MATHEMATICS OF COMPUTATION
Volume 75, Number 255, July 2006, Pages 1507–1518
S 0025-5718(06)01899-0
Article electronically published on April 3, 2006

DEPENDENCY OF UNITS IN NUMBER FIELDS

CLAUS FIEKER AND MICHAEL E. POHST

Abstract. We develop a method for validating the indepencence of units in algebraic number fields. In case that a given system of units has a dependency, we compute a certificate for this.

1. Introduction

A key problem in computational number theory is to decide whether a given system of units $\{\varepsilon_1, \ldots, \varepsilon_l\}$ is (multiplicatively) independent, i.e., to decide if for some $\mathbf{z} = (z_1, \ldots, z_l) \in \mathbb{Z}^l$, $\mathbf{z} \neq 0$, we have

$$\prod_{i=1}^{l} \varepsilon_i^{z_i} = 1.$$

This problem occurs naturally during the computation of class groups or unit groups and is therefore important for most applications.

There are known algorithmic solutions for this problem (e.g., the use of MLLL [8] or a real-gcd [3, Algorithm 6.5.7]), but they lack reliability in the sense that they utilize real arithmetic and do not provide rigorous error analysis.

In our new approach, we use a different numerical method to check for dependencies (with an error analysis) and then use any of the above methods to find a dependency.

2. Notation

Throughout this section and the subsequent ones F denotes an algebraic number field of degree d over the rational numbers $\mathbb{Q}$. We assume that it is generated by a root ρ of a monic irreducible polynomial

$$f(t) \;=\; t^d + a_1 t^{d-1} + \cdots + a_d \;\in\; \mathbb{Z}[t].$$

Over the complex numbers $\mathbb{C}$ the polynomial $f(t)$ splits into a product of linear factors

$$f(t) \;=\; \prod_{j=1}^{d} (t - \rho^{(j)}),$$

Received by the editor July 21, 2004.
2000 *Mathematics Subject Classification.* Primary 11Y16, 11-04.
This article was written while the second author visited the Computational Algebra Group at the University of Sydney in October, 2003.

where the conjugates $\rho = \rho^{(1)}, \ldots, \rho^{(d)}$ are ordered as usual; i.e., $\rho^{(1)}, \ldots, \rho^{(r_1)} \in \mathbb{R}$ and $\rho^{(r_1+1)}, \ldots, \rho^{(d)} \in \mathbb{C}\setminus\mathbb{R}$ subject to $\rho^{(r_1+j)} = \overline{\rho^{(r_1+r_2+j)}}$ $(1 \le j \le r_2)$, and where $\overline{\rho}$ denotes the complex conjugate of ρ. In particular, we have

$$d = r_1 + 2r_2.$$

Any element α of F can be presented as a linear combination of 1, $\rho, \ldots, \rho^{d-1}$, with rational coefficients. Substituting $\rho^{(j)}$ for ρ in that presentation, we obtain the jth conjugate $\alpha^{(j)}$ of α $(1 \le j \le d)$. Arithmetical problems usually require computations with algebraic integers contained in F; i.e., those elements of F whose minimal polynomials have coefficients in $\mathbb{Z}$. They form a ring o_F with a $\mathbb{Z}$-basis $\omega_1, \ldots, \omega_d$ (integral basis of F), the so-called maximal order of F. In the remainder we fix some integral basis. Any element β of F is then presentable by a vector of d rational numbers via

$$\beta \;=\; \sum_{i=1}^{d} b_i\,\omega_i \;\; (b_i \in \mathbb{Q}).$$

We note that β is in o_F precisely if all b_i are rational integers.

For a matrix $A \in \mathbb{R}^{l\times k}$, we write $\|A\|_\infty$ for the largest entry (by absolute value) of A and likewise for vectors. We write $\|\mathbf{x}\|_2$ to denote the usual Euclidean norm of a vector $\mathbf{x} \in \mathbb{R}^l$.

A positive definite matrix $B \in \mathbb{R}^{l\times l}$ gives rise to a positive definite form $Q : \mathbb{R}^n \to \mathbb{R} : \mathbf{x} \mapsto \mathbf{x}^{\mathrm{tr}} B\mathbf{x}$. By $d(Q)$ we denote the discriminant of this quadratic form, i.e., $d(Q) = \sqrt{\det B}$. Let $M_i(Q)$ be Minkowski's successive minima of Q:

$$M_i(Q) := \min_{\lambda>0}\{\exists \mathbf{x}_1, \ldots, \mathbf{x}_i \in \mathbb{Z}^l \text{ linearly independent with } Q(\mathbf{x}_i) \le \lambda\}$$

and let γ_l be Hermite's constant. We will make extensive use of the well known theorem ([11]):

Theorem 2.1. *For all quadratic forms Q we have*

$$d(Q)^2 \le \prod_{i=1}^{l} M_i(Q) \le \gamma_l^l d(Q)^2.$$

3. The unit lattice

By the Dirichlet unit theorem, the unit group $O^\times$ of any order O in F is of the form

$$O^\times = \langle\zeta\rangle \times \langle E_1\rangle \times \cdots \times \langle E_r\rangle \cong C_w \times \mathbb{Z}^r,$$

where $r := r_1 + r_2 - 1$ is the unit rank and ζ is a primitive wth root of unity and generates the torsion subgroup. Any system of generators $E_1, \ldots, E_r$ of the infinite part is called system of fundamental units.

As usual, the logarithmic map is used to transfer the multiplicative property of dependence/independence of units to the more familiar linear (in)dependency of real vectors:

$$L : O^\times \to \mathbb{R}^{r+1} : \varepsilon \mapsto (c_i \log|\varepsilon^{(i)}|)_{1\le i\le r_1+r_2},$$

where the weights c_i are chosen according to the infinite places: $c_i := 1$ for $1 \le i \le r_1$ and $c_i := 2$, otherwise.

We have the following well known results ([11]).

Theorem 3.1. *The units $\varepsilon_1, \dots, \varepsilon_l$ are multiplicatively independent if and only if $L(\varepsilon_1), \dots, L(\varepsilon_l)$ are $\mathbb{R}$-linearly independent.*

Theorem 3.2. *The image $L(O^\times)$ is a lattice of rank r in $\mathbb{R}^{r+1}$. The (normalized) volume of a fundamental domain of $L(O^\times)$ is called the regulator R_O of O.*

So, in principle, testing dependency of units is reduced to a problem in real linear algebra. However, the decision whether an integral linear combination of vectors of logarithms of units is indeed zero is highly nontrivial! A sincere discussion of this problem is not yet contained in the literature. For example, the MLLL algorithm yields a certificate for the dependency of units (i.e., it will find an integral relation which can be verified algebraically), but it cannot prove their independence.

So far, the independence of units is reduced to the independence of the corresponding real logarithm vectors, which is a difficult problem in numerical analysis and the results are usually not guaranteed.

In the following we develop a method for proving the independence of units. For this we will need a lower bound on the length of nonzero elements in the unit lattice. To get such an estimate we use the following result in [7, Theorem 2.2], [4].

Theorem 3.3. *Let F be a number field of degree $d > 1$ over $\mathbb{Q}$ and α an algebraic integer. Then either α is a torsion unit or there is at least one conjugate i such that*

$$|\alpha^{(i)}| > 1 + \frac{1}{6}\frac{\log d}{d^2}.$$

For totally real fields we can follow the proof in [12] to improve this

Corollary 3.4. *Let α be a integral number in a totally real field. Then either α is of the form $\cos q\pi$ ($q \in \mathbb{Q}$) or there is at least one conjugate i such that*

$$|\alpha^{(i)}| > 2 + \frac{1}{1152}\frac{\log^2 2d}{d^4}.$$

Proof. By [12] or [6] we know that either α is of the form $\cos q\pi$ for some $q \in \mathbb{Q}$ or there is at least one conjugate $|\alpha^{(i)}| > 2$. Let $K := F(\beta)$, where β is a root of $x^2 - x\alpha + 1 = 0$. Since for the ith conjugate we see that the discriminant $(\alpha^{(i)}/2)^2 - 1$ is positive, not all conjugates of β can be complex. Hence β is not a root of unity. Therefore by Theorem 3.3 there is a conjugate $\beta^{(j)}$ of β such that $|\beta^{(j)}| > 1 + \frac{1}{6}\frac{\log 2d}{(2d)^2}$. Let $\bar{j}$ be such that $\beta^{(j)}$ is a root of $x^2 - \alpha^{(\bar{j})}x + 1$. Then

$$\alpha^{(\bar{j})} = \beta^{(j)} + \bar{\beta}^{(j)} = \beta^{(j)} + \frac{1}{\beta^{(j)}}$$

since $\beta\bar{\beta} = 1$. Thus

$$\begin{aligned} |\alpha^{(i)}| &\geq 1 + \frac{1}{6}\frac{\log 2d}{(2d)^2} + \frac{1}{1 + \frac{1}{6}\frac{\log 2d}{(2d)^2}} \\ &\geq 2 + \frac{1}{2}(\frac{1}{6}\frac{\log 2d}{(2d)^2})^2 = 2 + \frac{1}{72}\frac{\log^2 2d}{(2d)^4} \end{aligned}$$

(using $\frac{1}{1+x} \geq 1 - x + \frac{1}{2}x^2$). □

Applying Theorem 3.3 to the unit group we immediately get

Corollary 3.5. *Let ϵ be a unit in a number field F of degree $d > 1$. Then either ϵ is a torsion unit or*

$$\|L(\epsilon)\|_2 > \frac{21}{128}\frac{\log d}{d^2}.$$

Proof. For $1 > x > 0$ we have $\log(1+x) > x - 1/2x^2$ so that for i as in Theorem 3.3 we get for any nontorsion unit ϵ,

$$\begin{aligned}\log|\epsilon^{(i)}| &> \log(1+\frac{1}{6}\frac{\log d}{d^2}) > \frac{1}{6}\frac{\log d}{d^2} - \frac{1}{2}\frac{1}{36}\frac{\log^2 d}{d^4}\\ &= \frac{1}{6}\frac{\log d}{d^2}(1 - \frac{1}{2}\frac{1}{6}\frac{\log d}{d^2})\\ &\geq \frac{1}{6}\frac{63}{64}\frac{\log d}{d^2},\end{aligned}$$

since for $d \geq 2$ the function $d^{-2}\log d$ is decreasing and $\log 2 < 3/4$. □

We note that the lower bound approaches 0 as the field degree grows to infinity so that the bound can be improved if we know that all units belong to a (totally real) subfield of F of small degree.

4. Deciding dependency

In [9], the following algorithm is given to decompose a positive definite quadratic form $Q(\mathbf{x}) = \mathbf{x}^{\mathrm{tr}}B\mathbf{x}$ as $Q(x_1,\dots,x_l) = \sum_{i=1}^{l} q_{i,i}(x_i + \sum_{j=i+1}^{l} q_{i,j}x_j)^2$:

Algorithm 4.1 (Quadratic supplement)**.**

Input: *A positive semi-definite matrix $B \in \mathbb{R}^{l\times l}$ of rank $\geq l-1$.*
Output: *A matrix Q and a permutation $\pi \in S_l$ such that*

$$\mathbf{x}^{\mathrm{tr}}B\mathbf{x} = Q(\mathbf{x}) = \sum_{i=1}^{l} q_{i,i}(x_{\pi(i)} + \sum_{j=i+1}^{l} q_{i,j}x_{\pi(j)})^2 \tag{4.1}$$

and $q_{1,1} \geq q_{2,2} \geq \cdots \geq q_{l,l}$.
Initialization: *Set $Q := B$ and $\pi := \mathrm{Id}_{S_l}$, the identity permutation.*
Main loop: *For $i = 1,\dots,l-1$ do*
Pivot: *Find $i \leq i_0 \leq l$ such that $q_{i_0,i_0} = \max_{j\geq i} q_{j,j}$.*
Swap: *Set $\pi := \pi\cdot(i,i_0)$ and swap the ith and i_0th row and column in the lower right minor starting at (i,i), also for $k \neq l$ set $q_{l,k} := q_{k,l}$.*
Divide: *For $j = i+1,\dots,l$ set $q_{j,i} := q_{i,j}$ and $q_{i,j} := q_{i,j}/q_{i,i}$*
Add multiple of row: *For $k = i+1,\dots,l$ and for $l := k,\dots,l$ set $q_{k,l} := q_{k,l} - q_{k,i}q_{i,l}$*
End for: *return Q and π.*

Proof. In each step of the main loop, the algorithm only operates on the lower right minor starting at (i,i) and performs a quadratic supplement on the corresponding quadratic form. □

We note that the pivot and swap steps are only neccessary to get error estimates [9, 5]:

Theorem 4.2. *If we replace* $Q(\mathbf{x}) = \mathbf{x}^{\mathrm{tr}} B\mathbf{x}$ *by* $\tilde{Q}(\mathbf{x}) = \mathbf{x}^{\mathrm{tr}}(B+\Delta)\mathbf{x}$ *for some matrix* $\Delta \in \mathbb{R}^{l\times l}$ *and if* $q_{i,i} \geq 1$ *for* $1 \leq i < l$*, then Algorithm* 4.1 *will compute*

$$\tilde{Q}(x_1,\dots,x_l) = \sum_{i=1}^{l} \tilde{q}_{i,i}(x_{\pi(i)} + \sum_{j=i+1}^{l} \tilde{q}_{i,j} x_{\pi(j)})^2 \tag{4.2}$$

with $|\tilde{q}_{i,j} - q_{i,j}| \leq 4^{l-1}\|\Delta\|_\infty$.

Since the rank of B is at least $l-1$, the condition on the size of the $q_{i,i}$ can easily be achieved by replacing B by λB for some $\lambda > 1$.

Together with the lower bound on the conjugates, the following lemma together with Theorem 4.2 will give us a test for dependency.

Lemma 4.3. *Let* Q *be a positive definite quadratic form and let* $q_{i,j}$ *be the decomposition as computed by Algorithm* 4.1*. Then we get*

$$d(Q)^2 = \prod_{i=1}^{r} q_{i,i}$$

for the discriminant $d(Q)$ *of the lattice with quadratic form* Q*.*

Combining the last lemma with Algorithm 4.1 we can decide whether a given system $\epsilon_1,\dots,\epsilon_l$ $(2 \leq l \leq r)$ is multiplicatively independent.

Algorithm 4.4 (Dependency test)**.**

Input: *Units* ϵ_i $(1 \leq i \leq l)$ *containing at least* $l-1$ *independent units, and the field degree* d*.*

Output: `true` *if the units are multiplicatively independent;* `false`*, otherwise.*

s: *Compute an upper bound* s *for* $\|L(\epsilon_i)\|_\infty$ $(1 \leq i \leq l)$*.*

δ: *Set* $\delta := \gamma_l^{-l}(\frac{21}{128}\frac{\log d}{d^2})^l$

Log Matrix: *Compute* $\tilde{A} := (L(\epsilon_1),\dots,L(\epsilon_l)) + \Delta$ *with*

$$\|\Delta\|_\infty \leq \frac{1}{3ns}\frac{\delta}{l(1+s)^{l-1}2^{2l-1}}.$$

Quadratic Form: *Use classical matrix multiplication to compute* $\tilde{B} := \tilde{A}^{\mathrm{tr}}\tilde{A}$*.*

Cholesky: *Use Algorithm* 4.1 *to compute* $\tilde{Q} = (\tilde{q}_{i,j})$ *as in* (4.2)*.*

Finish: *If* $\prod_{i=1}^{l} \tilde{q}_{i,i} < \delta/2$*, then return* `false`*; otherwise, return* `true`*.*

Proof. We have to justify that the numerical errors are small enough throughout the algorithm. At the beginning we have

$$\tilde{B} = (A+\Delta)^{\mathrm{tr}}(A+\Delta) = A^{\mathrm{tr}}A + \Delta^{\mathrm{tr}}A + A\Delta^{\mathrm{tr}} + \Delta^{\mathrm{tr}}\Delta.$$

Assuming $\|A\|_\infty \geq \|\Delta\|_\infty$ and using classical matrix multiplication, we immediately see

$$\|B - \tilde{B}\|_\infty \leq 3n\|A\|_\infty\|\Delta\|_\infty \leq 3ns\|\Delta\|_\infty \leq \frac{\delta}{l(1+s)^{l-i}2^{2l-1}}.$$

An application of Algorithm 4.1 computes $\tilde{q}_{i,j}$ with an absolute error

$$|q_{i,j} - \tilde{q}_{i,j}| \leq 4^{l-1}\frac{\delta}{l(1+s)^{l-1}2^{2l-1}} = \frac{\delta}{2l(1+s)^{l-1}}.$$

Suppose now that all the units are multiplicatively independent. In that case, the matrix $A := (L(\epsilon_1),\dots,L(\epsilon_l))$ will be of full rank so that $Q(\mathbf{x}) := \mathbf{x}^{\mathrm{tr}}A^{\mathrm{tr}}A\mathbf{x}$ is

a positive definite quadratic form. Application of Algorithm 4.1 to Q while fixing the same permutation π as obtained for $\tilde{Q}$, we get

$$d(Q) = \prod_{i=1}^{l} q_{i,i}.$$

Theorem 2.1 applied to Q gives

$$d(Q)^2 \leq \prod_{i=1}^{l} M_i(Q) \leq \gamma_l^l d(Q)^2.$$

Now, Corollary 3.5 shows $M_1(Q) \geq \frac{21}{128}\frac{\log d}{d^2}$ and thus

$$\delta = \gamma_l^{-l}(\frac{21}{128}\frac{\log d}{d^2})^l \leq \gamma_l^{-l} M_1(Q)^l \leq \gamma_l^{-l} \prod_{i=1}^{l} M_i(Q) \leq d(Q)^2. \tag{4.3}$$

Therefore, if the units are independent we obtain $d(Q)^2 \geq \delta$; otherwise, we get $d(Q) = 0$. Since $\prod_{i=1}^{l} \tilde{q}_{i,i}$ is an approximation to $d(Q)^2$, all we have to do is to estimate the error in the product:

$$\begin{aligned} |\prod_{i=1}^{l} \tilde{q}_{i,i} - d(Q)^2| &= |\prod_{i=1}^{l}(q_{i,i} + \varepsilon_i) - \prod_{i=1}^{l} q_{i,i}| \\ &\leq \sum_{i=1}^{l} \binom{l}{i} \|\varepsilon\|_\infty^i s^{l-i} \leq \|\varepsilon\|_\infty l(1+s)^{l-1} \\ &\leq \frac{\delta}{2l(1+s)^{l-1}}(1+s)^{l-1} \leq \frac{\delta}{2} \end{aligned}$$

(using $\|\varepsilon\|_\infty \leq 1$ and $q_{i,i} \leq s$).

Hence, $d(Q) = 0$ exactly when $\prod_{i=1}^{l} \tilde{q}_{i,i} < \delta/2$. □

Up to now we have not been explicit on step **Log Matrix** as it depends on the representation of the units. In applications, the following two representations are equally frequent:

- The units are given with respect to a fixed basis of the number field. In this case, using standard techniques for the computation of zeros of the defining polynomial of the number field, it is easy to get error estimates for the conjugates of each unit and thus for the logarithms (assuming no loss of relative precision in the computation of logarithms).
- The other representation that occurs frequently during computations is the so called product representation or compact representation. Here the units are given as a formal product of "small" algebraic integers, possibly with large exponents. In this situation, the procedure outlined above will give the logarithms of the "factor base" to any precision required. The logarithms of the units are then obtained simply as linear combinations—with obvious precision control.

Remark 4.5. (1) Algorithm 4.4 together with classical methods to test for dependencies (MLLL) can already be used to get proven results: After the dependency of the system of units is established with Algorithm 4.4 the MLLL procedure is performed with increasing precision until the dependency is detected.

(2) If $l = r - 1$, that is if a maximal set of independent units is already known, better bounds that are based on lower estimates for the regulator can be used [11, p. 366].

5. Finding dependencies

In this section, we give an alternative to the real MLLL to find dependencies between units. It is based on Belabas' [1] notion of lattice reduction: Suppose $A \in \mathbb{R}^{l\times l}$ is of full rank. Then there is some positive number μ such that $\lceil \mu A \rfloor$ is also of full rank where $\lceil \mu A \rfloor \in \mathbb{Z}^{l\times l}$ is the matrix obtained by rounding each entry to the nearest integer: $\lceil x \rfloor := \lfloor x + 1/2 \rfloor$. By applying an integral LLL reduction on the basis of the lattice spanned by $\lceil \mu A \rfloor$, we obtain an approximation to the real LLL reduction of A. Of course, the quality of the reduction, i.e., the distance from the true LLL reduction, depends on μ.

We start by collecting results on scaled matrices μA:

Lemma 5.1. *Let $\mu > 0$ and set $(\mu Q) := \mu^2 A^{\mathrm{tr}} A$. Then*

(1) $(\mu Q)(\mathbf{x}) = \sum_{i=1}^{l} \mu^2 q_{i,i}(x_i + \sum_{j=1+i}^{l} x_j q_{i,j})^2$.

(2) *If the rank of A is l, then the lattice with the quadratic form (μQ) has discriminant*

$$d(\mu Q)^2 = \mu^{2l} \prod_{i=1}^{l} q_{i,i}.$$

In order to avoid rounding errors in the subsequent LLL computations, we would like to work with exact forms over the integers rather than over the reals. Unfortunately, rounding a positive definite symmetric matrix will in general not produce a positive definite one. However, we have the following lemma.

Lemma 5.2. *Let $Q \in \mathbb{R}^{l\times l}$ be a positive definite symmetric matrix. Then for all $\lambda > l/2$,*

$$\lceil Q \rfloor + \lambda I_l$$

is positive definite.

Proof. As usual, we write $\lceil Q \rfloor = Q + \Delta$ with $\Delta \in [-1/2, 1/2]^{l\times l}$. Then $\mathbf{x}^{\mathrm{tr}} \lceil Q \rfloor \mathbf{x} = \mathbf{x}^{\mathrm{tr}} Q \mathbf{x} + \mathbf{x}^{\mathrm{tr}} \Delta \mathbf{x}$. We now conclude that

$$\begin{aligned} |\mathbf{x}^{\mathrm{tr}} \Delta \mathbf{x}| &\leq \|\mathbf{x}\|_2 \|\Delta \mathbf{x}\|_2 = \|\mathbf{x}\|_2 \sqrt{\sum_{i=1}^{l} (\sum_{j=1}^{l} \Delta_{i,j} x_j)^2} \\ &\leq \|\mathbf{x}\|_2 \sqrt{\sum_{i=1}^{l} (\|(\Delta_{i,j})_{1\leq j\leq l}\|_2 \|\mathbf{x}\|_2)^2} \leq \|\mathbf{x}\|_2^2 l/2. \end{aligned} \tag{5.1}$$

Therefore, for $\lambda > l/2$, we see that $\lceil Q \rfloor + \lambda I_l$ is positive definite. □

In what follows $A = (L(\epsilon_1), \ldots, L(\epsilon_l))$ is the exact real matrix containing the logarithm vectors of the units. We know that the units are dependent, in fact we assume that the rank of A is $l - 1$ and that there is some $\mathbf{0} \neq \mathbf{z} \in \mathbb{Z}^l$ such that $A\mathbf{z} = \mathbf{0}$ or, equivalently, $Q(\mathbf{z}) = \mathbf{z}^{\mathrm{tr}} A^{\mathrm{tr}} A \mathbf{z} = 0$.

Let us denote by $\lceil \mu Q \rfloor$ the integral quadratic form defined by

$$\lceil \mu Q \rfloor := \lceil \mu^2 A^{\mathrm{tr}} A \rfloor + \lceil l/2 \rceil I_l.$$

We then get

Lemma 5.3. (1) $\lceil \mu Q \rfloor(\mathbf{x}) \le (2l+1)/2 \|\mathbf{x}\|_2^2$ *for any* $\mathbf{x} \in \mathbb{Z}^l$ *such that* $A\mathbf{x} = 0$.
(2) $d(\lceil \mu Q \rfloor)^2 \le (2+l)2^{2l-3}\mu^{2l-2}\prod_{i=1}^{l-1} q_{i,i} + O(\mu^{2l-4})$ *for* $\mu \to \infty$.
(3) *For any* $\mathbf{x} \in \mathbb{Z}^l$ *such that* $A\mathbf{x} \neq 0$, *we get*

$$\lceil \mu Q \rfloor(\mathbf{x}) \ge \mu^2 (\frac{21}{128})^2 \frac{\log^2 d}{d^4} - O(1)$$

for $\mu \to \infty$.

Thus, if μ *is large enough, the first basis vector* $\mathbf{z}$ *of a LLL reduced basis will be the shortest vector in the lattice with scalar product induced by* $\lceil \mu Q \rfloor$.

Proof. We write $\lceil \mu^2 A^{\mathrm{tr}} A \rfloor = \mu^2 A^{\mathrm{tr}} A + \Delta$, where $\|\Delta\|_\infty \le 1/2$, depending on μ. This, together with (5.1) immediately yields

$$\lceil \mu Q \rfloor(\mathbf{z}) = (\mu Q)(\mathbf{z}) + \mathbf{z}^{\mathrm{tr}} In \Delta \mathbf{z} + \|\mathbf{z}\|_2^2 \lceil l/2 \rceil \le (2l+1)/2 \|\mathbf{z}\|_2^2,$$

as required.

Applying Algorithm 4.1 to $\lceil \mu Q \rfloor$ gives for $\mathbf{x}$ such that $A\mathbf{x} = 0$

$$\lceil \mu Q \rfloor(\mathbf{x}) = \sum_{i=1}^{l} \tilde{q}_{i,i}(x_i + \sum_{j=i+1}^{l} x_j \tilde{q}_{i,j})^2$$

with

$$|\tilde{q}_{i,i} - \mu^2 q_{i,i}| =: |\delta_i| \le 4^{l-1} \frac{l+2}{2} = 2^{2l-3}(l+2)$$

for the diagonal entries and

$$|\tilde{q}_{i,j} - q_{i,j}| \le 4^{l-1} \frac{l+2}{2} = 2^{2l-3}(l+2)$$

for all the others. For the discriminant, we therefore get

$$d(\lceil \mu Q \rfloor)^2 = \prod_{i=1}^{l} (\mu^2 q_{i,i} + \delta_i) = \mu^{2l} \prod_{i=1}^{l} q_{i,i} + \mu^{2l-2} \delta_l \prod_{i=1}^{l-1} q_{i,i} + O(\mu^{2l-4})$$

as the error terms are uniformly bounded independently of μ. Since A is singular by assumption, $q_{l,l} = 0$.

If $A\mathbf{x} \neq 0$, then $\prod_{i=1}^{l} \epsilon_i^{x_i} =: \epsilon$ is a nontorsion unit, so by Corollary 3.5 we have

$$Q(\mathbf{x}) = \|L(\epsilon)\|_2^2 > (\frac{21}{128})^2 \frac{\log^2 d}{d^4}.$$

Therefore, $\lceil \mu Q \rfloor(\mathbf{x}) = (\mu Q)(\mathbf{x}) + \mathbf{x}^{\mathrm{tr}} \Delta \mathbf{x} \ge \mu^2 (\frac{21}{128})^2 \frac{\log^2 d}{d^4} - \frac{2l+1}{2} \|\mathbf{x}\|_2^2$. □

Minkowski's Theorem 2.1 on successive minima now gives:

Theorem 5.4.

$$M_1(\lceil \mu Q \rfloor) \le \gamma_l^l (2+l)((\frac{128}{21})^2 \frac{d^4}{\log^2 d})^{l-1} 2^{2l-3} \prod_{i=1}^{l-1} q_{i,i}$$

for all sufficiently large μ.

Proof. Minkowski's theorem on successive minima states

$$M_1(\lceil \mu Q \rfloor) M_2(\lceil \mu Q \rfloor)^{l-1} \le \prod_{i=1}^{l} M_i(\lceil \mu Q \rfloor) \le \gamma_l^l d(\lceil \mu Q \rfloor)^2,$$

and thus $M_1(\lceil \mu Q \rfloor) \le M_2(\lceil \mu Q \rfloor)^{1-l}\gamma_l^l d(\lceil \mu Q \rfloor)^2$. Using Lemma 5.3, we see that for $\mu \to \infty$ we get

$$M_1(\lceil \mu Q \rfloor) \le \gamma_l^l (2+l)((\frac{128}{21})^2 \frac{d^4}{\log^2 d})^{l-1} 2^{2l-3} \prod_{i=1}^{l-1} q_{i,i}.$$

Since the right hand side is independent of μ, the theorem is proved. □

Therefore, if we choose μ such that

$$M_1(\lceil \mu Q \rfloor) 2^l \le \gamma_l^l (2+l)((\frac{128}{21})^2 \frac{d^4}{\log^2 d})^{l-1} 2^{3l-3} \prod_{i=1}^{l-1} q_{i,i} < \mu^2 (\frac{21}{128})^2 \frac{\log^2 d}{d^4},$$

the LLL reduction on $\lceil \mu Q \rfloor$ will find $\mathbf{z}$ corresponding to the first basis vector.

6. Easy independencies

An easy way for recognizing the independence of few units (with respect to the unit rank r) is based on the fact that nontorsion units have conjugates which are larger than one and others which are smaller than one in absolute value.

We assume that we are given $k < r$ independent units $\varepsilon_1, \dots, \varepsilon_k$ and that we want to test whether the unit ε_{k+1} is independent of those. We assume that the logarithmic vectors $L(\varepsilon_i)$ $(1 \le i \le k+1)$ are also given with sufficient precision such that row echelon form $A = (a_{ij}) \in \mathbb{R}^{k \times r}$ of the matrix with rows $L(\varepsilon_i)$ $(1 \le i \le k)$ could be computed satisfying

$$a_{ii} > 0 \ \ (1 \le i \le k), \ \ a_{ij} = 0 \ \ (1 \le i, j \le k, \ i \ne j).$$

For this, we note that any of these units can be replaced by its multiplicative inverse, and that we can change the order of the conjugates. For error estimates we refer to the usual methods from numerical analysis [13]. If we insert $(b_1, \dots, b_{r+1}) := L(\varepsilon_{k+1})$ as $(k+1)$-st row of A, Gaussian elimination turning b_j into 0 for $1 \le j \le k$ yields the new diagonal element

$$a_{k+1,k+1} = b_{k+1} - \sum_{i=1}^{k} b_i \frac{a_{i,k+1}}{a_{ii}}.$$

This is guaranteed to be nonzero (and therefore the new unit independent of the previous ones) if we can achieve by a suitable arrangement of the conjugates that

(1) $b_{k+1} \ne 0$, and
(2) $-\operatorname{sign}(b_{k+1}) = \operatorname{sign}(b_i a_{i,k+1})$ for all indices $i \in \{1, \dots, k\}$ for which the product $b_i a_{i,k+1}$ is nonzero.

This procedure is usually efficient if the number k is small with respect to r.

7. An upper bound

If we are just interested in a (rough) upper bound for the absolute values of the entries of a relation vector $\mathbf{z} \in \mathbb{Z}^l$ for the columns $\mathbf{a}_1, \dots, \mathbf{a}_l$ of a matrix $A \in \mathbb{R}^{m \times l}$ of rank $l-1$ we can proceed as follows. We note that we must assume that those columns belong to a lattice Λ in $\mathbb{R}^m$ for which we know a lower bound $C > 0$ for the Euclidean norm of a shortest vector of Λ. This properties are certainly satisfied for the vectors of logarithms of units. Also, we note that it suffices to consider vectors with $l-1$ coordinates appropriately chosen from the m original coordinates. The

relation $m = l - 1$ will be of importance later on. (A somewhat worse estimate in a special case of this is already contained in [10].)

To obtain such a bound, we introduce a much larger lattice $\bar{\Lambda}$ in $\mathbb{R}^{l+m}$ with basis vectors

$$\bar{\mathbf{a}}_i := \begin{cases} \begin{pmatrix} \mathbf{e}_i \\ 2^\lambda \mathbf{a}_i \end{pmatrix} & (1 \le i \le l), \\ 4^\lambda \bar{\mathbf{e}}_i & (l+1 \le i \le l+m). \end{cases}$$

(Here $\mathbf{e}_i$ and $\bar{\mathbf{e}}_i$ denote the ith unit vector in $\mathbb{R}^l$, repectively $\mathbb{R}^{l+m}$, and λ is a positive constant to be specified later.) Clearly, the lattice $\bar{\Lambda}$ is of rank $l+m$ and has determinant $D := 4^{\lambda m}$. Therefore, the first basis vector, say $\bar{\mathbf{a}}$ of a LLL-reduced basis of $\bar{\Lambda}$ satisfies

$$\|\bar{\mathbf{a}}\|_2 \le 2^{(l+m-1)/4} D^{1/(l+m)} =: U_1. \tag{7.1}$$

If $\bar{\mathbf{a}}$ is even a shortest vector of $\bar{\Lambda}$ we get the much better estimate

$$\|\bar{\mathbf{a}}\|_2 \le \sqrt{\gamma_{l+m}} D^{1/(l+m)} =: V_1 \tag{7.2}$$

in which γ_{l+m} again denotes Hermite's constant. Besides λ introduced above we need a second constant $\varepsilon > 0$. For these two constants we now require that they satisfy

$$U_1 \le 2^\lambda \varepsilon, \tag{7.3}$$

$$\bar{\mathbf{a}} = \sum_{j=1}^{l} m_j \bar{\mathbf{a}}_j \quad \text{with } m_j \in \mathbb{Z}, \text{ i.e., } m_j = 0 \text{ for } j > l. \tag{7.4}$$

$$\varepsilon < C. \tag{7.5}$$

The first condition will be used to guarantee that in the representation of

$$\bar{\mathbf{a}} = \sum_{i=1}^{l+m} m_i \bar{\mathbf{a}}_i$$

of $\bar{\mathbf{a}}$ by the basis vectors of $\bar{\Lambda}$ the coefficients of the last m basis vectors are 0.

To satisfy condition (7.3), we choose λ (in dependence of ε) subject to $U_1 = 2^\lambda \varepsilon$. This is tantamount to

$$\lambda = \frac{l+m}{l-m} \left(\frac{l+m-1}{4} - \frac{\log \varepsilon}{\log 2} \right). \tag{7.6}$$

Choosing λ in this way we know that $\|\bar{\mathbf{a}}\| \le 2^\lambda \varepsilon$. We write $\bar{\mathbf{a}} = \bar{\mathbf{b}}_1 + \bar{\mathbf{b}}_2$ with

$$\bar{\mathbf{b}}_1 = \sum_{i=1}^{l} m_i \bar{\mathbf{a}}_i, \qquad \bar{\mathbf{b}}_2 = \sum_{i=l+1}^{l+m} m_i \bar{\mathbf{a}}_i.$$

We recall that

$$\|\bar{\mathbf{b}}_1\|_2^2 = \sum_{i=1}^{l} m_i^2 + 4^\lambda \| \sum_{i=1}^{l} m_i \mathbf{a}_i \|_2^2 \le U_1^2$$

and therefore

$$\sum_{i=1}^{l} m_i^2 \le 4^\lambda \varepsilon^2. \tag{7.7}$$

Let s denote an upper bound for the Euclidean norms of the vectors $\mathbf{a}_i$ ($1 \leq i \leq l$). So, if we assume that $\bar{\mathbf{b}}_2$ has at least one nonzero coordinate we have the following estimates which will eventually yield a contradiction:

$$\begin{aligned} 2^\lambda \varepsilon &\geq \|\bar{\mathbf{a}}\|_2 \geq \|\bar{\mathbf{b}}_2\|_2 - \|\bar{\mathbf{b}}_1\|_2 \\ &\geq 4^\lambda - \|2^\lambda \sum_{i=1}^{l} m_i \mathbf{a}_i\|_2. \end{aligned} \tag{7.8}$$

To estimate $\|\sum_{i=1}^{l} m_i \mathbf{a}_i\|_2^2$ requires more work: Let $\|A\|_{2,\infty}$ the norm of A as a linear operator from the $\mathbb{R}^l$ with the $\|.\|_2$-norm to $\mathbb{R}^m$ with the $\|.\|_\infty$-norm. Then we have

$$\|\sum_{i=1}^{l} m_i \mathbf{a}_i\|_\infty = \|A\mathbf{m}\|_\infty \leq \|A\|_{2,\infty} \|\mathbf{m}\|_2.$$

We can compute $\|A\|_{2,\infty}$ as $\max_{i=1}^{l} \|\mathbf{a}_i\|_2$ and further estimate $\|.\|_\infty \leq \sqrt{m}\|.\|_2$ to finally get

$$\|\sum_{i=1}^{l} m_i \mathbf{a}_i\|_2 \leq \sqrt{m} s \|\mathbf{m}\|_2. \tag{7.9}$$

Combining this with (7.8) and (7.7) we see

$$2^\lambda \varepsilon \geq 4^\lambda - \sqrt{m} s 2^\lambda \|\mathbf{m}\|_2 \geq 4^\lambda - \sqrt{m} s \varepsilon 4^\lambda. \tag{7.10}$$

If we then choose ε small enough we get a contradiction, so $\mathbf{b}_2 = 0$ as claimed. In particular it suffices to choose ε as

$$\varepsilon < \frac{1}{1 + s\sqrt{m}} \leq \frac{1}{2^{-\lambda} + s\sqrt{m}}. \tag{7.11}$$

In practice, it usually suffices to choose $\varepsilon < C$ satisfying (7.11) and then determine λ according to (7.6).

Proposition 7.1. *Choosing ε and λ as described yields a presentation of $\mathbf{0}$ by the $\mathbf{a}_i$ for which the coefficient vector has a Euclidean norm bounded by $2^\lambda \varepsilon$.*

8. Example

All the algorithms developed in this article have been implemented in Magma [2]. The program code as well as electronic versions of the input used can be obtained from the first author.

We consider the following example that constitutes part of a computation related to class fields. Starting with the cyclic cubic field $k := Q(\alpha)$, where α is a root of $x^3 + x^2 - 292x + 1819$ with discriminant 769129 and class number 7, we use $K := k(\zeta_7)$ which is an abelian CM-field of degree 18 over $\mathbb{Q}$. During a (conditional) class group computation using a factor basis containing prime ideals of norm < 1000 a total of 331 relations were found. The analysis of the relation matrix found 105 units which are all given as power products of the 331 original relations (algebraic integers). We used our algorithms to compute a (multiplicative) basis for the free group generated by the 105 units: Starting with an empty set, we checked for each new unit if it is dependent on the already computed basis. If the unit is dependent, we used the integral LLL techniques to find the dependency and to compute a basis for the new subgroup. If the new unit proved to be independent, we simply add it to the list. The largest relation found had a 2-norm of size 10^{52}, while the largest

precision used was 10^{-245}. The total running time was easily dominated by the computations of the logarithms of the relations. On average, the size of the first basis vector was over estimated by a factor of 10^{70} which means that the precision was (probably) over estimated by a factor of 2.

9. Conclusions

We demonstrated that our new approach to reliably detect and compute dependencies between units works well in practice and the precision bounds obtained are not too large to be useful. On the other hand, realistic a priori bounds on the precision are still missing.

The worst results are obtained when the whole unit group is already known. In this case, the estimate predicts a relation of the size of the smallest sublattice while in practice the relation is usually very small.

References

1. Karim Belabas, *Topics in computational algebraic number theory*, J. Theor. Nombres Bordeaux, **16** (2004), 19–63. MR2145572 (2006a:11174)
2. John J. Cannon, *MAGMA*, http://magma.maths.usyd.edu.au, 2003.
3. Henri Cohen, *A course in computational algebraic number theory*, erste ed., Graduate Texts in Mathematics, vol. 138, Springer, 1993. MR1228206 (94i:11105)
4. Edward Dobrowolski, *On the maximal modulus of conjugates of an algebraic integer*, Bul. Acad. Pol. Sci. **26** (1978), no. 4, 291–292. MR0491585 (58:10811)
5. Nicholas J. Higham, *Analysis of the Cholesky decomposition of a semi-definite matrix.*, Reliable numerical computation, Proc. Conf. in Honour of J. H. Wilkinson, Teddington/UK, 161-185 , 1990. MR1098323 (92c:65036)
6. L. Kronecker, *Zwei Sätze über Gleichungen mit ganzahlingen Coeffizienten*, J. Reine Angew. Math **53** (1857), 173–175.
7. Władisław Narkiewicz, *Elementary and analytic theory of algebraic numbers*, 2nd ed., Springer, 1989. MR2078267 (2005c:11131)
8. Michael E. Pohst, *A modification of the LLL reduction algorithm*, J. Symb. Comput. **4** (1987), 123–127. MR0908420 (89c:11183)
9. Michael E. Pohst, *On computing isomorphisms of equation orders*, Math.Comp. **48** (1987), no. 177. MR0908420 (89c:11183)
10. Michael E. Pohst, *Computational algebraic number theory*, DMV Seminar. 21. Basel: Birkhäuser, 1993. MR1243639 (94j:11132)
11. Michael E. Pohst and Hans Zassenhaus, *Algorithmic algebraic number theory*, Encyclopaedia of mathematics and its applications, Cambridge University Press, 1989. MR1033013 (92b:11074)
12. Andrzej Schinzel and Hans Zassenhaus, *A refinement of two theorems of Kronecker*, Mich. Math. J. **12** (1965), 81–85. MR0175882 (31:158)
13. J. Stoer and R. Bulirsch, *Introduction to numerical analysis. Transl. from the German by R. Bartels, W. Gautschi, and C. Witzgall. 3rd ed.*, Texts in Applied Mathematics. 12. New York, NY: Springer., 2002 (English). MR1923481 (2003d:65001)

School of Mathematics and Statistics, University of Sydney, NSW 2006, Australia.
E-mail address: claus@maths.usyd.edu.au

Institut für Mathematik, Technische Universität Berlin, Strasse des 17. Juni 136, 10623 Berlin, Germany.
E-mail address: pohst@math.TU-Berlin.DE