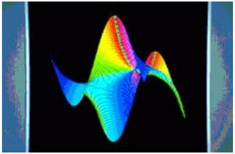
Automatic Proofs of Identities

Bruno Salvy
Bruno.Salvy@inria.fr

Algorithms Project, Inria



Séminaire du LIP, April 28, 2009

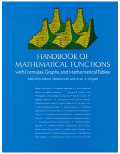
I Introduction

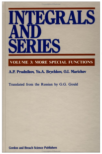
Dynamic Dictionary of Mathematical Functions

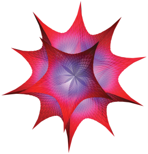
Aim of the project

DDMF = Mathematical Handbooks + Computer Algebra + Web

1. Develop and use computer algebra algorithms to generate the formulas;
2. Provide web-like interaction with the document and the computation.



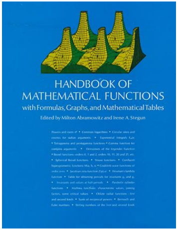




http://ddmf.msr-inria.inria.fr/

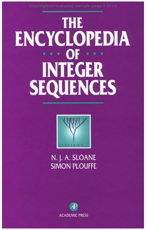
Equations Are a Good Data Structure

- Classical:
  polynomials represent their roots better than radicals.
  Algorithms: Euclidean division and algorithm, Gröbner bases.
- Recent:
  same for linear differential or recurrence equations.
  Algorithms: non-commutative analogues.



About 25% of Sloane's encyclopedia,
60% of Abramowitz & Stegun.

eqn+ini. cond.=data structure



Examples of Identities

$$\sum_{k=0}^{n}\binom{n}{k}^2\binom{n+k}{k}^2=\sum_{k=0}^{n}\binom{n}{k}\binom{n+k}{k}\sum_{j=0}^{k}\binom{k}{j}^3 \qquad \text{[Strehl92]}$$

$$\int_0^{+\infty} xJ_1(ax)I_1(ax)Y_0(x)K_0(x)\,dx=-\frac{\ln(1-a^4)}{2\pi a^2} \qquad \text{[GlMo94]}$$

$$\frac{1}{2\pi i}\oint\frac{(1+2xy+4y^2)\exp\left(\frac{4x^2y^2}{1+4y^2}\right)}{y^{n+1}(1+4y^2)^{\frac{3}{2}}}\,dy=\frac{H_n(x)}{\lfloor n/2\rfloor!} \qquad \text{[Doetsch30]}$$

$$\sum_{k=0}^{n}\frac{q^{k^2}}{(q;q)_k(q;q)_{n-k}}=\sum_{k=-n}^{n}\frac{(-1)^kq^{(5k^2-k)/2}}{(q;q)_{n-k}(q;q)_{n+k}} \qquad \text{[Andrews74]}$$

$$\sum_{j=0}^{n}\sum_{i=0}^{n-j}\frac{q^{(i+j)^2+j^2}}{(q;q)_{n-i-j}(q;q)_i(q;q)_j}=\sum_{k=-n}^{n}\frac{(-1)^kq^{7/2k^2+1/2k}}{(q;q)_{n+k}(q;q)_{n-k}} \qquad \text{[Paule85].}$$

More Identities

$$\sum_{k=0}^{n}\binom{n}{k} i(k+i)^{k-1}(n-k+j)^{n-k}=(n+i+j)^{n} \quad \text{[Abel1826]}$$

$$\sum_{k=0}^{n}(-1)^{m-k}k!\binom{n-k}{m-k}\left\{{n+1 \atop k+1}\right\}=\left\langle{n \atop m}\right\rangle, \quad \text{[Frobenius1910]}$$

$$\sum_{k=0}^{m}\binom{m}{k}B_{n+k}=(-1)^{m+n}\sum_{k=0}^{n}\binom{n}{k}B_{m+k}, \quad \text{[Gessel03]}$$

$$\int_0^\infty x^{k-1}\zeta(n,\alpha+\beta x)\,dx=\beta^{-k}B(k,n-k)\zeta(n-k,\alpha),$$

$$\int_0^\infty x^{\alpha-1}\operatorname{Li}_n(-xy)\,dx=\frac{\pi(-\alpha)^n y^{-\alpha}}{\sin(\alpha\pi)},$$

$$\int_0^\infty x^{s-1}\exp(xy)\Gamma(a,xy)\,dx=\frac{\pi y^{-s}}{\sin((a+s)\pi)}\frac{\Gamma(s)}{\Gamma(1-a)}$$

Computer Algebra Algorithms

Aim

- Prove these identities automatically (fast?);
- Compute the rhs given the lhs;
- Explain why these identities exist.

Examples:

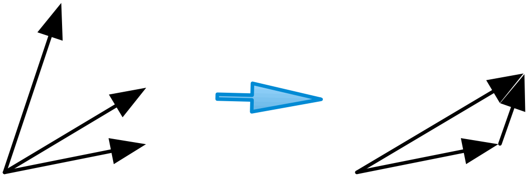
- 1st slide: Zeilberger's algorithm and variants;
- 2nd slide (1st 3): Majewicz, Kauers, Chen & Sun;
- last 3: new generalization of previous ones (with Chyzak & Kauers).

Ideas

Confinement in finite dimension + Creative telescoping.

II Confinement in Finite Dimension

Confinement Provokes Identities



Obvious

$k+1$ vectors in dimension $k \longrightarrow$ an identity.

Idea: confine a function and all its derivatives.

First Proof: $\sin^2 + \cos^2 = 1$

```
> series(sin(x)^2+cos(x)^2-1,x,4);
```

$$O(x^4)$$

Why is this a proof?

1. sin and cos satisfy a 2nd order LDE: $y'' + y = 0$;
2. their squares (and their sum) satisfy a 3rd order LDE;
3. the constant 1 satisfies a 1st order LDE: $y' = 0$;
4. $\rightarrow \sin^2 + \cos^2 - 1$ satisfies a LDE of order at most 4;
5. Cauchy's theorem concludes.

Second proof (same idea): $F_n^2 - F_{n+1}F_{n-1} = (-1)^{n+1}$

```
> for n to 5 do
  fibonacci(n)^2-fibonacci(n+1)*fibonacci(n-1)+(-1)^n od;
```

Third Proof: Contiguity of Hypergeometric Series

$$F(a,b;c;z)=\sum_{n=0}^{\infty}\underbrace{\frac{(a)_n(b)_n}{(c)_n n!}}_{u_{a,n}}z^n,\qquad (x)_n:=x(x+1)\cdots(x+n-1).$$

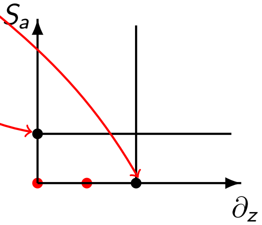
$$\frac{u_{a,n+1}}{u_{a,n}}=\frac{(a+n)(b+n)}{(c+n)(n+1)}\to\ z(1-z)F''+(c-(a+b+1)z)F'-abF=0,$$

$$\frac{u_{a+1,n}}{u_{a,n}}=\frac{n}{a}+1\to S_aF:=F(a+1,b;c;z)=\frac{z}{a}F'+F.$$

Gauss 1812: contiguity relation.

dim=2 $\Rightarrow S_a^2F, S_aF, F$ linearly dependent:

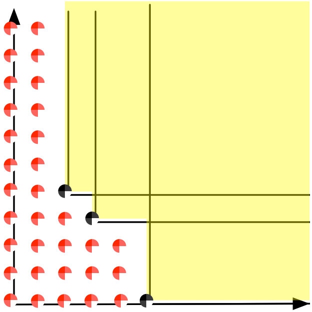
(Coordinates in $\mathbb{Q}(a,b,c,z)$.)



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

Gröbner Basis: Euclidean Division in Several Variables

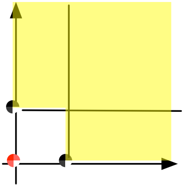
1. Monomial ordering: order on $\mathbb{N}^k$, compatible with $+$, 0 minimal.
2. Gröbner basis of a (left) ideal $\mathcal{I}$: corners of stairs.
3. Quotient mod$\mathcal{I}$: basis below the stairs (Vect$\{\partial^\alpha f\}$).
4. Reduction of P: Rewrite P mod $\mathcal{I}$ on this basis.
5. Dimension of $\mathcal{I}$: "size" of the quotient ∞ly far.
6. D-finiteness: dim $= 0$.



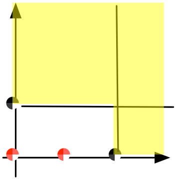
$\rightarrow$ An access to (finite dimensional) vector spaces

Examples

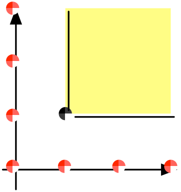
Binomial coeffs $\binom{n}{k}$ wrt S_n, S_k
Hypergeometric sequences



Bessel $J_\nu(x)$ wrt S_ν, ∂_x
Orthogonal pols wrt S_n, ∂_x



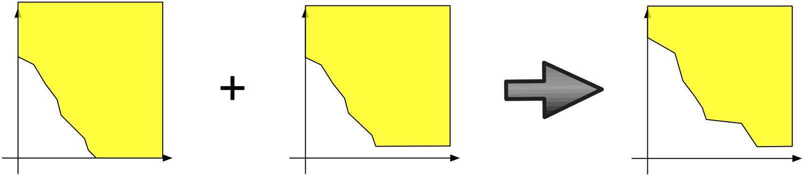
Stirling nbs wrt S_n, S_k



Abel type wrt S_m, S_r, S_k, S_s
$\mathrm{hgm}(m,k)(k+r)^k(m-k+s)^{m-k}\frac{r}{k+r}$

$\dim = 2$ in space of dim 4.

Closure Properties



Proposition

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

Algorithms by linear algebra.

Fourth Proof: Mehler's Identity for Hermite Polynomials

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

1. Definition of Hermite polynomials (D-finite over $\mathbb{Q}(x)$): recurrence of order 2;
2. Product by linear algebra: $H_{n+k}(x)H_{n+k}(y)/(n+k)!, k \in \mathbb{N}$ generated over $\mathbb{Q}(x,n)$ by

   $$\frac{H_n(x)H_n(y)}{n!}, \frac{H_{n+1}(x)H_n(y)}{n!}, \frac{H_n(x)H_{n+1}(y)}{n!}, \frac{H_{n+1}(x)H_{n+1}(y)}{n!}$$

   $\longrightarrow$ recurrence of order at most 4;
3. Translate into differential equation.

I. Definition

> $R_1 := \{H(n+2) = (-2n-2)H(n) + 2H(n+1)x, H(0)=1, H(1)=2x\}:$

> $R_2 := subs(H=H_2, x=y, R_1);$

$$R_2 := \{H_2(0)=1, H_2(n+2) = (-2n-2)H_2(n) + 2H_2(n+1)y, H_2(1)=2y\}$$

II. Product

> $R_3 := gfun\text{:-}poltorec\left(H(n)\cdot H_2(n)\cdot v(n), \left[R_1, R_2, \{v(n+1)\cdot(n+1) = v(n), v(1)=1\}\right], \left[H(n), H_2(n), v(n)\right], c(n)\right);$

$$R_3 := \left\{c(0)=1, c(1)=4xy, c(2)=8x^2y^2+2-4y^2-4x^2, c(3)=\frac{32}{3}x^3y^3+24xy-16xy^3-16x^3y, (16n+16)c(n)-16xyc(n+1)+\left(-8n-20+8y^2+8x^2\right)c(n+2)-4xc(n+3)y+(n+4)c(n+4)\right\}$$

III. Differential Equation

> $gfun\text{:-}rectodiffeq\left(R_3, c(n), f(u)\right);$

$$\left\{\left(16u^3-16u^2yx-4u+8uy^2+8ux^2-4xy\right)f(u)+\left(16u^4-8u^2+1\right)\left(\frac{d}{du}f(u)\right), f(0)=1\right\}$$

> $dsolve(\%, f(u));$

$$f(u) = \frac{I\,e^{\left(\frac{-4xyu+y^2+x^2}{(2u-1)(2u+1)}\right)}}{e^{\left(-y^2-x^2\right)}\sqrt{2u+1}\,\sqrt{2u-1}}$$

>

III Creative Telescoping

Summation by Creative Telescoping

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

IF one knows Pascal's triangle:

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

then summing over k gives

$$I_{n+1} = 2I_n.$$

The initial condition $I_0 = 1$ concludes the proof.

Creative Telescoping (Zeilberger 90)

$$F_n = \sum_k u_{n,k} =?$$

IF one knows $A(n, S_n)$ and $B(n, k, S_n, S_k)$ such that

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

then the sum “telescopes”, leading to $A(n, S_n) \cdot F_n = 0.$

Creative Telescoping (Zeilberger 90)

$$I(x) = \int_\Omega u(x,y)\,dy = ?$$

IF one knows $A(x,\partial_x)$ and $B(x,y,\partial_x,\partial_y)$ such that

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

then the integral "telescopes", leading to $A(x,\partial_x) \cdot I(x) = 0$.

Then I come along and try differentating under the integral sign, and often it worked. So I got a great reputation for doing integrals.

Richard P. Feynman 1985

Creative telescoping="differentiation" under integral+"integration" by parts

Diff. under $\int$ + Integration by Parts $\rightarrow$ Algorithm?

Ex.: $\displaystyle\int_0^1 \frac{\cos zt}{\sqrt{1-t^2}}\,dt = \frac{\pi}{2}J_0(z), \quad (\underbrace{zJ_0''+J_0'+zJ_0}_{A(z,\partial_z)\cdot J_0}=0,\ J_0(0)=1).$

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

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

$$I''(z)+I(z)=\underbrace{\left[\sqrt{1-t^2}\frac{\sin zt}{z}\right]_0^1}_{0}+\int_0^1\frac{t}{\sqrt{1-t^2}}\frac{\sin zt}{z}\,dt=-\frac{I'(z)}{z}.$$

$$\operatorname{ann}\frac{\cos zt}{\sqrt{1-t^2}}\ni\underbrace{A(z,\partial_z)}_{\text{no } t,\partial_t}-\partial_t\underbrace{\frac{t^2-1}{t}\partial_z}_{\text{anything}}$$

Diff. under $\int$ + Integration by Parts → Algorithm?

Ex.: $$\int_0^1 \frac{\cos zt}{\sqrt{1-t^2}}\,dt = \frac{\pi}{2} J_0(z), \quad (\underbrace{zJ_0'' + J_0' + zJ_0}_{A(z,\partial_z)\cdot J_0} = 0,\ J_0(0) = 1).$$

$$\operatorname{ann} \frac{\cos zt}{\sqrt{1-t^2}} \ni \underbrace{A(z,\partial_z)}_{\text{no } t,\partial_t} - \partial_t \underbrace{\frac{t^2-1}{t}\partial_z}_{\text{anything}}$$

Creative Telescoping

Input: generators of (a subideal of) ann f;
Output: A, B such that $A - \partial_t B \in \operatorname{ann} f$, A free of t, ∂_t.
Algorithm: sometimes. (Why would they exist?)

Telescoping of $\mathcal{I}$ wrt t:

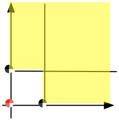
$$T_t(\mathcal{I}) := (\mathcal{I} + \partial_t \mathbb{Q}(z,t)\langle\partial_z,\partial_t\rangle) \cap \mathbb{Q}(z)\langle\partial_z\rangle.$$

Example: Pascal's Triangle Again

$$(S_nS_k - S_k - 1)\cdot\binom{n}{k} = 0 = (\underbrace{S_n - 2}_{\text{no } k,\, S_k} S_n - 2 + (S_k-1)(S_n-1))\cdot\binom{n}{k}.$$

Sum over $k \Rightarrow (S_n - 2)\sum_k \binom{n}{k} = 0.$

Reduce all monomials of degree $\leq s = 2$:



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

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

$$S_nS_k \to \frac{n+1}{k+1}1.$$

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

$D_2, D_2S_n, D_2S_k, D_2S_n^2, D_2S_k^2, D_2S_nS_k$ confined in

$$\mathrm{Vect}_{\mathbb{Q}(n)}(1, k1, k^21, k^31, k^41).$$

This has to happen for some degree: $\deg D_s = O(s)$.

Polynomial Growth (new)

Definition (Polynomial Growth p)

There exists a sequence of polynomials P_s, s.t. for all $(a_1, \dots, a_k)$ with $a_1 + \dots + a_k \leq s$, $P_s \partial_1^{a_1} \cdots \partial_k^{a_k}$ reduces to a combination of elements below the stairs with polynomial coefficients of degree $O(s^p)$.

Theorem (ChyzakKauersSalvy2009)

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

Proof. Same as above. Set $q := \dim \mathcal{I} + p$.

- In degree s, dim $O(s^q)$ below stairs.
- Number of monomials in $\partial_t, \partial_{i_1}, \dots, \partial_{i_q}$: $O(s^{q+1})$;

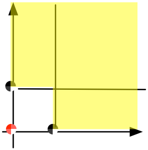
$\Rightarrow$ any q variables linearly dependent $\Rightarrow$ dim $\leq q - 1$.

This proof gives an algorithm. Also, bounds available.

Examples (all with $p = 1$)

- Proper hypergeometric [Wilf & Zeilberger 1992]:

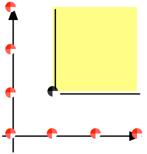
$$Q(n,k)\xi^k \frac{\prod_{i=1}^{u}(a_i n + b_i k + c_i)!}{\prod_{i=1}^{v}(u_i n + v_i k + w_i)!},$$



Q polynomial, $\xi \in \mathbb{C}$, a_i, b_i, u_i, v_i integers.

- Differential D-finite (definite integration);
- Stirling: ok for $n \geq 3$, e.g., Frobenius:

$$\sum_{k=0}^{n} (-1)^{m-k} k! \binom{n-k}{m-k} \left\{ {n+1 \atop k+1} \right\} = \left\langle {n \atop m} \right\rangle .$$



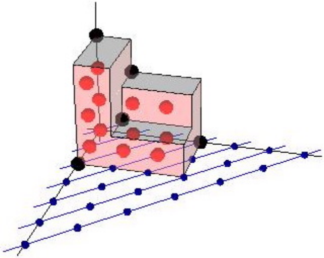
  - Abel type: dim $= 2 \to$ ok for $n \geq 4$, e.g., Abel:

$$\sum_{k=0}^{n} \binom{n}{k} i(k+i)^{k-1}(n-k+j)^{n-k} = (n+i+j)^n.$$

IV Conclusion

Conclusion

- Summary:
  - Linear differential/recurrence equations as a data structure;
  - Confinement in vector spaces + creative telescoping $\rightarrow$ identities.
- Also:
  - Fast algorithms: Zeilberger 1990 (hypergeom); Chyzak 2000 (D-finite) new (non-D-finite).
  - Bounds $\rightarrow$ identities;
  - Fast algorithms for special classes;
  - Efficient numerical evaluation.



- Open questions:
  - Replace polynomial growth by something intrinsic;
  - Exploit symmetries;
  - Structured Padé-Hermite approximants;
  - Understand non-minimality.