major impetus in the development of ergodic theory.) Unlike the assumption of equal probabilities in, say, the occurence of facets in the rolls of a (fair) six-sided die, the assignment of a priori probabilities in a setting without symmetry is a subtle matter. Moreover, due to the large dimension of the state space, we see that it is almost impossible to say anything useful in statistical mechanics without some application of randomness.

Games of complete information with no chance moves (dubbed *real game theory* in Beck's book) then form a completely disparate setting to our preceding discussion. Nevertheless, motivated by the SLG Conjecture, Beck proves in various cases that winning strategies exhibit behavior analogous to energy calculations in statistical physics. As laid out in Parts B and C, although real game theory is ultimately a finite setting which is amenable to brute-force search, randomness can give us deep insights into deriving winning strategies for deterministic (non-random) games.

Part B, consisting of eight chapters, deals with games on graphs and hypergraphs, and higher-dimensional variants of Tic-Tac-Toe, from the point of view of the SLG Conjecture. For instance, consider two players, named Red and Blue, who take turns (starting with Red) coloring the edges of the complete graph K_N on N vertices. (Red (resp. Blue) colors edges red (resp. blue).) Red wants to create a complete subgraph K_q with all edges red, with q as large as possible, while Blue simply wants to stop Red from doing so. The largest q that Red can always attain turns out to be

$$2\log_2\left(\frac{e^2}{8}\cdot\frac{N}{\log_2 N}\right) + o(1),$$

which is quite close to the expected size of the largest clique in a random graph on N vertices. This remarkable formula (along with a corresponding strategy that actually attains such a red K_q for Red) is clarified in Chapter 10. But more importantly, this result shows how randomness helps in a setting where one would expect brute force to be the only way to find a solution. Indeed, a good portion of Part B explains how "random play" can be turned into a deterministic strategy. Beck's discussion of Tic-Tac-Toe-like games actually quotes difficult theorems proved in

full in his earlier book [Bec08], which is triple the length of the book under review. So one of the key insights of Part B is a reinterpretation of [Bec08] in terms of the SLG Conjecture.

Part C narrows focus further by analyzing the *degree game on graphs*: put roughly, this is another game where (on a general graph) two players color edges as before, but now the goal is for Red to force some vertex to have as many red edges as possible. An invariant called "surplus" measures how much Red can gain over the obvious lower bound attainable via the Pigeon-hole Principle. The first main theorem of Part C gives upper and lower bounds on the surplus in terms of a quantity called the "core density" of the underlying graph. The core density turns out to be within a factor of 2 of several other important graph quantities: the arboricity, the greedy coloring number, the degeneracy, and the core-degree (see Chapter 14). The final main result of Part C refines these surplus bounds for the special case of d-regular graphs with $d \geq 200$: when the number of vertices is less than

$$2^{2^{2^{\cdot^{\cdot^{\cdot^{2^d}}}}}}$$

(where the number of 2's is $\log d$) the lower and upper bounds can be tightened to around $\sqrt{d}$, modulo an $O(\log^2 d)$ factor. Part C, while self-contained, is the most technically involved part of the book.

5. Final comments

Beck states around Chapter 9 that his book does not touch upon the complexity-theoretic aspects of randomness. This betrays considerable modesty on the author's part: Beck's treatment of games is a *tour de force* of discrete mathematics that, while not mentioning **P**, **BPP**, or **NP** explicitly, makes a serious conceptual advance in the algorithmic theory of games.

One should also be aware that there is another combinatorial setting where a deep structure versus randomness dichotomy has been rigourously proved: Szemerédi's Theorem [Sze75]. This celebrated result states that for any $k \in \mathbb{N}$ and positive real number $\delta \leq 1$, there is an integer $S(k, \delta) \geq 1$ such that for every $N \geq S(k, \delta)$, every set $A \subseteq \{1, \ldots, N\}$ of cardinality at least δN contains at least one arithmetic progression of length k. Tao observes in [Tao06, pg. 3] that all known proofs of Szemerédi's Theorem essentially split A into a *structured* portion and a *random* portion. (The definitions of structured and random can be made precise, relative to which proof is being used.) The metaphor of structure versus randomness thus clarifies the underpinnings of another important part of combinatorics.

As Beck innovatively demonstrates, using randomness to create deterministic strategies for games without random moves is an art. Beck's book also clearly reveals the SLG Conjecture to be a powerful conceptual tool worthy of broad attention.

Acknowledgments

I thank Peter Kuchment for valuable editorial remarks, and Leonid Gurvits, Dimitri Panchenko, and Joel Zinn for enlightening and enjoyable conversations.

References

[AH92] Leonard M. Adleman and Ming-Deh A. Huang, *Primality testing and abelian varieties over finite fields*, Lecture Notes in Mathematics, vol. 1512, Springer-Verlag, Berlin, 1992. MR1176511 (93g:11128)

[AKS02] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena, *PRIMES is in P*, Ann. of Math. (2) **160** (2004), no. 2, 781–793, DOI 10.4007/annals.2004.160.781. MR2123939 (2006a:11170)

[AB09] Sanjeev Arora and Boaz Barak, *Computational complexity: A modern approach*, Cambridge University Press, Cambridge, 2009. MR2500087 (2010i:68001)

[Bec08] József Beck, *Combinatorial games: Tic-Tac-Toe Theory*, Encyclopedia of Mathematics and its Applications, vol. 114, Cambridge University Press, Cambridge, 2008. MR2402857 (2009g:91038)

[DF88] Martin E. Dyer and Alan M. Frieze, *On the complexity of computing the volume of a polyhedron,* SIAM J. Comput., **17** (1988), no. 5, 967–974.

[DFK91] Martin Dyer, Alan Frieze, and Ravi Kannan, *A random polynomial-time algorithm for approximating the volume of convex bodies*, J. Assoc. Comput. Mach. **38** (1991), no. 1, 1–17, DOI 10.1145/102782.102783. MR1095916 (91m:68162)

[Ede87] Herbert Edelsbrunner, *Algorithms in combinatorial geometry*, EATCS Monographs on Theoretical Computer Science, vol. 10, Springer-Verlag, Berlin, 1987. MR904271 (89a:68205)

[For09] Lance Fortnow, *The status of the* **P** *versus* **NP** *problem,* Commun. ACM **52** (2009), no. 9, 78–86.

[IK04] Valentine Kabanets and Russell Impagliazzo, *Derandomizing polynomial identity tests means proving circuit lower bounds*, Comput. Complexity **13** (2004), no. 1-2, 1–46, DOI 10.1007/s00037-004-0182-6. MR2105971 (2005i:68025)

[IW97] Russell Impagliazzo and Avi Wigderson, P = BPP *if* E *requires exponential circuits: derandomizing the XOR lemma*, STOC '97 (El Paso, TX), ACM, New York, 1999, pp. 220–229 (electronic). MR1715634

[Koi11] Pascal Koiran, *Shallow Circuits with High-Powered Inputs,* in Proceedings of Innovations in Computer Science (ICS 2011, Jan. 6–9, 2011, Beijing China), Tsinghua University Press, Beijing.

[Lip09] Richard Lipton, *Gödel's Lost Letter and* **P** = **NP**, blog entry, `http://rjlipton.wordpress.com/the-gdel-letter` .

[Pap95] Christos H. Papadimitriou, *Computational complexity*, Addison-Wesley Publishing Company, Reading, MA, 1994. MR1251285 (95f:68082)

[Sim03] Miklós Simonovits, *How to compute the volume in high dimension?*, Math. Program. **97** (2003), no. 1-2, Ser. B, 337–374. ISMP, 2003 (Copenhagen). MR2004402 (2004j:68194)

[Sip92] Michael Sipser, *The history and status of the* **P** *versus* **NP** *question,* in Proceedings STOC '92 (Twenty-Fourth Annual ACM Symposium on Theory of Computing), pp. 603–618, ACM Press, 1992.

[SS77] R. Solovay and V. Strassen, *A fast Monte-Carlo test for primality*, SIAM J. Comput. **6** (1977), no. 1, 84–85. MR0429721 (55 #2732)

[Sto00] Arne Storjohann, *Algorithms for matrix canonical forms,* doctoral dissertation, Swiss Federal Institute of Technology, Zurich, 2000.

[Sze75] E. Szemerédi, *On sets of integers containing no k elements in arithmetic progression*, Acta Arith. **27** (1975), 199–245. Collection of articles in memory of Juriĭ Vladimirovič Linnik. MR0369312 (51 #5547)

[Tao06] Terence Tao, *A quantitative ergodic theory proof of Szemerédi's theorem*, Electron. J. Combin. **13** (2006), no. 1, Research Paper 99, 49. MR2274314 (2007i:37016)

J. Maurice Rojas

TAMU 3368, Texas A&M University, College Station, Texas 77843-3368

E-mail address: `rojas@math.tamu.edu`