Pure and Applied Mathematics

Neal Koblitz

When I received my PhD in pure mathematics in 1974, I assumed that nothing I did in my professional life would have practical value. Like a historian of Medieval Europe, I would in some small way contribute to human knowledge, but not in a way that would affect anyone's daily life.

A half century ago it was common to think that pure and applied mathematics were very different endeavors. At times pure mathematicians would look down on applied mathematicians, just as a poet might look down on script writers for soap operas. In 1940 the great British number theorist G. H. Hardy wrote about his mathematics that its "remoteness from ordinary human activities should keep it gentle and clean." An American mathematician named Halmos even wrote an article with the title *Applied Mathematics Is Bad Mathematics*.

However, even a half century ago there were many examples of pure mathematics unexpectedly providing powerful tools to help solve problems of the real world. For example, group theory was developed in the early 1800s for the purpose of proving that there are no general formulas for solving polynomial equations of degree 5 or more. This question was not of interest outside of pure mathematics. But in the decades and centuries that followed, group theory – which gives a way to study the intricate properties of different kinds of symmetries – has been applied to important problems in physics, chemistry, cryptography, and even music.

Elliptic Curves

One of the mathematical topics that I had worked with in my PhD dissertation was the arithmetic theory of elliptic curves, something which at the time was thought not to have any practical applications. To my surprise, about ten years later I (and, independently, another number theorist who had been trained in pure mathematics) discovered that elliptic curves could be used to improve the security of public key cryptography. Public key cryptography was a new branch of

cryptography that was destined to play a central role in internet security, e-commerce, cryptocurrencies, COVID-19 contact-tracing, and other applications. When I started working on elliptic curve cryptography, I left pure mathematics and became an applied mathematician. It was as if someone who thought of himself as a poet (whose work few people read) was suddenly in demand to write scripts for soap operas (that millions of people would watch on TV).

Nowadays few mathematicians express negative views about applied mathematics. The close interaction between pure and applied mathematics is well recognized. The winners of the prestigious 2021 Abel Prize – Lásaló Lovász and Avi Wigderson – were honored for their work that borders on both pure and applied mathematics. According to Lovász, a professor at Eötvös Loránd University in Budapest, "Today it's more and more difficult – and I think it's a good development – to distinguish pure mathematics and applied mathematics."

No Longer "Gentle and Clean"

The world of pure mathematics, as the word "pure" suggests, has generally been pure in the sense of being free from the challenges and ambiguities of working with human problems. However, when concepts of pure mathematics get pulled into applied areas, problems can arise. Suddenly there are financial and political interests at stake. Since mathematics does not model reality perfectly, one needs to make assumptions – assumptions that might inadequately reflect the human dimensions of the problem or might unintentionally reflect the researchers' own biases and cultural prejudices.

The most obvious danger is "hype", that is, exaggeration. Because the public interest and the amounts of money at stake are much greater for applied mathematics than for pure mathematics, it's common for people working in applied fields to vastly overstate their successes. For example, the term *Artificial Intelligence* is misleading. The term was invented in the middle of the last century, but even now, with all the technological advances since that time, computers are incapable of mimicking key parts of human intelligence. Driverless cars cannot be deployed in most environments because the computers that drive them cannot be counted on to correctly handle situations that are new and unexpected. This limitation has not been removed by so-called "machine learning" (which is also a poor word choice, since it is much more primitive than human learning).

Another example of a misleading term is *provable security* in cryptography, which I'll discuss later.

Quantum Computing

For about the last 20 years huge efforts have been put into developing quantum computing. Progress has been very slow, and there are major theoretical and practical obstacles to be overcome before anything of practical use can be constructed. There's no assurance that a quantum computer that can solve real-world problems will ever be constructed, and, if it can be constructed, no one knows when that might be.

Quantum computing makes heavy use of the mathematics of Hilbert spaces and operators on such spaces. These "spaces" are nothing like the 3-dimensional space of our intuition. They are theoretical tools used to analyze quantum systems of enormous size. For a quantum computer that can break RSA encryption, the dimension of this theoretical space would be roughly 2 raised to the power 4000. (The number of atoms in the Universe is less than 2 raised to the power 150.)

The best example of a practical problem that could be solved much faster by a quantum computer than by a classical computer is the integer factorization problem. The way to do this was discovered by Peter Shor in 1994; his algorithm would completely break both RSA and ECC cryptography, which are the two types of public key cryptography that are widely deployed. To do this would require a quantum computer of great size. One enthusiast for quantum computing estimated that one such computer would cost about 1.000.000.000 USD and require the energy of a dedicated nuclear power plant.

When we look for other problems of practical importance that could be efficiently solved by a quantum computer and not by a classical computer, one obstacle is that no one knows how to input large amounts of data – or in fact any data – into a quantum computer. In the case of Shor's algorithm, the only data needed is the value of the number that must be factored. The only way known to input that value is for a classical computer to rearrange the circuitry of the quantum computer in a way that corresponds to the bits of the number.

Despite all these obstacles, the hype about quantum computing has been amazing. According to a press release from IBM: "Quantum computers could one day provide breakthroughs in many disciplines, including materials and drug discovery, the optimization of complex systems, and artificial intelligence." And Microsoft agrees: "Quantum computing takes a giant leap forward…that will forever alter our economic, industrial, academic, and societal landscape…. This has massive implications for research in healthcare, energy, environmental systems, smart materials, and more." This is pure hype!

"Provable Security"

Besides exaggeration, another problem with the way pure mathematics has been brought into computer science is that researchers frequently exaggerate the assurances that can be provided by rigorous theorem-proving. The term "provable security" in cryptography is misleading, because it is impossible to *prove* that a cryptosystem cannot be breached in any way.

Rather, the theorems that cryptographers prove are much more limited. They are conditional theorems, not absolute theorems. They have the form "if P is true, then Q is true." The assumption P has the form *the adversary is unable to complete a certain computational task* (such as factoring a large integer) *in a reasonable amount of time*. The conclusion Q has the form *the adversary will not be able to breach this cryptosystem in a reasonable amount of time*.

Sometimes leading researchers in cryptography fail to appreciate the difference between proving a conditional theorem and proving an absolute theorem. For example, there is widespread misunderstanding of the concept of a *nonuniform* algorithm.

The usual type of computer algorithm is called a *uniform algorithm*. In contrast, "nonuniform" means that when solving a problem we're allowed an "advice string" that will help us, with no account taken of how long it would take someone in practice to find the advice string. Nonuniform algorithms are an interesting and important concept in theoretical computer science. But from a practical standpoint a nonuniform algorithm is not really an algorithm, because it relies on an advice string that no one knows how to find.

This is what two top researchers in cryptography wrote in their notes for a course given at MIT: “Clearly, the nonuniform adversary is stronger than the uniform one. Thus, to prove that something is secure even in presence of a nonuniform adversary is a better result than only proving it is secure in presence of a uniform adversary.”

This is wrong. The first sentence is correct – a nonuniform adversary can use an advice string, whereas a uniform adversary (the usual kind) cannot. However, the theorem does not become stronger. Its conclusion becomes stronger, but its assumption also becomes stronger. If instead of proving “if P, then Q” you prove “if R, then S” where R is a stronger assumption than P and S is a stronger conclusion than Q, your theorem is not stronger (or weaker) than before. The “if P, then Q” theorem is incomparable to the “if R, then S” theorem. That’s basic logic.

This misunderstanding led one of the researchers who made this statement to make a fundamental error in a paper published in the proceedings of the 2005 “Crypto” conference (the most prestigious annual cryptography meeting). His mistake went undiscovered for seven years.

COVID-19 Contact-Tracing

Perhaps the greatest danger in applications of mathematics to practical problems is that the human dimensions of the problems will not get adequate attention. I’ll give two examples, both concerning the COVID-19 pandemic.

Researchers have developed several smart phone apps for automated contact-tracing. Their priority in this research has been to use cryptography to preserve privacy, that is, to ensure that no one other than authorized medical people can learn who has tested positive or who has been in contact with someone who tested positive.

Susan Landau is a leading expert on online privacy, but she has criticized the excessive emphasis on privacy protection while more urgent issues of fairness have been largely ignored. She has written a book titled *People Count: Contact-Tracing Apps and Public Health*, in which she discusses the ways that careless

implementation of contact-tracing apps could cause much hardship, especially for poor people and racial minorities in the United States. Her main points are:

● "One of the limitations of app-based contact-tracing is that Bluetooth signals can travel through walls and floors." Thus, they would show a contact if someone is sitting on the other side of a wall from a COVID-positive person. This is called a *false positive*.

● In the U.S. it's mainly low-income people and racial/ethnic minorities who live in close quarters in apartment complexes or multi-family houses.

● It's mainly low-income people and racial/ethnic minorities who work in industries where they cannot work from home and are in close contact with coworkers (shop clerks, nurses, factory workers, etc.). During the pandemic, coworkers are often separated by barriers – but the barriers do not stop Bluetooth from giving a false positive.

● Therefore, contact-tracing apps will produce many more false positives for those people than for affluent white people.

● A false positive may mean that they have to stop working (and those people are living close to the margins even when employed), and in the U.S. that might lead to job loss, eviction from their apartment, and huge disruption in their life.

In the U.S. much has been written about the ways in which the COVID-19 pandemic has disproportionately impacted the poor and racial minorities. Landau's book extends this analysis to automated contact-tracing.

Curve-Fitting for COVID-19

Another case of a faulty response of applied mathematicians to the pandemic occurred at my own university, the University of Washington, at its Institute for Health Metrics and Evaluation (IHME). In the crucial early weeks of the pandemic – a time when Americans needed to understand the seriousness of the threat and respond with strong measures – the IHME became famous nationally because of its optimistic projections. The IHME predicted that the total number of U.S. deaths during the course of the pandemic would be only 60.000, roughly the

number of American fatalities during the 2017-18 flu season. In reality, the deaths at present exceed 500.000 and are expected to increase to more than ten times the IHME estimate.

Why did the IHME do so badly? Their mathematical model, developed by applied mathematicians who had little or no experience in epidemiology, was largely based on what's called "curve-fitting." They took the curves for infections and deaths from Wuhan, China and simply fit them to the U.S. data. They assumed that, as in Wuhan between January and March of 2020, the number would rapidly increase, then level off, and then rapidly decrease, with most of the deaths ending in two or three months. Their methods supposed that Americans would respond to the crisis in much the same way as the Chinese.

In retrospect, this was a foolish assumption. The politics and culture of the U.S. are very different. At the time we had a President who denied scientific facts and opposed mask-wearing. We also lack the discipline of the Chinese; as a *New York Times* reporter commented, "Americans don't like being told what to do."

Other mathematical models were more accurate. At about the same time as the IHME made its prediction of 60.000 deaths, a group of researchers at Imperial College London predicted that U.S. deaths would reach 480.000, a prediction that was reported on the front page of the *New York Times*. But it was the IHME prediction that was seized upon by the Trump administration to justify their refusal to take the pandemic seriously or to take appropriate measures.

Mathematical Ethics

How did the IHME react to this misuse of their work? Did they loudly object that their prediction would lose all validity if its assumptions were violated, that is, if the U.S. responded by delays and refusal to mandate mask-wearing or lockdowns? No, they did not object; they simply basked in the glory of being constantly cited in White House press conferences.

The medical profession has had ethical guidelines since the time of the ancient Greeks. The central principle of those ethics is embodied in the Hippocratic Oath: ***First do no harm***. When mathematicians venture into applications that will affect

millions of people, they should take a mathematicians' version of the Hippocratic Oath.