The Sum of Square Roots Problem

Nikhil Balaji
nbalaji@cse.iitd.ac.in

Department of CSE
IIT Delhi

SAMSA 2026

June 19, 2026

N. Balaji, S. Datta, USSR is in P/poly, SOSA 2024

The Sum of Square Roots Problem

SSR

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

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

The Sum of Square Roots Problem

SSR

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

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

- Fundamental primitive in Computational Geometry.

The Sum of Square Roots Problem

SSR

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

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

- Fundamental primitive in Computational Geometry.
- Approximate the square roots - what is the precision required?

The Sum of Square Roots Problem

SSR

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

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

- Fundamental primitive in Computational Geometry.
- Approximate the square roots - what is the precision required?
- Example (due to Ron Graham):
  $\sqrt{1000001} + \sqrt{1000025} + \sqrt{1000031} + \sqrt{1000084} + \sqrt{1000087} +$
  $\sqrt{1000134} + \sqrt{1000158} + \sqrt{1000182} + \sqrt{1000198} - \sqrt{1000002} -$
  $\sqrt{1000018} - \sqrt{1000042} - \sqrt{1000066} - \sqrt{1000113} - \sqrt{1000116} -$
  $\sqrt{1000169} - \sqrt{1000175} - \sqrt{1000199} < 10^{-34}$

Separation Bounds

- The minimal polynomial of $\alpha = \sum_{i=1}^{n} \delta_i \sqrt{a_i}$ has degree $d \leq 2^n$ (since $[\mathbb{Q}[\sqrt{a_1}, \ldots, \sqrt{a_i}] : \mathbb{Q}[\sqrt{a_1}, \ldots, \sqrt{a_{i-1}}] \leq 2$).

Separation Bounds

- The minimal polynomial of $\alpha = \sum_{i=1}^{n} \delta_i \sqrt{a_i}$ has degree $d \leq 2^n$ (since $[\mathbb{Q}[\sqrt{a_1}, \ldots, \sqrt{a_i}] : \mathbb{Q}[\sqrt{a_1}, \ldots, \sqrt{a_{i-1}}] \leq 2$).
- If $\alpha \neq 0$, then

$$\begin{aligned} N(\alpha) &= \prod_{\sigma \in Gal(\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_n})/\mathbb{Q})} \sigma(\alpha) \\ &\leq |\alpha| \cdot |\sigma(\alpha)|^{2^n - 1} \\ &\leq |\alpha| \cdot \left(n \cdot \max_{i \in [n]} |\sqrt{a_i}|\right)^{2^n - 1} \\ &\leq |\alpha| \cdot \left(n \cdot 2^{n/2}\right)^{2^n - 1} \end{aligned}$$

Since $N(\alpha) \in \mathbb{Z}$, this implies $\alpha \geq 2^{-2^{O(n)}}$

Separation Bounds

- The minimal polynomial of $\alpha = \sum_{i=1}^{n} \delta_i \sqrt{a_i}$ has degree $d \leq 2^n$ (since $[\mathbb{Q}[\sqrt{a_1}, \ldots, \sqrt{a_i}] : \mathbb{Q}[\sqrt{a_1}, \ldots, \sqrt{a_{i-1}}] \leq 2$).
- If $\alpha \neq 0$, then

$$\begin{aligned} N(\alpha) &= \prod_{\sigma \in Gal(\mathbb{Q}(\sqrt{a_1},\ldots,\sqrt{a_n})/\mathbb{Q})} \sigma(\alpha) \\ &\leq |\alpha| \cdot |\sigma(\alpha)|^{2^n - 1} \\ &\leq |\alpha| \cdot (n \cdot \max_{i \in [n]} |\sqrt{a_i}|)^{2^n - 1} \\ &\leq |\alpha| \cdot (n \cdot 2^{n/2})^{2^n - 1} \end{aligned}$$

  Since $N(\alpha) \in \mathbb{Z}$, this implies $\alpha \geq 2^{-2^{O(n)}}$
- Approximate α to $2^{O(n)}$ bits – and each $\sqrt{a_i}$ to $2^{O(n)}$ bits of precision suffices.

Separation Bounds

- The minimal polynomial of $\alpha = \sum_{i=1}^{n} \delta_i \sqrt{a_i}$ has degree $d \leq 2^n$ (since $[\mathbb{Q}[\sqrt{a_1}, \ldots, \sqrt{a_i}] : \mathbb{Q}[\sqrt{a_1}, \ldots, \sqrt{a_{i-1}}] \leq 2$).
- Approximate α to $2^{O(n)}$ bits – and each $\sqrt{a_i}$ to $2^{O(n)}$ bits of precision suffices.
- *Root separation bound (Mignotte'82).* If $p(x) = \sum_{i=0}^{d} a_i x^i \in \mathbb{Z}[x]$, then we have

$$|r_1 - r_2| \geq \frac{\sqrt{3}}{d^{d/2+1}(dH)^{d-1}}$$

where $H = \sqrt{\sum_{i=1}^{n} a_i^2}$.

Prior Work

- **Tiwari (1992)** SSR has an efficient algorithm in the real RAM model of computation (supports unit cost arithmetic): approximate each $\sqrt{a_i}$ up to $2^{O(n)}$ bits via n steps of Newton's method:

$$x_{t+1} = \frac{1}{2}\left(x_t + \frac{a_i}{x_t}\right)$$

Prior Work

- **Tiwari (1992)** SSR has an efficient algorithm in the real RAM model of computation (supports unit cost arithmetic): approximate each $\sqrt{a_i}$ up to $2^{O(n)}$ bits via n steps of Newton's method:

$$x_{t+1} = \frac{1}{2}\left(x_t + \frac{a_i}{x_t}\right)$$

- **Allender et al. (2006).** Newton's method gives a reduction of SSR to PosSLP (check if the number given by a straightline program is positive) which can be checked using $poly(n)$ space.

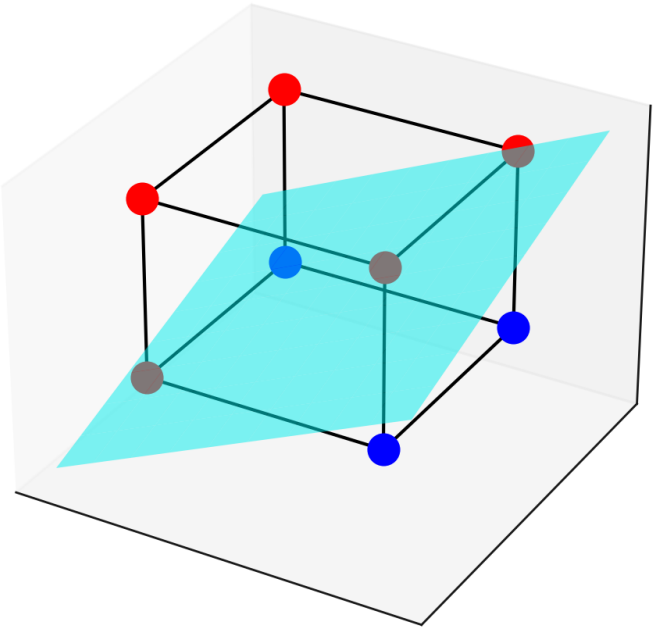
Prior Work

- **Tiwari (1992)** SSR has an efficient algorithm in the real RAM model of computation (supports unit cost arithmetic): approximate each $\sqrt{a_i}$ up to $2^{O(n)}$ bits via n steps of Newton's method:

$$x_{t+1} = \frac{1}{2}\left(x_t + \frac{a_i}{x_t}\right)$$

- **Allender et al. (2006).** Newton's method gives a reduction of SSR to PosSLP (check if the number given by a straightline program is positive) which can be checked using $poly(n)$ space.
- **SSR-hardness:** Feasibility of Semidefinite Programs (Goemans'98), Approximating 3-player Nash Equilibria (Etessami-Yannakakis'07), Solving systems of monotone polynomial systems (Esparaza-Kiefer-Luttenberger'08).

A different point of view

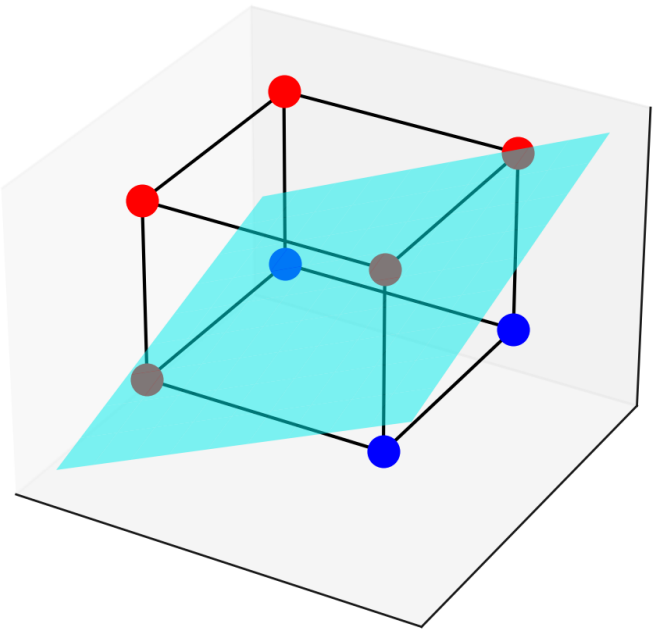


SSR

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

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

A different point of view



SSR

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

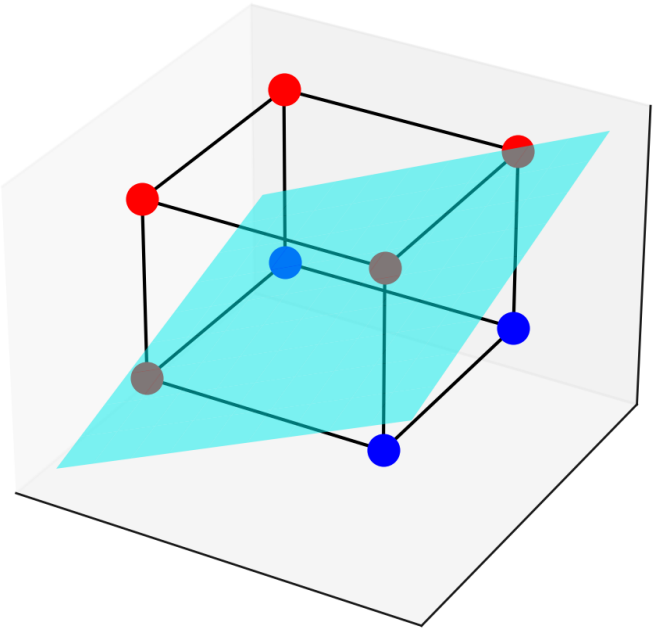
Output: $\operatorname{sgn}\left(\sum_{i=1}^{n} \delta_i \sqrt{a_i}\right)$

LTF (Perceptrons)

A Boolean function $f : \{\pm 1\}^n \to \{\pm 1\}$ is a Linear Threshold Function (LTF) if $\exists w_1, \ldots, w_n, \theta \in \mathbb{R}$ such that $\forall x \in \{\pm 1\}^n$

$$f(x) = 1 \iff \sum_{i=1}^{n} w_i x_i - \theta > 0$$

A different point of view



SSR = Evaluating a specific LTF at a point on the Boolean hypercube!

SSR

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

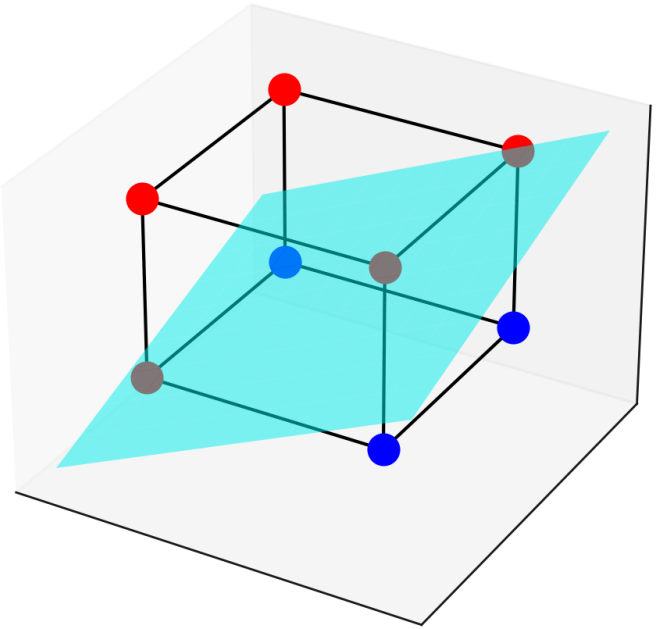
Output: $\operatorname{sgn}\left(\sum_{i=1}^{n} \delta_i \sqrt{a_i}\right)$

LTF (Perceptrons)

A Boolean function $f : \{\pm 1\}^n \to \{\pm 1\}$ is a Linear Threshold Function (LTF) if $\exists w_1, \ldots, w_n, \theta \in \mathbb{R}$ such that $\forall x \in \{\pm 1\}^n$

$$f(x) = 1 \iff \sum_{i=1}^{n} w_i x_i - \theta > 0$$

A different point of view



SSR = Evaluating a specific LTF at a point on the Boolean hypercube!

Do you need real numbers to define an LTF?

SSR

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

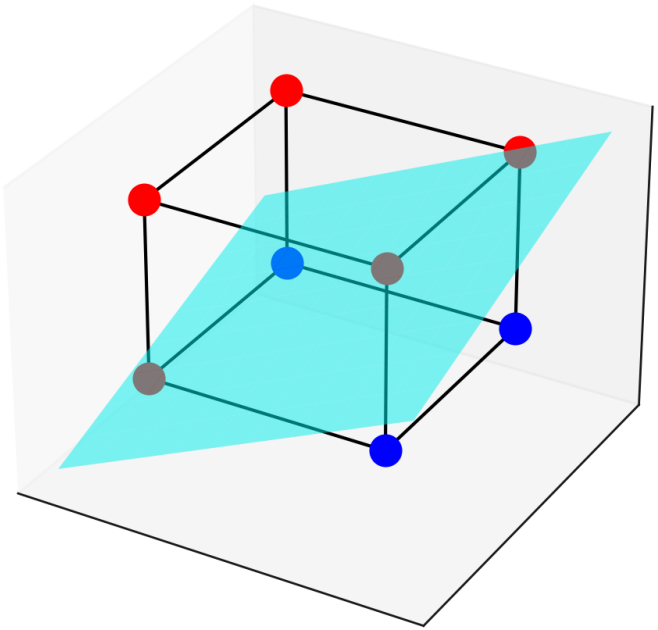
Output: $\operatorname{sgn}\left(\sum_{i=1}^{n} \delta_i \sqrt{a_i}\right)$

LTF (Perceptrons)

A Boolean function $f : \{\pm 1\}^n \to \{\pm 1\}$ is a Linear Threshold Function (LTF) if $\exists w_1, \ldots, w_n, \theta \in \mathbb{R}$ such that $\forall x \in \{\pm 1\}^n$

$$f(x) = 1 \iff \sum_{i=1}^{n} w_i x_i - \theta > 0$$

Linear Threshold functions

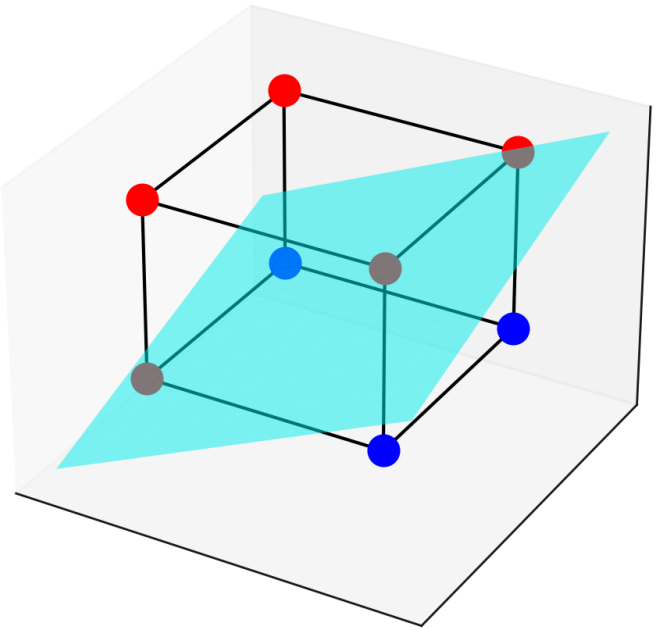


- Let $\varepsilon = min_{x \in \{\pm 1\}^n}(\langle w, x \rangle - \theta) \neq 0$
- Consider for all i, $(\frac{w_i - \varepsilon}{10n}, \frac{w_i + \varepsilon}{10n})$: if you pick w_i' in this interval, then $\forall x \in \{\pm 1\}^n$, $sgn\left(\sum_{i=1}^n w_i x_i - \theta\right) = sgn\left(\sum_{i=1}^n w_i x_i - \theta\right)$ (why?)
- But how small can ε be? If w_i are algebraic, again depends on root separation bounds!
- Can we have w_i' with the above property but with small bit-length (e.g., $poly(n)$ bits?)

Theorem (Muroga'71)

There exist $w_i' \in \mathbb{Z}$ of magnitude at most $2^{O(n \log n)}$ (i.e., representable in $O(n \log n)$ bits)

Linear Threshold functions

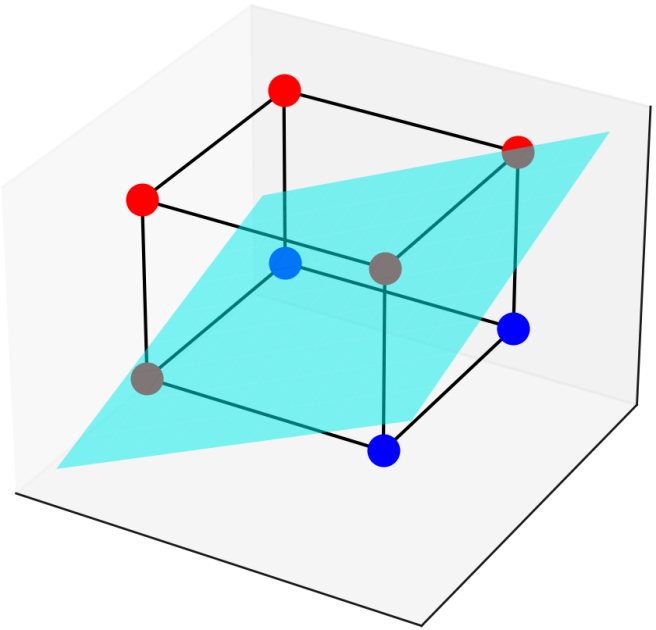


- Let $\varepsilon = min_{x \in \{\pm 1\}^n}(\langle w, x \rangle - \theta) \neq 0$
- Consider for all i, $(\frac{w_i - \varepsilon}{10n}, \frac{w_i + \varepsilon}{10n})$: if you pick w_i' in this interval, then $\forall x \in \{\pm 1\}^n$, $sgn\left(\sum_{i=1}^n w_i x_i - \theta\right) = sgn\left(\sum_{i=1}^n w_i x_i - \theta\right)$ (why?)
- But how small can ε be? If w_i are algebraic, again depends on root separation bounds!
- Can we have w_i' with the above property but with small bit-length (e.g., $poly(n)$ bits?)

Theorem (Muroga'71)

There exist $w_i' \in \mathbb{Z}$ of magnitude at most $2^{O(n \log n)}$ (i.e., representable in $O(n \log n)$ bits)

Linear Threshold functions

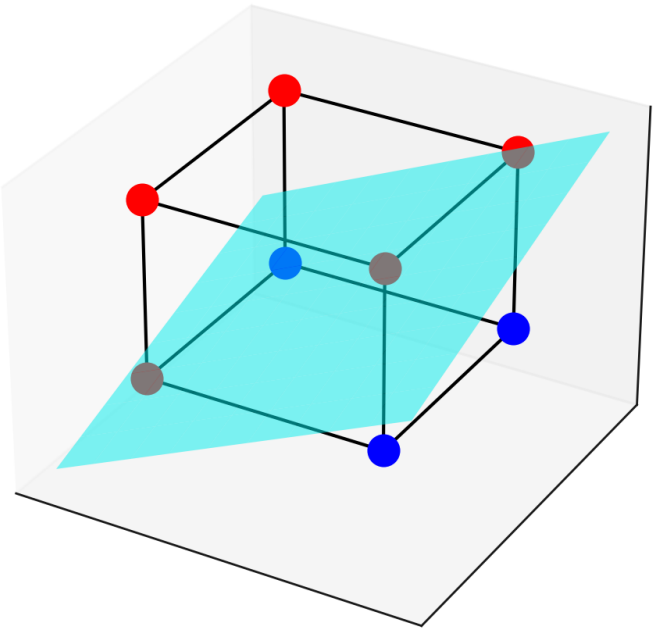


- Let $\varepsilon = min_{x \in \{\pm 1\}^n}(\langle w, x \rangle - \theta) \neq 0$
- Consider for all i, $(\frac{w_i - \varepsilon}{10n}, \frac{w_i + \varepsilon}{10n})$: if you pick w_i' in this interval, then $\forall x \in \{\pm 1\}^n$, $sgn\left(\sum_{i=1}^n w_i x_i - \theta\right) = sgn\left(\sum_{i=1}^n w_i x_i - \theta\right)$ (why?)
- But how small can ε be? If w_i are algebraic, again depends on root separation bounds!
- Can we have w_i' with the above property but with small bit-length (e.g., $poly(n)$ bits?)

Theorem (Muroga'71)

There exist $w_i' \in \mathbb{Z}$ of magnitude at most $2^{O(n \log n)}$ (i.e., representable in $O(n \log n)$ bits)

Linear Threshold functions

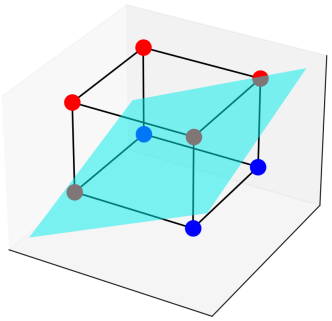


- Let $\varepsilon = min_{x \in \{\pm 1\}^n}(\langle w, x \rangle - \theta) \neq 0$
- Consider for all i, $(\frac{w_i - \varepsilon}{10n}, \frac{w_i + \varepsilon}{10n})$: if you pick w_i' in this interval, then $\forall x \in \{\pm 1\}^n$, $sgn\left(\sum_{i=1}^n w_i x_i - \theta\right) = sgn\left(\sum_{i=1}^n w_i x_i - \theta\right)$ (why?)
- But how small can ε be? If w_i are algebraic, again depends on root separation bounds!
- Can we have w_i' with the above property but with small bit-length (e.g., $poly(n)$ bits?)

Theorem (Muroga'71)

There exist $w_i' \in \mathbb{Z}$ of magnitude at most $2^{O(n \log n)}$ (i.e., representable in $O(n \log n)$ bits)

Linear Threshold Functions

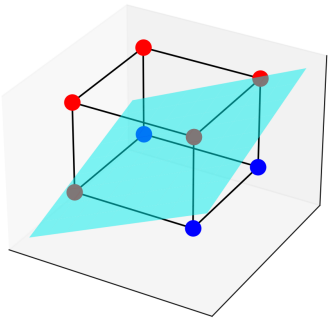


- Consider LTF $f : \{\pm 1\}^3 \to \{\pm 1\}$ given by $f(x) = 1 \iff w_1 x_1 + w_2 x_2 + w_3 x_3 \geq \theta$. where $w_i \in \mathbb{R}$.
- Consider the following LP (defined from the LTF):

$$\begin{aligned} \{-1,-1,-1\}: \quad & -z_1 - z_2 - z_3 \quad \geq 1 \\ \{-1,-1,+1\}: \quad & -z_1 - z_2 + z_3 \quad \leq -1 \\ & \dots \qquad\qquad \dots \\ & \dots \qquad\qquad \dots \\ \{+1,+1,+1\}: \quad & z_1 + z_2 + z_3 \quad \bowtie \pm 1 \end{aligned}$$

- LP is feasible: $z_i = w_i/\theta$ (if $\theta \neq 0$, else $z_i = w_i/\varepsilon$) is a solution.
- There exists a *basic feasible solution* (a vertex of the polytope)!
- Solve the 3×3 linear system: $Az = b$: All entries come from $\{-1, 1\} \implies$ By Cramer's rule, $z_i = p/q$ where $|p|, |q| \leq 3!$

Linear Threshold Functions

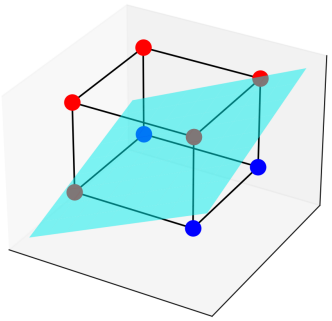


- Consider LTF $f : \{\pm 1\}^3 \to \{\pm 1\}$ given by $f(x) = 1 \iff w_1 x_1 + w_2 x_2 + w_3 x_3 \geq \theta$. where $w_i \in \mathbb{R}$.
- Consider the following LP (defined from the LTF):

$$\begin{aligned}
\{-1,-1,-1\}: &\quad -z_1 - z_2 - z_3 &&\geq 1\\
\{-1,-1,+1\}: &\quad -z_1 - z_2 + z_3 &&\leq -1\\
&\quad \dots &&\dots\\
&\quad \dots &&\dots\\
\{+1,+1,+1\}: &\quad z_1 + z_2 + z_3 &&\bowtie \pm 1
\end{aligned}$$

- LP is feasible: $z_i = w_i/\theta$ (if $\theta \neq 0$, else $z_i = w_i/\varepsilon$) is a solution.
- There exists a *basic feasible solution* (a vertex of the polytope)!
- Solve the 3×3 linear system: $Az = b$: All entries come from $\{-1, 1\} \implies$ By Cramer's rule, $z_i = p/q$ where $|p|, |q| \leq 3!$

Linear Threshold Functions

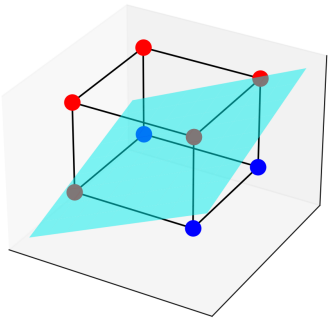


- Consider LTF $f : \{\pm 1\}^3 \to \{\pm 1\}$ given by $f(x) = 1 \iff w_1x_1 + w_2x_2 + w_3x_3 \geq \theta$. where $w_i \in \mathbb{R}$.
- Consider the following LP (defined from the LTF):

$$\begin{aligned} \{-1,-1,-1\}: &\quad -z_1 - z_2 - z_3 &&\geq 1 \\ \{-1,-1,+1\}: &\quad -z_1 - z_2 + z_3 &&\leq -1 \\ &\quad \dots &&\dots \\ &\quad \dots &&\dots \\ \{+1,+1,+1\}: &\quad z_1 + z_2 + z_3 &&\bowtie \pm 1 \end{aligned}$$

- LP is feasible: $z_i = w_i/\theta$ (if $\theta \neq 0$, else $z_i = w_i/\varepsilon$) is a solution.
- There exists a *basic feasible solution* (a vertex of the polytope)!
- Solve the 3×3 linear system: $Az = b$: All entries come from $\{-1, 1\} \implies$ By Cramer's rule, $z_i = p/q$ where $|p|, |q| \leq 3!$

Linear Threshold Functions

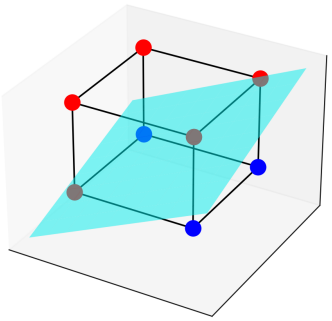


- Consider LTF $f : \{\pm 1\}^3 \to \{\pm 1\}$ given by $f(x) = 1 \iff w_1 x_1 + w_2 x_2 + w_3 x_3 \geq \theta$. where $w_i \in \mathbb{R}$.
- Consider the following LP (defined from the LTF):

$$\begin{aligned} \{-1,-1,-1\}: &\quad -z_1 - z_2 - z_3 &&\geq 1 \\ \{-1,-1,+1\}: &\quad -z_1 - z_2 + z_3 &&\leq -1 \\ &\quad \dots &&\dots \\ &\quad \dots &&\dots \\ \{+1,+1,+1\}: &\quad z_1 + z_2 + z_3 &&\bowtie \pm 1 \end{aligned}$$

- LP is feasible: $z_i = w_i/\theta$ (if $\theta \neq 0$, else $z_i = w_i/\varepsilon$) is a solution.
- There exists a *basic feasible solution* (a vertex of the polytope)!
- Solve the 3×3 linear system: $Az = b$: All entries come from $\{-1, 1\} \implies$ By Cramer's rule, $z_i = p/q$ where $|p|, |q| \leq 3!$

Linear Threshold Functions

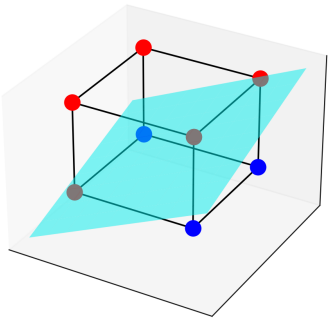


- Consider LTF $f : \{\pm 1\}^3 \to \{\pm 1\}$ given by $f(x) = 1 \iff w_1x_1 + w_2x_2 + w_3x_3 \geq \theta$. where $w_i \in \mathbb{R}$.
- Consider the following LP (defined from the LTF):

$$\begin{aligned} \{-1,-1,-1\}: &\quad -z_1 - z_2 - z_3 &&\geq 1 \\ \{-1,-1,+1\}: &\quad -z_1 - z_2 + z_3 &&\leq -1 \\ &\quad \dots &&\dots \\ &\quad \dots &&\dots \\ \{+1,+1,+1\}: &\quad z_1 + z_2 + z_3 &&\bowtie \pm 1 \end{aligned}$$

- LP is feasible: $z_i = w_i/\theta$ (if $\theta \neq 0$, else $z_i = w_i/\varepsilon$) is a solution.
- There exists a *basic feasible solution* (a vertex of the polytope)!
- Solve the 3×3 linear system: $Az = b$: All entries come from $\{-1, 1\} \implies$ By Cramer's rule, $z_i = p/q$ where $|p|, |q| \leq 3!$

Linear Threshold Functions



- Consider LTF $f : \{\pm 1\}^3 \to \{\pm 1\}$ given by $f(x) = 1 \iff w_1 x_1 + w_2 x_2 + w_3 x_3 \geq \theta$. where $w_i \in \mathbb{R}$.
- Consider the following LP (defined from the LTF):

$$\begin{aligned} \{-1,-1,-1\}: &\quad -z_1 - z_2 - z_3 &&\geq 1 \\ \{-1,-1,+1\}: &\quad -z_1 - z_2 + z_3 &&\leq -1 \\ &\quad \dots &&\dots \\ &\quad \dots &&\dots \\ \{+1,+1,+1\}: &\quad z_1 + z_2 + z_3 &&\bowtie \pm 1 \end{aligned}$$

- LP is feasible: $z_i = w_i/\theta$ (if $\theta \neq 0$, else $z_i = w_i/\varepsilon$) is a solution.
- There exists a *basic feasible solution* (a vertex of the polytope)!
- Solve the 3×3 linear system: $Az = b$: All entries come from $\{-1, 1\} \implies$ By Cramer's rule, $z_i = p/q$ where $|p|, |q| \leq 3!$

Ok, so what?

- For any given input $(a_1, \ldots, a_n)$ you could make 2^n different SSR instances (by varying $\Delta = (\delta_1, \ldots \delta_n)$). If you can solve SSR for a specific set of $\Delta_1, \ldots, \Delta_n \in \{\pm 1\}^n$ (those that correspond to basic feasible solution) you can solve SSR efficiently for all the other instances!

Ok, so what?

- For any given input $(a_1, \ldots, a_n)$ you could make 2^n different SSR instances (by varying $\Delta = (\delta_1, \ldots \delta_n)$). If you can solve SSR for a specific set of $\Delta_1, \ldots, \Delta_n \in \{\pm 1\}^n$ (those that correspond to basic feasible solution) you can solve SSR efficiently for all the other instances!
- Works for linear combinations of arbitrary (but fixed) set of real (even transcendental) numbers, for eg. $\sum_{i=1}^{n} \delta_i (\pi e)^i$ where $\delta_i \in \{-d, \ldots, d\}$

Ok, so what?

- For any given input $(a_1, \ldots, a_n)$ you could make 2^n different SSR instances (by varying $\Delta = (\delta_1, \ldots \delta_n)$). If you can solve SSR for a specific set of $\Delta_1, \ldots, \Delta_n \in \{\pm 1\}^n$ (those that correspond to basic feasible solution) you can solve SSR efficiently for all the other instances!

USSR

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

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

Ok, so what?

- For any given input $(a_1, \ldots, a_n)$ you could make 2^n different SSR instances (by varying $\Delta = (\delta_1, \ldots \delta_n)$). If you can solve SSR for a specific set of $\Delta_1, \ldots, \Delta_n \in \{\pm 1\}^n$ (those that correspond to basic feasible solution) you can solve SSR efficiently for all the other instances!

USSR

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

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

Theorem

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

Summary

- **Open Question:** Is there a short *witness* to test if a linear combination of square roots is positive? (i.e, is SSR in NP?

Summary

- **Open Question:** Is there a short *witness* to test if a linear combination of square roots is positive? (i.e, is SSR in NP?
- **Open Question 2:** Can we have better root separation/norm distribution bounds for linear combination of radicals?

Summary

- **Open Question:** Is there a short *witness* to test if a linear combination of square roots is positive? (i.e, is SSR in NP?
- **Open Question 2:** Can we have better root separation/norm distribution bounds for linear combination of radicals?

Summary

- **Open Question:** Is there a short *witness* to test if a linear combination of square roots is positive? (i.e, is SSR in NP?
- **Open Question 2:** Can we have better root separation/norm distribution bounds for linear combination of radicals?

Summary

- **Open Question:** Is there a short *witness* to test if a linear combination of square roots is positive? (i.e, is SSR in NP?
- **Open Question 2:** Can we have better root separation/norm distribution bounds for linear combination of radicals?

Summary

- **Open Question:** Is there a short *witness* to test if a linear combination of square roots is positive? (i.e, is SSR in NP?
- **Open Question 2:** Can we have better root separation/norm distribution bounds for linear combination of radicals?

Thank You!