On the Order of Power Series and the Sum of Square Roots Problem

Louis Gaillard
louis.gaillard@ens-lyon.fr
École Normale Supérieure de Lyon
Lyon, France

Gorav Jindal
gjindal@mpi-sws.org
Max Planck Institute for Software Systems
Saarbrücken, Germany

ABSTRACT

This paper focuses on the study of the order of power series that are linear combinations of a given finite set of power series. The order of a formal power series, known as $\mathrm{ord}(f)$, is defined as the minimum exponent of x that has a non-zero coefficient in $f(x)$. Our first result is that the order of the Wronskian of these power series is equivalent up to a polynomial factor, to the maximum order which occurs in the linear combination of these power series. This implies that the Wronskian approach used in (Kayal and Saha, TOCT'2012) to upper bound the order of sum of square roots is optimal up to a polynomial blowup. We also demonstrate similar upper bounds, similar to those of (Kayal and Saha, TOCT'2012), for the order of power series in a variety of other scenarios. We also solve a special case of the inequality testing problem outlined in (Etessami et al., TOCT'2014).

In the second part of the paper, we study the equality variant of the sum of square roots problem, which is decidable in polynomial time due to (Blömer, FOCS'1991). We investigate a natural generalization of this problem when the input integers are given as straight line programs. Under the assumption of the Generalized Riemann Hypothesis (GRH), we show that this problem can be reduced to the so-called "one dimensional" variant. We identify the key mathematical challenges for solving this "one dimensional" variant.

CCS CONCEPTS

• **Theory of computation** → **Algebraic complexity theory**; • **Mathematics of computing** → *Probabilistic algorithms.*

KEYWORDS

Formal power series, Sum of square roots, Wronskian, Differential equations, Straight line Programs.

ACM Reference Format:
Louis Gaillard and Gorav Jindal. 2023. On the Order of Power Series and the Sum of Square Roots Problem. In *International Symposium on Symbolic and Algebraic Computation 2023 (ISSAC 2023), July 24–27, 2023, Tromsø, Norway.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3597066.3597079

ISSAC 2023, July 24–27, 2023, Tromsø, Norway

ACM ISBN 979-8-4007-0039-2/23/07…$15.00
https://doi.org/10.1145/3597066.3597079

1 INTRODUCTION

For numerous decision problems that require determining the sign of expressions with real numbers, their complexity class (e.g., if they belong to P or not) is often unknown. A notable instance is the Sum of Square Roots problem, which can be described as:

Problem 1 (Sum of Square Roots (SSR)). *Given a list* $(a_1, a_2, \ldots, a_n)$ *of positive integers and* $(\delta_1, \delta_2, \ldots, \delta_n) \in \{-1, 1\}^n$, *decide whether* $\sum_{i=1}^{n} \delta_i \sqrt{a_i} > 0$.

The complexity of this problem has been extensively investigated and remains an open question according to Garey, Graham, and Johnson [13]. Additionally, it has been hypothesized that it lies in P, as proposed by Malajovich in 2001 [17]. The SSR problem shares deep connections with classical geometric problems such as the Euclidean Traveling Salesman Problem (ETSP), which is not known to be in NP. It is readily seen to be in NP relative to an oracle of SSR. An important related problem where the task is to determine the sign of an integer (encoded by a straight line program), is the so called PosSLP problem. A sequence P of integers $(b_0, b_1, b_2, \ldots, b_\ell)$ is said to be a straight line program (SLP) if $b_0 = 1$ and for all $1 \leq i \leq \ell$, $b_i = b_j \circ_i b_k$, where $\circ_i \in \{+, -, *\}$ and $j, k < i$. We say that this SLP P computes the integer b_ℓ. We say that ℓ is the size (or length) of this SLP P.

Problem 2 (PosSLP). *Given an SLP* P, *decide if the integer* n_P *computed by* P *is positive.*

The approximation of $\sqrt{a_i}$ in Problem 1 to an appropriate precision leads to the reduction of SSR to PosSLP, as demonstrated in [1]. PosSLP was introduced in this work to bridge the gap between classical models of computation and computation over the reals in the Blum-Shub-Smale (BSS) model [8], which is a widely studied model for the study of computational complexity in numerical analysis.

It was shown in [1] that PosSLP captures the "Boolean part" of languages decidable in the BSS model in polynomial time, with polynomial time Turing reductions. Additionally, PosSLP was proven to lie within the counting hierarchy CH, implying that SSR also falls within CH. To date, this represents the best known upper bound for the complexity of SSR.

Our contributions can be found in Section 1.2 after having introduced some useful previous work on Problem 1 in Section 1.1.

1.1 Related work

In different scenarios, there is a need to determine if the sum of square roots is equal to zero or not, rather than determining the sign of the expression. As a result, we encounter an intriguing problem known as $\mathrm{SSR}_{\mathrm{eq}}$.

Problem 3 ($\mathrm{SSR}_{\mathrm{eq}}$). *Given a list $(a_1, a_2, \ldots, a_n)$ of integers and $(\delta_1, \delta_2, \ldots, \delta_n) \in \{-1, 1\}^n$, decide whether $\sum_{i=1}^n \delta_i \sqrt{a_i} = 0$.*

Blömer [6] gave a polynomial time algorithm to compute sums of radicals and also proved that $\mathrm{SSR}_{\mathrm{eq}}$ is in P. Thus, testing if a signed sum of square roots is zero seems to be easier than deciding its sign. A natural idea for an algorithm for the SSR problem would be to approximate the sum with a floating point number thanks to classical numerical algorithms. However, one would need a result on the required number of bits of precision of the approximation to ensure that the two signs coincide. It is known ([11]) that for an integer of bit size at most B, its square root can be approximated up to m bits of precision in time $\mathrm{poly}(B, m)$. And this implies that a solution of the following number theoretic problem would lead to a polynomial time algorithm for the SSR problem.

Problem 4 (Lower-bound on a nonzero sum of square roots). *Given a sum $S = \sum_{i=1}^n \delta_i \sqrt{a_i}$, with $\delta_i \in \{-1, 1\}$ and $1 \leq a_i < 2^B$, can we find a polynomial $q(n, B)$ such that*

$$S \neq 0 \implies |S| \geq \frac{1}{2^{q(n,B)}}?$$

In contrast to Problem 4, one can also try to find a_i's and corresponding δ_i's such that the absolute value of $\sum_{i=1}^n \delta_i \sqrt{a_i}$ is *small*. In this direction, it was shown in [18] that $\left|\sum_{i=0}^m \binom{m}{i} (-1)^i \sqrt{n+i}\right| = O(n^{-m+\frac{1}{2}})$. Kayal and Saha [14] chose to approach Problem 4 by formulating a related question over polynomials. This approach proved to be simpler. They focused on non-zero sums of square roots of polynomials, which they viewed as power series, and demonstrated that the valuation (or order) of such a series cannot be *too high*.

Theorem 1 (Bounding the order of sum of square roots of polynomials [14]). *For $1 \leq i \leq n$, let $c_i \in \mathbb{C}$ and $f_i, g_i \in \mathbb{C}[x]$ of degree at most d with $f_i(0) \neq 0$. We denote and fix $\sqrt{f_i(x)} \in \mathbb{C}[[x]]$ one of the two square roots of $f_i(x)$. If the sum $S(x) = \sum_{i=1}^n c_i g_i(x) \sqrt{f_i(x)}$ is non-zero, then $\mathrm{ord}(S) \leq dn^2 + n$.*

The main technical argument of this proof is the study of the Wronskian determinant of the family $(g_i \sqrt{f_i})_{1 \leq i \leq n}$, because by Cramer's rule, one can easily bound the order of S with respect to the order of this Wronskian.

Next, they apply this result to a set of integers by representing them as polynomials and they confirm that the solution to Problem 4 is affirmative for a significant subclass of integers known as *polynomial integers*.

Theorem 2 (SSR for *polynomial integers* [14]). *Suppose $S = \sum_{i=1}^n \delta_i \sqrt{a_i}$ is non-zero with $\delta_i \in \{-1, 1\}$, such that every positive integer a_i is of the form $a_i = X^{d_i} + b_{1,i} X^{d_i - 1} + \cdots + b_{d_i,i}$ with $d_i > 0$, X a positive integer and $d_i, b_{j,i}$ are integers. Let $B = \max\left(\left\{\left|b_{j,i}\right|\right\}_{j,i}, 1\right)$ and $d = \max_i d_i$. There exist two fixed integer polynomials $p(n, d), q(n, d)$ in n and d such that if $X \geq (B+1)^{p(n,d)}$, then S is lower bounded as $|S| \geq \frac{1}{X^{q(n,d)}}$.*

Based on these observations, it raises the question of whether the concept of bounding the order of sums of power series can be generalized to other families beyond square roots. This could potentially yield significant insights into the complexity of determining the positivity of expressions involving irrational real numbers.

1.2 Our results

From now on, $\mathbb{K}$ denotes a field of characteristic 0. All the logarithms in this paper are natural logarithms with base e, unless otherwise stated. We now define some measures to formally state our results.

Definition 1. *Suppose $\mathcal{F} \subseteq \mathbb{K}[[x]]$ is a finite dimensional linear subspace of $\mathbb{K}[[x]]$, we define*

$$O(\mathcal{F}) := \sup\{\mathrm{ord}(f) \mid f \in \mathcal{F} \setminus \{0\}\} \in \mathbb{N} \cup \infty.$$

And for $\mathbf{f} = (f_1, f_2, \ldots, f_n)$ a family of linearly independent power series, we define

$$O(f_1, f_2, \ldots, f_n) = O(\mathbf{f}) := O(\mathrm{span}(f_1, f_2, \ldots, f_n)).$$

A set $\{f_1, f_2, \ldots, f_n\}$ of n functions over $\mathbb{K}$ is said to be linearly dependent if there exist scalars $c_1, c_2, \ldots, c_n \in \mathbb{K}$ (not all zero) such that $\sum_{i=1}^n c_i f_i$ is zero. To define the Wronskian of $\{f_1, f_2, \ldots, f_n\}$, we assume that each f_i is $n-1$ times differentiable. The Wronskian of $\{f_1, f_2, \ldots, f_n\}$, denoted $W(f_1, f_2, \ldots, f_n)$ is defined as the determinant of the following matrix:

$$W(\mathbf{f}) = W(f_1, f_2, \ldots, f_n) := \det \begin{pmatrix} f_1 & \cdots & f_n \\ f_1^{(1)} & \cdots & f_n^{(1)} \\ \vdots & \vdots & \vdots \\ f_1^{(n-1)} & \cdots & f_n^{(n-1)} \end{pmatrix}$$

Proposition 1. *Let $\mathcal{F} \subseteq \mathbb{K}[[x]]$ be an n-dimensional linear subspace. For any basis $(f_1, f_2, \ldots, f_n)$ of $\mathcal{F}$, $\mathrm{ord}(W(f_1, f_2, \ldots, f_n))$ does not depend on the choice of the basis $(f_1, f_2, \ldots, f_n)$. We denote this quantity by $W_{\mathrm{ord}}(\mathcal{F})$.*

Proof. Let $(g_1, g_2, \ldots, g_n)$ be another basis of $\mathcal{F}$. There exists an invertible $n \times n$ matrix A with entries in $\mathbb{K}$ such that

$$\begin{bmatrix} g_1 & \cdots & g_n \end{bmatrix} = \begin{bmatrix} f_1 & \cdots & f_n \end{bmatrix} \cdot A.$$

By linearity of the differentiation, we also have for all $0 \leq j < n$,

$$\begin{bmatrix} g_1^{(j)} & \cdots & g_n^{(j)} \end{bmatrix} = \begin{bmatrix} f_1^{(j)} & \cdots & f_n^{(j)} \end{bmatrix} \cdot A.$$

Thus we have $W(g_1, g_2, \ldots, g_n) = W(f_1, f_2, \ldots, f_n) \cdot \det(A)$. By using the fact that $\det(A) \in \mathbb{K}^*$, the result follows. □

The following theorem bounds $O(\mathcal{F})$ in terms of $W_{\mathrm{ord}}(\mathcal{F})$. This theorem is actually a result of Voorhoeve and Van der Poorten [21]. The same idea is used by Kayal and Saha [14] to establish the bound in Theorem 1.

Theorem 3 (Theorem 1 in [21]). *Let $\mathcal{F}$ be an n-dimensional linear subspace of $\mathbb{K}[[x]]$. Then, $O(\mathcal{F}) \leq W_{\mathrm{ord}}(\mathcal{F}) + n - 1$.*

In Section 2, we show that Theorem 3 is almost tight, in the sense that the order of the Wronskian of a family $(h_1, h_2, \ldots, h_n)$ of power series is equivalent, up to a polynomial factor, to the maximum order of a non-zero linear combination of the h_i's. This result is formalized in Theorem 4 below.

Theorem 4. *Let $\mathcal{F}$ be an n-dimensional linear subspace of $\mathbb{K}[[x]]$. Then, $W_{\mathrm{ord}}(\mathcal{F}) \leq n \cdot O(\mathcal{F}) - \binom{n}{2}$.*

For a full proof of Theorem 4, refer to Section 2. We then demonstrate that the approach of Kayal and Saha in Theorem 1 can be extended to sums of solutions of linear differential equations of order 1 with polynomial coefficients, resulting in a comparable bound

on the sum's order. This result is formally stated in Theorem 5 below.

Theorem 5. *Let $S(x) = \sum_{i=1}^{n} c_i g_i(x) y_i(x)$, with $y_i' - \frac{p_i}{q_i} y_i = 0$, where $c_i \in \mathbb{K}$ and $g_i, p_i, q_i \in \mathbb{K}[x]$ of degree at most d. We assume that $q_i(0) \neq 0$ and that each $y_i \in \mathbb{K}[[x]]$. If $S \neq 0$, then*

$$\operatorname{ord}(S) \leq \sum_{i=1}^{n} \operatorname{ord}(y_i) + n^2 d + n - 1.$$

Proof idea for Theorem 5. The bound for $\operatorname{ord}(S)$ follows from Theorem 3, once we have bounded the order of the Wronskian of the family $(g_i y_i)_{1 \leq i \leq n}$ by $\sum_i \operatorname{ord}(y_i) + n^2 d$. To do this, we study the entries of the Wronskian matrix and use the differential equations to replace derivatives of the y_i's. We show that every entry (i, j) of the Wronskian matrix can be written $y_i \frac{m_{i,j}}{q_i^{n-1}}$, where q_i is the denominator in the differential equation satisfied by y_i and $m_{i,j}$ is a polynomial of degree $\leq nd$. The result directly follows by bounding the order of the polynomials $m_{i,j}$ by their degree. For a full proof of Theorem 5, see Section 3.

In Section 4, we investigate the following Problem 5 ($\mathrm{SSR}_{\mathrm{SLP}}$) that can be regarded as a generalization of Problem 3 ($\mathrm{SSR}_{\mathrm{eq}}$) in the context of SLPs.

Problem 5 ($\mathrm{SSR}_{\mathrm{SLP}}$). *Given as input n straight line programs $(P_1, P_2, \ldots, P_n)$ of size $\leq s$ and $(\delta_1, \delta_2, \ldots, \delta_n) \in \{-1, 1\}^n$, such that P_i computes the positive integer a_i, decide whether $\sum_{i=1}^{n} \delta_i \sqrt{a_i} = 0$.*

Here we show that assuming GRH, under randomized polynomial time Turing reductions, $\mathrm{SSR}_{\mathrm{SLP}}$ can be reduced to the following "one-dimensional" variant of $\mathrm{SSR}_{\mathrm{SLP}}$,

Problem 6 (One dimensional $\mathrm{SSR}_{\mathrm{SLP}}$). *Given n straight line programs computing n positive integers $(a_1, a_2, \ldots, a_n)$ and $(\delta_1, \delta_2, \ldots, \delta_n) \in \{-1, 1\}^n$, with the promise that $\dim(\mathrm{span}_{\mathbb{Q}}(\sqrt{a_1}, \sqrt{a_2}, \ldots, \sqrt{a_n})) = 1$. Decide if $\sum_{i=1}^{n} \delta_i \sqrt{a_i} = 0$.*

Proof idea for reducing $\mathrm{SSR}_{\mathrm{SLP}}$ to one dimensional $\mathrm{SSR}_{\mathrm{SLP}}$. Given an instance of Problem 5, we separate the inputs into several one-dimensional subgroups. This is possible because we demonstrate an efficient randomized algorithm to test the linear dependency of square roots of integers given by SLPs, using the ideas of Kneser [15] and recounted out in Blömer's work in [6]. According to Kneser's result [15], a set of square roots are linearly dependent over $\mathbb{Q}$ if and only if there exists a pair of linearly dependent square roots within the set. Once the instance of Problem 5 is separated into one-dimensional subgroups, it remains only to determine if each subsum is zero, which can be done using an oracle for Problem 6. For a full proof, see Section 4.

In Section 5, we show a similar upper bound to that of Theorem 1, on the order of sums of logarithms of real polynomials.

Proposition 2. *Let $S(x) = \sum_{i=1}^{n} c_i \log(f_i(x)) \neq 0$, where $c_i \in \mathbb{R}$, $f_i \in \mathbb{R}[x]$ of degree at most d and $f_i(0) > 0$. Then $\operatorname{ord}(S) \leq nd$.*

We also show an analogous result to Theorem 2 but for the problem of the positivity testing of linear forms of logarithms of integers whose complexity is connected to deep conjectures in number-theory [12], such as a refinement of the *abc* conjecture formulated by Baker [3]. This result essentially follows from Theorem 6 below, which is our analogue of Theorem 2. For a full proof of Theorem 6, see Section 5.

Theorem 6 (Sum of logarithms of *polynomial integers*). *Suppose $E = \sum_{i=1}^{n} c_i \log a_i$ is non-zero, where $c_i \in \mathbb{Z}$, and every a_i is a positive integer of the form $a_i = X^{d_i} + b_{1,i} X^{d_i - 1} + \cdots + b_{d_i,i}$, where $d_i > 0$, X is a positive integer and $d_i, b_{j,i}$ are integers. Let $B = \max\left(\left\{\left|b_{j,i}\right|\right\}_{j,i}, 1\right)$, $d = \max_i d_i + 1$, and $C = \max_i |c_i|$. There exist two fixed integer polynomial $p_1(n, d), p_2(n, d)$ in n and d such that if $X > \max\left(C^2, (B+1)^{p_1(n,d)}\right)$, then E is lower bounded as $|E| \geq \frac{1}{X^{p_2(n,d)}}$.*

2 ORDER OF THE WRONSKIAN DETERMINANT

In this section we show that for a family of power series, the maximal order that can occur in a non-zero linear combination is the order of the Wronskian determinant of the family up to a polynomial factor. Our proof of Theorem 4 is inspired from the ideas developed in [10]. For $d, k \in \mathbb{N}$, we denote

$$(d)_k := d(d-1)\ldots(d-k+1),$$

with the convention $(d)_0 = 1$.

Definition 2 (Vandermonde determinant). *Let $(d_1, d_2, \ldots, d_n) \in \mathbb{K}^n$, we define the corresponding Vandermonde determinant as follows:*

$$V(d_1, d_2, \ldots, d_n) := \det\left((d_j^{i-1})_{1 \leq i,j \leq n}\right) = \prod_{1 \leq i < j \leq n} (d_j - d_i).$$

Lemma 7 (Wronskian of monomials, Lemma 1 in [10]). *The Wronskian of the monomials $a_1 x^{d_1}, \ldots, a_n x^{d_n}$ is*

$$W(a_1 x^{d_1}, \ldots, a_n x^{d_n}) = V(d_1, d_2, \ldots, d_n) \left(\prod_{i=1}^{n} a_i\right) x^{d_1 + \cdots + d_n - \binom{n}{2}}.$$

Lemma 8 (Lemma 2 in [10]). *Let $f_1, f_2, \ldots, f_n$ be a family of $\mathbb{K}[[x]]$ which are linearly independent over $\mathbb{K}$. There exists an invertible $n \times n$ matrix A with entries in $\mathbb{K}$ such that the power series $g_1, g_2, \ldots, g_n$ defined by*

$$\begin{bmatrix} g_1 & \ldots & g_n \end{bmatrix} = \begin{bmatrix} f_1 & \ldots & f_n \end{bmatrix} \cdot A \tag{1}$$

are all non-zero and have mutually distinct orders.

Lemma 9 (Wronskian of distinct order power series). *If the non-zero power series $g_1, g_2, \ldots, g_n \in \mathbb{K}[[x]]$ have mutually distinct orders $d_1, d_2, \ldots, d_n$, then their Wronskian $W(g_1, g_2, \ldots, g_n)$ is non-zero and satisfies:*

$$\operatorname{ord}(W(g_1, g_2, \ldots, g_n)) = \sum_{i=1}^{n} d_i - \binom{n}{2}.$$

Proof. If the g_j's are monomials, *i.e.*$g_j = a_j x^{d_j}$, the result is a direct consequence of Lemma 7, and in this case, the (i, j) entry of the Wronskian matrix is $w_{i,j} = a_j (d_j)_{i-1} x^{d_j - i + 1}$. In the general case, let $g_j = a_j x^{d_j} + u_j$ with $u_j \in \mathbb{K}[[x]]$ of order $> d_j$. Then the (i, j) entry of the Wronskian matrix now becomes $w_{i,j} \times (1 + x r_{i,j})$ for some $r_{i,j} \in \mathbb{K}[[x]]$.

So we have $W(g_1, g_2, \ldots, g_n) = a_1 \ldots a_n x^{d_1 + \cdots + d_n - \binom{n}{2}} \det(D)$ where D is the $n \times n$ matrix $D = ((d_j)_{i-1}(1 + x r_{i,j}))_{1 \leq i,j \leq n}$. Now

we evaluate D at $x = 0$, and we obtain $D(0) = ((d_j)_{i-1})_{1\le i,j\le n}$. With elementary row operations (which preserve the determinant), as in the proof of Lemma 7 in [10], we can transform $D(0)$ into the Vandermonde matrix associated to $d_1, \dots, d_n$. So, $\det(D(0)) = V(d_1, d_2, \dots, d_n) \neq 0$, because the d_i's are distinct. Thus $\det(D)$ is non zero modulo x, so $\det D$ has order zero and the result follows. □

We now formulate a tight variant (Theorem 10) of Theorem 4, which immediately implies Theorem 4. Suppose $\mathcal{F} \subseteq \mathbb{K}[[x]]$ is a finite dimensional subspace of $\mathbb{K}[[x]]$. Lemma 8 shows that if $\dim(\mathcal{F}) = n$ then there exist n power series $g_1, g_2, \dots, g_n$ in $\mathcal{F}$ which have distinct orders $d_1, d_2, \dots, d_n$. Moreover $g_1, g_2, \dots, g_n$ also form a basis of $\mathcal{F}$. We now claim that these are the only possible orders of any power series in $\mathcal{F}$. Assume $d_1 < d_2 < \cdots < d_n$. If $f = \sum_{i=1}^n \lambda_i g_i$ (with $\lambda_i \in \mathbb{K}$) is a non-zero power series in $\mathcal{F}$, then it is clear that $\operatorname{ord}(f) = d_j$ where j is the minimum index such that $\lambda_j \neq 0$. With this claim, we formulate the following tight variant of Theorem 4.

Theorem 10. *Let $\mathcal{F}$ be an n-dimensional linear subspace of $\mathbb{K}[[x]]$. Suppose $d_1, d_2, \dots, d_n$ are the distinct orders of power series which occur in $\mathcal{F}$. Then, $W_{\mathrm{ord}}(\mathcal{F}) = \sum_{i=1}^n d_i - \binom{n}{2}$.*

Proof. By Lemma 8, there exists a basis $(g_1, g_2, \dots, g_n)$ of $\mathcal{F}$ with distinct order $d_1, d_2, \dots, d_n$. By using Lemma 9, $W_{\mathrm{ord}}(\mathcal{F}) = \sum_{i=1}^n d_i - \binom{n}{2}$. □

Theorem 4. *Let $\mathcal{F}$ be an n-dimensional linear subspace of $\mathbb{K}[[x]]$. Then, $W_{\mathrm{ord}}(\mathcal{F}) \le n \cdot O(\mathcal{F}) - \binom{n}{2}$.*

Proof. The claim immediately follows from Theorem 10. □

This completes the proof of Theorem 4. By combining Theorem 4 and Theorem 3, we conclude that the order of the Wronskian determines the maximum order of linear combinations of power series, up to a polynomial factor in n.

Now we show an example where the bound claimed in Theorem 3 is tight. Suppose $\mathcal{G}$ is the linear subspace of $\mathbb{K}[[x]]$ generated by the monomials $1, x, x^2, \dots, x^{n-1}$. It is easy to see that Wronskian of $1, x, x^2, \dots, x^{n-1}$ is $\prod_{i=1}^{n-1} i!$. Hence $W_{\mathrm{ord}}(\mathcal{G}) = 0$. We also have that $O(\mathcal{G}) = n - 1$.

3 SUMS OF SOLUTIONS OF LINEAR DIFFERENTIAL EQUATIONS

As a generalization of Theorem 1 and as an application of Theorem 3, we now prove a polynomial bound on the order of a sum of power series that are solutions of linear differential equations of order 1 with polynomial coefficients.

Theorem 5. *Let $S(x) = \sum_{i=1}^n c_i g_i(x) y_i(x)$, with $y_i' - \frac{p_i}{q_i} y_i = 0$, where $c_i \in \mathbb{K}$ and $g_i, p_i, q_i \in \mathbb{K}[x]$ of degree at most d. We assume that $q_i(0) \neq 0$ and that each $y_i \in \mathbb{K}[[x]]$. If $S \neq 0$, then*

$$\operatorname{ord}(S) \le \sum_{i=1}^n \operatorname{ord}(y_i) + n^2 d + n - 1.$$

Proof. Let $h_i = g_i y_i$. Without loss of generality, we can assume that $\mathbf{h} = (h_1, h_2, \dots, h_n)$ are linearly independent. If they are not, we can rewrite S as a linear combination of a subfamily of the h_i's that are linearly independent.

We shall bound the order of the Wronskian $W(h_1, h_2, \dots, h_n)$ and apply Theorem 3. We have:

$$y_i' = \frac{p_i}{q_i} y_i,$$
$$y_i'' = \frac{p_i' q_i - p_i q_i'}{q_i^2} y_i + \frac{p_i}{q_i} y_i' = \frac{p_i' q_i - p_i q_i' + p_i q_i}{q_i^2} y_i.$$

So by induction, we deduce that for $0 \le j < n$,

$$y_i^{(j)} = \frac{P_{i,j}}{q_i^j} y_i = \frac{q_i^{n-1-j} P_{i,j}}{q_i^{n-1}} y_i,$$

where $q_i^{n-1-j} P_{i,j}$ is a polynomial of degree at most $(n-1)d$. Then, by the Leibniz's formula, $h_i^{(j)} = \sum_{k=0}^j \binom{j}{k} g_i^{(j-k)} y_i^{(j)}$, and the Wronskian has the form

$$W(h_1, h_2, \dots, h_n) = \prod_{i=1}^n \frac{y_i}{q_i^{n-1}} \det M,$$

with M being a matrix whose entries are polynomials of degree at most nd. In particular, $\operatorname{ord}(\det M) \le \deg(\det M) \le n^2 d$. As $q_i(0) \neq 0$ for all i, we have:

$$\operatorname{ord}(W(\mathbf{h})) = \sum_{i=1}^n \operatorname{ord}(y_i) + \operatorname{ord}(\det M) \le \sum_{i=1}^n \operatorname{ord}(y_i) + n^2 d.$$

Finally, Theorem 3 implies the claimed bound. □

As a direct corollary of Theorem 5, we obtain upper bounds for the order of a sum of power series in $\mathbb{C}[[x]]$ in several different contexts.

Corollary 1. *Let $S(x) = \sum_{i=1}^n c_i g_i(x) y_i(x)$ be a non-zero sum, where $c_i \in \mathbb{C}$, and $g_i \in \mathbb{C}[x]$ are of degree at most d. Let $f_i \in \mathbb{C}[x]$ of degree at most d.*

1. *If $y_i = \exp(f_i)$, then $\operatorname{ord} S \le n^2(d-1) + n - 1$.*
2. *If $y_i = \varphi(f_i)$ with $\varphi \in \{\cosh, \sinh, \cos, \sin\}$, then $\operatorname{ord} S \le 4n^2(d-1) + 2n - 1$.*
3. *If $y_i = \left(\frac{p_i}{q_i}\right)^{\alpha_i}$, with $p_i, q_i \in \mathbb{C}[x]$ of degree at most d, $\alpha_i \in \mathbb{R}$ and $p_i(0), q_i(0) \neq 0$, then $\operatorname{ord} S \le 2n^2 d + n - 1$.*

Proof. For Part (1), $y_i = \exp(f_i)$, y_i admits a power series expansion and $\operatorname{ord} y_i = 0$ because $y_i(0) = \exp f_i(0) \neq 0$. Moreover, $y_i' - f_i' y_i = 0$, with $\deg f_i' \le d - 1$. By Theorem 5, $\operatorname{ord} S \le n^2(d-1) + n - 1$.

For Part (2), one can write $\cosh f = \frac{e^f + e^{-f}}{2}$, $\sinh f = \frac{e^f - e^{-f}}{2}$, $\cos f = \frac{e^{if} + e^{-if}}{2}$, $\sin f = \frac{e^{if} - e^{-if}}{2i}$. We can then apply Part (1) with $2n$ terms in the sum and obtain the claimed bound.

For Part (3), because both $p_i(0)$ and $q_i(0)$ are non-zero for all i, y_i admits a power series expansion in 0 and $\operatorname{ord} y_i = 0$. Moreover, it satisfies $y_i' - \alpha_i \frac{p_i' q_i - p_i q_i'}{p_i q_i} y_i = 0$. Again, the bound is obtained by using Theorem 5. □

A similar bound for $y_i = \exp f_i$ was already established in [21] (see Example 1). The proof also relies on Wronskians.

4 SUM OF SQUARE ROOTS OF INTEGERS GIVEN BY STRAIGHT-LINE PROGRAMS

As we mentioned in introduction, testing if an expression involving square roots is zero is an interesting problem and Blömer [6] developed a polynomial time algorithm solving $\mathrm{SSR}_{\mathrm{eq}}$. In $\mathrm{SSR}_{\mathrm{eq}}$, the integers in input are given in binary and in this case, the problem is *easy*. It is a natural extension of $\mathrm{SSR}_{\mathrm{eq}}$ to ask what happens for the complexity of this problem in an algebraic model of computation, that is if the integers in input are given by straight line programs. More precisely, we want to study Problem 5.

We would like to know if zero testing for this class of expressions is as easy as testing zero for straight line programs computing integers, namely EquSLP defined in [1]. In the problem EquSLP, given an input SLP P, we want to test if the integer n_P computed by P is zero. In [1], it is proven that EquSLP reduces to Polynomial Identity Testing (PIT), so it admits a randomized polynomial time algorithm. In the hope of designing a randomized polynomial time algorithm for $\mathrm{SSR}_{\mathrm{SLP}}$, we present in this section how one can reuse some of the ideas of Blömer for $\mathrm{SSR}_{\mathrm{eq}}$ in the context of Problem 5. We show that the problem $\mathrm{SSR}_{\mathrm{SLP}}$ can be *reduced* under the General Riemann Hypothesis (GRH) to a one dimensional case where all the square roots involved are on the same line over $\mathbb{Q}$. Actually, this special one dimensional case captures all the hardness of the whole problem. One can also find related results in [5, 7]. They give randomized algorithms to decide if expressions involving radicals of depth 1 is equal to 0. In [5], some algorithms are also valid under GRH and use comparable arguments about density of certain prime numbers that we also develop in this section. However, the expressions involved in these results are different; the expressions are not only sums of square roots but general arithmetic circuits involving square-roots of integers given in binary.

4.1 Reduction to the one-dimensional case

We now explain formally why it is enough to focus on the *one dimensional* (Problem 6) version of Problem 5 in order to design an efficient algorithm for $\mathrm{SSR}_{\mathrm{SLP}}$. We actually prove Theorem 11.

Theorem 11. *Under GRH, there exists a randomized polynomial time Turing reduction from Problem 5 to Problem 6.*

The starting point is the following result due to Kneser [15] recalled by Blömer ([6], corollary 2.6).

Lemma 12. *Let $a_1, a_2, \ldots, a_n$ be n positive integers. Reals $\sqrt{a_1}$, $\sqrt{a_2}, \ldots, \sqrt{a_n}$ are linearly dependent over $\mathbb{Q}$ if and only if there exist $1 \leq i < j \leq n$ such that $(\sqrt{a_i}, \sqrt{a_j})$ are linearly dependent over $\mathbb{Q}$ or equivalently*

$$\frac{\sqrt{a_i}}{\sqrt{a_j}} \in \mathbb{Q}. \tag{2}$$

Corollary 2. *Let $a_1, \ldots, a_n$ be positive integers and $(\delta_1, \ldots, \delta_n) \in \{-1, 1\}^n$. Let $(\sqrt{a_{i_1}}, \ldots, \sqrt{a_{i_\ell}})$ be a basis of $\mathrm{span}_{\mathbb{Q}}(\sqrt{a_1}, \ldots, \sqrt{a_i})$. Then for all $1 \leq i \leq n$, there exists a unique $1 \leq j \leq \ell$ such that $\sqrt{a_i} \in \mathbb{Q} \cdot \sqrt{a_{i_j}}$. And*

$$\sum_{i=1}^{n} \delta_i \sqrt{a_i} = 0 \iff \forall 1 \leq j \leq \ell, \sum_{i:\ \sqrt{a_i} \in \mathbb{Q}\sqrt{a_{i_j}}} \delta_i \sqrt{a_i} = 0. \tag{3}$$

Proof. Without loss of generality, we can assume $i_j = j$. Assuming existence, uniqueness is clear because if $\sqrt{a_i} \in \mathbb{Q} \cdot \sqrt{a_j}$ and $\sqrt{a_i} \in \mathbb{Q} \cdot \sqrt{a_{j'}}$, then $\sqrt{a_j}$ and $\sqrt{a_{j'}}$ are not linearly independent. Now, for an element of the basis existence is clear and for $\sqrt{a_i}$ not in the basis, $(\sqrt{a_1}, \ldots, \sqrt{a_\ell}, \sqrt{a_i})$ is linearly dependent. By Lemma 12, two elements are linearly dependent, and it can not be between two elements of the basis. So $\sqrt{a_i}$ is involved in this pair.

We partition $\{1, \ldots, n\} = I_1 \cup \cdots \cup I_\ell$, with $I_j = \{i |\ \sqrt{a_i} = q_{i,j}\sqrt{a_j}, q_{i,j} \in \mathbb{Q}\}$. Now, $\sum_{i=1}^{n} \delta_i \sqrt{a_i} = \sum_{j=1}^{\ell} \left(\sum_{i \in I_j} \delta_i q_{i,j}\right) \sqrt{a_j}$. As $(\sqrt{a_j})_{1 \leq j \leq \ell}$ form a basis, the previous sum is zero if and only if for all $1 \leq j \leq \ell$, $\sum_{i \in I_j} \delta_i q_{i,j} = 0$. By multiplying by $\sqrt{a_j}$, we obtain

$$\sum_{i=1}^{n} \delta_i \sqrt{a_i} = 0 \iff \forall 1 \leq j \leq \ell, \sum_{i \in I_j} \delta_i \sqrt{a_i} = 0.$$

□

The reduction for Theorem 11 then works in two steps and can be found in Algorithm 1. Given an instance of Problem 5, we first build the partition of the set of square roots in ℓ one-dimensional subsets, and then use the oracle for Problem 6 to test if each associated subsum is zero. To build the partition, Algorithm 1 works as follows: for each integer a_i, either we have already seen an integer a_j before such that $\sqrt{a_i}/\sqrt{a_j} \in \mathbb{Q}$ and we add a_i to the same one dimensional sum as a_j or we construct a new one for a_i. To complete the proof of Theorem 11, it only remains to show that one can perform the test of Equation (2) efficiently under GRH.

Input : $a_1, a_2, \ldots, a_n$ integers given by SLPs, signs $\delta_1, \delta_2, \ldots, \delta_n \in \{-1, 1\}$.
Output: Decide if $S = \sum_{i=1}^{n} \delta_i \sqrt{a_i} = 0$.
SubSums ← [ ] ;
for $1 \leq i \leq n$ **do**
  $k \leftarrow 0$; FoundSubSum ← false ;
  while $k <$ |SubSums| *and not* FoundSubSum **do**
    Pick an element b in SubSums[k] ;
    if $\sqrt{a_i}/\sqrt{b} \in \mathbb{Q}$ **then**
      Add a_i to SubSums[k] ; FoundSubSum ← true ;
    else
      k++;
    end
  end
  if not FoundSubSum **then** Add $\{a_i\}$ to SubSums ;
end
For each element of SubSums, test if the corresponding one dimensional sum is zero using oracle for Problem 6;

Algorithm 1: Algorithm for Problem 5

Lemma 13. *Let a, b be two positive integers. $\frac{\sqrt{a}}{\sqrt{b}} \in \mathbb{Q}$ iff $\sqrt{ab} \in \mathbb{N}$.*

Proof. $\sqrt{a}/\sqrt{b} \in \mathbb{Q}$ is equivalent to the statement that for any prime p, the p-adic valuation $v_p(a/b)$ of a/b is even, $v_p(a/b) = v_p(a) - v_p(b)$, or equivalently $v_p(a) + v_p(b) = v_p(ab)$ is even, *i.e.*$\sqrt{ab} \in \mathbb{N}$. □

Lemma 13 suggests that for testing Equation (2), we just have to check if $a_i a_j$ is a perfect square. Note that if both a_i and a_j can be computed by SLPs of size s, then $a_i a_j$ admits an SLP of size $2s+1$. In the next section we design a randomized polynomial time algorithm to perform this task under GRH.

4.2 Testing if an SLP computes a perfect square

We now demonstrate an algorithm for the following Problem 7.

Problem 7. *Given an SLP of size t computing a positive integer a, decide if a is a perfect square.*

Let a be a positive integer computed by an SLP of size t. By induction on $t \geq 0$, we have the bound $a \leq 2^{2^t}$.

Our algorithm is the following: sample at random a prime $p \leq 2^{q(t)}$, with q a polynomial to be determined later, compute $a \bmod p$ and test if $a \bmod p$ is a square in $\mathbb{F}_p$. All these computations can be done in polynomial time in t [2]. If a is actually a perfect square, then for all such primes p, $a \bmod p$ is a square in $\mathbb{F}_p$ and the answer of the algorithm is correct. Whereas if a is not a perfect square, Chebotarev's density theorem guarantees that the set of primes p for which the polynomial $X^2 - a$ splits in $\mathbb{F}_p$, *i.e.*, the set of primes p where a is a square in $\mathbb{F}_p$ has density $\frac{1}{2}$ [20]. To ensure that we can use small primes and keep a non negligible probability to have a correct answer, we need an effective version. This effective version of Chebotarev's density theorem requires GRH and can be found in [19] (Theorem 4).

Our application of the effective Chebotarev's density theorem leads us to the following key lemma. The statement directly follows from [19] (Theorem 4) for the splitting field of $X^2 - a$. This only makes sense when $\mathrm{disc}(X^2 - a) = 4a$ does not vanish in $\mathbb{F}_p$. This is the reason why we only consider primes p that do not divide $4a$.

Lemma 14. *Let a be a positive integer that is not a square. For $x \geq 2$, we define:*

$$d_a(x) := \frac{|\{p \text{ prime } \leq x, a \text{ is not a square mod } p \text{ and } p \nmid 4a\}|}{|\{p \text{ prime } \leq x\}|}.$$

There exists a constant C such that, under GRH, for all $x \geq 2$,

$$\left| d_a(x) - \frac{1}{2} \right| \leq C \frac{\log_2 x}{\sqrt{x}} \left(\log_2(4a) + 2 \log_2 x \right).$$

Now we can state the main lemma.

Lemma 15. *Let $a \leq 2^{2^t}$ be a positive integer that is not a perfect square. Then there exists an integer polynomial q such that for $x = 2^{q(t)}$, we have $d_a(x) \geq \frac{1}{4}$.*

Proof. From Lemma 14, the following inequality holds:

$$d_a(x) \geq \frac{1}{2} - C \frac{\log_2 x}{\sqrt{x}} (\log_2(4a) + 2 \log_2 x).$$

To conclude, we need to ensure that

$$C \frac{\log_2 x}{\sqrt{x}} (\log_2(4a) + 2 \log_2 x) \leq \frac{1}{4}, \text{ i.e.,}$$

$$\log_2(4a) \leq \frac{1}{4} \frac{\sqrt{x}}{C \log_2 x} - 2 \log_2 x.$$

With $a \leq 2^{2^t}$, and $x = 2^{q(t)}$, it is sufficient to have

$$2^t + 2 \leq \frac{1}{4} \frac{2^{\frac{q(t)}{2}}}{C q(t)} - 2q(t). \tag{4}$$

and one can see that $q(t) = O(t^2)$ satisfies Equation (4). □

If one chooses $q(t)$ as in Lemma 15, our randomized algorithm runs in polynomial time and has a one sided error for solving Problem 7. This completes the proof of Theorem 11.

4.3 About the One Dimensional Variant

In the previous section, we showed that it is enough to focus on Problem 6. Suppose $\mathrm{span}_{\mathbb{Q}}(\sqrt{a_1}, \sqrt{a_2}, \ldots, \sqrt{a_n}) = \mathbb{Q} \cdot \sqrt{a_1}$. Then, for all i, $\sqrt{a_i a_1} \in \mathbb{N}$. And $S = \sum_{i=1}^n \delta_i \sqrt{a_i} = 0 \iff S\sqrt{a_1} = \sum_{i=1}^n \delta_i \sqrt{a_i a_1} = 0$, with $S\sqrt{a_1} \in \mathbb{N}$. One approach to design an algorithm to test $S\sqrt{a_1} = 0$, is reducing it modulo a randomly selected prime number p. The problem with this approach, is that once we have reduced $a_i a_1$ modulo p, one can compute its two square roots in $\mathbb{F}_p$ but there is no way to decide which one of the two is the correct representation of $\sqrt{a_1 a_i}$ in $\mathbb{F}_p$. Determining the correct reduction of $S\sqrt{a_1}$ modulo p seems like a non trivial task. And we most likely need a different approach in order to tackle Problem 6.

5 AN APPLICATION TO SUMS OF LOGARITHMS

In order to motivate the interest of proving bounds for the order of sums of certain power series, we show that the approach of Kayal and Saha [14] that led to a non trivial statement for the Sum of Square Roots problem can also be used to establish non-trivial statements for other fundamental number theoretic problems. In particular in this section, we focus on the sums of logarithms that is a well-studied problem [3, 12] and is related to deep number theory conjectures.

Problem 8. *Given two lists $(a_1, a_2, \ldots, a_n)$, $(c_1, c_2, \ldots, c_n)$ of integers with $a_i > 0$, decide if*

$$\sum_{i=1}^n c_i \log a_i > 0.$$

Similarly as for the Sum of Square roots problem (Problem 1), the complexity in the bit-model of Problem 8 is an open question. A refinement of the *abc*-conjecture formulated by Baker [4] would imply Problem 8 to be in P. Interesting details about the link between the complexity of Problem 8 and open questions in number-theory can be found in [12]. All these conjectures essentially state the existence of a *gap*, namely that a non-zero sum of logarithms can not be *too close to zero*. These *gaps* or lower bounds are very similar to Problem 4 but in the case of logarithms. Our goal is to reuse the analogy between polynomials and integers in order to deduce a lower bound for a non trivial class of instances of Problem 8 via a lower bound on the order of a non-zero sum of logarithms of real polynomials.

Proposition 2. *Let $S(x) = \sum_{i=1}^n c_i \log(f_i(x)) \neq 0$, where $c_i \in \mathbb{R}$, $f_i \in \mathbb{R}[x]$ of degree at most d and $f_i(0) > 0$. Then $\mathrm{ord}(S) \leq nd$.*

Proof. First, if $f_i(0) > 0$, the power series $\log f_i(x)$ is well defined in a neighborhood of 0. So, S admits a valid power series expansion. Now, we have

$$S'(x) = \sum_{i=1}^{n} c_i \frac{f_i'(x)}{f_i(x)} = \frac{\sum_{i=1}^{n} c_i F_i(x)}{\prod_{i=1}^{n} f_i(x)},$$

with $F_i(x) = f_i'(x) \prod_{j\neq i} f_j(x)$, is a polynomial of degree $\leq (n-1)d + d - 1 = nd - 1$. As $f_i(0) \neq 0$, we have:

$$\operatorname{ord}(S') = \operatorname{ord}\left(\sum_{i=1}^{n} c_i F_i(x)\right) \leq \deg\left(\sum_{i=1}^{n} c_i F_i(x)\right) \leq nd - 1.$$

Finally,

$$\operatorname{ord}(S) \leq \operatorname{ord}(S') + 1 \leq nd.$$

□

And now, we can instantiate Proposition 2 over integers and obtain the following gap theorem for a restricted but non trivial class of the instances of Problem 8.

Theorem 6 (Sum of logarithms of *polynomial integers*). *Suppose $E = \sum_{i=1}^{n} c_i \log a_i$ is non-zero, where $c_i \in \mathbb{Z}$, and every a_i is a positive integer of the form $a_i = X^{d_i} + b_{1,i}X^{d_i-1} + \cdots + b_{d_i,i}$, where $d_i > 0$, X is a positive integer and $d_i, b_{j,i}$ are integers. Let $B = \max\left(\left\{\left|b_{j,i}\right|\right\}_{j,i}, 1\right)$, $d = \max_i d_i + 1$, and $C = \max_i |c_i|$. There exist two fixed integer polynomial $p_1(n,d), p_2(n,d)$ in n and d such that if $X > \max\left(C^2, (B+1)^{p_1(n,d)}\right)$, then E is lower bounded as $|E| \geq \frac{1}{X^{p_2(n,d)}}$.*

Proof. We choose any integer polynomials p_1, p_2 satisfying the following conditions and show that they satisfy the claimed bounds:

$$p_1(n,d) \geq 20dn\log(dn), \tag{5}$$
$$p_2(n,d) \geq 1 + dn(\log(dn) + 1). \tag{6}$$

One can write E as follows:

$$E = \underbrace{\sum_{i=1}^{n} c_i d_i \log X}_{=A} + \underbrace{\sum_{i=1}^{n} c_i \log\left(1 + \frac{b_{1,i}}{X} + \cdots + \frac{b_{d_i,i}}{X^{d_i}}\right)}_{=S}.$$

If $\mathbf{A \neq 0}$, as $\sum_{i=1}^{n} c_i d_i$ is a non-zero integer, we have

$$|A| \geq \log X.$$

So an upper bound for S of the form $|S| \leq \frac{1}{2}\log X$ is enough to prove that $|E| \geq \frac{1}{2}\log X$. And we have the bound

$$|S| \leq nC \max_{1\leq i\leq n} \log\left(1 + \frac{b_{1,i}}{X} + \cdots + \frac{b_{d_i,i}}{X^{d_i}}\right).$$

Now, as $\forall x \geq 0, \log(1+x) \leq x$, and $\frac{b_{1,i}}{X} + \cdots + \frac{b_{d_i,i}}{X^{d_i}} \leq \frac{B}{X-1}$, we have

$$|S| \leq nC\frac{B}{X-1}.$$

But, as $C \leq X^{\frac{1}{2}}$

$$|S| \leq nC\frac{B}{X-1} \leq \frac{nBX^{\frac{1}{2}}}{X-1} \leq \frac{2nB}{X^{\frac{1}{2}}} \leq \frac{2nB}{(B+1)^{\frac{1}{2}p_1(n,d)}},$$

because $X - 1 \geq \frac{X}{2}$ since $X \geq 2$. Then, to have $|S| \leq \frac{1}{2}\log X$, it is sufficient that:

$$p_1(n,d)\log(B+1)(B+1)^{\frac{1}{2}p_1(n,d)} - 4nB \geq 0. \tag{7}$$

One can easily check that Equation (7) holds using Equation (5) and thus, $|E| \geq \frac{1}{2}\log X \geq \frac{1}{X^{p_2(n,d)}}$.

If $\mathbf{A = 0}$, we show that $|E| = |S| \geq \frac{1}{X^{p_2(n,d)}}$. Let $y = \frac{1}{X}$, we have

$$S = \sum_{i=1}^{n} c_i \underbrace{\log\left(1 + b_{1,i}y + \cdots + b_{d_i,i}y^{d_i}\right)}_{=h_i(y)} = \sum_{j\geq 1} y^j \underbrace{\sum_{i=1}^{n} c_i h_{i,j}}_{S_j}$$

$$\text{with } h_i(y) = \sum_{j=1}^{\infty} h_{i,j}y^j = \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k}\left(b_{1,i}y + \cdots + b_{d_i,i}y^{d_i}\right)^k.$$

By applying Proposition 2, the minimum exponent ℓ such that $S_\ell \neq 0$ is such that $\ell \leq dn$. The idea of the proof is to show that for every $t \geq 1$,

$$\frac{|S_{\ell+t}|}{|S_\ell|} \leq \frac{1}{2^{t+1}}, \tag{8}$$

because in this case, we would have

$$|S| \geq ||S_\ell| - |S_{\ell+1}| - \ldots| \geq \left||S_\ell| - \frac{1}{2}|S_\ell|\right| = \frac{1}{2}|S_\ell|, \tag{9}$$

and one can obtain a lower bound for $|S|$ via a lower bound for $|S_\ell|$. But to satisfy Equation (8), one also needs an upper bound on $S_{\ell+t}$, for every t.

These two lower and upper bounds are both obtained as in the proof of Theorem 2 in [14]. The technical details can be found in Section 5.1. In the end, we show that conditions on p_1 and p_2 (Equations (5) and (6)) are sufficient in order to satisfy Equations (8) and (9) and then deduce that $|E| = |S| \geq \frac{1}{X^{p_2(n,d)}}$.

□

5.1 Bounds for the Proof of Theorem 6

We recall that we have

$$S = \sum_{i=1}^{n} c_i \underbrace{\log\left(1 + b_{1,i}y + \cdots + b_{d_i,i}y^{d_i}\right)}_{=h_i(y)} = \sum_{j\geq 1} y^j \underbrace{\sum_{i=1}^{n} c_i h_{i,j}}_{S_j}$$

$$\text{with } h_i(y) = \sum_{j=1}^{\infty} h_{i,j}y^j = \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k}\left(b_{1,i}y + \cdots + b_{d_i,i}y^{d_i}\right)^k.$$

The goal is to show that $p_1(n,d)$ and $p_2(n,d)$ satisfying Equations (5) and (6) give both an upper bound and a lower bound on S_j that allows us to satisfy Equation (8).

An upper bound on S_j:

For any j, $h_{i,j}$ is contributed by the term of order j in the sum

$\sum \frac{(-1)^{k+1}}{k} \left(b_{1,i}y + \cdots + b_{d_i,i}y^{d_i}\right)^k$ for k in range $[1, j]$. Then

$$h_{i,j} = \sum_{k=1}^{j} \frac{(-1)^{k+1}}{k} v_{k,i,j}, \text{ with}$$

$$v_{k,i,j} = \sum_{\substack{k_1+2k_2+\cdots+d_ik_{d_i}=j \\ k_1+k_2+\cdots+k_{d_i}=k}} \binom{k}{k_1, k_2, \ldots, k_{d_i}} b_{1,i}^{k_1} \cdots b_{d_i,i}^{k_{d_i}}.$$

where $k_1, k_2, \ldots, k_{d_i}$ are non-negative integers. Notice that for $k < \frac{j}{d_i}$, $v_{k,i,j} = 0$ as the sum is empty. Then

$$\begin{aligned} \left|v_{k,i,j}\right| &\leq \sum_{k_1+k_2+\cdots+k_{d_i}=k} \binom{k}{k_1, k_2, \ldots, k_{d_i}} \left|b_{1,i}\right|^{k_1} \cdots \left|b_{d_i,i}\right|^{k_{d_i}} \\ &\leq (Bd_i)^k \leq (Bd)^k. \qquad \text{(Multinomial theorem)} \end{aligned}$$

Since $\left|\frac{(-1)^{k+1}}{k}\right| \leq 1$,

$$\left|h_{i,j}\right| \leq \sum_{k=0}^{j} (Bd)^k \leq (Bd)^{j+1}.$$

Hence, let $S = \sum_{j\geq 1} S_j$, with $S_j = y^j \sum_{i=1}^n c_i h_{i,j}$ satisfies for all $j \geq 1$

$$\left|S_j\right| \leq y^j nC(Bd)^{j+1}.$$

A lower bound on S_ℓ:
Now we prove a lower bound for $|S_\ell| = y^\ell \left|\sum_{i=1}^n c_i h_{i,\ell}\right| \neq 0$. We have

$$\sum_{i=1}^n c_i h_{i,\ell} = \sum_{i=1}^n c_i \sum_{k=1}^{\ell} \frac{(-1)^{k+1}}{k} v_{k,i,\ell} = \sum_{k=1}^{\ell} \frac{(-1)^{k+1}}{k} \underbrace{\left(\sum_{i=1}^n c_i v_{k,i,\ell}\right)}_{\in\mathbb{Z}}.$$

So $\ell!\left(\sum_{i=1}^n c_i h_{i,\ell}\right)$ is an integer. Then, if $\sum_{i=1}^n c_i h_{i,\ell} \neq 0$,

$$\ell! \left|\sum_{i=1}^n c_i h_{i,\ell}\right| \geq 1.$$

And finally, we obtain

$$|S_\ell| \geq \frac{y^\ell}{\ell!}.$$

With the obtained upper and lower bound, we can now deduce a requirement that ensures Equation (8) to be satisfied. Actually, it is sufficient that for every $t \geq 1$,

$$ny^t C(Bd)^{\ell+t+1}\ell! \leq \frac{1}{2^{t+1}}, \text{ i.e.} \tag{10}$$

$$X^t \geq 2^{t+1} nC(Bd)^{\ell+t+1}\ell!. \tag{11}$$

Recall that $C \leq X^{1/2}$ and $\ell \leq dn$, so it suffices that

$$X^{t-\frac{1}{2}} \geq 2^{t+1} n(Bd)^{nd+t+1}(nd)!.$$

By applying log, it is sufficient that for all $t \geq 1$,

$$\begin{aligned} (t-\frac{1}{2})p_1(n,d)\log(B+1) \geq &(t+1)\log(2) + \log(n) \\ &+ (nd+t+1)\log(Bd) + nd\log(nd). \end{aligned}$$

Therefore, one can show that $p_1(n,d) \geq 20dn\log(dn)$ is sufficient (this bound is not optimized at all). And in this case, by Equation (9), we have

$$|S| \geq \frac{1}{2}|S_\ell| \geq \frac{1}{2\ell!X^\ell} \geq \frac{1}{2^{\ell\log\ell+1}X^\ell} \geq \frac{1}{Xp_2(n,d)},$$

with $p_2(n,d) \geq dn(\log(dn)+1)+1$.

6 CONCLUSION AND OPEN QUESTIONS

In Theorem 5, we greatly generalized the ideas developed in [14]. This leads to the fact that the results in [14] can be generalized to various other families of power series, as evident in Corollary 1. The Wronskian approach of [14] was also proven to be tight, up to a polynomial blowup. Our work also made significant progress in the straight line variant of the classical SSR equality problem. We also extended the results of [14] for sign testing of the sum of square roots of polynomial integers to a linear combination of logarithms of polynomial integers, solving a special case of Problem 2 proposed in [12]. There are several directions for future research:

(1) Part (2) in Corollary 1 applies to some special cases of solutions of 2nd order differential equations, like $\cos f$ where f is a polynomial. It would be intriguing to see if this applies to generic solutions of higher order equations.
(2) Can we generalize Theorem 1 by bounding the order of sums of arbitrary algebraic power series? Square roots of polynomials are examples of algebraic functions. However, finding a satisfying way to bound the order of the Wronskian determinant of a family of algebraic power series is challenging. The best upper bound we could find is about $r^{\text{poly}(n)}d$ where (r,d) is a bound on the bi-degree of the polynomial equations satisfied by the algebraic power series.
(3) We saw that both the sign testing of the sum of square roots and logarithms are specific examples of PosSLP. In order to advance in understanding the complexity of PosSLP, it is important to consider other special cases. For instance, the following are additional special cases of PosSLP that are worth exploring.
   (a) Given positive integers a, b, c, n in binary, determine the sign of $a^n + b^n - c^n$. To our knowledge, even this very special case of PosSLP remains open.
   (b) Given an integer trinomial $f(x) := c_1 + c_2x_2^a + c_3x^{a_3} \in \mathbb{Z}[x]$ and a rational $\frac{p}{q}$, determine the sign of $f\left(\frac{p}{q}\right)$. This problem was posed in [16]. Significant progress was made on it in [9] but the general form of the problem remains open.

ACKNOWLEDGMENTS

Louis Gaillard expresses gratitude to Peter Bürgisser for hosting him during an internship at TU Berlin in the summer of 2022, where this research work was conducted. Gorav Jindal was a member of Graduiertenkolleg "Facets of Complexity/Facetten der Komplexität" (GRK 2434) and Institut für Mathematik, Technische Universität Berlin, where most of the work was completed.

REFERENCES

[1] Eric Allender, Peter Buergisser, Johan Kjeldgaard-Pedersen, and Peter Bro Miltersen. 2009. On the Complexity of Numerical Analysis. *SIAM J. Comput.* 38, 5 (2009), 1987–2006. https://doi.org/10.1137/070697926 arXiv:https://doi.org/10.1137/070697926

[2] Eric Bach and Jeffrey Shallit. 1996. *Algorithmic Number Theory.* MIT Press, Cambridge, MA, USA.

[3] A. Baker. 1998. *Logarithmic forms and the abc- conjecture.* De Gruyter, Berlin, New York, 37–44.

[4] A. Baker and G. Wüstholz. 1993. Logarithmic forms and group varieties. *Journal für die reine und angewandte Mathematik* 442 (1993), 19–62. http://eudml.org/doc/153550

[5] Nikhil Balaji, Klara Nosan, Mahsa Shirmohammadi, and James Worrell. 2022. Identity Testing for Radical Expressions. In *Proceedings of the 37th Annual ACM/IEEE Symposium on Logic in Computer Science* (Haifa, Israel) *(LICS '22)*. Association for Computing Machinery, New York, NY, USA, Article 8, 11 pages. https://doi.org/10.1145/3531130.3533331

[6] Johannes Blömer. 1991. Computing Sums of Radicals in Polynomial Time. In *32nd Annual Symposium on Foundations of Computer Science, 1-4 October 1991.* IEEE Computer Society, San Juan, Puerto Rico, 670–677. https://doi.org/10.1109/SFCS.1991.185434

[7] Johannes Blömer. 1998. A Probabilistic Zero-Test for Expressions Involving Roots of Rational Numbers. In *Algorithms — ESA' 98*, Gianfranco Bilardi, Giuseppe F. Italiano, Andrea Pietracaprina, and Geppino Pucci (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 151–162.

[8] Lenore Blum, Felipe Cucker, Michael Shub, and Steve Smale. 1997. *Complexity and Real Computation.* Springer-Verlag, Berlin, Heidelberg.

[9] Eric Boniface, Wei Deng, and J. Maurice Rojas. 2022. Trinomials and Deterministic Complexity Limits for Real Solving. arXiv:2202.06115

[10] Alin Bostan and Philippe Dumas. 2010. Wronskians and linear independence. *The American Mathematical Monthly* 117, 8 (2010), 722–727.

[11] Richard P Brent. 1976. Fast multiple-precision evaluation of elementary functions. *Journal of the ACM (JACM)* 23, 2 (1976), 242–251.

[12] Kousha Etessami, Alistair Stewart, and Mihalis Yannakakis. 2014. A Note on the Complexity of Comparing Succinctly Represented Integers, with an Application to Maximum Probability Parsing. *ACM Trans. Comput. Theory* 6, 2 (2014), 9:1–9:23. https://doi.org/10.1145/2601327

[13] M. R. Garey, R. L. Graham, and D. S. Johnson. 1976. Some NP-Complete Geometric Problems. In *Proceedings of the Eighth Annual ACM Symposium on Theory of Computing* (Hershey, Pennsylvania, USA) *(STOC '76)*. Association for Computing Machinery, New York, NY, USA, 10–22. https://doi.org/10.1145/800113.803626

[14] Neeraj Kayal and Chandan Saha. 2012. On the Sum of Square Roots of Polynomials and Related Problems. *ACM Trans. Comput. Theory* 4, 4, Article 9 (nov 2012), 15 pages. https://doi.org/10.1145/2382559.2382560

[15] Martin Kneser. 1975. Lineare Abhängigkeit von Wurzeln. *Acta Arithmetica* 26, 3 (1975), 307–308. http://eudml.org/doc/205320

[16] Pascal Koiran. 2019. Root separation for trinomials. *Journal of Symbolic Computation* 95 (2019), 151–161. https://doi.org/10.1016/j.jsc.2019.02.004

[17] Gregorio Malajovich. 2001. *An Eective Version of Kronecker's Theorem on Simultaneous Diophantine Approximation.* Technical Report. Technical report, City University of Hong Kong.

[18] Jianbo Qian and Cao An Wang. 2006. How much precision is needed to compare two sums of square roots of integers? *Inform. Process. Lett.* 100, 5 (2006), 194–198. https://doi.org/10.1016/j.ipl.2006.05.002

[19] Jean-Pierre Serre. 1981. Quelques applications du théoreme de densité de Chebotarev. *Publications Mathématiques de l'IHÉS* 54 (1981), 123–201.

[20] Peter Stevenhagen and Hendrik Willem Lenstra. 1996. Chebotarëv and his density theorem. *The Mathematical Intelligencer* 18, 2 (1996), 26–37.

[21] M Voorhoeve and A.J Van Der Poorten. 1975. Wronskian determinants and the zeros of certain functions. *Indagationes Mathematicae (Proceedings)* 78, 5 (1975), 417–424. https://doi.org/10.1016/1385-7258(75)90050-5