On combinatorial zeta functions

Christian Kassel

Institut de Recherche Mathématique Avancée CNRS - Université de Strasbourg Strasbourg, France

> Colloquium Potsdam 13 May 2015

• To a sequence $(a_n)_{n\geq 1}$ of numbers, it is customary to associate its generating function

$$
g(t)=\sum_{n\geq 1} a_nt^n
$$

• This is convenient because

∗ it puts an infinite number of data into a single expression

∗ very often finding equations for the generating function helps compute each individual number a_n

Another type of generating functions: Zeta functions

• To a sequence $(a_n)_{n\geq 1}$ of numbers, it is sometimes convenient to associate another generating function, a bit more involved, its zeta function:

$$
Z(t) = \exp\left(\sum_{n\geq 1} a_n \frac{t^n}{n}\right)
$$

• The ordinary generating function $g(t)$ of the sequence can be recovered from the zeta function as its logarithmic derivative:

$$
g(t) = t \frac{\text{dlog } Z(t)}{\text{d} t} = t \frac{Z't}{Z(t)} \tag{1}
$$

where $Z'(t)$ is the derivative of $Z(t)$ Note that $Z(t)$ is the unique solution of [\(1\)](#page-2-0) such that $Z(0) = 1$

• Let us give examples of zeta functions appearing in various situations

Zeta functions I. Geometric progressions

• Take the geometric progression $(a_n)_{n\geq 1}$ with $a_n = \lambda^n$ for some fixed scalar λ :

$$
g(t) = \sum_{n\geq 1} \lambda^n t^n = \frac{\lambda t}{1 - \lambda t}
$$

We deduce

$$
Z(t) = \frac{1}{1 - \lambda t} \tag{2}
$$

Observe that

- $* Z(t)$ is a rational function; we shall see more examples of rational zeta functions
- $* Z(t)$ is a "simpler" rational function than $g(t)$
- $∗$ In the special case of the constant sequence $a_n = 1$ for all $n \ge 1$,

$$
Z(t)=\frac{1}{1-t}
$$

Proof of [\(2\)](#page-3-0). We have $Z(0) = 1$ and

$$
t\frac{Z't}{Z(t)} = -t\frac{(1-\lambda t)'}{1-\lambda t} = -t\frac{-\lambda}{1-\lambda t} = \frac{\lambda t}{1-\lambda t} = g(t)
$$

• Let X be an algebraic variety defined as the set of zeroes of a system of polynomial equations with coefficients in the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

• Recall that any finite field extension of \mathbb{F}_p is of the form \mathbb{F}_q , where \mathbb{F}_q is a finite field of cardinality $q = p^n$ for some integer $n \geq 1$

• Now X has a finite number of points $a_n = |X(\mathbb{F}_{p^n})|$ in all finite fields \mathbb{F}_{p^n} , so that it makes sense to consider the zeta function

$$
Z_{X/\mathbb{F}_p}(t) = \exp\left(\sum_{n\geq 1} a_n \frac{t^n}{n}\right)
$$

introduced by Emil Artin in his Leipzig thesis (1921)

• Question. Why call this a zeta function?

To answer this question, let us consider the case when X is a point

The connection with Riemann's zeta function

• Example. Let X be a point. Then $a_n = |X(\mathbb{F}_{p^n})| = 1$ for all $n \ge 1$ and

$$
\mathsf{Z}_{X/\mathbb{F}_p(t)}=\frac{1}{1-t}
$$

• Now a point is defined over all finite fields. Putting all prime characteristics p together, we may form the global zeta function:

$$
\zeta_X(s)=\prod_{\rho \text{ prime}} Z_{X/\mathbb{F}_\rho}(\rho^{-s})
$$

• Let us compute the global zeta function when X is a point:

$$
\zeta_X(s) = \prod_{\substack{p \text{ prime} \\ p \text{ prime}}} \frac{1}{1 - p^{-s}}
$$

$$
\overset{\text{(Euler)}}{=} \sum_{n \ge 1} \frac{1}{n^s} = \zeta(s)
$$

which is the famous Riemann zeta function

Artin's zeta functions and Weil conjectures

• More examples of Artin's zeta functions.

(a) Let $X = \mathbb{A}^1$ be an affine line. Then $a_n = |\mathbb{F}_{p^n}| = p^n$ and

$$
\mathsf{Z}_{\mathbb{A}^1/\mathbb{F}_\rho}(t)=\frac{1}{1-\rho t}
$$

(b) Let $X = \mathbb{P}^1 = \mathbb{A}^1 \coprod \{\infty\}$ be a projective line. Then $a_n = p^n + 1$ and

$$
\displaystyle Z_{\mathbb{P}^1/\mathbb{F}_\rho}(t)=\frac{1}{(1-t)(1-\rho t)}
$$

• Weil conjectures. One of them is the following:

∗ If X is a quasi-projective variety (i.e. intersection of an open and of a closed subset of a projective space), then $Z_{X/\mathbb{F}_p}(t)$ is a rational function

∗ This conjecture was first proved by Dwork (Amer. J. Math. 82 (1960))

 $*$ Later $\mathsf{Deligne}$ proved all Weil conjectures and expressed $Z_{X/\mathbb{F}_p}(t)$ in terms of étale cohomology

- Let Γ be a finite connected graph (i.e. the set of vertices and the set of edges are finite, and one can pass from one vertex to another by a series of edges) Assume Γ has no vertex of degree 1 (i.e. no vertex is related to only one other vertex)
- Let a_n be the number of closed paths of length n (without backtracking)
- Y. Ihara (1966) formed the corresponding zeta function

$$
Z_{\Gamma}(t) = \exp\left(\sum_{n\geq 1} a_n \frac{t^n}{n}\right)
$$

• Theorem. The zeta function of a graph is a rational function

More precisely, ...

Ihara's zeta function: rationality

• The zeta function $Z_{\Gamma}(t)$ of a graph Γ is the inverse of a polynomial:

$$
Z_{\Gamma}(t) = \frac{1}{\det(I - tM)}
$$
\n(3)

Here M is the edge adjacency matrix of Γ defined as follows:

 \bullet M is a matrix whose entries are indexed by all couples (\vec{e},\vec{f}) of oriented edges of Γ (each edge has two orientations)

∗ By definition, $M_{\vec e,\vec f}=1$ if $\bullet \stackrel{\vec e}{\longrightarrow} \bullet \stackrel{\vec f}{\longrightarrow} \bullet$, i.e., if the terminal vertex of $\vec e$ is the initial vertex of \vec{f} (provided \vec{f} is not the edge \vec{e} with reverse orientation) ∗ Otherwise, $M_{\vec{e}, \vec{f}} = 0$

• To prove [\(3\)](#page-8-0) one checks that

 $a_n = ($ number of closed paths of length $n) = Tr(M^n)$

and one concludes with the following general fact

The zeta function of a matrix

• For any square matrix M with scalar entries (in a field, in \mathbb{Z}), define

$$
Z_M(t) = \exp\left(\sum_{n\geq 1} \operatorname{Tr}(M^n) \frac{t^n}{n}\right)
$$

Here $a_n = \text{Tr}(M^n)$ is the trace of the *n*-th power of M

• Proposition. We have Jacobi's formula

$$
Z_M(t) = \frac{1}{\det(I - tM)}
$$

• Proof. M is conjugate to an upper triangular matrix N; we have $\text{Tr}(M^n) = \text{Tr}(N^n)$ and det($I - tM$) = det($I - tN$)

∗ For Tr and det we need take care only of the diagonal elements

 $∗$ By multiplicativity we are reduced to a 1 $×$ 1-matrix $M = (λ)$, hence to a geometric progression:

$$
Z_M(t) = \frac{1}{1 - \lambda t} = \frac{1}{\det(I - tM)}
$$

Group rings

We next consider matrices with entries in a group ring

• Let G be a group (finite or infinite). Any element of the group ring $\mathbb{Z}G$ is a finite linear combination of elements of G of the form

$$
\mathsf{a}=\sum_{\mathsf{g}\in\mathsf{G}}\mathsf{a}_\mathsf{g}\mathsf{g}\qquad(\mathsf{a}_\mathsf{g}\in\mathbb{Z})
$$

• Let $\tau_0 : \mathbb{Z}G \to \mathbb{Z}$ be the linear form defined by

$$
\tau_0\left(\sum_{g\in G}a_g g\right)=a_e \qquad \text{ (e is the identity element of } G\text{)}
$$

Exercise. Prove that τ_0 is a trace map, i.e., $\tau_0(ab) = \tau_0(ba)$ for all $a, b \in \mathbb{Z}G$

• Example. If $G = \mathbb{Z}$ is the group of integers, then $\mathbb{Z} G = \mathbb{Z} [X, X^{-1}]$ is the algebra of Laurent polynomials in one variable X and $\tau_{0}\left(\sum_{k\in\mathbb{Z}}\,a_{k}X^{k}\right)=a_{0}$ is the constant coefficient of this Laurent polynomial

Matrices over group rings

• Let $M \in M_d(\mathbb{Z}G)$ be a $d \times d$ -matrix with entries in the group ring $\mathbb{Z}G$. Set

$$
\tau(M)=\tau_0\left(\text{Tr}(M)\right)=\sum_i\,\tau_0(M_{i,i})\in\mathbb{Z}
$$

• Definition. The zeta function of a matrix $M \in M_d(\mathbb{Z}G)$ is given by

$$
Z_M(t) = \exp\left(\sum_{n\geq 1} \tau(M^n) \, \frac{t^n}{n}\right)
$$

• If G is the trivial group, then $\mathbb{Z}G = \mathbb{Z}$ and $\tau(M^n) = \text{Tr}(M^n)$. Therefore,

$$
Z_M(t)=\frac{1}{\det(I-tM)}
$$

This again is a rational function

• Question. What can we say for a general group G?

Finite groups

• Proposition. Let G be a finite group of order N. For any $M \in M_d(\mathbb{Z}G)$,

$$
Z_M(t) = \left(\frac{1}{\det(I - tM')}\right)^{1/N} \tag{4}
$$

for some $M' \in M_{dN}(\mathbb{Z})$

• Proof. It follows from a simple trick. We show how it works for $d = 1$.

 $*$ To $a = \sum_{g \in G} \, a_g g \in \mathbb{Z} G$ associate the matrix $M_a \in M_N(\mathbb{Z})$ of the multiplication by a in a basis $\{g_1, \ldots, g_N\}$ of $\mathbb{Z}G$. It is easy to check that

$$
\tau(a)=\tau_0(a)=a_e=\frac{1}{N}\operatorname{Tr}(M_a)
$$

∗ Therefore,

$$
Z_{(a)}(t) = \exp \left(\sum_{n \ge 1} \tau(a^n) \frac{t^n}{n} \right) = \exp \left(\sum_{n \ge 1} \frac{1}{N} \text{Tr}(M_a^n) \frac{t^n}{n} \right)
$$

= $Z_{M_a}(t)^{1/N}$ ^(Jacobi) $1/\det(I - tM_a)^{1/N}$

So, if G is a non-trivial finite group, then $Z_M(t)$ is an algebraic function, not a rational function

• Definition. A function $y = y(t)$ is algebraic if it satisfies an equation of the form

$$
a_r(t)y^r + a_{r-1}(t)y^{r-1} + \cdots + a_0(t) = 0
$$

for some $r \ge 1$ and polynomials $a_0(t), a_1(t), \ldots, a_r(t)$ in t (not all of them 0)

 \bullet The zeta function $y=Z_M(t)=1/\det(I-tM')^{1/N}$ of (4) satisfies the algebraic equation

$$
\det(I-tM')y^N-1=0
$$

 \bullet Now we can state the main result.

The main result

• Theorem. Let G be a virtually free group and $M \in M_d(\mathbb{Z}G)$. Then $Z_M(t)$ is an algebraic function.

• Remarks. (a) A group G is virtually free if it contains a finite-index subgroup H which is free.

 $*$ A free group is virtually free: take $H = G$

* A finite group is virtually free: take $H = \{1\}$ (a free group of rank 0)

(b) The theorem is due to

 $*$ M. Kontsevich (Arbeitstagung Bonn 2011, arXiv:1109.2469) for $d = 1$,

 $*$ Christophe Reutenauer and me for $d \geq 1$ (Algebra Number Theory 2014)

• Using the finite group trick, one derives the theorem from the more precise following result:

Theorem 1. Let $G = F_N$ be a free group and $M \in M_d(\mathbb{Z}G)$. Then the formal power series $Z_M(t)$ has integer coefficients and is algebraic.

Let us now outline the proof of Theorem 1 following Kontsevich

Starting from a matrix $M \in M_d(\mathbb{Z}F_N)$,

- Step 1. Prove that $Z_M(t)$ is a formal power series with integer coefficients
- \bullet Step 2. Prove that $g_{M}(t)=t\,\operatorname{\sf dlog}(Z_{M}(t))/\operatorname{\sf dt}=t\,Z_{M}'(t)/Z_{M}(t)$ is algebraic
- Step 3. Deduce from Steps 1–2 that $Z_M(t)$ is algebraic
- Remark.
	- \triangleright Steps 1–2 use standard techniques of the theory of formal languages
	- \triangleright Step 3 follows from a deep result in arithmetic geometry

A general setup

• Let A be a set and A[∗] the free monoid on the alphabet A:

 $A^* = \{$ words from letters of the alphabet $A\}$

• Let $\mathbb{Z}\langle \langle A \rangle \rangle$ be the ring of non-commutative formal power series on A with integer coefficients. For $S \in \mathbb{Z} \langle \langle A \rangle \rangle$ we have a unique expansion of the form

$$
S = \sum_{w \in A^*} (S, w) w \quad \text{with } (S, w) \in \mathbb{Z}
$$

To such S we associate a generating function $g_S(t)$ and a zeta function $Z_S(t)$

 \bullet <code>Definition</code>. Set $a_n = \sum_{|w|=n} (S, w)$, where $|w|$ is the length of w . Then

$$
g_S(t) = \sum_{n\geq 1} a_n t^n \in \mathbb{Z}[[t]] \text{ and } Z_S(t) = \exp\left(\sum_{n\geq 1} a_n \frac{t^n}{n}\right) \in \mathbb{Q}[[t]]
$$

As above, $g_S(t)$ and $Z_S(t)$ are related by $g_S(t) = t \text{ dlog}(Z_S(t))/dt = t Z'_S(t)/Z_S(t)$

Cyclic non-commutative formal power series

\n- Definition. An element
$$
S \in \mathbb{Z} \langle \langle A \rangle \rangle
$$
 is cyclic if $* \forall u, v \in A^*, (S, uv) = (S, vu)$ and $* \forall w \in A^* - \{1\}, \forall r \geq 2, (S, w^r) = (S, w)^r$.
\n

Definition. (a) A word is primitive if it is not the power of a proper subword (b) Words w and w' are conjugate if $w = uv$ and $w' = vu$ for some u and v

• Proposition. If $S \in \mathbb{Z} \langle \langle A \rangle \rangle$ is cyclic, then we have the Euler product

$$
Z_S(t) = \prod_{[\ell]} \frac{1}{1 - (S, \ell) t^{|\ell|}} = \prod_{[\ell]} (1 + (S, \ell) t^{|\ell|} + (S, \ell)^2 t^{2|\ell|} + \cdots)
$$

where the product is taken over all conjugacy classes of non-trivial primitive words ℓ

• For the proof, take $t \, \text{dlog}/\text{d}t$ of both sides and use the following two facts: ∗ any word is the power of a unique primitive word $*$ if w is of length n, then there are n words conjugate to w, all of them of length n

• Corollary. If
$$
S \in \mathbb{Z} \langle \langle A \rangle \rangle
$$
 is cyclic, then $Z_S(t)$ has integer coefficients

Algebraic non-commutative formal power series

- One can define the notion of an algebraic non-commutative power series S Essentially, it means that S satisfies an algebraic system of equations
- Passing from $S \in \mathbb{Z} \langle \langle A \rangle \rangle$ to $g_S(t) \in \mathbb{Z}[[t]]$ consists in replacing in S each letter of the alphabet A by the variable t . Therefore,

if S is algebraic, then $g_S(t)$ is an algebraic function

• Relation between algebraicity and virtually free groups.

Let G be a group and $A \subset G$ be a subset generating G as a monoid. Consider

$$
S_G = \sum w \in \mathbb{Z} \langle\!\langle A \rangle\!\rangle
$$

where the sum is taken over all words $w \in A^*$ representing the identity element of G (The series S_G incarnates the word problem for G)

Theorem (Muller & Schupp, 1983) The non-commutative power series S_G is algebraic if and only if the group G is virtually free

• To a matrix $M \in M_d(\mathbb{Z}F_N)$ there is a procedure to associate a formal power series $S \in \mathbb{Z} \langle \langle A \rangle \rangle$ satisfying:

∗ the generating functions coincide:

$$
gs(t) = g_M(t)
$$
 and $Z_s(t) = Z_M(t)$

- ∗ S is cyclic
- ∗ S is algebraic

• Consequence. $Z_M(t)$ is a formal power series with integer coefficients and its logarithmic derivative $g_M(t)$ is algebraic

Step 3: An algebraicity theorem

To conclude we need the following

• Lemma. If $f \in \mathbb{Z}[[t]]$ is a formal power series with integer coefficients and t dlog f/dt is algebraic, then f is algebraic

• Remark. The integrality condition ("with integer coefficients") is crucial: the transcendental formal power series

$$
f(t) = \exp(t) = \sum_{n\geq 0} \frac{t^n}{n!}
$$

has a logarithmic derivative t dlog $f/dt = t$ which is algebraic (even rational)

• This lemma belongs to a list of similar results, such as the 19th century result: If $f \in \mathbb{Z}[[t]]$ is a formal power series with integer coefficients and its derivative is rational, then f is a rational function

But passing from "rational" to "algebraic" is a more challenging problem, having received an answer only in the last 30 years

• Problem. Find an elementary proof of the lemma!

• The Grothendieck-Katz conjecture is a very general, mainly unproved, algebraicity criterion:

If Y' = AY is a linear system of differential equations with $A \in M_r(\mathbb{Q}(t))$, then it has a basis of solutions which are algebraic over $\mathbb{Q}(t)$ if and only, for all large enough prime integers p, the reduction modulo p of the system has a basis of solutions that are algebraic over $\mathbb{F}_p(t)$

- Instances of the conjecture have been proved
	- \triangleright by Yves André (1989) following Diophantine approximation techniques of D. V. and G. V. Chudnovsky (1984),
	- \blacktriangleright and by Jean-Benoît Bost (2001) using Arakelov geometry
- These instances cover the system consisting of the differential equation

$$
y'=\frac{\mathcal{g}_M}{t}y
$$

which is of interest to us, and thus yield the desired lemma

(for an overview, see Bourbaki Seminar by Chambert-Loir, 2001)

An example by Kontsevich

• Let $G = F_2$ the free group with generators X and Y and

$$
M = X + X^{-1} + Y + Y^{-1} \in \mathbb{Z}F_2 = M_1(\mathbb{Z}F_2)
$$

• Easy to check that

$$
\tau(M^n) = |\text{ words in the alphabet } \{X, X^{-1}, Y, Y^{-1}\}
$$

of length *n* and **representing the identity element of** F_2 |

• Kontsevich proves the following algebraic expression for $Z_M(t)$:

$$
Z_M(t) = \frac{2}{3} \cdot \frac{1 + 2\sqrt{1 - 12t^2}}{1 - 6t^2 + \sqrt{1 - 12t^2}}
$$

Expanding $Z_M(t)$ as a formal power series, we obtain

$$
Z_M(t) = 1 + 2 \sum_{n \geq 1} 3^n \frac{(2n)!}{n!(n+2)!} t^{2n} \in \mathbb{Z}[[t]]
$$

See Sequence A000168 in Sloane's On-Line Encyclopedia of Integer Sequences

The zeta function is not always algebraic

• For $M = X + X^{-1} + Y + Y^{-1} \in \mathbb{Z}F_2 = M_1(\mathbb{Z}F_2)$ we observed that

 $\tau(M^n)=|\textrm{ words in the alphabet }\{X,X^{-1},Y,Y^{-1}\}$

of length *n* and representing the identity element of F_2

In particular, $\tau(XYX^{-1}Y^{-1})=0$

• Now, if $G = \mathbb{Z} \times \mathbb{Z}$ is the free abelian group with generators X and Y, then

$$
XYX^{-1}Y^{-1}=1
$$

and so $\tau(XYX^{-1}Y^{-1})=1$

• Taking $M=X+X^{-1}+Y+Y^{-1}$ now in $\mathbb{Z}[\mathbb{Z}\times\mathbb{Z}]=\mathbb{Z}[X,X^{-1},Y,Y^{-1}],$ one shows that

$$
\tau(M^n) = \binom{2n}{n}^2 \sim \frac{1}{\pi} \, \frac{16^n}{n}
$$

By a criterion due to Eisenstein (1852), the presence of $1/n$ in the previous asymptotics implies that the generating function $g_M(t)$, hence $Z_M(t)$, is not algebraic

The algebraic curve behind Kontsevich's example

• For $M = X + X^{-1} + Y + Y^{-1} \in \mathbb{Z}F_2$ the function $y = Z_M(t)$ satisfies the quadratic equation

$$
27t^4y^2 - (18t^2 - 1)y + (16t^2 - 1) = 0
$$
\n(5)

This equation defines an algebraic curve C_M over $\mathbb Z$

What can we say about the curve C_M ? about its genus?

 \bullet How to compute the genus from an equation of the form $\sum_{i,j\geq 0} \, a_{i,j} \, t^i y^j = 0?$

 $*$ Draw the Newton polygon which is the convex hull of the points $(i,j) \in \mathbb{R}^2$ for which $a_{i,j} \neq 0$

∗ The genus is the number of integral points of the interior of the Newton polygon

Reference. H. F. Baker, Examples of applications of Newton's polygon to the theory of singular points of algebraic functions, Trans. Cambridge Phil. Soc. 15 (1893), 403–450.

Newton polygon and genus

Equation of
$$
y = Z_M(t)
$$
 for $M = X + X^{-1} + Y + Y^{-1}$:

$$
27t^4y^2 - (18t^2 - 1)y + (16t^2 - 1) = 0
$$

The contour of the Newton polygon is in red It contains 2 interior integral points marked \times Therefore genus $= 2$

The algebraic curve behind a matrix

• For $M = X + X^{-1} + Y + Y^{-1}$, we have the formal power series expansion

 $Z_M(t) = 1 + 2t^2 + 9t^4 + 54t^6 + 378t^8$ $+ 2916 t^{10} + 24057 t^{12} + 208494 t^{14}$ $+ 1876446 t^{16} + 17399772 t^{18} + 165297834 t^{20} + \cdots$

The function $y = Z_M(t)$ satisfies the quadratic equation

$$
27t^4y^2 - (18t^2 - 1)y + (16t^2 - 1) = 0
$$

- For a general matrix $M \in M_d(\mathbb{Z}F_N)$, what are the connections between ∗ the entries of M,
	- ∗ the integer coefficients of the formal power series $Z_M(t)$,
	- * the integer coefficients of an algebraic equation satisfied by $Z_M(t)$,
	- ∗ the integral coordinates of the vertices of the Newton polygon of the equation?

Any idea?

• Y. André, Sur la conjecture des p-courbures de Grothendieck et Katz, Geometric aspects of Dwork theory, Vol. I, II, 55–112, Walter de Gruyter GmbH & Co. KG, Berlin, 2004.

• J.-B. Bost, Algebraic leaves of algebraic foliations over number fields, Publ. Math. Inst. Hautes Etudes Sci. 93 ´ (2001), 161–221.

• A. Chambert-Loir, Théorèmes d'algébricité en géométrie diophantienne (d'après J.-B. Bost, Y. André, D. & G. Chudnovsky), Séminaire Bourbaki, Vol. 2000/2001, Astérisque No. 282 (2002), Exp. No. 886, viii, 175–209.

• D. V. Chudnovsky, G. V. Chudnovsky, Applications of Padé approximations to the Grothendieck conjecture on linear differential equations, Number theory (New York, 1983–84), 52–100, Lecture Notes in Math., 1135, Springer, Berlin, 1985.

• C. Kassel, C. Reutenauer, Algebraicity of the zeta function associated to a matrix over a free group algebra, Algebra Number Theory 8-2 (2014), 497–511; doi:10.2140/ant.2014.8.497; arXiv:1303.3481

• M. Kontsevich, Noncommutative identities, talk at Mathematische Arbeitstagung 2011, Bonn; arXiv:1109.2469v1

• D. E. Muller, P. E. Schupp, Groups, the theory of ends, and context-free languages, J. Comput. System Sci. 26 (1983), 295–310.

• The On-Line Encyclopedia of Integer Sequences (2010), http://oeis.org

Ich danke für Ihre Aufmerksamkeit

Thank you for your attention!