Computer-Generated Proofs of Mathematical Theorems

David M. Bressoud
Macalester College

Glossary

algorithm
A recipe or set of instructions which, when followed precisely, will produce a desired result.
binomial coefficient
The binomial coefficient $\binom{n}{k}$ is the coefficient of x^k in the expansion of $(1+x)^n$. It counts the number of ways of choosing k objects from a set of n objects.
computer algebra system
A computer package that enables the computer to do symbolic computations such as algebraic simplification, formal differentiation, and indefinite integration.
Diophantine equation
An equation in several variables for which only integer solutions are accepted.
hypergeometric series
A finite or infinite summation, $1 + a_1 + \cdots + a_k + \cdots$, in which the first term is 1 and the ratio of successive summands, a_{k+1}/a_k, is a quotient of polynomials in k.
hypergeometric term
A function of, say, k that is the kth summand in a hypergeometric series.
proof certificate
A piece of information about a mathematical statement that makes it possible to prove the statement easily and quickly.
proper hypergeometric term
A function of two variables such as n and k which is of the form: a polynomial in n and k times $x^k y^n$ for some fixed x times a product of quotients of factorials of the form $(an + bk + c)!$ where a, b, and c are fixed integers.

rising factorial
A finite product of numbers in an arithmetic sequence with difference 1. It is written as $(a)_n = a(a+1)(a+2)\cdots(a+n-1)$.

In a computer-based proof, the computer is used as a tool to help guess what is happening, to check cases, to do the laborious computations that arise. The person who is creating the proof is still doing most of the work. In contrast, a computer-generated proof is totally automated. A person enters a carefully worded mathematical statement for which the truth is in doubt, hits the RETURN key, and within a reasonable amount of time the computer responds either that the statement is true or that it is false. A step beyond this is to have the computer do its own searching for reasonable statements that it can test.

Such fully automated algorithms for determining the truth or falsehood of a mathematical statement do exist. With Doron Zeilberger's program `EKHAD`, one can enter the statement believed or suspected to be correct. If it is true, the computer will not only tell you so, it is capable of writing the paper ready for submission to a research journal. Even the search for likely theorems has been automated. A good deal of human input is needed to set parameters within which one is likely to find interesting results, but computer searches for mathematical theorems are now a reality.

The possible theorems to which this algorithm can be applied are strictly circumscribed, so narrowly defined that there is still a legitimate question about whether this constitutes true computer-generated proof or is merely a powerful mathematical tool. What is not in question is that such algorithms are changing the kinds of problems that mathematicians need to think about.

1 The Ideal Versus Reality

1.1 What cannot be done

Mathematics is frequently viewed as a formal language with clearly established underlying assumptions or axioms and unambiguous rules for determining the truth of every statement couched in this language. In the early decades of the twentieth century, works such as Russell and Whitehead's *Principia Mathematica* attempted to describe all mathematics in terms of the formal language of logic. Part of the reason for this undertaking was the hope that it would lead to an algorithmic procedure for determining the truth of each mathematical statement. As the twentieth century progressed, this hope receded and finally vanished. In 1931, Kurt Gödel proved that no axiomatic system comparable to that of Russell and Whitehead could be used to determine the truth or falsehood of every mathematical statement. Every consistent system of axioms is necessarily incomplete.

One broad class of theorems deals with the existence of solutions of a particular form. Given the mathematical problem, the theorem either exhibits a solution of the desired type or states that no such solution exists. In 1900, as the tenth of his set of twenty-three problems, David Hilbert challenged the mathematical community:

> "Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers."

A well-known example of such a Diophantine equation is the Pythagorean equation, $x^2 + y^2 = z^2$, with the restriction that we only accept integer solutions such as $x = 3$, $y = 4$, and $z = 5$. Another problem of this type is Fermat's Last Theorem. This theorem asserts that no such positive integer solutions exist for the equation $x^n + y^n = z^n$ when n is an integer greater than or equal to 3. We know that the last assertion is correct, thanks to Andrew Wiles.

For a Diophantine equation, if a solution exists then it can be found in finite (though potentially very long) time just by trying all possible combinations of integers, but if no solution exists then we cannot discover this fact just by trying possibilities. A proof that there is no solution is usually very hard. In 1970, Yuri Matijasevič proved that Hilbert's algorithm could not exist. It is impossible to construct an algorithm that, for every Diophantine equation, is able to determine whether it does or does not have a solution.

There have been other negative results. Let E be an expression that involves the rational numbers, π, $\ln 2$, the variable x, the functions sine, exponential, and absolute value, and the operations of addition, multiplication, and composition. Does there exist a value of x where this expression is zero? As an example, is there a real x for which

$$e^x - \sin(\pi \ln 2) = 0?$$

For this particular expression the answer is "yes" because $\sin(\pi \ln 2) > 0$, but in 1968, Daniel Richardson proved that it is impossible to construct an algorithm that would determine in finite time whether or not, for every such E, there exists a solution to the equality $E = 0$.

1.2 What can be done

In general, the problem of determining whether or not a solution of a particular form exists is extremely difficult and cannot be automated. However, there are cases where it can be done. There is a simple algorithm that can be applied to each quadratic equation to determine whether or not it has real solutions and, if it does, to find them.

The fact that $x^2 - 4312x + 315 = 0$ has real solutions may not have been explicitly observed before now, but it hardly qualifies as a theorem. The theorem is the statement of the quadratic formula that sits behind our algorithm. The conclusion for this particular equation is simply an application of that theorem, a calculation whose relevance is based on the theory.

But as the theory advances and the algorithms become more complex, the line between a calculation and a theorem becomes less clear. The Risch algorithm is used by computer algebra systems to find indefinite integrals in Liouvillian extensions of difference fields. It can answer whether or not an indefinite integral can be written in a suitably defined closed form. If such a closed form exists, the algorithm will find it. Most people would still classify a specific application of this algorithm as a calculation, but it is no longer always so clear cut. Even definite integral evaluations can be worthy of being called theorems.

Freeman Dyson conjectured the following integral evaluation for positive integer z in 1962:

$$(2\pi)^{-n} \int_0^{2\pi} \cdots \int_0^{2\pi} \prod_{1 \le j < k \le n} \left| e^{i\theta_j} - e^{i\theta_k} \right|^{2z} \, d\theta_1 \cdots d\theta_n = \frac{(nz)!}{(z!)^n}.$$

Four proofs have since been published. Dyson's conjecture cannot be proven by the Risch or any other general integral evaluation algorithm because the dimension of the space over which the integral is taken is a variable, but its proof is now close to the boundary of what can be totally automated.

Most of this article will focus on the WZ-method developed by Wilf and Zeilberger in the early 1990s. Given a suitable hypergeometric series, the WZ-method will determine whether or not it has a closed form. If it does, the algorithm will find it. It can even be used to find new hypergeometric series that can be expressed in closed form. Again, the important mathematics is the theory that is used to create and justify the algorithm, but specific applications now look very much like theorems. One example of a result that can be proved by the WZ-method is the following identity, discovered and proved by J. C. Adams in the nineteenth century. Let $P_n(x)$ be the Legendre polynomial defined by

$$P_n(x) := \frac{1}{2^n} \sum_{k=0}^{n} \binom{n}{k}^2 (x-1)^k (x+1)^{n-k},$$

and let $A_k = \binom{2k}{k}$, then

$$\int_{-1}^{1} P_m(x) P_n(x) P_{m+n-2k}(x) \, dx = \frac{1}{(m+n+1/2-k)} \cdot \frac{A_k A_{m-k} A_{n-k}}{A_{m+n-k}}. \quad (1)$$

Note that the term-by-term integration is not difficult for a computer algebra system. What distinguishes this particular identity is that the number of terms in each summation is left as a variable.

Given a hypergeometric series, the WZ-method can be used to find the closed expression which it equals, provided such an expression exists. We take as an example

$$f(n) = \sum_{0 \le k \le n/3} 2^k \, \frac{n}{n-k} \binom{n-k}{2k}.$$

The algorithm produces a recursion satisfied by $f(n)$:

$$f(n+3) - 2f(n+2) + f(n+1) - 2f(n) = 0.$$

This is a particularly nice example because the coefficients are constants and standard techniques can be applied to discover that

$$\sum_{0 \le k \le n/3} 2^k \, \frac{n}{n-k} \binom{n-k}{2k} = 2^{n-1} + \frac{1}{2}(i^n + (-i)^n), \quad n \ge 2.$$

In general, the coefficients in the recursion will be polynomials in n. In 1991 Marko Petkovšek created an algorithm that will find a closed form solution for such a recursion, or prove that no such formula exists. The combination of the WZ-method with Petkovšek's algorithm gives an automated proof that a particular type of solution cannot exist, or else it finds such a solution. As an example, there is a computer-generated proof of the fact that

$$\sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2$$

cannot be written as a linear combination of hypergeometric terms in n.

The WZ-method combined with Petkovšek's algorithm is producing fully automated proofs of results that, until recently, have required considerable human ingenuity. Significantly, it replies not just with a statement that a particular identity is true, but also with a proof certificate, a critical insight that enables anyone with pencil and paper and a little time to verify that this identity is correct. At the very least, these algorithms have moved the line of demarcation between what constitutes a proof and what is only a computation.

2 Hypergeometric Series Identities

2.1 What is a Hypergeometric Series?

A series, $1 + a_1 + a_2 + a_3 + \cdots$, is called hypergeometric if the ratio of consecutive terms, a_{n+1}/a_n, is a rational function of n, say $a_{n+1}/a_n = P(n)/Q(n)$ where P and Q are polynomials. Most of the commonly encountered power series are hypergeometric or can be expressed in terms of hypergeometric series (see Figure 1). A hypergeometric term is a function of n that is a summand of a hypergeometric series indexed by n. In particular, a hypergeometric term is of the form

$$a_k = \prod_{n=0}^{k-1} \frac{a_{n+1}}{a_n} = \prod_{n=0}^{k-1} \frac{P(n)}{Q(n)},$$

Exponential function:

$$e^x = 1 + \sum_{n=1}^{\infty} \frac{x^n}{n!}, \qquad \frac{a_{n+1}}{a_n} = \frac{x}{n+1},$$

Sine function:

$$\sin x = x \left(1 + \sum_{n=1}^{\infty} \frac{(-1)^n x^{2n}}{(2n+1)!} \right), \qquad \frac{a_{n+1}}{a_n} = \frac{-x^2}{4(n+1)(n+3/2)},$$

Bessel function of the first kind:

$$J_k(x) = \frac{x^k}{\Gamma(k+1)} \left(1 + \sum_{n=1}^{\infty} \frac{(-1)^n x^{2n}}{4^n \, n! \, (k+1)_n} \right), \qquad \frac{a_{n+1}}{a_n} = \frac{-x^2}{4(n+1)(n+k+1)},$$

Error function:

$$\operatorname{erf}(x) = \frac{2x}{\sqrt{\pi}} \left(1 + \sum_{n=1}^{\infty} \frac{(-1)^n x^{2n}}{(2n+1) \, n!} \right), \qquad \frac{a_{n+1}}{a_n} = -x^2 \, \frac{(2n+1) \, n}{(2n+3)(n+1)}.$$

Figure 1: Examples of common functions expressed in terms of hypergeometric series.

Figure 2: The representation of "Pascal's" triangle in Chu's *Precious Mirror of the Four Elements* of 1303. Reprinted with the permission of Cambridge University Press.

for some pair of polynomials P and Q.

If we factor P and Q:

$$\begin{aligned} P(n) &= c_1(n+\alpha_1)(n+\alpha_2)\cdots(n+\alpha_m), \\ Q(n) &= c_2(n+\beta_1)(n+\beta_2)\cdots(n+\beta_{n+1}), \end{aligned}$$

then the hypergeometric term can be written as

$$a_k = c\,\frac{(\alpha_1)_k(\alpha_2)_k\cdots(\alpha_m)_k}{(\beta_1)_k(\beta_2)_k\cdots(\beta_{n+1})_k},$$

where $c = c_1/c_2$ and $(\alpha)_k$ is the rising factorial:

$$(\alpha)_k = \alpha(\alpha+1)(\alpha+2)\cdots(\alpha+k-1).$$

2.2 The Chu-Vandermonde Identity

A large part of the impetus behind the development of the WZ-method and the reason why it has been become such an influential tool is that there is a rich and ever-expanding store of useful identities for hypergeometric series. These recur throughout mathematics, playing important roles in the solutions of both theoretical and applied problems.

The binomial theorem was the first and is the most fundamental of these identities. It is the foundation upon which all others are proved. Mathematicians have been building upon the binomial theorem for many years. In 1303, Chu Shih-Chieh wrote *Precious Mirror of the Four Elements* (*Ssu Yü Chien*), in which he may have been the first person to state the fundamental result:

$$\sum_{i=0}^{\infty} \binom{a}{i} \binom{b}{k-i} = \binom{a+b}{k}. \tag{2}$$

In Chu's identity, a, b, and k are positive integers. Note that all summands will be zero once i is greater than a or k. Equation (2) is easily derived from the binomial theorem by comparing the coefficients of x^k in

$$(1+x)^a(1+x)^b = \sum_{i=0}^{a} \binom{a}{i} x^i \sum_{j=0}^{b} \binom{b}{j} x^j,$$

and

$$(1+x)^{a+b} = \sum_{k=0}^{a+b} \binom{a+b}{k} x^k.$$

Equation (2) was rediscovered by Alexandre Vandermonde in 1772 and is today known as the **Chu-Vandermonde Identity**.

The ratio of successive terms in the summation is

$$\binom{a}{n+1}\binom{b}{k-n-1}\Big/\binom{a}{n}\binom{b}{k-n} = \frac{(n-a)(n-k)}{(n+1)(n+b-k+1)}.$$

If we divide both sides of equation (2) by the first summand, $\binom{b}{k}$, it can be rewritten in terms of rising factorials as

$$1 + \sum_{n=1}^{\infty} \frac{(-a)_n(-k)_n}{n!\,(b-k+1)_n} = \frac{(a+b)!\,(b-k)!}{(a+b-k)!\,b!}. \tag{3}$$

In 1797, Johann Friedrich Pfaff showed that, subject only to convergence conditions, equation (3) holds for complex values, in which case it can be expressed as

$$1 + \sum_{n=1}^{\infty} \frac{(\alpha)_n\,(\beta)_n}{n!\,(\gamma)_n} = \frac{\Gamma(\gamma-\alpha-\beta)\,\Gamma(\gamma)}{\Gamma(\gamma-\alpha)\,\Gamma(\gamma-\beta)}. \tag{4}$$

Pfaff's student, Carl Friedrich Gauss, used hypergeometric series in his astronomical work and advanced their study. Among his contributions, he found sharp criteria for whether or not a hypergeometric series converges. Throughout the nineteenth and twentieth century, a great number of identities for hypergeometric series were discovered, many of which were collected in the Bateman Manuscript Project published as *Higher Transcendental Functions* in 1953–55.

2.3 Standardized Notation

Most hypergeometric series can be written as sums of rational products of binomial coefficients, but this representation is problematic because it is not unique.

As an example,

$$\sum_{n=0}^{m} 2^{m-k-2n} \binom{m}{n} \binom{m-n}{n+k} = \binom{2m}{m+k}$$

appears to be different from the Chu-Vandermonde identity, equation (2). But if we look at the ratio of consecutive summands, it is

$$\frac{1}{4} \frac{(m-2n-k-1)(m-2n-k)}{(n+1)(n+k+1)} = \frac{(n+(k+1-m)/2)(n+(k-m)/2)}{(n+1)(n+k+1)}.$$

This is simply the Chu-Vandermonde identity with $\alpha = (k+1-m)/2$, $\beta = (k-m)/2$, and $\gamma = k+1$.

There is clearly an advantage to using the rising factorial notation, in which case we write

$${}_mF_n\left(\begin{matrix} \alpha_1, \ldots, \alpha_m \\ \beta_1, \ldots, \beta_n \end{matrix} ; x\right) := 1 + \sum_{k=1}^{\infty} \frac{(\alpha_1)_k \cdots (\alpha_m)_k}{k!\,(\beta_1)_k \cdots (\beta_n)_k} x^k.$$

Even with this standardized notation, there are equivalent identities that look different because there are non-trivial transformation formulas for hypergeometric series. As an example, provided the series in question converge, we have that

$${}_2F_1\left(\begin{matrix} a,\ b \\ 2a \end{matrix} ; x\right) = \left(1-\frac{x}{2}\right)^{-b} {}_2F_1\left(\begin{matrix} b/2,\ (b+1)/2 \\ a+1/2 \end{matrix} ; \left(\frac{x}{2-x}\right)^2\right).$$

This is why, even if all identities for hypergeometric series were already known, it would not be enough to have a list of them against which one could compare the candidate in question. Just establishing the equivalence of two identities can be a very difficult task. This makes the WZ-method all the more remarkable because it is independent of the form in which the identity is given and can even be used to verify (or disprove) a conjectured transformation formula.

3 The WZ-Method

3.1 Sister Celine's Technique

The WZ-method for finding and proving identities for hypergeometric series builds on a succession of developments that began with the Ph.D. thesis of Sister Mary Celine Fasenmyer at the University of Michigan in 1945. We consider a sum of the form

$$f(n) = \sum_k F(n,k)$$

where $F(n,k)$ is a proper hypergeometric term. This means that it is a polynomial in n and k times $x^k y^n$, for fixed x and y, times a product of quotients of factorials of the form $(an+bk+c)!$, where a and b, and c are fixed integers. As an example,

$$\sum_{0\le k\le n/3} 2^k \frac{n}{n-k}\binom{n-k}{2k} \;=\; \sum_{0\le k\le n/3} n\cdot 2^k\cdot\frac{(n-k-1)!}{(2k)!\,(n-3k)!}.$$

is such a series.

Every such sum of proper hypergeometric terms will satisfy a finite recursion of the form

$$\sum_{j=0}^{J} a_j(n)\, f(n+j) = 0.$$

Sister Celine showed how to reduce the problem of finding these coefficients to one of solving a system of linear equations. It was Doron Zeilberger who realized that this gives us an algorithm for proving hypergeometric series identities because we need only verify that each side satisfies the same recursion and the same initial conditions. The problem with using Sister Celine's approach is that her particular algorithm for finding the coefficients is slow. Later developments would speed it up considerably, though in the process would lose the easy generalization of Sister Celine's technique to summations over several indices.

3.2 Gosper's algorithm

In 1977 and 1979, R. W. Gosper, Jr. took a different approach and became one of the first people to use computers to discover and check identities for hypergeometric series. Given a proper hypergeometric term $F(n,k)$, Gosper showed how to automate a search for a proper hypergeometric term $G(n,k)$ with the property that

$$G(n,k+1)-G(n,k)=F(n,k).$$

If such a G could be found, then

$$f(n)=\sum_{k=0}^{n}\Big(G(n,k+1)-G(n,k)\Big)=G(n,n+1)-G(n,0).$$

An example of the application of this algorithm is the computer-generated proof of an identity discovered and first proved by J. S. Lomont and John Brillhart: Let $1\le m\le n$ where $n\ge 2$ and $1\le s\le \min(m,n-1)$, then

$$\sum_{j=0}^{s}\frac{(-1)^j(m+n-2j)\binom{m}{j}\binom{m-j}{m-s}\binom{n}{j}\binom{n-j}{n-s}\binom{m+n}{j}\binom{m+n-s-j-1}{s-j}}{\binom{s}{j}^2}=0.$$

Given this conjecture, the program EKHAD replies with the proof certificate

$$-s,\ j*(m+n-s-j)/(m+n-2*j).$$

This means that if $F(n,j)$ is the summand in the conjectured identity, then

$$-s\,F(n,j) = G(n,j+1) - G(n,j)$$

where $G(n,j) = j(m+n-s-j)F(n,j)/(m+n-2j)$. The sum over j of $G(n,j+1) - G(n,j)$ telescopes, and therefore the original summation equals $[G(n,s+1) - G(n,0)]/(-s) = 0$.

Gosper's algorithm is a fertile approach that is often applicable, but it is limited by the fact that such a G does not always exist.

3.3 Wilf and Zeilberger

Major progress was made by Doron Zeilberger who, starting in 1982, began to combine the ideas of Sister Celine and William Gosper. In the early 1990s, Herbert Wilf joined Zeilberger in extending and refining these methods into a fully automated proof machine that is now known as the WZ-method. If $F(n,k)$ is a proper hypergeometric term, then there always is a proper hypergeometric term $G(n,k)$ such that $G(n,k+1) - G(n,k)$ is equal to a linear combination of $\{F(n+j,k)\,|\,0 \le j \le J\}$ for some explicitly computable J,,

$$\sum_{j=0}^{J} a_j(n)\,F(n+j,k) = G(n,k+1) - G(n,k), \tag{5}$$

where the $a_j(n)$ are polynomials in n. If $f(n) = \sum_{k=0}^{K} F(n,k)$, then we can sum both sides of equation (5) over $0 \le k \le K$. The right side telescopes, and we are left with the recursive formula

$$\sum_{j=0}^{J} a_j(n)\,f(n+j) = G(n,K+1) - G(n,0).$$

Gosper's technique—which is very fast—can be used to find the function G. The coefficients, $a_j(n)$, are then found by solving a system of linear equations.

Gosper's algorithm is the special case of the WZ-method in which $J = 0$. The other case of particular interest is when $J = 1$ and $a_1 = -a_0 = 1$. Consider the conjectured identity:

$$\sum_k \binom{n}{2k}\binom{2k+1}{k}\frac{n+2}{2k+1}\,2^{n-2k-1} = \binom{2n+1}{n}. \tag{6}$$

If we divide each side by $\binom{2n+1}{n}$, this can be rewritten as

$$f(n) = \sum_k \binom{n}{2k}\binom{2k+1}{k}\frac{n+2}{2j+1}\,2^{n-2k-1} \Big/ \binom{2n+1}{n} = 1.$$

If this is true, then $f(n)$ satisfies the recursion $f(n+1) - f(n) = 0$. Let $F(n,k)$ be the summand,

$$F(n,k) = \binom{n}{2k}\binom{2k+1}{k}\frac{n+2}{2j+1}\,2^{n-2k-1}\Big/\binom{2n+1}{n}.$$

If we could find a proper hypergeometric term $G(n,k)$ for which

$$F(n+1,k) - F(n,k) = G(n,k+1) - G(n,k), \tag{7}$$

then it would follow that $f(n+1) - f(n) = 0$, and so $f(n)$ would be constant. It would be enough to check that $f(0) = 1$.

In fact, such a G does exist. The WZ-method finds it. The proof certificate is the rational function

$$\frac{G(n,k)}{F(n,k)} = \frac{4k(k+1)}{(2n+3)(2k-n-1)}.$$

To check equation (6), we only need to verify that F and G, which we now know, do indeed satisfy equation (7).

In general, the WZ-method returns either the ratio $G(n,k)/F(n,k)$ (if the recursion is of the form given in equation (7)), or it returns the actual recursive formula satisfied by $f(n)$. The only drawback to the WZ-method is that the number of terms in the recursive formula may be too large for practical use.

3.4 Petkovšek and Others

In his Ph.D. thesis of 1991, Marko Petkovšek showed how to find a closed form solution—or to show that such a solution does not exist—for any recursive formula of the form

$$\sum_{j=0}^{J} a_j(n)\, f(n+j) = g(n)$$

in which $g(n)$ and the $a_j(n)$ are polynomials in n. By closed form, we mean a linear combination of a fixed number of hypergeometric terms.

Combined with the WZ-method, Petkovšek's algorithm implies that in theory if not in practice, given any summation of proper hypergeometric terms, there is a completely automated computer procedure that will either find a closed form for the summation or prove that no such closed from exists. A full account of the WZ-method and Petkovšek's algorithm is given in the book $A = B$ by Petkovšek, Wilf, and Zeilberger.

Others have worked on implementing and extending the ideas of the WZ-method. One of the centers for this work has been a group headed by Peter Paule at the University of Linz in Austria. Ira Gessel has been at the forefront of those who have used this algorithm to implement computer searches that both discovered and proved a large number of new identities for hypergeometric series.

4 Extensions, Future Work, and Conclusions

4.1 Extensions and Future Work

All of the techniques described in this article have been extended to q-hypergeometric series such as

$$1 + \sum_{k=0}^{n} q^{k^2} \frac{(1-q^n)(1-q^{n-1})\cdots(1-q^{n-k+1})}{(1-q)(1-q^2)\cdots(1-q^k)}$$

in which the ratio of consecutive summands is a rational function of q^k.

Many general determinant evaluations can be reduced to problems that can be solved using the WZ-method. Work is progressing on fully automating proofs of such results.

There are other theorems that appear to be amenable to an automated computer attack. These include results on real closed fields using techniques of George Collins and geometrical theorems proved using algebraic techniques such as Gröbner bases.

4.2 Conclusions

The net effect of the algorithms that prove identities for hypergeometric series is that a piece of mathematics that once could only be done by those with cleverness and insight has been turned into a purely mechanical calculation. Rather than limiting the scope of mathematics, the WZ-method has widened it. Problems that had once been intractable are now within reach. The situation is different in degree but not in kind from the invention of calculus. This was the discovery of mechanical procedures that enabled scientists to shift their attention away from laborious and ingenious techniques for finding areas and tangent lines and to begin addressing the really interesting questions.

Perhaps this will always be the fate of computer-generated proofs. The fact that one class of problems has been moved into the category of those that can be solved by computers means that we are freed to direct our attention to those questions that are most important.

Web sites for the WZ-method and related algorithms

Home page for the book $A = B$:
http://www.cis.upenn.edu/~wilf/AeqB.html

Wilf and Zeilberger's programs:
http://www.cis.upenn.edu/~wilf/progs.html

programs of the RISC group at the University of Linz:
http://www.risc.uni-linz.ac.at/research/combinat/risc/

Bibliography

Collins, G. E. (1975). Quantifier elimination for real closed fields by cylindrical algebraic decomposition. In *Automata theory and formal languages*. Lecture Notes in Computer Science, Vol. 33, pp. 134–183. Springer, Berlin.

Nemes, I., Petkovšek, M., Wilf, H., and Zeilberger, D. (1997). How to do MONTHLY problems with your computer. *American Mathematical Monthly* **104**, 505–519.

Petkovšek, M., Wilf, H., and Zeilberger, D. (1996). $A = B$. A K Peters. Wellesley, Mass.

Wilf, H., and Zeilberger, D. (1992). An algorithmic proof theory for hypergeometric (ordinary and "q") multisum/integral identities. *Inventiones Mathematicae* **108**, 575-633.