PosSLP and Sum of Squares


Markus Bläser[1] Julian Dörfler[2] Gorav Jindal[3]

December 16, 2024
FSTTCS 2024, IIT Gandhinagar, India

[1]Saarland University, Saarland Informatics Campus, Saarbrücken, Germany
[2]Saarland University, Saarland Informatics Campus, Saarbrücken, Germany
[3]Max Planck Institute for Software Systems, Saarbrücken, Germany

Table of Contents

1. Motivation
2. PosSLP
3. Certificates for Positivity
4. Positivity of Polynomials

Decision problems on Integers

- Given an integer N as input, how to decide if:
  - N is zero?
  - N is positive?

Decision problems on Integers

- Given an integer N as input, how to decide if:
  - N is zero?
  - N is positive?
- Of course, N is not given as input in its bit string representation.

Decision problems on Integers

- Given an integer N as input, how to decide if:
  - N is zero?
  - N is positive?
- Of course, N is not given as input in its bit string representation.

Example

Given $a, b, c, n \in \mathbb{N}$, $N := a^n + b^n - c^n$. Decide if:

- N is zero (Fermat's Last Theorem) ?
- N is positive?

Arithmetic circuits and SLPs

Arithmetic circuits and SLPs

Definition (Arithmetic circuit)

An arithmetic circuit is a directed acyclic graph whose inputs are constants $0, 1$ or indeterminates $x_1, x_2, \ldots, x_n$. Internal nodes are operations $+, -, \times$.

Arithmetic circuits and SLPs

Definition (Arithmetic circuit)

An arithmetic circuit is a directed acyclic graph whose inputs are constants $0, 1$ or indeterminates $x_1, x_2, \ldots, x_n$. Internal nodes are operations $+, -, \times$.

- Each arithmetic circuit computes a polynomial $f \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$.
- Size $=$ Number of nodes.

Arithmetic circuits and SLPs

Definition (Arithmetic circuit)

An arithmetic circuit is a directed acyclic graph whose inputs are constants $0, 1$ or indeterminates $x_1, x_2, \ldots, x_n$. Internal nodes are operations $+, -, \times$.

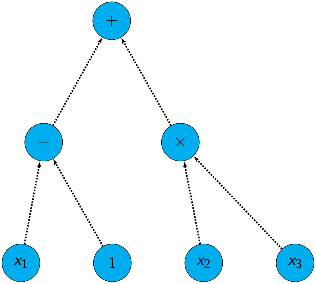
- Each arithmetic circuit computes a polynomial $f \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$.
- Size $=$ Number of nodes.

Definition (SLP)

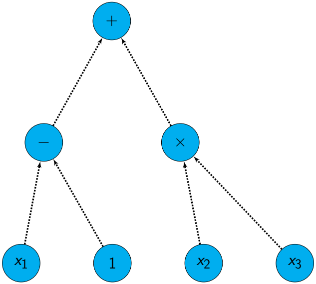
A straight-line program (SLP) is a sequence of instructions for evaluation of an arithmetic circuit.

- SLPs and arithmetic circuits are used interchangeably.

Example



Example



- This circuit computes the polynomial $(x_1 - 1) + x_2 x_3$.

Table of Contents

1 Motivation

2 PosSLP

3 Certificates for Positivity

4 Positivity of Polynomials

PosSLP

PosSLP

Definition (PosSLP)

Given a SLP P without indeterminates, decide if the integer N computed by P is positive.

PosSLP

Definition (PosSLP)

Given a SLP P without indeterminates, decide if the integer N computed by P is positive.

- Such a SLP P is sequence of integers $(b_0, b_1, b_2, \ldots, b_\ell)$ with
  - $b_0 = 1$.
  - for all $1 \leq i \leq \ell$, $b_i = b_j \circ_i b_k$, with $\circ_i \in \{+, -, *\}$ and $j, k < i$.

PosSLP

Definition (PosSLP)

Given a SLP P without indeterminates, decide if the integer N computed by P is positive.

- Such a SLP P is sequence of integers $(b_0, b_1, b_2, \ldots, b_\ell)$ with
  - $b_0 = 1$.
  - for all $1 \leq i \leq \ell$, $b_i = b_j \circ_i b_k$, with $\circ_i \in \{+, -, *\}$ and $j, k < i$.
- Integer computed by P is b_ℓ, size of P is ℓ.

PosSLP

Definition (PosSLP)

Given a SLP P without indeterminates, decide if the integer N computed by P is positive.

- Such a SLP P is sequence of integers $(b_0, b_1, b_2, \ldots, b_\ell)$ with
  - $b_0 = 1$.
  - for all $1 \leq i \leq \ell$, $b_i = b_j \circ_i b_k$, with $\circ_i \in \{+, -, *\}$ and $j, k < i$.
- Integer computed by P is b_ℓ, size of P is ℓ.

Remark

We **cannot** simply compute b_ℓ.

Sum of Square Roots Problem

Problem (SSR)

Given $S = \sum_{i=1}^{n} \delta_i \sqrt{a_i}$*, with* $\delta_i \in \{+1, -1\}$ *and* $a_i \in \mathbb{N}$*, decide if* $S > 0$.

Sum of Square Roots Problem

Problem (SSR)

Given $S = \sum_{i=1}^{n} \delta_i \sqrt{a_i}$, *with* $\delta_i \in \{+1, -1\}$ *and* $a_i \in \mathbb{N}$, *decide if* $S > 0$.

- Posed by (Garey, Graham, and Johnson 1976) in connection with the Euclidean Traveling Salesman Problem (ETSP).

Sum of Square Roots Problem

Problem (SSR)

Given $S = \sum_{i=1}^{n} \delta_i \sqrt{a_i}$, *with* $\delta_i \in \{+1, -1\}$ *and* $a_i \in \mathbb{N}$, *decide if* $S > 0$.

- Posed by (Garey, Graham, and Johnson 1976) in connection with the Euclidean Traveling Salesman Problem (ETSP).
- ETSP is in NP relative to SSR.

Sum of Square Roots Problem

Problem (SSR)

Given $S = \sum_{i=1}^{n} \delta_i \sqrt{a_i}$, *with* $\delta_i \in \{+1, -1\}$ *and* $a_i \in \mathbb{N}$, *decide if* $S > 0$.

- Posed by (Garey, Graham, and Johnson 1976) in connection with the Euclidean Traveling Salesman Problem (ETSP).
- ETSP is in NP relative to SSR.

Theorem ((Tiwari 1992))

SSR $\leq_{\mathrm{P}}$ PosSLP.

Sum of Square Roots Problem

Problem (SSR)

Given $S = \sum_{i=1}^{n} \delta_i \sqrt{a_i}$, *with* $\delta_i \in \{+1, -1\}$ *and* $a_i \in \mathbb{N}$, *decide if* $S > 0$.

- Posed by (Garey, Graham, and Johnson 1976) in connection with the Euclidean Traveling Salesman Problem (ETSP).
- ETSP is in NP relative to SSR.

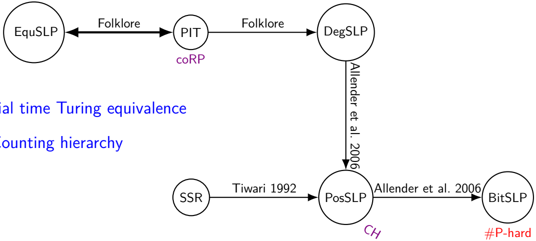
Theorem ((Tiwari 1992))

SSR $\leq_{\mathrm{P}}$ PosSLP.

Proof.

A lower bound on $|S|$. Newton iteration: If $x_0 = a$, $x_{i+1} = \frac{1}{2}\left(x_i + \frac{a}{x_i}\right)$ then $x_i \to \sqrt{a}$. □

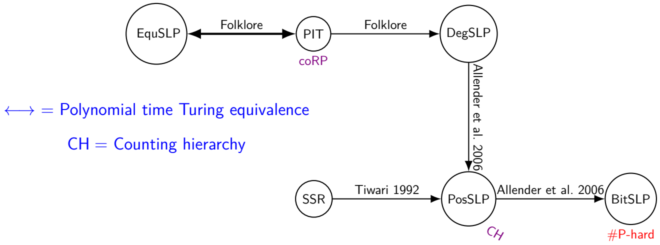
Complexity landscape of PosSLP



$\longleftrightarrow$ = Polynomial time Turing equivalence

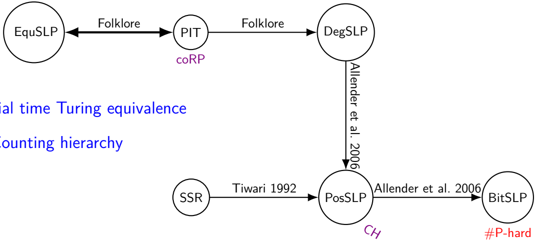
CH = Counting hierarchy

Complexity landscape of PosSLP



- EquSLP: Given a SLP computing $N \in \mathbb{Z}$, decide if $N = 0$.

Complexity landscape of PosSLP

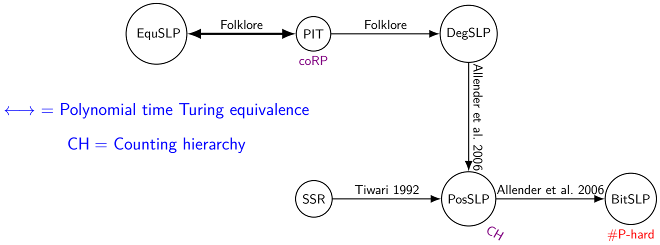


$\longleftrightarrow$ = Polynomial time Turing equivalence

CH = Counting hierarchy

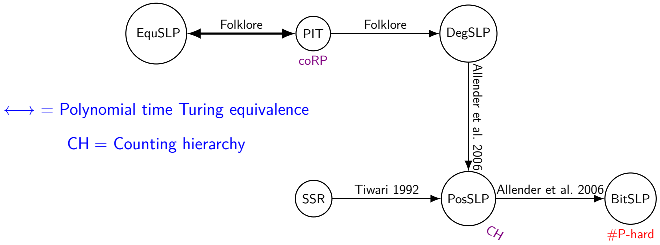
- EquSLP: Given a SLP computing $N \in \mathbb{Z}$, decide if $N = 0$.
- PIT: Given an arithmetic circuit computing a polynomial $f \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$, decide if $f = 0$.

Complexity landscape of PosSLP



- EquSLP: Given a SLP computing $N \in \mathbb{Z}$, decide if $N = 0$.
- PIT: Given an arithmetic circuit computing a polynomial $f \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$, decide if $f = 0$.
- DegSLP: Given a arithmetic circuit computing a polynomial $f \in \mathbb{Z}[x]$ and $d \in \mathbb{N}$, decide if $\deg(f) \leq d$.

Complexity landscape of PosSLP



- EquSLP: Given a SLP computing $N \in \mathbb{Z}$, decide if $N = 0$.
- PIT: Given an arithmetic circuit computing a polynomial $f \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$, decide if $f = 0$.
- DegSLP: Given a arithmetic circuit computing a polynomial $f \in \mathbb{Z}[x]$ and $d \in \mathbb{N}$, decide if $\deg(f) \leq d$.
- BitSLP: Given a SLP computing $N \in \mathbb{Z}$ and $i \in \mathbb{N}$, decide if i^{th} bit of N is 1.

Lower bounds for PosSLP

- Best upper bounds for PosSLP is CH.

Lower bounds for PosSLP

- Best upper bounds for PosSLP is CH.
- Unfortunately, nontrivial lower bounds for PosSLP remain unknown.

Lower bounds for PosSLP

- Best upper bounds for PosSLP is CH.
- Unfortunately, nontrivial lower bounds for PosSLP remain unknown.

Theorem ((Bürgisser and Jindal 2024))

If a constructive variant of the ***radical conjecture*** *of (Dutta, Saxena, and Sinhababu 2018) is true and* PosSLP $\in$ BPP *then* NP $\subseteq$ BPP.

Table of Contents

1. Motivation
2. PosSLP
3. Certificates for Positivity
4. Positivity of Polynomials

Monotone Complexity

- For $N > 0$, how do we certify the positivity of N?

Monotone Complexity

- For $N > 0$, how do we certify the positivity of N?
- $\tau(N) :=$ size of the smallest SLP which computes N.
- $\tau_+(N) :=$ size of the smallest subtraction free SLP which computes N.

Monotone Complexity

- For $N > 0$, how do we certify the positivity of N?
- $\tau(N) :=$ size of the smallest SLP which computes N.
- $\tau_+(N) :=$ size of the smallest subtraction free SLP which computes N.
- If $N > 0$ then there exists a subtraction free SLP which computes N.

Monotone Complexity

- For $N > 0$, how do we certify the positivity of N?
- $\tau(N) :=$ size of the smallest SLP which computes N.
- $\tau_+(N) :=$ size of the smallest subtraction free SLP which computes N.
- If $N > 0$ then there exists a subtraction free SLP which computes N.

Lemma ((Jindal and Saranurak 2012))

If $\tau_+(N) \leq \mathrm{poly}(\tau(N))$ *then* $\mathrm{PosSLP} \in \mathrm{PH}$.

Monotone Complexity

- For $N > 0$, how do we certify the positivity of N?
- $\tau(N) :=$ size of the smallest SLP which computes N.
- $\tau_+(N) :=$ size of the smallest subtraction free SLP which computes N.
- If $N > 0$ then there exists a subtraction free SLP which computes N.

Lemma ((Jindal and Saranurak 2012))

If $\tau_+(N) \leq \mathrm{poly}(\tau(N))$ *then* PosSLP $\in$ PH.

- There exist integer sequences where $\tau_+(n) > \tau(n)$ (Jindal and Saranurak 2012).

Monotone Complexity

- For $N > 0$, how do we certify the positivity of N?
- $\tau(N) :=$ size of the smallest SLP which computes N.
- $\tau_+(N) :=$ size of the smallest subtraction free SLP which computes N.
- If $N > 0$ then there exists a subtraction free SLP which computes N.

Lemma ((Jindal and Saranurak 2012))

If $\tau_+(N) \leq \mathrm{poly}(\tau(N))$ *then* $\mathrm{PosSLP} \in \mathrm{PH}$.

- There exist integer sequences where $\tau_+(n) > \tau(n)$ (Jindal and Saranurak 2012).

Lagrange's four-square theorem

Theorem (Lagrange 1770)

Every non-negative integer can be written as a sum of four non-negative integer squares.

Lagrange's four-square theorem

Theorem (Lagrange 1770)

Every non-negative integer can be written as a sum of four non-negative integer squares.

- So PosSLP is same as:
  - First check if $N = 0$ using EquSLP.
  - Given non-zero N (as SLP) decide if $\exists a, b, c, d \in \mathbb{N}$ such that $N = a^2 + b^2 + c^2 + d^2$.

Lagrange's four-square theorem

Theorem (Lagrange 1770)

Every non-negative integer can be written as a sum of four non-negative integer squares.

- So PosSLP is same as:
  - First check if $N = 0$ using EquSLP.
  - Given non-zero N (as SLP) decide if $\exists a, b, c, d \in \mathbb{N}$ such that $N = a^2 + b^2 + c^2 + d^2$.
- How about shorter Sum of Squares certificates?

Sum of fewer Squares

Sum of fewer Squares

- $n \in \mathbb{N}$ is 3SoS if it can be expressed as the sum of three squares (of integers).
- $n \in \mathbb{N}$ is 2SoS if it can be expressed as the sum of two squares (of integers).

Sum of fewer Squares

- $n \in \mathbb{N}$ is 3SoS if it can be expressed as the sum of three squares (of integers).
- $n \in \mathbb{N}$ is 2SoS if it can be expressed as the sum of two squares (of integers).

Problem (3SoSSLP)

Given a SLP computing $N \in \mathbb{Z}$, decide whether N is a 3SoS.

Sum of fewer Squares

- $n \in \mathbb{N}$ is 3SoS if it can be expressed as the sum of three squares (of integers).
- $n \in \mathbb{N}$ is 2SoS if it can be expressed as the sum of two squares (of integers).

Problem (3SoSSLP)

Given a SLP computing $N \in \mathbb{Z}$, decide whether N is a 3SoS.

Problem (2SoSSLP)

Given a SLP computing $N \in \mathbb{Z}$, decide whether N is a 2SoS.

3SoSSLP

Theorem ((Legendre 1798))

An integer is 3SoS *if and only if it is not of the form* $4^a(8b+7)$*, with* $a, b \in \mathbb{N}$*.*

3SoSSLP

Theorem ((Legendre 1798))

An integer is 3SoS *if and only if it is not of the form* $4^a(8b+7)$*, with* $a, b \in \mathbb{N}$*.*

Lemma

EquSLP $\leq_{\mathrm{P}}$ 3SoSSLP*.*

3SoSSLP

Theorem ((Legendre 1798))

An integer is 3SoS *if and only if it is not of the form* $4^a(8b+7)$, *with* $a, b \in \mathbb{N}$.

Lemma

EquSLP $\leq_P$ 3SoSSLP.

Proof.

Suppose $M = N^2$. If $M \in \mathbb{Z}_+$ then $7M^4$ not a 3SoS. □

3SoSSLP

- 3SoS integers are “dense” in $\mathbb{N}$ and occur very “frequently”.

3SoSSLP

- 3SoS integers are "dense" in $\mathbb{N}$ and occur very "frequently".

Theorem ((Landau 1908))

Asymptotic density of 3SoS *integers in* $\mathbb{N}$ *is* $5/6$.

3SoSSLP

- 3SoS integers are "dense" in $\mathbb{N}$ and occur very "frequently".

Theorem ((Landau 1908))

Asymptotic density of 3SoS *integers in* $\mathbb{N}$ *is 5/6.*

Lemma

$\forall n \in \mathbb{N}$ *at least one element in the set* $\{n, n+2\}$ *is* 3SoS.

3SoSSLP

- 3SoS integers are “dense” in $\mathbb{N}$ and occur very “frequently”.

Theorem ((Landau 1908))

Asymptotic density of 3SoS *integers in* $\mathbb{N}$ *is 5/6.*

Lemma

$\forall n \in \mathbb{N}$ *at least one element in the set* $\{n, n+2\}$ *is* 3SoS.

Theorem

$\mathrm{PosSLP} \in \mathrm{P}^{\mathrm{3SoSSLP}}$.

3SoSSLP

- 3SoS integers are "dense" in $\mathbb{N}$ and occur very "frequently".

Theorem ((Landau 1908))

Asymptotic density of 3SoS *integers in* $\mathbb{N}$ *is* $5/6$.

Lemma

$\forall n \in \mathbb{N}$ *at least one element in the set* $\{n, n+2\}$ *is* 3SoS.

Theorem

$\mathrm{PosSLP} \in \mathrm{P}^{\mathrm{3SoSSLP}}$.

Proof.

Given SLP for N, first check if $N \in \{0, -1, -2\}$. Assume $N \notin \{0, -1, -2\}$. Check if N is a 3SoS. Check if $N+2$ is a 3SoS. $\square$

3SoSSLP and Div2SLP

Problem (Div2SLP)

Given $N \in \mathbb{Z}$ by SLP, and $\ell \in \mathbb{N}$, decide if 2^{ℓ} divides $|N|$.

3SoSSLP and Div2SLP

Problem (Div2SLP)

Given $N \in \mathbb{Z}$ by SLP, and $\ell \in \mathbb{N}$, decide if 2^ℓ divides $|N|$.

Lemma

DegSLP $\leq_{\mathrm{P}}$ Div2SLP.

3SoSSLP and Div2SLP

Problem (Div2SLP)

Given $N \in \mathbb{Z}$ by SLP, and $\ell \in \mathbb{N}$, decide if 2^ℓ divides $|N|$.

Lemma

DegSLP $\leq_{\mathrm{P}}$ Div2SLP.

- It is natural that Div2SLP is useful for deciding 3SoSSLP.

3SoSSLP and Div2SLP

Problem (Div2SLP)

Given $N \in \mathbb{Z}$ by SLP, and $\ell \in \mathbb{N}$, decide if 2^ℓ divides $|N|$.

Lemma

DegSLP $\leq_{\mathrm{P}}$ Div2SLP.

- It is natural that Div2SLP is useful for deciding 3SoSSLP.

Theorem

3SoSSLP $\in \mathrm{P}^{\{\mathrm{Div2SLP},\mathrm{PosSLP}\}}$.

3SoSSLP and Div2SLP

Problem (Div2SLP)

Given $N \in \mathbb{Z}$ by SLP, and $\ell \in \mathbb{N}$, decide if 2^ℓ divides $|N|$.

Lemma

DegSLP $\leq_{\mathrm{P}}$ Div2SLP.

- It is natural that Div2SLP is useful for deciding 3SoSSLP.

Theorem

3SoSSLP $\in \mathrm{P}^{\{\mathrm{Div2SLP},\mathrm{PosSLP}\}}$.

Proof.

To decide if N is 3SoS, first check if $N > 0$. Then use Div2SLP oracle to check the 3SoS condition. □

2SoSSLP

Theorem (Gauss 1801; Jacobi 1829)

An integer $n > 1$ is not 2SoS if and only if the prime-power decomposition of n contains a prime of the form $4k + 3$ with an odd power.

2SoSSLP

Theorem (Gauss 1801; Jacobi 1829)

An integer $n > 1$ is not 2SoS if and only if the prime-power decomposition of n contains a prime of the form $4k + 3$ with an odd power.

Lemma

EquSLP $\leq_{\mathrm{P}}$ 2SoSSLP.

2SoSSLP

Theorem (Gauss 1801; Jacobi 1829)

An integer $n > 1$ is not 2SoS if and only if the prime-power decomposition of n contains a prime of the form $4k + 3$ with an odd power.

Lemma

EquSLP $\leq_{\mathrm{P}}$ 2SoSSLP.

Proof.

Suppose $M = N^2$. If $M \in \mathbb{Z}_+$ then $3M^2$ not a 2SoS. □

2SoSSLP

Theorem (Gauss 1801; Jacobi 1829)

An integer $n > 1$ is not 2SoS if and only if the prime-power decomposition of n contains a prime of the form $4k + 3$ with an odd power.

Lemma

EquSLP $\leq_P$ 2SoSSLP.

Proof.

Suppose $M = N^2$. If $M \in \mathbb{Z}_+$ then $3M^2$ not a 2SoS. □

Theorem

If Generalized Cramér conjecture is true then PosSLP $\in \mathrm{NP}^{\mathrm{2SoSSLP}}$.

SquSLP

Problem (SquSLP)

Given a SLP representing $N \in \mathbb{Z}$, decide whether $N = a^2$ for some $a \in \mathbb{Z}$.

SquSLP

Problem (SquSLP)

Given a SLP representing $N \in \mathbb{Z}$, decide whether $N = a^2$ for some $a \in \mathbb{Z}$.

Lemma

EquSLP $\leq_{\mathrm{P}}$ SquSLP.

SquSLP

Problem (SquSLP)

Given a SLP representing $N \in \mathbb{Z}$, decide whether $N = a^2$ for some $a \in \mathbb{Z}$.

Lemma

EquSLP $\leq_{\mathrm{P}}$ SquSLP.

Proof.

Suppose $M = N^2 + 1$. M is a square iff N is zero. □

SquSLP

Problem (SquSLP)

Given a SLP representing $N \in \mathbb{Z}$, decide whether $N = a^2$ for some $a \in \mathbb{Z}$.

Lemma

EquSLP $\leq_{\mathrm{P}}$ SquSLP.

Proof.

Suppose $M = N^2 + 1$. M is a square iff N is zero. $\square$

Theorem ((Jindal and Gaillard 2023))

SquSLP *can be decided in randomized polynomial time, assuming GRH.*

SquSLP

Problem (SquSLP)

Given a SLP representing $N \in \mathbb{Z}$, decide whether $N = a^2$ for some $a \in \mathbb{Z}$.

Lemma

EquSLP $\leq_{\mathrm{P}}$ SquSLP.

Proof.

Suppose $M = N^2 + 1$. M is a square iff N is zero. □

Theorem ((Jindal and Gaillard 2023))

SquSLP *can be decided in randomized polynomial time, assuming GRH.*

Proof.

To decide if $N = a^2$, choose a random prime p and decide if N mod p is a square in $\mathbb{F}_p$. □

Table of Contents

1. Motivation
2. PosSLP
3. Certificates for Positivity
4. Positivity of Polynomials

Positivity of Polynomials

- Given a polynomial $f \in \mathbb{Z}[x]$, decide if f is positive.

Positivity of Polynomials

- Given a polynomial $f \in \mathbb{Z}[x]$, decide if f is positive.
- What does it even mean?

Positivity of Polynomials

- Given a polynomial $f \in \mathbb{Z}[x]$, decide if f is positive.
- What does it even mean?

Definition

$f \in \mathbb{R}[x]$ is **positive** if $f(x) \geq 0$ for all $x \in \mathbb{R}$.

Positivity of Polynomials

- Given a polynomial $f \in \mathbb{Z}[x]$, decide if f is positive.
- What does it even mean?

Definition

$f \in \mathbb{R}[x]$ is **positive** if $f(x) \geq 0$ for all $x \in \mathbb{R}$.

Theorem (Folklore)

For every positive polynomial $f \in \mathbb{R}[x]$, there exist $g, h \in \mathbb{R}[x]$ such that $f = g^2 + h^2$.

Positivity of Polynomials

- Given a polynomial $f \in \mathbb{Z}[x]$, decide if f is positive.
- What does it even mean?

Definition

$f \in \mathbb{R}[x]$ is **positive** if $f(x) \geq 0$ for all $x \in \mathbb{R}$.

Theorem (Folklore)

For every positive polynomial $f \in \mathbb{R}[x]$, there exist $g, h \in \mathbb{R}[x]$ such that $f = g^2 + h^2$.

Theorem ((Pourchet 1971))

For every positive polynomial $f \in \mathbb{Q}[x]$, there exist $g_1, g_2, \ldots, g_5 \in \mathbb{Q}[x]$ such that $f = \sum_{i=1}^{5} g_i^2$.

Positivity of Polynomials

- Given a polynomial $f \in \mathbb{Z}[x]$, decide if f is positive.
- What does it even mean?

Definition

$f \in \mathbb{R}[x]$ is **positive** if $f(x) \geq 0$ for all $x \in \mathbb{R}$.

Theorem (Folklore)

For every positive polynomial $f \in \mathbb{R}[x]$, there exist $g, h \in \mathbb{R}[x]$ such that $f = g^2 + h^2$.

Theorem ((Pourchet 1971))

For every positive polynomial $f \in \mathbb{Q}[x]$, there exist $g_1, g_2, \ldots, g_5 \in \mathbb{Q}[x]$ such that $f = \sum_{i=1}^{5} g_i^2$.

Positivity of Polynomials

Problem (PosPolySLP)

Given a straight-line program computing a univariate polynomial $f \in \mathbb{Z}[x]$*, decide if* f *is positive.*

Positivity of Polynomials

Problem (PosPolySLP)

Given a straight-line program computing a univariate polynomial $f \in \mathbb{Z}[x]$, decide if f is positive.

Theorem

PosPolySLP *is* coNP-*hard* .

Positivity of Polynomials

Problem (PosPolySLP)

Given a straight-line program computing a univariate polynomial $f \in \mathbb{Z}[x]$, decide if f is positive.

Theorem

PosPolySLP *is* coNP-*hard* .

Problem (SquPolySLP)

Given a straight-line program representing a univariate polynomial $f \in \mathbb{Z}[x]$, decide if $\exists g \in \mathbb{Z}[x]$ such that $f = g^2$.

SquPolySLP

SquPolySLP

- Can we use SquSLP to solve SquPolySLP?

SquPolySLP

- Can we use SquSLP to solve SquPolySLP?

Theorem ((Murty 2008))

For $f \in \mathbb{Z}[x]$, $\exists g \in \mathbb{Z}[x]$ with $f = g^2$ iff $\forall t \in \mathbb{Z}$, $f(t)$ is a perfect square.

SquPolySLP

- Can we use SquSLP to solve SquPolySLP?

Theorem ((Murty 2008))

For $f \in \mathbb{Z}[x]$, $\exists g \in \mathbb{Z}[x]$ with $f = g^2$ iff $\forall t \in \mathbb{Z}$, $f(t)$ is a perfect square.

Lemma

SquPolySLP $\in$ coRP.

SquPolySLP

- Can we use SquSLP to solve SquPolySLP?

Theorem ((Murty 2008))

For $f \in \mathbb{Z}[x]$, $\exists g \in \mathbb{Z}[x]$ with $f = g^2$ iff $\forall t \in \mathbb{Z}$, $f(t)$ is a perfect square.

Lemma

SquPolySLP $\in$ coRP.

Proof.

Pick a random $t \in \mathbb{Z}$ and decide if $f(t)$ is a square using algorithm for SquSLP. This works by using an effective variant of Hilbert's irreducibility theorem. $\square$

Summary of Complexity reductions

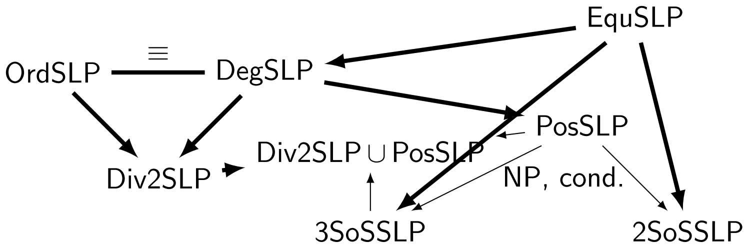
Problem (OrdSLP)

Given a SLP representing a polynomial $f \in \mathbb{Z}[x]$ and $\ell \in \mathbb{N}$, decide if x^ℓ divides f.

Summary of Complexity reductions

Problem (OrdSLP)

Given a SLP representing a polynomial $f \in \mathbb{Z}[x]$ and $\ell \in \mathbb{N}$, decide if x^ℓ divides f.



Future research directions

- Complexity of Div2SLP:
  - Div2SLP is at least as hard as DegSLP.
  - Is it NP-hard as well?
  - How does Div2SLP relate to PosSLP?

Future research directions

- Complexity of Div2SLP:
  - Div2SLP is at least as hard as DegSLP.
  - Is it NP-hard as well?
  - How does Div2SLP relate to PosSLP?
- SLP and Sum of Squares for Polynomials:
  - Complexity of polynomial analogues for 2SoSSLP, 3SoSSLP .

Future research directions

- Complexity of Div2SLP:
  - Div2SLP is at least as hard as DegSLP.
  - Is it NP-hard as well?
  - How does Div2SLP relate to PosSLP?
- SLP and Sum of Squares for Polynomials:
  - Complexity of polynomial analogues for 2SoSSLP, 3SoSSLP.
- Unconditional hardness results for the PosSLP problem?

Future research directions

- Complexity of Div2SLP:
  - Div2SLP is at least as hard as DegSLP.
  - Is it NP-hard as well?
  - How does Div2SLP relate to PosSLP?
- SLP and Sum of Squares for Polynomials:
  - Complexity of polynomial analogues for 2SoSSLP, 3SoSSLP .
- Unconditional hardness results for the PosSLP problem?
- Efficient algorithms for special cases of PosSLP.

Thanks for your attention! Any questions?

Literature I

Allender, E. et al. (2006). "On the complexity of numerical analysis". In: *21st Annual IEEE Conference on Computational Complexity (CCC'06)*, 9 pp.–339. DOI: 10.1109/CCC.2006.30.

Bürgisser, Peter and Gorav Jindal (2024). "On the Hardness of PosSLP". In: pp. 1872–1886. DOI: 10.1137/1.9781611977912.75. eprint: https://epubs.siam.org/doi/pdf/10.1137/1.9781611977912.75. URL: https://epubs.siam.org/doi/abs/10.1137/1.9781611977912.75.

Dutta, Pranjal, Nitin Saxena, and Amit Sinhababu (2018). "Discovering the roots: uniform closure results for algebraic classes under factoring". In: *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing*. STOC 2018. Los Angeles, CA, USA: Association for Computing Machinery, pp. 1152–1165. ISBN: 9781450355599. DOI: 10.1145/3188745.3188760. URL: https://doi.org/10.1145/3188745.3188760.

Literature II

Garey, M. R., 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*. STOC '76. Hershey, Pennsylvania, USA: Association for Computing Machinery, pp. 10–22. ISBN: 9781450374149. DOI: 10.1145/800113.803626. URL: https://doi.org/10.1145/800113.803626.

Jindal, Gorav and Louis Gaillard (2023). "On the Order of Power Series and the Sum of Square Roots Problem". In: *Proceedings of the 2023 International Symposium on Symbolic and Algebraic Computation*, pp. 354–362.

Jindal, Gorav and Thatchaphol Saranurak (2012). "Subtraction makes computing integers faster". In: *CoRR* abs/1212.2549. arXiv: 1212.2549. URL: http://arxiv.org/abs/1212.2549.

Literature III

- Landau, E. (1908). *Uber die Einteilung der positiven ganzen Zahlen in vier Klassen nach der Mindestzahl der zu ihrer additiven Zusammensetzung erforderliche Quadrate*. URL: https://books.google.de/books?id=e3XBnQAACAAJ.
- Legendre, Adrien Marie (1798). *Essai sur la théorie des nombres*. fr. Duprat. DOI: 10.3931/E-RARA-3663. URL: https://www.e-rara.ch/zut/doi/10.3931/e-rara-3663.
- Murty, M Ram (2008). "Polynomials assuming square values". In: *Number theory and discrete geometry*, pp. 155–163.
- Pourchet, Y. (1971). "Sur la représentation en somme de carrés des polynômes à une indéterminée sur un corps de nombres algébriques". fre. In: *Acta Arithmetica* 19.1, pp. 89–104. URL: http://eudml.org/doc/205020.

Literature IV

Tiwari, Prasoon (1992). "A problem that is easier to solve on the unit-cost algebraic RAM". In: *Journal of Complexity* 8.4, pp. 393–397. ISSN: 0885-064X. DOI: https://doi.org/10.1016/0885-064X(92)90003-T. URL: https://www.sciencedirect.com/science/article/pii/0885064X9290003T.