

An Analogue of the Nearest Integer Continued Fraction for Certain Cubic Irrationalities

By H. C. Williams* and G. W. Dueck

Abstract. Let θ be any irrational and define $Ne(\theta)$ to be that integer such that $|\theta - Ne(\theta)| < \frac{1}{2}$. Put $\rho_0 = \theta$, $r_0 = Ne(\rho_0)$, $\rho_{k+1} = 1/(r_k - \rho_k)$, $r_{k+1} = Ne(\rho_{k+1})$. Then the r 's here are the partial quotients of the nearest integer continued fraction (NICF) expansion of θ . When D is a positive nonsquare integer, and $\theta = \sqrt{D}$, this expansion is periodic. It can be used to find the regulator of $\mathcal{Q}(\sqrt{D})$ in less than 75 percent of the time needed by the usual continued fraction algorithm. A geometric interpretation of this algorithm is given and this is used to extend the NICF to a nearest integer analogue of the Voronoi Continued Fraction, which is used to find the regulator of a cubic field \mathcal{F} with negative discriminant Δ . This new algorithm (NIVCF) is periodic and can be used to find the regulator of \mathcal{F} .

If $I < \sqrt[4]{|\Delta|/148}$, the NIVCF algorithm can be used to find any algebraic integer α of \mathcal{F} such that $N(\alpha) = I$. Numerical results suggest that the NIVCF algorithm finds the regulator of $\mathcal{F} = \mathcal{Q}(\sqrt[3]{D})$ in about 80 percent of the time needed by Voronoi's algorithm.

1. Introduction. Let θ be any real number. We find the *Regular Continued Fraction* (RCF) expansion of θ by putting $\phi_0 = \theta$, $q_0 = [\phi_0]$, $\phi_{i+1} = 1/(\phi_i - q_i)$, $q_{i+1} = [\phi_{i+1}]$ ($i = 0, 1, 2, \dots, n, \dots$) and denote this as

$$\theta = [q_0, q_1, q_2, \dots, q_{n-1}, \phi_n].$$

Here $[\alpha]$ denotes that integer such that $\alpha - 1 < [\alpha] \leq \alpha$. We also define the convergent $C_n = [q_0, q_1, q_2, \dots, q_n]$. Further, if $A_{-2} = 0$, $A_{-1} = 1$, $B_{-2} = 0$, $B_{-1} = 1$,

$$A_{k+1} = q_{k+1}A_k + A_{k-1}, \quad B_{k+1} = q_{k+1}B_k + B_{k-1} \quad (k = -1, 0, 1, 2, \dots),$$

then $C_n = A_n/B_n$.

The *Nearest Integer Continued Fraction* (NICF) of θ is found by setting $\rho_0 = \theta$, $r_0 = Ne(\rho_0)$ and calculating $\rho_{i+1} = 1/(r_i - \rho_i)$, $r_{i+1} = Ne(\rho_{i+1})$ ($i = 0, 1, 2, \dots, n, \dots$). We denote this by

$$\theta = (r_0, r_1, r_2, \dots, r_{n-1}, \rho_n).$$

Here $Ne(\alpha)$ is that integer such that $|\alpha - Ne(\alpha)| < \frac{1}{2}$; that is, $Ne(\alpha)$ is the nearest integer to α . The convergent $\bar{C}_n = (r_0, r_1, r_2, \dots, r_n)$ can be calculated by noting that $\bar{C}_n = \bar{A}_n/\bar{B}_n$, $\bar{A}_{-2} = 0$, $\bar{A}_{-1} = 1$, $\bar{B}_{-2} = -1$, $\bar{B}_{-1} = 0$, and

$$\bar{A}_{k+1} = r_{k+1}\bar{A}_k - \bar{A}_{k-1}, \quad \bar{B}_{k+1} = r_{k+1}\bar{B}_k - \bar{B}_{k-1} \quad (k = -1, 0, 1, 2, 3, \dots).$$

Received March 8, 1983.

1980 *Mathematics Subject Classification*. Primary 10F20, 10A32, 12A30.

* Research supported by NSERC of Canada grant number A7649 and the I. W. Killam Program.

©1984 American Mathematical Society
 0025-5718/84 \$1.00 + \$.25 per page

The NICF was introduced in 1873 by Minnegerode [4] who used the NICF expansion of \sqrt{D} to solve the Pell Equation

$$(1.1) \quad t^2 - Du^2 = 1.$$

Later Hurwitz [3] gave further results concerning the NICF and more recently other results have been obtained by Williams [7], Williams and Buhr [6], and Adams [1].

For example, in [6], the following theorem is proved.

THEOREM 1.1. *If $c = (3 + \sqrt{5})/2$ and a, b are coprime integers such that*

$$|a/b - \theta| < 1/cb^2$$

for some irrational θ , then a/b must be a convergent in the NICF expansion of θ . \square

In this paper we shall at first be concerned with NICF expansions of quadratic irrationals. To this end we let D be a square free positive integer and put $\mathcal{K} = \mathcal{Q}(\sqrt{D})$, the quadratic field formed by adjoining D to the rationals \mathcal{Q} . Let $\mathcal{O}_{\mathcal{K}}$ be the ring of algebraic integers in \mathcal{K} . $\mathcal{O}_{\mathcal{K}}$ has as *basis* $\{1, \mu\}$, where $\mu = (1 + \sqrt{D})/2$ when $D \equiv 1 \pmod{4}$ and $\mu = \sqrt{D}$ otherwise. Let $\epsilon_0 (> 1)$ be the *fundamental unit* of \mathcal{K} and let Δ be the *discriminant* of \mathcal{K} . If $\alpha \in \mathcal{K}$, let α' denote the *conjugate* of α and $N(\alpha) = \alpha\alpha'$ be the *norm* of α .

It is well known that if $\theta \in \mathcal{K}$, the RCF expansion of θ is periodic. In fact, if $\theta = \mu$, then

$$\mu = [q_0, \overline{q_1, q_2, \dots, q_p}],$$

where we draw a bar over the periodic part of the continued fraction. From results in [3], we find that if $\theta = \mu$, then the NICF expansion of θ is also periodic; further,

$$\mu = (r_0, \overline{r_1, r_2, \dots, r_\pi})$$

when $N(\epsilon_0) = 1$ and

$$\mu = (r_0, \overline{r_1, r_2, \dots, r_\pi, -r_1, -r_2, \dots, -r_\pi})$$

when $N(\epsilon_0) = -1$. In fact we have the following theorem.

THEOREM 1.2. *If $D \neq 5$, then $\epsilon_0 = |\overline{A_{\pi-1}} - \mu' \overline{B_{\pi-1}}|$; if $D = 5$, then $\epsilon_0^2 = |\overline{A_{\pi-1}} - \mu' \overline{B_{\pi-1}}|$. \square*

Of course this result shows us how to solve (1.1) by using the NICF expansion of μ .

Theorem 1.2 can be regarded as a special case of

THEOREM 1.3. *If $\alpha = x + y\mu$, where x, y are coprime rational integers, $\alpha > 1$ and $|N(\alpha)| < \sqrt{\Delta/c_1}$, where $c_1 = c^2 = (7 + 3\sqrt{5})/2 \approx 6.85$, then*

$$\alpha = |\overline{A_m} - \mu' \overline{B_m}|$$

for some $m \geq 1$.

Proof. This result can be derived by using Theorem 1.1 and the simple observation that if $\overline{C_n}$ ($n \geq 0$) is any convergent in the NICF expansion of $\theta (> 2)$, then $-(\overline{C_n})^{-1}$ is a convergent in the NICF expansion of $-1/\theta$. \square

Thus, the NICF can be used to find all elements in $\mathcal{O}_{\mathcal{K}}$ with norm bounded by $\sqrt{\Delta/c_1}$. For, if $N(\alpha) = N$ and $|N| < \sqrt{\Delta/c_1}$ and $\alpha < 1$, then $\beta = \pm \epsilon_0^k \alpha > 1$ for some

k and $|N(\beta)| = |N(\alpha)|$. Since ϵ_0 and β can be found from the NICF expansion of μ , so can α . Further, if $\alpha = x + y\sqrt{D}$ and $\gcd(x,y) = d > 1$, then, since $|N/d^2| < |N|$, we can find α/d from the NICF expansion of μ .

From the several numerical results presented in [6] it seems that the ratio π/p is usually about .69. In fact Adams [1] gives results which suggest that this ratio should be $\log((1 + \sqrt{5})/2)/\log 2$ in the limit. This, of course, means that we can usually calculate ϵ_0 more rapidly by using the NIVCF algorithm rather than the NICF algorithm. Also, if we are attempting to solve the Diophantine equation

$$N(\alpha) = I,$$

where $\alpha \in \mathcal{O}_{\mathfrak{K}}$ and $|I| < \sqrt{\Delta/c_1}$, we should use the NICF algorithm rather than the RCF.

Let δ be the real zero of an irreducible (over \mathbb{Q}) cubic polynomial with integer coefficients and negative discriminant. In order to find the fundamental unit ϵ_0 (> 1) in $\mathfrak{F} = \mathbb{Q}(\delta)$, Voronoi's Continued Fraction (VCF) algorithm is often used. (See Delone and Faddeev [2] or Williams, Cormack, Seah [8].) This algorithm, which is particularly suited for the problem of finding the fundamental unit(s) in a cubic field, is an extension of the RCF algorithm. In view of the increased speed obtained by using the NICF algorithm over the RCF, it would be desirable to develop an analogue of the NICF algorithm for cubic irrationalities. In this paper we shall develop such an algorithm, called the nearest integer analogue of the Voronoi Continued Fraction (NIVCF), for use with elements from \mathfrak{F} above. We will also prove theorems analogous to Theorems 1.2 and 1.3 and compare (numerically) the speed of the NIVCF algorithm with that of the VCF. In order to do all of this we must first place the RCF and NICF in a geometric setting similar to that used for Voronoi's algorithm in [2] and [8]. This will be done in the next two sections.

2. The Lattices \mathfrak{S} and \mathfrak{R} . In this section we give a very brief description of certain properties of some special lattices \mathfrak{S} and \mathfrak{R} . While we confine our discussion here to these special lattices, it should be pointed out that much of what is said here can be extended to more general lattices. See, for example, the approach of Voronoi [5] and the general results given in Delone and Faddeev [2].

Let \mathfrak{E}_n represent Euclidean n -space. If $\beta \in \mathfrak{K}$, the point B of \mathfrak{E}_2 corresponding to β is (β, β') . If $\lambda, \mu \in \mathfrak{K}$, and λ, μ are rationally independent, define lattice \mathfrak{S} by

$$\mathfrak{S} = \{u\Lambda + vM \mid u, v \in \mathbf{Z}\},$$

where $\Lambda = (\lambda, \lambda')$, $M = (\mu, \mu')$. We say that \mathfrak{S} is the lattice with basis $\{\lambda, \mu\}$ or $\{\Lambda, M\}$ and will denote it by $\langle \lambda, \mu \rangle$.

If $\alpha \in \mathfrak{F}$, let α', α'' denote the conjugates of α and define A , the point of \mathfrak{E}_3 corresponding to α , to be

$$A = (\alpha, (\alpha' - \alpha'')/2i, (\alpha' + \alpha'')/2),$$

where $i^2 + 1 = 0$. Since the discriminant of the polynomial of which α is a zero is negative, we see that A is a point with real coordinates. If $\lambda, \mu, \nu \in \mathfrak{F}$ and λ, μ, ν are rationally independent, define the lattice \mathfrak{R} by

$$\mathfrak{F} = \{u\Lambda + vM + wN \mid u, v, w \in \mathbf{Z}\}.$$

Here \mathfrak{R} is the lattice with basis $\{\lambda, \mu, \nu\}$ and will be denoted by $\langle \lambda, \mu, \nu \rangle$.

Let \mathcal{L} represent either the lattice \mathfrak{S} or \mathfrak{R} . For the sake of brevity we will often write $\alpha \in \mathcal{L}$ as a means of denoting that it is the corresponding point A of \mathfrak{E}_2 or \mathfrak{E}_3 that is actually in \mathcal{L} . Also, if $\mathcal{L} = \langle \lambda, \mu \rangle$ and $\alpha \in \mathfrak{K}$ we define $\alpha\mathcal{L}$ to be $\langle \alpha\lambda, \alpha\mu \rangle$; similarly, if $\mathcal{L} = \langle \lambda, \mu, \nu \rangle$ and $\alpha \in \mathfrak{F}$, we define $\alpha\mathcal{L}$ to be $\langle \alpha\lambda, \alpha\mu, \alpha\nu \rangle$. Note that under this convention, if $\alpha\mathcal{L}_1 = \alpha\mathcal{L}_2$ and $\alpha \neq 0$, then $\mathcal{L}_1 = \mathcal{L}_2$.

If $A = (\alpha, \alpha')$ is a point of \mathfrak{S} , we define the *normed body* of A , $\mathfrak{N}(A)$ or $\mathfrak{N}(\alpha)$, to be

$$\mathfrak{N}(A) = \mathfrak{N}(\alpha) = \{(x, y) | (x, y) \in \mathfrak{E}_2, |x| < |\alpha|, |y| \leq |\alpha'|\}.$$

This is a semiopen rectangle which is symmetric about the origin O of \mathfrak{E}_2 . If A is a point of \mathfrak{R} , we define the normed body of A to be

$$\mathfrak{N}(A) = \mathfrak{N}(\alpha) = \{(x, y, z) | (x, y, z) \in \mathfrak{E}_3, |x| < |\alpha|, y^2 + z^2 \leq |\alpha'|^2\}.$$

This is a semiopen right circular cylinder, symmetric about the origin O of \mathfrak{E}_3 with axis the x -axis of \mathfrak{E}_3 . We point out here that if $|\alpha'| = |\beta'|$, then $\alpha = \pm\beta$ (see [2, p. 274]). Thus, if $|\beta'| = |\alpha'|$, then $B \notin \mathfrak{N}(\alpha)$.

We say that $\phi (\neq 0)$ or the point Φ corresponding to ϕ is a *minimum* of \mathcal{L} if $\mathfrak{N}(\phi) \cap \mathcal{L} = \{O\}$. If ψ and ϕ are minima of \mathcal{L} and $\psi > \phi$, we say that ψ and ϕ are adjacent minima when there does not exist a nonzero $\theta \in \mathcal{L}$ such that $\phi < \theta < \psi$ and $|\theta'| < |\phi'|$. If

$$(2.1) \quad \theta_1, \theta_2, \theta_3, \dots, \theta_n, \dots$$

is a sequence of minima of \mathcal{L} such that $\theta_{i+1} > \theta_i$ and θ_{i+1}, θ_i are adjacent, we call (2.1) a *chain* of minima of \mathcal{L} . By Minkowski's Theorem (see [2]) we can prove that there always exist such chains in \mathcal{L} . Further, if θ is any minimum of \mathcal{L} and $\theta > \theta_1$, then $\theta = \theta_m$ for some integer $m > 1$.

If $\mathcal{L} = \langle 1, \mu \rangle$ or $\mathcal{L} = \langle 1, \mu, \nu \rangle$ and \mathcal{L} has 1 as a minimum, we say that \mathcal{L} is a *reduced* lattice. We now give some theorems concerning these reduced lattices.

THEOREM 2.1. *Let \mathcal{L} be a reduced lattice and let $\theta (> 1)$ be the minimum of \mathcal{L} adjacent to 1. There exists a basis of \mathcal{L} which includes 1 and θ .*

Proof. The proof of this result for $\mathcal{L} = \langle 1, \mu, \nu \rangle$ is given in Section 2 of [10]. The proof for $\mathcal{L} = \langle 1, \mu \rangle$ is similar but easier. \square

THEOREM 2.2. *If $\mathcal{L}^* = (1/\theta)\mathcal{L}$, where \mathcal{L} and θ are defined in Theorem 2.1, then \mathcal{L}^* is a reduced lattice.*

Proof. By Theorem 2.1 we see that \mathcal{L}^* has a basis which includes 1. If \mathcal{L}^* is not reduced, there must exist $\alpha \in \mathcal{L}^*$ such that $|\alpha| < 1$, $|\alpha'| < 1$, and $\alpha \neq 0$. Since $\alpha\theta \in \mathcal{L}$, it follows that $|\alpha\theta| < |\theta|$, $|\alpha'\theta'| < |\theta'|$ and $\alpha\theta \neq 0$. This contradicts the definition of θ . \square

THEOREM 2.3. *Let \mathcal{L}^* , \mathcal{L} , θ be as defined in Theorem 2.2 and let $\omega (> \theta)$ be the minimum adjacent to θ in \mathcal{L} . If $\theta^* (> 1)$ is the minimum adjacent to 1 in \mathcal{L}^* , then $\omega = \theta\theta^*$.*

Proof. Let $\phi = \theta\theta^*$. We have $\phi > \theta$ and $|\phi'| < |\theta'|$; thus, if $\phi \neq \omega$, then $\omega < \theta\theta^*$, and $|\omega'| < |\theta'|$. Since $\omega/\theta \neq 0$, $\omega/\theta \in \mathcal{L}^*$, $0 < \omega/\theta < \theta^*$, and $|\omega'/\theta'| < 1$, we have a contradiction to the definition of θ^* ; thus, $\omega = \phi$. \square

COROLLARY. *If $\mathfrak{N} = (1/\omega)\mathcal{L}$, then \mathfrak{N} is a reduced lattice. \square*

Let $\mathcal{L}_1 = \mathcal{L}$ be any reduced lattice. Let $\theta_g^{(n)} (> 1)$ be the minimum in \mathcal{L}_n adjacent to 1 and define $\mathcal{L}_{n+1} = (1/\theta_g^{(n)})\mathcal{L}_n$. By the theorems above we see that each of the \mathcal{L}_i is a reduced lattice. Further, if θ_1 in (2.1) is 1, then

$$(2.2) \quad \theta_n = \prod_{i=1}^{n-1} \theta_g^{(i)}$$

and

$$(2.3) \quad \theta_n \mathcal{L}_n = \mathcal{L}_1.$$

If \mathcal{L} has as its basis a basis of $\mathcal{O}_{\mathfrak{K}}$ or $\mathcal{O}_{\mathfrak{F}}$, then \mathcal{L} is reduced and $\epsilon_0 \in \mathcal{L}$. Also, since $|N(\epsilon_0)| = 1$, ϵ_0 must be a minimum of \mathcal{L} ; consequently, when $\theta_1 = 1$ we have $\epsilon_0 = \theta_{p+1}$ for some $p \geq 1$. Since $\mathcal{L}_1 = \epsilon_0 \mathcal{L}_{p+1} = \mathcal{L}_{p+1}$, we see that the algorithm for finding the \mathcal{L}_i is periodic with period length p .

We conclude this section with the following simple result.

LEMMA 2.4. *If $\theta (> 1)$ is the minimum adjacent to 1 in a reduced lattice $\mathfrak{R} = \langle 1, \mu, \nu \rangle$, then $|\theta' - 1| > 1$.*

Proof. Suppose $|\theta' - 1| \leq 1$. If we put $\phi = \theta - 1 \in \mathfrak{R}$, then $0 < \phi < \theta$ and $|\phi'| \leq 1$. If $|\phi'| = 1$, then $\phi = \pm 1$ and $\theta = 2$, which is not possible. If $|\phi'| < 1$ we have a contradiction to the definition of θ ; hence, $|\theta' - 1| > 1$. \square

3. The RCF and NICF in \mathfrak{S} . Let $\mathcal{L}_1 = \mathfrak{S}_1 = \langle 1, \mu_1 \rangle$ be a reduced lattice. From the results of Section 2 we see that the elements in a chain (2.1) in \mathfrak{S}_1 can be found from (2.2) once we know how to find the minimum $\theta (> 1)$ adjacent to 1 in any reduced lattice $\mathfrak{S} = \langle 1, \mu \rangle$. The following theorem of Voronoi [5] can be used to do this.

THEOREM 3.1. *Let $\mathfrak{S} = \langle \theta, \psi \rangle$ and suppose that $\psi > \theta > 0$. Then θ and ψ are adjacent minima of \mathfrak{S} if and only if $|\theta'| > |\psi'|$ and $\psi'\theta' < 0$.*

Proof. If ψ and θ are adjacent minima of \mathfrak{S} , then by definition we have $|\theta'| > |\psi'|$. Since $0 < \psi - \theta < \psi$, we must have $|\psi' - \theta'| > |\psi'|$; otherwise, ψ could not be a minimum. Hence $\theta'\psi' < 0$.

Suppose $|\theta'| > |\psi'|$ and $\theta'\psi' < 0$. If θ is not a minimum of \mathfrak{S} , there must exist $\gamma \in \mathfrak{S}$ such that $|\gamma| < \theta$ and $|\gamma'| < |\theta'|$. Since $\gamma = a\theta + b\psi$ ($a, b \in \mathbf{Z}$), this means that

$$|a\theta + b\psi| < \theta, \quad |a\theta' + b\psi'| < |\theta'|.$$

Clearly, neither a nor b is zero; but, if $ab > 0$, then $|a\theta + b\psi| > \theta$ and if $ab < 0$, then $|a\theta' + b\psi'| > |\theta'|$. Thus, θ is a minimum of \mathfrak{S} and by similar reasoning so is ψ . Further, there cannot exist $a, b \in \mathbf{Z}$ such that both $|a\theta + b\psi| < \psi$ and $|a\theta' + b\psi'| < |\theta'|$ hold; thus, θ and ψ are adjacent minima. \square

Thus, if $\mathfrak{S} = \langle 1, \psi \rangle$ where $\psi > 0$ and $\psi' < -1$, we see by the above theorem that \mathfrak{S} must be a reduced lattice and $\psi + [-\psi']$ must be the minimum adjacent to 1 in \mathfrak{S} . If we put $\mathfrak{S}_1 = \mathfrak{S}$, we have $\theta_g^{(1)} = \psi + [-\psi']$; also, by Theorems 2.2 and 3.1, we have $\theta_g^{(n+1)} = 1/\theta_g^{(n)} + [-1/\theta_g^{(n)}]$. Thus, if we put $\phi = \phi_0 = -\psi'$, $q_0 = [\phi_0]$, $\phi_k = -1/\theta_g^{(k)'}$, $q_k = [\phi_k]$, we find that

$$\phi_0 = [q_0, q_1, q_2, \dots, q_{n-1}, \phi_n]$$

is the RCF expansion of ϕ_0 . The regular continued fraction expansion of ϕ , where $\phi > 1$, $\phi' < 0$, is therefore equivalent to the chain (2.1) of minima in the lattice $\langle 1, -\phi' \rangle$. In fact $\theta_n = A_{n-2} - \phi' B_{n-2}$.

We will now give a similar interpretation of the NICF algorithm in \mathfrak{S} . We first let $\mathfrak{S} = \langle 1, \mu \rangle$ be reduced and let $\chi \in \mathfrak{S}$ be defined by

$$(3.1) \quad \chi = \begin{cases} \theta & \text{when } \theta' > -\frac{1}{2}, \\ \omega & \text{when } \theta' < -\frac{1}{2}, \end{cases}$$

where $\theta (> 1)$ is the minimum adjacent to 1 in \mathfrak{S} and $\omega (> \theta)$ is the minimum adjacent to θ in \mathfrak{S} .

Algorithm 1. Put $\mathfrak{T}_1 = \mathfrak{S}_1$ and let $\chi_g^{(n)}$ be the value of χ in \mathfrak{T}_n . Define $\mathfrak{T}_{n+1} = (1/\chi_g^{(n)})\mathfrak{T}_n$.

We see that the lattices \mathfrak{T}_i are all reduced by Theorem 2.3; further, if

$$(3.2) \quad \chi_n = \prod_{i=1}^{n-1} \chi_g^{(i)},$$

then $\chi_n \mathfrak{T}_n = \mathfrak{T}_1$.

THEOREM 3.2. *In (3.1) above, we have $\omega = \theta + 1$.*

Proof. Clearly $\mathfrak{S} = \langle 1, \theta \rangle = \langle \theta, \theta + 1 \rangle$. Further, $0 < \theta' + 1 < \frac{1}{2}$; hence, $|\theta' + 1| < |\theta'|$ and $(\theta' + 1)\theta' < 0$. The theorem now follows from Theorem 3.1. \square

THEOREM 3.3. *If $\mathfrak{S} = \langle 1, \psi \rangle$, where $|\psi'| < \frac{1}{2}$, $\psi > 1$, and \mathfrak{S} is a reduced lattice, then χ in (3.1) must be ψ .*

Proof. If $\psi' < 0$, then θ in (3.1) must be ψ by Theorem 3.1. Also, since $\psi' > -\frac{1}{2}$, we have $\chi = \theta = \psi$. If $\psi' > 0$, then $-1 < \psi' - 1 < -\frac{1}{2}$ and $\mathfrak{S} = \langle 1, \psi - 1 \rangle$. Since \mathfrak{S} is reduced, we must have $\theta = \psi - 1$, and $\theta' < -\frac{1}{2}$. It follows that $\chi = \omega = \theta + 1 = \psi$ by Theorem 3.2. \square

THEOREM 3.4. *Let $\psi > 1$ and $|\psi'| < \frac{1}{2}$. If we put $\phi = \text{sgn}(\psi')/\psi$ and $\chi = Ne(\phi') - \phi$, we must have $\chi > 1$ and $|\chi'| < \frac{1}{2}$.*

Proof. Clearly $|\chi'| < \frac{1}{2}$. Also, since $\psi > 1$, we have $|\phi| < 1$. Now if $\psi' < 0$, then $-\frac{1}{2} < \psi' < 0$; hence, $1/\psi' < -2$ and $\phi' > 2$. We have $\chi > 2 - \phi > 1$. Similarly, $\chi > 1$ when $\psi' > 0$. \square

Suppose that $\mathfrak{T}_1 = \mathfrak{S}_1 = \langle 1, \psi \rangle$, where $\psi > 0$ and $\psi' < -1$. We have $\chi_g^{(1)} = \psi - Ne(\psi')$ by Theorem 3.3. Also, by Theorems 3.3 and 3.4, $\chi_g^{(i+1)} = Ne(\phi'_i) - \phi_i$, where $\phi_i = \eta_i/\chi_g^{(i)}$ and $\eta_i = \text{sgn}(\chi_g^{(i)})$. If we put $\rho_0 = -\psi'$ and $\rho_i = (\prod_{j=1}^i \eta_j)\phi'_i$, we have

$$\rho_{i+1} = \left(\prod_{j=1}^i \eta_j \right) / \chi_g^{(i+1)'} = \left(\prod_{j=1}^i \eta_j \right) / (Ne(\phi'_i) - \phi_i) = 1/(Ne(\rho_i) - \rho_i).$$

Thus, the problem of expanding ϕ into a NICF when $\phi > 1$ and $\phi' < 0$ is equivalent to the problem of finding the values of χ_n in (3.2) when $\mathfrak{T}_1 = \mathfrak{S}_1 = \langle 1, -\phi'_1 \rangle$. Note that $|\rho'_i| = 1/\psi_g^{(i)}$; also, $\chi_n = |\bar{A}_{n-2} - \phi' \bar{B}_{n-2}|$.

We now have an interpretation of the NICF algorithm as a means of finding certain elements in the lattice \mathfrak{S} . In the next section we will extend the NICF to the NIVCF by extending Algorithm 1 in \mathfrak{S} to an algorithm analogous to it in \mathfrak{R} .

4. The VCF and the NIVCF in \mathfrak{R} . Throughout this section and the remainder of this work we will assume that $\mathfrak{R} = \langle 1, \mu, \nu \rangle$ and that \mathfrak{R} is a reduced lattice. We have seen that the problem of finding the elements of a chain (2.1) can be solved when we can solve the problem of finding the minimum adjacent to 1 in \mathfrak{L} . When $\mathfrak{L} = \mathfrak{S}$ Theorem 3.1 provides us with an easy method for determining this minimum and this, in turn, leads to the RCF. When $\mathfrak{L} = \mathfrak{R}$, however, the problem is somewhat more difficult. In [5] Voronoi showed how this could be done for the minimum adjacent to 1 and less than 1. In Section 33 of [5] he also gave a method for finding the minimum which is adjacent to 1 and greater than 1, but did not provide a proof for his method. He stated that he had such a proof but that it was too complicated to give. In [8] a method, slightly different from that of Voronoi was given for doing this. In order to briefly describe this technique, we require some notation.

Let $\alpha \in \mathfrak{R}$. We define the *puncture* $P(\alpha)$ to be the point $(\xi_\alpha, \eta_\alpha)$ in the x - y plane, where

$$\xi_\alpha = (2\alpha - \alpha' - \alpha'')/2, \quad \eta_\alpha = (\alpha' - \alpha'')/2i.$$

Further, we define $\zeta_\alpha = (\alpha' + \alpha'')/2$. We note that $\alpha = \zeta_\alpha + \xi_\alpha$, $\xi_{\alpha+\beta} = \xi_\alpha + \xi_\beta$, $\eta_{\alpha+\beta} = \eta_\alpha + \eta_\beta$, $\zeta_{\alpha+\beta} = \zeta_\alpha + \zeta_\beta$. Also, if $\alpha \in \mathfrak{Q}$, we have $\eta_\alpha = \xi_\alpha = 0$ and $\zeta_\alpha = \alpha$. Thus, the set of all punctures formed from all the points of \mathfrak{R} also forms a lattice $\mathfrak{L}^{(p)}$ with basis $\{P(\mu), P(\nu)\}$. We also point out that if ξ_α or η_α is rational, then δ must be the zero of both a quadratic and cubic polynomial with integer coefficients unless $\alpha \in \mathfrak{Q}$. Since $\alpha - [\alpha] \in \mathfrak{R}$, $0 \leq \alpha - [\alpha] < 1$, and $0 \leq \alpha' - [\alpha] < 1$ when $\alpha \in \mathfrak{Q}$, we see that, since \mathfrak{R} is reduced, we must have $\alpha = [\alpha]$. Thus, if ξ_α or η_α is rational, then $\alpha \in \mathbf{Z}$ and $\xi_\alpha = \eta_\alpha = 0$.

In [8] it is shown that there exist $\phi, \psi \in \mathfrak{R}$ such that

$$\xi_\phi > \xi_\psi > 0; \quad \eta_\phi \eta_\psi < 0, \quad |\eta_\psi| > |\eta_\phi|$$

and

$$|\eta_\psi| > \sqrt{3}/4, \quad |\eta_\phi| < 1 - \sqrt{3}/4, \quad 2|\eta_\psi| > 1 - |\eta_\phi|.$$

Further such ϕ and ψ can be found by using the RCF in $\mathfrak{L}^{(p)}$ as described in [2] or [8]. Actually, there exist ϕ, ψ in \mathfrak{R} such that $\xi_\phi > \xi_\psi > 0$, $\eta_\phi \eta_\psi < 0$, $|\eta_\phi| < \frac{1}{2}$, $|\eta_\psi| > \frac{1}{2}$, but these may be difficult for a computer to find because of precision problems; hence, the more relaxed conditions given above are preferable for computational purposes. In [8] the following theorem is proved.

THEOREM 4.1. *If $\theta (> 1)$ is the minimum adjacent to 1 in \mathfrak{R} , then $P(\theta)$ must be one of $P(\phi)$, $P(\psi)$, $P(\phi - \psi)$, $P(\phi + \psi)$ or $P(2\phi + \psi)$.*

Thus, once ϕ and ψ have been found there are only a few choices for $P(\theta)$. We need only find that θ such that $P(\theta)$ is one of these five choices, $|\theta'| < 1$ and $\theta (> 0)$ is least. Since

$$(4.1) \quad |\alpha'|^2 = \eta_\alpha^2 + \zeta_\alpha^2,$$

we must have $|\zeta_\alpha| < 1$. Hence θ must be $a + \gamma$, where γ is in $\{\phi, \psi, \phi - \psi, \phi + \psi, 2\phi + \psi\}$ and $a = [-\zeta_\gamma]$ or $[-\zeta_\gamma] + 1$. It is then necessary to find the least of these 10 possibilities for θ such that $|\theta'| < 1$. By evaluating the integer $I = N(\theta - N(\theta))$ this latter condition can be checked by using only integer arithmetic. We have $|\theta'| < 1$ if and only if $I < 0$.

It is of some interest to know how frequently we might expect $P(\theta)$ to be $P(\phi)$, $P(\psi)$, $P(\phi - \psi)$, $P(\phi + \psi)$ or $P(2\phi + \psi)$. To this end we computed all the lattices \mathfrak{R}_i ($i = 1, 2, 3, \dots, p$) where $\mathfrak{R}_1 = \langle 1, \mu, \nu \rangle$ and $\{1, \mu, \nu\}$ is a basis of $\mathcal{O}_{\mathfrak{F}}$ for each distinct pure cubic field $\mathfrak{F} = \mathcal{Q}(\sqrt[3]{D})$ with $D \leq 67,000$. We determined a total of 233762826 lattices and found that $P(\theta) = P(\phi)$ 137074347 times, $P(\theta) = P(\psi)$ 70776182 times, $P(\theta) = P(\phi - \psi)$ 24432636 times, $P(\theta) = P(\phi + \psi)$ 1479661 times, and $P(\theta) \neq P(2\phi + \psi)$. One might be led to conclude from this large amount of evidence that $P(\theta)$ is never $P(2\phi + \psi)$, but when $D = 68781$ we find that in \mathfrak{R}_{2307} , $\phi = (-72036 + 1809\delta + 28\delta^2)/126539$, and $\psi = (117574 - 2668\delta + 67\delta^2)/126539$. We have $\theta = (-26498 + 950\delta + 71\delta^2)/126539$ and $P(\theta) = P(2\phi + \psi)$. It certainly appears that this case is a rarity and, as such, seems to be a nuisance to consider. In fact, as we shall see from results in this section and Lemma 7.2, we can find ϵ_0 by ignoring this case. We may not find all the \mathfrak{R}_i and θ_i this way but we will find ϵ_0 .

In order to develop the NIVCF, we use the idea of Algorithm 1 in Section 3 and extend it to \mathfrak{R} . The value of θ' for θ in \mathfrak{S} represents the last coordinate of the corresponding point Θ of the lattice \mathfrak{S} . The analogous quantity for $\theta \in \mathfrak{R}$ is $\zeta_\theta = (\theta' + \theta'')/2$. If $\theta (> 1)$ is the minimum of \mathfrak{R} adjacent to 1 and $\omega (> \theta)$ is the minimum of \mathfrak{R} adjacent to θ , we define

$$(4.2) \quad \chi = \begin{cases} \theta & \text{when } \theta' + \theta'' > -1, \\ \omega & \text{when } \theta' + \theta'' < -1. \end{cases}$$

This is analogous to the definition (3.1) of χ in \mathfrak{S} . We also point out here that $\theta' + \theta'' < -1$ if and only if $N(\theta' + \theta'' + 1) < 0$. Now if $T = \theta + \theta' + \theta''$, $S = \theta\theta' + \theta'\theta'' + \theta''\theta$, $N = \theta\theta'\theta''$, then $T, S, N \in \mathbf{Z}$ and $N(\theta' + \theta'' + 1) < 0$ if and only if $N(T + 1 - \theta) < 0$. Since $N(T + 1 - \theta) = T^2 + 2T + 1 + (T + 1)S - N$, we can use integer arithmetic only to test whether or not $\theta' + \theta'' < -1$.

We now have

The NIVCF Algorithm. Put $\mathfrak{T}_1 = \mathfrak{R}_1$, and let $\chi_g^{(n)}$ be the value of χ in \mathfrak{T}_n . Define $\mathfrak{T}_{n+1} = (1/\chi_g^{(n)})\mathfrak{T}_n$.

We have

$$(4.3) \quad \chi_n = \prod_{i=1}^{n-1} \chi_g^{(i)}$$

and

$$(4.4) \quad \chi_n \mathfrak{T}_n = \mathfrak{T}_1.$$

This, of course, is just the same as Algorithm 1 except that $\mathfrak{T}_1 = \mathfrak{R}_1$ and we use (4.2) to define χ .

When $\theta' + \theta'' < -1$, we have $|\theta' + 1| < |\theta'|$ and $\theta + 1 > \theta$; thus, $\chi = \omega \leq \theta + 1$. Unfortunately, we cannot, as we did in Section 3, prove that $\omega = \theta + 1$; for this is not always the case. In the next few sections we will develop an algorithm for finding ω when $\theta' + \theta'' < -1$. In the remainder of this section we will develop some results concerning our NIVCF algorithm. These results are analogous to some of those presented in Section 1. We first require some simple lemmas.

LEMMA 4.2. *If $\chi_s = \theta_n$, then $\mathfrak{T}_s = \mathfrak{R}_n$.*

Proof. From (2.3), we have $\theta_n \mathfrak{R}_n = \mathfrak{R}_1$, and from (4.4) we have $\chi_s \mathfrak{J}_s = \mathfrak{J}_1$; thus, $\theta_n \mathfrak{R}_n = \chi_s \mathfrak{J}_s$ and since $\chi_s = \theta_n$, we must have $\mathfrak{J}_s = \mathfrak{R}_n$. \square

LEMMA 4.3. *If $\chi_s = \theta_n$, then $\chi_{s+1} = \theta_{n+1}$ or θ_{n+2} .*

Proof. From Lemma 4.2 we have $\mathfrak{J}_s = \mathfrak{R}_n$; thus, θ in \mathfrak{J}_s is $\theta_g^{(n)}$. If $\theta_g^{(n)'} + \theta_g^{(n)''} > -1$, then $\chi_g^{(s)} = \theta_g^{(n)}$; if $\theta_g^{(n)'} + \theta_g^{(n)''} < -1$, then $\chi_g^{(s)} = \omega = \theta_g^{(n)} \theta_g^{(n+1)}$ by Theorem 2.3. The lemma now follows easily from (2.2) and (4.3). \square

COROLLARY. *Given any χ_s , there exists some θ_n ($n \geq s$) such that $\chi_s = \theta_n$.*

Proof. Since $\chi_1 = \theta_1 = 1$, the result follows by using the lemma and induction on s . \square

COROLLARY. *Given any pair θ_n and θ_{n+1} from (2.1), at least one of them must be some χ_s with $s \leq n + 1$.*

Proof. By induction on n . \square

Notice that these results are analogous to results, which are proved in [7], concerning the NICF.

LEMMA 4.4. *Let $\rho \in \mathcal{Q}(\delta)$, $0 < \rho < 2m$ and $|\rho'| < m$, then $|d(\rho)| < c_2 m^6$, where $d(\rho) = (\rho - \rho')^2 (\rho' - \rho'')^2 (\rho'' - \rho)^2$ and $c_2 = 9(1047 + 85\sqrt{153})/128 \approx 147.543$.*

Proof. Put $c = \rho$, $a + bi = \rho'$, $a - bi = \rho''$, where a, b, c are real. Then $|\rho'|^2 = a^2 + b^2 < m^2$, $|a| < m$, $|b| < m$, and

$$\sqrt{|d(\rho)|} = 2|b|((a - c)^2 + b^2).$$

Since $|d(\rho)| \leq 4b^2(c^2 + b^2)^2 < 100m^6 < c_2 m^6$ when $a \geq 0$, we need only consider the case of $a < 0$. We note that since $b^2 < m^2 - a^2$ and $|c - a| < 2m - a$, we have

$$(a - c)^2 + b^2 < (2m - a)^2 + m^2 - a^2 = 5m^2 - 4am$$

for values of x such that $|x| < m$, the function $f(x) = 4(m^2 - x^2)(5m^2 - 4xm)^2$ has a single maximum at $x = (5 - \sqrt{153})m/16$; thus, $f(x) < c_2 m^6$ when $|x| < m$. It follows that $|d(\rho)| < c_2 m^6$ when $-m < a < 0$. \square

We now prove a result which is analogous to Theorem 1.3. Part of the proof of this result is based on an idea which Arne Brentjes (personal communication) used to extend Theorem 1 of [9]. We assume that $\{1, \mu, \nu\}$ is a basis of $\mathcal{O}_{\mathfrak{F}}$ and $\mathfrak{R} = \langle 1, \mu, \nu \rangle$.

THEOREM 4.5. *Let $\alpha = x + y\mu + z\nu$, where $\gcd(x, y, z) = 1$, if $\alpha > 1$ and $N(\alpha) < \sqrt[4]{|\Delta|}/c_2$, then $\alpha = \chi_k$ for some $k > 1$.*

Proof. Certainly $\alpha \neq \chi_1 = 1$. Assume $\alpha \neq \chi_k$ for any $k > 1$. Since $\alpha > 1$, there must be some integer $n \geq 1$ such that

$$\theta_n \leq \alpha < \theta_{n+1}$$

in the chain (2.1) when $\theta_1 = 1$. If $\alpha \neq \theta_n$, put $\rho = N(\alpha)\theta_n/\alpha$. We have $\rho \in \mathcal{O}_{\mathfrak{F}}$, $0 < \rho < N(\alpha)$ and $|\rho'| < N(\alpha)$, the latter result following from the fact that α is not the minimum adjacent to θ_n . If $\alpha = \theta_n$, then, since $\alpha \neq \chi_k$ for any $k \geq 1$, we must have $\theta_{n+1} = \chi_k$ for some $k \geq 1$ by a corollary of Lemma 4.3. In this case put $\rho = N(\alpha)\theta_{n+1}/\alpha = N(\alpha)\theta_g^{(n)}$. Now $|\theta_g^{(n)}| < 1$ and $\chi_g^{(k-1)} = \theta_g^{(n-1)}\theta_g^{(n)} \leq \theta_g^{(n-1)} + 1$; thus, $|\rho'| < N(\alpha)$ and $0 < \rho \leq N(\alpha)(1 + 1/\theta_g^{(n-1)}) < 2N(\alpha)$. It follows from the

above observations that if $\alpha \neq \chi_k$ for any $k > 1$, there must exist some $\rho \in \mathcal{O}_{\mathfrak{F}}$ such that $0 < \rho < 2N(\alpha)$, $|\rho'| < N(\alpha)$. Further, since $\rho = N(\alpha)\beta/\alpha$, where $\alpha \neq \beta$ and $\beta = \theta_n$ or θ_{n+1} , we cannot have $d(\rho) = 0$. For, if $d(\rho) = 0$, then $\rho \in \mathbf{Z}$ as $\rho \in \mathcal{O}_{\mathfrak{F}}$. Since $\beta = a + b\mu + c\nu$, where $a, b, c \in \mathbf{Z}$, we get $x = N(\alpha)a/\rho$, $y = N(\alpha)b/\rho$, $z = N(\alpha)c/\rho$. Since $\gcd(x, y, z) = 1$ and $\gcd(a, b, c) = 1$ (otherwise β could not be a minimum of \mathfrak{R}), we get $\rho = N(\alpha)$ and $\beta = \alpha$, which is not so.

Now

$$d(\rho) = N(\alpha)^6 \left(\frac{\beta}{\alpha} - \frac{\beta'}{\alpha'}\right)^2 \left(\frac{\beta'}{\alpha'} - \frac{\beta''}{\alpha''}\right)^2 \left(\frac{\beta''}{\alpha''} - \frac{\beta}{\alpha}\right)^2$$

$$= \frac{N(\alpha)^6}{(\alpha\alpha'\alpha'')^4} \begin{vmatrix} \alpha^2 & \alpha\beta & \beta^2 \\ \alpha'^2 & \alpha'\beta' & \beta'^2 \\ \alpha''^2 & \alpha''\beta'' & \beta''^2 \end{vmatrix}.$$

Since $\alpha, \beta \in \mathcal{O}_{\mathfrak{F}}$, we have $A = (a_{ij})_{3 \times 3}$, where $a_{ij} \in \mathbf{Z}$ such that

$$(\alpha^2, \alpha\beta, \beta^2) = (1, \mu, \nu)A.$$

Thus, we have

$$\begin{vmatrix} \alpha^2 & \alpha\beta & \beta^2 \\ \alpha'^2 & \alpha'\beta' & \beta'^2 \\ \alpha''^2 & \alpha''\beta'' & \beta''^2 \end{vmatrix} = \begin{vmatrix} 1 & \mu & \nu \\ 1 & \mu' & \nu' \\ 1 & \mu'' & \nu'' \end{vmatrix} |A|$$

and $|d(\rho)| = N(\alpha)^2 |A|^2 |\Delta|$.

Since $d(\rho) \neq 0$, we have $|A| \neq 0$ and $|A| \in \mathbf{Z}$. By Lemma 4.4, $|d(\rho)| < c_2 N(\alpha)^6$; hence, $c_2 N(\alpha)^4 > |A|^2 |\Delta|$. We see that

$$N(\alpha) > \sqrt[4]{|A|^2 |\Delta| / c_2} \geq \sqrt[4]{|\Delta| / c_2}$$

and this is impossible. Thus $\alpha = \chi_k$ for some $k \geq 1$. \square

We also have a corollary which is analogous to Theorem 1.2.

COROLLARY. *If $\Delta < -23$, then $\varepsilon_0 + \chi_k$ for some $k > 1$; if $\Delta = -23$, then $\varepsilon_0^2 = \chi_2$.*

Proof. $N(\varepsilon_0) = 1$ and $1 < \sqrt[4]{|\Delta| / c_2}$ for $|\Delta| > c_2$. Thus we need only test directly the few cases (see, for example, [2]) where $|\Delta| < c_2$. For each of these cases we find that $\varepsilon_0 = \chi_k$ for some $k > 1$ except for the case of $\Delta = -23$ where $\chi_2 = \varepsilon_0^2$. \square

Note that if $\pi = k - 1$ in this corollary, we have $\mathfrak{F}_{\pi+1} = \mathfrak{F}_1$ and the NIVCF algorithm is periodic with period length π . We also note that the NIVCF algorithm can be used to find all of the solutions $\alpha \in \mathcal{O}_{\mathfrak{F}}$ of the Diophantine equation

$$N(\alpha) = I$$

when $|I| < \sqrt[4]{|\Delta| / c_2}$.

5. Geometric Inequalities. In order to find χ in any reduced lattice \mathfrak{R} we need to be able to find ω when $\theta' + \theta'' < -1$. We will do this by limiting the number of possibilities for $P(\omega)$. In order to do this we require the inequalities from plane Euclidean geometry which are presented in this section. For our further work the most important of these results are Lemmas 5.4, 5.5, 5.6 and 5.7. However, in order

to prove these results we require three simple lemmas which we give here without proof. We say that P is in a certain geometric figure if it is either on the boundary of that figure or within it.

LEMMA 5.1. *If P is any point in the triangle ABC , then $\overline{AP} \leq \max(\overline{AB}, \overline{AC})$. \square*

The next two lemmas refer to Figure 1 below.

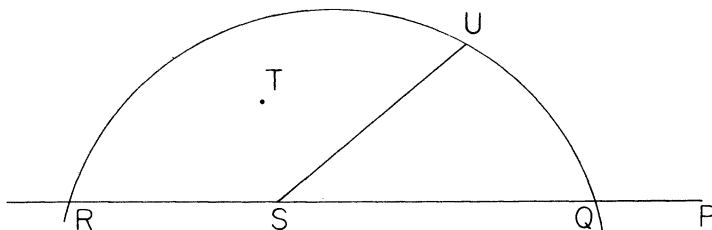


FIGURE 1

Here RQ is a chord of a circle and U lies on the smaller of the arcs cut off by RQ or on either of them if RQ is a diameter of the circle.

LEMMA 5.2. *If T is any point in the segment RUQ in Figure 1 and P is any point on the chord RQ produced, then $\overline{PT} \leq \overline{PR}$. \square*

LEMMA 5.3. *If T is any point in the region bounded by the lines RS , SU , and the arc RU , then $\overline{ST} \leq \max(\overline{RS}, \overline{SU})$. \square*

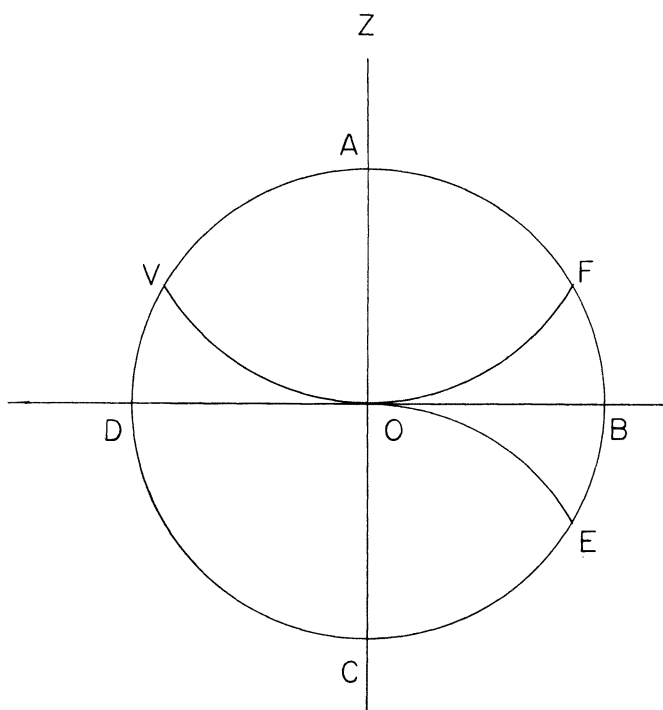


FIGURE 2

In the lemmas that follow we will refer to a figure (Figure 2) which we now describe. Let $OZ(z)$ and $OY(y)$ be perpendicular axes. The circle centre O and radius $\overline{OA} = 1$ cuts the positive z axis at A , and the positive y axis at B , the negative z and y axes at C and D , respectively. The arc VOF is described by a circle with centre A and radius 1. F is the point where this arc meets the arc AB and V is the point where this arc meets the arc AD . Also, the arc OE is described by a circle with centre C and radius 1 and E is the point where this arc meets the arc BC . We denote that figure bounded by the line OC and the arcs OF and FC by the symbol \mathcal{Q} .

We now consider the figure ABC (see Figure 3) which is bounded by three circular arcs with centres A, B, C , the vertices of an equilateral triangle, and radii equal to \overline{AB} .

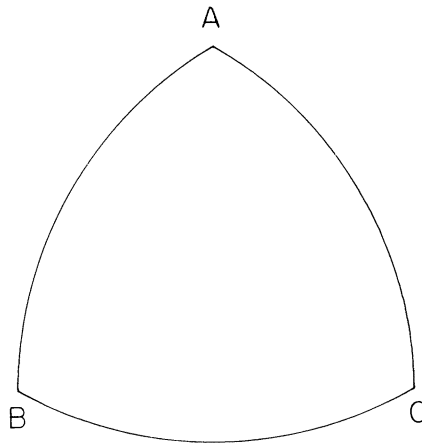


FIGURE 3

This is the Reuleaux triangle and is well known as a figure of constant breadth. As such it follows that if P, Q are any two points in the Reuleaux triangle above, we must have $\overline{PQ} \leq \overline{AB}$. Since the figure \mathcal{Q} is completely covered by two Reuleaux triangles with vertices at O, F, E and O, C, E , we have the following lemma.

LEMMA 5.4. *If P, Q are any two points in \mathcal{Q} and $\overline{PQ} > 1$, then one of the points must lie above the arc OE and the other must lie below the arc OE . Further, if R is any other point of \mathcal{Q} , then $\min(\overline{PR}, \overline{QR}) \leq 1$. \square*

LEMMA 5.5. *Let P, Q be any two points in the semicircle ABC of Figure 2 such that $\overline{PQ} = 1$ and PQ is parallel to AC . If R is any point in this same semicircle such that $\overline{OR} \leq \max(\overline{OP}, \overline{OQ})$, then $\min(\overline{PR}, \overline{QR}) \leq 1$.*

Proof. We refer to Figure 4 below.

We may assume with no loss of generality that $\overline{OP} \geq \overline{OQ}$. If $P = (a, b)$, $Q = (a, b - 1)$, then since both P, Q are in the semicircle, we have $\frac{1}{2} \leq b \leq 1$ and $0 \leq a \leq \sqrt{3}/2$. If $R = (r, s)$ and $|s| \geq \frac{1}{2}$, then R, Q are in the Reuleaux triangle OCE or R, P are in the Reuleaux triangle OFA . In either case we get $\min(\overline{PR}, \overline{QR}) \leq 1$. We now assume $|s| < \frac{1}{2}$. Let \mathcal{C}_1 and \mathcal{C}_2 be circles with radii 1 and centres P and Q ,

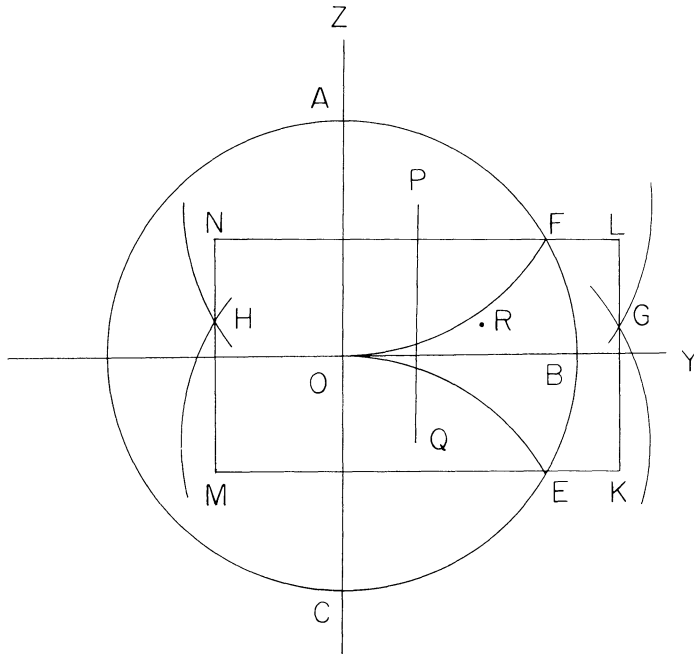


FIGURE 4

respectively. \mathcal{C}_1 and \mathcal{C}_2 intersect at points $G = (a + \sqrt{3}/2, b - \frac{1}{2})$ and $H = (a - \sqrt{3}/2, b - \frac{1}{2})$. Let $K = (a + \sqrt{3}/2, -\frac{1}{2})$, $L = (a + \sqrt{3}/2, \frac{1}{2})$, $M = (a - \sqrt{3}/2, -\frac{1}{2})$, $N = (a - \sqrt{3}/2, \frac{1}{2})$. The rectangle $LKMN$ is covered by the circles \mathcal{C}_1 and \mathcal{C}_2 ; thus, if R lies in this rectangle, the lemma is certainly true. In order, then, to prove the lemma completely, we need only show that it holds when $r > a + \sqrt{3}/2$. If $r > a + \sqrt{3}/2$ and $s \geq b - \frac{1}{2}$, then $r^2 + s^2 \leq a^2 + b^2$, $bs \geq b^2 - b/2$, and $ra > a^2 + a\sqrt{3}/2$; also,

$$\begin{aligned} \overline{PR}^2 &= (a - r)^2 + (b - s)^2 = a^2 + b^2 + r^2 + s^2 - 2(ar + bs) \\ &< 2a^2 + 2b^2 - 2b^2 + b - 2a^2 - \sqrt{3}a \\ &= b - \sqrt{3}a \leq 1. \end{aligned}$$

If $r > a + \sqrt{3}/2$ and $s < b - \frac{1}{2}$, we have $1 - b \geq 0$, $-s > \frac{1}{2} - b$, and $s(b - 1) > (1 - b)(\frac{1}{2} - b)$. Thus

$$\overline{PQ}^2 = (a - r)^2 + (b - 1 - s)^2 < b - \sqrt{3}a \leq 1.$$

Thus, one of \overline{PQ} or \overline{PR} must be less than 1 and the lemma is proved. \square

LEMMA 5.6. In Figure 2 let L be a point on OB such that $\overline{OL} = \lambda = \sqrt{(5 - \sqrt{5})/8}$. Let KLM be a line perpendicular to OB , meeting the arc AB at K , the arc OF at G , the arc OE at H , and the arc BC at M . Let P be any point on the figure bounded by the line GH and the arcs OG and OH . If Q is in the Figure \mathcal{Q} and $\overline{OP} \geq \overline{OQ}$, then $\overline{PQ} \leq 1$.

Proof. We refer to Figure 5 below.

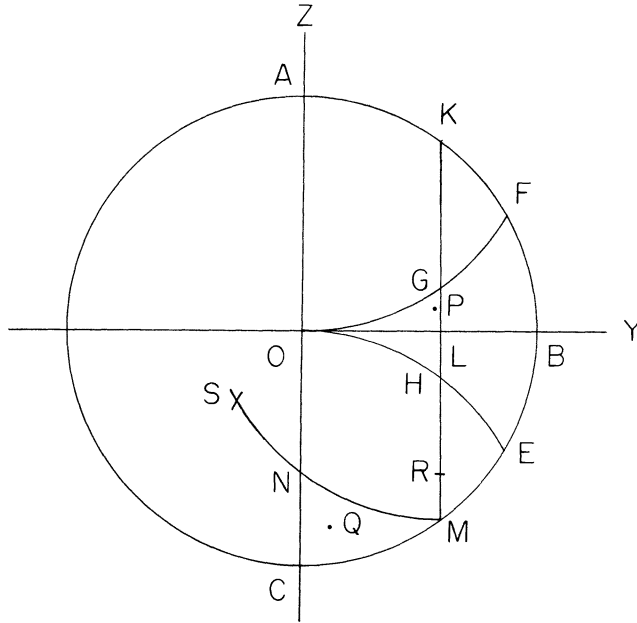


FIGURE 5

We first note that $\overline{GM} = \overline{OC} = 1$. Let S be that point such that $\overline{SM} = \overline{SG} = \overline{GM}$ and S is to the left of the z -axis. Let the arc SM with radius 1 and centre G cut OC at N . If Q lies in the Reuleaux triangle MSG , we have $\overline{PQ} \leq 1$. If Q lies above the arc OE , we have $\overline{PQ} \leq 1$. If Q lies below the arc OE and to the right of the line KLM , then $\overline{OQ} > \overline{OH} = \overline{OG} \geq \overline{OP}$, which is not so. Thus, we need only consider Q as lying on the figure bounded by the line NC and the arcs NM and CM . Put $g = \overline{GL}$, $a = \overline{OG}$, $b = \overline{ON}$. We have $\lambda^2 + g^2 = a^2$ and $(1 - g)^2 + \lambda^2 = 1$. It follows that $2g = a^2$ and $g = 1 \pm \sqrt{1 - \lambda^2} = 1 \pm (1 + \sqrt{5})/4$. Since $g < \frac{1}{2}$, we get $g = (3 - \sqrt{5})/4$ and $a = (\sqrt{5} - 1)/2$. If $\overline{RM} = \overline{GL}$, then $\overline{LR} = \overline{ON}$, $2g + b = 1$, and we find that $b = a$. Since we need not consider Q to be N , we have $\overline{OQ} > \overline{ON} = \overline{OG} \geq \overline{OP}$, which is not possible \square

LEMMA 5.7. Let Q be any point in \mathcal{Q} and let R be the point lying below Q such that $\overline{QR} \parallel AC$ and $\overline{QR} = 1$. Let P be any point of \mathcal{Q} such that P lies below the arc OE and $\overline{PQ} > 1$, $\overline{PR} > 1$. Let S be that point such that $\overline{SA} = \overline{PQ}$, $\overline{SO} = \overline{PR}$ and S is on the other side of AC from P . If T is any point in that region of the semicircle ADC below or on the arc VO , then $\min(\overline{PT}, \overline{ST}) \leq 1$.

Proof. Refer to Figure 6 below.

We first note that since $\overline{PQ} > 1$, Q must, by Lemma 5.4, lie above the arc OE . Let U be the point below S such that $\overline{US} = 1$, $\overline{US} \parallel AC$ and let M be the point above P such that $\overline{PM} = 1$ and $\overline{PM} \parallel AC$. We see that $SMPU$, $MPRQ$, and $ASUO$ are parallelograms. Also, M lies in the Reuleaux triangle AOE , and, since $\overline{OU} = \overline{SA} = \overline{PQ} > 1$, U lies outside the circle $ABCD$. Let \overline{MP} and \overline{QR} meet OB at N and W , respectively. Since $\overline{MQ} = \overline{PR} > 1$, it follows from Lemma 5.5 that $\overline{OQ} \geq \overline{OP}$. If

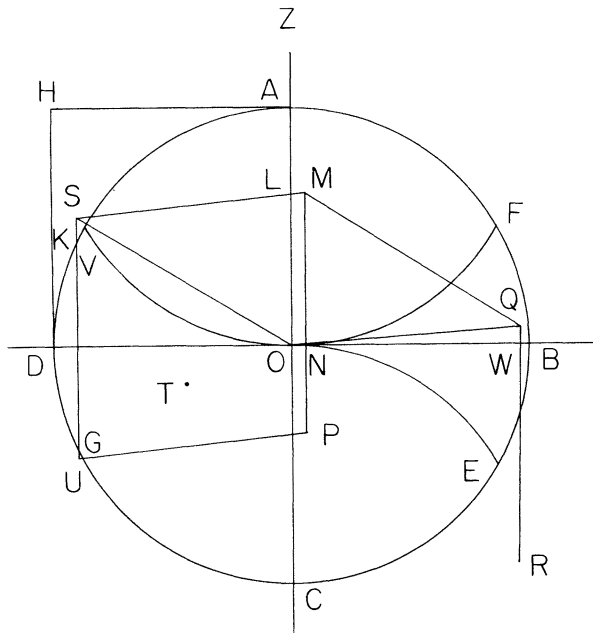


FIGURE 6

$\overline{ON} \geq \overline{OW}$, then $\overline{NP} \leq \overline{QW}$ and this means that P and Q must lie in the same Reuleaux triangle OFE , an impossibility. Hence $\overline{ON} < \overline{OW}$ and $OSMQ$ is a parallelogram with $MS \parallel OQ$ and $\overline{MS} = \overline{OQ} \leq 1$.

Since M lies in the Reuleaux triangle AOF , the angles OAM and AOM cannot be obtuse. Let SM meet AC at L . We have $\overline{SL} \leq \overline{SM} \leq 1$ and $\overline{SO} > 1, \overline{SA} > 1$; hence, the angles SAM and SOM must be acute. If L lies above A on the z -axis, then, since the angles LAM and OAM are complementary, we see that the angle SAM cannot be acute, a contradiction. Similarly, L cannot lie below O on the z -axis. Since L must lie between O and A on OA , we see that the angles SAL and SOL are acute. Since the perpendicular distance of S to PM is the same as that from Q to AO , we also see that S must lie in the square $DOAH$. Indeed, since $\overline{OS} = \overline{PR} > 1$, S must lie in the triangle DHA .

Suppose T lies in that segment of the circle $ABCD$ which is cut off by the chord formed by producing UP . Suppose further that T lies under this chord. Since U and P both lie below or on DB and on opposite sides of AC , by Lemma 5.3 we get $\overline{PT} \leq \max(\overline{PC}, \overline{UP})$. Since $\overline{UP} = \overline{SM} = \overline{OQ} \leq 1$ and P and C are in the Reuleaux triangle OCE , we get $\overline{PT} \leq 1$.

If T lies in the parallelogram $SUPM$, then by Lemma 5.1, either \overline{PT} or \overline{ST} must be less than or equal to $\max(\overline{UP}, \overline{PM}) = 1$. If T lies in the segment KDG which is cut off the circle $ABCD$ by SU , then, by Lemma 5.2 $\overline{ST} \leq \overline{SG} < \overline{SU} = 1$.

Since S must lie in the triangle DHA , we must have $\overline{HS} \leq 1$ by Lemma 5.1. Thus, if T lies in the triangle HSL , then $\overline{ST} \leq 1$ by Lemma 5.1. If T lies in the triangle HAL , then T lies in the triangle HAO and this means that T must lie above the arc VO , which is not so. Since there are no other possible regions of the semicircle ADC in which T could be, the lemma is proved. \square

6. Some Lemmas Concerning the Reduced Lattice \mathfrak{R} . In order to complete our development of the NIVCF algorithm in Section 8 we will make use of a number of lemmas concerning any reduced lattice $\mathfrak{R} = \langle 1, \mu, \nu \rangle$. We note that if $\theta \in \mathfrak{R}$, $|\theta'| \leq 1$, $|\theta' - 1| > 1$ and $\eta_\theta > 0$, then $P = (\eta_\theta, \zeta_\theta)$ is a point in \mathcal{Q} of Section 5.

LEMMA 6.1. *If $\omega, \chi \in \mathfrak{R}$; $|\omega'|, |\chi'| \leq 1$; and $2\chi = \omega + 1$, then $|\chi' - 1| \leq 1$.*

Proof. We have $2\zeta_\chi = \zeta_\omega + 1$ and $\eta_\omega = 2\eta_\chi$. Further, from (4.1), $\zeta_\omega^2 + \eta_\omega^2 = |\omega'|^2 \leq 1$ and $|\zeta_\omega| \leq 1$. It follows that

$$1 + \zeta_\omega^2 + \eta_\omega^2 + 2|\zeta_\omega| \leq 4$$

and, as a consequence, $(\zeta_\chi - 1)^2 + \eta_\chi^2 \leq 1$. Hence $|\chi' - 1| \leq 1$. \square

LEMMA 6.2. *Let $\omega, \chi, \psi \in \mathfrak{R}$, where ω, χ, ψ are all distinct $|\omega'|, |\chi'|, |\psi'| \leq 1$, and $|\omega' - 1|, |\chi' - 1|, |\psi' - 1| > 1$. If $\eta_\omega \eta_\chi > 0$ and $\eta_\chi \eta_\psi > 0$, we cannot have any b such that $b < \omega, \chi, \psi < b + 1$.*

Proof. By symmetry we may assume with no loss of generality that $P = (\eta_\omega, \zeta_\omega)$, $Q = (\eta_\chi, \zeta_\chi)$, $R = (\eta_\psi, \zeta_\psi)$ are all points in \mathcal{Q} . By Lemma 5.4, two of these points, say Q and R , are such that $\overline{QR} \leq 1$. Thus, $|\chi' - \psi'| \leq 1$. If $b < \chi, \psi < b + 1$, then $|\chi - \psi| < 1$, and we can only have $\chi = \psi$, a contradiction. \square

LEMMA 6.3. *Let $\theta, \omega \in \mathfrak{R}$ such that $|\theta'| \leq 1$, $|\omega'| \leq 1$, $\omega > \theta > 1$, and $|\omega'| < |\theta'|$. If $\eta_\omega \eta_\theta > 0$ and $|\theta' + 1| \leq 1$, then $\omega \geq \theta + 1$.*

Proof. Suppose $\omega < \theta + 1$. Since $\omega > \theta$, we have $0 < \omega - \theta < 1$ and $-1 < \omega - \theta - 1 < 0$. Since $\eta_\omega \eta_\theta > 0$ and $|\theta' + 1| \leq 1$, we may assume with no loss of generality that $P = (\eta_\theta, \zeta_\theta + 1)$, $Q = (\eta_\theta, \zeta_\theta)$, $R = (\eta_\omega, \zeta_\omega)$ in Figure 4. Since $|\omega'| = \overline{OR} < \overline{OP} = |\theta'|$, we must have one of $\overline{QR} = |\omega' - \theta'|$ or $\overline{PR} = |\omega' - \theta' - 1|$ less than or equal to 1 by Lemma 5.5. Since $\omega - \theta, \omega - \theta - 1 \in \mathfrak{R}$, we can only have $\omega = \theta$ or $\omega = \theta + 1$. The latter is impossible and the former is also impossible since $|\omega'| < |\theta'|$. Thus, we must have $\omega \geq \theta + 1$. \square

LEMMA 6.4. *Let $\theta, \omega \in \mathfrak{R}$ such that $\omega > \theta > 1$; $|\omega'|, |\theta'| \leq 1$; $|\theta' - 1|, |\omega' - 1| > 1$; and $\eta_\omega \eta_\theta > 0$. If $|\theta'| > |\omega'|$ and $|\eta_\theta| < \lambda$, then $\omega \geq \theta + 1$.*

Proof. If $|\theta' + 1| \leq 1$, then by Lemma 6.3, we have $\omega \geq \theta + 1$. Thus, we may assume $|\theta' + 1| > 1$. With no loss of generality, we may also assume $P = (\eta_\theta, \zeta_\theta)$, $Q = (\eta_\omega, \zeta_\omega)$ in Figure 5. Since $\overline{OP} = |\theta'| > |\omega'| = \overline{OQ}$, we must, by Lemma 5.6, have $\overline{PQ} = |\theta' - \omega'| \leq 1$. If $\theta < \omega < \theta + 1$, we find that $\theta - \omega = 0$, which is not possible; thus, $\omega \geq \theta + 1$. \square

LEMMA 6.5. *Let $\theta, \omega, \chi \in \mathfrak{R}$ such that $|\theta'| \leq 1$, $|\omega'| \leq 1$, $|\omega' + 1| \leq 1$, $|\omega' - 1| > 1$, $|\theta' - 1| > 1$, $|\chi' - 1| > 1$, $\eta_\theta \eta_\omega < 0$, $\eta_\omega \eta_\chi > 0$. If $|\omega' - \chi'| > 1$ and $|\omega' - \chi' + 1| > 1$, then either $|\theta' - \omega' + \chi' - 1| \leq 1$ or $|\theta' - \omega'| \leq 1$.*

Proof. With no loss of generality we may assume that $T = (\eta_\theta, \zeta_\theta)$, $P = (\eta_\omega, \zeta_\omega)$, $Q = (\eta_\chi, \zeta_\chi)$, $R = (\eta_\chi, \zeta_\chi - 1)$ in Figure 6. Since $\overline{PQ} = |\omega' - \chi'| > 1$ and $\overline{PK} = |\omega' - \chi' + 1| > 1$ and $S = (\eta_\omega - \eta_\chi, \zeta_\omega - \zeta_\chi + 1)$, we must have $\overline{ST} = |\theta' - \omega' + \chi' - 1|$ or $\overline{PT} = |\omega' - \theta'|$ less than or equal to 1 by Lemma 5.7. \square

LEMMA 6.6. Let $\theta, \omega, \chi \in \mathbb{R}$ and let $\theta (> 1)$ be the minimum adjacent to 1. Suppose that $|\omega'| \leq 1, |\chi'| \leq 1, |\theta' + 1| \leq 1, |\omega' + 1| \leq 1, \eta_\omega \eta_\theta < 0, \eta_\omega \eta_\chi > 0$. If $\theta < \chi, \omega < \theta + 1$, then $\theta = \omega + 1 - \chi$.

Proof. Since $0 < \chi - 1, \omega - 1 < \theta$, we see by the reasoning of Lemma 2.4 that $|\chi' - 1|, |\omega' - 1| > 1$.

If $|\omega' - \chi'|, |\omega' - \chi' + 1| > 1$, then, by Lemma 6.5, either $|\omega' - \theta'| \leq 1$ or $|\theta' - \omega' + \chi' - 1| \leq 1$. If $|\omega' - \theta'| \leq 1$, then since $|\omega - \theta| < 1$, we get $\omega = \theta$ which is not so. If $|\theta' - \omega' + \chi' - 1| \leq 1$, we see that $|\rho'| \leq 1$, where $\rho = \theta - \omega + \chi - 1$. Now $\theta + \chi > \theta + 1 > \omega$ and $\chi - (\omega + 1) < 0$; thus, $-1 < \rho < \theta$. It follows that ρ can only be 0 or 1. But if $\rho = 0$, then $\theta = \omega - \chi + 1$ and this is impossible because $|\omega' - \chi' + 1| > 1$. If $\rho = 1$, then $\theta = \omega - \chi + 2$. Since $|\omega' - \chi' + 1| > 1$ and $-3/2 < \zeta_\omega - \zeta_\chi < 1/2$, we cannot have $|\theta'| < 1$; thus, $\rho \neq 1$.

If $|\omega' - \chi'| \leq 1$, then $\omega = \chi$, which is not so. Hence, we must assume that $|\omega' - \chi' + 1| \leq 1$ and $|\omega' - \chi'| > 1$. Put $\rho = \omega - \chi + 1$. We have $|\rho'| < 1$ and $0 < \rho < 1 + 1 < 1 + \theta$. Since we cannot have $\rho < \theta$, we have $\theta \leq \rho < 1 + \theta$. If $\rho = \theta$, we have the lemma; thus, we will assume that $\theta < \rho < 1 + \theta$. By the reasoning of Lemma 2.4, we have $|\rho' - 1| > 1$.

Suppose $\eta_\rho \eta_\omega > 0$. If $\rho = \omega$, we get $\chi = 1$, an impossibility. If $\rho = \chi$, then $2\chi = \omega + 1$. Since $|\chi' - 1| > 1$, this cannot be true by Lemma 6.1. Thus, ρ, χ, ω are all distinct elements of \mathbb{R} such that $\eta_\rho, \eta_\omega, \eta_\chi$ have the same sign; $|\rho'|, |\omega'|, |\chi'| \leq 1$; $|\rho' - 1|, |\omega' - 1|, |\chi' - 1| > 1$; $\theta < \rho, \omega, \chi < \theta + 1$. By Lemma 6.2, this is impossible.

If $\eta_\rho = 0$, then $\omega - \chi \in \mathbb{Z}$. Since $|\omega - \chi| < 1$, this means that $\omega = \chi$, which is not so. We can only have $\eta_\rho \eta_\omega < 0$ and, as a consequence, $\eta_\rho \eta_\theta > 0$. Since $0 < \rho - \theta < 1$ and $-1 < \rho - \theta - 1 < 0$, we see that $|\theta' - \rho'| > 1$ and $|\theta' - \rho' + 1| > 1$. Since $|\theta' + 1| \leq 1$, we get $|\chi' - \theta'| \leq 1$ or $|\chi' - \theta' + \rho' - 1| \leq 1$ by Lemma 6.5. Since $0 < \chi - \theta < 1$, we cannot have $|\chi' - \theta'| \leq 1$. Since $\chi - \theta + \rho - 1 = \omega - \theta$, we also cannot have $|\chi' - \theta' + \rho' - 1| \leq 1$. It follows that $\rho = \theta$. \square

If $\omega \in \mathbb{R}, \omega \notin \mathbb{Q}$ and $P(\omega) = (\xi_\omega, \eta_\omega)$ is the puncture of ω , let ω^* be defined as that element of \mathbb{R} such that $P(\omega^*) = P(\omega), |\omega^*| \leq 1$ and $|\omega^*|$ is minimal. We note here that if $|\eta_\omega| > 1$, then ω^* cannot exist. Since there must exist $a \in \mathbb{Z}$ such that $|\zeta_\omega - a| \leq \frac{1}{2}$, we see that if $|\eta_\omega| < \sqrt{3}/2$, then $\eta_\omega^2 - (\zeta_\omega - a)^2 < 1$. That is, if $|\eta_\omega| < \sqrt{3}/2$, then ω^* exists. We also point out that if ω^* exists and $\omega^* > 0$, then $|\omega^* - 1| > 1$. For if $|\omega^* - 1| \leq 1$, then $\omega^* > 1$ and $|\omega^* - 1| < |\omega^*|$. Since $P(\omega^*) = P(\omega^* - 1)$, this contradicts the definition of ω^* .

We require the following lemma of [8] (Lemma 4.3).

LEMMA 6.7. Let $P(\chi) = (\xi_\chi, \eta_\chi)$ be the puncture of $\chi \in \mathbb{R}$ such that $\xi_\chi > 0, |\eta_\chi| < \sqrt{3}/2$, and let $P(\omega) = (\xi_\omega, \eta_\omega)$ be the puncture of $\omega \in \mathbb{R}$. If $|\omega'| \leq 1, \xi_\omega > \xi_\chi$, and $\eta_\omega \eta_\chi > 0$, then $\omega > \chi^*$. \square

LEMMA 6.8. Let $\theta (> 1)$ be the minimum of \mathbb{R} adjacent to 1 and let $\omega (> \theta)$ be the minimum of \mathbb{R} adjacent to θ . Suppose that $|\theta' + 1| \leq 1$ and $\omega < \theta + 1$. If there exists $\chi \in \mathbb{R}$ such that $|\eta_\chi| < \sqrt{3}/2, \xi_\omega > \xi_\chi > 0, \eta_\omega \eta_\chi > 0$, then $\chi^* = \omega + 1 - \theta$.

Proof. Since $|\eta_\chi| < \sqrt{3}/2, \chi^*$ exists. Further, since $|\chi^*| > 1$ and $\chi^* = \xi_\chi + \zeta_{\chi^*}$ with $\xi_\chi > 0$ and $\zeta_{\chi^*} \geq -1$, we have $\chi^* > 1$. Since $\eta_\chi \eta_\omega > 0, \xi_\omega > \xi_\chi$, and $|\omega'| \leq 1$,

we must have $\omega > \chi^*$ by Lemma 6.7. Since ω is a minimum of \mathfrak{R} , it follows that $|\chi^{*'}| > |\omega'|$. Since $|\chi^{*'}| < 1$ and $\chi^* > 0$, we must have $\chi^* > \theta$. If $\chi^* \geq \theta + 1$, then $\omega > \theta + 1$, which is not so; thus, $1 < \theta < \chi^* < \omega < \theta + 1 < \chi^* + 1$. Further, $|\chi^{*'} - 1| > 1$ and $|\omega' - 1| > 1$.

If $|\chi^* + 1| \leq 1$, by Lemma 6.3, we get $\omega > \chi^* + 1$, which is impossible. Since $|\omega - \chi^*| < 1$, we must have $|\omega' - \chi^{*'}| \geq 1$. By Lemma 5.4, we must have $|\omega' + 1| \leq 1$. If $\eta_\theta \eta_\omega > 0$, then $\omega \geq \theta + 1$ by Lemma 6.3. Thus, $\eta_\theta \eta_\omega < 0$ and $\theta = \omega + 1 - \chi^*$ by Lemma 6.6. \square

7. The Main Result. In this section we will show how to limit the possible values for ω in \mathfrak{R} . We assume that we have found $\phi, \psi \in \mathfrak{R}$ and a basis $\{P(\phi), P(\psi)\}$ of $\mathcal{L}^{(P)}$ with the properties given in Section 4. We require simple results concerning elements of \mathfrak{R} which have certain punctures in $\mathcal{L}^{(P)}$. Throughout this section and the next we denote by $\theta (> 1)$ the minimum adjacent to 1 in \mathfrak{R} and by $\omega (> \theta)$ the minimum adjacent to θ in \mathfrak{R} .

LEMMA 7.1. *If $\zeta_\theta < -\frac{1}{2}$, $\omega \neq \theta + 1$, $\theta \neq \phi^*$, $\omega \neq \phi^*$, and either $\xi_\theta > \xi_\phi$ or $\eta_\theta \eta_\phi < 0$, then $\xi_\phi > \xi_\omega$.*

Proof. Since $|\eta_\phi| < \sqrt{3}/2$, ϕ^* exists. Further, since $\xi_\phi > 0$, we have $\phi^* > 1$. Since $|\phi^{*'}| \leq 1$, we must have $\phi^* > \theta$. If $\xi_\theta > \xi_\phi$ and $\eta_\theta \eta_\phi > 0$, then $\theta > \phi^*$ by Lemma 6.7; thus, we may assume $\eta_\theta \eta_\phi < 0$. Since $\eta_\omega \eta_\theta < 0$ (see the proof of Lemma 6.8), we also have $\eta_\omega \eta_\phi > 0$. If $\xi_\omega > \xi_\phi$, we have $\omega > \phi^*$ by Lemma 6.7; thus, since ω is a minimum, $|\omega'| < |\phi^{*'}|$. If $\omega > \phi^*$, then, since $|\eta_\phi| < \lambda$, we must have $\omega \geq \phi^* + 1 > \theta + 1$ by Lemma 6.4. Since $\zeta_\theta < -\frac{1}{2}$, this is impossible. \square

LEMMA 7.2. *If $P(\theta) = 2P(\phi) + P(\psi)$, then $\zeta_\theta < -\frac{1}{2}$.*

Proof. Since $|\eta_\phi| < 1 - \sqrt{3}/4 < \sqrt{7}/4$, we have

$$\sqrt{1 - \eta_\phi^2} > 3/2 - \sqrt{1 - \eta_\phi^2}.$$

Since $|\phi^{*'} - 1| > 1$, we have $\zeta_{\phi^*} < 1 - \sqrt{1 - \eta_\phi^2}$. Since $\phi^* > 1$ and $\phi^* = \xi_\phi + \zeta_{\phi^*}$, we see that $\xi_\phi > \frac{1}{2} + \zeta_{\phi^*}$. Since $\theta < \phi^*$, we have $\zeta_\theta + 2\xi_\phi + \xi_\psi < \zeta_{\phi^*} + \xi_\phi$; hence, $\zeta_\theta < \zeta_\theta + \xi_\psi < \zeta_{\phi^*} - \xi_\phi < -\frac{1}{2}$.

LEMMA 7.3. *If $P(\theta) = 2P(\phi) + P(\psi)$, then $\theta < \phi^* < \theta + 1$, $|\theta'| > |\phi^{*'}|$, and $\zeta_{\phi^*} > 0$.*

Proof. Since $\theta = \zeta_\theta + \xi_\theta < \phi^* = \zeta_{\phi^*} + \xi_\phi$, we have $\zeta_{\phi^*} > \xi_\phi + \zeta_\theta$. Also, $\zeta_{\phi^*} + \xi_\phi = \phi^* > 1$; thus, $\zeta_{\phi^*} > 1 - \zeta_{\phi^*} + \zeta_\theta$ and $2\zeta_{\phi^*} > 1 + \zeta_\theta > 0$. Since $|\eta_\phi| < \sqrt{3}/2$ and $|\phi^{*'} - 1| > 1$, we must have $0 < \zeta_{\phi^*} < \frac{1}{2}$; further, $\xi_\phi > 1 - \zeta_{\phi^*} > \frac{1}{2} > \zeta_{\phi^*}$. Thus, $\zeta_\theta < \zeta_{\phi^*} - \xi_\phi < 0$ and $|\zeta_\theta| > \xi_\phi - \zeta_{\phi^*} > 1 - 2\zeta_{\phi^*} > 2\sqrt{1 - \eta_\phi^2} - 1$.

Now $\theta < \phi^* < 2\xi_\phi < 1 + \zeta_\theta + 2\xi_\phi + \xi_\psi = 1 + \theta$. Since $-\frac{1}{2} < -\zeta_{\phi^*} < 1 - \zeta_{\phi^*} + \zeta_\theta < \zeta_{\phi^*} < \frac{1}{2}$, we must have $|\eta_\theta - \eta_\phi| > \sqrt{3}/2$. Hence, $|\eta_\psi| > \sqrt{3}/2 + |\eta_\phi| > 2|\eta_\phi|$

and $\eta_\theta \eta_\phi < 0$. Thus, $|\eta_\theta| > \sqrt{3}/2 - |\eta_\phi|$ and

$$\begin{aligned} |\theta|^2 &= \eta_\theta^2 + \zeta_\theta^2 > (\sqrt{3}/2 - |\eta_\phi|)^2 + \left(2\sqrt{1 - \eta_\phi^2} - 1\right)^2 \\ &> (\sqrt{3}/2 - (1 - \sqrt{3}/4))^2 + \left(2\sqrt{1 - (1 - \sqrt{3}/4)^2} - 1\right)^2 \\ &> (1 - \sqrt{3}/4)^2 + \left(1 - \sqrt{1 - (1 - \sqrt{3}/4)^2}\right)^2 \\ &> \eta_\phi^2 + \zeta_\phi^2 \\ &= |\phi^*|^2. \quad \square \end{aligned}$$

LEMMA 7.4. *If $P(\theta) = P(\phi) + P(\psi)$ and $\zeta_\theta < -\frac{1}{2}$, then $P(\omega) \neq P(\phi) - P(\psi)$.*

Proof. Assume that $P(\omega) = P(\phi) - P(\psi)$. If $\phi^* > \theta + 1$, then $\zeta_{\phi^*} + \xi_\phi > \zeta_\theta + \xi_\phi + \xi_\psi + 1$ and $\zeta_{\phi^*} > \zeta_\theta + 1 + \xi_\psi > 0$. If ψ^* exists, then $\xi_\psi > 1 - \zeta_{\psi^*} > \frac{1}{2}$ and $\zeta_{\phi^*} > \frac{1}{2}$, which is not possible. If ψ^* does not exist, we must have $|\eta_\psi| > \sqrt{3}/2$. Consider $\chi = \phi^* - \omega$. Since $P(\chi) = P(\psi)$, we see that $|\phi^{*'} - \omega'| > 1$; for, otherwise, ψ^* would exist. Also $|\eta_\omega| = |\eta_\phi - \eta_\psi| = |\eta_\phi| + |\eta_\psi| > |\eta_\phi| + \sqrt{3}/2$ and $\zeta_{\phi^*} > 0$. Thus $P = (\eta_\phi, \zeta_{\phi^*})$ and $Q = (\eta_\omega, \zeta_\omega)$ must lie in the same Reuleaux triangle *FOE* in Figure 2 and $|\phi^{*'} - \omega'| = \overline{PQ} \leq 1$, a contradiction.

Thus, we must have $\phi^* \leq \theta + 1$. Since $P(\phi^*) \neq P(\theta)$, we can only have $\phi^* < \theta + 1$; hence, $\theta < \phi^*$, $\omega < \theta + 1$, $\eta_\theta \eta_\omega < 0$ and $\eta_\phi \eta_\omega > 0$. One of $|\omega' + 1|$ or $|\phi^{*'} + 1|$ must be less than or equal to 1; for if this were not the case we would see that the points P, Q above would be such that $|\phi^{*'} - \omega'| = \overline{PQ} \leq 1$, which is not possible. Thus, by Lemma 6.6, we get $\theta = \omega + 1 - \phi^*$ or $\theta = \phi^* + 1 - \omega$. Since $P(\theta) \neq -P(\psi)$ and $P(\theta) \neq P(\psi)$, neither of these is possible; hence, $P(\omega) \neq P(\phi) - P(\psi)$. \square

In the theorem below we are able to give the possibilities for the puncture of ω when $\zeta_\theta < -\frac{1}{2}$.

THEOREM 7.5. *When $\zeta_\theta < -\frac{1}{2}$, the puncture of $\omega, P(\omega)$, must be one of the punctures given in the second column of the table below.*

TABLE 7.1

$P(\theta)$	possible values of $P(\omega)$
$P(\phi)$	$P(\phi), P(\psi), P(\phi + \psi)$
$P(\psi)$	$P(\phi), P(\psi), P(\phi - \psi)$
$P(\phi - \psi)$	$P(\psi), P(\phi - \psi)$
$P(\phi + \psi)$	$P(\phi), P(\phi + \psi)$
$P(2\phi + \psi)$	$P(\phi)$

Proof. By Theorem 4.1 we know that $P(\theta)$ must be one of the 5 possible entries in the first column of Table 7.1. Since $P(\omega) \in \mathcal{L}^{(p)}$, we must have

$$(7.1) \quad P(\omega) = aP(\phi) + bP(\psi),$$

where $a, b \in \mathbf{Z}$. That is,

$$(7.2) \quad \xi_\omega = a\xi_\phi + b\xi_\psi,$$

$$(7.3) \quad \eta_\omega = a\eta_\phi + b\eta_\psi.$$

Further, we note that since θ, ω are minima of \mathfrak{R} , we have $|\omega' - 1| > 1, |\theta' - 1| > 1$; also, $|\theta' + 1| \leq 1$ and $\xi_\omega > 1 - \zeta_\omega > 0, \omega \leq \theta + 1, |\omega'| < |\theta'|$. When $\omega \neq \theta + 1$, we have $\eta_\omega \eta_\theta < 0$ by Lemma 6.3. Suppose $a < 0$ in (7.1). Since $\xi_\omega > 0$, we must have $b > 0$ and $|\eta_\omega| = |a||\eta_\phi| + b|\eta_\psi|$ from (7.3). Since $|\eta_\omega| < 1$, we have $b < 2$. Since $\xi_\phi > \xi_\psi$, we must also have $b > |a|$. Thus, $b = 1$ and $a = 0$, which is not possible. Thus $a \geq 0$ in (7.1).

Case 1. ($P(\theta) = P(\phi)$). If $a = 0$ in (7.1), then $\xi_\omega = b\xi_\psi$ and $\eta_\omega = b\eta_\psi$; thus, $0 < b < 3$. If $b = 2$, then $\eta_\omega \eta_\psi > 0, \xi_\omega > \zeta_\psi$ and $|\eta_\psi| < \frac{1}{2} < \sqrt{3}/2$. It follows that ψ^* exists and by Lemma 6.8 $\psi^* = \omega + 1 - \theta$. Since $P(\psi) = P(\psi^*) = P(\omega - \theta)$, we get $P(\psi) = P(\theta)$, which is impossible for $a = 0, b = 2$. Thus, if $a = 0$ we can only have $b = 1$.

Suppose $a > 0$. If $b \leq 0$, then from (7.3) we get $\eta_\omega \eta_\phi > 0$ and $\eta_\omega \eta_\theta > 0$. By Lemma 6.3, we can only have $\omega = \theta + 1$ and $a = 1, b = 0$. If $b \geq a$, put $c = b - a \geq 0$; we have, $\eta_\omega = a(\eta_\phi + \eta_\psi) + c\eta_\psi$ and $(\eta_\phi + \eta_\psi)\eta_\psi > 0$. Thus, if $|\eta_\phi + \eta_\psi| > \frac{1}{2}$, then $|\eta_\psi| > \frac{1}{2}$. If either $a \geq 2$ or $c \geq 1$, we have $|\eta_\omega| > 1$ which is not so. Thus $a = b = 1$. If $|\eta_\phi + \eta_\psi| < \frac{1}{2}$, then there exists $\chi = (\phi + \psi)^*$. Since $\eta_\omega \eta_\chi > 0$ and $\xi_\omega > \xi_\chi > 0$ when $(a, b) \neq (1, 1)$, we have (Lemma 6.8) $\chi = \omega + 1 - \theta$. Since this means that $P(\omega) = P(2\phi + \psi) = 2P(\phi) + P(\psi)$, we get a contradiction. When $1 \leq b < a$, we have $\omega = \zeta_\omega + \xi_\omega = \zeta_\omega + a\xi_\phi + b\xi_\psi > 2\xi_\theta + \zeta_\omega > \xi_\theta + 1 - \zeta_\theta - 1 > \xi_\theta + \zeta_\theta + 1$. Thus, $\omega > \theta + 1$ and this is impossible. We have proved the first row of Table 7.1. Before dealing with the remaining 4 cases we point out that if $P(\omega) \neq P(\phi), P(\theta) \neq P(\omega)$ and either $\eta_\theta \eta_\phi < 0$ or $\xi_\theta > \xi_\phi$, then $\xi_\phi > \xi_\omega$ by Lemma 7.1.

Case 2. ($P(\theta) = P(\psi)$). If $a = 0$, then $b > 0$ and $\eta_\theta \eta_\omega = b\eta_\psi^2 > 0$; thus, by Lemma 6.3, we get $\omega \geq \theta + 1$, which can only be so if $\omega = \theta + 1$ and $(a, b) = (0, 1)$. If $a > 0$, we have $P(\theta) \neq P(\omega)$ and $\eta_\theta \eta_\phi = \eta_\psi \eta_\phi < 0$. Thus, $\xi_\phi > \xi_\omega$ when $P(\omega) \neq P(\phi)$. If $b > 0$, then $P(\omega) \neq P(\phi)$ and $\xi_\omega > \xi_\phi$, which is not so. If $b = 0$, then $\xi_\omega > \xi_\phi$ unless $a = 1, b = 0$. If $b < 0$, we must have $|b| \leq 1$; otherwise, $|\eta_\omega| > 1$. If $b = -1$ and $a > 1$, then $P(\omega) \neq P(\phi)$ and $\xi_\omega > \xi_\phi$, thus $(a, b) = (1, -1)$.

Case 3. ($P(\theta) = P(\phi - \psi)$). Since $\zeta_\theta < -\frac{1}{2}$ and $|\theta'| < 1$, we must have $|\eta_\theta| < \sqrt{3}/2$. Thus, $|\eta_\theta| = |\eta_\phi| + |\eta_\psi| < \sqrt{3}/2$ and $|\eta_\psi| < \sqrt{3}/2$. If $P(\omega) \neq P(\theta)$, then $\eta_\omega \eta_\theta < 0$. Further, $\eta_\theta \eta_\phi > 0$ and $\eta_\phi \eta_\psi < 0$; thus, $\eta_\omega \eta_\psi > 0$ and $\eta_\omega \eta_\phi < 0$. If $\xi_\omega > \xi_\psi$, we must have $\psi^* = \omega + 1 - \theta$ by Lemma 6.8. This means that $P(\omega) = P(\phi)$, which cannot be so as $\eta_\omega \eta_\phi < 0$. Thus, $0 < \xi_\omega \leq \xi_\psi$ and $0 < a\xi_\phi + b\xi_\psi \leq \xi_\psi$ and $b < 1$ or $(a, b) = (0, 1)$. If $b = 0$, then $\eta_\omega \eta_\phi > 0$; hence, $b < 0$. Since $1 > |\eta_\omega| = a|\eta_\phi| + |b||\eta_\psi|$, we must have $b > -2$. Since $b = -1$ and $0 < a\xi_\phi - \xi_\psi < \xi_\psi$, we see that a can only be 1 and this contradicts $P(\omega) \neq P(\theta)$.

Case 4. ($P(\theta) = P(\phi + \psi)$). Assume $P(\omega) \neq P(\phi)$ and $P(\omega) \neq P(\theta)$. Since $\xi_\theta > \xi_\phi$, we have $\xi_\phi > \xi_\omega$. If $a > 0$, then, since $0 < a\xi_\phi + b\xi_\psi < \xi_\phi$, we must have $b < 0$. By the reasoning used in Case 2 we have $b = -1$ and $a = 1$. By Lemma 7.4, this is not possible. Thus, we can only have $a = 0$ and $b > 0$. If this is so, we notice that $\eta_\theta = \eta_\phi + \eta_\psi$ and $\eta_\omega = b\eta_\psi$ have the same sign. By Lemma 6.3, this means that

$\omega \geq \theta + 1$. If $\omega = \theta + 1$, we get a contradiction; thus, we can only have $P(\omega) = P(\phi)$ or $P(\omega) = P(\theta) = P(\phi + \psi)$.

Case 5. ($P(\theta) = P(2\phi + \psi)$). By Lemma 7.3, we have $0 < \phi^* < \theta + 1$ and $|\phi^*| < |\theta|$. If $\omega \neq \phi^*$, then $P(\omega) \neq P(\phi)$ and $\omega \neq \theta + 1$. Thus, $\theta < \omega$, $\phi^* < \theta + 1$. If $\eta_\theta \eta_\phi > 0$, then, since $\xi_\theta > \xi_\phi$, we get $\theta > \phi^*$ by Lemma 6.7. Since this is not possible, we must have $\eta_\theta \eta_\phi < 0$. Now $\eta_\omega \eta_\theta < 0$; hence, $\eta_\phi \eta_\omega > 0$. Using the reasoning of Lemma 7.4, we see that one of $|\omega' + 1|$ or $|\phi^{*'} + 1|$ is less than or equal to 1; thus, by Lemma 6.6, we have either $\theta = \phi^* + 1 - \omega$ or $\theta = \omega + 1 - \phi^*$. In the first case we put $P(\omega) = P(-\phi - \psi)$, an impossibility. In the second case we get $P(\omega) = P(3\phi + \psi)$; but then $\xi_\omega > \xi_\phi$ and this cannot be so as $P(\omega) \neq P(\phi)$. Thus we can only have $P(\omega) = P(\phi^*) = P(\phi)$. \square

8. Implementation of the NIVCF Algorithm. We now describe how to find the possible values of $P(\omega)$ and then how ω itself can be found. We let v be defined to be θ when $P(\theta) \neq P(2\phi + \psi)$. When $P(\theta) = P(2\phi + \psi)$ we define v to be ϕ^* . By Theorem 7.5, $\phi^* = \omega$ when $P(\theta) = P(2\phi + \psi)$; thus, v is that point of \mathfrak{R} such that $P(v)$ is one of $P(\phi)$, $P(\psi)$, $P(\phi - \psi)$ or $P(\phi + \psi)$, $|v| \leq 1$, $v > 0$ and v is the least point of \mathfrak{R} with all of these properties. Clearly v can be calculated by using the same methods as those described in Section 4 for finding θ . The only difference is that $P(v) \neq P(2\phi + \psi)$.

THEOREM 8.1. *If $\zeta_v > -\frac{1}{2}$, then $\omega = v$. If $\zeta_v < -\frac{1}{2}$, then the values of $P(\omega)$ can be found from the possibilities listed in the second column of Table 8.1.*

TABLE 8.1

$P(v)$	possible values of $P(\omega)$
$P(\phi)$	$P(\phi), P(\psi), P(\phi + \psi)$
$P(\psi)$	$P(\psi), P(\phi), P(\phi - \psi)$
$P(\phi - \psi)$	$P(\psi), P(\phi - \psi)$
$P(\phi + \psi)$	$P(\phi), P(\phi + \psi)$

Proof. If $\zeta_v > -\frac{1}{2}$, then either $\zeta_\theta > -\frac{1}{2}$ or $P(\theta) = P(2\phi + \psi)$. In the first case, $\omega = \theta = v$; in the second case, by Lemma 7.2 we have $\zeta_\theta < -\frac{1}{2}$ and $\omega = \phi^* = v$. If $\zeta_v < -\frac{1}{2}$, then we cannot have $P(\theta) = P(2\phi + \psi)$ by Lemma 7.3; hence, $v = \theta$ and $\zeta_\theta < -\frac{1}{2}$. The possibilities for the puncture of ω can now be found from Table 7.1. \square

Note that implicit in this result is the fact that we can run the Voronoi algorithm as given in Section 4 without ever having to consider the $(a, b) = (2, 1)$ case. That is, instead of finding $\theta_g^{(i)}$ in \mathfrak{R}_i , we find $v_g^{(i)}$ in \mathfrak{R}_i . We will still find ϵ_0 . In fact, $\epsilon_0 = \prod_{i=1}^r v_g^{(i)}$ and $r \leq p$.

If $P(\omega)$ is one of $P(\gamma_1), P(\gamma_2), \dots, P(\gamma_k)$, we need to know how to find ω . As described in Section 4 we find the at most $2k$ possible values $\gamma_{11}, \gamma_{12}, \gamma_{21}, \gamma_{22}, \dots, \gamma_{k1}, \gamma_{k2}$ that ω could be. After finding the least of these $2k$ values which exceeds θ , we need only determine whether or not $|\gamma| < |\theta|$. If so, $\omega = \gamma$; if not we delete this value of γ from among the possible values for ω and try again. A method of

determining whether or not $|\gamma'| < |\theta'|$ which involves calculations with integers only can be developed by examining the integer $I = N(\theta\gamma'\gamma'' - N(\theta))/N(\theta)$. We have $|\gamma'| < |\theta'|$ if and only if $I < 0$.

By using the ideas developed above together with the methods described in [8], a computer program was written to implement the NIVCF algorithm on an AMDAHL 470-V7 computer. To get some idea of how certain aspects of the algorithm behave, we computed all of the distinct lattices \mathfrak{T}_i , where $\mathfrak{T}_1 = \mathfrak{R}_1 = \langle 1, \mu, \nu \rangle$ and $\{1, \mu, \nu\}$ is a basis of $\mathcal{O}_{\mathfrak{F}}$ for each distinct pure cubic field $\mathfrak{F} = \mathcal{Q}(\sqrt[3]{D})$ with $D \leq 91000$. The total number of lattices found was 325354898. We had $\theta' + \theta'' < -1$ for 112413018 of these. We consider these latter lattices in more detail in Table 8.2.

TABLE 8.2

puncture of θ , frequency	puncture of ω , frequency
$P(\phi)$, 88139367	$P(\phi)$, 83928591; $P(\psi)$, 2759217; $P(\phi + \psi)$, 1451559
$P(\psi)$, 18584743	$P(\phi)$, 1673460; $P(\psi)$, 15267239; $P(\phi - \psi)$, 1644044
$P(\phi - \psi)$, 4440826	$P(\psi)$, 1123515; $P(\phi - \psi)$, 3317311
$P(\phi + \psi)$, 1248082	$P(\phi)$, 1248082; $P(\phi + \psi)$, 0

Notice that in most of these cases $\omega = \theta + 1$, the exception being the case in which the puncture of θ is $P(\phi + \psi)$, where we found no instance of $\omega = \theta + 1$. There does not appear to be any a priori reason for why ω should never be $\theta + 1$ in this case. However, it must be true that if $\omega = \theta + 1$, when $P(\theta) = P(\phi + \psi)$, then $\xi_\psi < \frac{1}{2}$ and $|\eta_\psi| < 2|\eta_\phi|$. It seems, therefore, that $\omega = \theta + 1$ would not occur very frequently in this case. Probably, if we were to continue our calculations beyond the values of D considered here, we would find an instance of $\omega = \theta + 1$, just as we finally found a θ with puncture $P(2\phi + \psi)$ in Section 4.

We also determined all the distinct \mathfrak{R}_i produced by the VCF when \mathfrak{R}_1 is defined above and $36000 \leq D \leq 64000$. We found that the VCF algorithm found a total of 144092600 distinct \mathfrak{R}_i and the NIVCF found a total of 108315954 distinct \mathfrak{T}_i for values of D in the same range. The ratio is .7517. In fact, for most values of D the ratio π/p seems to be between .74 and .75. For example, when $D = 252727$, $p = 135340$ and $\pi = 100911$ for a ratio of .7456. This value is somewhat larger than the corresponding value of about .69 for the NICF versus the RCF algorithm. When we compared the actual timings on running the VCF and NIVCF for finding a specific θ_n , we found that the NIVCF found this θ_n value in about 79 to 80 percent of the time needed by the VCF algorithm. Thus, the computational evidence seems to suggest that wherever one is using the VCF algorithm, one should instead use the faster NIVCF algorithm.

Department of Computer Science
 University of Manitoba
 Winnipeg, Manitoba, Canada R3T 2N2

1. W. W. ADAMS, "On the relationship between the convergents of the nearest integer and regular continued fractions," *Math. Comp.*, v. 33, 1979, pp. 1321-1331.
2. B. N. DELONE & D. K. FADDEEV, *The Theory of Irrationalities of the Third Degree*, Transl. Math. Monos., vol. 10, Amer. Math. Soc., Providence, R. I., 1964.

3. A. HURWITZ, "Über eine besondere Art der Kettenbruchentwicklung reeller Größen," *Acta Math.*, v. 12, 1889, pp. 367–405.
4. B. MINNIGERODE, "Über eine neue Methode, die Pellsche Gleichung aufzulösen," *Gött. Nachr.* 1873, 619–653.
5. G. VORONOI, *On a Generalization of the Algorithm of Continued Fractions*, Doctoral Dissertation, Warsaw, 1896. (Russian)
6. H. C. WILLIAMS & P. BUHR, "Calculation of the regulator of $Q(\sqrt{D})$ by use of the nearest integer continued fraction algorithm," *Math. Comp.* v. 33, 1979, pp. 369–381.
7. H. C. WILLIAMS, "Some results concerning the nearest integer continued fraction expansion of \sqrt{D} ," *J. Reine Angew. Math.*, v. 315, 1980, pp. 1–15.
8. H. C. WILLIAMS, G. CORMACK & E. SEAH, "Calculation of the regulator of a pure cubic field," *Math. Comp.*, v. 34, 1980, pp. 567–611.
9. H. C. WILLIAMS, "Improving the speed of calculating the regulator of certain pure cubic fields," *Math. Comp.*, v. 34, 1980, pp. 1423–1434.
10. H. C. WILLIAMS, G. W. DUECK & B. K. SCHMID, "A rapid method of evaluating the regulator and class number of a pure cubic field," *Math. Comp.*, v. 41, 1983, pp. 235–286.