Constructing lattice bases by means of approximations

Christoph Thiel

Fachbereich Medien
Fachhochschule Düsseldorf – University of Applied Sciences
Josef-Gockeln-Straße 9
D-40477 Düsseldorf
Germany

Abstract. The construction of a basis of a certain lattice of interest is a basic tool in many fields of algorithmic number theory. All too often we can not compute with the original lattices because of irrational numbers involved but have to work with approximations of them. While helpful bounds were shown about the reduction of lattice bases in [2], here we introduce the notion of a (ϵ, δ)-constructable basis of a lattice and determine the precision of vectors that is necessary to extend a set to a (ϵ, δ)-constructable basis.

1 Preliminaries and tools

Thorough this paper let m, n, i, j, k, l and q, p always be natural numbers. For $\mathbf{a}, \mathbf{b} \in \mathbb{R}^m$ we denote by $\langle \mathbf{a}, \mathbf{b} \rangle = \sum_{i=1}^{m} a_i b_i$ the inner product of $\mathbf{a}$ and $\mathbf{b}$. The euclidean norm or length of $\mathbf{a} \in \mathbb{R}^m$ is defined to be $\|\mathbf{a}\|_2 = \sqrt{\langle \mathbf{a}, \mathbf{a} \rangle}$. We shall also use the maximum norm of the vector $\mathbf{a}$, given by $\|\mathbf{a}\|_\infty = \max\{|\mathbf{a}_i| : 1 \le i \le m\}$. We simply write $\mathsf{A} = (a_{i,j}) \in S^{m \times k}$, when we want to state that A is a $m \times k$-matrix with coefficients $a_{i,j}$ belonging to a set $S \subseteq \mathbb{C}$ $(1 \le i \le m,\ 1 \le j \le k)$. We also write $\mathsf{A} = [\mathbf{a}_1, \ldots, \mathbf{a}_k]$, if $\mathbf{a}_j \in S^m$ denotes the j-th column vector of A. Finally, we denote the length of the shortest column vector of A by $\lambda(\mathsf{A})$.

In this work we will use several matrix norms. The first is the *Frobenius norm*, defined by $\|\mathsf{A}\|_\mathrm{f} = \left(\sum_{i=1}^{m} \sum_{j=1}^{k} a_{i,j}^2 \right)^{1/2}$. We also mention the *maximum entry norm* of the matrix A, given by $\|\mathsf{A}\|_\infty = \max\{|a_{i,j}| : 1 \le i \le m,\ 1 \le j \le k\}$, and the *spectral norm* $\|\mathsf{A}\|_2$, which is the largest singular value of A. For properties of those norms we refer to [6].

Let Λ be a lattice in the real euclidean space $\mathbb{R}^n$. For convenience, we shall often consider a basis of Λ as a matrix consisting of the vectors of the basis. Let $\lambda_i(\Lambda)$ denote the i-th successive minimum of Λ and let γ_k be the k-th Hermite constant. It can easily be shown that we have

$$\gamma_k \le k\,. \tag{1}$$

Theorem 1. *Let $n \in \mathbb{N}$, and let Λ be a lattice of dimension n in $\mathbb{R}^n$. Then $\prod_{i=1}^{n} \lambda_i(\Lambda) \leq \gamma_n^{\frac{n}{2}} \det(\Lambda)$. Especially, we have*

$$\lambda_1(\Lambda) \leq \gamma_n^{\frac{1}{2}} \det(\Lambda)^{\frac{1}{n}} . \tag{2}$$

Definition 2. *Let $(\mathbf{a}_1, \ldots, \mathbf{a}_k)$ be a sequence of linearly independent vectors in $\mathbb{R}^m$. Then the sequence $(\mathbf{a}_1^\star, \ldots, \mathbf{a}_m^\star)$ of their* Gram-Schmidt vectors *is defined by $\mathbf{a}_1^\star = \mathbf{a}_1$ and $\mathbf{a}_i^\star = \mathbf{a}_i - \sum_{j=1}^{i-1} \frac{\langle \mathbf{a}_i, \mathbf{a}_j^\star \rangle}{\langle \mathbf{a}_j^\star, \mathbf{a}_j^\star \rangle} \mathbf{a}_j^\star$*

In the following lemma we summarize some properties of Gram-Schmidt vectors we shall often refer to. Their proofs can be found for example in [7].

Lemma 3. *Let $(\mathbf{a}_1, \ldots, \mathbf{a}_k)$ be a sequence of linearly independent vectors in $\mathbb{R}^m$. Then the vectors $\mathbf{a}_1^\star, \ldots, \mathbf{a}_k^\star$ are mutually orthogonal. For $1 \leq i \leq k$ the vector $\mathbf{a}_i^\star$ is the orthogonal projection of $\mathbf{a}_i$ onto $\operatorname{span}(\mathbf{a}_1, \ldots, \mathbf{a}_{i-1})^\perp$, and we have*

$$\langle \mathbf{a}_i^\star, \mathbf{a}_i^\star \rangle = \langle \mathbf{a}_i^\star, \mathbf{a}_i \rangle , \quad \text{and} \quad \|\mathbf{a}_i^\star\|_2 \leq \|\mathbf{a}_i\|_2 . \tag{3}$$

Moreover, let $\mathbf{c} = \sum_{i=1}^{k} x_i \mathbf{a}_i$, where $x_i \in \mathbb{R}$ for $1 \leq i \leq k$. Then we have

$$\mathbf{c} = \sum_{i=1}^{k} \frac{\langle \mathbf{c}, \mathbf{a}_i^\star \rangle}{\langle \mathbf{a}_i^\star, \mathbf{a}_i^\star \rangle} \mathbf{a}_i^\star . \tag{4}$$

Finally, for $\mathsf{A} = (\mathbf{a}_1, \ldots, \mathbf{a}_k) \in \mathbb{R}^{m \times k}$ and $\mathsf{A}^\star = [\mathbf{a}_1^\star, \ldots, \mathbf{a}_k^\star]$, we have

$$\left(\det\left(\mathsf{A}^T \mathsf{A}\right)\right)^{\frac{1}{2}} = \left(\det\left(\mathsf{A}^{\star T} \mathsf{A}^\star\right)\right)^{\frac{1}{2}} = \prod_{i=1}^{k} \|\mathbf{a}_i^\star\|_2 \leq \prod_{i=1}^{k} \|\mathbf{a}_i\|_2 . \tag{5}$$

Next, we give some helpful estimates and introduce another notation. We start with the well known *Schwarz inequality*. Let $\mathbf{a}, \mathbf{b} \in \mathbb{R}^n$. Then

$$|\langle \mathbf{a}, \mathbf{b} \rangle| \leq \|\mathbf{a}\|_2 \|\mathbf{b}\|_2 \leq n \|\mathbf{a}\|_\infty \|\mathbf{b}\|_\infty . \tag{6}$$

Lemma 4. *For $\mathbf{a} \in \mathbb{R}^n$ we have $\|\mathbf{a}\|_2 \leq \sqrt{n} \|\mathbf{a}\|_\infty$.*

Lemma 5. *For $\mathsf{A}, \mathsf{B} \in \mathbb{R}^{n \times n}$ we have $\|\mathsf{AB}\|_\infty \leq n \|\mathsf{A}\|_\infty \|\mathsf{B}\|_\infty$.*

Definition 6. *For a matrix $\mathsf{A} = [\mathbf{a}_1, \mathbf{a}_2 \ldots, \mathbf{a}_n] \in \mathbb{R}^{n \times n}$ of rank n we define $\operatorname{dft}(\mathsf{A}) = \frac{1}{|\det(\mathsf{A})|} \prod_{i=1}^{n} \|\mathbf{a}_i\|_2$.*

We can also estimate several norms of the inverse of a matrix.

Corollary 7. *Let $\mathsf{B} \in \mathbb{R}^{n \times n}$ be a matrix of rank n. Then we have*

$$\left\|\mathsf{B}^{-1}\right\|_\infty \leq \frac{\operatorname{dft}(\mathsf{B})}{\lambda(\mathsf{B})} \quad \text{and} \quad \left\|\mathsf{B}^{-1}\right\|_{\mathrm{f}} \leq n \frac{\operatorname{dft}(\mathsf{B})}{\lambda(\mathsf{B})} .$$

Next we examine and describe the quality of certain approximations. After some preliminary observations, we start by examining the influence of approximations in the context of QR factorizations (see [10],[6]). For the proofs of the results we use "brute force" calculus and techniques from numerical analysis and matrix theory, similar to those of the proof of [9, Theorem3.1], but we shall use assumptions that are weaker than those in [9, Theorem 3.1]. Furthermore, our bounds are sharper.

Definition 8. *A rational number z' is called a* q-approximation to a real number z *if* $|z - z'| < 2^{-q-1}$.

Definition 9. *A rational number z' is called a* q-approximation to a real number z *if* $|z - z'| < 2^{-q-1}$. *A complex number z' is called an* q-approximation to the complex number z *if $\Re(z')$ and $\Im(z')$ are q-approximations to $\Re(z)$ and $\Im(z)$. A vector $\mathbf{v}' \in \mathbb{Q}^n$ is called a* q-approximation to a vector $\mathbf{v} \in \mathbb{R}^n$ *if $\mathbf{v}'_i$ is a q-approximation to $\mathbf{v}_i$ for $1 \leq i \leq n$. A matrix $\mathsf{A}' = (a'_{i,j}) \in \mathbb{R}^{n \times n}$ is called a* q-approximation to a matrix $\mathsf{A} = (a_{i,j}) \in \mathbb{R}^{n \times n}$ *if $a'_{i,j}$ is an q-approximation to $a_{i,j}$ for $1 \leq i \leq n$, $1 \leq j \leq n$.*

Definition 10. *A function $f \colon \mathbb{R}^m \to \mathbb{Q}^m$ is called an* approximating function of precision q, *if for all $\mathbf{v} \in \mathbb{R}^m$ the image $f(\mathbf{v})$ is an q-approximation to $\mathbf{v}$. A set $\Lambda' \subseteq \mathbb{Q}^m$ is a* q-approximation to a set $\Lambda \subseteq \mathbb{R}^m$, *if there exists an approximating function f of precision q, such that $f(\Lambda) = \Lambda'$. A sequence $B' = (\mathbf{v}'_1, \ldots, \mathbf{v}'_\ell)$ of vectors in $\mathbb{Q}^n$ is a* q-approximation to a sequence $B = (\mathbf{v}_1, \ldots, \mathbf{v}_\ell)$ *of vectors in $\mathbb{R}^n$ if there exists an approximating function f of precision q such that $B' = f(B)$.*

Proposition 11. *Let $\mathsf{A} \in \mathbb{R}^{n \times n}$ and let A' be a q-approximation to A. Then we have*

$$\|\mathsf{A} - \mathsf{A}'\|_{\mathrm{f}} \leq n 2^{-q-1} \,. \tag{7}$$

A *QR factorization* of a matrix $\mathsf{A} \in \mathbb{R}^{n \times n}$ of rank n is a factorization of A of the form $\mathsf{A} = \mathsf{QR}$, where $\mathsf{R} = (r_{i,j}) \in \mathbb{R}^{n \times n}$ is an upper triangular matrix of rank n with positive diagonal elements and $\mathsf{Q} \in \mathbb{R}^{n \times n}$ is orthonormal. The columns $\mathbf{q}_i$ $(1 \leq i \leq m)$ of Q are just the vectors that would be obtained by applying the Gram-Schmidt orthogonalization to the columns of A and then normalizing the obtained Gram-Schmidt vectors; thus we have $\mathbf{q}_i = \mathbf{a}^\star_i / \|\mathbf{a}^\star_i\|_2$ for $1 \leq i \leq m$, where $\mathbf{a}_i$ resp. $\mathbf{q}_i$ is the i-th column vector of A resp. Q. Furthermore, we know that the entry $r_{i,i}$ of R satisfies $r_{i,i} = \|\mathbf{a}^\star_i\|_2$. For $1 \leq \ell \leq m-1$ the last $m - \ell$ columns of Q form an orthonormal basis of the orthogonal complement of the space generated by the first ℓ columns of A. The effect of approximations on QR factorizations is explained in the following theorem. We start by the observation that the frobenius norm is *invariant under orthonormal transformations* (see [6]). Thus, we obtain

Proposition 12. *Let $\mathsf{A} \in \mathbb{R}^{n \times n}$ be a matrix of rank n and let $\mathsf{A} = \mathsf{QR}$ be its QR factorization. Then $\left\|\mathsf{A}^{-1}\right\|_{\mathrm{f}} = \left\|\mathsf{R}^{-1}\right\|_{\mathrm{f}}$ and $\|\mathsf{A}\|_{\mathrm{f}} = \|\mathsf{R}\|_{\mathrm{f}}$.*

We also need estimations about the quality of approximations of solutions to linear equations and related problems which can easily be shown by the techniques of [2]. We start with

Lemma 13. *Let* $\mathsf{A} \subseteq \mathbb{R}^{n\times n}$ *be a matrix of rank* n *and* A' *be a* q*-approximation to* A*. Let* $\mathbf{t} \in \mathbb{R}^n$*, and let* $c \in \mathbb{R}$*,* $0 < c < 1$*. If* $q \geq \lceil \log \|\mathbf{t}\|_2 - \log(c) - \log(\|\mathsf{A}\mathbf{t}\|_2) + \log(n) \rceil - 1$ *then* $\|\mathsf{A}\mathbf{t} - \mathsf{A}'\mathbf{t}\|_2 < c \|\mathsf{A}\mathbf{t}\|_2$ *.*

Corollary 14. *Let* $\mathsf{A} = [\mathbf{a}_1, \ldots, \mathbf{a}_n] \subseteq \mathbb{R}^{n\times n}$ *be a matrix of rank* n *and* $\mathsf{A}' = [\mathbf{a}'_1, \ldots, \mathbf{a}'_n]$ *be a* q*-approximation to* A*. Let* $c \in \mathbb{R}$*,* $0 < c < 1$*. If* $q \geq \lceil -\log(c) - \log(\lambda(\mathsf{A})) + \log(n) \rceil - 1$ *then we have for* $1 \leq i \leq n$ $\|\mathbf{a}_i - \mathbf{a}'_i\|_2 < c \|\mathbf{a}'_i\|_2$ *.*

Lemma 15. *Let* $\mathsf{A} \in \mathbb{R}^{n\times n}$ *and let* A' *be a* q*-approximation to* A*. Then we have* $|\det(\mathsf{A}') - \det(\mathsf{A})| \leq \mathrm{dft}(\mathsf{A}) |\det(\mathsf{A})| \left(\left(1 + 2^{-q} \frac{\sqrt{n}}{\lambda_1(A)} \right)^n - 1 \right)$ *.*

We also use an other formulation of this result proven in [4].

Lemma 16. *Let* $\mathsf{A} \in \mathbb{R}^{n\times n}$ *and let* A' *be a* q*-approximation to* A*. Then we have* $|\det(\mathsf{A}) - \det(\mathsf{A}')| \leq 2^{-q} \sqrt{n}\, 2^{n-1} n^{\frac{n+1}{2}} \|\mathsf{A}\|_\infty^{n-1}$ *.*

Corollary 17. *Let* $\mathsf{A} \subseteq \mathbb{R}^{n\times n}$ *be a matrix of rank* n *and* A' *be be a* q*-approximation to* A*. If* $q > \frac{3\log(n)}{2} + \log\left(\frac{\mathrm{dft}(\mathsf{A})}{\lambda(\mathsf{A})} \right) + 2$ *then* A' *has rank* n*.*

2 The Main Results

We start by introducing the notion of a (ϵ, δ)-constructable basis of an arbitrary lattice $\Lambda \in \mathbb{R}^r$ of dimension r. First, we need

Definition 18. *Let* B *be a finite sequence of vectors in* $\mathbb{R}^r$*, and let* $\mathbf{c} \in \mathbb{R}^r$*. We call* $|\mathbf{c}|_B = \max\{z \colon z = |\langle \mathbf{c}, \mathbf{a} \rangle|,\ \mathbf{a} \in B\}$ *the* height *of* $\mathbf{c}$ *with respect to* B*.*

Definition 19. *Let* A *be an arbitrary subset of* $\mathbb{R}^r$*, let* B *be a nonempty and finite sequence of vectors in* $\mathbb{R}^r$*, and let* $\epsilon \in \mathbb{R}$*,* $0 < \epsilon \leq 1$*. Then we denote by* $\mathcal{S}(A, B, \epsilon)$ *the set of all vectors* $\mathbf{a} \in A$ *with* $|\mathbf{a}|_B > 0$ *such that for all* $\mathbf{c} \in A$ *satisfying* $|\mathbf{c}|_B > 0$ *we have* $|\mathbf{c}|_B \geq \epsilon\, |\mathbf{a}|_B$ *.*

Definition 20. *Let* $\delta \in \mathbb{R}$*,* $0 < \delta \leq 1$*. Let* $\mathbf{a}_1, \ldots, \mathbf{a}_k$ *be pairwise orthogonal vectors in* $\mathbb{R}^r$ *and let* B_k *be a basis of* $\mathrm{span}(\mathbf{a}_1, \ldots, \mathbf{a}_k)^\perp$*. Then we define* $\mathcal{P}_\delta(\mathbf{a}_1, \ldots, \mathbf{a}_k)$ *to be the set of all vectors* $\mathbf{v} \in \mathbb{R}^r$ *of the shape*

$$\mathbf{v} = \sum_{j=1}^{k} x_j \mathbf{a}_j + \sum_{\mathbf{a} \in B_k} x_{\mathbf{a}} \mathbf{a},\ \text{where } x_j \in \mathbb{R},\ |x_j| \leq \delta \text{ for } 1 \leq j \leq k,\ x_{\mathbf{a}} \in \mathbb{R} \text{ for } \mathbf{a} \in B_k\,.$$

Note that $\mathcal{P}_\delta(\mathbf{a}_1, \ldots, \mathbf{a}_k)$ is independent of the choice of the basis B_k and hence is well defined.

Definition 21. *Let* $\epsilon, \delta \in \mathbb{R},\ 0 < \epsilon \leq 1, 0 < \delta \leq 1$. *A sequence* $(\mathbf{a}_1, \ldots, \mathbf{a}_\ell)$ $(1 \leq \ell \leq r)$ *of lattice vectors in a* r*-dimensional lattice* Λ *in* $\mathbb{R}^r$ *is called* (ϵ, δ)-constructable*, if for all* k *with* $0 \leq k \leq \ell - 1$ *we have* $\mathbf{a}_{k+1} \in \mathcal{S}(\Lambda, B_k, \epsilon) \cap \mathcal{P}_\delta(\mathbf{a}_1^\star, \ldots, \mathbf{a}_k^\star)$*, where* B_k *is an orthonormal basis of* $\operatorname{span}(\mathbf{a}_1, \ldots, \mathbf{a}_k)^\perp$.

In what follows we shall show that for every r-dimensional lattice Λ in $\mathbb{R}^r$ and for every $\epsilon, \delta \in \mathbb{R},\ 0 < \epsilon \leq 1, 0 < \delta \leq 1$ there exists a basis of Λ that is (ϵ, δ)-constructable. The proof of this claim shall be constructive and lead to an algorithm for computing such a basis. We start with the following observations:

Let $\mathbf{a}_1, \ldots, \mathbf{a}_k$ be linearly independent vectors in $\mathbb{R}^r$. Then for any orthogonal basis B_k of $\operatorname{span}(\mathbf{a}_1, \ldots, \mathbf{a}_k)^\perp$ the combination of $(\mathbf{a}_1, \ldots, \mathbf{a}_k)$ and B_k is a basis of the space $\mathbb{R}^r$. Thus for every $\mathbf{b} \in \mathbb{R}^r$ there are uniquely determined $x_i \in \mathbb{R}$ $(1 \leq i \leq k)$ and $x_{\mathbf{a}} \in \mathbb{R}$ $(\mathbf{a} \in B_k)$ such that $\mathbf{b} = \sum_{i=1}^k x_i \mathbf{a}_i + \sum_{\mathbf{a} \in B_k} x_{\mathbf{a}} \mathbf{a}$. Hence, $|\mathbf{b}|_{B_k} = \max\{z \colon z = |x_{\mathbf{a}}|,\ \mathbf{a} \in B_k\}$ If $\pi_k(\mathbf{b})$ is the projection of $\mathbf{b}$ onto $\operatorname{span}(\mathbf{a}_1, \ldots \mathbf{a}_k)^\perp$, then $\pi_k(\mathbf{b}) = \sum_{\mathbf{a} \in B_k} x_{\mathbf{a}} \mathbf{a}$, and $|\mathbf{b}|_{B_k} = |\pi_k(\mathbf{b})|_{B_k}$ and $\|\pi_k(\mathbf{b})\|_2 = \left(\sum_{\mathbf{a} \in B_k} x_{\mathbf{a}}^2\right)^{\frac{1}{2}}$ From this observation (and since for all $\mathbf{x} \in \mathbb{R}^n$ we have $\|\mathbf{x}\|_2 \leq \sqrt{n}\, \|\mathbf{x}\|_\infty$ we obtain

Proposition 22. *Let* $\{\mathbf{a}_1, \ldots, \mathbf{a}_k\}$ $(0 \leq k \leq r - 1)$ *be linearly independent vectors in* $\mathbb{R}^r$*. Let* B_k *be an orthogonal basis of* $\operatorname{span}(\mathbf{a}_1, \ldots, \mathbf{a}_k)^\perp$*. Let* $\mathbf{b} \in \mathbb{R}^r$*, and let* $\pi_k(\mathbf{b})$ *be the projection of* $\mathbf{b}$ *onto* $\operatorname{span}(\mathbf{a}_1, \ldots, \mathbf{a}_k)^\perp$*. Then we have*

$$\sqrt{r-k}\, |\mathbf{b}|_{B_k} \geq \|\pi_k(\mathbf{b})\|_2 \geq |\mathbf{b}|_{B_k} = |\pi_k(\mathbf{b})|_{B_k}\ .$$

A simple consequence of the above proposition is

Corollary 23. *Let* $B \subseteq \mathbb{R}^r$ *be a sequence of pairwise orthogonal vectors, and let* $\mathbf{c} \in \mathbb{R}^r$*. Then* $|\mathbf{c}|_B = 0$ *if and only if* $\mathbf{c} \in \operatorname{span}(B)^\perp$.

After these preliminaries we can describe the construction of a (ϵ, δ)-constructable basis of a lattice. We proceed in several steps. In each step we already know some vectors of a basis and try to find a new one.

Definition 24. *A sequence* $(\mathbf{a}_1, \ldots, \mathbf{a}_k)$ $(0 \leq k \leq r)$ *of vectors in a* r*-dimensional lattice* $\Lambda \subseteq \mathbb{R}^r$ *can be* extended *to a basis of* Λ *if there exists a basis of* Λ *of the form* $(\mathbf{a}_1, \ldots, \mathbf{a}_{k-1}, \mathbf{a}_k, \ldots, \mathbf{a}_r)$.

Clearly, the empty sequence $(k = 0)$ and every basis of Λ can be extended to a basis. We shall also use the following characterization given in [3].

Lemma 25. *Let* Λ *be a* r*-dimensional lattice in* $\mathbb{R}^r$*. A sequence* $(\mathbf{a}_1, \ldots, \mathbf{a}_k)$ $(0 \leq k \leq r)$ *of lattice vectors in* Λ *can be extended to a basis of* Λ *if and only if every vector* $\mathbf{c} \in \Lambda - \{\mathbf{0}\}$ *of the shape*

$$\mathbf{c} = \sum_{i=1}^k u_i \mathbf{a}_i$$

with real $u_1, \ldots, u_k$ *necessarily has* $u_1, \ldots, u_k$ *integral.*

Lemma 26. *Let* $(\mathbf{a}_1, \ldots, \mathbf{a}_k)$ $(0 \leq k \leq r-1)$ *be a sequence of vectors in a* r*-dimensional lattice* Λ *in* $\mathbb{R}^r$*, that can be extended to a basis of* Λ*, and let* B_k *be an orthonormal basis of* $\operatorname{span}(\mathbf{a}_1, \ldots, \mathbf{a}_k)^{\perp}$*. Then for all* $\epsilon \in \mathbb{R}$*,* $1/2 \leq \epsilon \leq 1$*, the set* $\mathcal{S}(\Lambda, B_k, \epsilon)$ *is not empty, and for all* $\mathbf{a}_{k+1} \in \mathcal{S}(\Lambda, B_k, \epsilon)$ *the sequence* $(\mathbf{a}_1, \ldots, \mathbf{a}_k, \mathbf{a}_{k+1})$ *can be extended to a basis of* Λ*.*

Proof. First we have to show that $\mathcal{S}(\Lambda, B_k, \epsilon)$ is not the empty set. For this we note that by 23 there is a vector $\mathbf{b} \in \Lambda$ with $|\mathbf{b}|_{B_k} > 0$. Otherwise the dimension of Λ would be less than r. Hence by Proposition 22 we see that the infimum of the set

$$\left\{z\colon z = |\mathbf{b}|_{B_k}\,,\ \mathbf{b} \in \Lambda,\ |\mathbf{b}|_{B_k} > 0\right\}$$

is greater than $\lambda_1(\Gamma)/\sqrt{r-k}$, where Γ is the lattice that we obtain by projecting all vectors of Λ onto the space $\operatorname{span}(\mathbf{a}_1, \ldots\ \mathbf{a}_k)^{\perp}$. This implies that $\mathcal{S}(\Lambda, B_k, \epsilon) \neq \emptyset$.

Let $\mathbf{a}_{k+1}$ belong to $\mathcal{S}(\Lambda, B_k, \epsilon)$ and let us assume that the sequence $(\mathbf{a}_1, \ldots, \mathbf{a}_k, \mathbf{a}_{k+1})$ can not be extended to a basis of Λ. Then by 25 there is a vector $\mathbf{c} \in \Lambda$, $\mathbf{c} \neq \mathbf{0}$, of the shape $\mathbf{c} = \sum_{i=1}^{k+1} u_i \mathbf{a}_i$, where $u_1, \ldots, u_{k+1} \in \mathbb{R}$ and for some j, $1 \leq j \leq k+1$, we have

$$u_j \notin \mathbb{Z}\,. \tag{8}$$

Since $\mathbf{a}_1, \ldots, \mathbf{a}_{k+1}$ and $\mathbf{c}$ are vectors in Λ, the vector

$$\mathbf{c}' = \sum_{i=1}^{k+1} u_i \mathbf{a}_i - \sum_{i=1}^{k+1} \lceil u_i \rfloor \mathbf{a}_i = \sum_{i=1}^{k+1} (u_i - \lceil u_i \rfloor)\, \mathbf{a}_i$$

belongs to Λ. We show that $|\mathbf{c}'|_{B_k} > 0$. Suppose, in contrary, that $|\mathbf{c}'|_{B_k} = 0$. Then by 23 we have $\mathbf{c}' \in \operatorname{span}(\mathbf{a}_1, \ldots\ \mathbf{a}_k) \cap \Lambda$. Since $(\mathbf{a}_1, \ldots\ \mathbf{a}_k)$ can be extended to a basis of Λ, by 25 it follows that $u_i - \lceil u_i \rfloor \in \mathbb{Z}$, and therefore $u_i \in \mathbb{Z}$ for $1 \leq i \leq k+1$. But this is in contradiction to (8). Hence $|\mathbf{c}'|_{B_k} > 0$. Therefore we have $|\mathbf{c}'|_{B_k} > \epsilon\, |\mathbf{a}_{k+1}|_{B_k}$. On the other hand we obtain

$$\begin{aligned}
|\mathbf{c}'|_{B_k} &= \max\{z\colon z = |\langle \mathbf{c}', \mathbf{b}\rangle|,\ \mathbf{b} \in B_k\} \\
&= \max\left\{z\colon z = \left|\textstyle\sum_{i=1}^{k+1} (u_i - \lceil u_i \rfloor)\, \langle \mathbf{a}_i, \mathbf{b}\rangle\right|,\ \mathbf{b} \in B_k\right\} \\
&= |u_{k+1} - \lceil u_{k+1} \rfloor| \max\{z\colon z = |\langle \mathbf{a}_{k+1}, \mathbf{b}\rangle|,\ \mathbf{b} \in B_k\} \\
&\leq \frac{1}{2} \max\{z\colon z = |\langle \mathbf{a}_{k+1}, \mathbf{b}_i\rangle|,\ \mathbf{b} \in B_k\} \\
&\leq \epsilon\, |\mathbf{a_{k+1}}|_{B_k}\ ,
\end{aligned}$$

which is clearly a contradiction.

Lemma 27. *Let* $(\mathbf{a}_1, \ldots, \mathbf{a}_k)$ $(0 \leq k \leq r-1)$ *be a sequence of vectors in a* r*-dimensional lattice* Λ *in* $\mathbb{R}^r$*, that can be extended to a basis of* Λ*, and let* B_k *be an orthonormal basis of* $\operatorname{span}(\mathbf{a}_1, \ldots, \mathbf{a}_k)^{\perp}$*. Let* $\delta \in \mathbb{R}$*,* $1/2 \leq \delta \leq 1$*. Then for every vector* $\mathbf{b}$ *in* Λ *there exists a vector* $\mathbf{d}$ *in* Λ *such that* $|\mathbf{b}|_{B_k} = |\mathbf{d}|_{B_k}$ *and* $\mathbf{d} \in \mathcal{P}_{\delta}(\mathbf{a}_1^{\star}, \ldots, \mathbf{a}_k^{\star})$*.*

Proof. Let $\mathbf{b} \in \Lambda \subseteq \mathbb{R}^r$. Since the combination of $(\mathbf{a}_1, \ldots, \mathbf{a}_k)$ and B_k is a basis of $\mathbb{R}^r$ from (4) it follows that there are uniquely determined $x_{\mathbf{a}} \in \mathbb{R}$ for all $\mathbf{a} \in B_k$ such that

$$\mathbf{b} = \sum_{i=1}^{k} \frac{\langle \mathbf{b}, \mathbf{a}_i^\star \rangle}{\langle \mathbf{a}_i^\star, \mathbf{a}_i^\star \rangle} \mathbf{a}_i^\star + \sum_{\mathbf{a} \in B_k} x_{\mathbf{a}} \mathbf{a} \,. \tag{9}$$

If we set

$$\mathbf{d} = \mathbf{b} - \sum_{i=1}^{k} \left\lceil \frac{\langle \mathbf{b}, \mathbf{a}_i^\star \rangle}{\langle \mathbf{a}_i^\star, \mathbf{a}_i^\star \rangle} \right\rfloor \mathbf{a}_i \,,$$

then $\mathbf{d}$ belongs to Λ. Moreover, we also know that $\mathbf{d}$ is of the shape

$$\mathbf{d} = \sum_{i=1}^{k} \frac{\langle \mathbf{d}, \mathbf{a}_i^\star \rangle}{\langle \mathbf{a}_i^\star, \mathbf{a}_i^\star \rangle} \mathbf{a}_i^\star + \sum_{\mathbf{a} \in B_k} x_{\mathbf{a}} \mathbf{a} \,,$$

where $x_{\mathbf{a}} \in \mathbb{R}$ for all $\mathbf{a} \in B_k$. Hence, $|\mathbf{b}|_{B_k} = \max\{z \colon z = x_{\mathbf{a}},\ \mathbf{a} \in B_k\} = |\mathbf{d}|_{B_k}$.

Furthermore, by (9) and (3) (first part) we have for $1 \leq j \leq k$

$$\left| \frac{\langle \mathbf{d}, \mathbf{a}_j^\star \rangle}{\langle \mathbf{a}_j^\star, \mathbf{a}_j^\star \rangle} \right| = \left| \frac{\langle \mathbf{b}, \mathbf{a}_j^\star \rangle}{\langle \mathbf{a}_j^\star, \mathbf{a}_j^\star \rangle} - \sum_{i=1}^{k} \left\lceil \frac{\langle \mathbf{b}, \mathbf{a}_i^\star \rangle}{\langle \mathbf{a}_i^\star, \mathbf{a}_i^\star \rangle} \right\rfloor \frac{\langle \mathbf{a}_j, \mathbf{a}_i^\star \rangle}{\langle \mathbf{a}_j^\star, \mathbf{a}_j^\star \rangle} \right| = \left| \frac{\langle \mathbf{b}, \mathbf{a}_i^\star \rangle}{\langle \mathbf{a}_j^\star, \mathbf{a}_j^\star \rangle} - \left\lceil \frac{\langle \mathbf{b}, \mathbf{a}_i^\star \rangle}{\langle \mathbf{a}_i^\star, \mathbf{a}_i^\star \rangle} \right\rfloor \right| \leq \frac{1}{2} \,.$$

Combining 26 and Lemma 27 we obtain

Corollary 28. *Let $(\mathbf{a}_1, \ldots, \mathbf{a}_k)$ $(0 \leq k \leq r-1)$ be a sequence of vectors in a r-dimensional lattice Λ in $\mathbb{R}^r$, that can be extended to a basis of Λ, and let B_k be an orthonormal basis of* $\operatorname{span}(\mathbf{a}_1, \ldots, \mathbf{a}_k)^\perp$. *Then for all $\epsilon, \delta \in \mathbb{R}$, $1/2 \leq \epsilon \leq 1$, $1/2 \leq \delta \leq 1$, the intersection $\mathcal{S}(\Lambda, B_k, \epsilon) \cap \mathcal{P}_\delta(\mathbf{a}_1^\star, \ldots, \mathbf{a}_k^\star)$ is not empty, and for all $\mathbf{a}_{k+1} \in \mathcal{S}(\Lambda, B_k, \epsilon) \cap \mathcal{P}_\delta(\mathbf{a}_1^\star, \ldots, \mathbf{a}_k^\star)$ the sequence $(\mathbf{a}_1, \ldots, \mathbf{a}_k, \mathbf{a}_{k+1})$ can be extended to a basis of the lattice Λ.*

Clearly, Corollary 28 immediately implies

Theorem 29. *For every r-dimensional lattice Λ in $\mathbb{R}^r$ and for every $\epsilon, \delta \in \mathbb{R}$, $1/2 \leq \epsilon \leq 1, 1/2 < \delta \leq 1$ there exists a basis of Λ that is (ϵ, δ)-constructable.*

We also have by Corollary 28

Corollary 30. *Let $\epsilon, \delta \in \mathbb{R}$, $1/2 \leq \epsilon \leq 1, 1/2 \leq \delta \leq 1$. Then each (ϵ, δ)-constructable sequence of a r-dimensional lattice Λ in $\mathbb{R}^r$ can be extended to a basis of Λ.*

The above ideas lead to a strategy to find a (ϵ, δ)-constructable basis by means of approximations. We note that in [1] a $(1/2, 1/2)$-constructable basis of a lattice in $\mathbb{R}^r$ is described. Since in real computations one can only find approximations of the real coefficients of the lattice vectors one can only compute (ϵ, δ)-constructable bases where $\epsilon - 1/2$ and $\delta - 1/2$ is arbitrary small but always greater than 0. But before we investigate those problems in greater detail we summarize, for further reference some technical but also important properties of (ϵ, δ)-constructable sequences.

Lemma 31. *Let $\epsilon, \delta \in \mathbb{R}$, $1/2 \leq \epsilon \leq 1, 1/2 \leq \delta \leq 1$, and let $(\mathbf{a}_1, \ldots, \mathbf{a}_\ell)$ $(1 \leq \ell \leq r)$ be a (ϵ, δ)-constructable sequence of a r-dimensional lattice Λ in $\mathbb{R}^r$. For k with $0 \leq k \leq \ell - 1$ let Λ_k be the lattice with basis $(\mathbf{a}_1, \ldots, \mathbf{a}_k)$, and denote by Γ_k the projection of Λ onto the space $\operatorname{span}(\mathbf{a}_1, \ldots, \mathbf{a}_k)^\perp$. Also, for $\mathbf{a} \in \Lambda$ let $\pi_k(\mathbf{a})$ be the projection of $\mathbf{a}$ onto $\operatorname{span}(\mathbf{a}_1, \ldots, \mathbf{a}_k)^\perp$. Then we have*

$$\epsilon^2 \left\|\pi_k(\mathbf{a}_{k+1})\right\|_2^2 \leq (r-k)\lambda_1(\Gamma_k)^2 \leq (r-k)\lambda_{k+1}(\Lambda)^2\,, \tag{10}$$

$$\epsilon^2 \left\|\mathbf{a}_{k+1}\right\|_2^2 \leq \delta^2 r(k+2)\lambda_{k+1}(\Lambda)^2\,, \tag{11}$$

$$\epsilon^{k+1} \prod_{j=1}^{k+1} \left\|\mathbf{a}_j\right\|_2 \leq \left(\delta^2 r \gamma_{k+1}\right)^{\frac{k+1}{2}} \det(\Lambda_{k+1}) \prod_{j=1}^{k+1} (j+2)^{\frac{1}{2}}\,, \tag{12}$$

$$\lambda_1(\Gamma_k)\sqrt{r-k}\left(\delta^2 r \gamma_{k+1}\right)^{\frac{k+1}{2}} \prod_{j=1}^{k+1} (j+2)^{\frac{1}{2}} \geq \epsilon^{k+2}\lambda_1(\Lambda)\,. \tag{13}$$

Proof. Let $\mathbf{b}$ be a vector in Λ such that $\left\|\pi_k(\mathbf{b})\right\|_2 = \lambda_1(\Gamma_k)$. Then by Proposition 22 we have

$$\lambda_1(\Gamma_k) = \left\|\pi_k(\mathbf{b})\right\|_2 \geq \left|\mathbf{b}\right|_{B_k} \geq \epsilon \left|\mathbf{a}_{k+1}\right|_{B_k} \geq \frac{\epsilon}{\sqrt{r-k}} \left\|\pi_k(\mathbf{a}_{k+1})\right\|_2\,.$$

Next, we note that in Λ there are $k+1$ linearly independent vectors in Λ of length bounded by $\lambda_{k+1}(\Lambda)$. At least one of them is of height greater than 0 with respect to B_k, since otherwise, by 23 there would be $k+1$ linearly independent vectors in $\operatorname{span}(\mathbf{a}_1, \ldots, \mathbf{a}_k)$. Thus, there exists a vector $\mathbf{c} \in \Lambda$, such that

$$\lambda_1(\Gamma_k) \leq \left\|\pi_k(\mathbf{c})\right\|_2 \leq \left\|\mathbf{c}\right\|_2 \leq \lambda_{k+1}(\Lambda)\,.$$

This proves (10).

To prove (11) we combine 20 with (10) and Lemma 3. Then we obtain

$$\begin{aligned}
\epsilon^2 \left\|\mathbf{a}_{k+1}\right\|_2^2 &\leq \epsilon^2 \left\|\pi_k(\mathbf{a}_{k+1})\right\|_2^2 + \epsilon^2\delta^2 \sum_{i=1}^{k} \left\|\mathbf{a}_i^\star\right\|_2 \\
&= \epsilon^2 \left\|\pi_k(\mathbf{a}_{k+1})\right\|_2^2 + \epsilon^2\delta^2 \sum_{i=2}^{k} \left\|\pi_{i-1}(\mathbf{a}_i)\right\|_2^2 + \epsilon^2\delta^2 \left\|\pi_0(\mathbf{a}_1)\right\|_2^2 \\
&\leq (r-k)\lambda_{k+1}(\Lambda)^2 + \delta^2 \sum_{i=2}^{k} (r-i)\lambda_i(\Lambda)^2 + \delta^2 r \lambda_1(\Lambda)^2 \\
&\leq \delta^2 r(k+2)\lambda_{k+1}(\Lambda)^2\,.
\end{aligned}$$

Since for $1 \leq j \leq k+1$ obviously $\lambda_j(\Lambda) \leq \lambda_j(\Lambda_{k+1})$, we can prove (12) by the following chain of inequalities,

$$(\epsilon)^{k+1} \prod_{j=1}^{k+1} \left\|\mathbf{a}_j\right\|_2 \leq \prod_{j=1}^{k+1} \left(\delta^2 r(j+2)\right)^{\frac{1}{2}} \lambda_j(\Lambda_{k+1}) \leq \left(\delta^2 r \gamma_{k+1}\right)^{\frac{k+1}{2}} \det(\Lambda_{k+1}) \prod_{j=1}^{k+1} (j+2)^{\frac{1}{2}}\,,$$

where the last inequality is a consequence of Theorem 1.

Finally, we note that by (10) and (12) and by the properties of the determinant (see [7]) we have

$$\lambda_1(\Gamma_k)(\delta^2 r\gamma_{k+1})^{\frac{k+1}{2}} \prod_{j=1}^{k+1}(j+2)^{\frac{1}{2}} \geq \epsilon \left\|\pi_k(\mathbf{a}_{k+1})\right\|_2 \frac{(\delta^2 r\gamma_{k+1})^{\frac{k+1}{2}}}{\sqrt{r-k}} \prod_{j=1}^{k+1}(j+2)^{\frac{1}{2}}$$

$$= \epsilon \frac{\det(\Lambda_{k+1})}{\det(\Lambda_k)} \frac{(\delta^2 r\gamma_{k+1})^{\frac{k+1}{2}}}{\sqrt{r-k}} \prod_{j=1}^{k+1}(j+2)^{\frac{1}{2}} \geq \frac{\epsilon^{k+2}}{\sqrt{r-k}} \left\|\mathbf{a}_{k+1}\right\|_2 \geq \frac{\epsilon^{k+2}}{\sqrt{r-k}} \lambda_1(\Lambda)\,.$$

This proves inequality (13).

The main problem is that we can in case of approximations we can not compute the Gram-Schmidt vectors but only approximations to them. So we have to show how to compute an appropriate vector only knowing those approximations. The following theorem gives the necessary bounds.

Theorem 32. *Let $\mathsf{A} \in \mathbb{R}^{n\times n}$ be a matrix of rank n and let $\mathsf{A} = \mathsf{QR}$ be its QR factorization. Let $\mathsf{A}' \in \mathbb{R}^{n\times n}$ be a q-approximation to A, let $c \in \mathbb{R}$, $0 < c < 1$. If*

$$q \geq \log\left(\left\|\mathsf{A}^{-1}\right\|_{\mathrm{f}}\right) + 3\log\left(\frac{3}{\sqrt{2}}(n+6)\right) - \min\left\{0, \log\left(\frac{n+6}{\|\mathsf{A}\|_{\mathrm{f}}}\right)\right\} - \log(c) \quad (14)$$

then A' has rank n, and there exists a QR factorization of A' of the form $\mathsf{A}' = (\mathsf{Q}+\mathsf{W})(\mathsf{R}+\mathsf{F})$, where $\mathsf{W} \in \mathbb{R}^{n\times n}$ and $\mathsf{F} \in \mathbb{R}^{n\times n}$ such that

$$\|\mathsf{W}\|_{\mathrm{f}} \leq c \quad \textit{and} \quad \|\mathsf{F}\|_{\mathrm{f}} \leq c\,. \quad (15)$$

Proof. Let $\mathfrak{L}$ be a linear mapping that maps the space $\mathrm{U}(\mathbb{R}, m)$ of upper triangular $n \times n$-matrices with real entries to the space $\mathrm{S}(\mathbb{R}, n)$ of symmetric $n \times n$-matrices, given by $\mathfrak{L}(\mathsf{X}) = \mathsf{X} + \mathsf{X}^T$. Since for any symmetric matrix H there is a unique upper triangular matrix X such that $\mathsf{H} = \mathfrak{L}(\mathsf{X})$, the map $\mathfrak{L}$ is injective and surjective. Furthermore, since by [8] we have $\sqrt{2}\,\|\mathsf{X}\|_{\mathrm{f}} \leq \left\|\mathsf{X} + \mathsf{X}^T\right\|_{\mathrm{f}} = \|\mathsf{H}\|_{\mathrm{f}}$, it follows that

$$\left\|\mathfrak{L}^{-1}(\mathsf{H})\right\|_{\mathrm{f}} \leq (1/\sqrt{2})\,\|\mathsf{H}\|_{\mathrm{f}}\,. \quad (16)$$

Let $\mathsf{E} = \mathsf{A}' - \mathsf{A}$. Then by (7) the matrix $\mathsf{E} \in \mathbb{R}^{n\times n}$ satisfies

$$\|\mathsf{E}\|_{\mathrm{f}} < n2^{-q}\,, \quad (17)$$

and we have $\mathsf{A}' = \mathsf{A} + \mathsf{E}$. Let $\mathrm{M}(\mathbb{R}, n)$ be the set of all $n \times n$-matrices.

Now, we consider at the function $\Phi\colon \mathrm{M}(\mathbb{R}, n) \to \mathrm{U}(\mathbb{R}, n)$, $\mathsf{X} \mapsto \mathfrak{L}^{-1}(\mathsf{Y} - \mathsf{X}^T\mathsf{X})$, where

$$\mathsf{Y} = \mathsf{Q}^T\mathsf{E}\mathsf{R}^{-1} + \left(\mathsf{Q}^T\mathsf{E}\mathsf{R}^{-1}\right)^T + \left(\mathsf{E}\mathsf{R}^{-1}\right)^T \mathsf{E}\mathsf{R}^{-1} \quad (18)$$

is a symmetric matrix. Applying (16) we obtain for all $\mathsf{X}_1, \mathsf{X}_2 \in \mathrm{U}(\mathbb{R}, n)$

$$\begin{aligned}\|\Phi(\mathsf{X}_1) - \Phi(\mathsf{X}_2)\|_{\mathrm{f}} &\leq \left\|\mathfrak{L}^{-1}\left(\mathsf{Y} - \mathsf{X}_1\mathsf{X}_1^T\right) - \mathfrak{L}^{-1}\left(\mathsf{Y} - \mathsf{X}_2\mathsf{X}_2^T\right)\right\|_{\mathrm{f}} \\ &\leq \sqrt{2}\max\left\{\|\mathsf{X}_1\|_{\mathrm{f}}, \|\mathsf{X}_2\|_{\mathrm{f}}\right\}\|\mathsf{X}_1 - \mathsf{X}_2\|_{\mathrm{f}}\,,\end{aligned}$$

and

$$\begin{aligned}\|\Phi(\mathsf{X}_2) - \mathsf{X}_2\|_{\mathrm{f}} &= \left\|\mathfrak{L}^{-1}\left(\mathsf{Y} - \mathfrak{L}^{-1}\left(\mathsf{X}_2\mathsf{X}_2^T\right)\right) - \mathsf{X}_2\right\|_{\mathrm{f}} \\ &\leq \frac{1}{\sqrt{2}}\left(\|\mathsf{Y}\|_{\mathrm{f}} + \|\mathsf{X}_2\|_{\mathrm{f}}^2 + \|\mathsf{X}_2\|_{\mathrm{f}}\right).\end{aligned}$$

By Banach's fixpoint theorem (see for example [10]) there exists a fixpoint X_0 of Φ such that $\|\mathsf{X}_0\|_{\mathrm{f}} \leq (1/\sqrt{2})\,\|\mathsf{Y}\|_{\mathrm{f}}$. From (18) and since the frobenius norm is invariant under orthogonal transformations, it follows that

$$\begin{aligned}\|\mathsf{X}_0\|_{\mathrm{f}} &\leq \frac{1}{\sqrt{2}}\left(\left\|\mathsf{Q}^T\mathsf{E}\mathsf{R}^{-1}\right\|_{\mathrm{f}} + \left\|\left(\mathsf{Q}^T\mathsf{E}\mathsf{R}^{-1}\right)^T\right\|_{\mathrm{f}}\left\|\mathsf{E}\mathsf{R}^{-1}\right\|_{\mathrm{f}}\right) \\ &\leq \sqrt{2}\left\|\mathsf{E}\mathsf{R}^{-1}\right\|_{\mathrm{f}} + \frac{1}{\sqrt{2}}\left\|\mathsf{E}\mathsf{R}^{-1}\right\|_{\mathrm{f}}^2.\end{aligned}$$

Now, using 12 we have

$$\|\mathsf{X}_0\|_{\mathrm{f}} \leq \sqrt{2}\left\|\mathsf{A}^{-1}\right\|_{\mathrm{f}}\|\mathsf{E}\|_{\mathrm{f}} + \frac{1}{\sqrt{2}}\left(\left\|\mathsf{A}^{-1}\right\|_{\mathrm{f}}\|\mathsf{E}\|_{\mathrm{f}}\right)^2. \tag{19}$$

From (14) and (17) we derive

$$\begin{aligned}\left\|\mathsf{A}^{-1}\right\|_{\mathrm{f}}\|\mathsf{E}\|_{\mathrm{f}} &\leq \left\|\mathsf{A}^{-1}\right\|_{\mathrm{f}}\left(\left(\frac{c}{n+6}\right)\frac{\sqrt{2}}{3}\left\|\mathsf{A}^{-1}\right\|_{\mathrm{f}}^{-1}\right)\min\left\{1, \frac{n+6}{\|A\|_{\mathrm{f}}}\right\} \\ &\leq \left(\frac{c}{n+6}\right)\frac{\sqrt{2}}{3}\min\left\{1, \frac{n+6}{\|A\|_{\mathrm{f}}}\right\},\end{aligned} \tag{20}$$

and thus $\|\mathsf{X}_0\|_{\mathrm{f}} \leq 1$. Applying [10] we see that $(\mathsf{I}+\mathsf{X}_0)^{-1}$ exists, where

$$\left\|(\mathsf{I}+\mathsf{X}_0)^{-1}\right\|_{\mathrm{f}} \leq \frac{1}{1-\|\mathsf{X}_0\|_{\mathrm{f}}}. \tag{21}$$

As a solution of the equation $\mathsf{X} = \mathfrak{L}^{-1}(\mathsf{Y} - \mathsf{X}^T\mathsf{X})$, the matrix X_0 is an upper triangular matrix. By (18) it satisfies

$$\mathsf{X}_0 + \mathsf{X}_0^T + \mathsf{X}_0^T\mathsf{X}_0 = \mathsf{Q}^T\mathsf{E}\mathsf{R}^{-1} + \left(\mathsf{Q}^T\mathsf{E}\mathsf{R}^{-1}\right)^T + \left(\mathsf{E}\mathsf{R}^{-1}\right)^T\mathsf{E}\mathsf{R}^{-1}.$$

Multiplying with R^T from the left and R from the right we see that

$$\mathsf{R}^T\mathsf{X}_0\mathsf{R} + \mathsf{R}^T\mathsf{X}_0^T\mathsf{R} + \mathsf{R}^T\mathsf{X}_0^T\mathsf{X}_0\mathsf{R} = \mathsf{A}^T\mathsf{E} + \mathsf{E}^T\mathsf{A} + \mathsf{E}^T\mathsf{E},$$

which, since $\mathsf{R}^T\mathsf{R} = \mathsf{A}^T\mathsf{A}$, is equivalent to

$$(\mathsf{R}+\mathsf{X}_0\mathsf{R})^T(\mathsf{R}+\mathsf{X}_0\mathsf{R}) = (\mathsf{A}+\mathsf{E})^T(\mathsf{A}+\mathsf{E}).$$

Clearly, the product $(\mathsf{I}+\mathsf{X}_0)\mathsf{R}$ is invertible. Hence, there exists a matrix $\mathsf{W} \in \mathbb{R}^{n\times n}$ such that $(\mathsf{A}+\mathsf{E})(\mathsf{R}+\mathsf{X}_0\mathsf{R})^{-1} = (\mathsf{Q}+\mathsf{W})$. Moreover, we have

$$(\mathsf{Q}+\mathsf{W})^T(\mathsf{Q}+\mathsf{W}) = \left((\mathsf{R}+\mathsf{X}_0\mathsf{R})^{-1}\right)^T(\mathsf{A}+\mathsf{E})^T(\mathsf{A}+\mathsf{E})(\mathsf{R}+\mathsf{X}_0\mathsf{R})^{-1} = \mathsf{I}.$$

Let $\mathsf{F} = \mathsf{X}_0\mathsf{R}$. Then, as a product of two upper triangular matrices, F is an upper triangular matrix too, and thus $\mathsf{A}' = \mathsf{A} + \mathsf{E} = (\mathsf{Q} + \mathsf{W})(\mathsf{R} + \mathsf{F})$ is a QR factorization of $\mathsf{A} + \mathsf{E} = \mathsf{A}'$. Especially, A' is invertible and has rank n.

Next, we have to find upper bounds on $\|\mathsf{W}\|_\mathrm{f}$ and $\|\mathsf{F}\|_\mathrm{f}$. Since $\mathsf{R} + \mathsf{F}$ is non-singular we have $\mathsf{W} = (\mathsf{QR} + \mathsf{E} - \mathsf{Q}(\mathsf{R} + \mathsf{F}))(\mathsf{R} + \mathsf{F})^{-1}$, and therefore,

$$\mathsf{W} = \mathsf{E}(\mathsf{R} + \mathsf{F})^{-1} - \mathsf{QX}_0(\mathsf{I} + \mathsf{X}_0)^{-1} . \tag{22}$$

The frobenius norm is invariant under orthogonal transformations, thus from (22) and (21) we obtain

$$\|\mathsf{W}\|_\mathrm{f} \leq \|\mathsf{E}\|_\mathrm{f} \left\|(\mathsf{R} + \mathsf{F})^{-1}\right\|_\mathrm{f} + \frac{\|\mathsf{X}_0\|_\mathrm{f}}{1 - \|\mathsf{X}_0\|_\mathrm{f}} . \tag{23}$$

It remains to find a bound of $\left\|(\mathsf{R} + \mathsf{F})^{-1}\right\|_\mathrm{f}$. Since $\mathsf{Q}+\mathsf{W}$ is orthogonal, $\mathsf{A}+\mathsf{E}$ and $\mathsf{R}+\mathsf{F}$ have the same singular values (see [5]). Let $\sigma(\mathsf{A})$ denote the smallest singular value of A. Then by [5, equation (5.3.14)] we have $\sigma(\mathsf{A})^{-1} = \left\|\mathsf{A}^{-1}\right\|_2 \leq \left\|\mathsf{A}^{-1}\right\|_\mathrm{f}$ and $\sigma(\mathsf{A} + \mathsf{E}) \geq \sigma(\mathsf{A}) - \|\mathsf{E}\|_2$. Therefore, we obtain

$$\begin{aligned} \left\|(\mathsf{R} + \mathsf{F})^{-1}\right\|_\mathrm{f} &\leq n \left\|(\mathsf{R} + \mathsf{F})^{-1}\right\|_2 = \frac{n}{\sigma(\mathsf{R} + \mathsf{F})} \\ &\leq \frac{n}{\sigma(\mathsf{A}) - \|\mathsf{E}\|_2} = \frac{n\,\sigma(\mathsf{A})^{-1}}{1 - \sigma(\mathsf{A})^{-1}\|\mathsf{E}\|_2} \leq \frac{n\left\|\mathsf{A}^{-1}\right\|_\mathrm{f}}{1 - \|\mathsf{A}^{-1}\|_\mathrm{f}\|\mathsf{E}\|_\mathrm{f}} . \end{aligned} \tag{24}$$

Finally, applying (19), (23), and (24), we have

$$\|\mathsf{W}\|_\mathrm{f} \leq \frac{n\left\|\mathsf{A}^{-1}\right\|_\mathrm{f}\|E\|_\mathrm{f}}{1 - \|\mathsf{A}^{-1}\|_\mathrm{f}\|\mathsf{E}\|_\mathrm{f}} + \frac{\sqrt{2}\left\|\mathsf{A}^{-1}\right\|_\mathrm{f}\|\mathsf{E}\|_\mathrm{f} + \frac{1}{\sqrt{2}}\left(\left\|\mathsf{A}^{-1}\right\|_\mathrm{f}\|\mathsf{E}\|_\mathrm{f}\right)^2}{1 - \left(\sqrt{2}\,\|\mathsf{A}^{-1}\|_\mathrm{f}\|\mathsf{E}\|_\mathrm{f} + \frac{1}{\sqrt{2}}\left(\|\mathsf{A}^{-1}\|_\mathrm{f}\|\mathsf{E}\|_\mathrm{f}\right)^2\right)} . \tag{25}$$

To estimate $\|\mathsf{F}\|_\mathrm{f}$ we note that $\mathsf{F} = \mathsf{X}_0\mathsf{R}$. Therefore, from (19) and 12 it follows that

$$\|\mathsf{F}\|_\mathrm{f} \leq \left(\sqrt{2}\left\|\mathsf{A}^{-1}\right\|_\mathrm{f}\|\mathsf{E}\|_\mathrm{f} + \frac{1}{\sqrt{2}}\left(\left\|\mathsf{A}^{-1}\right\|_\mathrm{f}\|\mathsf{E}\|_\mathrm{f}\right)^2\right)\|\mathsf{A}\|_\mathrm{f} . \tag{26}$$

Combining (20) and (25) we obtain $\|\mathsf{W}\|_\mathrm{f} \leq \frac{nc}{n+6} + \frac{6c}{n+6} = c$ and analogously by (26) we get $\|\mathsf{F}\|_\mathrm{f} \leq c \min\left\{1, \frac{n+6}{\|A\|_\mathrm{f}}\right\}\frac{\|\mathsf{A}\|_\mathrm{f}}{n+6} = c$. This proves the last assertion of the theorem.

Proposition 33. *If $q \in \mathbb{N}$, $q > -\log(\lambda_1(\Lambda)/(4\sqrt{r}))$, then each approximation Λ' of precision q to Λ is a discrete set such that the minimal distance between two elements of Λ' is greater than $\lambda_1(\Lambda)/2$. Moreover, each approximating function of precision q restricted on Λ is one-to-one.*

In what follows we shall always implicitely assume that the studied approximating functions are one-to-one on the given lattices. We can do this without loss of generality since the actual precisions will always be larger than the one suggested by the above proposition.

Definition 34. *Let Λ be a r-dimensional lattice Λ in $\mathbb{R}^r$, and let $1 \leq k \leq r-1$. Let $\epsilon, \delta, \sigma, \eta \in \mathbb{R}_{>0}$. Then we define*

$$q_0(\Lambda, k, \epsilon, \delta, \sigma, \eta) = -\log\left(\frac{1}{2}\min\left\{\sqrt{\eta}, \frac{\eta^2\epsilon^{k+2}\lambda_1(\Lambda)}{\sigma + (1+2(\delta+\eta))\frac{\sqrt{r-k}}{\epsilon}\lambda_{k+1}(\Lambda)}\right\}\right),$$

$$q_1(\Lambda, k, \epsilon, \delta) = -\log\left(\frac{\epsilon^{k+2}\lambda_1(\Lambda)}{\sqrt{r-k}\,(\delta^2 r\gamma_{k+1})^{\frac{k+1}{2}}\prod_{j=1}^{k+1}(j+2)^{\frac{1}{2}}}\right),$$

and

$$q_2(\Lambda, k, \epsilon, \delta, \sigma, \eta) = q_1(\Lambda, \epsilon, \delta, \sigma) - q_0(\Lambda, k, \epsilon, \delta, \sigma, \eta). \tag{27}$$

In what follows let $\epsilon, \delta \in \mathbb{R},\ 1/2 < \epsilon < 1, 1/2 < \delta < 1$, and let $(\mathbf{a}_1, \ldots, \mathbf{a}_\ell)$ $(1 \leq \ell \leq r)$ be a (ϵ, δ)-constructable sequence of a r-dimensional lattice Λ in $\mathbb{R}^r$. First we describe the effect of approximations to the set $\mathcal{P}_\delta(\mathbf{a}_1^\star, \ldots, \mathbf{a}_k^\star)$.

Theorem 35. *Let $\epsilon, \delta \in \mathbb{R},\ 1/2 < \epsilon < 1$, $1/2 < \delta < 1$, and let $(\mathbf{a}_1, \ldots, \mathbf{a}_k)$ $(1 \leq k \leq r-1)$ be a (ϵ, δ)-constructable sequence of a r-dimensional lattice Λ in $\mathbb{R}^r$. Let $\sigma \in \mathbb{R}_{>0}$ and $\mathbf{b} \in \Lambda$, with $\|\mathbf{b}\|_2 \leq \sigma$. Let $\eta \in \mathbb{R}$, $\eta > 0$. Finally, let $f\colon \mathbb{R}^r \to \mathbb{Q}^r$ be an approximating function of precision $q \in \mathbb{N}$ such that the vectors $f(\mathbf{a}_1^\star), \ldots, f(\mathbf{a}_k^\star)$ are pairwise orthogonal. If $q > q_2(\Lambda, k, \epsilon, \delta, \sigma, \eta)$ then we have:*

(a) If $\mathbf{b} \in \mathcal{P}_{1/2}(\mathbf{a}_1^\star, \ldots, \mathbf{a}_k^\star)$ then $f(\mathbf{b}) \in \mathcal{P}_{1/2+\eta}(f(\mathbf{a}_1^\star), \ldots, f(\mathbf{a}_k^\star))$.
(b) If $f(\mathbf{b}) \in \mathcal{P}_{1/2+\eta}(f(\mathbf{a}_1^\star), \ldots, f(\mathbf{a}_k^\star))$ then $\mathbf{b} \in \mathcal{P}_{1/2+2\eta}(\mathbf{a}_1^\star, \ldots, \mathbf{a}_k^\star)$.

Proof. Let B_k be an orthonormal basis of $\mathrm{span}(\mathbf{a}_1, \ldots, \mathbf{a}_k)^\perp$ and let B_k' be an orthonormal basis of $\mathrm{span}(f(\mathbf{a}_1), \ldots, f(\mathbf{a}_k))^\perp$. Let $\mathbf{b} \in \mathcal{P}_{1/2}(\mathbf{a}_1^\star, \ldots, \mathbf{a}_k^\star)$, i.e.

$$\mathbf{b} = \sum_{j=1}^{k} x_j \mathbf{a}_j^\star + \sum_{\mathbf{a} \in B_k} x_{\mathbf{a}} \mathbf{a}, \tag{28}$$

where $x_j \in \mathbb{R}$, $|x_j| \leq 1/2$ for $1 \leq j \leq k$, $x_{\mathbf{a}} \in \mathbb{R}$ for $\mathbf{a} \in B_k$. Since $B_k' \cup \{f(\mathbf{a}_1), \ldots, f(\mathbf{a}_k))$ is a basis of $\mathbb{R}^r$, we also have

$$f(\mathbf{b}) = \sum_{j=1}^{k} y_j f(\mathbf{a}_j^\star) + \sum_{\mathbf{a}' \in B_k'} x_{\mathbf{a}'} \mathbf{a}',$$

where $y_j \in \mathbb{R}$ for $1 \leq j \leq k$, $x_{\mathbf{a}'} \in \mathbb{R}$ for $\mathbf{a}' \in B_k'$. Thus, to prove (a), we only have to estimate y_j.

From (4) it follows that for $1 \leq j \leq k$

$$y_j = \frac{\langle f(\mathbf{b}), f(\mathbf{a}_j^\star)\rangle}{\langle f(\mathbf{a}_j^\star), f(\mathbf{a}_j^\star)\rangle}. \tag{29}$$

We set $\mathbf{e} = f(\mathbf{b}) - \mathbf{b}$, and for $1 \leq j \leq k$ we set $\mathbf{e}_j = f(\mathbf{a}_j^\star) - \mathbf{a}_j^\star$. Then, using (29) we have

$$y_j = \frac{\langle \mathbf{b}, \mathbf{a}_j^\star \rangle + \langle \mathbf{b}, \mathbf{e}_j \rangle + \langle \mathbf{e}, \mathbf{a}_j^\star \rangle + \langle \mathbf{e}, \mathbf{e}_j \rangle}{\langle \mathbf{a}_j^\star + \mathbf{e}_j, \mathbf{a}_j^\star + \mathbf{e}_j \rangle} .$$

From (28) it follows that $\langle \mathbf{b}, \mathbf{a}_j^\star \rangle = x_j \langle \mathbf{a}_j^\star, \mathbf{a}_j^\star \rangle$. Applying (6) we thus obtain

$$|y_j| \leq \frac{x_j \left\|\mathbf{a}_j^\star\right\|_2^2 + \|\mathbf{b}\|_2 \|\mathbf{e}_j\|_2 + \|\mathbf{e}\|_2 \left\|\mathbf{a}_j^\star\right\|_2 + \|\mathbf{e}\|_2 \|\mathbf{e}_j\|_2}{\left(\left\|\mathbf{a}_j^\star\right\|_2 - \|\mathbf{e}_j\|_2\right)^2} . \tag{30}$$

On the other hand, 34 and Theorem 31 imply that both $\|\mathbf{e}_j\|_2$ and $\|\mathbf{e}\|_2$ are at most

$$\frac{1}{2} \min \left\{ \sqrt{\eta} \left\|\mathbf{a}_j^\star\right\|_2 , \frac{\eta \left\|\mathbf{a}_j^\star\right\|_2^2}{\|\mathbf{b}\|_2 + (1 + 2(\delta + \eta)) \left\|\mathbf{a}_j^\star\right\|_2} \right\} . \tag{31}$$

Combining (30) and (31) we see that $y_j \leq 1/2 + \eta$. This proves part (a) of the theorem. The proof of (b) is absolutely analogous.

We also have to examine what happens with the set $\mathcal{S}(\Lambda, B_k, \epsilon)$ when we work with approximations. For further reference, we introduce a new abbreviation.

Definition 36. *Let Λ be a r-dimensional lattice Λ in $\mathbb{R}^r$, and let $1 \leq k \leq r-1$. Let $\epsilon, \delta, \sigma \in \mathbb{R}_{>0}$. Then we define*

$$q_3(\Lambda, k, \epsilon, \delta, \sigma) = q_1(\Lambda, k, \epsilon, \delta) - \log \left(\frac{1 - \epsilon}{\sqrt{r} 2(\sigma + 2)} \right) .$$

Theorem 37. *Let $\epsilon, \delta \in \mathbb{R}$, $1/2 < \epsilon < 1$, $1/2 < \delta < 1$, and let $(\mathbf{a}_1, \ldots, \mathbf{a}_k)$ $(1 \leq k \leq r-1)$ be a (ϵ, δ)-constructable sequence of a r-dimensional lattice Λ in $\mathbb{R}^r$. Let B_k be an orthonormal basis of $\operatorname{span}(\mathbf{a}_1, \ldots, \mathbf{a}_k)^\perp$. Furthermore, let $\sigma \in \mathbb{R}_{>0}$, $\sigma > (r + k + 2)^2 \lambda_{k+1}(\Lambda)^2 / \epsilon^2$, Let $f \colon \mathbb{R}^r \to \mathbb{Q}^r$ be an approximating function of precision $q \in \mathbb{N}$, let $B_k' = f(B_k)$ and let $\Lambda' = \{\mathbf{v} \colon \mathbf{v} = f(\mathbf{a}), \mathbf{a} \in \Lambda, \|\mathbf{a}\|_2 \leq \sigma\}$. Finally, let $\mathbf{a}_{k+1}$ be a vector of Λ such that $\|\mathbf{a}_{k+1}\|_2 \leq \sigma$. If $q > q_3(\Lambda, k, \epsilon^2, \delta, \sigma)$ then we have:*

(a) If $\mathbf{a}_{k+1} \in \mathcal{S}(\Lambda, B_k, 1)$, then $f(\mathbf{a}_{k+1}) \in \mathcal{S}(\Lambda', B_k', \sqrt{\epsilon})$.
(b) If $f(\mathbf{a}_{k+1}) \in \mathcal{S}(\Lambda', B_k', \sqrt{\epsilon})$, then $\mathbf{a}_{k+1} \in \mathcal{S}(\Lambda, B_k, \epsilon)$.

Proof. First, we show that for all $\mathbf{a} \in \Lambda$ with $\|\mathbf{a}\|_2 \leq \sigma$ we have

$$\frac{2}{1 + \epsilon} |f(\mathbf{a})|_{B_k'} > |\mathbf{a}|_{B_k} \geq \frac{2\sqrt{\epsilon}}{1 + \epsilon} |f(\mathbf{a})|_{B_k'} . \tag{32}$$

To do so, let $B_k' = \left(\mathbf{a}_{k+1}', \ldots, \mathbf{a}_r'\right)$ and $B_k = (\widehat{\mathbf{a}}_{k+1}, \ldots, \widehat{\mathbf{a}}_r)$. Applying the triangular inequality and Schwarz inequality we obtain for $k + 1 \leq i \leq r$

$$\begin{aligned} |\langle f(\mathbf{a}), \mathbf{a}_i' \rangle| &\geq |\langle \mathbf{a}, \widehat{\mathbf{a}}_i \rangle| - |\langle \mathbf{a}, \mathbf{a}_i' - \widehat{\mathbf{a}}_i \rangle| - |\langle f(\mathbf{a}) - \mathbf{a}, \mathbf{a}_i' \rangle| \\ &\geq |\langle \mathbf{a}, \widehat{\mathbf{a}}_i \rangle| - \|\mathbf{a}\|_2 \|\mathbf{a}_i' - \widehat{\mathbf{a}}_i\|_2 - \|f(\mathbf{a}) - \mathbf{a}\|_2 \|\mathbf{a}_i'\|_2 . \end{aligned} \tag{33}$$

By our assumptions and Proposition 11 we may assume that for $k+1 \le i \le r$ we have $\|\widehat{\mathbf{a}}_i - \mathbf{a}'_i\|_2 \le \sqrt{r}2^{-q}$. If we insert this estimation in (33), then we can derive from the definition of the height (see Definition 18) and from Theorem 31 and Definition 36 that

$$|f(\mathbf{a})|_{B'_k} > |\mathbf{a}|_{B_k} - \|\mathbf{a}\|_2 \sqrt{r}2^{-q} - \sqrt{r}2^{-q}(1+\sqrt{r}2^{-q}) \ge \frac{1+\epsilon}{2} |\mathbf{a}|_{B_k} .$$

This proves the left inequality of (32); the right one can analogously be proven.

To prove (a) we first assume that $f(\mathbf{a}_{k+1}) \notin \mathcal{S}(\Lambda', B'_k, \sqrt{\epsilon})$. That means that there exists $\mathbf{a} \in \Lambda, \|\mathbf{a}\|_2 \le s$ such that $|f(\mathbf{a})|_{B'_k} < \sqrt{\epsilon}\,|f(\mathbf{a}_{k+1})|_{B'_k}$. Thus by (32) we have

$$\frac{1+\epsilon}{2} |\mathbf{a}_{k+1}|_{B_k} \ge \sqrt{\epsilon}\,|f(\mathbf{a}_{k+1})|_{B'_k} \ge |f(\mathbf{a})|_{B'_k} > \frac{1+\epsilon}{2} |\mathbf{a}|_{B_k} .$$

Therefore, $\mathbf{a}_{k+1}$ does not belong to $\mathcal{S}(\Lambda, B_k, 1)$.

To prove (b), let $f(\mathbf{a}_{k+1}) \in \mathcal{S}(\Lambda', B'_k, \sqrt{\epsilon})$, and suppose that $\mathbf{a}_{k+1} \notin \mathcal{S}(\Lambda, B_k, \epsilon)$. That means that there exists a vector $\mathbf{a}$ of Λ with $\epsilon\,|\mathbf{a}_{k+1}|_{B_k} > |\mathbf{a}|_{B_k} > 0$. By Lemma 27 and Lemma 3 we may assume that

$$\|\mathbf{a}\|_2^2 \le \frac{1}{4}\sum_{j=1}^{k} \|\pi_{j-1}(\mathbf{a}_j)\|_2^2 + \|\pi_k(\mathbf{a})\|_2^2 , \tag{34}$$

where $\pi_j(\mathbf{a})$ is the projection of $\mathbf{a}$ onto $\mathrm{span}(\mathbf{a}_1, \ldots, \mathbf{a}_j)^\perp$ $(0 \le j \le k)$. Then applying Theorem 31 and Proposition 22 we obtain

$$\begin{aligned}
\|\mathbf{a}\|_2^2 &\le \frac{1}{4\epsilon^2}\sum_{j=2}^{k}(r-j)\lambda_j(\Lambda)^2 + \frac{r}{4\epsilon^2}\lambda_1(\Lambda)^2 + \sqrt{r-k}\,|\mathbf{a}|_{B_k} \\
&\le \frac{1}{4\epsilon^2}\sum_{j=2}^{k}(r-j)\lambda_j(\Lambda)^2 + \frac{r}{4\epsilon^2}\lambda_1(\Lambda)^2 + \epsilon\sqrt{r-k}\,\|\pi_k(\mathbf{a}_{k+1})\|_2^2 \\
&\le \frac{1}{4\epsilon^2}\sum_{j=2}^{k}(r-j)\lambda_j(\Lambda)^2 + \frac{r}{4\epsilon^2}\lambda_1(\Lambda)^2 + \frac{(r-k)^{\frac{3}{2}}}{\epsilon}\lambda_{k+1}(\Lambda)^2 \\
&\le \left(\frac{r+k+2}{\epsilon}\right)^2 \lambda_{k+1}(\Lambda)^2 \le \sigma .
\end{aligned} \tag{35}$$

By (32), it follows that

$$\frac{2\sqrt{\epsilon}}{1+\epsilon}\,|f(\mathbf{a})|_{B'_k} \ge \frac{2\sqrt{\epsilon}}{1+\epsilon}\,|f(\mathbf{a}_{k+1})|_{B'_k} > \epsilon\,|\mathbf{a}_{k+1}|_{B_k} \ge |\mathbf{a}|_{B_k} \ge \frac{2\sqrt{\epsilon}}{1+\epsilon}\,|f(\mathbf{a})|_{B'_k} .$$

But this is a contradiction.

References

1. Buchmann, J.: Zur Komplexität der Berechnung von Einheiten und Klassenzahlen algebraischer Zahlkörper. Habiliationsschrift (1987)

2. Buchmann, J.: Reducing lattice bases by means of approximations. In: ANTS. pp. 160–168 (1994), citeseer.ist.psu.edu/buchmann94reducing.html
3. Cassels, J.W.S.: An Introduction to the Geometry of Numbers. Springer-Verlag, Berlin et al. (1959)
4. Ge, G.: Algorithms Related to Multiplicative Representations of Algebraic Numbers. Ph.D. thesis, University of California at Berkeley (1993)
5. Gill, P.E., Murray, W., Wright, M.H.: Numerical Linear Algebra and Optimization (Volume 1). Addison-Wesley Publishing Company (1991)
6. Golub, G.H., Van Loan, C.F.: Matrix Computations. Johns Hopkins University Press, Baltimore, Maryland (1983)
7. Greub, W.H.: Linear Algebra. Springer-Verlag, Berlin et al. (1967)
8. Stewart, G.W.: Introduction to Matrix Computation. Academic Press (1973)
9. Stewart, G.W.: Perturbation bounds for the QR factorization of a matrix. SIAM J. Numer. Anal. 14(3), 509–518 (1977)
10. Stoer, J.: Einführung in die numerische Mathematik. Springer-Verlag, Berlin et al. (1978)