An Effective Version of Kronecker's Theorem on Simultaneous Diophantine Approximation *

Gregorio Malajovich †
Departamento de Matemática Aplicada
Instituto de Matemática da Universidade Federal do Rio de Janeiro
Caixa Postal 68530 – CEP 21945 – Rio de Janeiro – RJ – BRASIL
gregorio@lyric.labma.ufrj.br

October 5, 2001

Abstract

Kronecker's theorem states that if 1, $\theta_1, \ldots, \theta_n$ are real algebraic numbers, linearly independent over $\mathbb{Q}$, and if $\alpha \in \mathbb{R}^n$, then for any $\epsilon > 0$ there are $q \in \mathbb{Z}$ and $p \in \mathbb{Z}^n$ such that $|q\theta_i - \alpha_i - p_i| < \epsilon$.

Here, a bound on q is given in terms of the dimension n, of the precision ϵ, of the degree of the θ_i's and of their height.

A possible connection to the square-root sum problem is discussed.

1 Introduction

In most of the literature, Kronecker's theorem on simultaneous diophantine approximation is stated in an ineffective way. However, there are some effective versions, that require additional hypotheses on the θ_i's. See for instance Rieger [10], Theorem 1 or Larcher and Niederreiter [8] section 3. Other available statements (like in Baker Brüdern and Harman [2]) do not seem to imply a bound on q.

Here, an elementary constructive proof of Kronecker's theorem will be given. Using estimates on the height of algebraic numbers, it will be possible to obtain effective bounds on q. For more on heights, see Section 2. The main result of this paper is:

Main Theorem 1. * *There is a function* $K(d, n) \in d^{O(n^2)}$ *such that if* $\theta_1, \ldots,$ θ_n *are real algebraic numbers and*

1. *The numbers* $1, \theta_1, \ldots, \theta_n$ *are linearly independent over* $\mathbb{Q}$

*Preprint, City University of Hong Kong, October 5, 2001.
†Partially supported by CNPq (BRASIL)

2. *Each θ_i is algebraic of degree $\leq d$ over $\mathbb{Q}$*

3. *The height $H(\theta_i)$ of each θ_i is smaller than some $H \in \mathbb{N}$*

then, for any $\alpha \in \mathbb{R}^n$, for any $\epsilon > 0$, there are $q \in \mathbb{Z}$, $p \in \mathbb{Z}^n$ such that

$$|q\theta_i - \alpha_i - p_i| < \epsilon \ , \ \ i = 1, \ldots, n \tag{1}$$

$$|q| \leq \left(\epsilon^{-1} H\right)^{K(d,n)} \tag{2}$$

If $\alpha = 0$, this follows from Dirichlet's theorem (in fact, the bound will be $|q| \leq \epsilon^{-n}$). Removing conclusion (2), this is Kronecker's theorem (See Section 2).

An immediate consequence of the main theorem is the

Corollary 1. *Under conditions 1, 2 and 3 of the main theorem, for any $\epsilon > 0$, there are $q \in \mathbb{Z}$ and $p \in \mathbb{Z}^n$ such that:*

$$0 < q\theta_i - p < \epsilon$$

$$|q| \leq \left(2\epsilon^{-1} H\right)^{K(d,n)}$$

Indeed, set $\alpha_i = \epsilon/2$ and apply the main theorem to obtain an $\epsilon/2$ approximation of α.

The investigation of effective bounds for Kronecker's theorem and for Corollary 1 was motivated by square-root sum decision problem (SQRTS), arising from computational geometry: given $n, m, a_1 \ldots, a_m, b_1, \ldots, b_n \in \mathbb{N}$, decide if $\sum \sqrt{a_i} > \sum \sqrt{b_i}$. Another formulation: given two paths joining lattice points in the plane, decide which is shorter. This problem is not known to be in $\mathcal{NP}$. See Section 5 for further comments.

The idea of using 'gap theorems' to investigate the square-root sum problem was suggested by Steve Smale. The following people make important suggestions and comments: Manuel Blum, Wellington de Melo, Mike Shub, Steve Smale, Bob Williams.

This paper was written as I was visiting the City University of Hong Kong, which I thank for its generous support.

2 Related Results, and a Conjecture

The following are the classical results related to the main Theorem of this paper:

Theorem 1 ((Dirichlet)). *Let $\theta \in \mathbb{R}^n$ and let $\epsilon > 0$. Then there are $q \in \mathbb{N}$, $p \in \mathbb{Z}^n$ such that $|q\theta_i - p_i| < \epsilon$ for all i. Furthermore, $1 \leq q < \epsilon^{-n}$.*

See Schmidt [11] Theorem 1A page 27, or Baker [1], for a proof.

Theorem 2 ((Kronecker)). *Let* $1, \theta_1, \ldots, \theta_n$ *be real algebraic numbers, linearly independent over* $\mathbb{Q}$*. Then for any* $\alpha \in \mathbb{R}^n$*, there are* $q \in \mathbb{N}$ *and* $p \in \mathbb{Z}^n$ *such that* $|q\theta_i - \alpha_i - p_i| < \epsilon$*, for all* i*.*

In fact, the statement is more general (see Siegel [13] page 63), but no bound for q seems to be known. The proof is non-constructive.

The bound for $K(d, n)$ in the main theorem seems to be extremely pessimistic. Instead, I would conjecture that

Conjecture 1. *There is* $K'(d, n) = K'(n) \in n^{O(1)}$ *such that the main theorem is valid, for* $\theta_i = \pm\sqrt{a_i}$*,* $a_i \in \mathbb{N}$*, and* K *replaced by* K'*.*

Remark that this conjecture is false if one drops the assumption that the θ_i's are algebraic, or if one does not bound the height of θ. In that case, even if $n = 1$, one could have an arbitrarily small θ, so an arbitrarily large q would be necessary to approximate $\alpha = 1/2$.

Estimates on heights of algebraic number will be needed in the proof of the main theorem. The height is a function $H : \bar{\mathbb{Q}} \to \mathbb{N}$. The properties of heights that we will use are listed below. Here, a, $b \in \bar{\mathbb{Q}}_*$, and $p \in \mathbb{Z}_*$.

1. $H(a)^{-\deg_{\mathbb{Q}}(a)} \le |a| \le H(a)^{\deg_{\mathbb{Q}}(a)}$
2. $H(0) = H(1) = 1$
3. $H(p) = |p|$
4. $H(ab) \le H(a)H(b)$
5. $H(a^{-1}) = H(-a) = H(a)$
6. $H(a + b) \le 2H(a)H(b)$

For the precise definition, and proof of the properties above, see Blum, Cucker, Shub and Smale [4], Silverman [14] or Schmidt [12].

3 Translations of the Torus, Covering Number and Useful Lemmas

The n-dimensional torus T^n is the quotient $\mathbb{R}^n/\mathbb{Z}^n$. A point $x \in \mathbb{R}^n$ will represent the equivalence class $x + \mathbb{Z}^n$ in T^n .

Let $\theta \in \mathbb{R}^n$. The vector θ induces a mapping $f_\theta : x \mapsto x + \theta \mod \mathbb{Z}^n$ in the torus T^n . This mapping can be interpreted as a dynamical system in T^n.

For more applications of dynamical systems or ergodic theory and for more about mappings of the torus, see Furstenberg [6], or Baladi, Rockmore, Tongring and Tresser [3].

Dirichlet's theorem (Theorem 1) says that, whatever θ is, some iterate of the origin 0 will come back to an ϵ-neighborhood of it, in time bounded by ϵ^{-n}. It may also happen that θ is so small, that the first iterate will still be in an ϵ neighborhood of the origin.

In fact, any point of the torus will return to any neighborhood of itself. Points with that property are said to be recurrent (under F_θ), and in this case all points are recurrent. Also, we have an effective bound for the return time.

Now, if an arbitrary point $\alpha \in T^n$ is given, will some iterate of 0 come within an ϵ-neighborhood of α ? This is false in general (e.g. $\theta = \left(\sqrt{2}, 1 - \sqrt{2}\right)$. But this is true under the condition of Kronecker's theorem (Theorem 2).

In that case, the orbit of 0 is dense, and the dynamical system f_θ is *ergodic*. This means that :

1. There is a probability measure μ invariant by f_θ^{-1}
2. Any f_θ-invariant set has measure 1 or 0.

Ergodic systems behave at 'random', in the following sense: the average of any measurable function on almost any orbit of f_θ converges to the average of that function in T^n (This is the ergodic theorem). However, little is known about the rate of convergence.

If Conjecture 1 is false, then even for simple examples like $\theta_i = \sqrt{a_i}$ the rate of convergence may be extremely slow.

Let denote by $B(\epsilon, x)$ the ball of radius ϵ around $x \in T^n$, i.e. the set:

$$B(\epsilon, x) = \{y \in T^n \text{ s.t. } |x_i - y_i - p_i| < \epsilon \text{ for all } i \text{ and for some } p_i \in \mathbb{Z}\}$$

The orbit $\{q\theta \mod \mathbb{Z}^n\}$ of 0 generates a covering $\{B(\epsilon, q\theta)\}_{q \in \mathbb{N}}$ of the torus T^n . Since T^n is compact, there is a finite subcovering that can be chosen in the form:

$$\{B(\epsilon, q\theta)\}_{q=1,2,\ldots,N} \tag{3}$$

The smallest N such that (3) defines a covering of the torus will be called the covering number of θ and ϵ, and denoted $N(\epsilon, \theta)$. The conclusions of the main theorem (equations (1) and (2)) may now be restated as:

$$N(\epsilon, \theta) \leq \left((\epsilon^{-1} H\right)^{K(d,n)}$$

Some useful properties of the covering number follow:

Lemma 1.

1. *For all* $q \in \mathbb{Z}$, $N(\epsilon, \theta) \leq q N(\epsilon, q\theta)$
2. *For all* $p \in \mathbb{Z}^n$, $N(\epsilon, \theta + p) = N(\epsilon, \theta)$

of Lemma 1. Item 2 is trivial. In order to prove item 1, consider the orbit $\{r\theta\}_{1\leq r\leq qN(\epsilon,q\theta)}$ of 0 by f_θ . It contains the orbit $\{s(q\theta)\}_{1\leq s\leq N(\epsilon,q\theta)}$ of 0 under $f_{q\theta}$. Since this last orbit is within distance ϵ of any prescribed point, the former one also is. □ □

Also, on may embed the translation f_θ into a flow φ_θ^t of T^n, defined by:

$$\begin{array}{rclcl} \varphi_\theta & : & \mathbb{R}\times T^n & \rightarrow & T^n \\ & & t, x & \mapsto & \varphi_\theta^t(x) = x + t\theta \mod \mathbb{Z}^n \end{array}$$

We may define the covering number for φ_θ in an analogous way as the covering number for a discrete transformation. We define $\nu(\epsilon,\theta)$ as the infimum of all $s\in\mathbb{R}^+$ such that:

$$\bigcup_{t\in[0,s]} B(\epsilon,\varphi_\theta^t(0)) \supseteq T^n$$

We will use the following fact in the sequel:

Lemma 2. $N(\epsilon,\theta)\leq \nu(\epsilon-\max\theta_i,\theta)$

of Lemma 2. Let $\alpha\in T^n$. There is $t\leq\nu(\epsilon-\max|\theta_i|,\theta)$ such that $t\theta\in\bar{B}(\epsilon-\max|\theta_i,\alpha)$. Let s be the largest integer $\leq t$. Then $\varphi_\theta^s(0)-\varphi_\theta^t(0)=(t-s)\theta \mod \mathbb{Z}^n$, and $\max(t-s)|\theta_i| < \max|\theta_i|$. Therefore, by triangular inequality, $\varphi_\theta^s(0)\in B(\epsilon,\alpha)$. □ □

4 Proof of the Main Theorem

Assume, as in the hypothesis of the main theorem, that 1, θ_1, … , θ_n are real algebraic numbers, linearly independent over $\mathbb{Q}$. Let $H=\max H(\theta_i)$, and let d bound the degree of each θ_i over $\mathbb{Q}$. Let D be the degree of $\mathbb{Q}[\theta_1,\dots,\theta_n]$ over $\mathbb{Q}$. Then $D\leq d^n$.

Given ϵ, we have to bound the covering number $N(\epsilon,\theta)$. We will proceed by induction on the dimension n. We will need the

Lemma 3. *Under the conditions above, there are $\hat{\theta}_1$, … , $\hat{\theta}_{n-1}\in\mathbb{Q}[\theta_1,\dots,\theta_n]$, such that:*

1. 1, $\hat{\theta}_1$, … , $\hat{\theta}_{n-1}$ *are linearly independent over* $\mathbb{Q}$.
2. $H(\hat{\theta}_i)\leq\left(\epsilon^{-1}H(\theta)\right)^{4\max(n+1,D)}$
3. $N(\epsilon,\theta)\leq\left(\epsilon^{-1}H(\theta)\right)^{4D\max(n+1,D)} N(\frac{\epsilon}{2},\hat{\theta})$

of Lemma 3. According to Dirichlet's theorem (Theorem 1), there are $q \in \mathbb{N}$, $p \in \mathbb{Z}^n$ such that:

$$|q\theta_i - p_i| < \frac{\epsilon}{2} \text{ , for } i = 1, \dots, n$$

with $1 \leq |q| < \left(\frac{2}{\epsilon}\right)^n$. In other words, the q^{th} iteration of θ defines a 'small' translation of the torus.

We may also bound the 'rotation numbers' p_i of $q\theta$ as follows:

$$|p_i| \leq |q|(|\theta_i| + 1) \leq 2|q|H(\theta_i)^{\deg_{\mathbb{Q}}\theta_i}$$

We also obtain the following lower bound, to be used later:

$$\left|\theta_i - \frac{p_i}{q}\right| \geq \frac{1}{H\left(\theta_i - \frac{p_i}{q}\right)^{\deg_{\mathbb{Q}}\theta_i}} \geq \frac{1}{\left(4\left(\frac{2}{\epsilon}\right)^{2n} H(\theta_i)^{1+\deg_{\mathbb{Q}}\theta_i}\right)^{\deg_{\mathbb{Q}}\theta_i}} \qquad (4)$$

Remark 1. The bound above can be mad much sharper if one knows how to bound the constant c appearing in Liouville's theorem $|q\theta_i - p_i| > \frac{c}{q^{\deg_{\mathbb{Q}}\theta_i}}$. Unfortunately, we may only assume here a bound on $H(\theta)$.

The covering number of θ may be bounded as follows:

$$\begin{aligned} N(\epsilon, \theta) &\leq qN(\epsilon, q\theta) \\ &\leq qN(\epsilon, q\theta - p) \\ &\leq q\nu(\frac{\epsilon}{2}, q\theta - p) \end{aligned}$$

where the first two inequalities follow from Lemma 1, and the last one from Lemma 2, using the fact that $|q\theta_i - p_i| < \epsilon/2$.

At this point, we bounded the covering number of the translation f_θ in terms of the covering number of the flow φ_θ^t in the torus. Since θ_n is not a rational, this flow is transversal to the plane $x_n = \alpha_n$, where α_n is a constant, as in the main theorem.

We should look now at the first return map, also known as Poincaré transform, of the flow φ_θ^t in the plane $x_n = \alpha_n$. The first return map associates, to any point $X = (x_1, \dots, x_{n-1}, \alpha_n)$ of the plane $x_n = \alpha_n$, the next point in the orbit of X that belongs to $x_n = \alpha_n$. This point is given explicitly by:

$$\begin{pmatrix} x_1 \\ \vdots \\ x_{n-1} \\ \alpha_n \end{pmatrix} + \begin{pmatrix} \frac{q\theta_1 - p_1}{q\theta_n - p_n} \\ \vdots \\ \frac{q\theta_{n-1} - p_{n-1}}{q\theta_n - p_n} \\ \alpha_n \end{pmatrix}$$

Therefore, we set $\hat{\theta}_1 = \frac{q\theta_1 - p_1}{q\theta_n - p_n}$, ... , $\hat{\theta}_{n-1} = \frac{q\theta_{n-1} - p_{n-1}}{q\theta_n - p_n}$.

In order to arrive to a distance $\leq \epsilon/2$ of a point $\alpha = (\alpha_1, \dots, \alpha_n) \in T^n$, starting from the origin, one should follow the flow φ_θ^t until arrival to the plane $\alpha_n = 0$. Then, one performs as many iterations of the first return map as necessary. This number is finite (since $1, \hat{\theta}_1, \dots, \hat{\theta}_{n-1}$) are linearly independent over $\mathbb{Q}$) and bounded above by $N(\epsilon/2, \hat{\theta})$.

Each iteration of the first return map takes time $\frac{1}{|q\theta_n - p_n|}$ in the flow. Also, the plane $x_n = \alpha_n$ may be reached for the first time in time $< \frac{1}{|q\theta_n - p_n|}$.

Hence,

$$\nu(\frac{\epsilon}{2}, q\theta - p) \leq \frac{1}{|q\theta_n - p_n|} \left(1 + N(\frac{\epsilon}{2}, \hat{\theta})\right)$$

Therefore,

$$N(\frac{\epsilon}{2}, \theta) \leq \frac{1}{|\theta_n - p_n/q_n|} \left(1 + N(\frac{\epsilon}{2}, \hat{\theta})\right)$$

Using (4), one obtains:

$$N(\frac{\epsilon}{2}, \theta) \leq 2^{(2n+2)\deg_{\mathbb{Q}}\theta_n} \epsilon^{-2n\deg_{\mathbb{Q}}\theta_n} H(\theta_n)^{(1+\deg_{\mathbb{Q}}\theta_n)\deg_{\mathbb{Q}}\theta_n} \left(1 + N(\frac{\epsilon}{2}, \hat{\theta})\right)$$

Hence, since $H(\theta_n), \epsilon^{-1} \geq 2$, we can replace the right-hand side by a coarser estimate:

$$N(\frac{\epsilon}{2}, \theta) \leq \left(\epsilon^{-1} H(\theta)\right)^{D \max(4(n+1), D+1)} N(\frac{\epsilon}{2}, \hat{\theta}) \tag{5}$$

Also,

$$H(\hat{\theta}_i) \leq H(q\theta_i - p_i) H(q\theta_n - p_n) \leq 4|q|^2 H(\theta_i) H(\theta_n) |p_i||p_n|$$

This can be estimated by:

$$H(\hat{\theta}_i) \leq 2^{2n+4} \epsilon^{-2n} H(\theta_i)^{1+\deg_{\mathbb{Q}}\theta_i} H(\theta_n)^{1+\deg_{\mathbb{Q}}\theta_n} \leq \left(\epsilon^{-1} H(\theta)\right)^{\max(4(n+1), D+1)} \tag{6}$$

We may bound (5) and (6) by $(\epsilon^{-1}H)^{4D\max(n+1,D)}$ and $(\epsilon^{-1}H)^{4\max(n+1,D)}$, respectively, as in the statement of the lemma. □ □

We will prove now a more general version of the main theorem, where $K(d, n)$ is replaced by a power of $D = \deg_{\mathbb{Q}} \mathbb{Q}[\theta_1, \dots, \theta_n]$.

Induction Hypothesis 1. * Let $\theta_1, \dots, \theta_n$ be algebraic numbers, so that:

1. $1, \theta_1, \dots, \theta_n$ are linearly independent over $\mathbb{Q}$
2. $\deg_{\mathbb{Q}} \mathbb{Q}[\theta_1, \dots, \theta_n] \leq D$

3. The height $H(\theta_i)$ of each θ_i is smaller than $H \in \mathbb{N}$

Then $N(\epsilon,\theta) \leq \left(\epsilon^{-1}H\right)^{(4\max(D,n+1))^{2n}}$

For $n = 1$, $N(\epsilon,\theta) \leq \frac{1}{|\theta - p/q|}$ as above. Furthermore, we may bound the right-hand side by $4(\epsilon/2)^{-2D}H^{D(1+D)} \leq (H/\epsilon)^{4D^2}$.

Assume the induction hypothesis true at rank $n-1$. According to Lemma 3,

$$N(\epsilon,\theta) \leq \left(\epsilon^{-1}H\right)^{4D\max(D,n+1)} N(\epsilon/2,\hat{\theta})$$

with

$$H(\hat{\theta}) \leq \left(\epsilon^{-1}H\right)^{4\max(D,n+1)}$$

Hence, by induction,

$$N(\epsilon,\theta) \leq \left(\epsilon^{-1}H\right)^{4D\max(D,n+1)} \left(\left(\epsilon^{-1}H\right)^{4\max(D,n+1)} \frac{2}{\epsilon}\right)^{(4\max(n+1,D)^{2n-2}} \tag{7}$$

$$\leq \left(\epsilon^{-1}H\right)^{(4\max(n+1,D)^{2n}} \tag{8}$$

Recall that, under the hypotheses of the Main Theorem, $D \leq d^n$. Also, $n+1 \leq d^n$ for all $n \geq 1$, since we require $d \geq 2$. Hence $4\max(n+1,D) \leq 4d^n$, and:

$$\left(4d^n\right)^{2n} = 4^{2n}d^{2n^2} \leq d^{2n^2+4n} \leq d^{3n^2}$$

Therefore, we set $K(d,n) = d^{3n^2} \in d^{O(n^2)}$, and the main theorem is proved.

5 Connections with the square-root sum problem

The square-root sum decision problem is defined as:

Problem 1. (SQRTS) Given $m, n, a_1, \ldots, a_m, b_1, \ldots, b_m \in \mathbb{N}$, decide if $\sum \sqrt{a_i} > \sum \sqrt{b_i}$

A different formulation of this problem (decide $\sum \sqrt{a_i} > c$,$c \in \mathbb{N}$) appeared in Garey, Graham and Johnson [7] in connection with the traveling salesman problem in the plane:

Given a set of lattice (integer) points in the plane, decide if there is a path of length $< c$ covering all the points. This problem was proven to be $\mathcal{NP}$-complete for the $\|.\|_1$ metric.

However, the traveling salesman problem in the plane with the usual euclidian metric was only shown to be $\mathcal{NP}$-hard, due to the difficulty to check if a given path has length $< c$.

This last problem was studied by Tiwari [15], in a more particular setting (the a_i's were represented in the form $c\sqrt{p_1 \dots p_k}$, $c \in \mathbb{Z}$, p_i primes. He concluded that this problem could be solved in polynomial time by a RAM machine. (i.e., counting only the number of algebraic operations). It is not known if there is a polynomial time algorithm for this problem, in the bit-complexity model.

As Tiwari's problem, SQRTS can be solved in polynomial time over the reals or over $\mathbb{Z}$ (RAM machines, without counting bit operations). The strategy is to approximate each $\sqrt{a_i}$ and $\sqrt{b_i}$ up to the necessary precision δ, using $\log - \log \delta$ Newton iterations. Moreover, it can be proved that $\sum \sqrt{a_i} - \sum \sqrt{b_i}$ is either 0, or:

$$|\sum \sqrt{a_i} - \sum \sqrt{b_i}| > \max(a_i, b_i)^{-2^{O(m+n)}}$$

Indeed, write $x = \sum \sqrt{a_i} - \sum \sqrt{b_i}$ as a solution of:

$$\begin{array}{lcl} \theta_1^2 - a_1 & = & 0 \\ & \vdots & \\ \theta_m^2 - a_m & = & 0 \\ \theta_{m+1}^2 + b_1 & = & 0 \\ & \vdots & \\ \theta_{m+n}^2 + b_n & = & 0 \\ \theta_1 + \cdots + \theta_{m+n} - x & = & 0 \end{array}$$

and then apply Canny's gap theorem [5] or Pardo and Krick's Corollary 7 in [9].

Therefore, $O(m+n)$ Newton iteration will approximate a_i and b_i up to precision $\delta \leq \frac{1}{2(m+n)} \max(a_i, b_i)^{-2^{O(m+n)}}$. Thus, it is possible to compute x in time $O(m+n)$ with precision enough to decide SQRTS.

When bit-complexity (Turing complexity, or complexity over F_2) is concerned, the gap bound above is not satisfactory any more. Indeed, $\log - \log \delta$ iterations can produce numbers with $-\log \delta$ bits, making the above algorithm exponential time.

Proposition 1. *Conjecture 1 implies that SQRTS belongs to $\mathcal{P}$.*

of Proposition 1. Set $\theta_1 = \sqrt{a_1}, \dots, \theta_m = \sqrt{a_m}, \theta_{m+1} = -\sqrt{b_1}, \theta_{m+n} = -\sqrt{b_n}$. Now, Corollary 1 implies that for all $\epsilon > 0$, there are $q \in \mathbb{N}$, $p \in \mathbb{Z}^{m+n}$ such that $0 < \theta_i - p_i/q < \epsilon/q$, with $1 \leq q < (2\epsilon^{-1}H)^{(m+n)^{O(1)}}$.

Set $\epsilon = \frac{1}{2(m+n)}$. Then $q < ((4(m+n)H)^{(m+n)^{O(1)}}$. We may now distinguish two cases.

Case 1: Assume that $\sum \frac{p_i}{q} \neq 0$. Then $|\sum \frac{p_i}{q}| \geq \frac{1}{q}$, and:

$$|\sum \theta_i| \geq |\sum \frac{p_i}{q}| - |\sum \theta_i - \frac{p_i}{q}| \geq \frac{1}{q} - \frac{1}{2q} \geq \frac{1}{2q} \in H^{-(m+n)^{O(1)}}$$

Case 2: $\sum \frac{p_i}{q} = 0$, so $\sum \theta_i = \sum \theta_i - \frac{p_i}{q}$. However, according to Liouville's theorem, $|\theta_i - \frac{p_i}{q}| > \frac{c}{q^2}$, where the constant c may be chosen equal to $\frac{1}{2(\max(a_i,b_i)+1)}$. Therefore,

$$\sum \theta_i > \frac{nc}{q^2} \in H^{-(m+n)^{O(1)}}$$

Therefore, we conclude that $O((m+n)^{O(1)} \log H)$ steps of Newton iteration suffice to decide SQRTS. $\square$ $\square$

References

[1] Alan Baker: *A Concise Introduction to Number Theory.* Cambridge University Press, Cambridge 1984.

[2] R.C.Baker, J.Brüdern and G.Harman: Simultaneous Diophantine Approximation with Square-Free Numbers. *Acta Arithmetica* **63** num. 1, 51-60, 1993.

[3] V. Baladi, D. Rockmore, N. Tongring and C. Tresser: Renormalization on the n-dimensional torus. Nonlinearity **5**, 1111-1136, 1992.

[4] Lenore Blum, Felipe Cucker, Mike Shub and Steve Smale: Algebraic Settings for the Problem $\mathcal{P} = \mathcal{NP}$. Preprint, 1995.

[5] John Canny: *The complexity of robot motion planning.* MIT Press, Cambridge MA, 1988.

[6] Harry Furstenberg: *Recurrence in Ergodic Theory and Combinatorial Number Theory.* Princeton University Press, Princeton, 1981.

[7] M.R.Garey, R.L.Graham and D.S.Johnson: Some $\mathcal{NP}$-complete Geometric Problems. *Proceedings of the Eight Annual ACM Symposium on the Theory of Computing,* 10-21. Hershey, Pennsylvania, 1976.

[8] Gerhard Larcher and Harald Niederreiter: Kronecker-type Sequences and Nonarchimedean Diophantine Approximations *Acta Arithmetica* **63** Num. 4, 379-396, 1993.

[9] Luis Miguel Pardo Vasallo and Teresa Krick: A computational Method for Diophantine Approximation. *Proceedings of the MEGA'94.* Progress in Mathematics, Birkhauser, 1955.

[10] G.J.Rieger: Effective Simultaneous Approximation of Complex Numbers by Conjugate Algebraic Integers. *Acta Arithmetica* **63** num. 4, 325-334, 1993.

[11] Wolfgang M. Schmidt: *Diophantine Approximation*. Lecture Notes in Mathematics 785, Springer-Verlag, Berlin, 1980.

[12] Wolfgang M. Schmidt: *Diophantine Approximations and Diophantine Equations*. Lecture Notes in Mathematics 1467, Springer-Verlag, Berlin, 1991.

[13] Carl Ludwig Siegel: *Lectures on the Geometry of Numbers*. Springer-Verlag, Berlin, 1989.

[14] Joseph H. Silverman: *The Arithmetic of Elliptic Curves*. Springer-Verlag, New York, 1986.

[15] Prasoon Tiwari: A problem that is easier to solve on the unit-cost algebraic RAM. *Journal of Complexity* **8**, num. 4, 393-397, 1992.