Gröbner bases for enumerative combinatorics

Alin Bostan[1], Frédéric Chyzak[1], Hadrien Notarantonio[1,2], Mohab Safey El Din[2]

Inria Saclay[1] & Sorbonne Université[2]

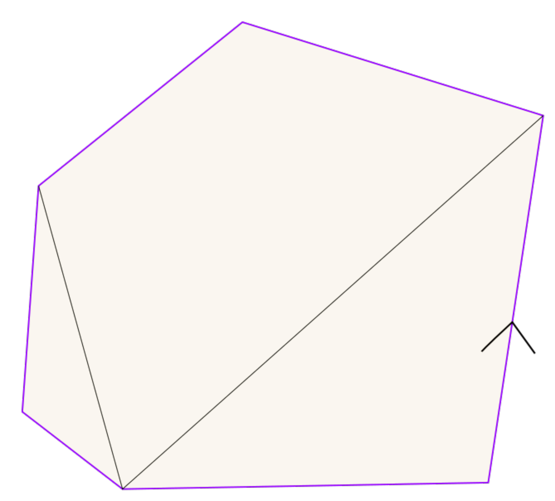
Motivation

Count

$c_n := \#\,\{$planar maps with n edges$\}$

$\downarrow$ refinement

$c_{n,d} := \#\,\{$planar maps with n edges, d of them on the external face$\}$



Solution in $\mathbb{K}[u][[t]]$

$G(t) := \sum_{n=0}^{\infty} c_n t^n$ generating function

$\downarrow$ refinement

$F(t,u) := \sum_{n=0}^{\infty} \sum_{d=0}^{n} c_{n,d} u^d t^n$ complete generating function

Functional equation [7]

$$F(t,u) = 1 + tu^2 F(t,u)^2 + tu \frac{uF(t,u) - F(t,1)}{u-1}$$

$\rightarrow$ **Nature of $F(t,1)$?** $\leftarrow$

Algebraicity result

Theorem [2] see also [6]

Let $f \in \mathbb{Q}[u]$ and $Q \in \mathbb{Q}[x,y,t,u]$. Let $F(t,u)$ be the *unique* solution in $\mathbb{Q}[u][[t]]$ of

$$F(t,u) = f(u) + tQ(F(t,u), \Delta F(t,u), t, u), \qquad \text{(FPE)}$$

where Δ is the divided difference operator $\Delta F := \frac{F(t,u)-F(t,1)}{u-1}$.

Then F is **algebraic** over $\mathbb{Q}(t,u)$.

Goal: Compute $R \in \mathbb{Q}[t,z]$ s.t. $R(t, F(t,1)) = 0$

$\Downarrow$

Compact object for $(c_n)_{n\geq 0}$, Fast computation of any c_N, Combinatorial properties

Geometric correspondence [2]

Fixed Point Equation (FPE)

$\Downarrow$ numerator

$$P(F(t,u), F(t,1), t, u) = 0$$

$\Downarrow \partial_u$

$$\partial_u F(t,u) \cdot \partial_x P(F(t,u), F(t,1), t, u) + \partial_u P(F(t,u), F(t,1), t, u) = 0$$

$u = U(t) \in \mathbb{Q}[[t]]$ solution of

$$\begin{cases} \partial_x P(F(t,u), F(t,1), t, u) = 0, \\ u \neq 1. \end{cases}$$

$\Longrightarrow$

$(F(t,U(t)), F(t,1), U(t)) \in \mathbb{Q}[[t]]^3$ solution of

$$(\mathcal{S}) \begin{cases} P(x,z,t,u) &= 0, \\ \partial_x P(x,z,t,u) &= 0 \\ \partial_u P(x,z,t,u) &= 0, \\ u \neq 1. \end{cases}$$

Direct elimination

Compute $\langle \mathcal{S} \rangle \cap \mathbb{Q}[t,z]$

Evaluation in $t = \theta_1, \ldots, \theta_{b_t} \in \mathbb{Q}$ $\rightarrow$ Compute a Gröbner basis of $\langle \mathcal{S}, t - \theta_i \rangle$ for $\prec_{\text{grevlex}}$

$\downarrow$ FGLM [4]

Deduce $R(\theta_i, z)$ s.t. $\langle R(\theta_i, z) \rangle = \langle \mathcal{S}, t - \theta_i \rangle \cap \mathbb{Q}[z]$ $\rightarrow$ Interpolate R from $R(\theta_1, z), \ldots, R(\theta_{b_t}, z)$

$b_t = \#V(\mathcal{S}, z - \mu)$, for $\mu \in \mathbb{Q}$ "generic"

$\deg(Q)$	b_t	Time (s.)	$\deg_z(R)$	$\deg_t(R)$	number of primes used
2	20	1.8	6	20	8
3	62	36	21	62	22
4	142	707	52	142	42
5	270	10744	104	270	75

$\hookrightarrow$ We consider dense polynomials for the inputs f and Q, with $\deg(f) = \deg(Q)$.

$\hookrightarrow$ Gröbner bases are computed with msolve [1] and we use *Maple*'s implementation of FGLM [4].

Hybrid Guess-and-Prove [3]

Geometry $\longrightarrow$ Guess-and-Prove paradigm [5]

Compute Gröbner bases of $\langle \mathcal{S}, z - \mu \rangle$ and $\langle \mathcal{S}, t - \theta \rangle$ for $\prec_{\text{grevlex}}$ $\rightarrow$ Deduce b_z, b_t s.t. $b_z = \#V(\mathcal{S}, t - \theta)$, $b_t = \#V(\mathcal{S}, z - \mu)$

Expand $F_1 = F(t,1) \mod t^{\sim 2b_t b_z}$ (Newton method) $\curvearrowright$ Guess $R \in \mathbb{Q}[t,z]$, $R(t, F_1) = O(t^{\sim b_t b_z})$ (Hermite-Padé) $\curvearrowright$ Prove $R(t, F_1) = O(t^{\sim 2b_t b_z})$ (multiplicity lemma)

Example: planar maps

- Direct elimination:
  - Draw μ "generic" in $\mathbb{Q}$ and compute $b_t = 5$,
  - Do direct elimination on $(\mathcal{S})$ and find $R = t(tz-1)(27t^2z^2 + (1-18t)z + 16t - 1)$,
  - Check that $27t^2z^2 + (1-18t)z + 16t - 1$ is the relevant factor.
- Hybrid Guess-and-Prove:
  - Draw θ, μ "generic" in $\mathbb{Q}$ and compute $b_t = 5, b_z = 4$,
  - Compute $F_1 = F(t,1) \mod t^{\sim 40}$,
  - Guess $R = 27t^2z^2 + (1-18t)z + 16t - 1$ s.t. $R(t, F_1) = O(t^{\sim 20})$,
  - Check that $R(t, F_1) = O(t^{\sim 40})$.

[1] J. Berthomieu, C. Eder and M. Safey El Din, msolve: A Library for Solving Polynomial Systems, ISSAC 2021 - 46th International Symposium on Symbolic and Algebraic Computation, 51–58, 2021.

[2] M. Bousquet-Mélou and A. Jehanne, Polynomial equations with one catalytic variable, algebraic series and map enumeration, J. Combin. Theory Ser. B, 96(5): 623–672, 2006.

[3] A. Bostan, F. Chyzak, H. Notarantonio and M. Safey El Din, Algorithms for discrete differential equations of order 1, ISSAC 2022 - 47th International Symposium on Symbolic and Algebraic Computation, 101–110, 2022.

[4] J. C. Faugère, P. Gianni, D. Lazard and T. Mora, Efficient computation of zero-dimensional Gröbner bases by change of ordering, J. Symbolic Comput., 16(4): 329–344, 1993.

[5] G. Pólya, Induction and analogy in mathematics, Mathematics and plausible reasoning, vol. I, Princeton University Press, Princeton, N. J., 1954.

[6] D. Popescu, General Néron desingularization and approximation, Nagoya Math. J., 104: 85–115, 1986.

[7] W. T. Tutte, On the enumeration of planar maps, Bull. AMS, 74: 64–74, 1968.