1

Yes You *Can* Prove a Negative!

1.1 Introduction to Impossibility

I have always reacted negatively when I hear the claim that "You can't prove a negative", because in theoretical computer science and mathematics, we do it all the time. Many famous negative results go back thousands of years. The beautiful ancient Greek proof that the square root of two cannot be written as the ratio of two integers (in other words, that $\sqrt{2}$ is *irrational*) is perhaps the best known example. Mathematics is full of such "negative" proofs.[1]

But in the 1900s, much deeper, more sweeping and "more negative" types of negative theorems were developed. These showed very unintuitive, profound, shocking, revolutionary, and even dangerous[2] types of impossibility, with implications far beyond their technical statements.

The first two of these sweeping, profound impossibility theorems were due to Kurt Gödel in 1931. Those two theorems (roughly) showed (a) the

[1] A recent book [63] and [89] explains the impossibility of solving four famous mathematical problems from antiquity. Some were open for several thousand years before being shown to be impossible. The book [65] focuses on a different famous problem from antiquity: whether there are formulas analogous to the quadratic formula (that solves equations with largest exponent equal to two), but for equations with exponents larger than two. After many failures, it was finally proven in the 1800s that there is no such analogous formula for equations with exponents of five (or larger), but there is a formula for equations where the largest exponent is three, and a different formula where the largest exponent is four. Those formulas are much more complex than the quadratic formula, which is taught to most high-school students.

[2] In Stalin's Soviet Union, some of these impossibility results were dangerous for anyone to study and teach. Stalin stated that "if there is a passionate desire to do so, every goal can be reached, every obstacle can be overcome" [53] – everything was achievable in the Utopian world of New Soviet Man. Moreover, "Stalin believed that science should serve the state. Pure research was not merely an indulgence - it was counter-productive. It was tantamount to wrecking [sabotage against the state]," and "theory must be refashioned to be of immediate service to the revolution" [53]. Many scientists whose work didn't fit with Stalin's views were sent to gulags or just disappeared. While this mostly affected biologists and physicists, logicians also knew to be careful – asserting impossibility was "counter-revolutionary", and dangerous.

https://doi.org/10.1017/9781009349451.002 Published online by Cambridge University Press

impossibility of finding an axiomatic theory of arithmetic in which all and only true statements about arithmetic can be derived and (b) the impossibility of finding a consistent theory of arithmetic that can prove its own consistency.[3]

At about the same time, related work by Alfred Tarski showed the impossibility of *defining truth* about arithmetic, in the language of arithmetic itself. Then followed the work of Alan Turing, who showed that many problems are impossible to *solve* by (always correct) algorithms, and hence by computer programs. Turing's theorems can also be used to prove Gödel-like theorems. Several decades later, Gregory Chaitin proved an impossibility theorem that can also be used to prove Gödel-like theorems but is considered to be even more "devastating" and "limiting" for mathematics than are Gödel's and Turing's theorems.

In a different domain, Bell's impossibility theorem and inequalities have had enormous impact in physics, philosophy, and more recently on technological developments such as quantum computing and quantum cryptography. In fact, it is Bell's theorem and inequalities that form the mathematical basis for the experiments done by three physicists who won the 2022 Nobel prize in Physics. Some people consider Bell's work to be the most impactful development in all of science. And yet, and despite many lay expositions, Bell's theorem and inequalities are not well known outside of physics, philosophy, and now computer science.[4] And even inside physics, many physicists [47] have not mastered or studied the technical details of Bell's theorem and inequalities.[5]

In the areas of Economics and Political Science, the impossibility-of-fair-elections theorem, proved by Kenneth Arrow in 1950, initiated a subarea of Economics called *social-welfare theory*. It led to many other impossibility theorems concerning voting, the most compelling (to me) being the Gibbard–Satterthwaite theorem (which we prove before proving Arrow's theorem) concerning the impossibility of devising fair election mechanisms where *deception* is never rewarded. Arrow's impossibility theorem has wide "name recognition" outside of professional circles, since Arrow shared a Nobel prize in Economics, in large part for his seminal contributions to social-welfare theory.

[3] I know this second statement is vague – it will be more fully explained in Chapter 9.

[4] Although, in 1993, David Mermin [71] wrote (somewhat derisively I think): "[Bell's theorem] is widely known not only among physicists, but also to philosophers, journalists, mystics, novelists, and poets."

[5] Scott Aaronson, a computer scientist, has written that he has had physicists ask him to explain Bell's inequalities. [1] p. 109

Consistent with the axiomatic framework of Arrow, Jon Kleinberg more recently proposed three axioms he asserted should be obeyed by good *data clustering* algorithms. Clustering is a somewhat ill-defined task, of huge importance in many data-intense areas, most recently in the growing field of *machine learning* and the emerging field of *data science*. Kleinberg showed that there is no algorithm that can simultaneously obey those three axioms. This impossibility also holds for other, more natural, axioms, but as we will see, those results are less robust.

1.2 What These Theorems and Proofs Have in Common

All of these (and other) deep, profound (even revolutionary) impossibility theorems have three things in common:

(a) They are the product of pure reason.
(b) They were originally (and some still are) considered too hard for nonmathematicians or nonspecialists to fully grasp, that is, to follow actual, rigorous, correct *proofs*.[6]
And most important:
(c) We are no longer bound by Statement (*b*)!

Statement (*b*) is less relevant than it once was, because simpler proofs, generalizations, and/or simpler expositions are now known that *should* allow

[6] For example, a recent book on Bell's theorem [47] states: "I have made no attempt to show the actual theorem Bell had proved. Rather, I have talked about it only in general terms. The reason is that his combination of mathematical quantities is something of a complicated mess, and the proof that they obey his restriction is more complicated still." A similar statement: "Bell's theorem is a mathematical construct which as such is indecipherable to the non-mathematician" appears in [113].
Concerning Gödel's incompleteness [23]: "At the time of its discovery, ... its proof was considered to be extremely difficult and recondite" [23], and in the major popularization of Gödel's proof [77]: "The details of Gödel's proofs in his epoch-making paper are too difficult to follow without considerable mathematical training." A related quote from [39]: "... even some accomplished mathematicians (for example ...) had difficulty grasping the proof."
Similarly, Arrow's original proofs are extremely hard to follow. His initial 18-page paper, [4], presented his general impossibility theorem but only proved the special case of two individuals (voters) rather than an unlimited number. As stated in [95]: "He uses a mathematical wave of the hand on the generalizability of proofs involving societies with two individuals." Arrow's original paper [4] only states: "... the results stated in this paper hold for any number of individuals." But the proof of the general theorem, given in Arrow's book [5] a year later, is very different from his proof of the special case. He provided a different, but still long and difficult, proof, in a second edition [6], 12 years later.

nonmathematicians and nonspecialists to understand and appreciate these profound theorems and proofs.[7]

1.3 This Book Builds on These Improvements

Even though the newer proofs are simpler, existing *expositions* of these proofs are still largely written in terse, mathematical language aimed at "mathematically mature" professionals. And unfortunately,

> ... in the finished product of mathematics it is not uncommon to find that all signs of intuition have been removed. [21]

That situation is the motivation for this book.

This book takes advantage of, and builds on, the newer, simpler proofs and generalizations, with the goal of bringing diverse, rigorous, impossibility proofs to a broad, *nonprofessional, lay* audience. The book requires little background knowledge, and no specialized mathematical training – but it does require work.

To achieve the goal of exposing fully rigorous, yet accessible proofs, I searched the various literatures (and the Internet) for the most accessible proofs and expositions, and then built on those to reduce the jargon and notational burden, and to provide more background, intuition (when possible), examples, and explanations, in slower-paced presentations. Sometimes just making the text less dense, adding headers and summaries, and spacing out equations makes the presentation easier to understand.

For example, the 2005 proof that I follow in discussing Arrow's general impossibility theorem was published in a research journal [41] in typical

[7] For example, the quote in the previous footnote from [113] was noted by David Mermin in [68], followed by the statement: "a view I hope the rest of this article will dispel." I think Mermin largely realized that hope.

With respect to Gödel's theorems, the quote in the previous footnote from [23] continues: "With the passage of time the situation has been reversed. A great many different proofs of Gödel's theorem are now known, and the result is now considered easy to prove and almost obvious." Well, I don't agree that its proof is easy or obvious, and many of the different proofs share the same high-level ideas (see [60] for a list and discussion of several proofs), but there are certainly now vastly easier and more understandable proofs and expositions than Gödel's original one.

And continuing the earlier quote from [39]: "Today, as in the case of other intellectual advances, both the subject and our understanding of it have developed to the point where the proof is not at all considered difficult. ... proofs have become streamlined and generalized."

With regard to Arrow's theorem, there have been huge improvements. There are now *single-page* proofs of Arrow's general theorem. And even Kleinberg's original proof on clustering, which is only a few years old, has since been simplified and extended.

terse-math style, and occupies *less than one page*, including a figure.[8] My slower, more explanatory retelling of that proof expands the exposition to eight pages, with seven figures.

1.4 Why Proofs?

I believe that understanding (or at least following) a rigorous *proof* of a revolutionary theorem is the best way to absorb and appreciate the revolution; to appreciate the power of pure reason and the beauty of mathematics; to understand its impact beyond mathematics (on philosophy, science, the mind, technology, and society); and to have a justified sense of personal accomplishment, especially when you have heard that only a few highly trained people can possibly understand these proofs.

Understanding the proof is also the best way to understand any continuing *controversies* and misuses of a theorem.[9] All of the theorems in this book are to some extent controversial and/or commonly misunderstood – particularly the theorems of Gödel and Bell. There are numerous and egregious examples of these theorems being misunderstood and/or abused, and there are books and articles that discuss these misuses, abuses, and controversies. It seems to me almost impossible (maybe even provably impossible!) to fully understand the controversies, and certainly impossible to come to some conclusion about them yourself, if you don't understand the technical details of the theorems and proofs. For example, the larger meaning of Bell's theorem continues to be debated in physics and philosophy, interconnected with debates about the larger meaning of quantum mechanics itself. But, the math underneath Bell's theorem (presented well) is *not* difficult, and understanding the math brings one much closer to facing the mystery and controversies of its *meanings*.

Emphasizing these points:

> Everything is vague to a degree you do not realise till you have tried to make it precise. Bertrand Russell [94]

> Often in mathematics, the proof of a result turns out to be more important than the result itself. [29]

[8] The same journal even published essentially (in my view) the same proof 10 years later by a different author, where the only selling point of the second paper was that it had even *less* explanation than the first one. That kind of terseness is prized in professional mathematical writing but is absolutely contrary to what I am trying to do in this book.

[9] The misunderstanding (by funding agencies and researchers) of an impossibility theorem concerning *perceptrons* is believed to have stalled (later successful) research into *artificial neural networks* (an area of enormous current importance) for more than a decade [63].

https://doi.org/10.1017/9781009349451.002 Published online by Cambridge University Press

Finally, understanding the proofs (or even just the general scope and nature of the proofs) will help you spot (common) *nonsensical* statements about famous theorems. For example, after the chapters on Gödel's theorems, you should have no trouble seeing that the following is total nonsense, unrelated to what Gödel's theorems actually concern:

> Basically, Gödel's Theorems prove the Doctrine of Original Sin, ... and that there is a future eternity. Gödel's Theorems mean that, in the human complex, things will go wrong and there will always be a "defect" of sorts about which forgiveness and corrective action will be needed. [80]

1.5 OK, Proofs Are Important, but Why Another Book?

> It is the act of a madman to pursue impossibilities.
>
> *–Marcus Aurelius*

Most of the topics in this book are well known, and some are the focus of many books and articles. So, why write another book on these topics?

1.5.1 Because

Because almost all[10] of the theorems in this book, despite how difficult their original proofs and expositions were, now have elementary, accessible, yet rigorous mathematical proofs. However, most expositions for *lay* audiences do not attempt rigorous *proofs*, and sometimes do not even attempt rigorous *statements* of the theorems. They just try to give the *gist*, or they just *talk about* the theorems, and maybe speculate on their larger impact. Worse, some expositions use loose, incorrect statements about the theorems to support ideological, religious, political, or philosophical viewpoints.[11]

For example, most discussions of Gödel's theorems fall into one of two types: either (1) they emphasize perceived philosophical "meanings" of the theorems, and maybe sketch some of the ideas of the proofs, usually relating Gödel's theorems and proofs to riddles and paradoxes, but they do not attempt to present rigorous, complete proofs or (2) they do present rigorous proofs, but in the traditional style of mathematical logic, with all of its heavy, weird

[10] I wrote "all" not "almost all" first, when I had decided not to discuss Gödel's Second Incompleteness Theorem – since I do not know an accessible, complete proof of it. But, then I changed my mind.

[11] And some writers doing this have the appropriate background and intellectual firepower to know better!

notation, difficult definitions, and technical issues that reflect Gödel's original motivation, proofs, and extensions.

Many people are frustrated by these two extreme types of expositions and want a complete, rigorous proof of incompleteness that they can understand, even if it doesn't exactly prove the same incompleteness that Gödel did. Fortunately, after Gödel published his seminal paper in 1931, people (read Turing and others) realized that somewhat weaker versions of Gödel's first incompleteness theorem have much simpler proofs and expositions. And, these variants of Gödel's first incompleteness theorem still have (in the opinion of many) most of the moral and philosophical force of Gödel's first incompleteness theorem. This book develops several such proofs.

Similarly, there are many lay-audience expositions of Bell's impossibility theorem and inequalities, but most only talk *about it* and/or its perceived philosophical implications.[12]

1.5.2 In Contrast

This book is as much about mathematical proofs as it is about impossibility.

My goal in writing this book is to make simpler, full, rigorous proofs of some of the most profound reasoning in human history accessible to a very broad, lay audience. All of the (full) proofs I discuss in this book involve only *elementary arithmetic and logic* – no advanced math or advanced logical manipulations are required. The book has complete, self-contained, mathematically rigorous proofs for most of the theorems that are discussed.

And, the proofs are "elementary" (in a different sense), meaning that they derive from basic *definitions* and *first principles*. And, although the theorems come from diverse application areas (physics, economics, logic, computer science, and machine learning), none of the proofs assume advanced knowledge of any application.

> Sometimes I've believed as many as six impossible things before breakfast. – Lewis Carroll

[12] With one great exception: The first half of the paper [68] by David Mermin, although originally published in a professional physics journal, is mostly (in my opinion) accessible to a larger lay audience. And, it *does* present a rigorous proof of Bell's impossibility theorem, although that isn't always appreciated. OK, Mermin's exposition doesn't have a lot of fancy mathematical symbols; it isn't written in the most obscure, terse way possible; and it doesn't even have the words "Theorem" or "Proof", but that doesn't keep it from being a truly rigorous mathematical argument. Much of Chapters 2 and 3 of this book are strongly influenced by Mermin's expositions, particularly [68], [70], and [72].

I believe that anyone with a high-school knowledge of mathematics, and the discipline to follow logical arguments (actively, with pen in hand), can understand all of the full proofs given in this book. The only background that some readers might not have is a very basic understanding that a computer program consists of a series of *textual* statements.[13] But, no actual programming knowledge is required, and I have a short Appendix where I discuss what one needs to know about computer programs.

1.5.3 Other Impossibilities

There are several well-developed impossibility theorems that I had initially hoped to include, but in the end I ran out of time and space. I recommend these topics and sources to interested readers. There are many impossibility proofs in the area of *distributed computation* and the *web*. That is an area summarized in the paper: "A hundred impossibility proofs for distributed computing" [67] and a whole book: *Impossibility Results for Distributed Computing* [7]. Also, see [92, 61] for an interesting impossibility theorem in the area of blockchains and Bitcoin.

1.6 How to Read This Book

All expositions are aimed at a general, lay audience, with no specialized background in any of the topics. But that doesn't mean the book is *light* reading. It takes work to fully understand the proofs. The most important thing is to read *actively* with pen in hand, and then to restate, re-justify, and explain in your own words the theorems and proofs. An even better way to learn is to try to *teach* the theorems and proofs to someone else – or pretend to.[14]

In several chapters that have long-ish derivations, I have broken up the expositions with fairly straightforward *Review questions*, to encourage readers to read actively and assure themselves that they are following the ideas in the chapter. Exercises at the end of each chapter are a bit more challenging than the review questions, and some are open-ended discussion questions.

The book is roughly divided into three parts that can be read *independently*. Chapters 2 and 3 form one part, and they should be read in order. Chapters 4

[13] As opposed, say, to the science-fiction image of a computer, probably named *HAL*, with some kind of mechanical (or green bubbling, gooey) brain that just spits out answers in a mysterious, condescending manner.

[14] It took me 40 years of teaching college students before I realized this and was able to give a helpful answer to the recurrent question of how best to study and learn – learn by teaching, if only to your invisible friend!

https://doi.org/10.1017/9781009349451.002 Published online by Cambridge University Press

and 5 form a second part, but can be read separately. Chapters 6–9 form the third part, although the technical material in Chapter 8 is self-contained and can be read separately. Chapter 9 could be read separately, but I don't advise it since it is probably the mathematically hardest chapter in the book[15] – at least read Chapter 6 first for a warm-up. The Appendix is a short discussion on what a computer *program* is, for anyone who has never seen one, making the crucial point that a computer program is a textual document.

[15] The mathematically easiest chapter is Chapter 2. The hardest-*looking* proofs are in Chapter 4, but that is only because they are the longest. Each step of those proofs is intended to be fairly simple, and I have included many *review questions* in that chapter.

https://doi.org/10.1017/9781009349451.002 Published online by Cambridge University Press