Counting Zeros of Polynomials

By

Wankhede Hitesh Vilas

MATH10202305001

The Institute of Mathematical Sciences, Chennai

A thesis submitted to the

Board of Studies in Mathematical Sciences

(Theoretical Computer Science)

in partial fulfillment of requirements

for the degree of

MASTER OF SCIENCE

of

HOMI BHABHA NATIONAL INSTITUTE



July, 2025

Certificate

Certified that the dissertation prepared by Wankhede Hitesh Vilas entitled "Counting Zeros of Polynomials" has been prepared under my supervision and has not been submitted elsewhere for a degree.

Date:

Place:

Prof. Vikram Sharma (Guide)
Theoretical Computer Science Group
The Institute of Mathematical Sciences, Chennai

Abstract

The τ-complexity of an integer polynomial is the minimum number of additions, substractions and multiplications needed to build it using just the scalar '1' and the indeterminate 'x'. The fourth problem in Smale's list of mathematical problems for the next century (1998) is the τ-conjecture due to Shub and Smale (1995): The number of distinct integer zeros of an integer polynomial is polynomially upper bounded by its τ-complexity. A real variant of this conjecture was posed by Koiran (2011), and we survey some of the progress towards it in this thesis. We begin by motivating the τ-conjecture and its real variant. Then we discuss the applicability of tools such as Descartes' rule, Rolle's theorem and the Wronskian to yield concrete results. We also discuss why studying the distribution of zeros is important to solve real τ-conjecture. We conclude the thesis with the most recent refinements of the conjecture.

To my parents:
my patient mother,
and in memory of my late father

Acknowledgements

Let me start by saying that I am very fortunate to have Prof. Vikram as my advisor. He has been kind, encouraging and patient, and I am very much influenced by his thinking and guidance, through which I've come to learn much more about reading, writing and speaking math. He often pushed me to discern motivations and intuitions behind the results, and led me to the core of the problems. His frequent prompt "...but what does this (algebraic identity) mean geometrically?" and his point of view helped me realize and appreciate the connection between algebra and geometry. I am also thankful to him for humanizing mathematics to me. He taught me three courses (discrete mathematics, linear programming and combinatorial optimization, algorithms for solving polynomial equations), and he would often begin his lectures with historical anecdotes to what we would learn next. I have found the historical perspective of mathematics really helpful; in fact, the present topic of study became even more fascinating after being able to trace its developments over the past four centuries. I feel this has also made many parts of mathematics a little less daunting for me. He encouraged me to write an exposition as well; this thesis is my first-ever attempt! If there is anything significant that I must mention in my life, it is that Prof. Vikram has given me new eyes to view mathematics and opened doors for me that I had never imagined.

Much of the content of this thesis is based on presentations that I have given over the past six months, and I would also like to acknowledge Satya and Om for attending some of them. This process was helpful in organizing my ideas, and I have roughly tried to include a chapter for each presentation. The motivating part for the Wronskian (Chapter 5) has been taken from Vikram's course notes of the previous offering of the Algorithms-for-Solving-Polynomial-Equations course; he taught me complex analysis prerequisites as well (Chapter 12) that helped me work out the proof of the bound on the angular discrepancy (Chapter 13). Some of the other coursework I have done in the past two years also supplemented by interest in the subject. It was in the Coding Theory course offered by Prof. Ramya that I encountered an application of polynomials with all integer zeros to prove

a nonexistence result for the perfect binary codes. I also had an opportunity to attend Algebra and Computation course by Amit Sinhababu and V. Arvind at CMI. Amit taught me Horner's method and Hajos' lemma, and he gave me two exercises: prove the optimality of Horner's method and prove Hajos' lemma using a system of linear equations. I have yet to prove the optimality, but I have proved Hajos' lemma (Lemma 11.3) in this thesis. I hope these exercises were not part of the course evaluation! It was very fascinating to learn that Horner's method motivates the complexity of computing polynomials, and I have tried to motivate this thesis with it as well (Chapter 1). Interestingly, Hajos' lemma motivates the most recent variant of the real τ-conjecture (Chapter 14). I thank Amit for his interest in my work. Hilbert Nullstellensatz is also a motivating problem in Chapter 2 and I learned about it earlier in the Proof Complexity course that Prof. Meena offered. Her survey on algebraic complexity classes [56] has also been helpful.

I would like to thank all the professors in the theoretical computer science group for their advice, encouragement and the excellent courses. If not for these courses, a psychological barrier which used to make me avoid words such as 'algorithms', 'inequalities', and 'approximation' would have still been there. I've also found much satisfaction in working on the assignments. Prof. Prakash Saivasan encouraged me to give my first-ever public talk to a general audience at the Institute Seminar Days; it is ten minutes long and now on YouTube. Prof. Vikram also advised me for a short project on nonnegative rank earlier on which I gave my first-ever technical talk. Prof. Saket Saurabh advised me before joining IMSc to go through all the coursework with an open mind, and then decide the research area. I have come to work on something very different than what I had imagined then. Prof. Ramya's gentle prompt in my first year that I prioritize my PhD over other research problems has kept me on track. I am very fortunate to have been taught algorithms and parameterized complexity by Prof. Venkatesh Raman, now that he has retired. I would look forward to his lectures with excitement. He taught me algorithms in IISER Pune as well, in 2019 as a guest lecturer, and I still remember the moment when he introduced 'automaton' (in the context of pattern matching), a word I had never heard before, I was in awe, it felt as if he had pulled out a bird from a magic hat. Prof. Meena Mahajan is a researcher that I admire very much. A friend of mine had said to me when I joined IMSc "Meena is everything I want to be", and as I tried to make sense of it over the two years I noticed her discipline, breadth of knowledge, directness and zeal. In every talk, she'll always have a question to ask the speaker. She taught me theory of computation and proof complexity, gave detailed feedback on assignments and tried to make sure that we understand mistakes in our solutions

and take away essential ideas. I thank Meena for her attention. I have also learned much more from her during coffee breaks and lunch breaks.

I would also like to acknowledge my previous supervisors Rajesh Kannan (IIT Hyderabad) and Ranveer Singh (IIT Indore) who gave me an opportunity to work on research problems for a year each; it led me to decide that I could pursue the doctoral program in theoretical computer science at IMSc. And, I cannot thank IMSc enough for making my stay comfortable here, for providing ample access to facilities, for the supportive research environment, and for the fellowship (no fees). I was able to locate almost all the references through the IMSc library, and if a certain book is not there, one could always request the library to purchase it and get it within a couple of weeks.

After I joined IISER Pune in 2016 for undergraduate studies, my father would proudly tell everyone, 'My son is a researcher!' (sometimes, 'a scientist!') I was never comfortable with those words until very recently. He passed away in 2021. I wish I could tell him that I am finally really a researcher. He would have been very happy seeing me where I am now. This thesis is dedicated to him and my patient mother, without them I would not have had the drive to do something meaningful. Thanks to my friends at IMSc including Anuran, Ishitva, Kushal, Purna, Ravi and Satya, without their company exploring around would not have been so exciting. With Purna and Satya, I have had many academic discussions; they also attended mocks of the public talks I gave which helped me prepare. Thanks to Nishad for his occasional check-ins. Without my friends and professors, I would not have been able to build up the little bit of confidence that I have. A special thanks to my friend Purna, who is now on the other side of the world, for her support, cheerful presence and insightful conversations, she helped me appreciate beauty in even little things.

Contents

Abstract i

Dedication ii

Acknowledgements iii

1 The τ-Conjecture and its History 1

2 Consequences of the τ-Conjecture 10

3 Descartes' Rule of Signs 21

4 Rolle's Theorem 26

5 Descartes System 30

6 Wronskian Identities 35

7 Wronskian and Linear Dependence 41

8 Zeros of the Sum of Two Functions 48

9 Zeros of the Sum of Multiple Functions 54

10 Upper Bound Towards Real τ-Conjecture 59

11 Multiplicities, Complex Zeros Cannot Be Ignored 64

12 Distribution of Zeros in the Complex Plane 71

13 Angular Discrepancy 79

14 Variants of Real τ-Conjecture 85

Conclusion and Future Directions 90

Bibliography 91

Chapter 1

The τ-Conjecture and its History

The birth of algebraic complexity theory can be credited to the two questions that Scholz (1937) and Ostrowski (1954) raised respectively (as in Strassen [82]), and we shall begin by discussing them both.

Polynomial Evaluation and Straight Line Programs

First, let us consider the basic problem of polynomial evaluation: Given a univariate polynomial $f(x) = \sum_{i=0}^{n} a_i x^i$ with the coefficients $a_i \in \mathbb{F}$ from some field $\mathbb{F}$, what is the minimum number of additions and multiplications required to compute $f(\alpha)$ for some $\alpha \in \mathbb{F}$? The trivial way is to first compute all the powers $\alpha^2, \ldots, \alpha^n$, then compute the monomials $a_1\alpha, a_2\alpha^2, \ldots, a_n\alpha^n$, and then add up all these monomials along with a_0. This incurs $2n-1$ multiplications and n additions. Can we do better? Here is another way: first express the polynomial as

$$f(x) = a_0 + x(a_1 + \cdots + x\left(a_{n-2} + x(a_{n-1} + xa_n)\right),$$

and then repeatedly evaluate the linear factors by substituting α from the right to the left. This method shows n additions and n multiplications suffice. Although this method is known as Horner's method (1819) [41], Horner himself credits this method to Lagrange (1736-1813), while Ostrowski observes that it was known to Newton (1723) as well. Now the question is "Is Horner's method optimal?", and by that we mean "Is there a polynomial for which every method requires at least n additions or n multiplications?" Ostrowski (1954) [64] noticed optimality with respect to addition is straightforward — computing $f(1) = a_0 + \cdots + a_n$ requires at least n additions, for f with all nonzero coefficients — and then raised the question of

optimality with respect to multiplication[1]. Pan (1966) [65] showed, after a decade, that Horner's method is optimal with respect to multiplication as well (also see Section 6.1 in Bürgisser, Clausen, Shokrollahicite (1996) [19] for a proof).

What is interesting is that a method of evaluating a polynomial like Horner's can also be seen as a method/algorithm/program to compute a polynomial using the indeterminate x and the scalars from the field. This can be formalized by a computational model known as the straight line program. We restrict to univariate polynomials in $\mathbb{F}[x]$, where $\mathbb{F}$ is either a ring or field. We denote by $\circ$ any of the arithmetic operation in $\{+, -, *, \div\}$. Division is used in the case $a \circ b$ and $b \neq 0$, and it may also be disallowed. We define a *straight line program* (SLP) computing a univariate polynomial $f \in \mathbb{F}[x]$ to be a sequence of polynomials $(u_0, u_1, \ldots, u_{l+1})$ in $\mathbb{F}[x]$ where each u_k is either a scalar from $\mathbb{F}$ or the indeterminate x or obtained as $u_k = u_i \circ u_j$ for some $0 \leq i, j \leq k-1$, and finally $u_{l+1} = f$. Here, u_{l+1} may be in a different form than f, e.g. $x^2 + 2x + 1$ can also be expressed as $(x+1)^2$, but they must be the same coefficient-wise. We shall refer to l as the length of the program; it is also the number of arithmetic operations involved. In this model of computation, no recursion or conditional steps are involved. This formalization first seems to have appeared in Ostrowski (1954) [64], and also in Pan (1966) [65] who calls it a 'scheme'. It has also been referred to as *computation sequence* or simply a *program*.

We can now introduce complexity measures for a polynomial: we define *arithmetic complexity* $L(f)$ to be the minimum length of a straight line program computing f. One detail to note in the definition of the model is that the scalars are freely available, e.g. the number $n!$ does not need to be computed and its complexity is not considered in $L(f)$[2]. Initial interest has been in the additive and the multiplicative complexity of computing polynomials. We define *multiplicative complexity* $\mu(f)$ as the minimum number of multiplications and divisions used in the program[3]. Similarly, we define *additive complexity* $\rho(f)$ to be the minimum number of additions and subtractions used in the program. By Horner's method, we have the inequalities

$$\mu(f) \leq n, \qquad \rho(f) \leq n,$$

which we know are realized with equality respectively. Before we talk about lower

[1]Belaga (1961) [4] shows there are polynomials for which n additions are required even with 'preconditioning' of the coefficients (for more details see Chapter 5 of Bürgisser, Clausen, Shokrollahicite (1996) [19]).

[2]We shall come back to this detail later on.

[3]The *nonscalar complexity* or *Ostrowski measure* is the multiplicative complexity ignoring the scalar multiplications (Heintz (1987) [36]), which we shall not discuss here.

bounds on these complexity measures, let us discuss the second motivating problem that Scholz (1937) considered.

Even before Ostrowski, the following problem was considered: What is the most efficient way to compute x^n using just multiplications starting from x, where n is a positive integer? Since we know that $x^{m+n} = x^m x^n$, this problem is the same as computing the integer n starting from 1 using just the addition operation. We define *addition chain* computing n as the sequence $u_0, u_1, \ldots, u_k$ where $u_0 = 1$, $u_1 = 2$, $u_k = n$ and $u_i = u_j + u_l$ for $j, l < i$, and denote by $l(n)$ as the minimum number of additions required by an addition chain to compute n. Observe that this computation sequence is simply a straight line program with only the addition operation and the scalar 1. According to Knuth (1969) [44], the problem of determining $l(n)$ was first raised by Dellac (1894) [23]. A trivial upper bound can be obtained as follows. First write n in binary where this binary expansion has $\lfloor \log_2 n \rfloor$ bits and among them say $\lambda(n)$ many are 1's. Compute the powers $1, 2, 2^2, \ldots, 2^{\lfloor \log_2 n \rfloor}$ using repeated additions, and then add only the powers for which the corresponding bit in the binary expansion is nonzero. This gives us n. Thus we have

$$l(n) \leq \lfloor \log_2 n \rfloor + \lambda(n) - 1. \tag{1.1}$$

Now some of the powers that we computed were not added to get n, so this upper bound can also be improved. But let us consider the integer $2^m - 1$ whose binary expansion is simply 1 repeated m-times, i.e. $\lambda(2^m - 1) = m$. Then we have

$$l(2^m - 1) \leq 2m - 2,$$

and it may appear that we need to compute $2m - 2$ many powers of 2. But Scholz (1937) [74], who also introduced the term 'addition chain', conjectured the following.

Conjecture 1.1 (Scholz Conjecture)**.** $l(2^m - 1) \leq l(m) + m - 1$.

This conjecture is still not resolved, although it has been verified to be true for all m less than a certain large number. We saw that the straight line program model seems to be motivated by the algorithmic problem of polynomial evaluation. For the addition chain model, the corresponding algorithmic problem may be the following: Given an integer n and a number a, what is the most efficient way to evaluate x^n at a using only multiplications? For a more detailed treatment, see Knuth (1969) [44] and for a current update check the webpage `www.additionchains.com`. With this history of straight line programs, we shall now discuss the complexity of computing both polynomials and integers.

Bounds on Complexity Measures

Continuing with the lower bound discussion from the previous page, let us note that the degree n of a polynomial f can at most double after every multiplication step, and so $n \leq 2^{\mu(f)}$ at the end of the program, and therefore we get a lower bound on the multiplicative complexity

$$\log n \leq \mu(f). \tag{1.2}$$

Strassen (1973) [79], according to Borodin and Cook (1976) [12], was the first to initiate the study of lower bounds on multiplicative complexity $\mu(f)$ using methods from algebraic geometry, in particular, in terms of the number of common zeros of system of equations (See also Section 3, Schönhage (1976) [75]). As for the lower bound on the additive complexity $\rho(f)$, Strassen (1973) also observed that the degree does not increase after an addition or a subtraction in the program, so we may not have lower bounds in terms of the degree. But since we know that the number of certain zeros, e.g. real or integer zeros, of the polynomial in construction may also increase as the degree increases, can we then give a lower bound on the additive complexity in terms of the number of those zeros? E.g., considering real polynomials, and denoting by $N_f^\circ\mathbb{R}$ the number of distinct real zeros of f, Equation 1.2 gives us[4]

$$\log N_f^\circ\mathbb{R} \leq \log n \leq \mu(f).$$

Borodin and Cook (1976) [12] hoped to prove $\log N_f^\circ\mathbb{R} \leq \rho(f)$, but instead showed existence of a polynomial f such that $\rho(f) \leq \log_3(N_f^\circ\mathbb{R})$ (See Section 4, FACT 2, [12]). Van de Wiele (1978) [86] had noticed that the inequality $\rho(f) \leq \log_3(N_f^\circ\mathbb{R})$ also holds for the Chebyshev polynomial C_n of degree n since all its zeros are real and the additive complexity $\rho(f)$ was shown to be at most $\log_3 n$ (See Proposition 1.6 for proof). This means that a lower bound for $\rho(f)$ in terms of (or polynomial function in) $\log N_f^\circ\mathbb{R}$ may not be useful either, although Risler (1985) [70] later proved the exact relation

$$\sqrt{\log N_f^\circ\mathbb{R}} \leq c\rho(f) \tag{1.3}$$

for some universal $c > 0$, and all real polynomials f with operations over $\mathbb{R}$.

We can observe that Risler's inequality is almost realized by the Chebyshev polynomials in the sense that we get $\sqrt{\log(N_f^\circ\mathbb{R})} \leq c\log_3(N_f^\circ\mathbb{R})$. Here, $\log_3(N_f^\circ\mathbb{R})$ is polynomially upper bounded by $\sqrt{\log(N_f^\circ\mathbb{R})}$. Risler's result is interesting in itself:

[4]Here, we use $\circ$ to indicate that only the distinct zeros are counted.

It gives an upper bound on the number of distinct real zeros of real polynomials, and the upper bound is independent of the size of coefficients since in our model we have assumed that the scalars are freely available[5].

At the end of their paper, Borodin and Cook (1976) asked whether counting the complex or the integer zeros may help for the additive complexity. For the multiplicative complexity, we obviously have $\log N_f^\circ\mathbb{C} \leq \mu(f)$ from Equation 1.2. But there does not seem to be a direct relationship for the additive complexity with complex zeros (See Van de Wiele (1978) [86]). E.g. consider the polynomials $x^n - 1$ and $(x-1)^n$ both of which have the same additive complexity 1, but the former has n distinct zeros, and the latter has only one. So let us focus on integer zeros instead. Equation 1.3 and Equation 1.2 easily imply

$$\log N_f^\circ\mathbb{Z} \leq c\rho(f)^2, \qquad \log N_f^\circ\mathbb{Z} \leq \mu(f). \tag{1.4}$$

To go about improving any of these lower bounds, let us consider an extremal example, a polynomial with a very large number of distinct integer zeros, e.g. the Pochhammer-Wilkinson polynomial[6]

$$PW_n = \prod_{k=1}^{n}(x-k)$$

for which we have $N_{PW_n}^\circ\mathbb{Z} = n$, $\rho(PW_n) \leq n$ and $\mu(PW_n) \leq n-1$. The additive complexity and the multiplicative complexity are very close for this extremal example, and this seems to suggest that we could consider the total complexity $L(f)$ instead of $\rho(f)$ and $\mu(f)$ separately when considering integer zeros. Again by the degree argument and Horner's method, we have

$$\log N_f^\circ\mathbb{Z} \leq \log n \leq L(f) = \mathcal{O}(n).$$

Now, an in Heintz (1987) [36] or Bürgisser (2000) [16] (Section 8.3), a univariate polynomial sequence (f_n) with $\deg(f_n) = n$ is called *easy to compute* if $L(f_n) = (\log n)^{\mathcal{O}(1)}$, and *hard to compute* otherwise. For example, the sequences (x^n) and $(\sum_{i=0}^n x^i)$ are easy to compute, the latter is easy-to-compute

[5]We also have for a polynomial f with k monomials the bound $\log N_f^\circ\mathbb{R} \leq \log(2k-1)$ by Descartes' rule (See Chapter 3). But here, we shall restrict to investigating connections between the zeros and the complexity measures.

[6]Pochhammer introduced the symbol $(x)_n$ in 1870 which he used to denote $\binom{x}{n}$. But this symbol is also used either to denote the falling factorial $\prod_{i=0}^{n-1}(x-i)$ or the rising factorial $\prod_{i=0}^{n-1}(x+i)$. Later Wilkinson (1963) studied these polynomials in the context of numerical analysis, and the sensitivity of zeros to the perturbation of its coefficients.

because $\sum_{i=0}^{n} x^i = \frac{x^{n+1}-1}{x-1}$. Heintz and Morgenstern (1993) [37] asked to show that Pochhammer-Wilkinson polynomials PW_n are hard to compute by division-free SLP's. A closely related polynomial family $\prod_{k=1}^{n}(x - \sqrt{k})$ was been shown to be hard to compute in the same paper (Theorem 18 [37]) using methods from algebraic geometry. Here is an interesting relation between these two families:

$$PW_n(x^2) = \left(\prod_{k=1}^{n}(x - \sqrt{k})\right)\left(\prod_{k=1}^{n}(x + \sqrt{k})\right).$$

Observe that the zeros of $\prod_{k=1}^{n}(x - \sqrt{k})$ are not all integers but reals or algebraic numbers, and on the other hand, the zeros of $PW_n = \prod_{k=1}^{n}(x-k)$ are integers. This seems to suggest that it might be easier to deal with real zeros than integer zeros. Along with this intuition, to summarize this discussion, we have also argued that it makes sense to study the relation between number of integers zeros and the total arithmetic complexity instead of multiplicative and additive complexity individually.

τ-Complexity

Shub and Smale (1995) [76] considered the problem of computing integer polynomials using division-free, scalar-free SLPs over $\mathbb{Z}[x]$. By scalar-free we mean that there will be a cost to computing integers other than 1. We could also disallow subtraction and say that scalars are allowed only from the set $\{-1, 0, 1\}$, but here we shall allow it. It makes sense to consider the scalar-free model for integer polynomials because integers have finite representation and the cost of computing them is also interesting to study. On the other hand, over reals or complex numbers we can't use the scalar-free model. In this restricted model, an integer polynomial $f \in \mathbb{Z}[x]$ is computed by the sequence $(u_0, u_1, \ldots, u_{l+1})$ in $\mathbb{Z}[x]$ where $u_0 = 1$, $u_1 = x$ and $u_k = u_i \circ u_j$ for $0 \leq i, j \leq k-1$ and $\circ \in \{+, -, *\}$. We define *τ-complexity* $\tau(f)$ as the number of $+, -, *$ operations involved in this computation sequence. If n denotes the degree of f, the Horner's method gives an $\mathcal{O}(n)$ upper bound on $\tau(f)$ but with an additional cost of computing each of the coefficients. We denote by $\tau(m)$ the τ-complexity of computing an integer m; the indeterminate x need not be used in the SLP while computing computing m. We always have $\tau(m) \leq 2 \log m$, roughly, from Equation 1.1. The *height* of a polynomial f is defined as $H(f) := \max_i |a_i|$, i.e., the maximum absolute value of its coefficients. Then,

$$\tau(f) = \mathcal{O}(n \log H(f)).$$

The upper bound was improved by Moreira (1997) [63] (Theorem 3) to $\mathcal{O}(\frac{n \log H(f)}{\log(n \log H(f))})$, but it still grows with $H(f)$. Essentially, the coefficients can be arbitrarily large, and therefore the τ-complexity, even for polynomials with a fixed degree. We shall discuss upper bound on the τ-complexity of integers later. As for the lower bound, we have

$$\log N_f^\circ \mathbb{Z} \leq \log n \leq L(f) \leq \tau(f),$$

and in particular $N_f^\circ \mathbb{Z} \leq 2^{\tau(f)}$. Shub and Smale (1995) [76] conjecture that the number of distinct integer zeros $N_f^\circ \mathbb{Z}$ of an integer polynomial built using (division-free, scalar-free) SLP cannot be very large, and it must be polynomial in the τ-complexity. This is the τ-conjecture. More precisely,

Conjecture 1.2 (τ-Conjecture)**.** *For every nonzero integer polynomial $f \in \mathbb{Z}[x]$, we have $N_f^\circ \mathbb{Z} \leq (1 + \tau(f))^c$ for some universal constant $c > 0$.*

We state the upper bound in this way instead of $a\tau(f)^c$ in order to include the case $f = x$ where $N_f^\circ \mathbb{Z} = 1$ and $\tau(f) = 0$. Let us discuss again the hard-to-compute polynomial candidate $PW_n = \prod_{i=1}^n (x - i)$ for which we have $N_{PW_n}^\circ \mathbb{Z} = n$. We may also need to compute some integers. A naive way of computing is given by the following sequence

$$1, x, (x-1), (x-2), \prod_{i=1}^{2}(x-i), (x-3), \ldots, (x-n), \prod_{i=1}^{n}(x-i).$$

It has length $2n-1$ since $n-1$ multiplications and n subtractions are involved, and therefore we have $\tau(PW_n) \leq 2n - 1$. Now if the τ-conjecture is true, then it means $n \leq (2n)^c$ for some $c > 0$, and as $n \to \infty$, it forces $c \geq 1$. Thus the τ-conjecture is false for $c < 1$. A basic question arises: Is the τ-conjecture true or false for $c = 1$? This is also an open problem. To falsify the τ-conjecture for $c = 1$, it suffices to show that $\tau(PW_n) < 2n - 1$. It also suffices to show that PW_n are easy to compute with respect to the τ-complexity, i.e. $\tau(PW_n) = (\log n)^{\mathcal{O}(1)}$. But even the weaker claim $L(PW_n) = (\log n)^{\mathcal{O}(1)}$ is yet to be shown.

Conjecture 1.3. *Pochhammer-Wilkinson polynomials are hard to compute with respect to the τ-complexity (avoids divisions, scalars not free) or the arithmetic complexity (allows divisions, scalars free).*

One more comment. We cannot replace integer zeros with real zeros in the conjecture, i.e. the claim $N_f^\circ \mathbb{R} \leq (1 + \tau(f))^c$ does not hold. Chebyshev polynomials provide a counterexample. All of their zeros are real (at most one integer zero),

but the τ-complexity is $\mathcal{O}(\log n)$ (See Proposition 1.6 for proof). We can say that for Chebyshev polynomials the number of distinct real zeros increases exponentially in the τ-complexity. *Does the number of distinct integer zeros of the Pochhammer-Wilkinson polynomial increase exponentially in the τ-complexity?*

There is also a τ-conjecture for integers that is closely related. We mentioned earlier the trivial upper bound $\tau(m) \leq 2 \log m$ for an integer m. For the lower bound, let $k = \tau(m)$. Then, the SLP must have computed k different integers in the process. In the worst case, every next integer may be obtained by the multiplication of the largest computed integer with itself. Thus $m \leq 2^{2^k}$ which means that

$$\log \log m \leq \tau(m),$$

and by taking $m = 2^{2^k}$ the inequality is tight. This lower bound is Proposition 1(b) in De Melo and Wellington (1996) [22]. Similar to the case of polynomials, we say that a sequence of integers (a_n) is *easy to compute* if $\tau(a_n) \leq (\log n)^c$ for all $n \geq 3$ and a universal constant $c > 0$, and *hard to compute* otherwise. The coefficient sequence in the Pochhammer-Wilkinson polynomial $\prod_{i=1}^{n}(x - i)$ is $(n!)$ for which the trivial upper bound gives $\tau(n!) \leq 2n \log n$.

Conjecture 1.4. *The sequence $(n!)$ is hard to compute.*

If this conjecture is false, then factoring integers can be done in polynomial time (See Strassen (1976) [81] and pg. 126 of Blum, Cucker, Shub, Smale (1997) [8]). We say that a sequence (a_n) is *ultimately easy to compute* if there are nonzero integers m_n such that $(a_n m_n)$ is easy to compute, and *ultimately hard to compute* otherwise.

Conjecture 1.5. *The sequence $(n!)$ is ultimately hard to compute.*

Next, we prove claims about Chebyshev polynomials that were mentioned earlier.

The Chebyshev Polynomials

Proposition 1.6. *The Chebyshev polynomials have all distinct real zeros, additive complexity at most $\log_3 n$ (ignoring computing the scalars), and τ-complexity at most $1 + 3 \log_2 n$ (considering computing the scalars), where n denotes the degree.*

Proof. We consider the Chebyshev polynomials (C_n) of the first kind: they are defined as $C_n(x) = \cos(n\theta)$ where $x = \cos(\theta)$. To simplify them, we observe that $\cos(n\theta) = \Re((\cos(\theta) + i \sin(\theta))^n)$. Using binomial expansion, we obtain a more explicit expression

$$C_n(x) = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2k} x^{n-2k}(x^2 - 1)^k.$$

It is now clear that $C_n(x)$ has degree n in x. Also because $x = \cos(\theta)$, any zero of $C_n(x)$ must lie in the interval $[-1, 1]$. Next, $C_n(x) = 0$ iff $\cos(n\theta) = 0$, so can we can find the set of zeros of $C_n(x)$ as

$$x = \cos\left(\frac{2l-1}{n}\frac{\pi}{2}\right) \qquad \text{for } l = 1, 2, \ldots.$$

We must also assume $0 \leq \frac{2l-1}{n}\frac{\pi}{2} \leq \pi$ which implies that l is at most n. Thus we have found all n zeros of $C_n(x)$. All of them are distinct and real, and has an integer zero only in the case $l = \frac{n+1}{2}$ is also an integer. Therefore, $C_n(x)$ has all irrational zeros in the case n is even, and has all irrational zeros except one which is an integer in the case n is odd.

If we use the expression for $C_n(x)$ that we obtained just now, then it has large coefficients, and so computing it will be costly. A recurrence relation might help. For example, using the identity $\cos(2y) = 2\cos^2(y) - 1$, we can get $C_{2n}(x) = 2C_n^2(x) - 1$. From this additive complexity comes out to be at most $\log_2 n$ (assuming scalars dont need to be computed), and the τ-complexity at most $1 + 3\log_2 n$ (considering the cost of computing scalars). We have not obtained the claimed additive complexity $\log_3 n$. We shall try the next identity $\cos(3y) = 4\cos^3(y) - 3\cos(y)$, using which we can get $C_{3n}(x) = C_n(x)(4C_n^2(x) - 3)$, and now this will lead to additive complexity at most $\log_3 n$ (assuming scalars dont need to be computed), and the τ-complexity at most $3 + 4\log_3 n$ (considering the cost of computing scalars). □

All three conjectures (1.3, 1.4, 1.5) have a major consequences in (algebraic) complexity theory, and we shall discuss them in Chapter 2 after introducing some basic terminologies. The detailed treatment and the history of many of the ideas of this chapter may also be found in Strassen (1990) [82] and Bürgisser, Clausen, Shokrollahicite (1996) [19].

Chapter 2

Consequences of the τ-Conjecture

Hilbert Nullstellensatz

In the last chapter, we discussed the number of real or complex zeros of polynomials. But how does one find a zero? For complex polynomials as well, i.e. polynomials with complex coefficients, there is Newton's method. Given a complex polynomial $f(x)$ and a point x_0 sufficiently close to the actual zero x^* such that $f(x^*) = 0$, we iteratively compute the point $x_n = g(x_{n-1})$ where $g(y) = y - \frac{f(y)}{f'(y)}$, and x_n would converge to x^*. Here, $f'(y)$ denotes the formal derivative of $f(y)$. This algorithm takes an input a complex polynomial f of degree d given as a vector of coefficients in $\mathbb{C}^{d+1}$, and for some small ϵ and chosen point x_0 as above, executes the following steps:

1. $x \leftarrow x_0$,
2. $x \leftarrow g(x)$,
3. If $|f(x)| \geq \epsilon$, then go to step 1.
4. Else output x.

Practical challenges aside, this method solves a search problem, and finds a complex number sufficiently close to the actual zero. What would be a corresponding decision problem? The problem "$\exists x \in \mathbb{C} : \ f(x) = 0$?" is trivial if f is a nonzero univariate polynomial; the reason is the fundamental theorem of algebra. The multivariate case is also trivial by extension. The meaningful decision problem would then be the following:

> **Hilbert Nullstellensatz over $\mathbb{C}$ (HN/$\mathbb{C}$).** Do the given m-variate polynomials $f_1, \ldots, f_k$ from $\mathbb{C}[x_1, \ldots, x_m]$ have a common zero in $\mathbb{C}^m$?

A brute-force approach to decide this problem by searching for a witness to YES answer does not work, because the polynomial system may have infinitely many common solutions in $\mathbb{C}^m$ for which polynomial evaluations will need to be computed. What are the conditions for a family of polynomials to (not) have a common zero? Clearly, if there exists $g_1, \ldots, g_k$ such that $\sum_{i=1}^{k} g_i f_i = 1$, then $f_1, \ldots, f_k$ do not have a common zeros. Hilbert (1893) [39] showed that the converse also holds.

Theorem 2.1. *HN/$\mathbb{C}$ has a NO answer if and only if there exists polynomials $g_1, \ldots, g_k$ in $\mathbb{C}[x_1, \ldots, x_m]$ such that $\sum_{i=1}^{k} g_i f_i = 1$.*

Now we may search for g_i's, which is a witness for a NO answer, if only we also know an upper bound on their degrees. Hermann (1926) [38] gave the upper bound $\deg g_i \leq D^{2^m}$ where $D = \max\{3, \deg f_1, \ldots, \deg f_k\}$. Treating the coefficients of g_i's as variables, one can solve $\sum_{i=1}^{k} g_i f_i = 1$ using system of linear equations, and therefore decide HN/$\mathbb{C}$ in a finite number of operations. But again, as in the Newton's method, solving HN/$\mathbb{C}$ on Turing machines also has practical considerations since Turing machines decide languages that are subsets of $\mathbb{Z}_2^* = \cup_{i=0}^{\infty} \mathbb{Z}_2^i$, and an input to HN/$\mathbb{C}$ would be the complex coefficients of f_i's. Clearly, Turing machines is not an appropriate model of computation for HN/$\mathbb{C}$ since it cannot encode complex numbers exactly.

Before we discuss Hilbert Nullstellensatz over $\mathbb{C}$ further, let us note that this problem seems to have a similar flavour as that of the Boolean Satisfiabily Problem (SAT) for which an input is the set of k clauses each of them having distinct literals from a fixed set of m variables and their negations, and the question is whether there is an assignment in $\{0,1\}^m$ to the variables such that it satisfies all the clauses. Let us consider the following problem.

> **Hilbert Nullstellensatz over $\mathbb{Z}_2$ (HN/$\mathbb{Z}_2$).** Do the given m-variate polynomials $f_1, \ldots, f_k$ from $\mathbb{Z}_2[x_1, \ldots, x_m]$ have a common zero in $\mathbb{Z}_2^m$?

Next, we study the complexity of this problem.

Proposition 2.2. *HN/$\mathbb{Z}_2$ is 'intractable' (i.e. HN/$\mathbb{Z}_2 \notin$ P) if and only if* P $\neq$ NP.

Proof. We shall prove that HN/$\mathbb{Z}_2$ is NP-complete. First, we reduce 3-SAT to it. Consider a 3-SAT instance. Let $x_1, \ldots, x_m$ denote the variables, and let $C_1, \ldots, C_k$ denote the clauses. Consider $C = l_1 \vee l_2 \vee l_3$, one of the k clauses, where $l_i \in \{x_1, \ldots, x_m\} \cup \{\neg x_1, \ldots, \neg x_m\}$. We encode C using the multivariate polynomial $f_C \in \mathbb{Z}_2[x_1, \ldots, x_m]$ defined as $f_C(x_1, \ldots, x_m) := h_1 h_2 h_3$, where $h_i := 1 - x_i$ if $l_i = x_i$, and $h_i := x_i$ if $l_i = \neg x_i$. The clause C is satisfied by an assignment $\sigma \in \{0,1\}^m$ if and only if $f_C(\sigma) = 0$. Now f_C is a multilinear polynomial of total degree 3 and at

most 8 monomials. Thus each clause may be encoded as a polynomial in constant time, and we can construct the family $f_{C_1}, \ldots, f_{C_k}$, which is an instance to HN/$\mathbb{Z}_2$, in time linear in k. We know that 3-SAT is NP-hard, and therefore HN/$\mathbb{Z}_2$ is also NP-hard. Now to show that HN/$\mathbb{Z}_2$ is also in NP, consider a candidate certificate $\sigma \in \mathbb{Z}_2^m$ of the YES answer. Suppose that $t_i = \deg(f_i)$ for $i = 1, \ldots, k$, and f_i's are given as a vector of coefficients. Then each f_i has $S(f_i) := \binom{m+t_i-1}{t_i}$ many coefficients (or $\binom{n}{t_i}$ if assumed multilinear[1]). Now what is the cost of testing whether f_i vanishes at σ? Not more than $\mathcal{O}(S(f_i))$. So the instance can be solved in time polynomial in the input size. Thus, HN/$\mathbb{Z}_2$ is NP-complete. □

The algorithm that we discussed earlier for solving HN/$\mathbb{C}$ takes an input from $\mathbb{C}^* = \cup_{i=0}^{\infty} \mathbb{C}^i$, and involves basic arithmetic operations $+, -, *, \div$ as well as branching over equality (e.g. on "$f_i(z) = 0$?")[2]. Blum, Shub and Smale (1989) [9] introduced a model of computation, now known as a BSS-machine, that supports such computations over $\mathbb{C}$, and also generally over any field or ring R, and on which an algebraic algorithm may be executed. For details on the BSS model, we refer to [9] or the book by Blum, Cucker, Shub and Smale (1997) [8]; the expository article by Blum (2004) [7] may also be helpful. Here, we discuss briefly only the machine over $\mathbb{C}$.

Essentially, a *BSS-machine M over* $\mathbb{C}$ is a directed connected graph with *input, computation, branch, shift*, and *output* nodes along with an infinite tape. The input nodes have no in-degree and they can write the input on the tape. The computation nodes compute a polynomial or a rational function and can write the result on the tape. The branch nodes have out-degree two, and the branching is over equality (in the case of $\mathbb{C}$). The infinite tape has a marker and the machine's view at any point is a fixed number of contiguous cells. The shift nodes can move this marker one cell to the left or the right. The output node outputs the contents written on the tape. The machine computes a function $f_M : \mathbb{C}^\infty \to \mathbb{C}^\infty$. We consider unit cost and assume that each cell of the tape holds a complex number. For an input $x \in \mathbb{C}^n$, we define *input size*[3] to be size$(x) = n$, and for a machine M, we define *computation length* $T_M(x)$ to be the number of nodes traversed from the input node to the output node when the input is x. The quantity $T_M(x)$ roughly reflects the number of arithmetic operations involved. The BSS-machine over $\mathbb{C}$ may be denoted by $(\mathbb{C}, =, \mathbb{1})$, where the last entry denotes that we consider unit cost. The classical Turing machine is simply $(\mathbb{Z}_2, =, \mathbb{1})$.

[1] To check for a common zero in $\mathbb{Z}_2^m$, we can substitute $x_j^2 = x_j$ for each j in each f_i, and then f_i's become multilinear.

[2] If the field is ordered, e.g. $\mathbb{R}$, then the branching may also be on inequality.

[3] The input size may be defined alternatively in the case of machines over e.g. $\mathbb{Z}$ or $\mathbb{Q}$ by taking into account the bit size.

We say that a language $L \subseteq \mathbb{C}^\infty$ is in the complexity class $\mathsf{P}_\mathbb{C}$ if and only if there is a machine M over $\mathbb{C}$ computing the characteristic function $\mathbb{1}_L$ and on all valid instances x the computation length $T_M(x)$ is polynomially bounded by size(x). Here, by allowing $T_M(x)$ to be just finite, we obtain the definition of *decidability*. Due to the bounds by Hermann, we saw that HN/$\mathbb{C}$ is decidable. We avoid defining the class $\mathsf{NP}_\mathbb{C}$ or the notion of reductions here, but mention that HN/$\mathbb{C}$ is shown to be $\mathsf{NP}_\mathbb{C}$-complete (See Chapter 5, BCSS (1997) [8]). Then HN/$\mathbb{C}$ is intractable (i.e. HN/$\mathbb{C} \notin \mathsf{P}_\mathbb{C}$) if and only if $\mathsf{P}_\mathbb{C} \neq \mathsf{NP}_\mathbb{C}$. Shub and Smale (1995) [76] discovered that the intractability of HN/$\mathbb{C}$ has a close relation with the τ-conjecture and the computation of integers.

Theorem 2.3 (Theorem 3, pg. 126 BCSS [8]). *If the τ-conjecture (1.2) is true, then HN/$\mathbb{C}$ is intractable.*

Theorem 2.4 (Theorem 2, pg. 126 BCSS [8]). *If the sequence $(n!)$ is ultimately hard to compute (Conjecture 1.5), then HN/$\mathbb{C}$ is intractable.*

Kollár (1988) [51] shows that Theorem 2.1 may be generalized to hold over algebraically closed fields R with bounded degree g_i's, and therefore HN/R is decidable for such fields. There are also transfer results between certain fields: $\mathsf{P}_\mathbb{C} \neq \mathsf{NP}_\mathbb{C}$ if and only if $\mathsf{P}_R \neq \mathsf{NP}_R$ for any algebraically closed field R of characteristic zero (Theorem 1, pg. 126 BCSS [8]). Therefore, the conclusion of both the results is equivalent to the intractability of HN/$\overline{\mathbb{Q}}$ and equivalently the separation $\mathsf{P}_{\overline{\mathbb{Q}}} \neq \mathsf{NP}_{\overline{\mathbb{Q}}}$, where $\overline{\mathbb{Q}}$ is the field of algebraic numbers (the set of rationals along with the numbers that are realized as zeros of rational polynomials), and unit cost for arithmetic operations is also assumed for machines over $\overline{\mathbb{Q}}$. Note that $\overline{\mathbb{Q}}$ is also the algebraic closure of the set of integers $\mathbb{Z}$ for which the τ-conjecture was stated. Since $\mathbb{Z}_2$ is not algebraically closed and has characteristic 2, it is not yet clear how the hypothesis $\mathsf{P}_{\overline{\mathbb{Q}}} \neq \mathsf{NP}_{\overline{\mathbb{Q}}}$ is related to the classical $\mathsf{P} \neq \mathsf{NP}$. Although Poizat (1995) [67] showed $\mathsf{P}_R \neq \mathsf{NP}_R$ holds for any infinite field R that is not algebraically closed (Theorem 9, Chapter 7 [8]). Now over infinite fields the only problem left to address is whether $\mathsf{P}_{\overline{\mathbb{Q}}} \neq \mathsf{NP}_{\overline{\mathbb{Q}}}$ holds. The τ-conjecture was included in the Smale's list of 'mathematical problems for the next century' (1998) [78].

Malajovich (2001) [57] considered a different model of computation over algebraic numbers where the length of the input not only depends on the dimension of the vector but also the height of the algebraic numbers involved, and the computation length also accounts for the height in the arithmetic operations. The braching is maintained over equality. In this model $(\overline{\mathbb{Q}}, =, \text{height})$, the separation $\mathsf{P} \neq \mathsf{NP}$ was proved (Theorem B [57]).

It is also interesting to note that over integers HN/$\mathbb{Z}$ is the Hilbert's Tenth Problem (1900) [40], and it was shown to be undecidable in 1970 due to the works of Davis, Matiyasevich, Putnam and Robinson [60].

Permanent

While Turing machines decides languages over $\mathbb{Z}_2$, the BSS-model seems to have grown out of the need to decide languages over an arbitrary ring or a field. There is another point of view that leads to a different generalization: a Turing machine computes a boolean function $f_n : \mathbb{Z}_2^n \to \mathbb{Z}_2$ on an input of length n when deciding whether that input is in the language $L \subseteq \mathbb{Z}_2^*$. We may write $L = \cup_{n=1}^{\infty} f_n^{-1}(1)$. A boolean function may be interpolated to a polynomial as $f_n(\mathbf{x}) = \sum_{a \in \mathbb{Z}_2^n} f(a)\mathbb{1}_{\mathbf{x}=a}$, where $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbb{1}_{\mathbf{x}=a}$ takes value 1 if $\mathbf{x} = a$ and 0 otherwise. The indicator function can be described by the monomial $\mathbb{1}_{\mathbf{x}=a} = \prod_{a_i=1} x_i \prod_{a_i=0}(1-x_i)$, and it makes sure that $\mathbb{1}_{b=a} = 0$ for all $b \in \mathbb{Z}_2^n \backslash a$. Here, the domain of the function is $\mathbb{Z}_2^n$, and in general, we may consider the problem of computing the polynomials from $\mathbb{F}[x_1, \ldots, x_n]$ where $\mathbb{F}$ is any field different than $\mathbb{Z}_2$.

For decision problems over $\mathbb{Z}_2$, we have the complexity classes P and NP, and for functional/counting problems, i.e., those computing $f_n : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ (equivalently $f_n : \mathbb{Z}_2^n \to \mathbb{N}$), we have FP and $\#\mathsf{P}$ respectively (See Arora-Barak [3] for definitions). Consider the counting problem: What is the number of perfect matchings in a bipartite graph? This problem is equivalent to computing the *permanent* of the biadjacency matrix of this bipartite graph. If $A = [a_{i,j}]$ denotes a $n \times n$ matrix, then its permanent is given by $\mathrm{per}(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} a_{i,\sigma(i)}$, where S_n is the set of all permutations of the set $\{1, \ldots, n\}$. Valiant (1979) [85] showed that computing the permanent of a $\{0,1\}$-matrix is a $\#\mathsf{P}$-complete problem. On the other hand, it is well-known that the *determinant* $\det(A) = \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}$, where $\mathrm{sgn}(\sigma)$ denote the sign of the permutation σ, can be computed in polynomially many arithmetic operations. We also have $\mathrm{per}(A) = \det(A) \mod 2$. These two matrix functions may also be viewed as polynomials in n^2 variables — replace each $a_{i,j}$ with an indeterminante $x_{i,j}$. If we consider the polynomial families

$$\mathrm{DET}_n = \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} x_{i,\sigma(i)} \qquad \text{and} \qquad \mathrm{PER}_n = \sum_{\sigma \in S_n} \prod_{i=1}^{n} x_{i,\sigma(i)},$$

for $n = 1, 2, \ldots$, then $\det(A)$ and $\mathrm{per}(A)$ are simply the evaluations of these polynomials at the point $A \in \{0,1\}^{n^2}$, respectively. What makes the computation of the permanent so hard comparared to the determinant? Also, along with count-

ing perfect matchings, there are many other counting problems that are solved by computing a certain polynomial.

Valiant (1979) [84] proposed an algebraic model of computation that could help us understand this computational dichotomy between the permanent and the determinant. The reason we shall be discussing this model is that the τ-conjecture has consequences on the separation between certain algebraic complexity classes as well. For details on algebraic complexity classes, see books by Bürgisser (2000) [16], (2024) [18] or the survey by Mahajan (2014) [56]. We once again consider the problem of computing multivariate polynomials over a field $\mathbb{F}$ and a finite set of indeterminates $\mathbb{X} := \{x_1, \ldots, x_m\}$ using the straight line programs introduced in Chapter 1. It will be convenient to represent straight line programs by arithmetic/algebraic circuits since they give more information about the computation sequence.

An *arithmetic circuit* φ computing a polynomial $f \in \mathbb{F}[\mathbb{X}]$ is a directed acyclic graph whose vertices have indegree either zero or two such that each vertex with indegree zero is labelled by either a scalar from $\mathbb{F}$ or an indeterminate from $\mathbb{X}$, and a vertex of indegree two is labelled by any of the arithmetic operation $+, -, *, /$. Vertices with indegree zero are called *input gates*, and those with indegree two are called *operation gates*. We shall assume there is one operation gate with zero outdegree, and that will be the *output gate*. Circuits that do not use division are called *division-free*, and circuits for which the scalars (labels of indegree zero nodes) are allowed only from the set $\{-1, 0, 1\}$ will be called *scalar-free*. We define *size* of a circuit $S(\varphi)$ to be the number of operations gates. In this representation, another useful complexity measure is the *depth* $D(\varphi)$ of a circuit which is the number of edges in the longest directed path. Observe that arithmetic circuits just defined are equivalent to straight line programs, and so we may alternatively define the arithmetic complexity as $L(f) := \min_{\varphi} S(\varphi)$, where the minimum is over all circuits φ computing f. We say that a sequence of arithmetic circuits (φ_n) computes a sequence of polynomials (f_n) if φ_n computes f_n for $n = 1, 2, \ldots$. We are interested in how $L(f_n)$ grows as $n \to \infty$.

Now how should we define easy-to-compute polynomial family? In Chapter 1, we defined it only for the univariate case, and we also assumed that $\deg(f_n) = n$. We shall relax this assumption. The (total) degree of the multivariate polynomial f_n need not be n, and it can also be a growing function of n. Let us also remember that we motivated the study of complexity of polynomials using the problem of polynomial evaluation in Chapter 1. The power sequence $(x_1^{2^n})$ has degree exponentially growing in n, but $L(x_1^{2^n}) \leq n$ because of repeated squaring. Easy-to-compute polynomials should not have that large degree. E.g. consider $\mathbb{F} = \mathbb{Q}$ and the integer

2 of bit-size 1; the evaluation of $x_1^{2^n}$ at 2 will have bit-size 2^n, exponential in n. Also, if the number of indeterminates in f_n is also large, then an evaluation point itself will have a large number of coordinates.

We shall consider *p-families* (see Bürgisser [16]) which are defined as the sequence of multivariate polynomials (f_n) where $f_n \in \mathbb{F}[\mathbb{X}]$ such that the (total) degree of f_n as well as the number of variables in f_n are polynomially bounded in n. E.g. both (DET_n) and (PER_n) are p-families. Now the determinant may be computed in $\mathcal{O}(n^3)$ arithmetic operations by Gaussian elimination (Also see Lemma 6.7). But it includes divisions. Strassen (1973) [80] shows for a polynomial of degree n computed by a circuit of size s, there is another division-free circuit of size $\mathcal{O}(n^2 s)$. So we have $L(\mathrm{DET}_n) = \mathcal{O}(n^5)$, which is still polynomial in n. On the other hand, the best known way to compute the permanent is by Ryser's formula (1963) [73]

$$\mathrm{PERM}_n = \sum_{k=0}^{n-1} (-1)^k \sum_{\substack{S \subseteq \{1,\ldots,n\}, \\ |S|=k}} \prod_{i=1}^{n} \sum_{j \notin S} x_{ij}; \tag{2.1}$$

it requires $\mathcal{O}(n^2 2^{n-1})$ arithmetic operations, which is exponential in n. By Strassen's idea, we can always avoid division with only a quadratic blowup. We shall consider then the division-free arithmetic circuits WLOG, and define easy-to-compute families as those p-families for which the arithmetic complexity is polynomially bounded[4]. In other words, a p-family (f_n) where $f_n \in \mathbb{F}[\mathbb{X}]$ is said to be *p-computable* if $L(f_n)$ is polynomially bounded in n, and the complexity class $\mathsf{VP} = \mathsf{VP}_{\mathbb{F}}$ is the set of all p-computable polynomial families over $\mathbb{F}$. In this model, we shall consider p-computability to be the indicator of tractability. Now (DET_n) is p-computable, and therefore is in VP, and tractable. Valiant's hypothesis is that $(\mathrm{PERM}_n) \notin \mathsf{VP}$. It is not known whether this is true. Analogous to NP, there is the class VNP for which (PERM_n) is complete, which we need not discuss here in detail, although we mention that Valiant's hypothesis is equivalent to the separation $\mathsf{VP} \neq \mathsf{VNP}$.

In the context of the τ-conjecture, we compute polynomials using division-free arithmetic circuits using just the scalars $\{-1, 0, 1\}$ and the set of indeterminates $\mathbb{X}$. Here, the notion of arithmetic complexity of a polynomial will be the τ-complexity extended to multivariate polynomials. Although $\mathbb{Z}$ is not a field, the polynomials so computed at every operation gate in the circuit are integer polynomials since division is not used, and for such polynomials we would like to introduce a tractable complexity class analogous to VP as the associated complexity measure $L(f)$ with

[4] A subtraction may be replaced with one scalar multiplication and an addition. So subtractions can also be avoided with only a constant blowup. Arithmetic circuits can then also be defined over just two operations — addition and multiplication — those are also the two field operations.

VP does not take into account the cost of computing scalars.

As before, we should at least assume for tractability that the polynomials have bounded (total) degree and bounded number of indeterminates. But now scalars cannot be freely used, so for tractability we should also assume that polynomials do not have large coefficients. We could ensure this at every operation gate of the circuit alternatively, and for this the notion of *formal degree* of a circuit is helpful. Let φ be an arithmetic circuit computing a polynomial $f \in \mathbb{Z}[\mathbb{X}]$, and let v be a vertex. The formal degree is defined inductively.

- If v is an input gate (scalar or indeterminate), then its formal degree is 1.
- If v is an operation gate, then there are two cases. If v is addition or subtraction, then its formal degree is the maximum of the formal degree of its children. If v is multiplication, then its formal degree is the sum of the formal degrees of its children.
- The formal degree of the circuit $\deg(\varphi)$ is the formal degree of root node that computes f.

If there are too many multiplications, then the formal degree is large. E.g. consider the integer polynomial $2^{2^n}(x_1 + \cdots + x_n)$; it is clearly in VP. Even when the scalars are not free, there is a circuit of size $2n + 1$ computing this polynomial. But the formal degree is $2^n + 1$, exponential! Such a polynomial cannot be tractable by scalar-free circuits. It is clear that $\deg(f) \leq \deg(\varphi)$. So we need not start with small degree polynomials. Also, the number of indeterminates is small if the circuit size is small. So we can avoid starting with p-families.

We say that a polynomial family (f_n) where $f_n \in \mathbb{Z}[\mathbb{X}]$ is p^0-*computable* if there is a corresponding sequence of division-free and scalar-free arithmetic circuits (φ_n) computing (f_n) such that the formal degree $\deg(\varphi_n)$ as well as the circuit size $S(\varphi_n)$ is polynomially bounded in n. We define the complexity class VP^0 to be the set of all p^0-computable polynomial. Clearly, $\mathsf{VP}^0 \subseteq \mathsf{VP}$. Also, we made sure that $2^{2^n}(x_1 + \cdots + x_n)$ is not in VP^0. There is also the corresponding classe VNP^0 but we need not discuss it here. The scalar-free classes were introduced by Malod (2003) [58] (Also see [59]). Note that $(\mathrm{PERM}_n) \notin \mathsf{VP}^0$ does not imply that the Valiant's hypothesis $(\mathrm{PERM}_n) \notin \mathsf{VP}$ is true, which means the former is a weaker hypothesis compared to Valiant's. Also, if $(\mathrm{PERM}_n) \in \mathsf{VP}^0$, then $\tau(\mathrm{PERM}_n)$ is polynomially bounded in n. Koiran (2005) [45] found a connection between hard to compute integers and this weaker hypothesis.

Theorem 2.5 (Theorem 5 and 8 in [45])**.**

- *If the sequence* $(n!)$ *is hard to compute (Conjecture 1.4), then either* $(PERM_n) \notin \mathsf{VP}^0$ *or* $\mathsf{P} \neq \mathsf{PSPACE}$.
- *If the sequence* $(n!)$ *is ultimately hard to compute (Conjecture 1.5), then either* $(PERM_n) \notin \mathsf{VP}^0$ *or* $\mathsf{P} \neq \mathsf{PSPACE}$.

There have also been number theoretic approaches to the τ-conjecture, e.g. by Rojas (2003) [71, 72], before this result. But Bürgisser (2009) [17] writes,

> "...a proof of the τ-conjecture (if true at all) should rely on very deep insights and techniques in arithmetic algebraic geometry, which are not yet developed and probably won't be so in the near future.... Our main result confirms the belief that solving the τ-conjecture is indeed very hard. In fact, we prove that the truth of the τ-conjecture would imply the truth of another major conjecture in algebraic complexity".

Bürgisser (2009) strengthened Koiran's result as well as discovered consequences of the τ-conjecture and hardness of Pochhammer-Wilkinson polynomial.

Theorem 2.6 (Theorem 1.1 and Corollary 4.2 in [17])**.**

- *If the sequence* $(n!)$ *is hard to compute (Conjecture 1.4), then* $(PERM_n) \notin \mathsf{VP}^0$.
- *If* τ*-conjecture (Conjecture 1.2) is true, then* $(PERM_n) \notin \mathsf{VP}^0$.
- *Under the generalized Riemann hypothesis, if the Pochhammer-Wilkinson polynomial is hard to compute with respect to the arithmetic complexity (Conjecture 1.3), then* $(PERM_n) \notin \mathsf{VP}_{\mathbb{C}} = \mathsf{VP}$

Real τ-Conjecture

If the goal is now to show that $(\mathrm{PERM}_n) \notin \mathsf{VP}^0$ or $(\mathrm{PERM}_n) \notin \mathsf{VP}$, then what is the most relaxed variant of the τ-conjecture that leads to such conclusions? Koiran (2011) [46] considered a restricted family of integer polynomials, denoted by $SPS_{s,e}$, which is the set of all univariate polynomials in $\mathbb{Z}[x]$ such that they can be represented in the form $f := \sum_{i=1}^{p} \prod_{j=1}^{q} f_{i,j}$ with $pqk \leq s$, where each $f_{i,j} \in \mathbb{Z}[x]$ has at most k monomials, degree at most e, coefficients of $f_{i,j}$'s have a sparse representation, i.e. the number of ones in their binary representation is at most s and the absolute value of the coefficients is at most 2^e (See Definition 8 [46]). Basically, the coefficients as well as the degree of these polynomials is controlled. What is the τ-complexity of such polynomials? Each power x^α takes $\mathcal{O}(\log e)$ and each coefficient takes $\mathcal{O}(s \log e)$ operations. So $\tau(f) = \mathcal{O}(s^2 \log e)$ or put simply it is bounded

by a polynomial in $(s + \log e)$. Now if the τ-conjecture is true, then any polynomial in $SPS_{s,e}$ has the number of distinct integer zeros bounded by a polynomial in $(s + \log e)$. The following variant was posed.

Conjecture 2.7 (τ-Conjecture for SPS polynomials [46])**.** *Let $f \in SPS_{s,e}$ be a nonzero polynomial, then it has at most $(s + \log e)^c$ many distinct integer zeros for some universal constant $c > 0$.*

The SPS polynomials are computable by depth-4 arithmetic circuits, and the idea to consider depth-4 circuits comes from Agrawal and Vinay (2008) [1] who showed that multilinear polynomials computable by "small" arithmetic circuits are also computable by "small" depth-4 arithmetic circuits. The converse suggests that it is enough to focus on showing lower bounds for depth-4 circuits. Using an analogous result for constant-free circuits (Theorem 4 [46]), Koiran showed that this weaker conjecture also implies that $(\text{PERM}_n) \notin \mathsf{VP}^0$.

Theorem 2.8 (Koiran [46])**.** *The τ-conjecture (Conjecture 1.2) implies τ-conjecture for SPS polynomials (Conjecture 2.7), and the latter implies $(PERM_n) \notin \mathsf{VP}^0$*

The new variant still refers to integer zeros and integer coefficients. A real or a complex variant of the τ-conjecture may be more approachable since techniques from real or complex analysis can be applied. Consider the following.

Conjecture 2.9 (Real τ-Conjecture [46])**.** *Let f be a nonzero polynomial in $\mathbb{R}[x]$ of the form $\sum_{i=1}^{p} \prod_{j=1}^{q} f_{i,j}$. Then it has at most $(pqk)^c$ many distinct real zeros for some universal constant $c > 0$.*

An upper bound on the number of real zeros is also an upper bound on the number of integer zeros. Also an upper bound polynomial in pqk is stronger than an upper bound polynomial in $(s + \log e)$, where $pqk \leq s$. So Conjecture 2.9 implies Conjecture 2.7, and as a result

Corollary 2.10. *Real τ-Conjecture implies $(PERM_n) \notin \mathsf{VP}^0$.*

It is not yet clear whether the truth of the real τ-conjecture implies truth of the τ-conjecture, although we know that if the τ-conjecture for SPS polynomials is false, then both the real τ-conjecture and the τ conjecture are false. Tavenas (2014) [83] (Theorems 3.25 and 3.38) shows that even the conclusion $(\text{PERM}_n) \notin \mathsf{VP}$ (over a field of characteristic zero, e.g. $\mathbb{C}$) can be obtained, and an upper bound polynomial in p, 2^q and k suffices.

Now that we have a real variant, we shall discuss how to count real zeros in the upcoming chapters. The rest of the thesis is essentially based on and motivated by

two ideas: Wronskian approach due to Koiran, Portier and Tavenas (2015) [48] and the complex analytic approach due to Hrubeš (2013) [42]. In Chapter 14, we shall discuss some more variants due to Hrubeš (2013) [42] and Tavenas (2014) [83].

Chapter 3

Descartes' Rule of Signs

Let $A(x)$ be a univariate polynomial of degree n with real coefficients. We denote by $N_A I$ the number of real zeros of $A(x)$ in an interval $I \subseteq \mathbb{R}$ counted with multiplicities, and following Rahman and Schmeisser [69], we denote by $N_A^\circ I$ the number of distinct real zeros of $A(x)$ in the interval I. The simplest and the oldest method to estimate these quantities is due to Descartes (1637) [24] based on the sign variations in the sequence of coefficients of the polynomial. We denote by $V(a_1, \ldots, a_n)$ the number of sign variations in a sequence of real numbers $(a_1, \ldots, a_n)$. If all the elements in the sequence are nonvanishing, i.e., $a_i \neq 0$ for all i, then we define $V(a_1, \ldots, a_n)$ to be the number of indices $j \in \{1, \ldots, n\}$ such that a_{j-1} and a_j have the opposite sign i.e. $a_{j-1}a_j < 0$. Otherwise, we consider the subsequence $\{a'_1, \ldots, a'_m\}$ obtained from $\{a_1, \ldots, a_n\}$ by ignoring all the vanishing numbers, and define $V(a_1, \ldots, a_n) := V(a'_1, \ldots, a'_m)$. The next result counts the number positive real zeros. By the sign variations of a polynomial, we mean the sign variations in the sequence of its coefficients arranged according to the increasing order of the exponents of the variable.

Theorem 3.1 (Strong Rule of Signs)**.** *Let $A(x) = \sum_{i=0}^{n} a_i x^i$ be a polynomial with real coefficients. Then, $N_A(0, \infty) \leq V(a_0, \ldots, a_n)$.*

Descartes did not give a proof of it, and he had also assumed that all the coefficients are nonvanishing. The first proof that is without this assumption, seems to be due to Fourier (1820) [30] and Budan (1822) [15], who gave results more general than the Descartes' rule, which are now known as the combined Budan-Fourier Theorem. Later, Gauss (1828) [32] gave a direct proof that is based on the sign variations only. Here we discuss a proof using induction on $N_A(0, \infty)$ due to Krishnaiah (1963) [52] which is more cleaner. For an historical overview, we refer the reader to Rahman and Schmeisser [69] (Section 10.1), and Bensimhoun (2013) [5].

If the polynomial $A(x)$ has no positive zeros, then it may be factored as $A(x) = x^e \prod_{\beta>0}(x+\beta)$ in which case there cannot be any sign variations, and so the base case is covered. Now suppose that $A(x)$ has r positive zeros, and let α be one of the positive zeros. By factoring the polynomial as $A(x) = (x-\alpha)B(x)$, we obtain another polynomial $B(x)$ that has $r-1$ positive zeros, and therefore by the induction hypothesis, at least $r-1$ sign variations. Next, we need to show that $A(x)$ has at least r sign variations. We do this as a separate lemma, again by induction. Then the proof of Theorem 3.1 follows.

Lemma 3.2. *[52] Let $B(x)$ be a polynomial with real coefficients and $r-1$ sign variations. Then for any positive number α, the product $A(x) := (x-\alpha)B(x)$ has at least r sign variations.*

Proof. Let S denote the sequence of coefficients of $A(x)$ arranged according to the increasing order of exponents of x. By writing $B(x) = \sum_{j=1}^{n-1} b_i x^i$, we notice that S is $\{(b_0 - \alpha b_1), (b_1 - \alpha b_2), \ldots, (b_{n-1} - \alpha b_n)\}$ where $b_0 = b_n = 0$. If $r = 1$, then all the coefficients of $B(x)$ have the same sign, in particular b_1 and b_{n-1} have the same sign, and therefore $b_0 - \alpha b_1$ and $b_{n-1} - \alpha b_n$ have opposite signs. Thus S must have at least one sign variation. This covers the base case.

Now suppose that $B(x)$ has $r-1$ sign variations, and let s to be the index such that the last sign variation is after b_s and it is due to $b_s b_{s+t} < 0$ for some $t \geq 1$ and $b_s \neq 0$. Next, we split $B(x)$ as $B(x) = C(x) + D(x)$ where $C(x) = \sum_{j=1}^{s} b_i x^i$ and $D(x) = \sum_{j=s+1}^{n-1} b_i x^i$. Now $C(x)$ has exactly $r-2$ sign variations, and $D(x)$ has none. This split will help us apply induction. Multiplying $B(x)$ by $(x-\alpha)$, we have $A(x) = (x-\alpha)C(x) + (x-\alpha)D(x)$, where by induction hypothesis, $(x-\alpha)C(x)$ has at least $r-1$ sign variations, and $(x-\alpha)D(x)$ has at least one. Now the polynomials $(x-\alpha)C(x)$ and $(x-\alpha)D(x)$ do not have a term of the same power of x if $t > 1$ in which case we can easily conclude that $A(x)$ has at least r sign variations.

If $t = 1$, then the highest power of x in $(x-\alpha)C(x)$ is the same as the smallest power of x in $(x-\alpha)D(x)$. There is no other overlap. We write $(x-\alpha)C(x) = C'(x) + b_s x^{s+1}$ and $(x-\alpha)D(x) = -\alpha b_{s+1} x^{s+1} + D'(x)$, so that the number of sign variations in $A(x)$ is the sum of the number of sign variations in $C'(x) + (b_s - \alpha b_{s+1})x^{s+1}$ and the number of sign variations in $(b_s - \alpha b_{s+1})x^{s+1} + D'(x)$. Now recall that there is a sign variation from s to $s+1$ due to $b_s b_{s+1} < 0$. If we consider $C'(x) + (b_s - \alpha b_{s+1})x^{s+1}$ such that s' is the degree of C', then $b_{s'}(b_s - \alpha b_{s+1})$ has the same sign as that of $b_{s'} b_s$. This can be shown by considering two cases. If $b_{s'} b_s > 0$, then $b_{s'} b_{s+1} < 0$ because there is a sign variation from s to $s+1$. Since α is positive, $b_{s'}(b_s - \alpha b_{s+1})$ also becomes positive. Similarly, if $b_{s'} b_s < 0$, then $b_{s'} b_{s+1} > 0$, and as a result, $b_{s'}(b_s - \alpha b_{s+1})$ becomes negative. Thus $C'(x) + (b_s - \alpha b_{s+1})x^{s+1}$ has the same number of sign

variations as that of $(x-\alpha)C(x)$ which is at least $r-1$. By a similar argument, we can show that $(b_s - \alpha b_{s+1})x^{s+1} + D'(x)$ and $(x-\alpha)D(x)$ have the same number of sign variations which is at least one. Thus in this case as well $A(x)$ has at least r sign variations. □

For convenience, we write $V(A)$ instead of $V(a_0, a_1, \ldots, a_n)$ when the coefficients are not specified. By applying the rule on $A(-x)$, the number of negative real zeros can also be counted since $N_A(-\infty, 0) = N_{A(-x)}(0, \infty) \leq V(A(-x))$. Descartes' rule is particularly useful for the sparse polynomials. By a k-sparse polynomial we mean that it has exactly k nonvanishing coefficients. Since there can be at most $k-1$ sign variations in the sequence of coefficients of a k-sparse polynomial, we obtain a weaker result.

Corollary 3.3 (Weak Rule of Signs)**.** *Let $A(x)$ be a real k-sparse polynomial. Then $N_A(0, \infty) \leq k-1$.*

The same upper bound also holds for the number of negative real zeros, i.e. $N_A(-\infty, 0) \leq k-1$. In general, the multiplicity of 0 does not depend on the sparsity because we could always multiply a polynomial by an arbitrary power of x and the sparsity remains the same. Therefore if we want an upper bound purely in terms of the sparsity, then by Descartes we can do it for either the number of distinct real zeros or the number of nonzero real zeros counted with multiplicities.

Proposition 3.4. *For any real k-sparse polynomial $A(x)$, the following holds.*

- *The number of real distinct zeros is at most $2k-1$, i.e. $N_A^{\circ}\mathbb{R} \leq 2k-1$.*
- *The number of nonzero real zeros counted with multiplicity is at most $2k-2$, i.e. $N_A\mathbb{R}^* \leq 2k-2$.*

Simply put, the upper bound is linear in the sparsity. It is also tight in both cases, realized by the k-sparse polynomial $x\prod_{j=1}^{k-1}(x^2-j)$ which has $2k-1$ distinct real zeros, and $2k-2$ nonzero real zeros counted with multiplicity. We shall refer to any of the above three results as simply Descartes' rule.

Application to the Real τ-Conjecture

Consider a polynomial of the form $f := \sum_{i=1}^{p}\prod_{j=1}^{q} f_{i,j}$ where each $f_{i,j}$ is k-sparse. Although the sparsity of each of the terms $\prod_{j=1}^{q} f_{i,j}$ can be $\mathcal{O}(k^q)$, the number of real distinct zeros is at most $\mathcal{O}(qk)$ because the number of zeros of a product of polynomials add up. But we do not yet understand the zeros of the sum, and since

f can potentially have sparsity $\mathcal{O}(pk^q)$, we can only conclude with a trivial upper bound $N_f^\circ\mathbb{R} = \mathcal{O}(pk^q)$ by Proposition 3.4. The simplest case towards the real τ-conjecture that we do not understand is $f := gh + t$, where g and h are k-sparse, and t is some real parameter. The product gh has $\mathcal{O}(k)$ real distinct zeros, but adding the parameter t may disrupt the distribution, and since f can have sparsity $\mathcal{O}(k^2)$, which is also the trivial upper bound on number of real zeros we can get by Descartes. Thus we are interested in the following problem, pointed out by Chattopadhyay [46].

Problem 3.5. *Let g and h be real k-sparse polynomials, and $f := gh + t$ for some real parameter t. Is it true that f has at most $\mathcal{O}(k)$ real distinct zeros? Is it true that f has at most $\mathcal{O}(k)$ nonzero real zeros counted with multiplicities?*

An affirmative answer to the second problem in 3.5 also gives an affirmative answer to the first. The case $g = h$ is a solved problem, an observation by Dutta (2021) [Theorem 9, [27]]. Consider $f := g^2+t$. In the case $t > 0$, f is a sum of squares of two polynomials, and therefore zeros of f are the common zeros of g^2 and t, i.e., f has no zeros. In the case $t < 0$, express f as the product $f = (g - \sqrt{t})(g + \sqrt{t})$. Now both the factors have sparsity at most $k+1$, and therefore f has at most $\mathcal{O}(k)$ real distinct zeros.

Nearly Exact Descartes Approach (An Attempt)

Next, let us attempt to address Problem 3.5 by controlling the dependancy between the number of real zeros and the sparsity through sign variations. Consider the first part of Problem 3.5 in which the number of distinct real zeros $N_f^\circ\mathbb{R}$ is expected to be smaller than $V(f)$ by a linear factor. Recall that we always have $N_f(0,\infty) = \mathcal{O}(V(f))$ by Descartes. What if we start with two polynomial g and h for which the number of real zeros and the number of sign variations are tightly related? Formally, let $\mathcal{E}^\circ$ be a family of real polynomials satisfying two conditions:

- For every $A \in \mathcal{E}^\circ$, $V(A) = \mathcal{O}(N_A^\circ\mathbb{R})$,
- For every pair $A, B \in \mathcal{E}^\circ$, $AB \in \mathcal{E}^\circ$.

Let us see why it makes sense to consider such polynomials. Consider $g, h \in \mathcal{E}^\circ$ that are k-sparse. Then by Descartes, $N_g^\circ\mathbb{R} = \mathcal{O}(k)$ and $N_h^\circ\mathbb{R} = \mathcal{O}(k)$. Since the set of real zeros of the product gets unionized, we have $N_{gh}^\circ\mathbb{R} = \mathcal{O}(k)$. Next, let us look at the sign variations. By the second property, we have $gh \in \mathcal{E}^\circ$, and so $V(gh) = \mathcal{O}(N_{gh}^\circ\mathbb{R})$ due to the first property. Adding t to gh can change the number

of sign variations by at most one, so we have $V(f) = \mathcal{O}(N^{\circ}_{gh}\mathbb{R}) = \mathcal{O}(k)$. Again by Descartes, we can conclude that $N^{\circ}_{f}\mathbb{R} = \mathcal{O}(k)$. Let us record this observation.

Proposition 3.6. *Let g and h be two k-sparse polynomials from $\mathcal{E}^{\circ}$, and $f := gh+t$ for some real parameter t. Then, $N^{\circ}_{f}\mathbb{R} = \mathcal{O}(k)$.*

The important question is of course to characterize $\mathcal{E}^{\circ}$. But could this approach be extended for the real τ-conjecture? Our object of interest are the polynomials of the form $f = \sum_{i=1}^{p}\prod_{j=1}^{q} f_{i,j}$ where each $f_{i,j}$ is k-sparse. Suppose $f_{i,j}$'s are drawn from $\mathcal{E}^{\circ}$, then for each term we have $V(\prod_{j=1}^{q} f_{i,j}) = \mathcal{O}(qk)$. Unfortunately, a similar argument seems to fail because many of the coefficients may change signs when we consider the sum of these terms over i. In the earlier case, only the constant coefficient could change. Let us see which polynomials are in $\mathcal{E}^{\circ}$. We claim that $\{A(x) \mid N^{\circ}_{A}\mathbb{R} = \Omega(n)\} \subseteq \mathcal{E}^{\circ}$, where n denotes the degree of $A(x)$. The condition $N^{\circ}_{A}\mathbb{R} = \Omega(n)$ is the same as $n = \mathcal{O}(N^{\circ}_{A}\mathbb{R})$. But $V(A) \leq n+1$ always holds, and so the first property $V(A) = \mathcal{O}(N^{\circ}_{A}\mathbb{R})$ is trivially satisfied. If A and B are two polynomials of degree n and m respectively such that $N^{\circ}_{A}\mathbb{R} = \Omega(n)$ and $N^{\circ}_{B}\mathbb{R} = \Omega(m)$, then the product AB is of degree $m+n$ and satisfies $N^{\circ}_{AB}\mathbb{R} = \Omega(\max\{m,n\}) = \Omega(m+n)$ because the set of zeros of the product AB is simply the union of the set of zeros of A and B. So the second condition is taken care of as well.

It appears that polynomials with at least linearly many (in the degree) real distinct zeros is a very narrow class. Let f be k-sparse polynomial of degree n and $N^{\circ}_{f}\mathbb{R} = \Omega(n)$. We always know by Descartes that $N^{\circ}_{f}\mathbb{R} = \mathcal{O}(k)$, so the sparsity $k = \Omega(n)$ becomes comparable to the degree. We are more interested in the case where the sparsity is independent of the degree. We leave the characterization of $\mathcal{E}^{\circ}$ as an open problem of separate interest. Corollary 10.1.12 in Rahman-Schmeisser [69] states that the strong rule of signs is exact for polynomials with only real zeros, and therefore for polynomials, lets assume with nonzero constant term, the sparsity is already at least $\Omega(n)$. Based on this, our hunch is that polynomials in $\mathcal{E}^{\circ}$ must also have high sparsity. We believe then an ideal approach would be to avoid going through sign variations, and consider the following variant instead.

Problem 3.7. *Let g and h be two polynomials with $\mathcal{O}(k)$ real distinct zeros. Is it always true that $f := gh + t$ also has $\mathcal{O}(k)$ real distinct zeros? What about nonzero real zeros counted with multiplicities?*

Although this problem avoids sign variations or the sparsity, it suggests that we may need analytic insights. In the next chapter, we will study the relation of a polynomial with its derivative, and also give an analytic proof of Descartes' rule. The proof that we discussed earlier is algebraic.

Chapter 4

Rolle's Theorem

What is the relation between the zeros of a polynomial and its derivative? Could it help us with studying the zeros of $gh + t$? Let us begin with a simple observation. Suppose that α is a zero of the real polynomial $A(x)$ with multiplicity m. Then, we can write $A(x) = (x-\alpha)^m B(x)$ for some $B(x)$ such that $B(\alpha) \neq 0$. Considering its derivative $A'(x) = (x-\alpha)^{m-1}\left((x-\alpha)B'(x) + B(x)\right)$, we see that the factor $(x-\alpha)B'(x)+B(x)$ does not vanish at α. Thus, if α is a zero of $A(x)$ with multiplicity m, then α is a zero of $A'(x)$ with multiplicity $m-1$. This means that the simple zeros of a polynomial are never the zeros of its derivative, where by *simple* we refer to the zeros with multiplicity one. What about *repeated* zeros, the zeros with multiplicity more than one? If we consider the polynomial in the form $A(x) = \prod_{i=1}^{d}(x-\alpha_i)^{m_i}$ with d distinct zeros $\alpha_1, \ldots, \alpha_d$ of multiplicities $m_1, \ldots, m_d$ respectively, and express its derivative as

$$A'(x) = \left(\prod_{\substack{i=1 \\ m_i \geq 2}}^{d} (x-\alpha_i)^{m_i-1}\right)\left(\frac{A'(x)}{A(x)}\prod_{j=1}^{d}(x-\alpha_j)\right),$$

then we can notice that any zero of $A'(x)$ is either a repeated zero of $A(x)$ or a zero of the second factor $B(x) := \frac{A'(x)}{A(x)}\prod_{j=1}^{d}(x-\alpha_j)$. Moreover, neither the simple nor the repeated zeros of $A(x)$ can be zeros of $B(x)$. Thus, the zeros of $B(x)$ are exactly the zeros of $\frac{A'(x)}{A(x)}$. We refer to the rational function $\frac{A'(x)}{A(x)}$ as the *logarithmic derivative* of $A(x)$ since $\frac{A'(x)}{A(x)} = \frac{\mathrm{d}}{\mathrm{d}x}(\log A(x))$.

The above observations may be summarized as follows.

Lemma 4.1. *(1) Zeros of the derivative $A'(x)$ are either the repeated zeros of $A(x)$ or the zeros of the logarithmic derivative $\frac{A'(x)}{A(x)}$. The same holds for real zeros. In particular,*

$$N_{A'}\mathbb{R} = (N_A\mathbb{R} - N_A^{\circ}\mathbb{R}) + N_{A'/A}\mathbb{R}.$$

(2) The number of distinct zeros of $A'(x)$ is the sum of number of distinct repeated zeros of $A(x)$ and the number of distinct zeros of $\frac{A'(x)}{A(x)}$. The same holds for real zeros. In notation,

$$N^{\circ}_{A'}\mathbb{R} = (N^{\circ}_{A}\mathbb{R} - S_A\mathbb{R}) + N^{\circ}_{A'/A}\mathbb{R},$$

where $S_A\mathbb{R}$ denotes the number of simple real zeros of $A(x)$.

Proof. These two statements are evident. The number of repeated zeros of $A(x)$, counted with multiplicity, is exactly $N_A\mathbb{R} - S_A\mathbb{R}$. Repeated zeros of $A(x)$ occur as zeros of $A'(x)$ with multiplicity one less. But now the number of distinct repeated zeros of $A(x)$ is exactly $N^{\circ}_{A}\mathbb{R} - S_A\mathbb{R}$. So the contribution of repeated zeros to $N_{A'}\mathbb{R}$ is the difference $(N_A\mathbb{R} - S_A\mathbb{R}) - (N^{\circ}_{A}\mathbb{R} - S_A\mathbb{R}) = N_A\mathbb{R} - N^{\circ}_{A}\mathbb{R}$. Similarly, the contribution of repeated zeros to $N^{\circ}_{A'}\mathbb{R}$ is the term $N^{\circ}_{A}\mathbb{R} - S_A\mathbb{R}$. □

How useful is this lemma for counting distinct real zeros of $A(x)$? Even if we do not have an idea about the zeros of $\frac{A'(x)}{A(x)}$ we can always state $N_{A'}\mathbb{R} \geq N_A\mathbb{R} - N^{\circ}_{A}\mathbb{R}$ and $N^{\circ}_{A'}\mathbb{R} \geq N^{\circ}_{A}\mathbb{R} - S_A\mathbb{R}$. For polynomials whose all real zeros are simple, we do not get any more information from these two inequalities because $S_A\mathbb{R} = N^{\circ}_{A}\mathbb{R} = N_A\mathbb{R}$. Otherwise, we need an estimate on $S_A\mathbb{R}$, the number simple real zeros, as well. We also need to understand the zeros of the logarithmic derivative $\frac{A'(x)}{A(x)}$ to be able to estimate $N_A\mathbb{R}$ or $N^{\circ}_{A}\mathbb{R}$. Since the zeros of the derivative are usually called *critical points*, following Rahman and Schmeisser [69], we may call repeated zeros of $A(x)$ as the *critical points of the first kind*, and the zeros of $\frac{A'(x)}{A(x)}$ as the *critical points of the second kind*.

Proposition 4.2. *A polynomial $A(x)$ has $N_A\mathbb{R} - N^{\circ}_{A}\mathbb{R}$ critical points of the first kind counting multiplicity. Among them $N^{\circ}_{A}\mathbb{R} - S_A\mathbb{R}$ many are distinct.*

Rolle's theorem (1691) gives us some idea about critical points of the second kind, although Rolle had proved it only for polynomials. Cauchy (1823) later proved it for functions using mean value theorem. We shall use it for both polynomials and functions.

Theorem 4.3 (Rolle's Theorem)**.** *Let A be a continuous function in the interval $[a, b]$ such that it is differentiable in (a, b) and vanishes at the points a and b. Then, its derivative A' has at least one zero in (a, b).*

Notice that critical points of the first kind cannot exist between two consecutive zeros. Since the polynomial $A(x)$ has $N^{\circ}_{A}\mathbb{R}$ distinct real zeros, Rolle's theorem guarantees at least $N^{\circ}_{A}\mathbb{R} - 1$ critical points of the second kind. Thus, $N_{A'/A}\mathbb{R} \geq N^{\circ}_{A}\mathbb{R} - 1$ and $N^{\circ}_{A'/A}\mathbb{R} \geq N^{\circ}_{A}\mathbb{R} - 1$, and after substituting these two inequalities in Lemma 4.1, we can conclude

Corollary 4.4. *$N_A\mathbb{R} \leq N_{A'}\mathbb{R} + 1$ and $2N_A^\circ\mathbb{R} \leq N_{A'}^\circ\mathbb{R} + S_A\mathbb{R} + 1$.*

Let us discuss the second inequality. The quantity $N_A^\circ\mathbb{R} - S_A\mathbb{R}$ is always non-negative, and it is zero if all real zeros of $A(x)$ are simple. In such cases, we can state $N_A^\circ\mathbb{R} \leq N_{A'}^\circ\mathbb{R} + 1$. Although this bound may be improved in the case that all real zeros of $A(x)$ are repeated, i.e. $S_A\mathbb{R} = 0$, as $N_A^\circ\mathbb{R} \leq \frac{N_{A'}^\circ\mathbb{R}+1}{2}$, we may not have an estimate on $S_A\mathbb{R}$. To summarize, we always have $N_A^\circ\mathbb{R} \leq N_{A'}^\circ\mathbb{R} + 1$, and simply put, the corollary states $N_A\mathbb{R} = \mathcal{O}(N_{A'}\mathbb{R})$ and $N_A^\circ\mathbb{R} = \mathcal{O}(N_{A'}^\circ\mathbb{R})$.

Analytic Proof of Descartes' Rule

The very first analytic approach to Descartes' rule seems to be by De Gua (1741) [21] (See also [5]). Laguerre (1879) [54] extended the rule using analytic approach to generalized polynomials in which we allow the exponents to be reals (Also see Problem 77, Part 5 in Pólya and Szegö [68]).

Theorem 4.5 (Descartes' Rule for Generalized Polynomials by Laguerre)**.** *Let $A(x) = \sum_{i=1}^{k} a_i x^{\alpha_i}$ be a generalized polynomial such that a_i's and α_i's are reals and $\alpha_1 < \alpha_2 < \cdots < \alpha_k$. Then, $N_A(0,\infty) \leq V(a_1, a_2, \ldots, a_k)$.*

Here, we prove a weaker version for the sake of demonstrating an application of Rolle's theorem. We shall discuss more along the lines of Theorem 4.5 in Chapter 5.

Theorem 4.6 (Weak Rule of Signs for Generalized Polynomials)**.** *Let $A(x) = \sum_{i=1}^{k} a_i x^{\alpha_i}$ be a generalized polynomial such that a_i's and α_i's are reals and $\alpha_1 < \alpha_2 < \cdots < \alpha_k$. Then, $N_A(0,\infty) \leq k - 1$.*

Recall that we inducted on $N_A(0,\infty)$ in the proof of Theorem 3.1. Here, we induct on k, the sparsity.

Proof. For $k = 1$, the polynomial $A(x)$ has exactly one monomial in $A(x)$ and therefore no positive zeros. Next, since the induction is on the sparsity, we must derive a polynomial of sparsity one less than $A(x)$. We factor out the smallest power of x, so that we get a polynomial with a nonzero constant term, $B(x) := x^{-\alpha_1}A(x) = a_1 + \sum_{i=2}^{k} a_i x^{\alpha_i - \alpha_1}$, and such that $N_A(0,\infty) = N_B(0,\infty)$. Next, we differentiate $B(x)$ once to obtain the $(k-1)$-sparse polynomial $B'(x) = \sum_{i=2}^{k} a_i(\alpha_i - \alpha_1)x^{\alpha_i - \alpha_1 - 1}$, and now by induction hypothesis, $N_{B'}(0,\infty) \leq k - 2$. By Rolle's theorem, B' must have at least $N_B(0,\infty) - 1$ positive zeros, and therefore $N_B(0,\infty) - 1 \leq k - 2$. Now since A and B have the same number of positive zeros, we get $N_A(0,\infty) \leq k - 1$. □

Application to $gh + 1$

Rolle's theorem helped us show that the number of real zeros of a polynomial is linear in the number of real zeros of its derivative. Applying Corollary 4.4 to $f := gh + t$, we get $N_f\mathbb{R} = \mathcal{O}(N_{(gh'+hg')}\mathbb{R})$ and $N_f^\circ\mathbb{R} = \mathcal{O}(N^\circ_{(gh'+hg')}\mathbb{R})$. It also appears that the parameter t does not have a large role to play. If g and h are k-sparse, then the derivative of their product can be k^2-sparse. It now makes sense to refine Problem 3.7 as

Problem 4.7. *Let g and h be two polynomials with $\mathcal{O}(k)$ real distinct zeros. Is it always true that $gh' + g'h$ also has $\mathcal{O}(k)$ real distinct zeros?*

The takeaway of this chapter is that we must understand the zeros of the derivative, and in particular, the logarithmic derivative. Although in this thesis we do not study zeros of the logarithmic derivative, we shall demonstrate an application of Rolle's theorem in the next chapter where we introduce an important idea of Wronskian. The Wronskian will help us talk about zeros of linear combination of functions. We shall also discuss a generalization of Descartes' rule for functions.

Chapter 5

Descartes System

Towards understanding the zeros of polynomials of the form

$$f = \sum_{i=1}^{p} \prod_{j=1}^{q} f_{i,j},$$

the simplest case that we considered earlier was the product of two polynomials perturbed by a constant. But another natural approach would be to study zeros of the sums or the linear combinations $f = \sum_{i=0}^{n} a_i \phi_i$ of a sequence of polynomials $\{\phi_0, \phi_1, \ldots, \phi_n\}$. We may start by generalizing the Descartes' rule for functions. The Descartes' rule states that if $A(x) = \sum_{i=0}^{n} a_i x^i$ is a polynomial with real coefficients then the number of zeros $N_A(0, \infty)$ in the interval $(0, \infty)$ is at most the number of signs variations $V(a_0, a_1, \ldots, a_n)$ in the sequence of its coefficients. Since the sign variations depend only on the nonvanishing coefficients, such a result helped us bound the number of real positive zeros in terms of the sparsity of the polynomial. The polynomial here is expressed in the monomial basis $\{1, x, x^2, \ldots, x^n\}$. We also saw in the previous chapter that Laguerre's generalization allowed us to use distinct real exponents. So now instead of polynomials, we could consider functions, and investigate different bases of functions which obey Descartes' rule. Let us formalize this.

Definition 5.1. *A sequence of functions $\{\phi_0, \phi_1, \ldots, \phi_n\}$ obeys Descartes' rule of signs (drs) in an open interval $I \subseteq \mathbb{R}$ if for all nontrivial real linear combinations $f := \sum_{i=0}^{n} a_i \phi_i$,*

$$N_f I \leq V(a_0, a_1, \ldots, a_n).$$

We refer to such a pair of sequence and interval as a Descartes system.

For example, the pair $(\{1, x, x^2, \ldots, x^n\}, (0, \infty))$ forms a Descartes system. A different basis may not necessarily form a Descartes system for the interval $(0, \infty)$

or $\mathbb{R}$. So we need to investigate the necessary and the sufficient conditions for a system to be a Descartes system. Let us work out the small cases first. For $n = 0$, let $\{\phi_0\}$ and I be our system. Consider the scaling $f = a_0\phi_0$ by a nonzero real number a_0. Since there are no sign variations, the function f does not have any zeros in I if the system obeys drs. Conversely, if f does not have any zeros in I, then $N_f I \leq V(a_0)$ holds and the system obeys drs. In particular,

Proposition 5.2. *The sequence $\{\phi_0\}$ obeys drs in I iff ϕ_0 does not have any zeros in I.*

For $n = 1$, let $\{\phi_0, \phi_1\}$ and I be our system. Consider the real linear combination $f = a_0\phi_0 + a_1\phi_1$, where not both of a_0 and a_1 are zero. If exactly one of a_0 and a_1 is zero, then $V(a_0, a_1) = 0$ and similar to the base case we have

> P1. *Let $f = a_0\phi_0 + a_1\phi_1$ be such that one of the coefficients is zero and the other is a nonzero real. Then, $N_f I \leq V(a_0, a_1)$ holds iff ϕ_0 and ϕ_1 do not have any zeros in I.*

If both a_0 and a_1 are nonzero but have the same sign, then $V(a_0, a_1) = 0$ and the drs conclusion holds iff f has no zeros in I. WLOG let $a_0 = 1$ and $a_1 > 0$, then this is equivalent to $\frac{\phi_0(x)}{\phi_1(x)} \neq -a_1$ for all $x \in I$, and in particular, $\frac{\phi_0(x)}{\phi_1(x)}$ is nonnegative for all $x \in I$ when ϕ_1 does not have zeros in I.

> P2. *Let $f = a_0\phi_0 + a_1\phi_1$ be such that both the coefficients are nonzero reals and have the same sign. Then, $N_f I \leq V(a_0, a_1)$ holds iff $\frac{\phi_0(x)}{\phi_1(x)}$ is nonnegative for all $x \in I$ and ϕ_1 does not have zeros in I.*

When the premise of P1 and P2 are combined, the rational function $\frac{\phi_0(x)}{\phi_1(x)}$ always takes positive values since ϕ_0 does not vanish in I. In other words, ϕ_0 and ϕ_1 have the same sign in I.

Next, let us look at the remaining subcase where both a_0 and a_1 are nonzero but have different signs. Here, $f = a_0\phi_0 + a_1\phi_1$ and $V(a_0, a_1) = 1$. WLOG write $f = \phi_0 - a_1'\phi_1$ such that $a_1' > 0$. The drs conclusion $N_f I \leq V(a_0, a_1)$ holds iff f has at most one zero in I. Now this is equivalent to $g := \frac{\phi_0}{\phi_1} = a_1'$ having at most one solution in I, when ϕ_1 does not vanish in I. This implies that g' does not vanish in I. Otherwise consider the fact that I is open, so if g has an extreme point inside I, i.e. if g' vanishes in I, then g takes the same value at two points around the extreme point both of which are inside I. Conversely, suppose that g' does not vanish in I, then g is strictly monotonous. So g must take each value at most once in I. In particular, $g = a_1'$ has most one solution in I. Thus, drs conclusion is equivalent to g' not vanishing in I, given that ϕ_1 does not vanish in I, which is again same as $\phi_0\phi_1' - \phi_0'\phi_1$ not vanishing in I.

P3. *Let $f = a_0\phi_0 + a_1\phi_1$ be such that both the coefficients are nonzero reals and have a different sign. Then, $N_f I \leq V(a_0, a_1)$ holds iff $\phi_0\phi_1' - \phi_0'\phi_1$ and ϕ_1 do not have any zeros in I.*

Note that one implicit assumption that we need to make here is that ϕ_0 and ϕ_1 are differentiable so that their derivatives are well defined. Now combining the premise of P1, P2 and P3, we have

Proposition 5.3. *The sequence of differentiable functions $\{\phi_0, \phi_1\}$ obeys drs in an interval I iff*

- *ϕ_0, ϕ_1 and $\phi_0\phi_1' - \phi_0'\phi_1$ do not have any zeros in I,*
- *ϕ_0 and ϕ_1 have the same sign in I.*

Observing

$$\phi_0\phi_1' - \phi_0'\phi_1 = \det \begin{bmatrix} \phi_0 & \phi_1 \\ \phi_0' & \phi_1' \end{bmatrix},$$

we extend this result for any $n \geq 3$ by introducing the Wronskian. For a sequence of n-times differentiable functions $\phi_0, \phi_1, \ldots, \phi_n$, we define its *Wronskian* as

$$W(\phi_0, \ldots, \phi_n) := \det \begin{bmatrix} \phi_0 & \phi_1 & \cdots & \phi_n \\ \phi_0' & \phi_1' & \cdots & \phi_n' \\ \vdots & \vdots & \ddots & \vdots \\ \phi_0^{(n)} & \phi_1^{(n)} & \cdots & \phi_n^{(n)} \end{bmatrix}.$$

This matrix may be called as the *Wronskian matrix* and its determinant as the *Wronskian determinant*. It was first introduced in 1812 by Wronski, but named 'Wronskian' only in 1882 by Muir. Notice that the Wronskian $W(\phi_{i_0}, \ldots, \phi_{i_k})$ of a subsequence is the determinant of a top submatrix of order $k+1$. In particular, it is the submatrix with the first $k+1$ rows whose columns are indexed by $i_0, \ldots, i_k$. The next result is due to Pólya and Szegö (1971).

Theorem 5.4 (Problem 87, Part 5 [68])**.** *The sequence of n-times differentiable functions $\{\phi_0, \phi_1, \ldots, \phi_n\}$ obeys drs in an interval I iff*

- *each $W(\phi_{i_0}, \phi_{i_1}, \ldots, \phi_{i_k})$ does not have any zeros in I for all $0 \leq i_0 < i_1 < \cdots < i_k \leq n$ and all $0 \leq k \leq n$.*
- *any two such Wronskians with the same number of rows have the same sign.*

We shall skip proof of this theorem here[1]. The important information for us is that Descartes system demands nonvanishing of an exponential number of Wronskians. However, the number of zeros in the specified interval of the linear combination is independent of the functions. Clearly, these exponential number of Wronskians are related to each other. There are only $n+1$ functions involved. So perhaps only the nonvanishing of a linearly (in n) many Wronskians is sufficient. We are interested in answering the following type of question.

Problem 5.5. *Let $\phi_0, \phi_1, \ldots, \phi_n$ be a sequence of n-times differentiable functions in an interval I. What is the factor X such that for any nontrivial linear combination $f := \sum_{i=0}^{n} a_i\phi_i$, we have*

$$N_f I \leq n + X,$$

and the factor X vanishes when $(\{\phi_i\}, I)$ is a Descartes system? Can X be expressed as a linear combination of the Wronskian of linearly many subsequences of $\phi_0, \phi_1, \ldots, \phi_n$?

We do not want to impose conditions of the sequence of functions, and yet find a good upper bound on the number of real zeros of their linear combinations. Theorem 5.4 was a good starting point as it helped us guess that the factor X may be closely related to the Wronskians. We answer Problem 5.5 in Chapter 8. We must also understand what it means for the Wronskian to not vanish in an interval. We shall learn in Chapter 7 that it is closely related to the linear dependence of the functions.

A short detour

Let us quickly verify that $\{1, x, \ldots, x^n\}$ and $(0, \infty)$ forms a Descartes system. Consider the corresponding Wronskian matrix

$$\begin{bmatrix} 1 & x & \ldots & x^n \\ 0 & 1 & \ldots & nx^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & n! \end{bmatrix}.$$

This is an upper triangular matrix with nonzero constant determinant. So it does not vanish in $(0, \infty)$. What about the Wronskian of subsequences? Consider the

[1] See Lecture 9 https://www.imsc.res.in/~vikram/poly-2012/poly.html for a complete proof.

sequence $0 \leq i_0 < i_1 < \cdots < i_k \leq n$, and the Wronskian submatrix

$$\begin{bmatrix} x^{i_0} & x^{i_1} & \dots & x^{i_k} \\ i_0 x^{i_0-1} & i_1 x^{i_1-1} & \dots & i_k x^{i_k-1} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{i_0!}{(i_0-k)!} x^{i_0-k} & \frac{i_1!}{(i_1-k)!} x^{i_1-k} & \dots & \frac{i_k!}{(i_k-k)!} x^{i_k-k} \end{bmatrix}. \tag{5.1}$$

We may first collect the common powers of x (given in the first column) from each of the rows such that every column has the same power of x which can then also bring out, and get

$$x^{i_0(k+1)+\binom{k}{2}} x^{-i_0 k + \sum_{j=1}^{k} i_j} \begin{bmatrix} 1 & 1 & \dots & 1 \\ i_0 & i_1 & \dots & i_k \\ \vdots & \vdots & \ddots & \vdots \\ \frac{i_0!}{(i_0-k)!} & \frac{i_1!}{(i_1-k)!} & \dots & \frac{i_k!}{(i_k-k)!} \end{bmatrix}.$$

After suitable row and column operations, the above matrix can be converted into a Vandermonde matrix of $i_0, i_1, \dots, i_k$ whose determinant is nonzero since i_j's are distinct. Now the other factor $x^{\binom{k}{2}+\sum_{j=0}^{k} i_j}$ has positive power for each $k \geq 1$ and can vanish only at 0, i.e., it never vanishes in $(0, \infty)$. As for $k = 0$, the submatrix is [1] which clearly does not vanish anywhere. This completes the verification.

Some other examples of Descartes system include (See Part 4, Section 7, Pólya and Szegö [68] for more).

- $\{1,\ (x - e_1),\ (x - e_1)(1 - e_2),\ \dots\}$ in $(\max e_i, \infty)$.
- $\{e^{\lambda_1 x}, e^{\lambda_2 x}, e^{\lambda_3 x}, \dots,\}$ in $(-\infty, \infty)$, where $\lambda_1 < \lambda_2 < \cdots$.

Chapter 6

Wronskian Identities

In this chapter, we prove some basic identities involving the Wronskian. They will be needed in Chapter 9 and 10.

Wronskian of the composition of functions

We know that the first derivative of compositions of functions can be obtained simply by chain rule. Faà di Bruno's formula, first stated by Arbogast (1800) [2], gives a generalization of chain rule for higher derivatives.

Proposition 6.1. *(Faà di Bruno's / Arbogast's formula) Let f and g be two r-times differentiable functions for a nonnegative integer r. Then*[1]

$$(f \circ g)^{(r)} = \sum_{s \in \Gamma_r} \frac{r!}{\prod_{l=1}^{r} s_l!(l!)^{s_l}} f^{(|s|)}(g) \prod_{l=1}^{r} \left(g^{(l)}\right)^{s_l},$$

where $\Gamma_r = \{(s_1, \ldots, s_r) \in \mathbb{N}^r : \sum_{l=1}^{r} l s_l = r\}$, *and* $|s| := \sum_{l=1}^{r} s_l$ *for* $s = (s_1, \ldots, s_r)$.

We want to use this formula to simplify the Wronskian of the compositions $\phi_0 \circ \lambda, \ldots, \phi_n \circ \lambda$. The idea is to write the Wronskian matrix of the functions $\phi_0 \circ \lambda, \ldots, \phi_n \circ \lambda$ as a product of two matrices. We can notice there are two factors in each term in Arbogast's formula, but both have a dependency on s. So we shall rewrite the formula. Notice that $|s|$ varies from 0 to r. Define $\Gamma_{r,k} = \{s \in \Gamma_r : |s| = k\}$. Then

$$(f \circ g)^{(r)} = \sum_{k=0}^{r} f^{(k)}(g) \sum_{s \in \Gamma_{r,k}} \frac{r!}{\prod_{l=1}^{r} s_l!(l!)^{s_l}} \prod_{l=1}^{r} \left(g^{(l)}\right)^{s_l}.$$

[1] We assume that $\mathbb{N}$ is the set of nonnegative integers $\mathbb{Z}_{\geq 0}$.

The second factor is now the Bell polynomial. If we define

$$B_{r,k}(y_1,\ldots,y_r) := \sum_{s\in\Gamma_{r,k}} \frac{r!}{\prod_{l=1}^{r} s_l!(l!)^{s_l}} \prod_{l=1}^{r} y_l^{s_l},$$

with $B_{0,k} := 1$, then we have

$$(f\circ g)^{(r)} = \sum_{k=0}^{r} f^{(k)}(g) B_{r,k}(g',g'',\ldots,g^{(r)}).$$

For simplicity, let $B_{r,k,g} := B_{r,k}(g',g'',\ldots,g^{(r)})$. Then, we write the expression as a row-column product

$$(f\circ g)^{(r)} = \begin{bmatrix} B_{r,0,g} & B_{r,1,g} & \ldots & B_{r,r,g} \end{bmatrix} \begin{bmatrix} f^{(0)}(g) & f^{(1)}(g) & \ldots & f^{(r)}(g) \end{bmatrix}^T.$$

Every entry of the Wronskian matrix of $\phi_0\circ\lambda,\ldots,\phi_n\circ\lambda$ has such a decomposition. Therefore, we have

$$W(\phi_0\circ\lambda,\ldots,\phi_n\circ\lambda) = \left(\det_{0\le i,j\le n}[B_{j,i,\lambda}]\right)[W(\phi_0(y),\ldots,\phi_n(y))],$$

where the Wronskian on the RHS is evaluated at $y=\lambda$. Let us examine now the entries of the matrix of Bell polynomials,

$$B_{j,i,\lambda} = B_{j,i}(\lambda',\ldots,\lambda^{(j)}) := \sum_{s\in\Gamma_{j,i}} \frac{j!}{\prod_{l=1}^{j} s_l!(l!)^{s_l}} \prod_{l=1}^{j} (\lambda^{(l)})^{s_l}.$$

For $i>j$, the set $\Gamma_{j,i} = \{s\in\Gamma_j : |s| = i\}$ is empty which means $B_{j,i,\lambda}=0$. Since all such entries lie above the diagonal, the determinant is simply the product of the diagonal entries. Now for $i=j$, the set $\Gamma_{i,i}$ is the singleton set $\{(i,0,\ldots,0)\}$. Therefore, $B_{i,i,\lambda} := (\lambda')^i$ for each $0\le i\le n$, and finally we have.

$$\left(\det_{0\le i,j\le n}[B_{j,i,\lambda}]\right) = (\lambda')^{\sum_{i=0}^{n} i} = (\lambda')^{\frac{n(n+1)}{2}}.$$

Let us summarize this.

Lemma 6.2 (Part Seven, Problem 56, Pólya and Szegö [68]). *Let $\phi_0,\ldots,\phi_n,\lambda$ be n-times differentiable functions. Then,*

$$W(\phi_0\circ\lambda),\ldots,\phi_n\circ\lambda)) = (\lambda')^{\frac{n(n+1)}{2}} W(\phi_0(y),\ldots,\phi_n(y)),$$

where we set $y = \lambda$.

Wronskian of product of functions

Using a similar approach, we can prove another identity for product of functions.

Lemma 6.3 (Part Seven, Problem 57, Pólya and Szegö [68]). *Let* $\phi_0, \dots, \phi_n, \lambda$ *be* n*-times differentiable functions. Then,*

$$W(\lambda\phi_0, \dots, \lambda\phi_n) = \lambda^{n+1} W(\phi_0, \dots, \phi_n).$$

Proof. For $i, j = 0, \dots, n$, the $(i+1, j+1)$th entry of the Wronskian matrix of the functions $\lambda\phi_0, \dots, \lambda\phi_n$ may be thought of as the dot-product of two vectors

$$(\lambda\phi_j)^{(i)} = \sum_{k=0}^{i} \binom{i}{k} \lambda^{(i-k)} \phi_j^{(i)} = \begin{bmatrix} \binom{i}{0}\lambda^{(i)} & \dots & \binom{i}{i}\lambda^{(0)} & 0 \dots 0 \end{bmatrix} \begin{bmatrix} \phi_j & \dots & \phi_j^{(i)} & \dots & \phi_j^{(n)} \end{bmatrix}^T.$$

Now the Wronskian matrix of $\lambda\phi_0, \dots, \lambda\phi_n$ can be expressed as the product

$$\begin{bmatrix} \lambda & 0 & & \dots & 0 \\ \binom{1}{0}\lambda^{(1)} & \lambda & 0 & \dots & 0 \\ \vdots & & \ddots & & \vdots \\ & & & \lambda & 0 \\ \binom{n}{0}\lambda^{(n)} & \dots & \binom{i}{i}\lambda & \dots & \lambda \end{bmatrix} \begin{bmatrix} \phi_0 & \dots & \phi_j & \dots & \phi_n \\ \vdots & & \vdots & & \vdots \\ \phi_0^{(i)} & \dots & \phi_j^{(i)} & \dots & \phi_n^{(i)} \\ \vdots & & \vdots & & \vdots \\ \phi_0^{(n)} & \dots & \phi_j^{(n)} & \dots & \phi_n^{(n)} \end{bmatrix},$$

in which the first matrix is a lower triangular matrix with only λ on the diagonal, while the second matrix is simply the Wronskian matrix of $\phi_0, \dots, \phi_n$, and as a result, their determinants are λ^{n+1} and $W(\phi_0, \dots, \phi_n)$ respectively. This proves the lemma. □

Now given $\phi_0, \dots, \phi_n$, if ϕ_0 is a common factor, then as a corollary we also have the following version that may also be useful.

Corollary 6.4 (Part Seven, Problem 58, Pólya and Szegö [68]). *Let* $\phi_0, \dots, \phi_n$ *be* n*-times differentiable functions. Then,*

$$\begin{aligned} W(\phi_0, \dots, \phi_n) &= \phi_0^{n+1} W\left(1, \phi_1/\phi_0, \dots, \phi_n/\phi_0\right) \\ &= \phi_0^{n+1} W\left((\phi_1/\phi_0)', \dots, (\phi_n/\phi_0)'\right). \end{aligned}$$

One particular application of the previous identities is to the case when $\phi_i(x) = x^{\alpha_i}$ for each $i = 0, \dots, n$ and α_i's are real numbers such that $\alpha_0 < \alpha_1 < \cdots < \alpha_n$.

Then for another function $\lambda(x)$, Lemma 6.2 gives

$$W(\lambda^{\alpha_0}, \lambda^{\alpha_0} \ldots, \lambda^{\alpha_n}) = (\lambda')^{\frac{n(n+1)}{2}} W(y^{\alpha_0}, y^{\alpha_1} \ldots, y^{\alpha_n}),$$

where $y = \lambda$ needs to be substituted on the RHS. Corollary 6.4 may be used to simplify the Wronskian on the RHS,

$$\begin{aligned} W(y^{\alpha_0}, y^{\alpha_1}, \ldots, y^{\alpha_n}) &= \left(y^{\alpha_0(n+1)}\right) W((y^{\alpha_1-\alpha_0})', \ldots, (g^{\alpha_n-\alpha_0})') \\ &= \left(y^{\alpha_0(n+1)}\right) W((\alpha_1-\alpha_0)y^{\alpha_1-\alpha_0-1}, \ldots, (\alpha_n-\alpha_0)y^{\alpha_n-\alpha_0-1}) \\ &= \left(y^{\alpha_0(n+1)} \prod_{j=1}^{n} (\alpha_j - \alpha_0)\right) W(y^{\alpha_1-\alpha_0-1}, \ldots, y^{\alpha_n-\alpha_0-1}) \end{aligned}$$

Continuing in this fashion, we conclude

$$W(y^{\alpha_0}, y^{\alpha_1}, \ldots, y^{\alpha_n}) = y^{\sum_{i=-1}^{n}(n-i)(\alpha_{i+1}-\alpha_i-1)} \prod_{0\le i<j\le n} (\alpha_j - \alpha_i),$$

where $\alpha_{-1} = -1$. The exponent of y simplifies to $\sum_{i=0}^{n} \alpha_i - \frac{n(n+1)}{2}$. Thus finally we have

Corollary 6.5. *Let λ be n-times differentiable function, and let $\alpha_0 < \alpha_1 < \cdots < \alpha_n$ be distinct real numbers. Then,*

$$W(\lambda^{\alpha_0}, \lambda^{\alpha_0} \ldots, \lambda^{\alpha_n}) = (\lambda')^{\frac{n(n+1)}{2}} \lambda^{\sum_{i=0}^{n}\alpha_i - \frac{n(n+1)}{2}} \prod_{0\le i<j\le n} (\alpha_j - \alpha_i).$$

The sum $(\sum_{i=0}^{n} \alpha_i)$ is at least $n(n+1)/2$, and the scalar $\prod_{0\le i<j\le n}(\alpha_j - \alpha_i)$ is nonzero both because α_i's are distinct. In certain case, RHS may also be expressed as

$$\lambda^{\sum_{i=0}^{n}\alpha_i} (\lambda'/\lambda)^{\frac{n(n+1)}{2}} \prod_{0\le i<j\le n} (\alpha_j - \alpha_i),$$

where λ'/λ is the logarithmic derivative. Corollary 6.5 is credited to Wilf (1998) [88], and we have given an alternate proof of it. It is also a generalization of an old determinantal identity due to Mina (1905) [61] where the exponent sequence $\{0, 1, 2, \ldots, n\}$ was considered. Van der Poorten (1978) [86]) says that Mina's identity is one those identities that should be better known.

Wronskian of Wronskians

The next result was known to Frobenius (1874) [31] in an even more general form.

Lemma 6.6 (Part Seven, Problem 59, Pólya and Szegö [68]). *Let $\psi_0, \dots, \psi_n$ be n-times differentiable functions. Then for all $i = 0, 1, \dots, n-1$,*

$$W(W(\psi_0, \dots, \psi_i), W(\psi_0, \dots, \psi_{i-1}, \psi_n)) = W(\psi_0, \dots, \psi_{i-1}) W(\psi_0, \dots, \psi_i, \psi_n),$$

where for $i = 0$ we set $W(\psi_0, \dots, \psi_{i-1}) = 1$.

Proof. Fix some index $i = 0, 1, \dots, n-1$. Then the LHS

$$W(W(\psi_0, \dots, \psi_i), W(\psi_0, \dots, \psi_{i-1}, \psi_n))$$

is a Wronskian of two Wronskians, and therefore involves the derivative of a Wronskian if expanded out. So let us study the derivative $W'(\psi_0, \dots, \psi_i)$ by first writing

$$W(\psi_0, \dots, \psi_i) = \sum_{\sigma \in S_{i+1}} (-1)^{\operatorname{sgn}(\sigma)} \psi^{(0)}_{\sigma(0)} \psi^{(1)}_{\sigma(1)} \cdots \psi^{(i)}_{\sigma(i)},$$

where S_{i+1} is the set of all permutations of $\{0, \dots, i\}$ with $\operatorname{sgn}(\sigma)$ denoting the sign of the permutation σ. Next, consider the derivative

$$\begin{aligned} W'(\psi_0, \dots, \psi_i) &= \sum_{\sigma \in S_{i+1}} (-1)^{\operatorname{sgn}(\sigma)} \sum_{k=0}^{i} \psi^{(0)}_{\sigma(0)} \cdots \psi^{(k-1)}_{\sigma(k-1)} \psi^{(k+1)}_{\sigma(k)} \psi^{(k+1)}_{\sigma(k+1)} \cdots \psi^{(i)}_{\sigma(i)} \\ &= \sum_{k=0}^{i-1} \sum_{\sigma \in S_{i+1}} (-1)^{\operatorname{sgn}(\sigma)} \psi^{(0)}_{\sigma(0)} \cdots \psi^{(k-1)}_{\sigma(k-1)} \psi^{(k+1)}_{\sigma(k)} \psi^{(k+1)}_{\sigma(k+1)} \cdots \psi^{(i)}_{\sigma(i)} \\ &\qquad + \sum_{\sigma \in S_{i+1}} (-1)^{\operatorname{sgn}(\sigma)} \psi^{(0)}_{\sigma(0)} \cdots \psi^{(i-1)}_{\sigma(i-1)} \psi^{(i+1)}_{\sigma(i)}, \end{aligned}$$

and notice that each of the $i+1$ sums can be thought of as the determinant of some matrices. For every $k = 0, \dots, i-1$, we have $\{\sigma(k) \mid \sigma \in S_{i+1}\} = \{\sigma(k+1) \mid \sigma \in S_{i+1}\} = \{0, 1, \dots, i\}$, and therefore for such a k, the sum is a determinant of a matrix whose $(k+1)$th and $(k+2)$th rows are identical. As a result, the first $i+1$ sums vanish, and we get

$$\begin{aligned} W'(\psi_0, \dots, \psi_i) &= \sum_{\sigma \in S_{i+1}} (-1)^{\operatorname{sgn}(\sigma)} \psi^{(0)}_{\sigma(0)} \cdots \psi^{(i-1)}_{\sigma(i-1)} \psi^{(i+1)}_{\sigma(i)} \\ &= \det \begin{bmatrix} \psi_0 & \psi_1 & \dots & \psi_i \\ \vdots & \vdots & \ddots & \vdots \\ \psi_0^{(i-1)} & \psi_1^{(i-1)} & \dots & \psi_i^{(i-1)} \\ \psi_0^{(i+1)} & \psi_1^{(i+1)} & \dots & \psi_i^{(i+1)} \end{bmatrix}, \end{aligned}$$

which is basically the determinant of the matrix obtained by replacing all the entries of the last row of the Wronskian matrix of $\psi_0, \ldots, \psi_i$ with their derivatives.

Next we have

$$LHS = W(\psi_0, \ldots, \psi_i)W'(\psi_0, \ldots, \psi_{i-1}, \psi_n) - W'(\psi_0, \ldots, \psi_i)W(\psi_0, \ldots, \psi_{i-1}, \psi_n),$$

$$RHS = W(\psi_0, \ldots, \psi_{i-1})W(\psi_0, \ldots, \psi_i, \psi_n),$$

and if we denote by X be the $(i+2) \times (i+2)$ Wronskian matrix of $\psi_0, \ldots, \psi_i, \psi_n$, then we can notice that each of the terms in the LHS and the RHS are minors of X, more precisely,

$$\begin{aligned}
W(\psi_0, \ldots, \psi_i) &= \det[X^{i+2}_{i+2}], \qquad & W'(\psi_0, \ldots, \psi_{i-1}, \psi_n) &= \det[X^{i+1}_{i+1}], \\
W'(\psi_0, \ldots, \psi_i) &= \det[X^{i+2}_{i+1}], \qquad & W(\psi_0, \ldots, \psi_{i-1}, \psi_n) &= \det[X^{i+1}_{i+2}], \\
W(\psi_0, \ldots, \psi_{i-1}) &= \det[X^{i+1,i+2}_{i+1,i+2}], \qquad & W(\psi_0, \ldots, \psi_i, \psi_n) &= \det[X],
\end{aligned}$$

where X^B_A denotes the submatrix obtained by removing rows indexed by A and columns indexed by B. Thus the question now is whether the identity

$$\det[X^{i+2}_{i+2}] \det[X^{i+1}_{i+1}] - \det[X^{i+2}_{i+1}] \det[X^{i+1}_{i+2}] = \det[X^{i+1,i+2}_{i+1,i+2}] \det[X]$$

holds true. □

The final identity in the previous proof is exactly the Desnanot-Jacobi identity. For a proof, see [13].

Lemma 6.7 (Desnanot-Jacobi Identity)**.** *Let M be a matrix of order n, then for any two distinct $i, j \in \{1, \ldots .n\}$, we have*

$$\det[M^i_i] \det[M^j_j] - \det[M^i_j] \det[M^j_i] = \det[M^{i,j}_{i,j}] \det[M].$$

According to Bressoud [13], it was discovered by Lagrange (1773) [53] for $n = 3$, proved by Desnanot (1819) [25] for $n \leq 6$, and then by Jacobi (1833) [43] for all n, where n is the order of the matrix. Desnanot-Jacobi Identity is also the basis of Dodgson condension or the method of contractants due to Dodgson (Lewis Caroll) (1866) [26] for computing the determinant of matrices.

Chapter 7

Wronskian and Linear Dependence

The Wronskian is closely related to the linear dependence of functions. Here, we assume real functions that are also real-valued, and they may be defined in all of the real-axis or a certain specified interval. For example, $f : I \to \mathbb{R}$ for any $I \subseteq \mathbb{R}$. The notion of linear dependence of functions is very similar to that of vectors.

Definition 7.1. *A sequence of functions $\phi_0, \phi_1, \ldots, \phi_n$ is linearly dependent in an interval I if there exists a nontrivial real linear combination $\sum_{i=0}^{n} c_i\phi_i$ vanishing at all points in I.*

Immediately, as in Bôcher (1900) [10], we observe the following.

Proposition 7.2. *In some interval, a sequence of functions is linearly dependent if there is a subsequence that is linearly dependent.*

If a function f vanishes at all points in I, then we denote it by $f \equiv_I 0$ or say that f is identically zero in I or write that $f \equiv 0$ in I. Conversely, a sequence of functions $\phi_0, \phi_1, \ldots, \phi_n$ is called *linearly independent* on an interval I if whenever $\sum_{i=0}^{n} c_i\phi_i \equiv_I 0$, it must be the trivial linear combination, i.e. $c_0 = \cdots = c_n = 0$. The derivative of linearly dependent functions are also linearly dependent, i.e., if $\phi_0, \ldots, \phi_n$ are n-times differentiable and linearly dependent functions in I, then there exists c_i's not all zero such that $\sum_{i=0}^{n} c_i\phi_i^{(j)} \equiv_I 0$ for each $j = 0, 1, \ldots n$. We may now capture these $n + 1$ equations using the Wronskian matrix as

$$\begin{bmatrix} \phi_0 & \phi_1 & \cdots & \phi_n \\ \phi_0' & \phi_1' & \cdots & \phi_n' \\ \vdots & \vdots & \ddots & \vdots \\ \phi_0^{(n)} & \phi_1^{(n)} & \cdots & \phi_n^{(n)} \end{bmatrix} \begin{pmatrix} c_0 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} \equiv_I 0.$$

Since the vector of c_i's is nonzero, the Wronskian determinant $W(\phi_0, \ldots, \phi_n)$ is identically zero in I. Thus we have shown.

Proposition 7.3. *Let $\phi_0, \phi_1, \ldots, \phi_n$ be a sequence of n-times differentiable functions in I. If this sequence is linearly dependent in I, then the Wronskian $W(\phi_0, \phi_1, \ldots, \phi_n)$ is identically zero in I.*

Equivalently, if the Wronskian $W(\phi_0, \phi_1, \ldots, \phi_n)$ takes a nonzero value for at least one point in I, then $\phi_0, \phi_1, \ldots, \phi_n$ are linearly independent in I. Peano (1889) [66] pointed out that the converse of this proposition is not necessarily true. Consider the pair of differentiable functions $\phi_0(x) = x^2$ and $\phi_1(x) = x|x|$. They are linearly independent in $\mathbb{R}$, while their Wronskian

$$W(\phi_0, \phi_1) = \begin{cases} \det \begin{bmatrix} x^2 & x^2 \\ 2x & 2x \end{bmatrix} = 0 & \text{if } x \geq 0 \\ \\ \det \begin{bmatrix} x^2 & -x^2 \\ 2x & -2x \end{bmatrix} = 0 & \text{if } x \leq 0 \end{cases}$$

is identically zero in all of $\mathbb{R}$. Bôcher (1901) [11] showed that converse does not become true even for infinitely differentiable real functions. Consider the three functions

$$\phi_0 = \begin{cases} 1 + e^{-1/x^2} & \text{if } x \neq 0, \\ 1 & \text{if } x = 0, \end{cases} \qquad \phi_1 = \begin{cases} 1 + e^{-1/x^2} & \text{if } x > 0, \\ 1 & \text{if } x = 0, \\ 1 - e^{-1/x^2} & \text{if } x < 0, \end{cases} \qquad \phi_2 = 1.$$

These are also linearly independent in $\mathbb{R}$, while their Wronskian

$$W(\phi_0, \phi_1, \phi_2) = \begin{cases} W(1 + e^{-1/x^2}, 1 + e^{-1/x^2}, 1) = 0 & \text{if } x > 0, \\ W(1, 1, 1) = 0 & \text{if } x = 0, \\ W(1 + e^{-1/x^2}, 1 - e^{-1/x^2}, 1) = 0 & \text{if } x < 0, \end{cases}$$

is identically zero in all of $\mathbb{R}$.

When some more information is provided about the Wronskian of a subsequence, then identical vanishing of the Wronskian implies linear dependence.

Theorem 7.4. *[10] Let $\phi_0, \phi_1, \ldots, \phi_n$ be a sequence of n-times differentiable functions in I. If $W(\phi_0, \phi_1, \ldots, \phi_n)$ vanishes identically in I and $W(\phi_0, \phi_1, \ldots, \phi_{n-1})$ does not vanish at any point in I, then $\phi_0, \phi_1, \ldots, \phi_n$ are linearly dependent in I.*

Here, we assume nonvanishing of the Wronskian of first n functions WLOG. But

it could be any n functions among the $n+1$, in which case we reorder the functions.

Proof. Let us proceed by induction. For $n = 0$, consider the function ϕ_0 with the Wronskian $W(\phi_0) = \phi_0 \equiv_I 0$. Clearly, ϕ_0 is linearly dependent in I since it is just a zero function there. Let us also discuss the $n = 1$ case for two functions $\{\phi_0, \phi_1\}$ since it motivates our argument in the general case. Suppose that $W(\phi_0, \phi_1) \equiv_I 0$, i.e., $\phi_0\phi_1' - \phi_0'\phi_1 \equiv_I 0$. Now since ϕ_0 is assumed to not vanish in I, we may divide both sides of the identity by ϕ_0^2 to get

$$\frac{\mathrm{d}}{\mathrm{d}x}\left(\frac{\phi_1}{\phi_0}\right) \equiv_I 0.$$

Then ϕ_1/ϕ_0 is constant in I and thus linearly dependent.

Next, consider the sequence of functions $\phi_0, \ldots, \phi_n$ with

$$W(\phi_0, \ldots, \phi_n) = \det \begin{bmatrix} \phi_0 & \phi_1 & \cdots & \phi_n \\ \phi_0' & \phi_1' & \cdots & \phi_n' \\ \vdots & \vdots & \ddots & \vdots \\ \phi_0^{(n)} & \phi_1^{(n)} & \cdots & \phi_n^{(n)} \end{bmatrix} \equiv_I 0, \tag{7.1}$$

and assume that the Wronskian $W(\phi_0, \ldots, \phi_{n-1})$ of the first $n-1$ functions does not vanish in I. Denote by $W_0, \ldots, W_n$ the cofactors corresponding to the entries of the last row of the Wronskian matrix of $\phi_0, \ldots, \phi_n$. Then we may observe that each

$$W_i = (-1)^{n+2+i} W(\phi_0, \ldots, \phi_{i-1}, \phi_{i+1}, \ldots, \phi_n) \qquad (i = 0, \ldots, n),$$

is given by the Wronskian of the sequence $\{\phi_0, \ldots, \phi_n\} \backslash \phi_i$. Thus expanding along the last row, we get

$$W_0\phi_0^{(n)} + W_1\phi_1^{(n)} + \cdots + W_n\phi_n^{(n)} \equiv_I 0.$$

Here, W_n does not vanish in I by hypothesis. We have obtained a linear combination of nth derivatives, but not yet of the original functions themselves. Moreover, it is not yet a real linear combination.

Next, recall that for any matrix A we have $A\mathrm{adj}(A) = \det(A)I$, where $\mathrm{adj}(A)$ is adjugate matrix, the transpose of the matrix of cofactors, and I is the identity matrix. If we take A to be the Wronskian matrix of $\phi_0, \ldots, \phi_n$, then $\det(A) =$

$W(\phi_0, \ldots, \phi_n) \equiv_I 0$. Now we may write $A\text{adj}(A) \equiv_I 0$ as

$$\begin{bmatrix} \phi_0 & \phi_1 & \ldots & \phi_n \\ \phi_0' & \phi_1' & \ldots & \phi_n' \\ \vdots & \vdots & \ddots & \vdots \\ \phi_0^{(n)} & \phi_1^{(n)} & \ldots & \phi_n^{(n)} \end{bmatrix} \begin{bmatrix} \star & \star & \ldots & W_0 \\ \star & \star & \ldots & W_1 \\ \vdots & \vdots & \ddots & \vdots \\ \star & \star & \ldots & W_n \end{bmatrix} \equiv_I 0,$$

and derive a total of $n+1$ identities given by the rows of the matrix-vector product

$$\begin{bmatrix} \phi_0 & \phi_1 & \ldots & \phi_n \\ \phi_0' & \phi_1' & \ldots & \phi_n' \\ \vdots & \vdots & \ddots & \vdots \\ \phi_0^{(n)} & \phi_1^{(n)} & \ldots & \phi_n^{(n)} \end{bmatrix} \begin{bmatrix} W_0 \\ W_1 \\ \vdots \\ W_n \end{bmatrix} \equiv_I 0. \tag{7.2}$$

To conclude from here that there is a nontrivial real linear combination of $\phi_0, \ldots, \phi_n$ that is identically zero in I, we could try to show that any two W_i's are linearly dependent, in particular,

Claim. *For each $i = 0, 1, \ldots, n-1$ there exists a constant c_i such that $W_i \equiv_I c_i W_n$.*

Substituting this claim in the equation given by the first row of 7.2, we get

$$W_n(c_0\phi_0 + \cdots + c_{n-1}\phi_{n-1} + \phi_n) \equiv_I 0.$$

Now W_n does not vanish in I by the hypothesis, so we can conclude that there is nontrivial linear combination of $\phi_0, \ldots, \phi_n$ that vanishes identically in I. This completes our proof of the theorem.

What remains now is the proof of the claim that we just used. The identities given by the first two rows of 7.2 seem to be related by differentiation. Let us disregard the $(n+1)$th row so as not to deal with $(n+1)$th derivatives, and consider the derivative of each of the first n identities

$$\begin{bmatrix} \phi_0' & \phi_1' & \ldots & \phi_n' \\ \phi_0'' & \phi_1'' & \ldots & \phi_n'' \\ \vdots & \vdots & \ddots & \vdots \\ \phi_0^{(n)} & \phi_1^{(n)} & \ldots & \phi_n^{(n)} \end{bmatrix} \begin{bmatrix} W_0 \\ W_1 \\ \vdots \\ W_n \end{bmatrix} + \begin{bmatrix} \phi_0 & \phi_1 & \ldots & \phi_n \\ \phi_0' & \phi_1' & \ldots & \phi_n' \\ \vdots & \vdots & \ddots & \vdots \\ \phi_0^{(n-1)} & \phi_1^{(n-1)} & \ldots & \phi_n^{(n-1)} \end{bmatrix} \begin{bmatrix} W_0' \\ W_1' \\ \vdots \\ W_n' \end{bmatrix} \equiv_I 0.$$

Here, the first term corresponds to the last n identities in 7.2 which are identically

zero. Thus we get a new system of n identities

$$\begin{bmatrix} \phi_0 & \phi_1 & \dots & \phi_n \\ \phi_0' & \phi_1' & \dots & \phi_n' \\ \vdots & \vdots & \ddots & \vdots \\ \phi_0^{(n-1)} & \phi_1^{(n-1)} & \dots & \phi_n^{(n-1)} \end{bmatrix} \begin{bmatrix} W_0' \\ W_1' \\ \vdots \\ W_n' \end{bmatrix} \equiv_I 0. \tag{7.3}$$

Next, multiply the system 7.3 by W_n and system 7.2 by W_n' and consider their difference

$$\begin{bmatrix} \phi_0 & \phi_1 & \dots & \phi_n \\ \phi_0' & \phi_1' & \dots & \phi_n' \\ \vdots & \vdots & \ddots & \vdots \\ \phi_0^{(n-1)} & \phi_1^{(n-1)} & \dots & \phi_n^{(n-1)} \end{bmatrix} \begin{bmatrix} W_0'W_n - W_0W_n' \\ W_1'W_n - W_1W_n' \\ \vdots \\ W_n'W_n - W_nW_n' \end{bmatrix} \equiv_I 0.$$

Here, the last column of the matrix becomes redundant since the last entry of the vector becomes zero. Thus we have now essentially reduced the dimension of the problem

$$\begin{bmatrix} \phi_0 & \phi_1 & \dots & \phi_{n-1} \\ \phi_0' & \phi_1' & \dots & \phi_{n-1}' \\ \vdots & \vdots & \ddots & \vdots \\ \phi_0^{(n-1)} & \phi_1^{(n-1)} & \dots & \phi_{n-1}^{(n-1)} \end{bmatrix} \begin{bmatrix} W_0'W_n - W_0W_n' \\ W_1'W_n - W_1W_n' \\ \vdots \\ W_{n-1}'W_n - W_{n-1}W_n' \end{bmatrix} \equiv_I 0.$$

The determinant of the matrix on the left is the Wronskian W_n which is nonvanishing in all of I. Thus we must have

$$W_i'W_n - W_iW_n' \equiv_I 0 \qquad \text{for each } i = 0, 1, \dots, n-1.$$

Dividing by W_n, we obtain, as done for $n = 1$ case,

$$\frac{\mathrm{d}}{\mathrm{d}x}\left(\frac{W_i}{W_n}\right) \equiv_I 0 \implies W_i \equiv_I c_i W_n,$$

for some real constant c_i, as required. □

Let us have a look at the hypothesis of Theorem 7.4 again. The nonvanishing of the Wronskian $W(\phi_0, \dots, \phi_{n-1})$ also implies that it is not identically zero in particular. By Proposition 7.3, the subsequence $\phi_0, \dots, \phi_{n-1}$ is thus assumed to be at least linearly independent. It is possible to remove this assumption to get a slightly different version.

Theorem 7.5. *[10] Let $\phi_0, \phi_1, \dots, \phi_n$ be a sequence of n-times differentiable func-*

tions in I. If $W(\phi_0, \phi_1, \ldots, \phi_n)$ vanishes identically in I, then there is a subinteval of I in which $\phi_0, \phi_1, \ldots, \phi_n$ are linearly dependent.

Proof. Let us proceed by induction again. Suppose only that $W(\phi_0, \ldots, \phi_n)$ vanishes identically in I. Then there are two cases. If $W(\phi_0, \ldots, \phi_{n-1})$ vanishes nowhere in I, then $\phi_0, \ldots, \phi_n$ are linearly dependent by Theorem 7.4. Otherwise, if $W(\phi_0, \ldots, \phi_{n-1})$ vanishes at some point I, then consider a subinterval of I where it does not vanish. The statement then follows by Theorem 7.4. Such a subinterval exists because otherwise $W(\phi_0, \ldots, \phi_{n-1})$ vanishes identically in I, in which case we conclude by inductive hypothesis that $\phi_0, \ldots, \phi_{n-1}$ are linearly dependent, and by Proposition 7.2 the statement follows. □

So far we have discussed linear dependence for real functions. The identical vanishing of the Wronskian is also a sufficient condition for the linear dependence of (complex) analytic functions. These functions are complex valued and defined over some region of the complex plane.

Theorem 7.6. *[10] A sequence $\phi_0, \phi_1, \ldots, \phi_n$ of analytic functions (defined over some $\Omega \subseteq \mathbb{C}$) are linearly dependent in $\mathbb{C}$ if and only if $W(\phi_0, \ldots, \phi_n) \equiv 0$.*

Does this result extend to real analytic functions, i.e., those analytic functions $f : I \to \mathbb{R}$ defined over a real interval $I \subseteq \mathbb{R}$ and may take real values? In the proof of the next result, we make use of the analytic continuation of functions which states that if a real analytic function f defined in an interval I vanishes identically in a subinterval $I' \subseteq I$ then it also vanishes identically in I.

Theorem 7.7. *A sequence $\phi_0, \phi_1, \ldots, \phi_n$ of real analytic functions defined in I are linearly dependent in I if and only if $W(\phi_0, \phi_1, \ldots, \phi_n)$ vanishes identically in I.*

Proof. Suppose that $W(\phi_0, \phi_1, \ldots, \phi_n) \equiv_I 0$. Then since the functions are infinitely differentiable in I, there exists a subinterval $I' \subseteq I$ on which they are linearly dependent by Theorem 7.5. Thus there exists a nontrivial linear combination $\sum_{i=0}^{n} c_i \phi_i$ that is is identically zero in I'. A property of real analytic functions implies that $\sum_{i=0}^{n} c_i \phi_i$ is then also identically zero in all of I. This means that the sequence of functions is linearly dependent in I. Converse is similar to the proof of Proposition 7.3. □

What is the usefulness of this theorem in the context of counting zeros? If the functions are linearly dependent, their their Wronskian has infinitely many zeros in that interval. So it makes sense to consider Wronskians of only the linearly independent functions if they were to appear in any upper found on some quantity.

Now the Wronskian of real analytic functions is also real analytic, and if it does not vanish identically in an interval, then all its zeros are isolated. In particular, the Wronskian of linearly independent real polynomials has finite number of zeros in that interval.

These insights about the Wronskian and the linear depedence will be helpful in the next two chapters where we discuss counting of zeros of sum of functions.

Chapter 8

Zeros of the Sum of Two Functions

We wish to study zeros of a linear combination of functions. Since we could assume that each scalar in the linear combination is nonzero, it suffices to restrict to just the sum of functions. As a customary approach, let us start with two real analytic function g and h in the interval I, and denote their sum by $f := g + h$. From Problem 5.5, we guess that the upper bound on the number of zeros of f must be of the form

$$N_f I \leq 1 + c_1 N_{W(g,h)} I + c_2 N_g I + c_3 N_h I.$$

Obviously, it may turn out that the upper bound does not have this form. But we have at least guessed that $N_{W(g,h)}I$ is likely to appear in the upper bound. So instead of finding an upper bound on $N_f I$, let us now focus on finding a lower bound on $N_{W(g,h)}I$. The advantage is that we have a little more information about the zeros of $W(g, h)$. For instance, a direct observation we can make about the sum $f := g+h$ is that the common zeros of g and h are also the zeros of f. On the other hand, from $W(g, h) = gh' - g'h$, we can say that not only the common zeros but also the repeated zeros of g and h are the zeros of $W(g, h)$. This suggests that we could express the Wronskian as follows

$$W(g, h) = gh \left(\frac{h'}{h} - \frac{g'}{g} \right).$$

Now there is a factor in this decomposition that is again a linear combination of two new rational functions, but linear combination of functions is what we want to understand in the first place. These new functions h'/h and g'/g are logarithmic derivatives of h and g respectively. It will be easier for us to deal with one logarithmic

derivative instead of two. Observe that

$$\frac{h'}{h} - \frac{g'}{g} = \frac{g}{h}\left(\frac{h}{g}\right)' \implies W(g,h) = g^2\left(\frac{h}{g}\right)'.$$

Remember our ultimate goal is to upper bound $N_f I$. So we must relate $W(g,h)$ with $f := g + h$ as well. The relation is given by the identity

$$W(g,h) = W(g,f),$$

which is easily obtained by writing out the RHS. So now, equivalently, we can examine zeros of $W(g,f)$ instead. Similarly for $W(g,f)$, we may write

$$W(g,f) = g^2\left(\frac{f}{g}\right)'.$$

This identity is going to be very crucial for us. However, there is a caveat: $W(g,f)$ is analytic in I, but the derivative $(f/g)'$ is analytic only at points where g does not vanish. Therefore, we must examine $W(g,f)$ separately in the subinterval where g vanishes and where it does not.

Let $Z_g I$ denote the set of zeros of g in I. Since g has $N_g^\circ I$ distinct zeros in I, we have $|Z_g I| = N_g^\circ I$. Also g is analytic in I and analytic functions can vanish at only isolated points, therefore $Z_g I$ is a discrete set. Now consider the subset $J := I \backslash (Z_g I)$ obtained by removing all the zeros of g in I. Then J is the disjoint union of $t := N_g^\circ I + 1$ many subintervals (say) $J_1, J_2, \ldots, J_t$ of I. Let us write

$$N_{W(g,f)} I = N_{W(g,f)}(Z_g I) + N_{W(g,f)} J,$$

and estimate each of the two quantities on the RHS separately.

Firstly, a point in J is a zero $W(g,f)$ if and only if it is also a zero of $(f/g)'$. Therefore,

$$N_{W(g,f)} J = N_{(f/g)'} J = \sum_{i=1}^{t} N_{(f/g)'} J_i.$$

By Rolle's theorem, to be precise, by Corollary 4.4, we have for each interval

$$N_{(f/g)'} J_i \geq N_{f/g} J_i - 1, \tag{8.1}$$

and therefore after adding these inequalities for $i = 1, \ldots, t$, we get

$$N_{(f/g)'} J \geq N_{f/g} J - N_g^\circ I - 1.$$

Here, we have $N_{f/g}J = N_f J$ because g has no zeros in J. Thus we have an estimate on the first quantity

$$N_{W(g,f)}J \geq N_f J - N_g^\circ I - 1.$$

Secondly, to estimate $N_{W(g,f)}(Z_g I)$, observe that a point in $Z_g I$ is already a zero of g, and so it is a zero of $W(g,f) := gf' - g'f$ if and only if it also a zero of $g'f$. Thus

$$N_{W(g,f)}(Z_g I) = N_{g'f}(Z_g I) = N_{g'}(Z_g I) + N_f(Z_g I). \tag{8.2}$$

The term $N_{g'}(Z_g I)$ counts the number of critical points of the first kind of g in $Z_g I$, and therefore in I, because g has no zeros in J. By Proposition 4.2, we have

$$N_{g'}(Z_g I) = N_g I - N_g^\circ I.$$

Finally, after these substitutions, we have the lower bound

$$\begin{aligned} N_{W(g,f)}I &\geq N_g I - N_g^\circ I + N_f(Z_g I) + N_f J - N_g^\circ I - 1 \\ &\geq N_g I - 2N_g^\circ I + N_f I - 1, \end{aligned}$$

where we combine $N_f(Z_g I) + N_f J$ as $N_f I$. Now rearranging and then substituting $N_{W(g,f)}I = N_{W(g,h)}I$, we get

$$N_f I \leq 1 + N_{W(g,h)}I + 2N_g^\circ I - N_g I.$$

Thus we have shown

Lemma 8.1. *Let g and h be real analytic on I, and let $f := g + h$. Then,*

$$N_f I \leq 1 + N_{W(g,h)}I + 2N_g^\circ I - N_g I.$$

We could assume that g and h are linearly independent in I in the premise of this lemma, otherwise $W(g,h)$ vanishes identically in I by Theorem 7.7 and the upper bound is not useful. It must be also stressed that the upper bound in Lemma 8.1 strongly depends on the lower bound in Equation 8.1 that we obtained through Corollary 4.4. In fact, it is the only source of inequality. Thus any hope for improving this result must come through strengthening Corollary 4.4, and we have seen that to do that we must understand zeros of logarithmic derivatives. If we write the

inequality we just obtained as

$$N_f I \leq 1 + N_{W(g,h)} I + N_g^\circ I - (N_g I - N_g^\circ I),$$

then the quantity $N_g I - N_g^\circ I$, by Proposition 4.2, is the number of critical points of the first kind of g, and such points are also the zeros of the Wronskian $W(g,h)$. Lemma 8.1 avoids this overcounting by subtracting $N_g I - N_g^\circ I$. Since $2N_g^\circ I - N_g I \leq N_g I$, a weaker result can also be stated if one prefers only the counting functions that take into account the zeros according to their multiplicities.

Corollary 8.2. *Let g and h be real analytic on I, and let $f := g + h$. Then,*

$$N_f I \leq 1 + N_{W(g,h)} I + N_g I.$$

In the case that both g and h have simple zeros, Lemma 8.1 and Corollary 8.2 give the same estimate. But Lemma 8.1 may be preferred when there are a lot of repeated zeros.

Counting Distinct Zeros

We may also count distinct real zeros by exactly the same argument. Analogous to Equation 8.1, we may write, by Corollary 4.4,

$$N_{(f/g)'}^\circ J_i \geq 2N_{f/g}^\circ J_i - S_{f/g} J_i - 1, \tag{8.3}$$

where $S_{f/g} J_i$ is the number of simple real zeros of f/g in J_i. Adding these inequalities for $i = 1, \ldots, t$, and using again the observation that f/g and f have the same zeros in J, to get

$$N_{W(g,f)}^\circ J = N_{(f/g)'}^\circ J \geq 2N_f^\circ J - S_f J - N_g^\circ I - 1.$$

Next, analogous to Equation 8.2, consider

$$N_{W(g,f)}^\circ(Z_g I) = N_{g'f}^\circ(Z_g I) = N_f^\circ(Z_g I) + N_{g'}^\circ(Z_g I) - N_{g',f}^\circ(Z_g I),$$

where $N_{g',f}^\circ(Z_g I)$ denotes the number of distinct common zeros of g' and f in $Z_g I$. Unlike the previous case where we accounted for multiplicities, the quantity $N_{g',f}^\circ(Z_g I)$ must be subtracted so as not to overcount distinct zeros of $g'f$. Let us observe that $N_{g'}^\circ(Z_g I) - N_{g',f}^\circ(Z_g I)$ is the number of non-simple distinct zeros of g in I that are not zeros of f. Thus if $J' := I \backslash (Z_f I)$ denotes the set of points where

f does not vanish, then we can write

$$N^\circ_{g'}(Z_g I) - N^\circ_{g',f}(Z_g I) = N^\circ_g J' - S_g J'.$$

Finally, combining the two estimates,

$$\begin{aligned} N^\circ_{W(g,f)} I &\geq (2N^\circ_f J - S_f J - N^\circ_g I - 1) + (N^\circ_f(Z_g I) + N^\circ_g J' - S_g J') \\ &\geq (N^\circ_f I - N^\circ_g I - 1) + (N^\circ_f J - S_f J) + (N^\circ_g J' - S_g J'), \end{aligned}$$

rearranging and then substituting $N^\circ_{W(g,f)} I = N^\circ_{W(g,h)} I$, we get

$$N^\circ_f I \leq (1 + N^\circ_{W(g,h)} I + N^\circ_g I) - (N^\circ_f J - S_f J) - (N^\circ_g J' - S_g J'), \tag{8.4}$$

Note that $(N^\circ_f J - S_f J)$ is nonnegative as it is the number of distinct critical points of the first kind of f that are not zeros of g in I (Proposition 4.2). Such points have already been accounted for in $N^\circ_{W(g,h)} I$ because the Wronskian $W(g,h)$ vanishes at those points. Likewise, $(N^\circ_g J' - S_g J')$ is also nonnegative as it is the number of critical points of the first kind of g that are not zeros of f, and the Wronskian $W(g,f) = W(g,h)$ vanishes at such points as well. Thus we have avoided overcounting. At this point, we may also state a weaker result analogous to Corollary 8.2.

Corollary 8.3. *Let g and h be real analytic on I, and let $f := g + h$. Then,*

$$N^\circ_f I \leq 1 + N^\circ_{W(g,h)} I + N^\circ_g I.$$

Technically, we must consider $\min\{N^\circ_g I, N^\circ_h I\}$ in place of $N^\circ_g I$ on the RHS of the inequality in the lemma, and likewise in the previous results or the following. We avoid mentioning this explicitly because we could assume without loss of generality that $N^\circ_g I \leq N^\circ_h I$ or simply flip the order of g and h.

Next, let us simplify the terms in Equation 8.4 by substituting back $J = I \backslash (Z_g I)$ and $J' = I \backslash (Z_f I)$. The RHS must be free of f, and involve only g and h. Consider first $N^\circ_f J$ which we can simplify as $N^\circ_f J = N^\circ_f I - N^\circ_f(Z_g I)$. Since $f = g + h$, the quantity $N^\circ_f(Z_g I)$ is the same as $N^\circ_h(Z_g I)$, which is the number of distinct common zeros of g and h in I, i.e. $N^\circ_{g^2+h^2} I$. Thus

$$N^\circ_f J = N^\circ_f I - N^\circ_{g^2+h^2} I.$$

Similarly, we obtain

$$S_f J = S_f I - S_{g^2+h^2} I, \qquad N^\circ_g J' = N^\circ_g I - N^\circ_{g^2+h^2} I, \qquad S_g J' = S_g I - S_{g^2+h^2} I.$$

Substituting these four identities in Equation 8.4, we conclude with

Lemma 8.4. *Let g and h be real analytic on I, and let $f := g + h$. Then,*

$$2N_f^\circ I - S_f I \leq (1 + N_{W(g,h)}^\circ I + S_g I) + 2(N_{g^2+h^2}^\circ I - S_{g^2+h^2} I).$$

Although the sum of two functions appear in the RHS, the quantity $N_{g^2+h^2}^\circ I$ is to be read as the number of distinct common zeros of g and h in I, and for polynomials, it will be the number of distinct zeros of the GCD of g and h in I. The LHS may be simplified by observing $N_f^\circ I \leq 2N_f^\circ I - S_f I$. We must also remark here that any improvement in Lemma 8.4 must come through Equation 8.3, i.e. Rolle's theorem, as it is the only source of inequality.

Lemma 8.4 gives a tighter estimate than Corollary 8.3. In the case that both g and h have only simple zeros, the estimate from Lemma 8.4 simplifies to $2N_f^\circ I - S_f I \leq 1 + N_{W(g,h)}^\circ I + N_g^\circ I$ which is more or less the same conclusion from Corollary 8.3. But Lemma 8.4 may be preferred when there are a lot of repeated zeros.

Application to $gh + t$

At this point, if we remember that we have also been looking for an upper bound on the number of real zeros of the sum $gh + t$, where g and h are real polynomials and t is some nonzero real number, then Lemma 8.1 and 8.4 do not help much because they give us the inequalities

$$N_{gh+t}\mathbb{R} \leq 1 + N_{(gh)'}\mathbb{R} \qquad \& \qquad 2N_{gh+t}^\circ\mathbb{R} \leq 1 + N_{(gh)'}^\circ\mathbb{R} + S_{gh+t}\mathbb{R},$$

both of which are also obtainable by a direct application of Rolle's theorem (Proposition 4.4). This is not surprising because the source of the offset in both Lemma 8.1 and 8.4 is precisely Proposition 4.4. So this is perhaps one more reason for us understand zeros of the logarithmic derivative.

Chapter 9

Zeros of the Sum of Multiple Functions

Let us start with the weaker result that is Corollary 8.2, and which says that for two real analytic functions g and h in I we have

$$N_{g+h}I - N_gI \leq 1 + N_{W(g,h)}I.$$

Our next goal is to generalize such a result to the sum of more than two functions. If we are given a sequence $\phi_0, \ldots, \phi_n$ of real analytic functions in I, then a naive approach to get an upper bound on $N_{\phi_0+\cdots+\phi_n}I$ would be to consider the sequence of inequalities

$$\begin{aligned}
N_{\phi_0+\cdots+\phi_n}I - N_{\phi_0+\cdots+\phi_{n-1}}I &\leq 1 + N_{W(\phi_0+\cdots+\phi_{n-1},\phi_n)}I,\\
N_{\phi_0+\cdots+\phi_{n-1}}I - N_{\phi_0+\cdots+\phi_{n-2}}I &\leq 1 + N_{W(\phi_0+\cdots+\phi_{n-2},\phi_{n-1})}I,\\
&\vdots\\
N_{\phi_0+\phi_1}I - N_{\phi_0}I &\leq 1 + N_{W(\phi_0,\phi_1)}I,
\end{aligned}$$

and add them up to get

$$N_{\phi_0+\cdots+\phi_n}I \leq n + \sum_{i=0}^{n} N_{W(\phi_0+\cdots+\phi_{i-1},\phi_i)}I.$$

However, there are partial sum of functions involved in the RHS. We expect to get an upper bound that involves the term $N_{W_i}I$ for $i = 0, \ldots, n$ where $W_i = W(\phi_0, \ldots, \phi_i)$. So we must use Corollary 8.2 in a clever manner. The crucial observation that led to the proof of Corollary 8.2 was $W(g, h) = W(g, f)$ where $f := g + h$, and it suggests that we could rephrase the result slightly differently.

Corollary 9.1. *Let f and g be real analytic on I. Then,*

$$N_f I - N_g I \leq 1 + N_{W(g,f)} I.$$

From now on let $f := \phi_0 + \cdots + \phi_n$. Let us also define $H_i := W(\phi_0, \ldots, \phi_{i-1}, f)$ for $i = 0, 1, \ldots, n$ where $H_0 = f$ and $H_n = W_n$. Then Corollary 9.1 for $H_0 = f$ and $W_0 = \phi_0$ gives us $N_f I - N_{\phi_0} I \leq 1 + N_{W(\phi_0,f)} I$, which is the same inequality as before if we set $n = 1$. We could now try generalizing from this point by applying Corollary 9.1 to H_i and W_i to get the inequality

$$N_{H_i} I - N_{W_i} I \leq 1 + N_{W(W_i,H_i)} I,$$

and sum it over $i = 0, 1, \ldots, n-1$ to get

$$N_f I = N_{H_0} I \leq n + \sum_{i=0}^{n-1} N_{W_i} I + \sum_{i=0}^{n-1} N_{W(W_i,H_i)} I - \sum_{i=0}^{n-2} N_{H_{i+1}} I. \tag{9.1}$$

We avoid adding the inequality for $i = n$ because it becomes trivial due to $H_n = W_n$. We have now brought $N_{W_i} I$'s in the upper bound as we expected, but with extra terms which may be simplified if we investigate the relation between W_i and H_i that they obviously have.

Next, consider for $i = 0, 1, \ldots, n-1$, the Wronskian

$$W(W_i, H_i) = W(W(\phi_0, \ldots, \phi_i), W(\phi_0, \ldots, \phi_{i-1}, f)).$$

Observe that $\phi_0, \phi_1, \ldots, \phi_{n-1}, f$ is the sequence of functions involved in the RHS, so we may study the RHS for any arbitrary $\psi_0, \psi_1, \ldots, \psi_n$, and ultimately substitute

$$\psi_i = \phi_i \text{ for each } i = 0, \ldots, n-1, \text{ and } \psi_n = f. \tag{9.2}$$

For $n = 1$ we have $W(\psi_0, \psi_1)$, so let us start with the nontrivial $n = 2$ case of which $i = 2$ is a nontrivial subcase. Consider ψ_0, ψ_1, ψ_2 and the Wronskian $W(W(\psi_0, \psi_1), W(\psi_0, \psi_2))$. Here, ψ_0 is a common function which may be brought outside

$$\begin{aligned} W(W(\psi_0, \psi_1), W(\psi_0, \psi_2)) &= W(\psi_0\psi_1' - \psi_0'\psi_1, \psi_0\psi_2' - \psi_0'\psi_2) \\ &= W(\psi_0^2(\psi_1/\psi_0)', \psi_0^2(\psi_2/\psi_0)') \\ &= \psi_0^4 W((\psi_1/\psi_0)', (\psi_2/\psi_0)') \\ &= \psi_0 W(\psi_0, \psi_1, \psi_2) \end{aligned}$$

using Lemma 6.3 and 6.4. By substituting $\psi_0 = \phi_0$, $\psi_1 = \phi_1$ and $\psi_2 = \phi_0 + \phi_1$, we obtain $W(W_1, H_1) = W_0 H_2$, and it suggests that perhaps its extension

$$W(W_i, H_i) = W_{i-1} H_{i+1} \tag{9.3}$$

is also true for all $i = 1, \ldots, n-1$. Now if can prove the identity

$$W(W(\psi_0, \ldots, \psi_i), W(\psi_0, \ldots, \psi_{i-1}, \psi_n)) = W(\psi_0, \ldots, \psi_{i-1}) W(\psi_0, \ldots, \psi_i, \psi_n),$$

then we can simply substitute 9.2 in it to get Equation 9.3. But this identity is exactly the Lemma 6.6. So now the consequence of Equation 9.3 is that for all $i = 0, 1, \ldots, n-1$

$$N_{W(W_i, H_i)} I = N_{W_{i-1}} I + N_{H_{i+1}} I, \tag{9.4}$$

with $W_{-1} = 1$, and after substituting it in Equation 9.1, we get

$$\begin{aligned} N_f I = N_{H_0} I &\leq n + \sum_{i=0}^{n-1} N_{W_i} I + \sum_{i=0}^{n-1} (N_{W_{i-1}} I + N_{H_{i+1}} I) - \sum_{i=0}^{n-2} N_{H_{i+1}} I \\ &\leq n + N_{W_{n-1}} I + 2 \sum_{i=0}^{n-2} N_{W_i} I + N_{H_n} I. \end{aligned}$$

Since $H_n = W_n$, we are led to the following result due to Voorhoeve and van der Poorten (1975).

Theorem 9.2. *[87] Let $\phi_0, \ldots, \phi_n$ be real analytic functions on an interval I. Then for the sum $f := \sum_{i=0}^{n} \phi_i$, we have*

$$N_f I \leq n + N_{W_n} I + N_{W_{n-1}} I + 2 \sum_{i=0}^{n-2} N_{W_i} I.$$

The upper bound of this theorem captures the conditions required for a Descartes system in the sense that when $(\{\phi_i\}, I)$ forms a Descartes system, then by Theorem 5.4, we get $N_f I \leq n$ since each W_i has no zeros in I. Indeed, the factor X in Problem 5.5 is a linear combination of $n+1$ Wronskians. This addresses Problem 5.5. The heart of the proof of Theorem 9.2 is Corollary 8.2. Since a stronger version of Corollary 8.2 is Lemma 8.1, we may improve Theorem 9.2 as well. By Lemma 8.1, we get an analogous result to Corollary 9.1.

Corollary 9.3. *Let f and g be real analytic on I. Then,*

$$N_f I \leq 1 + N_{W(g,f)} I + 2N_g^\circ I - N_g I.$$

Next, for H_i and W_i this Corollary and Equation 9.4 gives us the inqualitity

$$\begin{aligned} N_{H_i} I &\leq 1 + N_{W(W_i,H_i)} I + 2N_{W_i}^\circ I - N_{W_i} I \\ &\leq 1 + N_{W_{i-1}} I - N_{W_i} I + N_{H_{i+1}} I + 2N_{W_i}^\circ I, \end{aligned}$$

and now adding it for $i = 0, 1, \ldots, n-1$ gets us

$$N_{H_0} I \leq n - N_{W_{n-1}} I + N_{H_n} I + 2\sum_{i=0}^{n-1} N_{W_i}^\circ I. \tag{9.5}$$

Since $H_0 = f$ and $H_n = W_n$, we now have an improvement of Theorem 9.2.

Theorem 9.4. *Let $\phi_0, \ldots, \phi_n$ be real analytic functions on an interval I. Then for the sum $f := \sum_{i=0}^n \phi_i$, we have*

$$N_f I \leq n + N_{W_n} I - N_{W_{n-1}} I + 2\sum_{i=0}^{n-1} N_{W_i}^\circ I.$$

Counting Distinct Zeros

It will be helpful for us to obtain results analogous to Theorem 9.2 and 9.4 for counting distinct zeros, and in fact such results are needed in Section 10. Our main tool here will be Corollary 8.3 or Lemma 8.4. If we use Corollary 8.3, then the proof is identical to that of Theorem 9.2 except that we must replace Equation 9.4 with the following

$$N_{W(W_i,H_i)}^\circ I \leq N_{W_{i-1}}^\circ I + N_{H_{i+1}}^\circ I. \tag{9.6}$$

However, it does not affect the form of the conclusion. The next result is due to Koiran, Portier and Tavenas (2015) [48].

Theorem 9.5. *Let $\phi_0, \ldots, \phi_n$ be real analytic functions on an interval I. Then for the sum $f := \sum_{i=0}^n \phi_i$, we have*

$$N_f^\circ I \leq n + N_{W_n}^\circ I + N_{W_{n-1}}^\circ I + 2\sum_{i=0}^{n-2} N_{W_i}^\circ I.$$

It is possible to state an improvement of Theorem 9.5 by using Lemma 8.4 instead of Corollary 8.3. However, there will be terms counting simple zeros. So we must also investigate how to count simple zeros, in particular, simple common zeros of W_i and H_i.

Koiran et al also ask whether the constant factor of '2' can be shaved off, i.e. whether $N_f^\circ I \leq n + \sum_{i=0}^{n} N_{W_i}^\circ I$ also holds or not is an open problem. We remark that Theorem 9.5 can also be obtained alternatively assuming $n = 1$ case. E.g. when $n = 2$, consider $f = \psi_1 + \phi_2$ where $\psi_1 = \phi_0 + \phi_1$ and apply the base result twice. The $n = 2$ case makes it clear how the factor '2' starts appearing.

Koiran et al also showed the following variant for any nontrivial linear combinations of functions, with an additional linear factor in n incurred. Recall that arbitrary linear combinations were considered in the Descartes system.

Theorem 9.6. *[48] Let $\phi_0, \ldots, \phi_n$ be analytic functions on an interval I. If the real constants $a_0, \ldots, a_n$ are not all zero, then for $f := \sum_{i=0}^{n} a_i \phi_i$, we have*

$$N_f^\circ I \leq n + (n+1) \sum_{i=0}^{n} N_{W_i}^\circ I.$$

In Chapter 10, we shall use of Theorem 9.5 to get a concrete upper bound towards the real τ-conjecture.

Chapter 10

Upper Bound Towards Real τ-Conjecture

In the previous chapter, we obtained an upper bound on the number of real zeros of the sum of functions in terms of the Wronskian of the subsequences. However, these Wronskians may be simplified further if only we could exploit the relations between the functions. Thus it makes sense to consider a special class of functions that will help us realize the potential and the limitations of the Wronskian approach. For example, the sum of products

$$f := \sum_{i=1}^{p} \prod_{i=1}^{q} f_{i,j}$$

where each $f_{i,j}$ is k-sparse polynomial. We may denote the ith term by $g_i = \prod_{j=1}^{q} f_{i,j}$, and as we discussed we must impose some relation between any two g_i's. So one possible choice is to fix q polynomials $f_1, \ldots, f_q$ each of them being k-sparse, and consider g_i's to be the powers of f_j's. More precisely, we set $g_i := \prod_{j=1}^{q} f_j^{\alpha_{i,j}}$, where each $\alpha_{i,j}$ is a nonnegative integer, and consider the sum of sum of product of powers

$$f := \sum_{i=1}^{p} \prod_{i=1}^{q} f_j^{\alpha_{i,j}}.$$

Now the problem reduces to analyzing the Wronskian $W_i := W(g_1, g_2, \ldots, g_i)$ for $1 \leq i \leq p$. The sparsity of $f := \sum_{i=1}^{p} \prod_{i=1}^{q} f_j^{\alpha_{i,j}}$ depends on $\alpha_{i,j}$'s, and therefore the upper bound on $N_f^{\circ}\mathbb{R}$ obtained through the Descartes rule can be arbitrarily high. So our goal would be to obtain an upper bound purely in terms of p, q and k.

We first need to simply the derivatives of product of polynomials. Let us reserve the index i for the Wronskian, and consider the $(v-1)$th derivative $g_u^{(v-1)}$ for $1 \leq$

$u, v \leq p$ as

$$g_u^{(v-1)} = \sum_{r_1+\cdots+r_q=v-1} \prod_{j=1}^{q} \left(f_j^{\alpha_{u,j}}\right)^{(r_j)}, \tag{10.1}$$

where each r_j is a nonnegative integer. Now we need to simplify the derivatives of a power of a polynomial. For a nonnegative real α, the power f^α is simply the composition $h(f(x))$ where $h(x) = x^\alpha$. Thus by Faà di Bruno's formula (Proposition 6.1), we have for a nonnegative integer r,

$$(f^\alpha)^{(r)} = \sum_{s\in\Gamma_r} \frac{r!}{\prod_{l=1}^r s_l!(l!)^{s_l}} \frac{\alpha!}{(\alpha-|s|)!} f^{\alpha-|s|} \prod_{l=1}^{r} \left(f^{(l)}\right)^{s_l},$$

where $\Gamma_r = \{(s_1,\ldots,s_r) \in \mathbb{N}^r : \sum_{l=1}^r l s_l = r\}$, and $|s| := \sum_{l=1}^r s_l$ for $s = (s_1,\ldots,s_r)$. The scalar factor in this identity depends only on s and α since one can recover r from $s \in \Gamma_r$. We can now simplify the identity further by setting

$$\beta_{s,\alpha} := \frac{r!}{\prod_{l=1}^r s_l!(l!)^{s_l}} \frac{\alpha!}{(\alpha-|s|)!}.$$

There is also the factor $f^{\alpha-|s|}$ in the RHS that demands $\alpha \geq \max_{s\in\Gamma_r} |s| = r$. Finally, if we take into consideration this substitution and the assumption, then by this lemma, Equation 10.1 becomes

$$g_u^{(v-1)} = \sum_{r_1+\cdots+r_q=v-1} \prod_{j=1}^{q} \left(\sum_{s\in\Gamma_{r_j}} \beta_{s,\alpha_{u,j}} f_j^{\alpha_{u,j}-|s|} \prod_{l=1}^{r_j} \left(f_j^{(l)}\right)^{s_l} \right), \tag{10.2}$$

and it is valid as long as

$$\alpha_{u,j} \geq r_j \qquad \text{for all } 1 \leq j \leq q.$$

How do we get around this imposed condition? Let us note that $0 \leq r_j \leq v-1$ so in particular $\alpha_{u,j} \geq v-1$ for all $1 \leq j \leq q$. This must also be the case for each $1 \leq u, v \leq p$, and so it is sufficient to ensure $\alpha_{u,j} \geq p-1$ for all u and j. Now the fix to this is to consider[1]

$$\widetilde{g_u} := \prod_{j=1}^{q} f_j^{\alpha_{u,j}+p-1},$$

and state Equation 10.2 for $\widetilde{g_u}$'s. Before we analyze the Wronskian for these new

[1]Koiran et al [48] consider the power to be $\alpha_{i,j} + N + p$ where N is such that $\alpha_{i,j} + N > 0$ for all i and j.

polynomials, let us discuss what this fix does. We have $\widetilde{g_u} = g_u \prod_{j=1}^{q} f_j^{p-1}$, and if we define $\widetilde{f} = \sum_{u=1}^{p} \widetilde{g_u}$, then $\widetilde{f} = f \prod_{j=1}^{q} f_j^{p-1}$ such that $N_f^\circ \mathbb{R} \leq N_{\widetilde{f}}^\circ \mathbb{R}$, which suggests it is enough to find an upper bound on the number of distinct real zeros of $\widetilde{f}$ instead.

Now we state the analogue of Equation 10.2 for $\widetilde{g_u}$.

$$\widetilde{g_u}^{(v-1)} = \sum_{r_1+\cdots+r_q=v-1} \prod_{j=1}^{q} \left(\sum_{s \in \Gamma_{r_j}} \beta_{s,\alpha_{u,j}} f_j^{\alpha_{u,j}+p-1-|s|} \prod_{l=1}^{r_j} \left(f_j^{(l)} \right)^{s_l} \right).$$

At this point, we could consider the Wronskian $W_i = W(\widetilde{g_1}, \ldots, \widetilde{g_i})$, and upper bound the number of its real zeros by the only possible method we know so far, for arbitrary polynomials, which is to estimate its sparsity. However, the powers $f_j^{\alpha_{u,j}}$ may contribute arbitrarily large sparsity, and we must factor them out. We may rewrite the expression as

$$\widetilde{g_u}^{(v-1)} = \left(\prod_{j=1}^{q} f_j^{\alpha_{u,j}} \right) h_{u,v},$$

where

$$h_{u,v} = \sum_{r_1+\cdots+r_q=v-1} \prod_{j=1}^{q} \left(\sum_{s \in \Gamma_{r_j}} \beta_{s,\alpha_{u,j}} f_j^{p-1-|s|} \prod_{l=1}^{r_j} \left(f_j^{(l)} \right)^{s_l} \right).$$

Now $|s| \leq v-1 \leq p-1$, and the powers $\alpha_{u,j}$ and $p-1-|s|$ of f_j both are nonnegative, and so it precludes any more assumptions. The factor $\left(\prod_{j=1}^{q} f_j^{\alpha_{u,j}} \right)$ is common for the uth column of W_i. Thus

$$W_i = \left(\prod_{u=1}^{i} \prod_{j=1}^{q} f_j^{\alpha_{u,j}} \right) \det[(h_{u,v})_{1 \leq u,v \leq i}].$$

Since the source of the distinct zeros in the first factor here is simply the polynomials $f_1, \ldots, f_q$, we have

$$N_{W_i}^\circ \mathbb{R} \leq \left(\sum_{j=1}^{q} N_{f_j}^\circ \mathbb{R} \right) + N_{\det[(h_{u,v})_{1 \leq u,v \leq i}]}^\circ \mathbb{R}. \tag{10.3}$$

Our next problem is to estimate the number of real zeros of the polynomial $\det[(h_{u,v})_{1 \leq u,v \leq i}]$, and we do this by estimating its sparsity, i.e. the number of monomials in it. Let us examine $h_{u,v}$ first. We may think of $h_{u,v}$ as a polynomial in the variables $f_1^{(l)}, \ldots, f_q^{(l)}$ for $0 \leq l \leq v-1$. In this new variables then, $h_{u,v}$ is a homogeneous polynomial with the total degree $q(p-1-|s|+\sum_{l=1}^{r_j} s_l) = q(p-1)$,

and therefore the determinant $\det[(h_{u,v})_{1\le u,v\le i}]$ is also homogeneous and has total degree $\sum_{v=1}^{i} q(p-1) = q(p-1)i$. We express the determinant as

$$\det[(h_{u,v})_{1\le u,v\le i}] = \sum_{P} P(\{f_j^{(l)} : 1 \le j \le q, 0 \le l \le i-1\}),$$

where P is a formal monomial of degree $q(p-1)i$. Since f_j's and their derivatives are k-sparse in x, each term in the above sum has at most $k^{q(p-1)i}$ monomials in x. There are $i!$ terms, so $\det[(h_{u,v})_{1\le u,v\le i}]$ has then sparsity at most $i!k^{q(p-1)i}$ in x. Finally, we substitute this estimate using Descartes' rule (Proposition 3.4) in Equation 10.3 to get

$$N^{\circ}_{W_i}\mathbb{R} \le q(2k-1) + 2(i!k^{q(p-1)i}) - 1,$$

and now by Theorem 9.5,

$$\begin{aligned} N^{\circ}_{f}\mathbb{R} &\le p - 1 + N^{\circ}_{W_p}\mathbb{R} + N^{\circ}_{W_{p-1}}\mathbb{R} + 2\sum_{i=1}^{p-2} N^{\circ}_{W_i}\mathbb{R} \\ &\le cp!pk^{q(p-1)p} = k^{\mathcal{O}(qp^2)}. \end{aligned}$$

Thus we have shown

Theorem 10.1. *Let $f := \sum_{i=1}^{p}\prod_{j=1}^{q} f_j^{\alpha_{i,j}}$, where each f_j is a k-sparse real polynomial and each $\alpha_{i,j}$ is a nonnegative integer. Then, $N^{\circ}_{f}\mathbb{R} = k^{\mathcal{O}(qp^2)}$.*

This is essentially the result of Koiran, Portier and Tavenas (2015) [48], however we have simplified their analysis. Earlier, Grenet et al (2011) [33] had given $k^{\mathcal{O}(q2^p)}$ upper bound for the same type of polynomials, and the Wronskian approach improves upon it. We remark that so far these are the only two concrete upper bounds in the literature towards real τ-conjecture other than what we get by Descartes' rule.

Another restricted family

Tavenas (2014) [83] suggests in his thesis that it is also worthwhile to look at polynomials expressible as $\sum_{i=1}^{p} f_i^{\alpha_i}$ (more on this in Chapter 14). By setting $p = q$, Theorem 10.1 easily gives $N^{\circ}_{f}\mathbb{R} = k^{\mathcal{O}(p^3)}$. But an exactly the same argument can improve this bound.

Corollary 10.2. *Let $f := \sum_{i=1}^{p} f_i^{\alpha_j}$, where each f_i is a k-sparse real polynomial and each α_i is a nonnegative integer. Then, $N^{\circ}_{f}\mathbb{R} = k^{\mathcal{O}(p^2)}$.*

In the case that all of the f_i's are the equal, each term is a composition of two functions and there is a common function among all (Compare Lemma 6.2). We can assume that α_i's are all distinct, and then the upper bound on $N_f^\circ\mathbb{R}$ can be shown to be polynomial in p. Let $f_1 = \cdots = f_p = g$ and g be k-sparse. Also suppose that $p \geq 2$ and $\alpha_1 < \alpha_2 < \cdots < \alpha_p$. By generalized Mina's identity from Corollary 6.5, we have

$$W(g^{\alpha_1}, \ldots, g^{\alpha_p}) = g^{(\sum_{i=1}^p \alpha_i)} g^{-\frac{p(p-1)}{2}} (g')^{\frac{p(p-1)}{2}} \prod_{1 \leq i < j \leq p} (\alpha_j - \alpha_i).$$

Here's the scalar is nonzero, so we have

$$N^\circ_{W(g^{\alpha_1}, \ldots, g^{\alpha_p})}\mathbb{R} = N_g^\circ\mathbb{R} + N^\circ_{g'/g}\mathbb{R} \leq N_g^\circ\mathbb{R} + N_{g'}^\circ\mathbb{R} \leq 4k - 2$$

now by Theorem 9.5, $N_f^\circ\mathbb{R} \leq p - 1 + 2(p-1)(4k-2) = \mathcal{O}(pk)$.

Corollary 10.3. *Let $f := \sum_{i=1}^p g^{\alpha_i}$, where g is a k-sparse real polynomial, and $0 \leq \alpha_1 < \alpha_2 < \cdots < \alpha_p$. Then $N_f^\circ\mathbb{R} = \mathcal{O}(pk)$.*

The last two corollaries suggest that if we wish to understand the behaviour of the number of distinct real zeros of the polynomials of the type $\sum_{i=1}^p f_i^{\alpha_i}$, then it may be helpful to come up with a measure of similarity between the polynomials in the family $\{f_1^{\alpha_1}, \ldots, f_p^{\alpha_p}\}$. E.g. when all f_i's are the same the bound is $\mathcal{O}(pk)$, and when all are distinct the best we have been able to do is $k^{\mathcal{O}(p^2)}$.

We seek a different generalization of Corollary 6.5 to be able to simplify $W(f_1^{\alpha_1}, \ldots, f_p^{\alpha_p})$.

Chapter 11

Multiplicities, Complex Zeros Cannot Be Ignored

Let us recall the real τ-conjecture.

Conjecture 11.1 (Real τ-Conjecture)**.** *Let $f := \sum_{i=1}^{p} \prod_{j=1}^{q} f_{i,j}$ where each $f_{i,j}$ is a k-sparse real polynomial. Then the number of distinct real zeros of f is at most $(pqk)^c$, where c is an absolute constant.*

Apart from the complexity theoretic motivations, one may also think about this conjecture from a purely mathematical point of view. In view of the Descartes' rule, counting only the distinct zeros does not seem very special. In Chapter 3, we discussed that the estimates given by the Descartes' rule are tight whether we account for the multiplicities or not: we have an upper bound of $2k - 2$ on the number of nonzero real zeros of a k-sparse polynomial, and then to count the number of distinct real zeros (including 0), we simply add one to this estimate. We can multiply a polynomial by any power of x increasing the multiplicity of 0 arbitrarily while keeping sparsity the same. Thus we might as well state the conjecture for the number of nonzero real zeros counted with multiplicities.

Conjecture 11.2. *[42] [Real τ-Conjecture with Multiplicities] Let $f := \sum_{i=1}^{p} \prod_{j=1}^{q} f_{i,j}$ where each $f_{i,j}$ is a k-sparse real polynomial. Then the number of nonzero real zeros of f counted with multiplicities is at most $(pqk)^c$, where c is an absolute constant.*

It is clear that 11.2 implies 11.1; is the converse also true? In Chapter 10, we considered the polynomials of the type $\sum_{i=1}^{p} \prod_{j=1}^{q} f_j^{\alpha_{i,j}}$ which potentially had arbitrarily high sparsity, and the proof of the $k^{\mathcal{O}(qp^2)}$ upper bound does not go through for counting zeros with multiplicities. In such a scenario, an upper bound

independant of $\alpha_{i,j}$'s is remarkable. But it does not suggest that we must only examine distinct zeros.

There are two other details to note in 11.1. First, it talks about real polynomials, and second it counts only the real zeros. We gave two proofs of Descartes' rule, the first proof was based on the sign variations and therefore needed real coefficients, while the second was based on Rolle's theorem and therefore also required real coefficients. Moreover, we know that a polynomial is not completely determined by only its real zeros, and perhaps counting only the real zeros is also not very special.

The next result due to Hajós (1958) [34] indicates that the multiplicity of even the complex zeros of complex polynomials, and therefore real, can be controlled. We give two proofs. A direct proof (See Lemma 1, Montgomery and Schinzel (1977) [62]), and an inductive one (See Lemma 3.9, Koiran and Skomra (2020) [50]). Both are algebraic.

Lemma 11.3 (Hajós' Lemma)**.** *Suppose that $f(z)$ is a k-sparse complex polynomial such that it vanishes at a nonzero complex point $\gamma \in \mathbb{C}\backslash\{0\}$. Then, the multiplicity of γ as a zero of $f(z)$ is at most $k-1$.*

Direct Proof. Suppose that $f(z) = \sum_{i=1}^{k} a_i z^{\alpha_i}$ where $a_i \in \mathbb{C}$, and let γ be a nonzero complex zero of $f(z)$ with multiplicity m. Then, the derivative $f^{(i)}(z)$ vanishes at γ for each $i = 0, 1, \ldots, m-1$. Treating the coefficients $a_1, \ldots, a_k$ as variables, we now have a system of m linear equations $f^{(i)}(\gamma) = 0$ for $i = 0, 1, \ldots, m-1$ in k variables. This system has a nontrivial solution (i.e. not all a_i's are zero) if and only if $k \geq m$. The system can also be expressed as the matrix-vector equation

$$\begin{bmatrix} \gamma^{\alpha_1} & \gamma^{\alpha_2} & \cdots & \gamma^{\alpha_k} \\ \alpha_1\gamma^{\alpha_1-1} & \alpha_2\gamma^{\alpha_2-1} & \cdots & \alpha_k\gamma^{\alpha_k-1} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\alpha_1!}{(\alpha_1-m)!}\gamma^{\alpha_1-m+1} & \frac{\alpha_2!}{(\alpha_2-m)!}\gamma^{\alpha_2-m+1} & \cdots & \frac{\alpha_k!}{(\alpha_k-m)!}\gamma^{\alpha_k-m+1} \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_k \end{bmatrix} = 0.$$

In the case $k = m$, the above matrix becomes square, and it is exactly the same matrix from Equation 5.1 where we have computed its determinant as well. It follows that this square matrix is nonsingular because α_i's are distinct and γ is nonzero. Thus in the case $k = m$, each of the a_i's must be zero, which is a contradiction since we assume $f(z)$ to be k-sparse. This shows that m must be at most $k-1$. □

Inductive Proof. In the case $k = 1$, the polynomial $f(z)$ has no nonzero complex zeros, and so the claim is trivial. Next let us assume $f(0) \neq 0$, otherwise we consider instead the polynomial $g(z)$ where $f(z) = x^t g(z)$ and $g(0) \neq 0$, and prove the claim for $g(z)$. Now $f'(z)$ is $(k-1)$-sparse, and by the induction hypothesis, γ

is a zero of $f'(z)$ with multiplicity at most $k-2$. The polynomial $f(z)$ has degree just one more than $f'(z)$, and therefore γ can be a zero of $f(z)$ with multiplicity at most one more than that of $f'(z)$. Thus multiplicity of γ as a zero of $f(z)$ is at most $k-1$. □

We shall first explore the idea of allowing the coefficients to be complex to see why multiplicities cannot be ignored through an example. Afterwards, we shall discuss why complex zeros need to be taken into account as well.

Allowing Complex Coefficients

Consider $f(x) := (x+1)^n$, it has exactly one real distinct zero, i.e. constantly many, and therefore satisfies the real τ-conjecture. On the other hand, the number of nonzero real zeros counted with multiplicities depend on n, and so it may or may not satisfy Conjecture 11.2. But we can observe the following.

Proposition 11.4. *[42] Assume $f(x) := (x+1)^n = \sum_{i=1}^{p} \prod_{j=1}^{q} f_{i,j}$, where $f_{i,j}$'s are real and k-sparse. If $pqk = \mathcal{O}(n^c)$ for all $c > 0$, then Conjecture 11.2 is false.*

Thus $(x+1)^n$ may potentially be used as a counterexample to Conjecture 11.2. We only have to construct a subpolynomial sized SPS (Sum or Product of Sparse polynomials) representation of it. So far we know that 11.2 is stronger than 11.1, and now we shall argue that 11.2 may be replaced with 11.1 in the above Proposition at the cost of allowing $f_{i,j}$'s to be complex.

Lemma 11.5. *[42] Assume $f(x) := (x+1)^n = \sum_{i=1}^{p} \prod_{j=1}^{q} f_{i,j}$, where $f_{i,j}$'s are complex and k-sparse. If $pqk = \mathcal{O}(n^c)$ for all $c > 0$, then Conjecture 11.1 is false.*

We have not yet stated any analogue of real τ-conjecture for complex polynomials, but this lemma already suggests that 11.1 and 11.2 are related when complex coefficients are involved. Let us now go about proving Lemma 11.5. The proof is by contradiction. Suppose that Conjecture 11.1 holds. The idea is to construct using $(x+1)^n$ another real polynomial with at least around n distinct real zeros and has a SPS representation of size polynomial in p, q and k, and then the result follows by applying Conjecture 11.1. The starting point is the polynomial

$$h(x) := f(ix) + f(-ix) = (ix+1)^n + (-ix+1)^n$$

which has real coefficients. Now $h(x) = 0$ if and only if $\left(\frac{ix+1}{-ix+1}\right)^n + 1 = 0$. Setting $y = \frac{ix+1}{-ix+1}$, we get $x = \frac{2\Im(y)}{|1+y|^2}$ where $\Im(y)$ is the imaginary part of y. The ratio is well-defined because $y \neq -1$. Thus zeros of $h(x)$ are of the form $\frac{2\Im(w_k)}{|1+w_k|^2}$, and

therefore real, where w_k is an nth root of -1 and also described by $w_k = e^{i\frac{2k+1}{n}\pi}$ for integers $k = 0, 1, \ldots, n-1$, and therefore distinct. Next, observe that the degree of $h(x)$ is n if n is even, and $n-1$ otherwise. So depending on whether n is even or odd, the number of distinct real zeros of $h(x)$ is n or $n-1$ respectively[1].

Now although $h(x)$ is real, both $f(ix)$ and $f(-ix)$ are complex polynomials. We use the complex SPS representation of $f(x)$ from the hypothesis to write

$$h(x) = \sum_{i=1}^{2p} \prod_{j=1}^{q} f_{i,j}$$

for some complex k-sparse $f_{i,j}$'s (different than the hypothesis). Conjecture 11.1 may be applied to $h(x)$ if only it is expressed in a real SPS representation. Instead, we shall work with the the real part $\Re(h(x))$ because it has a real SPS representation. Also since the zeros of $h(x)$ are also the zeros of $\Re(h(x))$, the latter still has then at least $n-1$ distinct real zeros. Next, our goal is to show that $\Re(h(x))$ has a real SPS representation with parameters p', q' and k' such that $p'q'k'$ is polynomially bounded by pqk.

More formally, the real and the imaginary part of a univariate complex polynomial $f = \sum_{i=0}^{n} a_i x_i$ are defined as $\Re(f) := \sum_{i=0}^{n} \Re(a_i) x_i$ and $\Im(f) := \sum_{i=0}^{n} \Im(a_i) x_i$ respectively such that $f = \Re(f) + i\Im(f)$. The definition of the real/imaginary part may be extended to multivariate polynomials similarly, coefficientwise. We shall first look at the real part of a product of polynomials.

Lemma 11.6. *[42] For the indeterminates x_j and y_j $(j = 1, \ldots, n)$, we have*

$$\Re\left(\prod_{j=1}^{n}(x_j + iy_j)\right) = \sum_{l=1}^{n+1} b_l \prod_{j=1}^{n}(x_j + a_l y_j),$$

where b_l's and a_l's are real constants.

Proof. Let $f = \prod_{j=1}^{n}(x_j + zy_j)$ be a polynomial in the $2n+1$ variables x_j's, y_j's and z, it has degree n in the new variable z. Then the claim that needs to be proved is the following: $\Re(f(i))$ is a real linear combination of the evaluations $f(a_1), f(a_2), \ldots, f(a_{n+1})$ of $f(z)$ at $n+1$ real points $a_1, \ldots, a_{n+1}$ respectively. If we write $f(z) = \sum_{k=0}^{n} f_k z^k$ with each f_k independent of z, then these $n+1$ evalua-

[1] If n is odd, then there an integer l such that $n = 2l+1$, but $w_l = -1$ does not correspond to a zero of $h(x)$. Thus the set of zeros of $h(x)$ is exactly the set $\{e^{i\frac{2k+1}{n}\pi} \mid k \neq l, k = 0, 1, \ldots, n-1\}$ if n is odd, and $\{e^{i\frac{2k+1}{n}\pi} \mid k = 0, 1, \ldots, n-1\}$ otherwise.

tions may be expressed as a matrix-vector equation

$$\begin{bmatrix} f(a_1) \\ \vdots \\ f(a_{n+1}) \end{bmatrix} = V(a_1, \ldots, a_{n+1})^T \begin{bmatrix} f_0 \\ \vdots \\ f_n \end{bmatrix},$$

where $V(a_1, \ldots, a_{n+1})$ denotes the Vandermonde matrix. If $a_1, \ldots, a_{n+1}$ are chosen to be distinct real numbers, then this Vandermonde matrix is invertible, and therefore each f_i can be expressed as a real linear combination of $f(a_1), \ldots, f(a_{n+1})$. Next, $\Re(f(i))$ is also a real linear combination of f_j's since

$$\Re(f(i)) = \Re\left(\sum_{k=0}^{n} f_k i^k\right) = \sum_{2j \in \{0,\ldots,n\}} f_{2j}(-1)^j,$$

and therefore it is also a real linear combination of $f(a_1), \ldots, f(a_{n+1})$. □

Using this Lemma, we can now show that if a polynomial has a small complex SPS representation, then its real part has a small real SPS representation.

Lemma 11.7. *[42] Let $f = \sum_{i=1}^{p} \prod_{j=1}^{q} f_{i,j}$ such that $f_{i,j}$'s are complex k-sparse polynomials. Then, $\Re(f) = \sum_{i=1}^{p(q+1)} \prod_{j=1}^{q} g_{i,j}$ for some $g_{i,j}$'s that are real k-sparse polynomials.*

Proof. Writing for each $i = 1, \ldots, p$,

$$\Re(\prod_{j=1}^{q} f_{i,j}) = \Re(\prod_{j=1}^{q} (\Re(f_{i,j}) + i\Im(f_{i,j}))),$$

substituting $x_j \leftarrow \Re(f_{i,j})$ and $y_j \leftarrow \Im(f_{i,j})$ in Lemma 11.6, we get the identity

$$\Re(\prod_{j=1}^{q} f_{i,j}) = \sum_{l=1}^{q+1} b_{i,l} \prod_{j=1}^{q} (\Re(f_{i,j}) + a_{i,l}\Im(f_{i,j})),$$

which after adding over $i = 1, \ldots, p$ gives us

$$\sum_{i=1}^{p} \Re(\prod_{j=1}^{q} f_{i,j}) = \sum_{i=1}^{p} \sum_{l=1}^{q+1} b_{i,l} \prod_{j=1}^{q} (\Re(f_{i,j}) + a_{i,l}\Im(f_{i,j}))$$

$$\implies \Re(f) = \sum_{k=1}^{p(q+1)} \prod_{j=1}^{q} g_{k,j},$$

for some real polynomials $g_{k,j}$'s whose sparsity is the same as that of $\Re(f_{i,j}) + a_{i,l}\Im(f_{i,j})$ and therefore $f_{i,j}$'s, respectively. □

Now $\Re(h(x))$ has a real SPS representation with parameters $2p(q+1)$, q and k respectively, and if Conjecture 11.1 is true, then $\Re(h(x))$ has $\mathcal{O}((2p(q+1)qk)^c) = \mathcal{O}((pqk)^c)$ distinct real zeros. We also know that $\Re(h(x))$ has at least $n-1$ distinct real zeros. Thus $pqk = \Omega(n^{c'})$ for some $c' > 0$, and the proof of Lemma 11.5 is complete.

Finally, with Lemma 11.3 and 11.5, we have learned that we must also consider multiplicities of zeros, and allowing complex coefficients may also be useful. Next, let us see why we need a closer look at the complex zeros as well.

Accounting for Complex Zeros

Consider the polynomial $z^n - 1$ whose zeros are uniformly placed on the unit circle. For two angles α and β, where $0 < \beta - \alpha < 2\pi$, denote by $N_f S(\alpha, \beta)$ the number of zeros of f in the sector $S(\alpha, \beta) := \{z \in \mathbb{C} \mid |z| > 0, \alpha < \arg z < \beta\}$, counted according to their multiplicities. Then we notice that as $n \to \infty$, the ratio $N_{z^n-1}S(\alpha, \beta)/n$ converges to $(\beta - \alpha)/2\pi$. In words, we expect approximately $(\beta - \alpha)/2\pi$ fraction of zeros of $z^n - 1$ inside the sector $S(\alpha, \beta)$. More precisely, we have for any n,

$$\left| N_{z^n-1}S(\alpha, \beta) - \frac{(\beta - \alpha)}{2\pi} n \right| \leq 1,$$

where the quantity on the left measures the discrepancy from the expected number of zeros in a sector of the polynomial $z^n - 1$. Hayman (1972) [35] showed that this quantity in general depends on the sparsity of the polynomial, also indicated earlier by Biernacki (1928) [6].

Theorem 11.8 (Hayman's Theorem)**.** *Let f be a k-sparse complex polynomial of degree n such that $f(0) \neq 0$. Then*

$$\left| N_f S(\alpha, \beta) - \frac{(\beta - \alpha)}{2\pi} n \right| \leq k - 1.$$

Here, we assume $f(0) \neq 0$ to avoid dealing with the origin 0 as zeros of f. The origin is also not counted in $N_f S(\alpha, \beta)$. In the case $f(0) = 0$ and 0 occurs with multiplicity m, we consider instead the polynomial $g(z) = f(z)/z^m$ which is of degree $n - m$ and is also k-sparse. Then $N_f S(\alpha, \beta) = N_g S(\alpha, \beta)$, and Theorem 11.8

for $g(z)$ gives

$$\left| N_f S(\alpha, \beta) - \frac{\beta - \alpha}{2\pi}(n - m) \right| \leq k - 1. \tag{11.1}$$

The weak rule of signs (Corollary 3.3) for real polynomials can be obtained from Theorem 11.8 by letting $\beta \to 0_+$ and $\alpha \to 0_-$. Thus Hayman's theorem is a generalization of Descartes' rule for complex polynomials and sectors.

We shall discuss this generalization as well as the assumption $f(0) \neq 0$ in Chapter 12 as well. We shall prove an even more general result in Chapter 13 of which Theorem 11.8 is a corollary. Hayman's theorem suggests that we might as well count zeros in a sector than the real axis, and prompts us to pose the third variant of the real τ-conjecture.

Conjecture 11.9. *[42] [Complex τ-Conjecture for Sectors] Let $f := \sum_{i=1}^{p} \prod_{j=1}^{q} f_{i,j}$ be of degree n with $f(0) \neq 0$ such that each $f_{i,j}$ is a k-sparse complex polynomial. For every α and β with $0 < \beta - \alpha < 2\pi$,*

$$\left| N_f S(\alpha, \beta) - \frac{\beta - \alpha}{2\pi} n \right| = \mathcal{O}((pqk)^c).$$

Again by letting $\beta \to 0_+$ and $\alpha \to 0_-$, we observe that Conjecture 11.9 implies Conjecture 11.2 in the case $f(0) \neq 0$. When $f(0) = 0$, we could consider $g(z) = f(z)/z^m$ such that $g(0) \neq 0$. But the obstacle here is that the parameters p', q' and k' of $g(z)$ in the SPS represenation may be different than that of $f(z)$. We shall discuss in Chapter 12 how to get around this. Whether all three variants are equivalent or not will be investigated in Chapter 14. These two new conjectures were introduced by Hrubeš (2013) [42] who argues that the real τ-conjecture is deeply related to the structure of complex zeros. We now begin discussion on the distribution of the zeros in the complex plane.

Chapter 12

Distribution of Zeros in the Complex Plane

The simplest case of the real τ-conjecture is $gh + t$ where g and h are k-sparse real polynomials, and t is some real parameter. Understanding the location of zeros of $gh + t$ as t varies is a perturbation problem. Now consider f to be a k-sparse polynomial, and $f + t$ its perturbation. We have some idea about the location of zeros of $f + t$ when t is small enough due to the continuity of zeros of polynomials as a function of the coefficients, which we now discuss.

Continuity of Zeros

We use the notation $D(a; r) := \{z \in \mathbb{C} : |z - a| < r\}$ for an open disc of radius r centered at a, and, for convenience, assume f to be monic in this discussion. The next result appears as the supplement to Theorem 1.3.1 in Rahman and Schmeisser [69].

Theorem 12.1 (Continuity Theorem)**.** *Let $f(z) = z^n + \sum_{v=0}^{n-1} a_v z^v$ be a complex monic polynomial of degree n and zeros $z_1, \ldots, z_n$. Then for sufficiently small $\delta > 0$ such that when each coefficient a_v is perturbed to any point within $D(a_v; \delta)$ for $v = 0, \ldots, n-1$, each zero z_j stays within $D(z_k; 4A\delta^{1/n})$ for $j = 1, \ldots, n$, where $A := \max_v\{1, 2|a_v|^{1/(n-v)}\}$.*

Thus when t is small enough nonzero real number, each of the zero of $f + t$ is within an ϵ-neighbourhood of a zero of f where $\epsilon := 4At^{1/n}$. We now explain the assumption $f(0) \neq 0$ in Theorem 11.8 and Conjecture 11.9. If 0 occurs with multiplicity m as a zero of f, then it is expected to be perturbed into m distinct zeros of $f + t$ uniformly distributed in the ϵ-neighbourhood around the origin. Since $f + t$ does not vanish at the origin, applying Theorem 11.8 for $f + t$ gives us $|N_{f+t}S(\alpha, \beta) -$

$\frac{\beta-\alpha}{2\pi}n| \leq k-1$. Now because $N_{f+t}S(\alpha,\beta) = N_fS(\alpha,\beta) + \frac{\beta-\alpha}{2\pi}m \pm 1$, we can obtain $|N_fS(\alpha,\beta) - \frac{\beta-\alpha}{2\pi}(n-m)| \leq k$, a conclusion more or less the same as Equation 11.1.

What we have just showed is that Hayman's theorem applied on polynomials with $f(0) = 0$ gives us the same conclusion as that for a small perturbation $f + t$, and likewise for Conjecture 11.9. Thus if $f(0) = 0$, then we can work with $f + t$ instead. WLOG we may just assume $f(0) \neq 0$ and avoid dealing with the 0's.

At the end of the previous chapter, we were interested in showing that Conjecture 11.9 implies Conjecture 11.2 in the case $f(0) = 0$. Let us do this using the idea with just discussed. Consider the premise of Conjecture 11.2 and that $f(0) = 0$. We consider a nonzero perturbation $f + t$, and then Conjecture 11.9 gives us $|N_{f+t}S(\alpha,\beta) - \frac{\beta-\alpha}{2\pi}n| \leq ((p+1)qk)^c \leq \mathcal{O}((pqk)^{c'})$. Now the LHS of the inequality is the same as $|N_fS(\alpha,\beta) - \frac{\beta-\alpha}{2\pi}(n-m) \pm 1|$. Thus $N_fS(\alpha,\beta) \leq \frac{\beta-\alpha}{2\pi}(n-m) + \mathcal{O}((pqk)^c)$. By letting $\beta \to 0_+$ and $\alpha \to 0_-$, we can conclude that the number of nonzero real zeros of f is at most polynomial in pqk, and therefore Conjecture 11.2 holds.

Relation between Hayman's theorem and Descartes' rule

Next let us discuss the connection of Hayman's theorem with Descartes' using the lens of continuity of zeros. Consider the positive zeros of f. We can choose two small enough angles α and β such that the sector $S(\alpha,\beta)$ has at least as many zeros of $f + t$ as there are positive zeros of f. In fact, we can choose $\beta = \sin^{-1}(\epsilon/z_0) + \gamma$ and $\alpha = -\sin^{-1}(\epsilon/z_0) - \gamma$, where z_0 is the closest positive real zero of f from origin, and γ is an arbitrarily small positive number just to ensure $f + t$ does not have any zeros on the boundary of the sector $S(\alpha,\beta)$. Conversely, a complex zero w of f may be perturbed into a real zero of $f + t$ if the ϵ-neighbourhood around w overlaps with the real axis.

In any case, we are able to contain the zeros of the polynomial obtained by small perturbations. The challenge in front of us now is to find out what happens when we perturb f by a not-so-small constant. But let us understand in this case the meaning of Hayman's theorem (Theorem 11.8) when applied to $f + t$ assuming it is k-sparse with $f(0) \neq 0$ and $f(0) + t \neq 0$, and using the approximation $\beta - \alpha = 2\epsilon/z_0 + 2\gamma$, we get $|N_{f+t}S(\alpha,\beta) - \frac{\epsilon/z_0+\gamma}{\pi}n| \leq k-1$. As $t \to 0$, we have $\epsilon \to 0$, $\beta \to \gamma$ and $\alpha \to -\gamma$. Thus $|N_fS(-\gamma,\gamma) - \gamma n/\pi| \leq k-1$. Now γ was chosen to be arbitrarily small enough so $N_fS(-\gamma,\gamma) = N_f(0,\infty)$, and we obtain exactly the estimate of Descartes.

To conclude this discussion, we verified that Hayman's theorem is an extension of Descartes' for small enough perturbation of a real polynomial. But Hayman's theorem is stated for complex polynomials, and counts number of complex zeros in a sector and therefore we need tools from complex analysis to prove it. We shall now

consider the following general problem: how many zeros does the given polynomial f have in the subset Ω of the complex plane? Let us begin by recalling some of the basic definitions, following Rahman and Schmeisser [69].

Definitions

An *arc* $\gamma : [a, b] \to \mathbb{C}$ is continous complex-valued function, defined on a closed real interval $[a, b]$. The arc γ is called a *closed curve* if it takes the same value on the endpoints a and b, a *simple* or *Jordan arc* if it is injective, and a *simple closed curve* or a *Jordan curve* if it is injective except at the endpoints where it takes the same value.

By a point on the arc or a curve γ, we mean the evaluation $\gamma(t)$ for some $t \in [a, b]$. The curve γ is called *bounded* if it has finite length L, where the length is defiend to be the supremum $L := \sup_\pi \{\sum_{v=1}^{n} |\gamma(t_v) - \gamma(t_{v-1})|\}$ over all partitions $\pi = \{a = t_0 < t_1 < \cdots < t_n = n\}$. We may think of each restriction $\gamma : [t_{v-1}, t_v] \to \mathbb{C}$ as an arc. For example, we need only four arcs to describe a box, and only three arcs to describe a bounded sector.

We are interested in domains that are an interior region of Jordan curves. A non-empty, open, connected subset is called a *region*, where *connected* means that it cannot be expressed as a disjoint union of two non-empty open subsets. A region together with some or all of its boundary points is called a *domain*[1]. In particular, a region and its closure are both domains. We denote by $\partial\Omega$ the boundary of the region or the domain Ω. For example, open sectors and open half planes are regions, and the boundary of the upper half plane $\{z \mid \Im(z) > 0\}$ is the real axis $\mathbb{R}$.

The *Jordan Curve Theorem* says that the set $\mathbb{C}\backslash\text{Image}(\gamma)$, the complement of the set of points on a Jordan curve γ, has two disjoint regions. One is bounded, called as the *interior*, and another is unbounded. A Jordan curve $\gamma : [a, b] \to \mathbb{C}$ is said to be *positively oriented* if its interior is on the left of the point $\gamma(t)$ as t increases from a to b. The boundary of the interior of a Jordan curve is the curve itself.

For any function $f : \mathbb{C} \to \mathbb{C}$, we denote by $\Delta_\gamma \arg f(z)$ the change in the argument of f as z moves along the curve γ in positive/anticlockwise direction. We shall now discuss change in the argument for the case of polynomials.

[1]Sometimes the words 'domain' and 'region' are used interchangeably. But here we follow Rahman and Schmeisser [69].

Change in the Argument

Let $f(z)$ be a complex polynomial, and let Ω be a bounded domain given as an interior of a positively oriented Jordan curve $\gamma := \partial\Omega$. Suppose that $f(z)$ does not vanish on the curve γ. Then the zeros of $f(z)$ are either in the interior of γ (i.e. in Ω) or outside γ. We want to compute $N_f\Omega$ which is the number of zeros of f in Ω, counted with multiplicities. Let us factor the polynomial as

$$f(z) = \prod_{\alpha\in\Omega}(z-\alpha)\prod_{\alpha\notin\Omega}(z-\alpha),$$

and consider the change in its argument along γ,

$$\Delta_\gamma \arg f(z) = \sum_{\alpha\in\Omega}\Delta_\gamma \arg(z-\alpha) + \sum_{\alpha\notin\Omega}\Delta_\gamma \arg(z-\alpha).$$

Now if $\alpha \in \Omega$, then the argument of $(z-\alpha)$ changes by 2π along γ. Otherwise if $\alpha \notin \Omega$, then it is outside γ and the argument does not change along γ. Thus $\Delta_\gamma \arg f(z) = 2\pi N_f\Omega$. We shall call this observation as the argument principle for polynomials. This principle is due to Cauchy (1831) [20] which is generally stated for meromorphic functions.

Lemma 12.2 (Argument Principle)**.** *Let $f(z)$ be a complex polynomial, and let Ω be a bounded domain given as an interior of a positively oriented Jordan curve $\gamma := \partial\Omega$ such that $f(z)$ does not vanish on γ. Then $N_f\Omega = \frac{1}{2\pi}\Delta_\gamma \arg f(z)$.*

This result remarkable in the sense that one can compute the number of zeros in a domain by understanding the behaviour of the polynomial on its boundary. Our next task is to compute $\Delta_\gamma \arg f(z)$, and so we have to make the behaviour of the polynomial along the curve γ more explicit. For the purpose of computing the change in the argument let us assume that γ is an arc, and think of it as the parameterized function $\gamma(t) : [a,b] \to \mathbb{C}$ in t, which may or may not take the same value at the endpoints. Let us also continue with the assumption that f has no zeros along γ, i.e.

$$f\circ\gamma(t) \neq 0 \text{ for all } t \in [a,b]. \tag{12.1}$$

Now the real part $\Re(f\circ\gamma)$ and the imaginary part $\Im(f\circ\gamma)$ are both real polynomials in the real variable t, and we perhaps could gather some useful information from the sign variations of these polynomials as t varies from a to b.

The inspiration for this idea comes from Descartes' rule since it works for real polynomials, and the information there was gathered from the sign variation of the

coefficients. Let us focus on the former polynomial: the real part $\Re(f \circ \gamma)$ changes sign if and only if $f \circ \gamma$ traverses the imaginary axis. For sign variations of $\Re(f \circ \gamma)$ to make sense around a point in $[a, b]$, we shall consider only the open interval (a, b) and assume additionally that $\Re(f \circ \gamma)$ does not vanish at the endpoints a and b, i.e.

$$\Re(f \circ \gamma(a)) \neq 0 \text{ and } \Re(f \circ \gamma(b)) \neq 0. \tag{12.2}$$

Now more precisely, $\Re(f \circ \gamma)$ changes sign at a point $\eta \in (a, b)$ such that $\gamma(\eta) \neq 0$ if and only if $f \circ \gamma$ traverses the imaginary axis such that $\Im(f(\gamma(\eta))) \neq 0$. The real part $\Re(f \circ \gamma)$ may change sign from $-$ to $+$ or $+$ to $-$. Also the imaginary part $\Im(f \circ \gamma)$ at η may either be positive or negative. Thus there are four cases. These cases suggest that we consider the real rational function in t

$$F(t) := \frac{\Im(f \circ \gamma(t))}{\Re(f \circ \gamma(t))}.$$

We denote by N_-^+ the number of points in (a, b) where $F(t)$ jumps from $-\infty$ to $+\infty$, and by N_+^- be the number of points in (a, b) where $F(t)$ jumps from $+\infty$ to $-\infty$. We refer to these points as *Type-1 poles* and *Type-2 poles* respectively, and define their difference $I_a^b(F) := N_-^+ - N_+^-$ as the Cauchy index of F on $[a, b]$.

Now poles of $F(t)$ in (a, b) are exactly those points where $\Re(f \circ \gamma)$ vanishes but $\Im(f \circ \gamma)$ does not. We may categorize the poles $\eta \in (a, b)$ such that $\gamma(\eta) \neq 0$ in four groups according to the four cases.

Case 1. η is a Type-1 pole of F such that $\Re(f \circ \gamma)$ changes the sign from $-$ to $+$ and $\Im(f \circ \gamma(\eta)) > 0$.

Case 2. η is a Type-2 pole of F such that $\Re(f \circ \gamma)$ changes the sign from $-$ to $+$ and $\Im(f \circ \gamma(\eta)) < 0$.

Case 3. η is a Type-2 pole of F such that $\Re(f \circ \gamma)$ changes the sign from $+$ to $-$ and $\Im(f \circ \gamma(\eta)) > 0$.

Case 4. η is a Type-1 pole of F such that $\Re(f \circ \gamma)$ changes the sign from $+$ to $-$ and $\Im(f \circ \gamma(\eta)) < 0$.

These four categories may also be combined in two: Type-1 poles and Type-2 poles since we have learned which points on the arc are interesting. Along with the above poles η with $\gamma(\eta) \neq 0$, there may also be poles where $\gamma(\eta) = 0$. But at such points we have $\Re(f \circ \gamma(\eta)) = 0$, i.e. $\Re(f(0)) = 0$. Now if we simply assume

$$\Re(f(0)) \neq 0, \tag{12.3}$$

then we do not have to deal with such poles.

Next we want to compute the change in the argument $\Delta_\gamma \arg(f \circ \gamma(t)))$. We do this piecewise. Let $t_1, \ldots, t_k$ denote the above poles of F in $[a, b]$ such that $t_0 = a < t_1 < \cdots < t_k < b = t_{k+1}$. Then

$$\Delta_\gamma \arg(f \circ \gamma(t))) = \sum_{i=0}^{k} \Delta_{t \in [t_i, t_{i+1}]} \arg(f \circ \gamma(t)))$$

Now $\Re(f \circ \gamma(t_i)) = 0$ for all $i = 1, \ldots, k$. If $\Im(f \circ \gamma(t_i)) > 0$, then $\arg(f \circ \gamma(t_i))) = \pi/2$. Otherwise if $\Im(f \circ \gamma(t_i)) < 0$, then $\arg(f \circ \gamma(t_i))) = -\pi/2$.

- Now t_0 is not a pole. If t_1 is Type-1, then the change in the argument over $[t_0, t_1]$ is $-\sigma_1\pi$ for some $0 < \sigma_1 < 1$. If t_1 is Type-2, then it is $\sigma_2\pi$ for some $0 < \sigma_2 < 1$.

- Now t_{k+1} is not a pole. If t_k is Type-1, then the change in the argument over $[t_k, t_{k+1}]$ is $-\tau_1\pi$ for some $0 < \tau_1 < 1$. If t_k is Type-2, then it is $\tau_2\pi$ for some $0 < \tau_2 < 1$.

- (This and the observations below hold for $i = 1, \ldots, k-1$) If both t_i and t_{i+1} are Type-1 poles, then they must come under Case 1 and Case 4 or vise versa respectively, and in both situations the change in the argument over $[t_i, t_{i+1}]$ must be $-\pi$.

- Likewise, if both t_i and t_{i+1} are Type-2 poles, then they must come under Case 2 and Case 3 or vise versa respectively, and in both situations the change in the argument over $[t_i, t_{i+1}]$ must be π.

- In any other situation, the sign of the imaginary part $\Im(f \circ \gamma(t_i))$ stays the same, therefore there is no change in the argument over $[t_i, t_{i+1}]$.

Next we partition the sequence of poles $\{t_1, \ldots, t_k\}$ in two ways depending upon whether t_1 is Type-1 or Type-2. Suppose that t_1 is Type-1. Then we partition as follows: the first m_1 poles are Type-1, then next n_1 are Type-2, then the next m_2 are Type-1, and so on. If t_k is Type-2, then we let the last n_p poles be of Type-2 such that $m_1 + n_1 + \cdots + m_p + n_p = k$ and $I_a^b(F) = (m_1 + \cdots + m_p) - (n_1 + \cdots + n_p)$, which leads to

$$\begin{aligned}\Delta_\gamma \arg(f \circ \gamma(t))) &= -\sigma_1\pi - (m_1 + \cdots + m_p - p)\pi + (n_1 + \cdots + n_p - p)\pi + \tau_2\pi \\ &= -I_a^b(F)\pi + (-\sigma_1 + \tau_2)\pi.\end{aligned}$$

If t_k is Type-1, then we let the last m_p poles be of Type-1 such that $m_1 + n_1 + \cdots + m_p = k$ and $I_a^b(F) = (m_1 + \cdots + m_p) - (n_1 + \cdots + n_{p-1})$, which leads to

$$\begin{aligned}\Delta_\gamma \arg(f \circ \gamma(t))) &= -\sigma_1\pi - (m_1 + \cdots + m_p - p)\pi + (n_1 + \cdots + n_{p-1} - p + 1)\pi - \tau_1\pi \\ &= -I_a^b(F)\pi + (-\sigma_1 - \tau_1 + 1)\pi.\end{aligned}$$

In any case, we notice that $\Delta_\gamma \arg(f \circ \gamma(t))) = -I_a^b(F)\pi + \epsilon\pi$ for some $0 < \epsilon < 1$. It can also be verified that the same conclusion is obtained when t_1 is Type-2. Thus we have computed the change is the argument using the Cauchy index. Let us summarize this as a lemma which holds under assumptions 12.1, 12.2 and 12.3.

Lemma 12.3 (Lemma 11.1.1 Rahman and Schmeisser [69]). *Let $\gamma : [a, b] \to \mathbb{C}$ be a Jordan arc. Let f be a complex polynomial such that $\Re(f(0)) \neq 0$. Further, suppose that it does not vanish on γ, and its real part does not vanish at the endpoints $\gamma(a)$ and $\gamma(b)$ of the arc. Define the real rational function*

$$F(t) := \frac{\Im(f \circ \gamma(t))}{\Re(f \circ \gamma(t))}.$$

Then the net change in the argument of $f(z)$ as z traverses γ satisfies

$$\Delta_\gamma \arg(f) = -\pi I_a^b(F) + \pi\epsilon \qquad \text{for } |\epsilon| < 1.$$

This lemma is useful for computing change in the argument along an arc. If we take γ to be a curve, then by argument principle, we can relate the number of zeros inside the curve with the Cauchy index. This is the Cauchy Index Theorem (Theorem 11.1.3. Rahman and Schmeisser [69]).

Theorem 12.4 (Cauchy Index Theorem). *Let $f(z)$ be a complex polynomial such that $\Re(f(0)) \neq 0$, and let Ω be a bounded domain given as an interior of a positively oriented Jordan curve $\gamma := \partial\Omega$ such that $f(z)$ does not vanish on γ. If γ is represented by $\gamma : [a, b] \to \mathbb{C}$, then suppose that $\Re(f)$ does not vanish at $\gamma(a)$. Define the real rational function*

$$F(t) := \frac{\Im(f \circ \gamma(t))}{\Re(f \circ \gamma(t))}.$$

Then $N_f\Omega = \frac{1}{2}(-I_a^b(F) + \epsilon)$ for some $|\epsilon| < 1$.

Notice that the Cauchy index is expected to be nonpositive in the conclusion of this theorem because the number of zeros must be nonnegative. We could have defined Cauchy index such that we substract the number of Type-1 poles from the number of Type-2 poles instead so that Cauchy index is nonnegative. But

the next basic example suggests that it is also appropriate to continue with the earlier definition that we gave of Cauchy index. Another detail is that poles of F correspond to the zeros of the real part $\Re(f \circ \gamma)$, and we have counted them without multiplicities. This detail will be very important.

In the next chapter, we shall compute the number of zeros inside a bounded sector, and to do that, we shall employ Lemma 12.3 since a bounded sector is given by three arcs.

A Small Application of Cauchy Indices

Unrelated to the previous discussion, we discuss that the number of distinct real zeros of a polynomial may also be computed via the Cauchy index. Let $f(x) = \prod_{i=1}^{k}(x-\alpha_i)^{m_i}$ be a real polynomial with distinct zeros $\alpha_1, \ldots, \alpha_k$ with multiplicities $m_1, \ldots, m_k$ respectively, and among them let $\alpha_1, \ldots, \alpha_r$ be the real zeros, and let the remaining be the complex zeros. Define $F := f'/f$ to be the logarithmic derivative of f over $\mathbb{R}$. Then it can be written as the sum

$$F(x) = \sum_{i=1}^{r} \frac{m_i}{x - \alpha_i} + r(x)$$

where $r(x)$ has no real poles. Now the Type-1 poles of F are exactly the real points $\alpha_1, \ldots, \alpha_r$, and F has no Type-2 poles. Thus $I_{-\infty}^{\infty}(F) = N_f^{\circ}\mathbb{R}$, i.e, the Cauchy index of the logarithmic derivative of a real polynomial over $\mathbb{R}$ is exactly the number of distinct real zeros of that polynomial.

Chapter 13

Angular Discrepancy

For a complex polynomial $f(z) = \sum_{i=0}^{n} a_i z^i$ of degree n with $a_i \in \mathbb{C}$, and a sector $S(\alpha, \beta)$ with $0 < \beta - \alpha < 2\pi$, we refer to the quantity $|N_f S(\alpha, \beta) - \frac{(\beta-\alpha)}{2\pi} n|$ as the *angular discrepancy*. It appeared in Theorem 11.8, and we shall try to estimate it using the results from the previous chapters. We approximate the sector $S(\alpha, \beta)$ by the bounded subsector $S(R; \alpha, \beta) := \{z \in \mathbb{C} : R > |z| > 0, \alpha < \arg z < \beta\}$ for a large enough R such that it contains all the zeros of $f(z)$ inside $S(\alpha, \beta)$. If we denote this subsector by $\Omega := S(R; \alpha, \beta)$, then $N_f\Omega = N_f S(\alpha, \beta)$. The boundary $\partial\Omega$ of this subsector is the union of two arcs $\partial\Omega = \gamma(t) \cup \delta(t)$ where

$$\gamma(t) = \begin{cases} -te^{i\beta} & \text{if } t \in [-R, 0] \\ te^{i\alpha} & \text{if } t \in [0, R], \end{cases} \qquad \text{and} \qquad \delta(t) = Re^{it} \qquad \text{for } t \in [\alpha, \beta].$$

While the arc $\gamma(t)$ traces counterclockwise direction along the edges of the sector, $\delta(t)$ completes the loop. The boundary $\partial\Omega$ is a bounded simple curve of length $2R + (\beta - \alpha)R$, and we shall think of it as positively oriented. We cannot apply the Cauchy index theorem directly because the boundary is given piecewise. Instead, we start by computing arguments separately. To be able to apply the argument principle (Lemma 12.2), we must assume

$$f(z) \text{ does not vanish along } \partial\Omega, \tag{13.1}$$

and then we have $N_f\Omega = \frac{1}{2\pi}\Delta_{\partial\Omega} \arg f(z)$. Since $\partial\Omega$ is a union of γ and δ, the expression breaks into two parts

$$N_f S(\alpha, \beta) = \frac{1}{2\pi} \left(\Delta_\gamma \arg f(z) + \Delta_\delta \arg f(z) \right), \tag{13.2}$$

and now we can estimate net change in the argument along γ and δ separately.

The second case is easier to deal with. We express the polynomial as the product $f(z) = a_n z^n \left(1 + \sum_{i=0}^{n-1} \frac{a_i}{a_n z^{n-i}}\right)$ which requires assuming that

(13.3) the leading coefficient of $f(z)$ is nonzero, i.e. $a_n \neq 0$.

Then along the arc δ, we may write

$$\Delta_\delta \arg(f(z)) = \Delta_\delta \arg(a_n z^n) + \Delta_\delta \arg\left(1 + \sum_{i=0}^{n-1} \frac{a_i}{a_n z^{n-i}}\right),$$

and now compute the change in the argument of the two factors separately. Clearly, $\Delta_\delta \arg(a_n z^n) = n(\beta - \alpha)$. Since we have $z = R$ along δ, we may substitute it in the second term, and denote the second term by $\epsilon(R)$ where $\epsilon(R) = \Delta_\delta \arg\left(1 + \sum_{i=0}^{n-1} \frac{a_i}{a_n R^{n-i}}\right)$. Now $\epsilon(R)$ converges to $\Delta_\delta(1) = 0$ as $R \to \infty$. To conclude,

(13.4) $$\Delta_\delta \arg(f(z)) = n(\beta - \alpha) + \epsilon(R) \xrightarrow{R\to\infty} n(\beta - \alpha).$$

Let us now compute the net change in the argument along the arc γ. We shall do this by computing the Cauchy index and then applying Lemma 12.3. The interval in consideration is $[-R, R] = [-R, 0] \cup [R, 0]$. For $t \in [-R, 0]$, we have $\gamma(t) = -te^{i\beta}$ and for $t \in [0, R]$, we have $\gamma(t) = te^{i\alpha}$. The hypotheses of Lemma 12.3 must be satisfied for both the intervals and the corresponding arcs. The first condition that we assume is

(13.5) $\Re(f)$ does not vanish at the origin, i.e. $\Re(f(0)) \neq 0$.

Second, f must not vanish along γ, and this means in our case that $f(\gamma(t)) = f(-te^{i\beta})$ (in the variable t) does not have any nonpositive zeros in $[-R, 0]$ and $f(\gamma(t)) = f(te^{i\alpha})$ does not have any nonnegative zeros $[0, R]$. Thus f must not have any zeros on the boundary edges of $S(\alpha, \beta)$. This is simply a restatement of the assumption 13.1 when $R \to \infty$ because $f(z)$ obviously cannot have any zeros along δ as $R \to \infty$. Thus we may replace 13.1 with the following assumption

(13.6) f does not vanish on the boundary of $S(\alpha, \beta)$.

The next hypothesis of Lemma 12.3 requires that $\Re(f)$ does not vanish at the endpoints of the arc, but we consider two intervals $[-R, 0]$ and $[0, R]$, so this means

that $\gamma(-R), \gamma(0)$ and $\gamma(R)$ are not zeros of $\Re(f)$. Equivalently, we must assume

$$\Re(f(Re^{i\beta})) \neq 0, \Re(f(0)) \neq 0, \Re(f(Re^{i\alpha})) \neq 0, \tag{13.7}$$

where the second inequation already covers the assumption 13.5. The other two inequations have a dependency on R, and we have to avoid this. We write

$$\Re(f(Re^{i\beta})) = \Re\left(a_n R^n e^{in\beta}\right) + \left(\sum_{j=0}^{n-1} a_j R^j e^{ij\beta}\right),$$

where R is positive, and so the stronger assumption $\Re(a_n e^{in\beta}) \neq 0$ is also sufficient to ensure $\Re(f(Re^{i\beta})) \neq 0$. Likewise, $\Re(a_n e^{in\alpha}) \neq 0$ is sufficient to ensure $\Re(f(Re^{i\alpha})) \neq 0$. Thus instead of 13.7, it is enough to ensure

$$\Re(a_n e^{in\beta}) \neq 0, \Re(a_0) \neq 0, \Re(a_n e^{in\alpha}) \neq 0, \tag{13.8}$$

where $a_0 = f(0)$.

We collect all the assumptions made so far, i.e. 13.3, 13.6 and 13.8 as the regularity conditions a polynomial must satisfy.

Definition 13.1 (Regularity Conditions)**.** *We say that a complex polynomial $f(z) = \sum_{i=0}^{n} a_i z^i$ of degree n is regular with respect to the sector $S(\alpha, \beta)$ if each of the following hold:*

1. *f has no zeros on the boundary of $S(\alpha, \beta)$,*
2. *$\Re(f)$ does not vanish at the origin, i.e. $\Re(a_0) \neq 0$,*
3. *$\Re(a_n e^{in\alpha}) \neq 0$ and $\Re(a_n e^{in\beta}) \neq 0$.*

Assuming these regularity conditions, we proceed with defining two real rational functions

$$F(t) = \begin{cases} F_\beta(t) := \frac{\Im(f(-te^{i\beta}))}{\Re(f(-te^{i\beta}))} & \text{for } t \in [-R, 0], \\ F_\alpha(t) := \frac{\Im(f(te^{i\alpha}))}{\Re(f(te^{i\alpha}))} & \text{for } t \in [0, R]. \end{cases}$$

The Cauchy index of F over the two intervals may be computed separately since

$$I_{-R}^{R}(F) = I_{-R}^{0}(F_\beta) + I_{0}^{R}(F_\alpha). \tag{13.9}$$

By Lemma 12.3, we have

$$\Delta_\gamma \arg(f) = -\pi I_{-R}^{R}(F) + \pi\epsilon \qquad \text{for } |\epsilon| < 1, \tag{13.10}$$

and now substituting the Equations 13.4, 13.9 and 13.10 into 13.2,

$$N_f S(\alpha,\beta) = \frac{1}{2\pi}\left(n(\beta-\alpha) + \epsilon(R) - \pi(I^0_{-R}(F_\beta) + I^R_0(F_\alpha)) + \pi\epsilon\right),$$

and letting $R \to \infty$ and $\lambda = \frac{\epsilon}{2}$, we finally obtain

$$N_f S(\alpha,\beta) = \frac{(\beta-\alpha)}{2\pi}n - \frac{1}{2}\left(I^0_{-\infty}(F_\beta) + I^\infty_0(F_\alpha)\right) + \lambda, \tag{13.11}$$

where $\lambda \in (-1/2, 1/2)$ is a unique number such that the RHS becomes an integer. This is Equation 11.2.7 in Rahman and Schmeisser [69].

Let us now simplify the Cauchy indices. Consider the rational function

$$F_\beta(t) := \frac{\Im(f(-te^{i\beta}))}{\Re(f(-te^{i\beta}))}$$

defined over $[-\infty, 0]$, and recall that $I^0_{-\infty}(F_\beta)$ is the number of Type-1 poles in $(-\infty, 0)$ minus the number of Type-2 poles in $(-\infty, 0)$ of F_β. But the absolute value $I^0_{-\infty}(F_\beta)$ is bounded simply by the number of poles of F_β of any kind in $(-\infty, 0)$, and these poles are also the distinct negative zeros of $\Re(f(-te^{i\beta}))$. Due to the regularity conditions, 0 is not a zero of $\Re(f(-te^{i\beta}))$. Now $|I^0_{-\infty}(F_\beta)|$ is at most the number of distinct negative zeros of $\Re(f(-te^{i\beta}))$ which is the same as the number of distinct positive zeros of $\Re(f(te^{i\beta}))$, i.e. $|I^0_{-\infty}(F_\beta)| \le N^\circ_{\Re(f(te^{i\beta}))}\mathbb{R}^+$. Note that the positive zeros of $\Re(f(te^{i\beta}))$ are the nonzero zeros of $\Re(f)$ with argument β. By a similar argument $|I^\infty_0(F_\alpha)|$ is at most the number of distinct positive zeros of $\Re(f(te^{i\alpha}))$, i.e. $|I^\infty_0(F_\alpha)| \le N^\circ_{\Re(f(te^{i\alpha}))}\mathbb{R}^+$. By substituting these estimates in Equation 13.11, we obtain an upper bound on the angular discrepancy.

Theorem 13.2. *Let f be a complex polynomial of degree n regular with respect to the sector $S(\alpha,\beta)$ for $0 < \beta - \alpha < 2\pi$. Then*

$$\left|N_f S(\alpha,\beta) - \frac{(\beta-\alpha)}{2\pi}n\right| \le \frac{1}{2}\left(N^\circ_{\Re(f(te^{i\beta}))}\mathbb{R}^+ + N^\circ_{\Re(f(te^{i\alpha}))}\mathbb{R}^+\right) + |\lambda|,$$

where $|\lambda| < 1/2$ and $(N^\circ_{\Re(f(te^{i\beta}))}\mathbb{R}^+ + N^\circ_{\Re(f(te^{i\alpha}))}\mathbb{R}^+)$ is the number of distinct nonzero zeros of $\Re(f)$ on the boundary of this sector[1].

This theorem is interesting in the sense that on the LHS we have number of zeros inside a sector counted according to the multiplicities, while on the RHS we have the number of distinct zeros of the real part of the polynomial on the boundary of

[1]There was an assumption in Hrubeš [42] that $\Re(f(te^{i\alpha}))$ and $\Re(f(te^{i\beta}))$ do not have multiple zeros. It is not necessary.

the sector.

Let us examine more closely. Consider the plot of the real polynomials $\Re(f)$ and $\Im(f)$ on xy-plane, and assume they have a trivial GCD for now. Then the zeros of f are the intersection points of the curves $\Re(f)$ and $\Im(f)$. By Cauchy-Riemann equations, the tangents of the two curves at the intersection points are orthogonal. Thus if we trace $\Re(f)$ between any two consecutive zeros, it must make a sharp turn. The behaviour of $\Im(f)$ is likewise, and therefore it is sufficient to study just the behaviour of $\Re(f)$. While $(N^{\circ}_{\Re(f(te^{i\beta}))}\mathbb{R}^{+} + N^{\circ}_{\Re(f(te^{i\alpha}))}\mathbb{R}^{+})$ counts the number of times the curve $\Re(f)$ enters or exits the sector $S(\alpha, \beta)$, the term $N_f S(\alpha, \beta)$ corresponds to the number of times $\Re(f)$ makes a sharp turn inside the sector. Thus the geometric intuition behind Theorem 13.2 that we extract is the following: the number of times the curve $\Re(f)$ makes a sharp turn inside a sector depends on the number of times it enters or exits the sector. It remains to sufficiently justify the term $\frac{\beta-\alpha}{2\pi}n$ for an arbitrary polynomial. We saw that it originated from the net change in the argument of the leading term $a_n z^n$ along the arc δ that closed the loop, and it is also the number of zeros of the polynomial $z^n - 1$ in the sector.

Simplifying Regularity Conditions

The first regularity condition requires that f has no zeros on the boundary of the sector $S(\alpha, \beta)$. This can be achieved by perturbing α and β by a very small ϵ (with $|\epsilon| > 0$), and considering a new sector $S(\alpha + \epsilon, \beta + \epsilon)$ such that $N_f S(\alpha, \beta) = N_f S(\alpha + \epsilon, \beta + \epsilon)$ and the angular discrepancy also remains the same. Next, since f has degree n we always have $a_n \neq 0$. Let us also assume that $a_0 \neq 0$. We observe that the zeros of a polynomial, and also the angular discrepancy, are unaffected when we multiply the polynomial by any nonzero complex number c. Thus if we choose an appropriate nonzero c such that each of $\Re(ca_0)$, $\Re(ca_n e^{in\alpha})$ and $\Re(ca_n e^{in\beta})$ are nonzero, then the remaining two regularity conditions are satisfied. Now

$$\begin{aligned}
(i) \quad & \Re(ca_0) \neq 0 \iff \arg(c) \neq -\arg(a_0) + \pi/2 + \pi k_0, \\
(ii) \quad & \Re(ca_n e^{in\beta}) \neq 0 \iff \arg(c) \neq n\beta - \arg(a_n) + \pi/2 + \pi k_1, \\
(iii) \quad & \Re(ca_n e^{in\alpha}) \neq 0 \iff \arg(c) \neq n\alpha - \arg(a_n) + \pi/2 + \pi k_2.
\end{aligned}$$

A nonzero complex number c can always be chosen such that $\Re(ca_0) \neq 0$, i.e. $c = i$. To ensure (ii) and (iii), we shall again consider a small perturbation of α and β. Thus in conclusion, if $f(z)$ is a polynomial nonvanishing at the origin, i.e. $a_0 \neq 0$, then there exists a small $\epsilon > 0$, two angles α' and β' with $|\alpha' - \alpha| < \epsilon$ and

$|\beta' - \beta| < \epsilon$, and a nonzero complex number c such that

$$\left| N_f S(\alpha, \beta) - \frac{(\beta - \alpha)}{2\pi} n \right| \leq \frac{1}{2} \left(N^{\circ}_{\Re(cf(te^{i\beta'}))} \mathbb{R}^+ + N^{\circ}_{\Re(cf(te^{i\alpha'}))} \mathbb{R}^+ \right) + |\lambda|,$$

where $|\lambda| < 1/2$. To obtain a concrete and a useful upper bound, we define $M(f) := \max_{\phi \in [0,2\pi)} N^{\circ}_{\Re(f(te^{i\phi}))} \mathbb{R}^+$ to be the maximum number of nonzero distinct zeros of $\Re(f)$ on any ray with one endpoint at the origin. Thus there can be at most $2M(f)$ entry points for the curve $\Re(f)$ on any sector. The upper bound in Theorem 13.2 can now be replaced with $M(f) + |\lambda|$, a quantity that is independent of the sector chosen.

Theorem 13.3 (Proposition 3.1, Hrubeš [42]). *Let f be a complex polynomial of degree n that is nonvanishing at the origin. Then for any sector $S(\alpha, \beta)$ with $0 < \beta - \alpha < 2\pi$, we have*

$$\left| N_f S(\alpha, \beta) - \frac{(\beta - \alpha)}{2\pi} n \right| \leq M(f) + \frac{1}{2}.$$

The real polynomial $\Re(f(te^{i\phi}))$ has at most the same sparsity as f, and therefore if f is k-sparse, then we can use Descartes' weak rule of signs to get $M(f) \leq k - 1$. This is the Hayman's theorem (Theorem 11.8).

Corollary 13.4 (Hayman). *Let f be a complex k-sparse polynomial of degree n that is nonvanishing at the origin. Then for any sector $S(\alpha, \beta)$ with $0 < \beta - \alpha < 2\pi$, we have*

$$\left| N_f S(\alpha, \beta) - \frac{(\beta - \alpha)}{2\pi} n \right| \leq k - \frac{1}{2}.$$

One may also use Descartes' strong rule and state the upper bound in terms of the sign variations instead of the sparsity. We will need Theorem 13.3 in Chapter 14, where we discuss the relation between the real and the complex τ-conjecture.

Chapter 14

Variants of Real τ-Conjecture

Type 1: Considering Multiplicities and Complex Zeroes

For convenience, we state once again the three variants that we have seen so far of the real τ-conjecture.

Conjecture 14.1 (Real τ-Conjecture, 11.1 restated)**.** *Let $f := \sum_{i=1}^{p} \prod_{j=1}^{q} f_{i,j}$ where each $f_{i,j}$ is a k-sparse real polynomial. Then the number of distinct real zeros of f is at most $(pqk)^c$, where c is an absolute constant.*

Conjecture 14.2 (Real τ-Conjecture with Multiplicities, 11.2 restated)**.** *Let $f := \sum_{i=1}^{p} \prod_{j=1}^{q} f_{i,j}$ where each $f_{i,j}$ is a k-sparse real polynomial. Then the number of nonzero real zeros of f counted with multiplicities is at most $(pqk)^c$, where c is an absolute constant.*

Conjecture 14.3 (Complex τ-Conjecture for Sectors, 11.9 restated)**.** *Let $f := \sum_{i=1}^{p} \prod_{j=1}^{q} f_{i,j}$ be of degree n with $f(0) \neq 0$ such that each $f_{i,j}$ is a k-sparse complex polynomial. For every α and β with $0 < \beta - \alpha < 2\pi$,*

$$\left| N_f S(\alpha, \beta) - \frac{\beta - \alpha}{2\pi} n \right| = \mathcal{O}((pqk)^c).$$

We have seen that 14.3 implies 14.2, and 14.2 implies 14.1. We shall now show that 14.1, in fact, also implies 14.3.

Theorem 14.4. *[42] Conjectures 14.1, 14.2 and 14.3 are equivalent.*

Proof. Suppose that Conjecture 14.1 is true. Let $f := \sum_{i=1}^{p} \prod_{j=1}^{q} f_{i,j}$ be of degree n with $f(0) \neq 0$ such that each $f_{i,j}$ is a k-sparse complex polynomial, and let $S(\alpha, \beta)$ be any sector with $0 < \beta - \alpha < 2\pi$. By Theorem 13.3, we have $|N_f S(\alpha, \beta) - \frac{\beta-\alpha}{2\pi} n| \leq M(f) + \frac{1}{2}$. Now to be able to use the conclusion of Conjecture 14.1, we shall consider

the real part $\Re(f)$. Lemma 11.7 provides us with real k-sparse polynomials $g_{i,j}$'s such that $\Re(f) = \sum_{i=1}^{p(q+1)} \prod_{j=1}^{q} g_{i,j}$. Now by Conjecture 14.1, for any angle ϕ, the polynomial $\Re(f(te^{i\phi}))$ has at most $(p(q+1)qk))^c \leq (pqk)^{c'}$ distinct real zeros. Thus $M(f) \leq (pqk)^{c'}$ and the Conjecture 14.3 is true. □

We shall now draw two conclusions from this theorem. The polynomial $(x+1)^n$ already satisfies 14.1, and recall that we showed in Lemma 11.5 that if $(x+1)^n$ is a counterexample to Conjecture 14.2 when complex coefficients are allowed, then Conjecture 14.1 is false. We now prove such a conclusion without alluding to any particular polynomial. In particular, any counterexample to 14.1 when complex coefficients are allowed also falsifies original 14.1.

Corollary 14.5. *[42] If any of the Conjectures 14.1 or 14.2 is false when complex coefficients are allowed, then the original Conjecture 14.1 is also false.*

Proof. Suppose Conjecture 14.1 is true, then by Theorem 14.4, we can assume 14.3 as well. Since 14.2 implies 14.1, it is enough to show that 14.2 holds when complex coefficients are allowed. Let $f := \sum_{i=1}^{p} \prod_{j=1}^{q} f_{i,j}$ be of degree n such that each $f_{i,j}$ is a k-sparse complex polynomial. Next we consider the double sector $S(-\epsilon, \epsilon) \cup S(\pi - \epsilon, \pi + \epsilon)$ for a small $\epsilon > 0$ such that all the nonzero zeros of f are inside it, i.e. $N_f\mathbb{R}_{>0} = N_f S(-\epsilon, \epsilon)$ and $N_f\mathbb{R}_{<0} = N_f S(\pi - \epsilon, \pi + \epsilon)$

If $f(0) \neq 0$, then 14.3 implies $|N_f S(-\epsilon, \epsilon) - \frac{2\epsilon}{2\pi} n| \leq (pqk)^c$ and $|N_f S(\epsilon, -\epsilon) - \frac{2\epsilon}{2\pi} n| \leq (pqk)^{c'}$ respectively. Thus the number of nonzero real zeros of f is upper bounded by $\frac{2\epsilon}{\pi} n + (pqk)^{c''}$. It is sufficient to choose $\epsilon < \pi/n$ to conclude Conjecture 14.2 is true.

If $f(0) = 0$, then by the discussion following the continuity theorem in Chapter 12, it is sufficient to show that Conjecture 14.2 holds for the perturbation $g := f + t$ with $g(0) \neq 0$. Now the previous case applies, and since g has only one extra term than f, the upper bound on the number of nonzero real zeros of g is still polynomial in pqk. □

We may refer to Conjecture 14.1 with complex coefficients allowed as the 'Real τ-Conjecture over $\mathbb{C}$' (since it still counts real zeros), and likewise Conjecture 14.2 with complex coefficients allowed as the 'Real τ-Conjecture over $\mathbb{C}$ with Multiplicities'. Now Conjecture 14.3 implies the 'Real τ-Conjecture over $\mathbb{C}$ with Multiplicities' which in turn implies 'Real τ-Conjecture over $\mathbb{C}$'.

Next, we discuss how Conjecture 14.3 may also be used to produce a counterexample for 14.1. In the next corollary, observe that for $(x+1)^n$ the goal becomes the same as Lemma 11.5. Therefore it provides us a family of polynomials that may be tested for a counterexample.

Corollary 14.6. *[42] Assume $f = \sum_{i=1}^{p} \prod_{j=1}^{q} f_{i,j}$, where $f_{i,j}$'s are complex and k-sparse, and f has degree n. If any of the following holds:*

1. *f has a nonzero complex zero with multiplicity m with $pqk = \mathcal{O}(m^c)$ for all $c > 0$,*

2. *f is such that $N_f S(\pi/2, 3\pi/2) = n$ but $pqk = \mathcal{O}(n^c)$ for all $c > 0$,*

then Conjecture 14.1 is false.

Proof. Suppose on the contrary that Conjecture 14.1 is true, then by Theorem 14.4, we assume that Conjecture 14.3 is true. Let $re^{i\phi}$ $(r > 0)$ be a nonzero zero of $f(z)$ with multiplicity m. Now as in the proof of the previous corollary, we consider a small sector $S(\phi-\epsilon, \phi+\epsilon)$ containg $re^{i\phi}$ such that $m \leq N_f S(\phi-\epsilon, \phi+\epsilon)$. We shall prove that pqk is not polynomially bounded in m for some exponent. In the case $f(0) \neq 0$, Conjecture 14.3 implies $|N_f S(\phi-\epsilon, \phi+\epsilon) - \frac{2\epsilon}{2\pi} n| \leq (pqk)^c$, and then choosing $\epsilon < \pi/n$, we can conclude that m is at most $1 + (pqk)^c$ for some $c > 0$. In the case $f(0) = 0$ and m' is the largest power of x that divides $f(z)$, we apply Conjecture 14.3 to the perturbation $f+t$ instead. It gives us $|N_{f+t} S(\phi-\epsilon, \phi+\epsilon) - \frac{2\epsilon}{2\pi} n| \leq ((p+1)qk)^c$. Now $N_{f+t} S(\phi-\epsilon, \phi+\epsilon) = N_f S(\phi-\epsilon, \phi+\epsilon) + \frac{2\epsilon}{2\pi} m' \pm 1$. But choosing again $\epsilon < \pi/n$, we get an upper bound on m that is polynomial in pqk. In any case, we have $pqk = \Omega(m^{c'})$ for some $c' > 0$, contradicting the hypothesis.

Now for the second part, f has all zeros in the left half plane and therefore already satisfies $f(0) \neq 0$. Then Conjecture 14.3 gives us $n \leq 2(pqk)^c$ for some $c > 0$, also contradicting the hypothesis. □

For a polynomial with small complex SPS representation, the first part of this corollary suggests that the zeros cannot be concentrated in a very small sector, otherwise 14.1 is false, and the second part suggests that the zeros cannot all lie in the left half plane, otherwise 14.1 is false. This is a statement that relates Algebraic Complexity Theory with the Geometry of Polynomials.

We observed in Lemma 11.3 due to Hajós that the multiplicity of any nonzero complex zero of a complex k-sparse polynomial is at most $k-1$. Thus by the first part of Corollary 14.6, if a polynomial in a complex SPS representation with parameters p, q and k is shown to have a nonzero complex zero of multiplicity superpolynomial in pqk, then it also falsifies the following conjecture. The next conjecture appears essentially in Corollary 2.4 [42].

Conjecture 14.7 (Complex τ-Conjecture for Multiplicities)**.** *Let $f := \sum_{i=1}^{p} \prod_{j=1}^{q} f_{i,j}$ where each $f_{i,j}$ is a k-sparse complex polynomial. Then the multiplicity of any nonzero complex zero of f is at most $(pqk)^c$, where c is an absolute constant.*

Now the Complex τ-Conjecture for Sectors (Conjecture 14.3) implies Conjecture 14.7. Therefore, if 14.7 if false, then by Theorem 14.4 original real τ-conjecture (14.1) also becomes false. It would be an interesting open problem to investigate the strength of Conjecture 14.7 relative to the complex τ-conjecture for sectors (14.3) and the real τ-conjecture with multiplicities over $\mathbb{C}$. Tavenas (2014) [83] already showed that Conjecture 14.7 implies $\text{PERM}_n \notin \mathsf{VP}^0$. We know from Chapter 2 that real τ-conjecture implies $\text{PERM}_n \notin \mathsf{VP}$.

Type 2: Modifying the Form of the Polynomials and the Bound

Let us consider the variant proposed by Tavenas (2014) [83].

Conjecture 14.8 (Refined Real τ-Conjecture)**.** *Let $f := \sum_{i=1}^{p} \prod_{j=1}^{q} f_{i,j}$ where each $f_{i,j}$ is a k-sparse real polynomial. Then the number of distinct real zeros of f is at most $(p2^q k)^c$, where c is an absolute constant.*

Tavenas proposed another equivalent variant.

Conjecture 14.9 (Real τ-Conjecture with Powers)**.** *Let $f := \sum_{i=1}^{p} a_i f_i^{\alpha_i}$ where each f_i is a k-sparse real polynomial, $a_i \in \mathbb{R}$ and $\alpha_i \leq q$. Then the number of distinct real zeros of f is at most $(p2^q k)^c$, where c is an absolute constant.*

It is clear by chossing α_i many polynomials from $f_{i,1}, \ldots, f_{i,q}$ to be f_i and rest as the constant 1 for each i that 14.8 implies 14.9. For the other direction, we need to show that product of polynomials can be expressed sum of powers of polynomials. We shall use Fischer's trick [29]. Consider the $n \times n$ matrix X of indeterminates $x_1, \ldots, x_n$ such that for each i every entry in the ith column of X is the indeterminate x_i. The permanent of X is $n! \prod_{i=1}^{n} x_i$. By the Ryser's formula (Equation 2.1), we obtain

$$\prod_{i=1}^{n} x_i = \sum_{s=0}^{n-1} \sum_{\substack{S \subseteq \{1,\ldots,n\}, \\ |S|=s}} \frac{(-1)^s}{n!} \left(\sum_{j \notin S} x_j \right)^n .$$

Now we consider $f := \sum_{i=1}^{p} \prod_{j=1}^{q} f_{i,j}$, and if we apply this trick for each product term, then we get

$$f = \sum_{i=1}^{p} \sum_{s=0}^{q-1} \sum_{\substack{S \subseteq \{1,\ldots,q\}, \\ |S|=s}} \frac{(-1)^s}{q!} \left(\sum_{j \notin S} f_{i,j} \right)^q = \sum_{l=1}^{p(2^q-1)} a_l \tilde{f}_l^q,$$

for some $\tilde{f}_l$'s that are kq-sparse and real a_l's. By Conjecture 14.9, f has at most $(p(2^q-1)2^q kq)^c \leq (p2^q k)^{c'}$ many distinct real zeros. Thus

Theorem 14.10. *[83] Conjecture 14.8 and Conjecture 14.9 are equivalent.*

In Corollary 10.2, we were able to obtain the upper bound $k^{\mathcal{O}(p^2)}$ on the number of distinct real zeros of polynomials in Conjecture 14.9. This suggests that the powers α_i may be arbitrary, and we can seek an upper bound that is polynomial in just pk. The limitation of the Wronskian approach is that it helps count only the distinct real zeros. One can always reformulate Conjecture 14.9 for complex polynomials and complex zeros in a sector considering multiplicities.

Conclusion and Future Directions

In this thesis, we traced the history of the (real) τ-conjecture and learned two latest refinements of it. The variant due to Tavenas suggests that we focus on the sum of powers of sparse polynomials. The variant due to Hrubeš demands a closer look at distribution of zeros. We discussed how techniques from real or complex analysis apply. Studying complex zeros may be helpful since they have nice continuity property that real or integer zeros do not share. At the center of the Wronskian approach is the Rolle's theorem which gives some idea about the zeros of the derivative. But not completely! Location of the zeros of the derivative also need to be studied. How many of them are real? How many of them lie in a given sector? Already, Siebeck (1865) [77] and Linfield (1923) [55] showed that the zeros of the logarithmic derivative are the foci of a certain algebraic curve.

There are more variants of the τ-conjecture that are not discussed in this thesis. Koiran, Portier and Rojas (2013) [47] proposed a p-adic version; Koiran, Portier, Tavenas and Thomassé (2015) [49] proposed τ-conjecture for Newton polygons in the bivariate setting, and respectively techniques from number theory and combinatorial geometry may apply. In the random setting, Briquel and Bürgisser (2020) [14] showed that the real τ-conjecture is true on average. In the same spirit as Tavenas' variant, more recently, Dutta (2021) [27] [28] introduced τ-conjectures for sum-of-squares and sum-of-cubes.

Bibliography

[1] Manindra Agrawal and V Vinay. Arithmetic circuits: A chasm at depth four. In *2008 49th Annual IEEE Symposium on Foundations of Computer Science*, pages 67–75. IEEE, 2008.

[2] Louis François Antoine Arbogast. *Du calcul des dérivations*. Levrault, frères, 1800.

[3] Sanjeev Arora and Boaz Barak. *Computational complexity: a modern approach*. Cambridge University Press, 2009.

[4] EG Belaga. On computing polynomials in one variable with initial conditioning of the coefficients. *Problemy Kibernet*, 5:7–15, 1961.

[5] Michael Bensimhoun. Historical account and ultra-simple proofs of Descartes's rule of signs, De Gua, Fourier, and Budan's rule. *arXiv preprint arXiv:1309.6664*, 2013.

[6] M Biernacki. Sur les fonctions entières á série lacunaire. *CR Acad. Sci. Paris*, 187:477–479, 1928.

[7] Lenore Blum. Computing over the reals: Where Turing meets Newton. *Notices of the AMS*, 51(9):1024–1034, 2004.

[8] Lenore Blum, Felipe Cucker, Michael Shub, and Steve Smale. Complexity and real computation, 1997.

[9] Lenore Blum, Mike Shub, and Steve Smale. On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines. *Bulletin of the American Mathematical Society*, 21(1):1–46, 1989.

[10] Maxime Bôcher. The theory of linear dependence. *Annals of Mathematics*, 2(1/4):81–96, 1900.

[11] Maxime Bocher. Certain cases in which the vanishing of the Wronskian is a sufficient condition for linear dependence. *Transactions of the American Mathematical Society*, 2(2):139–149, 1901.

[12] Allan Borodin and Stephen Cook. On the number of additions to compute specific polynomials. *SIAM Journal on Computing*, 5(1):146–157, 1976.

[13] David M Bressoud. *Proofs and confirmations: the story of the alternating-sign matrix conjecture*. Cambridge University Press, 1999.

[14] Irénée Briquel and Peter Bürgisser. The real tau-conjecture is true on average. *Random Structures & Algorithms*, 57(2):279–303, 2020.

[15] F. D. Budan. *Nouvelle méthode pour la résolution des equations d'un degrè quelconque*. Bondé-Dupré, Bachelier, Paris, 1822.

[16] Peter Bürgisser. *Completeness and reduction in algebraic complexity theory*, volume 7. Springer Science & Business Media, 2000.

[17] Peter Bürgisser. On defining integers and proving arithmetic circuit lower bounds. *Computational Complexity*, 18(1):81–103, 2009.

[18] Peter Bürgisser. Completeness classes in algebraic complexity theory. *arXiv preprint arXiv:2406.06217*, 2024.

[19] Peter Bürgisser, Michael Clausen, and Amin Shokrollahi. *Algebraic Complexity Theory*, volume 315. Springer Science & Business Media, 1996.

[20] Augustin-Louis Cauchy. *Sur la mecanique celeste et sur un nouveau calcul qui s' applique a un grand nombre de questions diverses etc.* na, 1831.

[21] JP De Gua. Recherches du nombre des racines réelles ou imaginaires, réelles positives ou réelles négatives, qui peuvent se trouver dans les équations de tous les degrés. *Histoire de l'Academie royale des sciences (sec. mémoires)*, pages 435–494, 1741.

[22] Wellington De Melo and Benar Fux Svaiter. The cost of computing integers. *Proceedings-American Mathematical Society*, 124:1377–1378, 1996.

[23] H. Dellac. Question 49. *L'Intermédiaire des Mathématiciens*, 1:20, 1894.

[24] René Descartes. *La géométrie*. 1637.

[25] P Desnanot. *Complément de la théorie des équations du premier degré... par P. Desnanot...* Volland jeune, 1819.

[26] Charles L Dodgson. Condensation of determinants, being a new and brief method for computing their arithmetical values. *Proceedings of the Royal Society of London*, pages 150–155, 1866.

[27] Pranjal Dutta. Real τ-conjecture for sum-of-squares: A unified approach to lower bound and derandomization. In *International Computer Science Symposium in Russia*, pages 78–101. Springer, 2021.

[28] Pranjal Dutta. *A tale of hardness, de-randomization and de-bordering in complexity theory*. PhD thesis, PhD Thesis, 2022.

[29] Ismor Fischer. Sums of like powers of multivariate linear forms. *Mathematics Magazine*, 67(1):59–61, 1994.

[30] J. Fourier. Sur l'usage du théorème de descartes dans la recherches des limites des racines. *Bulletin des Sciences par la Société philomatique de Paris*, pages 156–165, 181–187, October and December 1820.

[31] Georg Frobenius and A Milinowski. Ueber die determinante mehrerer functionen einer variabeln. 1874.

[32] C. F. Gauss. Beweis eines algebraischen lehrsatzes. *Crelle's Journal für die reine und angewandte Mathematik*, 3, January 1828.

[33] Bruno Grenet, Pascal Koiran, Natacha Portier, and Yann Strozecki. The limited power of powering: Polynomial identity testing and a depth-four lower bound for the permanent. In Supratik Chakraborty and Amit Kumar, editors, *IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science, FSTTCS 2011, December 12-14, 2011, Mumbai, India*, volume 13 of *LIPIcs*, pages 127–139. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2011.

[34] György Hajós. Solution to problem 41. *Mat. Lapok*, 4(4):41, 1953.

[35] WK Hayman. Angular value distribution of power series with gaps. *Proceedings of the London Mathematical Society*, 3(4):590–624, 1972.

[36] Joos Heintz. On the computational complexity of polynomials and bilinear mappings. A survey. In *International Conference on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*, pages 269–300. Springer, 1987.

[37] Joos Heintz and Jacques Morgenstern. On the intrinsic complexity of elimination theory. *Journal of Complexity*, 9(4):471–498, 1993.

[38] G Hermann. Die frage der endlich vielen schritte in der theorie der polynomideale.(unter benutzung nachgelassener sätze von k. hentzelt). *Mathematische Annalen*, 95:736–788, 1926.

[39] D Hilbert. Ueber die vollen invariantensysteme. *Mathematische Annalen*, 42:313–373, 1893.

[40] David Hilbert. Mathematical problems. *Bulletin of the American Mathematical Society*, 8(10):437–479, 1902.

[41] William George Horner. Xxi. a new method of solving numerical equations of all orders, by continuous approximation. *Philosophical Transactions of the Royal Society of London*, (109):308–335, 1819.

[42] Pavel Hrubeš. On the real τ-conjecture and the distribution of complex roots. *Theory of Computing*, 9(10):403–411, 2013.

[43] Carl Gustav Jacob Jacobi. De binis quibuslibet functionibus homogeneis secundi ordinis per substitutiones lineares in alias binas tranformandis, quae solis quadratis variabilium constant; una cum variis theorematis de tranformatione etdeterminatione integralium multiplicium. 1834.

[44] DE Knuth. The art of computer programming: seminumerical algorithms. In *The art of computer programming: seminumerical algorithms*, pages 624–624. 1969.

[45] Pascal Koiran. Valiant's model and the cost of computing integers. *computational complexity*, 13(3):131–146, 2005.

[46] Pascal Koiran. Shallow circuits with high-powered inputs. In Bernard Chazelle, editor, *Innovations in Computer Science - ICS 2011, Tsinghua University, Beijing, China, January 7-9, 2011. Proceedings*, pages 309–320. Tsinghua University Press, 2011.

[47] Pascal Koiran, Natacha Portier, and J Maurice Rojas. Counting tropically degenerate valuations and p-adic approaches to the hardness of the permanent. *arXiv preprint arXiv:1309.0486*, 2013.

[48] Pascal Koiran, Natacha Portier, and Sébastien Tavenas. A Wronskian approach to the real τ-conjecture. *J. Symb. Comput.*, 68:195–214, 2015.

[49] Pascal Koiran, Natacha Portier, Sébastien Tavenas, and Stéphan Thomassé. A τ-conjecture for Newton polygons. *Foundations of computational mathematics*, 15(1):185–197, 2015.

[50] Pascal Koiran and Mateusz Skomra. Intersection multiplicity of a sparse curve and a low-degree curve. *Journal of Pure and Applied Algebra*, 224(7):106279, 2020.

[51] János Kollár. Sharp effective nullstellensatz. *Journal of the American Mathematical Society*, pages 963–975, 1988.

[52] PV Krishnaiah. A simple proof of Descartes' rule of signs. *Mathematics Magazine*, 36(3):190–190, 1963.

[53] Joseph-Louis Lagrange. Recherches d'arithmétique. 1773.

[54] Edmond Nicolas Laguerre. Sur la règle des signes de Descartes. *Nouvelles Annales de Mathématiques, 2e série*, 18:67–71, 1879.

[55] Ben Zion Linfield. On certain polar curves with their application to the location of the roots of the derivatives of a rational function. *Transactions of the American Mathematical Society*, 25(2):239–258, 1923.

[56] Meena Mahajan. Algebraic complexity classes. *Perspectives in Computational Complexity: The Somenath Biswas Anniversary Volume*, pages 51–75, 2014.

[57] Gregorio Malajovich. On a transfer theorem for the P$\neq$ NP conjecture. *Journal of Complexity*, 17(1):27–85, 2001.

[58] Guillaume Malod. *Polynômes et coefficients*. PhD thesis, Université Claude Bernard-Lyon I, 2003.

[59] Guillaume Malod and Natacha Portier. Characterizing Valiant's algebraic complexity classes. *Journal of complexity*, 24(1):16–38, 2008.

[60] Yuri V Matiyasevich. Hilbert's tenth problem, 1993.

[61] L Mina. Formole generali delle derivate successive d'una funzione espresse mediante quelle della sua inverse. *Giornale di Mat*, 43:196–212, 1904.

[62] H Montgomery and A Schinzel. Some arithmetic properties of polynomials in several variables. *Transcendence Theory: Advances and Applications*, pages 195–203, 1977.

[63] Carlos Moreira. On asymptotic estimates for arithmetic cost functions. *Proceedings of the American Mathematical Society*, 125(2):347–353, 1997.

[64] Alexander M Ostrowski. On two problems in abstract algebra connected with Horner's rule. In *Studies in Mathematics and Mechanics presented to Richard von Mises*, pages 40–48. Academic Press San Diego, 1954.

[65] V Ya Pan. Methods of computing values of polynomials. *Russian Mathematical Surveys*, 21(1):105, 1966.

[66] Giuseppe Peano. Sur le déterminant Wronskien. *Mathesis*, 9(75–76):110–2, 1889.

[67] Bruno Poizat. *Les petits cailloux*. 1995.

[68] George Pólya and Gabor Szegö. *Problems and theorems in analysis II: theory of functions. Zeros. Polynomials. Determinants. Number theory. Geometry*. Springer, 1976.

[69] Q I Rahman and G Schmeisser. *Analytic Theory of Polynomials*. Oxford University Press, 09 2002.

[70] Jean-Jacques Risler. Additive complexity and zeros of real polynomials. *SIAM Journal on Computing*, 14(1):178–183, 1985.

[71] J Maurice Rojas. Additive complexity and roots of polynomials over number fields and p-adic fields. In *International Algorithmic Number Theory Symposium*, pages 506–515. Springer, 2002.

[72] J Maurice Rojas. A direct ultrametric approach to additive complexity and the Shub-Smale tau conjecture. *arXiv preprint math/0304100*, 2003.

[73] Herbert John Ryser. *Combinatorial mathematics*, volume 14. American Mathematical Soc., 1963.

[74] Arnold Scholz. Aufgabe 253. *Jahresbericht der deutchen Mathematiker-Vereinigung*, 47:41–42, 1937.

[75] Arnold Schönhage. An elementary proof for strassen's degree bound. *Theoretical Computer Science*, 3(2):267–272, 1976.

[76] Michael Shub and Steve Smale. On the intractability of Hilbert's Nullstellensatz and an algebraic version of "$NP \neq P$?". *Duke Mathematical Journal*, 81(1):47 – 54, 1995.

[77] P Siebeck. Ueber eine neue analytische behandlungsweise der brennpunkte. 1865.

[78] Steve Smale. Mathematical problems for the next century. *The Mathematical Intelligencer*, 20:7–15, 1998.

[79] Volker Strassen. Die berechnungskomplexität von elementarsymmetrischen funktionen und von interpolationskoeffizienten. *Numerische Mathematik*, 20:238–251, 1973.

[80] Volker Strassen. Vermeidung von divisionen. *Journal für die reine und angewandte Mathematik*, 264:184–202, 1973.

[81] Volker Strassen. Einige resultate über berechnungskomplexität. *Jahresbericht der Deutschen Mathematiker-Vereinigung*, 78:1–8, 1976.

[82] Volker Strassen. Algebraic complexity theory. In *Algorithms and Complexity*, pages 633–672. Elsevier, 1990.

[83] Sébastien Tavenas. *Bornes inférieures et supérieures dans les circuits arithmétiques*. These de doctorat, Lyon, École normale supérieure, July 2014.

[84] Leslie G Valiant. Completeness classes in algebra. In *Proceedings of the eleventh annual ACM symposium on Theory of computing*, pages 249–261, 1979.

[85] Leslie G Valiant. The complexity of computing the permanent. *Theoretical computer science*, 8(2):189–201, 1979.

[86] Jean-Paul Van de Wiele. *Complexité additive et zéros des polynômes à coefficients réels et complexes*. PhD thesis, IRIA, 1978.

[87] M Voorhoeve and A.J Van Der Poorten. Wronskian determinants and the zeros of certain functions. *Indagationes Mathematicae (Proceedings)*, 78(5):417–424, 1975.

[88] Herbert S Wilf. A combinatorial determinant. *arXiv preprint math/9809120*, 1998.