


Bogdan Grechuk

Theorems of the 21st Century

Volume I

 Springer

Theorems of the 21st Century

Bogdan Grechuk

Theorems of the 21st Century

Volume I

 Springer

Bogdan Grechuk
Department of Mathematics
University of Leicester
Leicester, UK

ISBN 978-3-030-19095-8 ISBN 978-3-030-19096-5 (eBook)
<https://doi.org/10.1007/978-3-030-19096-5>

Mathematics Subject Classification (2010): 00-02, 00A05, 00A06, 00A09, 01-02, 01A61

© Springer Nature Switzerland AG 2019

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

Most of the theorems published recently in leading mathematical journals are so difficult that even their exact formulation is hard to understand for non-mathematicians, and, in some cases, even for mathematicians working in unrelated areas. For example, in 2009 Ngô Bảo Châu proved the result called the “Fundamental lemma of the Langlands program”, which was listed by Time magazine as one of the Top 10 scientific discoveries of 2009, and earned him a Fields Medal, one of the most prestigious awards in mathematics. However, even the exact formulation of the lemma (with all the notations defined) takes several pages to write down, and requires a high-level mathematical education to understand. We can compare this result with an abstract painting or a piece of modern art, which can be fully appreciated by a relatively small group of people. However, music, poetry, paintings, films, etc., tend to be described as “best” if they can be appreciated by millions.

Do there exist mathematical theorems like the songs of The Beatles, who had stadiums of fans at their concerts? That is, theorems which are sufficiently difficult and important to be accepted for publication into a leading mathematical journal, but at the same time with a sufficiently simple formulation which can be understood and appreciated by readers with at most an undergraduate (ideally high-school) education. The *Theorems of the 21st Century* project aims to show that such theorems do exist, and possibly, that there are more such theorems than you expected.

For this book, which is the first in the *Theorems of the 21st Century* series, we examine theorems published in the first decade of the twenty-first century in the *Annals of Mathematics*, which is undoubtedly one of the leading mathematical journals, and discover that the formulation of a significant portion of them (we selected 106 theorems published between 2001 and 2010) can indeed be explained to a reader with relatively little background.

This book consists of short introductions, each being 3–4 pages in length, aimed at explaining the formulations and importance of the selected theorems. Although we sometimes refer to earlier sections of the book “for more details”, each introduction is essentially self-contained and can be read independently. Because of this,

some repetitions are unavoidable. For example, the definition of a group is repeated multiple times throughout the book.

We aim to explain each theorem to the reader with the minimal possible background. For some easier-to-understand theorems, the introductions are aimed at a high-school audience, with very little preliminary knowledge assumed: sometimes even the definition of a prime number is included. Introductions to more advanced theorems assume at least an undergraduate level.

While aiming to be accessible, we also try to maintain mathematical rigor whenever possible. Instead of adopting a newspaper-style exposition, saying that “mathematicians have proved an important result, but the details are too difficult to be presented here,” we formulate each theorem rigorously, and, when possible, give the formal definitions of all the concepts involved. The main focus is on the formulation of each theorem, its importance, and applications—the proofs of the vast majority of the theorems are not discussed at all.

Each section is devoted to one theorem, and ends with the reference to the paper in which this theorem has been proved. Some papers have several main results, in which case we have selected one of them (the most important or most accessible) as the main “theorem” to be explained, sometimes giving brief informal descriptions of the other results.

Of course, the theorems described in this book form just a small portion of the amazing mathematical discoveries of the twenty-first century. Many theorems of the highest importance, such as Perelman’s proof of the Poincaré conjecture, were not published in the *Annals of Mathematics*, while some other important theorems have been omitted because we found their formulations to be too difficult to explain. Also, the period after 2011 is not covered at all. The descriptions of other great theorems will be included in future volumes of the series.

Leicester, UK
March 2019

Bogdan Grechuk

Acknowledgements

I would like to thank Tetiana, my wife, for her continued support, encouragement, and patience while I was writing this book.

I also thank Vasyl Grechuk, my father, for many useful discussions, suggestions, and help with the figures.

I thank Paayal Mehta, Benjamin Kettley, Hiren Ladha, Sazid Balayet, and Shashank Himatrai, who did *Theorems of the 21st Century* Nuffield research projects under my supervision, and provided me with a lot of very useful feedback, suggestions, and corrections. I also thank the Nuffield Foundation for the opportunity to be a project provider with them and for finding these students for my projects.

I thank my M.Sc. student, Luke Kempford, and my Ph.D. students, Dawei Hao and Sittichoke Som-Am, for reading the preliminary draft of this book, and for providing some suggestions and corrections.

I thank the authors of the theorems I describe in this book, prominent mathematicians who found time to read my descriptions of their theorems and provide me with very useful feedback, corrections, and suggestions. I especially thank Prof. Kevin Ford, who sent me a brilliant text about his Theorem 8.10, and allowed me to use this text in the book as is. I also received very valuable help and feedback from other authors, including Profs. Dimitris Achlioptas, Noga Alon, Marton Balazs, Itai Benjamini, Jean-Camille Birget, Yitwah Cheung, David Conlon, Jordan Ellenberg, Tamas Erdelyi, Alexandre Eremenko, Etienne Fouvry, Nicola Fusco, Loukas Grafakos, Andrew Granville, Ben Green, Roger Heath-Brown, Harald Helfgott, Bill Helton, Michael Hochman, David Hoffman, Dan Isaksen, Bo'az Klartag, Juergen Kluners, Oleg Kozlovski, Bryna Kra, Greg Kuperberg, Martin Liebeck, Mikhail Lyubich, Francesco Maggi, Jens Marklof, Christian Mauduit, William H. Meeks III, Manor Mendel, Tom Meyerovitch, Carlos Gustavo Moreira, Frank Morgan, Oleg Musin, Ken Ono, Aldo Pratelli, Omer Reingold, Joël Rivat, Jay Rosen, Muli Safra, Alexander Solynin, Jeffrey Steif, Michel Talagrand, Terence Tao, Robin Thomas, Van Vu, Matthias Weber, Michael Wolf, Trevor Wooley, Saeed Zakeri, and Ofer Zeitouni.

I thank my colleagues at the Department of Mathematics, University of Leicester, and especially Ruslan Davidchack, for reading parts of this book and providing suggestions and corrections.

I also thank the University of Leicester for granting me academic study leave, part of which I used to finish this book.

I thank Springer, and especially Rémi Lodh, for their interest in publishing this book. I also thank the referees for their suggestions, and Barnaby Sheppard for his careful copy edit of the manuscript.

Contents

1	Theorems of 2001	1
1.1	Moderate Deviations for the Volume of the Wiener Sausage	1
1.2	The Minimal Average Value of a Bounded Multiplicative Function	6
1.3	Counting Integer Solutions of Some Inequalities	10
1.4	On the Arithmetic Difference of Regular Cantor Sets	14
1.5	The Existence of Different Groups with Isomorphic Group Rings	18
1.6	Short Representations of Elements of Finite Simple Groups	23
1.7	The Existence of a Field with μ -Invariant 9	26
2	Theorems of 2002	31
2.1	Counting Rational Functions with Given Critical Points	31
2.2	Representing Braids as Matrices	35
2.3	Explicit Expander Constructions Using the Zig-Zag Product	38
2.4	Elliptic Curves Over Function Fields Can Have Arbitrarily Large Rank	42
2.5	The Optimality of the Standard Double Bubble	46
2.6	Counting Integer Solutions of Equations in Three Variables	49
2.7	The Regular-Stochastic Dichotomy for Quadratic Polynomials	53
2.8	A Finitely Presented Group with an NP-Complete Word Problem	58
2.9	Finitely Generated Groups with a Word Problem in NP	63
2.10	Positive Noncommutative Polynomials are Sums of Squares	66

2.11	The Only Space Isomorphic to Each of its Subspaces	69
2.12	Counting Matrices with Some Special Properties	73
2.13	Transforming Convex Bodies into Balls	77
3	Theorems of 2003	81
3.1	On the Differentiability of Lipschitz Maps on Infinite-Dimensional Spaces	81
3.2	Representing 1 as a Sum of Reciprocals of Selected Integers	85
3.3	The Optimal Hardy–Littlewood Maximal Inequality	88
3.4	Improved Upper Bounds on Sphere Packings	92
3.5	Sums <i>Versus</i> Products of Finite Sets of Integers	95
3.6	The Radius of Integer Points in the Plane	98
3.7	The Set of Nonergodic Directions Can Have Dimension $1/2$	102
3.8	A Real Number Which Is Far from All Cubic Algebraic Integers	106
4	Theorems of 2004	111
4.1	The Julia Set of Almost All Quadratic Polynomials is Locally Connected	111
4.2	The Regular Polygons have Minimal Logarithmic Capacity	116
4.3	On the Growth of the Diffusion Coefficient	119
4.4	On the Volume of the Intersection of Two Wiener Sausages	123
4.5	Controlling the Size of the Bilinear Hilbert Transform	127
4.6	Covering Convex Bodies by Balls	130
4.7	The Parametrization of Quartic Rings	133
4.8	The Time it Takes for a Random Walk to Cover the Plane	137
4.9	On the Geometry of the Uniform Spanning Forest	141
4.10	A Polynomial Time Algorithm for Primality Testing	144
5	Theorems of 2005	149
5.1	Structured Additive Patterns in Sets of Positive Density	149
5.2	A Sharp Form of Whitney’s Extension Theorem	154
5.3	Minimal Surfaces in 3-Space I	157
5.4	Statistical Properties of Quadratic Dynamics	161
5.5	Every Subset of Primes of Positive Density Contains a 3-Term Progression	164
5.6	Every Separable Infinite-Dimensional Banach Space Has Infinite Diameter	168
5.7	The NP-Hardness of the 1.36...-Approximation to the Minimum Vertex Cover	172

- 5.8 Embedding Large Subsets of Finite Metric Spaces
into Euclidean Space 176
- 5.9 On the Number of Quartic Fields with Bounded
Discriminant 180
- 5.10 Optimal Sphere Packing in Dimension 3 183
- 5.11 The Chromatic Number of a Random Graph 187
- 6 Theorems of 2006 191**
 - 6.1 Sufficient Conditions for Completeness of a Set of Integers . . . 191
 - 6.2 Counting Number Fields of Bounded Discriminant 194
 - 6.3 Perfect Powers in Fibonacci and Lucas Sequences 198
 - 6.4 A Characterization of Perfect Graphs 201
 - 6.5 Littlewood’s Conjecture Holds Outside of a Set of
Dimension 0 204
 - 6.6 The Connection Between Metric Entropy and Combinatorial
Dimension 208
 - 6.7 On the Approximation of Real Numbers by Irreducible
Fractions 211
- 7 Theorems of 2007 217**
 - 7.1 Bounding the Error in Approximation of Smooth
Functions by Polynomials 217
 - 7.2 Superlinear Growth of Digit Patterns in the Decimal
Expansion of Algebraic Numbers 221
 - 7.3 The Existence of Intervals with Too Many and Too Few
Primes 224
 - 7.4 Interval Exchange Transformations Are Almost Always
Weakly Mixing 228
 - 7.5 The Hopf Condition Over Arbitrary Fields 231
 - 7.6 Any Real Polynomial Can be Approximated by a Hyperbolic
Polynomial 235
 - 7.7 The Schinzel–Zassenhaus Conjecture for Polynomials
with Odd Coefficients 239
 - 7.8 Diophantine Approximation of Points on Smooth Planar
Curves 243
 - 7.9 The Hasse Principle for Systems of Two Diagonal Cubic
Equations 247
 - 7.10 An Effective Multidimensional Szemerédi Theorem 250
- 8 Theorems of 2008 255**
 - 8.1 Minimal Surfaces in 3-Space II 255
 - 8.2 Arbitrarily Long Arithmetic Progressions of Prime
Numbers 259
 - 8.3 On Poincaré’s Inequality 262

8.4	Representing Matrices in $SL_2(\mathbb{Z}/p\mathbb{Z})$ Using a Small Number of Generators	266
8.5	The Cayley Graphs of $SL_2(\mathbb{F}_p)$ Form a Family of Expanders	269
8.6	Determining the Shape of an Infected Region	272
8.7	A Negative Answer to Littlewood’s Question About Zeros of Cosine Polynomials	276
8.8	The Kissing Number in Dimension Four is 24	279
8.9	A Criterion for Embedding L_p into L_q Uniformly	283
8.10	The Distribution of Integers with a Divisor in a Given Interval	286
8.11	An Upper Bound for the Norm of the Inverse of a Random Matrix	291
8.12	An Isoperimetric Inequality with Optimal Exponent	294
8.13	A Negative Answer to Maharam’s Question	298
9	Theorems of 2009	303
9.1	On De Giorgi’s Conjecture in Dimension at Most 8	303
9.2	An Efficient Algorithm for Fitting a Smooth Function to Data	307
9.3	A Helicoid-Like Surface with a Hole	310
9.4	Bounding the Condition Number of Random Discrete Matrices	314
9.5	Characterizing the Legendre Transform of Convex Analysis	318
9.6	The Solution of the Ten Martini Problem	321
9.7	A Linear Time Algorithm for Edge-Deletion Problems	325
9.8	A Characterization of Stability-Preserving Linear Operators	328
9.9	On the Gaps Between Primes	332
9.10	A Proof of the B. and M. Shapiro Conjecture in Real Algebraic Geometry	335
9.11	Bounding Diagonal Ramsey Numbers	339
9.12	An Almost Optimal Upper Bound for Moments of the Riemann Zeta Function	342
9.13	Optimal Lattice Sphere Packing in Dimension 24	346
9.14	A Waring-Type Theorem for Large Finite Simple Groups	350
10	Theorems of 2010	355
10.1	Majority Votes Are the Most Stable	355
10.2	On Divisibility Properties of Dyson’s Rank Partition Function	360
10.3	Exceptional Times in Percolation Theory	364
10.4	Polynomial Parametrization for the Solutions of Diophantine Equations	367

- 10.5 The Order of Growth of Variance in the Asymmetric Simple Exclusion Process 370
- 10.6 Divergent Square Averages in Ergodic Dynamical Systems 374
- 10.7 Divisibility Properties of Sums of Digits of Prime Numbers 379
- 10.8 Prime Values of Linear Equations 383
- 10.9 Entropies of Multidimensional Shifts of Finite Type may be Impossible to Compute 389
- 10.10 Subgroups of 2-Generated Groups 393
- 10.11 On the Number of Quintic Fields with Bounded Discriminant 398
- 10.12 On the Negative Pell Equation 403
- 10.13 The Norms of Random Band Matrices 408
- 11 Further Reading 413**
- References 415**
- Author Index 431**
- Index 437**

Acronyms

Some standard mathematical notation.

- \mathbb{Z} – the set of all integers: $\dots, -3, -2, -1, 0, 1, 2, 3, \dots$
- \mathbb{Q} – the set of rational numbers, that is, numbers of the form $\frac{n}{m}$, where n and $m \neq 0$ are integers.
- \mathbb{R} – the set of all real numbers.
- \mathbb{R}^d – standard (Euclidean) d -dimensional space. For example, \mathbb{R}^2 is the plane, while \mathbb{R}^3 is the 3-dimensional space we live in.
- $[a, b]$ denotes the set of all real numbers x such that $a \leq x \leq b$.
- (a, b) denotes the set of all real numbers x such that $a < x < b$.
- $[a, b)$ and $(a, b]$ denote the set of all real numbers x such that $a \leq x < b$, and $a < x \leq b$, respectively.
- If x is a real number, $|x|$ denotes the absolute value of x . For example, $|3| = 3$, while $|-5| = 5$.
- $\exp(x)$ denotes e^x , where $e = 2.71828\dots$ is the base of the natural logarithm.
- \in denotes membership of a set. For example, $n \in \mathbb{Z}$ means that n is an integer, while $x \in \mathbb{R}$ states that x is a real number.
- $X \subset Y$ indicates that the set X is a subset of the set Y . For example, $\mathbb{Z} \subset \mathbb{Q}$, while $\mathbb{Q} \subset \mathbb{R}$.
- \forall – for every. For example, “ $\forall n \in \mathbb{Z}\dots$ ” means “For every integer $n\dots$ ”.
- \exists – exists. For example, “ $\exists n \in \mathbb{Z}\dots$ ” means “There exists an integer $n\dots$ ”.
- $\{\dots|\dots:\dots\}$ is a notation used to describe a set. For example, let A be the set of all even integers. In other words, A is the set of all integers n for which there exists an integer k such that $n = 2k$. This can be written as $A = \{n \in \mathbb{Z} | \exists k \in \mathbb{Z} : n = 2k\}$.
- If S is a finite set, $|S|$ denotes the number of elements in S . For example, $|\{7, 9, 11\}| = 3$.
- \sum denotes summation. For example, $\sum_{i=1}^n x_i$ is a notation for $x_1 + x_2 + \dots + x_n$. In particular, $\sum_{i=1}^3 i^2 = 1^2 + 2^2 + 3^2 = 14$.

- $\sum \sum$ denotes double summation for all pairs of the corresponding indices. For example, $\sum_{i=1}^2 \sum_{j=1}^2 x_{ij} = x_{11} + x_{12} + x_{21} + x_{22}$. Or,

$$\sum_{i=1}^2 \sum_{j=1}^2 i^2 j = 1^2 \cdot 1 + 1^2 \cdot 2 + 2^2 \cdot 1 + 2^2 \cdot 2 = 15.$$

- \prod denotes a product. For example, $\prod_{i=1}^n x_i$ is a notation for $x_1 \cdot x_2 \cdot \dots \cdot x_n$ (sometimes we omit \cdot and just write $x_1 x_2 \dots x_n$). Or,

$$\prod_{i=1}^2 \prod_{j=1}^2 (2i+j) = (2 \cdot 1 + 1)(2 \cdot 1 + 2)(2 \cdot 2 + 1)(2 \cdot 2 + 2) = 360.$$

- \cup denotes the union of sets. For example, $\{1, 2\} \cup \{2, 3, 4\} = \{1, 2, 3, 4\}$. Also, $\bigcup_{i=1}^n A_i$ denotes the union $A_1 \cup A_2 \cup \dots \cup A_n$.
- \cap denotes the intersection of sets. For example, $\{1, 2\} \cap \{2, 3, 4\} = \{2\}$. Also, $\bigcap_{i=1}^n A_i$ denotes the intersection $A_1 \cap A_2 \cap \dots \cap A_n$.
- For a positive integer n , $n!$ denotes the product of all integers from 1 to n , for example, $3! = 1 \cdot 2 \cdot 3 = 6$. We also define $0!$ to be 1.
- $:=$ denotes “equal by definition”. For example, $n! := 1 \cdot 2 \cdot \dots \cdot n$ for every positive integer n .
- \min denotes the operation of finding the minimum. For example, $\min(-2, 7, 3) = -2$. Also, $\min_{-1 \leq x \leq 2} (x^2 + 1) = 1$, because the minimum value of $x^2 + 1$ for $x \in [-1, 2]$ is equal to 1.
- Similarly, \max denotes the operation of finding maximum. For example, $\max(-2, 7, 3) = 7$, and $\max_{-1 \leq x \leq 2} (x^2 + 1) = 5$.
- \inf denotes the infimum. For a set $S \subset \mathbb{R}$, $\inf S$ is the largest real number x such that $y \geq x$ for all $y \in S$. For example, $\inf_{1 < x < 3} (x^2 + 1) = 2$.
- Similarly, \sup denotes the supremum. For a set $S \subset \mathbb{R}$, $\sup S$ is the smallest real number x such that $y \leq x$ for all $y \in S$. For example, $\sup_{1 < x < 3} (x^2 + 1) = 10$.
- $a \equiv b \pmod{c}$ means that integers a and b give the same remainder after division by c , or, in other words, $a - b$ is divisible by c . For example, $11 \equiv 2 \pmod{3}$.

Chapter 1

Theorems of 2001



1.1 Moderate Deviations for the Volume of the Wiener Sausage

Heat Conduction, and Particle Trajectories

When you turn on a radiator in your house, it first heats the air within a small distance from it. How long will it take for the “hot air” to “spread out”, mix well with the “cold air”, and make your house uniformly warm? This process is called *heat conduction*. To understand it, let us look at the trajectory of an individual particle which starts near the radiator. Of course, this trajectory is complicated, frequently changing direction (due to particle collisions), but initially it is *local*, that is, it moves within a small region near the radiator. If we wait long enough, however, the particle will eventually travel throughout the room. To understand heat conduction (and other similar important processes and phenomena), we need to understand how “big” the region “covered” by the trajectory of a particle gets before any given time t .

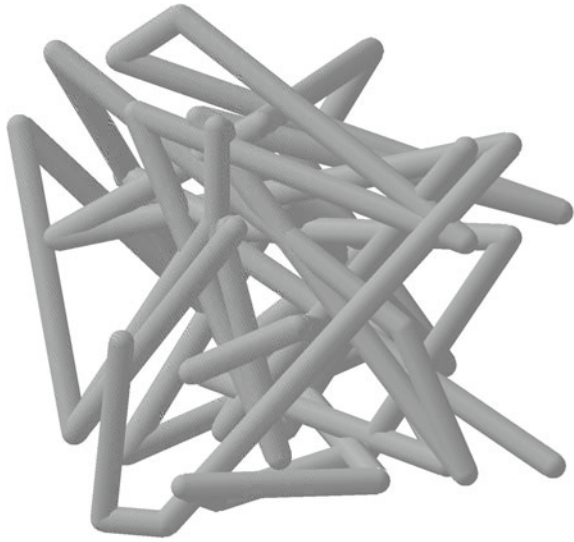
The Volume of the “Covered” Space

Let us be a bit more formal. Particle trajectories can be studied in any dimension d : for example, for $d = 1$, we can study particles moving in a very thin tube. Let the particle be modelled as a point, and let $W(t) = (w_1(t), \dots, w_d(t))$ denotes its coordinates at time t . For any $a > 0$, define

$$W^a(t) = \{x \in \mathbb{R}^d \mid \exists s \in [0, t] : \rho(x, W(s)) \leq a\}, \tag{1.1}$$

where ρ denotes the usual distance in \mathbb{R}^d . In other words, $W^a(t)$ is the set of all points at distance at most a from the particle trajectory (Fig. 1.1). The question

Fig. 1.1 The set $W^a(t)$ in (1.1) for a piecewise-linear curve $W(t)$ in dimension $d = 3$



“How big is the region covered by the trajectory?” can be formalized as “What is the (d -dimensional)¹ volume of $W^a(t)$?”. We will denote this volume by $|W^a(t)|$.

For example, let us assume for a moment that $d = 3$ and the particle moves in a straight line with constant velocity v during the time period t . In this case, $W(t)$ is a line segment of length vt , and $W^a(t)$ is a cylinder with radius a , height vt , and with semi-spheres attached to the top and the bottom. Hence, its total volume is $|W^a(t)| = \frac{4}{3}\pi a^3 + \pi a^2 vt$. In particular, $|W^a(t)|$ grows as a linear function of t . One could derive a similar result if $W(t)$ is a non-straight but smooth curve without too many self-intersections, because in this case $W^a(t)$ is essentially the same cylinder but bent.

However, the trajectories of the movement of actual particles are very far from being either straight or smooth lines. In fact, individual particle trajectories are so complicated and unpredictable that the best we can do is to consider them as “random”, and study them using the language and tools of *probability theory*. That is, instead of answering questions like “Where will this particle be after time t ?”, we will be talking about *the chance* that the particle, after time t , will be in this or that region.

A Simple Example of Random Movement

To understand what we mean by a “random trajectory” imagine a very drunk man moving along a street. He makes one step every second, but the direction of every

¹For example, for $d = 3$ we are talking about the “usual” volume, for $d = 2$ about the covered area, while for $d = 1$, about the length of the covered interval.

step may be left or right, with equal chance. For example, after 2 steps, he can move right and then again right (we denote this scenario as RR), or right and then left (RL), or left and then right (LR), or left and again left (LL). If we put him on the coordinate line, assume that he starts at 0, and his step length is 1, then, after 2 steps, he will reach point 2 in the RR scenario, return to 0 in the LR and RL scenarios, and reach point -2 in the LL scenario. In other words, if X_t denotes his position after t steps, then X_2 may be equal to 2, 0, or -2 . We cannot answer the question “what is X_2 ?”, we can only list its possible values, and we can also talk about the chances, or *probabilities*, that these values will happen. In our case, the probability that $X_2 = 2$, denoted as $P(X_2 = 2)$, is equal to $1/4$, because this can happen in 1 out of 4 possible scenarios. Similarly, $P(X_2 = 0) = 2/4 = 1/2$, because $X_2 = 0$ in 2 scenarios (LR and RL) out of 4. Finally, $P(X_2 = -2) = 1/4$.

The Average Length of the Covered Interval

Now, let V_t be the length of the interval the man “covered” up to time t . For example, let $t = 2$. In the RR scenario, the man moves straight from 0 to 2, the covered interval is $[0, 2]$, and $V_2 = 2$. In the RL scenario, the man moved from 0 to 1 and back to 0, hence he covered only the interval $[0, 1]$, and $V_2 = 1$. Similarly, in the LR scenario, the covered interval is $[-1, 0]$, and $V_2 = 1$, while in the LL scenario, the covered interval is $[-2, 0]$, and $V_2 = 2$. In summary, V_2 can take values 1 or 2, with probabilities $P(V_2 = 1) = P(V_2 = 2) = 2/4 = 1/2$. If $t = 3$, there are 8 scenarios of movements, RRR , RRL , RLR , RLL , LRR , LRL , LLR , and LLL , and a similar calculation shows that V_3 can take values 1, 2, and 3, with probabilities $P(V_3 = 1) = P(V_3 = 3) = 2/8 = 1/4$, and $P(V_3 = 2) = 4/8 = 1/2$.

In general, after t steps, there are $m = 2^t$ possible scenarios of movements, which we can denote as $\omega_1, \dots, \omega_m$ ($\omega_1 = RRR \dots RR$, $\omega_2 = RRR \dots RL$, \dots , $\omega_m = LLL \dots LL$). For each ω_i , $i = 1, 2, \dots, m$, we can calculate the length $V_t(\omega_i)$ of the covered interval in this scenario, which then allow us to list all possible values of V_t with the corresponding probabilities.

While we cannot predict what the actual value of V_t will be (because we do not know which particular scenario the drunk man will implement), we can at least calculate the *average* (also called *expected*) value of V_t over all possible scenarios: $E[V_t] = \frac{1}{m} \sum_{i=1}^m V_t(\omega_i)$. Equivalently, $E[V_t] = \sum_{i=1}^k v_i \cdot p_i$, where v_1, v_2, \dots, v_k is the list of values V_t may take, and p_1, p_2, \dots, p_k are the corresponding probabilities. For example, $E[V_2] = \frac{1}{4}(1 + 1 + 2 + 2) = 1 \cdot \frac{2}{4} + 2 \cdot \frac{2}{4} = 1.5$, while $E[V_3] = \frac{1}{8}(1 + 1 + 2 + 2 + 2 + 2 + 3 + 3) = 1 \cdot \frac{2}{8} + 2 \cdot \frac{4}{8} + 3 \cdot \frac{2}{8} = 2$.

The Probabilities of “Moderate” Deviations from the Average

The value of $E[V_t]$ gives us an approximate idea about how large V_t is. However, how good is this “approximation”? For example, what is the probability that the actual

covered length V_t will be no greater than, say, 70% of its average value $E[V_t]$? For $t = 2$, $P(V_2 \leq 0.7E[V_2]) = P(V_2 \leq 0.7 \cdot 1.5) = P(V_2 \leq 1.05) = 2/4 = 1/2$. For $t = 3$, $P(V_3 \leq 0.7E[V_3]) = P(V_3 \leq 0.7 \cdot 2) = P(V_3 \leq 1.2) = 2/8 = 1/4 < 1/2$. If we could prove that, for large t , $P(V_t \leq 0.7E[V_t])$ becomes negligibly small, and the same is true for $P(V_t \geq 1.3E[V_t])$, we could conclude that, with very high probability, $0.7E[V_t] < V_t < 1.3E[V_t]$, that is, $E[V_t]$ approximates V_t with at least 70% accuracy. Similarly, proving that $P(V_t \leq 0.99E[V_t])$ and $P(V_t \geq 1.01E[V_t])$ are small for large t would allow us to conclude that $E[V_t]$ approximates V_t with at least 99% accuracy. Probabilities of the form $P(V_t \leq cE[V_t])$ for some constant $c < 1$ are called probabilities of *moderate*² deviations. Estimates from above for such probabilities are crucial for understanding how well $E[V_t]$ approximates V_t .

The Standard Model of Particle Movement: The Wiener Process

In some sense, particle movement resembles the movement of a drunk man considered above. If the particle is modelled as a point and forces are ignored, we can assume that it moves in a straight line until the first collision, then changes direction randomly, moves until the next collision, changes direction again, and so on.

The standard model of particle movement is called the *Wiener process*. If $d = 1$ (movement in a thin tube), the Wiener process is, intuitively, the limiting case of the movement of the drunk man. That is, we assume that the step length of the man is ε , the number of steps is $N = 1/\varepsilon^2$ per unit of time, and then let ε go to 0. The intuition in dimensions $d \geq 2$ is similar.

The Volume of a Wiener Sausage

If $W(\cdot)$ is a Wiener process, then $W^a(t)$, as defined in (1.1), is called a *Wiener sausage*. It was introduced in 1964 by Frank Spitzer [355], and since then has been used in the description of a number of physical phenomena, including heat conduction. It is known [355] (but the proof is too difficult to be presented here) that the average (or expected) volume $E|W^a(t)|$ is, for large t , approximately equal to

$$E|W^a(t)| \approx \begin{cases} \sqrt{8t/\pi}, & \text{if } d = 1, \\ 2\pi t / \ln t, & \text{if } d = 2, \\ 2\pi at, & \text{if } d = 3, \end{cases} \quad (1.2)$$

and similarly $E|W^a(t)| = C(a, d)t$ for $d \geq 3$, where $C(a, d)$ is a constant depending on a and d .

²The term ‘‘moderate’’ comes from the fact that probabilities of the form $P(V_t \leq f(t)E[V_t])$ for some function $f(t)$ such that $\lim_{t \rightarrow \infty} f(t) = 0$ are known as probabilities of *large* deviations.

To understand how close $|W^a(t)|$ is to its average value (1.2), we need to have a good estimate from above for the probability of moderate deviation $P(|W^a(t)| \leq cE|W^a(t)|)$ for $c < 1$. The following theorem of M. van den Berg, E. Bolthausen and F. den Hollander [384] answers this question in all dimensions $d \geq 2$.

Theorem 1.1 For every $a > 0$, $b \in (0, 2\pi)$,

$$\lim_{t \rightarrow \infty} \frac{1}{\ln t} \ln P(|W^a(t)| \leq bt / \ln t) = -I^{2\pi}(b), \quad d = 2,$$

and for every $a > 0$, $b \in (0, C(a, d))$,

$$\lim_{t \rightarrow \infty} \frac{1}{t^{(d-2)/d}} \ln P(|W^a(t)| \leq bt) = -I^{C(a,d)}(b), \quad d \geq 3.$$

Here, $C(a, d)$ is the constant defined after Eq. (1.2), and $I^{C(a,d)}(b)$ is the “rate function”, for which a detailed analysis is given, with some analytic formulas, estimates, graphs, etc. In short, Theorem 1.1 completely resolves the problem of estimating the probabilities in question for large t .

Some Special Cases

For $d = 2$, $b = 1.98\pi$, and large t , Theorem 1.1 implies that

$$P(|W^a(t)| \leq 1.98\pi t / \ln t) \approx t^{-C},$$

where $C = I^{2\pi}(1.98\pi)$ is a positive constant. So, the probability that volume $|W^a(t)|$ is just 1% less than the average value $2\pi t / \ln t$ goes to 0 as $t \rightarrow \infty$.

Similarly, for $d = 3$, $b = 1.98\pi a$, and large t ,

$$P(|W^a(t)| \leq 1.98\pi at) \approx \exp(-Ct^{1/3}),$$

for some $C > 0$. In this case, the probability of 1% volume deviation from average not only goes to 0, but in fact decreases exponentially fast with t . That is, if we wait a little bit, we are guaranteed that the trajectory volume of essentially all particles will be within 1% from $2\pi at$. Obviously, 1% here can be replaced by any other arbitrary small constant.

Reference

M. van den Berg, E. Bolthausen and F. den Hollander, Moderate deviations for the volume of the Wiener sausage, *Annals of Mathematics* **153**-2, (2001), 355–406.

1.2 The Minimal Average Value of a Bounded Multiplicative Function

Multiplicative Functions with Small Average Values

A function $f : \mathbb{N} \rightarrow \mathbb{R}$, where \mathbb{N} is the set of positive integers and \mathbb{R} is the real line, is called *completely multiplicative* if $f(mn) = f(m)f(n)$ for all positive integers m, n . Assuming that $|f(n)| \leq 1$ for all $n \in \mathbb{N}$, what can the average value $\frac{1}{x} \sum_{n \leq x} f(n)$ be for large x ? Because $|f(n)| \leq 1$ for all n ,

$$\left| \frac{1}{x} \sum_{n \leq x} f(n) \right| \leq \frac{1}{x} \sum_{n \leq x} |f(n)| \leq \frac{1}{x} \sum_{n \leq x} 1 \leq \frac{1}{x} \cdot x = 1,$$

hence $\frac{1}{x} \sum_{n \leq x} f(n)$ is always between -1 and 1 . For the function $f(n) = 1, \forall n$, this average is equal to 1 , the maximal possible. However, it is not clear whether the lower bound -1 is achievable. The average is -1 for the function $f(n) = -1, \forall n$, but it is not completely multiplicative (for example, $f(6) = -1 \neq 1 = f(2)f(3)$).

Let us try to ensure that the values $f(n)$ are as small as possible. Because $f(1) \cdot f(1) = f(1 \cdot 1) = f(1)$, we have $f(1) = 0$ or $f(1) = 1$. If $f(1) = 0$, then for any n , $f(n) = f(n \cdot 1) = f(n) \cdot f(1) = f(n) \cdot 0 = 0$, and $\frac{1}{x} \sum_{n \leq x} f(n) = 0$. To try to do better, we should choose $f(1) = 1$. Following our strategy to assign values as small as possible, we can let $f(2) = f(3) = -1$, but then $f(4) = f(2)f(2) = 1$. Next, we can assign $f(5) = -1$, but then $f(6) = f(2)f(3) = 1$. Continuing, we can choose $f(7) = -1$, and also $f(8) = f(4)f(2) = -1$, but then $f(9) = f(3)f(3) = 1$ and $f(10) = f(2)f(5) = 1$. Checking the average so far, we get $\frac{1}{10} \sum_{n \leq 10} f(n) = 0$: no progress!

The Proof of a Conjecture of Hall

In 1996, Richard Hall [187] constructed an example of a completely multiplicative function f with average value $\frac{1}{x} \sum_{n \leq x} f(n)$ for large x approximately equal to

$$\delta_1 = 1 - 2 \ln(1 + \sqrt{e}) + 4 \int_1^{\sqrt{e}} \frac{\ln t}{t+1} dt \approx -0.656999, \quad (1.3)$$

and conjectured that this is the lowest possible. This conjecture was proved by A. Granville and K. Soundararajan [172].

Theorem 1.2 For a completely multiplicative function f taking values in $[-1, 1]$, we have

$$\delta_1 \leq \lim_{x \rightarrow \infty} \frac{1}{x} \sum_{n \leq x} f(n) \leq 1, \quad (1.4)$$

where δ_1 is given by (1.3). Conversely, for any $\delta \in [\delta_1, 1]$ there exists an f as above such that the limit is equal to δ .

Quadratic Residues and Non-residues

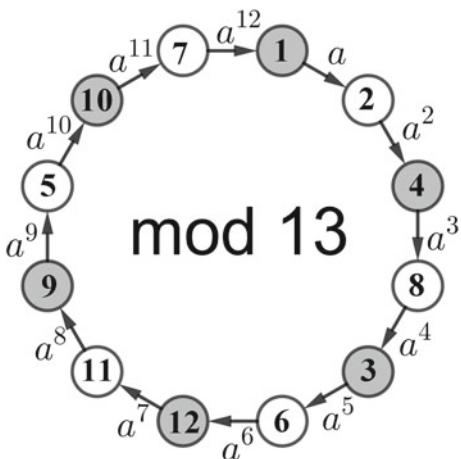
Applying Theorem 1.2 to various functions f , we can derive a number of interesting and non-trivial results. Here is one example. An integer n is called a *quadratic residue* modulo an integer p if $x^2 - n$ is divisible by p for some integer x , and a *quadratic non-residue* otherwise. For example, $2^2 - 1$ is divisible by 3, hence $n = 1$ is a quadratic residue modulo $p = 3$. However, what about $n = 2$? Can $x^2 - 2$ be divisible by 3? In fact, no. Indeed, every integer x can be written as either $x = 3k$, or $x = 3k + 1$, or $x = 3k + 2$, for some integer k . In the first case, $x^2 - 2 = 9k^2 - 2$ is not divisible by 3. Similarly, in the second case $x^2 - 2 = (3k + 1)^2 - 2 = 9k^2 + 6k + 1 - 2 = 3(3k^2 + 2k) - 1$, while in the third case $x^2 - 2 = (3k + 2)^2 - 2 = 9k^2 + 12k + 4 - 2 = 3(3k^2 + 4k) + 2$. In any case, $x^2 - 2$ is not divisible by 3, hence $n = 2$ is not a quadratic residue modulo $p = 3$.

In general, to check if $x^2 - n$ is divisible by p for some x , we should consider p cases: $x = pk, x = pk + 1, \dots, x = pk + (p - 1)$. For case $x = pk + r$, $x^2 - n = (pk + r)^2 - n = p(pk^2 + 2kr) + r^2 - n$, hence $x^2 - n$ is divisible by p if and only if $r^2 - n$ is. For simplicity, assume that $0 < n < p$. Then n is a quadratic residue modulo p if and only if r^2 gives remainder n after division by p for some $r = 1, 2, \dots, p - 1$. For example, for $p = 5$, numbers $1^2, 2^2, 3^2$ and 4^2 give remainders 1, 4, 4, and 1, respectively, after division by 5, hence 1 and 4 are quadratic residues modulo $p = 5$, while 2 and 3 are not. Similarly, for $p = 7$, $1^2, 2^2, 3^2, 4^2, 5^2$ and 6^2 give remainders 1, 4, 2, 2, 4 and 1, respectively, hence 1, 2 and 4 are quadratic residues, while 3, 5 and 6 are quadratic non-residues.

The Number of Quadratic Residues

In all these examples, exactly half of the positive integers less than p are quadratic residues, and half are non-residues. This is not a coincidence: in fact, this half-half distribution is true for every odd prime p . This is because for every odd p there exists an a such that the integers $a, a^2, a^3, \dots, a^{p-1}$ all give different remainders modulo p . Then the remainders corresponding to a^2, a^4, \dots, a^{p-1} are quadratic residues, while the ones corresponding to a, a^3, \dots, a^{p-2} are quadratic non-residues. Figure 1.2 illustrates this fact for $p = 13$ and $a = 2$.

Fig. 1.2 Quadratic residues and non-residues modulo $p = 13$



Quadratic residues have been intensively studied since the 17th and 18th centuries, but some basic questions about their distribution proved to be very difficult. For example, for some $p > 200$, can it be that all numbers from 1 to 100 are quadratic non-residues? Ok, they cannot, because perfect squares 1, 4, 9, 16, 25, 36, 49, 64, 100 are obviously quadratic residues, but can it be that all other 90 numbers are quadratic non-residues? More generally, for any large number x , can we find $p > x$ such that 90% of all numbers less than x are quadratic non-residues modulo p ? If this is impossible, what is the highest percentage of non-residues up to x we can achieve?

The 17.15% Law

Theorem 1.2 can be used to answer this difficult question in a few lines. For an odd prime p , define

$$f_p(n) = \begin{cases} 0, & \text{if } n \text{ is divisible by } p \\ 1, & \text{if } n \text{ is a quadratic residue modulo } p, \text{ but not divisible by } p, \\ -1, & \text{if } n \text{ is not a quadratic residue modulo } p. \end{cases}$$

One can check that $f_p(n)$ is a completely multiplicative function. For example, if $f_p(n) = 0$, then n is divisible by p , hence nm is divisible by p for every m , and $f_p(nm) = 0 = f_p(n) \cdot f_p(m)$. As a different example, consider the case $f_p(n) = f_p(m) = 1$, that is, both n and m are quadratic residues. Then $x^2 = n$ is divisible by p for some x , hence $x^2 = ap + n$ for some integer a . Similarly, $y^2 = bp + m$ for some integers y and b . Then $(xy)^2 = (ap + n)(bp + m) = p(abp + am + bn) + nm$, hence $(xy)^2 - nm$ is divisible by p , and, by definition, nm is a quadratic residue

modulo p , or $f_p(nm) = 1 = f_p(n) \cdot f_p(m)$. The proofs of $f_p(nm) = f_p(n) \cdot f_p(m)$ in the other cases are just a bit more complicated.

For $0 < n < p$, the expression $\frac{1+f_p(n)}{2}$ is equal to 1 if n is a quadratic residue modulo p and 0 otherwise, so the number of quadratic residues modulo p up to any $x < p$ is exactly equal to the sum $\frac{1}{2} \sum_{n \leq x} (1 + f_p(n))$.

Now, applying Theorem 1.2 to $f_p(n)$, we get

$$\lim_{x \rightarrow \infty} \frac{1}{x} \sum_{n \leq x} \frac{1 + f_p(n)}{2} \geq \frac{1 + \delta_1}{2} \approx 0.171500.$$

In other words, we have proved the following statement: *If x is sufficiently large then, for all primes $p > x$, more than 17.15% of the integers up to x are quadratic residues modulo p .* This statement also holds for $p \leq x$, and the estimate is the best possible.

Similarly, for any power $m > 2$, we can say that n is an m -th power residue modulo p if $x^m - n$ is divisible by p for some integer x . In this case, Granville and Soundararajan proved a similar result: for a given integer $m > 2$, there exists a constant $\pi_m > 0$ such that, if x is sufficiently large, then, for all primes p , more than $\pi_m\%$ of the integers up to x are m -th power residues modulo p .

Extension to Complex-Valued Functions

Granville and Soundararajan also extended Theorem 1.2 to complex-valued functions, which led to much more interesting results and applications. The set \mathbb{C} of complex numbers consists of numbers of the form $z = x + y\sqrt{-1}$, where x, y are real numbers. Any complex number can be represented as a point (x, y) in the coordinate plane. The absolute value of a complex number z is $|z| = \sqrt{x^2 + y^2}$. Let S be any set of complex numbers such that $|z| \leq 1$ for any $z \in S$. Geometrically, S is a subset of the unit disk $U = \{(x, y) \mid x^2 + y^2 \leq 1\}$. Let $F(S)$ be the set of all completely multiplicative functions $f : \mathbb{N} \rightarrow \mathbb{C}$ such that $f(p) \in S$ for any prime p . Then we can define $\Gamma_N(S)$ to be the set of complex numbers z representable in the form $z = \frac{1}{N} \sum_{n \leq N} f(n)$ for some $f \in F(S)$, and $\Gamma(S) = \lim_{N \rightarrow \infty} \Gamma_N(S)$.

Granville and Soundararajan called $\Gamma(S)$ the *spectrum* of the set S . In this notation, Theorem 1.2 corresponds to the special case $S = [-1, 1]$, and can be formulated as $\Gamma([-1, 1]) = [\delta_1, 1]$. However, their theory goes far beyond this special case—they proved many interesting properties of $\Gamma(S)$ for a general set S . For example, they proved that $\Gamma(S)$, when drawn in the coordinate plane, always looks like a connected picture, not a collection of disconnected pieces. However, an exact formula for $\Gamma(S)$ has been obtained only in the case $S = [-1, 1]$, and its extension to general S remains an intriguing open question.

Reference

A. Granville and K. Soundararajan, The spectrum of multiplicative functions, *Annals of Mathematics* **153-2**, (2001), 407–470.

1.3 Counting Integer Solutions of Some Inequalities

Counting Integer Points in Disks and Balls

How many pairs of integers (x, y) are solutions to the inequality $x^2 + y^2 \leq 100$? We can answer this question approximately by first describing its *real* solutions. In the coordinate plane, real solutions to this inequality form a disk with center $(0, 0)$ and radius $r = 10$. The question is, how many points with integer coefficients does this disk contain? Let us put into correspondence to every such point (x, y) a unit square, with vertices $(x, y), (x, y + 1), (x + 1, y + 1), (x + 1, y)$. If (x, y) is not close to the boundary of the circle, this square lies fully within it. Hence, the number of integer solutions to $x^2 + y^2 \leq 100$ is approximately the number of unit squares within the circle, which, in turn, is approximately equal to its area, see Fig. 1.3. The latter can be easily computed, and is equal to $\pi r^2 = 100\pi \approx 314$. In fact, the exact number of integer solutions to $x^2 + y^2 \leq 100$ is 309.

Similarly, the number of integer solutions to the inequality $x^2 + y^2 + z^2 \leq 100$ can be approximated by the volume of the corresponding ball, which is equal to $\frac{4}{3}\pi r^3 = \frac{4}{3}\pi 10^3 \approx 4189$. For the more general equation, $x_1^2 + x_2^2 + \dots + x_n^2 \leq m$, we need to calculate the volume of the n -dimensional ball of radius $r = \sqrt{m}$. What is the formula for it? Well, such a ball is just a ball with radius 1 enlarged by a factor of r . If we take any figure (not necessary a ball) in n -dimensional space, and enlarge it by a factor of r , its volume increases by a factor of r^n . Hence, the volume of the n -dimensional ball of radius r is Vr^n , where V is the volume of the ball $x_1^2 + x_2^2 + \dots + x_n^2 \leq 1$. Because $r = \sqrt{m}$, the volume is $V(\sqrt{m})^n = Vm^{n/2}$.

Monomials, Polynomials, and Some Volume Estimates

In general, a *monomial* in n variables x_1, x_2, \dots, x_n is any expression of the form $G(x_1, x_2, \dots, x_n) = x_1^{a_1} x_2^{a_2} \dots x_n^{a_n}$ for some non-negative integers a_1, a_2, \dots, a_n . The *degree* d of the monomial is just $a_1 + a_2 + \dots + a_n$. For example, $G(x, y, z) = xy^3z^2$ is a monomial of degree $d = 1 + 3 + 2 = 6$. If G is any monomial of degree d , then, for any $k \in \mathbb{R}$,

$$\begin{aligned} G(kx_1, kx_2, \dots, kx_n) &= (kx_1)^{a_1} (kx_2)^{a_2} \dots (kx_n)^{a_n} \\ &= k^d \cdot (x_1^{a_1} x_2^{a_2} \dots x_n^{a_n}) \\ &= k^d G(x_1, x_2, \dots, x_n). \end{aligned}$$

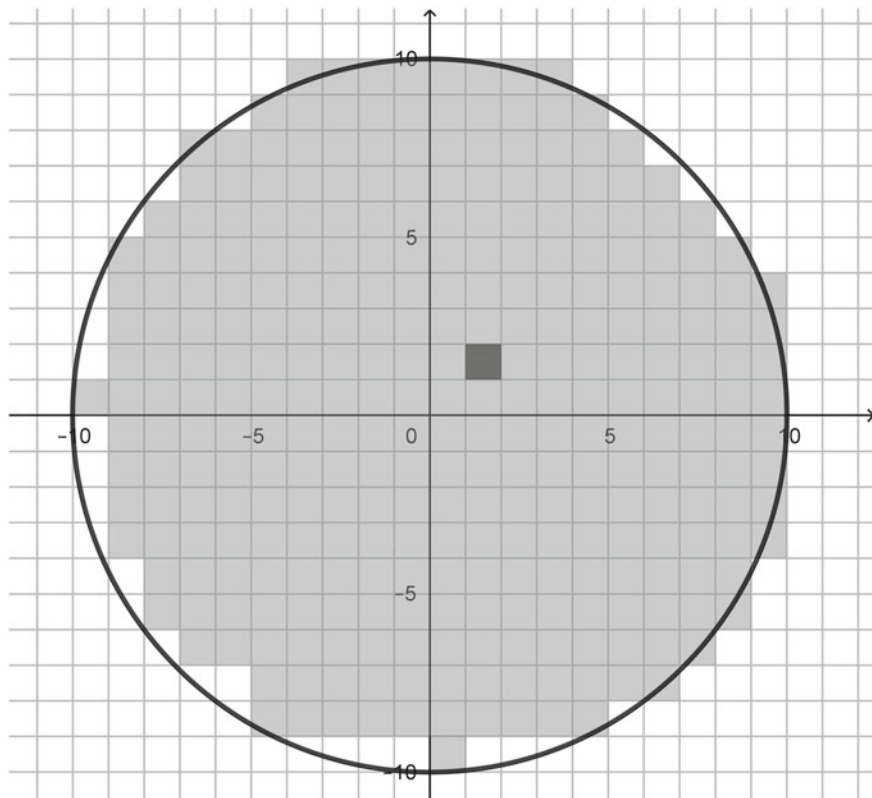


Fig. 1.3 Counting integer points in a disk

For example, if $G(x, y, z) = xy^3z^2$, then we have $G(kx, ky, kz) = (kx)(ky)^3(kz)^2 = k^6G(x, y, z)$.

A *polynomial* in n variables x_1, x_2, \dots, x_n is any sum of monomials, for example, $xy + xy^3z^2 + z^{15}$. In this example, we have a sum of three monomials of degree 2, 6, and 15, respectively. Here, we study only polynomials F which are the sums of monomials of the same degree. In particular, $F(x, y, z) = x^6 + yz^5 + xy^3z^2$ is an example of such a polynomial in $n = 3$ variables of degree $d = 6$. In this example, for any $k \in \mathbb{R}$, we have

$$\begin{aligned} F(kx, ky, kz) &= (kx)^6 + (ky)(kz)^5 + (kx)(ky)^3(kz)^2 \\ &= k^6(x^6 + yz^5 + xy^3z^2) \\ &= k^6F(x, y, z). \end{aligned}$$

In general, we have

$$F(kx_1, \dots, kx_n) = k^d F(x_1, \dots, x_n). \quad (1.5)$$

Now, let F be any polynomial in n variables with integer coefficients such that every monomial has degree d , and let the volume of the set $S_1 \subset \mathbb{R}^n$ defined by the inequality $|F(x_1, \dots, x_n)| \leq 1$ be equal to $V(F)$. Then what is the volume of the set $S_m \subset \mathbb{R}^n$ defined by $|F(x_1, \dots, x_n)| \leq m$? It follows from (1.5) that S_1 enlarged by a factor of k is defined by the equation $|F(x_1, \dots, x_n)| \leq k^d$, hence S_m is just S_1 enlarged by a factor of $k = m^{1/d}$. Thus, the volume of S_m is $V(F)k^n = V(F)m^{n/d}$.

Inequalities of Finite Type

Let $N_F(m)$ be the number $N_F(m)$ of integer solutions to $|F(x_1, \dots, x_n)| \leq m$. Motivated by the examples above, we might hope that $N_F(m)$ is approximately equal to the volume of S_m , that is,

$$N_F(m) \approx V(F)m^{n/d}. \quad (1.6)$$

Unfortunately, this is not always the case. For example, real solutions to $|x - y| \leq 0$ form a line $y = x$, and the 2-dimensional area of a line is 0. However, the number of integer solutions is obviously infinite. We say that an inequality of the form $|F(x, y)| \leq m$ is of *finite type* if the area of its set of real solutions is finite, and if its intersection with any line with rational coefficients has finite length. Similarly, if S is a set of real solutions to $|F(x, y, z)| \leq m$, then F is of finite type if the 3-dimensional volume of S is finite, the intersection of S with any plane with rational coefficients has finite area, and its intersection with any line with rational coefficients has finite length. The same definition extends to any dimension.

Decomposable Forms

Now, if the inequality $|F(x_1, \dots, x_n)| \leq m$ is of finite type, does it mean that it has a finite number of solutions, and can this number be bounded in terms of the n -dimensional volume of the set of its real solutions? In general, no: take $F(x, y) = 0$ if $y = x^2$ and $F(x, y) > m$ otherwise. Then the real solutions form a parabola $y = x^2$, it has area 0, and it intersects any line in at most two points, hence it is of finite type, but the number of integer solutions is infinite. However, Jeffrey Lin Thunder [376] proved that the answer to the above question is “yes” for functions F called *decomposable forms*. These are polynomials of degree d in n variables which are expressible as

$$F(x_1, \dots, x_n) = (a_{11}x_1 + \dots + a_{1n}x_n)(a_{21}x_1 + \dots + a_{2n}x_n) \dots (a_{d1}x_1 + \dots + a_{dn}x_n),$$

where the coefficients a_{ij} are non-zero complex numbers, that is, numbers of the form $x + y\sqrt{-1}$, with x, y being real numbers. For example, $F = x^2 + y^2$ belongs to this class, because $x^2 + y^2 = (x + y\sqrt{-1})(x - y\sqrt{-1})$.

Theorem 1.3 *Let F be a decomposable form of degree d in n variables with integer coefficients. Then the number $N_F(m)$ of integer solutions to the inequality $|F(x_1, \dots, x_n)| \leq m$ is finite for all m if and only if F is of finite type. Moreover, if F is of finite type, then $N_F(m) \leq c(n, d)m^{n/d}$, where $c(n, d)$ is an effectively computable constant depending only on n and d .*

Mahler [258] obtained similar results for $d = 2$ in 1933, and then essentially no progress was made in the general case $d > 2$ for almost 70 years, until the work of Thunder. Note that the bound in Theorem 1.3 does not depend on the coefficients of F . That is, if we fix n, d, m and compute that $c(n, d)m^{n/d}$ is, say, one million, then we can be sure that for any (integer) coefficients of a decomposable form F of degree d in n variables, the inequality $|F(x_1, \dots, x_n)| \leq m$ either has an infinite number of solutions, or at most a million. This resembles the fact that a quadratic equation $ax^2 + bx + c = 0$ can have either an infinite number of real solutions (if $a = b = c = 0$), or at most 2, but never exactly 3.

Thunder also proved that, under the conditions of Theorem 1.3, the approximation (1.6) works well for large m . Intuitively, the reason why m should be large is to remove some “boundary effects”. For example, the inequality $x^2 + y^2 \leq m$ with $m = 0.99$ has just 1 integer solution, $x = y = 0$, while the corresponding volume is $0.99\pi > 3$. With $m = 1$, the volume is still just above 3, but the number of solutions jumps to 5. For large m , such effects are negligible, and (1.6) works. Thunder also derived the exact form of the error term in this approximation.

A Concrete Example

As an application, let us approximately count the number of integer solutions to the inequality $x^4 + 4y^4 \leq 10^{10}$. First, let us factor this polynomial to check that it is a decomposable form.

$$x^4 + 4y^4 = (x^2)^2 - (2y^2i)^2 = (x^2 - 2y^2i)(x^2 + 2y^2i),$$

where $i = \sqrt{-1}$. Note that $(1 + i)^2 = 1^2 + 2i + i^2 = 2i$, hence $x^2 - 2iy^2 = (x - (1 + i)y)(x + (1 + i)y)$. Similarly, $(i - 1)^2 = -2i$, and $x^2 + 2y^2i = x^2 - ((i - 1)y)^2 = (x - (i - 1)y)(x + (i - 1)y)$. Hence,

$$x^4 + 4y^4 = (x - (1 + i)y)(x + (1 + i)y)(x - (i - 1)y)(x + (i - 1)y),$$

as required. Next, we need to calculate the area V of the shape $x^4 + 4y^4 \leq 1$. By symmetry, this is twice the area below the curve $y = \sqrt[4]{\frac{1-x^4}{4}}$ for $-1 \leq x \leq 1$, which can be found by integration:

$$V = 2 \int_{-1}^1 \sqrt[4]{\frac{1-x^4}{4}} \approx 1.311.$$

Finally, we apply (1.6) to conclude that the number of integer solutions in question is approximately

$$N \approx Vm^{n/d} \approx 1.311(10^{10})^{2/4} = 131100.$$

The method itself is based on the volume intuition and was known long before Theorem 1.3 was proved, always giving an accurate result in practice. However, there was no formal *proof* that this method *should* work. The work of Thunder finally filled this gap, and now the method above can be applied with full confidence.

Reference

J.L. Thunder, Decomposable form inequalities, *Annals of Mathematics* **153**-3, (2001), 767–804.

1.4 On the Arithmetic Difference of Regular Cantor Sets

Sets of Small Length but Large Cardinality

Does the interval $[0, 1]$ contain more real numbers than $[0, 1/2]$? If you are seeing this question for the first time, you might answer “Yes”. Mathematicians, however, say that two sets A and B have equal cardinality (that is, the same number of elements) if there exists a one-to-one correspondence between their elements. Now, we can take any number $x \in [0, 1]$, and put it in correspondence with the number $x/2 \in [0, 1/2]$. Hence, the cardinalities of these sets are actually equal, although the lengths are different.

By a similar argument, an interval of any length $\varepsilon > 0$ has the same cardinality as $[0, 1]$. But what about even smaller lengths? A set S of real numbers has length (or measure) 0 if, for any $\varepsilon > 0$, it can be covered by a set of intervals of total length ε . For example, the set of rational numbers in $[0, 1]$ has measure 0. Indeed, for any $\varepsilon > 0$, every number m/n can be covered by an interval

$$(m/n - \varepsilon/2n2^n, m/n + \varepsilon/2n2^n)$$

of length $\varepsilon/n2^n$. In this case, the n rational numbers $1/n, 2/n, \dots, n/n$ with denominator n are covered by n such intervals with total length $n \cdot (\varepsilon/n2^n) = \varepsilon/2^n$. So, rational numbers with denominators $n = 2, 3, 4, \dots$ are covered by intervals of total length $\varepsilon/2, \varepsilon/4, \varepsilon/8, \dots$ and the total length of all intervals is bounded by $\varepsilon/2 + \varepsilon/4 + \varepsilon/8 + \dots = \varepsilon$.

It is known that one cannot create a one-to-one correspondence between the set of rational numbers and the set of real numbers. One may ask, however, if there exists a set with measure 0 which still has the same cardinality as $[0, 1]$. Again, if you are new to the subject, you might guess that there is no such set, however there is, and here is an example.

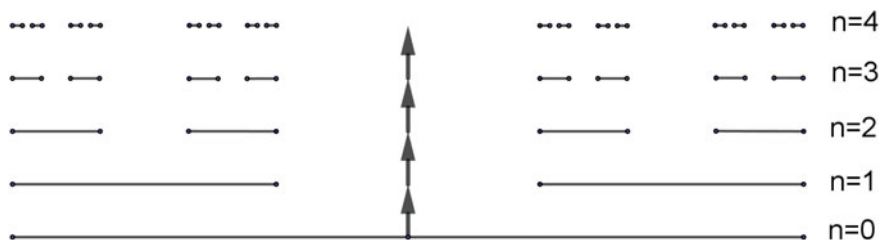


Fig. 1.4 The first four steps in the construction of the Cantor set

Cantor Sets

Take the interval $[0, 1]$, and delete the middle third $(1/3, 2/3)$, resulting in the set $[0, 1/3] \cup [2/3, 1]$. Then delete the middle third from each of these two intervals, resulting in $[0, 1/9] \cup [2/9, 1/3] \cup [2/3, 7/9] \cup [8/9, 1]$, and continue this process indefinitely, see Fig. 1.4. Let C be the set of points which is never deleted. After step 1, we have deleted an interval of length $1/3$, so the total length of the remaining part is $2/3$. At step 2, we have deleted $1/3$ of this, and the total length of the remaining part is $2/3 \cdot 2/3 = 4/9$. Similarly, the length of the part remaining after step n is $(2/3)^n$, hence the measure of C is $\lim_{n \rightarrow \infty} (2/3)^n = 0$. However, C is non-empty (in particular, one can easily check that $0 \in C$, and $1 \in C$), and in fact there is a one-to-one correspondence between C and the interval $[0, 1]$.

Indeed, take any number $x \in [0, 1]$, and assign to it the letter L or G according to whether it belongs to the subinterval $[0, 1/2)$ or $[1/2, 1]$, respectively. For example, $x = 1/3$ is assigned the letter L . Then divide the corresponding subinterval into two halves again, and assign a second letter, for example, numbers from $[0, 1/2)$ are assigned L or G if they belong to the subintervals $[0, 1/4)$ or $[1/4, 1/2)$, respectively, in particular $x = 1/3$ is assigned G this time. After repeating this infinitely, we can associate to each $x \in [0, 1]$ a unique infinite sequence of L 's and G 's. Now, in the process of constructing the set C as above, we can similarly assign to every $y \in C$ a first letter L if $y \in [0, 1/3]$ and G if $y \in [2/3, 1]$. Then, if, say, $y \in [0, 1/3]$, assign a second letter L if $y \in [0, 1/9]$ and G if $y \in [2/9, 1/3]$, and so on. In this way we associate infinite sequence of L 's and G 's to every $y \in C$. Finally, we put $x \in [0, 1]$ into correspondence with $y \in C$ if and only if x and y are associated with the same sequence of letters.

Hence, we have constructed a set C with measure (length) 0, but with the same number of elements as the full interval $[0, 1]$. Obviously, the construction above is not unique. For each $\beta \in (0, 1/2)$, we can delete the middle part $(\beta, 1 - \beta)$ of $[0, 1]$, and then repeat the process as above. Also, we can start with any interval $[a, b]$ instead of $[0, 1]$. The resulting sets all have as many elements as $[0, 1]$ but measure 0, and are examples of *Cantor sets*.