AN OPTIMIZATION PROBLEM FOR LATTICES

L. HAJDU[1,2,3,4], T. KOVÁCS[1,2,3], A. PETHŐ[1,3], M. POHST[1]

Abstract. We present theoretical and computational results concerning an optimization problem for lattices, related to a generalization of the concept of dual lattices. Let Λ be a k-dimensional lattice in $\mathbb{R}^n$ (with $0 < k \leq n$), and $p, q \in \mathbb{R}^+ \cup \{\infty\}$. We define the p, q-norm $N_{p,q}(\Lambda)$ of the lattice Λ and show that this norm always exists. In fact, our results yield an algorithm for the calculation of $N_{p,q}(\Lambda)$. Further, since this general algorithm is not efficient, we discuss more closely two particular choices for p, q, which arise naturally. Namely, we consider the case $(p, q) = (2, \infty)$, and also the choice $(p, q) = (1, \infty)$. In both cases we show that in general an optimal basis of Λ as well as $N_{p,q}(\Lambda)$ can be actually calculated. Finally, we illustrate our methods by several numerical examples.

1. Introduction

Let Λ be a k-dimensional lattice in $\mathbb{R}^n$ (with $0 < k \leq n$). We call

$$\hat{\Lambda} := \{\underline{\hat{x}} \in \mathbb{R}^n \ : \ (\underline{\hat{x}}, \underline{x}) \in \mathbb{Z} \text{ for all } \underline{x} \in \Lambda\}$$

the *dual set* of Λ. A lattice Λ^* in $\mathbb{R}^n$ is called a *dual lattice* of Λ, if $\hat{\Lambda} = \Lambda^* \oplus H$ holds with some subspace H of $\mathbb{R}^n$. In other words, Λ^* is a dual lattice of Λ if there exists a subspace H of $\mathbb{R}^n$ such that every $\underline{a} \in \hat{\Lambda}$ can be uniquely written in the form $\underline{a} = \underline{b} + \underline{h}$ ($\underline{b} \in \Lambda^*, \underline{h} \in H$). As it is well-known, if $k = n$ (i.e. Λ is a full lattice in $\mathbb{R}^n$) then $\hat{\Lambda}$ is just the dual (or polar or reciprocal) lattice of Λ (see e.g. [Lekkerkerker 69]). In that case we have $\Lambda^* = \hat{\Lambda}$ and $H = \{\underline{0}\}$. In Section 2 we show that

Date: September 23, 2012.

2010 *Mathematics Subject Classification.* 06B99.

Key words and phrases. Lattices, dual lattices, bases of lattices, basis reduction, LLL-reduction.

1) Research supported in part by the TÁMOP 4.2.1./B-09/1/KONV-2010-0007 project. The project is implemented through the New Hungary Development Plan, cofinanced by the European Social Fund and the European Regional Development Fund.

2) Research supported in part by the OTKA grant K75566.

3) Research supported in part by the OTKA grant K100339.

4) Research supported in part by the OTKA grant NK101680.

dual lattices do exist for any lattice Λ, and give some of their basic properties.

Let $p, q \in \mathbb{R}^+ \cup \{\infty\}$, and let $L \subset \mathbb{R}^n$ be a k-dimensional lattice. Then the p, q-size of L is

$$|L|_{p,q} = \min_{(\underline{a}_1,\dots,\underline{a}_k)} |(|\underline{a}_1|_p, \dots, |\underline{a}_k|_p)|_q,$$

where $(\underline{a}_1, \dots, \underline{a}_k)$ runs through all bases of L, and $|\underline{v}|_r = |\underline{v}^{tr}|_r$ is the L_r-norm of a vector $\underline{v}$ with $\underline{v}^{tr} = (v_1, \dots, v_n) \in \mathbb{R}^n$ given by

$$|\underline{v}|_r = |\underline{v}^{tr}|_r = \begin{cases} \left(\sum\limits_{i=1}^{n} |v_i|^r\right)^{1/r}, & \text{if } r \in \mathbb{R}^+, \\ \max\{|v_1|, \dots, |v_n|\}, & \text{if } r = \infty. \end{cases}$$

Then the p, q-norm of the lattice Λ is defined by

$$N_{p,q}(\Lambda) = \min_{\Lambda^*} |\Lambda^*|_{p,q} \tag{1}$$

where Λ^* runs through all the dual lattices of Λ. By the norm equivalence theorem any bounded region contains only finitely many vectors of a lattice $L \subset \mathbb{R}^n$. Hence the size $|L|_{p,q}$ exists for any lattice. As we shall see later, the minimum in (1) also exists, so $N_{p,q}(\Lambda)$ is well-defined, too.

It is worth to mention that in case of $k = n$, i.e. when we consider full lattices, the above notions are well-known and are of great importance in lattice theory and in many of its applications (see e.g. the books [Lekkerkerker 69] and [Pohst and Zassenhaus 89], and the papers [Kannan and Lovász 88] and [Schnell 92]). On the other hand, the problem of finding $N_{1,\infty}(\Lambda)$ in case of $k = n - 1$ naturally arises in the context of solving S-unit equations (see [Hajdu 09]).

In the paper we take up the problem for general $0 < k \leq n$ and p, q. First we show that $N_{p,q}(\Lambda)$ exists for any p, q and Λ. In fact, our results yield an algorithm for the calculation of $N_{p,q}(\Lambda)$. However, since this general algorithm is not really efficient, we discuss two particular cases separately. Namely, we consider the natural case $(p, q) = (2, \infty)$, and also the choice $(p, q) = (1, \infty)$, when as we indicated already, the problem arises from lattices connected to the unit groups of algebraic number fields. In both cases we show that an optimal basis of Λ can be explicitly calculated. Finally, we illustrate our methods by several numerical examples. At this point, our intention is to present some illustrative material, rather than to stress the computations to the limit.

2. Some basic properties of dual lattices

In this chapter we give some basic properties of dual lattices. On the one hand, as we demonstrate that, this notion is a natural generalization of the usual concept of the dual lattice of a full lattice. On the other hand, we need to establish a way to be able to work effectively with dual lattices.

Recall that the set

$$\hat{\Lambda} := \{\underline{\hat{x}} \in \mathbb{R}^n \ : \ (\underline{\hat{x}}, \underline{x}) \in \mathbb{Z} \text{ for all } \underline{x} \in \Lambda\}$$

is called the dual set of a k-dimensional lattice Λ in $\mathbb{R}^n$ $(0 < k \leq n)$. As we mentioned already, if $k = n$ (i.e. Λ is a full lattice in $\mathbb{R}^n$) then $\hat{\Lambda}$ is the dual (or polar or reciprocal) lattice of Λ (see e.g. [Lekkerkerker 69], [Kannan and Lovász 88] and [Schnell 92]). Our first aim is to describe the structure of $\hat{\Lambda}$ in the general case.

Theorem 2.1. *Let $\underline{a}_1, \dots, \underline{a}_k$ be an arbitrary, but fixed basis of Λ. Take any vectors $\underline{b}_i \in \mathbb{R}^n$ $(i = 1, \dots, k)$ such that*

$$(\underline{b}_i, \underline{a}_j) = \begin{cases} 1, & \textit{if } i = j, \\ 0, & \textit{otherwise} \end{cases} \qquad (1 \leq i, j \leq k).$$

Write Λ^* for the lattice generated by $\underline{b}_1, \dots, \underline{b}_k$, and let $\Lambda^\perp$ be the orthogonal complement of the subspace of $\mathbb{R}^n$ generated by $\underline{a}_1, \dots, \underline{a}_k$. Then we have

$$\hat{\Lambda} = \Lambda^* \oplus \Lambda^\perp,$$

that is, any $\underline{b} \in \hat{\Lambda}$ can be uniquely written as

$$\underline{b} = \underline{a}^* + \underline{a}^\perp \quad \textit{with } \underline{a}^* \in \Lambda^*, \ \underline{a}^\perp \in \Lambda^\perp. \tag{2}$$

Further, here Λ^* and $\Lambda^\perp$ are uniquely determined in the following sense. Let L and H be a lattice and a subspace in $\mathbb{R}^n$, respectively, such that

$$\hat{\Lambda} = L \oplus H.$$

Then we have $H = \Lambda^\perp$, and both

$$L \subseteq \Lambda^* + \Lambda^\perp \quad \textit{and} \quad \Lambda^* \subseteq L + \Lambda^\perp.$$

In particular, dim$(L) = k$ and dim$(H) = n - k$.

Proof. First we show that every element of $\hat{\Lambda}$ can be written in the form (2). For this, let $\underline{b} \in \hat{\Lambda}$ be arbitrary. Then we have

$$(\underline{b}, \underline{a}_i) = t_i \quad (t_i \in \mathbb{Z}, \ i = 1, \dots, k).$$

Put

$$\underline{a}^* := t_1 \underline{b}_1 + \cdots + t_k \underline{b}_k \quad \text{and} \quad \underline{a}^\perp := \underline{b} - \underline{a}^*.$$

Then we obviously have $\underline{a}^* \in \Lambda^*$. Moreover, by the definition of the vectors $\underline{b}_i$ $(i = 1, \dots, k)$, $\underline{a}^*$ and $\underline{a}^\perp$ we obtain

$$(\underline{a}^\perp, \underline{a}_i) = (\underline{b} - \underline{a}^*, \underline{a}_i) = (\underline{b}, \underline{a}_i) - (\underline{a}^*, \underline{a}_i) =$$

$$= (\underline{b}, \underline{a}_i) - (t_1\underline{b}_1 + \dots + t_k\underline{b}_k, \underline{a}_i) = t_i - t_i = 0 \quad (i = 1, \dots, k).$$

Hence we get that $\underline{a}^\perp \in \Lambda^\perp$ is also valid, which proves that $\hat{\Lambda} = \Lambda^* + \Lambda^\perp$.

To prove the uniqueness of the representation (2) of any $\underline{b} \in \hat{\Lambda}$, take arbitrary vectors $\underline{a}_{k+1}, \dots, \underline{a}_n \in \mathbb{R}^n$ such that $\underline{a}_1, \dots, \underline{a}_k, \underline{a}_{k+1}, \dots \underline{a}_n$ are linearly independent (over $\mathbb{R}$). Then we see that $\hat{\Lambda}$ contains the dual lattice of the full lattice generated by $\underline{a}_1, \dots, \underline{a}_n$ in $\mathbb{R}^n$. Hence $\hat{\Lambda}$ is not included in any proper subspace of $\mathbb{R}^n$, which shows that $\dim(\Lambda^*) + \dim(\Lambda^\perp) = n$ must hold. Hence the uniqueness of the representation (2) follows immediately. Thus we proved that $\hat{\Lambda} = \Lambda^* \oplus \Lambda^\perp$.

Assume now that we also have $\hat{\Lambda} = L \oplus H$ with some lattice L and subspace H in $\mathbb{R}^n$. Suppose that $\underline{h} \in H \setminus \Lambda^\perp$. Take an arbitrary $t \in \mathbb{R}$ and observe that by $t\underline{h} \in \hat{\Lambda}$ we have

$$(t\underline{h}, \underline{a}_i) = t(\underline{h}, \underline{a}_i) \in \mathbb{Z} \quad (i = 1, \dots, k).$$

However, this is clearly possible only if

$$(\underline{h}, \underline{a}_i) = 0 \quad (i = 1, \dots, k).$$

This yields $h \in \Lambda^\perp$, a contradiction. Hence we have $H \subseteq \Lambda^\perp$. Assume next that $\underline{h} \in \Lambda^\perp \setminus H$. Observe that for any $t \in \mathbb{R}$ we have $t\underline{h} \in \hat{\Lambda}$. Thus by $\hat{\Lambda} = L \oplus H$, for any $t \in \mathbb{R}$ there exist vectors $\underline{u}_t \in L$ and $\underline{v}_t \in H$ such that $t\underline{h} = \underline{u}_t + \underline{v}_t$. Since L is a countable set, the vectors $\underline{u}_t$ $(t \in \mathbb{R})$ cannot be all different. Thus there exist $t_1, t_2 \in \mathbb{R}$ with $t_1 \neq t_2$, such that $\underline{u}_{t_1} = \underline{u}_{t_2}$. This yields

$$(t_2 - t_1)\underline{h} = (\underline{u}_{t_2} + \underline{v}_{t_2}) - (\underline{u}_{t_1} + \underline{v}_{t_1}) = \underline{v}_{t_2} - \underline{v}_{t_1}.$$

However, since $\underline{v}_{t_1}, \underline{v}_{t_2} \in H$ and H is a subspace, we get that $(t_2 - t_1)\underline{h} \in H$. Hence also $\underline{h} \in H$, a contradiction. This shows that $\Lambda^\perp \subseteq H$ must also be valid. Thus $H = \Lambda^\perp$ indeed. In particular, we obviously have $\dim(H) = \dim(\Lambda^\perp) = n - k$.

On the other hand, since by $\underline{0} \in H = \Lambda^\perp$ we have both $L \subseteq \hat{\Lambda}$ and $\Lambda^* \subseteq \hat{\Lambda}$, we immediately obtain that both $L \subseteq \Lambda^* + \Lambda^\perp$ and $\Lambda^* \subseteq L + \Lambda^\perp$. So we only need to prove that $\dim(L) = k$. Assume to the contrary that $\dim(L) > k$. (Since $\hat{\Lambda} = L \oplus H$ and $\dim(H) = n - k$, $\dim(L) < k$ is clearly impossible.) Let $\underline{\ell}_1, \dots, \underline{\ell}_k \in L$ be linearly independent elements (over $\mathbb{R}$), such that

$$L_0 \cap H = \{\underline{0}\}, \tag{3}$$

where L_0 is the linear subspace of $\mathbb{R}^n$ generated by the vectors $\underline{\ell}_1, \dots, \underline{\ell}_k$. Since $\hat{\Lambda} = L \oplus H$, such vectors exist. By our assumption $\dim(L) > k$, we can find a vector $\underline{\ell} \in L \setminus L_0$. Observe that $\underline{\ell} \in \hat{\Lambda}$, and put

$$(\underline{\ell}, \underline{a}_i) = t_i \in \mathbb{Z} \quad (i = 1, \dots, k). \tag{4}$$

Since $\dim(L_0) = k$ and $\dim(H) = n - k$, by (3) we can write

$$\underline{\ell} = c_1\underline{\ell}_1 + \dots + c_k\underline{\ell}_k + \underline{h} \tag{5}$$

with some $c_1, \dots, c_k \in \mathbb{R}$ and $\underline{h} \in H$, which are uniquely determined. This by $(\underline{h}, \underline{a}_i) = 0$ $(i = 1, \dots, k)$ yields

$$(\underline{\ell}, \underline{a}_i) = (c_1\underline{\ell}_1 + \dots + c_k\underline{\ell}_k + \underline{h}, \underline{a}_i) = d_{i,1}c_1 + \dots + d_{i,k}c_k \quad (i = 1, \dots, k) \tag{6}$$

where $d_{i,j} = (\underline{\ell}_j, \underline{a}_i) \in \mathbb{Z}$ for $1 \le i, j \le k$. Combining (4) and (6) we obtain the system of linear equations

$$\begin{pmatrix} d_{1,1} & \dots & d_{1,k} \\ \vdots & \ddots & \vdots \\ d_{k,1} & \dots & d_{k,k} \end{pmatrix} \begin{pmatrix} c_1 \\ \vdots \\ c_k \end{pmatrix} = \begin{pmatrix} t_1 \\ \vdots \\ t_k \end{pmatrix} \tag{7}$$

for $c_1, \dots, c_k$. One can easily check that the matrix on the left hand side of (7) is invertible. Thus, using that $d_{i,j} \in \mathbb{Z}$ $(1 \le i, j \le k)$, we get that $c_1, \dots, c_k \in \mathbb{Q}$. So there exists a non-zero integer t such that $tc_i \in \mathbb{Z}$ for all $i = 1, \dots, k$. However, this by (5) yields that we have two distinct representations for $t\underline{\ell} \in \hat{\Lambda}$ of the form $\underline{u} + \underline{v}$ with $\underline{u} \in L$ and $\underline{v} \in H$, given by

$$t\underline{\ell} + \underline{0} = ((tc_1)\underline{\ell}_1 + \dots + (tc_k)\underline{\ell}_k) + t\underline{h}.$$

This is a contradiction showing that $\dim(L) = k$ indeed, and the theorem follows. □

As a simple consequence we obtain the following statement, which yields a complete and explicit characterization of the dual lattices of Λ.

Corollary 2.1. *Let $\underline{a}_1^*, \dots, \underline{a}_k^*$ be an arbitrary, but fixed basis of Λ^*. Then, using the notation of Theorem 2.1 we have the following.*

For any $\underline{h}_1, \dots, \underline{h}_k \in \Lambda^\perp$ the lattice L generated by the vectors $\underline{a}_1^* + \underline{h}_1, \dots, \underline{a}_k^* + \underline{h}_k$ is a dual lattice of Λ.

Vice versa, suppose that $\hat{\Lambda} = L \oplus H$, where L and H is a lattice and a subspace in $\mathbb{R}^n$, respectively. Then L (as a lattice) has a unique basis of the form $\underline{a}_1^* + \underline{h}_1, \dots, \underline{a}_k^* + \underline{h}_k$ with some $\underline{h}_1, \dots, \underline{h}_k \in \Lambda^\perp$.

Proof. The first part of the statement immediately follows by observing that since $\underline{a}_1^*, \dots, \underline{a}_k^*$ is a basis of Λ^* and $\Lambda^* \oplus \Lambda^\perp = \hat{\Lambda}$, we have that $\hat{\Lambda} = L \oplus \Lambda^\perp$.

To prove the second part of the statement, observe that since $\Lambda^* \subseteq \hat{\Lambda}$, and also $H = \Lambda^\perp$, there exist $\underline{b}_1, \dots, \underline{b}_k \in L$ and $\underline{h}_1, \dots, \underline{h}_k \in \Lambda^\perp$ such that $\underline{a}_i^* = \underline{b}_i + \underline{h}_i'$ $(i = 1, \dots, k)$. That is, we have

$$\underline{a}_1^* + \underline{h}_1, \dots, \underline{a}_k^* + \underline{h}_k \in L \text{ with } \underline{h}_1 = -\underline{h}_1', \dots, \underline{h}_k = -\underline{h}_k' \in \Lambda^\perp.$$

Note that obviously, the above vectors are linearly independent (over $\mathbb{R}$). We show that they form a basis of L as a lattice, as well. Let $\underline{b} \in L$ arbitrary. Then since $\underline{a}_1^*, \dots, \underline{a}_k^*$ is a basis of the lattice Λ^*, by Theorem 2.1 we can write

$$\underline{b} = t_1\underline{a}_1^* + \cdots + t_k\underline{a}_k^* + \underline{a}^\perp \quad (t_1, \dots, t_k \in \mathbb{Z},\ \underline{a}^\perp \in \Lambda^\perp).$$

On the other hand, we also have that the linear combination

$$t_1(\underline{a}_1^* + \underline{h}_1) + \cdots + t_k(\underline{a}_k^* + \underline{h}_k)$$

belongs to L. Thus we have

$$t_1\underline{h}_1 + \cdots + t_k\underline{h}_k - \underline{a}^\perp \in L \cap H,$$

which yields

$$t_1\underline{h}_1 + \cdots + t_k\underline{h}_k = \underline{a}^\perp.$$

That is, $\underline{b}$ is a linear combination of $\underline{a}_1^* + \underline{h}_1, \dots, \underline{a}_k^* + \underline{h}_k$ with integral coefficients, so the latter vectors form a basis of the lattice L indeed.

Finally, assume that

$$\underline{a}_i^* + \underline{h}_i, \underline{a}_i^* + \underline{h}_i' \in L$$

for some $i \in \{1, \dots, k\}$, with $\underline{h}_i, \underline{h}_i' \in H$. Then we have $\underline{h}_i - \underline{h}_i' \in L \cap H$, whence $\underline{h}_i = \underline{h}_i'$. This proves the uniqueness of the vectors $\underline{h}_i$ $(i = 1, \dots, k)$, and the statement follows. □

Remark 1. In view of Theorem 2.1 and Corollary 2.1 we see that the dual set $\hat{\Lambda}$ can be decomposed as a direct sum $L \oplus H$ of a lattice and a subspace of $\mathbb{R}^n$ "almost" uniquely. More precisely, the subspace H is in fact uniquely determined, while the lattice is determined "modulo" H. In particular, if Λ is a full lattice, then $H = \{\underline{0}\}$, and $L = \hat{\Lambda}$ is uniquely determined. In that case L is called the dual lattice of Λ. Thus in the general situation $0 < k \leq n$ it is natural to call the decomposing lattices L as dual lattices of Λ.

Now we give a reformulation of Corollary 2.1 for bases of Λ, since this will prove to be useful later on. We shall need the following notion. Let $A = (\underline{a}_1, \dots, \underline{a}_k)$ be a system of linearly independent vectors in $\mathbb{R}^n$ $(0 < k \leq n)$. A system $B = (\underline{b}_1, \dots, \underline{b}_k)$ is called a dual system of A if

$$(\underline{b}_i, \underline{a}_j) = \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{otherwise} \end{cases} \quad (1 \leq i, j \leq k).$$

Note that B forms a linearly independent system. In particular, if $k = n$, i.e. A is a basis of $\mathbb{R}^n$, then B is the dual basis for A.

Corollary 2.2. *Let $A = (\underline{a}_1, \ldots, \underline{a}_k)$ be a basis of the lattice Λ. Then there is a one-to-one correspondence between the dual systems of A and the dual lattices of Λ. More precisely, every dual lattice L of Λ has a unique basis $B = (\underline{b}_1, \ldots, \underline{b}_k)$ which is a dual system of A.*

Proof. Let $B = (\underline{b}_1, \ldots, \underline{b}_k)$ be a dual basis of A. Observe that a system $B' = (\underline{b}'_1, \ldots, \underline{b}'_k)$ of vectors in $\mathbb{R}^n$ is a dual system of A if and only if

$$\underline{b}'_i = \underline{b}_i + \underline{h}_i \ \text{ with some } \underline{h}_i \in \Lambda^\perp \ (i = 1, \ldots, k).$$

Hence the statement is an immediate consequence of Corollary 2.1. □

The last property we give concerning dual lattices is the following. Note that, once again, this property is a generalization of the corresponding one from the classical case $k = n$.

Corollary 2.3. *Let L be a dual lattice of Λ. Then Λ is also a dual lattice of L.*

Proof. Using that $B = (\underline{b}_1, \ldots, \underline{b}_k)$ is a dual system of $A = (\underline{a}_1, \ldots, \underline{a}_k)$ if and only if A is a dual system of B, by the already known properties of dual lattices, one can easily check that $\hat{L} = \Lambda \oplus L^\perp$ holds. Hence the statement immediately follows. □

3. The norm $N_{p,q}$ in the general case

We start with extending the notion of the norm $N_{p,q}$ to bases of Λ. The reason is that later on, instead of lattices we will work with their bases. First, let $B = (\underline{b}_1, \ldots, \underline{b}_k)$ be a system of linearly independent vectors in $\mathbb{R}^n$. Then the p, q-size of the system B is defined by

$$|B|_{p,q} = ||\underline{b}_1|_p, \ldots, |\underline{b}_k|_p|_q.$$

As above, let Λ be a k-dimensional lattice in $\mathbb{R}^n$ (with $0 < k \leq n$), and let $A = (\underline{a}_1, \ldots, \underline{a}_k)$ be any basis for Λ. The p, q-norm $N_{p,q}(A)$ of the system A is defined in the following way:

$$N_{p,q}(A) = \min_B |B|_{p,q},$$

where B runs through all the dual systems of A.

Throughout the section, let $p, q \in \mathbb{R}^+ \cup \{\infty\}$ be fixed. Note that *a priori* it is not clear whether $N_{p,q}(A)$ and $N_{p,q}(\Lambda)$ exist or not, however, we shall show that these norms (i.e. the minima) always exist.

Theorem 3.1. *For any basis $A = (\underline{a}_1, \ldots, \underline{a}_k)$ of Λ, $N_{p,q}(A)$ exists.*

Proof. Calculate the vectors $\hat{\underline{a}}_1, \ldots, \hat{\underline{a}}_k$ having the following properties:

(i) for all $i, j \in \{1, \ldots, k\}$

$$(\underline{\hat{a}}_i, \underline{a}_j) = \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{otherwise,} \end{cases}$$

(ii) $\underline{\hat{a}}_i \perp \Lambda^\perp$, that is $(\underline{\hat{a}}_i, \underline{a}^\perp) = 0$ for all $\underline{a}^\perp \in \Lambda^\perp$ $(i = 1, \ldots, k)$.

For this procedure, and other standard methods used see e.g. the book of Pohst and Zassenhaus [Pohst and Zassenhaus 89]. Note that property (i) just means that $\hat{A} = (\underline{\hat{a}}_1, \ldots, \underline{\hat{a}}_k)$ is a dual system of A. In particular, by Corollary 2.2, $\hat{A}$ is a basis of a dual lattice of Λ. In fact property (ii) is not important for the proof of the present statement, however, the vectors $\underline{\hat{a}}_1, \ldots, \underline{\hat{a}}_k$ play an important role also later on. Observe that by Corollary 2.1 we have that $B = (\underline{b}_1, \ldots, \underline{b}_k)$ is a dual system of A if and only if

(8) $\underline{b}_i$ belongs to the hyperplane $\underline{\hat{a}}_i + \Lambda^\perp$ for any $i = 1, \ldots, k$.

For $1 \leq i \leq k$, let μ_i be the smallest non-negative real number such that $(\underline{\hat{a}}_i + \Lambda^\perp) \cap \mu_i G_p$ is non-empty, where G_p is the unit sphere with respect to the L_p-norm in $\mathbb{R}^n$. Since G_p is compact, hence μ_i exists. Let $\underline{b}_i^* \in (\underline{\hat{a}}_i + \Lambda^\perp) \cap \mu_i G_p$, and let $B = (\underline{b}_1, \ldots, \underline{b}_k)$ be any dual system of A. Then we have $|\underline{b}_i^*|_p \leq |\underline{b}_i|_p$, whence $|(|\underline{b}_1^*|_p, \ldots, |\underline{b}_k^*|_p)|_q \leq |(|\underline{b}_1|_p, \ldots, |\underline{b}_k|_p)|_q$. Thus $N_{p,q}(A)$ exists; in particular, we have

$$N_{p,q}(A) = |(|\underline{b}_1^*|_p, \ldots, |\underline{b}_k^*|_p)|_q.$$

□

Remark 2. From the proof of Theorem 3.1 it follows that the vectors $\underline{b}_1^*, \ldots, \underline{b}_k^*$ realizing the minimum $N_{p,q}(A)$ are independent of q.

Theorem 3.2. *Let Λ be a k-dimensional lattice of $\mathbb{R}^n$ (with $k \leq n$). Then for any positive real t, Λ has only finitely many bases of p, q-norm smaller than t, and these bases can be effectively determined.*

Proof. Let $A = (\underline{a}_1, \ldots, \underline{a}_k)$ be an arbitrary, but fixed basis of Λ. It is sufficient to "bound" all $k \times k$ unimodular matrices U such that $N_{p,q}(AU) < t$.

First observe that if U is a $k \times k$ unimodular matrix, then a system $B' = (\underline{b}'_1, \ldots, \underline{b}'_k)$ is a dual system for $A' = AU$ if and only if

$$B'^{tr} = U^{-1} \begin{pmatrix} \underline{b}_1 \\ \vdots \\ \underline{b}_k \end{pmatrix}$$

with some dual system $B = (\underline{b}_1, \dots, \underline{b}_k)$ of A. Thus by (8) we have

$$B'^{tr} = U^{-1} \begin{pmatrix} \underline{\hat{a}}_1 + \underline{h}_1 \\ \vdots \\ \underline{\hat{a}}_k + \underline{h}_k \end{pmatrix} = U^{-1} \begin{pmatrix} \underline{\hat{a}}_1 \\ \vdots \\ \underline{\hat{a}}_k \end{pmatrix} + \begin{pmatrix} \underline{h}'_1 \\ \vdots \\ \underline{h}'_k \end{pmatrix}$$

where $\underline{h}_1, \dots, \underline{h}_k, \underline{h}'_1, \dots, \underline{h}'_k \in \Lambda^\perp$. Here we used that $\Lambda^\perp$ is a subspace of $\mathbb{R}^n$. Write $b_{i,1}, \dots, b_{i,k}$ and $u_{i,1}, \dots, u_{i,k}$ for the entries of $\underline{b}'_i$ and the i-th row of U^{-1} for $i = 1, \dots, k$, respectively. Then by the above equality we have

$$\underline{b}'_i = u_{i,1}\underline{\hat{a}}_1 + \cdots + u_{i,k}\underline{\hat{a}}_k + \underline{h}'_i \quad (i = 1, \dots, k).$$

Observe that here $\underline{h}'_i$ is orthogonal to the vectors $\underline{\hat{a}}_1, \dots, \underline{\hat{a}}_k$. Thus by the theorem of Pythagoras we obtain

$$(9) \qquad |\underline{b}'_i|_2^2 = |u_{i,1}\underline{\hat{a}}_1 + \cdots + u_{i,k}\underline{\hat{a}}_k|_2^2 + |\underline{h}'_i|_2^2 \quad (i = 1, \dots, k).$$

On the other hand, letting B' be such that $|B'|_{p,q} = N_{p,q}(AU)$, we have

$$|(|\underline{b}'_1|_p, \dots, |\underline{b}'_k|_p)|_q < t$$

implying

$$(10) \qquad |\underline{b}'_i|_2 < c(p,q,n,t) \quad (i = 1, \dots, k).$$

Here $c(p,q,n,t)$ is a positive constant depending only on p, q, n, t, and we used the equivalence of the norms L_r over the space $\mathbb{R}^n$.

Now combining (9) and (10), noting that A is chosen to be arbitrary but fixed, we get

$$|u_{i,1}\underline{\hat{a}}_1 + \cdots + u_{i,k}\underline{\hat{a}}_k|_2 < c(p,q,n,t) \quad (i = 1, \dots, k).$$

Observe that this inequality means that for any $i = 1, \dots, k$, $u_{i,1}\underline{\hat{a}}_1 + \cdots + u_{i,k}\underline{\hat{a}}_k$ is a vector of a fixed lattice inside a bounded region. This implies that these vectors, whence all entries of U^{-1} can be effectively bounded and determined. Hence the same is true for all entries of U, and the theorem follows. □

Our next result, besides showing that $N_{p,q}(\Lambda)$ exists indeed, provides a tool for its explicit calculation, as well.

Theorem 3.3. *For any k-dimensional lattice Λ of $\mathbb{R}^n$ (with $0 < k \leq n$), $N_{p,q}(\Lambda)$ exists. Further, we have*

$$(11) \qquad N_{p,q}(\Lambda) = \min_A N_{p,q}(A),$$

where A runs through all the bases of Λ.

Proof. In view of Theorem 3.2 we know that the minimum on the right hand side of (11) exists. Let $A = (\underline{a}_1, \dots, \underline{a}_k)$ be a basis of Λ realizing this minimum. We only need to show that for any dual lattice Λ^* of Λ we have $|\Lambda^*|_{p,q} \geq N_{p,q}(A)$.

For this purpose let $B = (\underline{b}_1, \dots, \underline{b}_k)$ be a dual basis of A with

$$N_{p,q}(A) = |B|_{p,q} = |(|\underline{b}_1|_p, \dots, |\underline{b}_k|_p)|_q.$$

Let L be the dual lattice of Λ generated by $\underline{b}_1, \dots, \underline{b}_k$. Let $B' = (\underline{b}'_1 \dots, \underline{b}'_k)$ be any other basis of L. Then by Corollaries 2.2 and 2.3, we can take a basis $\underline{a}'_1, \dots, \underline{a}'_k$ of Λ such that B' is a dual system of A'. This by the minimality of $N_{p,q}(A)$ gives

$$|(|\underline{b}_1|_p, \dots, |\underline{b}_k|_p)|_q = N_{p,q}(A) \leq N_{p,q}(A') \leq |(|\underline{b}'_1|_p, \dots, |\underline{b}'_k|_p)|_q.$$

Hence for the size of L we obtain that

$$|L|_{p,q} = |(|\underline{b}_1|_p, \dots, |\underline{b}_k|_p)|_q = N_{p,q}(A).$$

Let now Λ^* be any dual lattice of Λ, and take a basis $\underline{b}^*_1, \dots, \underline{b}^*_k$ in Λ^* such that

$$|\Lambda^*|_{p,q} = |(|\underline{b}^*_1|_p, \dots, |\underline{b}^*_k|_p)|_q.$$

Take a basis $A^* = (\underline{a}^*_1, \dots, \underline{a}^*_k)$ in Λ such that $B^* = (\underline{b}^*_1, \dots, \underline{b}^*_k)$ is a dual system of A^*. Then using again the minimality of $N_{p,q}(A)$ we have

$$|\Lambda^*|_{p,q} = |B^*|_{p,q} \geq N_{p,q}(A^*) \geq N_{p,q}(A).$$

Thus we conclude that for an arbitrary dual lattice Λ^* of Λ

$$|\Lambda^*|_{p,q} \geq |L|_{p,q}$$

is valid. This proves that $N_{p,q}(\Lambda)$ exists, and $N_{p,q}(\Lambda) = |L|_{p,q}$. Further, we also have

$$N_{p,q}(\Lambda) = N_{p,q}(A),$$

and the theorem is proved. □

Remark 3. Since the proofs of the previous results are constructive, we obtain an algorithm for the determination of the norm $N_{p,q}(\Lambda)$ for all p, q. This can be given in the following way.

3.1. **Algorithm 0 - $N_{p,q}$.** Execute the following steps.

(A0.1) Let $A = (\underline{a}_1, \dots, \underline{a}_k)$ be any basis of Λ. Determine the value $N_{p,q}(A)$ by using Theorem 3.1.

(A0.2) Determine all bases A^* of Λ using Theorem 3.2 which satisfy $N_{p,q}(A^*) \leq N_{p,q}(A)$.

(A0.3) Choose that basis from those obtained in Step (A0.2) for which $N_{p,q}(A^*)$ is minimal. Then $N_{p,q}(\Lambda) = N_{p,q}(A^*)$.

Although Algorithm 0 theoretically finds $N_{p,q}(\Lambda)$, it is not efficient from a practical point of view. Especially, Step (A0.2) is very time-consuming. In the following two sections we investigate the problem of developing substantially more efficient algorithms for determining $N_{p,q}$ in two special cases, namely for $(p,q) = (2,\infty)$ and $(1,\infty)$.

4. The case $(p,q) = (2,\infty)$

In this case the norm $N_{2,\infty}(A)$ for any basis $A = (\underline{a}_1,\dots,\underline{a}_k)$ of Λ can be immediately obtained.

Lemma 4.1. *For any basis $A = (\underline{a}_1,\dots,\underline{a}_k)$ of Λ we have*

$$N_{2,\infty}(A) = |(|\underline{\hat{a}}_1|_2,\dots,|\underline{\hat{a}}_k|_2)|_\infty,$$

where the vectors $\underline{\hat{a}}_1,\dots,\underline{\hat{a}}_k$ are defined in the proof of Theorem 3.1

Proof. Since $|\underline{\hat{a}}_i|_2 \leq |\underline{b}_i|_2$ holds for all $\underline{b}_i \in \underline{\hat{a}}_i + \Lambda^\perp$, the statement trivially follows. □

Remark 4. Lemma 4.1 holds for arbitrary values of q, not only for $q = \infty$.

Now we indicate how one could approximate efficiently $N_{2,\infty}(\Lambda)$ for any lattice Λ. Take an arbitrary basis $A = (\underline{a}_1,\dots,\underline{a}_k)$ of Λ. Then by Lemma 4.1 with the basis $\hat{A} = (\underline{\hat{a}}_1,\dots,\underline{\hat{a}}_k)$ we have $N_{2,\infty}(A) = |\hat{A}|_{2,\infty}$. Further, writing Λ^* for the lattice generated by $\hat{A}$, by the choice of the vectors in $\hat{A}$ in the proof of Theorem 3.1 we see that Λ^* is contained in the orthogonal complement subspace of $\Lambda^\perp$. Since it is valid for any basis of Λ, one can easily check that $N_{2,\infty}(\Lambda) = |\Lambda^*|_{2,\infty}$ with the particular Λ^* defined above. Thus a basis reduction (starting from $\hat{A}$) yielding a "small" basis of the lattice Λ^*, provides a good approximation of $N_{2,\infty}(\Lambda)$. For this purpose the LLL-algorithm ([Lenstra et al. 82], see also [Pohst and Zassenhaus 89]) can be efficiently used. Note that this approach works for any value of q, not only for $q = \infty$.

Now we give a heuristic method for which there is no guarantee to work. However, if it does, it gives $N_{2,\infty}(\Lambda)$ very quickly.

4.1. **Algorithm 1 - $N_{2,\infty}$.**

Starting with an arbitrary basis $\underline{a}_1,\dots,\underline{a}_k$ of Λ, execute the following steps.

(A1.1) Find the vectors $\underline{\hat{a}}_1,\dots,\underline{\hat{a}}_k$ as in the proof of Theorem 3.1.

(A1.2) Compute the successive minima and the corresponding vectors $\underline{b}_1,\dots,\underline{b}_k$ of the lattice L generated by $\underline{\hat{a}}_1,\dots,\underline{\hat{a}}_k$.

(A1.3) Check whether $\underline{b}_1,\dots,\underline{b}_k$ form a basis of L or not, by computing whether the determinant of the basis transformation matrix is ±1.

(A1.4) If this is not the case then output a failure message and terminate. Otherwise, output $N_{2,\infty}(\underline{b}_1, \dots, \underline{b}_k)$.

If $\underline{b}_1, \dots, \underline{b}_k$ form a basis, then by Lemma 4.1 we have $N_{2,\infty}(\Lambda) = N_{2,\infty}(\underline{b}_1, \dots, \underline{b}_k)$. Actually, this happens in all the cases we have considered. It is not surprising, since we have used lattices related to number fields, and such lattices behave nicely in general. However, it is well-known that it may happen that the successive minima vectors do not form a basis of the lattice (see e.g. [Pohst and Zassenhaus 89]). In that situation we should switch back to Algorithm 0, with $p = 2$ and $q = \infty$.

5. The case $(p, q) = (1, \infty)$

For this choice of p and q the situation is more complicated. In what follows, we develop a method for finding the norm $N_{1,\infty}(\Lambda)$ of a lattice Λ. Note that in view of Theorem 3.3, we know that $N_{1,\infty}(\Lambda)$ always exists.

We need to find a system $B = (\underline{b}_1, \dots, \underline{b}_k)$ (a dual system for some basis A of Λ) such that

$$|B|_{1,\infty} = \max(|\underline{b}_1|_1, \dots, |\underline{b}_k|_1) = N_{1,\infty}(\Lambda).$$

We shall in fact construct such a system B. The first algorithm we give is an adaptation of Algorithm 1 to this case.

5.1. **Algorithm 2a -** $N_{1,\infty}$**.** We heuristically expect that the basis obtained in Algorithm 1 is the one that corresponds to the norm $N_{1,\infty}$, too. Therefore after executing the first three steps (which are the same as in Algorithm 1), we continue with this basis and do further examinations. So starting with some rows $\underline{a}_1, \dots, \underline{a}_k$ of Λ, execute the following steps.

(A2a.1) Find the vectors $\hat{\underline{a}}_1, \dots, \hat{\underline{a}}_k$ as in the proof of Theorem 3.1.

(A2a.2) Compute the successive minima and the corresponding vectors $\underline{b}_1, \dots, \underline{b}_k$ of the lattice L generated by $\hat{\underline{a}}_1, \dots, \hat{\underline{a}}_k$.

(A2a.3) Check whether $\underline{b}_1, \dots, \underline{b}_k$ form a basis of L or not, i.e., compute whether the determinant of the basis transformation matrix is ± 1.

(A2a.4) If this does not hold then output a failure message and terminate. Otherwise, continue with the following steps.

(A2a.5) By Lemma 5.1, calculate the norm of the system $\underline{b}_1, \dots, \underline{b}_k$. That is, for all $i = 1, \dots, k$ find the norm of the shortest vector in $\underline{b}_i + \Lambda^\perp$, with respect to $|.|_1$. Observe that since the intersection of $\underline{b}_i + \Lambda^\perp$ and the set $\{\underline{x} \in \mathbb{R}^n \ : \ |\underline{x}|_1 \leq 1\}$ is a convex polytope, it can be done by solving a standard linear programming problem. Take the maximum of these norms, this is the norm $N_{1,\infty}(\underline{b}_1,\dots,\underline{b}_k)$.

(A2a.6) Find all "short vectors" in the lattice whose Euclidean lengths are between the largest successive minimum and $N_{1,\infty}(\underline{b}_1,\dots,\underline{b}_k)$.

(A2a.7) For all "short vectors" $\underline{b}$ find the norm of the shortest vector in $\underline{b}+\Lambda^{\perp}$ with respect to $|.|_1$. If these norms are $\geq N_{1,\infty}(\underline{b}_1,\dots,\underline{b}_k)$ then set the value of the logical variable "MINIMAL" as "true"; otherwise put MINIMAL:=false.

(A2a.8) Output the vectors $\underline{b}_1,\dots,\underline{b}_k$, the norm $N_{1,\infty}(\underline{b}_1,\dots,\underline{b}_k)$, and the variable MINIMAL.

Actually, the vectors $\underline{b}_1,\dots,\underline{b}_k$ obtained in step (A2a.2) do form a basis in all the cases we have considered. However, as we have mentioned already, it is not guaranteed: in such cases we should return to Algorithm 0, with $p=1$ and $q=\infty$.

If the output value of MINIMAL is "true", then we have $N_{1,\infty}(\Lambda) = N_{1,\infty}(\underline{b}_1,\dots,\underline{b}_k)$. Otherwise our algorithm fails to find the norm $N_{1,\infty}(\Lambda)$. Unfortunately, it happens several times. (Though note that the value of the norm $N_{1,\infty}(\underline{b}_1,\dots,\underline{b}_k)$ provided by the algorithm is not too far from $N_{1,\infty}(\Lambda)$. This can be easily seen from the inequalities between the norms $|.|_1$ and $|.|_2$.) However, even if the algorithm does find the norm $N_{1,\infty}(\Lambda)$, it has to list a lot of "short vectors" in Step (A2a.6) (which can be done by the method of Fincke and Pohst [Fincke and Pohst 85]), and finding them is very time-consuming. It means that the algorithm is not efficient enough, therefore we develop another one.

First we prove three statements, which form the basis of this new algorithm.

Let H be a subspace of $\mathbb{R}^n$ and $\underline{b} \in \mathbb{R}^n$ be a non-zero vector being orthogonal to H, and write $T = \underline{b} + H$. Further, write H^* for the subspace

$$H^* = \{t\underline{b} + \underline{h} \ \mid t \in \mathbb{R}, \underline{h} \in H\}.$$

The first theorem gives a method to find the shortest element of T with respect to $|.|_1$.

Lemma 5.1. *Let $\underline{e}$ be a vector in H^* of the form $\underline{e} = t_0\underline{b} + \underline{h}$ with some $t_0 > 0$ and $\underline{h} \in H$ such that $|\underline{e}|_1 = 1$ and t_0 is maximal with this property. Then $\underline{b}_0 = \underline{e}/t_0$ is the shortest element of T with respect to $|.|_1$, with $|\underline{b}_0|_1 = 1/t_0$.*

Proof. Obviously, $\underline{e}$ is well defined, and $\underline{b}_0 \in H^*$. Suppose that $\underline{b}' \in T$ and $|\underline{b}'|_1 = c < 1/t_0 = |\underline{b}_0|_1$. Write $\underline{b}' = \underline{b} + \underline{h}'$. Then letting $\underline{e}' = \underline{b}'/c$ we have both $|\underline{e}'|_1 = 1$ and $\underline{e}' = (1/c)\underline{b} + (1/c)\underline{h}'$, which by $1/c > t_0$ contradicts the definition of t_0. Hence the assertion follows. □

The next statement shows that the shortest vector in T w.r.t. $|.|_1$ cannot be "too short".

Lemma 5.2. *For any* $\underline{b}' \in T$ *we have* $|\underline{b}'|_1 \geq |\underline{b}|_2$.

Proof. Since $\underline{b}$ is orthogonal to H, it is the shortest vector in T w.r.t. $|.|_2$. Hence for any $\underline{b}' \in T$ we have

$$|\underline{b}'|_1 \geq |\underline{b}'|_2 \geq |\underline{b}|_2,$$

and the proof is complete. □

Let now $\underline{b}_1, \dots, \underline{b}_k$ be linearly independent vectors in $\mathbb{R}^n$. The third statement shows that if a linear combination of these vectors is "short" w.r.t. $|.|_2$, then the coefficient vector must also be "short".

Lemma 5.3. *Let* $\underline{a} = \lambda_1 \underline{b}_1 + \dots + \lambda_k \underline{b}_k$ *be a linear combination of* $\underline{b}_1, \dots, \underline{b}_k$ *with some* $\lambda_1, \dots, \lambda_k \in \mathbb{R}$, *such that* $|\underline{a}|_2 < c$ *with some positive real number* c. *Then we have*

$$|\underline{\lambda}|_2 < c\sqrt{\mu},$$

where $\underline{\lambda} = (\lambda_1, \dots, \lambda_k)$ *and* μ *is the largest eigenvalue of the matrix* $R^{tr}R$. *Here* R *is the inverse of the matrix*

$$S = (\underline{b}_1, \dots, \underline{b}_k).$$

Proof. Observe that we have $\underline{a} = S\underline{\lambda}$, whence $R\underline{a} = \underline{\lambda}$. Thus writing $||R||$ for the operator norm of R, i.e., $||R|| = \sup_{|\underline{x}|_2 \leq 1} |R\underline{x}|_2$, and using the well-known assertion $||R|| = \sqrt{\mu}$, we get

$$|\underline{\lambda}|_2 = |R\underline{a}|_2 \leq ||R|| \cdot |\underline{a}|_2 = \sqrt{\mu}|\underline{a}|_2 < c\sqrt{\mu},$$

and the statement follows. □

5.2. **Algorithm 2b -** $N_{1,\infty}$. Starting for any rows $\underline{a}_1, \dots, \underline{a}_k$ of Λ, execute the following steps.

(A2b.1) Find the vectors $\hat{\underline{a}}_1, \dots, \hat{\underline{a}}_k$ as in the proof of Theorem 3.1. Initially, put $B = (\hat{\underline{a}}_1, \dots, \hat{\underline{a}}_k)$.

(A2b.2) By Lemma 5.1, calculate the norm $N_{1,\infty}$ of this system. Write c for this value.

(A2b.3) Observe that by Lemma 5.2, if the actual system $B = (\underline{b}_1, \dots, \underline{b}_k)$ is not best possible, then there exists an unimodular matrix U, such that for the system $B' = (\underline{b}'_1, \dots, \underline{b}'_k)$ with $B'^{tr} = UB^{tr}$, $|\underline{b}'_i|_2 < c$ holds for all $i = 1, \dots, k$. Then by Lemma 5.3, we get that the $|.|_2$-norm of each row of U is $< c\sqrt{\mu}$. Checking all possible matrices U, we find the best basis B, and hence also the norm $N_{1,\infty}(\Lambda)$.

(a) Actually, we start by checking special matrices U who differ from the identity matrix in only one row. This row contains 1 as the main diagonal entry and all the other entries are zeros except for one value. The absolute value of the exceptional entry is smaller than $\sqrt{c^2\mu - 1}$. (That is, the absolute value of the exceptional entry is chosen not to violate the property that the $|.|_2$-norm of each row of U is $< c\sqrt{\mu}$.)

(b) After doing Step (A2b.3)(a) as many times as possible, we check the unimodular matrices U of general shape having the property that the $|.|_2$-norm of each row is $< c\sqrt{\mu}$.

Step (A2b.3)(a) is the heart of the algorithm. Practically speaking Step (A2b.3)(a) means that we would like to change the longest basis vector to another one which is a sum of this vector and a constant multiple of another basis vector. This can be done very quickly every time. We expect that after doing so as many times as possible, the basis obtained gives the norm $N_{1,\infty}$ of the lattice. Actually, this really happens in the considered cases, and it is demonstrated in Step (A2b.3)(b). Indeed, after executing Step (A2b.3)(b), in each considered case we get the same basis as after executing Step (A2b.3)(a). Note that Step (A2b.3)(b) is very time-consuming but must be done to have all possible bases checked that can give the norm $N_{1,\infty}$ of the lattice. In contrast with Algorithm 2a, Algorithm 2b never fails to find $N_{1,\infty}(\Lambda)$.

6. Examples

In our numerical investigations we work with lattices corresponding to the unit group of number fields and random lattices with real and integer entries. We apply the algorithms given in the previous sections to compute the norms $N_{1,\infty}$ and $N_{2,\infty}$ of the lattices under consideration. The algorithms were implemented in the computer algebra package MAGMA and were run on a PC having two INTEL XEON 3.00 GHz processors. Thus the comparison of the efficiency of the different methods is realistic.

Let $\mathbb{K}$ be an algebraic number field of degree n. We have s real and t pairs of complex embeddings $\mathbb{K} \to \mathbb{C}$ with $n = s + 2t$. Order them as $\sigma_1, \ldots, \sigma_s$ being the real ones and $\sigma_{s+1}, \overline{\sigma_{s+1}}, \ldots, \sigma_{s+t}, \overline{\sigma_{s+t}}$ being the pairs of complex ones. For $\alpha \in \mathbb{K}$ write

$$|\alpha^{(i)}| = \begin{cases} |\sigma_i(\alpha)|, & \text{for } i = 1, \ldots, s, \\ |\sigma_i(\alpha)|^2, & \text{for } i = s+1, \ldots, s+t. \end{cases}$$

The units of the ring of integers of $\mathbb{K}$ form a group. As is well-known, this group is finitely generated of rank $r = s + t - 1$. Therefore any unit $\eta \in U_{\mathbb{K}}$ can be written as

$$\eta = \varepsilon_0^{b_0} \varepsilon_1^{b_1} \cdots \varepsilon_r^{b_r}.$$

Here $\varepsilon_1, \ldots, \varepsilon_r$ is a fundamental system of units and ε_0 is a primitive root of unity in $\mathbb{K}$. The lattice corresponding to the unit group of $\mathbb{K}$ is generated by the vectors $\left(\log|\varepsilon_i^{(1)}|, \ldots, \log|\varepsilon_i^{(r+1)}|\right)$, $(i = 1, \ldots, r)$.

In Subsections 6.1 and 6.2 we present our results concerning these unit lattices for maximal real subfields of cyclotomic fields and number fields of the form $\mathbb{Q}(\sqrt[n]{2})$, respectively. In both cases we use Algorithm 1, Algorithm 2a and Algorithm 2b described in the previous sections to find $N_{2,\infty}$ and $N_{1,\infty}$ of the lattices in question. We summarize the results of our computations in Tables 1-6.

In Subsection 6.3 we consider a large number of random lattices with integer entries. In the random case we used again the algorithms described in Subsections 4.1, 5.1 and 5.2 to find $N_{2,\infty}$ and $N_{1,\infty}$ of the lattices in question, respectively.

6.1. **Maximal real subfields of cyclotomic fields.** Let $\mathbb{Q}(\zeta_n)$ denote the n-th cyclotomic field ($n > 2$), i.e. the field obtained by adjoining a primitive n-th root of unity ζ_n to the rational numbers. Note that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, where $\varphi(n)$ denotes Euler's totient function. The maximal real subfield of $\mathbb{Q}(\zeta_n)$ is $\mathbb{Q}(\zeta_n)^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ which is of degree $\varphi(n)/2$. Consider the unit lattice of $\mathbb{Q}(\zeta_n)^+$. Note that the unit rank is $\varphi(n)/2 - 1$ since we have only real embeddings. We summarize the results of our computations in Tables 1-3.

In Table 1 in distinct columns the value of n, the rank of the lattice Λ in question, the norm $N_{2,\infty}(\Lambda)$ obtained by Algorithm 1 and the processing time in each case are given.

In distinct columns of Table 2 we indicate the value of n, the rank of the lattice Λ in question, whether the vectors corresponding to the successive minima form a basis or not, whether the vectors corresponding to the successive minima form a basis of minimal norm or not, (to be more precise, this means, that the "successive basis" is of minimal norm if the algorithm finds that there are no "short vectors" whose norm $|.|_1$ is smaller than this value; however, as it will be seen later, sometimes it happens that the "successive basis" is the optimal basis, but the algorithm cannot prove this), the norm $N_{1,\infty}$ obtained by Algorithm 2a and corresponding to the "successive basis", and the processing time, respectively. The table shows that in about one quarter of the cases Algorithm 2a does not solve the problem of finding the norm $N_{1,\infty}$ of

n	Rank of Λ	$N_{2,\infty}$	Time (sec)	n	Rank of Λ	$N_{2,\infty}$	Time (sec)
5	1	1.469	0.02	15	3	1.039	0.11
7	2	1.126	0.02	16	3	0.709	0.25
8	1	0.802	0.00	17	7	0.597	7.71
9	2	0.886	0.02	18	2	0.886	0.01
10	1	1.469	0.01	19	8	0.559	4.32
11	4	0.798	0.33	20	3	1.039	0.11
12	1	0.537	0.02	21	5	0.874	0.69
13	5	0.711	0.49	22	4	0.798	0.33
14	2	1.126	0.02				

Table 1. The norm $N_{2,\infty}$ of the unit lattices of maximal real subfields of cyclotomic fields using Algorithm 1

the lattice, i.e., the norm corresponding to the "successive basis" is not best possible. Therefore we needed to develop another method.

As it can be seen from Table 3, Algorithm 2b fulfills the required task, i.e., it finds the norm of the lattice in all the cases. Table 3 contains the following data: the value of n, the rank of the lattice Λ in question, the initial norm obtained in Step (A2b.2), the number of iterations in Step (A2b.3)(a) required to find the optimal basis. We mention here that Step (A2b.3)(b) never provides a smaller norm than the one obtained in Step (A2b.3)(a), however, it must be executed. We remark that we stopped the computations in Algorithm 2b at $n = 22$ because of time consumption problems. The rows of $n = 20$ in Tables 2 and 3 show that both algorithms actually find the optimal basis but it is not proved by Algorithm 2a, it is done only by Algorithm 2b.

6.2. **Unit lattice of $K = \mathbb{Q}(\sqrt[n]{2})$.** Consider the unit lattice of the number field $K = \mathbb{Q}(\sqrt[n]{2})$. Now the unit rank is $\lfloor n/2 \rfloor$, since we have one or two real embeddings depending on the parity of n and all the other embeddings are complex ones. We summarize the results of our computations in Tables 4-6. We remark that we stopped the computations at $n = 17$ because of time consumption problems in Algorithm 2b. Tables 4-6 contain the same type of data as Tables 1-3. It is obvious from the tables that we could go further with the value of n with Algorithm 2b. Indeed, Algorithm 2a caused a memory overflow already in case of $n = 15$. Furthermore, we can see e.g. from the rows

n	Rank of Λ	Basis?	Of minimal norm?	Norm $N_{1,\infty}$ of the successive basis	Time (sec)
5	1	yes	no	2.159	0.01
7	2	yes	yes	1.541	0.02
8	1	yes	yes	1.135	0.01
9	2	yes	yes	1.245	0.02
10	1	yes	no	2.159	0.01
11	4	yes	yes	1.356	0.38
12	1	yes	yes	0.759	0.01
13	5	yes	yes	1.410	0.84
14	2	yes	yes	1.541	0.02
15	3	yes	yes	2.078	0.15
16	3	yes	no	1.166	0.25
17	7	yes	yes	1.284	24.28
18	2	yes	yes	1.245	0.03
19	8	yes	yes	1.344	288.11
20	3	yes	no	2.078	0.14
21	5	yes	yes	1.763	1.29
22	4	yes	yes	1.356	0.38

Table 2. Result of Algorithm 2a in case of maximal real subfields of cyclotomic fields

of $n = 13, 14$ in Tables 5 and 6 that even when both programs solve the problem, Algorithm 2b is much faster than Algorithm 2a.

6.3. **Random lattices.** We considered a large number of random lattices of rank k in $\mathbb{Z}^n$ $(0 < k \leq n)$ with entries of the lattice vectors in the range $[-10, 10]$. We started with running both Algorithms 2a and 2b and it turned out that Algorithm 2a is much slower and less efficient also in this case. Therefore we used Algorithm 2b in our computations.

We considered pairs (n, k) that satisfy $5 \leq n \leq 10$ and $n - 4 \leq k \leq n - 1$. For each pair (n, k) we generated 1000 random lattices and ran Algorithm 2b for them. The outputs were evaluated by the program Microsoft Excel. Since the cases are similar to each other, we show only one example. Let $n = 7$ and $k = 5$. Figure 1 is a histogram which shows the frequencies of the distinct values of the number of iterations needed in Step (A2b.3)(a) to calculate $N_{1,\infty}(\Lambda)$. It seems that the diagram (as well as the diagrams obtained for other values of n and k) follows a normal distribution.

n	Rank of Λ	Initial norm obtained in Step (A2b.2)	No. of iterations in Step (A2b.3)(a)	$N_{1,\infty}$	Time (sec)
5	1	2.078	0	2.078	0.01
7	2	1.541	0	1.541	0.02
8	1	1.135	0	1.135	0.01
9	2	1.245	0	1.245	0.03
10	1	2.078	0	2.078	0.01
11	4	1.608	3	1.356	0.60
12	1	0.759	0	0.759	0.02
13	5	1.946	5	1.410	2.15
14	2	1.541	0	1.541	0.03
15	3	2.078	0	2.078	0.20
16	3	1.166	2	1.135	0.31
17	7	1.910	8	1.284	75.64
18	2	1.245	0	1.245	0.03
19	8	1.873	15	1.344	1091.30
20	3	2.078	0	2.078	0.21
21	5	2.040	3	1.763	4.16
22	4	1.608	3	1.356	0.57

Table 3. The norm $N_{1,\infty}$ of the unit lattices of maximal real subfields of cyclotomic fields using Algorithm 2b

7. Acknowledgement

The authors are grateful to the referee for his/her helpful and useful suggestions to improve the presentation of the paper considerably.

References

[Bosma et al. 97] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language.*, J. Symbolic Comput. **24** (1997), 235–265.

[Fincke and Pohst 85] U. Fincke and M. Pohst, *Improved methods for calculating vectors of short length in a lattice, including a complexity analysis*, Math. Comp. **44** (1985), 463–471.

[Hajdu 09] L. Hajdu, *Optimal systems of fundamental S-units for LLL-reduction*, Period. Math. Hungar. **59** (2009), 79–105.

[Kannan and Lovász 88] R. Kannan and L. Lovász, *Covering minima and lattice-point-free convex bodies*, Ann. of Math. **128** (1988), 577–602.

[Lekkerkerker 69] C. G. Lekkerkerker, Geometry of numbers, North-Holland Publishing Company, 1969.

[Lenstra et al. 82] A.K. Lenstra, H.W. Lenstra, Jr. and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 515–534.

n	Rank of Λ	$N_{2,\infty}$	Time (sec)	n	Rank of Λ	$N_{2,\infty}$	Time (sec)
2	1	0.802	0.02	10	5	0.344	1.12
3	1	0.525	0.02	11	5	0.289	1.71
4	2	0.546	0.03	12	6	0.329	1.65
5	2	0.419	0.17	13	6	0.262	3.11
6	3	0.438	0.07	14	7	0.296	12.36
7	3	0.350	1.59	15	7	0.245	3.71
8	4	0.397	0.41	16	8	0.280	56.72
9	4	0.321	0.58	17	8	0.232	63.62

Table 4. The norm $N_{2,\infty}$ of the unit lattices of fields $\mathbb{Q}(\sqrt[n]{2})$ using Algorithm 1

n	Rank of Λ	Basis?	Of minimal norm?	Norm $N_{1,\infty}$ of the successive basis	Time (sec)
2	1	yes	yes	1.135	0.02
3	1	yes	yes	0.742	0.02
4	2	yes	yes	0.772	0.03
5	2	yes	yes	0.592	0.18
6	3	yes	yes	0.742	0.11
7	3	yes	yes	0.588	1.66
8	4	yes	yes	0.651	0.73
9	4	yes	yes	0.548	1.38
10	5	yes	no	0.743	8.52
11	5	yes	no	0.543	15.06
12	6	yes	no	0.743	134.10
13	6	yes	no	0.503	255.80
14	7	yes	no	0.700	3977.23

Table 5. Result of Algorithm 2a in case of fields $\mathbb{Q}(\sqrt[n]{2})$

[Pohst and Zassenhaus 89] M. Pohst and H. Zassenhaus, Algorithmic Algebraic Number Theory, Cambridge Univ. Press, 1989.

[Schnell 92] U. Schnell, *Minimal determinants and lattice inequalities*, Bull. London Math. Soc. **24** (1992), 606-612.

n	Rank of Λ	Initial norm obtained in Step (A2b.2)	No. of iterations in Step (A2b.3)(a)	$N_{1,\infty}$	Time (sec)
2	1	1.135	0	1.135	0.01
3	1	0.742	0	0.742	0.00
4	2	0.817	1	0.772	0.02
5	2	0.592	0	0.592	0.02
6	3	0.883	1	0.742	0.04
7	3	0.588	0	0.588	0.05
8	4	0.705	1	0.651	0.19
9	4	0.566	1	0.548	0.31
10	5	0.651	3	0.620	1.9
11	5	0.543	1	0.526	2.55
12	6	0.755	8	0.678	143.03
13	6	0.503	0	0.503	32.66
14	7	0.696	4	0.594	297.69
15	7	0.565	3	0.504	311.97
16	8	0.769	8	0.585	15973.09
17	8	0.581	2	0.464	5833.39

Table 6. The norm $N_{1,\infty}$ of the unit lattices of fields $\mathbb{Q}(\sqrt[n]{2})$ using Algorithm 2b

L. Hajdu
University of Debrecen, Institute of Mathematics
H-4010 Debrecen, P.O. Box 12.
Hungary
E-mail address: hajdul@science.unideb.hu

T. Kovács
University of Debrecen, Institute of Mathematics
H-4010 Debrecen, P.O. Box 12.
Hungary
E-mail address: tkovacs@science.unideb.hu

A. Pethő
University of Debrecen, Department of Computer Science
H-4010 Debrecen, P.O. Box 12.
Hungary
E-mail address: Petho.Attila@inf.unideb.hu

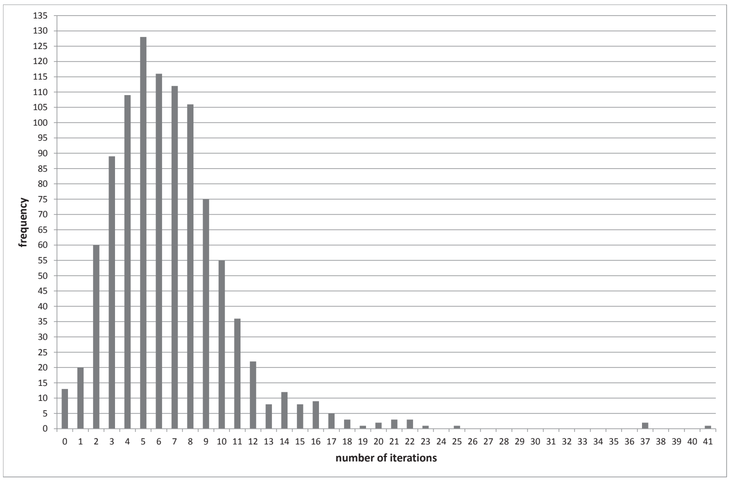

Figure 1. Number of iterations needed to calculate $N_{1,\infty}$ for random lattices of rank $k = 5$ in $\mathbb{Z}^7$

M. Pohst
Institut für Mathematik MA 8-1
Technische Universität Berlin
Straße des 17. Juni 136
10623 Berlin
Germany
E-mail address: pohst@math.tu-berlin.de