The Sixth International Symposium on Operations Research and Its Applications (ISORA'06)
Xinjiang, China, August 8–12, 2006
Copyright © 2006 ORSC & APORC, pp. 206–211

# An Optimal Bound for Sum of Square Roots of Special Type of Integers*

Jianbo Qian[1] Cao An Wang[2,†]

[1] Department of Computer Science, University of Waterloo, Ontario, Canada
[2] Department of Computer Science, Memorial University of Newfoundland,
St. John's, Newfoundland, Canada A1B 3X5

**Abstract** The *sum of square roots of integers* problem is to find the minimum nonzero difference between two sums of square roots of integers. Let $r(n,k)$ denote the minimum nonzero positive value: $|\sum_{i=1}^{k}\sqrt{a_i}-\sum_{i=1}^{k}\sqrt{b_i}|$, where $a_i$ and $b_i$ are positive integers not larger than integer $n$. We prove by an explicit construction that $r(n,k)=O(n^{-2k+\frac{3}{2}})$ for fixed $k$ and any $n$. Our result implies that in order to compare two sums of $k$ square roots of integers with at most $d$ digits per integer, one might need precision of as many as $(2k-\frac{3}{2})d$ digits. We also prove that this bound is optimal for a wide range of integers, *i.e.,* $r(n,k)=\Theta(n^{-2k+\frac{3}{2}})$ for fixed $k$ and for those integers in the form of $n=\binom{2k-1}{2i}^2(n'+2i)+\binom{2k-1}{2i+1}^2(n'+2i+1)$, where $n'$ is any integer satisfied the above form and $i$ is any integer in range $[0,2k-1]$.

## 1 Introduction

In order to find the optimal solution in an optimization problems, one frequently needs to compare the values of two arithmetic expressions. Each arithmetic expression represents a possible choice. This is actually similar to evaluate branch conditions in a computer program. As a consequence of incorrect result, a computation may follow an incorrect path. This may lead to catastrophic errors. For example in operations research, in order to design an efficient dispatch scheme for a taxi company in a city, one needs to compare the lengths of different routes, which is a geometric problem. In the realm of geometric computations, a route is a polygonal path. Moreover, paths are usually represented by sums of square roots of integers, where vertices are represented by integer coordinates. It is justified since in practice, integer coordinates of points are widely used in the implementation of geometric algorithms. In order to quickly determine the longer one of two such polygonal paths, one natural way is to compute them numerically. The correctness of this computation relies on the correct precision needed for identifying the difference. In complexity aspect, the

*This work is supported by NSERC grant OPG0041629.

†Correspondent author. E-mail: wang@cs.mun.ca

significance of this problem was indicated by David Eppstein [2]: “A major bottleneck in proving NP-completeness for geometric problems is a mismatch between the real-number and Turing machine models of computation: one is good for geometric algorithms but bad for reductions, and the other vice versa. Specifically, it is not known on Turing machines how to quickly compare a sum of distances (square roots of integers) with an integer or other similar sums, so even (decision versions of) easy problems such as the minimum spanning tree are not known to be in NP.” Therefore, this becomes a fundamental open problem in computational geometry [1].

The problem can be expressed in number-theoretic terms: what is the smallest nonzero number that is the difference of two sums of $k$ roots of integers not larger than some bound $n$? More precisely, find tight lower and upper bounds on $r(n,k)$, the minimum positive value of

$$\left|\sum_{i=1}^{k}\sqrt{a_i}-\sum_{i=1}^{k}\sqrt{b_i}\right|,$$

where $a_i$ and $b_i$ are integers not larger than $n$.

Examples [1] are:

$$r(20,2)\approx .0002=\sqrt{10}+\sqrt{11}-\sqrt{5}-\sqrt{18},$$
$$r(20,3)\approx .000005=\sqrt{5}+\sqrt{6}+\sqrt{18}-\sqrt{4}-\sqrt{12}-\sqrt{12}.$$

Historically speaking, the problem was formally posed by Joseph O’Rourke in 1981 [3], but it is likely an older problem since Ronald Graham had discussed it in some public lectures before. The problem is now included in “The Open Problems Project" as Problem 33: Sum of Square Roots [1].

Of particular importance is whether $\lg\frac{1}{r(n,k)}$ is bounded above by a polynomial in $k$ and $\lg n$. If this statement is true, then we can compare two sums of square roots of integers in polynomial time. Note that even though $\lg\frac{1}{r(n,k)}$ is not bounded by a polynomial in $k$ and $\lg n$, there may still exist polynomial-time algorithms to compare such two sums by other means.

A lower bound is implied through root-separation bounds [4]. When $k$ is fixed, the bound is that

$$r(n,k)=\Omega(n^{\frac{1}{2}-2^{2k-2}}).$$

To the authors’ best knowledge, the only known upper bound is $O(n^{-k+\frac{1}{2}})$ for fixed $k$ due to Ronald Graham [2], as an application of Prouhet-Tarry-Escott problem in number theory.

## 2 Our Results

Our idea for constructing this $O(n^{-2k+\frac{3}{2}})$ bound is based on the Taylor expansion, but we avoid using the solution of Prouhet-Tarry-Escott problem, which is hard to solve itself.

We can prove the following results.

**Lemma 1.** *Let $m(\geq 1)$ and $n'$ be integers. We have that*

$$\left|\sum_{i=0}^{m}\binom{m}{i}(-1)^i\sqrt{n'+i}\right| < \frac{(2m-3)!!}{2^m n'^{m-\frac{1}{2}}},$$

*where* $(2m-3)!! = 1\cdot 3\cdot \ldots \cdot (2m-3)$. *(we regard* $(-1)!!$ *as* $1$.*)*

**Proof.** First we prove the following recursive equality for $k \geq 1$, using combinatorial identity $i\binom{m}{i} = m\binom{m-1}{i-1}$: Let $s(m,j) = \sum_{i=0}^{m}\binom{m}{i}(-1)^i i^j$ for integers $m \geq 1$ and $j \geq 0$.

$$\begin{aligned}
s(m,k) =& \sum_{i=1}^{m} i\binom{m}{i}(-1)^i i^{k-1} \\
=& m\sum_{i=1}^{m}\binom{m-1}{i-1}(-1)^i i^{k-1} \\
=& m\sum_{i=1}^{m}\binom{m-1}{i-1}(-1)^i((i-1)+1)^{k-1} \\
=& m\sum_{i=1}^{m}\binom{m-1}{i-1}(-1)^i(\sum_{j=0}^{k-1}\binom{k-1}{j}(i-1)^j) \qquad \textbf{(binomial expansion)} \\
=& -m\sum_{l=0}^{m-1}\binom{m-1}{l}(-1)^l(\sum_{j=0}^{k-1}\binom{k-1}{j}l^j) \qquad \textbf{(let } l=i-1\textbf{)} \\
=& -m\sum_{j=0}^{k-1}\binom{k-1}{j}(\sum_{l=0}^{m-1}\binom{m-1}{l}(-1)^l l^j) \\
=& -m\sum_{j=0}^{k-1}\binom{k-1}{j}s(m-1,j).
\end{aligned}$$

Now we prove ome combinatorial identities:

(1) for $0 \leq j \leq m-1$, we have $s(m,j) = 0$ ($0^0$ is regarded as 1);

(2) $s(m,m) = (-1)^m m!$.

For (1), we prove it by induction on $j$. When $j = 0$, $s(m,0) = \sum_{i=0}^{m}\binom{m}{i}(-1)^i$ is exactly the binomial expansion of $(1-1)^m$, thus (1) holds for $m \geq 1$. We assume that $s(m,j) = 0$ holds for $0 \leq j \leq k-1$ and $m \geq k$, then for $j = k$ and $m \geq k+1$ by the recursive equality above we have

$$s(m,k) = -m\sum_{j=0}^{k-1}\binom{k-1}{j}s(m-1,j) = 0.$$

This proves (1).

Also by the recursive equality above:

$$s(m,m) = -m\sum_{j=0}^{m-1}\binom{m-1}{j}s(m-1,j) = (-m)\cdot s(m-1,m-1).$$

From this and the fact that $s(1,1) = -1$ we have

$$s(m,m) = (-1)^m m!.$$

Thus (2) is also proved.

For the proof of Lemma 1, let

$$f(n) = \frac{1}{\sqrt{n}}(\sum_{i=0}^{m}\binom{m}{i}(-1)^i\sqrt{n+i}) = \sum_{i=0}^{m}\binom{m}{i}(-1)^i\sqrt{1+\frac{i}{n}}.$$

Our idea is to prove that in its Taylor(or Maclaurin) expansion of $1/n$, all coefficients of the first $m-1$ terms are zero.

Function $\sqrt{1+x}$ can be expanded by Taylor's formula as:

$$\begin{aligned}\sqrt{1+x} =& 1 - \frac{1}{2}x + \frac{1}{8}x^2 - \frac{1}{16}x^3 + \cdots \\ &+ (-1)^{m-1}\frac{(2m-5)!!}{(2m-2)!!}x^{m-1} + (-1)^m\frac{(2m-3)!!}{(2m)!!}\xi^m \\ =& \sum_{j=0}^{m-1}(-1)^j\frac{(2j-3)!!}{(2j)!!}x^j + (-1)^m\frac{(2m-3)!!}{(2m)!!}\xi^m,\end{aligned}$$

where $0 < \xi < x$, $(2m-3)!! = 1\cdot 3\cdot \ldots \cdot(2m-3)$ and $(2m)!! = 2\cdot 4\cdot \ldots \cdot (2m)$.

For $0 \le j \le m$, let $c_j$ denote the coefficient of the $j$-th term in the Taylor expansion of $\sqrt{1+x}$, i.e. $c_j = (-1)^j\frac{(2j-3)!!}{(2j)!!}$. Let $M > n$ be some constant so that $0 \le \frac{i}{M} \le \frac{i}{n}$. By Taylor's formula we can expand $f(n)$ as

$$\begin{aligned}f(n) =& \sum_{i=0}^{m}\binom{m}{i}(-1)^i(\sum_{j=0}^{m-1}c_j(\frac{i}{n})^j) + \sum_{i=0}^{m}\binom{m}{i}(-1)^i c_m(\frac{i}{M})^m \\ =& \sum_{j=0}^{m-1}c_j(\sum_{i=0}^{m}\binom{m}{i}(-1)^i i^j)\frac{1}{n^j} + \sum_{i=0}^{m}\binom{m}{i}(-1)^i i^m c_m\frac{1}{M^m} \\ =& \sum_{j=0}^{m-1}c_j s(m,j)\frac{1}{n^j} + \frac{c_m s(m,m)}{M^m} \\ =& \frac{c_m(-1)^m m!}{M^m}.\end{aligned}$$

Thus we obtain

$$\begin{aligned}|\sum_{i=0}^{m}\binom{m}{i}(-1)^i\sqrt{n+i}| = \sqrt{n}|f(n)| = \sqrt{n}\frac{|c_m|m!}{M^m} \\ < \frac{|c_m|m!}{n^{m-\frac{1}{2}}} = \frac{m!(2m-3)!!}{(2m)!!n^{m-\frac{1}{2}}} = \frac{(2m-3)!!}{2^m n^{m-\frac{1}{2}}}.\end{aligned}$$

□

Using Lemma 1, we can prove the following theorem.

**Theorem 2.** $\left|\sum_{i=0}^{m}\binom{m}{i}(-1)^i\sqrt{n'+i}\right| = O((n')^{-m+\frac{1}{2}})$ *for fixed* $m \geq 1$.

In Theorem 1, let $m = 2k-1$, we have

$$\begin{aligned}&\left|\sum_{i=0}^{2k-1}\binom{2k-1}{i}(-1)^i\sqrt{n'+i}\right|\\ =&\left|(\sum_{i=0}^{k-1}\binom{2k-1}{2i}\sqrt{n'+2i})-(\sum_{i=0}^{k-1}\binom{2k-1}{2i+1}\sqrt{n'+2i+1})\right| \\ =&O((n')^{-2k+\frac{3}{2}}).\end{aligned} \tag{1}$$

By the definition of $r(n,k)$ and let $a_i = \binom{2k-1}{2i}^2(n'+2i)$ and $b_i = \binom{2k-1}{2i+1}^2(n'+2i+1)$ in (1) and note $n = O(n')$, we obtain the main result in this paper:

**Theorem 3.** $r(n,k) = O(n^{-2k+\frac{3}{2}})$ *for fixed* $k \geq 1$.

Note that the requirement that 'integer $a_i$ and $b_i$ are not larger than $n$ is satisfied as long as $k$ is fixed and $i$ is in range $[0,2k-1]$, and $n'$ is satisfied that $a_i = \binom{2k-1}{2i}^2(n'+2i)$ and $b_i = \binom{2k-1}{2i+1}^2(n'+2i+1)$.

One might wonder whether the upper bound of Theorem 2 can be improved by a more sophisticated type of linear combination in form of $\sum_{i=0}^{m}x_i\sqrt{n'+a_i}$.

The following theorem shows that such an improvement is impossible, which also implies that this bound is the best possible for the problem with the above mentioned specific type of integers.

**Theorem 4.** *Let* $m \geq 1$ *be a fixed integer, and let* $x_0, x_1, ..., x_m$ *and* $a_0, a_1, ..., a_m$ *be real numbers such that* $a_i \neq a_j$ *for* $0 \leq i \neq j \leq m$. *Let* $g(n') = \sum_{i=0}^{m}x_i\sqrt{n'+a_i}$. *Then* $|g(n')| = o((n')^{-m+\frac{1}{2}})(= o(n^{-m+\frac{1}{2}}))$ *if and only if* $x_i = 0$ *for* $0 \leq i \leq m$.

**Proof.** The 'If' part is trivial. Now we prove the 'Only If' part. Assume that $|g(n)| = |\sum_{i=0}^{m}x_i\sqrt{n+a_i}| = o(n^{-m+\frac{1}{2}})$, we shall show $x_i = 0$ for $0 \leq i \leq m$.

As in the proof of Lemma 1, for $0 \leq j \leq m$, let $c_j$ denote the coefficient of the $j$-th term in the Taylor series of $\sqrt{1+x}$, i.e.

$$\sqrt{1+x} = \sum_{j=0}^{m}c_jx^j + O(x^{m+1}).$$

We now can express $g(n)/\sqrt{n}$ as Taylor expansion of $a_i/n$ to its $m$-th term:

$$\begin{aligned}\frac{g(n)}{\sqrt{n}} =&\sum_{i=0}^{m}x_i\sqrt{1+\frac{a_i}{n}}\\ =&\sum_{i=0}^{m}x_i(\sum_{j=0}^{m}c_j(\frac{a_i}{n})^j + O(\frac{1}{n^{m+1}}))\end{aligned}$$

$$=\sum_{j=0}^{m} c_j(\sum_{i=0}^{m} x_i a_i{}^j)\frac{1}{n^j}+O(\frac{1}{n^{m+1}})$$

By the assumption that $|g(n)|=o(n^{-m+\frac{1}{2}})$, or equivalently $|g(n)/\sqrt{n}|=o(n^{-m})$, we have that

$$\sum_{i=0}^{m} x_i a_i{}^j=0$$

for $0\leq j\leq m$.

We can regard them as a group of $m+1$ equations for variables $(x_0,x_1,...,x_m)$, they have a non-zero solution if and only if the coefficient determinant $|a_i{}^j|_{0\leq i,j\leq m}$ is zero. But this is impossible since $|a_i{}^j|_{0\leq i,j\leq m}$ is exactly the Vandermonde Determinant of $(a_0,a_1,...,a_m)$, it is zero if and only if $a_i=a_j$ for some $0\leq i\neq j\leq m$. If $a_i=a_j$ for some $0\leq i\neq j\leq m$, then $g(n)$ cannot be bounded above by $o(n^{-m+\frac{1}{2}})$, a contradiction. Thus all $x_i$ must be zero. □

## References

[1] Erik D. Demaine, Joseph S. B. Mitchell and Joseph O'Rourke. The Open Problems Project, Problem 33: Sum of Square Roots. `http://cs.smith.edu/~orourke/TOPP/P33.html`.

[2] Usenet newsgroup sci.math 25 Dec 90. What is the minimum nonzero difference between two sums of square roots of integers? `http://www.ics.uci.edu/~eppstein/junkyard/small-dist.html`.

[3] Joseph O'Rourke. Advanced problem 6369. *Amer. Math. Monthly*, 88(10), 769, 1981.

[4] C. Burnikel, R. Fleischer, K. Mehlhorn and S. Schirra. A strong and easily computable separation bound for arithmetic expressions involving radicals. *Algorithmica*, 27(1), 87–99, 2000.

[5] Dana Angluin and Sarah Eisenstat. How close can $\sqrt{a}$ + $\sqrt{b}$ be to an integer? Manuscript in `ftp://ftp.cs.yale.edu/pub/TR/tr1279.pdf`.