Auxiliary functions in transcendence proofs

Michel Waldschmidt

http://www.math.jussieu.fr/∼miw/

Abstract

Transcendence proofs most often involve an auxiliary function. Such functions can take several forms. Historically, the first ones were Padé approximations, in Hermite's proof of the transcendence of e (1873). Next came functions whose existence is proved by means of the Dirichlet's box principle, with the work of Thue (early 1900) and Siegel (in the 1920's). Another tool was provided by interpolation formulae, mainly Newton interpolation (involving Hermite's formulae again) in the study by G. Polya (1914) and A.O. Gel'fond (1929) of integer valued entire functions. Along these lines, recent developments are due to T. Rivoal (to appear), who renewed the forgotten rational interpolation formulae of R. Lagrange (1935). In 1991 M. Laurent introduced interpolation determinants, and two years later J.B. Bost used Arakhelov theory to prove slope inequalities, which dispens of the choice of bases.

Existence of transcendental numbers

Theorem [Liouville, 1844] *Let* α *be a real algebraic number. There exists* $\kappa > 0$ *such that, for any rational number* p/q *distinct from* α *with* $q \geq 2$,

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{q^\kappa}.$$

Corollary *Let* ξ *be a real number. Assume that for any* $\kappa > 0$ *there exists a rational number* p/q *with* $q \geq 2$ *such that*

$$0 < \left|\xi - \frac{p}{q}\right| < \frac{1}{q^\kappa}.$$

Then ξ *is transcendental.*

Proof of Liouville's inequality

α is algebraic means that there exists a non–zero polynomial $f \in \mathbf{Z}[X]$ such that $f(\alpha) = 0$.
Let d be the degree of f. Since p/q is distinct from α we have $f(p/q) \neq 0$.
Hence $q^d f(p/q)$ is a non–zero rational integer

$$|f(p/q)| \geq \frac{1}{q^d}.$$

On the other hand

$$|f(p/q)| \leq c(\alpha) \left| \alpha - \frac{p}{q} \right|.$$

Therefore

$$\left| \alpha - \frac{p}{q} \right| \geq \frac{c(\alpha)}{q^d}.$$

Auxiliary function : f.

Irrationality proofs

Early methods : Involve continued fractions.

Lambert (1767) : irrationality of π

Close relation with Padé Approximation

Hermite, (1849) :

Tout ce que je puis, c'est de refaire ce qu'a déjà fait Lambert, seulement d'une autre manière.

All I can do is to repeat what Lambert did, just in another way.

`Reference` : C. Brezinski

The long history of continued fractions and Padé approximants. Padé approximation and its applications, Amsterdam 1980, pp. 1–27, Lecture Notes in Math., **888**, Springer, Berlin-New York, 1981.

History of continued fractions and Padé approximants. Springer Series in Computational Mathematics, **12**. Springer-Verlag, Berlin, 1991.

Fourier's proof (1815) for the irrationality of e

Truncate the Taylor expansion at the origin : the auxiliary function is a polynomial (or rather the remainder : the difference between e^z and the initial polynomial).

First examples of transcendental numbers : Liouville 1844, continued fractions, fast converging series.

Idea of Ch. Hermite

Ch. Hermite (1822 - 1901).
Approximate the exponential function e^z by rational fractions $A(z)/B(z)$.
Means : Taylor developments match for the first terms.

Auxiliary function :

$$B(z)e^z - A(z)$$

with a zero at the origin of high multiplicity.

Simultaneous approximation to the exponential function

Irrationality results follow from rational approximations $A/B \in \mathbf{Q}(x)$ to the exponential function e^x.

One of Hermite's ideas is to consider *simultaneous rational approximations to the exponential function*, in analogy with Diophantine approximation.

Let $B_0, B_1, \ldots, B_m$ be polynomials in $\mathbf{Z}[x]$. For $1 \le k \le m$ define

$$R_k(x) = B_0(x)e^{kx} - B_k(x).$$

Set $b_j = B_j(1)$, $0 \le j \le m$ and

$$R = a_0 + a_1 R_1(1) + \cdots + a_m R_m(1).$$

If $0 < |R| < 1$, then $a_0 + a_1 e + \cdots + a_m e^m \neq 0$.

Hermite : approximation to the functions $1, e^{\alpha_1 x}, \ldots, e^{\alpha_m x}$

Let $\alpha_1, \ldots, \alpha_m$ be pairwise distinct complex numbers and $n_0, \ldots, n_m$ be rational integers, all ≥ 0. Set $N = n_0 + \cdots + n_m$.

Hermite constructs explicitly polynomials B_0, $B_1, \ldots,$ B_m with B_j of degree $N - n_j$ such that each of the functions

$$B_0(z)e^{\alpha_k z} - B_k(z), \quad (1 \leq k \leq m)$$

has a zero at the origin of multiplicity at least N.

Padé approximants

Henri Eugène Padé (1863 - 1953)
Approximation of complex analytic functions by rational functions.

Padé Approximants of type II

Let $f_0, \ldots, f_m$ be complex functions which are analytic near the origin and $n_0, \ldots, n_m$ be rational integers, all ≥ 0. Set $N = n_0 + \cdots + n_m$.

There are two dual points of view, giving rise to the two types of *Padé Approximants*.

Padé approximants of second type : polynomials $B_0, \ldots, B_m$ with B_j having degree $\leq N - n_j$, such that each of the functions

$$B_i(z)f_j(z) - B_j(z)f_i(z) \quad (0 \leq i < j \leq m)$$

has a zero of multiplicity $> N$.

`Reference :` N.I. Feldman and Yu.V. Nesterenko, *Number Theory IV*, Transcendental Numbers, Encyclopaedia of Mathematical Sciences, **44** (1998) Chap. 2.

Padé approximants of type I

Let $f_1, \ldots, f_m$ be complex functions which are analytic near the origin and let $n_1, \ldots, n_m$ be non-negative integers. Set $M = n_1 + \cdots + n_m$.

Padé approximants of the first type : polynomials $P_1, \ldots, P_m$ with P_j of degree $\leq n_j$ such that the function

$$P_1(z)f_1(z) + \cdots + P_m(z)f_m(z)$$

has a zero at the origin of multiplicity at least $M + m - 1$.

Studied by Ch. Hermite in 1873 and 1893.

Hermite)1893)

If $\alpha_1, \dots, \alpha_m$ are pairwise distinct complex numbers, $n_0, \dots, n_m$ non–negative integers, Hermite constructs explicitely polynomials $P_1, \dots, P_m$ with P_j of degree $n_j$such that the function

$$P_1(z)e^{\alpha_1 z} + \cdots + P_m(z)e^{\alpha_m z}$$

has a zero at the origin of multiplicity at least $n_1 + \cdots + n_m + m - 1$.

C. Hermite (1917) : further integral formula for the remainder.

Application to transcendence : effective version of the Hermite, Lindemann and Weierstraß theorems by *K. Mahler (1930).*

Transcendental functions

A complex function is called transcendental if it is transcendental over the field $\mathbf{C}(z)$, which means that the functions z and $f(z)$ are algebraically independent : if $P \in \mathbf{C}[X, Y]$ is a non-zero polynomial, then the function $P\big(z, f(z)\big)$ is not 0.

Exercise. *An entire function (analytic in $\mathbf{C}$) is transcendental if and only if it is not a polynomial.*

Example. *The transcendental entire function e^z takes an algebraic value at an algebraic argument z only for $z = 0$.*

Weierstrass question

Is–it true that a transcendental entire function f takes usually *transcendental values at algebraic arguments?*

Answers by Weierstrass (letter to Strauss in 1886), Strauss, Stäckel, Faber, van der Poorten, Gramain…

If S is a countable subset of $\mathbf{C}$ and T is a dense subset of $\mathbf{C}$, there exist transcendental entire functions f mapping S into T, as well as all its derivatives.

Also there are transcendental entire functions f such that $D^k f(\alpha) \in \mathbf{Q}(\alpha)$ for all $k \geq 0$ and all algebraic α.

Integer valued entire functions

An integer valued entire function is a function f, which is analytic in $\mathbf{C}$, and maps $\mathbf{N}$ into $\mathbf{Z}$.

Example : 2^z *is an integer valued entire function, not a polynomial.*

Question : *Are-there integer valued entire function growing slower than* 2^z *without being a polynomial ?*

Let f be a transcendental entire function in $\mathbf{C}$. For $R > 0$ set

$$|f|_R = \sup_{|z|=R} |f(z)|.$$

Integer valued entire functions

G. Pólya (1914) :
if f *is not a polynomial*
and $f(n) \in \mathbf{Z}$ *for* $n \in \mathbf{Z}_{\geq 0}$*, then*

$$\limsup_{R\to\infty} 2^{-R}|f|_R \geq 1.$$

Further works on this topic by G.H. Hardy, G. Pólya, D. Sato, E.G. Straus, A. Selberg, Ch. Pisot, F. Carlson, F. Gross,...

Arithmetic functions

Pólya's proof starts by expanding the function f into a *Newton interpolation series* at the points $0, 1, 2, \ldots$:

$$f(z) = a_0 + a_1 z + a_2 z(z-1) + a_3 z(z-1)(z-2) + \cdots$$

Since $f(n)$ is an integer for all $n \geq 0$, the coefficients a_n are rational and one can bound the denominators. If f does not grow fast, one deduces that these coefficients vanish for sufficiently large n.

Newton interpolation series

From

$$f(z) = f(\alpha_1) + (z - \alpha_1)f_1(z), \quad f_1(z) = f_1(\alpha_2) + (z - \alpha_2)f_2(z), \ldots$$

we deduce

$$f(z) = a_0 + a_1(z - \alpha_1) + a_2(z - \alpha_1)(z - \alpha_2) + \cdots$$

with

$$a_0 = f(\alpha_1), \quad a_1 = f_1(\alpha_2), \ldots, \quad a_n = f_n(\alpha_{n+1}).$$

An identity due to Ch. Hermite

$$\frac{1}{x-z} = \frac{1}{x-\alpha} + \frac{z-\alpha}{x-\alpha} \cdot \frac{1}{x-z}.$$

Repeat :

$$\frac{1}{x-z} = \frac{1}{x-\alpha_1} + \frac{z-\alpha_1}{x-\alpha_1} \cdot \left(\frac{1}{x-\alpha_2} + \frac{z-\alpha_2}{x-\alpha_2} \cdot \frac{1}{x-z} \right).$$

An identity due to Ch. Hermite

Inductively we deduce the next formula due to Hermite :

$$\frac{1}{x-z} = \sum_{j=0}^{n-1} \frac{(z-\alpha_1)(z-\alpha_2)\cdots(z-\alpha_j)}{(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_{j+1})} + \frac{(z-\alpha_1)(z-\alpha_2)\cdots(z-\alpha_n)}{(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)} \cdot \frac{1}{x-z}.$$

Newton interpolation expansion

Application. Multiply by $(1/2i\pi)f(z)$ and integrate :

$$f(z) = \sum_{j=0}^{n-1} a_j(z-\alpha_1)\cdots(z-\alpha_j) + R_n(z)$$

with

$$a_j = \frac{1}{2i\pi}\int_{\mathcal{C}} \frac{f(x)dx}{(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_{j+1})} \quad (0 \le j \le n-1)$$

and

$$R_n(z) = (z-\alpha_1)(z-\alpha_2)\cdots(z-\alpha_n)\cdot \frac{1}{2i\pi}\int_{\mathcal{C}} \frac{f(x)dx}{(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)(x-z)}.$$

Rational interpolation

René Lagrange (1935).

$$\frac{1}{x-z} = \frac{\alpha-\beta}{(x-\alpha)(x-\beta)} + \frac{x-\beta}{x-\alpha}\cdot\frac{z-\alpha}{z-\beta}\cdot\frac{1}{x-z}.$$

Iterating and integrating yield

$$f(z) = \sum_{n=0}^{N-1} B_n \frac{(z-\alpha_1)\cdots(z-\alpha_n)}{(z-\beta_1)\cdots(z-\beta_n)} + \tilde{R}_N(z).$$

Hurwitz zeta function

T. Rivoal (2006) : consider Hurwitz zeta function

$$\zeta(s,z)=\sum_{k=1}^{\infty}\frac{1}{(k+z)^s}.$$

Expand $\zeta(2,z)$ as a series in

$$\frac{z^2(z-1)^2\cdots(z-n+1)^2}{(z+1)^2\cdots(z+n)^2}.$$

The coefficients of the expansion belong to $\mathbf{Q}+\mathbf{Q}\zeta(3)$.
This produces a new proof of Apéry's Theorem on the irrationality of $\zeta(3)$.
In the same way : new proof of the irrationality of $\log 2$ by expanding

$$\sum_{k=1}^{\infty}\frac{(-1)^k}{k+z}.$$

Mixing C. Hermite and R. Lagrange

T. Rivoal (2006) : new proof of the irrationality of $\zeta(2)$ by expanding

$$\sum_{k=1}^{\infty}\left(\frac{1}{k}-\frac{1}{k+z}\right)$$

as a Hermite–Lagrange series in

$$\frac{\bigl(z(z-1)\cdots(z-n+1)\bigr)^2}{(z+1)\cdots(z+n)}.$$

Taylor series and interpolation series

Taylor series are the special case of Hermite's formula with a single point and multiplicities — they give rise to Padé approximants.

Multiplicities can also be introduced in René Lagrange interpolation.

Integer valued entire function on $\mathbf{Z}[i]$

A.O. Gel'fond (1929) : growth of entire functions mapping the Gaussian integers into themselves.
Newton interpolation series at the points in $\mathbf{Z}[i]$.

An entire function f *which is not a polynomial and satisfies* $f(a+ib) \in \mathbf{Z}[i]$ *for all* $a+ib \in \mathbf{Z}[i]$ *satisfies*

$$\limsup_{R\to\infty} \frac{1}{R^2} \log |f|_R \geq \gamma.$$

F. Gramain (1981) : $\gamma = \pi/(2e)$.
This is best possible : *D.W. Masser (1980).*

Transcendence of e^π

A.O. Gel'fond (1929).

If

$$e^\pi = 23,140\,692\,632\,779\,269\,005\,729\,086\,367\ \ldots$$

is rational, then the function $e^{\pi z}$ takes values in $\mathbf{Q}(i)$ when the argument z is in $\mathbf{Z}[i]$.

Expand $e^{\pi z}$ into an interpolation series at the Gaussian integers.

A.O. Gel'fond and Th. Schneider (1934).
Solution of Hilbert's seventh problem :
transcendence of α^β
and of $(\log \alpha_1)/(\log \alpha_2)$
for algebraic α, β, α_2 *and* α_2.

Duality between the methods of Gel'fond and Schneider :
Fourier-Borel transform.

Gel'fond and Schneider methods

Assume α, β and $\alpha^\beta = \exp(\log \alpha)$ are algebraic with $\beta \notin \mathbf{Q}$ and $\log \alpha \neq 0$. Let $K = \mathbf{Q}(\alpha, \beta, \alpha^\beta)$.

A.O. Gelfond :
The two entire functions e^z and $e^{\beta z}$ are algebraically independent, they satisfy differential equations with algebraic coefficients and they take simultaneously values in K for infinitely many z, viz. $z \in \mathbf{Z} \log \alpha$.

Th. Schneider :
The two entire functions z and $\alpha^z = e^{z \log \alpha}$ are algebraically independent, they take simultaneously values in K for infinitely many z, viz. $z \in \mathbf{Z} + \mathbf{Z}\beta$.
No use of differential equations (coefficients are not all algebraic).

Duality between Gel'fond and Schneider

A.O. Gelfond :

$$\left(\frac{d}{dz}\right)^{t_0} \left(e^{(s_1+s_2\beta)z}\right)_{z=t_1 \log\alpha}$$

Th. Schneider :

$$\left(z^{t_0}\alpha^{t_1 z}\right)_{z=s_1+s_2\beta}$$

Result :

$$(s_1+s_2\beta)^{t_0}\alpha^{t_1 s_1}(\alpha^\beta)^{t_1 s_2}.$$

Dirichlet's box principle

Gel'fond and Schneider
use an *auxiliary function*,
the existence of which follows
from Dirichlet's box principle
(pigeonhole principle,
Thue-Siegel Lemma).

Thue's work on Diophantine Approximation

A. Thue ($\sim$1910). First improvement of Liouville's inequality on a lower bound for $|\alpha - p/q|$.

Idea : in place of evaluating the values at p/q of a polynomial in a single variable (viz. the irreducible polynomial of α), consider two approximations p_1/q_1 and p_2/q_2 of α and evaluate at the point $(p_1/q_1, p_2/q_2)$ a polynomial P in two variables.

This polynomial $P \in \mathbf{Z}[X, Y]$ is constructed (or rather is shown to exist) by means of Dirichlet's box principle. The required conditions are that P has zeroes of sufficiently large order at $(0, 0)$ and at $(p_1/q_1, p_2/q_2)$. The *order* is weighted (*index* of P at a point).

One of the main difficulties that Thue had to overcome was to produce a *zero estimate* (to find a non–zero value of some derivative).

For the method to work, one needs to select the second approximation p_2/q_2 depending on the first p_1/q_1. Hence a first very sharp approximation p_1/q_1 is required.
The method provides a satisfactory result for all p/q with at most one exception (J.W.S. Cassels, H. Davenport : *upper bound for the number of solutions of Diophantine equations*).

E. Bombieri has produced examples where a sufficiently sharp approximation exists for the method to work in an effective way. Later he produced *effective refinements* to Liouville's inequality by extending the argument.

Further improvement by C.L. Siegel in the 1920's – and application of the idea to transcendence questions (periods of elliptic functions).

K. F. Roth (1955) : introduces many variables – get the essentially sharpest possible exponent in Liouville's inequality, namely $2+\epsilon$ in place of the degree d of θ.

W.M. Schmidt (1970) : higher dimensional generalization of Thue–Siegel–Roth Theorem, *Subspace Theorem*. Requires a refined zero estimate.

Algebraic values of transcendental functions

Assume f is a *transcendental* entire function (analytic in $\mathbf{C}$) which takes algebraic values at a sequence of algebraic points, say $z_1, z_2, \ldots$ (may include derivatives : repeat the points).

For instance $f(z) = e^z$ with the points $\alpha, 2\alpha, 3\alpha, \ldots$

We want to get a contradiction (under suitable assumptions).

To say that f is transcendental means that if P is a non–zero polynomial in two variables, then the function $P(z, f(z))$ is not the zero function.

Algebraic values of transcendental functions

The idea is to get a contradiction by showing the existence of a non-zero polynomial P such that the function $F(z) = P(z, f(z))$ vanishes at all the z_k.

One first show the existence of P such that F vanishes at $z_1, z_2, \ldots, z_N$.

Then, by an extrapolation argument using an induction, one shows that F vanishes also at $z_{N+1}, z_{N+2}, \ldots$

Auxiliary functions

C.L. Siegel (1929) :
Hermite's explicit formulae
can be replaced by
Dirichlet's box principle
(Thue–Siegel Lemma)
which shows the existence
of suitable *auxiliary functions*.

Auxiliary functions

C.L. Siegel (1929) : auxiliary function for the study of values of E and G functions.

In case of G functions : consider two points, 0 and α, with multiplicity.

Similar with Hermite-Padé approximants of the first type, but the auxiliary functions are not explicit.

K. Mahler (1930's) : functions satisfying a functional equation ; the auxiliary function is constructed by means of linear algebra.

Transcendence criterion of Schneider–Lang

1949, Th. Schneider, general statement on values of analytic functions.
Corollaries : *Hermite–Lindemann, Gel'fond–Schneider, Six Exponentials*
1957, variants in his book on transcendental numbers.

$\sim$1964's, S. Lang, simpler statements,
• one for functions satisfying differential equations – contains the Theorem of Hermite–Lindemann and the solution of Hilbert's seventh problem by Gel'fond's method,
• one for other functions– contains the solution of Hilbert's seventh problem by Schneider's method as well as the Six Exponentials Theorem.

Order of growth of an entire functions

Definition : *An entire function* f *has finite order of growth if*

$$|f|_r := \sup_{|z|=r} |f(z)|$$

satisfies

$$|f|_r \leq e^{Cr^\varrho}.$$

Transcendence criterion of Schneider–Lang

Theorem. *Let f_1, f_2 be two algebraically independent entire functions of finite order of growth. Let K be a number field. Assume the derivatives f_1' and f_2' of f_1 and f_2 are polynomials with coefficients in K in f_1 and f_2. Then the set of $w \in \mathbf{C}$ such that $f_1(w)$ and $f_2(w)$ are in K is finite.*

Assumption : differential equations

$$f_1' = A_1(f_1, f_2), \qquad f_2' = A_2(f_1, f_2)$$

with A_1 and A_2 in $K[X_1, X_2]$.

Conclusion :

$$S = \bigl\{w \in \mathbf{C} \; ; \; f_1(w) \in K \; , \; f_2(w) \in K\bigr\}$$

is finite.

Corollaries

Examples.

• *Hermite–Lindemann's Theorem on the transcendence of e^β for algebraic $\beta \neq 0$.*

Take $f_1(z) = z$, $f_2(z) = e^z$, the differential equations are

$$f_1' = 1, \quad f_2' = f_2,$$

and the two functions take values in $\mathbf{Q}(\beta, e^\beta)$ at $w = s\beta$, $s \in \mathbf{Z}$.

• *Gel'fond–Schneider's Theorem on the transcendence of α^β for algebraic $\alpha \neq 0, 1$ and $\beta \notin \mathbf{Q}$.*

Take $f_1(z) = e^z$, $f_2(z) = e^{\beta z}$, the differential equations are

$$f_1' = f_1, \quad f_2' = \beta f_2,$$

and the two functions take values in $\mathbf{Q}(\alpha, \beta, \alpha^\beta)$ at $w = s \log \alpha$, $s \in \mathbf{Z}$.

Remarks

• Explicit upper bounds for the number of exceptional w, in terms of the growth order ϱ_i of f_i $(i = 1, 2)$ and the degree $[K : \mathbf{Q}]$:

$$\mathrm{Card} S \leq (\varrho_1 + \varrho_2)[K : \mathbf{Q}].$$

• Extends to meromorphic functions (need to avoid poles).

• More general differential equations are allowed – for instance elliptic functions.

Higher dimension

Extensions to several variables : Th. Schneider, S. Lang, E. Bombieri (conjecture of M. Nagata). Generalization of the finiteness condition to higher dimension : subsets of algebraic hypersurfaces.

Replace the number of elements of a finite set by the smallest degree of an algebraic hypersurface containing the set.

Schwarz' Lemma in several variables : Schneider for Cartesian products, Bombieri–Lang using Lelong's theory of functions in several variables, Bombieri using L^2–estimates of L. Hörmander.

Idea of the proof

We argue by contradiction : assume f_1 and f_2 take simultaneously their values in K for many $w \in \mathbf{C}$. We want to show that there exists a non–zero polynomial $P \in K[X_1, X_2]$ such that the function $P(f_1, f_2)$ is the zero function.

The first step is to show that there exists a non–zero polynomial $P \in K[X_1, X_2]$ such that $F = P(f_1, f_2)$ has a zero of high multiplicity at each w :

$$\left(\frac{d}{dz}\right)^t F(w) = 0 \quad \text{for} \quad 0 \leq t < T.$$

Linear algebra vs Thue–Siegel Lemma

$$\left(\frac{d}{dz}\right)^t F(w) = 0 \quad \text{for} \quad 0 \le t < T$$

is a finite set of homogeneous linear equations with coefficients in K. As soon as the number T of equations is less than the number of *unknown*, namely the coefficients of P, there is a non–trivial solution.

Thue–Siegel Lemma : estimate for the coefficients of P (rational integers). Needs only to have sufficiently many unknowns (say twice the number of equations).

Induction

Our goal is to prove that $F=0$. We already know

$$\left(\frac{d}{dz}\right)^t F(w)=0 \quad \text{for} \quad 0\le t<T.$$

By induction on $T'\ge T$ we shall prove

$$\left(\frac{d}{dz}\right)^t F(w)=0 \quad \text{for} \quad 0\le t<T'.$$

At the end of the induction we deduce $F=0$, which is the contradiction with the algebraic independence of f_1 and f_2.

Extrapolation

If F has a zero of multiplicity $\geq T'$ at each w, then F has many zeroes, hence it is *small* in a disk containing these points (Schwarz Lemma), and also its derivatives (Cauchy's inequalitites) have small absolute values.

From the assumptions it follows that $(d/dz)^{T'}F(w)$ is an algebraic number in K with a small absolute value. From the product formula (or the size inequality, or other variants of Liouville's inequality) one deduces $(d/dz)^{T'}F(w) = 0$.

Schwarz Lemma for functions of a single variable

Lemma. *Let* f *be an analytic function in a disc* $|z| \leq R$ *having at least* N *zeroes (counting multiplicities) in a disc of radius* r *with* $r < R$. *Recall* $|f|_r = \sup_{|z|=r} |f(z)|$. *Then*

$$|f|_r \leq \left(\frac{2rR}{R^2 + r^2}\right)^N |f|_R.$$

Proof. Let $z_1, \ldots, z_N$ be zeroes of f in $|z| \leq r$, counting multiplicities. Then the function

$$g(z) = f(z) \prod_{j=1}^{N} \left(\frac{R^2 - z z_j}{R(z - z_j)}\right)^N$$

is analytic in $|z| \leq R$, hence $|g|_r \leq |g|_R$.

Universal auxiliary functions

Alternative argument for the construction of the auxiliary function : joint work with M. Mignotte (1974).

Given arbitrary analytic functions $f_1, \ldots, f_n$, construct a non–zero polynomial $P \in \mathbf{Z}[X_1, \ldots, X_n]$ such that the the first Taylor coefficients at the origin of $F = P(f_1, \ldots, f_n)$ are small.

To solve a system of finitely many linear inequalities, use Dirichlet's box principle – get also an upper bound for the coefficients of P in $\mathbf{Z}$.

It follows that $|f|_r$ is small. Hence f and its first derivatives have small absolute values in $|z| \le r$.

Using the universal auxiliary function

If all $f_i(w)$ are algebraic (maybe including some derivatives), use Liouville's inequality to produce many zeroes of F.

Very efficient with a zero estimate : avoids use of Schwarz' Lemma.

Especially useful in several variables.
Example : *Transcendence of values of exponential functions in several variables.*

Lehmer's Problem

Let θ be a non–zero algebraic integer of degree d. Mahler's *measure* of θ is

$$M(\theta) = \prod_{i=1}^{d} \max(1, |\theta_i|) = \exp\left(\int_0^1 \log|f(e^{2i\pi t}|dt\right),$$

where $\theta = \theta_1$ and $\theta_2, \cdots, \theta_d$ are the conjugates of θ and f the monic irreducible polynomial of θ in $\mathbf{Z}[X]$.

Kronecker : $M(\theta) \geq 1$, and $M(\theta) = 1$ *if and only if* θ *is a root of unity.*

D.H. Lehmer asked whether *there is a constant* $c > 1$ *such that* $M(\theta) < c$ *implies that* θ *is a root of unity.*

M. Mignotte (1977) : Ordinary Vandermonde determinants.

Auxiliary functions and interpolation determinants

C.L. Stewart (1978) introduces an auxiliary function, using Thue–Siegel's Lemma.

E. Dobrowolski (1979) : refined estimate, using congruences modulo p.

D. Cantor and E.G. Straus (1982) : replace Stewart-Dobrowolski auxiliary function by a determinant.

Dobrowolski's Theorem

Theorem [E. Dobrowolski (1979)].
There is a constant c *such that, for* θ *a non–zero algebraic integer of degree* d,

$$M(\theta) < 1 + c(\log\log d/\log d)^3$$

implies that θ *is a root of unity.*

Best unconditional result so far in this direction – improvements only on the numerical value for c.

Dobrowolski's Lemma. *For* θ *not a root of unity,*

$$\prod_{i,j} |\theta_i^p - \theta_j| \geq p^d$$

for any prime p.

Introducing determinants

D. Cantor and E.G. Straus (1979) : Generalised Vandermonde determinant.

This determinant is *big* : has many factors of the form $\prod_{i,j} |\theta_i^p - \theta_j|^k$, for many primes p.

Hadamard's inequality : upper bound for the determinant, in terms of $M(\theta)$.

Remark : lower bounds for the determinants also follow from Schwarz' inequality for p–adic function.

Extensions of the argument : *F. Amoroso and S. David.*

Laurent's interpolation determinants

Underlying idea : a *zero estimate* shows that some matrix whose components are values of polynomials has maximal rank.

Select a non-zero maximal minor, bound it from above and from below.

M. Laurent (1991) : instead of using the pigeonhole principle for proving the existence of solutions to homogeneous linear systems of equations, consider the matrices of such systems and take determinants.

Slope inequalities in Arakelov theory

J–B. Bost (1994) :
matrices and determinants require choices of bases.
Arakelov's Theory produces *slope inequalities* which avoid the need of bases.

Périodes et isogénies des variétés abéliennes sur les corps de nombres, (d'après D. Masser et G. Wüstholz).
Séminaire Nicolas Bourbaki, Vol. 1994/95.

Auxiliary functions in transcendence proofs

Michel Waldschmidt

http://www.math.jussieu.fr/∼miw/