University of Bath

PHD

Use of algebraically independent numbers in computation

Elsonbaty, Ahmed

Award date:
2004

Awarding institution:
University of Bath

Link to publication

Alternative formats
If you require this document in an alternative format, please contact:
openaccess@bath.ac.uk

Copyright of this thesis rests with the author. Access is subject to the above licence, if given. If no licence is specified above, original content in this thesis is licensed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivs 4.0 International (CC BY-NC-ND 4.0) Licence (https://creativecommons.org/licenses/by-nc-nd/4.0/). Any third-party copyright material present remains the property of its respective owner(s) and is licensed under its existing terms.

Take down policy
If you consider content within Bath's Research Portal to be in breach of UK law, please contact: openaccess@bath.ac.uk with the details. Your claim will be investigated and, where appropriate, the item will be removed from public view as soon as possible.

Download date: 28. Apr. 2025

Use of algebraically independent numbers in computation

submitted by

Ahmed Elsonbaty

for the degree of Doctor of Philosophy

of the

University of Bath

2004

COPYRIGHT

Attention is drawn to the fact that copyright of this thesis rests with its author. This copy of the thesis has been supplied on the condition that anyone who consults it is understood to recognise that its copyright rests with its author and that no quotation from the thesis and no information derived from it may be published without the prior written consent of the author.

This thesis may be made available for consultation within the University Library and may be photocopied or lent to other libraries for the purposes of consultation.

Signature of Author .....

Ahmed Elsonbaty

UMI Number: U601777

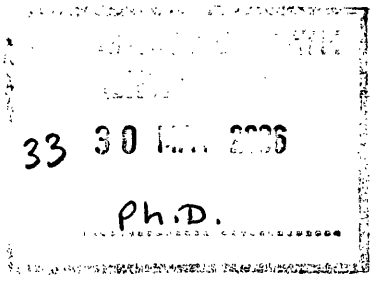
All rights reserved

INFORMATION TO ALL USERS
The quality of this reproduction is dependent upon the quality of the copy submitted.

In the unlikely event that the author did not send a complete manuscript
and there are missing pages, these will be noted. Also, if material had to be removed,
a note will indicate the deletion.

UMI U601777
Published by ProQuest LLC 2013. Copyright in the Dissertation held by the Author.
Microform Edition © ProQuest LLC.
All rights reserved. This work is protected against
unauthorized copying under Title 17, United States Code.

ProQuest LLC
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106-1346


33 30
Ph.D.

Dedication

Thanks to God with His beautiful names and His high attributes. Without His approval nothing can happen. I thank him for giving me a very good supporting family. My father, God bless him, was the one who encouraged me to read and seek knowledge despite the fact that he did not have the chance to do so. He used to value and appreciate knowledge and knowledgeable people and he gave me the chance to understand and appreciate why the Qura'n or simply the Koran begins the revelation with the verses
{Read in the name of thy Lord and Cherisher, who created, created man, out of a leech-like clot. Proclaim and thy Lord is most bountiful, He who taught (the use of) the pen, taught man that which he knew not.} [96:1-5] ([S:V] here and in the other Koranic quotations denotes the chapter number and the verse or verses from the Koran to be translated into English).
For this and more I dedicate this little work to

my beloved father
Abd Elgwad Elsonbaty
and all my teachers.

Acknowledgements

I want to thank the university of Ain Shams in Cairo and the Egyptian culture bureau in London for giving me this opportunity to study for my Ph.D. in Mathematics in the respectable university of Bath. They funded me and supervised my progress.

I am very happy to express my sincere gratitude to my thesis supervisor Dr. Daniel Richardson for his constant encouragement and endless support. He was very patient with me, helped me at very difficult times, gave me confidence and encouraged me to complete my research and write this thesis. I would also like to thank my colleagues at the department of computer science who were very helpful and kind. I am very happy also to thank all of our friends in Bath who helped me and my family and they never let us alone, especially Mrs. Elizabeth Thomas and Mr. Stanley Smith. I am really grateful to you and wish you the best.

This is a very nice occasion to express my gratitude and love to my wife Nashwa Elbadawy who supports me in all times with confidence and belief. I am also grateful to our two little lovely daughters Hedaya and Maryam. Simply, you fill our life with happiness and give us hope for future. Lastly, I cannot forget to thank my friends and my big family in Egypt especially my mother. Her care, love and prayers for me, my brothers and sisters make a real difference. My mother, God bless you and bless all those I owe much.

Abstract

This thesis is concerned with the Zero testing problem for numbers and polynomials presented in the form of *polynomial terms* i.e., trees with operators on the interior nodes and natural numbers and variables on the frontier. We attempt to decide whether or not such a tree represents the zero polynomial by substituting algebraically independent real numbers for the variables and attempting to decide whether or not the resulting constant is zero.

We got a probabilistic zero recognition test for polynomials which is somewhat more expensive computationally than the usual probabilistic method of choosing random integers in a large interval and evaluating, but which depends on the ability to choose a random point in the unit cube and to approximate a polynomial at that point.

Counterexamples to the uniformity and the witness conjectures were discovered but the case of testing polynomials is still plausible. The method for finding counterexamples may help to resolve other related conjectures.

We introduced family of new conjectures to deal with sets of constants like the Pfaffian constants defined by Pfaffian functions with rational coefficients and some boundary conditions.

This thesis also introduces a new effective proof of the famous Lindemann theorem in the form which give us many sets of algebraically independent numbers and more than that it shows the lower bound (called transcendence measure) of some constants compared to the hypothetical ones.

Extended Abstract

This thesis is concerned with the Zero testing problem for numbers and polynomials presented in the form of *polynomial terms* i.e., trees with operators on the interior nodes and natural numbers and variables on the frontier. Testing a number or a polynomial to check if it is zero or not is a fundamental problem in theoretical pure mathematics and in applications in all fields without exception; where we process statistical data and solve some equations.
We attempt to decide whether or not such a tree represents the zero polynomial by substituting algebraically independent real numbers for the variables and attempting to decide whether or not the resulting constant is zero. From this we get a probabilistic zero recognition test for polynomials which is somewhat more expensive computationally than the usual probabilistic method of choosing random integers in a large interval and evaluating, but which depends on the ability to choose a random point in the unit cube and to approximate a polynomial at that point.

We define *Exp-Log expressions* as expressions built up from the natural numbers using field operations, radicals, exponentials and logarithms. Let $\mid V(E) \mid$ be the value of expression E; given choice of principal branch.

The Uniformity Conjecture (UC) claims that for expressions in expanded form (i.e., for any exponential subexpression $\exp(A)$ of E, we have $\mid V(A) \mid \leq 1$), a small multiple of the syntactic length bounds the number of decimal places needed to distinguish the defined number from zero, if it is non zero.

The UC is a simple form of the family of the witness conjectures which may be stated as follows:

For each positive rational number N, denote by Ξ_N the set of all nested radical exponential and logarithmic expressions A such that if E is any subexpression of A, then

$$N^{-1} \leq |V(E)| \leq N\,.$$

The Witness conjectures say that if A is in Ξ_N, then there is a function $\omega_N(n)$ so that $|V(A)| \leq e^{-\omega_N(n)}$, where n is the length of A. The strong witness conjecture is that we can take $\omega_N(n) = Kn$, where K depends on N, and the weak witness conjecture is that we can take $\omega_N(n) = K^n$, where K depends on

N

These conjectures imply a deterministic zero test for polynomials, which should be compared with the deterministic method of reducing to canonical form.

One of the results of this research is that after spending some time trying to resolve the conjecture, counterexamples to the uniformity and the witness conjectures were discovered. This opened a new page in this direction for more thoughts and trials of more sophisticated relations between the values and some parameter of the representation of a number e.g., syntactic length, height (maximum number), level of nesting or composition of the functions we call *depth.*

It is notable that the community of exact geometric computation (EGC) has a theoretical-practical approach to the zero testing problem and a very interesting going project toward robust computation. They use different polynomial root bounds to improve current software computations. Examples of this kind such as degree-height and degree-measure bound use Mahler measure, degree, height for algebraic numbers.

Our technique for finding counterexamples involves constructing expressions for functions with zeros of very high multiplicity at the origin. We try to find expressions in which there are only two occurrences of x but which represent functions so that $g_n(x) = O(x^{n+1})$. Once we have such an expression, we define $E_k(x)$ to be an expression representing the k-th iterate of $g_n(x)$. Such $E_k(x)$ would have length $O(2^k)$, and the resulting function would be $O(x^{(n+1)^k})$ at the origin. The method may help to resolve other related conjectures.

We introduced some ways to generalise this conjectural approach toward including other parameters and toward more general set of constants like the Pfaffian constants defined by Pfaffian functions with rational coefficients and some boundary conditions. This family of new conjectures include the introduction of some fields that satisfies such conjectures, we call them uniform and regular fields.

This thesis also introduces a new effective proof of the famous Lindemann theorem in the form which give us many sets of algebraically independent numbers and more than that it shows the lower bound (called transcendence measure) of some constants compared to the hypothetical ones. Moreover the proof given in details uses important logical technique in a lemma about the functions and numbers defined in the classical proof. We end with a comparison between the result introduced and a recent similar result using matrix interpolation.

Related Keywords

Exact geometric computation.
Probabilistic and Deterministic zero equivalence testing.
Integer Relation, LLL Algorithm, PSLQ Algorithm.
Schanuel conjecture, Witness conjectures and Uniformity conjecture.
Tarski's Problem: Decidability of the theory of the real ordered field with exponent.
Lindemann Theorem, Algebraic independence and Transcendence measure.
Intuitionistic logic, Constructive mathematics.

Contents

Dedication i

Acknowledgements ii

Abstract iii

Extended Abstract iv

Table of Contents vii

1 Introduction 1

1.1 Conjectural Approach 5

1.2 Checking by random inputs 6

1.3 Structure of the thesis 7

2 Background Material 8

2.1 Introduction 8

2.1.1 Basic definitions 8

2.2 Classical results in diophantine approximation 12

2.3 Some Mathematical Bounds 13

2.3.1 Norm estimate 13

2.3.2 Mahler Measure 14

2.3.3 Liouville Estimate 15

2.3.4 Baker-Waldschmidt Estimates 16

2.3.5 Thue-Siegel-Roth Estimates 17

2.3.6 Liouville Inequality 17

2.4 Recent Work On Exact Geometric Computation 19

2.4.1 Exact Geometric Computation (EGC) 20
2.5 Open questions 23

3 The Uniformity Conjecture **24**
3.1 Introduction 24
3.2 Expressions 26
3.2.1 Length of an expression 29
3.2.2 Expressions with variables 30
3.2.3 Gap Functions 30
3.3 Equality catching via the Schanuel Conjecture 30
3.4 Inequality catching via approximation measure 34
3.4.1 Uniformity Conjecture 34
3.5 Comparison to other estimates 35
3.6 Computational Consequences 38
3.6.1 Lazy exact computation 38
3.6.2 Inverse symbolic calculation 38
3.7 Relation with other conjectures 38

4 Zero Recognition of Polynomial Terms **41**
4.1 Polynomial Terms 41
4.2 Square roots of square free numbers 43
4.2.1 Algebraic Independence 45
4.3 probabilistic zero recognition 46
4.3.1 Random choice of integers 46
4.3.2 Random choice of reals 47
4.3.3 Choice of points in the unit cube 49
4.4 Fixed choice based on a conjecture about independence 50
4.5 Complexity of Approximation 52
4.6 Testing the Derivatives 53
4.6.1 The Class NC 57
4.7 Further Work 58

5 Counter Examples to The Uniformity Conjecture **59**
5.1 Introduction 59
5.2 Search for a Counterexample to the Uniformity Conjecture 60

5.2.1 Good rational approximations 60
5.2.2 Near Integer Relations 61
5.2.3 Various Results 63
5.3 Counterexamples 65
5.4 How to generate more counterexamples 67
5.5 Further Work 75

6 New Conjectures **77**
6.1 Uniform fields 78
6.1.1 Extended Mahler measure 78
6.2 Regular fields 85
6.3 Modified uniformity conjecture 89
6.4 Pfaffian functions 91
6.4.1 Basic definitions and examples 91
6.4.2 Khovanskii's bound and some properties 94
6.5 Zero testing of Pfaffian constants 95
6.6 Pfaffian intersections and zero testing 97

7 An Effective Proof Of Lindemann's Theorem **101**
7.1 Number theoretic background 102
7.2 Classic Proof of the Lindemann theorem 107
7.2.1 The classical proof 117
7.3 Effective Proof Of Lindemann theorem 119
7.4 Discussion 124
7.5 Another effective version of the Lindemann-Weierstrass theorem . 127

8 Conclusion **130**

A Koranic Quotations **135**

BIBLIOGRAPHY **140**

Chapter 1

Introduction

> {Say: "travel through the earth and see how He did originate creation; so will God produce a later creation: for God has power over all things".} [29:20]

A fundamental part of the algorithms which are used in Scientific Computing is the zero test. This has the form
If $C = 0$ Then Do A
Else Do B
The constant C is typically a real or complex number which is exactly defined either explicitly by an expression or implicitly by some set of conditions. For example, consider a set of n linear equations in n unknowns $x_1, x_2, \ldots, x_n$ with coefficients in a field F typically the real numbers $\boldsymbol{R}$ or the complex numbers $\boldsymbol{C}$

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n &= b_n \end{aligned} \tag{1.1}$$

Gaussian elimination is the process by which we perform the elimination to be able to solve the resulting equivalent system of equations by backward substitution, forward substitution or pre-multiplying the inverse matrix of the matrix of the coefficients by the column of constants $[b_1, b_2, \ldots, b_n]^{\mathrm{t}}$. This is a corner stone to all linear algebra and to apply we have zero tests to check all the way. We start

by subtracting multiples of the first equation from the other equations so that the first variable is removed from those equations. In order to do this we need to be sure that the first variable does occur in the first equation, i.e., $a_{11} \neq 0$. If $a_{11} = 0$, we search for j so that $a_{j1} \neq 0$ and interchange equation 1 and equation j. Then, we subtract multiples of the second equation from the third and subsequent so that now the first and second variables are removed from them. We continue this process until the system that is left has an upper-triangular form:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{nn}x_n &= b_n \end{aligned} \tag{1.2}$$

where $a_{11} \neq 0, a_{22} \neq 0, \ldots, a_{nn} \neq 0$.
The above triangular system of linear equations may be solved by the back-substitution as follows:

$$x_n = \frac{b_n}{a_{nn}},$$

$$x_{n-1} = \frac{b_{n-1} - a_{n-1,n}\,(b_n/a_{nn})}{a_{n-1,n-1}},$$

$$x_{n-2} = \frac{b_{n-2} - (a_{n-2,n-1}/a_{n-1,n-1})[b_{n-1} - a_{n-1,n}\,(b_n/a_{nn})] - (a_{n-2,n}/a_{nn})}{a_{n-2,n-2}},$$

and in general we determine x_k substituting the previously obtained values of $x_n, x_{n-1}, \ldots, x_{k+1}$ in the kth equation:

$$x_k = \frac{b_k - \sum_{m=k+1}^{n} a_{km}x_m}{a_{kk}} \tag{1.3}$$

It is clear that if the zero tests are incorrect then the flow of control may be incorrect and the result of the algorithm may be incorrect. An extensive literature on the problem exists for example, Computer algebra [DYS88], Effective polynomial computation [Zip93], How to Recognise Zero [Ric97], Exact geometric computing [Li01], Zero testing and the witness conjectures [Hoe97, Hoe00].
Zero tests occur in algorithms, as we see, even for solving a system of linear equations by the standard Gaussian elimination method. If we want robust com-

puting we have to deal with the question of whether some constant is zero. This is an important issue even when we deal with constants formed from algebraic numbers generally or the simple case of radicals.
One approach to a solution to $C = 0\,?$ is the numerical approximation to compute a bound $\epsilon > 0$ so that

$$C \neq 0 \rightarrow |C| > \epsilon$$

Once we have this ϵ we can test $C = 0\,?$ by approximating c to within $\epsilon/2$.
Testing zero, practically speaking, is always done by engineers using numerical approximations with aid of double precision or big number packages. The problem with this is that we cannot rely on this method while having in the same time many examples of "high precision fraud". [BB92] gives some examples of this sort. For instance we have the well-known examples of small but non-zero expressions

$$e^{\pi\sqrt{163/9}} - 640320 \quad \text{and} \quad e^{e^{e^{10}}} + e^{-e^{e^{10}}} - e^{e^{e^{10}}} - 1$$

The counter examples of the uniformity conjecture and the witness conjecture we produced is a topic in this research. This gives another reason, at hand, why one cannot believe high precision computation without another supporting evidence.

Another approach is the exact computation techniques with the height and degree bounds explained in section 2.4, [Li01] or the ongoing research project trying to do exact computation in the the field of primitive element $\boldsymbol{Q}(\alpha)$ based on the standard representation as a vector space, [Li01]. The problem with the latter method is the high complexity (the dimension of the vector space) involved when the constants become more complicated.

The aim is to extend the possibility of exact computation beyond the field of rational numbers in such a way that each expression for a real or complex number can easily be approximated to any desired precision. One important step in this direction would be to understand how to compute with the nested radical and exponential-logarithmic expressions. For this I will introduce the field of closed form numbers defined by T.Chow in [Cho99].

Even without the exponential and the logarithm, basic questions about nested radical expressions may seem quite difficult to decide. In particular, equality

is not always easy to recognise, as illustrated by the following examples, from [DYS88].

$$\begin{aligned}
\sqrt{5+2\sqrt{6}}+\sqrt{5-2\sqrt{6}} &= 2\sqrt{3} \\
\sqrt{16-2\sqrt{29}+2\sqrt{55-10\sqrt{29}}} &= \sqrt{22+2\sqrt{5}} \\
&\quad -\sqrt{11+2\sqrt{29}}+\sqrt{5} \\
\sqrt[3]{\sqrt[5]{32/5}-\sqrt[5]{27/5}} &= (1+\sqrt[5]{3}-\sqrt[5]{3}^2)/\sqrt[5]{25} \\
\sqrt{112+70\sqrt{2}+(46+34\sqrt{2})\sqrt{5}} &= 5+4\sqrt{2}+(3+\sqrt{2})\sqrt{5}
\end{aligned} \tag{1.4}$$

The goal for this thesis is to introduce some ways of testing zero or testing equivalence of polynomials using some conjectures about tree representations of expressions and polynomials. We try to compare these methods with probabilistic methods of testing for equality on randomly chosen set of inputs like the theorem of Schwartz-Zippel, [Sch80] and [Zip79]. In [Sha98] T. Shahoumian studied when random testing is effective in determining polynomial equivalence and program equivalence. It is also extended for testing the radical expressions and checking geometric theorems, see [Li01]. Also we present recent treatment of the problem from the point of view of exact geometric computation and the constructive root bounds and the software library they develop, [Li01].

The study showed that the family of conjecture should be revised and new parameters should be used like the depth of the expression and some suggestions of revision and sets of expressions or numbers to be applied to are studied. A simple existential lemma about the functions and quantities involved in a classical proof of Lindemann theorem enabled us to give a new effective proof of the theorem and a transcendence measure for linear combinations of exponentials

This chapter is organised as follows: section 1.1 discusses the original different conjectures we are studying with their scope of interest. In section 1.2 I will present some theorem in random substitution with some examples for the problem of equivalence. Finally the structure of the thesis is outlined in section 1.3.

1.1 Conjectural Approach

Witness conjectures and the uniformity conjecture

Joris Van Der Hoeven explained his motivation for formulating the witness conjectures [Hoe95], [Hoe97], [Hoe00] for zero testing for many classes of constants, functions and power series as a generalisation for results in the classical(and differential) theory of diophantine approximation. This theory is concerned with the approximation of a given real number x by rationals or equivalently to ask how small $|nx - m|$ can get for large $n, m \in \boldsymbol{Z}$. More generally, the question is how small $|P(x)|$ can get as a function of $P \in \boldsymbol{Z}[x] - \{0\}$. Even more generally, we may consider complex numbers $z_1, \ldots, z_k$ and ask how small $|P(z_1, \ldots, z_k)|$ can get as a function of $P \in \boldsymbol{Z}[z_1, \ldots, z_k] - \{0\}$. According to Liouville, one can see that $|\alpha - p/q|$ can be bounded from below by an expression of the form β/q^n, where β can be expressed as a function of the polynomial P and n is the degree of P (and actually as a function of its size). This seems according to give an evidence for a strong witness conjecture for at least algebraic numbers. For the family of constants we are considering (i.e., the normalised exp-log-radical expressions), the witness conjectures may be stated as follows:
For each positive rational number N, denote by Ξ_N the set of all nested radical exponential and logarithmic expressions A such that if E is any subexpression of A, then

$$N^{-1} \leq |V(E)| \leq N.$$

The Witness conjectures say that if A is in Ξ_N, then there is a function $\omega_N(n)$ so that $|V(A)| \leq e^{-\omega_N(n)}$, where n is the length of A. The strong witness conjecture is that we can take $\omega_N(n) = Kn$, where K depends on N, and the weak witness conjecture is that we can take $\omega_N(n) = K^n$, where K depends on N. Of course the Uniformity Conjecture is much more specific than either of the Witness Conjectures, since van Der Hoeven did not attempt to estimate K.

The Uniformity conjecture is an attempt to extend the witness conjectures to a much wider class of constants. It assumes in the first formulation a very simple linear dependence of the length of the expression in the form:

If E is an exp-log expression in expanded form (i.e., containing no subexpres-

sion having any power bigger than 1), and $V(E) \neq 0$, then

$$|V(E)| > 10^{-2\text{length}(A)}.$$

The Uniformity conjecture should be regarded as an extreme case of the Witness conjecture. In this thesis we will show some counter examples for both of the trials and some recent bounds on the possible revisions to be suggested for future work.

1.2 Checking by random inputs

A related question is zero testing for polynomials. Given $P \in \boldsymbol{Z}[x_1, \ldots, x_n]$, but not in canonical form, we want to decide if $P \equiv 0$. One method is to substitute randomly chosen integers for the variables and check whether the result is zero or not. The theorem of Schwartz-Zippel [Sch80], and [Zip79] gives an upper-bound on the probability that things can go wrong. This means it upper bounds the probability of falsely concluding that something is an identity. For example, we would like to check identities like

$$x^6 + y^6 = (x^2 + y + 2)\left(y^4 + (x^2 + xy)(x^2 - xy)\right)$$

and another example T. Shahoumian cited in [Sha98] the example of verifying the determinant of a $n \times n$ Vandermonde matrix

$$\begin{vmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^{n-1} \\ 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & x_{n-1} & x_{n-1}^2 & \cdots & x_{n-1}^{n-1} \end{vmatrix} = \prod_{0 \leq j \leq k \leq n-1} (x_j - x_k)$$

Verifying this identity for any modest n, seems simple enough: just multiply out the polynomials and see whether the terms all match up. However, these polynomials have an exponential number terms. In many cases, it is much easier to substitute in a random number for the variables and see whether the two polynomials (and some other functions in some cases are equal) are equal on those inputs e.g., in the above identity the polynomials have exponential number

of terms. If the polynomials are unequal on those inputs, the identity has been proved false. More basic examples of the problem will be presented in the next chapter.

1.3 Structure of the thesis

The thesis is organised as follows: Chapter 2 is a quick survey to recent studies in testing equivalence in theoretical and practical sides especially the exact geometric computation approach of root bounds and use of big number packages. Chapter 2 gives a mathematical background and presents most of the standard definitions to be referred through the thesis. In chapter 3 we introduce our conjectural approach through the uniformity conjecture [Ric00] and the witness conjectures [Hoe97] and explain some relations to known facts and conjectures. An application of the conjecture is introduced in chapter 4 which is originally was a joint work [RE03] and in the later part of chapter 4 some new ideas and results are added e.g., checking the derivatives and reconstructing the coefficients. Chapter 5 reveals the first set of counter examples to the uniformity and witness conjectures and explain our method of producing such examples and explains the problems involved. In chapter 6 some new ways are suggested to replace the uniformity conjecture and some bigger sets of constants are to be tested using analogue of old conjecture but with Khovanskii's bound of roots of system of equations of Pfaffian functions. Chapter 7 introduces a new bound for the effective version of the Lindemann theorem and compare the results to the ones we expect from the modified conjectures. The main conclusions of this thesis are the subject of chapter 8. I conclude this work with appendix A of the Koranic quotations I have quoted at the beginning of each chapter and quote some more few verses from one of the chapters of the Koran. My aim is to put in this thesis a part of the basis of my faith and my original language in which I think of my philosophy of mathematics, science and life.

Chapter 2

Background Material

{Slowly will We show them Our signs in the horizons and in their own selves, until it becomes manifest to them that this is the truth. Is it not enough that thy Lord doth witness all things?} [41:53]

2.1 Introduction

2.1.1 Basic definitions

Definition 2.1.1 (Algebraic numbers). *A real or complex number α is said to be algebraic if it is a zero of a non-zero polynomial with integer coefficients.*

In general setting, let α be an algebraic element over a field K of characteristic 0. The *minimal polynomial* of α is the monic polynomial $P(x) \in K[x]$ of lowest degree such that $P(\alpha) = 0$. The minimal polynomial of an algebraic element must be irreducible. Define the degree of α to be the degree of its minimal polynomial P_α. When the leading coefficient of P_α is unity we call α an *algebraic integer.* The totality of algebraic numbers over $\boldsymbol{Q}$ forms a field but this field does not coincide with $\boldsymbol{C}$, the field of the complex numbers. In fact there are real and complex numbers which do not satisfy any polynomial equations with integer coefficients. This is because the set of polynomials with integer coefficients and hence the set of their roots is denumerable set while the set of real numbers is not denumerable. Such a number is called a *transcendental number* and I will give

some brief historical remarks about the discovery of concrete examples of such numbers in the following

Remarks 2.1.1. *1. In 1844 Liouville [Lio44] showed for the first time examples of transcendental numbers of some sort e.g.,*

$$\xi = \sum_{m=1}^{\infty}(-1)^m 2^{-m!} \text{ and } \sum_{m=1}^{\infty} 10^{-m!} \text{ and } \xi + i\xi$$

The proof of the transcendence of such numbers come from the following approximation theorem of Lioville.

Theorem 2.1.1 (Liouville approximation theorem). *Let α be an algebraic number with degree $d > 1$. There exists a constant $c(\alpha)$, which can be easily computed, such that, for any rational number p/q with ($p/q \neq \alpha$ and $p, q \in \boldsymbol{Z}, q > 0$)*

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

2. *In 1873 Hermite proved that e is transcendental, using Padé approximation of $e^x, \ldots, e^{nx}$.*

3. *Lindemann [Lin82] extended Hermite's method to $e^{\alpha_1 x}, \ldots, e^{\alpha_n x}$ and showed thereby in 1882 that π is transcendental. Simple proofs of the transcendence of e, π can be found in [HW02] or [Lan69].*

4. *It is only since 1929 that numbers such as e^{π} and $2^{\sqrt{2}}$ have been shown to be transcendental This is a consequence of a general theorem of Gelfond and Schneider. An account of it is in [Hil42].*

   Theorem 2.1.2 (Gelfond-Schneider theorem). *Let α and β be algebraic numbers different from 0 and 1. If the number*

$$\eta = \frac{\log \alpha}{\log \beta}$$

   is not rational, then it is transcendental.

5. *In 1966 A. Baker found some far-reaching generalisations of the Gelfond-Schneider theorem. For example, he proved*

Theorem 2.1.3 (Baker theorem). *Let $\alpha_1, \ldots, \alpha_n$ be algebraic numbers and assume $\log \alpha_1, \ldots, \log \alpha_n$ are linearly independent over the rationals $\boldsymbol{Q}$. Then $1, \log \alpha_1, \ldots, \log \alpha_n$ are linearly independent over the algebraic numbers.*

In this statement linear independence is defined as usual in linear algebra i.e., $\alpha_1, \ldots, \alpha_n$ are said to be linearly dependent over $\boldsymbol{Q}$ if there are some rational numbers $r_1, \ldots, r_n$ not all zero and satisfy

$$r_1 \alpha_1 + \cdots + r_n \alpha_n = 0$$

otherwise $\alpha_1, \ldots, \alpha_n$ are linearly independent over the rationals. I will show some simple result of this kind in chapter 4.

For more recent results in transcendental number theory one can refer to , [Bak75], [Wal92], [Bak98].

In this thesis we are dealing with different sorts (notions) of heights of algebraic numbers. see [Mig92] and [Zip93] for the following

Definition 2.1.2 (Height of Algebraic numbers). *We have a few different measures on the size of the coefficients of a polynomial*

$$P(x) = p_0 x^d + \cdots + p_{d-1} x + p_d \text{ where } p_0 \neq 0$$

the height of $P(x)$ is defined by

$$|P| = ||P||_\infty = max\{|p_0|, |p_1|, \ldots, |p_d|\}$$

In case α is an algebraic number, we define height$(\alpha) = |P|$, where $p(x)$ is the minimal defining polynomial for α in $\boldsymbol{Z}[x]$. The usual norm $||.||_2$ of P, is called the length of P or of any algebraic number having P as its minimal polynomial.

$$||P|| = ||P||_2 = \left(|p_0|^2 + |p_1|^2 + \cdots + |p_d|^2\right)^{1/2}$$

The relation between these two norms of a polynomial P is given by

$$|P| \leq ||P|| \leq \sqrt{d+1}\,|P|\,,\ d = \deg(P)$$

Definition 2.1.3 (Logarithmic height). *Define the logarithmic height, $h(P)$, of a polynomial P with integral coefficients to be the logarithm (base 10) of the maximum of the absolute values of the coefficients. Define the logarithmic height of an algebraic number to be the logarithmic height of the minimal defining polynomial in $\boldsymbol{Z}[x]$.*

The simple field extension $F(\theta)$, defined to be the smallest field containing F, θ is classified into two distinct cases according to whether θ is algebraic element over the field or not.

Theorem 2.1.4 (Algebraic number fields). *If θ is algebraic over F, then every element α of $F(\theta)$ can be written as a polynomial in θ in the form*

$$\alpha = a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1}$$

where the a_i are in F and n is the degree of θ over F

Theorem 2.1.5 (The primitive element theorem). *If F is any finitely generated field of algebraic numbers then there is an algebraic number γ so that $F = \boldsymbol{Q}[\gamma]$.*

The number γ is called a primitive element for F. This fact is known as the primitive element theorem. One can refer to [DYS88] for a formal statement and an informal one showing the uses of it in modern computer algebra.

Remarks 2.1.2.

1. *An algebraic number field is any finite and hence simple extension of $\boldsymbol{Q}$*
2. *It is clear that $F = \boldsymbol{Q}[\alpha]$ is a vector space over the ground field F and the dimension of the extension is the same as d the degree of α. A canonical basis is $\{1, \alpha, \ldots, \alpha^{d-1}\}$.*
3. *$(F(\theta_1, \ldots, \theta_k) : F)$ will denote the degree of $F(\theta_1, \ldots, \theta_k)$ over F.*

2.2 Classical results in diophantine approximation

If α is an algebraic number with $P(\alpha) = 0$ for some polynomial $P \in Z[z]$ of minimal degree $n \geq 2$ and minimal leading coefficient $c \in N^*$. Let

$$P = c(z - \alpha_1) \cdots (z - \alpha_n)$$

be the factorisation of P with $\alpha = \alpha_1$, $\alpha_i \neq \alpha_j$ for all $i \neq j$ and $\alpha_1, \ldots, \alpha_n$ lie in the algebraic closure of $\boldsymbol{Q}$. Given $p/q \in \boldsymbol{Q}$ close to α, say

$$\left|\frac{p}{q} - \alpha\right| < \left|\frac{p}{q} - \alpha_i\right| \quad \text{for all } i \neq 1 \,,$$

we then have

$$\left|\alpha - \frac{p}{q}\right| = \frac{P(\frac{p}{q})}{c\left|\alpha_2 - \frac{p}{q}\right| \cdots \left|\alpha_n - \frac{p}{q}\right|} \geq \frac{1}{2^{n-1}\, c\, |\alpha_2 - \alpha_1| \cdots |\alpha_n - \alpha_1|\, q^n}$$

since $q^n P(\frac{p}{q}) \in \boldsymbol{Z}^*$. This bound which is due to Liouville, shows that $|\alpha - p/q|$ can be bounded from below by an expression of the form β/q^n, where β can be expressed as a function of the polynomial P (and actually as a function of its size). This seemed according to Joris Van Der Hoeven to give an evidence for a strong witness conjecture for at least algebraic numbers. Actually, the above bound can be sharpened in an asymptotic way. Given a real number x, let $||x||$ be the distance between x and the closest point in $\boldsymbol{Z}$. The following theorem is due to Roth [Rot55], based on previous work by Schneider [Sch36].

Theorem 2.2.1. *Given an algebraic irrational number x and $\epsilon > 0$, there are only a finite number of solutions to the inequality*

$$||qx|| < \frac{1}{q^{1+\epsilon}}, \text{ for } q \in \boldsymbol{N}^* \,.$$

Unfortunately, asymptotic bounds are not really suited for establishing witness theorems, because such theorems do not accommodate exceptions, even if finite number. Nevertheless, they contribute to the likeliness of witness conjectures. Another very general, probabilistic and asymptotic result is the following

[Khi92]:

Theorem 2.2.2. *Let ψ be a positive function, such that $\sum_{q=1}^{\infty} \psi(q)$ converges . Then for almost all numbers x (for the Lebesgue measure), the equation $||qx|| < \psi(x)$ admits only a finite number of solutions.*

[Lan71],[Bak75], [Wal92], [Bak98], [Eve98] give recent improvements and detailed surveys on diophantine approximation and in particular on the diophantine approximation of transcendental constants like e, logarithms and exponentials of algebraic numbers and so on.

2.3 Some Mathematical Bounds

Studying polynomials and their roots forms a huge part of classical algebra literature. This history began with the ninth-century mathematician Al-khowarizmi who deduced the well known formula for the roots of the quadratic equations.

2.3.1 Norm estimate

Theorem 2.3.1. *Suppose α is an algebraic number with defining polynomial*

$$P_\alpha = a_d x^d + \cdots + a_0 = a_d(x-\alpha_1)\cdots(x-\alpha_d) \in Z[x]$$

Then

$$\log|\alpha| \geq -d\, max(\log|a_d|, \log|\alpha_1|, \ldots, \log|\alpha_d|)$$

Proof

The formula for the product of the roots is known to be $|a_d\alpha_1\cdots\alpha_d| = |a_0|$, and a_0 is a non zero integer, since the defining polynomial is chosen with minimal degree. So $|a_d\alpha_1\cdots\alpha_d| \geq 1$ which gives

$$\log|a_d| + \log|\alpha_1| + \cdots + \log|\alpha_d| \geq 0$$

and the theorem follows from this.

2.3.2 Mahler Measure

Another useful measure of a polynomial's size is how far outside the unit disk its zeros lie. Let $P(x)$ be a polynomial in one variable with complex coefficients. Suppose

$$P(x) = a_d x^d + \cdots + a_0 = a_d(x - z_1) \cdots (x - z_d)$$

where $z_1, \ldots, z_d$ are the roots of $P(x)$. Define the Mahler measure or simply the measure of $P(x)$ by

$$m(P) = |a_d| \prod_{j=1}^{d} \max(1, |z_j|)$$

We have, in general, $m(x^d P(1/x)) = m(P)$, $x^d P(1/x)$ is called the inverse polynomial , and $m(PQ) = m(P)\, m(Q)$.
Also, for any positive integer k, $m(P(x^k)) = m(P(x))$.
In case α is an algebraic number, we define $m(\alpha) = m(P)$, where $P(x)$ is the minimal defining polynomial for α in $\boldsymbol{Z}[x]$.

Lemma 2.3.1. *If α and β are algebraic, with degrees d_1 and d_2 respectively, then*

1. $1/m(\alpha) \leq |\alpha| \leq m(\alpha)$
2. $m(\alpha \times \beta) \leq m(\alpha)^{d_2}\, m(\beta)^{d_1}$
3. $m(\alpha + \beta) \leq 2^{d_1 d_2} m(\alpha)^{d_2} m(\beta)^{d_1}$
4. *If k is a positive integer,* $m(\alpha^{1/k}) \leq m(\alpha)$
5. *If k is a positive integer,* $m(\alpha^k) \leq m(\alpha)^k$
6. $m(1/\alpha) = m(\alpha)$

proof
All of this is standard, using the fact that the defining polynomials have integral coefficients. See [Mig92], pp. 148. In this thesis I present some generalisation of Mahler measure to polynomials over algebraic fields. See chapter 6
Define the logarithmic Mahler measure to be the logarithm base 2 of the Mahler measure. As early as 1905 Landau [Lan69] gave an upper bound for $m(p)$ in the inequality

Lemma 2.3.2 (Landau's Inequality). *If the polynomial P is not reduced to a monomial, we have the inequality*

$$m(P) \leq ||P||$$

For a proof see [Mig92] pp.152, and [Zip93] pp.177.

2.3.3 Liouville Estimate

Theorem 2.3.2 (Liouville Estimate). *Let $\xi_1, \ldots, \xi_m$ be algebraic numbers, of degrees $d_1, \ldots, d_m$ and logarithmic heights $h_1, \ldots, h_m$ respectively. Let d be the degree of the extension $\boldsymbol{Q}(\xi_1, \ldots, \xi_m)$ over $\boldsymbol{Q}$. Let P be a polynomial in $\boldsymbol{Z}[x_1, \ldots, x_m]$, of degree n_i in x_i. If $P(\xi_1, \ldots, \xi_m) \neq 0$, then*

$$-d\left(h(P) + \sum_{i=1}^{m}(n_i h_i/d_i) + 2n_i\right) \leq \log|P(\xi_1, \ldots, \xi_m)|$$

For proof, see Lang [Lan93].

Examples 2.3.1. *Consider a linear form in radicals.*

$$\lambda = b_1(a_1)^{1/n_1} + b_2(a_2)^{1/n_2} + \cdots + b_k(a_k)^{1/n_k} + b_{k+1}, \text{ with } b_i \in \boldsymbol{Z}$$

and n_i, a_i positive natural numbers for all i. Assume $\lambda \neq 0$. Then we get the following contrasting estimates. (Note that logarithms here are base 2.)

1. *Norm estimate and Mahler measure. We have $deg(\lambda) \leq \prod n_i$, and the denominator of λ is 1. So we get*

$$\log|\lambda| \geq -(\prod n_i)(\log(|b_{k+1}| + \sum_{i \leq k}|b_i|\,|a_i|^{1/n_i}))$$

2. *Liouville estimate.*

$$\log|\lambda| \geq -(\prod n_i)(\log Max_i(|b_i|) + \sum_i \log(|a_i|)/n_i + 2k)$$

2.3.4 Baker-Waldschmidt Estimates

Theorem 2.3.3 (Baker-Waldschmidt). *Suppose* $p_1, \ldots, p_n \in \boldsymbol{Z}$ *with* $2 \leq p_1 < \cdots < p_n$ *and that*

$$(\boldsymbol{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}) : \boldsymbol{Q}) = 2^n$$

Let $b_1 \ldots, b_n \in \boldsymbol{Z}$, *with* $B = max_{1 \leq i \leq n} |b_i|$.
Suppose $\lambda = b_1 \log p_1 + \cdots + b_n \log p_n \neq 0$.
Let $v_i = max(1, \log p_i)$, *for* $i = 1, \ldots, n$.
Let $\omega = v_1 \ldots v_n$.
Let

$$C_1 = 2^{9n+26} n^{n+4} \omega \log(ev_{n-1})$$

$$C_2 = C_1 \log(ev_n)$$

Then

$$|\lambda| > e^{-(C_1 \log B + C_2)} .$$

See [Weg87] for a proof.

Remark 2.3.1. *This should be compared with the uniformity conjecture (will be presented in the coming chapter), which predicts:*

$$|\lambda| > 10^{-2(\sum length(p_i) + length(b_i) + 2n - 1)}$$

In this case, the most striking difference is that the coefficient C_1 *in the Baker-Waldschmidt result increases as the product of the lengths of the* p_i, *whereas in the prediction from the uniformity conjecture, only the sum of the lengths appears. Patrice Philippon relates a similar lower bound on linear forms in logarithms with the abc-conjecture. See [Phi99], [Phi00]. This is a very simply stated conjecture which, if proved to be correct, would have very important consequences in Diophantine analysis.*

Conjecture 1 (The abc-Conjecture). *If* a, b, c *are integers and*

$$a + b + c = 0, \quad (a, b, c) = 1$$

then, for any $\epsilon > 0$, we have

$$max(|a|, |b|, |c|) << N^{1+\epsilon},$$

where N is the product of all the distinct prime factors of abc and the implied constant depends only on ϵ.

It was shown that if max is replaced by logmax *then the conjecture would be true and the exponent $1+\epsilon$ to be replaced by $\frac{2}{3}+\epsilon$.*

2.3.5 Thue-Siegel-Roth Estimates

There are other forms of 2.2.1, see [HS00], [Spr80] for improvements of the Liouville theorem made by Thue, Siegel and Roth. We state here a result due to Roth, [Rot55]:

Theorem 2.3.4. *(Thue-Siegel-Roth) Let α be an an algebraic number and let δ be a positive real number. There exists a number $C_0 = C_0(\alpha, \delta) > 0$ such that for any rational number p/q with $q > 0$ and $p/q \neq \alpha$,*

$$\left|\frac{p}{q} - \alpha\right| > \frac{C_0}{q^{2+\delta}}$$

There is the following form of the theorem by which we get rid of the constant for the price of finite exception of rational numbers

Theorem 2.3.5. *(Thue-Siegel-Roth) Let α be an an algebraic number and let δ be a positive real number. Then*

$$\left|\frac{p}{q} - \alpha\right| > \frac{1}{q^{2+\delta}}$$

for all but finitely many p/q in $\boldsymbol{Q}$.

2.3.6 Liouville Inequality

Suppose α is an algebraic number, and that the defining polynomial for α is $P(x) = a_0(x - \alpha_1)\ldots(x - \alpha_d)$, where $P(x)$ has integral coefficients, and is irre-

ducible over $\boldsymbol{Q}$. We defined the Mahler measure of α to be

$$m(\alpha) = |a_0| \prod_{i=1}^{d} (1, |\alpha_i|)$$

One approach to exact computing with symbolically defined real and complex numbers is to try to obtain a bound on the smallness of a non zero defined number in terms of the complexity of its definition. A classic expression of this is the Liouville inequality. For two algebraic numbers α and β, this gives a bound on $|\alpha - \beta|$ if $\alpha \neq \beta$. One form of this bound is:

$$2^{-rs} m(\alpha)^{-s} m(\beta)^{-r},$$

provided that α has degree r and β has degree s. Some computational experiments suggest that this bound is often too large. There is also some theoretical evidence for this. The Thue Siegel Roth theorem states that for any given algebraic number and any $\delta > 0$ there are only finitely many $p/q \in \boldsymbol{Q}$ so that $|\alpha - p/q| < q^{2+\delta}$. An improvement by LeVeque says that for any algebraic number field K, any algebraic number α, and and $\delta > 0$ there are at most finitely many algebraic numbers $\beta \in K$ so that

$$|\alpha - \beta| < m(\beta)^{2+\delta}.$$

A symmetric form of the Thue Siegel Roth theorem has also been conjectured. See [Eve98]. This would say that for any number fields K_1 and K_2, and any $\delta > 0$ there are only finitely many α and β with $K_1 = \boldsymbol{Q}(\alpha)$, $K_2 = \boldsymbol{Q}(\beta)$, and

$$|\alpha - \beta| < (\max(m(\alpha), m(\beta))^{2+\delta}.$$

It seems that in order to improve the practical usefulness of the Liouville inequality, some other parameters ought to be considered, not only Mahler measure, height and degree. One possibility is to take the length of the defining expression into account. This possibility is a motivation for some conjectures included in this thesis.

2.4 Recent Work On Exact Geometric Computation

Straight-forward implementation of geometric algorithms using floating point numbers could easily introduce some undesirable numerical errors (disasters in some views). It is often difficult to predict the occurrence of these errors and their magnitude, [Li01].

Yap [Yap00] suggests that " geometric exactness" does not mean necessarily that numerical values must be represented and computed exactly. This means that the conditional tests , which determine the control flow of a program, must be handled in a mathematically correct way. This will guarantee the correctness of combinatorial structure involved in a computation and will free us from keeping and computing exact numerical values which is not always feasible (e.g., when irrational numbers such as $\sqrt{2}$ are involved). This leads to the development of a number of techniques that can improve performance, such as precision-driven computation [Li01], lazy computation [Ric97], adaptive computation and floating-point filters.

The set of real numbers $\boldsymbol{R}$ and the set of complex numbers $\boldsymbol{C}$ are uncountable. Therefore it is not possible to represent all of them uniquely in a countable language. The computable real numbers (which are computable by Turing machines) form a countable subfield of $\boldsymbol{R}$ which we can represent but in this case the zero test is recursively unsolvable problem. Although it is not easy we can go for testing equality for algebraic numbers. This is an old and everyday mathematical and computational problem. The problem of root bounds, more generally, root location, is very classical one with an extensive literature. .See for example [Ded96], [PD98], [DYS88], [Mig92], [Yap00], [Li01]. Some classical bounds are highly non-constructive. But many known root bounds are given in terms of simple function of P's coefficients and degree. For instance, Landau's bound says that any non-zero root α of $P(x)$ satisfies

$$|\alpha| \geq \frac{1}{||P||}$$

I will show some of the recent results about the problem. First what does it mean to say we are given an algebraic number α ?

1. *real algebraic number*

   we are given polynomial $P(x) \in \boldsymbol{Z}[x]$, $deg(P) \geq 1$, $P(\alpha) = 0$ and $P'(\alpha) \neq 0$ and to distinguish which root is meant we consider isolated roots in the sense of

   Definition 2.4.1. *[DYS88] A root α of a polynomial P is said to be isolated if two rational numbers a and b are given such that $a \leq \alpha \leq b$ and P has only one root in the interval $[a, b]$. This interval is called isolating interval of α.*

2. *complex algebraic number*

   In the case of complex algebraic number α obviously no ordering (in a normal sense) but we still can specify a particular root if we apply the Newton's method of approximating roots to a good initial rational approximation

   $$\alpha_0 = x_0 + iy_0 \; ; x_0 \, , y_0 \in \boldsymbol{Q}$$

   so that

   $$\alpha_{i+1} = \alpha_i - \frac{p(\alpha_i)}{p'(\alpha_i)} \rightarrow \alpha \text{ as } i \rightarrow \infty.$$

   [LB97] for details about Newton's method and its real complexity and the general model of real computation.

Unfortunately, in many applications, the coefficients of P are not explicitly given. For instance, in the LEDA and CORE libraries (They deal with the issues of robust numerical and geometric computation) an algebraic number α is presented as a radical expression which is constructed from integers, and recursively built-up using the four arithmetic operations $(+, -, \times, \div)$ and radical extraction $\sqrt[k]{}$. For more details, one can refer to the papers [BFMS99], [BFea01] and [Li01].

2.4.1 Exact Geometric Computation (EGC)

Comparing two real algebraic expressions can be reduced to determining the sign of real algebraic numbers. EGC focuses on determining the sign of expressions correctly (algebraic expressions), e.g., [Li01].

Yap and others adopt a numerical approach based on algebraic root bounds. Basically they approximate the value of a real expression to sufficient precision until a positive or negative sign comes out or we know from root bounds that its value is really zero. Computation of root bounds usually depends on various attributes associated with that value (such as degree and length etc.). The results mentioned here are for *constructive root bounds* which can efficiently computed from the structure of an algebraic expression

Definition 2.4.2. *[Li01]*
constructive root bounds
Given an algebraic expression E, if a bound for its value val(E) can be computed inductively from the structure description of E, we consider it a constructive root bound.

For example, a set of recursive rules for computing root bound for radical expressions are given in [BFMS99] and [Li01] based on Landau's bound $|\alpha| \geq \frac{1}{\|p\|}$ [table 2.4.1]. Expression here means a directed acyclic graph (DAG) in which nodes are labelled by the appropriate constants and operations.

Degree-length and degree-height bounds.
The assumption here is that E_1 and E_2 are expressions for algebraic numbers with degree, length and height d_1, l_1, h_1 and d_2, l_2, h_2 respectively.

$E(expression)$	$d(degree)$	$l(length)$	$h(height)$
rational$\frac{a}{b}$	1	$\sqrt{a^2+b^2}$	$\max\{\|a\|, \|b\|\}$
$E_1 \pm E_2$	$d_1 d_2$	$l_1^{d_2} l_2^{d_1} 2^{d_1 d_2 + \min\{d_1, d_2\}}$	$(h_1 2^{1+d_1})^{d_2} (h_2\sqrt{1+d_2})^{d_1}$
$E_1 \times E_2$	$d_1 d_2$	$l_1^{d_2} l_2^{d_1}$	$(h_1\sqrt{1+d_1})^{d_2} (h_2\sqrt{1+d_2})^{d_1}$
$E_1 \div E_2$	$d_1 d_2$	$l_1^{d_2} l_2^{d_1}$	$(h_1\sqrt{1+d_1})^{d_2} (h_2\sqrt{1+d_2})^{d_1}$
$\sqrt[k]{E_1}$	$k d_1$	l_1	h_1

Table 2.1

Degree-measure bound.
Based on Mignotte's work, Burnikel et al [BFMS99] developed recursive rules to compute upper bounds for degrees and measures (Mahler measure); and called it the degree-measure bound. These rules are given in the last two columns of [table

2.2] where $M'(E)$ and $D'(E)$ are (respectively) upper bounds on $m(E)$ deg(E). The degree-measure bound is always better than the degree-length bound.

BFMS (Burnikel et al) bound

For an expression E having r radical nodes with indices $k_1, k_2, \ldots, k_r$, the BFMS bound is given by

$$\text{val}(E) \neq 0 \Rightarrow (u(E)^{D(E)^2-1}\, l(E))^{-1} \leq |\text{val}(E)| \leq u(E)\, l(E)^{D(E)^2-1},$$

where $D(E) = \prod_{i=1}^{r} k_i$, and $u(E)$ and $l(E)$ are (respectively) upper bounds on the absolute values of algebraic conjugates of val$(U(E))$ and val$(L(E))$. For division-free expressions, the BFMS bound improves to

$$\text{val}(E) \neq 0 \Rightarrow (u(E)^{D(E)-1})^{-1} \leq |\text{val}(E)|\,.$$

The bound for division-free expressions was shown to be essentially sharp but in presence of divisions, the BFMS bound is not necessarily an improvement of the degree-measure bound.

The BFMS bound is based on transformation of an expression E to eliminate all but one division, producing two associated division-free expressions. The upper bounds of the absolute value of conjugates of these two expressions are maintained recursively.

Improved degree-measure bound

One of the main results of [Li01] Ph.D thesis is extending the set of expressions to include roots of polynomials and to to exploit the sharing of common sub-expressions to get a better upper bound on measures, denote it by $M(E)$

E	$M(E)$ *(new bound)*	$M'(E)$ *(old)*	$D'(E)$ *(old)*
rational $\frac{a}{b}$	max $\{\|a\|, \|b\|\}$	max $\{\|a\|, \|b\|\}$	1
Root(p)	$\|\|p\|\|$	-	-
$E_1 \pm E_2$	$M_1^{D_2} M_2^{D_1} 2^{D(E)}$	$M_1'^{D_2'} M_2'^{D_1'} 2^{D_1' D_2'}$	$D_1' D_2'$
$E_1 \times E_2$	$M_1^{D_2} M_2^{D_1}$	$M_1'^{D_2'} M_2'^{D_1'}$	$D_1' D_2'$
$E_1 \div E_2$	$M_1^{D_2} M_2^{D_1}$	$M_1'^{D_2'} M_2'^{D_1'}$	$D_1' D_2'$
$\sqrt[k]{E_1}$	M_1	M_1'	kD_1'
E_1^k	M_1^k	$M_1'^k$	-

Table 2.2

In this table $D(E) = \prod_{i=1}^{k} k_i$ where k_i is either the index of r_i if r_i is a radical node, or the degree of the polynomial if r_i is a polynomial root node. $D(E)$ is an upper bound on deg (E).

The results of EGC previously mentioned can be applied to the examples 1.4 in the introduction chapter. For example, to check the Ramanujan identity

$$\sqrt[3]{\sqrt[5]{32/5} - \sqrt[5]{27/5}} = (1 + \sqrt[5]{3} - \sqrt[5]{3}^2)/\sqrt[5]{25}$$

we can calculate the improved degree-measure bound for the expression successively from the leaves of the tree until we reach its top.

2.5 Open questions

Open Problem 1. *What is the computational difficulty of deciding $V(A) = 0$, where A is a radical expression, i.e. a radical exponential logarithmic expression with no exponential or logarithmic terms?*

See [Str97], [Poh97], [Loo82], [Joh92], [Lan02] for some methods currently used or proposed to solve such problems.

In particular, it would be interesting to know whether or not the zero equivalence problem for radical expressions can be solved in a number of steps which is bounded by some polynomial in the length of the expression. In other words, is this basic problem *tractable* in the sense of Blum-Cucker-Shub-Smale? See [LB97].

We would also like to know:

Open Problem 2. *What is the computational complexity of finding $V(A)$ to n decimal places, given nested radical exponential and logarithmic expression A ?*

Note that for this question we want the complexity in terms of the two input parameters, length(A) and n. We know that for fixed A, we can approximate to n decimal places in a number of steps bounded by $O(\log(n)m(n))$, where $m(n)$ is the complexity of multiplication of n digit numbers. See [BB88].

Chapter 3

The Uniformity Conjecture

{In the creation of the heavens and the earth, and the alteration of night and day, there are indeed signs for men of understanding.} [3:190]

3.1 Introduction

In scientific computing we need some set of constants for some subset D of the complex numbers. It is not at all clear what the domain D could be. We certainly need more than just the rational numbers, or the algebraic numbers. On the other hand, it seems that such a domain D should not include all the computable real and complex numbers, since we may wish to use algorithms which require a method to decide equality between two constants. There may not exist a good universal domain D. In the following, we give a list of minimal conditions which a domain D would have to satisfy in order to be a candidate for a domain for scientific computation.

1. We must have a formal language E of notations for elements of D. $E \subset \Sigma^*$ for some finite set Σ of symbols. We must have a decision method which, given arbitrary string $s \in \Sigma^*$, decides whether or not $s \in E$.

2. Each expression in $s \in E$ either has a value $V(s)$ in D or is undefined. Every element x of D can be expressed as $V(s)$ for some $s \in E$. Given $s \in E$, we can decide whether or not $V(s)$ is defined. If it is defined, then,

given any number n we can compute rational numbers x_n and y_n so that $|V(s) - (x_n + iy_n)| < 10^{-n}$. The computational complexity of finding x_n and y_n (given that the value is defined) is bounded by some polynomial in n, which may also depend on s.

3. Given $s \in E$, where $V(s)$ is defined, we can decide whether or not $V(s) = 0$.

4. The domain D is closed under the field operations, and also closed under operation of e^x and $\log x$, and taking of n-th roots, for each natural number $n > 1$. For the logarithm and the radicals, we define a single value by choosing the principle branch. These operations are also effective on E, so that, for example, given expressions s_1 and s_2 in E, we can effectively find an expression s_3 in E so that $V(s_3) = V(s_1) + V(s_2)$, provided that s_1 and s_2 have defined values.

We do not know whether or not there are *any* such domains D. This is in spite of the fact that the closure condition (4) above is extremely mild. Condition (3) is essential. Scientific computing without a test for zero is so impoverished as to be unrecognisable. Hardly any algorithms survive. For example, systems of linear equations with coefficients in D can not be solved in any satisfactory way. In general, in scientific computing without a test for equality, outputs always depend continuously on inputs. This is a severe distortion of reality.

Not only are we not able to solve the quite basic problems described above, we also have no evidence that these problems are especially difficult. That is, we do not possess any significantly difficult examples. In spite of this, many people consider these problems, in their general form, unrealistically hard. For the purposes of this thesis we will consider only the collection of closed form numbers, as described by Chow, see [Cho99] for relation to Schanuel conjecture and related open problems.

Definition 3.1.1 (*closed form numbers). A subfield F of $\mathbf{C}$ is closed under* exp *and* log *if*

1. $\exp(x) \in F$ *for all* $x \in F$

2. $\log(x) \in F$ *for all nonzero* $x \in F$, *where* log *is the branch of the natural logarithm function such that* $-\pi < Im(\log(x)) \leq \pi$ *for all* x

The field of exp-log closed form numbers is the intersection of all subfields of $\mathbf{C}$ *that are closed under* exp *and* log.

This is essentially the smallest subfield of the complex numbers with the closure properties (4) above, described by the usual set E of expressions. For discussion of efficient approximation of these numbers, see [Bre75] and [BB87].

E can be constructed as follows. Set $E_0 = \{0\}$, and for each $n > 0$ let E_n be the set of all complex numbers obtained either by applying a field operation to any pair of (not necessarily distinct) elements of E_{n-1} or by applying exp or log to any element of E_{n-1}; of course, division by zero and taking the logarithm of zero are forbidden. Then it is clear that E is the union of all the E_n. This shows that E is countable, and that every element of E admits an explicit finite expression in terms of rational numbers, field operations, exp and log.

In section 3.2 the family of nested radical exponential-logarithmic expressions is described and the field of closed form numbers is defined. An expanded form is defined for the expressions, and the Uniformity Conjecture (UC) is stated.

In section 3.3 and 3.4 two approaches to deciding equality over the closed form numbers are described in the following two sections. The first one uses the Schanuel conjecture, and attempts to detect equalities. The second approach uses various conjectures about approximation measure.

Section 3.5 discusses relation of the UC with other estimates mentioned in the background materials.

In section 3.6, some consequences of the UC are compared with known, fairly simple, approximation estimates. In the next section, some practical computational consequences of the UC are stated.

Relation of the UC to the well known conjecture of Schanuell is explained in section 3.7.

3.2 Expressions

We assume, to begin with, the usual canonical representation for the natural numbers base 10. Then the set of nested radical exponential and logarithmic expressions is the smallest set of expressions so that:

1. All the canonical representations of natural numbers are in the set.

2. If A and B are in the set so are $(A+B)$, $(A-B)$, and $(A*B)$, (A/B).

3. If A is in the set, so are $-A$, $\exp(A)$ and $\log(A)$

4. If A is in the set and n is a canonical representation of a natural number bigger than 1, then $A^{1/n}$ is in the set.

Each nested radical exponential and logarithmic expression E is either undefined, or is interpreted as a real or complex number $V(E)$, as follows.

1. If E is a representation of an natural number, $V(E)$ is that natural number.

2. The operators are given the usual precedence in the absence of brackets.

3. If A and B are defined, then $V(A+B), V(A-B), V(A*B)$ and $V(-A)$ are defined with the usual interpretation of the operators. If B is defined, and $V(B)$ is not zero, then $V(A/B)$ is defined, with the usual interpretation.

4. If A is defined, then $\exp(A)$ is defined with meaning e^A.

5. If A is defined, and $V(A) \neq 0$, then $\log(A)$ is defined, as the branch of the logarithm base e so that $-\pi < \mathrm{Im}(\log(A)) \leq \pi$.

6. If A is defined and and $V(A) \neq 0$, and n is a canonical representation of a natural number bigger than 1, then $A^{1/n}$ is defined and equal to $\exp(\log(A)/n)$.

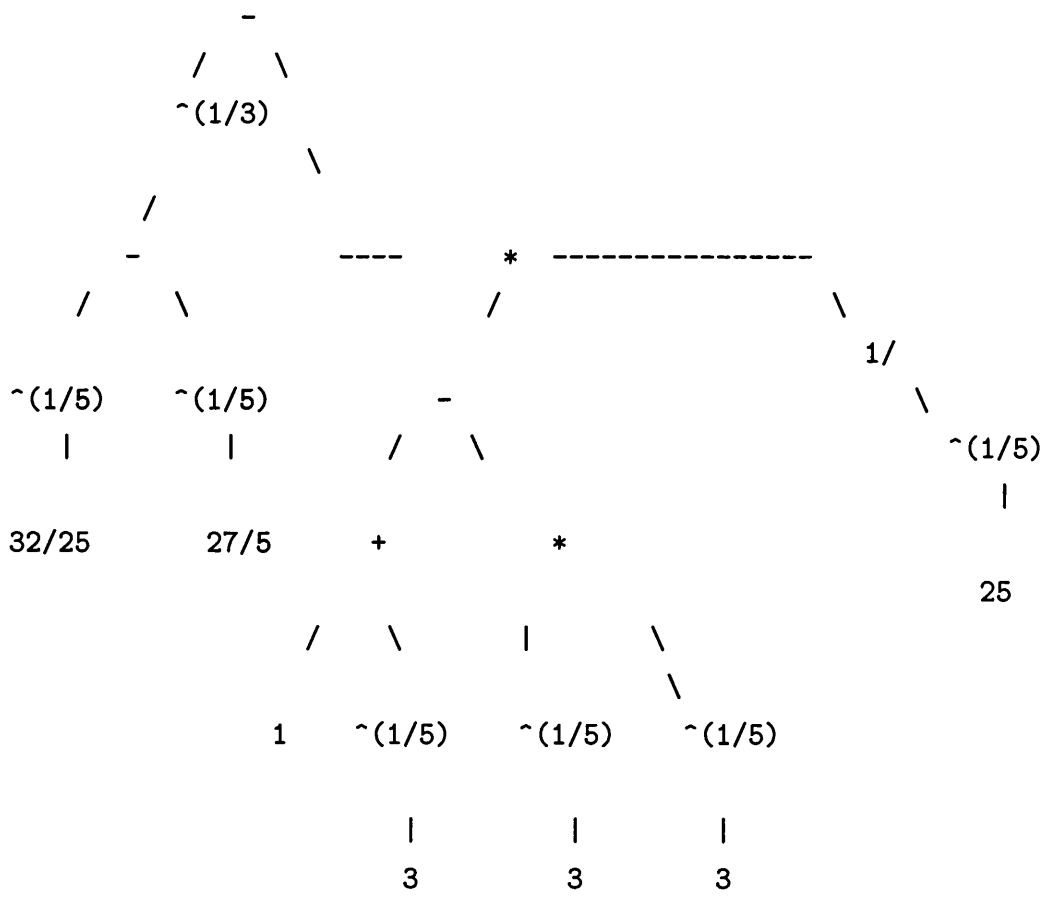
The operator V is called evaluation.

The complex numbers defined in this are what we called *closed form numbers.*

A field with good closure properties including the closed form numbers is the field of elementary numbers. These are numbers of the form $q(\alpha)$, where q is in $\boldsymbol{Q}[x_1, \ldots, x_n]$, and $\alpha \in \boldsymbol{C}^n$ is a non singular solution of a system of equations $(p_1, \ldots, p_n) = 0$ and each p_i is in $\boldsymbol{Z}[x_1, \ldots, x_n, e^{x_1}, \ldots, e^{x_n}]$. It has been shown that this is an effective field i.e., equality is decidable if the Schanuel conjecture is true. See [Ric97], [Ric01]. We define the *real closed form numbers* to be the closed form numbers which happen to have zero imaginary part. Thus the real closed form numbers are closed under trigonometric functions as well as exponentiation and logarithms.

The nested radical exponential and logarithmic expressions which do not use either the exponential or the logarithm will be called radical expressions. The numbers defined by radicals are the closed form numbers represented by such expressions.

The nested radical and exponential-logarithmic expressions can also be written as expression trees. Such trees have representations of integers at the leaves, and have interior nodes labelled with operator symbols. So, for example,



We will regard the expression trees and the expressions as equivalent from now on, since the translation from one form to the other is straightforward.

Please notice that although we have expressions here for n th roots, we do not have expressions for n th powers. If we want A^2, for example, we have to write it as $A * A$.

3.2.1 Length of an expression

We define the length of a natural number to be the number of digits base 10 which are used to represent it in the usual canonical form.

Each exp-log expression may be considered as a tree with representations of natural numbers on the frontier and operators among $\{+, -, *, /, \sqrt[n]{}, \exp, \log\}$ on the interior nodes. We allow $-$ to have arity either 1 or 2. The radical sign has arity 2, and its first argument must be a natural number > 1 in canonical form. We define the length of an expression to be the sum of the number of interior nodes, i.e., the number of operators, and the sum of the lengths of the representations of natural numbers on the frontier. We use length(E) to denote the length of expression E.

Our set of nested radical exponential and logarithmic expressions depends on a choice of canonical representation for the integers. Assume that we have chosen some base b for representation of the integers. We define the length of a non negative integer in this representation to be the number of digits base b which are used.

We define the *length* of a nested radical exponential and logarithmic expression by the following:

$\text{length}(A + B) = \text{length}(A) + \text{length}(B) + 1$

$\text{length}(A - B) = \text{length}(A) + \text{length}(B) + 1$

$\text{length}(-A) = \text{length}(A) + 1$

$\text{length}(A * B) = \text{length}(A) + \text{length}(B) + 1$

$\text{length}(A/B) = \text{length}(A) + \text{length}(B) + 1$

$\text{length}((A)) = \text{length(A)} + 2$

$\text{length}(A^{1/n}) = \text{length}(A) + \text{length}(n) + 1$

$\text{length}(e^A) = \text{length}(A) + 1$

$\text{length}(\log(A)) = \text{length}(A) + 1.$

So, for example, in decimal notation, $4 - 3 * (10)^{1/8}$ would have length 8, since it has 5 digits and 3 operator symbols.

3.2.2 Expressions with variables

All of the above may be generalised by allowing a certain set $x_1, \ldots, x_k$ of variables to appear on the leaves of the expression trees, as well as representations of integers. Of course, in this case, the expressions represent partially defined complex valued functions of k complex variables. The same notion of length can be applied to such expressions, provided that we define the length of the variables in some way. We might take length$(x_i) = 1$ for each i or length$(x_i) = \log i$ for each i.

3.2.3 Gap Functions

Definition 3.2.1. *A gap function for the closed form numbers is a function $g : Exp \to \boldsymbol{R}_+$, where Exp is the set of nested radical exponential and logarithmic expressions, so that if x is a closed form number represented by an expression A, and $x \neq 0$ then $|x| > 10^{-g(A)}$.*

A gap function tells us the amount of decimal precision which is needed to distinguish a non zero number from zero. Of course gap functions exist. We hope that there is a computable gap function, and even an easily computable gap function.

We have a natural scale, i.e. length, on expressions; and we also have a natural scale, i.e. the logarithm of the absolute value, on the complex numbers which are non zero. An important question is : How does the evaluation operator, V, behave with respect to the two natural measures we have namely, the length of an expression and the logarithm of the absolute value of complex numbers?

3.3 Equality catching via the Schanuel Conjecture

Let F be a subfield of the complex numbers. We will say that $(x_1, \ldots, x_n), y$ is a proper set of generators of F if $F = \boldsymbol{Q}(x_1, \ldots, x_n)[y]$, and $x_1, \ldots, x_n$ are algebraically independent over $\boldsymbol{Q}$, and y is integral and algebraic over $\boldsymbol{Q}(x_1, \ldots, x_n)$.

And finitely generated subfield of the complex numbers has such a proper set of generators. A proper set of generators for F defines a canonical form for F.

Provided that we know the defining polynomial for y over $\boldsymbol{Q}(x_1, \ldots, x_n)$, we can effectively put any element of F into its canonical form, and thus we can obtain a decision method for equality over F.

Given an expression for a closed form number x, we can construct a finitely generated subfield F of the complex numbers which contains x. The usual way of doing this is by a sequence of extensions, (see [Sha03]).

$\boldsymbol{Q} = F_1 \subset F_2 \subset \cdots \subset F_n = F$

where for all i either

1. $F_{i+1} = F_i[\theta]$, and θ is algebraic and integral over F_i, or
2. $F_{i+1} = F_i(\theta)$ and $\theta = e^{\alpha}$, where $\alpha \in F_i$, or
3. $F_{i+1} = F_i(\theta)$, and $\theta = \log \alpha$, where $\alpha \in F_i$.

Suppose we had a method which, given a proper set of generators for F_i, would construct a proper set of generators for F_{i+1}. We could then work our way up the sequence, and eventually get a proper set of generators, and therefore a canonical form, for F.

The basic question which arises in this regard is whether or not an exponential or logarithmic extension of F_i is transcendental over F_i. If it is, then we get the new proper set of generators immediately, just by adding the new element θ. On the other hand, if we know that an extension is actually algebraic over the existing field, then we can reduce to case (1), which can be handled by standard methods, once we can identify the defining polynomial for θ.

Assume that we have proper set of generators $(x_1, \ldots, x_n), y$ for F_i. This implies that n of the previous extensions were transcendental. Thus in the process of constructing F_i we have found n pairs of numbers $(z_1, w_1), \ldots, (z_n, w_n)$ with $w_j = e^{z_j}$ for all j, and $x_j \in \{z_j, w_j\}$ for all j and $x_1, \ldots, x_n$ are algebraically independent over $\boldsymbol{Q}$.

Suppose that the next extension is $\theta = e^{\alpha}$, with $\alpha \in F_i$. In this case we will say that θ is *obviously algebraic* over F_i if α is a linear combination of $z_1, \ldots, z_n$ with rational coefficients.

On the other hand, if $\theta = \log \alpha$, we will say that θ is *obviously algebraic* over F_i if α is equal to some power product of $w_1, \ldots, w_n$ with rational exponents.

The Schanuel conjecture, stated below, implies that if θ is not obviously algebraic over F_i as described above, then it is not algebraic over F_i.

To state the Schanuel conjecture we need to recall the following

Definition 3.3.1 (transcendence degree). *Let k and K be two fields with $k \subset K$. $x_1, \ldots, x_n \in K$ are called algebraically independent over k if there is no non-zero polynomial, $P \in k[x_1, \ldots, x_n]$ such that $P(x_1, \ldots, x_n) = 0$. A transcendence basis of K over k is a maximal algebraically independent subset of K. The cardinal number of such a set is called the transcendence degree of the extension $K : k$.*

The transcendence degree is well defined since transcendence bases always exist and any two of them have the same cardinal number of elements. For a proof we can refer to [Ste98], [Lan71] or [Sam72].

For example, $\{x, e^x\}$ and $\{x, e^x + \sqrt{x}\}$ are two transcendence bases of $\boldsymbol{R}(x, e^x)$ over $\boldsymbol{R}$.

Conjecture 2 (Schanuel Conjecture). *If $a_1, \ldots, a_r$ are complex numbers which are linearly independent over the rational numbers $\boldsymbol{Q}$, then $\{a_1, \ldots, a_r, e^{a_1}, \ldots, e^{a_r}\}$ contains at least r algebraically independent numbers. In other words the transcendence degree of*

$$\boldsymbol{Q}(a_1, \ldots, a_r, e^{a_1}, \ldots, e^{a_r}) : \boldsymbol{Q}$$

is at least r.

The conjecture implies in particular that e and π are algebraically independent. For $2\pi i$ and 1 are linearly independent over $\boldsymbol{Q}$ and so the transcendence degree of $\boldsymbol{Q}(1, 2\pi i, e, e^{2\pi i}) : \boldsymbol{Q}$ is at least 2. Thus the transcendence degree of $\boldsymbol{Q}(\pi, e) : \boldsymbol{Q}$ is 2 and hence e and π are algebraically independent, the case which is not yet verified. The conjecture implies the Lindemann theorem which will be subject of chapter 7.

It remains to show that we can detect whether or not θ is obviously algebraic over F_i.

The case in which $\theta = e^\alpha$ is relatively easy, since $\alpha \in F_i$. We put $\alpha, z_1, \ldots, z_n$ in canonical form and test for linear dependence over $\boldsymbol{Q}$ of the vectors of rational coefficients.

In the other case, $\theta = \log \alpha$ with $\alpha \in F_i$. We will say that numbers $b_1, \ldots, b_n$ are multiplicatively dependent if there exists integers $k_1, \ldots, k_n$ not all zero so that

$$b_1^{k_1} \cdots b_n^{k_n} = 1$$

We need to test for multiplicative dependence of $\alpha, w_1, \ldots, w_n$.

$$(\exists\, k_0, k_1, \ldots, k_n \in \boldsymbol{Z} \text{ not all zero})\ \alpha^{k_0} w_1^{k_1} \cdots w_n^{k_n} = 1 \tag{3.1}$$

We express $\alpha, w_1, \ldots, w_n$ in canonical form in F_i. We then solve equation 3.1 by induction on n. The case $n = 0$ is to decide whether or not α is a root of unity, which can be done, as shown in [BD88]. For the induction step, it is sufficient to find one non trivial linear relationship between possible $k_0, k_1, \ldots, k_n$ satisfying equation 3.1, since this will allow eliminating one of $w_1, \ldots, w_n$.

We can regard $\alpha, w_1, \ldots, w_n$ as algebraic functions of $x_1, \ldots, x_n$, take derivatives of the logarithms and put these in canonical form in F_i, and consider the resulting linear equations with rational coefficients in $k_0, \ldots, k_n$. If even one of the derivatives is non zero, this will either show multiplicative independence or give us at least one non trivial linear relationship between the possible exponents.

In case all the derivatives with respect to $x_1, \ldots, x_n$ are zero, it must be that $\alpha, w_1, \ldots, w_n$ are all algebraic numbers. For purposes of solving the problem in this case, we reduce to the case in which F_i is an algebraic number field.

We can do further reduction using any map $v : F_i \to \boldsymbol{Z}$ which behaves like a logarithm, in that $v(xy) = v(x) + v(y)$. One way to do this is to consider a ring homomorphism h from the algebraic integers of F_i to a finite integral domain D, where h maps some of $\alpha, w_1, \ldots, w_n$ into 0. Let I be the ideal which is the kernel of h. For x, an algebraic integer of F_i, define $v(x)$ to be $k - 1$ where k is the smallest positive integer so that x is not in I^k. Now extend v to F_i using $v(x/y) = v(x) - v(y)$. Then solve $k_0 v(\alpha) + \cdots + k_n v(w_n) = 0$.

Eventually we get down to the case in which $\alpha, w_1, \ldots, w_n$ are all units. But by standard methods we can construct a canonical basis for the multiplicative group of units, and thus solve the problem.

More details and discussion of (a variant of) this method can be found in [Ric01]. All the equalities detected by this method are correct. If the Schanuel

conjecture is true, then this method finds all correct equalities. But if the Schanuel conjecture is wrong, it could happen that some true equalities would not be detected. Even more annoying, the general opinion is that although the Schanuel conjecture is probably true, it will not be proved in the near future.

3.4 Inequality catching via approximation measure

Not only do we not have any surprising equalities among closed form numbers, we also do not know of any surprising near inequalities. Of course in order to make this remark into something useful, we need a precise definition of surprise in this context.

Let E be the collection of expressions for closed form numbers. Suppose $g : E \to \boldsymbol{N}$. We will say that g is an approximation measure for the closed form numbers if for any closed form number $x \neq 0$, if x is represented by expression A then $|x| > 10^{-g(A)}$.

Of course, such approximation measures exist. In order to solve the equality problem we need a computable approximation measure.

3.4.1 Uniformity Conjecture

Using iterated exponentiation, it is possible to define very large numbers. Since we have division, it is also possible to define very small numbers with expressions involving iterated exponentiation, followed by division. There does not seem to be any other way to get very large numbers, or very small non zero numbers. Note that although we allow n-th roots, we do not have nth powers. So we can not easily write a short expression for the result of a sequence of repeated squaring, for example.

We consider an expression E to be a subexpression of itself.

We will say that an expression E is in expanded form if for any exponential subexpression e^A of E, we have $|V(A)| \leq 1$.

It appears to be true that it is not possible to define any very large numbers, or any very small non zero numbers using small expressions in expanded form.

Definition 3.4.1. *We consider an expression E to be a subexpression of itself. We will say that an expression E is in expanded form if for any exponential subexpression e^A of E, we have $|V(A)| \leq 1$.*

Conjecture 3. Uniformity Conjecture: If E is an expression in expanded form, and $V(E) \neq 0$, then $| V(E) |$ is bigger than 10^{-2k}, where k is the length of E.

Roughly speaking, the conjecture says that the amount of base S precision which is needed to discriminate the value of an expanded form expression from zero is proportional to the length of the expression.

Examples 3.4.1. $4/3 - 10^{1/8}$ *is zero to three decimal places;*

$7 \log 2 - 3 \log 5$ *is zero to 2 decimal places;*

Even if we add π as a constant to our language, The constant

$$\lambda = \frac{3 \log(640320)}{\sqrt{163}} - \pi$$

is zero to 15 decimal places, length(λ) = 15+length(π), whereas its syntactic length is 15 plus the length of π. If we represent π as $\log(-1)/(-1)^{1/2}$, in which case the length of π would be 8.

3.5 Comparison to other estimates

Consider a linear form in radicals.

$$\lambda = b_1(a_1)^{1/n_1} + b_2(a_2)^{1/n_2} + \cdots + b_k(a_k)^{1/n_k} + b_{k+1},$$

with $b_i \in \boldsymbol{Z}$, and n_i, a_i positive natural numbers for all i. Assume $\lambda \neq 0$. Then we get the following contrasting estimates. (Note that logarithms here are base 2.)

1. Norm estimate and Mahler measure. We have $deg(\lambda) \leq \prod n_i$, and the denominator of λ is 1. So we get

$$\log |\lambda| \geq -(\prod n_i)(\log(|b_{k+1}| + \sum_{i \leq k} |b_i|\,|a_i|^{1/n_i})).$$

2. Liouville Estimate.

$$\log|\lambda| \geq -(\prod n_i)(\log Max_i(|b_i|) + \sum_i \log(|a_i|)/n_i + 2k).$$

3. Uniformity Conjecture.

$$\log|\lambda| \geq -2(\sum \log|n_i| + \sum \log|a_i| + \sum \log|b_i| + 3k).$$

We see in all the earlier estimates that the precision needed increases as the product of the radical degrees. This is the case with the root bounds used in EGC mentioned in 2 ; but according to the uniformity conjecture all that is needed is the sum of the logarithms. Thus even in this simple algebraic case, the uniformity conjecture would imply quite strong new results.

The uniformity conjecture would predict that if A is an expression representing α then:

$|p/q - \alpha| > 10^{-2k}$, where k is the length of $p/q - A$, i.e., $k = \text{length}(p) + \text{length}(q) + \text{length}(A) + 2$

provided $\alpha \neq p/q$. In this case the inequality directly implied by the uniformity conjecture is weaker than that of Thue-Siegel-Roth, but does not allow exceptions. So even in this case, the uniformity conjecture would imply new results. On the other hand, the Thue-Siegel-Roth theorem implies a bound on the number of counterexamples to the uniformity conjecture of the form $\alpha - p/q$, for fixed algebraic closed form α.

Suppose we represent integers base 10, and therefore count length base 10.

Proposition 3.5.1. *Suppose α is an algebraic closed form number represented by an expression A. Then there are at most only finitely many p/q in $\boldsymbol{Q}$ so that $|\alpha - p/q| < 10^{-2k}$ with*

$k = length(p) + length(q) + length(A) + 2.$

Proof.

Suppose, for the sake of a contradiction, that α is a fixed algebraic closed form number and that there are infinitely many counterexamples to the uniformity conjecture of the form

$$\alpha - p/q$$

Let (p_i/q_i) be a sequence of rationals, with $q_i \to \infty$,

$$k_i = \text{length}(p_i) + \text{length}(q_i) + \text{length}(A) + 2$$

and

$$|\alpha - p_i/q_i| < 10^{-2k_i}.$$

Since $p_i/q_i \to \alpha$ and $\alpha \neq 0$, and
length$(q_i) \to \infty$, so
length(p_i)/length$(q_i) \to 1$.
since length$(p_i)/\log(p_i) \to 1$
Thus

$$\left|\alpha - \frac{p_i}{q_i}\right| < 10^{-2\,(\text{length}_{(p_i)}+\text{length}_{(q_i)}+\text{length}_{(A)})}$$

for sufficiently large i.

$$\left|\alpha - \frac{p_i}{q_i}\right| < 10^{-2\text{length}_{q_i}(\text{length}_{(p_i)}\,/\,\text{length}_{(q_i)}+1+\text{length}_{(A)}\,/\,\text{length}_{(q_i)})}$$

for sufficiently large i.

Hence,

$$|\alpha - p_i/q_i| < 10^{-4\,\log_{10}\,q_i+\epsilon}$$

for sufficiently large i.

Thus for some $\epsilon > 0$ and for infinitely many p/q in $\boldsymbol{Q}$ we have

$$|\alpha - p/q| < q^{-3}$$

which contradicts Thue-Siegel-Roth.

Thus although there may be counterexamples to the uniformity conjecture of the form $a^{1/n} - p/q$, we should not expect very many of them.

3.6 Computational Consequences

3.6.1 Lazy exact computation

We hope eventually to extend the possibility of exact computation beyond the field of rational numbers in such a way that each expression for a real number can easily be approximated to any desired precision. One important step in this direction would be to understand how to compute with the nested radical and exponential-logarithmic expressions.

Even without the exponential and the logarithm, basic questions about nested radical expressions may seem quite difficult to decide. In particular, equality is the main question in EGC.

3.6.2 Inverse symbolic calculation

The uniformity conjecture implies that the decimal approximation of precision $\log_{10}(19) * 2n$ is a code for the closed form expression, with integers in decimal notation, and length n, with that value. This implies the existence of a potentially quite useful inverse symbolic calculator, that is a method of deriving a closed form expression from a decimal approximation.

3.7 Relation with other conjectures

It has been shown that if the Schanuel conjecture is true, then the zero equivalence problem for closed form numbers is decidable. Thus the Schanuel conjecture implies the existence of a computable gap function. See [Ric97], [Ric00].

It seems that it might be possible to prove some transcendence results, via Gelfond's method, from the uniformity conjecture. For a good exposition of Gelfond's method, see [Lan66]. Roughly speaking, Gelfond's method would construct a function $F(t)$ with a large number of roots from the existence of a counterexample to the Schanuel conjecture. A closed form number $F(w)$ would then be found which has a fairly small length but is non zero. The maximum modulus principle (an analytic function defined on an open set including a ball has modulus inside the ball bounded by maximum modulus on the boundary of the ball)

is then applied to show that the modulus of $F(w)$ is so small that it contradicts the uniformity conjecture.

In chapter 6 we will introduce some revision to the UC and some weak forms too. One of the generalisations is to define uniform fields as follows.

Definition 3.7.1. *Let K be a finitely generated subfield of the complex numbers. We will say that K is uniform if there is a function $\lambda : K \to \boldsymbol{N}_+$ and a constant C (depends on the field) so that*

1.
$$\forall x, y \in K \; \lambda(x \circ y) \leq \lambda(x) + \lambda(y) + 1 \; , \circ \in \{+, -, \times, \div\}$$

2.
$$\forall x \in K \; x \neq 0 \to |x| > 10^{-C\lambda(x)}.$$

In this case λ is called a length function and C a uniformity constant.

Conjecture 4. If K is a field of closed form numbers with transcendence rank d, and K is uniform, and $\alpha_1 \ldots, \alpha_m$ are in K, and are linearly independent over $\boldsymbol{Q}$, and $m > d$ then $e^{\alpha_1}, \ldots, e^{\alpha_m}$ are not all in K.

Here is a result which shows how the Gelfond method can be used.

We will say that $(x_1, \ldots, x_d, y)$ is a proper set of generators of a subfield F of $\boldsymbol{C}$ if $x_1, \ldots, x_d$ are algebraically independent and y is algebraic and integral over $\boldsymbol{Z}[x_1, \ldots, x_d]$, and F is $\boldsymbol{Z}(x_1, \ldots, x_d)[y]$. Any number in such a field has a canonical form as a polynomial in $\boldsymbol{Z}(x_1, \ldots, x_d)[y]$ with y-degree less than the degree of y over $\boldsymbol{Z}[x_1, \ldots, x_d]$. If $A_1, \ldots, A_j$ are numbers in K and we wish to solve an equation

$$a_1 A_1 + \cdots + a_j A_j = 0$$

for integers $a_1, \ldots, a_j$, we can do this by putting $A_1, \ldots, A_j$ into canonical form in K and replacing this equation by a system of equations, one for each power product which appears in the canonical forms. The number of such equations is bounded in terms of the degree in $(x_1, \ldots, x_d)$ of $A_1, \ldots, A_j$.

If E is an expression in canonical form for an element of field F, with proper set of generators $(x_1, \ldots, x_d, y)$, let $h(E)$ be the maximum of the lengths of the

integral coefficients in E; and let $\deg(E)$ be the maximum of the degrees of any x_i in E. The number of integral coefficients in E is then bounded by $O(\deg(E)^d)$. Using this, we can bound $h(E_1 * E_2)$ in terms of $h(E_1)$ and $h(E_2)$ and $\deg(E_1)$ and $\deg(E_2)$.

Lemma 3.7.1. *Suppose E_1, E_2, and E_3 are canonical form elements of field F, with proper set of generators. Then*

1. *If $E_3 = E_1 * E_2$ then $deg(E_3) \leq deg(E_1) + deg(E_2)$ and $h(E_3) \leq O(h(E_1) + h(E_2) + deg(E_1) + deg(E_2))$*
2. *If $E_2 = E_1^j$, then $deg(E_2) \leq O(j(h(E_1)+deg(E_1)))$ and $h(E_2) \leq O(j(h(E_1)+deg(E_1)))$*

The constant multipliers implied in the big O notation do depend on the defining polynomial for y over $\boldsymbol{Z}[x_1, \ldots, x_d]$, but can be chosen independent of E_1, E_2, E_3, j. For a proof of this standard result, see [Lan93], Ch V, Lemma 1.

Theorem 3.7.1. *(D. Richardson)*

Suppose K is a uniform finitely generated subfield of $\boldsymbol{C}$ with transcendence rank d. Suppose $c_1, \ldots, c_{d_1}$ are complex numbers which are linearly independent over $\boldsymbol{Q}$, and $\alpha_1, \ldots \alpha_{d_2}$ are complex numbers which are linearly independent over $\boldsymbol{Q}$. Then not all of

$e^{c_i \alpha_j}$, for $1 \leq i \leq d_1, 1 \leq j \leq d_2$

can be in K, provided $(d_1 + d_2)(d + 1) \leq d_1 d_2$

Here is a sample consequence of the previous theorem

Corollary 3.7.1. *Assuming that $\boldsymbol{Q}(e)$ is uniform then it cannot be the case that all the numbers e^{e^n} are in $\boldsymbol{Q}(e)$ for $n = 0, 1, \ldots, 6$.*

Proof

Take $d = 1$ and $d_1 = 4, d_2 = 4$ in the proposition, and $c_i = e^{i-1} = \alpha_i$.

Chapter 4

Zero Recognition of Polynomial Terms

> {Do not the unbelievers see that the heavens and the earth were joined together (as one unit of creation), before we clove them asunder? We made from water every living thing. Will they not then believe?} [21:30]

In this chapter some applications of the UC are studied. We will begin with polynomial terms which is representation of polynomials as trees with $+, -, *$ on the interior nodes and with variables and natural numbers on the the leaves. This is the subject of section 4.1. Some known results about independence over the rationals are given with proof and some consequences based on Lindemann theorem are discussed in 4.2. Section 4.5 is devoted to analysis of the complexity of the algorithm which we explain to test whether or not a given expression represents the zero polynomial. the algorithm is generalised to test the derivatives as well in 4.6. 4.3 gives a measure theoretic approach parallel to our method using substitution by transcendental numbers. In the last section 4.7 we show some future goals.

4.1 Polynomial Terms

We would like to consider representation of polynomials as trees with $+, -, *$ on the interior nodes and with variables and natural numbers on the the leaves. Such

a representation is significantly more succinct than any of the usual canonical representations of $\boldsymbol{Z}[x_1, \ldots, x_n]$. On the other hand, it is much weaker (less succinct) than the computation tree representation discussed in the book, Complexity and Real Computation, see [LB97]; and also much weaker than the standard straight line program representation. It is known that there is a probabilistic polynomial time method for zero recognition of straight line programs. See [IM83]. On the other hand, there is no known deterministic polynomial time solution for this problem. This question was discussed in the PhD thesis of Bill Naylor [Nay99], who constructs GCD for polynomials represented as SLP (straight line programs). In general, the zero recognition problem for non canonical representations of polynomials is of much interest in computer algebra. See [Zip93] for a discussion. In this chapter we solve it by substituting algebraically independent numbers (see section 4.2) in place of the variables and assuming the Uniformity Conjecture. If k is the length of the resulting nested exp-log expression we could recognise whether the given polynomial was zero by approximation with decimal precision k. The resulting algorithm is not only polynomial time in theory, it is also feasible in practice. It compares very well in practice with other known deterministic algorithms.

For example, let $Q(x)$ be some univariate polynomial with integer coefficients. Let $P_n(x_1, \ldots, x_n) = \prod_{i=1}^{n} Q(x_i)$. The length of P_n increases only linearly with n. If we are given the fact that P_n has degree less than d in each variable, we could deterministically verify that P_n was not the zero polynomial by evaluating it on the cross product $(\{1, 2, ..., d\})^n$. We need d^n elements in the product to avoid all the roots. It seems therefore that the method of zero recognition by substitution of integers uses a number of substitutions which must increase exponentially with the number of variables. However, if we can compute with algebraically independent numbers, we only need one substitution. This gives us an extra motivation for learning more about how to compute with classical non algebraic numbers.

Now we generalise the definition of *length* of expressions to the case of trees representing polynomial terms as follows

Definition 4.1.1. *size(T) where T is a polynomial term is defined by induction*

as follows:

$$size(A+B) = size(A-B) = size(A*B) := size(A) + size(B) + 1.$$

For every natural number n, $size(n) := length(n)$.
For the variables $x_1, \ldots, x_n$ we define $size(x_i) := 1$.

By induction on the number of nodes or the size of a polynomial term one can prove the following

Lemma 4.1.1. *If T is an polynomial term with real numbers on the frontier, $s(T)$ nodes, and the real numbers are bounded by $10^{h(T)}$ then the value $|T|$ represented by T is bounded by $10^{h(T)s(T)}$.*

4.2 Square roots of square free numbers

Lemma 4.2.1. *If $p_1, \ldots, p_n$, $q_1, \ldots, q_m$; $n+m > 0$ are all different primes then*

$$\frac{\prod_i \sqrt{p_i}}{\prod_j \sqrt{q_j}} \notin \mathbf{Q}.$$

This is well known proof which uses unique factorisation among the integers. Similarly,

Lemma 4.2.2. *If $x \in \boldsymbol{N}$ is a square-free natural number then $\sqrt{x}$ is an irrational number.*

A more general form of the last lemma is

Lemma 4.2.3. *If $x \in \boldsymbol{N}$ is not a perfect square then its square root is an irrational number.*

Proof.
x is not a perfect square means that it is of the form $x = a^2 s$ where s is the square free part of x . So we have $\sqrt{x} = a\sqrt{s}$ and hence $\sqrt{x} \in \boldsymbol{Q} \iff \sqrt{s} \in \boldsymbol{Q}$. But by the last lemma we have $\sqrt{s}$ is irrational and hence $\sqrt{x}$ is irrational.

Now to prove the main lemma of this section we need some notions from algebra .

Theorem 4.2.1. *(Besicovitch Lemma)* $\sqrt{p_n} \notin \boldsymbol{Q}\left(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}}\right)$ *where, for all* i, p_i *is the* i*-th prime number.*

Proof.

We make the convention: $\boldsymbol{Q}_0 := \boldsymbol{Q}$ and by recursion we define for every natural number k

$$\boldsymbol{Q}_k := \boldsymbol{Q}\left(\sqrt{p_1}, \ldots, \sqrt{p_k}\right)$$

We assume that $\sqrt{p_n} \in \boldsymbol{Q}_{n-1} = \boldsymbol{Q}_{n-2}\left(\sqrt{p_{n-1}}\right)$ for the sake of contradiction. This means that

$$\sqrt{p_n} = a + b\sqrt{p_{n-1}}$$

for some $a, b \in \boldsymbol{Q}_{n-2}$. Depending on the values of a, b we get the following possibilities:

1. $\sqrt{p_n} \in \boldsymbol{Q}_{n-2}$. This happens when $b = 0$.
2. $\frac{\sqrt{p_n}}{\sqrt{p_{n-1}}} \in \boldsymbol{Q}_{n-2}$. This happens when $a = 0$.
3. $\sqrt{p_{n-1}} \in \boldsymbol{Q}_{n-2}$. This is the case when a and b are not zero. In this case we square both sides of the equation above and arrange the resulting terms.

Continuing with this process, we reach at last a relation of the form

$$\frac{\sqrt{p_i}}{\prod_{j \in S} \sqrt{p_j}} \in \boldsymbol{Q}_0 = \boldsymbol{Q}$$

Where the product in the last relation is to be taken over some finite subset S of $\{1, 2, \ldots, i-1\}$. (As usual the empty product is the unity). This relation contradicts either lemma 2) or lemma 3) and hence the theorem follows.

Remarks 4.2.1. *1. Using the conventions of the preceding proof we have* $\sqrt{p_n} \notin \boldsymbol{Q}_i$ *for all* $i < n$. *And more generally we have*

$$\sqrt{p_t} \notin \boldsymbol{Q}\left(\sqrt{p_i}, \ldots, \sqrt{p_j}\right)$$

where $p_t, p_i, \ldots, p_j$ are any different primes. Here they are not necessarily subsequent primes.

2. *We also conclude from the proof of the preceding theorem that the dimension of $\boldsymbol{Q}_i$ over $\boldsymbol{Q}_{i-1}$ is exactly two for every pair of such fields. This also proves that: the dimension of $\boldsymbol{Q}_n$ over $\boldsymbol{Q}$ is 2^n.*

Corollary 4.2.1. *The square roots of any finite number of different primes are linearly independent over the rationals. Also, we have that: the square roots of any finite number of reciprocals of different primes are linearly independent over the rationals.*

Proof.
Assume a relation $a_1\sqrt{p_1} + \cdots + a_n\sqrt{p_n} = 0$ where p_i is the i-th prime and the coefficients $a_i \in \boldsymbol{Q}$ are not all zero. Since we have some non zero rationals we get $\sqrt{p_n} \in \boldsymbol{Q}_i$ for some $i < n$ which contradicts the first remark above. Similarly we get the case of the reciprocals.

In the same way, we have the following general result

Corollary 4.2.2. *If $q_1, \ldots, q_k$ are different square free numbers then $\left(\sqrt{q_1}, \ldots, \sqrt{q_k}\right)$ are linearly independent over the rationals; Also $\left(1/\sqrt{q_1}, \ldots, 1/\sqrt{q_k}\right)$ are linearly independent over the rationals.*

For the standard proofs we refer to the classical introduction to number theory [HW02].

4.2.1 Algebraic Independence

Definition 4.2.1. *Complex numbers $a_1, \ldots, a_n$ are algebraically independent if $P(a_1, \ldots, a_n) \neq 0$ for all not identically zero polynomials P in $\boldsymbol{Z}[x_1, \ldots, x_n]$.*

Theorem 4.2.2. *Lindemann's Theorem.*

For any distinct algebraic numbers $\alpha_1, \ldots, \alpha_n$ and non zero algebraic numbers $\beta_1, \ldots, \beta_n$ we have

$$\beta_1 e_1^{\alpha} + \cdots + \beta_n e_n^{\alpha} \neq 0$$

Corollary 4.2.3. *If the algebraic numbers $\alpha_1, \ldots, \alpha_n$ are linearly independent over $\boldsymbol{Q}$, then $e^{\alpha_1}, \ldots, e^{\alpha_n}$ are algebraically independent.*

For proof, see [Bak75],[Lan66], for effective proofs and 7. Applying Lindemann's theorem to the results of the last section we get

Corollary 4.2.4. *If $q_1, \ldots, q_n$ are different square free natural numbers, then $e^{1/\sqrt{q_1}}, \ldots, e^{1/\sqrt{q_n}}$ are algebraically independent.*

Remark 4.2.1. *We use the reciprocals of the radicals above and not the radicals themselves to fulfil the requirements of applying the uniformity conjecture i.e., to have the value of the exponent no more than 1 so that the resulting expressions are in expanded form.*

4.3 probabilistic zero recognition

4.3.1 Random choice of integers

A probabilistic method which can be used for zero recognition among such terms is independently to pick n integers $(x_1, \ldots, x_n)$ at random in the range $[0, d*n*N]$, where d is an upper bound on the degree and N is some large multiplier, and then substitute these integers into the polynomial and evaluate. The following theorem implies that the probability of an error (caused by accidentally choosing a root of the polynomial) would be no more than $1/N$, provided that the polynomial is independent of the random number generator.

Let $\deg(T, x_i)$ be the degree of variable x_i in polynomial term T. Suppose T has variables $x_1, \ldots, x_n$. Define $d(T) = \sum_{i=1}^{n} \deg(T, x_i)$.

An informal statement of Schwartz' theorem is as follows: take any polynomial of total degree d that is not identically zero. For each of its variables, plug in a random value chosen from a large enough field. Each of these values should be chosen uniformly at random from a finite subset S of the field . The probability of the polynomial being zero for those inputs is at most $d/|S|$. For example, the field chosen might be the set of rational numbers, and S might be chosen from $\{1, 2, \ldots, 2d\}$; this gives a probability of failure of at most $1/2$. The formal statement of the theorem is as follows.

Theorem 4.3.1. *Let $P \in A[x_1, \ldots, x_n]$ be a not identically zero polynomial over an integral domain A. Let S be a subset of A of cardinality B. Suppose $x_1, \ldots, x_n$*

are chosen independently, with uniform probability, from S. Then the probability that $P(x_1, \ldots, x_n) = 0$ *is bounded by* $d(T)/B$.

See [Zip93] for a proof.

Define $h(n)$ where n is a natural number to be the number of digits used in the canonical base 10 representation of n. We will call $h(n)$ the logarithmic height of n. For a polynomial terms T, define $h(T)$ to be the maximum of $h(n)$ for n on the frontier of T. Define length$(n) = h(n)$, and length$(x_n) = h(n) + 1$. Extend this notion of length to polynomial terms by setting

length$(A + B)$ =length$(A - B)$ =length$(A * B)$ = length(A)+ length$(B) + 1$.

According to the above theorem, if we want the probability of an error to be, for example, less than 10^{-100}, we need to evaluate the polynomial with n natural number arguments of logarithmic height no more than $100 + h(d(T))$. After substitution, the length of the term is bounded by length$(T) * (50 + h(d(T)))$. Assume that there are no more than $s(T)$ nodes in the tree. The largest integer in the computation has length no more than length $(T) * (50 + h(d(T)))$. There are no more than $s(T)$ computations to be done. So the total complexity is bounded by $s(T)M(\text{length}(T) * (50 + h(d(T))))$, where $M(k)$ is the complexity of multiplication of two natural numbers of length k.

4.3.2 Random choice of reals

We next prove an analogous theorem about points X chosen at random in the unit cube in R^n.

Let $\{|T(X)| < 10^{-k}\}$ be the subset of R^n in which $|T(X)| < 10^{-k}$.

Theorem 4.3.2. *If polynomial term* T *is not identically zero, then the intersection of the unit cube in* $\boldsymbol{R}^n$ *with* $\{|T(X)| < 10^{-k}\}$ *has Lebesgue measure* $\leq 2d(T)10^{-k/d(T)}$.

Proof.

We use induction on n and the fact that if $|a_1 \cdots a_d| > |b_1 \cdots b_d|$ then for some i we must have $|a_i| > |b_i|$.

Assume $T(X)$ is not identically zero. Let x be one of the variables in T, d =deg (T, x), $D = d(T) - d$.

For almost all values of the variables,

$T(X) = a_d(x - \alpha_1) \cdots (x - \alpha_d)$

where $\alpha_1, \ldots, \alpha_d$ depend algebraically on the other variables, and a_d is a non zero polynomial in the other variables.

$\{|T(X)| < 10^{-k}\}$

$= \{|a_d|\,|m(x)| < 10^{-k}\}$

$\subseteq \{|a_d| < 10^{-k\alpha}\} \cup \{|m(x)| < 10^{-k\beta}\}$

where $\alpha = D/(d+D)$, $\beta = d/(d+D)$, and $m(x) = (x - \alpha_1) \ldots (x - \alpha_d)$.

Observe that $\{m(x) < 10^{-k\beta}\} \subseteq \bigcup_{i=1}^{d} \{|x - \alpha_i| < 10^{-k\beta/d}\}$.

Let L be Lebesgue measure, and I^n the unit cube in $\boldsymbol{R}^n$.

We apply our induction hypothesis to get an upper bound on $L(I^n \cap \{|a_d| < 10^{-k\alpha}\}$, (using the fact that the measure of a projection parallel to the x axis of a subset of the unit cube is an upper bound on the measure of the subset) and then apply the observation above.

$L(I^n \cap \{|T(X)| < 10^{-k}\})$

$\leq L(I^n \cap \{|a_d| < 10^{-k\alpha}\}) + L(I^n \cap |m(x)| < 10^{-k\beta}\})$

$\leq 2D10^{-k\alpha/D} + 2d10^{-k\beta/d}$

$\leq 2(d+D)10^{-k/(d+D)}$

(since α/D and β/d are both $1/(d+D)$), which verifies the theorem.

Remark 4.3.1. *For the sake of simplicity the theorem is stated in terms of the unit cube. We could change the scale so that it would apply to any cube* $[0, B]^n$ *in* $\boldsymbol{R}^n$ *by multiplying the measure by a factor of* B^n.

To compare with the method stated earlier, suppose we choose X at random and we want the probability of an error to be less than 10^{-100}. According to the theorem it would be acceptable, from this point of view, to assume that $T = 0$ if $|T(X)| < 10^{-k}$, where $k/d(T) > h(2d(T)) + 100$. Therefore it suffices to choose:

$$k > d(T)(h(2d(T)) + 100)$$

We have a bound of $B = 10^{\text{length(T)}}$ on the absolute values of the numbers which appear in the tree.

At each operation $+, *, -$ within the polynomial term we lose no more than length(T) decimal places of precision.

During the whole computation the total precision lost is bounded by $s(T)*\text{length}(T)$.

It suffices, according to the above theorem, to finish the computation with precision k.

The precision needed for the whole computation is bounded by

$$\text{precision} = s(T) * \text{length}(T) + d(T) * (h(2d(T)) + 100)$$

Since we have $s(T)$ interior nodes (operations), the bit complexity of the computation is $s(T)\, M((\text{precision})$. It can be seen that this test is more expensive computationally than the previously described integer test.

4.3.3 Choice of points in the unit cube

When we choose integers to test whether or not a polynomial term is zero, we make a different random choice each time we have a term to test. Otherwise, someone could discredit the test by constructing a polynomial which happened to be zero at the test point. However, it may not be necessary to choose a new point for each test if we use a randomly chosen point in the unit cube. That is, it may be possible to use always the same point.

Suppose that $k(T)$, mapping polynomial terms into natural numbers, is such that $\sum d(T)10^{-k(T)}$ (taken over all polynomial terms) converges to a finite limit. (For example, $k(T) = 2*\text{length}(T)$ would do.) It is a consequence of the theorem above that for almost all points X in the unit cube there is a number N so that for all non zero polynomial terms T, $d(T) > N \rightarrow |T(X)| \geq 10^{-k(T)d(T)}$.

We also have:

Theorem 4.3.3. *For almost all points X in the unit cube, there is a number C so that for all non zero polynomial terms T we have $|T(X)| > 10^{-C-k(T)d(T)}$.*

Proof.

Let $(T_i)_{i>0}$ enumerate all the polynomial terms. We assume that $\sum d(T_i)10^{-k(T_i)}$ converges. This implies that for any $\epsilon > 0$ there is an N such that

$\sum_{i>N} d(T_i)10^{-k(T_i)} < \epsilon$

This means, as a consequence of the theorem above, that the points X so that $|T_i(X)| < 10^{-k(T)d(T)}$ for some T_i with $i > N$, have measure no more than ϵ. We can choose ϵ as small as we wish. The probability is therefore zero that $|T(X)| < 10^{-k(T)d(T)}$ for infinitely many T, when X is chosen at random. Let S

be a subset of the unit cube of measure 1 so that for points X picked in S there are only finitely many polynomial terms T with

$|T(X)| < 10^{-k(T)d(T)}$.

For each point in S there is a constant C so that

$|T(X)| > 10^{-C-k(T)d(T)}$

for all polynomial terms T which are not the zero polynomial.

Thus if we had a way of computing with any of these very common values, and we could find an appropriate constant C, we could have a deterministic zero test for polynomial terms, and always use the same test point. This possibility is discussed below.

4.4 Fixed choice based on a conjecture about independence

We extend our notion of length by defining

length$(A^{1/n})$ to be length(A)+length$(n)+1$,

length$(1/A)$ =length(e^A) = length$(A)+1$ and

length$(A+B)$ = length$(A-B)$ =length$(A*B)$ = length(A)+ length$(B)+1$.

Conjecture 5. *Let $T(x_1,\ldots,x_n)$ be a polynomial term, and let A be the term which is obtained by substituting $e^{-1/\sqrt{p_1}},\ldots,e^{-1/\sqrt{p_n}}$ for $x_1,\ldots,x_n$ respectively, where $p_1,\ldots,p_n$ are natural numbers. Then*

$$A \neq 0 \rightarrow |A| > 10^{-2\,length(A)}$$

This is a special version of the uniformity conjecture, which is part of an attempt to solve the zero recognition problem for some of the constants which appear frequently in scientific computing. See [Ric97], [Ric01], [Ric00] for discussion of this problem and the conjecture. This is also related to a family of conjectures, called witness conjectures explained in the introduction, see [Hoe00] . The general form of the uniformity conjecture, and the strongest version of the witness conjecture, have recently been shown to be incorrect, via a counterexample found by Joris Van Der Hoeven. However the more specialised conjecture

above still seems plausible.) We note that the substitution chosen is in the unit cube.

Theorem 4.4.1. *(Using conjecture 5). Let T be a polynomial term, and let A be the term obtained by the substitution used in the conjecture above, with $q_1, \ldots, q_n$ the first n square free numbers. Then T is identically zero if and only if $|A| < 10^{-10length(T)}$*

Proof.

The substituted values are algebraically independent, as a consequence of the Lindemann theorem and the lemma of Besicovitch [Bes40] stated and proved in the previous section. So T is the zero polynomial if and only if A is zero. According to the conjecture, A is zero if and only if $|A| < 10^{-2length(A)}$. The first n square free numbers all have length bounded by n. (This follows from the Bertrand postulate, see [Zip93] and we can do better than that using the density of the square free numbers) So length($e^{-1/sqrtq_n}$) is bounded by $h(n) + 5$, and therefore length(A) is bounded by 5 length(T).

Corollary 4.4.1. *(Using conjecture 5).*

There is a deterministic test for zero equivalence of a polynomial term T which has bit complexity which is polynomial in length(T).

Proof.

We need to approximate A with precision at least $k = 10$ length(T). The numbers which occur in the computation have absolute value bounded by $10^{\text{length(T)}}$. Therefore the precision lost at each step of the computation is bounded by length(T). There are $s(T)$ steps. Thus the total precision lost in the computation is bounded by $s(T)$ length(T). We need to do the whole computation with precision no more than $k_2 = (s(T) + 10)$ length(T). At the beginning of the computation, we approximate the numbers $e^{-1/\sqrt{q_i}}$ with precision k_2. Using the results in [BB87], [BB88], [Bre75] we can do this in $O(M(k_2))$ bit operations, where $M(k)$ is the bit complexity of multiplying two k-digit natural numbers. Thus the whole computation has bit complexity bounded by $O(s(T)M(s(T)\text{length}(T)))$, which is bounded by a polynomial in the length of the term T.

Note that a much weaker form of the conjecture will still give a polynomial time deterministic solution of the zero recognition problem for polynomial terms.

The bound k on the precision could be any polynomial in the length of T. For example, the bound obtained in the first part of this paper for the random substitution from the unit cube would also establish the corollary. In spite of this, we have not so far been able to establish the existence of such a deterministic decision procedure without use of some as yet unproved statement of independence measure such as the conjecture above. We also note the somewhat surprising fact that the *non existence* of a polynomial time deterministic solution to the zero recognition problem for polynomial terms would have very interesting consequences for independence measure of many familiar numbers, including exponentials of algebraic numbers.

4.5 Complexity of Approximation

Using the results mentioned in [BB87], [BB88], [Bre75] we can get $e^{1/\sqrt{q}}$ to precision $n >$ length(q) decimal places in $O(M(n))$ bit operations, where $M(n)$ is the bit complexity of multiplying two n-digit natural numbers.

We have a bound of $B = 10^{s(T)\,h(T)}$ on the numbers which appear in the tree (See lemma 4.1.1).

At each operation $+, *, -$ within the polynomial term we lose no more than $O(s(T)h(T))$ decimal places. To do one operation of multiplication for example, xy to k decimal places, we have

$$|(x+\epsilon_1)(y+\epsilon_2) - xy| < (\epsilon_1+\epsilon_2)\max(|x|,|y|)$$

and therefore we would need $(\epsilon_1+\epsilon_2)10^{s(T)\,h(T)} < 10^{-k}$

It suffices, according to the above theorem, to finish the computation with precision $k = 2 * s(T) * \max(h(T), n+1)$.

The precision needed for the whole computation is bounded by

$$2\ s(T)\max(h(T),n+1) + O(s(T)(s(T)h(T))) \;=\; O\left(s(T)^2\,h(T)\right)$$

Since we have $s(T)$ interior nodes (operations), the bit complexity of the computation is $O\left(s(T)\,M(s(T)^2\ h(T))\right)$.

Theorem 4.5.1. *(Assuming the uniformity conjecture 5). Suppose a polynomial $P(x_1, \ldots, x_n)$ is represented by polynomial term $T(x_1, \ldots, x_n)$ with $s(T)$ nodes and logarithmic height $h(T)$. Then the bit complexity of deciding whether or not P is the zero polynomial is bounded by $O\left(s(T)\, M(s(T)^2\, h(T))\right)$*

Remark 4.5.1. *The properties of $e^{1/\sqrt{q_1}}, \ldots, e^{1/\sqrt{q_n}}$ that were needed to apply this algorithm are the following:*

- *calculating their k-th digit can be done quickly in the sense of Borwein see [BB87], [BB88]. See, as well, [Bre75].*
- *They are algebraically independent.*
- *We assumed also the Uniformity Conjecture. We can use a weaker version of the uniformity conjecture and still get a useful result. For example, to have*

$$\left|P\left(e^{1/\sqrt{q_1}}, \ldots, e^{1/\sqrt{q_n}}\right)\right| < 10^{-k} \rightarrow P\left(e^{1/\sqrt{q_1}}, \ldots, e^{1/\sqrt{q_n}}\right) = 0.$$

  We would still have a polynomial complexity test if we defined k to be any polynomial in $s(T)$ and $h(T)$.

We, thus, can use any list of numbers satisfying these properties to recognise zero polynomials. So either the zero recognition problem for polynomial terms can be solved in polynomial time, or there is no such list of numbers (which seems highly unlikely, even if we do not believe the uniformity conjecture).

4.6 Testing the Derivatives

We claim that we can also decide the zero equivalence of the derivatives in polynomial time using algebraically independent numbers and assuming the uniformity conjecture.

By definition of algebraically independent numbers, we can test whether a polynomial $P(x_1, x_2, \ldots, x_n)$ is identically zero or not by substituting n algebraically independent numbers $a_1, a_2, \ldots, a_n$ for the variables $x_1, x_2, \ldots, x_n$. We can use the same idea to test the derivatives of P as well. For the rest of this

subsection we assume $P \in \boldsymbol{Z}[x, y_1, y_2, \ldots, y_n]$ and test the different derivatives with respect to x. We prove this claim as follows.

1. $D_x P \equiv 0$ is equivalent to each of the following statements

   - P does not depend on x.
   - $(\forall x_1, x_2, y_1, \ldots, y_n)\ P(x_1, y_1, \ldots, y_n) = P(x_2, y_1, \ldots, y_n)$
   - $\underbrace{P(x_1, y_1, \ldots, y_n) - P(x_2, y_1, \ldots, y_n)}_{h(x_1, x_2, y_1, \ldots, y_n)} \equiv 0$
   - $h(a_1, a_2, b_1, \ldots, b_n) = 0$ where $a_1, a_2, b_1, \ldots, b_n$ are algebraically independent.
   - $P(a_1, b_1, \ldots, b_n) - P(a_2, b_1, \ldots, b_n) = 0$ (in terms of) P

2. $D_x^2 P \equiv 0 \iff P$ linearly depends on x i.e., $P = Ax + B$ where $A, B \in \boldsymbol{Z}[y_1, \ldots, y_n]$.

   $\iff$ $(\forall\, x_1, x_2, x_3; y_1, \ldots, y_n)\ (x_1, p_1), (x_2, p_2), (x_3, p_3)$ are collinear points

   in the p vs., x plane where we mean by p_i the value $P(x_i, y_1, \ldots, y_n)$. From this collinearity we get the equivalent condition:

   $$\begin{vmatrix} p_1 & 1 & x_1 \\ p_2 & 1 & x_2 \\ p_3 & 1 & x_3 \end{vmatrix} \equiv 0$$

   Treating the left hand determinant as a new polynomial $h(x_1, x_2, x_3, y_1, \ldots, y_n)$ yields the analogous condition of the first derivative (case 1) in the form

   $$(a_2 - a_3)p_1 - (a_1 - a_3)p_2 + (a_1 - a_2)p_3 = 0$$

   where $p_i := P(a_i, b_1, \ldots, b_n)$ and the numbers $a_1, a_2, a_3, b_1, \ldots, b_n$ are algebraically independent.

3. Similarly $D_x^3 P \equiv 0 \iff P$ quadratically depends on x which yields the

following condition:

$$\begin{vmatrix} p_1 & 1 & a_1 & a_1^2 \\ p_2 & 1 & a_2 & a_2^2 \\ p_3 & 1 & a_3 & a_3^2 \\ p_4 & 1 & a_4 & a_4^2 \end{vmatrix} = 0$$

where $p_i := P(a_i, b_1, \ldots, b_n)\,; i = 1, 2, 3, 4$ and $a_1, \ldots, a_4, b_1, \ldots, b_n$ are algebraically independent numbers. Expanding using the entries of the first column we equivalently get

$$p_1 v_1 - p_2 v_2 + p_3 v_3 - p_4 v_4 = 0$$

where

$$\begin{aligned} v_1 &= (a_4 - a_3)(a_4 - a_2)(a_3 - a_2) \\ v_2 &= (a_4 - a_3)(a_4 - a_1)(a_3 - a_1) \\ v_3 &= (a_4 - a_2)(a_4 - a_1)(a_2 - a_1) \\ v_4 &= (a_3 - a_2)(a_3 - a_1)(a_2 - a_1) \end{aligned}$$

4. Now we can (by induction) generalise the above result to the m^{th} derivative case as follows

$$D_x^m P \equiv 0 \iff p_1 v_1 - p_2 v_2 + p_3 v_3 - \cdots + (-1)^m p_{m+1} v_{m+1} = 0$$

where $p_i := P(a_i, b_1, \ldots, b_n)\,; i = 1, 2, \ldots, m+1$ and $a_1, \ldots, a_{m+1}, b_1, \ldots, b_n$ are as usual algebraically independent. The general form of v_i is given by

$$\begin{aligned} v_i &= \det(V(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_{m+1})) \\ &= \prod_{\substack{1 \le j < k \le m+1 \\ j,k \notin \{i\}}} (a_k - a_j) \end{aligned}$$

Here, we used the expansion of the determinant of the Vandermonde matrix $V(a_1, \ldots, a_{i-1}, a_{i+1}, a_{m+1})$ as a product of differences. This Vandermonde

matrix is given below.

$$\begin{bmatrix} 1 & a_1 & a_1^2 & a_1^3 & \cdots & a_1^{m-1} \\ 1 & a_2 & a_2^2 & a_2^3 & \cdots & a_2^{m-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & a_{i-1} & a_{i-1}^2 & a_{i-1}^3 & \cdots & a_{i-1}^{m-1} \\ 1 & a_{i+1} & a_{i+1}^2 & a_{i+1}^3 & \cdots & a_{i+1}^{m-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & a_{m+1} & a_{m+1}^2 & a_{m+1}^3 & \cdots & a_{m+1}^{m-1} \end{bmatrix}$$

For more details about the Vandermonde matrix and related things in computer algebra one may consult [Zip93].

Corollary 4.6.1. *If $P \in \boldsymbol{Z}[x, y_1, \ldots, y_m]$ is represented as polynomial term T with $s(T)$ nodes and $h(T)$ height then we can decide whether the n-th derivative with respect to x is zero in time polynomial in $s(T), h(T)$ and n.*

This seems to depend on the the special form of the Vandermonde determinant, which allows a fairly compact representation as a term. We do not know whether or not any determinant with polynomial entries can be represented as a polynomial term with size bounded polynomially in the size of the determinant and the size of the entries. It has been conjectured that this is not the case, see [Bur00]. We also do not know whether or not any polynomial term can be represented as a determinant with entries which are either natural numbers or variables in some compact way.

We can use the last corollary to determine the degree of x in T in polynomial time. This can be done using derivative testing until we get the first identically zero derivative.

Furthermore, we can compute the coefficients of T with respect to x as follows: Suppose T is polynomial term with degree n i.e., $P = c_0 + c_1 x + \cdots + c_n x^n$ where the coefficients are polynomials (polynomial terms) in the other variables. We get the following system of equations by substituting $0, 1, \ldots, n$ for x.

$$\begin{aligned}
T[x := 0] &= c_0 \\
T[x := 1] &= c_0 + c_1.1 + c_2.1^2 + \cdots + c_n.1^n \\
T[x := 2] &= c_0 + c_1.2 + c_2.2^2 + \cdots + c_n.2^n \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
T[x := n] &= c_0 + c_1.n + c_2.n^2 + \cdots + c_n.n^n
\end{aligned}$$

In matrix form, we have

$$A.(c_0, \ldots, c_n)^T = (T[x := 0], T[x := 1], \ldots, T[x := n])^T$$

Where A is the matrix of coefficients in this system of equations given by $a_{ij} := i^j$; $i, j \geq 0$ and $0^0 := 1$. Clearly A is invertible (again it gives rise to a Vandermonde matrix) and hence

$$(c_0, \ldots, c_n)^T = A^{-1}.(T[x := 0], \ldots, T[x := n])^T .$$

The last equation gives the coefficients $c_0, \ldots, c_n$ as a rational combination of polynomial terms, as the inverse of A has rational entries. It seems that we can do other algebraic computations e.g., finding GCD of polynomials represented as polynomial terms if we work in the field of fractions.

4.6.1 The Class NC

The complexity class NC uses poly-logarithmic time but allows polynomially many processors. We can show that our zero recognition algorithm for polynomial terms is in class NC. In order to do this we need to show that evaluation of terms can be done in parallel efficiently. This can be done as follows. Suppose given a large term T. Find a sub-term T_x whose size is more than a quarter the size of T but no more than a half of the size of T. This can be done by starting at the root of T and going down, always choosing the larger of two subtrees, while the size of the subtree exceeds half the size of T. Replace the subtree T_x by indeterminate x; call the result $T(x)$. Construct terms A and B which are no bigger than $T(x)$ so that $T(x) = Ax + B$. Now evaluate A, B, x in parallel and then compute $Ax + B$.

Let $p(n)$ be the number of processors needed for a problem of size n and let

$t(n)$ be the time. We have

$$p(n) \leq 3p(3n/4) + \sigma \text{ and } t(n) \leq t(3n/4) + \tau$$

where σ is the number of processors needed and τ is the time needed for the computation of $Ax+B$ from A, x, B. These inequalities imply that we can do the computation in poly logarithmic time with polynomially many processors. See [Bre75], [Bur00].

4.7 Further Work

- What is a good lower bound for the value of a non singular determinant whose entries are exp-log expressions? Is the precision necessary to distinguish such a value from zero polynomial in the size of the determinant and the lengths of the entries? A more specific question: Does there exist a non singular matrix whose entries are exp-log expressions, but whose determinant is smaller in absolute value than 10^{-m}, where m is the sum of the lengths of the entries of the matrix? (This is related to the question of whether or not the matching problem is in NC.)

- Consider

$$\begin{aligned}\Gamma_n \;=\; & \{(x_1,\ldots,x_n) \in \boldsymbol{C}^n : \forall k \; \exists \text{ polynomial term } T(x_1,\ldots,x_n) \\ & \text{with } s(T) \text{ nodes and height } h(T) \text{ so that} \\ & T \not\equiv 0 \text{ but } |T(x_1,\ldots,x_n)| < 10^{-k(s(T)h(T))}\}\end{aligned}$$

  Does Γ_n have measure 0 ?

  Note that if $(x_1,\ldots,x_n) \notin \Gamma_n$ and have decimal expansion which can be computed in polynomial time then they can be used to test zero equivalence of polynomial term.

Chapter 5

Counter Examples to The Uniformity Conjecture

{Do they not observe the birds above them, spreading their wings and folding them in? None can uphold them except The Most Gracious: truly it is He that watches over all things.} [67:19]

5.1 Introduction

Counterexamples are found for the uniformity conjecture. These counterexamples are barriers to attempts to find improvements to the Liouville inequality, which is basic to effective computation with algebraic numbers.

Suppose $A(x)$ is an expression obtained by replacing some of the integers on the frontier of expression tree for $A \in E$ by x. Let $f_A(x)$ be the function represented by $A(x)$. Suppose that there are k occurrences of x in $A(x)$, and that $A(x)$ is $O(x^n)$ for x near to zero, where $n > k$. Define $A_1(x) = A(x)$, and $A_{j+1}(x) = A(A_j(x))$, for $j = 1, 2, 3, \ldots$. Then $A_j(x)$ has k^j occurrences of x in it, and $F_{A_j}(x)$ is $O(n^j)$ for x near zero. Let $x = 10^{-p} = \epsilon$. Then length$(A_j(\epsilon))$ will be $O(k^j p)$ but $\left|f_{A_j}(\epsilon)\right| = O(10^{-n^j p})$. Thus if $n/k > c$ we can not have $c\,\text{length}(A)$ as an approximation measure. This implies that counterexamples to the uniformity conjecture can be found. The first example of this type was constructed by Joris van der Hoeven:

$$A(x) = 2\log(1 - \log(1 - x/2)) - x$$

which has only two occurrences of x in it but is $O(x^3)$ near zero.

There are also examples of this kind using radicals. Let

$$G(x) = \sqrt{1+x} - \frac{25}{4} + \frac{21}{4}\sqrt{\frac{7}{5} - \frac{2}{5}\sqrt{-7+8\sqrt{1+\frac{5}{21}x}}}$$

we notice that $G(x) = O(x^5)$ near zero.

These examples are found in the following way. We begin with an expression for a function $f(x)$ with $f(0) = 0$. Then construct $g(a_0, x) = a_0 f(x)$, $g(a_n, a_{n-1}, \ldots, a_0, x) = a_n f(g(a_{n-1}, \ldots, a_0, x))$. Then try to determine $a_0, a_1, \ldots, a_n$ not all zero so that $g(a_n, \ldots, a_0, x) - f(x)$ is $O(x^n)$ near zero. This method is explained and more counterexamples with other base functions are given in section 5.4.

The conjecture has stood for several years. I will present some of the earlier trials to find counterexamples using some approximation techniques e.g., continued fraction expansion in section 5.2 . Counterexamples have recently been found however. Therefore the problem of formulating a practical lower bound remains open, we try to give some attempts in the next chapter of this thesis.

5.2 Search for a Counterexample to the Uniformity Conjecture

5.2.1 Good rational approximations

If α is real we can look for good rational approximations to α by searching for large coefficients in the continued fraction expansion of α. In this way we might find counterexamples or near counterexamples to the Uniformity conjecture of the form $\alpha - p/q$.

5.2.2 Near Integer Relations

If a is a vector of n real numbers, an integer relation for a is a non zero integer vector c so that $c^t a = 0$. A near integer relation is a non zero integer vector c so that $c^T a$ has "small" absolute value.

We can make the notion of "small" precise if a consists of closed form numbers. Define length(a) to be the sum of the lengths of the components, considering these as closed form numbers. We will say that $c^t a$ is small if

$$|c^T a| < 10^{-(\text{length}(c)+\text{length}(a)+2n-1)}$$

These near integer relations include all possible counterexamples to the uniformity conjecture of the form $c^T a$.

For fixed a, we can search for such near integer relations using the LLL algorithm.

Let the Euclidean length of a vector $v \in \boldsymbol{R}^n$ be, as usual $(\sum v_i^2)^{1/2}$.

Suppose $B = \{v^{(1)}, \ldots, v^{(n)}\}$ is a set of n vectors in $\boldsymbol{R}^n$ which are linearly independent over $\boldsymbol{R}$. By the lattice spanned by B we mean the set

$$L = \sum r_i v^{(i)} \; ; \; r_i \in \boldsymbol{Z}$$

This lattice has dimension n and rank n. The determinant of the lattice, $\det(L)$ is the determinant of any matrix of real numbers whose rows span the lattice. This is independent of basis. For more details about geometry of numbers we refer to [Zip93], [Sie89].

A lattice reduction algorithm, such as LLL, finds a reduced basis for a given lattice, the first vector of which has Euclidean length at most $2^{(n-1)/2} m(L)$, where $m(L)$ is the Euclidean length of the shortest non zero vector in the lattice. The first vector in a reduced basis also has Euclidean length bounded by $2^{(n-1)/4} \det(L)^{1/n}$. I will give definition of reduced basis

Definition 5.2.1. *A basis $b_1, b_2, \ldots, b_n$ of a lattice of $\boldsymbol{R}^n$ is said to be reduced if it satisfies the following conditions*

$$\mu_{ij} \leq 1/2, \quad \textit{for} \quad 1 \leq j \leq i \leq n$$

and

$$|b_i^* + \mu_{i,i-1} b_i^*|^2 \geq \frac{3}{4} |b_{i-1}^*|^2, \quad for \quad 1 < i \leq n.$$

The proofs of the basic properties can be found in [LLL82] paper and [Mig92].

This can be used to find near integer relations in the following way. Suppose we are given $a = (a_1, \ldots, a_n)$, and let $(a'_1, \ldots, a'_n)$ be a vector of their rational approximations. Let M be a large rational constant. Let A be the n by n matrix which is obtained from the n by n identity matrix by replacing the last column by the transpose of $(Ma'_1, \ldots, Ma'_n)$. Consider the lattice L spanned by the n dimensional vectors $v^{(i)}, 1 \leq i \leq n$, which are the rows of the matrix A.

If V is a short vector in a reduced basis for L

$$V = \left(w_1, \ldots, w_{n-1}, M \sum_{i \leq n} w_i a'_i \right)$$

then

$$\left| \sum w_i a'_i \right|$$

is small and thus $(w_1, \ldots, w_n)$ is a good candidate for a near integer relation for $(a_1, \ldots, a_n)$.

The problem now is to pick the precision of the approximation and the size of the multiplier M in such a way the first vector in a reduced basis can be used to indicate the non existence of small $c^t a$ with some conditions on c. We will fix length(c) and also put an upper bound on the length of each component of c.

Assume that $(a_1, \ldots, a_n)$ is ordered so that $|a_n|$ is maximal among $|a_i|$. The determinant of the lattice is $M\, a_n$.

Suppose we are looking for small $c^T a$ with Max(length(c_i))= m, and thus length(c) $\leq nm$. Let

$$M = 10^{length(c)+m+length(a)+2n-1}$$

. Approximate a with precision more than $(n+1)m + length(a) + 2n - 1$. Find the reduced basis. If b_1 is the first vector in the reduced basis, we expect

$$|b_1| \leq 2^{(n-1)/4} (M\, a_n)^{1/n}$$

However a small $c^T a$ with length(c_i) $\leq m$ for all i would imply

$c^T a < 10^{-(\text{length}(c)+\text{length}(a)+2n-1)}$, and thus each component of the shortest vector in the lattice would have length no more than m, and thus

$$|b_1| \leq 2^{(n-1)/2} n^{1/2} 10^m$$

Therefore, if this condition does not happen, we can eliminate the possibility of small $c^t a$ of this kind. This can be used to eliminate some parts of the search space for counterexamples.

5.2.3 Various Results

Assorted near counterexamples

Examples 5.2.1. *The following examples were found with LLL algorithm:*

$4\log(3) + 13^{1/2} - 8$ *is zero to 6 decimal places.*

$199\log(3) + 142\log(7) - 183$ *is zero to 8 decimal places.*

$143\log(3) - 183\log(7) + 199$ *is zero to 8 decimal places.*

In [Weg87] LLL is used to find small linear forms in logarithms, and many results are tabulated. No counterexample to the uniformity conjecture was found using this method.

Numbers of the from $a^{1/n} - p_k/q_k \neq 0$ were examined for natural numbers a between 2 and 100, and natural numbers n between 2 and 100, with p_k/q_k the kth convergent of the continued fraction approximation for values of k up to 80, and found no counterexamples to the uniformity conjecture. Some small numbers were found for example

Examples 5.2.2. *The following are quite small numbers, but not small enough. These examples were found by looking for large numbers in the continued fraction expansions of n-th roots.*

$11^{1/5} - 21/13$, *which is zero to 5 decimal places.*

$109^{1/5} - 23/9$, *which is zero to 6 decimal places.*

$3^{1/6} - 6/5$, *which is zero to 4 decimal places.*

$544^{1/6} - 20/7$, *which is zero to 6 decimal places.*

$89^{1/6} - 374/177$, *which is zero to 9 decimal places.*

$11^{1/6} - 6772/4541$, *which is zero to 10 decimal places.*

$823^{1/6} - 1849/604$, *which is zero to 13 decimal places.*
$2^{1/8} - 494/453$, *which is zero to 6 decimal places.*
$27^{1/8} - 77/51$, *which is zero to 6 decimal places.*
$7^{1/8} - 311830/244501$, *which is zero to 14 decimal places.*
$61^{1/11} - 93/64$, *which is zero to 6 decimal places.*
$65^{1/11} - 19/13$, *which is zero to 6 decimal places.*
$3^{1/14} - 53/49$, *which is zero to 6 decimal places.*
$12^{1/17} - 4015/3496$. *is zero to 10 decimal places.*
$21^{1/20} - 7243/6958$, *which is zero to 11 decimal places.*
$17^{1/25} - 28/25$ *is zero to 6 decimal places.*
$38^{1/50} - 92/83$, *which is zero to 8 decimal places.*
$14^{1/95} - 73/71$, *which is zero to 7 decimal places.*
$31^{1/97} - 115/111$, *which is zero to 8 decimal places.*

We also have $\pi - 355/113$, zero to 6 decimal places, could be found by looking for large numbers in the continued fraction expansion of π, and is also well known.

$3 * \log(640320)/\sqrt{163} - \pi$. This is famous for being small, but it is only 0 to 15 decimal places.

Linear forms in radicals: an example

Consider the linear form

$$\lambda = c_1\sqrt{2} + c_2\sqrt{3} + c_3$$

Suppose there were a counterexample to the uniformity conjecture with the length$(\lambda) = k + 8$, where k is the sum of the lengths of c_i, which are assumed to be integral. Let m be the maximum length of the coefficients c_i. In the counterexample, λ must be small, and so $2m \leq k \leq 3m$.

Let $j = k + 8 + m$, and take LLL multiplier $M = 10^j$, as described in section 5.2.2. Then if b_1 is the first vector in a reduced basis, we must have

$$|b_1| \leq 2\sqrt{(3)}10^m .$$

An upper bound for m is $(j - 8)/3$. The LLL algorithm was run for $j = 1, \ldots, 50$. The results all violate this constraint, and thus show that there is no counterexample of this form with coefficients using up to 12 digits. This is

quite an easy computation, and it is clear that other regions of the search space could be investigated in this way.

Remark 5.2.1. *Other methods were used to test the UC, for more examples one can refer to [Ric02]. An important method used in the search of near integer relation is the PSLQ algorithm which guarantees to find for any vector of real or complex numbers* $x = (x_1, x_2, \ldots, x_n)$ *an integer relation*

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = 0$$

if there exists such integers a_i*, not all zero. This algorithm enable us to recognise a numerical constant in terms of the mathematical formula it satisfies. Although the algorithm operates by manipulating a lattice, it does not reduce it to a short vector basis, and is therefore not a lattice reduction algorithm. PSLQ is based on a partial sum of squares scheme implemented using QR matrix decomposition. It was developed by Ferguson and Bailey (1992). A much simplified version of the algorithm was subsequently developed by Ferguson et al. (1999), which also extends the algorithm to complex numbers and quaternions. The PSLQ algorithm terminates after a number of iterations bounded by a polynomial in n and uses a numerically stable matrix reduction procedure. PSLQ tends to be faster than the LLL algorithm because of clever techniques that allow machine arithmetic to be used at many intermediate steps. The LLL algorithm, by comparison, must use moderate precision.*

While the LLL algorithm is a more general lattice reduction algorithm than PSLQ, using LLL to obtain integer relations is in some sense a "trick," whereas with PSLQ one gets either a relation or lower bounds on degrees of polynomials and sizes of coefficients for which such a relation must satisfy. See [FF79], [FB92], [FBA99] and [Bai00] for this important algorithm and some recent applications in Mathematics and Physics.

5.3 Counterexamples

A number of computationally intense searches for counterexamples using the above methods failed to find any. We know as a result of these searches, for example, that there are no counterexamples of length less than 8. The coun-

terexamples began to be discovered quite recently in the following way. David Bailey suggested that we look at Borwein's fourth order approximation method for calculating π. See [BB88].

$$\begin{aligned} y_0 &= \sqrt{2}-1, \\ x_0 &= 6-4\sqrt{2} \\ y_n &= (1-(1-y_n)^4)^{1/4}/(1+(1-y_n^4)^{1/4} \\ x_n &= (1+y_n)^4 x_{n-1} - 2^{2n+1} y_n(1+y_n+y_n^2) \end{aligned}$$

with x_n tending to $1/\pi$ as $n \to \infty$.

After 15 iterations, this produces an approximation with billions of digits of accuracy. By substituting the recurrence relation into itself a number of times, expressions can be found for the approximation. This was quite a helpful idea, but it did not seem to produce a counterexample. The reason was that although the precision grows by a factor of four at each substitution, the length of the approximating expression grows even faster.

If $E(x)$ is some expression with k occurrences of x in it, then $E(E(x))$ has k^2 occurrences of x in it. In general if we define $E_1(x) = E(x)$, and $E_{n+1}(x) = E_n(E(x))$, then $E_n(x)$ will have k^n occurrences of x in it, and the length of $E_n(x)$ grows like k^n. On the other hand, we observe that if $E(x)$ has a zero at zero of multiplicity m, then $E_n(x) = O(x^{m^n})$. So to get a counterexample we would require $k < m$. At this point Joris Van Der Hoeven produced the counterexample generator:

$$E(x) = \log(1+x) - 2\log(1+\log(1+x/2)).$$

This has only two occurrences of x, but is $O(x^3)$ at zero. This means that if $x = 10^{-N}$, then $E_n(x)$ has length approximately $2^n N$, but $|E_n(x)|$ is approximately $10^{-3^n N}$.

The length of $E(x)$ is $2\,\text{length}(x)+14$. Let $x = 10^{-N}$. Since the length of x is $N+3$, the length of $E_2(x)$ is $4N+54$. So choosing $N = 109$ gives a counterexample. In fact $|E_2(10^{-109})| < 10^{-986}$. On the other hand $2\,\text{length}(E_2(10^{-109})) \leq 980$.

5.4 How to generate more counterexamples

We have also constructed more counterexamples with logarithms, exponentials, radicals . An example is

$$F(x) = \sqrt{1+x} - 2\sqrt[3]{1+\frac{3}{4}x} + 1$$

$F(x)$ is, again, $O(x^3)$ at zero.

We can write $F(x) = \alpha(x) - \beta(x)$,

with $\alpha(x) = \sqrt{1+x} - 1$,

and $\beta(x) = 2 - 2\sqrt[3]{1+\frac{3}{4}x}$.

Suppose $x = 10^{-N}$. The length of x is then $N+2$. Thus length$(\alpha(x)) = N+7$ and length$(\beta(x)) = N+11$. Thus length$(F(x)) = 2N+19$. On the other hand $|F(x)| < 10^{-3N}$. We do not yet get a counterexample however because of the factor of 2 in the exponent appearing in the conjecture.

However, $F(F(x)) = O(x^9)$ So a counterexample is obtained by choosing N sufficiently large and substituting $x = 10^{-N}$ into $F(F(x))$. In this case

$$\left|F(F(10^{-126}))\right| < 10^{-1141} \text{ and } 2 \text{ length}(F(F(10^{-126}))) \leq 1134\,.$$

Define $F_1(x) = F(x)$ and $F_{n+1}(x) = F_n(F(x))$. Then, assuming $x = 10^{-N}$ we get

$$\text{length}(F_n(x)) = O(2^n) \text{ and } |F_n(x)| = O(x^{3^n})\,.$$

We can also compute the Mahler measures for this example.

$$M(\alpha(x)) \leq 3 * 10^N, M(\beta(x)) \leq 3 * 10^N.$$

Iterating, we can define $F_1(x) = F(x)$ and $F_{n+1}(x) = F_n(F(x))$, and we get, assuming $x = 10^{-N}$:

length$(F_n(x)) = O(2^n)$ and $|F_n(x)| = O(x^{3^n})$

There are even worse examples, also with two occurrences of x. Let

$$G(x) = \sqrt{1+x} - \frac{25}{4} + \frac{21}{4}\sqrt{\frac{7}{5} - \frac{2}{5}\sqrt{-7+8\sqrt{1+\frac{5}{21}\,x}}}.$$

$G(x) = O(x^5)$ near zero. In this case we could get a counterexample from $G(x)$ with $x = 10^{-N}$ and N sufficiently large.

Our method of constructing counterexamples involves finding solutions to the equation given above $g_n(x) = O(x^{n+1})$. Once we have such a solution, we define $E_k(x)$ to be an expression representing the k^{th} iterate of $g_n(x)$. Such $E_k(x)$ would have length $O(2^k)$, and the resulting function would be $O(x^{(n+1)^k})$ at the origin. We only succeeded in finding appropriate solutions up to $n = 4$.

All of the examples we have constructed involve fairly deep nesting,

The method we have used for searching for such functions is the following. We take any exp-log function $f(x)$ with $f(0) = 0$, and such that $f(x)$ has an expression representing it in which there is only one occurrence of x. Set

$$h_1(x) = a_1 f(a_0\, x)$$

$$h_{k+1}(x) = a_{k+1} f(h_k(x))$$

for $k = 1, \ldots, n-1$, so that $h_n(x) = a_n f(a_{n-1} f(\ldots a_1 f(a_0\, x))\ldots)$,
and

$$g_n(x) = f(x) - h_n(x)$$

In the expression for $g_n(x)$ there are two occurrences of x, and there are $n+1$ parameters $a_0, \ldots, a_n$. We have $g_n(0) = 0$ since $f(0) = 0$. We now try to find values of the parameters so that $g_n(x)$ is $O(x^{n+1})$ at the origin, but $g_n(x)$ is not identically zero. This involves solving n polynomial equations in $n+1$ unknowns. If there is a solution, there is a solution which is algebraic in the coefficients of the Taylor series for $f(x)$, since the equations are polynomial in these coefficients. In order to construct a counterexample, we also require that the parameters in the solution are closed form numbers. In practice this means that we look for solutions which can be constructed by nested radicals from the Taylor coefficients of $f(x)$. A problem with the construction is that as soon as one parameter takes

the value zero then $h_n(x)$ is identically zero.

Suppose we take $f(x) = \sqrt[r]{1+x} - 1$.

In this case we can find values of the parameters represented by radicals, depending on r, so that $g_n(x) = O(x^{n+1})$ at the origin, for $n = 1, 2, 3, 4$. In some cases, we found solutions which were rational, depending on r, and in other cases the solutions required use of radicals and sometimes imaginary. numbers. We were not able to solve the equations, or even to decide whether or not they have an algebraic solution (or solution in radicals in accordance with Abel's theorem), in any case with $n > 4$.

Examples 5.4.1. *The solution for the examples with radicals are as follows:*

1.

$$g_1 = a_1 \left(\sqrt[r]{1+a_0\,x} - 1\right) - \sqrt[n]{1+x} + 1$$

We have rational solution e.g., $a_1 = 2\,, a_0 = 1/2$ *which gives*

$$\begin{aligned} g_1 &= 2\sqrt[n]{1+\frac{1}{2}x} - 1 - \sqrt[n]{1+x} \\ &= \frac{-1+n}{4n^2}x^2 + O\left(x^3\right) \end{aligned}$$

2.

$$g_2 = a_2\left(1 + a_1\left(\sqrt[n]{\sqrt[r]{1+a_0\,x} - 1} - 1\right)\right) - \sqrt[r]{1+x} + 1$$

We have rational solutions i.e., rational values for the coefficients in terms of n *e.g.,* $a_1 = -1\,, a_2 = -n+1\,, a_0 = \frac{n}{n-1}$ *which gives*

$$\begin{aligned} g_2 &= (-n+1)\left(\sqrt[n]{2 - \sqrt[n]{1+\frac{nx}{n-1}}} - 1\right) - \sqrt[r]{1+x} + 1 \\ &= \frac{n+1}{6n^2\,(n-1)}x^3 + O\left(x^4\right) \end{aligned}$$

3.

$$g_3 = a_3 \left(\sqrt[n]{1 + a_2 \left(\sqrt[n]{1 + a_1 \left(\sqrt[n]{1 + a_0\, x} - 1 \right)} - 1 \right)} - 1 \right) - \sqrt[n]{1+x} + 1.$$

We still have a rational solution given by

$$a_2 = 2\,,\; a_0 = \frac{-2n}{n^2+2n+4}\,,\; a_1 = -\frac{n(n+2)}{2}\,,\; a_3 = \frac{n^2+2n+4}{2(2+n)} \quad ,$$

$$g_3 = \frac{1}{12} \frac{(n-1)\left(28\,n + 38\,n^2 + 25\,n^3 + 8\,n^4 + n^5 + 8\right)}{\left(2\,n + n^2 + 4\right)^3 n^2} x^4 + O\left(x^5\right)$$

4.

$$\begin{aligned} g_4 &= a_4 \left(\sqrt[n]{1 + a_3 \left(\sqrt[n]{1 + a_2 \left(\sqrt[n]{1 + a_1 \left(\sqrt[n]{1 + a_0\, x} - 1 \right)} - 1 \right)} - 1 \right)} - 1 \right) - \\ &\quad - \sqrt[n]{1+x} + 1\,. \\ &= \Big(650 - 250211\,n^3 - 284\,n^{10} + 8\,n^{11} + 89252\,n^2 - 12602\,n + 8\,n^{10}\sqrt{n^2-10\,n+1} - \\ &\quad -244\,n^9\sqrt{n^2-10\,n+1} - 646\sqrt{n^2-10\,n+1} + 192515\,n^4 + 124571\,n^7 - \\ &\quad -246800\,n^6 + 138664\,n^5 + 4106\,n^9 - 30797\,n^8 - 49176\,n^2\sqrt{n^2-10\,n+1} \\ &\quad +2982\,n^8\sqrt{n^2-10\,n+1} + 9440\,n\sqrt{n^2-10\,n+1} + 57016\,n^6\sqrt{n^2-10\,n+1} - \\ &\quad -72948\,n^5\sqrt{n^2-10\,n+1} - 8888\,n^4\sqrt{n^2-10\,n+1} + 83383\,n^3\sqrt{n^2-10\,n+1} - \\ &\quad -18335\,n^7\sqrt{n^2-10\,n+1}\Big)(-1+n)\,/ \\ &\quad /\left(15n^5\left(3n^2 - 22n + 3n\sqrt{n^2-10n+1} + 11 - 7\sqrt{n^2-10\,n+1}\right)^4\right) x^5 + O(x^6). \end{aligned}$$

Actually one gets rational solution or simplest radical form when a_2, the free parameter w.r.t. the system of equations, is a factor of n or its fractional multiple. This depends on the quadratic involved. $a_2 = n$ gives a simple solution.

A specific example with $n = 32$ yields the following using Maple

```
> f:=(1+x)^(1/32)-1;
```

$$f := (1+x)^{(1/32)} - 1$$

```
> h1:=a1*subs(x=a0*x,f):
> h2:=a2*subs(x=h1,f):
> h3:=a3*subs(x=h2,f):
> h4:=a4*subs(x=h3,f):
> g:=h4-f;
```

$$g := a4\,(1 + a3\,((1 + a2\,((1 + a1\,((1 + a0\,x)^{(1/32)} - 1))^{(1/32)} - 1))^{(1/32)} - 1))^{(1/32)} - 1 - (1+x)^{(1/32)} + 1$$

```
> g1:=diff(g,x):
> g2:=diff(g1,x):
> g3:=diff(g2,x):
> g4:=diff(g3,x):
> s1:=subs(x=0,{g1,g2,g3,g4});
```

$$s1 := \{ -\frac{31\,a4\,a3^2\,a2^2\,a1^2\,a0^2}{1099511627776} - \frac{31\,a4\,a3\,a2^2\,a1^2\,a0^2}{34359738368} - \frac{31\,a4\,a3\,a2\,a1^2\,a0^2}{1073741824} - \frac{31\,a4\,a3\,a2\,a1\,a0^2}{33554432} + \frac{31}{1024}, \frac{a4\,a3\,a2\,a1\,a0}{1048576} - \frac{1}{32}, \frac{1953\,a4\,a3^3\,a2^3\,a1^3\,a0^3}{1152921504606846976} + \frac{2883\,a4\,a3^2\,a2^3\,a1^3\,a0^3}{36028797018963968} + \frac{2883\,a4\,a3^2\,a2^2\,a1^3\,a0^3}{1125899906842624} + \frac{2883\,a4\,a3^2\,a2^2\,a1^2\,a0^3}{35184372088832} + \frac{1953\,a4\,a3\,a2^3\,a1^3\,a0^3}{1125899906842624} + \frac{2883\,a4\,a3\,a2^2\,a1^3\,a0^3}{35184372088832} + \frac{2883\,a4\,a3\,a2^2\,a1^2\,a0^3}{1099511627776} + \frac{1953\,a4\,a3\,a2\,a1^3\,a0^3}{1099511627776} + \frac{2883\,a4\,a3\,a2\,a1^2\,a0^3}{34359738368} + \frac{1953\,a4\,a3\,a2\,a1\,a0^3}{1073741824} - \frac{1953}{32768}, \frac{185535}{1048576} - \frac{181629\,a4\,a3^3\,a2^3\,a1^3\,a0^4}{18446744073709551616} - \frac{185535\,a4\,a3^4\,a2^4\,a1^4\,a0^4}{1208925819614629174706176} - \frac{181629\,a4\,a3^4\,a2^4\,a1^4\,a0^4}{18889465931478580854784} - \frac{181629\,a4\,a3^3\,a2^3\,a1^4\,a0^4}{590295810358705651712} - \frac{268119\,a4\,a3^2\,a2^3\,a1^3\,a0^4}{576460752303423488} - \frac{331545\,a4\,a3^2\,a2^4\,a1^4\,a0^4}{1180591620717411303424} - \frac{268119\,a4\,a3^2\,a2^3\,a1^4\,a0^4}{18446744073709551616} - \frac{268119\,a4\,a3^2\,a2^2\,a1^3\,a0^4}{18014398509481984} - \frac{331545\,a4\,a3^2\,a2^2\,a1^4\,a0^4}{1152921504606846976}$$

$$-\frac{331545\,a4\,a3^2\,a2^2\,a1^2\,a0^4}{1125899906842624}-\frac{181629\,a4\,a3\,a2^3\,a1^3\,a0^4}{18014398509481984}$$
$$-\frac{185535\,a4\,a3\,a2^4\,a1^4\,a0^4}{36893488147419103232}-\frac{181629\,a4\,a3\,a2^3\,a1^4\,a0^4}{576460752303423488}$$
$$-\frac{268119\,a4\,a3\,a2^2\,a1^3\,a0^4}{562949953421312}-\frac{331545\,a4\,a3\,a2^2\,a1^4\,a0^4}{36028797018963968}$$
$$-\frac{331545\,a4\,a3\,a2^2\,a1^2\,a0^4}{35184372088832}-\frac{181629\,a4\,a3\,a2\,a1^3\,a0^4}{17592186044416}$$
$$-\frac{185535\,a4\,a3\,a2\,a1^4\,a0^4}{1125899906842624}-\frac{331545\,a4\,a3\,a2\,a1^2\,a0^4}{1099511627776}$$
$$-\frac{185535\,a4\,a3\,a2\,a1\,a0^4}{34359738368}\}$$

```
> s:=solve(s1);
```

$$s := \{a3 = -\frac{1024\,(a2\,\%1 + 32\,a2 + 1024)}{a2\,(32\,\%1 + 1024 + a2\,\%1)},\ a2 = a2,\ a1 = \%1,\ a4 = -\frac{1}{544}(17\,\%1\,a2^4$$
$$+ 1584\,\%1\,a2^3 + 33280\,a2^3 + 34816\,\%1\,a2^2 + 1572864\,a2^2 + 1114112\,a2\,\%1$$
$$+ 34078720\,a2 + 17825792\,\%1 + 1090519040)\,/((32\,a2 + a2^2 + 1024)$$
$$(a2\,\%1 + 32\,a2 + 1024)),\ a0 = 16$$
$$(31\,\%1\,a2^3 - 1088\,\%1\,a2^2 + 2080\,a2^3 + 98304\,a2^2 + 2129920\,a2 + 68157440)\,/$$
$$(17\,\%1\,a2^4 + 1584\,\%1\,a2^3 + 33280\,a2^3 + 34816\,\%1\,a2^2 + 1572864\,a2^2$$
$$+ 1114112\,a2\,\%1 + 34078720\,a2 + 17825792\,\%1 + 1090519040)\}$$
$$\%1 := \mathrm{RootOf}((31\,a2^3 - 1088\,a2^2)\,\_Z^2$$
$$+ (32505856 - 98304\,a2 + 28672\,a2^2 + 992\,a2^3)\,\_Z - 1140850688$$
$$- 35651584\,a2 - 1114112\,a2^2)$$

```
> s1r:=convert(s,radical);
```

$$s1r := \left\{a2 = a2,\ a0 = 16\right.$$
$$(\frac{31\,\%1\,a2^3}{2\,\%2} - \frac{544\,\%1\,a2^2}{\%2} + 2080\,a2^3 + 98304\,a2^2 + 2129920\,a2 + 68157440)$$
$$\Big/(\frac{17\,\%1\,a2^4}{2\,\%2} + \frac{792\,\%1\,a2^3}{\%2} + 33280\,a2^3 + \frac{17408\,\%1\,a2^2}{\%2} + 1572864\,a2^2$$
$$+ \frac{557056\,a2\,\%1}{\%2} + 34078720\,a2 + \frac{8912896\,\%1}{\%2} + 1090519040),$$
$$a3 = -\frac{1024\,(\frac{a2\,\%1}{2\,\%2} + 32\,a2 + 1024)}{a2\,(\frac{16\,\%1}{\%2} + 1024 + \frac{a2\,\%1}{2\,\%2})},\ a1 = \frac{\%1}{2\,\%2},\ a4 = -(\frac{17\,\%1\,a2^4}{2\,\%2}$$
$$+ \frac{792\,\%1\,a2^3}{\%2} + 33280\,a2^3 + \frac{17408\,\%1\,a2^2}{\%2} + 1572864\,a2^2 + \frac{557056\,a2\,\%1}{\%2}$$
$$+ 34078720\,a2 + \frac{8912896\,\%1}{\%2} + 1090519040)\Big/(544\,(32\,a2 + a2^2 + 1024)$$

$$\left.\left(\frac{a2\,\%1}{2\,\%2}+32\,a2+1024\right)\right)\Bigg\}$$

$$\%1 := -32505856+98304\,a2-28672\,a2^2-992\,a2^3+32(1031865892864 -6241124352\,a2-3018850304\,a2^2+44105728\,a2^3+194560\,a2^4+190464\,a2^5 +961\,a2^6)^{(1/2)}$$

$$\%2 := 31\,a2^3-1088\,a2^2$$

```
> for i from -16 to -16
> do s1r1:=simplify(subs(a2=i,s1r)):
> end do;
```

$$s1r1 := \{a0=\frac{5}{9},\ -16=-16,\ a1=\frac{128}{3},\ a3=\frac{-32}{5},\ a4=\frac{27}{2}\}$$

```
> gnew:=subs({a2 = -16, a1 = 128/3, a0 = 5/9, a4 = 27/2, a3 = -32/5},g);
```

$$gnew := \frac{27\left(\frac{37}{5}-\frac{32\left(17-16\left(-\frac{125}{3}+\frac{128\,(1+\frac{5\,x}{9})^{(1/32)}}{3}\right)^{(1/32)}\right)^{(1/32)}}{5}\right)}{2}-\frac{23}{2}-f$$

```
> simplify(series(gnew,x=0,6));
```

$$\frac{544227475}{17832200896512}\,x^5+\mathrm{O}(x^6)$$

Using similar methods, we can construct examples based on different base functions, namely, $\ln(x), \sin(x)$, although in this case the original exp-log expression has two occurrences of x rather than just one, and the result, as an exp-log expression, has four occurrences of x.

Here are some other examples:

Examples 5.4.2. *1.*

$$\ln(1+x)+3\ln\left(1-\frac{1}{2}\ln\left(1+\ln\left(1+\frac{2}{3}x\right)\right)\right)$$

$$=-\frac{1}{1215}x^5+O\left(x^6\right)$$

2.

$$2\sin\left(\frac{1}{3}\sqrt{3}\sin\left(\frac{1}{2}\sqrt{3}x\right)\right)-\sin(x)$$

$$=\frac{1}{80}x^5+O\left(x^6\right)$$

3.

$$\frac{1}{2}\sqrt{2}\sqrt{3}\sin\left(\sin\left(\sqrt{-2}\sin\left(\frac{1}{6}\sqrt{3}\sqrt{2}\sqrt{-2}x\right)\right)\right)-\sin(x)$$

$$=\frac{4}{1701}x^7+O\left(x^8\right)$$

4.

$$\frac{3}{2}\exp\left(\exp\left(-2\exp(-\frac{1}{3}x)+2\right)-1\right)-\frac{1}{2}-\exp(x)$$

$$=-\frac{1}{1215}x^5+O\left(x^6\right)$$

We could not solve the equations to satisfy $g_n(x) = O(x^{n+1})$ for $n > 4$. Actually, what happens is that we try to solve a number of polynomial equations in a bigger number of parameters. The problem is the system of equations is getting more complicated and of higher degree as we do more nesting. For higher order of nesting we expect no solution or at least no solution in radicals.

5.5 Further Work

To check if we can do this testing to the power series of some class of functions we will need to use the Faa Di Bruno formula for the n-th derivative of the composite function $f(g(x))$ (discovered in 1850 and recently was generalised to the multi-variable case to suit recent applications)

Theorem 5.5.1. *(Faa Di Bruno formula) Let $h(x) = f(g(x))$. The derivative at x^0 is given by*

$$h_n = \sum_{k=1}^{n} f_k \sum_{p(n,k)} n! \prod_{i=1}^{n} \frac{g_i^{\lambda}}{(\lambda_i!)(i!)^{\lambda_i}}$$

where

$$h_n = \frac{d^n}{dx^n} h(x^0)\,,\ f_k = \frac{d^k}{dy^n} f(y^0),$$

$$y^0 = g(x^0)\,,\ g_i = \frac{d^i}{dx^i} g(x^0)$$

and

$$p(n,k) = \{(\lambda_1, \ldots, \lambda_n) : \lambda_i \in \boldsymbol{Z}_0\,,\ \sum_{i=1}^{n} \lambda_i = k\,,\ \sum_{i=1}^{n} i\,\lambda_i = n\}.$$

Remark 5.5.1. *$\boldsymbol{Z}_0$ is the set of non negative integers. A member $(\lambda_1, \ldots, \lambda_n) \in p(n.k)$ represents a partition of a set with n elements into λ_1 classes of cardinality 1 , ..., and λ_n classes of cardinality n.*

For our case we use the following notations:
Assume given a power series

$$f(x) = c_1 x + c_2 x^2 + c_3 x^3 + \cdots\,,$$

We define

$$h_1(x) = a_1 f(a_0 x)\,,\ h_{k+1}(x) = a_{k+1} f(h_k(x))\,,\ k = 1, 2, \ldots, n-1.$$

Let $D_n h_{k+1}$ be the n-th derivative of $h_{k+1}(x)$ evaluated at $x = 0$. Suppose $n < k$.

The problem is for which numbers $r_1, \ldots, r_k$ can we find values of the param-

eters $a_0, a_1, \ldots, a_n$ so that

$$D_i h_n = r_i\,,\ i = 1, \ldots, k$$

Assume $r_1, \ldots, r_k \in \boldsymbol{Q}$ can we have $a_0, a_1, \ldots, a_n \in \boldsymbol{Q}$?

Chapter 6

New Conjectures

> {And pursue not that of which thou hast no knowledge; for surely the hearing, the sight, the heart all of those shall be questioned of.} [17:36]

We will introduce in this chapter some new forms of the uniformity conjecture for some fields of complex numbers even when some of them are not in closed form. This what we call uniform and regular fields. That will be introduced in sections 6.1 and 6.2.

Another revised form of the UC for the expanded form numbers will be presented in section 6.3. This conjecture takes into account a new parameter which is the depth of the exression or the degree of nesting.

To extend some forms of the uniformity conjecture one may think in many directions. A natural extension is to consider the set of constants which acn be expressed by the Pfaffian functions and Pfaffian intersections. An introduction to this important set of functions and some important results will be the subject of section 6.4.

Suggested generalisations of the UC in the cases of the Pfaffian constants and Pfaffian intersections are presented in sections 6.5 and 6.6 using Khovanskii's bound on the multiplicity of intersection of Pfaffian functions.

Examples of the last kind are the algebraic and elementary numbers. In case of elementary numbers our conjecture gives a result which acn solve the decidability question of Tarski for the theory of exponential real field.

6.1 Uniform fields

Definition 6.1.1. *Let K be a finitely generated subfield of the complex numbers. We will say that K is uniform if there is a function $\lambda : K \to \boldsymbol{N}_+$ and a constant C (depends on the field) so that*

1.
$$\forall x, y \in K \; \lambda(x \circ y) \leq \lambda(x) + \lambda(y) + 1 \, , \circ \in \{+, -, \times, \div\}$$

2.
$$\forall x \in K \; x \neq 0 \to |x| > 10^{-C\,\lambda(x)}.$$

In this case λ is called a length function and C a uniformity constant.

We will need to use the following definitions

Definition 6.1.2. *A denominator for an algebraic number α is an integer n so that $n\alpha$ is an algebraic integer.*

Let in our case K be a field. A denominator for a-K algebraic number α is an integer of K, say n so that $n\alpha$ is an algebraic integer over K.

There may be many denominators for an algebraic number α, the lowest of them (in $\boldsymbol{N}$) is the denominator of α. It is always true that if α has a defining polynomial $a_d x^d + \cdots + a_0$ then a_d is a denominator of α.

In the case $K = \boldsymbol{Q}(x_1, x_2, \ldots, x_n) \subset \boldsymbol{C}$, any pure transcendental extension, the denominator of an algebraic number α over K is the lowest in the sense of h.c.f. of denominators of α since we have unique factorisation in the ring of integers of K. In this case also, denominator of α is the leading coefficient of its defining polynomial.

6.1.1 Extended Mahler measure

Assume K is a pure extension of $\boldsymbol{Q}$ i.e., $K = \boldsymbol{Q}(x_1, x_2, \ldots, x_n) \subset \boldsymbol{C}$ where $x_1, x_2, \ldots, x_n$ are algebraically independent over $\boldsymbol{Q}$ or equivalently $x_1, x_2, \ldots, x_n$ are variables. Any element in K is a fractional polynomial in $x_1, x_2, \ldots, x_n$ with integer coefficients. Let us call the elements of the polynomial ring $\boldsymbol{Z}[x_1, x_2, \ldots, x_n]$ integers of K. We remember also that in this ring we have unique factorisation.

We will here define Mahler measure for K

If $P = a_d x^d + \cdots + a_0 = a_d(x - \alpha_1) \cdots (x - \alpha_d) \in K[x]$

we define the Mahler measure of p as

$$m(P) = |a_d| \prod_{j=1}^{d} max(1, |\alpha_j|)$$

If α is **integral** over K then it satisfies a polynomial $P(\alpha) = 0$ where

$P = x^d + a_{d-1}x^{d-1} \cdots + a_0$

and $a_0, \ldots, a_{d-1}$ are integers of K

or generally suppose α algebraic over K then α satisfies $P(\alpha) = 0$ where the defining polynomial $P = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$ is irreducible over $K[x]$.

We define measure of α by

$m(\alpha) = m(P)$ where content $(P) = 1$, (i.e., GCD of the coefficients=1).

I'll verify the main properties of Mahler measure mentioned in chapter 2 for this case.

Proposition 6.1.1.

$$\frac{|a_0|}{m(\alpha)} \leq |\alpha| \leq \frac{m(\alpha)}{|a_d|}$$

Proof.

Assume α has a defining polynomial

$P = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0 = a_d(x - \alpha_1) \cdots (x - \alpha_d)$

with $a_d, \ldots, a_0$ integers in $K = \boldsymbol{Q}(x_1, \ldots, x_n)$

So $m(\alpha) \geq |a_d|\,|\alpha|$ i.e.,

$$|\alpha| \leq \frac{m(\alpha)}{|a_d|}$$

When α has a defining polynomial P as given above then $1/\alpha$ has a defining polynomial $x^d P(1/x)$. It is irreducible since otherwise P will be reducible too.

$$P(1/x) = a_d(1/x - \alpha_1) \cdots (1/x - \alpha_d)$$

and so

$$x^d P(1/x) = a_d(1 - x\alpha_1) \cdots (1 - x\alpha_d)$$

therefore,

$$x^d P(1/x) = (-1)^d a_d \alpha_1 \cdots \alpha_d (x - 1/\alpha_1) \cdots (x - 1/\alpha_d)$$

Hence

$$\begin{aligned} m(1/\alpha) &= m(x^d P(1/x)) \\ &= \left|(-1)^d a_d \alpha_1 \cdots \alpha_d\right| \prod_{j=1}^{d} max\,(1, 1/\left|\alpha_j\right|) \\ &= |a_d| \prod_{j=1}^{d} max\,(1, |\alpha_j|) \\ &= m(\alpha) \end{aligned}$$

so $m(1/\alpha) = m(\alpha)$ and hence applying the result we get

$$\left|\frac{1}{\alpha}\right| \leq \frac{m(1/\alpha)}{|a_d| \prod_{j=1}^{d} |\alpha_j|} = \frac{m(\alpha)}{|a_0|}$$

Hence

$$|\alpha| \geq \frac{|a_0|}{m(\alpha)}$$

Then the the result.

Proposition 6.1.2. *If α_1, α_2 are algebraic over K with degrees d_1, d_2*

$$m(\alpha_1 \alpha_2) \leq m(\alpha_1)^{d_2} m(\alpha_2)^{d_1}$$

Proof.

Assume α_1 has a defining polynomial

$P_1 = a_{d_1} x^{d_1} + a_{d_1 - 1} x^{d_1 - 1} + \cdots + a_0 = a_{d_1}(x - \alpha_1) \cdots (x - \alpha_{d_1})$.

and α_2 has a defining polynomial

$P_2 = b_{d_2} x^{d_2} + b_{d_2 - 1} x^{d_2 - 1} + \cdots + b_0 = b_{d_2}(x - \beta_1) \cdots (x - \beta_{d_2})$.

with the same conditions for coefficients as in 1.

Define the polynomial

$$q(x) = a_{d_1}^{d_2} b_{d_2}^{d_1} \prod_{i,j} (x - \alpha_i \beta_j)$$

The product in the definition is an invariant (with respect to the automorphisms which leave K fixed and hence only permute the roots) so the coefficients are in K.

$\alpha_1\,\alpha_2$ is a root of the polynomial $q(x)$. Moreover, this polynomial has coefficients $\in \boldsymbol{Z}[x_1,\ldots,x_n]$, what we call integers of K. Since the defining polynomial for $\alpha_1\alpha_2$ divides $q(x)$, this implies the estimates

$$\begin{aligned} m(\alpha_1\,\alpha_2) &\leq a_{d_1}^{d_2}\, b_{d_2}^{d_1} \prod_{i,j} max(1,|\alpha_i\beta_j|) \\ &\leq a_{d_1}^{d_2}\, b_{d_2}^{d_1} (\prod_{i} max(1,|\alpha_i|))^{d_2}\ (\prod_{j} max(1,|\beta_j|))^{d_1} \\ &= m(\alpha_1)^{d_2}\, m(\alpha_2)^{d_1} \end{aligned}$$

Proposition 6.1.3. *If α_1, α_2 are algebraic over K with degrees d_1, d_2*

$$m(\alpha_1+\alpha_2) \leq 2^{d_1 d_2} m(\alpha_1)^{d_2} m(\alpha_2)^{d_1}$$

Proof.

Assume as in the last property that α_1 has a defining polynomial

$P_1 = a_{d_1}x^{d_1} + a_{d_1-1}x^{d_1-1} + \cdots + a_0 = a_{d_1}(x-\alpha_1)\cdots(x-\alpha_{d_1})$.

and α_2 has a defining polynomial

$P_2 = b_{d_2}x^{d_2} + b_{d_2-1}x^{d_2-1} + \cdots + b_0 = b_{d_2}(x-\beta_1)\cdots(x-\beta_{d_2})$. with the usual conditions.

Define the polynomial

$$q(x) = a_{d_1}^{d_2}\, b_{d_2}^{d_1} \prod_{i,j}(x-(\alpha_i+\beta_j))$$

where a_{d_1}, a_{d_2} are the respective leading coefficients of the minimal polynomials P_1, P_2 of α_1, α_2 .

The product in the definition is an invariant (as in property 1) so the coefficients are in K.

$(\alpha_1+\alpha_2)$ is a root of the polynomial $q(x)$. So the irreducible polynomial defining $(\alpha_1+\alpha_2)$ is a factor of $q(x)$ and hence $m(\alpha_1+\alpha_2) \leq m(q(x))$. Moreover, this polynomial has coefficients $\in \boldsymbol{Z}[x_1,\ldots,x_n]$, what we call integers. This implies the estimates

$$\begin{aligned} m(\alpha_1 + \alpha_2) &\leq a_{d_1}^{d_2} b_{d_2}^{d_1} \prod_{i,j} max(1, |\alpha_i + \beta_j|) \\ &\leq a_{d_1}^{d_2} b_{d_2}^{d_1} 2^{d_1 d_2} max(1, |\alpha_i|)^{d_2} max(1, |\beta_j|)^{d_1} \\ &= 2^{d_1 d_2} m(\alpha_1)^{d_2} m(\alpha_2)^{d_1} \end{aligned}$$

Special case:

If $d_1 d_2 \leq d$

Then

$$m(\alpha_1 + \alpha_2) \leq 2^{d^2} [m(\alpha_1) m(\alpha_2)]^d$$

Proposition 6.1.4.

$$m(\alpha^{1/k}) \leq m(\alpha) \quad , k \in \boldsymbol{N}_+$$

Proof.

If $P = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0 = a_d(x - \alpha_1) \cdots (x - \alpha_d)$ is the the minimal polynomial of α over $\boldsymbol{Z}[x_1, \ldots, x_n]$. Then $\alpha^{1/k}$ is a root of the polynomial

$$\begin{aligned} q(x) &= P(x^k) \\ &= a_d(x^k)^d + a_{d-1}(x^k)^{d-1} + \cdots + a_0 \\ &= a_d(x^k - \alpha_1) \cdots (x^k - \alpha_d) \end{aligned}$$

This gives for every bracket k roots of the same modulus whether $|\alpha_i| > 1$ or $|\alpha_i| < 1$

hence we have

$$m(\alpha^{1/k}) \leq m(q) = m(P) = m(\alpha)$$

Proposition 6.1.5.

$$m(\alpha^{-1}) = m(\alpha) \; and \; m(\alpha^k) \leq m(\alpha)^k$$

Proof.

First part is already done in property 1

For the second part, It is clear that α^k is a root of $p(x^k)$ where $p(x)$ is the

minimal polynomial defining α with conjugates $\alpha_1, \ldots \alpha_d$.

$$\begin{aligned} m(\alpha^k) &= m(P(x^k)) \\ &= |a_d| \prod_{i=1}^{d} max(1, |\alpha_i|^k) \\ &= |a_d| \prod_{i=1}^{d} max(1, |\alpha_i|)^k \\ &\leq m(\alpha)^k \end{aligned}$$

This proves the result.

An upper bound bound for $m(c_1\,\alpha_1 + \cdots + c_n\,\alpha_n)$ can be deduced by induction in the following cases

Corollary 6.1.1. *If $c_1, \ldots, c_n \in \boldsymbol{Q} - \{0\}$ and $\alpha_1, \ldots, \alpha_n$ are algebraic over K of degrees bounded by d then*

$$m(c_1\,\alpha_1 + \cdots + c_n\,\alpha_n) \leq 2^{dn^2} \left| \prod_{i=1}^{n} m(c_i) \right|^{dn^2} (\prod_{i=1}^{n} m(\alpha_i))^{nd^n}$$

For this general case we will use the notation K^* for the integers of $K = \boldsymbol{Z}[x_1, \ldots, x_n]$

For $c \in K^*$ and α defined by $P(x) = 0$ then $c^n P(x/c)$ defines $c\alpha$

Corollary 6.1.2. *If $c_1, \ldots, c_n \in K^*$ and $\alpha_1, \ldots, \alpha_n$ are algebraic over K of degrees bounded by d then*

$$m(c_1\,\alpha_1 + \cdots + c_n\,\alpha_n) \leq 2^{dn^2} \left| \prod_{i=1}^{n} m(c_i) \right|^{dn^2} (\prod_{i=1}^{n} m(\alpha_i))^{nd^n}$$

Remarks 6.1.1. *1. If $c \in \boldsymbol{Z} - \{0\}$ then $m(c) = |c|$*

2. If $c \in \boldsymbol{Z} - \{0\}$ and α is algebraic of degree d over K then
$m(c\,\alpha) \leq |c|^d\, m(\alpha)$

3. If $c_1, c_2 \in \boldsymbol{Z} - \{0\}$ and α is algebraic of degree d over K then
$m(c_1 + c_2\,\alpha) \leq 2^d\, |c_1\,c_2|^d\, m(\alpha)$

4. *If* $c = p/q \in \boldsymbol{Q} - \{0\}$ *then* $m(c) = max(|p|, |q|)$

Open Problem 3. *Is every algebraic number field uniform?*

Discussion

Let α *be a primitive element for an algebraic number field* K *i.e.,* $K = \boldsymbol{Q}[\alpha]$.
Let us try $\lambda(x) = \lceil \log m(x) \rceil \ m(x) > 0$
A.
1.
$m(x \pm y) \leq 2^{d^2}[m(x)m(y)]^d$
so $\lambda(x \pm y) < d^2 \log 2 + d[\lambda(x) + \lambda(y)]$
2.
$m(xy) \leq [m(x)m(y)]^d$
so $\lambda(xy) < d[\lambda(x) + \lambda(y)]$
3.
$m(x/y) = m(x * 1/y) \leq [m(x)m(1/y)]^d$
so $\lambda(x/y) < d[\lambda(x) + \lambda(y)]$
since $m(1/y) = m(y)$
B.
If $x \in K/\{0\}$ *then* $\frac{1}{m(x)} \leq |x| \leq m(x)$
$\lambda(x) = \lceil \log m(x) \rceil \ \ m(x) > 0$
$\lambda(x) \geq \log m(x)$ *and hence* $m(x) \leq 10^{\lambda(x)} < 10^{c\lambda(x)}$ *where* $c > 1$ *say* $c = 2$
therefore, $|x| > 10^{-2\lambda(x)}$
It does not suffice to have or to prove
$\lambda(x + y) \leq K(\lambda(x) + \lambda(y))$. *So we can not use the* $\lambda(x)$ *as a length function.*
Every x *in* K *can be represented as*
$c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1}$, $n =$ *degree*(α).
If we define

$$\lambda(x) = \lceil (\log max|c_0, c_1, \ldots, c_{n-1}|) \ \rho \rceil$$

for some ρ *dependent on* K, *where* $\lceil a \rceil$ *is the smallest integer* $n \geq a$.

Open Problem 4. *Suppose* K *is a uniform finitely generated subfield of the complex numbers* $\boldsymbol{C}$ *then any algebraic extension of* K *is uniform.*

6.2 Regular fields

Definition 6.2.1. *Let K be a finitely generated subfield of the complex numbers. We will say that K is regular if there is a length function $\lambda : K \to \boldsymbol{N}_+$ and a degree function $\delta : K \to \boldsymbol{N}$ and a uniformity constant C so that*

1.
$$\forall x, y \in K \;\; \lambda(x \circ y) \leq \lambda(x) + \lambda(y) + 1 \, , \circ \in \{+, -, \times, \div\}$$

2.
$$\forall x, y \in K \;\; \delta(x \pm y) \leq max(\delta(x), \delta(y))$$

3.
$$\forall x, y \in K \;\; \delta(x \circ y) \leq \delta(x) + \delta(y) \, , \circ \in \{\times, \div\}$$

4.
$$\forall x \in K \;\; x \neq 0 \to |x| > 10^{-C\,\lambda(x)(\delta(x)+1)}.$$

The uniform fields defined earlier are all regular, since we can let $\delta(x) \equiv 0$

Definition 6.2.2. *Let K be a finitely generated subfield of the complex numbers. A proper set of generators for K is $(x_1, \ldots, x_n), y$ where $(x_1, \ldots, x_n)$ are algebraically independent over $\boldsymbol{Q}$ and y is integral and algebraic over $\boldsymbol{Q}(x_1, \ldots, x_n)$.*

So if $(x_1, \ldots, x_n), y$ is a proper set of generators for K then y has a defining equation $y^d + a_{d-1}y^{d-1} + \cdots + a_0 = 0$ where $(a_{d-1}, \ldots, a_0) \in \boldsymbol{Z}[x_1, \ldots, x_n]$. The number d is the degree of y over $\boldsymbol{Z}[x_1, \ldots, x_n]$.

Given a proper set of generators for K we get a canonical form for any element $\alpha \in K$ and hence we can compute upper bounds for $\lambda(\alpha)$ and $\delta(\alpha)$ from $\lambda(x_1), \ldots, \lambda(x_n), \lambda(y)$ and $\delta(x_1), \ldots, \delta(x_n), \delta(y)$, by referring to degree and length of the canonical form.

Theorem 6.2.1. *For almost all $(x_1, \ldots, x_n)$ in the unit cube $\boldsymbol{Q}(x_1, \ldots, x_n)$ is regular.*

We begin by some notations:
Let us write $[0,1]^n$ for the unit cube in $\boldsymbol{R}^n$ and identify $\boldsymbol{C}^n$ with $\boldsymbol{R}^{2n}$
Let the domain $D \subset [0,1]^{2n} \subset \boldsymbol{R}^{2n}$ and map to $\boldsymbol{C}^n$

We know that Lebesgue measure L is a generalisation of volume (Prob $((x_1,\ldots,x_n) \in S) = L(S)$*), so assume that we have uniform probability distribution on the domain D. See Zippel [Zip93] for the results about uniform probability distributions and see also theorem 4.3.1.*

Proof.

1.

We need to show that the set

$$S = \{(x_1,\ldots,x_n) : (\exists\, \infty\, many) P \in \boldsymbol{Z}[x_1,\ldots,x_n] : (|P(x_1,\ldots,x_n)| < 10^{-k(P)})\}$$

is a measurable set.

Let us look at

$$S_N = \{(x_1,\ldots,x_n) : (\exists\, i > N)(|P_i(x_1,\ldots,x_n)| < 10^{-k(P_i)})\}$$

We can show that

$$S = \bigcap_{N=1}^{\infty} S_N = \overline{\bigcup_{N=1}^{\infty} \overline{S_N}}$$

and thus we need only to show that each S_i *is measurable set and hence S. (because the class of measurable sets is closed under the operations of countable intersection and union.)*

To prove that $S = \bigcap_{N=1}^{\infty} S_N$*:*

(1a)

Clearly we have $S_{j+1} \subset S_j$ *and hence if* $(x_1,\ldots,x_n) \in S$ *then there are infinitely many polynomials satisfying the condition and so*

$(x_1,\ldots,x_n) \in S_j \forall j$.

and so $(x_1,\ldots,x_n) \in \bigcap S_j$.

which gives $S \subset \bigcap_{N=1}^{\infty} S_N$

(1b)

Suppose $(x_1,\ldots,x_n) \notin S$*. This means that there are only finitely many* P_i *with the required condition* $|P_i(x_1,\ldots,x_n)| < 10^{-k(P_i)}$

Let t be an upper bound on i so $(x_1,\ldots,x_n) \notin S_{t+1}$.

$(x_1,\ldots,x_n) \notin \bigcap_{j=1}^{\infty} S_j$.

Therefore, $S \supset \bigcap_{N=1}^{\infty} S_N$. *Hence the claim.*

Back to the proof that S *is measurable set, we have*

$$S_j = \bigcup_{i=j}^{\infty} \{(x_1, \ldots, x_n) : P_i \neq 0\,,\ |P_i(x_1, \ldots, x_n)| < 10^{-k(P_i)}\}$$

This is a countable union of semi-algebraic sets i.e., (sets defined by Boolean combinations of polynomial inequalities). S_j *is a simple one defined by only one inequality* $|P_i(x_1, \ldots, x_n)| < 10^{-k(P_i)}$ *where* $k(P_i)$ *is a constant (the value of the function* k *at* P_i *).*

We know that semi-algebraic sets are measurable sets and hence the requirement.

2.

Let $P_i\,;\ i = 1, 2, \ldots$ *enumerate* $\boldsymbol{Z}[x_1, \ldots, x_n]$ *and suppose*

$k : \boldsymbol{Z}[x_1, \ldots, x_n] \longrightarrow \boldsymbol{R}$ *is some map i.e.,* $(k(P_i) \in \boldsymbol{R})$

Suppose the series $\sum_{i=1}^{\infty} d(P_i)\, 10^{-k(P_i)/d(P_i)}$ *converges. This means that*

$\forall\, \epsilon > 0\, \exists\, N \in \boldsymbol{N}$ *such that*

$\sum_{i=N}^{\infty} d(P_i)\, 10^{-k(P_i)/d(P_i)} < \epsilon$

Suppose $(x_1, \ldots, x_n)$ *is picked at random in* D *with uniform distribution then we have the following*

$$Prob\left(|P_i(x_1, \ldots, x_n)| < 10^{-k(P_i)}\right) < L(D)$$

therefore by theorem 4.3.1 we have

$$Prob\left(|P_i(x_1, \ldots, x_n)| < 10^{-k(P_i)}\right) < 2\, d(P_i)\, 10^{-k(P_i)/d(P_i)}$$

And

$$Prob\left(\exists\, P \in \boldsymbol{Z}[x_1, \ldots, x_n] : (|P(x_1, \ldots, x_n)| < 10^{-k(P)})\right) < \sum_{i=1}^{\infty} 2\, d(P_i)\, 10^{-k(P_i)/d(P_i)}$$

$(x_1, \ldots, x_n)$ *is picked at random in* D *and the probability that there are infinitely many* $P \in \boldsymbol{Z}[x_1, \ldots, x_n]$ *such that* $(|P(x_1, \ldots, x_n)| < 10^{-k(P)})$ *is*

$$Prob\left(\exists\infty\, many\right)P \in \boldsymbol{Z}[x_1,\ldots,x_n] : \left(|P(x_1,\ldots,x_n)| < 10^{-k(P)}\right) < \sum_{i=N}^{\infty} 2\,d(P_i)\,10^{-k(P_i)/d(P_i)}$$

This sum $\longrightarrow 0$ *as* $N \longrightarrow \infty$. *But this is true for every* $N \in \boldsymbol{N}$ *so we must have*

$$Prob\left(\exists\infty many\right)P \in \boldsymbol{Z}[x_1,\ldots,x_n] : \left(|P(x_1,\ldots,x_n)| < 10^{-k(P)}\right) = 0$$

3.

Since

$$Prob\left(\exists\infty\, many\right)P \in \boldsymbol{Z}[x_1,\ldots,x_n] : \left(|P(x_1,\ldots,x_n)| < 10^{-k(P)}\right) = 0$$

Therefore, we have with probability 1 only finitely many P_i; $i = 1,\ldots,N$ *so that* $|P_i(x_1,\ldots,x_n)| < 10^{-k(P_i)}$.

So we can pick c (large enough to take care of $P_1,\ldots,P_N$*) so that*

$$|P_i(x_1,\ldots,x_n)| > 10^{-c\,k(P_i)}\ \forall\, P \in \boldsymbol{Z}[x_1,\ldots,x_n]$$

Of course c depends on the chosen point $(x_1,\ldots,x_n)$.

4.

We need to show $\sum_{i=1}^{\infty} d(P_i)\,10^{-k(P_i)/d(P_i)}$ *really converges so we divide it according to the length or the degree as follows*

$$\sum_{i=1}^{\infty} d(P_i)\,10^{-k(P_i)/d(P_i)} = \sum_{l=1}^{\infty}\sum_{P:l(P)=l} d(P)\,10^{-k(P)/d(P)}$$

where $l(P)$ *is the length of* P *and we notice that the number of polynomials with length* $l < 10^{l+1}$ *and hence*

$$\sum_{i=1}^{\infty} d(P_i)\,10^{-k(P_i)/d(P_i)} = \sum_{l=1}^{\infty} 10^{l+1}\ max_{\{l(P)=l\}}\left\{d(P)\,10^{-k(P)/d(P)}\right\}$$

Since $d(P) \le l(P)$ *and choosing the map k to be* $k(P) = 2\,d(P)\,l(P)$, *then*

$$max_{\{l(P)=l\}}\left\{d(P)\,10^{-k(P)/d(P)}\right\} \le l(P)\,10^{-2\,l(P)} = l\,10^{-2l}$$

and therefore

$$\sum_{i=1}^{\infty} d(P_i)\, 10^{-k(P_i)/d(P_i)} \leq \sum_{l=1}^{\infty} 10^l\, l\, 10^{-2l} = \sum_{l=1}^{\infty} l\, 10^{-l}$$

which is convergent. This completes the proof.

Remark 6.2.1. *With Probability 1 at any random point $X = (x_1, \ldots, x_n)$ there exists $C_X > 1$ such that*

$$|P(x_1, \ldots, x_n)| \geq 10^{-2\, C_X\, l(P_i)\, d(P_i)} \text{ for all } P \neq 0$$

This does not say we are absolutely sure that if we pick a point we get the result because we can still have countably or even uncountably infinite many exceptions in a set with measure zero, saying that all such fields (even algebraic fields) are regular! But this is our conjecture.

We have more conjectures for future study

Conjecture 6. *Suppose K is a regular finitely generated subfield of the complex numbers $\boldsymbol{C}$ then any algebraic extension of K is regular and*

Conjecture 7. *Suppose K is a regular subfield of $\boldsymbol{C}$ and y is integral and algebraic over K. Does it follow that $K[y]$ is regular?*

6.3 Modified uniformity conjecture

Conjecture 8. *Let E be an expanded form exp-log expression representing a non zero number x then*

$$|x| \geq \max(H, 2)^{-C\, 2^{d(E)}}$$

where H is the maximum of the absolute values of the integers in E, C is some universal constant as in the V.D.Hoeven paper (counter examples to witness conjectures) and $d(E)$, the depth of E is defined by

$d(n) = 1,$

$d(A \circ (B) = 1 + max(d(A), d(B)) \,,\ \circ \in \{+, -, \times, \div\}\ ,$

$d(\circ(A)) = 1 + d(A) \,,\ \circ \in \{exp, log, \sqrt{}\}$

This is quite close to the uniformity conjecture, but it avoids the counter examples as we can see or as I mentioned in chapter 5 for the counter examples there.

I will begin by showing some results about the depth of expressions representing polynomials using complete binary trees.

Lemma 6.3.1. *If $P \in \boldsymbol{Z}[x]$ of degree n then P has a representation of depth d*
$d \leq 2\lceil \log_2 n \rceil + 1$

A similar result applies to the case of polynomials of multi variables as follows

Lemma 6.3.2. *If $P \in \boldsymbol{Z}[x_1, \ldots, x_k]$ of total degree n then P has a representation E of depth $\leq d_1 + d_2 + 1$ where*
$2^{d_1} \geq$ *number of monomials in the distributed form and* $2^{d_2} \geq n$

The proof is clear by induction on the height of the binary trees representing the polynomials and using enough ones and zeros for addition and multiplication in place of the missing variables.

Examples 6.3.1. *1. Let the expression E represent*

$f(z) = 2\log(1 - \log(1 - z/2)) - z = O(z^3)$

when $z = 10^{-k}$. The height $H = 10^k$ and the depth of E is the number of nodes in the longest branch added 1 i.e., $d(E) = 9$.

2. *$K = \boldsymbol{Q}[\sqrt{\eta}]$, $\eta \in \boldsymbol{N}$ satisfies the conjecture*

This is because for any $\alpha \in K$ it has a canonical representation $\alpha = a + b\sqrt{\eta}$, $a = p_1/q_1$, $b = p_2/q_2 \in \boldsymbol{Q}$

Let $H = max(= p_1, q_1, p_2, q_2, \eta)$ so H is the height of the expression with depth $d(E) = 4$. Using the properties and corollaries in the last section we get

$m(\alpha) < 4H^5$

While $\max(H, 2)^{c\,2^{d(E)}} = \max(H, 2)^{c\,2^4} > m(\alpha)$ *using even* $c = 1$

This implies $|\alpha| > \max(H, 2)^{c\,2^{d(E)}}$

3. $K = \boldsymbol{Q}[\sqrt[n]{\eta}]$, $\eta \in \boldsymbol{N}$ *where* $n > 1$

   This is similar to the case in the second example but in the general case where we cannot verify the conjecture using the technique of the bound of Mahler measure we have. This shows the gap between what we can prove and we conjecture which is interesting.

Comparison between the revised conjecture and EGC results

Comparing this conjecture with the EGC and the improved height measure bounds mentioned in chapter 2 we see that there is a big gap between them. For example let us compute the bound for a simple expression say,

$E = \sqrt[n]{a} - p/q$

the BFMS bound is given by

$val(E) > u(E)^{-n^2+1}/l(E)$

while the modified conjecture supposes the bound to be

$\max(H,2)^{-c2^{d(E)}} = \max(H,2)^{-8c}$ *where* $H = max(n, |a|, |p|, |q|)$.

The difference will be very significant when n is larger which encourages us to work with such conjectures until it is proved or disproved .

6.4 Pfaffian functions

Pfaffian functions are solutions of certain triangular systems of first order partial differential equations with polynomial coefficients.

This special class of transcendental functions, which was first introduced by Khovanskii [Kho80], contains many important members such as polynomials, the exponential and logarithmic functions and trigonometric functions in bounded domains. Khovanskii proved that in the real domain the number of non-degenerate solutions of a system of Pfaffian equations is finite and that it admits an explicit bound in terms of the format of the Pfaffian functions involved. We are interested in the case when the coefficients involved in definitions (Of the polynomial and the differential equations) are rational numbers.

6.4.1 Basic definitions and examples

Definition 6.4.1. *A* Pfaffian chain *of the order* $r \geq 0$ *and degree* $\alpha \geq 1$ *in an open domain* $G \subset \boldsymbol{R}^n$ *is a sequence of real analytic functions* $f_1, \ldots, f_r$ *in* G

satisfying Pfaffian equations

$$df_j(X) = \sum_{1 \le i \le n} g_{ij}(X, f_1(X), \ldots, f_j(X))dX_i \tag{6.1}$$

for $1 \le j \le r$. *Here each* $g_{ij}(X,Y)$ *is a polynomial with real coefficients in* $X = (X_1, \ldots, X_n)$ *and* $Y = (Y_1, \ldots, Y_j)$, *of degree not exceeding* α. *The system of equations 6.1 is triangular in the sense that* g_{ij} *does not depend on* f_k *for* $k > j$. *A function*

$$f(X) = P(X, f_1(X), \ldots, f_r(X))$$

where $P(X, Y_1, \ldots, Y_r)$ *is a polynomial over* $\boldsymbol{R}$ *of degree not exceeding* $\beta \ge 1$ *is a* Pfaffian function *of order* r *and degree* (α, β).

This standard definition and the following list of examples are taken from S. Pericleous Ph.D thesis [Per02] and [GV95]. There are more general definitions which can be referred in [Kho80].

We define rational Pfaffian chain and rational Pfaffian function as a special case considering rational coefficients in all the equations and the polynomial $P(X, Y_1, \ldots, Y_r)$ *is a polynomial over* $\boldsymbol{Q}$. *For the purpose of our conjectures we need to define another parameter, namely, the height* H *of a rational Pfaffian function as the height of the maximum coefficient appearing in the defining polynomial and whole system of equations.*

Next, we consider some examples of Pfaffian functions taken from [Kho91], [GV95] with restriction to the case of rationals

Examples 6.4.1. *1. Pfaffian functions of order 0 and degree* $(1, \beta)$ *are polynomials of degree not exceeding* β.

2. *The exponential univariate function* $f(X) = e^{aX}$ *is a (rational) Pfaffian function of order 1 and degree* $(1,1)$ *in* $\boldsymbol{R}$, *due to the equation*

$$df(X) = af(X)dX\,, a \in \boldsymbol{Q}$$

3. *The function* $f(X) = 1/X$ *is a (rational) Pfaffian function of order 1 and degree* $(2,1)$ *in the domain* $X \neq 0$, *due to the equation*

$$df(X) = -f^2(X)dX.$$

4. *The logarithmic function* $f(X) = \ln(|X|)$ *is a (rational) Pfaffian function of order 2 and degree* $(2,1)$ *in the domain* $X \neq 0$, *due to the equations*

$$df(X) = g(X)dX, \qquad dg(X) = -g^2(X)dX,$$

with $g(X) = 1/X$.

5. *The polynomial* $f(X) = X^p$ *can be considered as a (rational) Pfaffian function of order* 2 *and degree* $(2,1)$ *in the domain* $X \neq 0$, *due to the equations*

$$df(X) = pf(X)g(X)dX, \qquad dg(X) = -g^2(X)dX,$$

with $g(X) = 1/X$.

6. *The function* $f(X) = tan(X)$ *is a Pfaffian function of order* 1 *and degree* $(2,1)$ *in the domain* $X \neq \pi/2 + k\pi$, *for all* $k \in \boldsymbol{Z}$, *due to the equation*

$$df(X) = (1 + f^2(X))dX.$$

7. *The function* $f(X) = arctan(X)$ *is a Pfaffian function in* $\boldsymbol{R}$ *of order* 2 *and degree* $(2,1)$, *due to the equations*

$$df(X) = g(X)dX, \qquad dg(X) = -2Xg^2(X)dX,$$

with $g(X) = (X^2 + 1)^{-1}$.

8. *The function* $cos(X)$ *is Pfaffian of order* 2 *and degree* $(2,1)$ *in the domain* $X \neq \pi + 2k\pi$, *for all* $k \in \boldsymbol{Z}$, *due to the equations*

$$cos(X) = 2f(X)-1, \quad df(X) = -f(X)g(X)dX, \quad dg(X) = 1/2(1+g^2(X))dX,$$

with $f(X) = cos^2(X/2)$ *and* $g(X) = tan(X/2)$.

9. *The function* $sin(X)$ *is Pfaffian of order* 3 *and degree* $(2,1)$ *in the domain* $X \neq \pi + 2k\pi$, *for all* $k \in \boldsymbol{Z}$, *due to the equation*

$$df(X) = g(X)dX,$$

with $g(X) = cos(X)$.

More examples of general Pfaffian functions can be found in [Kho91], [GV95], [Zel99].

6.4.2 Khovanskii's bound and some properties

The set of Pfaffian functions in an open domain G is clearly, a subalgebra of the algebra of analytic functions in G, that is closed under differentiation.

In addition, one can effectively estimate the complexity cost of the application of any given operation.

The following two lemmas are from [Kho91], [GV95] and they discuss the basic algebraic properties of the set of Pfaffian over some domain.

Lemma 6.4.1. *1. The sum (resp. product) of two Pfaffian functions,* f_1 *and* f_2*, of orders* r_1 *and* r_2 *and degrees* (α_1, β_1) *and* (α_2, β_2)*, is a Pfaffian function of the order* $r_1 + r_2$ *and degree* $(max(\alpha_1, \alpha_2), max(\beta_1, \beta_2))$ *(resp.* $(max(\alpha_1, \alpha_2), \beta_1 + \beta_2)$*). If the two Pfaffian functions are defined by the same Pfaffian chain of order r, then the order of the sum and product is also r.*

2. A partial derivative of a Pfaffian function of order r and degree (α, β) *is a Pfaffian function of order r and degree* $(\alpha, \alpha + \beta - 1)$.

Lemma 6.4.2. *Let G be an open domain in* $\boldsymbol{R}^n$ *and* $f : G \longrightarrow \boldsymbol{R}$ *a Pfaffian function with Pfaffian chain* $f_1, \ldots, f_r$ *of degree* (α, β)*. Then its Taylor expansion*

$$\check{f}_\lambda(X - z) := \sum_{k:|k|\leq\lambda} \frac{1}{k_1! \cdots k_n!} \frac{\partial^{|k|} f}{\partial X^k}(z)(X - z)^k, \tag{6.2}$$

of order λ *at* $z \in G$*, with* $|k| = k_1 + \cdots + k_n$*, is a polynomial in* $X, z, f_1(z), \ldots, f_r(z)$ *of degree* $\beta + \alpha\lambda$.

Proof. *The proof of these results is straightforward and can be found in [GV95].*

Also we have the following

Lemma 6.4.3. *1. The set of Pfaffian functions contains algebraic functions ,*

2. The set of Pfaffian functions is closed under the operation of composition of Pfaffian functions and

3. Functions implicitly defined from Pfaffian functions are Pfaffian.

The following important bound for the multiplicity at a specific point was introduced by Khovanskii.

Theorem 6.4.1. *Let $f_1, \ldots, f_n$ be Pfaffian functions in an open domain $G \subset \boldsymbol{R}^n$ of degree at most β in a common Pfaffian chain of order r and degree α. The number of non-degenerate solutions in G of the system $f_1 = \cdots = f_n = 0$ is bounded by*

$$\beta^n O(n\beta + min(r,n)\alpha)^r 2^{r(r-1)/2}. \tag{6.3}$$

And we have a more explicit result also from [GV03] in the form of

Theorem 6.4.2. *Consider a system of equations $f_1 = \cdots = f_n = 0$, where $f_i, 1 \leq i \leq n$ are Pfaffian functions in a domain $G \subset \boldsymbol{C}^n$ having a common Pfaffian chain of order r and degrees (α, β_i) respectively. Then the number of non-degenerate solutions of this system does not exceed*

$$M(n, r, \alpha, \beta_1, \ldots \beta_n) := 2^{r(r-1)/2}\, \beta_1 \cdots \beta_n\, (min\{n, r\}\alpha + \beta_1 + \cdots \beta_n - n + 1)^r. \tag{6.4}$$

Remarks 6.4.1. *1. Khovanskii's bound can be considered as a generalisation of the known Bezout's bound. This gives (for finite case) an upper bound on the number of isolated points of intersection of polynomials $f_1, \ldots, f_n$ as the product of their degrees $d_1 \ldots d_n$.*

2. What we mean by non-degenerate is that the tangents at the points of intersection are linearly independent or the Jacobian of the functions at that point does not vanish.

6.5 Zero testing of Pfaffian constants

Define Pfaffian chain with parameters (r, α, β, n) Take $n = 1$ and the domain $G \supset [0, 1]$ in the real or complex case.

Suppose $\gamma = f(1) = P(1, f_1(1), \ldots, f_r(1))$ is a given constant where $f(x)$ is a rational Pfaffian function. Assume also that (to get rid of arbitrary constants)

$$f_i(0) = 0\ , i = 1, \ldots, r$$

To try an analogue of the uniformity conjecture to such constants we have to have bounded functions over the domain D. Let H be an upper bound on the absolute values of $f_1, \ldots, f_r$ for $x \in G \subset D$ and the height of coefficients in the system of equations and polynomial and define also $Kh(f)$ to be the previously defined Khovanskii's bound for f.

Conjecture 9.

$$\gamma \neq 0 \longrightarrow |\gamma| > \max(H, 2)^{-C\,kh(f)}$$

The first thing to ask and try to check in this sort of generalisation is what constants γ would this apply to?

Examples 6.5.1. *1.* **Case of rationals**

The first and easiest case is to check the rationals. For a rational number $C = \frac{p}{q}$ we easily say $C = f(1)$ where $f = \frac{px}{q}$.

$h(f) = max(l(p), l(q))$, $f' = \frac{p}{q}$,

order $r = 0$ since we have an empty chain,

degree is $(\alpha, \beta) = (1, 1)$

and so $kh(f) = 1$ since $n = 1$

and hence 6.4 says in this simple case that

$$C = \frac{p}{q} \neq 0 \longrightarrow \left|\frac{p}{q}\right| > 10^{-max(l(p),l(q))}$$

which is clearly true.

2. **Case of radicals**

We can verify the conjecture in cases of the form

$$\lambda = n_1 a_1^{p_1/q_1} + n_2 a_2^{p_2/q_2}$$

Consider the first part $c_1 = n_1 a_1^{p_1/q_1}$. It is a Pfaffian constant with our conditions using $f(x) = n_1(a_1 x)^{p_1/q_1}$ and so $c_1 = f(1)$

$h(f) = max(l(n_1(a_1)^{p_1/q_1}))$

$f' = (a_1 x)^{p_1/q_1 - 1} n_1 p_1/q_1$.

6.6 Pfaffian intersections and zero testing

Another way to represent some important constants like algebraic numbers and elementary numbers is to deal with them as Pfaffian intersection which simply means a point of intersection of a system of equations of Pfaffian functions. The following formal definitions are from [GV03].

Definition 6.6.1. *Let K be either $\boldsymbol{R}$ or $\boldsymbol{C}$. A deformation of a Pfaffian function $f(X)$ in $G \subset K^n$ is an analytic function $\theta(X, \epsilon)$ such that $\theta(X, 0) = f(X)$ and, for a fixed ϵ, the function $\theta(X, \epsilon)$ is Pfaffian having the same Pfaffian chain and the same degree as $f(X)$.*

Definition 6.6.2. *Let $f_1(X), \ldots, f_n(X)$ be Pfaffian functions in $G \subset K^n$. The multiplicity at $Y \in G$ of the Pfaffian intersection*

$$f_1(X) = \cdots = f_n(X) = 0$$

is a maximal number of isolated complex solutions, for a fixed $\epsilon \neq 0$, of the system of equations

$$\theta_1(X, \epsilon) = \cdots = \theta_n(X, \epsilon) = 0$$

converging to Y as $\epsilon \to 0$. Here $\theta_i(X, \epsilon)$ is any deformation of $f_i(X)$ for all $1 \leq i \leq n$.

The following theorem from [Gab95] states that the bound for multiplicity is given by the same Khovanskii's bound 6.4.

Theorem 6.6.1. *Let $f_1(X), \ldots, f_n(X)$ be Pfaffian functions in a domain $G \subset K^n$ having a common Pfaffian chain of order r and degrees (α, β_1), ..., (α, β_n) respectively. Then the multiplicity of the Pfaffian intersection*

$$f_1(X) = \cdots = f_n(X) = 0$$

at any point $Y \in G$ does not exceed 6.4.

Now we propose the following important conjecture

Conjecture 10. *Suppose γ is a number defined by Pfaffian intersection $\in K^n$*

$$f_1(X) = \cdots = f_n(X) = 0$$

with parameters $(r, \alpha, \beta_1, \ldots, \beta_n)$. *Let* $Kh(\gamma)$ *be the bound as in (6.4) and* H *be the height of the intersection as in conjecture 9. Then if* $x_i \neq 0$ *is any coordinate of* γ

$$|x_i| > \max(H, 2)^{-C\,kh(\gamma)}$$

Examples 6.6.1. *1.* **Case of algebraic numbers**

Say $\gamma \neq 0$ *is an algebraic number, defined by* $P(x) = 0$ *where* $P(x) \in \boldsymbol{Z}[x]$ *with degree* d *and height* H. *Assume* $|\gamma| \leq 1$. *The Pfaffian chain is empty. The parameters in the Pfaffian chain in this case are* $r = 0,\ \alpha = 0,\ \beta = d,\ n = 1$

Hence the Khovanskii's bound is d *and the conjecture says*

$$|\gamma| > \max(H, 2)^{-Cd}$$

which is true for $C = 1$, *and can be proved using Mahler measure.*

2. **Case of general algebraic equations**

Suppose x, y *are in unit ball in* $\boldsymbol{C}$ *and related by*

$$y - Q(x) = 0\ P(x) = 0$$

where $P, Q \in Z[x]$ *of degree* d *and height* H. $\gamma = (x, y)$ *is a Pfaffian intersection with an empty chain again and* $Kh(\gamma) = d^2$ *according to (6.4). The conjecture gives*

$$y \neq 0 \longrightarrow |y| > \max(H, 2)^{-Cd^2}$$

which is true with $C = 1$. *It can be proved by using Mahler meassure or using the Liouville estimate theorem 2.3.2.*

3. **Case of elementary numbers**

Definition 6.6.3. *An* elementary number *is a number of the form* $q(\alpha)$ *where* $q \in \boldsymbol{Z}[x_1, \ldots, x_n]$, *and* α *is a point in* $\boldsymbol{C}^n$ *which is a non singular solution of a system of equations* $S(x) = 0$, *and* $S = (P_1, \ldots, P_n)$ *with*

each P_i a polynomial with integral coefficients in $x_1, e^{x_1}, \ldots, x_n, e^{x_n}$. Such a number will be defined by:

$$\eta = q(\alpha), S(\alpha) = 0, \alpha \in B$$

where B is a ball in $\boldsymbol{C}^n$ which contains the point α and which does not contain any other solution of $S(x) = 0$. (The assumption that α is a non singular solution means that the Jacobian of S, evaluated at α is non zero.)

We will say that such a definition is in expanded form if B is the unit ball around the origin in $\boldsymbol{C}^n$. An example of elementary numbers is $\eta = \sqrt{\log 2}$. In this case we take the chain to be $e^{x_1} - 1, \ldots, e^{x_n} - 1$. We can rewrite the equations $S(x) = 0$ in terms of these functions. This does not change the degree but may change the height. Assume all the polynomials have degree $\leq d$ and the height of the system (after) rewriting is $H > 1$.

$$\gamma = (x_1, \ldots, x_n, \eta) \in \boldsymbol{C}^{n+1}$$

is a Pfaffian intersection and according to 6.4

$$K(\gamma) = 2^{(n+1)n/2}\, d^{n+1}\, (n + (n+1)d)^n$$

The conjecture 10 says that if $\eta \neq 0$ then

$$|\eta| > \max(H, 2)^{-C\,K h(\gamma)}.$$

In this case the result is new. We do know that if the Schanuel conjecture is true then zero testing for elementary numbers is decidable. Conjecture 10 is another conjecture which implies decidability of zero testing for elementary numbers. A. Tarski [Tar48] proved the decidability of the theory of the real ordered field. He asked if this could be extended to include the exponential function. Using model theoretic methods Wilkie and Macintyre [MW95] showed assuming Schanuel conjecture that the first order theory $\boldsymbol{R}_{\exp}$ of the reals with exponentiation is indeed decidable. Richardson [Ric97] obtained a similar result related to the work of Wilkie and Macintyre [MW95]: he

showed that the zero recognition problem for the elementary numbers can be solved provided that the Schanuel conjecture is true.

Essentially the Schanuel conjecture is used to solve the zero testing problem in this case. Conjecture 10 can also be used in this way to solve Tarski's problem. That is, conjecture 10 implies that the theory of $(\boldsymbol{R}, +, \times, \exp, 0, 1)$ *is decidable.*

Chapter 7

An Effective Proof Of Lindemann's Theorem

{*Verily, all things have We created in proportion and measure.*} *[54:49]*

In this chapter we study one of the important classical theorems in mathematics namely, Lindemann-Weierstrass theorem and show how such proof can be modified to be an effective one. By this we mean to replace the proofs that some constants exist by trying to find explicit values for them.
Beside the importance of having such a proof for its own sake, we introduce some computational application of the transcendental measure resulting from the new proof. It is aimed to use this measure to solve the zero recognition problem for polynomials. At the end we compare the result of this method with the conjectural approach discussed in the previous chapters to solve the zero recognition problem for polynomials using the syntactic length (or the height and depth) of the expressions representing them.
This theorem goes back to 1882 and it has been improved over long history of study by great mathematicians. It proves the transcendence of e, π *and numbers of the form* e^{α}, $\log \alpha$, *for algebraic* $\alpha \neq 0, 1$ *and also the trigonometric functions* $\cos \alpha$, $\sin \alpha$, *and* $\tan \alpha$ *for algebraic* $\alpha \neq 0$.
The classical proof we'll give here is a proof refined over decades by the work of Lindemannn, Weierstrass, Hermite, and other great mathematicians. In section 7.2 I will introduce one of the classical proofs.
Lastly I will explain in section 7.3 our logic behind transforming this classical

proof in section 7.2 into a new effective proof.
At the end I'll present the results of another effective version of Lindemann theorem based on determinants of interpolation. This was done by Alain Sert (see [Ser99]).

7.1 Number theoretic background

From the classical book of number theory [HW02] we have the following standard definitions where in this section p always denotes a prime number or represent a set of prime numbers.

$$\pi(x) := \textit{number of primes} \leq x \,,$$

$$R(x) := \prod_{p \leq x} p \,,$$

$$\theta(x) := \sum_{p \leq x} \log p = \log R(x) \,,$$

$$\omega(x) := \textit{number of prime factors of } x \sim \frac{\log x}{\log \log x}$$

The last estimate is from [HW02] p.354

Lemma 7.1.1 (Tchebychev's Theorem). *For any $x \geq 8$ we have*

$$\frac{\log 2}{4} \frac{x}{\log x} < \pi(x) < 30 \, (\log 2) \frac{x}{\log x}$$

For a proof one can refer to [HW02] and [And94] for concrete results. With respect to $\theta(x)$ we have

$$\theta(x) \leq \pi(x) \log x$$

and hence

$$\theta(x) \leq 30 \, (\log 2) \, x$$

In the other side also we have

$$\theta(x) \geq (\log 2) \pi(x)$$

and hence we have

$$\theta(x) \geq \frac{(\log 2)^2}{4} \frac{x}{\log x}$$

so the previous lemma can be put in the form

Lemma 7.1.2. *For any $x \geq 8$ we have*

$$\frac{(\log 2)^2}{4} \frac{x}{\log x} \leq \theta(x) < 30\,(\log 2)\,x$$

We can improve the left side if $x \geq 8$ to be

$$\frac{(\log 2)(\log 7)}{4} \frac{x}{\log x} \leq \theta(x)$$

An important question we have to answer through our proof of Lindemann theorem is how to find a small enough prime number $p \nmid x$.
We use the notation

$$f = o(\phi) \text{ to mean } \frac{f}{\phi} \to 0$$

so $\forall\, \delta > 0$ we have $\log x = o(x^\delta)$
since

$$\lim_{x \to \infty} \frac{\log x}{x^\delta} = 0$$

i.e., $\log x$ tends to ∞ more slowly than x^δ $\forall \delta > 0$
and hence
$\log(\log x)$ tends to ∞ more slowly than $(\log x)^\delta$ $\forall \delta > 0$
Now since $\sqrt{y} > \log y$ for large enough values of y so

$$\frac{y}{\log y} > \frac{y}{\sqrt{y}}$$

and hence if

$$\sqrt{y} = \frac{y}{\sqrt{y}} > \frac{4}{\log 2 \log 7} \log x$$

which means approximately that $y > 8.79\,(\log x)^2$, so if $y > (3 \log x)^2$, this guarantees

$$\frac{y}{\log y} > \frac{4}{\log 2 \log 7} \log x$$

which means

$$\theta(y) > \log x \text{ which means } \log R(y) > \log x$$

This simply says

$$R(y) > x \text{ which proves that } \exists \text{ a prime } p < (3\log x)^2 \text{ such that } p \nmid x$$

Since otherwise every prime less than or equal to y will be a factor of x and hence $R(y) \mid x$ therefore, $R(y) \leq x$ which contradicts what we got.
We can generalise this result to be

Lemma 7.1.3. *Given any $\delta > 0$ one can choose a prime number $p \nmid x$ such that*

$$p < [\frac{4}{\log 2 \log 7}]^{1+\delta} (\log x)^{1+\delta}$$

For example, $\delta = 0.01$ gives

$$[\frac{4}{\log 2 \log 7}]^{1+\delta} \simeq 2.998$$

and hence

$$p < 2.998 (\log x)^{1.01}.$$

Proof
The proof follows the same steps and uses the following

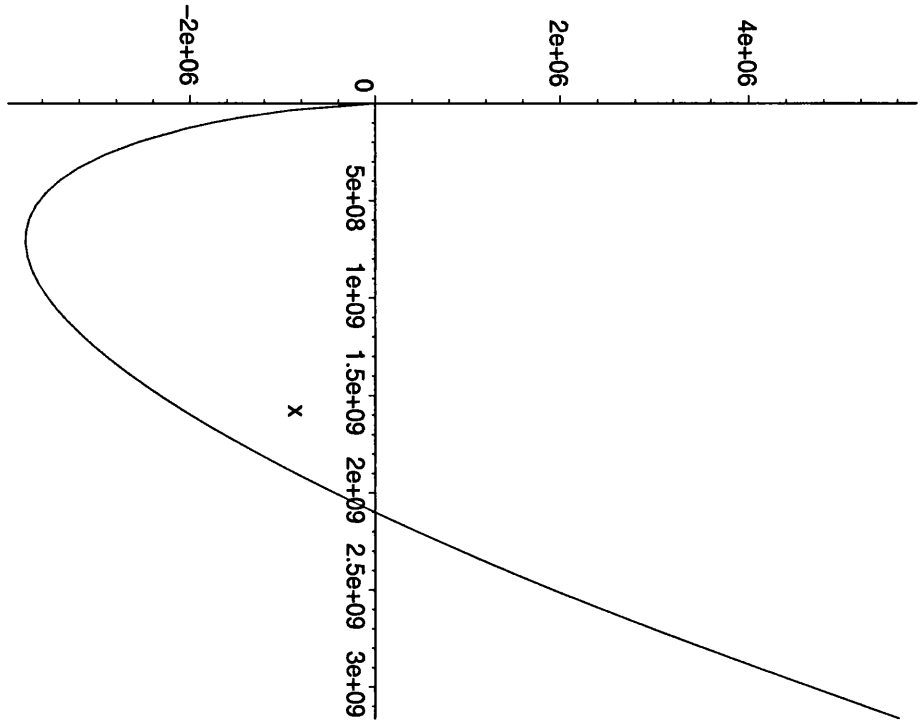
Lemma 7.1.4. *For enough large x we have*

$$\frac{x}{\log x} > x^{1-\delta} \text{ where } 1 > \delta > 0$$

This is clear and we can check it using any CAS (Computer Algebra System) like Maple e.g., we have for $\delta = 1/7$,

$$\frac{x}{\log x} > x^{6/7} \text{ for } x > 10^{10}$$

```
> plot(x/log(x)-x^(6/7),x=2..10^(9.5));
```


-2e+06
0
2e+06
4e+06
5e+08
1e+09
1.5e+09
2e+09
2.5e+09
3e+09
x

Corollary 7.1.1. *If* $x^{1-\delta} > K_1$ *for* $1 > \delta > 0$ *for all* x *or for all large enough* x *then*

$$\frac{x}{\log x} > K_1^{\frac{1}{1-\delta}}$$

To have an idea about how large x *should be I will use series expansion. For enough large* x *we have*

$$x^{\delta} > \log x$$

which is equivalent to

$$\frac{x}{\log x} > x^{1-\delta}$$

Substitute $y = \log x$ *we get*

$$e^{\delta y} > y$$

Using the series expansion of the exponential function around zero we get an approximation which guarantees the last equation if

$$1 + \delta y + (\delta y)^2/2 > y$$

which is guaranteed if

$$(\delta y)^2/2 > y \text{ or } y > \frac{2}{\delta^2}$$

So we have proved that

$$x > e^{\frac{2}{\delta^2}} \longrightarrow \frac{x}{\log x} > x^{1-\delta}$$

e.g., if $\delta = 1/2$ *then* $x > e^8$ *guarantees* $\frac{x}{\log x} > x^{1/2}$ *which is verified by Maple. So we can put the previous lemma in the form*

Lemma 7.1.5. *For enough large* x *satisfying*

$$x > e^{\frac{2}{\delta^2}}$$

we have

$$\frac{x}{\log x} > x^{1-\delta} \text{ where } 1 > \delta > 0$$

Lemma 7.1.6. *Let*

$$\kappa = \frac{8}{\log 2}(1 + 30 \log 2) \approx 251.5415604$$

then $\forall x > \kappa$ *we have*

$$\pi(\kappa x) - \pi(x) > \frac{x}{\log x}$$

Proof

By Techebychev's theorem (lemma 7.1.1) we have

$$\pi(\kappa x) - \pi(x) > \frac{x}{\log x}$$

$$\pi(\kappa x) - \pi(x) > \frac{\log 2}{4}\frac{\kappa x}{\log(\kappa x)} - 30 \log 2 \frac{x}{\log x}$$

If $x > \kappa$ *then* $2 \log x > \log(\kappa x)$ *and hence*

$$\pi(\kappa x) - \pi(x) > \frac{\log 2}{4}\frac{\kappa x}{2 \log x} - 30 \log 2 \frac{x}{\log x}$$

Choosing κ *as mentioned in the statement of the lemma we complete the proof.*

Lemma 7.1.7. *Suppose* $x > 8$ *and* $e^x > M$ *where* M *is a natural number. Then there is a prime* p *with* $x \leq p \leq \kappa x$ *so that* $p \nmid M$.

Proof

The number of primes in the interval $[x, \kappa x]$ *does not exceed* $\pi(\kappa x) - \pi(x)$ *and hence*

$$\prod_{x \leq p \leq \kappa x} p > x^{\pi(\kappa x) - \pi(x)}$$

and by the previous lemma (7.1.6) we have

$$\prod_{x \leq p \leq \kappa x} p > x^{\frac{x}{\log x}} = e^{\log x \frac{x}{\log x}} = e^x > M$$

So some prime p *in the interval* $[x, \kappa x]$ *does not divide* M *otherwise the product of such primes has to divide* M *and hence has to be* $\leq M$.

7.2 Classic Proof of the Lindemann theorem

Here we remind the reader with some basic definitions to be used

Definition 7.2.1 (integral basis). *Let* $K = \boldsymbol{Q}(\theta)$ *be an algebraic number field of degree* n. *By virtue of definition 6.1.2 and the remarks which follow we may*

assume θ to be an algebraic integer. By theorem 2.1.4 every element of K can be written uniquely in the form

$$\sum_{i=0}^{n-1} a_i \theta^i, \text{ where the } a_i \in \boldsymbol{Q}.$$

A set of algebraic integers $\alpha_1, \ldots, \alpha_s$ is called an integral basis of K if every integer α in K can be written uniquely in the form

$$\alpha = b_1\alpha_1 + \cdots + b_s\alpha_s,$$

where the b_i are rational integers.

Conjugates and discriminants

If α is algebraic over the field F then the conjugates of α over F are the roots of the minimal polynomial of α over F. Let $K = F(\theta)$ be a finite extension of degree n over F. (The degree of $\alpha \in K$ has to divide n according to field extension theorem). Moreover we know that α can be written uniquely in the form

$$\alpha = \sum_{i=0}^{n-1} c_i\, \theta^i = r(\theta) \text{ where } c_i \in F$$

Let $\theta_1, \ldots, \theta_n$ be the conjugates of θ over F. Then the numbers

$$\alpha_i = r(\theta_i), \quad i = 1, \ldots, n$$

are called the conjugates of α for $F(\theta)$. So α has n conjugates in the new sense, but m in the old, where $m|n$. It is important to notice that these new conjugates do not depend on θ but only on the field K.
Suppose $\alpha_1, \ldots, \alpha_n$ is a basis for $K = F(\theta)$ over F. Denote by $\alpha_j^{(i)}$, $i = 1, \ldots, n$ the conjugates of α_j for K. The discriminant of the set $\{\alpha_1, \ldots, \alpha_n\}$ is defined by

$$\Delta[\alpha_1, \ldots, \alpha_n] = \left|\alpha_j^{(i)}\right|^2,$$

where $\left|\alpha_j^{(i)}\right|$ *is the determinant*

$$\begin{vmatrix} \alpha_1^{(1)} & \alpha_2^{(1)} & \cdots & \alpha_n^{(1)} \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \alpha_1^{(n)} & \alpha_2^{(n)} & \cdots & \alpha_n^{(n)} \end{vmatrix}$$

It is worth mentioning the following facts about the integral bases

Theorem 7.2.1. *1. An integral basis is really a basis.*

2. Every algebraic number field has at least one integral basis.

3. All integral bases for a field $K = \boldsymbol{Q}(\theta)$ *have the same discriminant, we call it the discriminant of the field.*

The proof can be referred to in any standard book of algebraic number theory for example [Wey40], [Lan69], [Lan70], [LeV65], [Sam72], [PD98]. These references provide some good examples for integral bases in some fields of great importance in applications e.g.,

Examples 7.2.1. *1. An integral basis for* $\boldsymbol{Q}\sqrt{D}$ *is* $1, \sqrt{D}$ *if* $D \not\equiv 1 \,(mod\, 4)$ *and* $1, (1+\sqrt{D})/2$ *if* $D \equiv 1 \,(mod\, 4)$*.In the former case* $d = 4D$*, In the latter* $d = D$ *where* d *is the discriminant of the field*

2. An integral basis for the cyclotomic field $\boldsymbol{Q}(\xi)$ *where* ξ *is a primitive p-th root of unity for p an odd prime is* $1, \xi, \ldots, \xi^{p-2}$*. This field has discriminant* $(-1)^{(p-1)/2}\, p^{p-2}$ *.*

Definition 7.2.2 (Galois field). *If* $\alpha_1, \ldots, \alpha_n$ *are non zero algebraic integers satisfying*

$$b_0 + b_1\, e^{\alpha_1} + \cdots + b_n\, e^{\alpha_n} = 0$$

for some rational integers $b_0, b_1, \ldots, b_n$ *with* $b_0 \neq 0$ *. We call the field* $\boldsymbol{Q}(\alpha_1, \ldots, \alpha_n)$ *a Galois field if* $\alpha_1, \ldots, \alpha_n$ *can be written as complete sets of conjugates, and that, for each such set, say* $\alpha_{k_1}, \ldots, \alpha k_m$*, the corresponding* $b_{k_1}, \ldots, k_{\underline{m}}$ *are equal.*

Theorem 7.2.2 (Lindemann's Theorem: version 1). *If* $a_1, \ldots, a_k$ *are algebraic numbers linearly independent over* $\boldsymbol{Q}$*, then* $e^{a_1}, \ldots, e^{a_k}$ *are algebraically independent.*

As an example, $e^{1/\sqrt{p_1}}, e^{1/\sqrt{p_2}}, \ldots, e^{1/\sqrt{p_n}}$ *are algebraically independent, where* $p_1, \ldots, p_n$ *are the first n prime numbers or in general any different n square free numbers, details about the proof concerning this example are in section 4.2.*

Lindemann's theorem is referred through this thesis (in chapter 4) in the following classical equivalent form

Theorem 7.2.3 (Lindemann's Theorem: Version 2). *Whenever* $\alpha_1, \ldots, \alpha_n$ *are distinct algebraic numbers and* $\beta_1, \ldots, \beta_n$ *are non-zero algebraic numbers then*

$$\beta_1 e^{\alpha_1} + \cdots + \beta_n e^{\alpha_n} \neq 0 \tag{7.1}$$

Proof of equivalence

We note that if $\alpha_1, \ldots, \alpha_n$ *are distinct algebraic numbers and* $\omega_1, \ldots, \omega_d$ *is an integral basis for* $\boldsymbol{Q}(\alpha_1, \ldots, \alpha_n)$ *then for some positive integer l, each* α_j *is expressible as a linear combination of* $\omega_1/l, \ldots, \omega_d/l$ *with integer coefficients [PD98]. Assume negation of 7.2.3 is right and let* $\alpha_1, \ldots, \alpha_n$ *be algebraic numbers linearly independent over* $\boldsymbol{Q}$ *and let* $\beta_1, \ldots, \beta_n$ *be non-zero algebraic numbers or that*

$$\beta_1 e^{\alpha_1} + \cdots + \beta_n e^{\alpha_n} = 0 \tag{7.2}$$

Applying the fact mentioned above about integral basis we get

$$\beta_1' e^{\alpha_1} + \cdots + \beta_n' e^{\alpha_n} = 0 \tag{7.3}$$

and hence $e^{\alpha_1}, \ldots, e^{\alpha_n}$ *are algebraic dependent which contradicts 7.2.2.*
To obtain the converse we note that for any polynomial $P(x_1, \ldots, x_n)$ *not identically 0,*

$$P(e^{\alpha_1}, \ldots, e^{\alpha_n}) = 0 \Rightarrow \beta_1 e^{\alpha_1'} + \cdots + \beta_m e^{\alpha_m'} = 0$$

with algebraic $\alpha_1', \ldots, \alpha_m'$ *which are different linear combinations of* $\alpha_1, \ldots, \alpha_n$ *with integer coefficients and with* $\beta_1, \ldots, \beta_m$ *not all zero. So we have the denial of 7.2.3 which completes the proof.*

I will break the proof into the following lemmas. Assume to begin that some polynomial p is not identically zero, it has integral coefficients and we have

$$p(e^{a_1}, \ldots, e^{a_k}) = 0$$

although $a_1, \ldots, a_k$ are algebraic and linearly independent over $\boldsymbol{Q}$. Starting from this point we will eventually arrive at a contradiction. The first step is to write the equation in the form:

$$\beta_1 e^{\alpha_1} + \cdots + \beta_n e^{\alpha_n} = 0. \tag{7.4}$$

The number n here is the number of monomials in p. The numbers $\alpha_1, \ldots, \alpha_n$ are distinct algebraic numbers, obtained by integral linear combinations of $a_1, \ldots, a_k$. An upper bound on n is $(d+1)^k$, where d is the total degree of p. We will actually prove that equation (7.4) is impossible for any non zero algebraic $\beta_1, \ldots, \beta_k$.

Lemma 7.2.1. *[Galois Assumption] Suppose we can satisfy equation (7.4) for some $n > 0$ with non zero algebraic numbers $\beta_1, \ldots, \beta_n$ and distinct algebraic numbers $\alpha_1, \ldots, \alpha_n$. Then we can satisfy equation (7.4) for some $N \geq n$ with $\beta_1, \ldots, \beta_N$ rational integers and so that there exist integers $0 = n_0 < n_1 < \cdots < n_r = n$ and $\alpha_{n_t+1}, \ldots, \alpha_{n_{t+1}}$ is a complete set of conjugates and $\beta_{n_t+1} = \cdots = \beta_{n_{t+1}}$ for all t .*

Proof

Multiplying (7.4) by all the expressions obtained on allowing $\beta_1, \ldots, \beta_n$ on the left to run independently through their respective conjugates. Using the properties of symmetric polynomials or sums of products of roots of polynomials, see for example ([Zip93], Ch.9, p.138) and other references mentioned there), we get a similar equation with rational coefficients. We can now multiply by a common denominator to be sure that we have rational integers.

To prove the second part, assume that $\alpha_1, \ldots, \alpha_n$ are all in some number field F. Let $\sigma_1, \ldots, \sigma_k$ list all the conjugate maps or to say mono morphisms : $F \to \boldsymbol{C}$ i.e., (injective homomorphisms) and k is the degree of F. Now form

$$\prod (\beta_1 e^{\sigma(\alpha_1)} + \cdots + \beta_n e^{\sigma(\alpha_n)}) = 0,$$

where the product is taken over all σ in $(\sigma_1, \ldots, \sigma_k)$. The degree of the new polynomial is increased by a factor of k.

More Notations for the proof:

Let A be the maximum of $|\alpha_i|$ and let B be the maximum of $|\beta_i|$ for $i = 1, \ldots, n$. Also let l be any positive integer such that $l\alpha_1, \ldots, l\alpha_n$ and $l\beta_1, \ldots, l\beta_n$ are alge-

braic integers i.e., the leading coefficient in each defining minimal polynomial is one. Let $\mathcal{D}_F$ be the algebraic integers of F, where $F = \boldsymbol{Q}(\alpha_1, \ldots, \alpha_n)$.
We are going to introduce the following set of polynomials

$$f_i(x) = l^{np}\left[(x-\alpha_1)\cdots(x-\alpha_n)\right]^p/(x-\alpha_i)\ ;1 \le i \le n, \tag{7.5}$$

where p is a large prime. The property of $f_i(x)$ which we will use is that for each i and each α_j, $f_i(x)$ has a zero of high multiplicity at α_j where $j \neq i$.
We also need to introduce the following set of integrals

$$I_i(t) := \int_0^t e^{t-u} f_i(u)\mathrm{d}u\ \ ;1 \le i \le n. \tag{7.6}$$

We mean here line integration over the line segment between $0, t$ where t is any complex number.
Lastly, we introduce the quantities $J_1, \ldots, J_n$ defined by

$$J_i = \beta_1 I_i(\alpha_1) + \cdots + \beta_n I_i(\alpha_n)\ \ ;1 \le i \le n \tag{7.7}$$

Lemma 7.2.2 (does not assume (7.4)). *The complex line integrals defined by (7.6) can be put into the form*

$$I_i(t) = e^t \sum_{j=0}^{m} f_i^{(j)}(0) - \sum_{j=0}^{m} f_i^{(j)}(t)$$

where $f_i^{(j)}(x)$ means, as usual, the j-th derivative and $m = np-1$ is the degree of each of the polynomials $f_i(x)$.

Proof
We prove the lemma for $I(t) = \int_0^t e^{t-u} f(u)\,\mathrm{d}u$ where $f(u)$ is any polynomial of degree m and not necessarily the polynomials $f_i(x)$. Applying the rule of integration by parts we easily get the required result.

Lemma 7.2.3 (assuming (7.4)). *The quantities $J_1, \ldots, J_n$ defined by (7.7) can be put into the form*

$$J_i = -\sum_{j=0}^{m}\sum_{k=1}^{n} \beta_k f_i^{(j)}(\alpha_k).$$

Proof

By definition and using lemma 7.2.2 we have

$$\begin{aligned} J_i &= \sum_{k=1}^{n} \beta_k \, I_k(\alpha_k) \\ &= \sum_{k=1}^{n} \beta_k \left[e^{\alpha_k} \sum_{j=0}^{m} f_i^{(j)}(0) - \sum_{j=0}^{m} f_i^{(j)}(\alpha_k) \right] \\ &= \sum_{j=0}^{m} f_i^{(j)}(0) \sum_{k=1}^{n} \beta_k \, e^{\alpha_k} - \sum_{j=0}^{m} \sum_{k=1}^{n} \beta_k \, f_i^{(j)}(\alpha_k) \end{aligned}$$

Now using the main assumption $\sum_{k=1}^{n} \beta_k \, e^{\alpha_k} = 0$ *we get*

$$J_i = -\sum_{j=0}^{m} \sum_{k=1}^{n} \beta_k \, f_i^{(j)}(\alpha_k).$$

Lemma 7.2.4 (assuming (7.4)). *We can find a natural number* M *so that if* $p \nmid M$ *then* J_i *is a non zero algebraic integer divisible by* $(p-1)!$, *where we mean divisibility in the ring of algebraic integers* $\mathcal{D}_F$ *of* F.

Proof

$$f_i(x) = l^{np} \left[(x - \alpha_1) \cdots (x - \alpha_n) \right]^p / (x - \alpha_i) \; ; 1 \leq i \leq n.$$

Direct differentiation using the n-th derivative formula shows that

$$f_i^{(t)}(\alpha_j) = 0 \quad \textit{where} \quad t < p - 1.$$

We deal with the case $t = p-1$ *in some detail*

$$\begin{aligned} f_1^{(p-1)}(x) &= l^{np}\left[D^{p-1}(x-\alpha_1)^{p-1}\, D^0\left[(x-\alpha_2)\cdots(x-\alpha_n)\right]^p + \right. \\ &\quad +(p-1)\, D^{p-2}(x-\alpha_1)^{p-1}\, D^1\left[(x-\alpha_2)\cdots(x-\alpha_n)\right]^p + \\ &\quad \vdots \\ &\quad \left. +D^0(x-\alpha_1)^{p-1}\, D^{p-1}\left[(x-\alpha_2)\cdots(x-\alpha_n)\right]^p \right. \\ &= l^{np}\left[(p-1)!\ \left[(x-\alpha_2)\cdots(x-\alpha_n)\right]^p + \right. \\ &\quad \left. +(p-1)(p-1)!(x-\alpha_1)\, p\sum_{i=2}^{n}\prod_{\substack{j=1\\ j\neq i}}^{n}(x-\alpha_j)+\cdots \right] \end{aligned}$$

Therefore we have

$$\begin{aligned} f_1^{(p-1)}(\alpha_1) &= l^{np}\,(p-1)!\prod_{j=2}^{n}(\alpha_1-\alpha_j)^p \text{ and} \\ f_1^{(p-1)}(\alpha_j) &= 0 \quad \text{if} \quad j\neq 1, \end{aligned}$$

and in general we have

$$\begin{aligned} f_i^{(p-1)}(\alpha_j) &= l^{np}\,(p-1)!\prod_{\substack{k=1\\ k\neq i}}^{n}(\alpha_i-\alpha_k)^p \quad \text{if} \quad j=i, \\ f_i^{(p-1)}(\alpha_j) &= 0 \quad \text{if} \quad j\neq i. \end{aligned}$$

In the other cases, $f_i^{(j)}(\alpha_k)$ *is divisible by* $p!$ *for all* $j \neq p-1$ *or* $k \neq i$. *In the case when* $j = p-1$, $k = i$, *we have* $f_i^{(p-1)}(\alpha_i)$ *is divisible by* $(p-1)!$ *but not* $p!$ *if we choose* p *outside of a finite set of bad primes. This can be seen as follows. Let*

$$G := \prod_{i\neq j}(\alpha_i-\alpha_j).$$

and suppose also that we have the Galois assumption. Then G *is invariant under conjugation, and is therefore a rational number. So the quantity* $l^{n^2}G$ *is an integer. If* p *does not divide this integer, then* $p!$ *does not divide* $f_i^{p-1}(\alpha_i)$.

Substituting these values of derivatives into J_i we get (mod(p!)) the following

$$\begin{aligned} J_i &= -\sum_{j=0}^{m}\sum_{t=1}^{n} \beta_t \, f_i^{(j)}(\alpha_j). \\ &= -\beta_i \, f_i^{(p-1)}(\alpha_i) \\ &= -\beta_i \, l^{np} \, (p-1)! \prod_{\substack{k=1 \\ k\neq i}}^{n} (\alpha_i - \alpha_k)^p \\ &= (p-1)! \, q_i \quad , \end{aligned}$$

where the quotient q_i is an algebraic integer since

$$q_i = -\, \beta_i \, l^{np} \prod_{k\neq i} (\alpha_i - \alpha_k)^p,$$

is a result of sums and products of algebraic integers. Provided that p does not divide any of the coefficients $\beta_1, \ldots, \beta_n$ and does not divide G too this means that $p \not| J_i$ in $\mathcal{D}_F$. We say that a prime is bad if it divides some J_i in $\mathcal{D}_F$. We let M be the product of the bad primes. We can compute M as the square free part of

$$l \, \beta_1 \cdots \beta_n \prod_{i\neq j} (\alpha_i - \alpha_j)$$

so we have the following bound on M

$$|M| \leq l \, B^n \, (2A)^{n^2}$$

The Galois assumption was only used at this point. Even without the Galois assumption we can still get the result by replacing J_i by $N_F(J_i)$ and M by $N_F(M)$ where N_F is the norm in the field F.

Lemma 7.2.5 (Assuming 7.4). *The product $J_1 \cdots J_n$ is a rational non zero integer divisible by $[(p-1)!]^n$ if $p \not| M$.*

Proof

$\boldsymbol{Q}(\alpha_1, \ldots, \alpha_n)$ is a Galois field. Conjugation, or any automorphism, will permute $\alpha_1, \ldots, \alpha_n$ and hence $\prod J_i$ is a symmetric function in $\alpha_1, \ldots, \alpha_n$. $\prod J_i$ is an invariant under conjugation and hence a rational number since the only invariant

numbers in $\boldsymbol{Q}(\alpha_1, \ldots, \alpha_n)$ *are the rationals. Therefore* $\prod J_i$ *is an integer and by the result of lemma 4 we get* $\prod J_i$ *is divisible by* $[(p-1)!]^n$. *Hence* $|\prod J_i| \geq [(p-1)!]^n$.

Lemma 7.2.6 (does not assume (7.4)). *Assuming the same notations we have*

$$|J_i| \leq nABe^A(2lA)^{np}$$

Proof

1. *We denote by* $\bar{f}_i(x)$ *the polynomials obtained from* $f_i(x)$ *by replacing each coefficient with its absolute value. An over estimate for* $\bar{f}_i(x)$ *is*

$$l^{np}\left[(x+|\alpha_1|)\cdots(x+|\alpha_n|)\right]^p/(x+|\alpha_i|).$$

   This gives

$$\left|\bar{f}_i(x)\right| \leq l^{np}\,(2A)^{np-1},$$

   where $A = max\{\alpha_j\,; j = 1, \ldots, n\}$ *and* $x \in [-k, k] \subset [-A, A]$

2. *Now we can bound the integrals* $I_i(t)$ *as follows:*

$$|I_i(t)| \leq \int_0^t \left|e^{t-u} f_i(u)\right| du \leq |t|e^{|t|}\left|\bar{f}_i\,|t|\right| \leq |t|e^{|t|}l^{np}\,(2A)^{np-1},$$

3. *Applying these upper bounds to* $I_i(\alpha_j)$ *we conclude:*

$$|J_i| = \left|\sum_{j=1}^{n} \beta_j\, I_i(\alpha_j)\right| \leq \sum_{j=1}^{n} |\beta_j|\,|\alpha_j|\,e^{|\alpha_j|}\,\bar{f}_i\,(|\alpha_j|),$$

   and therefore we have

$$|J_i| \leq nABe^A(2lA)^{np}$$

Note that the form of this bound is $C_1C_2^p$, *where* C_1 *and* C_2 *are independent of* p. *It can also be put in the form* C^p *for some constant* C *independent of* p *as we 'll see in the following*

Lemma 7.2.7 (does not assume (7.4)). *Assuming the same notations , we can use the constant*

$$C = (2lA)^n \log B$$

to have

$$|J_i| \leq C^p \text{ for every } i \text{ and where } p > C$$

Proof

We need to show that

$$C^p \geq nABe^A(2lA)^{np}$$

i.e.,

$$(\log B)^p \geq nABe^A$$

If the condition $p > C$ is satisfied then it would be enough to have

$$(\log B)^{(2lA)^n \log B} \geq nABe^A$$

which is true and clear if we take the logarithms of both sides

$$(2lA)^n \log B \log\log B \geq \log n + \log A + \log B + A$$

Then the result.

$$C = (2lA)^n \log\log B \text{ and } p > C$$

also works for the same reasons.

7.2.1 The classical proof

We now give another version of the classical proof in [Bak75] using the previous lemmas. Let $\alpha_1, \ldots, \alpha_n$ be distinct algebraic numbers and $\beta_1, \ldots, \beta_n$ be non zero algebraic numbers. We need to show that $\beta_1 e^{\alpha_1} + \cdots + \beta_n e^{\alpha_n} \neq 0$. Assume not, that is,

$$\beta_1 e^{\alpha_1} + \cdots + \beta_n e^{\alpha_n} = 0$$

Without any loss of generality, by the Galois assumption proved in lemma 7.2.1, one can assume that $\beta_1, \ldots, \beta_n$ are rational integers and there exist integers

$$0 = n_0 < n_1 < \cdots < n_r = n$$

such that $\alpha_{n_t+1}, \ldots, \alpha_{n_{t+1}}$ is a complete set of conjugates for $t = 0, 1, \ldots, r-1$ and $\beta_{n_t+1} = \cdots = \beta_{n_{t+1}}$.

By lemma 7.2.5, we have that $\prod J_i$ *is a rational integer divisible by* $((p-1)!)^n$. *Hence we have*

$$\left| \prod_{i=1}^{n} J_i \right| \geq ((p-1)!)^n$$

But from lemma 7.2.7, also we have $|J_i| \leq C^p$, *where the constant* $C = (2lA)^n \log B$ *is independent of* p. *The inequalities yield*

$$(p-1)! \leq C^p$$

which is wrong if p *is chosen sufficiently large according to the following lemma.*

Lemma 7.2.8.

$$\textit{If } p > 5C \textit{ then } (p-1)! > 2C^p$$

We can give a choice for such p *using Stirling formula*

$$\log M! \sim M \log M - M$$

or

$$M! \geq \sqrt{2\pi M}\,(M/e)^M$$

Applying this fact to $(p-1)!$ *we get that* $p > 5C$ *will prove the lemma.*

$$(p-1)! \geq \sqrt{2\pi(p-1)}\,\left[\frac{p-1}{e}\right]^{p-1}$$

If we suppose

$$(p-1)! \leq 2C^p$$

then

$$2C^p \geq \sqrt{2\pi(p-1)}\,\left[\frac{p-1}{e}\right]^{p-1}$$

and if

$$\frac{p-1}{e} > \frac{3}{2}C \quad \textit{which is satisfied if } p > 5C$$

and then

$$\left(\frac{3}{2}C\right)^{p-1} \sqrt{p-1} < C^p$$

so

$$\left(\frac{3}{2}\right)^{p-1} < C$$

which is a contradiction if $p > C$, $C > 2$. *This completes the proof.*

7.3 Effective Proof Of Lindemann theorem

The logic behind the modification of the previous proof to be effective is contained in the following

Lemma 7.3.1. *Suppose* $\beta_1 e^{\alpha_1} + \cdots + \beta_n e^{\alpha_n} = \varepsilon$ *where* $\beta_1, \ldots, \beta_n \in \boldsymbol{Z}$. *If there are functions*

$$J_i(R);\ \mu_i(R)\,;\, J_i^0(R) \quad ; 1 \le i \le n$$

computable in $R = (p, n, \beta_1, \ldots, \beta_n, \alpha_1, \ldots, \alpha_n)$ *and satisfying*
(a) $J_i = \varepsilon\,\mu_i + J_i^0$,
(b) $|J_i| \le C^p$ *for some constant* C *independent of* p *and*
(c) $|\prod_{i=1}^n J_i^0| \ge [(p-1)!]^n$
provided that p *is prime and does not divide some integer* M *which is computable in* $n, \beta_1, \ldots, \beta_n, \alpha_1, \ldots, \alpha_n$ *and* M *is independent of* p
Then we can effectively find a prime number p *such that*

$$|\varepsilon| > \left|\frac{C^p}{\mu_i(p)}\right| \quad \textit{for some } i$$

Proof

In the original proof we have $\varepsilon = 0$ *and then (b) and (c) are contradictory if* p *is chosen sufficiently large.*
Now if

$$|\varepsilon\,\mu_i| \le C^p \ \forall\, i$$

then using (b) we get

$$\left|J_i^0\right| \le 2\,C^p \ \forall\, i,$$

and hence using (c) we get

$$[(p-1)!]^n \le \left|\prod_{i=1}^n J_i^0\right| < 2^n\, C^{np}$$

Then, $(p-1)! < 2C^p$ *which yields a contradiction for large* p *e.g.,* $p \geq 5C$ *Therefore, if we take* p *to be a prime larger than* $5C$ *and not dividing* M *we get*

$$|\varepsilon\,\mu_i| > C^p \text{ for some } i$$

which completes the proof.

Remark 7.3.1. *The lemma does not depend on the Galois assumption, or even on* $\alpha_1, \ldots, \alpha_n$ *being algebraic. However these assumptions will be used in the proof of the premises of the lemma.*

We now give the details of the proof of the premises following the same notation in section (7.2). Assume

$$\beta_1 e^{\alpha_1} + \cdots + \beta_n e^{\alpha_n} = \varepsilon\ ;\ \beta_1, \ldots, \beta_n \in \boldsymbol{Z} \tag{7.8}$$

Then for $i = 1, \ldots, n$ *we have*

$$J_i = \varepsilon \sum_{j=0}^{m} f_i^{(j)}(0) - \sum_{j=0}^{m}\sum_{k=1}^{n} \beta_k\, f_i^{(j)}(\alpha_k) \tag{7.9}$$

Defining

$$\mu_i = \sum_{j=0}^{m} f_i^{(j)}(0) \text{ and } J_i^0 = -\sum_{j=0}^{m}\sum_{k=1}^{n} \beta_k\, f_i^{(j)}(\alpha_k),$$

where $m = np - 1$, *we can rewrite equation 7.9 in the form*

$$J_i = \varepsilon\,\mu_i + J_i^0 \quad ; 1 \leq i \leq n \tag{7.10}$$

As before let A *and* B *be upper bounds for the absolute values of* α*'s and* β*'s respectively.*
Define $H(f_i^j(x))$ *to be the maximum of the absolute values of the coefficients of this polynomial* f_i^j. *We have* $\left|f_i^j(0)\right| \leq H(f_i^j(x))$. *Also*

$$H(f_i^j(x)) \leq m!\, H(f_i(x)) \leq 2^m A^m m!$$

Therefore,

$$\left|f_i^j(0)\right| \leq (2A)^m m!$$

Hence we have

Lemma 7.3.2.

$$|\mu_i| \leq (m+1)!\,(2A)^m \tag{7.11}$$

Combining this result with lemma (7.3.1) we conclude

Lemma 7.3.3. *Suppose $\alpha_1, \ldots, \alpha_n$ are algebraic and the Galois assumption is true then*

$$\left|\prod_{i=1}^{n} J_i^0\right| \geq [(p-1)!]^n$$

provided that $p \nmid M = l\,\beta_1 \cdots \beta_n\, G$ where G is the same invariant quantity defined before.

Proof

Same as lemmas 7.2.4 and 7.2.5.
Now choose C, independent of p, so that $C^p \geq nABe^A(2Al)^{np}$.For example $C = (2lA)^n \log B$ as seen in lemma 7.2.7

Theorem 7.3.1 (Effective Lindemann Theorem).

$$\textit{If} \quad \beta_1 e^{\alpha_1} + \cdots + \beta_n e^{\alpha_n} = \varepsilon \quad \textit{where} \quad \beta_1, \ldots, \beta_n \in \boldsymbol{Z},$$

then there is some choice of

$$p \leq 5\,\kappa\,(2lA)^n \log B$$

such that

$$|\varepsilon| \geq \frac{1}{(np)!}$$

Proof

$$|\varepsilon| \geq \left|\frac{C^p}{\mu_i}\right| \geq \frac{[(2lA)^n \log B]^p}{(2A)^m m!}$$

but $[(2lA)^n \log B]^p > (2A)^m$ *and so*

$$|\varepsilon| > \frac{(2A)^m}{(2A)^m m!}$$

Hence we have

$$|\varepsilon| > \frac{1}{(np)!}$$

To choose p we need

$$\textit{first,} \quad p > 5C \quad \textit{where} \quad C = (2lA)^n \log B$$

$$\textit{second,} \quad p \nmid M = l\beta_1 \cdots \beta_n \prod_{i \neq j} (\alpha_i - \alpha_j)$$

so we have

$$M \leq lB^n (2A)^{n^2} < e^{5C}$$

and hence we can choose p so that $5C < p < 5\kappa C$ *according to lemma (7.1.7) where* κ *as stated in lemma (7.1.6).*

Remark 7.3.2.

$$5\,(2lA)^n \log B \leq p \leq 5\,\kappa\,(2lA)^n \log B$$

and therefore

$$|\varepsilon| \geq \frac{1}{[5\,\kappa\,n\,(2lA)^n \log B]!}$$

Taking the natural logarithms we get

$$0 > \log|\varepsilon| \geq \log \frac{1}{[5\,\kappa\,n\,(2lA)^n \log B]!} = -\log [5\,\kappa\,n\,(2lA)^n \log B]!$$

Applying the Stirling formula and taking the absolute values of the negative numbers in the last inequality yield

$$|\log|\varepsilon|| \leq 5\,\kappa\,n\,(2lA)^n \log B\ |\log [5\,\kappa\,n\,(2lA)^n \log B] - 1|\,.$$

Now I will show the original estimates we had with direct computations. The bounds are worse than the ones given before.

Another proof *From the argument of the classical proof we know that* $f_i^{(j)}(\alpha_t)$ *is an algebraic integer divisible by* $p!$ *unless* $j = p-1$, $t = i$ *and in this case we*

have

$$f_i^{(p-1)}(\alpha_i) \;=\; (p-1)!\, l^{np} \prod_{k=1}^{n} (\alpha_i - \alpha_k),$$

so that it is an algebraic integer divisible by $(p-1)!$ *but not by* $p!$ *if* $p \nmid M$. *To get an upper bound for the product* $J_1 \cdots J_n$

$$\begin{aligned}
\textit{we have} \qquad J_i^0 \;&=\; -\sum_{j=0}^{m}\sum_{k=1}^{n} \beta_k\, f_i^{(j)}(\alpha_k) \\
\Rightarrow |J_i^0| \;&\leq\; l^{np}\,(p-1)!\prod_{k=1}^{n} |\alpha_i - \alpha_k|^p \; m\, n\, max\{\beta_k\} \\
\Rightarrow |J_i^0| \;&\leq\; l^{np}\,(p-1)!\,(2k)^{np}\, m\, n\, k. \\
\Rightarrow |J_i^0| \;&\leq\; 2^{np}\, l^{np}\,(p-1)!\, k^{np+1}\, n^2\, p. \\
\Rightarrow |J_i^0| \;&\leq\; p!\, n^2\, 2^{np}\, l^{np}\, k^{np+1} \quad ; 1 \leq i \leq n. \qquad (7.12)
\end{aligned}$$

$$\textit{Therefore,} \qquad \prod_{i=1}^{n} J_i^0 \;\leq\; \left(p!\, n^2\, 2^{np}\, l^{np}\, k^{np+1}\right)^n \; ; 1 \leq i \leq n\,. \qquad (7.13)$$

$$\begin{aligned}
\textit{We get} \quad |J_1 \cdots J_n| \;&=\; \prod_{i=1}^{n} |J_i^0 + \varepsilon\, \mu_i| \\
&\leq\; \prod_{i=1}^{n} |J_i^0| + |\varepsilon|\, |\mu_i| \left(\prod_{i=1}^{n-1} |J_i^0|\right) + \cdots + |\varepsilon|^n \prod_{i=1}^{n} |\mu_i|\,.
\end{aligned}$$

So we can make the following bound using $|\varepsilon| < 1$ *since otherwise we have nothing to prove.*

$$\left| \prod_{i=1}^{n} |J_i| - \prod_{i=1}^{n} |J_i^0| \right| \;\leq\; |\varepsilon|\, 2^n \prod_{i=1}^{n} max\left(|J_i^0|\,, |\mu_i|\right), \quad \textit{and hence}$$

$$\left| \prod_{i=1}^{n} |J_i| - \prod_{i=1}^{n} |J_i^0| \right| \;\leq\; |\varepsilon|\, 2^n \prod_{i=1}^{n} \left[(p+1)\, p!\, 2^{np}\, l^{np}\, n^{n+1}\, k^{n^2p^2}\right].$$

Using the bounds given for μ_i *and* $|J_i^0|$ *, one gets*

$$\left| \prod_{i=1}^{n} |J_i| - \prod_{i=1}^{n} |J_i^0| \right| \;\leq\; |\varepsilon|\, 2^n \left[(p+1)!\, 2^{np}\, l^{np}\, n^{n+1}\, k^{n^2p^2}\right]^n. \qquad (7.14)$$

Define the term $T(\varepsilon) := |\varepsilon|\ 2^n \left[(p+1)!\ 2^{np}\ l^{np}\ n^{n+1}\ k^{n^2p^2}\right]^n$. (7.15)

If we assume $T(\varepsilon) \leq C^{np}$ *we get*

$$\left| \prod_{i=1}^{n} |J_i| - \prod_{i=1}^{n} |J_i^0| \right| \leq C^{np} \tag{7.16}$$

Using the fact that $|J_i| \leq C^p\ \forall i$ *gives* $\prod_{i=1}^n |J_i| \leq C^{np}$. *We conclude that* $\prod_{i=1}^n |J_i^0| \leq 2\ C^{np}$, *which contradicts the inequality* $\prod_{i=1}^n |J_i^0| \geq (p-1)!$ *(deduced from the divisibility argument above), for a suitable choice of p. For example* $(2C)^n < p < 2(2C)^n$. *Our result, due to this contradiction, is that* $T(\varepsilon) > C^{np}$. *i.e.,*

$$|\varepsilon|\ 2^n \left[(p+1)!\ 2^{np}\ l^{np}\ n^{n+1}\ k^{n^2p^2}\right]^n > C^{np}\ ,$$

and hence we have

$$|\varepsilon| > \frac{C^{np}}{2^n\ [(p+1)!\ 2^{np}\ l^{np}\ n^{n+1}\ k^{n^2p^2}]^n} \tag{7.17}$$

which explicitly gives a transcendence measure, lower bound, for the expression $\beta_1 e^{\alpha_1} + \cdots + \beta_n e^{\alpha_n}$. *The importance of such results is that it can give us a bound on the number of decimal places required to verify that a polynomial vanishes.*

7.4 Discussion

Here, we use the Lindemann theorem 7.3.1 to recognise the zero polynomials represented as expression trees. If $P(x_1, \ldots, x_n) = \sum_{i=0} c_i x_1^{k_{i_1}} \ldots x_n^{k_{i_n}}$ *is a polynomial with degree bound d in each variable, we can substitute* $x_i = e^{r_i}, \ldots, e^{r_n}$ *for* $x_1, \ldots, x_n$ *with* $r_1, \ldots, r_n \in \boldsymbol{Q}$ *to get*

$$P(e^{r_1}, \ldots, e^{r_n}) = \sum_{i=0} c_i\ e^{\sum_{j=1}^n k_{i_j} r_j}.$$

To apply the Lindemann theorem, the question is: what is the condition on the rationals (or how to find) $r_1, \ldots, r_n$ *to have different exponents?*

Some answer to this question is the following

Lemma 7.4.1. *Let* $n_1, \ldots, n_k \in \boldsymbol{Z}$ *and* $|n_i| \leq d$. *The following rationals*

$$r_1 = \frac{1}{(d+1)^{k-1}}, r_2 = \frac{1}{(d+1)^{k-2}}, \ldots, 1 \text{ satisfy}$$

$$r_1 n_1 + r_2 n_2 + \cdots + r_k n_k \neq 0 \tag{7.18}$$

unless all of the n_i *are zeros.*

Proof

We show how to find some integers $M_1, \ldots, M_k$ *satisfying*

$$M_1 n_1 + M_2 n_2 + \cdots + M_k n_k \neq 0 \tag{7.19}$$

Unless all of the n_i *or some* n_i *has* $n_i > d$. *Therefore, it will be clear how we have got these, required, rationals. Any choices for* $M_i \in \boldsymbol{Z}^+ where M_2 > dM_1, M_3 > d(M_1 + M_2), \ldots, M_k > d(M_1 + \cdots + M_{k-1})$. *will work. As a concrete choice for a solution of these inequalities, we take*

$$M_1 = 1, M_2 = dM_1 + 1, M_3 = d(M_1 + M_2) + 1, \ldots, M_k = d(M_1 + \cdots + M_{k-1}) + 1.$$

This means $M_1 = 1$, $M_2 = d+1$, $M_3 = (d+1)^2$, ..., $M_k = (d+1)^{k-1}$.

It is clearly evident that these quantities satisfy equation (7.19) because otherwise we get $1.n_1 + (d+1)n_2 + \cdots + (d+1)^{k-1} n_k = 0$. *Then we have,*
$n_1 = -(d+1)[n_2 + \cdots + (d+1)^{k-2} n_k]$ *which yields the contradiction*
$|n_1| \geq (d+1)$; $k \geq 2$ *This completes the proof of this lemma by taking the rationals*

$$r_1 = M_1/M_k, r_2 = M_2/M_k, \ldots, r_k = M_k/M_k.$$

Remark 7.4.1. *In fact, we can use the integers* M_i *included in the proof since they give rise to different exponents and hence we can apply Lindemann theorem in the last version but this requires higher precision than what the UC in its new form requires.*

Now we try to answer the question: what is the precision needed to distinguish, verify, a non zero polynomial $P(x_1, \ldots, x_n)$ *using the* ϵ *bound in bound we get in the proof of Lindemann theorem and the bound we have assuming the the new form of the Uniformity Conjecture. First, we introduce the following lemma*

which can be easily verified by induction on the number of interior nodes of trees, polynomial terms or expressions representing polynomials.

Lemma 7.4.2. *Let $T = T(x_1, \ldots, x_n)$ be a polynomial term having $s(T)$ interior nodes and logarithmic height $h(T)$, the maximum of lengths of the natural numbers on the frontiers. If T represents the polynomial*

$$P = \sum_{i=1}^{M} c_i x_1^{i_1} \cdots x_n^{i_n}, \text{ then we have}$$

1. $c_i \leq 10^{h(T)s(T)}$; $i = 1, \ldots, M$
2. *total degree* $:= \max_{i=1,\ldots,M} \sum_{j=1}^{n} i_j \leq s(T) + 1$
3. $M \leq (s(T) + 2)^n$

The proof is by direct induction on the number of interior nodes. For the number of monomials M we have n choices for each variable varying over $0, 1, \ldots, s(T)+1$.

We conclude this discussion by comparing conjecture 8 with theorem 7.3.1.

Suppose a polynomial $P(x_1, \ldots, x_n) = \sum_{i=0}^{M} c_i x_1^{k_{i_1}} \ldots x_n^{k_{i_n}}$ in $\boldsymbol{Z}[x_1, \ldots, x_n]$ is represented by a polynomial term $T(x_1, \ldots, x_n)$ with $s(T)$ interior nodes and base 10 logarithmic height $h(T)$.

The total degree of P is bounded by $s(T) + 1$. We can find natural numbers $r_1, \ldots, r_n$ so that the numbers

$$\alpha_j = r_1 i_1 + \cdots + r_n i_n$$

are all distinct. Take $d = 2\,s(T) + 2$ in lemma 7.4.1 we get

$$r_j = \frac{1}{(2\,s(T) + 3)^{n-j}}, j = 1, 2, \ldots, n.$$

The number M of terms in $P(x_1, \ldots, x_n)$ is bounded by $(s(T) + 2)^n$ by lemma 7.4.2. $P(x_1, \ldots, x_n)$ can be represented by an expression where depth $d(P)$ satisfies

$$2^{d(P)} \leq 8(s(T) + 2)^{n+1}$$

by lemma 6.3.2.

Suppose $P(x_1, \ldots, x_n) = \varepsilon$. *By conjecture 8*

$$\log|\varepsilon| \leq 8C(s(T)+2)^{n+1} \max\left(h(T), \log(2s(T)+1)^n\right)$$

where $h(T)$ *is the height of the polynomial and* C *is some universal constant. The precision needed is singly exponential in* n. *However the bound from theorem 7.3.1*

$$|\varepsilon| > \frac{1}{(Mp)!}$$

with

$$M \leq (s(T)+2)^n$$

and

$$p \leq 5\,\kappa\,(2lA)^M \log B$$

where

$$l = (2s(T)+3)^n\,,\; A \leq s(T)+1$$

and κ *is as in lemma 7.1.6. We can bound* $\log|\varepsilon|$ *by* $Mp\log(Mp)$. *But* p *is very large if there are many variables because* M *occurs as an exponent.*

The advantage of using theorem 7.3.1 is that we have an explicit bound. The precision needed is doubly exponential in the number of variables n.

7.5 Another effective version of the Lindemann-Weierstrass theorem

We will present here the main results of the work done in [Ser99] by Alain Sert in the direction of having better effective results for the Lindemann-Weierstrass theorem. Mahler began the work in this direction in 1932 ([Mah32]) in which he proved that there exists a constant

$$H_0 = H_0(d, \alpha_1, \ldots, \alpha_p) > 0$$

such that

$$H \geq H_0 \textit{ implies } \log|P(e^{\alpha_1}, \ldots, ^{\alpha_p})| \geq -c\,d^p \log H\,,$$

where $c = c(\alpha_1, \ldots, \alpha_p) > 0$ *and* P *is a non zero polynomial over* $\boldsymbol{Z}[x_1, \ldots, x_p]$ *with degree* $\leq d$ *and with height* $\leq H$. *The work continued until the recent result of Ably in [Abl94] concluded the following minimisation*

Theorem 7.5.1 (Ably Theorem). *If* P *is a non zero polynomial in* $K[x_1, \ldots, x_p]$ *with degree* $\leq d$ *and* K *denotes a number field of degree* D *over* $\boldsymbol{Q}$. *Assume* $\alpha_1, \ldots, \alpha_p$ *are algebraic independent over the rationals then*

$$\log |P(e^{\alpha_1}, \ldots, ^{\alpha_p})| \geq -c\, d^p\, (\log H + exp(C\, d^p \log(d+1))),$$

$c = 2^{4p^3} + 18p^2 + 25p + 4\, p^{p^2+p+2}\, (4D + p + 1)^{p+2}\, D^{p^2+p+1}$ *and* $C = C(\alpha_1, \ldots, \alpha_p)$.

Alain Sert in his work [Ser99] improved this result and showed the dependence on $\alpha_1, \ldots, \alpha_p$ *explicitly in the following version of the theorem. This is a special case of his theorem*

Theorem 7.5.2 (effective version of the Lindemann-Weierstrass theorem). *If* P *is a non zero polynomial in* $\boldsymbol{Z}[x_1, \ldots, x_p]$ *with degree* $\leq d\, (d \geq 1)$ *and with height* H. *Let* K *denote a number field of degree* D *over* $\boldsymbol{Q}$. *Assume* $\alpha = (\alpha_1, \ldots, \alpha_p)$ *where* $\alpha_1, \ldots, \alpha_p$ *are elements of* K *linearly independent over the rationals. Then we have the bound*

$$\log |P(e^{\alpha_1}, \ldots, e^{\alpha_p})| \geq -c\, d^p\, [\log H + \exp\, (c'\, d^p + c''\, d^p\, \log d + 72\, |\alpha|)]$$

where

$$|\alpha| = \max\{1, \max_i |\alpha_i|\},$$

$$c = 41 \times 3^{2p} \times 2^{-p+1} p^p D^{p+1},$$

$$c' = 2^{2-p}\, 3^{2p+1}\, p^p\, D^{p+1} + (1+6D)\, 2^{4-p}\, 3^{2p}\, p^p\, D^p\, \log(9pD) + 2^{4-p}\, 3^{2p}\, p^p\, D^{p+1}\, (1+6p)\, \log h_a(\alpha),$$

where

$$h_a(\alpha) = \frac{\log(m(\alpha))}{deg(\alpha)}$$

is the absolute height of α *defined with respect the the field* K *and*

$$c'' = (1 + 6D)\, 2^{4-p}\, 3^{2p}\, p^p\, D^p.$$

We can notice the improvement of the result compared to the one in [Abl94]. The constant c is better and the dependence on $\alpha_1, \ldots, \alpha_p$ is totally explicit. However the precision needed is again doubly exponential in n since c' increases exponentially with n.

Example 7.5.1. *If P is a non zero polynomial in $\boldsymbol{Z}[X,Y]$ with degree $\leq d$ ($d \geq 1$) and height $\leq H$. Considering the value of this polynomial at the point $(e^{\sqrt{2}}, e^{\sqrt{3}})$, the inequality in the setting of the theorem gives us the minimisation*

$$\log \left| P(e^{\sqrt{2}}, e^{\sqrt{3}}) \right| \geq -5 \times 10^5 \, d^2 \left[\log H + e^{5 \times 10^6 d^2 \log(d+1)} \right].$$

We can compare this with the result of theorem 7.3.1. Let

$$P(e^{\sqrt{2}}, e^{\sqrt{3}}) = \varepsilon$$

where

$$|\varepsilon| > \frac{1}{(Mp)!}$$

with

$$M \leq (4d+1)^2.$$

The degree is multiplied by 4 to satisfy the Galois assumption. Since $p \leq 5\kappa(2lA)^M \log B$, $l = 1$, κ is as in lemma 7.1.6 and $A \leq 6(4d)$. It seems that our results will be better in some cases especially for small number of monomials.

Chapter 8

Conclusion

{Blessed be He in His hands is the Dominion, and He over all things hath Power; He Who created Death and life, that He may try which of you is best in deed. And He is the Exalted in Might, Oft-Forgiving.} [67:1-2]

This thesis presents the following results

1. *We introduced a representation of polynomials as a polynomial term which is a tree with operators $*, +, -$ on the interior nodes and natural numbers and variables on the frontier.*

   We attempt to decide whether or not such a tree represents the zero polynomial by substituting algebraically independent real numbers for the variables and attempting to decide whether or not the resulting constant is zero.

   We proved a measure theoretic analogue to the Schwartz' theorem of probabilistic zero recognition in case of choosing points at random in the unit cube in $\boldsymbol{R}^n$. This proposition can be stated as follows:

   If polynomial term T is not identically zero, then the intersection of the unit cube in $\boldsymbol{R}^n$ with $\{|T(X)| < 10^{-k}\}$ has Lebesgue measure $\leq 2d(T)10^{-k/d(T)}$, where $\{|T(X)| < 10^{-k}\}$ is the subset of R^n in which $|T(X)| < 10^{-k}$.

   We also proved that:

   For almost all points X in the unit cube, there is a number C so that for all non zero polynomial terms T we have $|T(X)| > 10^{-C-k(T)d(T)}$.

   where T has variables $x_1, \ldots, x_n$, $d(T) = \sum_{i=1}^{n} deg(T, x_i)$ and $deg(T, x_i)$ is the degree of x_i in T.

$k(T)$ is a mapping polynomial terms into natural numbers, is such that $\sum d(T)10^{-k(T)}$ (taken over all polynomial terms) converges to a finite limit. (For example, $k(T) = 2*length(T)$ would do.)

From this we get a probabilistic zero recognition test which is somewhat more expensive computationally than the usual method of choosing random integers in a large interval and evaluating, but which depends on the ability to choose a random point in the unit cube and to approximate a polynomial at that point.

We also stated a conjecture about algebraic independence measure which would give us a deterministic test with a uniformly chosen test point. The result is that if a polynomial term has $s(T)$ nodes, then the bit complexity of deterministic zero recognition is bounded by

$$O\left(s(T)M\left(s(T)length(T)\right)\right),$$

where $length(T)$ measures the length of the term T and $M(n)$ is the bit complexity of multiplication of two n-th digit natural numbers.

2. *The uniformity conjecture postulates a relationship between the syntactic length of expressions built up from the natural numbers using field operations, radicals and exponentials and logarithms, and the smallness of non zero complex numbers defined by such expressions. The Uniformity Conjecture claims that if the expressions are written in an expanded form in which all the arguments of the exponential function have absolute value bounded by 1, then a small multiple of the syntactic length gives a bound for the number of decimal places needed to distinguish the defined number from zero.*

   We discussed applications of the conjecture, showing that it implies an efficient zero recognition algorithm for algebraic numbers represented by radicals, and that it implies an efficient zero recognition algorithm for multivariate polynomial expressions with radical coefficients.

3. *However, counterexamples to the uniformity conjecture and to the witness conjectures in general are found by solving some system of polynomial equa-*

tions. An example of this is the following example

$$G(x) = \sqrt{1+x} - \frac{25}{4} + \frac{21}{4}\sqrt{\frac{7}{5} - \frac{2}{5}\sqrt{-7+8\sqrt{1+\frac{5}{21}x}}}.$$

In this example we have only two occurrences of x but $G(x) = O(x^5)$ near zero. In such case we could get a counterexample from $G(x)$ with $x = 10^{-N}$ and N sufficiently large. Other examples were formed with different basis functions.

4. *We introduced some modifications for the violated conjecture that may help improve the studies in this direction and help other areas of interest like the exact geometric computation to compare with existing root bounds.*

   The counterexamples show that one of the conditions we should expect for an approximation measure is:

$$\frac{g(A)}{\log(h(A))} > \textit{ multiplicity of any root of } f_A(x) \textit{ near} 0$$

   It is not too hard to compute such an upper bound on multiplicity, using the ideas of Khovanskii, since all of the functions $f_A(x)$ are Pfaffian in some neighbourhood of zero.

   Let K be either $\boldsymbol{R}$ or $\boldsymbol{C}$. A Pfaffian chain of order r and degree $\alpha \geq 1$ in an open domain $G \subset K^n$ is a sequence of analytic functions $f_1, \ldots, f_r$ in G satisfying differential equations

$$df_j(x) = \sum_{1 \leq i \leq n} g_{ij}(x, f_1(x), \ldots, f_j(x))dx_i$$

   for $1 \leq j \leq r$. Here $g_{ij}(x, y_1, \ldots, y_j)$ are polynomials in $x = (x_1, \ldots, x_n), y_1, \ldots, y_j$ of degrees not exceeding α. A function $f(x) = P(x, f_1(x), \ldots, f_r(x))$ where $P(x, y_1, \ldots, y_r)$ is a polynomial of degree not exceeding $\beta \geq 1$, is a Pfaffian function of order r and degree (α, β). An upper bound for the multiplicity of a zero of such a function is

$$kh(f) = M(n, r, \alpha, \beta) = 2^{r(r-1)/2}\beta(min(n, r)\alpha + \beta - n + 1)^r$$

Aside from being close to a zero of high multiplicity, the only other way we know to construct very small values is via the pigeon hole principle. Consider an expression tree for A with $d(A) = d$. The frontier may have up to 2^{d-1} integers on it. Consider such expression up to absolute height H. There are no more than $(2H+1)^{2^{d-1}}$ of them. If these are all real and distinct and we consider them all mod 1, we will get two such expressions whose distance apart (mod 1) is $O((2H+1)^{-2^{d-1}})$. This gives us another approximate bound on $g(A)$.

$$g(A) \geq 2^{d-1} \log(2H+1)$$

Combining these two ideas, we suggest the following form of the UC:

UC revisited

If x is a non zero closed form number, then

$$|x| \geq \max(2, H)^{-c\,kh(d)},$$

where $kh(d)$ is an upper bound on multiplicity of a zero of a function $f_B(x)$ where B is an expression in E and $d(B) \leq d$, and c is a universal constant. It is clear that $kh(d)$ is at least 2^d and in fact this may suffice. We are not able to construct any examples of expressions $A(x)$ with $d(A) \leq d$, and $|x| < \max(H, 2)^{-2^d}$.

In practice the best known technique for attempting to recognise zero among closed form numbers seems to be the following.

Given closed form number x represented by expression A,

(a) Test if $|x| > \max(H, 2)^{-2^d}$, where $d = d(A)$, $H = h(A)$. If so, $x \neq 0$. Otherwise,

(b) Construct a sequence of fields $\mathbf{Q} \subset F_1 \subset F_2 \subset \ldots \subset F_k$, where $x \in F_k$. Attempt to find a canonical form for x, by attempting to find a proper set of generators for F_k. If the canonical form of x is 0, then $x = 0$. Otherwise,

(c) Test if $|x| > \max(2, H)^{-kh(d)}$, where $kh(d)$ is the Khovanskii's bound on multiplicity as given above. If so then $x \neq 0$.

If the question is still unresolved, then x is either non zero and surprisingly small, or somewhere in F_k there is a counterexample to the Schanuel conjecture. Either of these two outcomes would be quite interesting.

5. *We introduced a new effective proof of the famous Lindemann theorem in the following form*

Effective Lindemann Theorem

Given distinct algebraic numbers $\alpha_1, \ldots \alpha_n$ and $\beta_1, \ldots, \beta_n \in \boldsymbol{Z}$ not all zero and

$$\textit{If} \quad \beta_1 e^{\alpha_1} + \cdots + \beta_n e^{\alpha_n} = \varepsilon \quad \textit{where} \quad \beta_1, \ldots, \beta_n \in \boldsymbol{Z},$$

Then we can find a natural number N and a prime number p such that

$$|\varepsilon| \geq \frac{1}{(Np)!}$$

which gives an upper bound on the precision needed to distinguish ε from zero. The precision is higher than that is required by the modified UC and it is comparable to the precision needed by the recent results of Alain Sert on Effective Lindemann theorem.

Appendix A

Koranic Quotations

{Verily, all things have We created in proportion and measure.} [54:49]

This verse from Surat 54: Al-Qamar, the Moon says that everything goes by law and plan whether we see it or not and whether we discover or not even the laws for uncertainty and random motion!. All fields of science are evidences of that and give no chance for accepting accidental being. After studying and researching for about 5 years about a specific problem in some area of knowledge my belief in this progressively increases. For me, this is the main conclusion of my work. We feel what the law or the formula may look like so we guess and conjecture and then test it and move toward discovering the facts. The important thing is that the facts were there all the times: before we try our conjectures, and when we do and even if we do not discover them at all. It is always the fact that punctual laws govern all phenomena under consideration and beyond consideration.

This is a translation for the Arabic tongue preserved through the Koran for over 14 centuries till now. I think in this language and I like to thank every reader for reflecting through this message of mercy and wisdom. For this reason I made my choice for these Koranic quotations which appeared in the thesis. Now I will add their original Arabic pronunciation in what is called transliteration.

1. *Dedication: I quoted the first revelation of the Koran*

   {Read in the name of thy Lord and Cherisher, who created, created man, out of a leech-like clot. Proclaim and thy Lord is most bountiful, He who taught (the use of) the pen, taught man that which he knew not.} [96:1-5]

The Arabic reads:

{Iqra/ bi-ismi rabbika allathee khalaqa ⋆ Khalaqa al-insana min AAalaqin ⋆ Iqra/ warabbuka al-akramu ⋆ Allathee AAallama bialqalami ⋆ AAallama al-insana ma lam yaAAlam ⋆} [96:1-5]

2. *Chapter 1: Introduction*

{Say: "travel through the earth and see how He did originate creation; so will God produce a later creation: for God has power over all things".} [29:20]

The Arabic reads:

{Qul seeroo fee al-ardi faonthuroo kayfa badaa alkhalqa thumma Allahu yunshi-o alnnash-ata al-akhirata inna Allaha AAala kulli shayin qadeerun ⋆} [29:20]

3. *Chapter 2: Background material*

{Slowly will We show them Our signs in the horizons and in their own selves, until it becomes manifest to them that this is the truth. Is it not enough that thy Lord doth witness all things?} [41:53]

The Arabic reads:

{Sanureehim ayatina fee al-afaqi wafee anfusihim hatta yatabayyana lahum annahu alhaqqu awa lam yakfi birabbika annahu AAala kulli shay-in shaheedun ⋆} [41:53]

4. *Chapter 3: Uniformity conjecture*

{In the creation of the heavens and the earth, and the alteration of night and day, there are indeed signs for men of understanding.} [3:190]

The Arabic reads:

{Inna fee khalqi alssamawati waal-ardi waikhtilafi allayli waalnnahari laayatin li-olee al-albabi ⋆} [3:190]

5. *Chapter 4: Zero Recognition of Polynomial Terms*

{Do not the unbelievers see that the heavens and the earth were joined together (as one unit of creation), before we clove them asun-

der? We made from water every living thing. Will they not then believe?} [21:30]

The Arabic reads:

{Awa lam yara allatheena kafaroo anna alssamawati waal-arda kanata ratqan fafataqnahuma wajaAAalna mina alma-i kulla shay-in hayyin afala yu/minoona ⋆} [21:30]

6. *In chapter 5: Counter Examples to The Uniformity Conjecture*

{Do they not observe the birds above them, spreading their wings and folding them in? None can uphold them except The Most Gracious: truly it is He that watches over all things.} [67:19]

The Arabic reads:

{Awa lam yaraw ila alttayri fawqahum saffatin wayaqbidna ma yumsikuhunna illa alrrahmanu innahu bikulli shay-in baseerun ⋆} [67:19]

7. *In chapter 6: New Conjectures*

{And pursue not that of which thou hast no knowledge; for surely the hearing, the sight, the heart all of those shall be questioned of.} [17:36]

The Arabic reads:

{Wala taqfu ma laysa laka bihi AAilmun inna alssamAAa waalbasara waalfu-ada kullu ola-ika kana AAanhu mas-oolan ⋆} [17:36]

8. *In chapter 7: An Effective Proof Of Lindemann's Theorem*

{Verily, all things have We created in proportion and measure.} [54:49]

The Arabic reads:

{Inna kulla shay-in khalaqnahu biqadarin ⋆} [54:49]

9. *In chapter 8: Conclusion and Future Work*

{Blessed be He in His hands is the Dominion, and He over all things hath Power; He Who created death and life, that He may try which of you is best in deed. And He is the Exalted in Might, Oft-Forgiving.} [67:1-2]

The Arabic reads:

{Tabaraka allathee biyadihi almulku wahuwa AAala kulli shay-in qadeerun ⋆ Allathee khalaqa almawta waalhayata liyabluwakum ayyukum ahsanu AAamalan wahuwa alAAazeezu alghafooru ⋆} [67:1-2]

The Koran is full of signs for mankind to think about and they are real motivation for people to make developments in all directions to help man and woman to discover his/her purpose of life and serve all of the humanity with justice and mercy. I will add to this collection some more quotations of these signs mentioned in Surat 30: Ar-Rum, The Romans.

1. *{And among His Signs is this, that He created for you mates from among yourselves, that ye may dwell in tranquillity with them, and He has put love and mercy between your (hearts): verily in that Are signs for those who reflect.} [30:21]*
2. *{And among His Signs is the creation of the heavens and the earth, and the variations in your languages and your colours: verily in that are Signs for those who know.} [30:22]*
3. *{And among His Signs is the sleep that ye take by night and by day, and the quest that ye (make for livelihood) out of His Bounty: verily in that are Signs for those who hearken.} [30:23]*
4. *{And among His Signs, He shows you the lightning, by way of both fear and of hope, and He sends down rain from the sky and with it gives life to the earth after it is dead: verily in that are Signs for those who are wise.} [30:24]*

The Arabic reads:

{Wamin ayatihi an khalaqa lakum min anfusikum azwajan litaskunoo ilayha wajaAAala baynakum mawaddatan warahmatan inna fee thalika laayatin liqawmin yatafakkaroona ⋆ Wamin ayatihi khalqu alssamawati waal-ardi waikhtilafu alsinatikum waalwanikum inna fee thalika laayatin lilAAalimeena ⋆ Wamin ayatihi manamukum biallayli waalnnahari waibtighaokum min fadlihi inna fee thalika laayatin liqawmin yasmaAAoona ⋆ Wamin ayatihi yureekumu albarqa khawfan watamaAAan

wayunazzilu mina alssama-i maan fayuhyee bihi al-arda baAAda mawtiha inna fee thalika laayatin liqawmin yaAAqiloona ⋆} [30:21-24]

The conclusion I like to end with is to express the feeling and the fact that everything has some sort of life and realisation from the atoms to the galaxies. I have this in my heart and mind from the verse

{The seven heavens and the earth, and all beings therein, declare His glory: there is not a thing but celebrates His praise; and yet ye understand not how they declare His glory! Verily He is Oft-Forbearing, Most Forgiving!} [17:44]

The Arabic reads:

{Tusabbihu lahu alssamawatu alssabAAu waal-ardu waman feehinna wa-in min shay-in illa yusabbihu bihamdihi walakin la tafqahoona tasbeehahum innahu kana haleeman ghafooran ⋆} [17:44].

Bibliography

[Abl94] *M. Ably. Une version quantitative du théorème de lindemann-weierstrass.* Acta Arith, *67:29–30, 1994.*

[And94] *George E. Andrews.* Number Theory. *Dover Publications, Inc., 1994.*

[Bai00] *David H. Bailey. Integer relation detection.* Computing in Science and Engineering, *Jan-Feb. 2000. LBNL-44639.*

[Bak75] *A. Baker.* Transcendental number theory. *CUP, 1975.*

[Bak98] *A. Baker. Diophantine analysis and transcendental theory. Extract from "Logarithmic Forms and Diophantine Geometry" by A. Baker and G. Wüstholz, 1998.*

[BB87] *J. M. Borwein and P. B. Borwein.* Pi and the AGM. *John Wiley, Canadian Mathematical Society, 1987.*

[BB88] *J. M. Borwein and P. B. Borwein. On the complexity of familiar functions and numbers.* SIAM Review, *30(4):589–601, December 1988.*

[BB92] *J. M. Borwein and P. B. Borwein. Strange series and high precision fraud.* Mathematical monthly, *(99):622–640, 1992.*

[BD88] *R. J. Bradford and J. H. Davenport. Effective tests for cyclotomic polynomials.* Springer-Verlag Lecture Notes in Computer Science, *(368):244–251, 1988. P. Gianni Ed.*

[Bes40] *A. S. Besicovitch. On the linear independence of fractional powers of integers.* J. London math. Society, *15:3–6, 1940.*

[BFea01] *C. Burnikle, S. Funke, and K. Mehlhorn et al. A separation bound for real algebraic expressions. In* Lecture Notes in Computer Science, *pages 254–265. Springer, 2001. to appear, Algorithmica.*

[BFMS99] *C. Burnikle, R. Fleischer, K. Mehlhorn, and S. Schirra. Exact geometric computation made easy. In* Proc. 15th ACM Symp. Comp. Geom., *pages 341–450. ACM Press, 1999.*

[Bre75] *Richard P. Brent. Multiple-precision zero- finding methods and the complexity of elementary functions. In J.F.Traub, editor,* Analytic Computational Complexity, *pages 151–176. Academic Press, 1975.*

[Bur00] *Peter Burgisser.* Completeness and reduction in algebraic complexity theory, *volume vol. 7. Springer, 2000.*

[Cho99] *T. Y. Chow. What is a closed form number?* American Mathematical Monthly, *106(5):440–448, 1999.*

[Ded96] *Richard Dedekind.* Theory of Algebraic Integers. *Cambridge University Press, 1996. First published in French 1877.*

[DYS88] *J. H. Davenport and E. Tournier Y. Siret.* Computer Algebra: Systems and Algorithms for Algebraic Computation. *Academic Press, Harcourt Brace Jovanovich, Publishers, 1988.*

[Eve98] *J. H. Evertse. Symmetric improvements of liouville's inequality: A survey in algebraic number theory and diophantine analysis. In F. Halter and R. F. Tichy, editors,* Proc. Conf. Graz 1998, *pages 129–141. Walter de Gruyter, 1998.*

[FB92] *H. R. P. Ferguson and D. H. Bailey. A polynomial time, numerically stable integer relation algorithm. Technical Report RNR-91-032, RNR Techn. Rept., Jul. 14, 1992.*

[FBA99] *H. R. P. Ferguson, D. H. Bailey, and S. Arno. Analysis of pslq, an integer relation finding algorithm.* Math. Comput., *(68):351–369, 1999.*

[FF79] *H. R. P. Ferguson and R. W. Forcade. Generalaization of the euclidean algorithm for real numbers to all dimensions higher than two.* Bulletin of the American Mathematical Society, *pages 912–914, 1979.*

[Gab95] *A. Gabrielov. Multiplicities of pfaffian intersections and the łojasiewicz inequality.* Selecta Mathematica, New Series, *1:113–127, 1995.*

[GV95] *A. Gabrielov and N. Vorobjov. Complexity of stratifications of semi-pfaffian sets.* Discrete Comput. Geom., *(14):71–91, 1995.*

[GV03] *A. Gabrielov and N. Vorobjov. Complexity of computations with pfaffian and noetherian functions. preprint, 2003.*

[Hil42] *E. Hille. An account of gelfond schneider theorem.* American Mathematical Monthly, *vol. 49:654–661, 1942.*

[Hoe95] *Joris Van Der Hoeven. Automatic numerical expansions. In J. M. Moreau J. C. Bajard, D. Micheucci and J. M. Muller, editors,* Proc. of the conference "Real numbers and computers", *pages 261–274, Saint-Etienne, France, 1995.*

[Hoe97] *Joris Van Der Hoeven.* Automatic Asymptotics. *PhD thesis, Ecole Polytechnique, 1997.*

[Hoe00] *Joris Van Der Hoeven. Zero-testing, witness conjectures and differential diophantine approximation. Preprint, 2000.*

[HS00] *M. Hindry and J. Silverman.* Diophantine Geometry, An Introduction. *Springer Graduate Texts in Mathematics. 2000.*

[HW02] *G. H. Hardy and E. M. Wright.* An Introduction to the Theory of Numbers. *Oxford University Press, fifth edition edition, 2002.*

[IM83] *O. Ibarra and S. Moran. Probabilistic algorithms for deciding equivalence of straight line programs.* Journal of the ACM, *(30:1):217–228, 1983.*

[Joh92] *J. R. Johnson. Real algebraic number computation using interval arithmetic.* ISSAC'92, *pages 195–205, 1992.*

[Khi92] *A. Ya. Khinchin.* Continued Fractions. *Dover Publications, Inc., third edition edition, 1992. English translation.*

[Kho80] *A. Khovanskii. On a class of systems of transcendental equations.* Soviet Math. Dokl., *22:762–765, 1980.*

[Kho91] *A. Khovanskii.* Fewnomials. *AMS Transl. Math. Monographs, 1991.*

[Lan66] *S. Lang.* Introduction to Transcendental Numbers. *Addison Wesely, 1966.*

[Lan69] *E. Landau.* Vorlesungen uber Zahlentheorie. *Chelsea, New York, 1969. 3 volumes, S. Hirzel, Leipzig, 1927.*

[Lan70] *S. Lang.* Algebraic Number Theory. *Addison-Wesely, Reading, Mass., 1970.*

[Lan71] *S. Lang. Transcendental numbers and diophantine approximation.* Bull. Amer. Math. Soc., *(77(5)):635–677, 1971.*

[Lan93] *S. Lang.* Algebra. *Addison Wesley, 1993. third edition.*

[Lan02] *S. Langley. Linear methods for the algebraic constant problem. 2002.*

[LB97] *M. Shub S. Smale L. Blum, F. Cucker.* Complexity and Real Computation. *Springer-Verlag, 1997.*

[LeV65] *W. J. LeVoeque.* Topics in Number Theory, *volume vol. II. Addison-Wesley, Reading, Mass., 1965.*

[Li01] *Chen Li.* Exact Geometric Computation: Theory and Applications. *PhD thesis, Depatment of Computer Science, New York University, January 2001.*

[Lin82] *F. Lindemann. 'Uber die zahl π.* Math. Annalen, *(20):213–225, 1882.*

[Lio44] *J. Liouville. Sur des classes très-étendues de quantités dont la valeur n'est ni algébrique , ni même reductible à des irrationalles algébriques.* Comptes Rend.,, *(18):883–885, 910–911, 1844.*

[LLL82] *A. K. Lenstra, H. W. Lenstra, and L. Lovasz. Factoring polynomial with rational coefficients.* Mathematical Annalen, *261:515–534, 1982.*

[Loo82] *R. Loos. Computing in algebraic extentions.* Computing, *(4):173–187, 1982.*

[Mah32] *K. Mahler. Zur approximation der exponential funktion und des logarithmus i.* J. Reine Angew. Math., *166:118–136, 1932.*

[Mig92] *Maurice Mignotte.* Mathematics for Computer Algebra. *Springer-Verlag, 1992.*

[MW95] *A. J. Macintyre and A. J. Wilkie. On the decidability of the real exponential field. In P. G. Odifreddi, editor,* Kreisel 70th Birthday Volume. *CLSI, 1995.*

[Nay99] *Bill Naylor.* Polynomial GCD using straight line program representation. *PhD thesis, School of Mathematical Sciences, University of Bath, 1999.*

[PD98] *Harry Pollard and Harold G. Diamond.* The Theory of Algebraic Numbers. *Dover Publications, Inc., 1998.*

[Per02] *S. Pericleous.* Complexity bounds for cylinderical cell decompositions of sub-Pfaffian sets. *PhD thesis, Computer Science, University of Bath, 2002.*

[Phi99] *P. Philippon. Quelques remarques sur des questions d'approximation diophantine.* Bull Austral. Math. Soc., *vol. 59(2):323–334, 1999.*

[Phi00] *P. Philippon. Addendum a quelques remarques sur des questions d'approximation diophantine.* Bull Austral. Math. Soc., *vol 61(1):167–169, 2000.*

[Poh97] *M. Pohst. On validated computing in algebraic number fields.* J. Symbolic Computation, *(24):657–666, 1997.*

[RE03] *D. Richadson and A. Elsonbaty. Use of algebraically independent numbers for zero recognition of polynomial terms.* Journal of Complexity and Algorithms, *19:631–637, 2003.*

[Ric97] *D. Richardson. How to recognize zero.* J. Scientific Computation, *24, 1997.*

[Ric00] *D. Richardson. The uniformity conjecture. In* Proceedings of Computability and Complexity in Analysis, *CCA2000, Swansea, Wales, September 17-19 2000.*

[Ric01] *D. Richardson. Multiplicative independence of algebraic numbers and expressions.* Journal of pure and applied algebra, *(164):231–245, 2001.*

[Ric02] *D. Richardson. Testing the uniformity conjecture. Available at http://www.bath.ac.uk/ masdr/, 2002.*

[Rot55] *K. Roth. Rational approximations to algebraic numbers.* Mathematika, *(2):1–20, 1955. Corrigendum, 168, MR 17, 242.*

[Sam72] *P. Samuel.* Algebraic Theory of Numbers. *Kershaw, London, 1972.*

[Sch36] *T. Schneider. Über die approximationt algebraischer zahlen.* J. Reine Angew. Math, *(175):110–128, 1936.*

[Sch80] *J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities.* J. of the ACM, *(27(4)):701–717, 1980.*

[Ser99] *Alain Sert. Une version effective du théorème de lindemann-weierstrass par les déterminants d'interpolation.* Journal of Number Theory, *76:94–119, 1999.*

[Sha98] *T. A. Shahoumian1998.* Some Programs Need Only Be Checked For Correctness on Random Inputs. *PhD thesis, Computer Science in the Graduate Division of the University of California at Berkeley, 1998.*

[Sha03] *John Shackell.* An Approach to Symbolic Asymptotics. *Springer, 2003.*

[Sie89] *Carl Ludwig Siegel.* Lectures on the geometry of numbers. *Berlin ; London : Springer-Verlag, 1989. notes by B. Friedman.*

[Spr80] *V. G. Sprinkzhuk. Achievements and problems in diophantine approximation theory.* Russian Mathematical Surveys, *(35(4)):1–80, 1980.*

[Ste98] *Ian Stewart.* Galois Theory. *Chapman Hall Mathematics, 1998.*

[Str97] *A. W. Strsebonski. Computing in the field of complex algebraic numbers.* J. Symbolic Computation, *(24):647–656, 1997.*

[Tar48] *A. Tarski.* A decision method for elementary algebra and geometry. *RAND Corporation monograph, 1948.*

[Wal92] *M. Waldschmidt. Linear independence of logarithms of algebraic numbers. Technical Report Report no.116, The Institute of Mathematical Sciences, IMSc, Madras, 1992.*

[Weg87] *B. M. M. De Weger. Solving exponential diophantine equations using lattice basis reduction algorithms.* J. Number Theory, *(26):325–367, 1987.*

[Wey40] *H. Weyl.* Algebraic Theory of Numbers. *U. Press, Princeton, 1940.*

[Yap00] *Chee Keng Yap.* Fundamental Problems of Algorithmic Algebra. *Oxford University Press, 2000.*

[Zel99] *T. Zell. Betti numbers of semi-pfaffian sets.* J. Pure Appl. Algebra, *139(1-3):323–338, 1999.*

[Zip79] *R. Zippel. Probabilistic algorithms for sparse polynomials. Lecture Notes in Computer Science, pages 216–226. Springer Verlag, 1979. New York, NY, 1979.*

[Zip93] *R. Zippel.* Effective Polynomial Computation. *Kluwer Academic Publishers, 1993.*