

## FORMULAS FOR SOME DIOPHANTINE APPROXIMATION CONSTANTS

T. W. CUSICK and S. KRASS

(Received 16 September 1986)

Communicated by J. H. Loxton

### Abstract

Let  $M$  be a full  $\mathbf{Z}$ -module in  $F$  a real number field of degree at least 3 with  $N(\alpha)$  denoting the norm of  $\alpha \in F$ . Given any nonzero number  $\phi$  in  $M$  we make the plausible conjecture that one can find a number  $\beta$  in  $M$  such that  $N(\beta) = N(\phi)$  and the algebraic conjugates of  $\beta$  (not including  $\beta$ ) have ratios arbitrarily near any given numbers consistent with the complex algebraic conjugates of elements of  $F$ . We use the conjecture to give explicit formulas for some diophantine approximation constants. Without the conjecture our methods lead to corresponding lower bounds for these constants.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*): 10 F 10, 10 F 25.

### 1. Introduction

Two well-known constants are associated with each  $n$ -tuple  $\mathbf{x} = (x_1, \dots, x_n)$  of real numbers.

The simultaneous diophantine approximation constant of  $\mathbf{x}$ , denoted by  $c(\mathbf{x})$ , is the infimum of those  $c > 0$  for which the inequality

$$|m_0| \max_{1 \leq j \leq n} |m_0 x_j - m_j|^n < c$$

has infinitely many solutions in integers  $m_0 \neq 0, m_1, \dots, m_n$ .

The linear form (or dual) approximation constant of  $\mathbf{x}$ , denoted by  $c^*(\mathbf{x})$ , is the infimum of those  $c > 0$  for which the inequality

$$|m_0 + m_1 x_1 + \dots + m_n x_n| \max_{1 \leq j \leq n} |m_j|^n < c$$

has infinitely many solutions in integers  $m_0, m_1, \dots, m_n$  with  $m_1, \dots, m_n$  not all zero.

In Cusick [3] explicit formulas for  $c(\xi), c^*(\xi)$  are given in the case  $\xi = (\xi_1, \xi_2)$  where  $1, \xi_1, \xi_2$  is a basis for a real cubic field. In this paper we obtain formulas for  $c(\xi), c^*(\xi)$  where  $\xi = (\xi_1, \dots, \xi_n)$  with  $1, \xi_1, \dots, \xi_n$  a basis for a real number field of degree  $n + 1$ . But these formulas are subject to a conjecture, described below, on the existence of units with conjugates “very nearly” in any given ratio consistent with complex conjugates.

Without the conjecture the methods used here lead to lower bounds.

### 2. Unit conjecture

Let  $\mathbf{F}$  be a real number field of degree  $n + 1$  with  $s$  pairs of complex conjugates. So  $0 \leq 2s < n + 1$ . We put  $r = n - 2s$  and denote (algebraic) conjugates of  $\alpha \in \mathbf{F}$  by  $\alpha_{[0]} = \alpha, \alpha_{[1]}, \dots, \alpha_{[n]}$  ordered so that

$$\alpha_{[j]} \in \mathbf{R}, \quad j = 0, \dots, r; \quad \alpha_{[j]} = \bar{\alpha}_{[s+j]} \in \mathbf{C}, \quad j = r + 1, \dots, r + s.$$

$N(\alpha) = \prod_{j=0}^n \alpha_{[j]}$  is the norm of  $\alpha$ .

Any basis  $\mu_0, \dots, \mu_n$  of  $\mathbf{F}$  determines a full  $\mathbf{Z}$ -module

$$M = \left\{ \sum_{i=0}^n m_i \mu_i : m_i \in \mathbf{Z}, i = 0, \dots, n \right\}.$$

$\mathcal{R}(M)$ , the coefficient ring of  $M$ , is defined by

$$\mathcal{R}(M) = \{ \alpha \in \mathbf{F} : \alpha M \subseteq M \}.$$

We will write

$$\mathbf{C}^{r,s} = \{ \mathbf{x} = (x_1, \dots, x_n) : x_j \in \mathbf{R}, j = 1, \dots, r, x_j = \bar{x}_{s+j} \in \mathbf{C}, j = r + 1, \dots, r + s \},$$

$$\mathbf{C}_*^{r,s} = \{ \mathbf{x} = (x_1, \dots, x_n) \in \mathbf{C}^{r,s} : x_j \neq 0, j = 1, \dots, n \},$$

$$\mathbf{C}_+^{r,s} = \{ \mathbf{x} = (x_1, \dots, x_n) \in \mathbf{C}_*^{r,s} : x_j > 0, j = 1, \dots, r \}.$$

We can now state the unit conjecture, (U.C.).

(U.C.). *Given any  $\mathbf{x} = (x_1, \dots, x_n) \in \mathbf{C}_+^{r,s}$  and any  $\varepsilon > 0$  there exists a unit  $\alpha \in \mathcal{R}(M) \subseteq \mathbf{F}$  with  $\alpha_{[j]} > 0, j = 0, \dots, r$  such that*

$$\alpha_{[j]} / \alpha_{[1]} = x_j / x_1 + \varepsilon_j, \quad |\varepsilon_j| < \varepsilon, \quad j = 2, \dots, n.$$

Observe for the above unit  $\alpha$  that  $N(\alpha) = 1$ .

In the case  $s = 0$ , that is where  $\mathbf{F}$  is a totally real number field, (U.C.) is equivalent to a conjecture of Adams in [1, page 192]. Adams' conjecture in turn is a special case of a conjecture of Schanuel (see Ax, [2]). As multiplication by units plays a vital role in our arguments, and assuming (U.C.) leads to exact results in all real (algebraic) number fields including those with complex conjugates, it seems convenient to express the conjecture in the above form.

By a result of Peck [6]—also see Krass [5]—we know (U.C.) holds for the special case  $\mathbf{x} = (1, \dots, 1) \in \mathbf{C}_+^{r,s}$ .

For convenience we express Peck's result in the following lemma.

**LEMMA 1.** *There exists an infinite sequence  $\Gamma = (\gamma_k, k = 1, 2, \dots)$  of units in  $\mathcal{R}(M)$  such that*

- (i)  $\gamma_{k[j]} > 0, j = 0, \dots, r,$
- (ii)  $\lim_{k \rightarrow \infty} \gamma_k = \infty,$
- (iii)  $\lim_{k \rightarrow \infty} \gamma_{k[j]} / \gamma_{k[1]} = 1, j = 2, \dots, n,$

where, above,  $\gamma_{k[j]} = (\gamma_k)_{[j]} = j$ th conjugate of  $\gamma_k$ .

Observe that (iii) can be expressed in the form

- (iii')  $\lim_{k \rightarrow \infty} \gamma_k^{1/n} \gamma_{k[j]} = 1, j = 1, \dots, n.$

We say  $\Gamma$ , an infinite sequence of units in  $\mathcal{R}(M)$  satisfying Lemma 1 is a Peck sequence in  $\mathcal{R}(M)$ .

### 3. Preliminaries

We now fix  $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbf{F}^n$  such that  $1, \alpha_1, \dots, \alpha_n$  is a (rational) basis for  $\mathbf{F}$ . Our next theorem gives formulas for  $c(\alpha)$  and  $c^*(\alpha)$  but we first need some notation.

In matrix definitions we use exclusively  $i$  as a row index and  $j$  as a column index.

Writing  $\alpha_0 = 1$  we construct the  $n + 1$  by  $n + 1$  matrix

$$A = (\alpha_{j[i]}), \quad \alpha_{j[i]} = (\alpha_j)_{[i]}, \quad i, j = 0, \dots, n.$$

It is well known  $\det A \neq 0$ . Note rows of  $A$  are obtained by conjugation respectively of  $(1, \alpha_1, \dots, \alpha_n)$  and this row conjugate structure induces a column conjugate structure on the inverse of  $A$ . So we may write

$$A^{-1} = U = (u_{i[j]}), \quad u_{i[j]} = (u_i)_{[j]}, \quad i, j = 0, \dots, n.$$

Of course  $u_i = u_{i[0]}, i = 0, \dots, n$ .  $u_0, \dots, u_n$  is called the dual basis of the basis  $1, \alpha_1, \dots, \alpha_n$ .

Associated with  $A$  and  $U$  are the  $n$  by  $n$  matrices

$$A_1 = (\alpha_{j[i]} - \alpha_j), \quad 1 \leq i, j \leq n,$$

$$U_1 = (u_{i[j]}), \quad 1 \leq i, j \leq n.$$

Since  $\alpha_{0[i]} = 1, i = 0, \dots, n$ , it easily follows that  $\det A_1 = \det A$ , and  $U_1 = A_1^{-1}$ . By our conjugate ordering conventions for any  $\mathbf{x} \in \mathbf{R}^n$  we have  $\mathbf{x}U_1 \in \mathbf{C}^{r,s}$ , and  $A_1\mathbf{x}^t \in \mathbf{C}^{r,s}$ . For any  $\mathbf{y} = (y_1, \dots, y_n) \in \mathbf{C}^{r,s}$  we define

$$g(\mathbf{y}) = g(\mathbf{y}^t) = \prod_{j=1}^n |y_j|.$$

From now on  $M$  denotes the module with basis  $1, \alpha_1, \dots, \alpha_n$  and  $M^*$  its dual module. Namely, recalling  $\alpha_0 = 1$

$$M = \left\{ \sum_{i=0}^n m_i \alpha_i : m_i \in \mathbf{Z}, i = 0, \dots, n \right\},$$

$$M^* = \left\{ \sum_{i=0}^n m_i u_i : m_i \in \mathbf{Z}, i = 0, \dots, n \right\}.$$

We will need to consider the signs of real conjugates of nonzero elements of  $\mathbf{F}$ .  $\sigma(\mathbf{x})$  the signature of  $\mathbf{x} = (x_1, \dots, x_n) \in \mathbf{C}_*^{r,s}$  is defined as  $\sigma(\mathbf{x}) = (\text{sgn } x_1, \dots, \text{sgn } x_r)$  where  $\text{sgn } x = x/|x| = \pm 1$ , all real nonzero  $x$ . The signature set  $\Sigma$ , with  $2^r$  elements, is

$$\Sigma = \{ \sigma = (e_1, \dots, e_r) : e_j = \pm 1, j = 1, \dots, r \}.$$

For any  $\alpha \in \mathbf{F}, \alpha \neq 0$ , we write rather loosely  $\sigma(\alpha) = (\text{sgn } \alpha_{[1]}, \dots, \text{sgn } \alpha_{[r]}) \in \Sigma$ . For each signature  $\sigma \in \Sigma$  we define

$$\eta_\sigma = \min \{ |N(\beta)| : \beta \in M, \beta \neq 0, \text{ and } \sigma(\beta) = \sigma \},$$

$$\eta_\sigma^* = \min \{ |N(\beta)| : \beta \in M^*, \beta \neq 0, \text{ and } \sigma(\beta) = \sigma \}.$$

We note (proof omitted) that  $\eta_\sigma$  and  $\eta_\sigma^*$  are well defined strictly positive numbers for each  $\sigma \in \Sigma$ .

The formulas for the diophantine approximation constants are now stated. Note  $\|\mathbf{x}\| = \max_{1 \leq j \leq n} |x_j|$ , for  $\mathbf{x} = (x_1, \dots, x_n) \in \mathbf{R}^n$ .

**THEOREM 1.** For  $\alpha = (\alpha_1, \dots, \alpha_n)$  with  $1, \alpha_1, \dots, \alpha_n$  a basis for  $\mathbf{F}$  a real number field of degree  $n + 1$

- (i)  $c(\alpha) \geq \min_{\sigma \in \Sigma} \{ \eta_\sigma^* / \max \{ g(\mathbf{x}U_1) : \mathbf{x} \in \mathbf{R}^n, \|\mathbf{x}\| = 1, \text{ and } \sigma(\mathbf{x}U_1) = \sigma \} \}$ ,
- (ii)  $c^*(\alpha) \geq \min_{\sigma \in \Sigma} \{ \eta_\sigma / \max \{ g(A_1\mathbf{x}^t) : \mathbf{x} \in \mathbf{R}^n, \|\mathbf{x}\| = 1, \text{ and } \sigma(A_1\mathbf{x}^t) = \sigma \} \}$ .

Furthermore, under the assumption of (U.C.)

- (i')  $c(\alpha) = \min_{\sigma \in \Sigma} \{ \eta_\sigma^* / \max \{ g(\mathbf{x}U_1) : \mathbf{x} \in \mathbf{R}^n, \|\mathbf{x}\| = 1, \text{ and } \sigma(\mathbf{x}U_1) = \sigma \} \}$ ,
- (ii')  $c^*(\alpha) = \min_{\sigma \in \Sigma} \{ \eta_\sigma / \max \{ g(A_1\mathbf{x}^t) : \mathbf{x} \in \mathbf{R}^n, \|\mathbf{x}\| = 1, \text{ and } \sigma(A_1\mathbf{x}^t) = \sigma \} \}$ .

4. Proof of (i) and (i') of Theorem 1

By  $\mathbf{m} \in \mathbf{Z}^{n+1}$  we mean  $\mathbf{m} = (m_0, \dots, m_n) \in \mathbf{Z}^{n+1}$ . Clearly we need only consider elements of  $\mathbf{Z}_*^{n+1} = \{\mathbf{m} \in \mathbf{Z}^{n+1}: m_0 \neq 0\}$ . Motivated by the definition of  $c(\alpha)$  we write

$$\mathbf{h}(\mathbf{m}) = |m_0|^{1/n}(m_1 - m_0\alpha_1, \dots, m_n - m_0\alpha_n), \quad \text{for } \mathbf{m} \in \mathbf{Z}_*^{n+1}.$$

We say  $\mathbf{h}(\mathbf{m})$  is an approximation vector for  $\alpha$ . It is a standard result that there are infinitely many  $\mathbf{m} \in \mathbf{Z}_*^{n+1}$  so that

$$\|\mathbf{h}(\mathbf{m})\| = \max_{1 \leq j \leq n} |m_0|^{1/n}|m_j - m_0\alpha_j| < 1.$$

We introduce the notation  $\mathbf{u}_j = (u_{0[j]}, \dots, u_{n[j]})^t = j$ th column of  $U$ ,  $j = 0, \dots, n$  and often write  $\mathbf{u}_0 = \mathbf{u} = (u_0, \dots, u_n)^t$ . An important identity is

$$(1) \quad \mathbf{h}(\mathbf{m}) \cdot U_1 = |m_0|^{1/n}(\mathbf{m} \cdot \mathbf{u}_1, \dots, \mathbf{m} \cdot \mathbf{u}_n), \quad \text{for } \mathbf{m} \in \mathbf{Z}_*^{n+1}$$

where

$$\mathbf{m} \cdot \mathbf{u}_j = \sum_{i=0}^n m_i u_{i[j]} = (\mathbf{m} \cdot \mathbf{u})_{[j]}, \quad j = 0, \dots, n.$$

To prove (1) observe, writing  $\alpha_0 = (1, \alpha_1, \dots, \alpha_n)$ , and noting  $AU = I$

$$\alpha \cdot U_1 = (\alpha_0 \cdot \mathbf{u}_1, \dots, \alpha_0 \cdot \mathbf{u}_n) - (u_{0[1]}, \dots, u_{0[n]}) = -(u_{0[1]}, \dots, u_{0[n]})$$

and

$$(m_1, \dots, m_n) \cdot U_1 = (\mathbf{m} \cdot \mathbf{u}_1, \dots, \mathbf{m} \cdot \mathbf{u}_n) - m_0(u_{0[1]}, \dots, u_{0[n]})$$

which implies (1).

The identity (1) establishes a relationship between the approximation vector  $\mathbf{h}(\mathbf{m})$  and the conjugates of  $\omega = \mathbf{m} \cdot \mathbf{u} \in M^*$ . Ultimately using (U.C.), the conjecture defined in Section 2, to obtain a "suitable" unit  $\gamma \in \mathcal{R}(M^*)$ , we will have  $\psi = \gamma\omega = \mathbf{m}' \cdot \mathbf{u} \in M^*$  for which the entries of  $(\mathbf{m}' \cdot \mathbf{u}_1, \dots, \mathbf{m}' \cdot \mathbf{u}_n) = (\psi_{[1]}, \dots, \psi_{[n]})$  determine an "appropriate" approximation vector  $\mathbf{h}(\mathbf{m}')$ .

By (1) and the definition in Section 3 of the map  $g$

$$(2) \quad g(\mathbf{h}(\mathbf{m}) \cdot U_1) = \prod_{j=1}^n |m_0|^{1/n} |\mathbf{m} \cdot \mathbf{u}_j| = |m_0/\mathbf{m} \cdot \mathbf{u}| |N(\mathbf{m} \cdot \mathbf{u})|.$$

We will construct infinite subsets of  $\mathbf{Z}_*^{n+1}$  for which in (2) above  $|m_0/\mathbf{m} \cdot \mathbf{u}| = 1 + o(1)$ .

For  $\omega \neq 0$  in  $M^*$  and  $\Gamma = (\gamma_k, k = 1, 2, \dots)$  a Peck sequence in  $\mathcal{R}(M^*)$  we define

$$Z[\omega; \Gamma] = \{\mathbf{m}_k \in \mathbf{Z}^{n+1}: \gamma_k\omega = \mathbf{m}_k \cdot \mathbf{u}, k = 1, 2, \dots\}.$$

For  $\mathbf{m}_k = (m_{k0}, \dots, m_{kn}) \in Z[\omega; \Gamma]$  we will show

$$(3) \quad m_{k0} \neq 0, \quad \text{for all sufficiently large } k.$$

By our definitions

$$m_{k0} = 0 \Rightarrow (m_{k1}, \dots, m_{kn}) = (\gamma_{k[1]}\omega_{[1]}, \dots, \gamma_{k[n]}\omega_{[n]})U_1^{-1}.$$

But by Lemma 1  $\gamma_{k[j]}\omega_{[j]} \rightarrow 0$ , as  $k \rightarrow \infty$ ,  $j = 1, \dots, n$ . So if  $m_{k0} = 0$  and  $k$  sufficiently large we must have  $\mathbf{m}_k = 0 \in \mathbf{Z}^{n+1}$  contradicting  $\gamma_k \neq 0$  and proving (3).

Next we show there exists  $J \geq 1$  so that

$$(4) \quad \|\mathbf{h}(\mathbf{m}_k)\| < J, \quad \text{for } \mathbf{m}_k \in Z[\omega; \Gamma].$$

By the definition of  $Z[\omega; \Gamma]$  and properties of  $\Gamma$

- (a)  $|N(\mathbf{m}_k \cdot \mathbf{u})| = |N(\omega)| = \eta$ , say,
- (b)  $|\mathbf{m}_k \mathbf{u}| \rightarrow \infty$ , as  $k \rightarrow \infty$ ,
- (c) For any  $\delta > 0$ , and all sufficiently large  $k$

$$\mathbf{m}_k \cdot \mathbf{u}_j / \mathbf{m}_k \cdot \mathbf{u}_1 = \omega_{[j]} / \omega_{[1]} + \delta_{kj}, \quad |\delta_{kj}| < \delta, \quad j = 2, \dots, n.$$

We rewrite (c) in the form

$$(d) |m_{k0}|^{1/n} (\mathbf{m}_k \cdot \mathbf{u}_1, \dots, \mathbf{m}_k \cdot \mathbf{u}_n) = \rho_k (\omega + \omega_{[1]}\delta_k) \text{ where } \omega = (\omega_{[1]}, \dots, \omega_{[n]}),$$

$$\delta_k = (0, \delta_{k2}, \dots, \delta_{kn}) \text{ and } \rho_k = |m_{k0}|^{1/n} \mathbf{m}_k \cdot \mathbf{u}_1 / \omega_{[1]}.$$

By (d) and identity (1)

$$(e) \mathbf{h}(\mathbf{m}_k) \cdot U_1 = \rho_k (\omega + \omega_{[1]}\delta_k).$$

We need to show

$$(f) \rho_k = O(1).$$

Note by (c) that

$$\prod_{j=1}^n |\mathbf{m}_k \cdot \mathbf{u}_j / \mathbf{m}_k \cdot \mathbf{u}_1| = (1 + O(\delta)) \prod_{j=1}^n |\omega_{[j]} / \omega_{[1]}|.$$

But

$$\eta = \prod_{j=0}^n |\mathbf{m}_k \cdot \mathbf{u}_j| = |\mathbf{m}_k \cdot \mathbf{u} / m_{k0}| \cdot |m_{k0}| \cdot |\mathbf{m}_k \cdot \mathbf{u}_1|^n \prod_{j=1}^n |\mathbf{m}_k \cdot \mathbf{u}_j / \mathbf{m}_k \cdot \mathbf{u}_1|.$$

So by above and definition of  $\rho_k$

$$\eta = (1 + O(\delta)) |\mathbf{m}_k \cdot \mathbf{u} / m_{k0}| |\rho_k|^n \prod_{j=1}^n |\omega_{[j]}|.$$

Then (f) follows if we can show  $m_{k0} / \mathbf{m}_k \cdot \mathbf{u} = O(1)$ . We suppose  $m_{k0} / \mathbf{m}_k \cdot \mathbf{u} \neq O(1)$ . So for any  $J' > 1$ ,

$$(g) \quad |m_{k0} / \mathbf{m}_k \cdot \mathbf{u}| > J' \quad \text{for some } \mathbf{m}_k \in Z[\omega; \Gamma].$$

By (a), (b) and (c) it easily follows that for any  $\varepsilon > 0$ ,

$$|\mathbf{m}_k \cdot \mathbf{u}_j| < \varepsilon, \quad j = 1, \dots, n, \text{ all sufficiently large } k$$

and so

$$|\mathbf{m}_k \cdot \mathbf{u}_j / m_{k0}| < \varepsilon, \quad j = 1, \dots, n, \text{ all sufficiently large } k.$$

We write

$$\mathbf{m}_k \cdot \mathbf{u}_j / m_{k0} = \varepsilon_{kj}, \quad j = 0, \dots, n, \text{ and } \varepsilon_k = (\varepsilon_{k0}, \dots, \varepsilon_{kn}).$$

For  $J' > \varepsilon^{-1}$  we have by (g) and above that

$$\|\varepsilon_k\| < \varepsilon \text{ for some } \mathbf{m}_k \in Z[\omega; \Gamma].$$

But for  $\varepsilon > 0$  sufficiently small this gives the contradiction

$$1 \leq \|m_{k0}^{-1} \mathbf{m}_k\| = \|m_{k0}^{-1} \mathbf{m}_k U U^{-1}\| = \|\varepsilon_k U^{-1}\| = O(\varepsilon).$$

Thus (g) is false and (f) is proven. Finally (4) follows by (e) and (f).

We now prove

$$(5) \quad |m_{k0}| \rightarrow \infty, \text{ as } k \rightarrow \infty.$$

Observe for  $\mathbf{m} \in \mathbf{Z}_*^{n+1}$ , recalling  $\alpha_0 = (1, \alpha_1, \dots, \alpha_n)$ ,

$$\mathbf{m} = m_0 \alpha_0 + (0, m_1 - m_0 \alpha_1, \dots, m_n - m_0 \alpha_n).$$

But  $\alpha_0 \cdot \mathbf{u} = 1$ , as  $AU = I$ , and so  $\mathbf{m} \cdot \mathbf{u} = m_0 + \sum_{j=1}^n (m_j - m_0 \alpha_j) u_j$  and for (fixed)  $J \geq 1$ ,

$$\|\mathbf{h}(\mathbf{m})\| < J \Rightarrow \left| \sum_{j=1}^n (m_j - m_0 \alpha_j) u_j \right| < (J/|m_0|^{1/n}) \sum_{j=1}^n |u_j|.$$

In fact, putting  $\mathbf{m} = \mathbf{m}_k$ , we have by (4) and above, since  $|\mathbf{m}_k \cdot \mathbf{u}| \rightarrow \infty$ , as  $k \rightarrow \infty$ ,

$$(6) \quad \lim_{k \rightarrow \infty} m_{k0} / \mathbf{m}_k \cdot \mathbf{u} = 1.$$

Then (5) immediately follows.

We now define for each  $\sigma \in \Sigma$  and  $J \geq 1$ ,

$$Z(\sigma, J) = \{\mathbf{m} \in \mathbf{Z}_*^{n+1}: \|\mathbf{h}(\mathbf{m})\| < J, \text{ and } \sigma(\mathbf{m} \cdot \mathbf{u}) = \sigma\},$$

$$W(\sigma, J) = \{\mathbf{m} \in Z(\sigma, J): |N(\mathbf{m} \cdot \mathbf{u})| = \eta_\sigma^*\}.$$

For fixed  $\sigma \in \Sigma$  let  $\omega \in M^*$  with  $\sigma(\omega) = \sigma$  and  $|N(\omega)| = \eta_\sigma^*$ . (That  $\omega$  exists has been noted earlier.)

By (3), (4) and our definitions there exists  $J \geq 1$  such that  $Z[\omega; \Gamma]$  is an infinite subset of  $W(\sigma, J)$  and so there exists  $\mathbf{m} \in W(\sigma, J) \subseteq Z(\sigma, J)$  with  $|m_0|$  arbitrarily large. Then, as we proved (6) but now letting  $|m_0| \rightarrow \infty$  we have

$$(7) \quad m_0 / \mathbf{m} \cdot \mathbf{u} \rightarrow 1 \text{ as } |m_0| \rightarrow \infty, \text{ for } \mathbf{m} \in Z(\sigma, J).$$

Then by (2), (7) and definition of  $W(\sigma, J)$

$$(8) \quad g(\mathbf{h}(\mathbf{m}) \cdot U_1) \rightarrow \eta_\sigma^*, \text{ as } |m_0| \rightarrow \infty, \text{ for } \mathbf{m} \in W(\sigma, J).$$

Also by the discreteness of norm values there exists  $\epsilon_0 > 0$  such that

$$(8') \quad g(\mathbf{h}(\mathbf{m}) \cdot U_1) > (1 + \epsilon_0)\eta_\sigma^*, \quad \text{for } \mathbf{m} \in Z(\sigma, J) - W(\sigma, J) \text{ with } |m_0|$$

sufficiently large.

For each  $\sigma \in \Sigma$  the surface  $K_\sigma$  in  $\mathbf{R}^n$  is defined by

$$K_\sigma = \{\mathbf{x} \in \mathbf{R}^n: \sigma(\mathbf{x}U_1) = \sigma, \text{ and } g(\mathbf{x}U_1) = \eta_\sigma^*\}.$$

We put

$$K = \bigcup_{\sigma \in \Sigma} K_\sigma.$$

Given  $\lambda > 0$  we say  $\mathbf{x}$  is *inside*  $\lambda K = \{\lambda \mathbf{y}: \mathbf{y} \in K\}$  if  $\rho \mathbf{x} \in \lambda K$  for some  $\rho \geq 1$ .

We have proved above the following lemma.

LEMMA 2. For any  $\sigma$  in  $\Sigma$ ,  $J \geq 1$  such that  $W(\sigma, J)$  is an infinite set, and  $\epsilon$  with  $0 < \epsilon < 1$ ,

(i)  $\mathbf{h}(\mathbf{m})$  is inside  $(1 + \epsilon)K$  but not inside  $(1 - \epsilon)K$  for all  $\mathbf{m} \in W(\sigma, J)$  with  $|m_0|$  sufficiently large.

(ii) there exists  $\epsilon_0 > 0$ , not dependent on  $\epsilon$ , such that  $\mathbf{h}(\mathbf{m})$  is not inside  $(1 + \epsilon_0)K$  for all  $\mathbf{m} \in Z(\sigma, J) - W(\sigma, J)$  with  $|m_0|$  sufficiently large.

Lemma 2 and the following Lemma 3 go back to the thesis of the second author [4]. Observe Lemma 2 does not depend on (U.C.).

LEMMA 3. Let  $\sigma \in \Sigma$  and  $\mathbf{x} \in K_\sigma \subseteq K$ . Then, assuming (U.C.), for any  $\epsilon > 0$  there exist  $J \geq 1$  and infinitely many  $\mathbf{m} \in W(\sigma, J)$  such that

$$\|\mathbf{h}(\mathbf{m}) - \mathbf{x}\| < \epsilon.$$

PROOF. Put  $\mathbf{y} = (y_1, \dots, y_n) = \mathbf{x}U_1 \in \mathbf{C}^{r,s}$ . As  $\mathbf{x} \in K_\sigma$ ,  $\sigma(\mathbf{y}) = \sigma(\mathbf{x}U_1) = \sigma$ . Let  $\psi \neq 0$  in  $M^*$  with  $\sigma(\psi) = \sigma$  and  $|N(\psi)| = \eta_\sigma^*$ . Observe that since  $\sigma(\mathbf{y}) = \sigma(\psi) = \sigma$ ,

$$\frac{\psi_{[1]}y_j}{\psi_{[j]}y_1} > 0, \quad j = 1, \dots, r.$$

Then, assuming (U.C.) for any  $\delta' > 0$  there exists a unit  $\gamma$  in  $\mathcal{R}(M^*)$ , with  $\gamma_{[j]} > 0$ ,  $j = 1, \dots, r$ , such that

$$(9) \quad \frac{\gamma_{[j]}}{\gamma_{[1]}} = \frac{\psi_{[1]}y_j}{\psi_{[j]}y_1} + \delta'_j, \quad |\delta'_j| < \delta', \quad j = 2, \dots, n.$$

We put  $\omega = \gamma\psi$ . Then

$$\omega = (\omega_{[1]}, \dots, \omega_{[n]}) = (\omega_{[1]}/y_1)\mathbf{y} + \delta'$$

where  $\delta' = \gamma_{[1]}(0, \psi_{[1]}\delta'_2, \dots, \psi_{[n]}\delta'_n)$ .

For any Peck sequence in  $\mathcal{R}(M^*)$ ,  $\Gamma$ , there exists, by (4) above,  $J \geq 1$  such that

$$Z[\omega; \Gamma] \subseteq W(\sigma, J).$$

Choosing in (c) above  $0 < \delta < \delta'$  we substitute for  $\omega$  in (e), recalling,  $\mathbf{y} = xU_1$ , to get

$$(10) \quad \mathbf{h}(\mathbf{m}_k) = \rho'_k \mathbf{x} + \delta'_k$$

where  $\rho'_k = \rho_k \omega_{[1]}/y_1 = |m_{k0}|^{1/n} \mathbf{m}_k \cdot \mathbf{u}_1/y_1$  and  $\delta'_k = \rho_k(\delta' + \omega_{[1]}\delta_k) \cdot U_1^{-1}$ .

As shown in (f)  $\rho_k = O(1)$  and so  $\|\delta'_k\| = O(\delta')$ . We can, in fact, use (9), (6) and  $\eta_\sigma^* = |N(\mathbf{m}_k \cdot \mathbf{u})| = \prod_{j=1}^n |y_j|$  to show  $\rho'_k = 1 + O(\delta')$ , the proof then following from (10) by choosing  $\delta' > 0$  sufficiently small. But since  $\rho'_k = \rho_k \omega_{[1]}/y_1 = O(1)$  and  $\sigma(\mathbf{h}(\mathbf{m}_k) \cdot U_1) = \sigma(\mathbf{x}U_1) = \sigma$  the proof follows from (i) of Lemma 2 using (10) and (5) above for sufficiently large  $k$  and sufficiently small  $\delta' > 0$ .

We now complete the proof of (i) and (i') of Theorem 1. For each  $\sigma \in \Sigma$  let

$$\mathcal{X}_\sigma = \{\mathbf{x} \in \mathbf{R}^n: \sigma(\mathbf{x}U_1) = \sigma, \text{ and } g(\mathbf{x}U_1) = 1\}.$$

Observe

$$\mathcal{K}_\sigma = \eta_\sigma^{*1/n} \mathcal{X}_\sigma.$$

We also define for  $t > 0$  the box in  $\mathbf{R}^n$

$$B_t = \{\mathbf{x} \in \mathbf{R}^n: \|\mathbf{x}\|^n \leq t\}.$$

It follows from Lemma 2 and the definition of  $c(\alpha)$

$$\begin{aligned} c(\alpha) &\geq \sup\{t: \text{(each point of)} B_t \text{ is inside } \mathcal{K}\} \\ &= \min_{\sigma \in \Sigma} \inf\{t: B_t \cap \mathcal{K}_\sigma \text{ is not empty}\} \\ &= \min_{\sigma \in \Sigma} \inf\{\|\mathbf{x}\|^n: \mathbf{x} \in \mathcal{K}_\sigma\} \\ &= \min_{\sigma \in \Sigma} \inf\{\eta_\sigma^* \|\eta_\sigma^{*-1/n} \mathbf{x}\|^n: \eta_\sigma^{*-1/n} \mathbf{x} \in \mathcal{X}_\sigma\} \\ &= \min_{\sigma \in \Sigma} \eta_\sigma^* \inf\{\|\mathbf{x}\|^n: \mathbf{x} \in \mathcal{X}_\sigma\}. \end{aligned}$$

By Lemma 3, and assuming (U.C.) equality holds and

$$c(\alpha) = \min_{\sigma \in \Sigma} \eta_\sigma^* \inf\{\|\mathbf{x}\|^n: \mathbf{x} \in \mathcal{X}_\sigma\}.$$

But

$$\begin{aligned} \inf\{\|\mathbf{x}\|^n: \mathbf{x} \in \mathcal{X}_\sigma\} &= \inf\{\|\mathbf{x}\|^n: g(\mathbf{x}U_1) = 1, \sigma(\mathbf{x}U_1) = \sigma\} \\ &= \inf\{\|\mathbf{x}\|^n/g(\mathbf{x}U_1): \mathbf{x} \in \mathbf{R}^n, \sigma(\mathbf{x}U_1) = \sigma\}, \\ &\quad \text{by homogeneity,} \\ &= \inf\{1/g(\mathbf{x}U_1): \mathbf{x} \in \mathbf{R}^n, \|\mathbf{x}\| = 1, \sigma(\mathbf{x}U_1) = \sigma\}, \\ &\quad \text{by homogeneity,} \\ &= 1/\max\{g(\mathbf{x}U_1): \mathbf{x} \in \mathbf{R}^n, \|\mathbf{x}\| = 1, \sigma(\mathbf{x}U_1) = \sigma\}, \\ &\quad \text{by homogeneity.} \end{aligned}$$

This completes the proof of (i) and (i') of Theorem 1.

### 5. Proof of (ii) and (ii') of Theorem 1

The proof may be brief where it follows that for (i) and (i') of Theorem 1.

In this section  $\mathbf{m} = (m_0, \dots, m_n)^t \in \mathbf{Z}^{n+1}$  with  $\overline{\mathbf{m}}$  the projection on  $\mathbf{m}$  defined by  $\overline{\mathbf{m}} = (m_1, \dots, m_n)^t$ . We need only consider elements of

$$\mathbf{Z}_{**}^{n+1} = \left\{ \mathbf{m} \in \mathbf{Z}^{n+1}: \|\overline{\mathbf{m}}\| = \max_{1 \leq j \leq n} |m_j| > 0 \right\}.$$

Recalling  $\alpha_0 = 1$  we write

$$\alpha_i = (\alpha_{0[i]}, \dots, \alpha_{n[i]}) = i\text{th row of } A, \quad i = 0, \dots, n.$$

So for  $\mathbf{m} \in \mathbf{Z}_{**}^{n+1}$ ,

$$\alpha_i \cdot \mathbf{m} = \sum_{j=0}^n \alpha_{j[i]} m_j = i\text{th conjugate of } \alpha_0 \cdot \mathbf{m} \in M.$$

We often write for  $\mathbf{m}, \mathbf{m}_k \in \mathbf{Z}_{**}^{n+1}$ ,

$$\phi = \phi(\mathbf{m}) = \alpha_0 \cdot \mathbf{m}, \quad \text{and} \quad \phi_k = \phi(\mathbf{m}_k) = \alpha_0 \cdot \mathbf{m}_k.$$

The dual approximation vector of  $\mathbf{m} \in \mathbf{Z}_{**}^{n+1}$  is defined by

$$\mathbf{h}^*(\mathbf{m}) = |\alpha_0 \cdot \mathbf{m}|^{1/n} (m_1, \dots, m_n)^t = |\phi|^{1/n} \overline{\mathbf{m}}, \quad \phi = \phi(\mathbf{m}).$$

It is a classical result that infinitely many dual approximation vectors exist with  $\|\mathbf{h}(\mathbf{m})\| < 1$ .

The following identity—analogue to (1)—is easily shown

$$(11) \quad A_1 \cdot \mathbf{h}^*(\mathbf{m}) = |\phi|^{1/n} (\phi_{[1]} - \phi, \dots, \phi_{[n]} - \phi)^t, \quad \phi = \phi(\mathbf{m}).$$

Thus

$$(12) \quad g(A_1 \mathbf{h}^*(\mathbf{m})) = |N(\phi)| \prod_{j=1}^n |1 - \phi/\phi_{[j]}|, \quad \phi = \phi(\mathbf{m}).$$

Infinite subsets of  $\mathbf{Z}_{**}^{n+1}$  where  $\prod_{j=1}^n |1 - \phi/\phi_{[j]}| = 1 + o(1)$  are constructed. For  $\omega \neq 0$  in  $M$  and  $\Gamma = (\gamma_k, k = 1, 2, \dots)$  a Peck sequence in  $\mathcal{R}(M)$

$$Z^*[\omega; \Gamma] = \{\mathbf{m}_k \in \mathbf{Z}^{n+1}: \gamma_k^{-1} \omega = \alpha_0 \cdot \mathbf{m}_k, k = 1, 2, \dots\}.$$

Trivially for  $\mathbf{m}_k = (m_{k0}, \dots, m_{kn})^t \in Z^*[\omega; \Gamma]$

$$(13) \quad \overline{\mathbf{m}}_k \neq 0 \in \mathbf{Z}^n, \quad \text{for (nearly) all } k.$$

We will show there exists  $J \geq 1$ , so that

$$(14) \quad \|\mathbf{h}^*(\mathbf{m}_k)\| < J, \quad \text{for } \mathbf{m}_k \in Z^*[\omega; \Gamma].$$

Clearly for  $\mathbf{m}_k \in Z^*[\omega; \Gamma]$ , with  $\phi_k = \phi(\mathbf{m}_k)$ ,

- (a)  $|N(\phi_k)| = |N(\omega)|$ ,
- (b)  $\phi_k = \omega/\gamma_k \rightarrow 0$ , as  $k \rightarrow \infty$ ,
- (c) For any  $\delta > 0$  and all sufficiently large  $k$ ,

$$\phi_{k[j]}/\phi_{k[1]} = \omega_{[j]}/\omega_{[1]} + \delta_{kj}, \quad |\delta_{kj}| < \delta, \quad j = 2, \dots, n.$$

Employing here (b) as well as (c) we have

- (d)  $|\phi_k|^{1/n}(\phi_{k[1]} - \phi_k, \dots, \phi_{k[n]} - \phi_k)^t = \rho_k(\omega + \omega_{[1]}\delta_k) + o(1)$ , where

$$\omega = (\omega_{[1]}, \dots, \omega_{[n]})^t, \quad \delta_k = (0, \delta_{k2}, \dots, \delta_{kn})^t$$

and

$$\rho_k = |\phi_k|^{1/n} \phi_{k[1]}/\omega_{[1]} = |\omega|^{1/n}/(\gamma_k^{1/n} \gamma_{k[1]}).$$

By (d) and (11)

- (e)  $A_1 \cdot \mathbf{h}^*(\mathbf{m}_k) = \rho_k(\omega + \omega_{[1]}\delta_k) + o(1)$ . Clearly, as  $\gamma_k^{1/n} \gamma_{k[1]} \rightarrow 1$ , as  $k \rightarrow \infty$ .
- (f)  $\rho_k = O(1)$ , and (14) follows immediately from (e).

Observe  $\|\overline{\mathbf{m}}_k\| = O(1) \Leftrightarrow \|\mathbf{m}_k\| = \max_{0 \leq j \leq n} |m_{kj}| = O(1)$ , as  $m_{k0} = -\alpha \cdot \overline{\mathbf{m}}_k + o(1)$ . So, as there are infinitely many  $\mathbf{m}_k \in Z^*[\omega; \Gamma]$ ,

$$(15) \quad \|\overline{\mathbf{m}}_k\| \rightarrow \infty, \quad \text{as } k \rightarrow \infty.$$

For each  $\sigma \in \Sigma$  and  $J \geq 1$ , we define

$$Z^*(\sigma, J) = \{\mathbf{m} \in Z_{**}^{n+1}: \|\mathbf{h}^*(\mathbf{m})\| < J, \text{ and } \sigma(\alpha_0 \cdot \mathbf{m}) = \sigma\},$$

$$W^*(\sigma, J) = \{\mathbf{m} \in Z^*(\sigma, J): |N(\alpha_0 \cdot \mathbf{m})| = \eta_\sigma\}.$$

For fixed  $\sigma \in \Sigma$  let  $\omega \in M$  with  $\sigma(\omega) = \sigma$  and  $|N(\omega)| = \eta_\sigma$ . By (13) and (14) there exists  $J \geq 1$  such that

$$Z^*[\omega; \Gamma] \subseteq W^*(\sigma, J) \subseteq Z^*(\sigma, J).$$

We need to show

$$(16) \quad \lim_{\|\overline{\mathbf{m}}\| \rightarrow \infty} \phi/\phi_{[j]} = 0, \quad j = 1, \dots, n, \text{ for } \phi = \phi(\mathbf{m}), \mathbf{m} \in Z^*(\sigma, J).$$

Suppose (16) is false. Then there exists  $\delta > 0$  so that for any  $K > 1$

$$|\phi/\phi_{[j]}| > \delta, \text{ at least one } j = 1, \dots, n, \text{ some } \phi = \phi(\mathbf{m}) \text{ with } \|\overline{\mathbf{m}}\| > K.$$

Without loss of generality we suppose  $j = 1$  and then

$$|\phi_{[1]}| < |\phi|/\delta.$$

But then

$$\delta^{-1}|\phi|^2 \prod_{j=2}^n |\phi_{[j]}| > \prod_{j=0}^n |\phi_{[j]}| \geq \eta_\sigma.$$

Then for at least one  $j = 2, \dots, n$ , say  $j = 2$ ,

$$|\phi_{[2]}| > |\phi|^{-2/(n-1)}(\eta_\sigma \delta)^{1/(n-1)}$$

and so

$$|\phi|^{1/n}|\phi_{[2]}| > (|\phi|^{-1/n})^{(n+1)/(n-1)}(\eta_\sigma\delta)^{1/(n-1)}.$$

But  $\phi = \phi(\mathbf{m})$ ,  $\mathbf{m} \in Z^*(\sigma, J)$  with  $\|\overline{\mathbf{m}}\| > K$  and so

$$|\phi|^{1/n} < J/\|\overline{\mathbf{m}}\| < J/K.$$

Substituting in the right side of the previous inequality

$$|\phi|^{1/n}|\phi_{[2]}| > (K/J)^{(n+1)/(n-1)}(\eta_\sigma\delta)^{(1)/(n-1)}.$$

But by (11) since  $\|\mathbf{h}^*(\mathbf{m})\| = O(1)$  we must have  $|\phi|^{1/n}\phi_{[2]} = O(1)$  which is contradicted by the above inequality as  $K$  may be arbitrarily large. This contradiction proves (16). Then by (16)

$$(17) \quad \prod_{j=1}^n |1 - \phi/\phi_{[j]}| \rightarrow 1, \quad \text{as } \|\overline{\mathbf{m}}\| \rightarrow \infty, \text{ for } \phi = \phi(\mathbf{m}), \mathbf{m} \in Z^*(\sigma, J).$$

By (12), (17) and our definitions of  $W^*(\sigma, J)$ ,  $Z^*(\sigma, J)$

$$(18) \quad g(\mathbf{A}_1 \cdot \mathbf{h}^*(\mathbf{m})) \rightarrow \eta_\sigma, \quad \text{as } \|\overline{\mathbf{m}}\| \rightarrow \infty, \text{ for } \mathbf{m} \in W^*(\sigma, J)$$

and there exists  $\varepsilon_0 > 0$  such that

$$(18') \quad g(\mathbf{A}_1 \cdot \mathbf{h}^*(\mathbf{m})) > (1 + \varepsilon_0)\eta_\sigma, \quad \text{for } \mathbf{m} \in Z^*(\sigma, J) - W^*(\sigma, J) \\ \text{with } \|\overline{\mathbf{m}}\| \text{ sufficiently large.}$$

For each  $\sigma \in \Sigma$  the surface  $K_\sigma^*$  is defined by

$$K_\sigma^* = \{\mathbf{x} \in \mathbf{R}^n: \sigma(\mathbf{A}_1\mathbf{x}) = \sigma, \text{ and } g(\mathbf{A}_1\mathbf{x}) = \eta_\sigma\}.$$

We put  $K^* = \bigcup_{\sigma \in \Sigma} K_\sigma^*$ . We have proved

LEMMA 4. For any  $\sigma$  in  $\Sigma$ ,  $J \geq 1$  such that  $W^*(\sigma, J)$  is an infinite set, and  $\varepsilon$  with  $0 < \varepsilon < 1$ .

(i)  $h^*(\mathbf{m})$  is inside  $(1 + \varepsilon)K^*$  but not inside  $(1 - \varepsilon)K^*$  for all  $\mathbf{m} \in W^*(\sigma, J)$  with  $\|\overline{\mathbf{m}}\|$  sufficiently large.

(ii) there exists  $\varepsilon_0 > 0$  not dependent on  $\varepsilon$ , such that  $h^*(\mathbf{m})$  is not inside  $(1 + \varepsilon_0)K^*$  for all  $\mathbf{m} \in Z^*(\sigma, J) - W^*(\sigma, J)$  with  $\|\overline{\mathbf{m}}\|$  sufficiently large.

Lemma 4 is the analogue of Lemma 2. We give Lemma 5, the analogue of Lemma 3, without proof since its proof is virtually identical to the proof of Lemma 3.

LEMMA 5. Let  $\sigma \in \Sigma$  and  $\mathbf{x} \in K_\sigma^* \subseteq K$ . Then, assuming (U.C.), for any  $\varepsilon > 0$  there exists  $J \geq 1$  and infinitely many  $\mathbf{m} \in W^*(\sigma, J)$  such that

$$\|\mathbf{h}^*(\mathbf{m}) - \mathbf{x}\| < \varepsilon.$$

Finally we observe (ii) and (ii') of Theorem 1 follow from Lemmas 4 and 5 by precisely the same arguments proving (i) and (i') of Theorem 1 from Lemmas 2 and 3.

### References

- [1] W. W. Adams, 'Simultaneous asymptotic diophantine approximations to a basis of a real cubic number field', *J. Number Theory* **1** (1969), 179–194.
- [2] J. Ax, 'On Schanuel's Conjecture', *Ann. of Math.* **93** (1971), 252–268.
- [3] T. W. Cusick, 'Formulas for some diophantine approximation constants, II', *Acta Arithmetica* **26** (1974–75), 117–128.
- [4] S. Krass, *The n-dimensional diophantine approximation constants* (Ph.D. Thesis, University of New South Wales, 1984).
- [5] S. Krass, 'On a conjecture of Littlewood in diophantine approximations', *Bull. Austral. Math. Soc.* **32** (1985), 379–387.
- [6] L. G. Peck, 'Simultaneous rational approximations to algebraic numbers', *Bull. Amer. Math. Soc.* **67** (1961), 197–201.

Department of Mathematics  
State University of New York  
Buffalo, New York 14214  
U.S.A.

School of Mathematics  
University of New South Wales  
Kensington, New South Wales 2033  
Australia