A Silent Revolution in Mathematics

The Rise of Applications, Numerical Methods, and Computational Approaches

PETER SCHUSTER

Peter Schuster, Editor-in-chief of Complexity is at the Institut für Theoretische Chemie der Universität Wien, Währingerstraße 17, Wien, 1090, Austria E-mail: pks@tbi.univie.ac.at

Fifty years ago there has been still a clear cut separation between pure and applied mathematics: pure mathematics had its home in the Olympus of academic sciences, whereas applied mathematics was left to the technical universities for teaching and research. Some time ago a colleague of mine from the department of mechanics of the Technical University of Vienna said partly amused partly offended: "Our people in the math department do pure[1] mathematics, is it then dirty mathematics what I am doing?" Mathematics has undergone a true silent revolution within the last few decades. The difference between pure and applied mathematics—thought to be fundamental in the past—has almost completely disappeared. Computer modeling in science is in widespread use and almost every university houses a department for computational science but this is only one usage of electronic computers in present day mathematics although a very powerful one. As most people are familiar with the achievements and problems of numerical modeling and computer simulations, we shall focus here more on other issues that are not so much commonplace.

PROGRESS IN COMPUTATION—DUE TO IMPROVEMENT IN HARDWARE OR IN ALGORITHMS?

Speed of computation and digital storage capacities are growing exponentially since 1960 with an approximate doubling time of 18 month—a fact that is commonly addressed as Moore's law [1]. It is not so well known, however, that the spectacular exponential growth in computer power has been overshadowed by the progress in numerical mathematics that led to an enormous increase in the efficiency of algorithms. To give just one example that has been presented to the President of the United States in the 2010 report by Martin Grötschel from the Konrad Zuse-Zentrum, Berlin [2]: "The solution of a benchmark production-planning model by linear programming would have taken 82 years CPU time in 1988, using the computers and the linear programming algorithms of the day. In 2003—fifteen years later—the same model could be solved in one minute and this means an improvement by a factor of about 43 million. Out of this, a factor of roughly 1000 resulted from the increase in processor speed whereas a factor of 43,000 was due to improvement in the algorithms." Many other examples of similar progress in the design of algorithms could be given.

[1] *The German translation of pure mathematics is "reine Mathematik," where "rein" means "clean" when directly translated, and dirty is the antonym to clean.*

 Vol. 18 No. 6
DOI 10.1002/cplx.21464
Published online 30 July 2013 in Wiley Online Library (wileyonlinelibrary.com)

Understanding, analyzing, and designing high-performance numerical methods, however, requires a firm background in mathematics. The availability of cheap computing power has also changed the attitude toward exact results in terms of complicated functions: It does not take so much more computer time to compute a sophisticated expression like a hypergeometric function than to calculate an ordinary sine or cosine for an arbitrary argument. Symbolic computation has changed everyday life of mathematicians as well as scientists who apply mathematics: operations on complex and sophisticated expressions are enormously facilitated and in this way the present day computational facilities have large impact on analytical work as well.

NEW APPLICATIONS FROM OLD AND NEW MATHEMATICS

Many examples of interesting new applications could be given, we mention only two illustrative and representative ones: (i) number theory in cryptography applying established mathematics to present day problems and (ii) solution of inverse problems, which required the development of new mathematical techniques to be able to deal with ill-posed problems.

A famous example of unexpected applications of a branch of pure mathematics in everyday applications is the use of number theory—a discipline that is traced back to the Old Babylonians by some historians—in modern cryptography [3]. To allow for security of messages during transmission from sender to receiver enciphering and deciphering keys are required. Symmetric encryption schemes, which have been applied for thousands of years, use a single secret key for both encryption and decryption, and accordingly sender and receiver must share the key in advance. Security of the transmission depends on how well the key is kept private by both persons. Asymmetric-key algorithms are used in *public-key* cryptography and they are based on pairs of keys for each user: (i) a public encryption key and (ii) a private decryption key that is exclusively in the hand of its proprietor. Both keys are required to be able to read the transmitted message. The two keys are related mathematically but the parameters are chosen in such a way that a calculation of the private key from the known public key is prohibitively expensive, and number theory does the job to make such a calculation practically impossible.

Around 1900 Jaques Hadamard coined the notion of well-posed problems in mathematics that have to fulfill three criteria: (i) a solution exists, (ii) the solution is unique, and (iii) the behavior of the solution hardly changes on slight changes in the initial conditions. If one of the three criteria is not fulfilled, the problem is ill-posed. Commonly, solution curves or data points are calculated from model equations whereby initial and boundary conditions as well as a set of given parameters are supplied. Such a task is a typical forward problem. In applied science, the inverse problems are occurring more frequently: data points are recorded and the task is to compute the parameters of the system, which created the data [4]. In contrast to typical forward problems, inverse problems are often ill-posed. A joint analytical and computational approach, however, has been successful and satisfactory solutions can be obtained by means of methods called regularization [5] that prevent artifacts and divergence. Currently, inverse problems are an established branch of mathematics and several specialized journals are publishing a great number of methodological advances and applications.

PROOFS BY NUMERICAL COMPUTATION

In 1852, the South-African mathematician and botanist Francis Guthrie formulated an innocent looking puzzle of coloring planar maps, the famous four color problem [6], which states: "The regions of any simple planar map can be colored with only four colors, in such a way that any two adjacent regions have different colors."[2] No proof has been found for this simple looking problem until Kenneth Appel and Wolfgang Haken were able to present one [7,8]. The problem with the Appel and Haken approach, however, was that the publication of their proof initiated a mathematical controversy, because part of the proof used computer calculations for excluding critical and possibly contradictory cases. The mathematics community was split into two groups of researchers, one willing to accept a numerical proof and others who were not. Some progress was made when the number of critical cases had been drastically reduced by a revised version of the Appel and Haken proof [9] and the current proof that is accepted by the majority of mathematicians was performed with the so-called Coq system that provides a tool for computer assisted formal proofs [6,10].

The second example presented here deals with the proof of a 400-years old conjecture originally done by the famous astronomer Johannes Kepler: "The densest arrangement of spheres is one in which they are stacked in a square pyramid." Every grocer or merchant on the market apparently knows this solution when piling up oranges,

[2] *Adjacent countries must have a common boundary that is larger than a single point. An illustrative nongeneric case that has to be excluded is Four Corners in the US, where Colorado, Utah, Arizona, and New Mexico meet in a single spot. At Four Corners Utah and Arizona have a common boundary and so do New Mexico and Colorado, but Utah and New Mexico as well as Colorado and Arizona meet only in a single point*

DOI 10.1002/cplx

apples or melons, and every cannoneer storing cannonballs makes unconsciously use of the same principle for closest stacking of identical balls in 3D space according to face-centered-cubic geometry. Many mathematicians tried to provide a proof for the solution being the densely packed pyramid and it took 400 years before a proof derived by Thomas Hales with extensive use of computers was published [11]. The publication has been preceded by several years reviewing by about a dozen experts in mathematics and they said that they were 99% sure that the proof is correct but they raised the issue of being unable to check carefully every line of the computer code when it had been visited by the running program—what would have been necessary for absolute certainty [12]. As said in the previous paragraph on the four-color problem, computer codes have been and are currently being developed, which check computer assisted proofs for consistency and possible errors. The present-day situation is not untypical for rapid or revolutionary change in science: Procedures that are still rejected now by the scientific community may well be the standard in several years.

The difficulties of acceptance of results derived from huge amounts of data that have been never seen by human eyes nor checked by expert brains are not uncommon in science. These amounts may be so huge that only high-performance computer programs can handle, store, and retrieve them, as it happens, for example, in elementary particle physics or in bioinformatics. Then, only computers with special software can debug and check the computer programs. Evolutionary methods applied to software error correction are a highly promising new field [13,14].

NEW INSTITUTIONS IN MATHEMATICS

The mathematical and the scientific communities as well as the funding agencies have already reacted to the reorientation of goals in academic research in mathematics. New institutions encouraging and facilitating direct cooperation between basic research in mathematics and applied science were founded. Initially, physics, engineering science and technology oriented industry benefited most from the interaction with mathematics, later other disciplines like chemistry, biology, and sociology followed. Economics and physics have been traditionally in close cooperation with mathematics for long time already. The National Science Foundation is financing eight institutes for application of mathematics, which are spread all over the US, most countries of the European Union created new institutes, which are housing mathematicians interacting with scientists, and similar developments are occurring in South-East Asia, for example, in Singapore, in China and in India.

Mathematicians, in contrast to most scientists, do neither require large groups nor expensive equipment for their research work. In case mathematicians use computers, as a rule, they do not need large supercomputers. What mathematicians need, however, is exchange of ideas and the personal dialogue between researchers. The new institutes have one thing in common and this is a well-organized and intensive visitors program and specialized meetings of experts in order to facilitate joint research.

PURE AND APPLIED SCIENCE

Compared to most scientific disciplines, the merger between basic and applied research came a little late in mathematics. In physics and chemistry of the 19th century, scientific innovations found their way into industrial exploitation already without substantial delay and since then the time span between discovery, patent application, and translation into an industrial process became shorter and shorter. Chemistry is a good example: applied chemistry never had a lower reputation than basic research, because the motto was and is "pure chemistry is poor chemistry"—the money is made in the chemical industry and not in academia. The famous international journal "Angewandte Chemie" with an English translation was founded in 1887, it is publishing new results from basic research as well as interesting application. Any border between the sister disciplines pure chemistry and chemical engineering would be artificial and obsolete. An impressive representative of this union between academia and industry in a single person is the Austrian chemist Carl Auer von Welsbach: He discovered four new elements of the periodic table, did three major inventions, and has been a successful entrepreneur.

Modeling and numerical simulation were the first fields where computers became an instrument of research. The application of quantum mechanics to problems of molecular structures and molecular spectroscopy required and is still requiring enormous computer resources; the mathematics is relatively simple, and the challenge is the size of the problems to be treated. Modeling in physics has a very long tradition and is typically more demanding as far as the necessary mathematical tools are concerned. Biology is joining physics and chemistry in the requirement for large scale computing since relatively short time only and it introduces new issues: so far there is no theoretical biology that provides a secure frame for model building. The model in biology does not declare itself out from a commonly accepted theoretical body like quantum mechanics, and to conceive a useful model needs empirical knowledge, skill, and intuition.

The revolution in mathematics did not come by itself. It has been initiated and guided by the spectacular development in computer technology. Problems of direct relevance for applications in

DOI 10.1002/cplx

science and technology became accessible through the combination of mathematical analysis and numerical computation: Simplified mathematical models could be adapted to the necessarily complex realities and became highly valuable tools for the experimentalists. Finally, it should be stressed that the close cooperation of mathematicians, scientists, and engineers provided and provides the basis for all the fascinating new developments.

REFERENCES

1. Moore, G.E. Cramming more components onto integrated circuits. Electronics 1965, 38, 4-7.
2. Grötschel, M. In: Designing a Digital Future: Federally Funded Research and Development in Networking and Information Technology; Holdren, J.P.; Lander, E.; Varmus, H., Eds.; President's Council of Advisors on Science and Technology: Washington, DC, 2010.
3. Koblitz, N. A Course in Number Theory and Cryptography; Springer-Verlag: New York, 1994.
4. Aster, R.; Borchers, B.; Thurber, C. Parameter Estimation and Inverse Problems; Elsevier: Amsterdam, NL, 2012.
5. Tikhonov, A.N.; Arsenin, V.Y. Solutions of Ill-Posed Problems; Winston: New York, 1977.
6. Gonthier, G. Formal Proof—The four-color theorem. Not Am Math Soc 2008, 55, 1382-1393.
7. Appel, K.; Haken, W. Every map is four colorable. Bull Am Math Soc 1976, 82, 711–712
8. Appel, K., Haken, W. Every map is four colorable. Ill J Math 1977, 21,429-567.
9. Robertson, N.; Sanders, D.; Seymour, P.; Thomas, R. The four-color theorem. J Combinatorial Theory B 1997, 70, 2-44.
10. Gonthier, G. A Computer-Checked Proof of the Four Colour Theorem; Microsoft Research Cambridge: UK, 2005; Available at: http://research.microsoft.com/en-us/people/gonthier/4colproof.pdf. Accessed July 25, 2013.
11. Hales, T.C. A proof of the Kepler conjecture. Ann Math 2005, 162, 1065-1185.
12. Szpiro, G. Does the proof stack up? Nature 2003, 424, 12-13.
13. Weimer, W.; Forrest, S.; Le Goues, C.; Nguyen, T.V. Automatic program repair with evolutionary programs. Commun ACM 2010, 53, 109-116.
14. Le Goues, C.; Nguyen, T.V.; Forrest, S.; Weimer, W. GenProg: A generic method for automated software repair. Trans Software Eng 2012, 38, 54-72.

DOI 10.1002/cplx