Guessing a Conjecture in Enumerative Combinatorics and Proving It with a Computer Algebra System

Alain Giorgetti
INRIA Nancy - Grand Est / CASSIS project
LIFC, University of Franche-Comté,
16 route de Gray, 25030 Besançon, France
alain.giorgetti@univ-fcomte.fr

Abstract

We present a theorem-proving experiment performed with a computer algebra system. It proves a conjecture about the general pattern of the generating functions counting rooted maps of given genus. These functions are characterized by a complex non-linear differential system between generating functions of multi-rooted maps. Establishing a pattern for these functions requires a sophisticated inductive proof. Up to now these proofs were made by hand. This work is the first computer proof of this kind of theorem. Symbolic computations are performed at the same abstraction level as the hand-made proofs, but with a computer algebra system. Generalizing this first success may significantly help solving algebraic problems in enumerative combinatorics.

1 Introduction

This work shows how a computer algebra system can help establishing new results in enumerative combinatorics. It is illustrated by the example of a recent conjecture about the general pattern of generating functions counting rooted maps by genus.

The general context is Problem 6 identified by Bender [2] in his list of ten unsolved problems in map enumeration. This problem is to find a “simple formula” defining the generating function $M_g(z)$ counting rooted maps of genus g by number of edges (exponent of z) for each positive genus. Rooted maps are combinatorial objects that were first enumerated by Tutte [7, 8] in the 1960’s. A common pattern for all the $M_g(z)$, where g ranges over the positive integers, was first proposed in [3]. Each $M_g(z)$ was proved to be expressible as a rational function of $\rho = \sqrt{1-12z}$. However there is an unknown polynomial of ρ in the numerator of this function. An upper bound for its degree was conjectured but not proved. In [1] we provide the first proof of a more precise pattern, with a maximal degree for each unknown polynomial, when counting by number of vertices and faces. Focusing back on counting by number of edges, we [9] prove from it that a general pattern for the generating function $M_g(z)$ is

$$M_g(z) = m^{2g}(1-2m)^{4-5g}(1-3m)^{2g-2}(1-6m)^{3-5g}P_g(m), \tag{1}$$

where $m = \dfrac{1-\sqrt{1-12z}}{6}$ and $P_g(m)$ is a polynomial of degree $6g-6$. After computing the explicit formulas for $g=1$ to $g=6$, we [9] conjecture that this polynomial is divisible by $(1-2m)^{2g-2}$ for all $g \geq 1$. The proof is obvious for $g=1$. The present work proves this conjecture for $g \geq 2$.

All the formerly mentioned proofs of general patterns were made by hand or with minimal computer assistance. These proofs are long, tedious and subject to errors. We expect to avoid errors and to reduce the proof construction effort by assisting it with a computer. The proof difficulty does not come from the underlying logical theory but from the size of the recursive definition of the polynomials $P_g(m)$. They indeed depend on two other families of polynomials. A challenge is to generalize the initial conjecture by guessing a more general conjecture for all the involved polynomials. Symbolic computations help to discover this generalized conjecture. Then three proofs by induction are constructed by substitution and algebraic computations. Difficulties are reduced by replacing the exact system of equations by an abstraction of it that preserves the property to be proved.

The price to pay for computer assistance is to encode the problem and strategies for its resolution in a computer language. In the present case the problem is essentially algebraic. The definition of the polynomials $P_g(m)$ is composed of sums and products of polynomials (and anecdotally of some rational functions). This is a good reason for choosing a computer algebra system rather than a theorem prover. Certain unknown powers of $(1-2m)$ are conjectured to depend linearly on certain parameters. This idea comes from previous experience but is also motivated by the hope of obtaining a linear system to solve the generalized conjecture. Here again a theorem prover is not needed. The linear systems to be solved are of small size. Linear systems of equalities are solved by Gaussian elimination [6]. Linear systems of inequalities are solved by Fourier-Motzkin elimination [6] or with the simplex method [6] when it is possible to add an optimization goal. All these procedures are available in computer algebra systems.

Our contribution is to provide the first computer proof of an algebraic conjecture from enumerative combinatorics. The Maple code produces a trace of the conjectures discovered and of the three proofs by induction performed.

A definition of the polynomials $P_g(m)$ is given in Section 2. Section 3 presents the keys of an abstraction that simplifies this definition whilst preserving the divisibility property to be proved. Section 4 explains how symbolic computations help to guess a maximal power of $(1-2m)$ dividing each kind of polynomials appearing in the definition of the polynomial $P_g(m)$. Section 5 presents other symbolic computations performing proofs by induction of a divisibility property for each kind of polynomials.

2 Algebraic Problem

This section presents the large system of equations defining the polynomial $P_g(m)$. Since all the polynomials and rational functions defined hereafter are in the single indeterminate m, this indeterminate is omitted. For instance we write P_g instead of $P_g(m)$.

The polynomial P_g is defined in terms of another polynomial U_g by

$$P_g = U_g(1-m)^{4-4g}. \tag{2}$$

That polynomial is itself defined from a family of polynomials $S_g(n_1,\ldots,n_r)$ in the indeterminate m by

$$U_g = S_{g-1}(0,0) + m(1-2m)\,(1-m)^2 \sum_{j=1}^{g-1} S_j(0)S_{g-j}(0). \tag{3}$$

The goal is to construct a proof that $P_g(m)$ is divisible by $(1-2m)^{2g-2}$ for all $g \geq 1$. The proof difficulty comes from the size of the recursive definition of the polynomials $S_g(n_1,\ldots,n_r)$, called the *S-polynomials*. For any sequence $n_1,\ldots,n_r$ of non-negative integers, any non-negative integer g and any positive integer r such that $(g,r) \neq (0,1)$, the polynomial $S_g(n_1,\ldots,n_r)$ is indeed recursively defined in terms of some polynomials $S_j(p_1,\ldots,p_h)$ with j less than or equal to g. When j equals g the number h of parameters is less than or equal to r. When h equals r, the sum $p_1+\ldots+p_h$ is strictly less than $n_1 + \ldots + n_r$. It is also known [9] that the polynomials $S_g(n_1,\ldots,n_r)$ are symmetric in $n_1,\ldots, n_r$.

Before giving the recursive definition of the S-polynomials in Section 2.2 some convenient notations are introduced in Section 2.1.

2.1 Notations

For any positive integer r, $[r]$ denotes the sequence $(2,\ldots,r)$ if $r \geq 2$ and the empty sequence if $r = 1$. For any subsequence X of $[r]$, $[r]-X$ denotes the subsequence of the elements of $[r]$ that are not in X.

For any sequence $(n_2,\dots,n_r)$ of integers, N_X denotes the sequence of those n_i such that i is in X and N_j denotes the sequence $(n_2,\dots,n_{j-1},n_{j+1},\dots,n_r)$. The polynomials K_i are defined for $i \geq 0$ by $K_0 = -m$, $K_1 = -1-m$, $K_2 = -1$ and $K_i = 0$ if $i \geq 3$. The polynomials L_k are defined for $k \geq 0$ by $L_0 = -m$, $L_1 = -1-2m$, $L_2 = -2-m$, $L_3 = -1$ and $L_k = 0$ if $k \geq 4$. Finally we introduce an infinite family $(E_k)_{k\geq 1}$ of rational functions of m, all but the first two of which are polynomials, defined recursively by

$$E_1 = \frac{1}{2m(1-2m)(1-m)^2}, \qquad E_2 = \frac{-5}{2(1-m)^2}, \qquad E_3 = -1, \tag{4}$$

and

$$E_k = -m(1-2m)(1-m)^2 \sum_{i=2}^{i=k-1} E_i E_{k+1-i} \text{ for all } k \geq 4. \tag{5}$$

2.2 Recursive definition

The polynomials $S_0(n_1)$ are not defined. The recursive definition of the polynomials $S_g(n_1,\dots,n_r)$ starts with $g=0$ and $r=2$. We have

$$\begin{aligned} S_0(n_1,n_2) \;=\;& -n_2(1-6m)(1-2m)E_{n_1+n_2+2} - (n_2+1)E_{n_1+n_2+3} \\ & +2m(1-2m)(1-m)^2 \sum_{\substack{i+j+k=n_1+1 \\ i>0,k<n_1}} (-1)^{j+1}(1-6m)^j(1-2m)^j E_i S_0(k,n_2). \end{aligned} \tag{6}$$

If $(g,r) \neq (0,2)$, then $S_g(n_1,\dots,n_r) = \text{term}_1 + \text{term}_2 + \text{term}_3 + \text{term}_4$, where

$$\text{term}_1 = 2m(1-2m)(1-m)^2 \sum_{\substack{i+j+k=n_1+1 \\ i>0,k<n_1}} (-1)^{j+1}(1-6m)^j(1-2m)^j E_i S_g(k,n_2,\dots,n_r), \tag{7}$$

$$\text{term}_2 = m(1-2m)(1-m)^2 \sum_{\substack{k+l+i=n_1+1 \\ 0\leq j\leq g \\ X\subseteq[r] \\ (j,X)\neq(0,\emptyset) \\ (j,X)\neq(g,[r])}} K_i(1-6m)^i(1-2m)^i S_j(k,N_X)S_{g-j}(l,N_{[r]-X}), \tag{8}$$

$$\text{term}_3 = \sum_{i+j+k=n_1+1} K_i(1-6m)^i(1-2m)^i S_{g-1}(k,j,N_{[r]}) \tag{9}$$

and

$$\text{term}_4 = \sum_{j=2}^{r} \begin{pmatrix} n_j \sum_{k+l=n_1+n_j+2} L_k(1-6m)^{k+1}(1-2m)^{k+1} S_g(l,N_j) \\ +(n_j+1)\sum_{k+l=n_1+n_j+3} L_k(1-6m)^k(1-2m)^k S_g(l,N_j) \end{pmatrix}. \tag{10}$$

Formulas (2)-(10) are derived from formulas in [9] by replacing two parameters p and q by the parameter m. See [9] for details.

3 Abstraction

It is obvious from (2) that P_g is divisible by $(1-2m)^{2g-2}$ if and only if the same property holds for U_g. Each polynomial U_g (for $g \geq 1$) is defined by (3) as a sum of g terms. Proving that U_g is divisible by $(1-2m)^{2g-2}$ is easy if each of these terms is itself divisible by $(1-2m)^{2g-2}$. This sufficient but obviously not necessary condition is called the *term-by-term divisibility property* of (3). We conjecture that this property holds for (3) and try to prove it. Since each term in the right-hand side (RHS) of (3) involves one or two S-polynomials, we conjecture that these S-polynomials are divisible by some power of $(1-2m)$ which is high enough for the initial conjecture to be provable.

The exact system of equations (6)-(10) defining the S-polynomials, called *the S system*, is large and complex. It is replaced by a simpler one by performing the following transformations. All of them preserve the term-by-term divisibility property.

3.1 Reasoning about indefinite sums

The sum of the last $g-1$ terms in (3) is an *indefinite* sum, i.e. a generalized summation, expressed with the mathematical sign $\sum$. The complexity of the S system mainly comes from the indefinite sums it contains.

An indefinite sum is a formal expression of the form

$$\sum_F E$$

also written $\sum_F E$. It denotes the summation of the expression E for all the models of the formula F, or 0 is F is not satisfiable. Technically, the $\sum$ sign is called a *binder*, the formula F is called the *sum constraint* and the expression E is called the *summed term*. The ($\sum$ sign of the) indefinite sum binds all the variables that appear in F and that are not bound or defined earlier in the formal expression where the indefinite sum appears.

In the S system, the variables defined earlier are g, r and the n_is for $1 \leq i \leq r$. Thus the set of variables bound by the indefinite sums in the expressions (6), (7), (8) and (9) is respectively $\{i,j,k\}$, $\{i,j,k\}$, $\{k,l,i,j,X\}$ and $\{i,j,k\}$. In (10) the external $\sum$ sign binds j and the two internal $\sum$ signs bind k and l. The bound variables i, j, k and l are non-negative integers, whereas X is a finite set of positive integers, or equivalently a strictly increasing sequence of such numbers.

To prove divisibility, we essentially need the factorization property that

$$\sum_{\cdots} AB = A \sum_{\cdots} B \tag{11}$$

when no variable bound by the indefinite sum appears in expression A, formally meaning that A is independent of these variables.

We plan to apply this property to all the indefinite sums of the S system, when A is $(1-2m)^d$ and d is an expression whose variables are not bound by the indefinite sum. If an algebraic expression E is divisible by $(1-2m)^d$, i.e. can be factorized as $(1-2m)^d B$, then by Property (11) any indefinite sum $\sum_F E$, where the variables in d are not bound in F, can also be factorized as $(1-2m)^d \sum_F B$, i.e. is divisible by $(1-2m)^d$. This sufficient condition of *term-by-term divisibility* allows the proof to be established on an abstract version of the S system where each indefinite sum is replaced by its summed term. At the same time, its sum constraint is transformed as described in the sext section.

3.2 Sum constraints

The sum constraint of an indefinite sum in the S system is composed of inequalities (in the large sense, including set inclusions), disequalities and exactly one equality. In (8) the inequalities are $0 \leq j$, $j \leq g$ and $X \subseteq [r]$, the disequalities are $(j,X) \neq (0,\emptyset)$ and $(j,X) \neq (g,[r])$, and the equality is $k+l+i = n_1+1$.

The equality is used to eliminate one of the bound variables in the summed term and in the sum constraint. For instance the summed term in (6) is

$$(-1)^{j+1}(1-6m)^j(1-2m)^j E_i S_0(n_1+1-(i+j),n_2) \tag{12}$$

and the sum constraint is $i > 0 \wedge n_1 + 1 - (i + j) < n_1$ whose simplification is $i > 0 \wedge 1 < i + j$. This transformation also eliminates n_1 from the other inequality (7) where it appeared.

Then all the inequalities and disequalities are turned into global hypotheses where their variables have been renamed for unicity in the whole system. The implicit constraints that all the bound integer variables are non-negative is made explicit. For instance, the inequalities in (6) are turned into the global hypotheses $i_0 > 0$, $j_0 \geq 0$ and $1 < i_0 + j_0$. The constraints $i_0 \leq n_1 + 1$ and $j_0 \leq n_1 + 1$ are thrown away because n_1 can be arbitrarily large. The other global hypotheses are $i_1 > 0$, $j_1 \geq 0$ and $1 < i_1 + j_1$ from (7), $0 \leq j_2$, $j_2 \leq g$, $X_2 \subseteq [r]$, $(j_2, X_2) \neq (0, \emptyset)$ and $(j_2, X_2) \neq (g, [r])$ from (8), $i_3 \geq 0$ and $j_3 \geq 0$ for (9), $2 \leq j_4$, $j_4 \leq r$ and $0 \leq k$ from (10).

3.3 Length and sum of a sequence of parameters

The second simplification comes from the fact that all the polynomials $S_g(n_1, \ldots, n_r)$ are symmetric in $n_1, \ldots, n_r$. The sequence $n_1, \ldots, n_r$ is abstracted by its length r and its sum $n = n_1 + \ldots + n_r$. In the S system the expression $S_g(n_1, \ldots, n_r)$ is replaced by the expression $\tilde{S}(g, r, n)$ such that $n = n_1 + \ldots + n_r$. For instance the term (12) is replaced by

$$(-1)^{j+1}(1-6m)^j(1-2m)^j E_i \tilde{S}(0, 2, n+1-(i+j)). \tag{13}$$

Simultaneously, any set Y of integers is replaced by its cardinality c_Y and the sum n_Y of its elements. For instance the global hypothesis $X_2 \subseteq [r]$ coming from (8) is replaced by the global hypothesis $c_{X_2} \leq r - 1$. The constraint $n_{X_2} \leq n_{[r]}$ is thrown away because $n_{[r]} = n - n_1$ can be arbitrarily large.

After these simplifications, there remain two occurrences of n_2 in (6) and two occurrences of n_j in (10) as multiplicative factors. They are considered as new formal symbols.

It is planned to automate all these transformations from a symbolic representation of the S system. At the current stage of this research the simplified system is directly written by hand in a Maple file. It is claimed that this Maple code is the correct definition of the simplified system. We do not reproduce this definition here on purpose, because writing it by hand presents a risk of typographical error and translating it from the Maple code into LaTeX syntax is not yet fully automatized.

3.4 Property preservation

Property preservation does not claim for an equivalence, but only for the following entailment: if the divisibility property of $\tilde{S}(g, r, n)$ is proved on the simplified system, then the same divisibility property holds for all the polynomials $S_g(n_1, \ldots, n_r)$ such that $n = \sum_{1 \leq i \leq r} n_i$ and the simplified proof can be lifted up on the S system.

In a near future we expect to derive from a formal specification of all the simplifications a formal proof that they preserve the term-by-term divisibility property. For the moment we can only justify this fact informally. Preservation by replacement of indefinite sums by their summed term has already been justified in Section 3.1. Once the sequences of integers have been replaced by their length and sum it cannot be conjectured anymore that the polynomials $S_g(n_1, \ldots, n_r)$ are divisible by a power of $(1 - 2m)$ which directly depends on the n_is but only on their sum and cardinality. Finally, the integers n_2 and n_j replaced by formal symbols are all multiplicative factors of products where divisibility by a power of $(1 - 2m)$ has to be observed; so divisibility after replacement entails divisibility before it, with the same power.

Altogether these simplifications lead to a proof of a stronger conjecture than the initial one. In case of failure, some of them will have to be relaxed in order to find a more subtle proof argument.

4 Conjecture Synthesis

The goal in this proof step is to guess a function of g, r, and n that computes a non-negative integer d such that (i) all the polynomials $\tilde{S}(g,r,n)$ are divisible by $(1-2m)^d$, (ii) this divisibility property is provable (term by term) by induction from the equations defining these polynomials, and (iii) the degree d is high enough to prove the divisibility conjecture for U_g. We try to synthetize d as a linear function of g, r and n by translating (i) into the property that there exists four integers c_g, c_r, c_n, c_1 and a polynomial $T(g,r,n)$ such that the equality

$$\tilde{S}(g,r,n) = (1-2m)^{c_g g + c_r r + c_n n + c_1} T(g,r,n) \tag{14}$$

always holds.

But the polynomials $\tilde{S}(g,r,n)$ are also computed from expressions E_k which probably contribute to the total degree of $(1-2m)$. We also have to conjecture this contribution and prove it.

The first two expressions E_1 and E_2 are not polynomials but rational functions. The factor $(1-2m)$ appears in the denominator of E_1. For sake of simplicity we prefer to consider only polynomials and non-negative powers of $(1-2m)$. Thus we introduce the polynomial D_k related to the polynomial E_k by

$$D_k = -2m(1-2m)(1-m)^2 E_k \tag{15}$$

for all $k \geq 1$. From (4), (5) and (15) the computer easily yields the following recursive definition

$$D_1 = -1, \qquad D_2 = 5m(1-2m), \qquad D_3 = 2m(1-2m)(1-m)^2 \tag{16}$$

and

$$D_k = \frac{1}{2} \sum_{i=2}^{i=k-1} D_i D_{k+1-i} \quad \text{for all } k \geq 4 \tag{17}$$

of the infinite family $(D_k)_{k\geq 1}$.

It is again expected that (iv) there exists two integers e_k, e_1 and a polynomial $F(k)$ such that

$$D_k = (1-2m)^{e_k k + e_1} F(k) \tag{18}$$

always holds, (v) there is a term-by-term divisibility proof by induction of this conjecture, and (vi) the degree $e_k k + e_1$ is high enough to contribute to the proof of conditions (i)-(iii) about $\tilde{S}(g,r,n)$. Note that conditions (iv), (v) and (vi) are respectively similar to conditions (i), (ii) and (iii), showing that the approach can be generalized.

The next two sections translate conditions (v) and (iii) into two equivalent systems of inequalities. Then they show how conjectures are elaborated by interpretation of values extracted from these systems.

4.1 Guessing a pattern for the polynomials D_k

The Maple code translates condition (v) into the equivalent system of four inequalities

$$\{e_k + e_1 \leq 0, \quad 2e_k + e_1 \leq 1, \quad 3e_k + e_1 \leq 1, \quad 0 \leq e_k + e_1\}. \tag{19}$$

The first three inequalities come from the three base cases $k = 1,2,3$ and the last one comes from the induction step of the proof by induction of term-by-term divisibility of D_k by $(1-2m)^{e_k k + e_1}$. The Maple function `solve()` decomposes this system into two systems, depending on the sign of e_k. Because we want to maximize the degree $e_k k + e_1$ of $(1-2m)$ we choose the reduced system

$$\left\{ e_k \leq \frac{1}{2}, \quad 0 \leq e_k, \quad e_1 = -e_k \right\}, \tag{20}$$

where e_k is not negative. Unfortunately its unique solution with integral coefficients $e_k = e_1 = 0$ provides no contribution of the expressions E_k to the factorization of the polynomials $\tilde{S}(g,r,n)$.

We relax the condition that the coefficients should be integers and obtain a solution $e_k = \frac{1}{2}, e_1 = -\frac{1}{2}$ which maximizes the degree $e_k k + e_1$ of $(1-2m)$ at the value $\frac{k-1}{2}$. When k is even this degree is not an integer but a half-integer and condition (iv) is not established. We shall see in the next section that half-integers also arise from the same method applied to the polynomials U_g. We jointly discuss their interpretation and possible treatments in Section 4.3.

4.2 Guessing a pattern for the polynomials U_g and $\tilde{S}(g,r,n)$

We now apply the same method to condition (iii). We try to factorize the polynomials $\tilde{S}(g,r,n)$ with a power of $(1-2m)$ that is sufficiently high to make U_g divisible by $(1-2m)^{2g-2}$ for any $g \geq 2$.

The method proceeds as follows. Three instances of (14) are generated by setting the triple of variables (g,r,n) to the values $(g-1,2,0)$, $(j,1,0)$ and $(g-j,1,0)$. The three instances are then introduced in the RHS of the abstraction of (3) to eliminate the polynomials $\tilde{S}(g-1,2,0)$, $\tilde{S}(j,1,0)$ and $\tilde{S}(g-j,1,0)$. The result is simplified and then divided term by term by $(1-2m)^{2g-2}$. Condition (iii) is equivalent to the condition that the remaining degree of $(1-2m)$ in each term should not be negative. Due to the indefinite sum in (3) only two terms are considered: one coming from $S_{g-1}(0,0)$ and one coming from the term under the $\sum$ summation sign. The corresponding conditions respectively are

$$\forall g \,.\, g \geq 2 \Rightarrow c_g(g-1) + 2c_r + c_1 - 2g + 2 \geq 0 \tag{21}$$

and

$$\forall g \,.\, g \geq 2 \Rightarrow c_g g + 2c_r + 2c_1 - 2g + 3 \geq 0. \tag{22}$$

For $g = 2$ and $g = 3$ we know from explicit values that the divisibility property of the polynomials $\tilde{S}(g,r,n)$ is just sufficient for the corresponding property of the polynomials U_g to be true. In other words the corresponding inequalities in these conditions are equalities. The system of these four equalities for the cases $g = 2$ and $g = 3$ is over-constrained because there are only three unknowns but it admits the solution $c_g = 2$, $c_r = \frac{3}{2}$ and $c_1 = -3$, provided by the Maple function `solve()`. With this solution the two general conditions (21) and (22) are satisfied.

Condition (iii) does not determine c_n because all the n_is are 0 in (3). A value for c_n can be derived from a known S-polynomial with a non-null sum of n_i parameters. The polynomials

$$S_0(0,1) = (1-2m)(4m+1) \tag{23}$$

and

$$S_1(1,1) = (1-m)(1-2m)(16m^3 - 38m^2 + 21m - 4) \tag{24}$$

respectively provide the constraint $c_n \leq 1$ and $c_n \leq \frac{1}{2}$. We retain $c_n = \frac{1}{2}$ to complete the conjecture about the polynomials $\tilde{S}(g,r,n)$.

4.3 How to deal with half degrees?

Our best effort to guess a maximal power of $(1-2m)$ dividing the polynomials D_k and $\tilde{S}(g,r,n)$ has lead to the strange conjecture that this power is sometimes not an integer but a half-integer. How can this result be interpretated?

An accurate observation of the first values suggests that it should be possible to prove a divisibility by an integral power of $(1-2m)$. For instance a stronger conjecture for the polynomials D_k would be that D_{2k} and D_{2k-1} are divisible by $(1-2m)^k$ for $k \geq 1$. But this obversation and the previously guessed conjecture also indicate that this proof should distinguish odd and even values of the parameters k, r and n. Taking the parity of the parameters k, r and n into account would multiplying by two the size of the proof by induction for the polynomials D_k and by four the one for the polynomials $\tilde{S}(g,r,n)$. Even if this multiplication of cases can be delegated to the computer, we prefer the more compact but more abstract approach exposed in the next section.

5 Proof synthesis

Let $H(E)$ by the property that E belongs to the ring $\mathbb{Q}[m]+(1-2m)^{\frac{1}{2}}\mathbb{Q}[m]$, where $\mathbb{Q}[m]$ is the ring of polynomials in the indeterminate m. This means that the algebraic expression E is either a polynomial in the indeterminate m or the product by $(1-2m)^{\frac{1}{2}}$ of a polynomial in the indeterminate m. We denote by *the theory of H* the axioms that the property H is satisfied by all the polynomials in the indeterminate m and by the expression $(1-2m)^{\frac{1}{2}}$ and is preserved by addition and multiplication.

With the help of the property H the divisibility properties to be proved are expressed in terms of powers $\frac{k-1}{2}$ and $2g+\frac{3}{2}r+\frac{1}{2}n-3$ that can be half-integers. The proofs proceed by application of the theory of H.

There is no divisibility proof to construct for the polynomials U_g because the coefficients c_g, c_r and c_1 have been guessed so that U_g is divisible by $(1-2m)^{2g-2}$ for all $g \geq 1$, as explained in Section 4.2. The three proofs to construct concern the expressions E_k (through the polynomials D_k for simplicity), the polynomials $\tilde{S}(0,2,n)$ and the polynomials $\tilde{S}(g,r,n)$ for $(g,r) \neq (0,2)$.

5.1 Polynomials D_k

We now prove by induction on k that there exists an expression $F(k)$ such that $H(F(k))$ holds and

$$D_k = (1-2m)^{\frac{k-1}{2}} F(k) \tag{25}$$

for all $k \geq 1$. The base cases $k = 1,2,3$ are checked from (16) by instantiation of (25) and extraction of $F(1)$, $F(2)$ and $F(3)$.

The induction step consists of fixing k and assuming that there exists an expression $F(h)$ such that $H(F(h))$ holds and $D_h = (1-2m)^{\frac{h-1}{2}} F(h)$ for all $1 \leq h < k$. This induction step is computer-assisted as follows. With the Maple function `subs` three substitutions replace the three expressions D_k, D_i and D_{k+1-i} in (17) by the corresponding RHS of (25). The result after simplification is the equality

$$F(k) = \frac{1}{2} F(i) F(k+1-i) \tag{26}$$

for $k \geq 4$. The theory of H is applied to this equality to state that $H(F(i))$ and $H(F(k+1-i))$ imply $H(F(k))$. This step ends the proof for the polynomials D_k.

The polynomials D_k are intermediate expressions to obtain a general pattern for the expressions E_k. The following lemma required for the next proofs is established by elimination of D_k according to (15).

Lemma 1. *For all $k \geq 1$ there exists an expression $F(k)$ such that $H(F(k))$ holds and*

$$E_k = \frac{-(1-2m)^{\frac{k-3}{2}}}{2m(1-m)^2} F(k). \tag{27}$$

5.2 Polynomials $\tilde{S}(0,2,n)$ and $\tilde{S}(g,r,n)$

It remains to prove the following lemma by induction on g, r and n.

Lemma 2. *For any $g \geq 0$, $r > 0$ and $n \geq 0$ such that $(g,r) \neq (0,1)$ there exists an expression $T(g,r,n)$ such that $H(T(g,r,n))$ holds and*

$$\tilde{S}(g,r,n) = (1-2m)^{2g+\frac{3}{2}r+\frac{1}{2}n-3}T(g,r,n). \tag{28}$$

The goal of this section is not to sketch this proof but to explain how it is produced by Maple code. The proof construction is divided into two cases, because the polynomials $\tilde{S}(0,2,n)$ are defined an equation different from the polynomials $\tilde{S}(g,r,n)$ when $(g,r) \neq (0,2)$. The two proof cases are treated the same way as in Section 5.1.

Let A be the simplified system of equations defining $\tilde{S}(g,r,n)$ and obtained from the S system by the abstraction defined in Section 3 (where the sequences $n_1,\ldots,n_r$ are abstracted by their sum n and their length r, some sets of integers are replaced by their cardinality and the sum of their elements, some multiplicative factors are abstracted by uninterpreted symbols, and indefinite sums are replaced by their summed term).

The induction hypotheses and lemma 1 are used to replace all the occurrences of polynomials $\tilde{S}(\ldots,\ldots,\ldots)$ and expressions $E_{\ldots}$ in the RHS of the equations in A by their factorized forms. Then an iterative process considers each monomial in these RHS one by one. For each monomial the simplification functions of Maple are called to sum up the total power of $(1-2m)$. This power is divided by $(1-2m)^{2g+\frac{3}{2}r+\frac{1}{2}n-3}$ and it is observed whether the result satisfies property H.

5.3 Final remark

There remains a final deductive step from the relaxed proofs to proofs of divisibility by an integral power of $(1-2m)$. From Lemma 2 and the fact that $\tilde{S}(g,r,n)$ is a polynomial we deduce more about $T(g,r,n)$ than $H(T(g,r,n))$, namely that $T(g,r,n)$ is a polynomial when $2g+\frac{3}{2}r+\frac{1}{2}n-3$ is even and is the product of a polynomial by $(1-2m)^{\frac{1}{2}}$ when $2g+\frac{3}{2}r+\frac{1}{2}n-3$ is odd. A similar argument is required for the polynomials D_k to complete the mathematical proofs. These final arguments are not supported by the actual symbolic computations.

6 Discussion

After the coefficients have been guessed from a part of the problem in Section 4, these coefficients are checked to satisfy the remaining conditions of the problem in Section 5. We could think that it is possible to remove the checking step by converting the whole problem into a system of inequalities. This approach of *full guessing* is attractive but failed during the present experiment, because some of the generated inequalities are not linear. The resulting problem is to satisfy a first-order formula of elementary number theory (first-order arithmetic over integers) and we know from Gödel's theorem [5] that there is no decision procedure for this theory. We expect that this formula belongs to a decidable fragment of this theory but we have not identified it yet. This is why the present proof construction is not fully automated, but only computer-assisted.

Some human decisions are required. The most difficult one was to select the subproblem to submit to the guessing method. This choice was guided by the layered structure of the recursive definition of the polynomials P_g. The problem has been successfully divided into smaller sub-problems that have been solved one after the other. Some remaining non linearities required doing extra assumptions before finding a solution. Finally nonintegral powers appeared that required relaxing the conjectures. All these difficulties indicate that the initial problem was difficult.

6.1 Maple code

The conjecture and proof syntheses respectively described in Section 4 and 5 are implemented in the Maple program `abstrac.mpl`. They both start from a Maple encoding of the abstract system described in Section 3. At the present time the abstraction is performed by hand from the equations in [9] but an automation is planned.

The Maple code produces a trace in a LaTeX file. The result of its compilation is presented in Appendix A. Its first part explains the conjecture guessing process. Its second part contains the synthetized mathematical proofs by induction. All the equalities and inequalities shown in this trace are Maple expressions handled by the program to produce subsequent results. Many computed expressions are too large to be reproduced here. The Maple code writes them in another text file. It is envisaged to extend the function outputting LaTeX with line-breaking in order to fit a document width requested by the user.

6.2 Related work

The problem complexity mainly comes from the indefinite sums in the equalities composing the S system.

We need a theory for reasoning about these indefinite sums. An idea could have been to define these $\sum$ signs as a special kind of “big operators” specified in [4] for the Coq proof assistant. They indeed generalize the sum operator $(+)$ of two polynomials of m. The properties required during the proof search can certainly be found within the rich theory defined in [4]. The advantage of this theory is its generality, but it is a drawback in the present proof construction, because of the numerous prerequisites before applying it. We first have to define the ring of polynomials in m. We then have to reduce the multivariate summations to the univariate ones that are the only ones supported by this package. After all these preparations, we would have observed that the proof most often uses the lemmas gathered in the factorization property (11) that has inspired the abstraction of indefinite sums by their summed term in Section 3.1. Our approach is clearly less general but much lighter.

7 Conclusion

We have experienced constructing the proof of a conjecture of enumerative combinatorics with the help of a computer algebra system. To our knowledge it is the first strong computer assistance for this kind of conjectures.

The divisibility of the polynomials P_g by $(1-2m)^{2g-2}$ has been easily conjectured by human observation from the first computed explicit values of these polynomials. But the definition of these polynomials made it much harder to find a proof of this conjecture by hand. The definition is not complex from a mathematical point of view. Its complexity mainly comes from the indefinite sums in the equalities composing it and from the numerous parameters of the intermediate expressions introduced to decompose it. Finding a uniform way to treat all these cases is not only a way to reduce the proof search effort, but is also a key to assist it with a computer. Our proposal is a strong uniformization because the same factorization property is applied for all the indefinite sums, independently of the number and nature of the variables they bind.

The symbolic encoding of computations allows many tries to be repeated and many errors to be avoided. The symbolic computations in the present experiment are performed at the same abstraction level as the hand-made proof, but with a computer algebra system that avoids many errors and makes it possible to fix the remaining ones quickly. The code outputs a mathematical proof of the divisibility property that looks like a proof by induction written by hand, for instance in [9]. The complete code represents about 700 lines of Maple code.

Many similar conjectures remain open in this research domain, for which the same approach could be re-used. The abstraction and conjecture synthesis techniques identified and presented here are general enough to be applied to these other conjectures. It is a part of our future work in collaboration with combinatoricians.

In a commented version of [2] published on his web site in 2002, Bender concludes Problem 6 (to provide a general pattern for the generating functions of rooted maps counted by number of edges) by writing "Arquès and Giorgetti [1] may have done as much as possible". This claim leaves implicit the means that can be employed to do more than has already been done. We agree with this claim if these means are limited to our human brain faculties (in any case mine). But we disagree if the proof search can be assisted by a computer. The present computer-assisted proof synthesis justifies this disagrement. It is a first success whose generalization may significantly contribute to the solution of many algebraic problems in the mathematical field of map enumeration.

8 Acknowledgment

We would like to thank Prof. T. R. S. Walsh for his stimulating discussion by electronic mail and for his corrections to a preliminary version of the present text.

References

[1] D. Arquès and A. Giorgetti. Énumération des cartes pointées de genre quelconque en fonction des nombres de sommets et de faces. *J. Combin. Theory Ser. B*, 77(1):1–24, sep 1999.

[2] E. A. Bender. Some unsolved problems in map enumeration. *Bull. Inst. Combin. Appl*, 3:51–56, 1991.

[3] E. A. Bender and E. R. Canfield. The number of rooted maps on an orientable surface. *J. Comb. Theory, Ser. B*, 53(2):293–299, 1991.

[4] Y. Bertot, G. Gonthier, S. Ould Biha, and I. Pasca. Canonical big operators. In O. Aït Mohamed, C. Muñoz, and S. Tahar, editors, *TPHOLs*, volume 5170 of *Lecture Notes in Computer Science*, pages 86–101. Springer, 2008.

[5] K. Gödel. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I. *Monatshefte für Mathematik und Physik*, 38:173–98, 1931.

[6] A. Schrijver. *Theory of linear and integer programming*. John Wiley & Sons, Inc., New York, NY, USA, 1986.

[7] W. T. Tutte. A census of planar maps. *Canad. J. Math.*, 15:249–271, 1963.

[8] W. T. Tutte. On the enumeration of planar maps. *Bull. Amer. Math. Soc.*, 74:64–74, 1968.

[9] T. R. S. Walsh and A. Giorgetti. Efficient enumeration of rooted maps of a given orientable genus by number of faces and vertices. Submitted.

A Synthetized mathematical text

The software outputs the following trace, composed of two parts. The first part explains how the conjectures are guessed. The second part sketches mathematical proofs by induction.

A.1 Conjecture synthesis

The goal is to find six coefficients e_k, e_1, c_g, c_r, c_n and c_1 such that there exists three families $V(g)$, $T(g,r,n)$ and $F(k)$ of elements of $\mathbb{Q}[m]+(1-2m)^{\frac{1}{2}}\mathbb{Q}[m]$ such that

$$U_g = (1-2m)^{2g-2}V(g), \tag{29}$$

$$\tilde{S}(g,r,n) = (1-2m)^{c_g g+c_r r+c_n n+c_1}T(g,r,n), \tag{30}$$

$$D_k = (1-2m)^{e_k k+e_1}F(k), \tag{31}$$

$$D_k = -2m(1-2m)(1-m)^2 E_k \tag{32}$$

and the S system hold.

A.1.1 Polynomials D_k

Base cases

Case k = 1

$$(1-2m)^{e_k+e_1}F(1) = -1 \tag{33}$$

gives the constraint

$$e_k+e_1 \leq 0. \tag{34}$$

Case k = 2

$$(1-2m)^{2e_k+e_1}F(2) = -5m(-1+2m) \tag{35}$$

gives the constraint

$$2e_k+e_1 \leq 1. \tag{36}$$

Case k = 3

$$(1-2m)^{3e_k+e_1}F(3) = 2m(1-2m)(1-m)^2 \tag{37}$$

gives the constraint

$$3e_k+e_1 \leq 1. \tag{38}$$

Induction step

$$(1-2m)^{e_k k+e_1}F(k) = \frac{1}{2}(1-2m)^{2e_1+e_k k+e_k}F(i)F(k+1-i) \tag{39}$$

gives the constraint

$$0 \leq e_k+e_1. \tag{40}$$

Optimization The solution maximizing e_k is $e_1 = -\frac{1}{2}$ and $e_k = \frac{1}{2}$. With this solution, the hypothesis for the polynomials D_k is

$$D_k = (1-2m)^{\frac{k-1}{2}} F(k) \tag{41}$$

Pattern of the rational functions The hypothesis

$$E_k = -\frac{1}{2}(1-2m)^{\frac{k-3}{2}} F(k) m^{-1} (-1+m)^{-2} \tag{42}$$

is obtained by elimination of D_k.

A.1.2 Polynomials U_g

The constraints

$$2g-2 \leq c_g g - c_g + 2c_r + c_1 \tag{43}$$

and

$$2g \leq 3 + 2c_r + 2c_1 + c_g g \tag{44}$$

have to be satisfied.

A solution is $c_1 = -3$, $c_g = 2$ and $c_r = \frac{3}{2}$. The value $c_n = \frac{1}{2}$ is guessed from the case

$$S_1(1,1) = (-1+m)(-1+2m)(16m^3 - 38m^2 + 21m - 4) \tag{45}$$

A.2 Proofs by induction

A.2.1 Induction step for the polynomials D_k

After simplification the equality is

$$F(k) = \frac{1}{2} F(i) F(k+1-i) \tag{46}$$

A.2.2 Case $(g,r) = (0,2)$

Base case $(g,r,n) = (0,2,0)$

$$(1-2m)^{2c_r + c_1} T(0,2,0) = 1 \tag{47}$$

gives the constraint

$$2c_r + c_1 \leq 0 \tag{48}$$

which evaluates to true.

Induction step for $(g,r) = (0,2)$ Let $n \geq 1$. The induction hypothesis is

$$\tilde{S}(0,2,p) = (1-2m)^{2c_r + c_n p + c_1} T(0,2,p) \tag{49}$$

for all $0 \leq p < n$. The three terms in the RHS are considered one by one. The three resulting inequalities

$$2c_r + c_n n + c_1 \leq \frac{n+1}{2} \tag{50}$$

$$2c_r + c_n n + c_1 \leq \frac{n}{2} \tag{51}$$

and

$$2c_r + c_n n + c_1 \leq j - \frac{1}{2} + \frac{1}{2}i + 2c_r + nc_n + c_n - ic_n - jc_n + c_1 \tag{52}$$

are satisfied.

A.2.3 Case $(g,r) \neq (0,2)$

The induction hypothesis is

$$\tilde{S}(j,h,p) = (1-2m)^{c_g j + c_r h + c_n p + c_1} T(j,h,p) \tag{53}$$

with conditions on j, h and p too long to be reproduced here, but suitable for induction.

For term$_1$ the constraint is

$$0 \leq j - \frac{1}{2} + \frac{1}{2}i + c_n - c_n i - c_n j \tag{54}$$

which simplifies to

$$0 \leq \frac{1}{2}j \tag{55}$$

For term$_2$ the constraint is

$$0 \leq 1 + i + c_r + c_1 + c_n - c_n i \tag{56}$$

which simplifies to

$$0 \leq \frac{1}{2}i \tag{57}$$

For term$_3$ the constraint is

$$0 \leq k - c_g + c_r + c_n - c_n k \tag{58}$$

which simplifies to

$$0 \leq \frac{1}{2}k \tag{59}$$

For the first part of term$_4$ the constraint is

$$0 \leq k + 1 - c_r + 2c_n - c_n k \tag{60}$$

which simplifies to

$$0 \leq \frac{1}{2}k + \frac{1}{2} \tag{61}$$

For the second part of term$_4$ the constraint is

$$0 \leq k - c_r + 3c_n - c_n k \tag{62}$$

which simplifies to

$$0 \leq \frac{1}{2}k \tag{63}$$

All these constraints are satisfied, and this ends the proof.