Opinion

The Opinion column offers mathematicians the opportunity to write about any issue of interest to the international mathematical community. Disagreement and controversy are welcome. The views and opinions expressed here, however, are exclusively those of the author and neither the publisher nor the editor-in-chief endorses or accepts responsibility for them. An Opinion should be submitted to the editor-in-chief, Chandler Davis.

Theorems for a Price: Tomorrow's Semi-Rigorous Mathematical Culture

Doron Zeilberger[1]

Today

The most fundamental precept of the mathematical faith is *thou shalt prove everything rigorously*. While the practitioners of mathematics differ in their views of what constitutes a rigorous proof, and there are fundamentalists who insist on even a more rigorous rigor than the one practiced by the mainstream, the belief in this principle could be taken as the *defining property* of *mathematician*.

The Day After Tomorrow

There are writings on the wall that, now that the silicon savior has arrived, a new testament is going to be written. Although there will always be a small group of "rigorous" old-style mathematicians (e.g., [Ref. 1]) who will insist that the true religion is theirs and that the computer is a false Messiah, they may be viewed by future mainstream mathematicians as a fringe sect of harmless eccentrics, as mathematical physicists are viewed by regular physicists today.

The computer has already started doing to mathematics what the telescope and microscope did to astronomy and biology. In the future not all mathematicians will care about absolute certainty, since there will be so many exciting new facts to discover: mathematical pulsars and quasars that will make the Mandelbrot set seem like a mere Galilean moon. We will have (both human and machine[2]) professional *theoretical* mathematicians, who will develop conceptual paradigms to make sense out of the empirical data and who will reap Fields medals along

Doron Zeilberger (with l. to r. Celia, Tamar, Hadas)

Doron Zeilberger, (1950– ; Ph.D., 1976, Weizmann Inst.) is (almost) a fourth-generation Ph.D. His father, Yehuda H. Zeilberger (1915–1994; expected Ph.D. 1995, Geneva) interrupted his dissertation work on education at the University of Geneva in 1946, resumed it in 1985, after retiring, and expected to complete a thesis by 1995. Unfortunately, he died unexpectedly in 1994. The author's maternal grandfather, Paul Alexander (1870–1944; Dr.phil. 1897, Leipzig) was an industrial chemist and entrepreneur who invented and applied a process for recycling rubber. His great-grandfather (Paul's father-in-law), Adolf Pinner (1842–1912; Dr.phil. 1867, Berlin), was Professor of Chemistry in Berlin. His many contributions include a detailed study of nicotine.

[1] Supported in part by the NSF. Based in part on a Colloquium talk given at Rutgers University. Reprinted from "Theorems for a Price: Tomorrow's Semi-Rigorous Mathematical Culture", by Doron Zeilberger, *Notices of the American Mathematical Society*, Volume 40, Number 8, October 1993, pp. 978–981, by permission of the American Mathematical Society.

with (human and machine) *experimental* mathematicians. Will there still be a place for *mathematical* mathematicians?

This will happen after a transitory age of *semi-rigorous mathematics* in which identities (and perhaps other kinds of theorems) will carry price tags.

A Taste of Things to Come

To get a glimpse of how mathematics will be practiced in the not-too-distant future, I will describe the case of algorithmic proof theory for *hypergeometric identities* (Refs. [11], [13], [WZ1], [WZ2], [Z1], [Z2], [Z3], [Z4], [Ca]). In this theory one may rigorously prove, or refute, any conjectured identity belonging to a wide class of identities, which includes most of the identities between the classical special functions of mathematical physics.

Any such identity is proved by exhibiting a *proof certificate* that reduces the proof of the given identity to that of a finite identity among rational functions, and hence, by clearing denominators, to one between specific polynomials.

This algorithm can be performed successfully on all "natural identities" of which we are now aware. It is easy, however, to concoct artificial examples for which the running time and memory are prohibitive. Undoubtedly, in the future, "natural" identities will be encountered whose complete proof will turn out to be not worth the money. We will see later how, in such cases, one can get "almost certainty" with a tiny fraction of the price along with the assurance that, if we robbed a bank, we would be able to know for sure.

This is vaguely reminiscent of *transparent proofs* introduced recently in theoretical computer science [4–6]. The result that there exist short theorems having arbitrarily long proofs, a consequence of Gödel's incompleteness theorem, also comes to mind [7].[3] I speculate that similar developments will occur elsewhere in mathematics and will "trivialize" large parts of mathematics by reducing mathematical truths to routine, albeit possibly very long and exorbitantly expensive to check, *"proof certificates."* These proof certificates would also enable us, by plugging in random values, to assert "probable truth" very cheaply.

Identities

Many mathematical theorems are *identities*, statements of type "=", which take the form $A = B$. Here is a sample, in roughly an increasing order of sophistication.

1. $2 + 2 = 4$.
2. $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$.
3. $\sin(x+y) = \sin(x)\cos(y) + \cos(x)\sin(y)$.
4. $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$.
5. $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$.
6. $\sum_{k=-n}^{n} (-1)^k \binom{2n}{n+k}^3 = \binom{3n}{n}$.
7. Let $(q)_r := (1-q)(1-q^2)\cdots(1-q^r)$; then

$$\sum_{r=0}^{n} \frac{q^{r^2}}{(q)_r (q)_{n-r}} = \sum_{r=-n}^{n} \frac{(-1)^r q^{(5r^2-r)/2}}{(q)_{n-r}(q)_{n+r}}.$$

7′. Let $(q)_r$ be as in 7; then

$$\sum_{r=0}^{\infty} \frac{q^{r^2}}{(q)_r} = \prod_{i=0}^{\infty} (1-q^{5i+1})^{-1}(1-q^{5i+4})^{-1}.$$

8. Let H_n be given by

$$H_n = H_n(q) = \frac{(1+q)}{(1-q)} \frac{(1+q^2)}{(1-q^2)} \cdots \frac{(1+q^n)}{(1-q^n)};$$

then

$$\left(\sum_{k=0}^{n} \frac{2(-q^{n+1})^k}{1+q^k} H_k \right)^4 \sum_{k=-n}^{n} \frac{4(-q)^k}{(1+q^k)^2} \frac{H_{n+k}}{H_n} \frac{H_{n-k}}{H_n} = \left(\sum_{k=-n}^{n} (-q)^{k^2} \right)^4.$$

8′. $$\left(\sum_{k=-\infty}^{\infty} q^{k^2} \right)^4 = 1 + 8 \sum_{k=1}^{\infty} \frac{q^k}{(1+(-q)^k)^2}.$$

9. Analytic Index = Topological Index.
10. $\mathrm{Re}(s) = \frac{1}{2}$ for every nonreal s such that $\zeta(s) = 0$.

All the identities are trivial, except possibly the last two, which I think quite likely will be considered trivial in 200 years. I will now explain.

Why Are the First Eight Identities Trivial?

The **first** identity, while *trivial* nowadays, was very deep when it was first discovered, independently, by several anonymous cave dwellers. It is a general abstract theorem that contains, as special cases, many apparently unrelated theorems—Two Bears and Two Bears Make Four Bears, Two Apples and Two Apples Make Four Apples, etc. It was also realized that, in order to prove it rigorously, it suffices to prove it for any one special case, say, marks on the cave's wall.

[2] For example, my computer Shalosh B. Ekhad and its friend Sol Tre already have a nontrivial publication list, e.g., Refs. 2 and 3.

[3] Namely, the ratio (proof length)/(theorem length) grows fast enough to be nonrecursive. Adding an axiom can shorten proofs by recursive amounts [8, 9].

The **second** identity, $(a+b)^3 = a^3+3a^2b+3ab^2+b^3$, is one level of generality higher. Taken literally (in the semantic sense of the word *literally*), it is a fact about *numbers*. For any specialization of a and b we get yet another correct numerical fact, and as such it requires a "proof," invoking the commutative, distributive, and associative "laws." However, it is completely routine when viewed *literally*, in the syntactic sense, i.e., in which a and b are no longer symbols denoting numbers but rather represent themselves, qua (commuting) literals. This shift in emphasis roughly corresponds to the transition from *Fortran* to *Maple*, i.e., from *numeric* computation to *symbolic* computation.

Identities **3** and **4** can be easily embedded in classes of routinely verifiable identities in several ways. One way is by defining $\cos(x)$ and $\sin(x)$ by $(e^{ix}+e^{-ix})/2$ and $(e^{ix}-e^{-ix})/(2i)$ and the Fibonacci numbers F_n by Binet's formula.

Identities **5–8** were, until recently, considered genuine nontrivial identities, requiring a human demonstration. One particularly nice human proof of **6** was given by Cartier and Foata [10]. A one-line computer-generated proof of identity **6** is given in [2]. Identities **7** and **8** are examples of so-called *q-binomial coefficient identities* (a.k.a. *terminating q-hypergeometric series*). All such identities are now routinely provable [11] (see below). The machine-generated proofs of **7** and **8** appear in [3] and [12], respectively. Identities **7** and **8** immediately imply, by taking the limit $n\to\infty$, identities **7′** and **8′**, which in turn are equivalent to two famous number-theoretic statements: The first Rogers–Ramanujan identity, which asserts that the number of partitions of an integer into parts that leave remainder 1 or 4 when divided by 5 equals the number of partitions of that integer into parts that differ from each other by at least 2; and Jacobi's theorem which asserts that the number of representations of an integer as a sum of 4 squares equals 8 times the sum of its divisors that are not multiples of 4.

The WZ Proof Theory

Identities **5–8** involve sums of the form

$$\sum_{k=0}^{n} F(n,k), \qquad \text{(sum)}$$

where the summand, $F(n,k)$, is a *hypergeometric term* (in **5** and **6**) or a *q-hypergeometric term* (in **7** and **8**) in both n and k, which means that both quotients, $F(n+1,k)/F(n,k)$ and $F(n,k+1)/F(n,k)$, are *rational functions* of (n,k) $[(q^n\, q^k,\, q)$, respectively].

For such sums and multisums we have [11] the following result.

THE FUNDAMENTAL THEOREM OF ALGORITHMIC HYPERGEOMETRIC PROOF THEORY. Let $F(n;k_1,\ldots,k_r)$ be a *proper* (see [11]) hypergeometric term in all of $(n;k_1,\ldots,k_r)$. Then there exist polynomials $p_0(n),\ldots,p_L(n)$ and rational functions $R_j(n;k_1,\ldots,k_r)$ such that $G_j := R_jF$ satisfies

$$\sum_{i=0}^{L} p_i(n)F(n+i;k_1,\ldots,k_r) = \sum_{j=1}^{r}[G_j(n;k_1,\ldots,k_j+1,\ldots,k_r) - G_j(n;k_1,\ldots,k_j,\ldots,k_r)]. \qquad \text{(multiWZ)}$$

Hence, if for every specific n, $F(n;-)$ has compact support in $(k_1,\ldots,k_r)$, the definite sum $g(n)$ given by

$$g(n) := \sum_{k_1,\ldots,k_r} F(n;k_1,\ldots,k_r) \qquad \text{(multisum)}$$

satisfies the linear recurrence equation with polynomial coefficients:

$$\sum_{i=0}^{L} p_i(n)g(n+i) = 0. \qquad (P\text{-recursive})$$

(P-recursive) follows from (multiWZ) by summing over $\{k_1,\ldots,k_r\}$ and observing that all the sums on the right telescope to zero.

If the recurrence happens to be first-order, i.e., $L=1$ above, then it can be written in *closed form*: For example, the solution of the recurrence $(n+1)g(n)-g(n+1)=0$, $g(0)=1$, is $g(n)=n!$.

This "existence" theorem also implies an algorithm for finding the recurrence (i.e., the p_i) and the accompanying certificates R_j (see below).

An analogous theorem holds for q-hypergeometric series [13, 14].

Since we know how to find and prove the recurrence satisfied by any given hypergeometric sum or multisum, we have an effective way of proving any equality of two such sums or the equality of a sum with a conjectured sequence. All we have to do is check whether both sides are solutions of the same recurrence and match the appropriate number of initial values. Furthermore, we can also use the algorithm to find new identities. If a given sum yields a first-order recurrence, it can be solved, as mentioned above, and the sum in question turns out to be explicitly evaluable. If the recurrence obtained is of higher order, then most likely the sum is not explicitly evaluable (in closed form), and Petkovsek's algorithm [15], which decides whether a given linear recurrence (with polynomial coefficients) has *closed form* solutions, can be used to find out for sure.

Almost Certainty for an ϵ of the Cost

Consider identity (multisum) once again, where $g(n)$ is "nice." Dividing through by $g(n)$ and letting $F\to F/g$, we can assume that we have to prove an identity of the form

$$\sum_{k_1,\dots,k_r} F(n;k_1,\dots,k_r) = 1. \qquad \text{(Nice)}$$

The WZ theory promises that the left side satisfies some linear recurrence, and if the identity is indeed true, then the sequence $g(n) = 1$ should be a solution (in other words, $p_0(n) + \cdots + p_L(n) \equiv 1$). For the sake of simplicity let us assume that the recurrence is minimal, i.e., $g(n+1) - g(n) = 0$. (This is true anyway in the vast majority of the cases.) To prove the identity by this method, we have to find *rational functions* $R_j(n;k_1,\dots,k_r)$ such that $G_j := R_jF$ satisfies

$$F(n+1;k_1,\dots,k_r) - F(n;k_1,\dots,k_r) = \sum_{j=1}^{r} [G_j(n;k_1,\dots,k_j+1,\dots,k_r) - G_j(n;k_1,\dots,k_j,\dots,k_r)]. \qquad \text{(multiWZ}')$$

By dividing (multiWZ′) through by F and clearing denominators, we get a certain functional equation for the $R_1,\dots,R_r$, from which it is possible to determine their denominators $Q_1,\dots,Q_r$. Writing $R_j = P_j/Q_j$, the proof boils down to finding *polynomials* $P_j(k_1,\dots,k_r)$ with coefficients that are rational functions in n and possibly other (auxiliary) parameters. It is easy to predict upper bounds for the degrees of the P_j in $(k_1,\dots,k_r)$. We then express each P_j symbolically with "undetermined" coefficients and substitute into the above-mentioned functional equation. We then expand and equate coefficients of all monomials $k_1^{a_1}\dots k_r^{a_r}$ and get an (often huge) system of inhomogeneous linear equations with *symbolic* coefficients. The proof comes down to proving that this inhomogeneous system of linear equations has a solution. It is very time-consuming to solve a system of linear equations with *symbolic* coefficients. By plugging in specific values for n and the other parameters if present, one gets a system with *numerical* coefficients, which is much faster to handle. Since it is unlikely that a random system of inhomogeneous linear equations with more equations than unknowns can be solved, the solvability of the system for a number of special values of n and the other parameters is a very good indication that the identity is indeed true. It is a waste of money to get absolute certainty, unless the conjectured identity in question is known to imply the Riemann Hypothesis.

Semi-Rigorous Mathematics

As wider classes of identities, and perhaps even other kinds of classes of theorems, become routinely provable, we might witness many results for which we would know how to find a proof (or refutation); but we would be unable or unwilling to pay for finding such proofs, since "almost certainty" can be bought so much cheaper. I can envision an abstract of a paper, c. 2100, that reads, "We show in a certain precise sense that the Goldbach conjecture is true with probability larger than 0.99999 and that its complete truth could be determined with a budget of $10 billion."

It would then be acceptable to rely on such a priced theorem, provided that the price is stated explicitly. Whenever statement A, whose price is p, and statement B, whose price is q, are used to deduce statement C, the latter becomes a priced theorem priced at $p + q$.

If a whole chain of boring identities would turn out to imply an interesting one, we might be tempted to redeem all these intermediate identities; but we would not be able to buy out the whole store, and most identities would have to stay unclaimed.

As absolute truth becomes more and more expensive, we would sooner or later come to grips with the fact that few nontrivial results could be known with old-fashioned certainty. Most likely we will wind up abandoning the task of keeping track of price altogether and complete the metamorphosis to nonrigorous mathematics.

Note: *Maple* programs for proving hypergeometric identities are available by anonymous ftp to `math.temple.edu` in directory `pub/zeilberger/programs`. A *Mathematica* implementation of the single-summation program can be obtained from Peter Paule at `paule@risc.uni-linz.ac.at`.

References

1. A. Jaffe and F. Quinn, "Theoretical mathematics": *Toward a cultural synthesis of mathematics and theoretical physics*, Bull. Amer. Math. Soc. (N.S.) **29** (1993), 1–13.
2. S.B. Ekhad, *A very short proof of Dixon's theorem*, J. Combin. Theory Ser. A **54** (1990), 141–142.
3. S. B. Ekhad and S. Tre, *A purely verification proof of the first Rogers-Ramanujan identity*, J. Combin. Theory Ser. A **54** (1990), 309–311.
4. B. Cipra, *Theoretical computer scientists develop transparent proof techniques*, SIAM News **25** (May 1992).
5. S. Arora, C. Lund, R. Motwani, M. Sudan, and M. Szegedy, *Proof verification and intractability of approximation problems*, Proc. 33rd Symp. on Foundations of Computer Science (FOCS), IEEE Computer Science Press, Los Alamos, 1992, pp. 14–23.
6. S. Arora and M. Safra, *Probabilistic checking of proofs*, ibid, pp. 2–13.
7. J. Spencer, *Short theorems with long proofs*, Amer. Math. Monthly **90** (1983), 365–366.
8. K. Gödel, *On length of proofs*, Ergeb. Math. Colloq. **7** (1936), 23–24, translated in *The Undecidable* (M. Davis, Ed.), Raven Press, Hewitt, NY, 1965, pp. 82–83.
9. J. Dawson, *The Gödel incompleteness theorem from a length of proof perspective*, Amer. Math. Monthly **86** (1979), 740–747.
10. P. Cartier and D. Foata, *Problèmes combinatoires de commutation et réarrangements*, Lecture Notes in Math. **85**, Springer, 1969.

Continued on page 76

not enough of others. I was pleased with the considerable attention paid to probability and statistics, in comparison with other general histories. But Katz's treatment of twentieth-century mathematics is sketchy, emphasizing only set theory, its problems and paradoxes; topology; new ideas in algebra; and computers and applications. And some will think that, though three good chapters treat the nineteenth century, the importance of the century and the sheer amount of its mathematics are underrepresented. There are some minor errors, some typographical, some of emphasis. One supposedly useful feature of the book is the breaking up of each chronological chapter into topics, so that a teacher can emphasize, say, the history of equation-solving from ancient Egypt and Babylonia, Greece, China, Islam, up to Abel, Gauss, and Galois. These divisions sometimes make the narrative seem choppy.

Students found the book "challenging" (that means not easy); they also found it interesting to read. Readers may agree with some of my students who found the book too long and felt that often one couldn't see the forest for the trees. Here one must remember that Katz is writing a textbook. The mathematical demands on the student reader must remain finite. An excellent, much briefer work is Struik's *Concise History* [3]. Still, the history of mathematics is sufficiently tangled that one welcomes Katz's attention to specifics. Readers wanting a more detailed account of nineteenth- and twentieth-century topics can consult the general works by Carl Boyer (in the edition updated by Uta C. Merzbach) and Morris Kline, or the many items in Katz's full bibliography on specific topics.

The most serious criticism one can make is that Katz's coverage reflects the limitations of twentieth-century scholarship. One might think this is good in that Katz's scholarship is up-to-date and the materials this scholarship addresses are important. However, because the book is not itself one of path-breaking scholarship, it shares many of the emphases and the omissions of the existing literature. Much remains to be studied. Important questions like whether ibn al-Haytham's formulas or the Islamic and Jewish work on induction influenced their (re)discoverers in Europe, whether the medieval Chinese or Indian "Pascal" triangles influenced Pascal, whether seventeenth-century mathematicians knew, directly or indirectly, the Indian work on trigonometric series (such as the arctangent series above), have recently been the subject of much speculation. Equally important questions about Cauchy's use of infinitesimals or Leibniz's philosophy are not yet settled. Readers with unanswered queries must await another decade of research.

In the meantime, Victor J. Katz should be congratulated on having produced an excellent and readable text, based on sound scholarship and attractively presented. A mathematician could appropriately put this book on the family coffee table, but would be even better advised to read the many fascinating things it contains. I will enthusiastically use it again when I next teach the history of mathematics.

References

1. Carl B. Boyer and Uta C. Merzbach, *A History of Mathematics*. New York, Wiley, 1989.
2. Morris Kline, *Mathematical Thought from Ancient to Modern Times*. New York, Oxford, 1972.
3. Dirk J. Struik, *A Concise History of Mathematics*. 4th Edition. New York, Dover, 1967.

Pitzer College
Claremont, CA 91711-6110
USA

Zeilberger *Continued from page 14*

11. H. S. Wilf and D. Zeilberger, *An algorithmic proof theory for hypergeometric (ordinary and "q") multisum/integral identities*, Invent. Math. **108** (1992), 575–633.
12. G. E. Andrews, S. B. Ekhad, and D. Zeilberger, *A short proof of Jacobi's formula for the number of representations of an integer as a sum of four squares*, Amer. Math. Monthly **100** (1993), 274–276.
13. H. S. Wilf and D. Zeilberger, *Rational functions certify combinatorial identities*, J. Amer. Math. Soc. **3** (1990), 147–158.
14. T. H. Koornwinder, *Zeilberger's algorithm and its q-analogue*, Univ. of Amsterdam, preprint.
15. M. Petkovsek, *Hypergeometric solutions of linear recurrence equations with polynomial coefficients*, J. Symbolic Comput. **14** (1992), 243–264.

[AZ] G. Almkvist and D. Zeilberger, *The method of differentiating under the integral sign*, J. Symbolic Comput. **10** (1990), 571–591.

[Ca] P. Cartier, *Démonstration "automatique" d'identités et fonctions hypergéometriques* [d'apres D. Zeilberger], Séminaire Bourbaki, exposé no. 746, Astérisque **206** (1992), 41–91.

[WZ1] H. S. Wilf and D. Zeilberger, *Towards computerized proofs of identities*, Bull. Amer. Math. Soc. (N.S.) **23** (1990), 77–83.

[WZ2] ———, *Rational function certification of hypergeometric multi-integral/sum/"q" identities*, Bull. Amer. Math. Soc. (N.S.) **27** (1992) 148–153.

[Z1] D. Zeilberger, *A holonomic systems approach to special functions identities*, J. Comput. and Appl. Math. **32** (1990), 321–368.

[Z2] ———, *A fast algorithm for proving terminating hypergeometric identities*, Discrete Math. **80** (1990), 207–211.

[Z3] ———, *The method of creative telescoping*, J. Symbolic Comput. **11** (1991), 195–204.

[Z4] ———, *Closed form (pun intended!)*, Special volume in memory of Emil Grosswald, (M. Knopp and M. Sheingorn, eds.), Contemp. Math. vol. 143, Amer. Math. Soc., Providence, RI, 1993, pp. 579–607.

Department of Mathematics
Temple University
Philadelphia, PA 19122 USA
e-mail:zeilberg@math.temple.edu

The Death of Proof? Semi-Rigorous Mathematics? You've Got to Be Kidding!

George E. Andrews[1]

Introduction

Through the summer of 1993 I was desperately clinging to the belief that mathematics was immune from the giddy relativism that has pretty well destroyed a number of disciplines in the university. Then came the October *Scientific American* and John Horgan's article, "The death of proof" [H]. The theme of this article is that computers have changed the world of mathematics forever, in the process making proof an anachronism. Oh well, all my friends said, Horgan is a nonmathematician who got in way over his head. Apart from his irritating comments and obvious slanting of the material, "The death of proof" actually contains interesting descriptions of a number of important mathematics projects. Indeed, as W. Thurston has said, [T] "A more appropriate title would have been 'The Life of Proof.' "

Semi-Rigorous Mathematics

Then came the October *Notices of the A. M. S.* and an article [Z2] by my friend and collaborator Doron Zeilberger: "Theorems for a price: tomorrow's semi-rigorous mathematical culture" [reprinted above—Editor]. The theme of this article is reasonably summarized by the following quote:

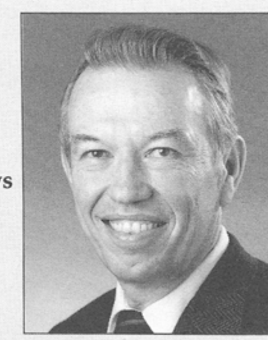
> There are writings on the wall that, now that the silicon savior has arrived, a new testament is going to be written. Although there will always be a small group of 'rigorous' old-style mathematicians . . . , they may be viewed by future mainstream mathematicians as a fringe sect of harmless eccentrics . . . In the future not all mathematicians will care about absolute certainty, since there will be so many exciting new facts to discover . . . As absolute truth becomes more and more expensive, we would sooner or later come to grips with the fact that few nontrivial results could be known with old-fashioned certainty. Most likely we will wind up abandoning the task of keeping track of price altogether and complete the metamorphosis to nonrigorous mathematics.

The Evidence?

Unlike Horgan, Zeilberger is a first-rate mathematician. Thus one expects that his futurology is based on firm ground. So what is his evidence for this *paradigm shift*? It was at this point that my irritation turned to horror. In a list of identities used to back up his predictions, he lists two intimately related to me, and it is these which turn out to be the star witnesses in his case.

To present his argument fairly, let us refer to his 10 identities, of which he says, "All the above identities are

George E. Andrews



George Andrews received his Ph.D. at the University of Pennsylvania in 1964. He was the late Professor Hans Rademacher's last student and is currently Evan Pugh Professor of Mathematics at the Pennsylvania State University. He has spent leaves of absence at the I.B.M. T. J. Watson Research Center, the University of Waterloo, the University of Minnesota, MIT, the University of Wisconsin, the University of New South Wales, the Australian National University, and the University of Strasbourg. He has published extensively on the theory of partitions and related areas of mathematics. His most recent book is *q-Series*, a monograph derived from his Regional Conference Lectures at Arizona State University in 1985. He was the J. S. Frame $\pi\mu\varepsilon$ lecturer in 1993, and he received the Distinguished University Teaching Award from the Allegheny Mountain Section of the Mathematics Association of America.

[1] Partially supported by National Science Foundation Grant DMS 8702695-04.

trivial, except possibly the last two, which I think quite likely will be considered trivial in two hundred years." Your guess is as good as mine why 9 and 10 will be trivial in 200 years.

He then focuses on 1–8. Identities 1–5 are pre-eighteenth-century. It is quite true that these theorems are easy to prove once you know how — many theorems are. However, at least for 3–8, their proofs yield insights well beyond the bare statements of the identities. Consequently if we regard them as merely results to be verified or turned up by computer, we are incurring a staggering loss of insight. Don't worry, Zeilberger assures us: "We will have (both human and machine) professional *theoretical* mathematicians, who will develop conceptual paradigms to make sense out of the empirical data and who will reap Fields medals along with (human and machine) *experimental* mathematicians."

And what is the evidence for this? Zeilberger tells us, "For example, my computer Shalosh B. Ekhad and its friend Sol Tre already have a nontrivial publication list, e.g., [E], [ET]."

But there is a problem here. While the computer has indeed generated proofs of 1–8, it discovered none of the identities. The two most recent theorems on the list are 7 ([A1], [B], [ET]) and 8 [AEZ]. The actual discovery of 7 [A1] was from an examination of G. N. Watson's massive general identity [Wa] that he used to prove the Rogers-Ramanujan identities (i.e., 7′). Surely one can argue that Watson's proof of his theorem is as trivial as Zeilberger's computer's proof of 7; the main observation used by Watson is that a polynomial with more zeroes than degree is identically zero. However, Watson's identity has spawned both new discoveries and new research that reach way beyond its original purposes.

The actual discovery of 8 [AEZ: p. 276] was from an examination of Jackson's q-analog [J] of Dougall's theorem [Do]. Again a result proved originally by the old game of exhibiting too many zeroes of a polynomial.

On this account, then, what exactly is the contribution of Zeilberger and his computer? Very simply, he has made a substantial contribution to proving identities, i.e., to rigorous mathematics. He and Herb Wilf [WZ], [Z1] have found an algorithm which can be implemented on the computer and which will produce rigorous proofs of numerous identities of which 7 and 8 are prototypical examples.

A natural response is that the computer can be programmed using Zeilberger's algorithms to find new identities also. Indeed, Wilf spoke on this very topic in a talk [Wi] entitled "Billions and billions of combinatorial identities." Therein lies another difficulty. Which among these "billions and billions" are really important? Which are just mild changes of variable in classical results? Which are sterile in their relation to the rest of mathematics? Ira Gessel [G] has undertaken a serious study of the possibilities; but it is not clear that he has produced answers to these questions yet.

The Insight of Proof

Ignored completely in Zeilberger's futurology is the insight provided by proof.

"In the future," says Zeilberger, "not all mathematicians will care about absolute certainty, since there will be so many exciting new facts to discover."

Let us consider an example of an exciting new fact described by J. and P. Borwein and K. Dilcher [BBD; p. 681]:

> Gregory's series for π, truncated at 500,000 terms, gives to forty places
>
> $$4\sum_{k=1}^{500{,}000}\frac{(-1)^{k-1}}{2k-1} = 3.14159\underline{0}65358979324\underline{04}6264338326\underline{9}502884197.$$
>
> The number on the right is not π to forty places. As one would expect, the 6th digit after the decimal is wrong. The surprise is that the next 10 digits are correct. In fact, only the 4 underlined digits aren't correct. This intriguing observation was sent to us by R. D. North . . . of Colorado Springs with a request for an explanation.

Well, there it is: a computer-discovered, exciting, mathematical fact! Who among us would respond to this observation by saying, "Great! Now let's go discover some other exciting new fact"? Surely anyone who has applied the alternating series test in a calculus class to show that, for example, the above error in Gregory's series occurs at the sixth decimal must indeed be intrigued by the astounding accuracy of 30 of the next 33 terms, and would want to stop and explain it! What can the computer tell us about this phenomenon? Only what it already has! I do not mean to minimize its contribution. No one could make the above evaluation without a computer. But *that is it* for the computer. Fortunately for us, that was *not* it for Dilcher and the Borweins. They provide in the remainder of [BBD] absolute certainty about what is going on, and they provide concomitantly great insight and, dare I say it, beauty. Their paper is an almost perfect example of the computer aiding crucially in the discovery of facts but not in their proof — and not in the perception that they cried out for proof.

Conclusion

Zeilberger has proved some breathtaking theorems [ZB], [Z3], and his W–Z method (joint with Wilf [WZ]) has been a godsend to me [A2] and an inspiration [A3]. However, there is not one scintilla of evidence in his accomplishments to support the coming ". . . metamorphosis to nonrigorous mathematics."

Until Zeilberger can provide identities which are (1) discovered by his computer, (2) important to some mathematical work external to pure identity tracking, and (3) too complicated to allow an actual proof using his algorithm, then he has produced exactly no evidence that his Brave New World is on its way.

I regret feeling compelled to write this article. Unfortunately articles on why rigorous mathematics is dead create unintended side effects. We live in an age of rampant "educational reform." Many proponents of mathematics education reform impugn the importance of proofs, and question whether there are right answers, etc. A wonderfully sane account of these problems has been given by H.-H. Wu [Wu1], [Wu2]. A much more disturbing account "Are proofs in high school geometry obsolete?" concludes Horgan's article [H]. It is a disservice to mathematics inadvertently to provide unfounded ammunition for the epistemological relativists.

If anyone reading this believes the last paragraph is rubbish because attempts (unknown to me) are currently underway to insert the Continuum Hypothesis or the Theory of Large Cardinals into the NCTM Standards for School Mathematics, please don't write to tell me about them. I can take only so many shocks to my system.

Finally, wisdom suggests that grand predictions of life in 2193 ought to be treated with scepticism. ("Next Wednesday's meeting of the Precognition Society has been postponed due to unforeseen circumstances.") A long-overdue analysis of some of our current prophets has been attempted by Max Dublin [Du]. Especially noteworthy is Dublin's Chapter 5, "Futurehype in Education." I won't give the plot away, but I recall the words of Claude Rains near the end of *Casablanca*: "Round up the usual suspects!"

References

[A1] G. E. Andrews, *Problem 74-12*, SIAM Review **16** (1974), 390.

[A2] G. E. Andrews, *Plane partitions V: the T.S.S.C.P.P. conjecture*, J. Combin. Theory Ser. A **66** (1994), 28–39.

[A3] G. E. Andrews, *Schur's theorem, Capparelli's conjecture and q-trinomial coefficients*, Contemp. Math. (in press).

[AEZ] G. E. Andrews, S. B. Ekhad and D. Zeilberger, *A short proof of Jacobi's formula for the number of representations of an integer as a sum of four squares*. Amer. Math. Monthly **100** (1993), 274–276.

[BBD] J. M. Borwein, P. B. Borwein and K. Dilcher, *Pi, Euler numbers, and asymptotic expansions*. Amer. Math. Monthly **96** (1989), 681–687.

[B] D. M. Bressoud, *Solution to Problem 74–12*. SIAM Review **23** (1981), 101–104.

[Do] J. Dougall, *On Vandermonde's theorem and some more general expansions*, Proc. Edinburgh Math. Soc. **25** (1907), 114–132.

[Du] M. Dublin, *Futurehype. The Tyranny of Prophecy*, Viking (the Penguin Group), London and New York, 1989.

[E] S. B. Ekhad, *A very short proof of Dixon's theorem*, J. Combin. Theory Ser. A **54** (1990), 141–142.

[ET] S. B. Ekhad and S. Tre, *A purely verification proof of the first Rogers-Ramanujan identity*, J. Combin. Theory Ser. A **54** (1990), 309–311.

[G] I. Gessel, *Finding identities with the WZ method*, talk presented at the ACSyAM Workshop on Symbolic Computation in Combinatorics at MSI/Cornell University, September 21–24, 1993.

[H] J. Horgan, *The death of proof*, Scientific American **269** (1993), no. 4, 74–103.

[J] F. H. Jackson, *Summation of q-hypergeometric series*, Mess. Math. **50** (1921), 101–112.

[T] W. Thurston, *Letter to the editor*, Scientific American **270** (1994), no. 1, 9.

[Wa] G. N. Watson, *A new proof of the Rogers-Ramanujan identities*, J. London Math. Soc. **4** (1930), 4–9.

[Wi] H. Wilf, *Billions and billions of combinatorial identities*, talk presented at Allerton Park in the Conference in Honor of Paul Bateman, April 25–27, 1989.

[WZ] H. Wilf and D. Zeilberger, *Rational functions certify combinatorial identities*, J. Amer. Math. Soc. **3** (1990), 147–158.

[Wu1] H.-H. Wu, *The role of open-ended problems in mathematics education*, The Journal of Mathematical Behavior (to appear).

[Wu2] H.-H. Wu, *The role of Euclidean geometry in high school*, The Journal of Mathematical Behavior (to appear).

[Z1] D. Zeilberger, *The method of creative telescoping*, J. Symbolic Computing **11** (1991), 195–204.

[Z2] D. Zeilberger, *Theorems for a price: tomorrow's semi-rigorous mathematical culture*, Notices of the A.M.S. **40** (1993), 978–981.

[Z3] D. Zeilberger, *The alternating sign matrix conjecture* (to appear).

[ZB] D. Zeilberger and D. Bressoud, *A proof of Andrews' q-Dyson conjecture*, Discrete Math. **54** (1985), 201–224.

Department of Mathematics
Pennsylvania State University
University Park, PA 16802 USA