# An Improved Bound on Sums of Square Roots via the Subspace Theorem

**Friedrich Eisenbrand**
EPFL, Lausanne, Switzerland

**Matthieu Haeberle**
EPFL, Lausanne, Switzerland

**Neta Singer**
EPFL, Lausanne, Switzerland

## Abstract

The *sum of square roots* is as follows: Given $x_1, \ldots, x_n \in \mathbb{Z}$ and $a_1, \ldots, a_n \in \mathbb{N}$ decide whether $E = \sum_{i=1}^n x_i \sqrt{a_i} \geq 0$. It is a prominent open problem (Problem 33 of the *Open Problems Project*), whether this can be decided in polynomial time. The state-of-the-art methods rely on separation bounds, which are lower bounds on the minimum nonzero absolute value of $E$. The current best bound shows that $|E| \geq (n \cdot \max_i(|x_i| \cdot \sqrt{a_i}))^{-2^n}$, which is doubly exponentially small.

We provide a new bound of the form $|E| \geq \gamma \cdot (n \cdot \max_i |x_i|)^{-2n}$ where $\gamma$ is a constant depending on $a_1, \ldots, a_n$. This is singly exponential in $n$ for fixed $a_1, \ldots, a_n$. The constant $\gamma$ is not explicit and stems from the *subspace theorem*, a deep result in the *geometry of numbers*.

**2012 ACM Subject Classification** Theory of computation → Computational geometry; Theory of computation → Algebraic complexity theory

**Keywords and phrases** Exact computing, Separation Bounds, Computational Geometry, Geometry of Numbers

**Digital Object Identifier** 10.4230/LIPIcs.SoCG.2024.54

## 1 Introduction

Several geometric optimization problems such as *euclidean traveling salesman* or *euclidean shortest path*, rely on comparisons of *sums of square roots*, which is a decision problem as follows. Given integers $x_1, \ldots, x_n \in \mathbb{Z}$ and positive integers $a_1, \ldots, a_n \in \mathbb{N}$ decide whether

$$E = \sum_{i=1}^n x_i \sqrt{a_i} \geq 0. \tag{1}$$

While the decision problem (1) is easy to state, it is not known to be decidable in polynomial time on a Turing machine, nor is it known to be NP [13], see also [1, 10, 20]. The best known complexity class containing the decision problem (1) is PSPACE. This follows by modeling the decision as a problem in the *existential theory of the reals* for which a PSPACE-algorithm exists [6, 22]. The *zero test* (when $\geq 0$ is replaced by $= 0$) can be decided in polynomial time with an algorithm of Blömer [3, 4].

The state-of-the-art method to decide (1) is based on *separation bounds*, see, e.g. [18]. Separation bounds are lower bounds on the absolute value of $E$, defined in (1), when it is nonzero. The best known bound in our setting is by Burnikel et al. [5]. The bound follows from the fact that the product of the *conjugates*, see, e.g. [16], of $E$ is an integer. Each conjugate of $E$ is of the form

$$\sum_{i=1}^n y_i \cdot x_i \sqrt{a_i}, \quad y \in \{\pm 1\}^n,$$


40th International Symposium on Computational Geometry (SoCG 2024).
Editors: Wolfgang Mulzer and Jeff M. Phillips; Article No. 54; pp. 54:1–54:8
Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

of absolute value bounded by $n \max_i (|x_i|\sqrt{a_i})$. This implies that

$$|E| \geq \left(n \max_i \left(|x_i|\sqrt{a_i}\right)\right)^{-(2^n-1)} \tag{2}$$

whenever $E \neq 0$. It follows that (1) can be decided with an approximation of the numbers $x_i\sqrt{a_i}$ in which $\mathcal{O}\left[2^n \log\left(n \max_i \left(|x_i|\sqrt{a_i}\right)\right)\right]$ bits of the respective fractional parts are correct. This bound is exponential in $n$.

On the other hand, there is no empirical evidence [8] that the reciprocal $1/|E|$ can be doubly exponential in $n$. The best empirical lower bounds [21] observed for $1/|E|$ are of the form $(\max_i a_i)^{\Omega(n)}$. The question of whether singly-exponential separation bounds for $|E|$ exist, is a highly visible open problem in computing [20], see also [9, Problem 33].

## Contribution of this paper

Our main result is a new separation bound for $|E|$ that shows single-exponential dependence on $n$ if $a_1, \ldots, a_n$ are fixed. More precisely, we show the following.

**i)** If $E \neq 0$, then

$$|E| \geq \left(\frac{1}{n \cdot \|x\|_\infty}\right)^{2n} \cdot \gamma, \text{ where } \gamma \in \mathbb{R}_+ \text{ is a constant depending on } \sqrt{a_1}, \ldots, \sqrt{a_n}.$$

Compared to the bound (2) of Burnikel et al. this decreases the dependence on $\|x\|_\infty$ from doubly exponential in $n$ to exponential. The new bound is obtained by applying tools and concepts from the *geometry of numbers* such as *lattices*, *Minkowski's first and second theorem*, and Schmidt's [23] celebrated *subspace theorem*. This bound is asymptotically tight with respect to the exponent of $\|x\|_\infty$ in the following sense.

**ii)** For each $L \in \mathbb{N}_{\geq 2}$ there exists $x \in \mathbb{Z}^n$, $x \neq 0$ with $\|x\|_\infty \leq L$ with

$$0 < |E| \leq \frac{n \max_i \sqrt{a_i}}{L^{n-1}}.$$

This bound follows form the pigeon-hole principle, similar to its application to the *number-balancing problem* [15, 14].

▶ Remark. The format of Problem 33 in [9] differs slightly from the problem description (1) in this paper. Using our notation, Problem 33 requires $n$ to be even and $x_i \in \{\pm 1\}$ for $i = 1, \ldots, n$. Furthermore exactly half of the $x_i$ are positive one. However, the question whether the logarithm of the reciprocal of the best separation bound is exponential or sub-exponential in $n$ is equivalent in both settings. The problem (1) can be reformulated in the format of Problem 33 by replacing $x_i\sqrt{a_i}$ with $x_i \neq 0$ with $(x_i/|x_i|)\sqrt{x_i^2 a_i}$ and doubling $n$ if necessary.

## Simplifying assumptions

Before we develop the connection of separation bounds for (1) to the geometry of numbers, we justify simplifying assumptions on the input of (1). If some $a_i$ is divisible by a square $y^2$ with $y \in \mathbb{N} \setminus \{0, 1\}$, then $a_i$ can be replaced by $a_i/y^2$ as long as $x_i$ is replaced by $x_i \cdot y$. Furthermore, if $a_i = a_j$ for $i \neq j$, then we can delete $a_j$ and replace $x_i$ with $x_i + x_j$, thereby reducing the dimension $n$ that appears in the exponent of our bound. We can therefore assume, without loss of generality, that each $a_i \in \mathbb{N}$ is *square-free* and that the $a_i$ are *distinct*. We recall the following fact (see e.g. Theorem 2 in [2]).

▶ **Theorem 1.** *Let $a_1, \dots, a_n \in \mathbb{N}_+$ be distinct square-free integers. The set*

$$\{\sqrt{a_1}, \dots, \sqrt{a_n}\}$$

*is linearly independent over the rational numbers $\mathbb{Q}$.*

## 2 Lattices and separation bounds

Let $A \in \mathbb{R}^{n\times n}$ be a matrix of full rank. The set $\Lambda(A) = \{Ax : x \in \mathbb{Z}^n\}$ is the *lattice* generated by the *(lattice) basis* $A$. If $A \in \mathbb{Q}^{n\times n}$ is rational, then the lattice $\Lambda(A)$ is rational. A *shortest vector* w.r.t. a norm $\|\cdot\|$ of a lattice $\Lambda \subseteq \mathbb{R}^n$ is a nonzero $v \in \Lambda$ of minimal norm. Lattices have been used in the context of computing separation bounds by Cheng et al. [8]. Here, the main idea is to consider the lattice generated by the basis

$$\begin{pmatrix} N & -N\sqrt{a_1} & \cdots & -N\sqrt{a_n} \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} \tag{3}$$

where $N \in \mathbb{N}_+$ is a positive integer. Suppose one is interested in the minimum absolute value of $E$ in (1) where the $x_i$ are bounded by one in absolute value. If the length of the shortest vector w.r.t. $\ell_2$ is larger than $\sqrt{n+1}$, then $1/N$ is a lower bound on $E$ in that case. Using algorithms for computing or approximating shortest vectors in the $\ell_2$-norm [17, 25] can then be used to find the smallest such $N$. The approach of Cheng et al. [8] is suitable for computing good lower bounds for large instances of the sum-of-square-roots problem.

Our approach is based on the dual of the lattice generated by (3). Recall that the *dual* lattice of $\Lambda \subseteq \mathbb{R}^n$ is the lattice

$$\Lambda^* = \{y \in \mathbb{R}^n : y^T v \in \mathbb{Z} \text{ for each } v \in \Lambda\}.$$

If $\Lambda$ is generated by $A \in \mathbb{R}^{n\times n}$, then $\Lambda^*$ is generated by $A^{-T}$, see, e.g. [7]. Let $Q = N^{1/(n+1)}$ and denote $\beta_i = \sqrt{a_i}$ for $i = 1, \dots, n$. The dual of the lattice generated by (3) is thus generated by the basis

$$B = \begin{pmatrix} 1/Q^{n+1} & & & \\ \beta_1 & 1 & & \\ \vdots & & \ddots & \\ \beta_n & & & 1 \end{pmatrix} \tag{4}$$

Let $\|\cdot\|$ be a norm and $i \in \{1, \dots, n\}$. The *$i$-th successive minimum* of $\Lambda$ is the smallest radius $R > 0$ such that $\{x \in \mathbb{R}^n : \|x\| \leq R\}$ contains $i$ linearly independent lattice vectors. $i$-th successive minimum is denoted by $\lambda_i$. In the following, we will restrict our attention to the successive minima w.r.t. the $\ell_\infty$-norm.

The absolute value of the determinant of any basis of a lattice $\Lambda \subseteq \mathbb{R}^n$ is an invariant of the lattice. It is called the *lattice determinant* and is denoted by $\det(\Lambda)$. The following is referred to as Minkowski's second theorem, which we state for the $\ell_\infty$-norm [19].

▶ **Theorem 2** (Minkowski's theorem for $\ell_\infty$)**.** *Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice. One has*

$$\lambda_1 \cdots \lambda_n \leq \det(\Lambda), \tag{5}$$

*where the successive minima $\lambda_i$ are with respect to the $\ell_\infty$-norm. In particular, one has*

$$\lambda_1 \leq \det(\Lambda)^{1/n}.$$

We now develop the connection between separation bounds for (1) and the theory described so far. Observe that the determinant of the lattice generated by the basis $B$ in (4) is $1/Q^{n+1}$ and that the dimension is $n+1$. Theorem 2 implies that $\Lambda(B)$ contains a nonzero lattice vector $v$ with $\|v\|_\infty \leq 1/Q$. If this bound is almost tight, then the value of $Q$ carries over to a separation bound for $E$ in (1). This is our next theorem.

▶ **Theorem 3.** *Consider*

$$E = \sum_{i=1}^{n} x_i \sqrt{a_i}$$

*with $a_1, \ldots, a_n \in \mathbb{N}$ and $x = (x_1, \ldots, x_n) \in \mathbb{Z}^n \setminus \{0\}$ and let $\Lambda(B)$ be the lattice generated by $B$ in (4).*

*If $Q \geq (2n\|x\|_\infty)^{3/2}$ and if $\lambda_1 \geq 1/Q^{1+\frac{1}{3n}}$, then*

$$|E| \geq \frac{1}{Q^{n+1}}. \tag{6}$$

**Proof.** Minkowski's second theorem gives the bound

$$\prod_{i=1}^{n+1} \lambda_i \leq \frac{1}{Q^{n+1}}. \tag{7}$$

Since $\lambda_1 \geq 1/Q^{1+\frac{1}{3n}}$ one has

$$\lambda_i \leq \frac{1}{Q^{2/3}} \text{ for each } i \in \{1, \ldots, n+1\}.$$

The successive minima are attained at $n+1$ linearly independent lattice vectors. Therefore, one of the successive minima is attained at a lattice vector

$$v = B \cdot \begin{pmatrix} q \\ -p \end{pmatrix}$$

with $q \in \mathbb{N}$ and $p = (p_1, \ldots, p_n)^T \in \mathbb{Z}^n$ such that $p^T x \neq 0$. Since $p^T x \in \mathbb{Z}$, one has

$$|p^T x| \geq 1. \tag{8}$$

The condition $\|v\|_\infty \leq 1/Q^{2/3}$ implies that

$$|q \cdot \beta_i - p_i| \leq \frac{1}{Q^{2/3}} \leq \frac{1}{2n\|x\|_\infty} \text{ for each } i \in \{1, \ldots, n+1\}.$$

By the triangle inequality,

$$|q\beta^T x - p^T x| \leq \frac{1}{2}$$

which, together with $|p^T x| \geq 1$ implies that

$$|\beta^T x| \geq \frac{1}{2q}. \tag{9}$$

On the other hand, $\|v\|_\infty \leq 1/Q^{2/3}$ implies that $q \leq Q^{n+\frac{1}{3}}$. The claim follows with (9) and since $2 \cdot Q^{n+\frac{1}{3}} \leq Q^{n+1}$ for $Q \geq (2n\|x\|_\infty)^{3/2} \geq 2^{3/2}$. ◀

▶ Remark. This proof generalizes the main idea of a technique of Frank and Tardos [12]. An integer vector $p \in \mathbb{Z}^n$ stemming from $(q, p^T) \in \mathbb{N} \times \mathbb{Z}^n$ that is a sufficiently good simultaneous approximation to a real vector $\beta \in \mathbb{R}^n$, separates the same set of integer points $y$ with bounded infinity norm, as long as $p^T y \neq 0$. We use this principle in (8), when all successive minima are sufficiently good approximations.

## Using the subspace theorem

We consider again a lattice vector in $v \in \Lambda(B)$

$$v = \begin{pmatrix} 1/Q^{n+1} & & & \\ \beta_1 & 1 & & \\ \vdots & & \ddots & \\ \beta_n & & & 1 \end{pmatrix} \cdot \begin{pmatrix} q \\ -p_1 \\ \vdots \\ -p_n \end{pmatrix} \tag{10}$$

with $q \in \mathbb{N}$ and $p = (p_1, \ldots, p_n)^T \in \mathbb{Z}^n$. Minkowski's bound $\lambda_1 \leq 1/Q$ implies the theorem of Dirichlet on *simultaneous Diophantine approximation* ([24] Chapter II Theorem 1A).

▶ **Theorem 4** (Dirichlet's Theorem)**.** *Given $\beta_1, \ldots, \beta_n \in \mathbb{R}$ and $Q \in \mathbb{N}_+$, there exist integers $q, p_1, \ldots, p_n \in \mathbb{Z}$ with*
**i)** *$1 \leq q \leq Q^n$ and*
**ii)** *$|q\beta_i - p_i| \leq 1/Q$ for $i = 1, \ldots, n$.*

The *subspace theorem* of Wolfgang Schmidt [23] implies a lower bound that is almost tight.

▶ **Theorem 5** (Theorem 1B in [24])**.** *Let $\beta_1, \ldots, \beta_n \in \mathbb{R}$ be real algebraic numbers such that $\{1, \beta_1, \ldots, \beta_n\}$ is linearly independent over $\mathbb{Q}$ and let $\delta > 0$. There are only finitely many positive integers $q \in \mathbb{N}_+$ such that*

$$q^{1+\delta} \operatorname{dist}_{\mathbb{Z}}(q \cdot \beta_1) \cdots \operatorname{dist}_{\mathbb{Z}}(q \cdot \beta_n) < 1.$$

Here $\operatorname{dist}_{\mathbb{Z}}(x)$ is the distance of the real number $x \in \mathbb{R}$ to the integers. It remains to show that there exists a good $Q$ satisfying the conditions of Theorem 3, which together with Theorem 5 will prove our main result.

▶ **Theorem 6.** *Consider*

$$E = \sum_{i=1}^{n} x_i \sqrt{a_i}$$

*with $a_1, \ldots, a_n \in \mathbb{N}$ and $x = (x_1, \ldots, x_n) \in \mathbb{Z}^n \setminus \{0\}$. There exists a constant $\gamma \in \mathbb{R}$ depending on $a_1, \ldots, a_n$ such that $E \neq 0$ implies*

$$|E| \geq \left( \frac{1}{n \cdot \|x\|_\infty} \right)^{2n} \cdot \gamma. \tag{11}$$

**Proof.** Following the arguments in Section 1 we can assume that the $a_i$ are distinct square-free integers. And assume for now that all $a_i$ are different from one. This implies that the set

$$\{1, \beta_1 = \sqrt{a_1}, \ldots, \beta_n = \sqrt{a_n}\}$$

is linearly independent over $\mathbb{Q}$. It remains to show that there exists some $Q_0 \in \mathbb{N}_+$ such that the first successive minimum $\lambda_1$ of the lattice $\Lambda(B)$ satisfies $\lambda_1 \geq 1/Q^{1+\frac{1}{3n}}$ for all $Q \geq Q_0$. The assertion then follows with Theorem 3 applied to $Q = (Q_0 \cdot (2n\|x\|_\infty)^{3/2})$. To this end, let $\delta = \frac{1}{3n}$ and suppose to the contrary that the first successive minimum of $\Lambda(B)$ satisfies

$$\lambda_1 \leq \frac{1}{Q^{1+\delta}}.$$

This means that there exists a $q \in \mathbb{N}_+$ with

i) $q \leq Q^{n-\delta}$ and
ii) $\mathrm{dist}_{\mathbb{Z}}(q\beta_i) \leq 1/Q^{1+\delta}$ for each $i \in \{1, \dots, n\}$.

The condition i) implies that

$$q^{1+\delta} \leq Q^{(n-\delta)(1+\delta)} < Q^{n(1+\delta)}.$$

Together with ii) this implies that

$$q^{1+\delta}\,\mathrm{dist}_{\mathbb{Z}}(q\beta_1)\cdots\mathrm{dist}_{\mathbb{Z}}(q\beta_n) < 1. \tag{12}$$

By Theorem 5, the number of integral $q$ verifying (12) is finite. Furthermore, given that $\beta_1$ is a square root of an integer, we have that

$$\frac{1}{q\cdot(2\beta_1+1)} \leq \mathrm{dist}_{\mathbb{Z}}(q\beta_1) \leq \frac{1}{Q^{1+\delta}}.$$

Therefore, $q$ is bounded from below by an increasing function of $Q$. As there are finitely many $q$ verifying (12), there are also finitely many $Q$ for which $\lambda_1 \leq \frac{1}{Q^{1+\delta}}$. Therefore, there exists a bound $Q_0$ such that for all $Q \geq Q_0$ the successive minimum $\lambda_1$ of $\Lambda(B)$ satisfies $\lambda_1 \geq 1/Q^{1+\frac{1}{3n}}$.

We now also consider the case $a_1$ is equal to 1. In this case, $\beta_1 = 1$ and the lattice basis $B$ is given by

$$B = \begin{pmatrix} 1/Q^{n+1} & & & & \\ 1 & 1 & & & \\ \beta_2 & & 1 & & \\ \vdots & & & \ddots & \\ \beta_n & & & & 1 \end{pmatrix}$$

It is easy to see that the first successive minimum of $\Lambda(B)$ remains the same upon deletion of the second row and column. Denote this updated basis by $B' \in \mathbb{R}^{n\times n}$. With exactly the same argument as above, it follows that there exists a $Q_0$ such that, for all $Q \geq Q_0$ one has $\lambda_1$ of $\Lambda(B')$ satisfies $\lambda_1 \geq 1/Q^{1+\frac{1}{3n}}$.

Finally, by choosing $Q = (Q_0 \cdot (2n\|x\|_\infty)^{3/2})$, we obtain the lower bound dependent on $Q_0$ and a single exponential in $n \cdot \|x\|_\infty$. Moreover, $Q_0$ depends only on the bound for the finitely many $q$ verifying the statement of Theorem 5. This means that $Q_0$ is a constant depending only on $a_1, \dots, a_n$. ◀

▶ Remark. The exponent $2n$ of equation (11) can be decreased to any $n+\epsilon$, with $\epsilon > 0$ using a suitable $\delta$ when applying Theorem 5. Note that this would affect the constant $\gamma$ by making it dependent on $\epsilon$.

## 3 An upper bound via number balancing

We now show asymptotic (almost) tightness of the bound on $|E|$ when $a_1, \dots, a_n$ are fixed and distinct square-free positive integers. Since $\sqrt{a_1}, \cdots, \sqrt{a_n}$ are linearly independent over $\mathbb{Q}$, $E$ is nonzero whenever $x \in \mathbb{Z}^n$ is not equal to zero. We show that there exist solutions asymptotically (almost) tight in $\|x\|_\infty$ via the pigeon-hole principle, as it is used in the *number balancing problem* [14, 15].

▶ **Theorem 7.** *Let $L \geq 2$. There exists a nonzero $x \in \mathbb{Z}^n$ with $\|x\|_\infty \leq L$ such that*

$$|E| \leq \frac{n \max_i \sqrt{a_i}}{L^{n-1}}.$$

**Proof.** Let $\beta = (\sqrt{a_1}, \ldots, \sqrt{a_n}) \in \mathbb{R}^n$. The number of vectors $y \in \mathbb{Z}^n$ such that $\|y\|_\infty \leq L/2$ holds is at most $L^n$. On the other hand one always has

$$|y^T \beta| \leq \frac{nL}{2} \max_i \sqrt{a_i}$$

for such vectors $y$. By the pigeon-hole principle, there exist $y_1 \neq y_2 \in \mathbb{Z}^n$ of infinity norms at most $L/2$ such that their corresponding values are close:

$$|y_1^T \beta - y_2^T \beta| \leq \frac{2nL}{2(L^n - 1)} \max_i \sqrt{a_i}.$$

The difference $x = y_1 - y_2$ hence verifies $\|x\|_\infty \leq L$ and the required bound. ◀

## 4 Discussion

The subspace theorem (Theorem 5) does not provide explicit bounds on the number of solutions $q \in \mathbb{N}_+$. The existing *quantitative* versions of the subspace theorem, see, e.g. [11], do not provide such bounds either. This is still the case when all algebraic numbers are square roots of integers. An explicit bound on the number of solutions would immediately apply to a separation bound for the sum of square roots.

In light of the relationship of the subspace theorem and separation bounds that we describe in this paper, it is an interesting open problem to find explicit upper and lower bounds on the number of solutions $q \in \mathbb{N}_+$ satisfying the equations of Theorem 5 for $\beta_i = \sqrt{a_i}$ and $\delta = 1/\operatorname{poly}(n)$.

## References


1 Eric Allender, Peter Bürgisser, Johan Kjeldgaard-Pedersen, and Peter Bro Miltersen. On the complexity of numerical analysis. *SIAM Journal on Computing*, 38(5):1987–2006, 2009.

2 Abram S Besicovitch. On the linear independence of fractional powers of integers. *Journal of the London Mathematical Society*, 1(1):3–6, 1940.

3 Johannes Blömer. Computing sums of radicals in polynomial time. In *Proceedings of the 32nd annual symposium on Foundations of computer science*, pages 670–677, 1991.

4 Johannes Blömer. A probabilistic zero-test for expressions involving roots of rational numbers. In *Algorithms – ESA'98: 6th Annual European Symposium Venice, Italy, August 24–26, 1998 Proceedings 6*, pages 151–162. Springer, 1998.

5 Christoph Burnikel, Rudolf Fleischer, Kurt Mehlhorn, and Stefan Schirra. A strong and easily computable separation bound for arithmetic expressions involving radicals. *Algorithmica*, 27(1):87–99, 2000.

6 John Canny. Some algebraic and geometric computations in pspace. In *Proceedings of the twentieth annual ACM symposium on Theory of computing*, pages 460–467, 1988.

7 John William Scott Cassels. *An introduction to the geometry of numbers*. Springer Science & Business Media, 2012.

8 Qi Cheng, Xianmeng Meng, Celi Sun, and Jiazhe Chen. Bounding the sum of square roots via lattice reduction. *Mathematics of computation*, 79(270):1109–1122, 2010.

9 Erik D. Demaine, Joseph S. B. Mitchell, and Joseph O'Rourke. The open problems project. `http://topp.openproblem.net/`.

10 Kousha Etessami and Mihalis Yannakakis. Recursive markov chains, stochastic grammars, and monotone systems of nonlinear equations. *Journal of the ACM (JACM)*, 56(1):1–66, 2009.

11 J-H Evertse and Roberto G Ferretti. A further improvement of the quantitative subspace theorem. *Annals of Mathematics*, pages 513–590, 2013.

12 András Frank and Éva Tardos. An application of simultaneous diophantine approximation in combinatorial optimization. *Combinatorica*, 7:49–65, 1987.
13 Michael R Garey, Ronald L Graham, and David S Johnson. Some np-complete geometric problems. In *Proceedings of the eighth annual ACM symposium on Theory of computing*, pages 10–22, 1976.
14 Rebecca Hoberg, Harishchandra Ramadas, Thomas Rothvoss, and Xin Yang. Number balancing is as hard as minkowski's theorem and shortest vector. In *International Conference on Integer Programming and Combinatorial Optimization*, pages 254–266. Springer, 2017.
15 Narendra Karmarkar and Richard M Karp. *The differencing method of set partitioning.* Computer Science Division (EECS), University of California Berkeley, 1982.
16 Serge Lang. *Algebra*, volume 211. Springer Science & Business Media, 2012.
17 Arjen K Lenstra, Hendrik Willem Lenstra, and László Lovász. Factoring polynomials with rational coefficients. *Mathematische annalen*, 261(ARTICLE):515–534, 1982.
18 Chen Li, Sylvain Pion, and Chee-Keng Yap. Recent progress in exact geometric computation. *The Journal of Logic and Algebraic Programming*, 64(1):85–111, 2005.
19 Hermann Minkowski. *Geometrie der Zahlen.* BG Teubner, 1910.
20 Joseph O'Rourke. Advanced problem 6369. *American Mathematical Monthly*, 88(10):769, 1981.
21 Jianbo Qian and Cao An Wang. How much precision is needed to compare two sums of square roots of integers? *Information Processing Letters*, 100(5):194–198, 2006.
22 James Renegar. A faster pspace algorithm for deciding the existential theory of the reals. Technical report, Cornell University Operations Research and Industrial Engineering, 1988.
23 Wolfgang M Schmidt. Norm form equations. *Annals of Mathematics*, 96(3):526–551, 1972.
24 Wolfgang M Schmidt. *Diophantine approximation.* Springer Science & Business Media, 1996.
25 Claus-Peter Schnorr. A hierarchy of polynomial time lattice basis reduction algorithms. *Theoretical computer science*, 53(2-3):201–224, 1987.