Exceptional algebraic values of E-functions

Tanguy Rivoal,
CNRS and Université Grenoble Alpes

joint work with Boris Adamczewski, CNRS and Université Lyon 1

Workshop "Computer Algebra in Combinatorics",
ESI Wien, 17/11/2017

Definition of E-functions

We fix an embedding of $\overline{\mathbb{Q}}$ into $\mathbb{C}$.

Definition 1 (Siegel, 1929)

An E-function is a power series $F(z) = \sum_{n=0}^{\infty} \frac{a_n}{n!} z^n \in \overline{\mathbb{Q}}[[z]]$

(*i*) *$F(z)$ is solution of an homogeneous linear differential equation with coefficients in $\overline{\mathbb{Q}}(z)$.*

and there exists $C > 0$ s.t.

(*ii*) *For any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and any $n \geq 0$, $|\sigma(a_n)| \leq C^{n+1}$.*

(*iii*) *For any $n \geq 0$, there exists $d_n \in \mathbb{N}$ s.t. $0 < |d_n| \leq C^{n+1}$ and $d_n a_m \in \mathcal{O}_{\overline{\mathbb{Q}}}$ for all $0 \leq m \leq n$.*

Siegel: Eine Funktion y, deren Potenzreihe diese drei Eigenschaften hat, möge kurz eine E-Funktion genannt werden. Offenbar ist die Exponentialfunktion eine E-Funktion.

A function y whose power series has these three properties shall be called an E-function. The exponential function is obviously an E-function.

Siegel's original definition was in fact slightly more general, but both definitions are now believed to be equivalent.

Examples

Polynomial in $\overline{\mathbb{Q}}[z]$,

$$J_0(z) = \sum_{n=0}^{\infty}(-1)^n \frac{(z/2)^{2n}}{n!^2} = \sum_{n=0}^{\infty} \frac{(-1)^n \binom{2n}{n}}{4^n} \frac{z^{2n}}{(2n)!},$$

$$\sum_{n=0}^{\infty} \frac{1}{n!}\Big(\sum_{j=0}^{n} \binom{n}{j}\binom{n+j}{j}\Big) z^n = e^{3z} J_0\big(2i\sqrt{2}z\big),$$

$$\sum_{n=0}^{\infty} \frac{1}{n!}\Big(1 + \frac{1}{2} + \cdots + \frac{1}{n+1}\Big) z^n$$

$$\sum_{n_1 > n_2 > \cdots > n_k \geq 1} \frac{1}{n_1^{s_1} n_2^{s_2} \cdots n_k^{s_k}} \frac{z^{n_1}}{n_1!}, \quad s_1, \ldots, s_k \in \mathbb{Z}.$$

Non-polynomial algebraic functions, $-\log(1-z) = \sum_{n=1}^{\infty} \frac{z^n}{n}$ and $J_0(\sqrt{z})$ are not E-functions.

Structural properties of E-functions

E-functions are entire functions; they form a ring, stable by $\frac{d}{dz}$ and $\int_0^z$.

Its units are of the form $\alpha e^{\beta z}$, where $\alpha \in \overline{\mathbb{Q}}^*$ and $\beta \in \overline{\mathbb{Q}}$ (André 2000).

The generalized hypergeometric function

$$ {}_pF_q \left[\begin{matrix} a_1, \dots, a_p \\ b_1, \dots, b_q \end{matrix} ; z \right] := \sum_{n=0}^{\infty} \frac{(a_1)_n \cdots (a_p)_n}{(b_1)_n \cdots (b_q)_n} \frac{z^n}{n!}, $$

is an E-function iff $p = q$ and the a_j's and b_j's are in $\mathbb{Q}$.

Siegel's problem: Is any E-function a finite linear combination (over $\overline{\mathbb{Q}}(z)$) of finite products of ${}_pF_p$ series?

The answer is yes if the E-function satisfies a linear differential equation of order ≤ 2. But the question is still open for E-functions of order ≥ 3.

Diophantine properties of the exponential function

Siegel defined E-functions to generalize the Diophantine properties of exp.

Theorem 1 (Hermite-Lindemann)

For any $\alpha \in \overline{\mathbb{Q}}^*$, $e^\alpha \notin \overline{\mathbb{Q}}$.

More generally,

Theorem 2 (Lindemann-Weierstrass)

Let $\alpha_1, \ldots, \alpha_k \in \overline{\mathbb{Q}}$ be $\mathbb{Q}$-linearly independent. Then $e^{\alpha_1}, \ldots, e^{\alpha_k}$ are $\overline{\mathbb{Q}}$-algebraically independent.

Equivalently:

Let $\alpha_1, \ldots, \alpha_k \in \overline{\mathbb{Q}}$ be pairwise distinct. Then $e^{\alpha_1}, \ldots, e^{\alpha_k}$ are $\overline{\mathbb{Q}}$-linearly independent.

The Siegel-Shidlovskii Theorem

$Y(z) = {}^t(F_1(z), \dots, F_n(z))$ a vector of E-functions solution of a differential system $Y'(z) = M(z)Y(z)$ where $M(z) \in M_n(\overline{\mathbb{Q}}(z))$.

$T(z) \in \overline{\mathbb{Q}}[z]$ the least common denominator of the entries of $M(z)$.

Theorem 3 (Siegel-Shidlovskii 1929, 1956)

For any $\alpha \in \overline{\mathbb{Q}}$ s.t. $\alpha T(\alpha) \neq 0$,

$$\mathrm{degtr}_{\overline{\mathbb{Q}}(z)}\big(F_1(z), \dots, F_n(z)\big) = \mathrm{degtr}_{\overline{\mathbb{Q}}}\big(F_1(\alpha), \dots, F_n(\alpha)\big).$$

If $\alpha_1, \dots, \alpha_n$ are $\overline{\mathbb{Q}}$-linearly independent, $\mathrm{degtr}_{\overline{\mathbb{Q}}(z)}(e^{\alpha_1 z}, \dots, e^{\alpha_n z}) = n$.

Problem 1: If $\mathrm{degtr}_{\overline{\mathbb{Q}}(z)}(F_1(z), \dots, F_n(z)) < n$, the theorem does not imply that $F_1(\alpha) \notin \overline{\mathbb{Q}}$ at any $\alpha \in \overline{\mathbb{Q}}$ s.t. $\alpha T(\alpha) \neq 0$.

Problem 2: It does not say anything about the Diophantine nature of $F_1(\alpha)$ when $T(\alpha) = 0$ and $\alpha \neq 0$.

Beyond Siegel and Shidlovskii

Theorem 4 (Beukers 2006)

Consider $\alpha \in \overline{\mathbb{Q}}$ s.t. $\alpha T(\alpha) \neq 0$. Assume that $P\big(F_1(\alpha), \ldots, F_n(\alpha)\big) = 0$ for some $P \in \overline{\mathbb{Q}}[X_1, \ldots, X_n]$. Then, there exists $Q \in \overline{\mathbb{Q}}[Z, X_1, \ldots, X_n]$ s.t.

$$Q\big(z, F_1(z), \ldots, F_n(z)\big) = 0 \quad \text{and} \quad Q(\alpha, X_1, \ldots, X_n) = P(X_1, \ldots, X_n).$$

Theorem 5 (Beukers' Corollary 1.4)

Assume that $F_1(z), \ldots, F_n(z)$ are $\overline{\mathbb{Q}}(z)$-linearly independent. Then for any $\alpha \in \overline{\mathbb{Q}}$ s.t. $\alpha T(\alpha) \neq 0$, the number $F_1(\alpha), \ldots, F_n(\alpha)$ are $\overline{\mathbb{Q}}$-linearly independent.

When $T(\alpha) = 0$, the relation

$$0 = \lim_{z \to \alpha} T(z) Y'(z) = \lim_{z \to \alpha} T(z) M(z) Y(z)$$

implies that $F_1(\alpha), \ldots, F_n(\alpha)$ are $\overline{\mathbb{Q}}$-linearly dependent.

Exceptional algebraic values of E-functions

Theorem 6 (Adamczewski-R., 2017)

There exists an algorithm to perform the following tasks.

Given an E-function $f(z)$ as input, it first says whether $f(z)$ is transcendental or not.

If it is transcendental, it then outputs the finite list of algebraic numbers α such that $f(\alpha)$ is algebraic, together with the corresponding list of values $f(\alpha)$.

Other classes of arithmetic special functions, I

• A Mahlerian function is a power series $F(z) \in \overline{\mathbb{Q}}[[z]]$ s.t

$$\sum_{j=0}^{d} P_j(z)F(z^{b^j}) = 0$$

for some integers $b \geq 2$, $d \geq 1$ and P_j's in $\overline{\mathbb{Q}}[z]$. For instance,

$$\sum_{n=0}^{\infty} z^{2^n}, \qquad \prod_{n=0}^{\infty}(1 + z^{3^n}).$$

• There exist analogues of the Siegel-Shidlovskii and Beukers' Theorems, obtained by Nishioka (1990), and Adamczewski-Faverjon and Philippon (2015) respectively.

• Adamczewski-Faverjon (2016) have also found an algorithm to describe explicitly the algebraic numbers at which a given Mahlerian function takes an algebraic value.

Other classes of arithmetic special functions, II

• Siegel (1929). A G-function is a power series $\sum_{n=0}^{\infty} a_n z^n \in \overline{\mathbb{Q}}[[z]]$ s.t. $\sum_{n=0}^{\infty} \frac{a_n}{n!} z^n$ is an E-function.

Siegel: Solche Funktionen mögen G-Funktionen genannt werden; zu ihnen gehört trivialerweise die geometrische Reihe.

Such functions will be called G-functions; the geometric series is a trivial example.

• Other less trivial examples: algebraic functions/$\overline{\mathbb{Q}}(z)$, $\log(1-z)$, polylogarithms, hypergeometric series ${}_{p+1}F_p$ with rational paramaters.

• The Diophantine theory of the values taken by G-functions is much weaker. There is no general transcendence result.

• The $\overline{\mathbb{Q}}$-algebraic (in)dependence of values of G-functions at algebraic points might fall under the scope of Grothendieck *"Conjecture des périodes"* because of the Bombieri-Dwork Conjecture *"G-functions come from geometry"*.

How is the input given?

• Let $f(z) = \sum_{n=0}^{\infty} \frac{a_n}{n!} z^n$ be an E-function. By definition, $Lf(z) = 0$ for some $L \in \overline{\mathbb{Q}}[z, \frac{d}{dz}]$ or equivalently $Ra_n = 0$ for some $R \in \overline{\mathbb{Q}}[n, \mathit{Shift}]$.

The expression "Given an E-function $f(z)$" means that

(i) One knows explicitly $L \in \overline{\mathbb{Q}}(z)[\frac{d}{dz}]$ s.t. $Lf(z) = 0$.

(ii) One knows enough Taylor coefficients of $f(z)$ to be able to compute from L as many coefficients as needed.

In general, no explicit formulas are known for the solutions of a given $L \in \overline{\mathbb{Q}}(z)[\frac{d}{dz}]$.

No algorithm is known to decide if L has an E-function as solution.

(iii) An oracle guarantees that $f(z)$ is an E-function.

• In practice, an E-function is given by an explicit expression for its Taylor coefficients as a multiple hypergeometric sum.

Both L and R can then be computed in principle using algorithms à la Zeilberger.

1^{st} step: minimal equation

Input: f and L, of order r_0 and degree δ_0.

Output: $L_{\min} \in \overline{\mathbb{Q}}[z, \frac{d}{dz}] \setminus \{0\}$ such that $L_{\min} f(z) = 0$ and minimal for the order.

• Grigoriev (1991): there exist an explicit $\delta_1 = \delta_1(r_0, \delta_0)$ and an $L_{\min}$ s.t. $\deg(L_{\min}) \leq \delta_1$. Obviously, $\mathrm{ord}(L_{\min}) \leq r_0$.

• Let $1 \leq r \leq r_0$ and $0 \leq \delta \leq \delta_1$. For any $P_0(z), \ldots, P_r(z) \in \overline{\mathbb{Q}}[z]$ not all zero, of degrees $\leq \delta$, set

$$R(z) := P_0(z)f(z) + \cdots + P_r(z)f^{(r)}(z).$$

Bertrand-Beukers (1985): There exists an explicit integer $N = N(L)$ s.t.

$$R \equiv 0 \iff \mathrm{ord}_{z=0} R(z) \geq N.$$

• Deciding if $R \equiv 0$ amounts to finding a non-trivial element in the kernel of an $(r+1)(\delta+1) \times (N+1)$ matrix with algebraic entries that depend on the first $N+1$ Taylor coefficients of f.

An $L_{\min}$ will eventually be found.

2^{nd} step: minimal inhomogeneous equation

Input: f and $L_{\min}$ written in the form

$$\sum_{j=0}^{r} P_j(z) f^{(j)}(z) = 0, \qquad P_j(z) \in \overline{\mathbb{Q}}(z) \text{ and } P_r(z) \equiv 1\,.$$

Output: A minimal non-zero inhomogenous equation $L_{inhom} f(z) = 0$ of order s, with coefficients in $\overline{\mathbb{Q}}(z)$.

- Necessarily, $s \in \{r, r-1\}$.
- If $s = r - 1$, write L_{inhom} in the form

$$1 + \sum_{j=0}^{r-1} Q_j(z) f^{(j)}(z) = 0, \qquad Q_j(z) \in \overline{\mathbb{Q}}(z).$$

The Q_j's are solutions of the system

$$\begin{pmatrix} Q_0 \\ Q_1 \\ Q_2 \\ \vdots \\ Q_{r-1} \end{pmatrix}' = \begin{pmatrix} 0 & 0 & \dots & 0 & P_0 \\ -1 & 0 & \dots & 0 & P_1 \\ 0 & -1 & \dots & 0 & P_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & -1 & P_{r-1} \end{pmatrix} \begin{pmatrix} Q_0 \\ Q_1 \\ Q_2 \\ \vdots \\ Q_{r-1} \end{pmatrix}. \qquad (1)$$

• There exist algorithms to decide whether a given differential system with coefficients in $\overline{\mathbb{Q}}(z)$ has a non-zero vector of rational solutions (and then compute them) or not. For instance, Barkatou's algorithm (1999).

• If (1) has no such rational vector, then $s = r$ and we set $L_{inhom} := L_{\min}$.

• If (1) has a non-zero vector of rational solutions A_j's, then by construction of (1),

$$\sum_{j=0}^{r-1} A_j(z) f^{(j)}(z) = c \tag{2}$$

for some $c \in \overline{\mathbb{Q}}$ to be determined.

The A_j's are explicitely known and we know as many Taylor coefficients of f as needed: expanding the LHS of (2) in Laurent series at $z = 0$, the constant c can be explicitely computed.

The resulting explicit equation (2) is L_{inhom}.

3^{rd} step: capturing the exceptional algebraic values of f

Input: f and L_{inhom} of order s.

- If $s = 0$, then f is a polynomial and the algorithm stops here.
- If $s \geq 1$, then f is transcendental over $\mathbb{C}(z)$. Rewrite L_{inhom} as

$$\begin{pmatrix} 0 \\ f'(z) \\ f''(z) \\ \vdots \\ f^{(s)}(z) \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \frac{u_1(z)}{u_0(z)} & \frac{u_2(z)}{u_0(z)} & \cdots & \cdots & \cdots & \frac{u_{s+1}(z)}{u_0(z)} \end{pmatrix} \begin{pmatrix} 1 \\ f(z) \\ f'(z) \\ \vdots \\ f^{(s-1)}(z) \end{pmatrix} \tag{3}$$

where the u_j's are in $\overline{\mathbb{Q}}[z]$, with $u_0 \not\equiv 0$.

- The functions $1, f(z), \ldots, f^{(s-1)}(z)$ are $\overline{\mathbb{Q}}(z)$-linearly independent.

By Corollary 1.4, when $\alpha u_0(\alpha) \neq 0$, the numbers $1, f(\alpha), \ldots, f^{(s-1)}(\alpha)$ are $\overline{\mathbb{Q}}$-linearly independent. In particular, $f(\alpha) \notin \overline{\mathbb{Q}}$.

- In other words, if $f(\alpha) \in \overline{\mathbb{Q}}$, then $\boxed{\alpha u_0(\alpha) = 0}$.

Last steps

Goal: Given $\alpha \neq 0$ such that $u_0(\alpha) = 0$, decide whether $f(\alpha) \in \overline{\mathbb{Q}}$ or not.

• Beukers' Theorem 1.5: there exists an $(s+1) \times (s+1)$ invertible matrix $\mathcal{M}(z)$ with entries in $\overline{\mathbb{Q}}[z]$ such that

$$\begin{pmatrix} 1 \\ f(z) \\ \vdots \\ f^{(s-1)}(z) \end{pmatrix} = \mathcal{M}(z) \begin{pmatrix} e_0(z) \\ e_1(z) \\ \vdots \\ e_s(z) \end{pmatrix},$$

where the e_j's are E-functions solutions of a differential system with entries in $\overline{\mathbb{Q}}[z, 1/z]$. Their common denominator is z^b for some integer b.

• The e_j's are $\overline{\mathbb{Q}}(z)$-linearly independent. By Corollary 1.4, when $\alpha \in \overline{\mathbb{Q}}^*$, the numbers

$$e_1(\alpha), e_2(\alpha), \ldots, e_s(\alpha)$$

are $\overline{\mathbb{Q}}$-linearly independent.

• $f(\alpha) \in \overline{\mathbb{Q}}$ if and only if there exists $\lambda = (\beta, 1, 0, \ldots, 0) \in \overline{\mathbb{Q}}^{s+1}$ s.t.

$$0 = \lambda \cdot \begin{pmatrix} 1 \\ f(\alpha) \\ \vdots \\ f^{(s-1)}(\alpha) \end{pmatrix} = \lambda \mathcal{M}(\alpha) \begin{pmatrix} e_0(\alpha) \\ e_1(\alpha) \\ \vdots \\ e_s(\alpha) \end{pmatrix}.$$

Hence

$$\{\alpha \in \overline{\mathbb{Q}} : f(\alpha) \in \overline{\mathbb{Q}}\} = \\ \{\alpha \in \overline{\mathbb{Q}} : u_0(\alpha) = 0 \text{ and } \exists (\beta, 1, 0, \ldots, 0) \in \text{left kernel}\, \mathcal{M}(\alpha)\} \cup \{0\}. \quad (4)$$

• Beukers constructs the matrix $\mathcal{M}(z)$ by desingularization of (3). His procedure can be implemented.

Properties used: 1) the finite non-zero singularities of a minimal operator that annihilates an E-function are apparent (André 2000).
2) If an E-function F and $\alpha \in \overline{\mathbb{Q}}$ are s.t. $F(\alpha) \in \overline{\mathbb{Q}}$, then $\frac{F(z)-F(\alpha)}{z-\alpha}$ is an E-function (Beukers 2006).

• The set on the RHS of (4) can be explicitly computed. The algorithm stops here.

Example 1

Consider the transcendental E-function

$$f(z) = \sum_{n=0}^{\infty} \frac{n^2\binom{2n}{n}}{(n+1)^2} \frac{(z/2)^{n+1}}{n!}.$$

$$L_{min}: \quad f'''(z) + \frac{1-2z-2z^2}{z(1+z)} f''(z) - \frac{1+4z+z^2}{z^2(1+z)} f'(z) = 0. \qquad (5)$$

L_{inhom} is either (5) or is of order 2.

The differential system

$$Y'(z) = \begin{pmatrix} 0 & 0 & 0 \\ -1 & 0 & -\frac{1+4z+z^2}{z^2(1+z)} \\ 0 & -1 & \frac{1-2z-2z^2}{z(1+z)} \end{pmatrix} Y(z)$$

has the non-zero solution

$$Y(z) = \left(1, \frac{(1-z)(1-z+2z^2)}{z(1+z)}, \frac{(1-z)^2}{1+z}\right).$$

Hence,

$$L_{inhom}: \quad f(z) + \frac{(1-z)(1-z+2z^2)}{z(1+z)} f'(z) + \frac{(1-z)^2}{1+z} f''(z) = \frac{1}{2}. \quad (6)$$

$u_0(z) = z(z-1)^2$.

Here, it is not necessary to compute Beukers' matrix $\mathcal{M}(z)$. Put $z = 1$ in (6): we obtain $f(1) = \frac{1}{2}$.

Conclusion: $f(\alpha) \notin \overline{\mathbb{Q}}$ for any $\alpha \in \overline{\mathbb{Q}} \setminus \{0, 1\}$, and $f(1) = \frac{1}{2}$.

$$f(z) = \frac{1}{2} + (z-1) \sum_{n=0}^{\infty} \frac{\binom{2n}{n}}{2^{n-1} n!} z^n.$$

Example 2

The roots of u_0 are not always exceptional values for f.

Given two distinct integers $a, b \geq 1$, set $f(z) = z^a e^{az} + z^b e^{bz}$.

$$L_{min}: \quad f''(z) + \frac{1-(a+b)(1+z)^2}{z(1+z)} f'(z) + \frac{ab(1+z)^2}{z^2} f(z) = 0.$$

$L_{inhom} = L_{min}$ and $u_0(z) = z^2(1+z)$.

Hence $f(\alpha) \notin \overline{\mathbb{Q}}$ for any $\alpha \in \overline{\mathbb{Q}} \setminus \{0, -1\}$.

$f(-1) = (-1)^a e^{-a} + (-1)^b e^{-b} \notin \overline{\mathbb{Q}}$ by the Lindemann-Weierstrass Theorem.

Hence there is no exceptional $\alpha \neq 0$ for f.

But $f'(-1) = 0$ because $f'(z) = (z+1)(az^{a-1}e^{az} + bz^{b-1}e^{bz})$.