Lectures on
Automatic Proof

Lecturer

Husam Luti Saad

Department of Mathematics, College of Science,

Basrah University

Department of Mathematics, College of Science
Basrah University, Basrah, Iraq

Syllabus of M. Sc. in Mathematics

Course Name: Automatic Proof
Credits : 3 units

1. **Sister Celine's Method:**

   Introduction, Background, Notations and Definitions: Monic polynomials, Hypergeometric term, Doubly hypergeometric term, Sister Celine's General Algorithm, Example on Sister Celine's algorithm, Sister Celine's general algorithm, The Fundamental Theorem, Proper hypergeometric term, Rising and falling factorial polynomials, The fundamental theorem, Example on the fundamental theorem.

2. **Gosper's Algorithm**

   Introduction, Hypergeometric to Rational to Polynomial, Hypergeometric to Rational, Rational to Polynomial, Polynomial Solutions, A systematic way for nonzero polynomial solutions, Outline of Gosper's algorithm, Example on Gosper's algorithm, Gosper's Ansatz, The Full Algorithm, Step 2: The resultant of two polynomials, Gosper's Algorithm (Step 2), The GP representation.

3. **Zeilberger's Algorithm**

   Introduction, Existence of the telescoped recurrence, How the algorithm works, Example.

4. **Hypergeometric Solutions with Polynomial Coefficients**

   Introduction, Algorithm Hyper: The derivation of algorithm `Hyper`, Example on algorithm `Hyper`, Gosper's Algorithm & the GP Representation, An Approach for Gosper's Algorithm, A derivation of Gosper's algorithm by using the GP representation, Example on Gosper's algorithm by using the GP representation, Another Approach for Gosper's Algorithm & its Generalization, Another derivation of Gosper's algorithm by using the GP representation, Example on Gosper's algorithm by using the GP representation, Gosper's Algorithm for Recurrences of Arbitrary Order, Example.

References

[1] W.Y.C. Chen and H.L. Saad, On the Gosper-Petkovšek representation of rational functions, *J. Symbolic Computation*, **40** (2005) 955–963.

[2] R.W., Jr. Gosper, Decision procedure for infinite hypergeometric summation, *Proc. Natl. Acad. Sci. USA*, **75** (1978) 40-42.

[3] W. Koepf, *Hypergeometric Summation*, Vieweg, Braunschweig/Wiesbaden, 1998.

[4] P. Paule and V. Strehl, Symbolic summation – some recent developments, RISC Linz Report Series 95-11, Johannes Kepler University, Linz. *Computer Algebra in Science and Engineering – Algorithms, Systems, and Applications*, J. Fleischer, J. Grabmeier, F. Hehl, W. Küchlin (eds.), World Scientific, Singapore, 1995.

[5] M. Petkovšek, H.S. Wilf and D. Zeilberger, $A=B$, A. K. Peters, 1996.

Chapter 1

Sister Celine's Method

1.1 Introduction

The subject of computerized proofs of identities begins with the Ph.D. thesis of Sister Mary Celine Fasenmyer (who is often called Sister Celine) at the University of Michigan in 1945. There she developed a method for finding recurrence relations for hypergeometric polynomials directly from the series expansions of the polynomials. The method is quite effective and easily computerized, though it is usually slow in comparison to the method of Zeilberger. Her algorithm is also important because it has yielded general existence theorems for the recurrence relations satisfied by hypergeometric sums. In spite of that, this method have not been used widely because of the lack of tools, such as computer algebra systems, for the necessary calculations.

1.2 Sister Celine's Algorithm

We begin by illustrating her method on a simple sum.

Example 1.1. *Let*

$$f(n) = \sum_k k\binom{n}{k}, \quad n = 1, 2, \ldots,$$

and let's look for the recurrence that $f(n)$ satisfies. To do this we first look for the

recurrence that the summand

$$F(n,k) = k\binom{n}{k}$$

satisfies. It is a function of two variables (n,k)*, so we try to find a recurrence of the form*

$$a(n)F(n,k) + b(n)F(n+1,k) + c(n)F(n,k+1) + d(n)F(n+1,k+1) = 0, \quad (1.1)$$

in which the coefficients a,b,c,d *depend on* n *only, and not on* k*.*

To find the coefficients, if they exist, we divide (1.1) *through by F(n,k) getting*

$$a + b\frac{F(n+1,k)}{F(n,k)} + c\frac{F(n,k+1)}{F(n,k)} + d\frac{F(n+1,k+1)}{F(n,k)} = 0. \quad (1.2)$$

Substitute $F(n,k) = k\binom{n}{k}$ *in* (1.2) *we get*

$$a + b\frac{n+1}{n+1-k} + c\frac{n-k}{k} + d\frac{n+1}{k} = 0.$$

Put the whole thing over a common denominator. The numerator is, after collecting the powers of k*,*

$$(d + (c+2d)n + (c+d)n^2) + (a+b-c-d+(a+b-2c-d)n)k + (c-a)k^2 = 0.$$

The coefficient of each power of k *must vanish. This gives us a system of three equations in four unknowns, namely*

$$\begin{aligned} nc + (n+1)d &= 0, \\ (n+1)a + (n+1)b + (-2n-1)c - (n+1)d &= 0, \\ -a + c &= 0, \end{aligned}$$

to solve for a,b,c,d*.*

Finding a nontrivial solution is now guaranteed simply because the number of unknowns are more than the number of equations. If we actually solve these equations we find that

$$a = -\frac{n+1}{n}\,d, \quad b = 0, \quad c = -\frac{n+1}{n}\,d.$$

We now substitute these values into the recurrence relation (1.1), *and we have the desired "k-free" recurrence for the summand* $F(n,k)$, *namely*

$$-\frac{n+1}{n}F(n,k)-\frac{n+1}{n}F(n,k+1)+F(n+1,k+1)=0.$$

$$F(n+1,k+1)=\frac{n+1}{n}F(n,k)+\frac{n+1}{n}F(n,k+1). \tag{1.3}$$

Now sum (1.3) *over all integers* k, *noticing that the coefficients in the recurrence are free of* k*'s, so the summation over* k *can operate directly on the* F *in each term. We get the recurrence*

$$\begin{aligned} f(n+1) &= \frac{n+1}{n}f(n)+\frac{n+1}{n}f(n) \\ f(n+1) &= 2\frac{n+1}{n}f(n), \quad n=1,2,\ldots, \end{aligned}$$

such that $f(1)=1$. *We can now easily find* $f(n)$, *the desired sum, since*

$$\begin{aligned} f(n+1) &= 2\frac{n+1}{n}f(n) \\ &= 2^2\frac{n+1}{n}\frac{n}{n-1}f(n-1) \\ &= 2^n(n+1)f(1) \\ &= 2^n(n+1). \end{aligned}$$

Hence

$$\begin{aligned} f(n) &= 2^{n-1}n \\ \sum_k k\binom{n}{k} &= 2^{n-1}n, \quad n=1,2,\ldots. \end{aligned}$$

□

Definition 1.1. *A nonzero term* $F(n,k)$ *is called doubly hypergeometric if both*

$$F(n+1,k)/F(n,k) \quad \textit{and} \quad F(n,k+1)/F(n,k)$$

are rational functions of n *and* k.

Now let's discuss her algorithm in general. We are given a sum $f(n) = \sum_k F(n,k)$, where F is doubly hypergeometric. We want to find a recurrence formula for the sum $f(n)$, so for a first step, we will find a recurrence for the summand $F(n,k)$, of the form

$$\sum_{i=0}^{I}\sum_{j=0}^{J} a_{ij}(n)F(n-j,k-i) = 0. \tag{1.4}$$

The complete sequence of steps is the following.

1. Fix trial values of I and J, say $I = J = 1$.

2. Assume the recurrence formula in the form of (1.4), with the coefficients $a_{ij}(n)$ to be determined, if possible.

3. Divide each term of (1.4) by $F(n,k)$, and reduce each ratio $F(n-j,k-i)/F(n,k)$ by simplifying the ratios of the factorials that it contains, so that only rational functions of n and k remain.

4. Place the entire expression over a single common denominator. Then collect the numerator as a polynomial in k.

5. Solve the system of linear equations that results from equating to zero the coefficients of each power of k in the numerator polynomial, for the unknown coefficients $a_{ij}(n)$. If the system has no solution, try the whole thing again with larger values of I and/or J. That is, look for a bigger recurrence.

We will prove below that under suitable hypotheses Sister Celine's algorithm is guaranteed to succeed if I, J are large enough, and the "large enough" can be estimated in advance.

1.3 The Fundamental Theorem

The "Fundamental Theorem" states that every proper hypergeometric term $F(n,k)$ satisfies a recurrence relation of the kind we have found in the previous sections, and it

validates the procedure that we have used to find these recurrences in the sense that it guarantees that Sister Celine's method will work if the span of the assumed recurrence is large enough. The theorem also finds explicit precomputable upper bounds on the span.

Definition 1.2. *A function $F(n,k)$ is said to be a proper hypergeometric term if it can be written in the form*

$$F(n,k) = P(n,k)\frac{\prod_{i=1}^{uu}(a_i n + b_i k + c_i)!}{\prod_{i=1}^{vv}(u_i n + v_i k + w_i)!}\, x^k, \tag{1.5}$$

in which x is an indeterminate over, say, the complex numbers, and

1. P is a polynomial,
2. the a's, b's, u's, v's are specific integers, that is to say, they do not contain any additional parameters.
3. the quantities uu and vv are finite, nonnegative, specific integers.

An F of the form (1.5) is well defined at a point (n,k) if none of the numbers $\{a_i n + b_i k + c_i\}_{i=1}^{uu}$ is a negative integer. We will say that $F(n,k) = 0$ if F is well defined at (n,k) and at least one of the numbers $\{u_i n + v_i k + w_i\}_{i=1}^{vv}$ is a negative integer, or $P(n,k) = 0$.

Some examples of proper hypergeometric terms are as follows:

Example 1.2. *The term $\binom{n}{k}2^k$ is proper hypergeometric.*

Solution. The term $\binom{n}{k}2^k$ can be written

$$F(n,k) = \binom{n}{k}2^k = \frac{n!}{k!(n-k)!}2^k,$$

If we identify the above specific F with the general form in (1.5) by taking $P(n,k)=1$, $uu=1, vv=2, x=2, (a_1,b_1,c_1)=(1,0,0)$ and for the two (u,v,w) vectors,

$$(0,1,0),(1,-1,0)$$

So the above F is exactly of the required form.

Example 1.3. *The term* $1/(n+3k+1)$ *is proper hypergeometric.*

Solution. The term $F(n,k)=1/(n+3k+1)$ is not in proper hypergeometric form. It doesn't contain any of the factorials, and it isn't a polynomial. However, the definition says "...if it can be written in the form ..." This $F(n,k)$ can be written in proper hypergeometric form, even though it was not given to us in that form! All we have to do is to write

$$\frac{1}{n+3k+1}=\frac{(n+3k)!}{(n+3k+1)!}.$$

If we identify the above specific F with the general form in (1.5) by taking $P(n,k)=1$, $uu=1, vv=1, x=1, (a_1,b_1,c_1)=(1,3,0)$ and $(u_1,v_1,w_1)=(1,3,1)$, So the above F is exactly of the required form.

Definition 1.3. *The rising factorial* (rf) *and falling factorial* (ff) *polynomials, for nonnegative integer values of* x *(the empty product is* $=1$*) are defined by*

$$\begin{aligned}\mathrm{rf}(x,y) &= \prod_{j=1}^{x}(y+j)=(y+1)(y+2)\cdots(y+x),\\ \mathrm{ff}(x,y) &= \prod_{j=0}^{x-1}(y-j)=y(y-1)\cdots(y-x+1).\end{aligned}$$

Let $\deg(p)$ denotes the polynomial degree. Now we can state the main theorem.

Theorem 1.1. *Let* $F(n,k)$ *be a proper hypergeometric term. Then* F *satisfies a* k*-free recurrence relation. That is to say, there exist positive integers* I,J*, and polynomials* $a_{ij}(n)$ *for* $i=0,1,\ldots,I$*;* $j=0,1,\ldots,J$*, not all zero, such that the recurrence*

$$\sum_{i=0}^{I}\sum_{j=0}^{J}a_{ij}(n)F(n-j,k-i)=0 \tag{1.6}$$

holds at every point (n,k) *at which* $F(n,k) \neq 0$ *and all of the values of* F *that occur in* (1.6) *are well defined. Furthermore, there is such a recurrence with* $(I,J) = (I^*, J^*)$ *where*

$$J^* = \sum_s |b_s| + \sum_s |v_s|; \quad I^* = 1 + \deg(P) + J^* \left(\left\{ \sum_s |a_s| + \sum_s |u_s| \right\} - 1 \right). \quad (1.7)$$

Note that the recurrence (1.6) is *k-free* since the coefficients $a_{ij}(n)$ depend only on n, not on k.

Proof. (H.W.) If $F(n,k) = (an+bk+c)!$ then for $i,j \geq 0$ we have

$$\frac{F(n-j,k-i)}{F(n,k)} = \begin{cases} \{(an+bk+c)\cdots(an+bk+c-aj-bi+1)\}^{-1}, & \text{if } aj+bi \geq 0; \\ (an+bk+c+|aj+bi|)\cdots(an+bk+c+1), & \text{if } aj+bi < 0. \end{cases} \quad (1.8)$$

The result is either a polynomial in n and k, or is the reciprocal of such a polynomial, depending on the sign of $aj+bi$. In terms of rf and ff, we can rewrite (1.8) as

$$\frac{F(n-j,k-i)}{F(n,k)} = \begin{cases} 1/\mathrm{ff}(aj+bi, an+bk+c), & \text{if } aj+bi \geq 0; \\ \mathrm{rf}(|aj+bi|, an+bk+c), & \text{if } aj+bi < 0. \end{cases} \quad (1.9)$$

Now consider a function $F(n,k)$ as in (1.5)

$$F(n,k) = P(n,k) \frac{\prod_{s=1}^{uu} (a_s n + b_s k + c_s)!}{\prod_{s=1}^{vv} (u_s n + v_s k + w_s)!} x^k.$$

Let

$$\rho = F(n-j,k-i)/F(n,k)$$

By using (1.9)

$$\rho = \frac{\nu(n,k)}{\delta(n,k)},$$

where

$$\nu(n,k) \;=\; P(n-j,k-i) \prod_{\substack{s=1 \\ a_s j + b_s i < 0}}^{uu} \mathrm{rf}(|a_s j + b_s i|, a_s n + b_s k + c_s)$$

$$\prod_{\substack{s=1 \\ u_s j+v_s i\geq 0}}^{vv} \mathrm{ff}(u_s j+v_s i, u_s n+v_s k+w_s),$$

and

$$\begin{aligned}\delta(n,k) &= P(n,k)x^i \prod_{\substack{s=1 \\ a_s j+b_s i\geq 0}}^{uu} \mathrm{ff}(a_s j+b_s i, a_s n+b_s k+c_s) \\ &\quad \prod_{\substack{s=1 \\ u_s j+v_s i<0}}^{vv} \mathrm{rf}(|u_s j+v_s i|, u_s n+v_s k+w_s). \end{aligned} \tag{1.10}$$

Let's assume the recurrence in the form (1.6) and try to solve for the coefficients $a_{ij}(n)$. After dividing by $F(n,k)$, the left side of the assumed recurrence will be

$$\sum_{i=0}^{I}\sum_{j=0}^{J} a_{ij}(n)\frac{\nu_{ij}}{\delta_{ij}}. \tag{1.11}$$

The next step is to collect all of the terms in the sum (1.11) over a single least common denominator. The first thing to notice is that, by (1.10), each and every denominator in (1.11) contains the same factor $P(n,k)$, so $P(n,k)$ will be in the least common denominator that we are constructing.

We introduce the symbol $x^+ = \max(x,0)$, where x is a real number. Then for all real numbers a, b we have

$$\max\{|aj+bi| : aj+bi<0; 0\leq i\leq I; 0\leq j\leq J\} = (-a)^+ J + (-b)^+ I,$$

and

$$\max\{aj+bi : aj+bi\geq 0; 0\leq i\leq I; 0\leq j\leq J\} = a^+ J + b^+ I,$$

so the 'x^+' notation is a device that saves the enumeration of many different cases.

Now we can address the question of finding the least common multiple of all of the δ_{ij}'s in (1.11). For each s, a common multiple of all of the falling factorials that appear there will be the one whose first argument is largest, i.e.,

$$\mathrm{ff}((a_s)^+ J + (b_s)^+ I, a_s n+b_s k+c_s),$$

and a common multiple of all of the rising factorials that appear there will similarly be

$$\mathrm{rf}((-u_s)^+J+(-v_s)^+I, u_sn+v_sk+w_s).$$

Consequently the least common denominator of the expression (1.11), when that expression is thought of as a rational function of k, with n as a parameter, surely divides $P(n,k)$ times

$$\prod_{s=1}^{uu}\mathrm{ff}((a_s)^+J+(b_s)^+I; a_sn+b_sk+c_s)\prod_{s=1}^{vv}\mathrm{rf}((-u_s)^+J+(-v_s)^+I; u_sn+v_sk+w_s). \quad (1.12)$$

Therefore we can clear (1.11) of fractions if we multiply it through by (1.12). The result of multiplying (1.11) through by (1.12) will be the polynomial in k

$$\sum_{i=0}^{I}\sum_{j=0}^{J}a_{ij}(n)\nu_{ij}(n,k)\frac{\Delta}{\delta_{ij}(n,k)}, \quad (1.13)$$

in which Δ is the common denominator in (1.12).

In order to prove the theorem we must show that if I and J are large enough, then the system of linear equations in the unknown a_{ij}'s that one obtains by equating to zero the coefficient of every power of k that appears in (1.13) actually has a nontrivial solution. This will surely happen if the number of unknowns exceeds the number of equations.

Indeed, the number of unknown a_{ij}'s is obviously $(I+1)(J+1)$. The number of equations that they must satisfy is the number of different powers of k that appear in (1.13). We claim that the number of different powers of k that appear there grows only linearly with I and J, that is, as $c_1I+c_2J+c_3$, where the c's are independent of I, J. This claim would be sufficient to prove the theorem because then the number of unknowns would grow like IJ, for large I and J, whereas the number of equations would grow only as $c_1I+c_2J+c_3$. Hence for large enough I, J the latter would be less than the former.

Since the degree in k of each rising factorial and each falling factorial that appears in (1.13) grows linearly with I, J, and there are only a fixed number of each of them,

the degrees in k of all of the ν's, δ's and Δ grow linearly with I, J. Hence the claim is clearly true, and the proof of the main theorem is complete. A more detailed argument, which we omit here, shows that the values I^* and J^* that are in the statement of the theorem are already sufficiently large. □

Example 1.4. *The classical Laguerre polynomials is defined by*

$$L_n(x) = \sum_k (-1)^k \binom{n}{k} \frac{x^k}{k!}, \quad n = 0, 1, 2, \ldots,$$

We'll estimate the order of a two-variable recurrence that is satisfied by the summand

$$F(n,k) = (-1)^k \binom{n}{k} \frac{x^k}{k!}, \quad n = 0, 1, 2, \ldots,$$

which can be written as

$$F(n,k) = \frac{n!}{k!(n-k)!} \frac{1}{k!} (-x)^k, \quad n = 0, 1, 2, \ldots. \tag{1.14}$$

The "Fundamental Theorem", Theorem 1.1 *above, guarantees that this F satisfies a recurrence. To estimate the order of the recurrence, identify the specific F in* (1.14) *with the general form in* (1.5) *above by taking $P(n,k) = 1$, $uu = 1, vv = 3, x = -x, (a_1, b_1, c_1) = (1, 0, 0)$ and for the three (u, v, w) vectors,*

$$(0, 1, 0), (1, -1, 0), (0, 1, 0)$$

Then for the quantitative estimates provided by the theorem, namely the (I^*, J^*) of (1.14)*, we find $J^* = 3, I^* = 4$. Hence there is surely a recurrence for $F(n,k)$ of the form*

$$\sum_{i=0}^{4} \sum_{j=0}^{3} a_{ij}(n) F(n-j, k-i) = 0,$$

in which the a_{ij}'s are polynomials in n, and are not all zero. □