Automatic Proofs of Identities

Bruno Salvy
summary of the talk by Flavia Stan

Séminaire Philippe Flajolet. May 26, 2011

Abstract

We present the ideas behind algorithmic proofs of identities involving sums and integrals of large classes of special functions. Recent results allowed a new extension of the class of holonomic functions.

1 Introduction

Dictionaries of mathematical formulas like Abramowitz and Stegun's *Handbook of Mathematical Functions* are among the most cited and used by scientists. This type of collections were traditionally prepared, checked and proof-read by specialists from various domains. With the development of computer algebra systems, algorithms lead to error-free and automatic ways to generate, manipulate and prove entries from these tables. However, the implementation of special functions in systems like Maple or Mathematica still relies heavily on table look-up techniques.

The latest step in the evolution of these handbooks is combining the way information can be retrieved from a website, as a front-end to computer algebra algorithms. The Dynamic Dictionary of Mathematical Functions (DDMF)[1] is a project employing these two aspects. Its end-result is a website containing interactive tables of properties for various special functions. All formulas and graphics are generated in real-time by computer algebra routines. This web-interaction is flexible enough, for example, to deliver more digits of numerical values for which correctness is guaranteed or generate and display proofs of various properties.

The symbolic computation engine behind the DDMF is based on very recent algorithms [2, 7] as well as on standard Maple routines. Procedures from the package `gfun` [8] are used heavily to manipulate differential and recurrence relations satisfied by holonomic functions. A version of `gfun` is integrated in the Maple system.

In the DDMF, mathematical functions are modeled as linear differential or recurrence equations coupled with finite sets of initial values. Functions or sequences that can be viewed as solutions of such linear relations constitute about 25% of Sloane's *Encyclopedia of Integer Sequences* and, more importantly, 60% of Abramowitz and Stegun's handbook. Based on

[1] `http://ddmf.msr-inria.inria.fr/`

this data structure, computer algebra algorithms can determine and prove identities involving a large variety of special functions.

Initiated by Zeilberger, the method of creative telescoping leads to automatic proofs of special function identities. It was first applied to definite summation problems with hypergeometric summands [10, 9] and later to holonomic systems of differential and difference equations [11, 6]. We extend its input class with types of non-holonomic functions [5].

In this talk we present the ideas which lie at the foundation of algorithms for proving special functions identities, i.e., confinement in finite dimension and creative telescoping. We also discuss our extension of these algorithms to classes of non-holonomic functions.

2 Confinement in finite dimension

Given $k+1$ vectors $v_0, v_1, \dots v_k$ from a k-dimensional vector space over a field F, there exists an identity

$$c_0 v_0 + c_1 v_1 + \dots + c_k v_k = 0$$

with coefficients in F. This simple idea can be exploited to find difference or differential equations satisfied by certain classes of functions. For this we will confine the function and all its derivatives, respectively its shifts, in a vector space of finite dimension.

For example, to prove the identity

$$\sin^2 x + \cos^2 x = 1$$

we consider the function $f(x) = \sin^2 x + \cos^2 x - 1$ and show that it satisfies a linear differential equation of order at most 4.

Since both sin and cos are defined by the differential equation $y'' + y = 0$ (but different sets of initial values), the functions $\sin^2$ and $\cos^2$ will also be defined by a common differential equation. Indeed, by induction we see that y^2 and all its derivatives belong to the vector space generated by $\{y^2, yy', y'^2\}$. Thus y^2 is the solution of an order 3 differential equation, independent of any initial conditions. This equation is therefore satisfied by $\sin^2, \cos^2$ and their sum.

This means, the sum of squares and all its derivatives are confined in a vector space of dimension 3. Additionally, the constant function is a solution of $y' = 0$. Since derivation is a linear operation, the function $f(x)$ and its derivatives belong to a vector space of dimension 4, i.e., the sum of the dimensions determined above. This implies that f solves a differential equation of order at most 4. Using Cauchy's theorem, the proof is completed by checking 4 initial values, e.g., by the Maple call

$$> \mathrm{series}(\sin^2 \mathrm{x} + \cos^2 \mathrm{x} - 1, \mathrm{x}, 4);$$

$$\mathrm{O}(\mathrm{x}^4).$$

By a similar dimension argument, Cassini's identity for the Fibonacci numbers F_n can be proven. For this purpose, it suffices to check whether the first 5 initial values of the function $f(n) = F_n^2 - F_{n+1}F_{n-1} + (-1)^n$ are zero.

The crucial point in the proof was the dimension argument which led to the existence of a differential equation for the squares and the sums of functions involved. This type of closure properties follow along the same lines for the entire class of ∂-finite functions which we shortly discuss in the following section.

2.1 Gröebner bases in Ore algebras

Let us consider an example in several variables for identities obtained with the confinement method. Going back to Gauß (1812), the contiguity relations for the hypergeometric series

$$F(a,b;c;z) = \sum_{n=0}^{\infty} \frac{(a)_n (b)_n}{(c)_n n!} z^n$$

are recurrences involving the shifts with respect to the parameters a, b, c. Here, the Pochhammer symbol $(x)_n$ denotes the rising factorial $x(x+1)\dots(x+n-1)$ for $n \in \mathbb{N}$ and $x \in \mathbb{C}$.

Contiguity relations result from confining F, its derivatives with respect to z and its shifts in the other parameters to a vector space of finite dimension. For example, let $u_{a,n}$ denote the hypergeometric term of the series F. From the ratios $\frac{u_{a,n+1}}{u_{a,n}}$ and $\frac{u_{a+1,n}}{u_{a,n}}$ two mixed difference-differential equations follow

$$z(1-z)F'' + (c - (a+b+1)z)\, F' - abF = 0,$$

$$S_a F = \frac{z}{a} F' + F \text{ with } S_a F := F(a+1, b; c; z).$$

By induction we see that all higher order shifts and derivatives can be expressed via the two equations in terms of elements from the set $\{F, F'\}$.

The general framework for studying mixed difference-differential equations is that of Ore algebras [6], denoted by $\mathcal{A} = \mathbb{K}(x_1, \dots x_n) \langle \partial_1, \dots \partial_n \rangle$ where $\mathbb{K}$ is a field. The ∂_{x_i}'s represent either a derivation operator D_{x_i}, a shift operator S_{x_i} or a more general Ore operator with respect to the variable x_i.

Back to our example, we consider the left ideal $\mathcal{I}$ spanned by the two difference-differential operators in $\mathcal{A} = \mathbb{Q}(a,b,c,z) \langle \partial_z, S_a \rangle$. Since all higher order shifts and derivatives of F can be expressed using the two equations, $\mathcal{A}/\mathcal{I}$ has vector-space dimension 2 over $\mathbb{Q}(a,b,c,z)$. Therefore $S_a^2 F, S_a F$ and F must be linearly dependent. By simple linear algebra we arrive at the contiguity relation

$$(a+1)(z-1)S_a^2 F + ((b-a-1)z + 2 - c + 2a)\, S_a F + (c-a-1)F = 0.$$

In the same way we prove Mehler's identity for Hermite polynomials

$$\sum_{n=0}^{\infty} H_n(x) H_n(y) \frac{u^n}{n!} = \frac{1}{\sqrt{1-4u^2}} \exp\left(\frac{4u(xy - u(x^2+y^2))}{1-4u^2} \right).$$

Since the computations become more involved we call procedures from the package `gfun`.

Other computations of this type are facilitated by the use of Gröbner bases in the setting of Ore algebras [6]. Generalizing both Gaussian elimination to find linear dependence between vectors and Euclidean division from univariate polynomials, Gröbner bases can be used to find unique representations of elements in these more complicated structures in terms of finitely many generators.

To define the Gröbner basis of an ideal $\mathcal{I} \subset \mathcal{A}$, we introduce a well order on the set of monomials in the ∂_{x_i}'s. Additionally, $1 = \partial_{x_1}^0 \dots \partial_{x_n}^0$ has to be its minimal element. A Gröbner basis of the (left) ideal $\mathcal{I}$ can be visualized as the corners of a staircase in the multidimensional lattice $\mathbb{N}^n$. Elements of the algebra modulo this ideal $\mathcal{I}$ can be written as linear combinations of the monomials under the staircase. To find a unique representation of an element in $\mathcal{A}/\mathcal{I}$, we use a generalized Euclidean division algorithm with respect to the given Gröbner basis of the ideal. This unique remainder is called the normal form of the given element.

When the set of monomials under the staircase is finite, $\mathcal{A}/\mathcal{I}$ is the finite dimensional vector space over $\mathbb{K}(x_1, \dots, x_n)$ generated by these monomials. In this case $\mathcal{I}$ is called ∂-finite and all computations modulo this ideal can be formulated in terms of linear algebra. For an infinite dimensional vector space $\mathcal{A}/\mathcal{I}$ we generalize the notion of dimension using the Hilbert function. This generalization defines a ∂-finite ideal as zero-dimensional.

The set of operators annihilating a given function f has the algebraic structure of a left ideal and is denoted by $\operatorname{ann} f$. When its annihilating ideal is ∂-finite, we also refer to the function as ∂-finite. Functions of this type include, for instance, the classical orthogonal polynomials considered with respect to the shift operator in the index and differentiation in the argument. The hypergeometric series of the previous example also fulfills this property. On the other hand, the Stirling numbers $S_2(n,k)$ are not ∂-finite. Their annihilating ideal is generated by the relation

$$S_2(n,k) = S_2(n-1,k-1) + kS_2(n-1,k)$$

and has Hilbert dimension 1 in $\mathbb{Q}(n,k)\,\langle \partial_n, \partial_k \rangle$.

Using dimensional arguments similar to the ones from the proofs of the above identities, we find the following closure properties for the class of ∂-finite functions

$$\begin{aligned} \dim \operatorname{ann}(f+g) &\leq \max(\dim \operatorname{ann}\, f, \dim \operatorname{ann}\, g), \\ \dim \operatorname{ann}(fg) &\leq \dim \operatorname{ann}\, f + \dim \operatorname{ann}\, g, \\ \dim \operatorname{ann}\, \partial f &\leq \dim \operatorname{ann}\, f. \end{aligned}$$

The Maple package `Mgfun` [3] implements closure properties in the ∂-finite case together with algorithms for computing generators of these ideals. It also includes an extension of Zeilberger's creative telescoping method to ∂-finite ideals [4]. We discuss these aspects in the next section.

3 Creative telescoping

To illustrate the idea of creative telescoping we prove the identity

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

by rewriting Pascal's triangle as

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1} = 2\binom{n}{k} + \binom{n}{k-1} - \binom{n}{k}$$

and summing over all $0 \leq k \leq n+1$

$$\sum_{k=0}^{n+1} \binom{n+1}{k} = 2\sum_{k=0}^{n} \binom{n}{k}.$$

Solving the first order recurrence $I_{n+1} = 2I_n$ and checking an initial condition completes the proof. In general, we have a recurrence for the sum

$$F_n = \sum_k u_{n,k} \tag{1}$$

provided one can determine operators $A(n, S_n)$ and $B(n, k, S_n, S_k)$ such that

$$(A(n, S_n) + \Delta_k B(n, k, S_n, S_k))\, u_{n,k} = 0.$$

Using the telescoping property of the forward-difference operator Δ_k and assuming a summand having finite support included in the summation range, we obtain a homogeneous recurrence for the sum $A(n, S_n)F_n = 0$.

Similarly, in the integration case,

$$I(x) := \int_\Omega u(x, y)dy\,, \tag{2}$$

we obtain a differential equation after determining operators $A(x, \partial_x)$ and $B(x, y, \partial_x, \partial_y)$ satisfying

$$(A(x, \partial_x) + \partial_y B(x, y, \partial_x, \partial_y))\, u(x, y) = 0.$$

Creative telescoping can be viewed as an algorithmic combination of differentiation under the integral sign and integration by parts. Let us prove here that the equation $zJ_0'' + J_0' + zJ_0 = 0$ together with the initial value $J_0(0) = 1$ define the Bessel function

$$J_0 = \frac{2}{\pi} \int_0^1 \frac{\cos zt}{\sqrt{1-t^2}} dt.$$

By successive differentiation under the integral sign, we have

$$I(z) = \int_0^1 \frac{\cos zt}{\sqrt{1-t^2}} dt, \quad I'(z) = \int_0^1 -t\frac{\sin zt}{\sqrt{1-t^2}} dt$$

$$I''(z) = -I(z) + \int_0^1 \sqrt{1-t^2}\cos zt\, dt.$$

After integration by parts, the last identity leads to the desired differential equation.

$$I''(z) + I(z) = \sqrt{1-t^2}\frac{\sin zt}{z}\bigg|_0^1 + \int_0^1 \frac{t}{\sqrt{1-t^2}}\frac{\sin zt}{z}dt$$
$$= \int_0^1 \partial_t\left(\frac{1-t^2}{zt}\partial_z\right)\frac{\cos zt}{\sqrt{1-t^2}}dt - \frac{I'(z)}{z}.$$

We denote by $A(z,\partial_z) = z\partial_z^2 + \partial_z + z$ the operator from the Ore algebra $\mathbb{Q}(z)\langle\partial_z\rangle$. In this way we found that $A(z,\partial_z) - \partial_t\frac{1-t^2}{t}\partial_z$ belongs to the annihilating ideal of the integrand of $I(z)$.

Note that several non-algorithmic aspects were involved in the approach. For a large class of integrals, it is not clear how to integrate by parts, in particular, which parts to choose. Additionally, a bound for the degree of the differential equation is not known. This last issue means that termination of the method is not guaranteed.

In the general setting of the integral (2) the input of the creative telescoping method are operators belonging to the annihilating ideal of the integrand u. These operators generate an ideal $\mathcal{I}$ in the Ore algebra $\mathbb{Q}(x,y)\langle\partial_x,\partial_y\rangle$. The output are operators A, B from this algebra such that the relation $A - \partial_y B$ annihilates u and $A \in \mathbb{Q}(x)\langle\partial_x\rangle$. The summation problem (1) can be formulated in similar terms. In other words, we search for the set of telescopers of the ideal $\mathcal{I}$ with respect to y, denoted by

$$T_y(\mathcal{I}) := (\mathcal{I} + \partial_y\mathbb{Q}(x,y)\langle\partial_x,\partial_y\rangle) \cap \mathbb{Q}(x)\langle\partial_x\rangle.$$

An extension of Zeilberger's fast algorithm to ∂-finite functions is presented in [3, 6]. It proceeds by making an ansatz for the operators A, B and computing the normal form of $Q := A - \partial_y B \in \mathcal{I}$ with respect to a given Gröbner basis $\mathcal{G}$ of the ideal $\mathcal{I}$. Since the operator Q is confined to the annihilating ideal $\mathcal{I}$, all coefficients of its normal must be zero. This leads to a coupled system of equations for the unknown coefficients of the operators A and B.

In the ∂-finite case, the operator B can be written as a linear combination of the monomials under the staircase of $\mathcal{G}$. We proceed by increasing the total degree in the ansatz for A till a solution for the resulting system of equations is found. This procedure is guaranteed to terminate if we start with an integrand u from Zeilberger's class of holonomic functions for which $T_y(\mathcal{I})$ is non-trivial.

In [5] the algorithm was extended to types of non-holonomic functions. We introduce a new class of functions and give an upper bound for the dimension of $T_y(\mathcal{I})$ which provides termination of the approach.

Let us go back to the simple example of Pascal's identity for the sequence of summands $\left(\binom{n}{k}\right)_{n,k\geq 0}$. To discover this identity algorithmically we want to find the operator $S_nS_k - S_k - 1$ in the annihilating ideal of $\binom{n}{k}$. We start with a Gröbner basis of this ideal which has leading terms $\{S_n, S_k\}$ and only the minimal monomial under the resulting staircase. Reducing all monomials of degree $s \leq 2$

$$1 \to 1, \quad S_n \to \frac{n+1}{n+1-k}1, \quad S_k \to \frac{n-k}{k+1}1, \quad S_nS_k \to \frac{n+1}{k+1}1,$$

$$S_n^2 \to \frac{(n+1)(n+2)}{(n+1-k)(n+2-k)}1, \quad S_k^2 \to \frac{(n-k)(n-k-1)}{(k+1)(k+2)}1$$

we compute their common denominator

$$D_2 = (k+1)(k+2)(n+1-k)(n+2-k).$$

All operators $D_2 S_n^\alpha S_k^\beta$ for $\alpha + \beta \leq 2$ are confined in the vector space over $\mathbb{Q}(n)$ generated by $\{1, k, k^2, k^3, k^4\}$. The linear dependency between these operators will deliver the identity we want to prove.

Additionally, this technique leads to a sequence of polynomials with the property $\deg D_s = O(s)$. On the other hand the number of operators $S_n^\alpha S_k^\beta$ with $\alpha + \beta \leq s$ is given by $\binom{s+2}{2}$ and behaves like $O(s^2)$ as s tends to infinity. Since the number of operators will eventually exceed the dimension of the vector space confining them, an identity can be found. This property holds for all holonomic functions.

More generally we define the notion of polynomial growth for an ideal $\mathcal{I} \subset \mathbb{K}(x_1, \ldots, x_n) \langle \partial_1, \ldots, \partial_n \rangle$ with respect to a given graded order. This means the existence of a sequence of polynomials $P_s \in \mathbb{K}[x_1, \ldots, x_n]$ such that for all monomials $\partial_1^{a_1} \ldots \partial_n^{a_n}$ with $\sum_{i=1}^n a_i \leq s$ the operator $P_s \partial_1^{a_1} \ldots \partial_n^{a_n}$ has a normal form with polynomial coefficients of degrees $O(s^p)$ with respect to the Gröbner basis of $\mathcal{I}$. In this case the ideal has polynomial growth p in the graded order used for the computation of the Gröbner basis.

The main result from [5] is a bound on the dimension of the ideal $T_y(\mathcal{I})$. Namely, if $\mathcal{I}$ has polynomial growth p with respect to a given graded order, we have

$$\dim T_y(\mathcal{I}) \leq \max\left(\dim(\mathcal{I}) + p - 1, 0\right).$$

As soon as the bound on the right-hand side of this inequality is smaller than the number of variables remaining after integration or summation, a non-trivial identity exists and can be found.

For instance, coming back to the Stirling numbers of the first and second kind we obtain annihilating ideals of dimension 1 and polynomial growth 1. Using the above bound on the telescoping ideal, we can algorithmically find Frobenius identity

$$\sum_{k=0}^{n} (-1)^{m-k} k! \binom{n-k}{m-k} S_2(n+1, k+1) = S_1(n, m).$$

4 Conclusions

In the Dynamic Dictionary of Mathematical Functions (DDMF) project [1], linear differential or difference equations together with finite sets of initial values form data structures for storing and manipulating special functions. The main goal of the project is that all formulas in this library are generated and proven dynamically through summation and integration algorithms. We present the foundations of these algorithms, namely the idea of confinement in finite dimension and the method of creative telescoping. We also discuss our extension of their input class to include non-holonomic functions.

Our generalized algorithms rely on the notion of polynomial growth defined in [5]. For an arbitrary ideal in an arbitrary Ore algebra, it is not clear how to determine its polynomial growth algorithmically. Future research will focus on this open question by reducing the notion of polynomial growth to an intrinsic property of the given ideal.

References

[1] Benoit, A., Chyzak, F., Darrasse, A., Gerhold, S., Mezzarobba, M., and Salvy, B. The Dynamic Dictionary of Mathematical Functions (DDMF). In *Proceedings of ICMS'10* (2010), vol. 6327 of *Lecture Notes in Computer Science*, pp. 35–41.

[2] Benoit, A., and Salvy, B. Chebyshev expansions for solutions of linear differential equations. In *Proceedings of ISSAC'09* (2009), ACM, pp. 23–30.

[3] Chyzak, F. *Fonctions holonomes en calcul formel.* Thèse universitaire, École polytechnique, 1998. INRIA, TU 0531. 227 pages.

[4] Chyzak, F. An extension of Zeilberger's fast algorithm to general holonomic functions. *Discrete Mathematics 217*, 1-3 (2000), 115–134.

[5] Chyzak, F., Kauers, M., and Salvy, B. A Non-Holonomic Systems Approach to Special Function Identities. In *Proceedings of ISSAC'09* (2009), ACM, pp. 111–118.

[6] Chyzak, F., and Salvy, B. Non-commutative elimination in Ore algebras proves multivariate holonomic identities. *Journal of Symbolic Computation 26*, 2 (1998), 187–227.

[7] Mezzarobba, M., and Salvy, B. Effective bounds for P-recursive sequences. *Journal of Symbolic Computation 45*, 10 (2010), 1075–1096.

[8] Salvy, B., and Zimmermann, P. Gfun: a Maple package for the manipulation of generating and holonomic functions in one variable. *ACM Transactions on Mathematical Software 20*, 2 (1994), 163–177.

[9] Wilf, H. S., and Zeilberger, D. An algorithmic proof theory for hypergeometric (ordinary and "q") multisum/integral identities. *Invent. Math. 108*, 3 (1992), 575–633.

[10] Zeilberger, D. A fast algorithm for proving terminating hypergeometric identities. *Discrete Math. 80*, 2 (1990), 207–211.

[11] Zeilberger, D. A holonomic systems approach to special functions identities. *Journal of Computational and Applied Mathematics 32*, 3 (1990), 321–368.