Review of[1]

Theorems of the 21st Century: Volume I
by Bogdan Grechuk
Publisher: Springer-Verlag
$30.00 hardcover, 446 pages, Year: 2019

Reviewer: William Gasarch gasarch@cs.umd.edu

1 Introduction

In the movie *Oh God! Book II* God (played by George Burns) says:

Mathematics, that was a mistake. I should have made the whole thing a little easier.

While I am not one to argue with God, George Burns, or George Burns playing God, I do not think Mathematics was a mistake. But I do wish it was easier. Or perhaps its easy enough to make so much progress in that it becomes hard.

In the 21st century there are many theorems whose statements *cannot* be explained to a good undergraduate math major. Or even a professor of mathematics who is not in that area. But all is not bleak. There are also theorems whose statements *can* be explained to a good undergraduate math major, though you might need to supply some context.

The book under review is about those theorems. Every chapter gives definitions and context for a theorem proven in the 21st century, in 4–6 pages. No proofs are given. The chapters are organized by year. There are 106 chapters total.

In this review I will summarize five of the chapters. I intentionally *do not* summarize any of the chapters that (1) involve theoretical computer science, or (2) are results you've probably already heard of (e.g., there are arbitrarily long arithmetic sequences of primes) since the biggest benefit of this book is *broaden your horizons.* After the summaries I will have a section that lists all of the chapters in this book that involve TCS. I will then render an opinion. Spoiler Alert: this book is awesome.

2 There is Also a Website!

The author has put up a website which has the theorems in the book, more theorems which will appear in a sequel, along with pointers to the papers where the results appeared and were proven. The website is here:

https://theorems.home.blog/theorems-list/

3 Counting Integer Solutions of Some Inequalities (2001)

Consider the region

$$D = \{(x_1, \ldots, x_n) : x_1^2 + \cdots + x_n^2 \leq m\}.$$

The number of integer point in D is well approximated by the volume of D. We generalize this notion.

Def 3.1 Let $f(x_1, x_2)$ be a homogenous polynomial. An inequality of the form $|f(x_1, x_2)| \leq m$ is of *finite type* if (1) the area of its set of real solutions is finite, and (2) the intersection of it with any line with rational coefficients has finite length. Note that the disc is an example. One can easily generalize the definition to higher dimensions. For example, in 3-dimensions it would be (1) the volume of its set of real solutions is finite, (2) the intersection of it with any plane with rational coefficients has finite area, and (3) the intersection of it with any line with rational coefficients has finite length.

Def 3.2 Let $f(x_1, \ldots, x_n)$ be homog of degree d. Then f is *decomposable* if there exists complex linear polynomials $L_1(x)$, $L_2(x)$, ..., $L_d(x)$ such that

$$f(x_1, \ldots, x_n) = L_1(x) \cdots L_d(x).$$

ALSO- all of the coefficients of all of the L_i's are non-zero. So you cannot have, for example $x_1 + 3x_4$ as one of the linear factors.

The big theorem says, in essence, that under certain conditions the volume of an n-dim solid is a good approximation for the number of lattice points in it.

Theorem 3.3 *(Jefferey Lin Thunder) Let $F(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ be a homog poly of degree d. Let F be decomposable. Let $N_F(m)$ be the number of integer solutions to $|F(x_1, \ldots, x_n)| \leq m$.*

1. *$(\forall m)[N_F(m) < \infty]$ iff F is of finite type.*
2. *If F is of finite type then $|N_F(m)| \leq c(n, d)m^{n/d}$.*

4 The Existence of a Field with u-invariant 9

Let F be a field. Solving linear equations over F is easy. We look at quadratic equations of the form

$$\sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij} x_i x_j = 0$$

and seek non-zero solutions. If $n = 1$ then the equation is $a_{11}x^2 = 0$ so their are no non-trivial solutions. If the number of variables goes up, do we get a solution?

Def 4.1 Let F be a field. The *u-invariant of F* is the number u such that

1. There is an quadratic form with n variables that has NO non-trivial solution.
2. Every quadratic form with $n + 1$ variables has a non-trivial solution.

Examples:

1. $F = \mathbb{R}$. For all n, there is a quadratic form on n variables with NO nontrivial solution: $x_1^2 + \cdots + x_n^2 = 0$. So $u(\mathbb{R}) = \infty$.

2. $F = \mathbb{C}$. $x^2 = 0$ only has the trivial solution, but then $ax^2 + bxy + c^2 = 0$ always has a nontrivial solution. So $u(\mathbb{C}) = 1$.

3. Let $F = \mathbb{Z}_p$ where p is prime, $p \geq 3$.

   - Let a be a NON-square in $\mathbb{Z}_p$. Then $x^2 - ay^2 = 0$ has no solution since if it did then $a = (\frac{x}{y})^2$.
   - One can show that every quadratic form in 3 variables has a non-trivial solution.
   - Hence, for all primes $p \geq 3$, $u(\mathbb{Z}_p)) = 2$.

4. It is known that $u(\mathbb{Q}(i)) = 4$.

5. It is known that $u(\mathbb{C}(x_1, \ldots, x_n)) = 2^n$.

Note that all of the $u(F)$ are powers of 2. In 1953 Kaplansky conjectured that, for all fields F, $u(F)$ is a power of 2. In 1989 Merkurev disproved this by showing there was a field F such that $u(F) = 6$. He also showed that for every even number $2k$ there is a field F with $u(F) = 2k$. It was also shown that $u(F)$ cannot be 3,5, or 7. This naturally leads to the conjecture that the numbers that can be $u(F)$ are exactly the evens.

Alas, in 2003 Izhboldin showed the following:

Theorem 4.2 *There is a field F with $u(F) = 9$.*

5 Counting Rational Functions with Given Critical Points (2002)

We consider $\mathbb{R}(x)$, the set of rational functions over $\mathbb{R}$. Such a function is *of degree d* if both the numerator and denominator are of degree d. We denote the set of such functions $\mathbb{R}_d(x)$. A *critical point* of $f \in \mathbb{R}(x)$ is a place where its derivative is 0. Since $f \in \mathbb{R}_d(x)$ has both numerator and denominator of degree d, there are $\leq 2d - 2$ critical points (counting multiplicities).

Given d and the set of critical points, can you recover the function? The answer is no for two reasons:

1. The question as phrased isn't quite what we want. If $f, g \in \mathbb{R}_d(x)$ but there is a linear rational function L such that $f(x) = L(g(x))$ then we want to consider f and g the same. So we restate the question: does the set of critical points determine the equivalence class of functions?

2. There are sets of critical points so that there is more than one equivalence class with that set. But there are only a finite number of equivalence class.

   Theorem 5.1 *(Andrei Gabrielov) For all d, for all sets of $2d-2$ critical points, there exists exactly*

   $$\frac{1}{d}\frac{(2d-2)!}{(d-1)!(d-1)!}$$

   equivalence classes of rationals of degree d with those critical points.

6 A Real Number that is Far from All Cubic Algebraic Integers (2003)

If $\zeta \notin \mathbb{Q}$ we seek $\frac{a}{b} \in \mathbb{Q}$ such that $|\zeta - \frac{a}{b}|$ is small. How to measure smallness? Clearly, the larger b is the closer we can make ζ and $\frac{a}{b}$. Hence we want to measure the distance as a function of b. The following are known.

1. For every $\zeta \notin \mathbb{Q}$ there exists infinitely many $\frac{a}{b} \in \mathbb{Q}$ such that $|\zeta - \frac{a}{b}| \leq \frac{1}{\sqrt{5}b^2}$. We would like to improve the 2 to a larger number. But we can't due to the next item.

2. There exists ζ such that, for every $\frac{a}{b} \in \mathbb{Q}$, $|\zeta - \frac{a}{b}| \geq \frac{1}{\sqrt{5}b^2}$. One such ζ is $\frac{1+\sqrt{5}}{2}$, the Golden Ratio..

In other words, you can always get quadratic error, but there are times you can't do any better than that.

The above is about approximating irrationals with rationals. What if we approximate irrationals with numbers that involve square roots of integers? Cube Roots? Let

$$\mathbb{Q}_d = \{x \in \mathbb{R} : \ x \text{ is the root of a degree } d \text{ polynomial with coefficients in } \mathbb{Z}\}.$$

We want to approximate $\zeta \in \mathbb{Q}$ by some $\alpha \in \mathbb{Q}_2$. So we want

$$|\zeta - \alpha| \leq ???$$

We need some measure of how complicated the number α is. For $\frac{a}{b}$ we used b. Note that $\frac{a}{b}$ satisfies $bx - a = 0$. So we could rephrase this as using the highest coefficient in a poly of least degree that b satisfies. This is how we generalize. Let $\alpha \in \mathbb{Q}_2$. Look at all of the quadratic equations over $\mathbb{Z}$ that α solves. Take the one with the smallest largest coefficient. That coefficient is $H(\alpha)$.

1. For every $\zeta \notin \mathbb{Q}$ there exists infinitely many $\alpha \in \mathbb{Q}_2$ such that $|\zeta - \alpha| \leq \frac{C}{H(\alpha)^2}$. This is not impressive. We wanted to improve 2 to a large number. But we can't due to the next item.

2. There exists a constant D and a $\zeta \notin \mathbb{Q}$ such that, for every $\alpha \in \mathbb{Q}_2$, $|\zeta - \alpha| \geq \frac{D}{H(\alpha)^2}$. Darn!

What if we approximate irrationals with numbers in $\mathbb{Q}_3$?

1. For every $\zeta \notin \mathbb{Q}$ there exists infinitely many $\alpha \in \mathbb{Q}_3$ such that $|\zeta - \alpha| \leq \frac{C}{H(\alpha)^{\phi^2}}$ where $\phi = \frac{1+\sqrt{5}}{2}$. Note that $\phi^2 = \frac{3+\sqrt{5}}{2} \sim 2.618$. Yes! We broke he barrier of 2. Well not US, but actually Davenport and Schmidt in 1969. Can we do better? Can they do better? Can anyone do better? In 2003 the answer came: No.

Theorem 6.1 *(Damien Roy) There exists a constant D and a $\zeta \notin \mathbb{Q}$ (in fact, ζ is transcendental) such that, for every $\alpha \in \mathbb{Q}_3$, $|\zeta - \alpha| \geq \frac{D}{H(\alpha)^{\phi^2}}$.*

7 On Divisibility Properties of Dyson's Rank Partition Function (2010)

A *partition* of a natural number is a way to write it as a sum of naturals. For example, $5 = 1+2+2$ is a partition of 13. Let $p(n)$ be the number of partitions of n. We do NOT care about the order. For example, the following is the set of all partitions of 5 $(1,1,1,1,1)$, $(1,1,1,2)$, $(1,1,3)$, $(1,2,2)$, $(1,4)$, $(2,3)$. Note that $p(5) = 6$. The following is known.

Theorem 7.1 *For all $n \in \mathbb{N}$:*

1. *(Ramanjuan)* $p(5n+4) \equiv 0 \pmod 5$.
2. *(Ramanjuan)* $p(7n+5) \equiv 0 \pmod 7$.
3. *(Ramanjuan)* $p(11n+6) \equiv 0 \pmod{11}$.
4. *(Atkin and O'Brien)* $p(17303n+237) \equiv 0 \pmod{13}$.
5. *(Ono) For all primes $q \geq 5$ there exists $A, B \in \mathbb{N}$ such that $p(An+B) \equiv 0 \pmod q$.*

By the above $p(9) \equiv 0 \pmod 5$ and in fact $p(9) = 30$. So one can take all of the partitions of 9 and divide them arbitrarily into 5 groups of size 6. Dyson outlined a way to do this non-arbitrarily.

For each partition take the difference between the largest summand and the number of summands. We call this the *rank of the partition*. We list the ranks of some of the partitions of 9:

$(2,2,1,1,1,1)$ has rank $2-7 = -5$
$(3,3,3)$ has rank $3-3 = 0$
$(4,2,2,1)$ has rank $4-4 = 0$
$(4,3,1,1)$ has rank $4-4 = 0$
$(5,1,1,1,1)$ has rank $5-5 = 0$
$(7,2)$ has rank $7-2 = 5$

So these 6 partitions all have rank $\equiv 0 \pmod 5$. It turns out that no other partitions map to a number $\equiv 0 \pmod 5$. In fact, each of $i = 0,1,2,3,4$ has exactly 6 partitions of rank $\equiv i \pmod 5$. Is this always the case? Dyson conjectured yes. We state this formally.

Let $N(r,q;m)$ be the number of partitions of m which have a rank that is $\equiv r \mod q$. Dyson conjectured that

$$N(0,5;5n+4) = N(1,5;5n+4) = N(2,5;5n+4) = N(3,5;5n+4) = N(4,5;5n+4) = \frac{p(5n+4)}{5}$$

This was proven by Atkin and Swinnerton-Dyer in 1954. They also proved a similar theorem for $p(7n+5)$. Is there a similar theorem for $p(An+B)$? Yes by this result from 2010.

Theorem 7.2 *(Bringmann and Ono) Let t be a positive odd integer, and let q be a prime such that $6t$ is not divisible by q. If j is a positive integer, then there are infinitely many non-nested arithmetic progressions $An+B$ such that for every $0 \leq r < t$ we have*

$$(\forall n)[N(r,t;An+B) \equiv 0 \pmod{q^j}]$$

8 Theorems from Theoretical Computer Science

The following chapters in the book are about theorems that are from theoretical computer science. I may have missed a few since the line between *theoretical computer science* and *combinatorics* (and sometimes other fields of math) is not that sharp.

1. Explicit expander constructions using the zig-zag product (2002).
2. A finitely presented group with an NP-complete word problem (2002).
3. Finitely generated groups with a word problem in NP (2002).
4. A polynomial time algorithm for primality testing (2004).
5. The NP-hardness of the 1.36...-approximation to the minimum vertex cover (2005).
6. The Cayley Graphs of $SL_2(F_p)$ form a family of expanders (2008).
7. A linear time algorithm for the edge-deletion problem (2008).
8. Majority votes are the most stable (2010).

9 Opinion

Every chapter gives just enough definitions and contexts to *understand* the theorem presented. Hence from this book you can learn a lot about many different areas of mathematics as well as the new theorems in those areas.

This is a great book! You can learn a lot *about* mathematics. You are best off reading it slowly and carefully and taking notes on what you read, putting it in your own words, and doing your own examples (the five summaries I gave were from my efforts). The effort is worth it.

If the reader is wondering *how come Theorem X is not in the book?* then note:

- Check the website given above. It might be in the sequel.
- If someone goes to the effort of looking at the Math literature and picking out 106 papers then I would not want to second guess them. Its a hard task and I appreciate, not just the effort, but the result.