ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 26, Number 3, Summer 1996

DIOPHANTINE APPROXIMATION OF MATRICES

G.N. TEN HAVE AND R. TIJDEMAN

ABSTRACT. Upper and lower bound results are given for the approximation of real matrices by quotients of integer matrices.

Introduction. In the theory of Diophantine approximations the approximated objects are usually numbers or functions. In this study we consider matrices as objects of which we investigate approximation properties. A typical question is the following. Let m and n be given positive integers. Let A be an $m \times m$ matrix with integer entries. Let $\sqrt[n]{A}$ be a matrix whose n-th power equals A. How well can $\sqrt[n]{A}$ be approximated by rational matrices if it is not rational itself? The question shows some essential differences with the classical cases. For example, it is not even obvious how to define the distance between two matrices. Furthermore, there may be infinitely many choices for $\sqrt[n]{A}$, since

$$\begin{pmatrix} 1 & \lambda \\ 0 & -1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

for any choice of λ.

In Section 2 we introduce some notation. In Sections 3, 4 and 5, we shall deal with upper bounds for approximations. In the homogeneous case we prove an analogue of Dirichlet's theorem on simultaneous approximations. It will turn out that the choice of the distance function is essential for the quality of the bounds. Lattice basis reduction algorithms can be used for computing good approximations in polynomial time. In the inhomogeneous case we derive an analogue of Kronecker's theorem on simultaneous diophantine approximations. We further state an effective version of this result which follows from the work of Kannan and Lovász.

In Sections 6, 7 and 8 we study lower bounds for approximations. We show that a generalization of Roth's theorem holds for 2×2-matrices,

Received by the editors on December 28, 1994, and in revised form on October 5, 1995.

but with the exception of an explicitly given set of matrices which are well approximable. Here we apply a result of Schmidt on Roth systems. In Section 9 we apply the result of Section 8 to give an answer to the question posed at the beginning. It turns out that a 2×2-matrix $\sqrt[n]{A}$ is badly approximable by rational matrices if A is rational, but not a rational multiple of the identity matrix.

The methods used in this paper are the same as those introduced in Chapters 4 and 5 of the thesis of the first named author [**4**], but some results are new or more general and some are formulated differently. The mentioned chapters also contain a definition and some properties of algebraic matrices and an algorithm for computing good inhomogeneous approximations in polynomial time which are not treated in this article. The present paper is an elaborated version of a talk given by the second named author at a conference in Boulder held at the occasion of the sixtieth birthday of W.M. Schmidt.

2. Notation. The letters k, l, m and n stand for positive integers, the letters A, B, P and Q for matrices. The field of algebraic numbers is denoted by $\bar{\mathbf{Q}}$. We write $M(l, m, K)$ for the set of all $l \times m$-matrices with entries in a ring K and $M(m, K)$ in case $l = m$. For given $B = (b_{ij}) \in M(l, m, \mathbf{C})$, we put

$$|B| = \max_{i,j} |b_{ij}| \quad \text{and} \quad ||B|| = \min_{P \in M(l,m,\mathbf{Z})} |B - P|.$$

If $b = (b_1, \ldots, b_m)$ is a vector, then the Euclidean norm $(\sum_{\mu=1}^{m} |b_\mu|^2)^{1/2}$ is denoted by $|b|_2$. For $B \in M(l, m, \mathbf{C})$ the geometric mean of the Euclidean lengths of the row vectors is given by

$$|B|_2 = \left(\prod_{k=1}^{l} |e_k B|_2 \right)^{1/l},$$

where e_k is the kth unit vector $(0, 0, \ldots, 0, 1, 0, \ldots, 0)$.

Finally we put

$$||B||_2 = \min_{P \in M(l,m,\mathbf{Z})} |B - P|_2.$$

3. Upper bounds in the homogeneous case. Minkowski's theorem on linear forms can be stated as follows (see [**8**, p. 104] or [**2**, p. 153]).

Minkowski's theorem 3A. *For any real numbers b_{ij}, $1 \le i \le l$, $1 \le j \le l$ and c_j, $1 \le j \le l$, there are integers q_i, $1 \le i \le l$, not all zero, such that*

$$\begin{aligned} \left|\sum_{i=1}^{l} q_i b_{ij}\right| &< c_j, \qquad 1 \le j < l, \\ \left|\sum_{i=1}^{l} q_i b_{il}\right| &\le c_l, \end{aligned} \tag{3.1}$$

provided that $c_1 \dots c_l \ge |\det(b_{ij})| > 0$.

Let a_{ij}, $1 \le i \le l$, $1 \le j \le m$, and N be real numbers with $N > 1$. On applying Minkowski's theorem with $l+m$ in place of l to the system of inequalities

$$\begin{cases} |\sum_{i=1}^{l} q_i a_{ij} - q_{l+j}| < N^{-l/m} & 1 \le j \le m \\ |q_i| \le N & 1 \le i \le l \end{cases}$$

we obtain Dirichlet's theorem on simultaneous approximation in the following form (cf. [**2**, p. 13]).

Dirichlet's theorem 3B. *Suppose that $A \in M(l, m, \mathbf{R})$ and that $N \in \mathbf{R}$, $N > 1$. Then there exists a $Q \in M(1, l, \mathbf{Z})$ with*

$$0 < |Q| \le N \quad \textit{and} \quad ||QA|| < \frac{1}{N^{l/m}}. \tag{3.2}$$

An obvious consequence is that

$$||QA|| < |Q|^{-l/m}. \tag{3.3}$$

The following statement is a straightforward extension of Theorem 3B.

Theorem 3C. *Let k be an integer with $1 \le k \le l$. Suppose $A \in M(l, m, \mathbf{R})$ and $N \in \mathbf{R}_{>1}$. Then there exists a $Q \in M(k, l, \mathbf{Z})$ of rank k such that*

$$|Q| \le N \quad \textit{and} \quad ||QA|| < N^{-(l-k+1)/m}.$$

Proof. By Dirichlet's theorem 3B, the first row of $Q = (q_{k\lambda})$ can be chosen in such a way that $Q_{1\lambda_1} \neq 0$ for some λ_1 and that, for $\kappa = 1$,

$$|Q_{k\lambda}| \leq N, \qquad \lambda = 1, \ldots, l \tag{3.4}$$

and

$$||(QA)_{k\mu}|| < \frac{1}{N^{(l-k+1)/m}}, \qquad \mu = 1, \ldots, m. \tag{3.5}$$

By another application of Dirichlet's theorem, the second row can be chosen such that $Q_{2\lambda_1} = 0$, $Q_{2\lambda_2} \neq 0$ for some λ_2 and that (3.4) and (3.5) hold for $\kappa = 2$. For the third row we have $Q_{3\lambda_1} = Q_{3\lambda_2} = 0$, $Q_{3\lambda_3} \neq 0$ for some λ_3 and (3.4) and (3.5) for $\kappa = 3$. Iterating the procedure for $\kappa = 4, \ldots, k$, we obtain a $Q \in M(k, l, \mathbf{Z})$ of rank k which satisfies the requirements. □

Corollary 3D. *For every $A \in M(l, m, \mathbf{R})$ there exists a nonsingular $Q \in M(l, \mathbf{Z})$ such that*

$$|Q| \leq N \quad \textit{and} \quad ||QA|| \leq \frac{1}{N^{1/m}}. \tag{3.6}$$

The proofs of the above mentioned results do not provide a method to construct $Q = (q_{\kappa\lambda})$ effectively. Such a method was introduced by Lenstra, Lenstra and Lovász [**7**] at the cost of a factor depending only on the size of the matrix. Their algorithm, L^3-algorithm for short, provides on the other hand a nonsingular matrix Q such that $|Q(b_{ij})|_2$ is small, whereas Minkowski's theorem 3A only provides a single vector q such that $|q(b_{ij})|$ is small. We formulate the result of the L^3-algorithm in terms of $|\ |_2$, the geometrical mean of the Euclidean norms of the row vectors (cf. Lenstra, Lenstra and Lovász [**7**, (1.8) and (1.26)]).

Lemma 3E. *Let $B = (b_{ij}) \in M(l, \mathbf{Z})$ be nonsingular. Let $\beta \in \mathbf{R}_{\geq 2}$ be such that $|b_{ij}| \leq \beta$ for all i and j. The L^3-algorithm finds a nonsingular matrix $Q \in M(l, \mathbf{Z})$ such that*

$$|QB|_2 \leq 2^{(l-1)/4} |\det B|^{1/l} \tag{3.7}$$

in time and space which is polynomial in l and linear in $\log \beta$.

If $q = (q_1, \dots, q_l)$ is the row vector for which the corresponding row of QB has the smallest Euclidean norm, then (3.7) implies

$$|qB| \le |qB|_2 \le 2^{(l-1)/4} |\det(B)|^{1/l} \quad \text{(cf. (3.1))}.$$

The L^3-algorithm can be used to prove the following variant of Corollary 3D. To compare both results, apply Corollary 3D with $N^{m/(m+1)}$ in place of N.

Theorem 3F. *Let $A \in M(l, m, \mathbf{R})$ and $N \in \mathbf{Z}$, $N > 2^{m(m+1)/4}$. Put $\alpha = \max\{2, |NA|\}$. Assume that the rounding of the entries of NA to integers can be done in polynomial time in terms of l, m and $\log \alpha$. Then one can find in polynomial time in $lm \log \alpha$ a nonsingular matrix $Q \in M(l, \mathbf{Z})$ such that*

$$(3.8) \qquad |Q| \le 2^{m/4} N^{m/(m+1)} \quad \textit{and} \quad ||QA|| \le 2^{(m+3)/4} N^{-1/(m+1)}.$$

Proof. Set $\tilde{A} = (\tilde{\alpha}_{\lambda\mu})$ as $A = (\alpha_{\lambda\mu})$ with the entries rounded to multiples of N^{-1}. Put

$$J = \begin{pmatrix} -I_m & 0 \\ A & (1/N) I_l \end{pmatrix} \quad \text{and} \quad \tilde{J} = \begin{pmatrix} -I_m & 0 \\ \tilde{A} & (1/N) I_l \end{pmatrix},$$

where I_m denotes the $m \times m$ identity matrix and 0 the zero matrix. We have $N\tilde{J} \in M(l+m, \mathbf{Z})$. Applying the L^3-algorithm to the row vectors of $N\tilde{J}$ may result in a singular matrix Q. To avoid this, form $N\tilde{J}_{(\lambda)} \in M(m+1, \mathbf{Z})$ for $1 \le \lambda \le l$ by skipping the last l rows and columns in $N\tilde{J}$ except for row and column $m + \lambda$. Now the L^3-algorithm [**7**, p. 521] provides a short vector $(p_{\lambda 1}, \dots, p_{\lambda m}, q_\lambda) N\tilde{J}_{(\lambda)}$ in the lattice spanned by the row vectors of $N\tilde{J}_{(\lambda)}$ for $\lambda = 1, \dots, l$. Put $b_\lambda = (p_{\lambda 1}, \dots, p_{\lambda m}, q_\lambda)\tilde{J}_{(\lambda)}$. We have

$$|b_\lambda| \le |b_\lambda|_2 \le 2^{m/4} N^{-1/(m+1)}, \qquad \lambda = 1, \dots, l$$

by (3.7). Let Q be the diagonal matrix with entries $q_1, \dots, q_l$. If $q_\lambda = 0$, then b_λ is a nonzero vector with integral entries, but $2^{m/4} N^{-1/(m+1)} <$

1. Hence $q_1 \dots q_l \neq 0$. Then Q is nonsingular. Since

$$\begin{aligned} ||q_\lambda \alpha_{\lambda\mu}|| &= ||q_\lambda \tilde{\alpha}_{\lambda\mu} + q_\lambda(\alpha_{\lambda\mu} - \tilde{\alpha}_{\lambda\mu})|| \\ &\leq ||q_\lambda \tilde{\alpha}_{\lambda\mu}|| + |q_\lambda|\,|\alpha_{\lambda\mu} - \tilde{\alpha}_{\lambda\mu}| \\ &\leq 2^{m/4} N^{-1/(m+1)} + \frac{1}{2} 2^{m/4} N^{-1/(m+1)} \\ &\leq 2^{(m+3)/4} N^{-1/(m+1)} \end{aligned}$$

and

$$|q_\lambda| \leq N|b_\lambda| \leq 2^{m/4} N^{m/(m+1)},$$

we obtain (3.8). □

By a standard argument Corollary 3D implies the following result.

Corollary 3G. *Let $A \in M(l, m, \mathbf{R})$. There exist infinitely many nonsingular matrices $Q \in M(l, \mathbf{Z})$ such that*

$$||QA|| < |Q|^{-1/m}. \tag{3.9}$$

Proof. See [**4**, p. 40]. □

If we want to construct such matrices Q, we can apply Theorem 3F in place of Corollary 3D. Then there is an additional factor $2^{m/4+1}$ on the right side of (3.9).

One may wonder how much Corollary 3G can be improved, since the proofs of Theorem 3C and 3F do not employ the free choice of all entries of Q. In Theorem 3F the matrix Q is even a diagonal matrix. The surprising answer is that in Corollary 3G the exponent $-1/m$ of $|Q|$ is the best possible. According to Perron [**9**], Dirichlet's theorem 3B is the best possible in the sense that for every positive integer m there exist real numbers $\alpha_1, \dots, \alpha_m$ and $c > 0$ such that

$$|q\alpha_\mu - p_\mu| < \frac{c}{|q|^{1/m}}, \qquad \mu = 1, \dots, m$$

admits only finitely many solutions $(p_1, \dots, p_m, q) \in \mathbf{Z}^{m+1}$ with $q \neq 0$. (Such a set of real numbers $\alpha_1, \dots, \alpha_m$ is commonly referred to as a

badly approximable system of m numbers.) Thus there exists a positive number $c' = c'(m, \alpha_1, \dots, \alpha_m)$ such that

$$||q\alpha_\mu|| < \frac{c'}{|q|^{1/m}}, \qquad \mu = 1, \dots, m \tag{3.10}$$

admits no solutions with $q \in \mathbf{Z}$, $q \neq 0$. Put

$$A = \begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_m \\ -1 & & & \\ & \ddots & & \\ & & -1 & 0 \end{pmatrix}$$

where the blanks represent zeros. We claim that $||QA|| < c'|Q|^{-1/m}$ has no nonsingular solution Q. Otherwise, for $\mu = 1, \dots, m$ we would have

$$\begin{aligned} ||q_{\mu 1}\alpha_1 - q_{\mu 2}|| &< \frac{c'}{|Q|^{1/m}} \\ &\vdots \\ ||q_{\mu 1}\alpha_{m-1} - q_{\mu m}|| &< \frac{c'}{|Q|^{1/m}} \\ ||q_{\mu 1}\alpha_m|| &< \frac{c'}{|Q|^{1/m}}. \end{aligned} \tag{3.11}$$

Since (3.11) has no solutions $q_{\mu 1} \neq 0$, we conclude that $q_{\mu 1} = 0$ for $\mu = 1, \dots, m$ so that Q is singular.

In the next section we shall show that if we use $|\ |_2$ in place of the maximum norm $|\ |$ then the exponent of $|Q|$ in (3.9) may be considerably improved upon.

4. Upper bounds in the simultaneous homogeneous case. The results from the preceding section can be applied directly to obtain results on simultaneous approximation of matrices. For example, Corollary 3D applied with $N^{mn/(mn+l)}$ in place of N and mn in place of m has the following consequence.

Corollary 4A. *Let $N \in \mathbf{R}_{>1}$. For any $A_1, \dots, A_n \in M(l, m, \mathbf{R})$ there exists a nonsingular $Q \in M(l, \mathbf{Z})$ such that*

$$|Q| \le N^{mn/(mn+l)} \quad \text{and} \quad ||QA_\nu|| \le N^{-1/(mn+l)}, \quad \nu = 1, \dots, n. \tag{4.1}$$

We shall show that the exponent $-1/(mn+l)$ can be replaced by $-l/(mn+l)$ if we use $|\ |_2$. We recall that, for $B \in M(l, m, \mathbf{R})$, we have set $||B||_2 = \min_{P \in M(l,m,\mathbf{Z})} |B - P|_2$.

Theorem 4B. *Let $A_1, \dots, A_n \in M(l, m, \mathbf{R})$ and $N > 2^{(m+l)^3}$. Then there exists a nonsingular $Q \in M(l, \mathbf{Z})$ such that*

$$|Q|_2 < 2^{mn+l} N^{mn/(mn+l)} \quad \text{and} \quad ||QA_\nu||_2 < 2^{mn+l} N^{-l/(mn+l)}, \quad \nu = 1, \dots, n.$$

Proof. Set $\tilde{A}_\nu$ as A_ν with its entries rounded to multiples of $1/N$. Put

$$J = \begin{pmatrix} -I_m & & & \\ & \ddots & & \\ & & -I_m & \\ A_1 & \cdots & A_n & (1/N) I_l \end{pmatrix}$$

and

$$\tilde{J} = \begin{pmatrix} -I_m & & & \\ & \ddots & & \\ & & -I_m & \\ \tilde{A}_1 & \cdots & \tilde{A}_n & (1/N) I_l \end{pmatrix}.$$

We have $N\tilde{J} \in M(mn+l, \mathbf{Z})$. Let $b_1, \dots, b_{mn+l}$ be the reduced basis vectors of $\tilde{J}$ as found by the L^3-algorithm. Set $b_k = (p_{k1}^{(1)}, \dots, p_{km}^{(n)}, q_{k1}, \dots, q_{kl})\tilde{J}$ for $k = 1, \dots, mn+l$. Let $k_1 \le \cdots \le k_l$ be the minimal indices such that, for $\lambda = 1, \dots, l$, the matrix $(q_{k_j,\mu})$ for $j = 1, \dots, \lambda$; $\mu = 1, \dots, l$ corresponding to b_{k_j} for $j = 1, \dots, \lambda$ has rank λ. Hence $k_1 = 1$. For $i = 1, \dots, mn+l$ we set

$$B_i = \begin{pmatrix} b_1 \\ \vdots \\ b_i \end{pmatrix} \in M(i, mn+l, \mathbf{Q})$$

and $R_i = ((p_{\lambda\mu}^{(1)}), \dots, (p_{\lambda\mu}^{(n)}), (q_{\lambda\mu})) \in M(i, mn+l, \mathbf{Z})$ for $\lambda = 1, \dots, i$ and $\mu = 1, \dots, l$.

To complete the proof, we need the following three lemmas.

We use the notation introduced above.

Lemma 4C. *Denoting the rank of* $(q_{\lambda\mu})_{1\le\lambda\le i, 1\le\mu\le l}$ *by* s, *we have* $|b_1|_2 \cdots |b_i|_2 \ge N^{-s}$.

Lemma 4D. *Suppose that* $N > 2^{(mn+l)^3}$. *Then* $k_j \le (j-1)(mn+l)/l + 1$ *for* $j = 1, \dots, l$.

Lemma 4E. *Suppose* $N > 2^{(mn+l)^3}$. *Then*

$$\prod_{j=1}^{l} |b_{k_j}|_2 < 2^{l(mn+l)/2} N^{-l^2/(mn+l)}.$$

Proof of Lemma 4C. Since $R_i \tilde{J} = B_i$ and rank $B_i = i$, there are i linearly independent columns of R_i. We may therefore suppose that we can choose s columns of $(q_{\lambda\mu})$ and $i-s$ columns of $((p_{\lambda\mu}^{(1)}) \cdots (p_{\lambda\mu}^{(n)}))$ such that these i columns form a linearly independent set of vectors. Define R_i' as the submatrix of R_i consisting of these i columns and

$$B_i' = \begin{pmatrix} b_1' \\ \vdots \\ b_i' \end{pmatrix} \in M(i, \mathbf{Q})$$

as the matrix consisting of the corresponding columns of B_i. Let $\tilde{J}'$ be the matrix satisfying $R_i' \tilde{J}' = B_i'$. By the nonsingularity of R_i', the matrix $\tilde{J}'$ exists and is unique. We will give a construction of $\tilde{J}'$ which shows that $\tilde{J}'$ is a lower triangular matrix with determinant N^{-s}. To get $R_i' \tilde{J}' = B_i'$ from $R_i \tilde{J} = B_i$, we must delete the jth column of $\tilde{J}$ if we delete the jth column of B_i. This jth column of B_i is deleted if and only if the jth column of R_i and hence the jth row of $\tilde{J}$ is deleted. Removing the jth row of $\tilde{J}$ may be done without problems if $j \le mn$, since the only nonzero element in this row is in place (j, j). Hence it only affects

the jth column of B_i which had already been removed. If $j > mn$, the jth column of R_i (if it is to be deleted) is linearly dependent on some of the previous $j-1$ columns of the R_i. Hence a rational multiple of the jth row of $\tilde{J}$ must be added to some of the previous rows of $\tilde{J}$ for still getting the same B_i' at the end. Since the element $1/N$ in place (j,j) of $\tilde{J}$ was already removed when deleting the jth column, no above-diagonal elements are added. Thus, the determinant of $\tilde{J}'$ is only affected by the deletions. Since s columns of $(q_{\lambda\mu})$ are left in R_i', also s of the last i rows and last l columns of $\tilde{J}$ are left in $\tilde{J}'$ whence $\det \tilde{J} = N^{-s}$. The coefficients of R_i' are integral whence $|\det R_i'| \geq 1$. Thus we obtain

$$\begin{aligned} |b_1|_2 \cdots |b_i|_2 &\geq |b_1'|_2 \cdots |b_i'|_2 \geq |\det B'| \\ &= |\det R_i'| \cdot |\det \tilde{J}'| \geq N^{-s}. \end{aligned}$$ □

Proof of Lemma 4D. The statement is obvious for $j = 1$. Let $1 \leq i < l$. Put $T = [i(mn+l)/l + 1]$. Suppose that the rows $(q_{j1} \ldots q_{jl})$ for $j = 1, \ldots, T$ corresponding to $b_1, \ldots, b_T$ have rank at most i. Then, by Lemma 4C, $|b_1|_2 \cdots |b_T|_2 \geq N^{-i}$ whence, according to [**7**, (1.7) and (1.8)],

$$\begin{aligned} \prod_{k=1}^{mn+l} |b_k|_2 &= \prod_{k=1}^{T} |b_k|_2 \prod_{k=T+1}^{mn+l} |b_k|_2 \\ &\geq N^{-i} 2^{-(1/2)\sum_{k=T+1}^{mn+l}(k-1)} \left(\prod_{k=1}^{T} |b_k|_2 \right)^{(mn+l-T)/T} \\ &= 2^{-(mn+l)^2/4} N^{-i(mn+l)/T}. \end{aligned}$$

Note that $T \geq (i(mn+l)+1)/l$, whence $i(mn+l)/T \leq l - 1/T$. Since [**7**, (1.8)] gives

$$\prod_{k=1}^{mn+l} |b_k|_2 \leq 2^{(mn+l)^2/4} N^{-l},$$

we obtain a contradiction for

$$N^{1/T} > 2^{(mn+l)^2}.$$

To get a contradiction for all i, take $N > 2^{(mn+l)^3}$ and use that $T < mn + l$. □

Proof of Lemma 4E. We first show that there exists a bijective mapping f from the multiset consisting of the elements $k_1, \dots, k_l$ where each element is taken $mn + l$ times to the multiset consisting of the elements $1, 2, \dots, mn+l$ where each element is taken l times such that $f(x) \geq x$ for all x. Recall that, by Lemma 4D, $k_j \leq (j-1)(mn+l)/l+1$. Hence, there are at least

$$l\left(mn + l - \left[\frac{(j-1)(mn+l)}{l}\right]\right) \geq (l-j+1)(mn+l)$$

permitted values for $f(k_j)$. We use induction on $l-j$. If $l-j=0$, then there are at least $mn+l$ permitted values for the $mn+l$ images $f(k_l)$ which is just sufficient. If the images of $f(k_l), f(k_{l-1}), \dots, f(k_{j+1})$ are fixed, there are at least

$$(l-j+1)(mn+l) - (l-j)(mn+l) = mn+l$$

remaining permitted values for $f(k_j)$ which is sufficient too. This proves the existence of the mapping f.

By applying formula (1.7) of [**7**] to b_{k_j} and $b_{f(k_j)}$ we obtain

$$\left(\prod_{j=1}^{l} |b_{k_j}|_2\right)^{mn+l} \leq \left(2^{(1/2)\sum_{k=1}^{mn+l}(k-1)} \prod_{k=1}^{mn+l} |b_k|_2\right)^l.$$

Hence, by (1.8) of [**7**],

$$\begin{aligned}\left(\prod_{j=1}^{l} |b_k|_2\right)^{mn+l} &\leq 2^{l(mn+l)^2/2}(|\det L|)^l \\ &\leq 2^{l(mn+l)^2/2} N^{-l^2}.\end{aligned}$$ □

Proof of Theorem 4B (continued). Take $P_1, \dots, P_n$, $Q \in M(l, \mathbf{Z})$, Q nonsingular, such that

$$(P_1, \dots, P_n, Q)\tilde{J} = \begin{pmatrix} b_{k_1} \\ \vdots \\ b_{k_l} \end{pmatrix}.$$

Thus we have $e_j(Q\tilde{A}_1 - P_1, \dots, Q\tilde{A}_n - P_n, (1/N)Q) = b_{k_j}$, whence

$$\max_\nu |e_j(Q\tilde{A}_\nu - P_\nu)|_2 \le |b_{k_j}|_2$$

and

$$|e_j Q|_2 \le N|b_{k_j}|_2.$$

Hence, by Lemma 4E,

$$\begin{aligned} |Q|_2^l &= \prod_{j=1}^{l} |e_j Q|_2 < 2^{l(mn+l)} N^{l-l^2/(mn+l)} \\ &= 2^{l(mn+l)} N^{lmn/(mn+l)}. \end{aligned}$$

Further, we have, by the Cauchy-Schwarz inequality and Lemma 4E,

$$\begin{aligned} &\prod_{j=1}^{l} (\max_\nu |e_j(QA_\nu - P_\nu)|_2 \\ &\qquad = \prod_{j=1}^{l} (\max_\nu |e_j(Q\tilde{A}_\nu - P_\nu)|_2 + \max_\nu |e_j Q(A_\nu - \tilde{A}_\nu)|_2) \\ &\qquad \le \prod_{j=1}^{l} \left(\max_\nu |e_j(Q\tilde{A}_\nu - P_\nu)|_2 + \frac{1}{2N}|e_j Q|_2 \right) \\ &\qquad \le \prod_{j=1}^{l} \left(\frac{3}{2}|b_{kj}|_2 \right) \\ &\qquad < \left(\frac{3}{2} \right)^l 2^{l(mn+l)/2} N^{-l^2/(mn+l)}. \end{aligned}$$

This implies

$$\begin{aligned} ||QA_\nu||_2 &\le \left(\prod_{j=1}^{l} (\max_\nu |e_j(QA_\nu - P_\nu)|_2 \right)^{1/l} \\ &< 2^{mn+l} N^{-l/(mn+l)}. \qquad \square \end{aligned}$$

Remark 4F. In case $l = m$ a slightly stronger statement than Theorem 4B would read: Let $A_1, \dots, A_n \in M(m, \mathbf{R})$. Then there exists a nonsingular $Q \in M(m, \mathbf{Z})$ such that

$$||QA_\nu||_2 < c|Q|_2^{-1/n}, \qquad \nu = 1, \dots, n, \tag{4.2}$$

where c is some constant. We conjecture that this statement is correct. The following simple argument shows that the exponent $-1/n$ in (4.2) cannot be improved. This implies that the exponent of N in Theorem 4B is the best possible.

Use Perron's construction to select $A_1, \dots, A_n \in M(m, \mathbf{R})$ in such a way that

$$||q\det(A_\nu)|| < c'/|q|^{1/n}, \qquad \nu = 1, \dots, n \tag{4.3}$$

admits no solutions with $q \in \mathbf{Z}$, $q \neq 0$ (cf. (3.10)). Consider any nonsingular matrix $Q \in M_m(\mathbf{Z})$. Then $|\det(Q)| \leq |Q|_2^m$. Furthermore, by (4.2),

$$||\det(QA_\nu)|| = ||\det(Q) \cdot \det(A_\nu)|| \geq \frac{c'}{|\det(Q)|^{1/n}}$$

for at least one ν. It follows that

$$\begin{aligned} \max_{\nu=1,\dots,n} ||QA_\nu||_2 &\geq \max_{\nu=1,\dots,n} ||\det(QA_\nu)||^{1/m} \\ &\geq \frac{(c')^{1/m}}{|Q|_2^{1/n}}. \end{aligned}$$

Hence, (4.2) cannot be improved upon.

5. Upper bounds in the inhomogeneous case. In 1884, Kronecker derived the following approximation theorem (see [**6**, pp. 85–88] or, for a more compact description, [**12**, Theorem 24]).

(5A). *Let $G \in M(l, m, \mathbf{R})$ and $\beta \in M(1, m, \mathbf{R})$. Then the following statements are equivalent:*

1. *for every $\varepsilon > 0$ there is an $x \in M(1, l, \mathbf{Z})$ with $|xG - \beta| < \varepsilon$.*
2. *for every $t \in M(m, 1, \mathbf{R})$ with $Gt \in M(l, 1, \mathbf{Z})$ we have $\beta \cdot t \in \mathbf{Z}$.*

Applying Kronecker's theorem to $G = \begin{pmatrix} -I_m \\ A \end{pmatrix}$ where $A \in M(l, m, \mathbf{R})$, it follows that

(5B). 1′. *For every $\varepsilon > 0$ and every $\beta \in M(1, m, \mathbf{R})$ there exist $p \in M(1, m, \mathbf{Z})$ and $q \in M(1, l, \mathbf{Z})$ with $|qA - p - \beta| < \varepsilon$ if and only if*

$2'$. *For every* $t \in M(m,1,\mathbf{Z})$ *with* $|t| > 0$ *we have* $At \notin M(l,1,\mathbf{Z})$.

Another formulation of this equivalence says that, for any $A \in M(l,m,\mathbf{R})$,

(5C). $1''$. *For every* $\varepsilon > 0$ *and every* $\beta \in M(1,m,\mathbf{R})$ *there exists a* $q \in M(1,l,\mathbf{Z})$ *with* $||qA - \beta|| < \varepsilon$ *if and only if*

$2''$. $||At|| \neq 0$ *for every* $t \in M(m,1,\mathbf{Z})$ *with* $|t| > 0$.

The implication $2'' \Rightarrow 1''$ is the case $k = n = 1$ of the following result.

Theorem 5D. *Let* k,l,m,n *be positive integers with* $k \leq l$. *Let* $A_1,\ldots,A_n \in M(l,m,\mathbf{R})$. *Suppose* $||A_1t_1 + \cdots + A_nt_n|| \neq 0$ *for all* $t_1,\ldots,t_n \in M(m,1,\mathbf{Z})$ *not all identically zero. Let* $\varepsilon > 0$. *Then, for every* $B_1,\ldots,B_n \in M(k,m,\mathbf{R})$ *there exists a* $Q \in M(k,l,\mathbf{Z})$ *with* rank $Q = k$ *such that* $||QA_\nu - B_\nu|| < \varepsilon$ *for* $\nu = 1,\ldots,n$.

Proof. Apply Kronecker's theorem to the matrix

$$G = \begin{pmatrix} -I_m & & \\ & \ddots & \\ & & -I_m \\ A_1 & \cdots & A_n \end{pmatrix} \in M(mn+l, mn, \mathbf{R}).$$

By the supposition of the theorem, $Gt \in M(mn+l,1,\mathbf{Z})$ for $t \in M(mn,1,\mathbf{R})$ implies $t = 0$ so that condition 2 is satisfied. It follows that there is an $X \in M(k,mn+l,\mathbf{Z})$ with $|XG - B| < \varepsilon/2$ where $B = (B_1,\ldots,B_n) \in M(k,mn,\mathbf{R})$. This implies that there exists a $Q' \in M(k,l,\mathbf{Z})$ such that $||Q'A_\nu - B_\nu|| < \varepsilon/2$ for $\nu = 1,\ldots,n$.

Let s be the rank of Q'. If $s = k$, then we can take $Q = Q'$. Otherwise we use Theorem 3C with $N > (2/\varepsilon)^{ln/(l-k+1)}$ to find a $Q'' \in M(k,l,\mathbf{Z})$ with rank $Q'' = k$ and $||Q''A_\nu|| < \varepsilon/2$ for $\nu = 1,\ldots,n$. Write $q'_1,\ldots,q'_k$ and $q''_1,\ldots,q''_k$ for the row vectors of Q' and Q'', respectively. Let $i_1,\ldots,i_s$ be the indices of s rows of Q' which are linearly independent and $j_1,\ldots,j_{k-s}$ the indices of $k-s$ rows of Q'' such that $q'_{i_1},\ldots,q'_{i_s},q''_{j_1}\ldots,q''_{j_{k-s}}$ are linearly independent. Let $Q''' \in M(k,l,\mathbf{Z})$ be the matrix with only zeros at the rows $i_1,\ldots,i_s$ and

$q''_{j_1}, \dots, q''_{j_{k-s}}$ as the other rows. Put $Q = Q' + Q'''$. Then rank $Q = k$ and

$$||QA_\nu - B_\nu|| \le ||Q'A_\nu - B_\nu|| + ||Q'''A_\nu|| < \varepsilon. \qquad \square$$

An essential difference between the formulation of Theorem 3C and Theorem 5D is that the former contains an upper bound for $|Q|$ and the latter does not. It is obvious that a localized Kronecker-type sequence requires a measure of linear independence of $A_1, \dots, A_n$ in place of the linear independence condition itself. This is expressed by the following result of Kannan and Lovász [**5**, p. 599]. Here c_0 is some absolute constant with $c_0 \ge 1$.

(5E). *Suppose $a_1, \dots, a_n$ are any reals, and let N and ε be positive reals such that for all integers $t_1, \dots, t_n$, not all zero,*

$$N||a_1t_1 + \cdots + a_nt_n|| + \varepsilon \sum_{\nu=1}^{n} |t_\nu| \ge c_0 n^2. \tag{5.1}$$

Then for all reals $\beta_1, \dots, \beta_n$, there exists an integer q with $|q| \le N$ such that

$$||qa_\nu - \beta_\nu|| \le \varepsilon, \qquad \nu = 1, \dots, n. \tag{5.2}$$

Conversely, if for all reals $\beta_1, \dots, \beta_n$, there exists an integer q with $|q| \le Q$ such that (5.2) *is satisfied, then for all integers $t_1, \dots, t_n$, not all zero,*

$$N||a_1t_1 + \cdots + a_nt_n|| + \varepsilon \sum_{\nu=1}^{n} |t_\nu| \ge 1/2.$$

Kannan and Lovász [**5**, p. 600] remark that, by using a result of Hastad, one can obtain a version which would assert a similar "pseudo-equivalence" for each particular choice of the β_i as in Kronecker's original theorem, but with a worse value (n^3 instead of n^2) on the right side.

From the result of Kannan and Lovász the following quantitative version of Theorem 5D in case $k = l = m$ can be derived.

Theorem 5F. *Let $A_1, \dots, A_n \in M(m, \mathbf{R})$. Let N and ε be positive reals such that for all $t_1, \dots, t_n \in M(m, 1, \mathbf{Z})$, not identically zero,*

$$N||A_1t_1 + \cdots + A_nt_n|| + \varepsilon \sum_{\nu=1}^{n} |t_\nu| \geq c_0(mn+m)^2. \tag{5.3}$$

Then for all matrices $B_1, \dots, B_n \in M(m, \mathbf{R})$ there exists a nonsingular matrix $Q \in M(m, \mathbf{Z})$ with $|Q| \leq N$ such that

$$||QA_\nu - B_\nu|| \leq \varepsilon, \qquad \nu = 1, \dots, n. \tag{5.4}$$

For the proof of Theorem 5F we refer to [**4**, pp. 47–50]. There Theorem 5F is formulated under a weaker condition than (5.3).

Theorem 5D is a direct consequence of Theorem 5F. There are only finitely many $t_1, \dots, t_n \in M(m, 1, \mathbf{Z})$ for which $\varepsilon \sum_{\nu=1}^{n} |t_\nu| < c_0(mn+m)^2$. Because of the linear independence condition in Theorem 5D, there is a positive minimum v of $||A_1t_1 + \cdots + A_nt_n||$ taken over all these finitely many $t_1, \dots, t_n$, not all identically zero. Choose N such that $Nv \geq c_0(mn+m)^2$. Then (5.3) is satisfied for all $t_1, \dots, t_n$ not all identically 0, and (5.4) follows.

In [**4**, pp. 50–54] it is shown how an algorithm of Babai [**1**, Theorem 7.1] for nonhomogeneous simultaneous diophantine approximation combined with Theorem 3F can be used to actually construct nonsingular matrices Q such that $||QA_\nu - B_\nu||$ is small if the rational matrices A_ν and B_ν admit such a solution with $|Q|$ not too large.

6. Lower bounds in the homogeneous case. In 1955, Roth [**10**] proved his famous result on rational approximation of algebraic numbers, thereby finishing the preceding work of Liouville, Thue, Siegel, Dyson and Gelfond. We denote the set of algebraic numbers by $\bar{\mathbf{Q}}$. Roth proved that

Roth's theorem 6A. *For every $\alpha \in \bar{\mathbf{Q}} \cap \mathbf{R}$ and every $\varepsilon > 0$, there exists a number $c = \mathbf{c}(\alpha, \varepsilon) > 0$ such that, for all $q \in \mathbf{Z}$ with $q \neq 0$ either $||q\alpha|| = 0$ or $||q\alpha|| > c/|q|^{1+\varepsilon}$.*

Does the corresponding result for square matrices hold true? That is, is it true that for every $A \in M(m, \bar{\mathbf{Q}} \cap \mathbf{R})$ and every $\varepsilon > 0$ there

exists a number $c = c(A, \varepsilon) > 0$ such that, for all $Q \in M(m, \mathbf{Z})$ with Q nonsingular either $||QA|| = 0$ or $||QA|| > c/|Q|^{1+\varepsilon}$?

We shall deal with the question in case $m = 2$. We first show that the answer is sometimes no. Later we shall use a result of Schmidt on so-called Roth systems to characterize all exceptions.

Let α_1 and α_2 be real algebraic numbers such that 1, α_1 and α_2 are linearly independent over $\mathbf{Q}$. According to Dirichlet's theorem 3B applied with $l = 2$ and $m = 1$, there exist integers p_1, q_1 and q_2 such that

$$0 < |q_1\alpha_1 + q_2\alpha_2 - p_1| < (\max(|q_1|, |q_2|))^{-2} < \frac{1}{100}. \tag{6.1}$$

Without loss of generality, we may assume $\gcd(p_1, q_1, q_2) = 1$. Put $r = \max(|q_1|, |q_2|)$ and $s = \gcd(q_1, q_2)$. Then $s \leq r$ and $||q_1\alpha_1 + q_2\alpha_2|| < r^{-2}$. We apply Dirichlet's theorem again, but now with $N = r - 1$. Hence, there exist integers p_2, q_3 and q_4 such that

$$0 < |q_3\alpha_1 + q_4\alpha_2 - p_2| < \frac{1}{(r-1)^2} \leq (\max(|q_3|, |q_4|))^{-2}. \tag{6.2}$$

Put $t = \gcd(q_3, q_4)$. Then $t < r$ and $||q_3\alpha_1 + q_4\alpha_2|| < 2/r^2$. Put

$$Q = \begin{pmatrix} q_1 & q_2 \\ q_3 & q_4 \end{pmatrix}.$$

Suppose that Q is singular. Then $tq_1 = sq_3$ and $tq_2 = sq_4$. If $tp_1 = sp_2$, then $s|t$ in view of $\gcd(q_1, q_2, p_1) = 1$, whence $r = \max(|q_1|, |q_2|) \leq \max(|q_3|, |q_4|) \leq r - 1$, which is a contradiction. If $tp_1 \neq sp_2$, then we obtain, by subtracting $(t/s)(q_1\alpha_1 + q_2\alpha_2 - p_1)$ and $q_3\alpha_1 + q_4\alpha_2 - p_2$, that

$$\frac{1}{s} \leq \left| p_2 - \frac{t}{s}p_1 \right| < \frac{2}{r^2} + \frac{t}{sr^2} = \frac{2s+t}{r^2 s} < \frac{3}{rs} < \frac{3}{10s}.$$

We conclude that Q is nonsingular. Let A be of the form

$$A = \begin{pmatrix} \alpha_1 & b \\ \alpha_2 & c \end{pmatrix}$$

where b and c are rational numbers such that both $q_1b + q_2c$ and $q_3b + q_4c$ are integers. (For example, we can take $b, c \in \mathbf{Z}$.) Then, by (6.1) and (6.2),

$$|Q| = \max(|q_1|, |q_2|, |q_3|, |q_4|) \leq r \quad \text{and} \quad ||QA|| \leq 2/r^2,$$

so that $||QA|| \leq 2/|Q|^2$. It will turn out in Section 8 that this is essentially the only class of matrices A for which the answer to the above question is negative.

7. Roth systems. In 1971, Schmidt [**11**] extended Roth's theorem 6A to a result on linear forms in rational integers with real algebraic coefficients. Let $L_1(x), \ldots, L_v(x)$ be v linear forms with real algebraic coefficients in the $u+v$ variables $x = (x_1, \ldots, x_{u+v})$. Suppose that $\{L_1, \ldots, L_v\}$ has rank v. It is no restriction to assume, by permuting the variables $x_1, \ldots, x_{u+v}$ if necessary, that rank $\{L_1, \ldots, L_v, x_1, \ldots, x_u\} = u+v$. Now Minkowski's theorem 3A on linear forms, applied to these $u+v$ linear forms, implies that there exist infinitely many $x \in \mathbf{Z}^{u+v} \setminus \{0\}$ such that

$$|L_j(x)| < c_1 \{\max(|x_1|, \ldots, |x_u|)\}^{-u/v}, \qquad j = 1, \ldots, v \tag{7.1}$$

where the constant $c_1 = c_1(L_1, \ldots, L_v)$ depends on the L_j's only. Hence, (7.1) remains true if $\max(|x_1|, \ldots, |x_u|)$ is replaced by $|x| := \max(|x_1|, \ldots, |x_{u+v}|)$ and c_1 by another constant c_2 depending only on the L_j's. Schmidt defined $L_1(x), \ldots, L_v(x)$ to be a Roth system if, with $|x| = \max(|x_1|, \ldots, |x_{u+v}|)$, for every $\varepsilon > 0$ the system of inequalities

$$|L_j(x)| < |x|^{-(u/v+\varepsilon)}, \qquad j = 1, \ldots, v$$

has finitely many solutions in integer points $x \neq 0$. Schmidt [**11**] proved the following criterion for Roth-systems.

(7A). *Suppose that $L_1(x), \ldots, L_v(x)$ are linear forms in $x = (x_1, \ldots, x_{u+v})$ with real algebraic coefficients. Necessary and sufficient for $L_1(x), \ldots, L_v(x)$ to be a Roth-system is that, on every rational subspace S^d of dimension d with $1 \leq d \leq u+v$, the forms $L_1(x), \ldots, L_v(x)$ have rank r satisfying $r \geq dv/(u+v)$.*

We will work out what this means for nonsingular algebraic 2×2 matrices. Let

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in M(2, \bar{\mathbf{Q}} \cap \mathbf{R})$$

be nonsingular, and let $L_1(x)$ and $L_2(x)$ be given by

$$L_1(x) = \alpha x_1 + \gamma x_2 + x_3,$$
$$L_2(x) = \beta x_1 + \delta x_2 + x_4.$$

For each d we check for which A we can have $r < d/2$.

$d = 1$. $r = 0$ happens only for

$$A = \begin{pmatrix} \mu & \nu \\ a\mu + b & a\nu + c \end{pmatrix}$$

on the subspace given by $x_1 = -ax_2$, $x_3 = -bx_2$, $x_4 = -cx_2$, where $a, b, c \in \mathbf{Q}$ and μ, ν are algebraic over $\mathbf{Q}$, and for

$$A = \begin{pmatrix} b & c \\ \mu & \nu \end{pmatrix}$$

on the subspace given by $x_2 = 0$, $x_3 = -bx_1$, $x_4 = -cx_1$.

$d = 2$. $r = 0$ happens only if $A \in M(2, \mathbf{Q})$.

$d = 3$. $r = 0$ is impossible, since A is nonsingular.

$r = 1$ happens only for

$$A = \begin{pmatrix} \mu & a\mu + b \\ \nu & a\nu + c \end{pmatrix}$$

on the subspace given by $x_4 = -bx_1 - cx_2 + ax_3$, where $a, b, c \in \mathbf{Q}$ and μ, ν are algebraic over $\mathbf{Q}$, and for

$$A = \begin{pmatrix} b & \mu \\ c & \nu \end{pmatrix}$$

on the subspace $x_3 = -bx_1 - cx_2$.

We conclude that

(7B). *A nonsingular matrix $A \in M(2, \bar{\mathbf{Q}} \cap \mathbf{R})$, corresponds to a Roth-system if and only if it is not of the form*

$$\begin{pmatrix} \mu & a\mu + b \\ \nu & a\nu + c \end{pmatrix}, \qquad \begin{pmatrix} \mu & \nu \\ a\mu + b & a\nu + c \end{pmatrix} \tag{7.2}$$

where rows and columns may be interchanged and where $a, b, c \in \mathbf{Q}$ and $\mu, \nu \in \bar{\mathbf{Q}} \cap \mathbf{R}$.

8. Lower bounds in the homogeneous case (continued). We shall prove the following theorem.

Theorem 8A. *Let $A \in M(2, \bar{\mathbf{Q}} \cap \mathbf{R})$ with $A \notin M(2, \mathbf{Q})$. Then either for every $\varepsilon > 0$ there exists a number $c_1 = c_1(A, \varepsilon) > 0$ such that*

$$||QA|| > \frac{c_1}{|Q|^{1+\varepsilon}}$$

for every nonsingular $Q \in M(2, \mathbf{Z})$ or A is of the form

$$\begin{pmatrix} \mu & a\mu + b \\ \nu & a\nu + c \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} a\mu + b & \mu \\ a\nu + c & \nu \end{pmatrix} \tag{8.1}$$

where $a, b, c \in \mathbf{Q}$ and $1, \mu, \nu$ are $\mathbf{Q}$-linearly independent algebraic numbers. In the latter case there exist numbers $c_2 = c_2(A, \varepsilon) > 0$ and $c_3 = c_3(A) > 0$ such that

$$||QA|| > \frac{c_2}{|Q|^{2+\varepsilon}}$$

for every nonsingular $Q \in M(2, \mathbf{Z})$, and there exist infinitely many nonsingular $Q \in M(2, \mathbf{Z})$ such that $||QA|| < c_3 |Q|^{-2}$.

We call matrices A of the first kind badly approximable and matrices A of the second kind well approximable. It is remarkable that there are no matrices A for which the optimal exponent is between 1 and 2. If $A \in M(2, \mathbf{Q})$, then, for every nonsingular $\mathbf{Q} \in M(2, \mathbf{Z})$, we have $||QA|| = 0$ or $||QA|| > c > 0$ for some number c depending only on the denominators of the entries of A. Just as in the case of numbers the rational case is not interesting.

In the proof of Theorem 8A we shall use the following lemma where $*$ can represent any real number.

Lemma 8B. *Let $\varepsilon > 0$. Let*

$$A = \begin{pmatrix} \mu & * \\ a\mu + b & * \end{pmatrix} \in M(2, \mathbf{R})$$

with $a, b \in \mathbf{Q}$ *and* $\mu \in \bar{\mathbf{Q}} \cap \mathbf{R}$ *with* $\mu \notin \mathbf{Q}$. *Then there exists a positive constant* $c_4(A, \varepsilon)$ *such that* $||QA|| > c_4(A, \varepsilon)|Q|^{-1-\varepsilon}$ *for all nonsingular* $Q \in M(2, \mathbf{Z})$.

Proof. Put $a = a_1/a_2$, $b = b_1/b_2$ with a_1, a_2, b_1, b_2 integers in lowest terms, $a_2 > 0$, $b_2 > 0$. For any nonsingular matrix

$$Q = \begin{pmatrix} x & y \\ \tilde{x} & \tilde{y} \end{pmatrix}$$

in $M(2, \mathbf{Z})$ we have either $x + ay \neq 0$ or $\tilde{x} + a\tilde{y} \neq 0$. Hence, we may assume that $x + ay \neq 0$. Put $x' = x + ay$. Then

$$||QA|| \geq ||x'\mu + by||. \tag{8.2}$$

Since $\mu \notin \mathbf{Q}$, Roth's theorem 6A implies that there is a number $c_5(\mu, \varepsilon) > 0$ such that

$$||a_2b_2(x'\mu + by)|| > c_5(\mu, \varepsilon)|a_2b_2x'|^{-1-\varepsilon}. \tag{8.3}$$

On the other hand, we have $|x'| \leq |x| + |a|\,|y| \leq (1 + |a|)|Q|$. Combining these inequalities with (8.2) and (8.3), we obtain

$$||QA|| > c_5(\mu, \varepsilon)|a_2b_2|^{-2-\varepsilon}(1 + |a|)^{-1-\varepsilon}|Q|^{-1-\varepsilon}. \qquad \square$$

Proof of Theorem 8A. Suppose that

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

corresponds to a Roth-system. This implies that, for every $\varepsilon > 0$, the system of inequalities

$$\begin{cases} ||\alpha x_1 + \gamma x_2|| < |x|^{-1-\varepsilon} \\ ||\beta x_1 + \delta x_2|| < |x|^{-1-\varepsilon} \end{cases}$$

has only finitely many solutions. Hence, $||QA|| > c(A, \varepsilon)|Q|^{-1-\varepsilon}$ for every nonsingular $Q \in M(2, \mathbf{Z})$.

In the remaining case A corresponds to one of the forms (7.2). If, after interchanging rows and columns, if necessary, A is of the form considered in Lemma 8B, then the assertion follows immediately from the lemma. It remains to consider matrices of the form (8.1) with $a, b, c \in \mathbf{Q}$ and $\mu, \nu \in \bar{\mathbf{Q}} \cap \mathbf{R}$. If $1, \mu$ and ν are $\mathbf{Q}$-linearly dependent, then they can be rewritten in the form considered in the previous case. This proves the first statement.

We may now suppose that

$$A = \begin{pmatrix} \mu & a\mu + b \\ \nu & a\nu + c \end{pmatrix}$$

where $a, b, c \in \mathbf{Q}$ and $1, \mu, \nu$ are $\mathbf{Q}$-linearly independent algebraic numbers. We have

$$\left\| \begin{pmatrix} x & y \\ * & * \end{pmatrix} A \right\| \geq ||\mu x + \nu y||.$$

According to Schmidt's theorem 7A the linear form $L(X) := \mu x_1 + \nu x_2 + x_3$ forms a Roth system if and only if the rank of $L(x)$ is ≥ 1 on every rational subspace of $\mathbf{R}^3$. This is the case since $1, \mu, \nu$ are linearly independent over $\mathbf{Q}$. It follows that there exists a number $c_6(A, \varepsilon) > 0$ such that for all integer pairs x, y, not both zero,

$$\left\| \begin{pmatrix} x & y \\ * & * \end{pmatrix} A \right\| \geq c_6(A, \varepsilon)(\max(|x|, |y|))^{-2-\varepsilon}.$$

Hence, $||QA|| \geq c_6(A, \varepsilon)|Q|^{-2-\varepsilon}$ for all nonsingular (even nontrivial) $Q \in M(2, \mathbf{Z})$. For the proof of the last statement, we apply Dirichlet's theorem 3B to show that there exist integers p_1, q_1, q_2, not all zero, with $\gcd(p_1, q_1, q_2) = 1$ such that (6.1) holds. Note that $r := \max(|q_1|, |q_2|)$ can be taken larger than any prescribed bound. Subsequently, we apply Dirichlet's theorem with $N = r^{-1}$ to obtain p_2, q_3, q_4, not all zero, such that (6.2) holds. Let k be the product of the denominators of a, b and c. It then follows that

$$Q := \begin{pmatrix} kq_1 & kq_2 \\ kq_3 & kq_4 \end{pmatrix}$$

is nonsingular. We have $|Q| \leq kr$ on one hand and $||QA|| \leq 2k|a|r^{-2}$ on the other. Hence, $||QA|| \leq 2k^3|a|\,|Q|^{-2}$ for infinitely many nonsingular matrices $Q \in M(2, \mathbf{Z})$. □

Remark 8C. It is natural to ask for a result similar to that of Theorem 8A for $m \times m$ matrices. Application of a Liouville-type argument yields that, for every nonsingular matrix $A \in M(m, \bar{\mathbf{Q}} \cap \mathbf{R})$ with $A \notin M(m, \mathbf{Q})$ and for every $\varepsilon > 0$ there exists a number $c_0 = c_0(A, \varepsilon) > 0$ such that

$$||QA|| > \frac{c_0}{|Q|^{m+\varepsilon}}$$

for every nonsingular $Q \in M(m, \mathbf{Z})$. On the other hand, Schmidt's theorem 7A can be used to formulate a condition on A under which

$$||QA|| > \frac{c_1}{|Q|^{1+\varepsilon}}$$

for every nonsingular $Q \in M(m, \mathbf{Z})$. It is probably rather complicated to describe the optimal exponent for every matrix A. In particular, it is an open problem whether this optimal exponent is always an integer as in case $m = 2$.

9. Approximability of roots of matrices. We can now restate the question posed at the beginning of the introduction as follows: Which roots of rational matrices are well approximable? We shall give a criterion for 2×2-matrices.

Theorem 9A. *Let n be a positive integer and $A \in M(2, \mathbf{Q})$. If a matrix $B \in M(2, \bar{\mathbf{Q}} \cap \mathbf{R})$ is well approximable with $B^n = A$, then $A = dI_2$ for some $d \in \mathbf{Q}$, $d \neq 0$ and B has eigenvalues ρ, σ with $\rho = \bar{\sigma}$, $\rho \neq \sigma$ such that $\rho^n = \sigma^n = d$.*

Corollary 9B. *Every matrix $B \in M(2, \bar{\mathbf{Q}} \cap \mathbf{R})$ with $B^2 \in M(2, \mathbf{Q})$ is rational or badly approximable.*

Example. The following matrix B satisfies $B^8 = 4I$ and is well approximable.

$$B = \begin{pmatrix} 2^{1/4} & 2^{1/4} \\ 2^{5/8} - 2^{1/4} - 1 & 2^{5/8} - 2^{1/4} \end{pmatrix}.$$

Proof of Theorem 9A. We shall use the following notation:

$$B = \begin{pmatrix} p & q \\ r & s \end{pmatrix},$$

$$K = \det A, \qquad L = \operatorname{tr} A, \qquad k = \det B, \qquad l = \operatorname{tr} B,$$
$$x^2 - Lx + K = (x-\alpha)(x-\beta), \qquad x^2 - lx + k = (x-p)(x-\sigma),$$
$$v = \sqrt{l^2 - 4k}, \quad v > 0 \quad \text{if } l^2 - 4k > 0, \qquad R = \frac{\alpha - \beta}{v}.$$

We choose $\rho = (l+v)/2$, $\sigma = (l-v)/2$, $\rho^n = \alpha$, $\sigma^n = \beta$, $v = \rho - \sigma$.

Note that $k^n = K$.

If $v = 0$, we have (cf. [**3**, p. 59])

$$B^j = \begin{pmatrix} (\frac{p-\rho}{\rho} j + 1)\rho^j & qj\rho^{j-1} \\ rj\rho^{j-1} & (\frac{s-\rho}{\rho} j + 1)\rho^j \end{pmatrix}, \qquad j = 1, 2, \ldots . \tag{9.1}$$

If $v \neq 0$, we have (cf. [**3**, p. 58])

$$B^j = \begin{pmatrix} d_j + R_j(p-s) & R_j q \\ R_j r & d_j \end{pmatrix}, \qquad j = 1, 2, \ldots , \tag{9.2}$$

where $R_j = (\rho^j - \sigma^j)/(\rho - \sigma)$ and d_j is some real number. Note that $R_n = R$.

We assume that B is well approximable. Then B is of the form (8.1) with $a, b, c \in \mathbf{Q}$ and $1, \mu, \nu \in \bar{\mathbf{Q}} \cap \mathbf{R}$ linearly independent over $\mathbf{Q}$. Suppose $\det B = 0$. Then $|\mu c - b\nu| = 0$, whence $b = c = 0$. If

$$B = \begin{pmatrix} \mu & a\mu \\ \nu & a\nu \end{pmatrix},$$

then $A = B^n = (\mu + a\nu)^{n-1} B \in M(2, \mathbf{Q})$. This contradicts the fact that μ and ν are $\mathbf{Q}$-linearly independent. Thus, $\det B \neq 0$.

Suppose $v = 0$. Then $A \in M(2, \mathbf{Q})$ is given by (9.1) with $j = n$. Since $K, L \in \mathbf{Q}$ and $\alpha = \beta$, we have $\alpha = \beta \in \mathbf{Q}$ and therefore $\rho^n \in \mathbf{Q}$. It follows from the previous paragraph that $\rho \neq 0$. We conclude from (9.1) that $p, q, r, s \in \rho Q$. Hence, μ and ν are $\mathbf{Q}$-linearly dependent.

It remains to consider the case $v \neq 0$. Then A is given by (9.2) with $j = n$. If

$$B = \begin{pmatrix} \mu & a\mu + b \\ \nu & a\nu + c \end{pmatrix},$$

then both $R\nu \in \mathbf{Q}$ and $R(\mu - a\nu - c) \in \mathbf{Q}$, whence $R = 0$. Hence $A = dI_2$ where $d = d_n$. This implies $\rho^n = \sigma^n = d$. Since $B \in M(2, \mathbf{R})$,

we have both $\rho+\sigma \in \mathbf{R}$ and $\rho\sigma \in \mathbf{R}$ whence $\sigma = \bar{\rho}$ or $\rho = -\sigma \in \mathbf{R}$. In the latter case $R_2 = \rho + \sigma = 0$, whence, by (9.2), $B^2 = d_2 I_2$. This implies $\nu(\mu + a\nu + c) = 0$. This contradicts the $\mathbf{Q}$-linear independence of 1, μ and ν. Thus, $\rho = \bar{\sigma}$, $\rho \neq \sigma$. □

Proof of Corollary 9B. Suppose

$$B = \begin{pmatrix} \mu & a\mu + b \\ \nu & a\nu + c \end{pmatrix}$$

is well approximable. Then, by Theorem 9A,

$$B^2 = \begin{pmatrix} * & (a\mu+b)(\mu+a\nu+c) \\ \nu(\mu+a\nu+c) & * \end{pmatrix} = d_2 I_2.$$

Hence, $\mu + a\nu + c = 0$ or $a\mu + b = \nu = 0$. Both options are in contradiction with the conditions $a, b, c \in \mathbf{Q}$ and $1, \mu, \nu$ are $\mathbf{Q}$-linearly independent. □

Acknowledgment. The authors thank the referee for his comments.

REFERENCES

1. L. Babai, *On Lovász' lattice reduction and the nearest lattice point problem*, Combinatorica **6** (1986), 1–13.

2. J.W.S. Cassels, *An introduction to diophantine approximation*, Cambridge University Press, Cambridge, 1965.

3. G.N. ten Have, *Matrix solutions of the equation* $X^n = A$, Indag. Math. (N.S.) **2** (1991), 57–64.

4. ———, *Diophantine analysis of matrices*, thesis, Leiden University, The Netherlands, 1993.

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

6. L. Kronecker, *Näherungsweise ganzzahlige Auflösung linearer Gleichungen*, Monatsber. Königl. Preuss. Akad. Wiss. Berlin (1884); L. Kronecker's Werke, Band III-1, Teubner, Leibzig, 1899.

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

8. H. Minkowski, *Geometrie der Zahlen*, Teubner, Leipzig, 1896, Reprint: Chelsea, New York, 1953.

9. O. Perron, *Über Diophantische Approximationen*, Math. Ann. **83** (1921), 77–84.

10. K.F. Roth, *Rational approximations to algebraic numbers*, Mathematika **2** (1955), 1–20.

11. W.M. Schmidt, *Linear forms with algebraic coefficients*, J. Number Theory **3** (1971), 253–277.

12. C.L. Siegel, *Lectures on the geometry of numbers*, Springer-Verlag, Berlin-New York, 1989.

Mathematical Institute, Leiden University, P.O. Box 9512, 2300 RA Leiden, The Netherlands