

Diophantine Approximation of Ternary Linear Forms*

By T. W. Cusick

Abstract. The paper gives an efficient method for finding arbitrarily many solutions in integers x, y, z of the Diophantine inequality $|x + \alpha y + \beta z| \max(y^2, z^2) < c$, where α defines a totally real cubic field F over the rationals, the numbers $1, \alpha, \beta$ form an integral basis for F , and c is a constant which can be calculated in terms of parameters of the method. For certain values of c , the method generates all solutions of the inequality.

1. Introduction. The following theorem is a standard result in the theory of Diophantine approximation [1, p. 14]:

Let n be any positive integer and let $\theta_1, \dots, \theta_n$ be any n real numbers; then for any constant $c \geq 1$ there exist infinitely many solutions of

$$|\theta_1 x_1 + \dots + \theta_n x_n - y| \max_{1 \leq i \leq n} |x_i|^n < c$$

in integers x_1, \dots, x_n, y .

If $n = 1$, the continued fraction algorithm enables us to actually calculate arbitrarily many solutions x_1, y of the above inequality with $c = 1$ for any given θ_1 . If $n > 1$, I do not know of any method for finding arbitrarily many solutions which is both efficient and applicable to a wide class of $\theta_1, \dots, \theta_n$.

The purpose of this paper is to give an efficient method for finding arbitrarily many solutions in integers x, y, z of

$$|x + \alpha y + \beta z| \max(y^2, z^2) < c,$$

where α defines a totally real cubic field F over the rationals, the numbers $1, \alpha, \beta$ form an integral basis for F , and c is a constant which can be calculated in terms of parameters of the method. For small values of c , the method generates *all* solutions of the inequality (see Section 7 below).

There is a paper by Peck [4] which discusses the dual problem of simultaneous Diophantine approximation to two irrationals in a cubic field; indeed, the general problem of simultaneous approximation to $n \geq 2$ irrationals in an algebraic number field of degree $n + 1$ is treated. However, Peck does not deal with the problem of actually finding solutions to the Diophantine inequalities; his approach gives information on other aspects of the situation (see the results in [4]).

The method of this paper can readily be used for actual machine computation of solutions. I have attempted to write the proofs with this end in view, even if this results in some sacrifice of brevity. A numerical example of the application of the method is given in Section 6.

Received February 26, 1970.

AMS 1969 subject classifications. Primary 1030, 1003.

Key words and phrases. Diophantine inequality, ternary linear forms, totally real cubic field.

* This research was partially supported by NSF grant GP-12042 to SUNY at Buffalo.

Copyright © 1971, American Mathematical Society

The first step in applying the method is to find a pair θ, φ of fundamental units with norm 1 in F , such that θ and its conjugates satisfy certain inequalities (formula (27) in Section 5 below). In order to simplify the exposition, I give complete details of the method only in the special case in which $\beta = \alpha^2$ and $\alpha = \theta$. The modifications necessary to deal with the more general form $x + \alpha y + \beta z$ are discussed in Section 5.

2. A Paper of Minkowski. Let $\xi = \xi_1x + \xi_2y + \xi_3z, \eta = \eta_1x + \eta_2y + \eta_3z, \zeta = \zeta_1x + \zeta_2y + \zeta_3z$ be three real linear forms with positive determinant Δ . The inequalities $|\xi| \leq \rho, |\eta| \leq \sigma, |\zeta| \leq \tau$ define a parallelepiped symmetric with respect to the origin in three-dimensional space. Let $\{\rho, \sigma, \tau\}$ denote this parallelepiped. Suppose that $\{\rho, \sigma, \tau\}$ has no integer lattice points other than the origin in its interior, but has at least one lattice point not on an edge on each of its six faces. Minkowski [3] called a parallelepiped with these properties *extremal*, and I adopt his definition. Clearly $\{\rho, \sigma, \tau\}$ is extremal if and only if its interior contains no lattice point other than the origin and no one of its defining parameters ρ, σ, τ can be increased without introducing a lattice point into the interior.

Minkowski's paper [3] is mainly devoted to a detailed discussion of extremal parallelepipeds. In particular, he stated the following:

THEOREM A (MINKOWSKI [3, p. 281]). *Let ξ, η, ζ be any three real ternary linear forms with positive determinant Δ and with the property that none of ξ, η, ζ vanishes for any integral point other than the origin. If $\{a, g, l\}$ is an extremal parallelepiped for ξ, η, ζ , then $agl < \Delta$. There is exactly one integral lattice point in each face of $\{a, g, l\}$, the points in opposite faces having coordinates with opposite signs. One can always find in one and only one way three lattice points (r_i, s_i, t_i) ($i = 1, 2, 3$) in the respective planes $\xi = \epsilon_1a, \eta = \epsilon_2g, \zeta = \epsilon_3l$ ($\epsilon_i = \pm 1$) such that $\epsilon_1\epsilon_2\epsilon_3 = 1$ and such that, if the matrix P is defined by*

$$P = \begin{bmatrix} r_1 & r_2 & r_3 \\ s_1 & s_2 & s_3 \\ t_1 & t_2 & t_3 \end{bmatrix},$$

then

$$\begin{bmatrix} \epsilon_1\xi_1 & \epsilon_1\xi_2 & \epsilon_1\xi_3 \\ \epsilon_2\eta_1 & \epsilon_2\eta_2 & \epsilon_2\eta_3 \\ \epsilon_3\zeta_1 & \epsilon_3\zeta_2 & \epsilon_3\zeta_3 \end{bmatrix} P = \begin{bmatrix} a & \pm b & \pm c \\ \pm f & g & \pm h \\ \pm j & \pm k & l \end{bmatrix} = \Phi, \text{ say,}$$

where the numbers $a, b, c, f, g, h, j, k, l$ are all positive and have signs agreeing with one of the following six systems:

I	II	III	IV	V	VI
+	+	+	+	+	+
+	-	-	+	-	-
-	+	+	-	+	-
-	-	+	+	+	-

Furthermore, $\det P = 1$ in cases I to V and $\det P = 0$ in case VI. In every case the inequalities

(1) $a > b, a > c, g > f, g > h, l > j, l > k$

hold, and in the separate cases the following further conditions are satisfied:

<p>I</p> $b + c > a$ $f > h \text{ or } j > k$	<p>II</p> $h + f > g$ $k > j \text{ or } b > c$	<p>III</p> $j + k > l$ $c > b \text{ or } h > f$	<p>IV</p> $b > c \text{ or } h > f$ $\text{or } j > k$
<p>V</p> $c > b \text{ or } f > h \text{ or } k > j$	<p>VI</p> $b + c = a, \quad f + h = g, \quad j + k = l$		

As Minkowski points out [3, p. 281], the restriction in Theorem A on the integral points for which ξ, η or ζ can vanish is made only for convenience in stating the theorem. In any case, all the linear forms considered in this paper will satisfy the conditions of Theorem A.

Following Minkowski, we say that the matrix P transforms the system $\epsilon_1\xi, \epsilon_2\eta, \epsilon_3\zeta$ to Φ , and that P (which is completely determined by $\{a, g, l\}$) is the matrix associated with $\{a, g, l\}$. We also say that P belongs to ξ, η, ζ .

The conditions of Theorem A, cases I to V, are not only necessary for a matrix to belong to ξ, η, ζ , but are also sufficient, because of the following:

THEOREM B (MINKOWSKI [3, p. 282]). *If an integral matrix P of determinant 1 is so chosen that it transforms $\epsilon_1\xi, \epsilon_2\eta, \epsilon_3\zeta$ with suitable signs $\epsilon_1, \epsilon_2, \epsilon_3$, into a matrix Φ which satisfies all the conditions of Theorem A for one of the cases I to V, then P is a matrix belonging to ξ, η, ζ .*

Minkowski went on to give a rather complicated algorithm by means of which all extremal parallelepipeds for ξ, η, ζ can be constructed from any given extremal parallelepiped. The algorithm associates with each extremal parallelepiped exactly three others called the neighbors of the given parallelepiped. For example, the ξ -neighbor of the extremal parallelepiped $\{\rho, \sigma, \tau\}$ is obtained by lowering the ξ -faces of $\{\rho, \sigma, \tau\}$ (that is, decreasing ρ) until each meets an integral point in one of the η - or ζ -faces; then the η - or ζ -faces, respectively, are raised until each meets an integral point. This process clearly results in a new extremal parallelepiped. The η -neighbor and ζ -neighbor of $\{\rho, \sigma, \tau\}$ are defined analogously. Minkowski proved that any extremal parallelepiped for ξ, η, ζ can be connected with any other by a sequence of neighbors, and he therefore called the totality of all extremal parallelepipeds for ξ, η, ζ the chain of extremal parallelepipeds for ξ, η, ζ .

The discussion in Sections 3 and 4 below makes no use of the Minkowski neighbor algorithm; what is important is that Theorems A and B give a complete characterization of all nonsingular matrices P which belong to ξ, η, ζ . In more general situations (see Section 5), some acquaintance with the Minkowski algorithm may be necessary. This algorithm is fully explained in a book by Hancock [2] and a paper by Zeisel [5].

Throughout this paper, F will denote a totally real cubic field with conjugate fields F' and F'' ; if ω is an element of F , the conjugates of ω will be denoted by ω' and ω'' .

Suppose the coefficients ξ_1, ξ_2, ξ_3 of ξ are an integral basis of F , and let η and ζ be the respective conjugate linear forms ξ' and ξ'' . The discriminant D of F is positive, and we may assume that the signs of ξ_1, ξ_2, ξ_3 have been chosen in such a way that the determinant of ξ, ξ', ξ'' is equal to $+\sqrt{D}$.

The norm function $\xi\eta\zeta = \xi\xi'\xi'' = N(\xi)$, say, is a cubic form in x, y, z with rational

integer coefficients and discriminant D . If P is any matrix belonging to ξ, η, ζ , and we apply the substitution $P[x' y' z']^T = [x y z]^T$ (here $[\dots]^T$ denotes a column vector) to the form $N(\xi)$, we obtain another form $N'(\xi)$ with integral coefficients and determinant D or 0 , depending on whether P has determinant 1 or 0 . We say that the matrix P transforms the form $N(\xi)$ into $N'(\xi)$.

Minkowski [3, p. 287] proved that transforming $N(\xi)$ by all of the infinitely many matrices P which belong to ξ, η, ζ results in only a finite number of different forms, and also obtained the following theorem.

THEOREM C (MINKOWSKI [3, p. 288]). *Let F be a totally real cubic field. Let ξ_1, ξ_2, ξ_3 be an integral basis of F and suppose*

$$\begin{aligned} \xi &= \xi_1x + \xi_2y + \xi_3z, \\ \eta &= \xi'_1x + \xi'_2y + \xi'_3z, \\ \zeta &= \xi''_1x + \xi''_2y + \xi''_3z. \end{aligned}$$

If $\{\rho, \sigma, \tau\}$ is an arbitrary extremal parallelepiped for ξ, η, ζ and P is the associated matrix, then if ω is an arbitrary unit of norm 1 in F and S is the integral matrix which satisfies

$$(2) \quad [\xi_1 \ \xi_2 \ \xi_3]S = [\omega\xi_1 \ \omega\xi_2 \ \omega\xi_3],$$

it follows that $\{\rho |\omega|^{-1}, \sigma |\omega'|^{-1}, \tau |\omega''|^{-1}\}$ is always an extremal parallelepiped for ξ, η, ζ . The matrix $S^{-1}P$ is associated with this parallelepiped and transforms $N(\xi)$ into the same form that P does.

Following Minkowski, we say that two external parallelepipeds which are related to each other in the manner described in Theorem C are *equivalent*. The chain of extremal parallelepipeds for ξ, η, ζ is divided up into a finite number of classes of equivalent parallelepipeds.

If S is an integral matrix satisfying (2), we say that S takes ξ to $\omega\xi$. Then, of course, S takes η to $\omega'\eta$ and ζ to $\omega''\zeta$; and, as Minkowski remarked [3, p. 288], this means $\det S = \omega\omega'\omega'' = 1$, since ω is assumed to have norm 1 .

Theorem C is the basis for the discussion which follows; this is the reason for considering only linear forms whose coefficients form an integral basis of a totally real cubic field.

3. Multiplicative Groups of Matrices with Two Generators. First, consider the general linear form $x + \alpha y + \beta z$, where α defines a totally real cubic field F over the rationals and $1, \alpha, \beta$ is an integral basis for F . Suppose θ is a unit of norm 1 in F such that θ and its conjugates satisfy

$$(3) \quad \theta > 1, \quad 0 > \theta' > -1, \quad -1 > \theta''$$

and

$$(4) \quad |\theta''| > \theta.$$

The need for these inequalities will become apparent later on. In fact, only a weaker form of the assumption (3) is actually required (see Section 5 below). The

stronger form given here is used to obtain the convenient but inessential Lemma 3 below.

Suppose the equation satisfied by $\theta, \theta', \theta''$ is

$$(5) \quad x^3 - d_2x^2 - d_1x - 1 = 0,$$

where d_1 and d_2 are rational integers, of course.

In accordance with the remarks in the introduction, we now specialize the linear form by taking $\alpha = \theta, \beta = \theta^2$. This, of course, places on θ the additional restriction that $1, \theta, \theta^2$ is an integral basis for F .

We are now prepared to begin looking at the method for finding solutions of $|x + \theta y + \theta^2 z| \max(y^2, z^2) < c$. We define

$$(6) \quad \begin{aligned} \xi &= -(x + \theta y + \theta^2 z), \\ \eta &= -(x + \theta' y + \theta'^2 z), \\ \zeta &= -(x + \theta'' y + \theta''^2 z). \end{aligned}$$

The determinant of these linear forms is $(\theta - \theta')(\theta - \theta'')(\theta' - \theta'')$, which is positive by (3).

If ω is any unit of norm 1 in F , let $Q(\omega)$ denote the matrix which takes ξ to $\omega\xi$. It is obvious from (5) and (6) that

$$Q(\theta) = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & d_1 \\ 0 & 1 & d_2 \end{bmatrix}.$$

Let φ be a unit with norm 1 such that θ and φ are a pair of fundamental units for F , and suppose for later convenience that $|\varphi| > 1$. Since $1, \theta, \theta^2$ is an integral basis for F , there exist unique integers A, B, C such that

$$(7) \quad \varphi = A + B\theta + C\theta^2.$$

Similar expressions for $\varphi\theta$ and $\varphi\theta^2$ can be calculated by using (5) and (7); we thus obtain

$$Q(\varphi) = \begin{bmatrix} A & C & B + d_2C \\ B & A + d_1C & C + d_1(B + d_2C) \\ C & B + d_2C & A + d_1C + d_2(B + d_2C) \end{bmatrix}.$$

LEMMA 1. *The set of matrices Γ defined by*

$$\Gamma = \{Q(\omega) : \omega \text{ is a unit with norm 1 in } F\}$$

is a commutative group under matrix multiplication with generators $Q(\theta)$ and $Q(\varphi)$.

Proof. Any unit ω with norm 1 in F is equal to $\theta^m\varphi^n$ for some unique integers m and n . Let $Q^{-1}(\omega)$ denote the inverse of the matrix $Q(\omega)$ and $Q^k(\omega)$ (k an integer) denote the k th power under matrix multiplication of $Q(\omega)$. It is obvious that $Q^{-1}(\omega) = Q(\omega^{-1})$ and $Q(\omega^k) = Q^k(\omega)$. Since $Q(\theta)$ and $Q(\varphi)$ clearly commute, we have $Q(\theta^m\varphi^n) = Q^m(\theta)Q^n(\varphi)$, which proves the lemma.

LEMMA 2. Each matrix in Γ has the form

$$\begin{bmatrix} -d_1b + g & b & k \\ -d_2b + k & g & b + d_1k \\ b & k & g + d_2k \end{bmatrix}$$

for some integers b, g and k .

Proof. Both $Q(\theta)$ and $Q(\varphi)$ have the indicated form (with (b, g, k) equal to $(0, 0, 1)$ and $(C, A + d_1C, B + d_2C)$, respectively). It is easily verified that the product of any two matrices with the given form again has that form, so Lemma 2 follows from Lemma 1.

The set of all matrices S which satisfy (2) with $\xi_1 = 1, \xi_2 = \theta, \xi_3 = \theta^2$ for some unit ω of norm 1 is of course Γ . In order to make use of Theorem C with ξ, η, ζ as defined by (6), it is necessary to exhibit one extremal parallelepiped and its associated matrix. The special form of the coefficients of ξ , plus the conditions (3), enable us to find an extremal parallelepiped with a very simple associated matrix, as the following lemma shows. This simplifies the writing of some later proofs; however, the remarks in Section 5 below show that one could begin with an arbitrary extremal parallelepiped.

LEMMA 3. Suppose (3) holds and ξ, η, ζ are defined by (6). Let μ denote the greatest integer in $(\theta^2 - 1)\theta^{-1}$. Then $\{\theta, 1, \theta'^2 - \mu\theta'' - 1\}$ is an extremal parallelepiped for ξ, η, ζ and the associated matrix is

$$P_1 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & \mu \\ 0 & 0 & -1 \end{bmatrix}$$

Proof. In the notation of Theorem A, if we take $\epsilon_1 = \epsilon_2 = -1, \epsilon_3 = +1$, then the matrix P_1 transforms the system $\epsilon_1\xi, \epsilon_2\eta, \epsilon_3\zeta$ to

$$\Phi = \begin{bmatrix} \theta & 1 & -\theta^2 + \mu\theta & +1 \\ \theta' & 1 & -\theta'^2 + \mu\theta' & +1 \\ -\theta'' & -1 & \theta''^2 - \mu\theta'' & -1 \end{bmatrix} = \begin{bmatrix} +a & +b & -c \\ -f & +g & +h \\ +j & -k & +l \end{bmatrix}$$

The signs of b, g and k are obvious, the signs of a, f and j follow from (3), and the signs of c, h and l follow from (3) and the fact that $(\theta^2 - 1)\theta^{-1} > \mu \geq 0$. Thus the matrix Φ has the appropriate system of signs for case IV of Theorem A.

The special condition " $b > c$ or $h > f$ or $j > k$ " for case IV is satisfied because $j = |\theta''| > 1 = k$ by (3). Hence by Theorem B the lemma follows if the inequalities (1) hold. The inequalities $a > b$ and $g > f$ follow from (3), and $l > j$ implies $l > k$ because $j > k$. Only the inequalities $a > c, g > h$ and $l > j$ remain to be verified, and these are respectively equivalent to

(8) $\mu\theta > \theta^2 - \theta - 1,$

(9) $\theta'^2 > \mu\theta',$

(10) $\theta''^2 + \theta'' > \mu\theta'' + 1.$

Clearly (8) and (9) follow from (3) and the fact that $\mu > (\theta^2 - 1)\theta^{-1} - 1$. Finally,

(10) is obvious if $\mu > 0$, for then by (3) the left side of (10) is positive and the right side is negative. If $\mu = 0$ and (10) is false, then both $\theta^2 - \theta - 1 < 0$ and $\theta'^2 + \theta' - 1 < 0$ hold; these inequalities imply, in conjunction with (3), that

$$(11) \quad \frac{1}{2}(1 + \sqrt{5}) > \theta > 0 \quad \text{and} \quad 0 > \theta' > -\frac{1}{2}(1 + \sqrt{5}).$$

A simple calculation shows that in fact there are no cubic polynomials of form (5) with three irrational roots satisfying (3) and (11). This proves the lemma.

Let $Q(\omega)$ be any element of Γ and suppose that the middle column of $Q(\omega^{-1})$ has entries b, g, k . By Lemmas 2 and 3 and Theorem C,

$$\{\theta|\omega|^{-1}, |\omega'|^{-1}, (\theta'^2 - \mu\theta' - 1)|\omega''|^{-1}\}$$

is an extremal parallelepiped for ξ, η, ζ with associated matrix $Q(\omega^{-1})P_1$. The first column of $Q(\omega^{-1})P_1$ has entries b, g, k ; hence by Theorem A and the definition of associated matrix

$$(12) \quad |b + g\theta + k\theta^2| = \theta/|\omega|.$$

4. An Array of Numbers. Any unit ω of norm 1 satisfies $\omega^{-1} = \theta^m\varphi^n$ for some unique integers m and n . Given this unique representation of ω , define $R(m, n) = \theta\omega^{-1}$. We remark for future reference that if b, g, k are the entries of the middle column of $Q(\omega^{-1})$, then it follows from (12) that

$$(13) \quad |R(m, n)| = \theta/|\omega| = |b + g\theta + k\theta^2|.$$

Given (13), define

$$S(m, n) = |R(m, n)| \max(g^2, k^2).$$

I give below a method for finding, for each fixed n , that value of m for which $S(m, n)$ is a minimum. Let $v(n)$ denote this value of m , so that $S(v(n), n) \leq S(m, n)$ for all integers m . We shall see later that the function $v(n)$ is well defined.

If the values of $S(m, n)$ are tabulated in a rectangular array with the integers m arranged on a vertical axis and the integers n arranged on a horizontal axis (see Section 6 below), the method just mentioned is simply a procedure for locating the smallest entry in a given column of the array. It is convenient to think of the $S(m, n)$ array as being divided into quadrants, the first to fourth quadrants being defined by $m \geq 0, n \geq 0$; $m \geq 0, n < 0$; $m < 0, n < 0$; $m < 0, n \geq 0$, respectively.

We are only interested in small values of $S(m, n)$, so we may assume from now on that

$$(14) \quad |\omega|^{-1} = |\theta^m\varphi^n| < 1.$$

Since $\theta > 1$ and $|\varphi| > 1$, this eliminates the first quadrant of the $S(m, n)$ array from further consideration.

LEMMA 4. *Let n be any fixed integer and define $\omega_m^{-1} = \theta^m\varphi^n$. Let b_m, g_m, k_m denote the entries of the middle column of $Q(\omega_m^{-1})$. Then for every integer m ,*

$$(15) \quad \begin{aligned} b_{m+1} &= d_2b_m + d_1b_{m-1} + b_{m-2}, \\ g_{m+1} &= d_2g_m + d_1g_{m-1} + g_{m-2}, \\ k_{m+1} &= d_2k_m + d_1k_{m-1} + k_{m-2}. \end{aligned}$$

Further, let p be any fixed integer and define

$$\begin{aligned}
 D &= (\theta - \theta')(\theta - \theta'')(\theta'' - \theta'), \\
 B(p) &= D^{-1}(\theta'' - \theta')\theta^{-1}(b_p + g_p\theta + k_p\theta^2), \\
 G(p) &= D^{-1}\theta(\theta'^2 - \theta''^2)\theta^{-1}(b_p + g_p\theta + k_p\theta^2)
 \end{aligned}$$

and

$$K(p) = D^{-1}\theta(\theta'' - \theta')\theta^{-1}(b_p + g_p\theta + k_p\theta^2).$$

Then for every integer m ,

$$\begin{aligned}
 (16) \quad b_{m+p} &= B(p)\theta^m + B'(p)\theta'^m + B''(p)\theta''^m, \\
 g_{m+p} &= G(p)\theta^m + G'(p)\theta'^m + G''(p)\theta''^m, \\
 k_{m+p} &= K(p)\theta^m + K'(p)\theta'^m + K''(p)\theta''^m,
 \end{aligned}$$

where $B'(p), B''(p); G'(p), G''(p);$ and $K'(p), K''(p)$ are the respective conjugates of $B(p), G(p), K(p)$.

Proof. By definition, $Q(\omega_{m+1}^{-1}) = Q(\theta)Q(\omega_m^{-1})$, so matrix multiplication gives $b_{m+1} = k_m, g_{m+1} = b_m + d_1k_m, k_{m+1} = g_m + d_2k_m$. A simple calculation using these equations gives (15).

Thus b_m, g_m, k_m satisfy linear recurrence relations, each with associated polynomial (5). Straightforward computation of the solutions of these recursion relations in terms of the roots of (5) gives (16).

The important fact about the coefficients $B(p), G(p), K(p)$ in Lemma 4 is that, by (13), each coefficient is the product of ω_p^{-1} and some constant depending only on $\theta, \theta', \theta''$, apart from sign.

I next show that the function $v(n)$ is closely related to another function $u(n)$ defined in the following way: Let n be any fixed integer and suppose $\omega_m^{-1} = \theta^m\varphi^n$. Define $u(n)$ to be that value of m satisfying $|\omega'_{u(n)}/\omega_{u(n)}| - 1| \leq |\omega'_m/\omega_m| - 1|$ for all integers m ; that is, $u(n)$ is the value of m for which $|\omega'_m/\omega_m|$ is nearest to 1. Let $E(n)$ denote $\omega'_{u(n)}/\omega_{u(n)}$. Note that it follows immediately from the definition of $u(n)$ that

$$(17) \quad \frac{2}{1 + \theta\theta'^2} > |E(n)| > \frac{2}{1 + (\theta\theta'^2)^{-1}}$$

for every n . For $E(n) = \theta'^{u(n)}\varphi^n/\theta'^{u(n)}\varphi'^n = (\theta\theta'^2)^{u(n)}(\varphi\varphi'^2)^n$, and if $|E(n)| > 1$, then by the definition of $u(n)$,

$$(\theta\theta'^2)^{u(n)}|\varphi\varphi'^2|^n - 1 < 1 - (\theta\theta'^2)^{u(n)+1}|\varphi\varphi'^2|^n.$$

This gives the first inequality in (17), and a similar argument in the case $|E(n)| < 1$ gives the second inequality.

It is easy to compute the value of $u(n)$ for a given n by using the definition of the function $u(n)$. The following lemma gives an alternative simple procedure for calculating $u(n)$.

LEMMA 5. Define $E_1 = \theta\theta'^2$ and $E_2 = |\varphi\varphi'^2|$. The integer $u(n)$ is equal to the unique integer m which satisfies

$$(18) \quad \frac{\log(2(1 + E_1)^{-1})}{\log E_1} < m + \frac{n \log E_2}{\log E_1} < 1 + \frac{\log(2(1 + E_1)^{-1})}{\log E_1}.$$

Proof. We have $|E(n)| = E_1^{u(n)} E_2^n$ and $0 < E_1 < 1$ (by (3)). Therefore it follows from (17) that either

$$\log (2(1 + E_1)^{-1}) > u(n) \log E_1 + n \log E_2 > 0 \quad (\text{if } |E(n)| > 1)$$

or

$$0 > u(n) \log E_1 + n \log E_2 > \log (2E_1(1 + E_1)^{-1}) \quad (\text{if } |E(n)| < 1).$$

Rearranging and combining these inequalities gives (18), which obviously defines a unique integer m . In fact, since

$$0 > \log (2(1 + x)^{-1})/\log x > -\frac{1}{2} \quad \text{for } 0 < x < 1,$$

the fraction m/n determined by the inequalities in (18) is one of the two fractions of form k/n which are closest in value to $-\log E_2/\log E_1$.

COROLLARY. *Let λ denote $-\log E_2/\log E_1$; then $\lim_{n \rightarrow \pm\infty} u(n)/n = \lambda$.*

It follows from the above corollary that the path through the $S(m, n)$ array formed by the numbers $S(u(n), n)$, n any integer, approximates a straight line of slope λ passing through the "origin" of the array. Thus the path lies either in the first and third quadrants of the $S(m, n)$ array (if $\lambda > 0$) or in the second and fourth quadrants (if $\lambda < 0$). However, by (14), the only numbers in the $S(m, n)$ array which are of interest are those for which $m \log \theta + n \log |\varphi| < 0$. Hence we need consider only part of the $S(u(n), n)$ path, namely (as a simple calculation shows) the part in

- the third quadrant if $\lambda > 0$,
- (19) the second quadrant if $\lambda < 0$ and $\frac{\log |\varphi|}{\log \theta} > \frac{\log |\varphi'|}{\log |\theta'|}$,
- the fourth quadrant if $\lambda < 0$ and $\frac{\log |\varphi|}{\log \theta} < \frac{\log |\varphi'|}{\log |\theta'|}$.

For later reference, define the *principal quadrant* to be the quadrant specified in (19) and define

- $\gamma = +1$ the principal quadrant is the fourth quadrant,
- $= -1$ the principal quadrant is the second or third quadrant.

Thus $n \rightarrow \gamma\infty$ means $|n| \rightarrow \infty$ in the principal quadrant.

The connection between $u(n)$ and $v(n)$ is exhibited in the following theorem, which is the cornerstone of the method introduced in this paper. The proof given is not the simplest possible, but enables very good values of c_1 and c_2 to be computed.

THEOREM 1. *For every integer n such that $\gamma n > 0$,*

$$c_1 \geq v(n) - u(n) \geq c_2,$$

where c_1 and c_2 are integers which depend only on $\theta, \theta', \theta''$.

Some new notations are necessary for the proof. For the remainder of this section, let n be a fixed integer, arbitrary unless otherwise specified, and define $\omega_m^{-1} = \theta^m \varphi^n$. Let b_m, g_m, k_m denote the entries of the middle column of $Q(\omega_m^{-1})$, so that Lemma 4 applies. Define

$$B = \omega_{u(n)} B(u(n)), \quad G = \omega_{u(n)} G(u(n)), \quad K = \omega_{u(n)} K(u(n)).$$

Thus the numbers $|B|$, $|G|$, $|K|$ and their conjugates depend only on θ , θ' , θ'' , and in particular are independent of n . Further let $T_m = \max(|g_{u(n)+m}|, |k_{u(n)+m}|)$.

Since by definition $R(u(n) + m + 1, n) = \theta R(u(n) + m, n)$ and $S(u(n) + m, n) = |R(u(n) + m, n)|T_m^2$, the inequality $S(u(n) + m, n) < S(u(n) + m + 1, n)$ holds if and only if

$$(20) \quad T_{m+1}/T_m > \theta^{-1/2}.$$

The assumptions (3) and (4) (here (4) is used for the first time) and the equations (16) with $p = u(n)$ imply that T_m is equal to either $g_{u(n)+m}$ or $k_{u(n)+m}$ for all large m , depending on whether $|\theta + \theta'|$ is > 1 or < 1 , respectively. Similarly, T_{-m} is equal to either $g_{u(n)-m}$ or $k_{u(n)-m}$ for all large m , depending on whether $|\theta + \theta''|$ is > 1 or < 1 , respectively. It follows that $T_{m+1}/T_m \rightarrow |\theta''| > \theta^{-1/2}$ as $m \rightarrow +\infty$ and $T_{m+1}/T_m \rightarrow |\theta'| < \theta^{-1/2}$ as $m \rightarrow -\infty$; thus (20) is true for all sufficiently large m and false for all sufficiently small m .

Clearly $v(n)$ satisfies $m_+ \geq v(n) - u(n) \geq m_-$ for any integers m_+ and m_- such that (20) holds for all $m \geq m_+$ and (20) is false for all $m \leq m_- - 1$. Provided m_+ and m_- depend only on θ , θ' , θ'' we may take $c_1 = m_+$ and $c_2 = m_-$ in Theorem 1. The following lemma shows that integers m_+ and m_- satisfying this proviso do exist.

LEMMA 6. *Let n be any integer such that $\gamma n > 0$. For each integer $m \geq 0$, the assumption $T_{m+1}/T_m < \theta^{-1/2}$ implies an inequality of the form*

$$(21) \quad \pm E(n) > k(m),$$

where $k(m)$ is a constant depending only on θ , θ' , θ'' and m . There exists an integer $m_1 \geq 0$ depending only on θ , θ' , θ'' such that for each integer $m \geq m_1$, the inequality (21) is false.

For each integer $m \leq 0$, the assumption $T_{m+1}/T_m > \theta^{-1/2}$ implies an inequality of the form (21), where $k(m)$ is a constant depending only on θ , θ' , θ'' and m . There exists an integer $m_2 \leq 0$ depending only on θ , θ' , θ'' such that for each integer $m \leq m_2$, the inequality (21) is false.

Proof. For any m , T_{m+1}/T_m is equal to one of the four quotients

$$|g_{u(n)+m+1}/g_{u(n)+m}|, \quad |g_{u(n)+m+1}/k_{u(n)+m}|, \quad |k_{u(n)+m+1}/k_{u(n)+m}|, \quad |k_{u(n)+m+1}/g_{u(n)+m}|;$$

let us say T_{m+1}/T_m is of type 1, 2, 3 or 4, respectively. Of course for a given m the type of T_{m+1}/T_m may be different for different n . Whatever the type of T_{m+1}/T_m , if we let $I(u(n))$ denote the appropriate one of the numbers $G(u(n))$, $K(u(n))$ for T_{m+1} , and let $J(u(n))$ denote the appropriate one of the numbers $G(u(n))$, $K(u(n))$ for T_m , then by (16)

$$(22) \quad \frac{T_{m+1}}{T_m} = \frac{|I(u(n))\theta^{m+1} + I'(u(n))\theta'^{m+1} + I''(u(n))\theta''^{m+1}|}{|J(u(n))\theta^m + J'(u(n))\theta'^m + J''(u(n))\theta''^m|}.$$

The next step is to multiply the numerator and denominator of the expression on the right-hand side of (22) by $\omega'_{u(n)}/\theta^m$. If we define $I = |\omega_{u(n)}I(u(n))|$ and $J = |\omega_{u(n)}J(u(n))|$, (22) becomes

$$(23) \quad \frac{T_{m+1}}{T_m} = \frac{|\theta(\omega'_{u(n)}/\omega_{u(n)})I + \theta'E(n)I'(\theta'/\theta)^m + \theta''I''(\theta''/\theta)^m|}{|(\omega'_{u(n)}/\omega_{u(n)})J + E(n)J'(\theta'/\theta)^m + J''(\theta''/\theta)^m|}.$$

It is easy to verify that $|\omega_{u(n)}| \rightarrow \infty$ as $n \rightarrow \gamma\infty$. Thus for n satisfying $\gamma n > 0$ the terms involving $\omega'_{u(n)}/\omega_{u(n)}$ on the right-hand side of (23) have such small absolute

value (except possibly for a few values of n with $|n|$ small) that they can be neglected. It follows that the assumption $T_{m+1}/T_m < \theta^{-1/2}$ is essentially equivalent to

$$(24) \quad \frac{|\theta' E(n) I'(\theta'/\theta)^m + \theta'' I''(\theta''/\theta)^m|}{|E(n) J'(\theta'/\theta)^m + J''(\theta''/\theta)^m|} < \theta^{-1/2},$$

and this inequality can be rearranged into the form (21), since everything on the left-hand side except $E(n)$ is independent of n .

For the next step in the argument, we may assume that the numbers I', J', I'', J'' (which are defined in terms of T_{m+1} and T_m , and so vary with the type of T_{m+1}/T_m) have fixed values, corresponding to a single type of T_{m+1}/T_m , as m varies in (24). Then, since by (17) $|E(n)|$ is bounded above for all n , the left-hand side of (24) tends to $|\theta'' I''/J''|$ uniformly with respect to n as $m \rightarrow +\infty$. Provided that $|\theta'' I''/J''| > \theta^{-1/2}$, it follows that (24) is false for all sufficiently large m ; thus if we calculate $k(m)$ for $m = 0, 1, 2, \dots$ in succession, we must reach a value $m = m_0$, depending only on $\theta, \theta', \theta''$ and the type to which the values of I'' and J'' correspond, such that the inequality (21) contradicts the first inequality in (17) for all $m \geq m_0$. If $|\theta'' I''/J''| > \theta^{-1/2}$ holds for all four types, the first part of the lemma follows if we take m_1 equal to the largest of the four values of m_0 found for the different types.

It is obvious from (3) that $|\theta'' I''/J''| > \theta^{-1/2}$ holds for types 1 and 3, and a calculation using (3) shows that the inequality also holds for type 2. However, for type 4, $|\theta'' I''/J''| > \theta^{-1/2}$ is equivalent to $|\theta''| > \theta^{1/2}(\theta + \theta')$, which might be false. If so, it is necessary to use an additional argument, similar to the above, to show that T_{m+1}/T_m is necessarily of type 1 or 3 if m is larger than some integer depending only on $\theta, \theta', \theta''$. Then the first part of the lemma follows.

Similar reasoning gives the second part of the lemma, if we let $m \rightarrow -\infty$ in (24) with the inequality sign reversed and use the second inequality in (17) in place of the first. The relevant inequality is $|\theta' I'/J'| < \theta^{-1/2}$. This follows from (3) in the case of types 1 and 3, and from a calculation using (3) and (4) in the case of type 2. The inequality $|\theta' I'/J'| < \theta^{-1/2}$ for type 4 is equivalent to $\theta^{1/2} |\theta'| < |\theta + \theta''|$, which may be false. If so, as in the first part of the lemma, an extra argument is needed to complete the proof.

It follows from Lemma 6 that (20) holds for $m \geq m_1$ and is false for $m \leq m_2$. Thus we may take $m_+ = m_1$ and $m_- = m_2 + 1$, and Theorem 1 holds with $c_1 = m_1$ and $c_2 = m_2 + 1$.

The following lemma shows that the restriction $\gamma n > 0$ in Theorem 1 and Lemma 6 can exclude only a finite number of small values of $S(m, n)$, since the only values of interest are, by (14), those for which $m \log \theta + n \log |\varphi| < 0$.

LEMMA 7. *Except possibly for some values of n with $|n|$ small, the inequality $v(n) \log \theta + n \log |\varphi| > 0$ holds for each n satisfying $\gamma n < 0$.*

Proof. By Lemma 5, Corollary and the definitions of γ and λ , the inequality $u(n) \log \theta + n \log |\varphi| > 0$ holds for each n satisfying $\gamma n < 0$, except possibly for some values of n with $|n|$ small, and indeed

$$\lim_{n \rightarrow -\gamma \infty} n^{-1}(u(n) \log \theta + n \log |\varphi|) = \lambda \log \theta + \log |\varphi|.$$

We shall show that $v(n) - u(n)$ is bounded below by a function which depends on $\theta, \theta', \theta''$ and on n , and that this function is small enough in absolute value to give the lemma.

The reasoning resembles that in the proof of Lemma 6, the notation of which is also used here. First we rewrite (22) by multiplying the numerator and denominator of the right-hand side by $\omega_{u(n)}/\theta^m$:

$$\frac{T_{m+1}}{T_m} = \frac{|\theta I + \theta' I'(\omega_{u(n)}/\omega'_{u(n)})(\theta'/\theta)^m + \theta'' I''(\omega_{u(n)}/\omega''_{u(n)})(\theta''/\theta)^m|}{|J + J'(\omega_{u(n)}/\omega'_{u(n)})(\theta'/\theta)^m + J''(\omega_{u(n)}/\omega''_{u(n)})(\theta''/\theta)^m|}.$$

Since $|\omega_{u(n)}| \rightarrow 0$ as $n \rightarrow -\gamma\infty$ and $|\theta''/\theta| > 1$ holds by (4), if $m \leq 0$ the terms involving $\omega_{u(n)}/\omega''_{u(n)}$ on the right-hand side have such small absolute value (except possibly for a few values of n with $|n|$ small) that they can be neglected. Thus the assumption $T_{m+1}/T_m > \theta^{-1/2}$ is essentially equivalent to

$$(25) \quad \frac{|\theta I + \theta' I'(\omega_{u(n)}/\omega'_{u(n)})(\theta'/\theta)^m|}{|J + J'(\omega_{u(n)}/\omega'_{u(n)})(\theta'/\theta)^m|} > \theta^{-1/2}.$$

The left-hand side of (25) tends to $|\theta' I'/J'|$ as $m \rightarrow -\infty$, but the approach to the limit is not uniform in n (this is different from the corresponding situation in Lemma 6). However,

$$(26) \quad \left| \frac{\omega_{u(n)}}{\omega'_{u(n)}} \left(\frac{\theta'}{\theta} \right)^m \right| \geq 1 \quad \text{if and only if } m \leq n \left(\frac{\log |\varphi| - \log |\varphi'|}{\log |\theta'| - \log \theta} \right) - u(n)$$

and

$$\frac{\log |\varphi| - \log |\varphi'|}{\log |\theta'| - \log \theta} - \frac{u(n)}{n} \rightarrow \frac{\log |\varphi| - \log |\varphi'|}{\log |\theta'| - \log \theta} - \lambda = w, \quad \text{say,}$$

as $n \rightarrow -\gamma\infty$. It is easy to verify that nw is negative if $\gamma n < 0$.

Thus if we take $m = nw + m'$ in (25), it follows from (26) by an argument similar to that used in the proof of Lemma 6 that there exists an integer $m_2 \leq 0$ depending only on $\theta, \theta', \theta''$ such that for each n satisfying $\gamma n < 0$, the inequality (25) is false for all $m' \leq m_2$. Hence $v(n) \geq u(n) + nw + m_2$, and in order to prove the lemma it suffices to verify that $|\log |\varphi| \cdot (\log \theta)^{-1} + \lambda| > |w|$.

The method for finding $S(v(n), n)$ is now clear. By Lemma 7, we need only consider n satisfying $\gamma n > 0$. For each such n , it follows from Theorem 1 that only $S(u(n) + i, n)$ ($i = c_2, c_2 + 1, \dots, c_1$) need be calculated. These calculations are easily made because $u(n)$ can be determined very simply (for example, by using Lemma 5). Given $u(n)$, it is only necessary to compute the middle column of $Q(\theta^{u(n)+i}\varphi^n)$ ($i = c_2, c_2 + 1, \dots, c_1$); this gives all the information needed to find $S(u(n) + i, n)$.

The only important fact which remains to be established is that the numbers $S(v(n), n), \gamma n > 0$, are bounded above by a constant independent of n . This means that the numbers $S(v(n), n)$ are uniformly small values of $S(m, n)$, as we require. The following lemma suffices for our purpose.

LEMMA 8. *Let n be any integer such that $\gamma n > 0$. Then the inequality $S(u(n), n) \leq c_3$ holds, where c_3 is a constant depending only on $\theta, \theta', \theta''$.*

Proof. It follows from the definition of $E(n)$ that $E(n) = \omega_{u(n)}\omega''_{u(n)} = (\omega_{u(n)}\omega'_{u(n)})^{-1}$. Since $|\omega_{u(n)}| \rightarrow \infty$ as $n \rightarrow \gamma\infty$, it follows from (16) with $m = 0$ and $p = u(n)$ that

$$\limsup_{n \rightarrow \gamma\infty} |\omega^{-1} g_{u(n)}^2| \leq \sup_{n \rightarrow \gamma\infty} D^{-2}(|E(n)|^{1/2} |\theta'(\theta'^2 - \theta^2)| + |E(n)|^{-1/2} |\theta''(\theta^2 - \theta'^2)|)^2$$

and

$$\limsup_{n \rightarrow \gamma_\infty} |\omega^{-1} k_u^{(n)}| \leq \sup_{n \rightarrow \gamma_\infty} D^{-2} (|E(n)|^{1/2} |\theta'(\theta - \theta')| + |E(n)|^{-1/2} |\theta''(\theta' - \theta)|)^2,$$

where the supremum on the right-hand side of each inequality is finite because of (17). By (13), these inequalities imply the lemma.

5. The Method Applied to General Linear Forms. It is not difficult to modify the above discussion so that it applies to the more general form $\xi = x + \alpha y + \beta z$, where α defines a totally real cubic field F over the rationals and $1, \alpha, \beta$ form an integral basis for F . We replace (6) by

$$\begin{aligned} \xi &= \pm(x + \alpha y + \beta z), \\ \eta &= \pm(x + \alpha' y + \beta' z), \\ \zeta &= \pm(x + \alpha'' y + \beta'' z), \end{aligned}$$

where the \pm sign is chosen so that the determinant of the forms is positive.

The first step is to find a pair θ, φ of fundamental units with norm 1 in F such that the inequalities

$$(27) \quad \theta > 1, \quad |\theta'| < 1, \quad |\theta''| > \theta$$

and $|\varphi| > 1$ hold. Lemma 9 below shows that such a pair can always be found.

The set of matrices Γ is defined as before (of course $Q(\theta)$ no longer has the particularly simple form of Section 2 above), and Lemma 1 holds. Lemma 2 may be restated as follows: For each matrix in Γ , the first column is equal to the matrix product of $Q(\alpha^{-1})$ and the second column; and the third column is equal to the matrix product of $Q(\alpha^{-1}\beta)$ and the second column.

It is no longer possible to give a simple explicit way of finding an initial extremal parallelepiped, as was done in Lemma 3; so we suppose that $\{a, g, l\}$ is an extremal parallelepiped for ξ, η, ζ with associated matrix

$$P_1 = \begin{bmatrix} r & r_2 & r_3 \\ s & s_2 & s_3 \\ t & t_2 & t_3 \end{bmatrix}.$$

Let n be any fixed integer, define $\omega_m^{-1} = \theta^m \varphi^n$ and suppose

$$Q(\omega_m^{-1}) = \begin{bmatrix} b_m^{(1)} & b_m & b_m^{(2)} \\ g_m^{(1)} & g_m & g_m^{(2)} \\ k_m^{(1)} & k_m & k_m^{(2)} \end{bmatrix},$$

where by Lemma 2 the entries in the first and third columns are linear combinations of b_m, g_m, k_m whose coefficients depend on the entries of the matrices $Q(\alpha^{-1})$ and $Q(\alpha^{-1}\beta)$. By the argument used to derive (13), we obtain

$$(28) \quad \bar{b}_m + \bar{g}_m \alpha + \bar{k}_m \beta = (r + s\alpha + t\beta) / \omega_m,$$

where $\bar{b}_m, \bar{g}_m, \bar{k}_m$ denote the entries of the first column of $Q(\omega_m^{-1})P_1$; each of $\bar{b}_m, \bar{g}_m, \bar{k}_m$ is therefore a linear combination of b_m, g_m and k_m with coefficients depending on

the entries of the matrices $Q(\alpha^{-1})$ and $Q(\alpha^{-1}\beta)$, and on r, s and t . We denote the right-hand side of (28) by $R(m, n)$, and define $S(m, n) = |R(m, n)| \max(\bar{g}_m^2, \bar{k}_m^2)$.

The recursion relations (15) remain valid, which implies that the same relations hold for $\bar{b}_m, \bar{g}_m, \bar{k}_m$. Solving the latter recursion relations gives (16) with $b_{m+p}, g_{m+p}, k_{m+p}$ replaced by $\bar{b}_{m+p}, \bar{g}_{m+p}, \bar{k}_{m+p}$, respectively, and with coefficients (using (28)) $B(p) = D^{-1}B\omega_p^{-1}, G(p) = D^{-1}G\omega_p^{-1}, K(p) = D^{-1}K\omega_p^{-1}$, where D denotes the determinant of ξ, η, ζ and B, G, K are numerical constants.

This analogue of Lemma 4, in conjunction with (28), enables all the previous arguments concerning the functions $u(n)$ and $v(n)$ to be carried through as before. Note that the conditions (27) are used in the proof of Theorem 1. It can be shown that these conditions, although sufficient, are not necessary for the truth of Theorem 1.

Finally, we show that there always exists a pair θ, φ of fundamental units with norm 1 in F such that (27) holds.

LEMMA 9. *Suppose γ, δ is a pair of fundamental units for F such that γ and δ have norm 1, $\gamma > 1, |\gamma'| < 1, |\gamma''| < 1$ and $|\delta| > 1$. Then there exist integers M and N such that $\theta = \gamma^M \delta^N$ satisfies (27) and such that there exists a unit φ for which θ, φ is a pair of fundamental units for F .*

Proof. Define

$$A = (-\log |\delta|)(\log \gamma)^{-1}, \quad A' = (-\log |\delta'|)(\log |\gamma'|)^{-1},$$

$$A'' = (-\log |\delta''|)(\log |\gamma''|)^{-1} \quad \text{and} \quad B = (\log \gamma)(\log |\gamma''|)^{-1}.$$

The hypothesis that γ and δ are fundamental units implies that no two of A, A', A'' are equal.

We distinguish two cases: suppose first that at least one of the two inequalities $A < A', A < A''$ is false. We may assume that $A'' < A$ and $A'' < A'$ by interchanging the definitions of F' and F'' (as is permissible), if necessary. In order that $\theta = \gamma^M |\delta|^N$ satisfy (27) for some integers M, N with $N < 0$ it is necessary and sufficient that $M/N < A, M/N < A'$ and $M/N > A'' + N^{-1}B$ hold. Since $A'' < \min(A, A')$, these inequalities are satisfied for any integers $M, N < 0$ such that $|N|$ is sufficiently large and M/N lies in the interval $(A'', \min(A, A'))$. If we further take M and N to be relatively prime, with N even if δ is negative, then $\theta = \gamma^M \delta^N$ satisfies the lemma: for it is easily seen that given any integers P, Q satisfying $MQ - PN = \pm 1$, the hypothesis that γ, δ is a pair of fundamental units for F implies that $\theta, \gamma^P \delta^Q$ is also such a pair

Next suppose $A < A'$ and $A < A''$. We may assume that $A < A' < A''$ by interchanging the definitions of F' and F'' , if necessary. An argument similar to the above shows that $\theta = \gamma^M \delta^N$ satisfies the lemma for any integers M, N with $N > 0$ such that N is sufficiently large, M/N lies in the interval (A', A'') , and M and N are relatively prime with N even if δ is negative. This completes the proof of the lemma.

A pair of fundamental units satisfying the hypotheses of Lemma 9 exists in any totally real cubic field F : Given any pair γ, δ of fundamental units, each with norm 1, we may suppose $\gamma > 1$ and $|\delta| > 1$ (replacing γ, δ by $\gamma\delta, \gamma\delta^2$ if both γ and δ are negative). If γ does not have two conjugates whose absolute values are less than 1, we may define F' and F'' so that $|\gamma'| < 1$ and $|\gamma''| > 1$. Then by reasoning almost exactly the same as in the proof of Lemma 9, we can find a pair $\gamma^M \delta^N, \gamma^P \delta^Q$ (M, N, P, Q integers satisfying $MQ - PN = \pm 1$) of fundamental units for F which satisfies the hypotheses of Lemma 9.

6. A Numerical Example. Let F be the field defined by $\theta = 2 \cos(2\pi/7)$. Then θ is a root of the polynomial equation $x^3 + x^2 - 2x - 1 = 0$, which is of the form (5) and has roots

$$\theta \approx 1.247, \quad \theta' \approx -.445, \quad \theta'' \approx -1.802.$$

We apply the above method to the linear form $x + \theta y + \theta^2 z$, which is permissible since $1, \theta, \theta^2$ is an integral basis for F . The conditions (3) and (4) are satisfied, and we take θ and $\varphi = 1/\theta'$ as a pair of fundamental units of F (θ' and θ'' belong to F , because F is a cyclic or Abelian field). We take the parallelepiped $\{\theta, 1, \theta''^2 - 1\}$, given in Lemma 3, as the initial extremal parallelepiped.

The principal quadrant is the second quadrant, and $\lambda \approx -.263$. The inequalities $|\theta''I''/J''| > \theta^{-1/2}$ and $|\theta'I'/J'| < \theta^{-1/2}$ in the notation of Lemma 6 hold for each type of T_{m+1}/T_m , and carrying out the computations indicated in the proof of Lemma 6 gives $c_1 = 1$ and $c_2 = -3$ in Theorem 1.

Table 1 gives a portion of the second quadrant of the $S(m, n)$ array; a few values with $n = -1$ do not satisfy (14) and are omitted. The numbers $S(u(n), n)$ are indicated by an asterisk. Table 2 gives the entries b, g, k of the middle column for the matrices $Q(\theta^s \varphi^n)$. These entries all satisfy $|b + \theta g + \theta^2 k| \max(g^2, k^2) < 1$.

7. Finding all Solutions Below a Certain Bound. It is well known [1, p. 79] that $\inf |x + \alpha y + \beta z| \max(y^2, z^2) > 0$, where $1, \alpha, \beta$ are elements of a real cubic field which are linearly independent over the rationals and the infimum is taken over all integers x, y, z not all zero. For the example of Section 6, we have:

LEMMA 10. Let $\theta = 2 \cos(2\pi/7)$; then

$$\liminf_{M \rightarrow \infty} \min_M |x + \theta y + \theta^2 z| \max(y^2, z^2) = \frac{4}{9}(\theta^2 + 3\theta - 3) \approx .1874,$$

where the min is taken over all integers x, y, z such that $\max(|y|, |z|) = M$.

Proof. If $x + \theta y + \theta^2 z$ is small, then

$$\begin{aligned} 1 &\leq |(x + \theta y + \theta^2 z)(x + \theta' y + \theta'^2 z)(x + \theta'' y + \theta''^2 z)| \\ &\approx |(x + \theta y + \theta^2 z)((\theta' - \theta)y + (\theta'^2 - \theta^2)z)((\theta'' - \theta)y + (\theta''^2 - \theta^2)z)| \\ (29) \quad &= |(x + \theta y + \theta^2 z)(\theta - \theta')(\theta - \theta'')(y^2 + (\theta - 1)yz + (\theta^2 - 2)z^2)| \\ &\leq |x + \theta y + \theta^2 z|(3\theta^2 + 2\theta - 2)(1 + (\frac{1}{2}(\theta - 1))^2(2 - \theta^2)^{-1})|y^2| \\ &\leq |x + \theta y + \theta^2 z|(49/4)(\theta^2 + 3\theta - 3)^{-1} \max(y^2, z^2). \end{aligned}$$

The second inequality holds because the maximum of $1 + (\theta - 1)x + (\theta^2 - 2)x^2$ (which occurs at $x = \frac{1}{2}(\theta - 1)(2 - \theta^2)^{-1}$) is greater than the maximum of $-x^2 - (\theta - 1)x - (\theta^2 - 2)$ (which occurs at $x = \frac{1}{2}(1 - \theta)$).

Equality can occur in the first inequality of (29) only if $x + \theta y + \theta^2 z$ is a unit, that is, only if x, y, z are the entries of the middle column of $Q(\theta^m \varphi^n)$ (in the notation of Section 6) for some m and n . Near equality can occur in the second inequality of (29) only if z/y is nearly equal to $\frac{1}{2}(\theta - 1)(2 - \theta^2)^{-1} \approx .2775$. It is a straightforward matter to verify that this near equality does in fact occur for infinitely many values of z/y . (Indeed, more can be shown: We have $z/y \approx .2775$, where y and z are the last two entries of the middle column of $Q(\theta^m \varphi^n)$, only if n is even and $m = u(n) - 1$.)

TABLE 1. Second quadrant of $S(m, n)$ array

2.47	4.08	5.38	8.29	11.5	17.1	24.2	35.4	50.7	73.8	106	154	222	321	463	670	969	1393	2042	<i>m</i>	
.524	1.18	1.18	2.21	2.68	4.38	5.81	8.91	12.4	18.4	26.0	38.1	54.6	79.4	114	166	238	347	491	6	
.220*	.493*	.323*	.726*	.556	1.25	1.28	2.36	-2.90	4.70	6.27	9.58	13.3	19.8	28.1	41.0	59.0	84.8	126	5	
.204	.459	.188	.423	.226*	.508*	.339*	.762*	.591	1.33	1.40	2.53	3.14	5.05	6.77	10.3	14.3	21.5	29.3	4	
.912	.995	.343	.609	.200	.450	.190	.426	-.233*	.525*	.357*	.801*	.629	1.41	1.52	2.70	3.41	5.33	7.66	3	
4.30	3.33	1.95	1.71	.833	.941	.307	.585	.197	.442	.191	.430	.242*	.543*	.377*	.846	.684	1.54	1.54	2	
18.0	12.8	8.52	6.26	3.97	3.11	1.80	1.60	.760	.891	.273	.563	.194	.435	.193	.434*	.244*	.548*	.308*	1	
73.6	51.3	35.1	24.7	16.7	11.9	7.90	5.82	3.68	2.90	1.65	1.51	.693	.845	.242	.544	.196	.440	.247	.553*	0
-20	-19	-18	-17	-16	-15	-14	-13	-12	-11	-10	-9	-8	-7	-6	-5	-4	-3	-2	-1	<i>n</i>
.395*	.887	.754	1.60	1.78	3.09	3.95	6.22	8.47	12.7	17.9	26.4	37.6	54.9	78.8	114	165	239	344	498	<i>m</i>
.196	.441*	.260*	.583*	.417*	.937	.827	1.70	1.94	3.31	4.27	6.68	9.14	13.7	19.3	28.4	40.5	59.1	84.9	123	11
.234	.526	.190	.426	.200	.449*	.270*	.607*	.441*	.990	.905	1.81	2.10	3.55	4.61	7.18	9.86	14.7	20.8	30.6	10
1.41	1.33	.575	.765	.227	.510	.188	.423	.204	.458*	.282*	.633*	.466*	1.05	.989	1.94	2.28	3.80	4.98	7.71	9
6.32	4.73	2.92	2.38	1.29	1.26	.521	.729	.220	.495	.188	.422	.208	.468*	.294*	.661*	.494	1.11	1.08	2.07	8
26.2	18.5	12.4	8.97	5.85	4.41	2.69	2.22	1.19	1.18	.471	.695	.214	.481	.187	.421	.214*	.480*	.308*	.692*	7
107	74.2	51.0	35.7	24.3	17.2	11.5	8.34	5.42	4.11	2.49	2.08	1.09	1.11	.425	.664	.209	.469	.188	.422	6
433	300	207	143	99.1	68.9	47.3	33.1	22.6	16.0	10.7	7.76	5.02	3.83	2.29	1.95	.997	1.05	.382	.635	5
-40	-39	-38	-37	-36	-35	-34	-33	-32	-31	-30	-29	-28	-27	-26	-25	-24	-23	-22	-21	<i>n</i>

TABLE 2. Entries of middle column of $Q(\theta^{v(n)}\varphi^n)$

n	$v(n)$	b	g	k	n	$v(n)$	b	g	k
-1	-1	-2	0	1	-21	5	-2,258	-243	1,647
-2	-1	3	-1	-1	-22	5	2,626	-1,647	-368
-3	0	3	0	-2	-23	5	-6,531	368	3,905
-4	0	-4	2	1	-24	5	9,525	-3,905	-2,994
-5	1	-5	-1	4	-25	6	10,436	911	-7,442
-6	1	5	-4	0	-26	6	-12,519	7,442	2,083
-7	1	-14	0	9	-27	7	-17,878	-5,359	15,795
-8	1	19	-9	-5	-28	7	14,602	-15,795	3,276
-9	2	23	4	-18	-29	7	-48,275	-3,276	33,673
-10	2	-24	18	1	-30	7	59,601	-33,673	-11,326
-11	2	65	-1	-41	-31	8	81,948	22,347	-70,622
-12	2	-90	41	25	-32	8	-70,927	70,622	-11,021
-13	3	-106	-16	81	-33	8	223,497	11,021	-152,570
-14	3	115	-81	-9	-34	8	-283,403	152,570	59,906
-15	3	-302	9	187	-35	9	-376,067	-92,664	316,161
-16	3	426	-187	-124	-36	9	343,309	-316,161	32,758
-17	4	489	63	-365	-37	9	-1,035,537	-32,758	692,228
-18	4	-550	365	61	-38	9	1,346,088	-692,228	-310,551
-19	4	1,404	-61	-854	-39	10	1,727,765	381,677	-1,417,214
-20	4	-2,015	854	611	-40	10	-1,656,639	1,417,214	-71,126

This proves that given any $\epsilon > 0$, the inequality

$$|x + \theta y + \theta^2 z| \max(y^2, z^2) < (4/49)(\theta^2 + 3\theta - 3) + \epsilon$$

has infinitely many solutions in integers x, y, z . Since it is clear from (29) that given any $\epsilon > 0$,

$$|x + \theta y + \theta^2 z| \max(y^2, z^2) > (4/49)(\theta^2 + 3\theta - 3) - \epsilon$$

for all except possibly a finite number of integer triples x, y, z , the lemma follows.

A calculation similar to (29) can be performed for any linear form $x + \alpha y + \beta z$, where $1, \alpha, \beta$ form an integral basis for a totally real cubic field. The calculation gives a constant $L(\alpha, \beta)$ such that given any $\epsilon > 0$

$$|x + \alpha y + \beta z| \max(y^2, z^2) > L(\alpha, \beta) - \epsilon$$

holds except possibly for a finite number of integer triples x, y, z . Since the lower bound 1 in the first line of (29) can be replaced by 2 if $x + \theta y + \theta^2 z$ is not a unit, all but a finite number of solutions of $|x + \alpha y + \beta z| \max(y^2, z^2) < 2L(\alpha, \beta) - 2\epsilon$ occur with x, y, z such that $x + \alpha y + \beta z$ is a unit. Hence if in the notation of (28) the initial extremal parallelepiped is chosen in such a way that $r + s\alpha + t\beta$ is a unit, then for some $c \leq 2L(\alpha, \beta)$ all solutions of $|x + \alpha y + \beta z| \max(y^2, z^2) < c$ can be generated by the method of this paper.

1. J. W. S. CASSELS, *An Introduction to Diophantine Approximation*, Cambridge Tracts in Math. and Math. Phys., no. 45, Cambridge Univ. Press, New York, 1957. MR 19, 396.
2. H. HANCOCK, *Development of the Minkowski Geometry of Numbers*, Macmillan, New York, 1939, pp. 371–452. MR 1, 67.
3. H. MINKOWSKI, "Zur Theorie der Kettenbrüche," in *Gesammelte Abhandlungen*. Vol. I, Teubner, Leipzig, 1911, pp. 278–292.
4. L. G. PECK, "Simultaneous rational approximations to algebraic numbers," *Bull. Amer. Math. Soc.*, v. 67, 1961, pp. 197–201. MR 23 #A111.
5. M. ZEISEL, "Zur Minkowskischen Parallelepipedaapproximation," *S.-B. Akad. Wiss. Wien.* v. 126, 1917, pp. 1221–1247.