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

Louis Gaillard[1] Gorav Jindal[2]

[1]ENS de Lyon, Lyon, France

[2]Max Planck Institute for Software Systems, Saarbrücken, Germany

ISSAC 2023, Tromsø, July 26

Sum of Square Roots Problem

Problem (SSR)

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

Sum of Square Roots Problem

Problem (SSR)

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

- Introduced by Garey, Graham & Johnson in 1976. Conjectured to be in P.
- Difficult open problem: number of bits of precision needed to represent S?

Sum of Square Roots Problem

Problem (SSR)

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

- Introduced by Garey, Graham & Johnson in 1976. Conjectured to be in P.
- Difficult open problem: number of bits of precision needed to represent S?

Lemma (Gap property [Tiwari 1992])

If $a_i < 2^B$ *for all* i*, and* $S \neq 0$*, then* $|S| > 2^{-2^n \mathrm{poly}(n,B)}$.

Conjecture

If $S \neq 0$, then $|S| > 2^{-\mathrm{poly}(n,B)}$.

Sum of Square Roots Problem

Problem (SSR)

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

- Introduced by Garey, Graham & Johnson in 1976. Conjectured to be in P.
- Difficult open problem: number of bits of precision needed to represent S?

Lemma (Gap property [Tiwari 1992])

If $a_i < 2^B$ *for all* i, *and* $S \neq 0$, *then* $|S| > 2^{-2^n \mathrm{poly}(n,B)}$.

Conjecture

If $S \neq 0$, then $|S| > 2^{-\mathrm{poly}(n,B)}$.

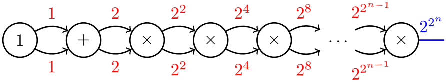
- Applications: Euclidean Traveling Salesman Problem $\in$ NP with access to an oracle for SSR.

Positivity testing for straight line programs

Definition (Straight line program (SLP))

A sequence of integers $(a_0, a_1, \ldots, a_\ell)$ is a SLP if $a_0 = 1$ and for all $1 \le i \le \ell$, $a_i = a_j \circ_i a_k$, where $\circ_i \in \{+, -, *\}$ and $j, k < i$.

$$a_1 = a_0 + a_0,$$
$$a_i = a_{i-1} \times a_{i-1}, \text{ for } 2 \le i \le n+1$$

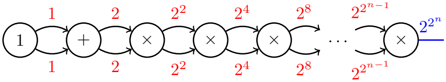


Positivity testing for straight line programs

Definition (Straight line program (SLP))

A sequence of integers $(a_0, a_1, \ldots, a_\ell)$ is a SLP if $a_0 = 1$ and for all $1 \leq i \leq \ell$, $a_i = a_j \circ_i a_k$, where $\circ_i \in \{+, -, *\}$ and $j, k < i$.

$$a_1 = a_0 + a_0,$$
$$a_i = a_{i-1} \times a_{i-1}, \text{ for } 2 \leq i \leq n+1$$



Problem (PosSLP)

Allender, Bürgisser, Kjeldgaard-Pedersen, Miltersen 2009

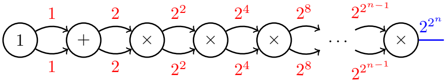
Given a SLP that computes an integer N, decide whether $N > 0$.

Positivity testing for straight line programs

Definition (Straight line program (SLP))

A sequence of integers $(a_0, a_1, \ldots, a_\ell)$ is a SLP if $a_0 = 1$ and for all $1 \le i \le \ell$, $a_i = a_j \circ_i a_k$, where $\circ_i \in \{+, -, *\}$ and $j, k < i$.

$$a_1 = a_0 + a_0,$$
$$a_i = a_{i-1} \times a_{i-1}, \text{ for } 2 \le i \le n+1$$



Problem (PosSLP)

Allender, Bürgisser, Kjeldgaard-Pedersen, Miltersen 2009

Given a SLP *that computes an integer N, decide whether $N > 0$.*

- Complexity of PosSLP characterizes the hardness of deciding the sign of expressions involving real numbers
- PosSLP $\in$ CH (Counting Hierarchy)
- SSR $\le$ PosSLP

$\rightarrow$ SSR $\in$ CH: Best known complexity upper-bound / Far from SSR $\in$ P

Part 1: The polynomial analogue

$$N = 9876 = 9 \cdot 10^3 + 8 \cdot 10^2 + 7 \cdot 10 + 6$$

$$P(x) = 9x^3 + 8x^2 + 7x + 6$$

Sum of square roots of polynomials

Variant of SSR with polynomials proposed by Kayal and Saha [KS12]

Sum of square roots of polynomials

Variant of SSR with polynomials proposed by Kayal and Saha [KS12]

$$\boxed{S = \sum_{i=1}^{n} \delta_i \sqrt{a_i}} \quad \text{becomes} \quad \boxed{S(x) = \sum_{i=1}^{n} c_i g_i(x) \sqrt{f_i(x)}}$$

$k = \mathbb{Q}, \mathbb{C}, \ldots$

with $c_i \in k$, $f_i, g_i \in k[x]$ of degree $\leq d$ and $f_i(0) = 1$.

Sum of square roots of polynomials

Variant of SSR with polynomials proposed by Kayal and Saha [KS12]

$$\boxed{S = \sum_{i=1}^{n} \delta_i \sqrt{a_i}} \quad \text{becomes} \quad \boxed{S(x) = \sum_{i=1}^{n} c_i g_i(x) \sqrt{f_i(x)}}$$

$k = \mathbb{Q}, \mathbb{C}, \ldots$

with $c_i \in k$, $f_i, g_i \in k[x]$ of degree $\leq d$ and $f_i(0) = 1$.

$\mathrm{ord}(S) := \sup\{t \mid x^t \mid S(x)\}$

Theorem ([KS12])

$S(x) \neq 0 \implies \mathrm{ord}(S) \leq dn^2 + n - 1.$

Main argument: study of the order of the Wronskian determinant of $(g_i\sqrt{f_i})_i$.

Sum of square roots of polynomials

Variant of SSR with polynomials proposed by Kayal and Saha [KS12]

$$\boxed{S = \sum_{i=1}^{n} \delta_i \sqrt{a_i}} \quad \text{becomes} \quad \boxed{S(x) = \sum_{i=1}^{n} c_i g_i(x) \sqrt{f_i(x)}}$$

$k = \mathbb{Q}, \mathbb{C}, \ldots$

with $c_i \in k$, $f_i, g_i \in k[x]$ of degree $\leq d$ and $f_i(0) = 1$.

$\mathrm{ord}(S) := \sup\{t \mid x^t \mid S(x)\}$

Theorem ([KS12])

$S(x) \neq 0 \implies \mathrm{ord}(S) \leq dn^2 + n - 1.$

Main argument: study of the order of the Wronskian determinant of $(g_i\sqrt{f_i})_i$.

They deduced that SSR is *easy* for a nontrivial class of instances called *polynomial integers*: suppose $S = \sum_{i=1}^{n} \delta_i \sqrt{a_i} \neq 0$ ($\delta_i \in \{-1, 1\}$), with $a_i = X^{d_i} + b_{1,i}X^{d_i - 1} + \cdots + b_{d_i,i}$ for $d_i > 0$, $X > 0$ and $b_{j,i}$ integers.

If $|b_{j,i}| \ll X$ then it is *easy* to decide the sign of S.

Sum of square roots of polynomials

Variant of SSR with polynomials proposed by Kayal and Saha [KS12]

$$\boxed{S = \sum_{i=1}^{n} \delta_i \sqrt{a_i}} \quad \text{becomes} \quad \boxed{S(x) = \sum_{i=1}^{n} c_i g_i(x) \sqrt{f_i(x)}}$$

$k = \mathbb{Q}, \mathbb{C}, \dots$

with $c_i \in k$, $f_i, g_i \in k[x]$ of degree $\leq d$ and $f_i(0) = 1$.

$\mathrm{ord}(S) := \sup\{t \mid x^t \mid S(x)\}$

Theorem ([KS12])

$S(x) \neq 0 \implies \mathrm{ord}(S) \leq dn^2 + n - 1.$

Main argument: study of the order of the Wronskian determinant of $(g_i\sqrt{f_i})_i$.

They deduced that SSR is *easy* for a nontrivial class of instances called *polynomial integers*: suppose $S = \sum_{i=1}^{n} \delta_i \sqrt{a_i} \neq 0$ ($\delta_i \in \{-1, 1\}$), with $a_i = X^{d_i} + b_{1,i} X^{d_i - 1} + \cdots + b_{d_i,i}$ for $d_i > 0$, $X > 0$ and $b_{j,i}$ integers.

If $|b_{j,i}| \ll X$ then it is *easy* to decide the sign of S.

Goal

Extend this to other special families of power series (y_i). Bound $\mathrm{ord}(S)$ for $S(x) = \sum_i c_i g_i(x) y_i(x)$.

Order of the Wronskian

Let $\mathcal{F}$ be a n-dimensional linear subspace of $k[[x]]$ with basis $\mathbf{f} := (f_1, \ldots, f_n)$. Define

$$\mathcal{O}(\mathcal{F}) := \sup\{\mathrm{ord}(f) \,|\, f \in \mathcal{F} \setminus \{0\}\} .$$

Order of the Wronskian

Let $\mathcal{F}$ be a n-dimensional linear subspace of $k[[x]]$ with basis $\mathbf{f} := (f_1, \ldots, f_n)$. Define

$$\mathcal{O}(\mathcal{F}) := \sup\{\mathrm{ord}(f) \,|\, f \in \mathcal{F} \setminus \{0\}\}.$$

Given $\mathcal{F}$, how to bound $\mathcal{O}(\mathcal{F})$?

Order of the Wronskian

Let $\mathcal{F}$ be a n-dimensional linear subspace of $k[[x]]$ with basis $\mathbf{f} := (f_1, \ldots, f_n)$. Define

$$\mathcal{O}(\mathcal{F}) := \sup\{\mathrm{ord}(f) \,|\, f \in \mathcal{F} \setminus \{0\}\}\,.$$

Given $\mathcal{F}$, how to bound $\mathcal{O}(\mathcal{F})$?

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

Fact: $\mathrm{ord}(W(\mathbf{f}))$ does not depend on the choice of the basis $\mathbf{f}$. We can define

$$W_{\mathrm{ord}}(\mathcal{F}) := \mathrm{ord}(W(\mathbf{f})).$$

Order of the Wronskian

Let $\mathcal{F}$ be a n-dimensional linear subspace of $k[[x]]$ with basis $\mathbf{f} := (f_1, \dots, f_n)$. Define

$$\mathcal{O}(\mathcal{F}) := \sup\{\mathrm{ord}(f) \,|\, f \in \mathcal{F} \setminus \{0\}\}.$$

Given $\mathcal{F}$, how to bound $\mathcal{O}(\mathcal{F})$?

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

Fact: $\mathrm{ord}(W(\mathbf{f}))$ does not depend on the choice of the basis $\mathbf{f}$. We can define

$$W_{\mathrm{ord}}(\mathcal{F}) := \mathrm{ord}(W(\mathbf{f})).$$

Theorem

$\mathcal{O}(\mathcal{F})$ and $W_{\mathrm{ord}}(\mathcal{F})$ are equivalent up to a polynomial factor.

Order of the Wronskian

Let $\mathcal{F}$ be a n-dimensional linear subspace of $k[[x]]$ with basis $\mathbf{f} := (f_1, \ldots, f_n)$. Define

$$\mathcal{O}(\mathcal{F}) := \sup\{\mathrm{ord}(f) \,|\, f \in \mathcal{F} \setminus \{0\}\}\,.$$

Given $\mathcal{F}$, how to bound $\mathcal{O}(\mathcal{F})$?

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

Fact: $\mathrm{ord}(W(\mathbf{f}))$ does not depend on the choice of the basis $\mathbf{f}$. We can define

$$W_{\mathrm{ord}}(\mathcal{F}) := \mathrm{ord}(W(\mathbf{f})).$$

Theorem

$\mathcal{O}(\mathcal{F})$ and $W_{\mathrm{ord}}(\mathcal{F})$ are equivalent up to a polynomial factor.

$$\mathcal{O}(\mathcal{F}) \leq W_{\mathrm{ord}}(\mathcal{F}) + n - 1$$ Voorhoeve & and Van Der Poorten, 1975

$$W_{\mathrm{ord}}(\mathcal{F}) \leq n \cdot \mathcal{O}(\mathcal{F}) - n(n-1)$$ Our result

Both bounds are tight. Ex: $\mathcal{F} = \mathrm{span}(1, x, \ldots, x^{n-1})$.

Bound for solutions of differential equations of order 1

Bound for solutions of differential equations of order 1

Theorem

Let $S(x) = \sum_{i=1}^{n} c_i g_i(x) y_i(x)$*, with* $y_i' - \frac{p_i}{q_i} y_i = 0$*, for* $c_i \in k, g_i, p_i, q_i \in k[x]$ *of degree* $\leq d$*, with* $q_i(0) \neq 0$*. If* $S \neq 0$ *then* $\operatorname{ord}(S) \leq \sum_{i=1}^{n} \operatorname{ord} y_i + n^2 d + n - 1$*.*

Proof:

Bound for solutions of differential equations of order 1

Theorem

Let $S(x) = \sum_{i=1}^{n} c_i g_i(x) y_i(x)$, with $y_i' - \frac{p_i}{q_i} y_i = 0$, for $c_i \in k, g_i, p_i, q_i \in k[x]$ of degree $\leq d$, with $q_i(0) \neq 0$. If $S \neq 0$ then $\operatorname{ord}(S) \leq \sum_{i=1}^{n} \operatorname{ord} y_i + n^2 d + n - 1$.

Proof: Let $f_i := g_i y_i$. We have

$$f_i^{(j)} = \sum_{k=0}^{j} \binom{j}{k} g_i^{(j-k)} y_i^{(k)}$$

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

with $P_{i,k} \in k[x]$ of degree $\leq kd$ (by induction).

Bound for solutions of differential equations of order 1

Theorem

Let $S(x) = \sum_{i=1}^n c_i g_i(x) y_i(x)$*, with* $y_i' - \frac{p_i}{q_i} y_i = 0$*, for* $c_i \in k, g_i, p_i, q_i \in k[x]$ *of degree* $\leq d$*, with* $q_i(0) \neq 0$*. If* $S \neq 0$ *then* $\operatorname{ord}(S) \leq \sum_{i=1}^n \operatorname{ord} y_i + n^2 d + n - 1$*.*

Proof: Let $f_i := g_i y_i$. We have

$$f_i^{(j)} = \sum_{k=0}^{j} \binom{j}{k} g_i^{(j-k)} y_i^{(k)}$$

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

with $P_{i,k} \in k[x]$ of degree $\leq kd$ (by induction).

$$W(\mathbf{f}) = \prod_{i=1}^{n} \frac{y_i}{q_i^{n-1}} \det D$$

where D is matrix with polynomial entries of degree at most nd.

Bound for solutions of differential equations of order 1

Theorem

Let $S(x) = \sum_{i=1}^{n} c_i g_i(x) y_i(x)$, *with* $y_i' - \frac{p_i}{q_i} y_i = 0$, *for* $c_i \in k, g_i, p_i, q_i \in k[x]$ *of degree* $\leq d$, *with* $q_i(0) \neq 0$. *If* $S \neq 0$ *then* $\operatorname{ord}(S) \leq \sum_{i=1}^{n} \operatorname{ord} y_i + n^2 d + n - 1$.

Proof: Let $f_i := g_i y_i$. We have

$$f_i^{(j)} = \sum_{k=0}^{j} \binom{j}{k} g_i^{(j-k)} y_i^{(k)}$$

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

with $P_{i,k} \in k[x]$ of degree $\leq kd$ (by induction).

$$W(\mathbf{f}) = \prod_{i=1}^{n} \frac{y_i}{q_i^{n-1}} \det D$$

where D is matrix with polynomial entries of degree at most nd.

$$\operatorname{ord} W(\mathbf{f}) = \sum_i \operatorname{ord} y_i + \underbrace{\operatorname{ord}(\det D)}_{\leq \deg(\det D) \leq n^2 d}$$

$$\begin{aligned} \operatorname{ord}(S) &\leq \operatorname{ord} W(\mathbf{f}) + n - 1 \\ &\leq \sum_{i=1}^{n} \operatorname{ord}(y_i) + n^2 d + n - 1 \end{aligned}$$

Applications

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

Applications

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

Theorem

Let $S(x) = \sum_{i=1}^{n} c_i g_i(x) y_i(x) \neq 0$ *for* $c_i \in k$, $g_i, p_i, q_i \in k[x]$ *of degree* $\leq d$ *and* $y_i = \exp\left(\frac{p_i}{q_i}\right)$ *with* $q_i(0) \neq 0$ *or* $y_i = \left(\frac{p_i}{q_i}\right)^{\alpha_i}$ *with* $p_i(0), q_i(0) \neq 0$ *and* $\alpha_i \in k$. *We have*

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

Applications

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

Theorem

Let $S(x) = \sum_{i=1}^{n} c_i g_i(x) y_i(x) \neq 0$ *for* $c_i \in k$, $g_i, p_i, q_i \in k[x]$ *of degree* $\leq d$ *and* $y_i = \exp\left(\frac{p_i}{q_i}\right)$ *with* $q_i(0) \neq 0$ *or* $y_i = \left(\frac{p_i}{q_i}\right)^{\alpha_i}$ *with* $p_i(0), q_i(0) \neq 0$ *and* $\alpha_i \in k$. *We have*

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

Proof:

- If $y_i = \exp\left(\frac{p_i}{q_i}\right)$, then $y_i' - \frac{p_i' q_i - p_i q_i'}{q_i^2} y_i = 0$.
- If $y_i = \left(\frac{p_i}{q_i}\right)^{\alpha_i}$, then $y_i' - \alpha_i \dfrac{p_i' q_i - p_i q_i'}{p_i q_i} y_i = 0$.

Application to sums of logarithms

Application to sums of logarithms

Problem (Sum of Logs)

Given integers $(a_1, \ldots, a_n)$ *and* $(b_1, \ldots, b_n)$ *with* $a_i > 0$*, decide whether* $\sum_{i=1}^{n} b_i \log a_i > 0$*.*

- Analogue to SSR but with log.
- Complexity of this problem connected to a refinement of the *abc*-conjecture formulated by Baker.
- Reduces to PosSLP.

Application to sums of logarithms

Problem (Sum of Logs)

Given integers $(a_1, \ldots, a_n)$ *and* $(b_1, \ldots, b_n)$ *with* $a_i > 0$, *decide whether* $\sum_{i=1}^{n} b_i \log a_i > 0$.

- Analogue to SSR but with log.
- Complexity of this problem connected to a refinement of the *abc*-conjecture formulated by Baker.
- Reduces to PosSLP.

Theorem

Let $S(x) = \sum_{i=1}^{n} c_i \log(f_i(x)) \neq 0$, *with* $c_i \in k$ *and* $f_i \in k[x]$ *of degree* $\leq d$ *such that* $f_i(0) = 1$. *Then* $\operatorname{ord} S \leq nd$.

- With the same techniques as in [KS12], we deduce that Sum of Logs is *easy* for a restrictive but nontrivial class of instances.

Part 2: Back to integers

Testing zero for sums of square roots

Problem (Testing Equality)

Given n *positive integers* $(a_1, \ldots, a_n)$ *and* $(\delta_1, \ldots, \delta_n) \in \{-1, 1\}^n$, *decide whether* $S = \sum_{i=1}^{n} \delta_i \sqrt{a_i} = 0$.

Testing zero for sums of square roots

Problem (Testing Equality)

Given n positive integers $(a_1, \ldots, a_n)$ *and* $(\delta_1, \ldots, \delta_n) \in \{-1, 1\}^n$*, decide whether* $S = \sum_{i=1}^{n} \delta_i \sqrt{a_i} = 0$*.*

- a_i's given in binary $\rightarrow$ Blömer gave a polynomial-time algorithm

Testing zero for sums of square roots

Problem (Testing Equality)

Given n positive integers $(a_1, \ldots, a_n)$ *and* $(\delta_1, \ldots, \delta_n) \in \{-1, 1\}^n$*, decide whether* $S = \sum_{i=1}^{n} \delta_i \sqrt{a_i} = 0$.

- a_i's given in binary $\to$ Blömer gave a polynomial-time algorithm
- a_i's given by SLPs $\to$ $\mathrm{SSR}_{\mathrm{SLP}}$

Testing zero for sums of square roots

Problem (Testing Equality)

Given n positive integers $(a_1, \ldots, a_n)$ *and* $(\delta_1, \ldots, \delta_n) \in \{-1, 1\}^n$*, decide whether* $S = \sum_{i=1}^{n} \delta_i \sqrt{a_i} = 0$.

- a_i's given in binary $\rightarrow$ Blömer gave a polynomial-time algorithm
- a_i's given by SLPs $\rightarrow$ $\mathrm{SSR}_{\mathrm{SLP}}$
- a_i's given by SLPs and $\dim\left(\mathrm{span}_{\mathbb{Q}}(\sqrt{a_1}, \ldots, \sqrt{a_n})\right) = 1 \rightarrow$ 1-dim $\mathrm{SSR}_{\mathrm{SLP}}$

Testing zero for sums of square roots

Problem (Testing Equality)

Given n positive integers $(a_1, \dots, a_n)$ and $(\delta_1, \dots, \delta_n) \in \{-1, 1\}^n$, decide whether $S = \sum_{i=1}^{n} \delta_i \sqrt{a_i} = 0$.

- a_i's given in binary $\rightarrow$ Blömer gave a polynomial-time algorithm
- a_i's given by SLPs $\rightarrow$ $\mathrm{SSR}_{\mathrm{SLP}}$
- a_i's given by SLPs and $\dim\left(\mathrm{span}_{\mathbb{Q}}(\sqrt{a_1}, \dots, \sqrt{a_n})\right) = 1 \rightarrow$ 1-dim $\mathrm{SSR}_{\mathrm{SLP}}$
- Goals:
  - Compare $\mathrm{SSR}_{\mathrm{SLP}}$ with PIT (or EqSLP [Allender et al. 2009])
  - Find an efficient randomized algorithm to solve $\mathrm{SSR}_{\mathrm{SLP}}$

Testing zero for sums of square roots

Problem (Testing Equality)

Given n positive integers $(a_1, \ldots, a_n)$ *and* $(\delta_1, \ldots, \delta_n) \in \{-1, 1\}^n$*, decide whether* $S = \sum_{i=1}^{n} \delta_i \sqrt{a_i} = 0$.

- a_i's given in binary $\to$ Blömer gave a polynomial-time algorithm
- a_i's given by SLPs $\to$ $\mathrm{SSR}_{\mathrm{SLP}}$
- a_i's given by SLPs and $\dim\left(\mathrm{span}_{\mathbb{Q}}(\sqrt{a_1}, \ldots, \sqrt{a_n})\right) = 1 \to$ 1-dim $\mathrm{SSR}_{\mathrm{SLP}}$
- Goals:
  - Compare $\mathrm{SSR}_{\mathrm{SLP}}$ with PIT (or EqSLP [Allender et al. 2009])
  - Find an efficient randomized algorithm to solve $\mathrm{SSR}_{\mathrm{SLP}}$

Theorem

Under GRH, there exists a randomized polynomial time algorithm with an oracle for 1-dim $\mathrm{SSR}_{\mathrm{SLP}}$ *that solves* $\mathrm{SSR}_{\mathrm{SLP}}$.

Ingredients of the proof

Let $a_1, \ldots, a_n$ be positive integers and $(\delta_1, \ldots, \delta_n) \in \{-1, 1\}^n$. Wlog, we can assume $(\sqrt{a_1}, \ldots, \sqrt{a_\ell})$ to be a basis of $\mathrm{span}_{\mathbb{Q}}(\sqrt{a_1}, \ldots, \sqrt{a_n})$.

Ingredients of the proof

Let $a_1, \ldots, a_n$ be positive integers and $(\delta_1, \ldots, \delta_n) \in \{-1, 1\}^n$. Wlog, we can assume $(\sqrt{a_1}, \ldots, \sqrt{a_\ell})$ to be a basis of $\mathrm{span}_{\mathbb{Q}}(\sqrt{a_1}, \ldots, \sqrt{a_n})$.

Lemma (Kneser)

For all $1 \leq i \leq n$, there exists a unique $1 \leq j \leq \ell$ such that $\sqrt{a_i} \in \mathbb{Q} \cdot \sqrt{a_j}$.

Ingredients of the proof

Let $a_1, \dots, a_n$ be positive integers and $(\delta_1, \dots, \delta_n) \in \{-1, 1\}^n$. Wlog, we can assume $(\sqrt{a_1}, \dots, \sqrt{a_\ell})$ to be a basis of $\operatorname{span}_{\mathbb{Q}}(\sqrt{a_1}, \dots, \sqrt{a_n})$.

Lemma (Kneser)

For all $1 \le i \le n$, there exists a unique $1 \le j \le \ell$ such that $\sqrt{a_i} \in \mathbb{Q} \cdot \sqrt{a_j}$.

This implies

$$\sum_{i=1}^{n} \delta_i \sqrt{a_i} = 0 \iff \forall 1 \le j \le \ell, \sum_{i:\ \sqrt{a_i} \in \mathbb{Q}\sqrt{a_j}} \delta_i \sqrt{a_i} = 0.$$

Ingredients of the proof

Let $a_1, \ldots, a_n$ be positive integers and $(\delta_1, \ldots, \delta_n) \in \{-1, 1\}^n$. Wlog, we can assume $(\sqrt{a_1}, \ldots, \sqrt{a_\ell})$ to be a basis of $\operatorname{span}_{\mathbb{Q}}(\sqrt{a_1}, \ldots, \sqrt{a_n})$.

Lemma (Kneser)

For all $1 \leq i \leq n$, there exists a unique $1 \leq j \leq \ell$ such that $\sqrt{a_i} \in \mathbb{Q} \cdot \sqrt{a_j}$.

This implies

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

Need an efficient way to build the 1-dimensional subsums, *i.e.* need an efficient way to test if $\sqrt{a}/\sqrt{b} \in \mathbb{Q}$ or equivalently if ab is a perfect square.

Ingredients of the proof

Let $a_1, \ldots, a_n$ be positive integers and $(\delta_1, \ldots, \delta_n) \in \{-1, 1\}^n$. Wlog, we can assume $(\sqrt{a_1}, \ldots, \sqrt{a_\ell})$ to be a basis of $\mathrm{span}_{\mathbb{Q}}(\sqrt{a_1}, \ldots, \sqrt{a_n})$.

Lemma (Kneser)

For all $1 \leq i \leq n$, there exists a unique $1 \leq j \leq \ell$ such that $\sqrt{a_i} \in \mathbb{Q} \cdot \sqrt{a_j}$.

This implies

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

Need an efficient way to build the 1-dimensional subsums, *i.e.* need an efficient way to test if $\sqrt{a}/\sqrt{b} \in \mathbb{Q}$ or equivalently if ab is a perfect square.

Lemma

Given an SLP of size t computing an integer N, under GRH, there exists a randomized algorithm running in polynomial time (in t) to decide if N is a perfect square.

Ingredients of the proof

Let $a_1, \dots, a_n$ be positive integers and $(\delta_1, \dots, \delta_n) \in \{-1, 1\}^n$. Wlog, we can assume $(\sqrt{a_1}, \dots, \sqrt{a_\ell})$ to be a basis of $\mathrm{span}_{\mathbb{Q}}(\sqrt{a_1}, \dots, \sqrt{a_n})$.

Lemma (Kneser)

For all $1 \le i \le n$, there exists a unique $1 \le j \le \ell$ such that $\sqrt{a_i} \in \mathbb{Q} \cdot \sqrt{a_j}$.

This implies

$$\sum_{i=1}^{n} \delta_i \sqrt{a_i} = 0 \iff \forall 1 \le j \le \ell, \sum_{i:\ \sqrt{a_i} \in \mathbb{Q}\sqrt{a_j}} \delta_i \sqrt{a_i} = 0.$$

Need an efficient way to build the 1-dimensional subsums, *i.e.* need an efficient way to test if $\sqrt{a}/\sqrt{b} \in \mathbb{Q}$ or equivalently if ab is a perfect square.

Lemma

Given an SLP of size t computing an integer N, under GRH, there exists a randomized algorithm running in polynomial time (in t) to decide if N is a perfect square.

Idea: Reduce N modulo a random prime $p \le 2^{q(t)}$. If N is not a square, the density of prime numbers p such that N is a square in $\mathbb{Z}/p\mathbb{Z}$ is $1/2$. Use an effective version of the Chebotarev's theorem (valid under GRH).

Conclusion

- Bound on the order of linear combination of solutions of differential equations of order 1. Can we extend this to higher order D-finite functions? What about algebraic functions?

- $W_{\text{ord}}(\mathcal{F}) \leq n \cdot \mathcal{O}(\mathcal{F}) - n(n-1)$.

- Open question related to PosSLP

  Given positive integers a, b, c, n in binary, determine the sign of $a^n + b^n - c^n$.

  Can we find an algorithm that solves this problem in time $O(\log(\max(a, b, c, n)))$?

References I

Neeraj Kayal and Chandan Saha.
On the sum of square roots of polynomials and related problems.
ACM Transactions on Computation Theory (TOCT), 4(4):1–15, 2012.