A Practical Version of the Generalized Lagrange Algorithm

Johannes Buchmann, Max Jüntgen and Michael Pohst

CONTENTS

We describe an implementation of the generalized Lagrange algorithm for computing units in algebraic number fields [Buchmann 1987a], together with extensive experimental data of the algorithm's application (to all totally real quartic fields of discriminant below 60000). We also present an improved algorithm, with related experimental data.

1. INTRODUCTION

The computation of units in number fields is one of the most important and most difficult tasks in computational algebraic number theory. In recent years many new methods for this purpose have been proposed, such as the ones in [Buchmann and Pethő 1989; Fincke and Pohst 1985].

In this paper we describe an implementation of the generalized Lagrange algorithm (GLA) for computing the unit group $\mathcal{O}^*$ of an order $\mathcal{O}$ of an algebraic number field F of arbitrary degree n. The GLA works by enumerating the connected graph of reduced ideals of $\mathcal{O}$. It was introduced in [Buchmann 1987a], where complexity results were proved but nothing was said about performance in practice.

In Section 2 we describe the implementation of the original GLA, which yields a finite generating system for $\mathcal{O}^*$. We applied the GLA to all totally real quartic fields of discriminant below 60000. The data obtained from that computation are presented in Section 4.

For unit rank bigger than three, it turns out that the GLA is not efficient. This is because enumerating the complete graph of reduced ideals seems to be far too time-consuming.

1991 Mathematics Subject Classification: 11Y40

Key words and phrases: units, fundamental units, principal ideal test

All authors were supported by the Deutsche Forschungsgemeinschaft.

© A K Peters, Ltd.
1058-6458/96 $0.50 per page

However, if we restrict ourselves to enumerating a suitable subgraph only, a modification of the GLA, called PGLA, turns out to be efficient. The PGLA yields a subgroup of finite index in $\mathcal{O}^*$, not necessarily $\mathcal{O}^*$ itself. So far, we have not been able to prove an upper bound for that index; in practice, however, it seems to always be very small. The PGLA and the corresponding numerical results are presented in Section 3.

2. THE GENERALIZED LAGRANGE ALGORITHM AND ITS IMPLEMENTATION

We fix an algebraic number field F and an order $\mathcal{O}$ of F. Throughout the paper, d and R will denote the discriminant and regulator of $\mathcal{O}$.

Let $\sigma_1, \dots, \sigma_{r_1}$ be the real isomorphisms of F and let $\sigma_{r_1+1}, \overline{\sigma_{r_1+1}}, \dots, \sigma_m, \overline{\sigma_m}$ be the nonreal isomorphisms of F into the field of complex numbers. Denote by $|\ |_1, \dots, |\ |_m$ the normalized archimedean valuations of F: explicitly, for $\xi \in F$ define $|\xi|_i = |\sigma(\xi)|^{e_i}$, where $e_i = 1$ if σ_i is real and $e_i = 2$ otherwise. We assume that σ_1 is the identity map, and so write $|\alpha|$ instead of $|\alpha|_1$ for $\alpha \in F$.

Let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}$. A number $\mu \in \mathfrak{a}$ is called a *minimum* of $\mathfrak{a}$ if 0 is the unique $\alpha \in \mathfrak{a}$ such that $|\alpha|_i < |\mu|_i$ for $1 \le i \le m$. The ideal $\mathfrak{a}$ is called *reduced* if 1 is a minimum in $\mathfrak{a}$. Two minima μ and ν in $\mathfrak{a}$ are called *neighbors* if 0 is the unique $\alpha \in \mathfrak{a}$ such that $|\alpha|_i < \max\{|\mu|_i, |\nu|_i\}$ for all $1 \le i \le m$. Two reduced ideals $\mathfrak{a}$ and $\mathfrak{b}$ are called *neighbors* if $\mu(\mathfrak{a},\mathfrak{b})\mathfrak{b} = \mathfrak{a}$ with μ a neighbor of 1 in $\mathfrak{a}$. Thus the reduced ideals of $\mathcal{O}$ with this neighbor relation form a directed graph, the reduced ideals being the vertices and the edges being in one-to-one correspondence with the elements $\mu(\mathfrak{a},\mathfrak{b})$.

It is proved in [Buchmann 1987a] that the subgraph whose vertices are the reduced ideals in the ideal class of $\mathfrak{a}$ is connected. The set of reduced ideals in the ideal class of $\mathfrak{a}$ is called the *cycle of reduced ideals* in that class. It is finite and its cardinality, called the *period length*, is denoted by $p(\mathfrak{a})$. It was proved in [Buchmann 1987b] that $p(\mathfrak{a}) = O(R)$.

First we present the GLA to construct the graph of reduced ideals for a given ideal class and to compute a basis of $\mathcal{O}^*$. The details are explained below.

Algorithm 2.1 (GLA). Input: A reduced ideal $\mathfrak{a}$.
Output: The cycle C of reduced ideals in the class of $\mathfrak{a}$ and a minimal generating system U for $\mathcal{O}^*$.

- (Initialize) Set $C = \{\mathfrak{a}\}$ and $U = \varnothing$.
- For all $\mathfrak{b} \in C$:
  - Compute the set N of neighbors $\mathfrak{c}$ of $\mathfrak{b}$ with corresponding $\mu(\mathfrak{b},\mathfrak{c})$.
  - For all $\mathfrak{c} \in N$:
    - If $\mathfrak{c} \notin C$, add $\mathfrak{c}$ to C.
    - Else, there is $\mathfrak{c}'$ in C such that $\mathfrak{c} = \mathfrak{c}'$. In that case there is a chain $\mathfrak{c} = \mathfrak{c}_1, \mathfrak{c}_2, \dots, \mathfrak{c}_k = \mathfrak{c}'$ of reduced ideals contained in C such that $\mathfrak{c}_{i+1} = \mu(\mathfrak{c}_{i+1},\mathfrak{c}_i)\mathfrak{c}_i$ for $1 \le i < k$. Because $\mathfrak{c} = \mathfrak{c}'$, the element
    $$\eta = \prod_{i=1}^{k-1} \mu(\mathfrak{c}_{i+1},\mathfrak{c}_i)$$
    is a unit. Replace U by a minimal generating system for $\langle U, \eta\rangle$.

In [Buchmann 1988] it is proved that the complexity of this algorithm is $O(R\,|d|^{\varepsilon})$ for every $\varepsilon > 0$.

Another application of Algorithm 2.1 is testing whether a given ideal $\mathfrak{a}$ is principal. If we know the reduced principal ideals in $\mathcal{O}$ we compute a reduced ideal $\mathfrak{b}$ in the principal cycle of $\mathfrak{a}$ and check whether $\mathfrak{b}$ belongs to the cycle.

In order to find all neighbors of 1 in a reduced ideal we calculate for that ideal all the *minimal sets* containing 1, a concept that we now define. For any finite nonempty $S \subset \mathcal{O}^*$ and $1 \le i \le m$, we set
$$|S|_i = \max\{|\alpha|_i : \alpha \in S\}.$$
We call S a minimal set in $\mathfrak{a}$ if
$$\{\alpha \in \mathfrak{a} : 0 < |\alpha|_i \le |S|_i \text{ for } 1 \le i \le m\} = S$$
and
$$\{\alpha \in \mathfrak{a} : |\alpha|_i < |S|_i \text{ for } 1 \le i \le m\} = \{0\}.$$

Now, given a reduced ideal $\mathfrak{b}$, clearly all elements of a minimal set containing 1 are neighbors of 1, and each neighbor of 1 is contained in such a minimal set. Starting from the minimal set

$$\{\beta \in \mathfrak{b} : |\beta|_i \leq 1 \text{ for } 1 \leq i \leq m\},$$

we can find all the other minimal sets by means of *expansions* and *compressions*. To define these operations, let $S(i)$ be the set of $\alpha \in S$ such that $|\alpha|_i = |S|_i$ and $|\alpha|_j < |S|_j$ for all $1 \leq j \leq m$ with $j \neq i$. For $i \in \{1, \dots, m\}$, the i-th expansion $e_i(S)$ of S is the minimal set S' satisfying $S'(i) = \varnothing$ and

$$|S'|_j = |S|_j \text{ for } 1 \leq j \leq m \text{ and } j \neq i.$$

The i-th compression is

$$k_i(S) = \{\alpha \in S : |\alpha|_i < |S|_i\}.$$

Using expansions and compressions we are able to compute all neighbors of 1 by determining all minimal sets containing 1:

Algorithm 2.2 (Finding all minimal sets containing 1).
Input: The set S' of $\beta \in \mathfrak{b}$ such that $|\beta|_i \leq 1$ for $1 \leq i \leq m$.
Output: The set $\mathcal{S}$ of all minimal sets containing 1.
- (Initialize) Set $\mathcal{S} = \{S'\}$.
- For all $S \in \mathcal{S}$:
  - For all $i = 1, \dots, m$:
    - Set $\mathcal{S} = \mathcal{S} \cup \{e_i(S)\}$.
    - If $1 \in k_i(S)$, set $\mathcal{S} = \mathcal{S} \cup k_i(S)$.

In [Buchmann 1987a] it is proved that $\mathcal{S}$ can only contain finitely many elements, and therefore the algorithm terminates. It remains to explain the implementation of expansion and compression. The compression of a set S is easily computed:

Algorithm 2.3 (Compression).
Input: A minimal set S and an index $i \in \{1, \dots, m\}$.
Output: $k_i(S)$.
- (Initialize) Set $k_i(S) = \varnothing$.
- For all $\alpha \in S$:
  - If $|\alpha|_i < \max\{|\beta|_i : \beta \in S\}$, set
$$k_i(S) = k_i(S) \cup \{\alpha\}.$$

Computing the i-th expansion of a minimal set S is more complicated. We first determine $|e_i(S)|$ by means of a divide and conquer strategy. Then we determine $e_i(S)$ by complete enumeration.

Algorithm 2.4 (Expansion).
Input: A minimal set S and an index $i \in \{1, \dots, m\}$.
Output: $e_i(S)$.
- (Initialize) Set $e_i(S) = \varnothing$, found = false, $C_j = |S|_j$ for $1 \leq j \leq m$ and $j \neq i$, $C_i = 2\,|d|^{1/n}$, and denom = 2.
- While found = false or denom = 2:
  - If there exists $\beta \neq 0$ with $|\beta|_j < C_j$ for all $j \neq i$:
    - Set found = true and $C_j = |\beta|_j/$ denom.
  - Else:
    - If found = false, set $C_i = 2C_i$.
    - Else:
      - If denom = 2, set denom = 1 and $C_i = 2C_i$.
- Replace $e_i(S)$ by the set of all α with $|\alpha|_j \leq C_j$ for $1 \leq j \leq m$.

The initialization $C_i = 2\,|d|^{1/n}$ is based on experience. This choice works pretty well in practice.

Next we explain how to solve the enumeration problems in Algorithm 2.4. This is done by rescaling the Minkowski lattice corresponding to $\mathfrak{a}$ in such a way that the box that we want to enumerate becomes the unit cube. Then we use the algorithm of Fincke and Pohst [1983] to enumerate a sphere containing the cube, and collect all admissible points. This is a lot faster than using the algorithm of Fincke and Pohst without rescaling, since scaling decreases the number of enumeration steps (Figure 1).

Algorithm 2.5 (Finding all elements within given bounds).
Input: A $\mathbb{Z}$-basis $\alpha_1, \dots, \alpha_n$ of $\mathfrak{a}$ and positive real bounds $C_1, \dots, C_m$.
Output: The set Z of all $\alpha \in \mathfrak{a}$ with $|\alpha|_i \leq C_i$ for $1 \leq i \leq m$.
- (Initialize) Set $Z = \varnothing$ and

$$\begin{aligned}\mathbf{b}_j = (&{\alpha_j}^{(1)}/C_1, \dots, {\alpha_j}^{(r_1)}/C_{r_1},\\ &\operatorname{Re}\alpha_j^{(r_1+1)}/\sqrt{C_{r_1+1}}, \dots, \operatorname{Re}\alpha_j^{(r_1+r_2)}/\sqrt{C_{r_1+r_2}},\\ &\operatorname{Im}\alpha_j^{(r_1+1)}/\sqrt{C_{r_1+1}}, \dots, \operatorname{Im}\alpha_j^{(r_1+r_2)}/\sqrt{C_{r_1+r_2}}).\end{aligned}$$

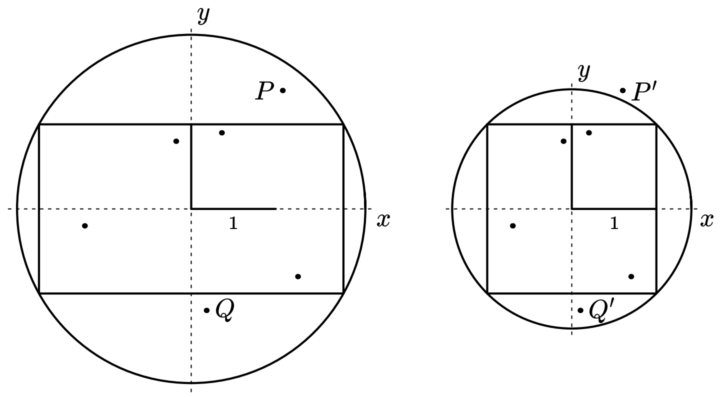

FIGURE 1. Effect of rescaling on enumeration of boxes. Left: Original situation. Right: After rescaling; note how the image of P now falls outside the ball.

- Use the algorithm of [Fincke and Pohst 1983] to find the set X of all $\mathbf{x} \in \mathbb{Z}^n$ with $\left\|\sum x_j \mathbf{b}_j\right\| \leq m$.
- For all $\mathbf{x} \in X$:
  - Set $\beta = (\mathbf{b}_1, \ldots, \mathbf{b}_n)\mathbf{x}$.
  - If $|\beta|_j \leq C_j$ for $1 \leq j \leq m$, set $Z = Z \cup \{\beta\}$.

An easy modification of this algorithm finds instead of all the admissible points just one of them or returns the message that there is none.

This concludes the description of the GLA. Numerical examples can be found in Section 4.

3. THE MODIFIED ALGORITHM

Our experience shows that computing the complete graph of reduced principal ideals is extremely time-consuming and is in general hopeless for unit rank larger than two. Therefore we have studied a modification of the algorithm in which we only determine a few neighbors that are easier to find. For $k \in \{1, \ldots, m\}$, a *k-th degree neighbor* of 1 is a neighbor μ with $|\mu|_j < |1|_j$ for all $j \in \{1, \ldots, m\}$ except for k values of j. The k-th degree neighbors of a reduced ideal are defined analogously. Computing first-degree neighbors is fairly simple. Also the partial graph that we obtain by only computing those neighbors still yields a subgroup of $\mathcal{O}^*$ of finite index. Experience shows, however, that for orders of unit rank greater than three this index tends to be very large. There we have to determine higher-degree neighbors. For example, in order to determine the unit group of the maximal order of a field of unit rank 11 it was useful to compute fourth-degree neighbors. Such neighbors can be computed by means of the following procedure.

Algorithm 3.1 (Computing a k-th degree neighbor).

Input: A reduced ideal $\mathfrak{a}$ and a set $U \subset \{1, \ldots, m\}$ with k elements.

Output: A k-th degree neighbor β with $|\beta|_j > |1|_j$ for all $j \in U$ and $|\beta|_j < |1|_j$ otherwise (or the information that such a neighbor does not exist).

- (Initialize) Set $C_j = 1$ for $j \notin U$ and $C_j = |d|^{1/n}$ for $j \in U$; set denom $= 2$ and found $=$ false.
- While found $=$ false or denom $= 2$:
  - If there exists $\beta \neq 0$ with $|\beta|_j < C_j$ for $j \in U$:
    - Set found $=$ true and $C_j = |\beta|_j /$ denom for $j \in U$.
  - Else:
    - If found $=$ false, set $C_j = 2C_j$ for $j \in U$.
    - Else:
      - If denom $= 2$, set denom $= 1$ and $C_j = 2C_j$ for $j \in U$.
- If β is an m-th degree neighbor with $m < k$, set found $=$ false and return.
- Else, return β.

Which neighbors should be used for a given number field? In general we recommend computing only first- and second-degree neighbors. That is based on computational experience with many fields, and on the fact that Algorithm 3.1 gets more time-consuming for higher-degree neighbors. In all cases considered, with fields of degree up to twenty and various signatures, we found subgroups of units with small indices in the full unit group using first- and second-degree neighbors.

4. NUMERICAL RESULTS AND OBSERVATIONS

All computations were done on Apollo workstations DN3000 and DN4500 (CPU Motorola 68020/68030). We used the Fortran version of the number theoretic program library Kant, developed in Düsseldorf [Schmettow 1991]. More data is contained in [Jüntgen 1990]. All algorithms described in this paper are now a part of Kant V1.

We first present a detailed example to illustrate what a complete graph produced by Algorithm 2.1 looks like. Let $\mathcal{O}$ be the maximal order of the totally real field of degree four generated by a root of $f(t) = t^4 - t^3 - 16t^2 - 5t + 5$. The discriminant is 10025 and an integral basis is given by $\omega_1 = 1$, $\omega_2 = \rho$, $\omega_3 = \rho^2$, $\omega_4 = \frac{1}{20}(-5 - 8\rho^2 + \rho^3)$.

Figure 2 shows the graph of minima in $\mathcal{O}$. Two minima are neighbors if and only if the corresponding vertices are connected by an edge. There are nine minima that are pairwise non associated, corresponding to nine reduced principal ideals; The corresponding vertices are labeled $\mu_1, \dots, \mu_9$. Remaining vertices are labeled with expressions of the form $k(\mu_i)$, which have the following meaning: If the vertex μ_j is connected to a vertex labeled $k(\mu_i)$, the minimum μ_j has k neighbors associated to μ_i.

After the computation of all neighbors of 1 we already have fourteen units. Using MLLL [Pohst 1987], we obtain a basis of the corresponding subgroup of $\mathcal{O}^*$ consisting of only two units, so we have not yet found a subgroup of finite index. After the computation of all neighbors of μ_2 we have seven more units, and it turns out that those 21 units generate $\mathcal{O}^*$. The graph required the computation of 257 minimal sets by 798 expansions and 610 compressions, and 30% of all expansions and compressions do not yield new minimal sets.

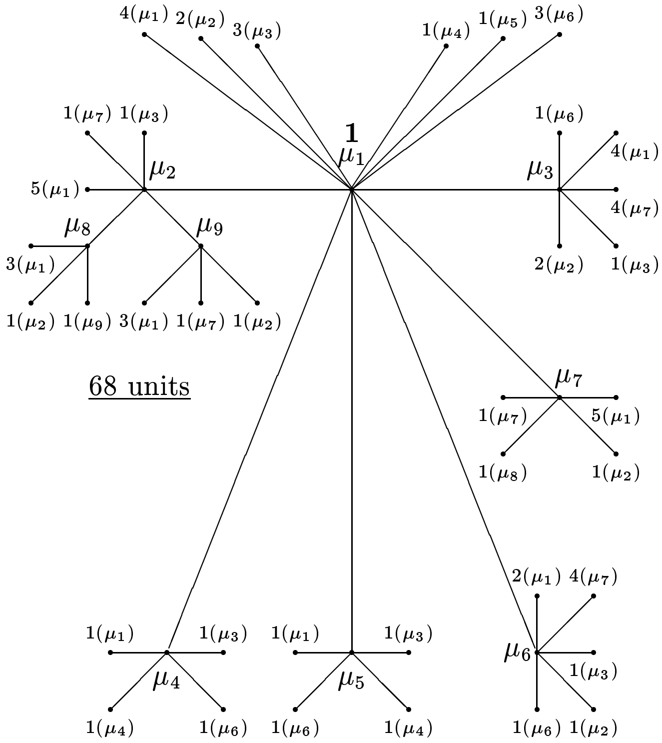

FIGURE 2. Example of a graph of minima. See text to the left for the meaning of the labels.

To compute all neighbors of all nine minima by the expansion and compression technique we had to compute the absolute values of 22000 algebraic numbers. Only 77 of those numbers are necessary for the construction of the graph.

We observe that the number of neighbors of 1 is much larger than the number of neighbors of all the other minima. Experimental experience suggests that this is typical. In fact, for the minima that are "far away" from 1 the number of neighbors seems to be four. We obtain the following system of fundamental units:

$$\eta_1 = -\omega_1 + 2\omega_2 - \omega_3 - 3\omega_4,$$
$$\eta_2 = \omega_2 + \omega_4,$$
$$\eta_3 = \omega_1 + 2\omega_2 - \omega_4;$$

the regulator is approximately 6.1491.

d	R	p	$\#(U)$
19773	9.447	17	131
19796	17.135	26	192
19821	7.782	8	58
20032	7.662	7	51
20225	7.835	11	94
20308	19.780	17	190
20808	11.760	11	107
21025	5.041	9	70
21056	7.801	6	53
21200	12.639	17	133
21208	14.648	19	134
21308	12.253	15	105
21312	16.105	22	157

d	R	p	$\#(U)$
21469	7.951	10	70
21568	17.222	19	133
21725	5.537	6	63
21737	8.622	8	62
21801	10.605	12	100
21964	12.377	14	96
22000	8.457	8	91
22221	10.178	11	94
22545	14.827	16	120
22592	18.338	17	152
22676	18.784	24	171
22784	11.234	12	91
22896	12.981	17	119

d	R	p	$\#(U)$
23252	18.856	24	194
23297	11.286	11	85
23301	9.846	12	82
23377	14.492	17	127
23525	7.569	7	76
23552	12.682	16	90
23600	7.350	10	82
23665	15.175	18	127
23724	14.408	14	112
24197	20.307	27	208
24336	12.310	10	111
24400	9.835	12	126
24417	11.877	12	111

TABLE 1. Discriminant, regulator, period length and cardinality of minimal generating system for a sample of totally real quartic fields. A complete list was computed up to discriminant 69025.

As already mentioned, the number p of reduced principal ideals of the maximal order $\mathcal{O}$ satisfies

$$\frac{R}{\log^r |d|} \leq p \leq \frac{k_0}{w} R,$$

where $k_0 \in \mathbb{R}^{\geq 0}$ depends on the signature of F, and w is the order of the torsion subgroup of $\mathcal{O}^*$ [Buchmann 1987b]. For totally real fields of degree four the value of k_0 turns out to be $2 \cdot 4^3 / \log^3 2 \approx 384$.

Table 1 is part of a list we compiled of all totally real quartic fields up to discriminant 69025. The value of the regulator is close to the period length and for all 560 fields up to discriminant 69025 the quotient p/R is less than 2. Unfortunately we could not find any asymptotic behavior such as is known for totally real quadratic fields.

We also applied the algorithm to the maximal orders of all the totally real fields of minimal discriminant and degrees four, five and six. To find the result for the field of degree six we computed 4062 different minimal sets. We needed 20310 expansions and 17636 compressions which, in turn, required the enumeration of 53857 boxes in $\mathbb{R}^6$.

We also tried to apply the algorithm to totally real fields of minimal discriminant in degrees seven and eight. In both cases we stopped the computation after 36000 seconds of computing time. Although we computed more than 100 neighbors of 1, we were not able to find all neighbors of 1 in that time. Among the neighbors that we did compute there was a generating system for the unit group.

We found similar results for fields of mixed signature and unit rank greater than three. The time-consuming computation of all neighbors of 1 makes the algorithm highly inefficient, so it takes a long time to compute all vertices in the graph of reduced principal ideals. Hence, in general, computing all reduced principal ideals does not seem to be an efficient method for calculating fundamental units and to decide principality of a given ideal.

It is therefore interesting to use the modified algorithm of Section 3 (the PGLA), and see how it performs. For quartic fields of discriminant less than 10^6, we computed a subgroup of finite index of the unit group of the maximal order, using

n	d	R	N	p	run time
4	725	0.825	9	1	60 seconds
5	14641	1.636	37	2	14290 seconds
6	300125	3.278	101	1	several days

TABLE 2. Discriminant, regulator, number N of neighbors of 1, period length, and running time for maximal order of the totally real field of minimum discriminant in each degree from 4 to 6.

index	1	2	3	4	5	6	7	8
fields	12897	134	16	13	6	5	1	1
vertices in partial graph	< 200	6	2	2	2	2	1	1

TABLE 3. Distribution of the index of the unit group computed with first-degree neighbors in the full unit group for the maximal order, for all totally real quartic fields of discriminant $< 10^6$.

first-degree neighbors (Section 3). We observed the value of the index in each case, and tabulated how often each value occurred (Table 3).

We see that the index is usually very small, and if the number of vertices is larger than 6 we already have fundamental units. Very similar results were observed for totally real fields of degree five up to discriminant $2 \cdot 10^6$. Unfortunately the index increases with the degree of the field. Consider the totally real field of degree eight generated by a root ρ of

$$f(t) = t^8 + 2t^7 - 7t^6 - 8t^5 + 15t^4 + 8t^3 - 9t^2 - 2t^1 + 1,$$

which is of (minimum) discriminant $282300416 = 2^{13} \cdot 41^3$. It has a power integral basis $\omega_i = \rho^{i-1}$ for $1 \le i \le n$. All first-degree neighbors of 1 are units, and among those neighbors there is the following maximal system of independent units:

$$\begin{aligned}
\varepsilon_1 &= 2\omega_1 + \omega_2 + 4\omega_3 - 5\omega_4 - 11\omega_5 + 4\omega_7 + \omega_8\\
\varepsilon_2 &= -16\omega_1 + 12\omega_2 + 151\omega_3 + 64\omega_4\\
&\qquad - 143\omega_5 - 56\omega_6 + 34\omega_7 + 12\omega_8\\
\varepsilon_3 &= 23\omega_1 - 28\omega_2 - 229\omega_3 + 22\omega_4\\
&\qquad + 366\omega_5 + 68\omega_6 - 117\omega_7 - 34\omega_8\\
\varepsilon_4 &= 4\omega_2 - \omega_3 - 14\omega_4 + 4\omega_5 + 12\omega_6 - 3\omega_7 - 2\omega_8\\
\varepsilon_5 &= -102\omega_1 - 163\omega_2 + 327\omega_3 + 345\omega_4\\
&\qquad - 284\omega_5 - 181\omega_6 + 67\omega_7 + 29\omega_8\\
\varepsilon_6 &= 54\omega_1 - 226\omega_2 + 3\omega_3 + 422\omega_4\\
&\qquad - 112\omega_5 - 191\omega_6 + 39\omega_7 + 25\omega_8\\
\varepsilon_7 &= -8\omega_1 - 17\omega_2 + 34\omega_3 + 27\omega_4\\
&\qquad - 25\omega_5 - 13\omega_6 + 5\omega_7 + 2\omega_8
\end{aligned}$$

The regulator of this system is ≈ 7811.5107, and the index of the unit group generated by those units in the full unit group is 355. Computing a set of fundamental units by means of the algorithm in [Arenz 1991; Pohst and Zassenhaus 1987] starting with a subgroup of such a large index is far too time consuming. Using three more second-degree neighbors we found the following system of fundamental units:

$$\begin{aligned}
\eta_1 &= -2\omega_1 - 9\omega_2 + 8\omega_3 + 15\omega_4 - 8\omega_5 - 7\omega_6 + 2\omega_7 + \omega_8\\
\eta_2 &= -6\omega_2 + 12\omega_4 - 5\omega_5 - 6\omega_6 + 2\omega_7 + \omega_8\\
\eta_3 &= 3\omega_1 - 6\omega_2 - 19\omega_3 + 10\omega_4 + 26\omega_5 + \omega_6 - 8\omega_7 - 2\omega_8\\
\eta_4 &= -3\omega_1 + 5\omega_2 + 15\omega_3 - 5\omega_4 - 15\omega_5 - \omega_6 + 4\omega_7 + \omega_8\\
\eta_5 &= -\omega_1 - 5\omega_2 - \omega_3 + 9\omega_4 + 3\omega_5 - 3\omega_6 - \omega_7\\
\eta_6 &= 5\omega_2 + 2\omega_3 - 9\omega_4 - 3\omega_5 + 3\omega_6 + \omega_7\\
\eta_7 &= \omega_1 + \omega_2 + 6\omega_3 + 4\omega_4 - 17\omega_5 - 6\omega_6 + 6\omega_7 + 2\omega_8
\end{aligned}$$

The reason for the index being so large in the first case is probably that our field contains the quadratic subfield $\mathbb{Q}(\sqrt{5})$, whose fundamental unit is not a first-degree neighbor but only a fourth-degree neighbor.

The PGLA works quite fast for fields of larger degree. We applied it to fields of degree up to 20. For example, consider the field generated by a root ρ of the polynomial

$$\begin{aligned}
f(t) = t^{12} &+ 4t^{11} - 17t^{10} - 68t^9 + 108t^8\\
&+ 416t^7 - 314t^6 - 1129t^5 + 358t^4\\
&+ 1353t^3 - 36t^2 - 540t - 72,
\end{aligned} \tag{4.1}$$

with discriminant $1397546311750178 49 = 3^6 \cdot 61^8$ and unit rank 11. An integral basis is given in the sidebar at the top of the next page.

We applied the PGLA with second-degree neighbors. After computing less than 30 neighbors, we detected the following maximal system of independent units:

$$\begin{aligned}
\eta_1 &= \omega_1 + \omega_3 + 2\omega_5 - \omega_6 - \omega_7 - \omega_8 - \omega_9\\
\eta_2 &= \omega_1 - \omega_3 - \omega_4 - 3\omega_5 + \omega_6 + 2\omega_7 + 2\omega_8 + 2\omega_9 - \omega_{10} + \omega_{11}\\
\eta_3 &= -\omega_3 + \omega_4 - \omega_5 + \omega_6 + \omega_7 + 2\omega_9 + \omega_{11}\\
\eta_4 &= \omega_1 + \omega_2 + \omega_5 - \omega_6\\
\eta_5 &= \omega_3 + \omega_6 + \omega_7\\
\eta_6 &= \omega_3 - \omega_4 + \omega_5 - \omega_6 - \omega_7 - \omega_9 - \omega_{11} - \omega_{12}\\
\eta_7 &= -\omega_2 - \omega_3 + \omega_4 - \omega_5 + \omega_{10}\\
\eta_8 &= -\omega_1 - 2\omega_2 + \omega_5 - \omega_6 - 2\omega_7 - \omega_8 - \omega_9 - 2\omega_{11} - \omega_{12}\\
\eta_9 &= -2\omega_1 - \omega_2 + \omega_3 - \omega_5 + \omega_6 + \omega_7 - \omega_8 + \omega_9 - \omega_{10}\\
\eta_{10} &= \omega_3 - \omega_4 - \omega_5 - \omega_{10}\\
\eta_{11} &= -\omega_1 + \omega_7 + \omega_{12}.
\end{aligned}$$

$$
\begin{aligned}
\omega_1 &= 1\\
\omega_2 &= \rho\\
\omega_3 &= (97200 - 55176\rho - 264400\rho^2 - 66734\rho^3 + 185390\rho^4 - 23108\rho^5\\
&\qquad - 51192\rho^6 + 14792\rho^7 + 9248\rho^8 - 1000\rho^9 - 730\rho^{10} - 66\rho^{11})/71232\\
\omega_4 &= (384864 + 3268848\rho - 388144\rho^2 - 6744804\rho^3 - 740772\rho^4 + 3896136\rho^5\\
&\qquad + 617728\rho^6 - 829024\rho^7 - 155216\rho^8 + 58960\rho^9 + 12004\rho^{10} - 196\rho^{11})/71232\\
\omega_5 &= (-253872 - 342648\rho + 755744\rho^2 + 650462\rho^3 - 321926\rho^4 - 327964\rho^5\\
&\qquad - 27448\rho^6 + 60584\rho^7 + 23664\rho^8 - 1848\rho^9 - 2214\rho^{10} - 278\rho^{11})/71232\\
\omega_6 &= (-375168 - 1860192\rho + 341344\rho^2 + 3700712\rho^3 + 813376\rho^4 - 1952944\rho^5\\
&\qquad - 693456\rho^6 + 351952\rho^7 + 169936\rho^8 - 10640\rho^9 - 12728\rho^{10} - 1440\rho^{11})/71232\\
\omega_7 &= (143184 + 1697928\rho + 26528\rho^2 - 2718394\rho^3 - 297374\rho^4 + 1445204\rho^5\\
&\qquad + 175496\rho^6 - 301144\rho^7 - 39888\rho^8 + 22920\rho^9 + 2994\rho^{10} - 302\rho^{11})/71232\\
\omega_8 &= (400680 + 1833588\rho - 594024\rho^2 - 4314677\rho^3 - 94711\rho^4 + 2656042\rho^5\\
&\qquad + 163028\rho^6 - 601020\rho^7 - 47912\rho^8 + 50668\rho^9 + 4081\rho^{10} - 1007\rho^{11})/71232\\
\omega_9 &= (-319104 - 911136\rho + 127680\rho^2 + 1592920\rho^3 + 855968\rho^4 - 814928\rho^5\\
&\qquad - 639472\rho^6 + 118512\rho^7 + 148336\rho^8 + 6832\rho^9 - 10760\rho^{10} - 1664\rho^{11})/71232\\
\omega_{10} &= (-303336 - 2094612\rho + 4040\rho^2 + 4145733\rho^3 + 1259511\rho^4 - 2226954\rho^5\\
&\qquad - 948596\rho^6 + 391580\rho^7 + 230824\rho^8 - 6380\rho^9 - 17441\rho^{10} - 2257\rho^{11})/71232\\
\omega_{11} &= (-449856 - 1717824\rho + 1731760\rho^2 + 3153528\rho^3 - 2312904\rho^4 - 2083536\rho^5\\
&\qquad + 1174880\rho^6 + 602272\rho^7 - 228640\rho^8 - 83344\rho^9 + 14792\rho^{10} + 4504\rho^{11})/71232\\
\omega_{12} &= (271416 - 978084\rho - 2770680\rho^2 + 1558449\rho^3 + 4388883\rho^4 - 406722\rho^5\\
&\qquad - 2287860\rho^6 - 150660\rho^7 + 463128\rho^8 + 68916\rho^9 - 31341\rho^{10} - 6261\rho^{11})/71232
\end{aligned}
$$

An integral basis of the field generated over a root ρ of the polynomial (4.1).

The regulator of this system is ≈ 55324.63. We tried to enlarge the subgroup generated by $\eta_1, \ldots, \eta_{11}$ using 22 more units and stopped that computation since the regulator did not change. Using the method of [Pohst and Zassenhaus 1987] we proved that $\eta_1, \ldots, \eta_{11}$ generate the full unit group.

Our computations indicate that in order to determine the full unit group it suffices to use low degree neighbors. It would be very interesting to prove such a result.

REFERENCES

[Arenz 1991] B. Arenz, "Computing fundamental units from independent ones", pp. 163–171 in *Computational Number Theory, Debrecen (Hungary), 1989* (edited by A. Pethő et al.), de Gruyter, Berlin, 1991.

[Buchmann 1987a] J. Buchmann, "On the computation of units and class numbers by a generalization of Lagrange's algorithm", *J. Number Theory* **26** (1987), 8–30.

[Buchmann 1987b] J. Buchmann, "On the period length of the generalized Lagrange algorithm", *J. Number Theory* **26** (1987), 31–37.

[Buchmann 1988] J. Buchmann, "Zur Komplexität der Berechnung von Einheiten und Klassenzahlen algebraischer Zahlkörper", Habilitationsschrift, U. Düsseldorf, 1988.

[Buchmann and Pethő 1989] J. Buchmann and A. Pethő, "On the computation of independent units in number fields by Dirichlet's method", *Math. Comp.* **52** (1989), 149–159.

[Buchmann et al. 1989] J. Buchmann, M. Pohst and J. v. Schmettow, "On the computation of unit groups and class groups of totally real quartic fields", *Math. Comp.* **53** (1989), 387–397.

[Fincke and Pohst 1983] U. Fincke and M. Pohst, "A procedure for determining algebraic integers of given norm", pp. 194–202 in *Computer Algebra: EUROCAL '83, London, 1983* (edited by J. A. van Hulzen), Lecture Notes in Computer Science **162**, Springer, Berlin, 1983.

[Fincke and Pohst 1985] U. Fincke and M. Pohst, "A new method for computing fundamental units in algebraic number fields", pp. 470–479 in *Computer Algebra: EUROCAL '85, Linz, 1985* (edited by Bob Caviness), Lecture Notes in Computer Science **204**, Springer, Berlin, 1985.

[Jüntgen 1990] M. Jüntgen, "Berechnung von Einheiten in algebraischen Zahlkörpern mittels des verallgemeinerten Lagrangeschen Kettenbruchalgorithmus", Diplomarbeit, U. Düsseldorf, 1990.

[Pohst 1987] M. Pohst, "A modification of the LLL–algorithm", *J. Symbolic Comp.* **4** (1987), 123–128.

[Pohst and Zassenhaus 1987] M. Pohst and H. Zassenhaus, *Algorithmic Algebraic Number Theory*, Encyc. of Math. and Its Applications, Cambridge University Press, Cambridge, 1989.

[Schmettow 1991] J. Graf v. Schmettow, "Kant: A tool for computations in algebraic number fields", pp. 321–330 in *Computational Number Theory*, *Proc. Coll. Comp. Number Theory*, *Debrecen* (*Hungary*), 1989 (edited by A. Pethő et al.), de Gruyter, Berlin, 1991.

Johannes Buchmann, Universität des Saarlandes, FB-14 Informatik, 66041 Saarbrücken, Germany (buchmann@cs.uni-sb.de)

Max Jüntgen, Fachbereich 3 Mathematik MA 8-1, Technische Universität Berlin, Straße des 17. Juni 136, 10623 Berlin, Germany (juentgen@math.tu-berlin.de)

Michael Pohst, Fachbereich 3 Mathematik MA 8-1, Technische Universität Berlin, Straße des 17. Juni 136, 10623 Berlin, Germany (pohst@math.tu-berlin.de)

Received February 23, 1994; accepted in revised form September 7