The Sum of Square Roots Problem

Based on joint work with Samir Datta (Chennai Mathematical Institute)

Nikhil Balaji

IIT Delhi

July 10, 2023

WORReLL @ ICALP '23

The Problem

SSR

Input: Positive integers $1 \leq a_1, \ldots, a_n \leq 2^n$ and signs $\delta_1, \ldots, \delta_n \in \{\pm 1\}$

The Problem

SSR

Input: Positive integers $1 \leq a_1, \ldots, a_n \leq 2^n$ and signs $\delta_1, \ldots, \delta_n \in \{\pm 1\}$

Output: $\operatorname{sgn}\left(\sum_{i=1}^{n} \delta_i \sqrt{a_i}\right)$

The Problem

SSR

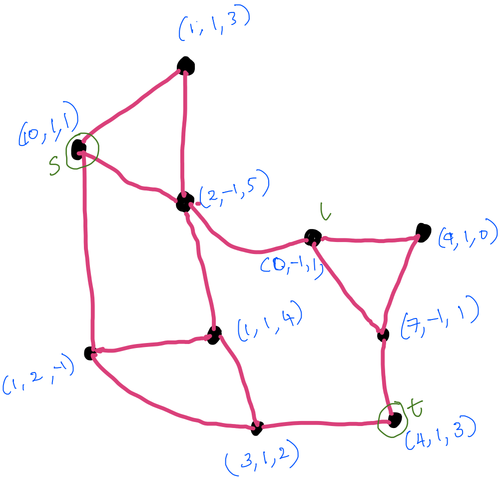
Input: Positive integers $1 \leq a_1, \ldots, a_n \leq 2^n$ and signs $\delta_1, \ldots, \delta_n \in \{\pm 1\}$

Output: $\operatorname{sgn}\left(\sum_{i=1}^{n} \delta_i \sqrt{a_i}\right)$

- Fundamental primitive in Computational Geometry.

An application: Shortest paths in graphs

Shortest paths in graphs embedded in $\mathbb{Z}^n$



The Problem

SSR

Input: Positive integers $1 \leq a_1, \ldots, a_n \leq 2^n$ and signs $\delta_1, \ldots, \delta_n \in \{\pm 1\}$

Output: $\operatorname{sgn}\left(\sum_{i=1}^{n} \delta_i \sqrt{a_i}\right)$

- Fundamental primitive in Computational Geometry.
- Shortest paths in graphs embedded in $\mathbb{Z}^n$ is in P relative to SSR.

The Problem

SSR

Input: Positive integers $1 \leq a_1, \ldots, a_n \leq 2^n$ and signs $\delta_1, \ldots, \delta_n \in \{\pm 1\}$

Output: $\text{sgn}\left(\sum_{i=1}^{n} \delta_i \sqrt{a_i}\right)$

- Fundamental primitive in Computational Geometry.
- Shortest paths in graphs embedded in $\mathbb{Z}^n$ is in P relative to SSR.
- Example due to Ron Graham:
  $\sqrt{1000001} + \sqrt{1000025} + \sqrt{1000031} + \sqrt{1000084} + \sqrt{1000087} + \sqrt{1000134} + \sqrt{1000158} + \sqrt{1000182} + \sqrt{1000198} - \sqrt{1000002} - \sqrt{1000018} - \sqrt{1000042} - \sqrt{1000066} - \sqrt{1000113} - \sqrt{1000116} - \sqrt{1000169} - \sqrt{1000175} - \sqrt{1000199} < 10^{-34}$

The Problem

SSR

Input: Positive integers $1 \leq a_1, \ldots, a_n \leq 2^n$ and signs $\delta_1, \ldots, \delta_n \in \{\pm 1\}$

Output: $\operatorname{sgn}\left(\sum_{i=1}^{n} \delta_i \sqrt{a_i}\right)$

- Fundamental primitive in Computational Geometry.
- Shortest paths in graphs embedded in $\mathbb{Z}^n$ is in P relative to SSR.
- Example due to Ron Graham:
  $\sqrt{1000001} + \sqrt{1000025} + \sqrt{1000031} + \sqrt{1000084} + \sqrt{1000087} + \sqrt{1000134} + \sqrt{1000158} + \sqrt{1000182} + \sqrt{1000198} - \sqrt{1000002} - \sqrt{1000018} - \sqrt{1000042} - \sqrt{1000066} - \sqrt{1000113} - \sqrt{1000116} - \sqrt{1000169} - \sqrt{1000175} - \sqrt{1000199} < 10^{-34}$
- Is this problem even decidable?

The Problem

SSR

Input: Positive integers $1 \leq a_1, \ldots, a_n \leq 2^n$ and signs $\delta_1, \ldots, \delta_n \in \{\pm 1\}$

Output: $\mathrm{sgn}\left(\sum_{i=1}^{n} \delta_i \sqrt{a_i}\right)$

- Fundamental primitive in Computational Geometry.
- Shortest paths in graphs embedded in $\mathbb{Z}^n$ is in P relative to SSR.
- Example due to Ron Graham:
  $\sqrt{1000001} + \sqrt{1000025} + \sqrt{1000031} + \sqrt{1000084} + \sqrt{1000087} + \sqrt{1000134} + \sqrt{1000158} + \sqrt{1000182} + \sqrt{1000198} - \sqrt{1000002} - \sqrt{1000018} - \sqrt{1000042} - \sqrt{1000066} - \sqrt{1000113} - \sqrt{1000116} - \sqrt{1000169} - \sqrt{1000175} - \sqrt{1000199} < 10^{-34}$
- Is this problem even decidable?
- Yes! We need *effective separation bounds*.

Separation Bounds

Definition

A separation bound is a computable function $sep : E \to \mathbb{R}$ such that the value of any non-zero expression E is lower bounded by $sep(E)$.

Separation Bounds

Definition

A separation bound is a computable function $sep : E \to \mathbb{R}$ such that the value of any non-zero expression E is lower bounded by $sep(E)$.

For e.g, Let $\alpha = \sum_{i=1}^{n} \delta_i \sqrt{a_i} \neq 0$. If $|\alpha| \neq 0$ then $|\alpha| \geq sep(\alpha)$.

Separation Bounds

Definition

A separation bound is a computable function $sep : E \rightarrow \mathbb{R}$ such that the value of any non-zero expression E is lower bounded by $sep(E)$.

For e.g, Let $\alpha = \sum_{i=1}^{n} \delta_i \sqrt{a_i} \neq 0$. If $|\alpha| \neq 0$ then $|\alpha| \geq sep(\alpha)$.

Can we prove *good* separation bounds?

Separation Bounds

Definition

A separation bound is a computable function $sep : E \to \mathbb{R}$ such that the value of any non-zero expression E is lower bounded by $sep(E)$.

For e.g, Let $\alpha = \sum_{i=1}^{n} \delta_i \sqrt{a_i} \neq 0$. If $|\alpha| \neq 0$ then $|\alpha| \geq sep(\alpha)$.

Can we prove *good* separation bounds?

In practice, $O(n \log 2^n) = O(n^2)$-bit approximation (i.e., $|p_i|, |q_i| \leq 2^{n^2}$) is usually sufficient to infer the sign of α.

Some easy bounds

Some easy bounds

Lemma (CK'96, Blö'98, BFMS'00)

Let α be an algebraic integer of degree d and U be an upper bound on the absolute value of any conjugate of α. Then, $sep(\alpha) \leq U^{1-d}$.

Some easy bounds

Lemma (CK'96, Blö'98, BFMS'00)

Let α be an algebraic integer of degree d and U be an upper bound on the absolute value of any conjugate of α. Then, $sep(\alpha) \leq U^{1-d}$. i.e. if $|\alpha| \neq 0$, then $|\alpha| > U^{1-d}$.

Some easy bounds

Lemma (CK'96, Blö'98, BFMS'00)

Let α be an algebraic integer of degree d and U be an upper bound on the absolute value of any conjugate of α. Then, $sep(\alpha) \leq U^{1-d}$. i.e. if $|\alpha| \neq 0$, then $|\alpha| > U^{1-d}$.

Proof. Since α is an algebraic integer, $\prod_{i=1}^{d} \alpha_i \in \mathbb{Z}$. Thus, $|\alpha \cdot U^{d-1}| \geq 1$.

Some easy bounds

Lemma (CK'96, Blö'98, BFMS'00)

Let α be an algebraic integer of degree d and U be an upper bound on the absolute value of any conjugate of α. Then, $sep(\alpha) \leq U^{1-d}$. i.e. if $|\alpha| \neq 0$, then $|\alpha| > U^{1-d}$.

Proof. Since α is an algebraic integer, $\prod_{i=1}^{d} \alpha_i \in \mathbb{Z}$. Thus, $|\alpha \cdot U^{d-1}| \geq 1$.

Corollary

SSR can be solved in $poly(d \log U)$ time and $poly(\log d \log U)$ space

Some easy bounds

Lemma (CK'96, Blö'98, BFMS'00)

Let α be an algebraic integer of degree d and U be an upper bound on the absolute value of any conjugate of α. Then, $sep(\alpha) \leq U^{1-d}$. i.e. if $|\alpha| \neq 0$, then $|\alpha| > U^{1-d}$.

Proof. Since α is an algebraic integer, $\prod_{i=1}^{d} \alpha_i \in \mathbb{Z}$. Thus, $|\alpha \cdot U^{d-1}| \geq 1$.

Corollary

SSR can be solved in $poly(d \log U)$ time and $poly(\log d \log U)$ space

- $|U| \leq n\sqrt{a_n} \leq n2^{n/2}$.

Some easy bounds

Lemma (CK'96, Blö'98, BFMS'00)

Let α be an algebraic integer of degree d and U be an upper bound on the absolute value of any conjugate of α. Then, $sep(\alpha) \leq U^{1-d}$. i.e. if $|\alpha| \neq 0$, then $|\alpha| > U^{1-d}$.

Proof. Since α is an algebraic integer, $\prod_{i=1}^{d} \alpha_i \in \mathbb{Z}$. Thus, $|\alpha \cdot U^{d-1}| \geq 1$.

Corollary

SSR can be solved in $poly(d \log U)$ time and $poly(\log d \log U)$ space

- $|U| \leq n\sqrt{a_n} \leq n2^{n/2}$.
- For every $i, [\mathbb{Q}[\sqrt{a_1}, \ldots, \sqrt{a_i}] : \mathbb{Q}[\sqrt{a_1}, \ldots, \sqrt{a_{i-1}}] \leq 2 \implies d \leq 2^n$.

Some easy bounds

Lemma (CK'96, Blö'98, BFMS'00)

Let α be an algebraic integer of degree d and U be an upper bound on the absolute value of any conjugate of α. Then, $sep(\alpha) \leq U^{1-d}$. i.e. if $|\alpha| \neq 0$, then $|\alpha| > U^{1-d}$.

Proof. Since α is an algebraic integer, $\prod_{i=1}^{d} \alpha_i \in \mathbb{Z}$. Thus, $|\alpha \cdot U^{d-1}| \geq 1$.

Corollary

SSR can be solved in $poly(d \log U)$ time and $poly(\log d \log U)$ space

- $|U| \leq n\sqrt{a_n} \leq n2^{n/2}$.
- For every $i, [\mathbb{Q}[\sqrt{a_1}, \ldots, \sqrt{a_i}] : \mathbb{Q}[\sqrt{a_1}, \ldots, \sqrt{a_{i-1}}] \leq 2 \implies d \leq 2^n$.

Some easy bounds

Lemma (CK'96, Blö'98, BFMS'00)

Let α be an algebraic integer of degree d and U be an upper bound on the absolute value of any conjugate of α. Then, $sep(\alpha) \leq U^{1-d}$. i.e. if $|\alpha| \neq 0$, then $|\alpha| > U^{1-d}$.

Proof. Since α is an algebraic integer, $\prod_{i=1}^{d} \alpha_i \in \mathbb{Z}$. Thus, $|\alpha \cdot U^{d-1}| \geq 1$.

Corollary

SSR can be solved in $poly(d \log U)$ time and $poly(\log d \log U)$ space

- $|U| \leq n\sqrt{a_n} \leq n2^{n/2}$.
- For every $i, [\mathbb{Q}[\sqrt{a_1}, \ldots, \sqrt{a_i}] : \mathbb{Q}[\sqrt{a_1}, \ldots, \sqrt{a_{i-1}}] \leq 2 \implies d \leq 2^n$.

The degree bound is tight - consider $a_1 = 2, \ldots a_n = p_n$, then the minimal polynomial of $\sum_{i=1}^{n} \sqrt{p_i}$ has degree exactly 2^n.

A hard (but tractable) subclass of SSR

Consider $\alpha = \sum_{i=1}^{n} \delta_i \sqrt{p_i} \implies |\alpha| \geq 2^{-n2^n}$

A hard (but tractable) subclass of SSR

Consider $\alpha = \sum_{i=1}^{n} \delta_i \sqrt{p_i} \implies |\alpha| \geq 2^{-n2^n}$

- By Prime number theorem, $p_n = O(n \log n)$.

A hard (but tractable) subclass of SSR

Consider $\alpha = \sum_{i=1}^{n} \delta_i \sqrt{p_i} \implies |\alpha| \geq 2^{-n2^n}$

- By Prime number theorem, $p_n = O(n \log n)$.

UnarySSR

Input: Positive integers $1 \leq a_1, \ldots, a_n \leq n^2$ and signs $\delta_1, \ldots, \delta_n \in \{\pm 1\}$

Output: $\operatorname{sgn}\left(\sum_{i=1}^{n} \delta_i \sqrt{a_i}\right)$

A hard (but tractable) subclass of SSR

Consider $\alpha = \sum_{i=1}^{n} \delta_i \sqrt{p_i} \implies |\alpha| \geq 2^{-n2^n}$

- By Prime number theorem, $p_n = O(n \log n)$.

UnarySSR

Input: Positive integers $1 \leq a_1, \ldots, a_n \leq n^2$ and signs $\delta_1, \ldots, \delta_n \in \{\pm 1\}$

Output: $\operatorname{sgn}\left(\sum_{i=1}^{n} \delta_i \sqrt{a_i}\right)$

- No better complexity bound known for even this "unary" case.

A hard (but tractable) subclass of SSR

UnarySSR

Input: Positive integers $1 \leq a_1, \ldots, a_n \leq n^2$ and signs $\delta_1, \ldots, \delta_n \in \{\pm 1\}$

Output: $\operatorname{sgn}\left(\sum_{i=1}^{n} \delta_i \sqrt{a_i}\right)$

Theorem (B.-Datta'20)

USSR $\in$ P/poly

There is a non-uniform polynomial time algorithm for USSR.

- For every n, there exists a *poly*(n)-sized "advice" string which helps you decide the sign of any instance of "length" n.

A hard (but tractable) subclass of SSR

UnarySSR

Input: Positive integers $1 \leq a_1, \ldots, a_n \leq n^2$ and signs $\delta_1, \ldots, \delta_n \in \{\pm 1\}$

Output: $\operatorname{sgn}\left(\sum_{i=1}^{n} \delta_i \sqrt{a_i}\right)$

Theorem (B.-Datta'20)

There is a non-uniform polynomial time algorithm for USSR.

- For every n, there exists a $poly(n)$-sized "advice" string which helps you decide the sign of any instance of "length" n.
- Idea: Rewrite $\alpha = \sum_{i=1}^{n} \delta_i \sqrt{a_i} = \sum_{i=1}^{n^2} \gamma_i \sqrt{i}$ where $\gamma_i \in \{0, \pm 1\}$.
  Note: We have 2^{n^2} different instances of USSR at length n.

A hard (but tractable) subclass of SSR

UnarySSR

Input: Positive integers $1 \leq a_1, \ldots, a_n \leq n^2$ and signs $\delta_1, \ldots, \delta_n \in \{\pm 1\}$

Output: $\operatorname{sgn}\left(\sum_{i=1}^{n} \delta_i \sqrt{a_i}\right)$

Theorem (B.-Datta'20)

There is a non-uniform polynomial time algorithm for USSR.

- For every n, there exists a $poly(n)$-sized "advice" string which helps you decide the sign of any instance of "length" n.
- Idea: Rewrite $\alpha = \sum_{i=1}^{n} \delta_i \sqrt{a_i} = \sum_{i=1}^{n^2} \gamma_i \sqrt{i}$ where $\gamma_i \in \{0, \pm 1\}$.

Theorem (Muroga'70)

There are integers $0 \leq |w_i| \leq 2^{n^3}$, $\sum_{i=1}^{n^2} \delta_i \sqrt{i} > 0 \iff \sum_{i=1}^{n^2} \delta_i w_i > 0$

Aside: What about testing $= 0$?

Aside: What about testing $= 0$?

ExactSSR

Input: Positive integers $1 \leq a_1, \ldots, a_n \leq 2^n$ and signs $\delta_1, \ldots, \delta_n \in \{\pm 1\}$

Output: 1 iff $\sum_{i=1}^{n} \delta_i \sqrt{a_i} = 0$

Aside: What about testing $= 0$?

ExactSSR

Input: Positive integers $1 \leq a_1, \ldots, a_n \leq 2^n$ and signs $\delta_1, \ldots, \delta_n \in \{\pm 1\}$

Output: 1 iff $\sum_{i=1}^{n} \delta_i \sqrt{a_i} = 0$

- In **P** (polynomial time)

Aside: What about testing $= 0$?

ExactSSR

Input: Positive integers $1 \le a_1, \ldots, a_n \le 2^n$ and signs $\delta_1, \ldots, \delta_n \in \{\pm 1\}$

Output: 1 iff $\sum_{i=1}^{n} \delta_i \sqrt{a_i} = 0$

- In **P** (polynomial time), in fact in $\mathbf{TC}^0$ (BHMOW'10).

Aside: What about testing $= 0$?

ExactSSR

Input: Positive integers $1 \leq a_1, \ldots, a_n \leq 2^n$ and signs $\delta_1, \ldots, \delta_n \in \{\pm 1\}$

Output: 1 iff $\sum_{i=1}^{n} \delta_i \sqrt{a_i} = 0$

- In **P** (polynomial time), in fact in $\mathbf{TC}^0$ (BHMOW'10).
- For any (given) polynomial f, checking $f(\sqrt{a_1}, \ldots, \sqrt{a_n}) = 0$ is in **coNP** unconditionally and in **coRP** assuming GRH (BNSW'22).

Aside: What about testing $= 0$?

ExactSSR

Input: Positive integers $1 \leq a_1, \ldots, a_n \leq 2^n$ and signs $\delta_1, \ldots, \delta_n \in \{\pm 1\}$

Output: 1 iff $\sum_{i=1}^{n} \delta_i \sqrt{a_i} = 0$

- In **P** (polynomial time), in fact in $\mathbf{TC}^0$ (BHMOW'10).
- For any (given) polynomial f, checking $f(\sqrt{a_1}, \ldots, \sqrt{a_n}) = 0$ is in **coNP** unconditionally and in **coRP** assuming GRH (BNSW'22).

Conclusion

Conclusion

- Better complexity upper bound for UnarySSR.

Conclusion

- Better complexity upper bound for UnarySSR.
- Corollary: UnarySSR cannot be NP-hard under widely believed complexity-theoretic assumptions.

Conclusion

- Better complexity upper bound for UnarySSR.
- Corollary: UnarySSR cannot be NP-hard under widely believed complexity-theoretic assumptions.
- Works for arbitrary but fixed set of real numbers, for eg. $\sum_{i=1}^{n} \delta_i (\pi e)^i$ where $\delta_i \in \{-d, \ldots, d\}$

Conclusion

- Better complexity upper bound for UnarySSR.
- Corollary: UnarySSR cannot be NP-hard under widely believed complexity-theoretic assumptions.
- Works for arbitrary but fixed set of real numbers, for eg. $\sum_{i=1}^{n} \delta_i (\pi e)^i$ where $\delta_i \in \{-d, \ldots, d\}$
- **Question:** Is there a short "witness" to test if a linear combination of square roots is positive?
- Applications to algorithmic questions in Diophantine approximation?

Conclusion

- Better complexity upper bound for UnarySSR.
- Corollary: UnarySSR cannot be NP-hard under widely believed complexity-theoretic assumptions.
- Works for arbitrary but fixed set of real numbers, for eg. $\sum_{i=1}^{n} \delta_i (\pi e)^i$ where $\delta_i \in \{-d, \ldots, d\}$
- **Question:** Is there a short "witness" to test if a linear combination of square roots is positive?
- Applications to algorithmic questions in Diophantine approximation?

Happy Birthday Ben!