EATCS BULLETIN NO. 28, FEB. 1986, PP. 16-20.

On the Question "Is $\sum_1^n \sqrt{a_i} \leq L$?"

(Preliminary Report)

Varol Akman and Wm. Randolph Franklin
Dept. of Electrical, Computer, and Systems Eng.
Rensselaer Polytechnic Institute
Troy, New York 12180, USA

1. Introduction

In [2] R.L. Graham asked the following question:

> Given n positive integers $a_1, \cdots, a_n$ and integer L, can we decide "Is $\sum_1^n \sqrt{a_i} \leq L$?" in time polynomial in n plus the number of bits needed to express the integers $a_1, \cdots, a_n$ and L ?

In this paper we summarize three approaches to this question. The first one is a straight algebraic manipulation which reduces the question to a question about the roots of a polynomial. The second approach is based on the identification of algebraic numbers. The last approach is known as Diophantine approximation and has close ties with continued fractions. Although we cannot rule out the possibility, our results show that an affirmative answer to the above question is highly unlikely. Throughout the paper, we shall only deal with the "equality" question. We think that the "less than" question is more difficult to answer although we do not currently have a proof of this.

2. Repeated Squaring

One approach to answer the equality question is to use repeated squaring to get rid of all the square roots. Let $\sum_1^n \sqrt{a_i} = x$. Assume that P_{n-1} is the polynomial with integral coefficients given in terms of a_i, $1 \leq i \leq n-1$, such that $P_{n-1}(\sum_1^{n-1} \sqrt{a_i}) = 0$. Then one obtains $P_{n-1}(x - \sqrt{a_n}) = 0$. Notice that when we make the last substitution, the only coefficients that are not integers would be made of several odd powers of $\sqrt{a_n}$. Clearly, all these terms can be written as $K\sqrt{a_n}$ where K is integer. Thus, P_n is obtained from P_{n-1} by just squaring to eliminate $\sqrt{a_n}$. $P_n(\sum_1^n \sqrt{a_i})$ is necessarily zero and all coefficients of P_n are integers in terms of a_i, $1 \leq i \leq n$. Furthermore, note that only the even powers of x are present in P_n.

EXAMPLE. Since $P_n(x)$ is of degree 2^n, we give only the first few polynomials (using a, b, c instead of a_1, a_2, a_3):

$$P_1(x) = x^2 - a$$

$$P_2(x)=x^4-2(a+b)x^2+(a-b)^2$$

$$\begin{aligned}P_3(x)=x^8&-4(a+b+c)x^6+(6(a^2+b^2+c^2)+4(ab+ac+bc))x^4\\&-(4(a^3+b^3+c^3)-4(a^2b+a^2c+b^2a+b^2c+c^2a+c^2b)+40abc)x^2\\&+(a^4+b^4+c^4-4(a^3b+a^3c+b^3a+b^3c+c^3a+c^3b)\\&+6(a^2b^2+a^2c^2+b^2c^2)-4(a^2bc+b^2ac+c^2ab))\end{aligned}$$

Once $P_n(x)$ is obtained we can answer the equality question by evaluating $P_n(L)$. Thus, for example, $\sqrt{2}+\sqrt{3}+\sqrt{5}+\sqrt{7}$ cannot be equal to 8 since for these numbers one can compute

$$\begin{aligned}P_4(x)=x^{16}&-136x^{14}+6476x^{12}-141912x^{10}+1513334x^8\\&-7453176x^6+13950764x^4-5596840x^2+46225\end{aligned}$$

which is not equal to zero at $x=8$. It is important to observe that one in fact very quickly detects this since 8 is not a divisor of the constant term 46225 of P_4. (Any rational root of a monic polynomial with integer coefficients must be an integer which is a divisor of its constant term.)

An important property of P_n is the following. All 2^n roots of P_n are real and symmetric about the origin. They are given as $\pm\sqrt{a_1}\pm\cdots\pm\sqrt{a_n}$. Fig. 1 shows how the graph of P_n looks like assuming that $a_1<\cdots<a_n$.

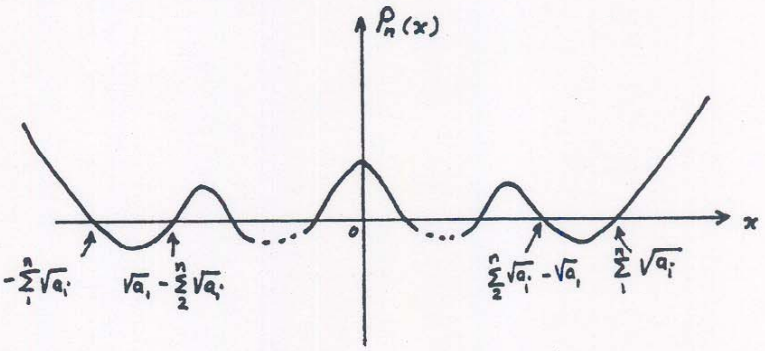

Fig. 1. The graph of $P_n(x)$

3. Mignotte's Method

In [6] M. Mignotte gives a method to answer the following question. If α and β are given algebraic numbers, can we decide whether $\alpha=\beta$ or not by just inspecting their approximations α' and β' ? (It is convenient to think that we can obtain these approximations via a numerical technique.) We first give some definitions to make the following discussion clear.

A real number α is *algebraic* if there exists a polynomial P with integer coefficients such that $P(\alpha)=0$. By $\mathrm{Irr}(\alpha)$ we denote the *minimal polynomial* of α; this is the unique polynomial R such that (i) $R(\alpha)=0$, (ii) the coefficients of R are integer, (iii) the degree of R is minimal,

and (iv) if $R(x)=a_0x^d+a_1x^{d-1}+\cdots+a_d$ then $a_0>0$ and $\sum_0^d |a_i|$ is minimal. We denote the *length* of α by $L(\alpha)$ which is equal to $\sum_0^d |a_i|$. The *degree* of α is denoted by $\deg(\alpha)$ and is equal to d. α and other roots of P are called the *conjugates* of α. An algebraic number becomes an *algebraic integer* if it is the root of a monic polynomial with integer coefficients. Clearly, for every algebraic number α there exists a least positive integer $\mathrm{den}(\alpha)$ (called the *denominator* of α) such that $\alpha\,\mathrm{den}(\alpha)$ is an algebraic integer.

A *size* function s for algebraic numbers satisfies the following conditions:

1. For all real numbers r, $\mathrm{card}\{\alpha : s(\alpha)\leq r\}<\infty$
2. $s(0)=0$; $s(1)=1$
3. $s(\alpha+\beta)\leq s(\alpha)+s(\beta)$
4. $s(\alpha\beta)\leq s(\alpha)s(\beta)$
5. $s(-\alpha)=s(\alpha)$

Mignotte showed that $s(\alpha)=\log S(\alpha)$ is a size where

$$S(\alpha)=\mathrm{den}(\alpha)\deg(\alpha)(1+\max_i |\alpha_i|)$$

(Here α_i are the conjugates of α.) He also proved the very important result

$$|\alpha-\beta| \geq e^{-\deg(\alpha)\deg(\beta)(s(\alpha)+s(\beta))}$$

when α and β are *different* algebraic numbers.

Returning to our original problem, let us try to see if $\sum_1^n \sqrt{a_i}$ is equal to L. Size of the former term is $\leq \sum_i \log(2(1+\sqrt{a_i}))$. Furthermore, we have seen in the previous section that the degree of this term is $\leq 2^n$. Size of L is $\log(L+1)$ whereas its degree is 1. (We omit the details of how the sizes are computed.) Using the result of Mignotte it is seen that we should evaluate approximations α' and β' to a precision of $O(e^{-2^n(\log L+\sum_i \log a_i)})$. We think that reaching to such a precision must take exponential time in n.

4. Simultaneous Diophantine Approximation

We start with some facts from the area of continued fractions. (R.W. Gosper provides a good summary in [1].) We shall denote the continued fraction $a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cdots\cfrac{1}{a_n}}}$ by the shorthand $[a_0,a_1,a_2,\cdots,a_n]$. Any rational number can be represented by a finite continued fraction. The main interest however lies in the application of continued fractions to the representation of irrationals. For this infinite continued fractions are needed. Call an irrational root of a quadratic equation with integral coefficients a *quadratic irrationality*. (Thus, a positive integer inside square root is a special case of it.) It is known that the continued fraction which represents a quadratic irrationality is periodic. (A *periodic* continued fraction is an

infinite continued fraction in which $a_l = a_{l+k}$ for a fixed k and all $l \geq M$. The set of partial quotients $a_M, \cdots, a_{M+k-1}$ is the *period* and the fraction is denoted $[a_0, \cdots, a_{M-1}, \dot{a}_M, a_{M+1}, \cdots, \dot{a}_{M+k-1}]$ where the "dot" points out to the periodic portion.) Thus, for example, $\sqrt{2}=[1,\dot{2}]$, $\sqrt{3}=[1,\dot{1},\dot{2}]$, and $\sqrt{7}=[2,\dot{1},1,1,\dot{4}]$.

We shall say that an irrational number α is approximable by rationals to *order* k if there is a $c(\alpha)$, depending only on α, for which $| p/q - \alpha | < c(\alpha)/q^k$ where p and q are integers. Clearly, a rational is approximable to order 1, and no higher. Any irrational is approximable to order 2. A quadratic irrationality is approximable to order 2, and no higher.

In simultaneous Diophantine approximation (SDA) one tries to approximate a given vector $\overline{\alpha}=(\alpha_1, \cdots, \alpha_d)$ by a vector of rational numbers $\overline{p}=(p_1/q, \cdots, p_d/q)$. Here d is the *dimension* of the problem. For a historical review of the area, the reader is referred to [3, 5]. In the first reference it is shown that the system of inequalities

$$| p_i/q - \alpha_i | < 1/q^{(1+\mu)} \text{ where } \mu = 1/d, i = 1, \cdots, d$$

has at least one solution. If one α_i is irrational then it has an infinity of solutions. (Note that by a solution we mean the determination of p_i since q is given.)

THEOREM (Dirichlet) [3]. Given $\alpha_1, \cdots, \alpha_d$ and any positive ϵ, one can find an integer q such that $q\,\alpha_i$ differs from an integer, for every i, by less than ϵ.

The following has the same general character as the above theorem but is deeper.

THEOREM (Kronecker) [3]. If $\alpha_1, \cdots, \alpha_d, 1$ are linearly independent, $\beta_1, \cdots, \beta_d$ are arbitrary, and N and ϵ positive, then there exist integers $n > N$, $p_1, \cdots, p_d$ such that

$$| n\,\alpha_i - p_i - \beta_i | < \epsilon, i = 1, \cdots, d$$

Recently, J.C. Lagarias obtained several important results regarding the SDA problem. For instance, he gives the following theorem for SDA of a *rational* vector $\overline{\alpha}$.

THEOREM 1 [4]. For a fixed dimension d, there exist algorithms to solve the following two problems in worst case polynomial time in input length.

1. Given $\overline{\alpha}=(x_1/y_1, \cdots, x_d/y_d)$ (where x_i and y_i are integers) and positive integers N, s_1, and s_2, find a denominator Q $(1 \leq Q \leq N)$ such that $\{\{Q\,\overline{\alpha}\}\} \leq s_1/s_2$, provided at least one exists, and $Q = 0$ otherwise.

2. Given $\overline{\alpha}=(x_1/y_1, \cdots, x_d/y_d)$ (where x_i and y_i are integers) and positive integer N, find a complete list of all best simultaneous approximation denominators Q to $\overline{\alpha}$ for which $Q \leq N$.

It is noted that in Theorem 1 $\{\{Q\,\overline{\alpha}\}\}$ is given by $\max_{1 \leq i \leq d} \{Q\,\alpha_i\}$ where $\{\beta\}$ is the distance of β to the nearest integer. The *best* simultaneous approximation denominators are exactly those Q for which $\{\{Q\,\overline{\alpha}\}\} < \{\{Q'\,\overline{\alpha}\}\}$ with $1 \leq Q' < Q$. However, if one allows d to vary then the following decision version of the SDA problem is NP-complete.

THEOREM 2 [4]. The set recognition problem "Is there an integer Q $(1 \leq Q \leq N)$ such that $\{\{Q\,\overline{\alpha}\}\} \leq s_1/s_2$?" is NP-complete for a given instance $\overline{\alpha}=(x_1/y_1, \cdots, x_d/y_d)$ and positive integers N, s_1, and s_2.

We now shortly look at the consequences of the above facts. Although the fact that a quadratic irrationality necessarily has a periodic continued fraction is seemingly a nice property, the amount of effort to detect this period may be arbitrarily large. This is certainly very discouraging since we may always err in answering the question in Section 1 if we employ the incomplete continued fractions of the given irrationalities. The limit on the approximability of quadratic irrationalities is less severe. One can always choose Q very large to obtain good approximations *a la* Lagarias. Yet, we know from Theorem 2 that currently we cannot do this in polynomial time (unless P=NP) in the dimension of the problem even for a vector of rationals. Since irrationals are more *complex* than rationals, a polynomial method for them is at least as unexpected.

Acknowledgment

This material is based upon work supported by the National Science Foundation under Grant No. ECS-8351942.

References

1. R.W. Gosper, "Continued Fractions," in *HAKMEM (AI Memo no. 239)*, pp. 36-44, Artificial Intelligence Lab, Massachusetts Inst. of Technology, Cambridge, Mass., Feb. 1972.
2. R.L. Graham, "Problem 85-5: Euclidean Minimum Spanning Trees," *Journal of Algorithms*, vol. 6, pp. 285-286, 1985.
3. G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, London, 1960.
4. J.C. Lagarias, "The Computational Complexity of Simultaneous Diophantine Approximation Problems," *SIAM Journal on Computing*, vol. 14, no. 1, pp. 196-209, Feb. 1985.
5. S. Lang, *Introduction to Diophantine Approximations*, Addison-Wesley, Reading, Mass., 1966.
6. M. Mignotte, "Identification of Algebraic Numbers," *Journal of Algorithms*, vol. 3, pp. 197-204, 1982.