Computer Algebra: The End of Mathematics? *

Bruno Buchberger
Research Institute for Symbolic Computation,
Johannes Kepler University, A4232 Castle of Hagenberg, Austria

Abstract

Mathematical software systems, such as Mathematica, Maple, Derive, and so on, are substantially based on enormous advances in the area of mathematics known as *Computer Algebra* or *Symbolic Mathematics*. In fact, everything taught in high school and in the first semesters of a university mathematical education, is available in these systems 'at the touch of the button'. Will mathematics become unnecessary because of this? In the three sections of this essay, I answer this question for non-mathematicians, for mathematicians and for (future) students of mathematics.

1 Computer Algebra: Mathematics at the touch of the button

Many non-mathematicians remember mathematical education as something burdensome: endless drills of things that one never really understood! Or, particularly perfidious, exercises that require a special trick to solve them. The inventor was a colossus, we petty students peep about at the exercises. Above all, the students ask: 'Will we ever need this? Who of us, having graduated, will ever differentiate or integrate a function again? Not even extracting a root will really occur later, and if it does, we simply use the pocket calculator! How many of us have, in later life, been assigned problems from mathematics classes ("Two trains travelling from A to B with speed u, ...")?'

It is not just that a lot of people never need mathematics, many people of great influence are proud of having been weak in mathematics in school and 'nevertheless' got somewhere. (I experience it frequently, for example, when economic delegations, company representatives, politicians and others visit the prosperous Software-Park in Hagenberg, which was founded by our institute RISC. Most visitors are impressed by the economic dynamics resulting from the connection of mathematical research and economy, but at the outset many confess, with an embarrassed or superior smile, that mathematics were always incomprehensible or uninteresting to them.)

Meanwhile the situation has become much more extreme. There exist not only pocket calculators, with which everything one learns up to the age of fourteen in 'Calculations', can be done by pressing buttons. Now there are also software systems (like Mathematica, Maple, Macsyma, Derive, etc.), which make everything one learns in high school or in the mathematical lectures of the engineering sciences available at the touch of a button, even almost everything presented in the first two years of a regular mathematics program – and also a lot more. These systems also provide graphical user interfaces, which make the handling very simple for everybody. Hundreds of ready-to-use software packages, programmed on the basis of these mathematical software systems, can be downloaded easily from the Internet and can be executed on the computer at home for applications in the natural sciences, medicine, economy and many more areas.

Do you want to calculate, for example, how a robot, whose platform is controlled by 6 rods, reacts to a displacement of these rods? Or to compare the quality of financial products? Or to calculate the diffraction of a complex optical system of lenses? Or to study how the easiest cellular structures evolve over thousands of generations? And this all with graphical input and output, and animated illustrations? You only have to visit the homepages of the

*Mitteilungen der Deutschen Mathematiker-Vereinigung, Vol. 2, pp. 16-19, 2000. Translated by C. Schulzky

common mathematical software systems (e.g. www.wolfram.com for Mathematica), download one of these systems via the Internet (for which – thank god! – you have to pay something), and navigate through the application pages. In many cases you will find a prepared software package for your application; you can teach yourself the professional use of the appropriate package through interactive introductory examples, and, if necessary, you can quickly build, from the existing functionalities of your package, new functionalities, which are optimally suited to your needs. One example of such an application can be found in appendix 1.

The qualitative innovation of today's mathematical software systems – as opposed to the collections of numerical algorithms[1] twenty years ago – is the development of methods that can be used to calculate with a computer 'like a human being'. This means that one can work not just with (rounded) numbers in the computer but also with formulas, symbolic expressions, verbal structures, which represent the considered mathematical problems exactly and which then allow 'exact' solutions 'in closed form', 'analytically', or 'symbolically'. Many of the things, which had to be developed by mathematicians arduously and with much consideration 'with paper and pencil' before one could start writing a computer program for the (numerical) solution of a given problem, can be done today by the computer with the methods of 'symbolic mathematics' (or 'computer algebra', as it is also called). Owing to the essential contribution of computer algebra, the situation regarding the usability of existing mathematical knowledge and mathematical problem-solving techniques has now changed radically within a few years. Nowadays, in fact, the whole of the mathematics one learns in high school and in the first semesters at university – including the steps that require 'thinking' – is 'available at the computer'.

For the example in appendix 1, this means not only that given images can be compressed with a system of wavelets, e.g. for fast transmission, but also that usable systems of wavelets can be developed today at the computer, see [2], with the methods of computer algebra (in this case with the methods of so-called Gröbner-bases [1]). Until recently, the latter task had to be solved by mathematicians 'non-numerically' and 'with paper and pencil', before an image compression procedure could emerge from such a wavelet system.

If the methods of mathematics are available for everybody now at the touch of the button, and if even the 'paper and pencil work' of the mathematicians is now done with the methods of computer algebra by the computer, if anyone, in fact, even without a special mathematical education, can solve the most complicated mathematical problems, and if even people who are proud of 'having always been bad in mathematics' can start, as playfully as in a video game, the most sophisticated mathematical machinery, what actually remains to be done by the mathematicians? Is computer algebra the end of mathematics?

For users of today's computer-algebra-based software systems, it might be enough to know that they now have the potency of mathematics, including mathematics that even the best mathematicians do not carry in their heads, available at the touch of the button and without the strain of thinking. For them, the question about the end of mathematics is probably irrelevant. It might be much more important that the message gets across to the 'broad public' as soon as possible that mathematics can now be used by everybody at the touch of the button.

But for the mathematicians themselves the question about the end of mathematics may sound disturbing. Will we soon have ourselves rationalized out of business? Will we soon have to confess honestly that our institutes are too big, that the public money spent on mathematics in the universities is too opulent, and that the hours for mathematical education in schools and also in those university programs in which mathematics is just an auxiliary science, are way out of proportion? Are we honestly allowed to motivate young people to study mathematics or to become mathematics teachers? Shouldn't we rather turn our attention instead to the contents of those subjects that need 'real creativity' (e.g. the political sciences or biotechnology), since apparently even the 'creative' things in mathematics are done 'by the computer'?

[1] Numerical Mathematics: All mathematical problems are replaced by approximate, 'finite' problems. These substitute problems are then solved approximately by rounded numbers.

2 Computer Algebra: Trivial or Trivialized Mathematics?

The answer to these questions should be simple and natural for mathematicians, but it is surprising how many mathematicians (among them also a lot of 'pure' mathematicians and especially many mathematics teachers) have a very diffused conception of what today's situation of the automation of mathematics means for mathematics itself. There are two main groups with apparently contradictory opinions to these questions:

The *purists*: they believe that what is done today in mathematical software packages with numerical and computer algebra methods is just 'trivial' mathematics. As a 'real' mathematician, one should not and need not meddle with these things and one should leave these systems to users or to those mathematicians who are not capable of doing 'real' mathematics. The purists among the mathematicians are using the computer at best to read email, to search for literature in the web, or to type a work in LaTeX. In their opinion, one should banish these software systems from mathematical education, in order that the students are not corrupted by these systems.

The *populists*: they believe that the parts of mathematics which are accessible today in mathematical software systems need not be taught anymore or just as a 'black box'. Then the head would be free for the 'creative parts' of mathematics and their applications, whatever they might be. Extreme supporters of this opinion even believe that the time of proofs is over, in the sense that, to develop new mathematical results, one should rather do experiments on the computer – like a physicist – using existing systems, instead of verifying results with the 'old-fashioned' method of proof.

I do not agree with either of these opinions and instead I think the following:

- Mathematics is characterized by the method of proving. Although experimenting with examples (today: experimenting using mathematical software systems) is certainly essential for gaining new conjectures and although ideas for proofs typically evolve from examples, the method of proving is, in the end, the essence of mathematics.

- 'Slaying' an infinite number of instances of a problem with *one* good theory, *one* new insight, *one* new proof, or *one* new method, has always been the aim of mathematics. At the moment, when the infinitely many instances of a problem can be treated by means of a nontrivial theorem, including its nontrivial proof, and resulting method, then the corresponding problem area of mathematics is 'trivialized'. The computer age differs from earlier mathematical times only in the way that the notion of the 'method', which is used to kill the infinite number of instances of a problem, has a more concrete and extreme meaning: a method for a problem, a method which can be executed on a computer, solves that problem so completely that no form of creativity is needed while applying this method to any one instance of the problem. Thus, mathematics is used to make unnecessary an infinite number of reflections at the level of an instance of a problem, by means of thinking thoroughly one time (working on the 'basic' level). In other words, with nontrivial mathematics on a level A, a complete area of mathematics is 'trivialized' on a level B. (One example: level A is the Liouville theory of the necessary field extension for the description of elementary transcendental functions; level B is the problem of integrating elementary transcendental functions with the Risch algorithm. A simple example: level A is theorems about the invariance of solution spaces of linear systems with respect to row operations; level B is solving linear systems, given by matrices, with the Gauss algorithm.)

- The more one strives to solve problems in mathematics not just 'by any means' but by computer executable algorithms, the more sophisticated is the mathematics (i.e. more delicate theories, deeper theorems, more difficult proofs) necessary to make solutions possible. This is true because it is certainly more difficult (it requires more thinking) to reduce a given problem to well defined building blocks (e.g. to already available algorithms) using well defined methods (e.g. recursions, finite loops) instead of reducing it by using powerful reduction constructs (e.g. set building quantors, set union quantors) to mighty axiomatic 'black boxes' (e.g. the axiom of choice). (One example is given in appendix 2.) In other words, what we have now available in mathematical software systems is not trivial mathematics, but rather, mathematics trivialized by extremely nontrivial mathematics!

- This has the following consequence for the 'sociology of mathematics'. It should not be those mathematicians who are incapable of doing 'real' ('pure') mathematics who should deal with algorithmic mathematics (e.g. computer algebra), it should be the reverse: algorithmic mathematics needs the best mathematical heads. Or another way: 'pure' mathematicians, who only know the computer so far from writing emails, should earnestly occupy themselves with making their working areas more algorithmic and they will find a lot of stimulation and newer, more interesting, and mathematically extremely difficult questions, which can only be answered by an enormous deepening of the mathematical theory.

- The algorithmic development of mathematics will never be finished. Thus one need never fear that reduction to algorithms will be the end of mathematics. Higher and higher problem areas of mathematics will be algorithmically opened, making deeper and deeper mathematics necessary. In this sense, the surface of algorithmization is just scratched, despite the enormous development of computer algebra. Compared with what is not yet understood, penetrated, algorithmized, or trivialized, what can be done with the computer will always be a tiny fraction. The impossibility of finishing the algorithmization of mathematics is not just the practical experience of all the workers on that field – because every time, when another piece of mathematics is algorithmized, new horizons appear – it is also an intrinsic property of mathematics, which is provable (!) and constitutes a practical manifestation of Gödel's incompleteness theorem.

- This has the following consequence for the didactics of mathematics. On the one hand, it is very naive to exclude the computer from mathematics today; on the contrary, it is not just an auxiliary tool but the motive and driving force for the rigorous development of the basic aim of mathematics, which is to make difficult problems solvable – by extensive thinking – systematically and even automatically. It was and still is 'politically' a serious mistake to let the using of computers, i.e. the algorithmic solution of problems, drift away from mathematics and to neglect the banished child 'computer science'. On the other hand it is also naive to use the computer as a 'black box' in places where one needs to develop comprehension of what the problem is and what the corresponding basic mathematical concepts, insights, and reasons are. There is no absolute answer to the question of where in mathematical education 'the computer' should be used. It is rather the case that for a given topic the blind use of existing algorithms is pointless during the phase in which new concepts, insights and reasons have to be worked out – 'the white box phase of the lesson'. However, in the phase in which all discussions of the basic concepts are completed, it is equally pointless to exclude the use of existing algorithms – 'the black box phase of the lesson'. For a detailed description of this 'white box/black box principle' see [3].

3 Computer Algebra: Key Technology of the information society

Of course, mathematics is not at its end; it is dynamic as never before. Especially because of the explosive development of the algorithmization of mathematics, we rather have to speak about a new beginning of mathematics. In the application of mathematics to itself, there lies an enormous driving force, which has reached a new dimension especially through new mathematical software systems, and there is an unprecedented dynamism in mathematical research, education and applications.

- In all areas of mathematical research it is now possible to get theoretical stimulation by extensive and easy experimentation with the parts of mathematics already algorithmized.

- The aim of the algorithmization of more and more parts of mathematics in a more and more efficient form yields a lot of new questions and problems to mathematical research. To get answers and solutions one has to develop new or deepened ideas, definitions and theories.

- Mathematical education in the subjects in which mathematics is just an auxiliary science will change dramatically, and will provide a more comprehensive and enriched view of the problem solving capacity of

mathematics to a wider range of people.

- The education of the new generation of mathematicians will change drastically. It will be possible to grasp basic mathematical thoughts in a more comprehensive and thorough manner in less time, and advance to the actual topics of research more quickly. Therefore the new generation of mathematicians will be able to work at the frontier of mathematical research earlier.

- A high level of formal education is necessary especially for the algorithmization of abstract areas in mathematics, and therefore the abstraction of mathematics will be raised even higher, because the automation of thoughts requires their complete formalization and a faultless formal plumbing of their depths.

The thinking technology of mathematics - the working in abstract models - is at the heart of technological progress on the basis of natural sciences. Algorithmic mathematics, and especially the most abstract peculiarity of algorithmic mathematics in the form of symbolic computation (computer algebra), has the automation of working in abstract models as an aim. All technological progress aims at the automation of problem solving in all areas. Computational mathematics aims at the core area of the progress spiral, at the automation of the thinking technology. Therefore it should be obvious that *computational mathematics is one of the technologies, if not the key technology, of today's information society.*

Only a few people are really aware of this simple fact, and I want to stress it here for following reasons.

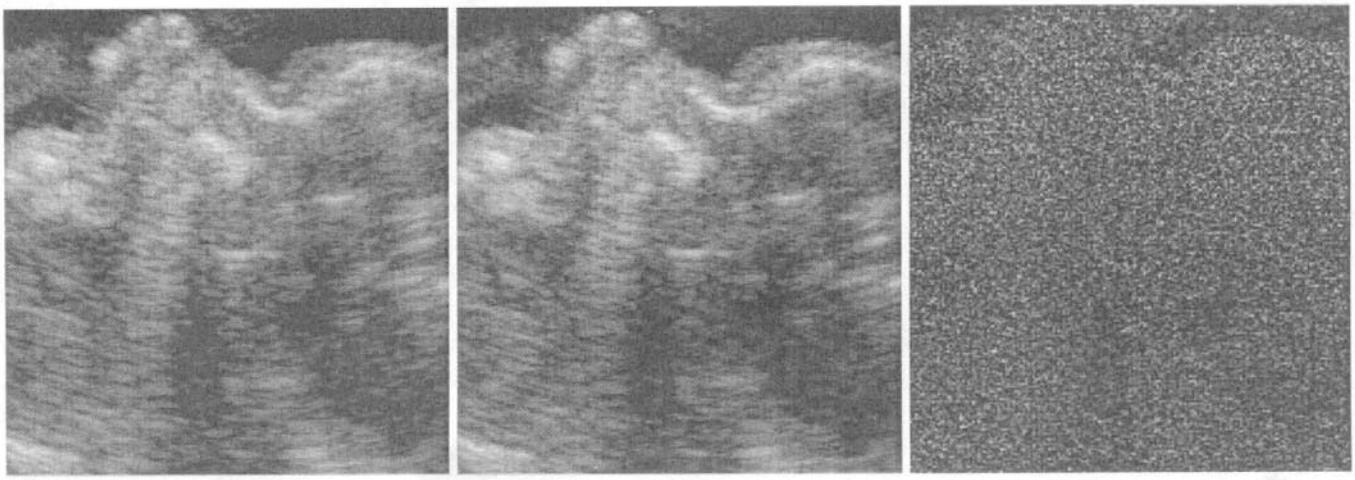
- It is rammed into today's youth (and they see it every day) that technology development, and the economy building on that, is the result of the decisions of the people working in politics, finance, marketing, and management. Without playing down the contribution of all these areas, one has to clarify the intrinsic logic of technological and economic progress to prevent it from sinking into oblivion. The driving force of success comes from the creativity of the technological disciplines. Somebody who is studying technology or mathematics stands in the 'eye of the hurricane' of modern developments and not just somewhere in a back room. Today it is motivating as never before for a young person to get involved with the adventure of mathematics based technology.

- Algorithmic mathematics, especially, has an enormous range, which requires the combination of the best techniques of logic, mathematics, and computer sciences. Algorithmic mathematics has theoretical depth and practical power. It lives in the world of international academic research as well as in the world of the hottest information- and communication-technology companies. The best students particularly should feel motivated to build their careers in this area.

- The people who are politically responsible have to see clearly where the power sources of technological progress and economical development lies. Therefore everything must be done to open the doors for the young to a modern comprehension of mathematics and to establish the best conditions in the education and research institutions, which are responsible for this basic area of the technological and economical structure.

- In recent years it has become fashionable to re-discover applications in research funding programs. Though this has been important as a reaction to the ivory tower behaviour of some scientists, it is dangerously overdrawn today in many places (see e.g. the fifth framework program of the EU). The driving force in the 'eye of the hurricane' of technological and economic progress is and will be the finer and finer understanding of nature's structure and the more and more efficient use of the scientific technology of thinking, whose essence is mathematics and, today, self-automated mathematics.

Appendix 1: Wavelet-transformation of a ultrasonics image



The first image is a section of a three dimensional ultrasonics dataset of an embryo. This image needs approximately 16MB of memory and the transmission of many hundreds of such sections needs a correspondingly long time. The second image shows the same section after a data compression and subsequent decompression with the new wavelet method based on Gröbner bases. The compressed image needs just 1/25 of the memory of the original image! Therefore the transmission time also reduces to 1/25. The compressed image cannot be distinguished from the original with the bare eye. The third image shows the difference set intensified 12 times, and demonstrates that there is in fact almost no difference between the original and the compressed/decompressed original.

With this method, therefore, the transmission performance in time-critical applications, such as in medicine, can be increased dramatically with no suffering of the quality of the information.

Appendix 2: Non-constructive proof of the existence of Gröbner bases

Let $\mathbf{P}$ be the set of multivariate polynomials over a field. For $F \subseteq \mathbf{P}$, $I(F) := \{\sum_{i=1}^{m} h_i f_i \,|\, h_i \in \mathbf{P}, f_i \in F\}$ is the ideal produced by F. For sets T of power products let $\mathrm{I}(T)$ be the set of all multiples of elements in T. Moreover let $\mathrm{L}(f)$ be the highest power product that occurs in the polynomial f (within a fixed allowed order of the power products) and correspondingly let $\mathrm{L}(F)$ be the set of all highest power products of polynomials in F. This set F is called Gröbner basis if $\mathrm{I}(\mathrm{L}(F)) = \mathrm{L}(\mathrm{I}(F))$. The problem is now to find for every set of polynomials F a set of polynomials G such that $\mathrm{I}(G) = \mathrm{I}(F)$ and that G is a Gröbner basis. In fact this problem is very important as one can show that many fundamental problems in commutative algebra (algebraic geometry) can be solved algorithmically if one can find not only some basis but a Gröbner basis for the ideal of polynomials in question. The construction of Gröbner bases is therefore a key problem of algebraic geometry.

A first 'solution' of this problem is to set $G := \mathrm{I}(F)$. The proof that this solution has the required properties results directly from the definitions and simple properties of ideals. This solution has the three properties which sharp tongues refer to as the typical properties of mathematical statements: It is prompt and correct but 'entirely useless'. In our case the solution is useless in the sense that the definition of the function I uses the set building quantor, which describes an infinite non-algorithmic process in this case.

A second solution can be 'constructed' in the following way: At first one defines

$$\mathrm{M}(F) := \{s \in \mathrm{L}(\mathrm{I}(F)) \,|\, \nexists t \in \mathrm{L}(\mathrm{I}(F))(t \neq s \wedge t|s)\} \ .$$

Owing to Dixon's lemma, $\mathrm{M}(F)$ is always finite. Let now S be a function of choice, which has the following property

$$\forall t \in \mathrm{M}(F)(\mathrm{S}(F,t) \in \mathrm{I}(F) \wedge t = \mathrm{L}(\mathrm{S}(F,t))) \ .$$

Then

$$G := \{S(F,t) \,|\, t \in M(F)\}$$

has the required properties. For the proof note that the highest power product of a polynomial $f \in I(F)$ is always a multiple of the highest power product of a polynomial in G. Thus, by subtracting a suitable multiple of a polynomial in G, the polynomial f can be reduced to a polynomial in an ideal with a lower highest power product. Since allowed orders are Noetherian, f can be reduced to zero in finitely many steps by using polynomials in G.

This solution of the problem is still prompt (i.e. producible in a few steps of thinking) and also correct, but it is already much more 'useful' in the sense that one knows at least that the constructed G must be always finite (which gives Hilbert's basis theorem as a corollary after all). But still the solution is 'not really useful', since, even in the case of a finite F, the intermediate steps for constructing G use a lot of 'infinite' operations (the construction of $I(F)$, the $\exists$-quantor with an infinite range and finally the function of choice S), which cannot be executed algorithmically.

A third solution, which is 'really useful' (i.e. which yields a suitable G for every arbitrary F in a finite number of algorithmic steps) needs a much more complicated proof (thus many more steps of thinking) with additional mathematical ideas (concepts), which are not included in the structure above, see [1]. And only with the complete algorithmic solution of the construction problem of Gröbner bases will all the many other fundamental problems of algebraic geometry (theory of ideals of polynomials) for example the construction of syzygies, the complete solution of algebraic equation systems, the problem of implicitization, the problem of inverting polynomial maps, etc. be algorithmically solvable. Even more theory is necessary if one wants to construct Gröbner bases efficiently, this means with the least possible effort. There are dozens of paper about this topic. This means: The more algorithmically and then the more efficiently one likes to solve mathematical problems, more mathematical theory and the more difficult proofs become necessary and not the opposite.

References

[1] B. Buchberger. An Introduction to Gröbner Bases. In B. Buchberger, F. Winkler, editors, *Gröbner Bases and Applications*. Cambridge University Press, 1998, pp. 3-31.

[2] F. Chyzak, P. Paule, O. Scherzer, A. Schoisswohl, B. Zimmermann. The Construction of Orthonormal Wavelets Using Symbolic Methods and a Matrix Analytical Approach for Wavelets on the Interval. *Experimental Mathematics*, 10(1): 67 – 86, 2001.

[3] B. Buchberger. Should Students Learn Integration Rules? *ACM SIGSAM Bulletin*, 24(1):10–17, 1990.