An effective version of Lindemann-Weierstrass theorem by methods of algebraic independence

Damien Roy (University of Ottawa)

Days of Transcendence (online)

celebrating Yuri Nesterenko's 75th birthday,

January 31–February 2, 2022

Lindemann-Weierstrass theorem

Two equivalent forms:

(i) If $\beta_1, \ldots, \beta_N \in \bar{\mathbb{Q}}$ are distinct, then $e^{\beta_1}, \ldots, e^{\beta_N}$ are linearly independent over $\mathbb{Q}$.

Lindemann-Weierstrass theorem

Two equivalent forms:

(i) If $\beta_1, \ldots, \beta_N \in \bar{\mathbb{Q}}$ are distinct, then $e^{\beta_1}, \ldots, e^{\beta_N}$ are linearly independent over $\mathbb{Q}$.

(ii) If $\alpha_1, \ldots, \alpha_t \in \bar{\mathbb{Q}}$ are linearly independent over $\mathbb{Q}$, then $e^{\alpha_1}, \ldots, e^{\alpha_t}$ are algebraically independent over $\mathbb{Q}$.

Lindemann-Weierstrass theorem

Two equivalent forms:

(i) If $\beta_1, \ldots, \beta_N \in \bar{\mathbb{Q}}$ are distinct, then $e^{\beta_1}, \ldots, e^{\beta_N}$ are linearly independent over $\mathbb{Q}$.

(ii) If $\alpha_1, \ldots, \alpha_t \in \bar{\mathbb{Q}}$ are linearly independent over $\mathbb{Q}$, then $e^{\alpha_1}, \ldots, e^{\alpha_t}$ are algebraically independent over $\mathbb{Q}$.

Quantitative form of (ii):

Let $0 \neq P \in \mathbb{Z}[X_1, \ldots, X_t]$ with $\boxed{\deg(P) \leq D \text{ and } H(P) = \|P\| \leq H}$.

Lindemann-Weierstrass theorem

Two equivalent forms:

(i) If $\beta_1, \ldots, \beta_N \in \bar{\mathbb{Q}}$ are distinct, then $e^{\beta_1}, \ldots, e^{\beta_N}$ are linearly independent over $\mathbb{Q}$.

(ii) If $\alpha_1, \ldots, \alpha_t \in \bar{\mathbb{Q}}$ are linearly independent over $\mathbb{Q}$, then $e^{\alpha_1}, \ldots, e^{\alpha_t}$ are algebraically independent over $\mathbb{Q}$.

Quantitative form of (ii):

Let $0 \neq P \in \mathbb{Z}[X_1, \ldots, X_t]$ with $\boxed{\deg(P) \leq D \text{ and } H(P) = \|P\| \leq H}$.

- **Mahler (1931):** $|P(e^{\alpha_1}, \ldots, e^{\alpha_t})| \geq H^{-c_1 D^t}$ if $H \geq H_0(D)$, for some non-explicit c_1 and H_0.
- **Dirichlet box principle** $\Rightarrow c_1 \geq 1/(2t!)$.

Lindemann-Weierstrass theorem

Two equivalent forms:

(i) If $\beta_1, \dots, \beta_N \in \bar{\mathbb{Q}}$ are distinct, then $e^{\beta_1}, \dots, e^{\beta_N}$ are linearly independent over $\mathbb{Q}$.

(ii) If $\alpha_1, \dots, \alpha_t \in \bar{\mathbb{Q}}$ are linearly independent over $\mathbb{Q}$, then $e^{\alpha_1}, \dots, e^{\alpha_t}$ are algebraically independent over $\mathbb{Q}$.

Quantitative form of (ii):

Let $0 \neq P \in \mathbb{Z}[X_1, \dots, X_t]$ with $\deg(P) \leq D$ and $H(P) = \|P\| \leq H$.

- **Mahler (1931):** $|P(e^{\alpha_1}, \dots, e^{\alpha_t})| \geq H^{-c_1 D^t}$ if $H \geq H_0(D)$, for some non-explicit c_1 and H_0.
- **Dirichlet box principle** $\Rightarrow c_1 \geq 1/(2t!)$.
- **Nesterenko (1977):** from his result about E-functions, one can take:

$$c_1 = (4d)^t(td^2 + d + 1) \text{ and } H_0(D) = \exp(\exp(c_2 D^{2t} \log(D+1)))$$

where $d = [K : \mathbb{Q}]$ and $K = \mathbb{Q}(\alpha_1, \dots, \alpha_t)$.

Main result

Theorem (2013). $|P(e^{\alpha_1}, \ldots, e^{\alpha_t})| \geq H^{-3dS^t} \exp\left(-(cqS)^{18S^t}\right)$

where $S = 6dt(t!)D$,

$$c = \max_{v|\infty}\{|\alpha_1|_v, \ldots, |\alpha_t|_v\},$$

$$q \in \mathbb{Z}_{>0} \text{ such that } q\alpha_1, \ldots, q\alpha_t \in \mathcal{O}_K.$$

- Thus, one can take $c_1 = 6d(6dt(t!))^t$ and $H_0(D) = \exp((cqS)^6)$.
- Improves on the measure of **Ably (1994)**,
- but worst than that of **Sert (1999)**.

Reference: Une version effective du théorème de Lindemann-Weierstrass par des méthodes d'indépendance algébrique, *L'Enseignement Mathématique, Revue Internationale*, **59** (2013), 287–306.

The method

A first proof of Lindemann-Weierstrass by purely algebraic independence method was proposed by Chudnovsky for $t \leq 3$ in 1980, followed by that of Ably in 1994.

① auxiliary function with prescribed vanishing

$\downarrow$

② Schwarz lemma

$\downarrow$

③ zero estimate

$+$

④ Criterion for algebraic independence

The method

A first proof of Lindemann-Weierstrass by purely algebraic independence method was proposed by Chudnovsky for $t \leq 3$ in 1980, followed by that of Ably in 1994.

①	auxiliary function with prescribed vanishing	**explicit construction**
	↓	
②	Schwarz lemma	**growth estimates**
	↓	
③	zero estimate	**“almost direct”**
	+	
④	Criterion for algebraic independence	**resultants**

Interpolation polynomials

Let $\mathbb{N} = \{0, 1, 2, \dots\}$. For each $\mathbf{m} = (m_1, \dots, m_t) \in \mathbb{N}^t$, set

$$\mathbf{m} \cdot \boldsymbol{\alpha} = m_1\alpha_1 + \cdots + m_t\alpha_t \quad \text{and} \quad |\mathbf{m}| = m_1 + \cdots + m_t.$$

Define also

$$\Sigma(S) = \{\mathbf{m} \in \mathbb{N}^t\,;\,|\mathbf{m}| < S\} \quad \text{and} \quad N = |\Sigma(S)| = \binom{S-1+t}{t}.$$

Interpolation polynomials

Let $\mathbb{N} = \{0, 1, 2, \dots\}$. For each $\mathbf{m} = (m_1, \dots, m_t) \in \mathbb{N}^t$, set

$$\mathbf{m} \cdot \boldsymbol{\alpha} = m_1\alpha_1 + \cdots + m_t\alpha_t \quad \text{and} \quad |\mathbf{m}| = m_1 + \cdots + m_t.$$

Define also

$$\Sigma(S) = \{\mathbf{m} \in \mathbb{N}^t \,;\, |\mathbf{m}| < S\} \quad \text{and} \quad N = |\Sigma(S)| = \binom{S-1+t}{t}.$$

For each C^∞ function $f\colon \mathbb{C} \to \mathbb{C}$ and each integer $T \geq 1$, there is a unique polynomial $p(x) \in \mathbb{C}[x]$ with $\deg(p) < NT$ such that

$$p^{(j)}(\mathbf{m} \cdot \boldsymbol{\alpha}) = f^{(j)}(\mathbf{m} \cdot \boldsymbol{\alpha})$$

for each $\mathbf{m} \in \Sigma(S)$ and $j = 0, 1, \dots, T-1$. It is given by

$$p(x) = \sum_{\mathbf{m},j} f^{(j)}(\mathbf{m} \cdot \boldsymbol{\alpha}) A_{\mathbf{m},j}(x) \quad \text{with } A_{\mathbf{m},j}(x) \in K[x].$$

① The auxiliary function

It is

$$g(x) = e^x - p(x)$$

where $p(x)$ is the interpolation polynomial for $f(x) = e^x$. Thus

$$g(x) = e^x - \sum_{\substack{\mathbf{m}\in\Sigma(S) \\ 0\le j<T}} e^{\mathbf{m}\cdot\boldsymbol{\alpha}} A_{\mathbf{m},j}(\mathbf{x}).$$

① The auxiliary function

It is

$$g(x) = e^x - p(x)$$

where $p(x)$ is the interpolation polynomial for $f(x) = e^x$. Thus

$$g(x) = e^x - \sum_{\substack{\mathbf{m}\in\Sigma(S)\\ 0\le j<T}} e^{\mathbf{m}\cdot\boldsymbol{\alpha}} A_{\mathbf{m},j}(\mathbf{x}).$$

For each $\mathbf{n} \in \mathbb{N}^t$ and $\ell \in \mathbb{N}$, we find

$$g^{(\ell)}(\mathbf{n}\cdot\boldsymbol{\alpha}) = e^{\mathbf{n}\cdot\boldsymbol{\alpha}} - \sum_{\substack{\mathbf{m}\in\Sigma(S)\\ 0\le j<T}} e^{\mathbf{m}\cdot\boldsymbol{\alpha}} A^{(\ell)}_{\mathbf{m},j}(\mathbf{n}\cdot\boldsymbol{\alpha}) = Q_{\mathbf{n},\ell}(1, e^{\alpha_1}, \dots, e^{\alpha_t}),$$

for some homogeneous polynomial $Q_{\mathbf{n},\ell} \in K[X_0, X_1, \dots, X_t]$ of degree $\max\{S-1, |\mathbf{n}|\}$.

② Growth estimate

Since $e^x = \sum_{k=0}^{\infty} x^k/k!$, we also have

$$g(x) = \sum_{k=NT}^{\infty} \frac{1}{k!}(x^k - p_k(x))$$

where $p_k(x)$ is the interpolation polynomial of x^k. The coefficient $1/k!$ makes the summands small (as in Hermite's method). We find

$$g(x) = \sum_{k=NT}^{\infty} \frac{1}{k!}\left(x^k - \sum_{\substack{\mathbf{m}\in\Sigma(S)\\ 0\le j<T}} k^{(j)}(\mathbf{m}\cdot\boldsymbol{\alpha})^{k-j}A_{\mathbf{m},j}(\mathbf{x})\right),$$

thus

$$g^{(\ell)}(\mathbf{n}\cdot\boldsymbol{\alpha}) = \sum_{k=NT}^{\infty} \frac{1}{k!}\left(k^{(\ell)}(\mathbf{n}\cdot\boldsymbol{\alpha})^{k-\ell} - \sum_{\substack{\mathbf{m}\in\Sigma(S)\\ 0\le j<T}} k^{(j)}(\mathbf{m}\cdot\boldsymbol{\alpha})^{k-j}A^{(\ell)}_{\mathbf{m},j}(\mathbf{n}\cdot\boldsymbol{\alpha})\right)$$

for each $\ell \in \mathbb{N}$ and $\mathbf{n} \in \mathbb{N}^t$.

③ Zero estimate

Recall that, for $\mathbf{n} \in \mathbb{N}^t$ and $\ell \in N$ with $|\mathbf{n}| = S$ and $\ell < T$, we have

$$g^{(\ell)}(\mathbf{n} \cdot \boldsymbol{\alpha}) = Q_{\mathbf{n},\ell}(1, e^{\alpha_1}, \ldots, e^{\alpha_t})$$

for some homogeneous polynomial $Q_{\mathbf{n},\ell} \in K[X_0, \ldots, X_t]$ of degree S.

These polynomials have no common zero in $\mathbb{P}^t(\mathbb{C})$.

Note however that, by construction, $Q_{\mathbf{m},\ell}(1, e^{\alpha_1}, \ldots, e^{\alpha_t}) = 0$ for each $\mathbf{m} \in \mathbb{N}^t$ with $|\mathbf{m}| < S$ (i.e $\mathbf{m} \in \Sigma(S)$) and $\ell = 0, \ldots, T-1$.

④ Resultant

Let $\tilde{P} \in \mathbb{Z}[X_0, \dots, X_n]$ the homogeneous polynomial of degree D such that

$$P(X_1, \dots, X_t) = \tilde{P}(1, X_1, \dots, X_t).$$

Let $\Delta \in \mathbb{Z}[\alpha_1, \dots, \alpha_t]$, $B \geq 1$ and $\delta > 0$ such that

(i) $\Delta Q_{\mathbf{n},\ell} \in \mathcal{O}_k[X_0, \dots, X_n]$,

(ii) $\max_{v|\infty} \|\Delta Q_{\mathbf{n},\ell}\|_v \leq B$,

(iii) $|\Delta Q_{\mathbf{n},\ell}(1, e^{\alpha_1}, \dots, e^{\alpha_t})| \leq \delta$.

for each $\mathbf{n} \in \mathbb{N}^t$ with $|\mathbf{n}| = S$, and each $\ell = 0, 1, \dots, T-1$.

Then, there are integer linear combinations $\tilde{Q}_1, \dots, \tilde{Q}_t$ of the polynomials $\Delta Q_{\mathbf{n},\ell}$ such that $\tilde{P}, \tilde{Q}_1, \dots, \tilde{Q}_t$ have no common zero in $\mathbb{P}^t(\mathbb{C})$, and

$$\begin{aligned} 1 &\leq \left|\mathrm{Norm}_{K/\mathbb{Q}}(\mathrm{Res}(\tilde{P}, \tilde{Q}_1, \dots, \tilde{Q}_t))\right| \\ &\leq H(P)^{dS^t} \left((t+1)^{8S} S^{2t} B\right)^{dtDS^{t-1}} \max\left\{\frac{\delta}{B}, |P(e^{\alpha_1}, \dots, e^{\alpha_t})|\right\}. \end{aligned}$$

⑤ Choice of parameters

To simplify, let c_1, c_2, c_3, ... denote quantities that depend only on c, q, d, and D. For a suitable Δ, we can take

$$B = (c_1 T^2)^T \quad \text{and} \quad \delta = \frac{B}{T^{NT}}.$$

⑤ Choice of parameters

To simplify, let c_1, c_2, c_3, ... denote quantities that depend only on c, q, d, and D. For a suitable Δ, we can take

$$B = (c_1 T^2)^T \quad \text{and} \quad \delta = \frac{B}{T^{NT}}.$$

Recall that $S = 6dt(t!)D$ and that

$$N = |\Sigma(S)| = \binom{S-1+t}{t} \geq \frac{S^t}{t!} \geq 6dtDS^{t-1}.$$

Thus we get

$$\begin{aligned} 1 &\leq c_2 H(P)^{dS^t} B^{dtDS^{t-1}} \max\left\{\frac{\delta}{B}, |P(e^{\alpha_1}, \dots, e^{\alpha_t})|\right\} \\ &\leq (c_3 H(P))^{dS^t} T^{NT/3} \max\left\{T^{-NT}, |P(e^{\alpha_1}, \dots, e^{\alpha_t})|\right\} \end{aligned}$$

⑤ Choice of parameters

To simplify, let c_1, c_2, c_3, ... denote quantities that depend only on c, q, d, and D. For a suitable Δ, we can take

$$B = (c_1 T^2)^T \quad \text{and} \quad \delta = \frac{B}{T^{NT}}.$$

Recall that $S = 6dt(t!)D$ and that

$$N = |\Sigma(S)| = \binom{S-1+t}{t} \geq \frac{S^t}{t!} \geq 6dtDS^{t-1}.$$

Thus we get

$$\begin{aligned} 1 &\leq c_2 H(P)^{dS^t} B^{dtDS^{t-1}} \max\left\{\frac{\delta}{B}, |P(e^{\alpha_1}, \ldots, e^{\alpha_t})|\right\} \\ &\leq (c_3 H(P))^{dS^t} T^{NT/3} \max\left\{T^{-NT}, |P(e^{\alpha_1}, \ldots, e^{\alpha_t})|\right\} \end{aligned}$$

If $H(P) \geq c_4$, then $(c_3 H(P))^{dS^t} \leq T^{NT/3} \leq (c_3 H(P))^{2dS^t}$ for some integer $T \geq 1$, and thus

$$|P(e^{\alpha_1}, \ldots, e^{\alpha_1})| \geq (c_3 H(P))^{-3dS^t}.$$

$\ln \|L_N\| \leq \sigma(N),$

$c_1 e^{-\tau_1 \sigma(N)} \leq |L_N(\theta)| \leq c_2 e^{-\tau_2 \sigma(N)}$

$\chi_{\mathcal{Y}}(\nu) \leq 4^{r-1} N(\mathcal{Y}) \nu^{r-1}$

Bon anniversaire!

$\gamma_2 = \left(\exp\exp[\tau \cdot d^{2m} \ln(d+1)]\right)^{-1}$

$\operatorname{trdeg}_{\mathbb{Q}} \mathbb{Q}(q, P(q), Q(q), R(q)) \geq 3$ if $0 < |q| < 1$

$\mathcal{Y}_0 < \mathcal{Y}_1 < \dots < \mathcal{Y}_{r-1} < \mathcal{Y}_r = \mathcal{Y}$