PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 97, Number 1, May 1986

A SHORT PROOF OF THE EXISTENCE OF VECTOR EUCLIDEAN ALGORITHMS

HELAMAN FERGUSON

ABSTRACT. The classical Euclidean algorithm for pairs of real numbers is generalized to real n-vectors by $\mathrm{Alg}(n, \mathbf{Z})$. An iteration of $\mathrm{Alg}(n, \mathbf{Z})$ is defined by three steps. Given n real numbers $\mathrm{Alg}(n, \mathbf{Z})$ constructs *either* n coefficients of a nontrivial integral linear combination which is zero *or* n independent sets of simultaneous approximations. Either the coefficients will be a column of a $\mathrm{GL}(n, \mathbf{Z})$ matrix or the simultaneous approximations will be rows of $\mathrm{GL}(n, \mathbf{Z})$ matrices constructed by $\mathrm{Alg}(n, \mathbf{Z})$. This algorithm characterizes linear independence of reals over rationals by $\mathrm{GL}(n, \mathbf{Z})$ orbits of rank $n - 1$ matrices.

Let $x \in \mathbf{R}^n$ be a row vector, $n \geq 1$, $M(n, \mathbf{R})$ the $n \times n$ real matrices, and I_n the $n \times n$ identity matrix. An integral vector $b \in \mathbf{Z}^n$ is a nearest integral vector to $x \in \mathbf{R}^n$ if the corresponding coordinate entries of b and x differ by no more than one half. Let $\hat{A}$ denote the transpose of the matrix A. Define the matrix norm of A by $|A|$ where $|A|^2 = \mathrm{Trace}\, A\hat{A}$, and similarly define $|x|$. This norm is submultiplicative as well as subadditive. Define $m \in \mathbf{Z}^n$ to be a relation for x if $m \neq 0$ and $x\hat{m} = 0$. The coordinates of x are said to be $\mathbf{Z}$-linearly independent if x has no relation. If $x \neq 0$, set $P = x\hat{x}I_n - \hat{x}x$, then $xP = 0$ and rank $P = n - 1$. Let $\mathrm{GL}(n, \mathbf{Z})$ be the integral $n \times n$ matrices with $\det = \pm 1$. Any row or column of any $\mathrm{GL}(n, \mathbf{Z})$ matrix consists of relatively prime integers. $\mathrm{GL}(n, \mathbf{Z})$ acts on $M(n, \mathbf{R})$ by multiplication on the left.

The algorithm $\mathrm{Alg}(n, \mathbf{Z})$ will be defined by a single iteration which replaces a vector, matrix pair x, P by a pair xA^{-1}, AP for the integral matrix $A \in \mathrm{GL}(n, \mathbf{Z})$ as constructed in Steps 1_n, 2_n and 3_n below. The following notation for x and P will be assumed in this inductive definition of $\mathrm{Alg}(n, \mathbf{Z})$, cf. Step 2_n. Suppose $x \neq 0$, $xP = 0$, rank $P = n - 1$ for a real $n \times n$ matrix P. If the last entry of x is $t \in \mathbf{R}$ and $t \neq 0$, set $x = (ut, t)$, $u \in \mathbf{R}^{n-1}$. Set $P = \begin{bmatrix} W \\ v \end{bmatrix}$ where v is the last row of P. Note that $xP = 0$ implies $uW = -v$.

$\mathrm{Alg}(1, \mathbf{Z})$, $n = 1$. If $x = 0$, terminate; otherwise set $A = 1$ and replace x, P by x, P where $P = 0$.

$\mathrm{Alg}(n, \mathbf{Z})$, $n > 1$. If some entry of x is zero, terminate; otherwise perform the following three steps.

Step 1_n. Let the permutation matrix E exchange a smallest row of P with the last row of P. Replace x, P by xE^{-1}, EP.

Received by the editors March 5, 1985 and, in revised form, May 31, 1985.
1980 *Mathematics Subject Classification.* Primary 10E45, 10F10; Secondary 20H05, 10F20, 10M20.
Key words and phrases. Euclidean algorithm, relations, simultaneous approximations, linear dependence, independence, $\mathrm{GL}(n, \mathbf{Z})$, orbits.

0002-9939/86 $1.00 + $.25 per page

Step 2_n. Let $Q = u\hat{u}I_{n-1} - \hat{u}u$. Upon u, Q perform $\mathrm{Alg}(n-1, \mathbf{Z})$ until it terminates or $B \in \mathrm{GL}(n-1, \mathbf{Z})$ is constructed such that $|BQW| < u\hat{u}|v|/2\sqrt{n+1}$.

Step 3_n. Let c be a nearest integral vector to $B\hat{u}/u\hat{u}$, $\hat{c} \in \mathbf{Z}^{n-1}$. Set

$$A = \begin{bmatrix} B & c \\ 0 & 1 \end{bmatrix} \in \mathrm{GL}(n, \mathbf{Z}).$$

Replace x, P by xA^{-1}, AP.

Case $n = 2$, $\mathrm{Alg}(2, \mathbf{Z})$, is equivalent to the classical Euclidean algorithm. Cf. [**1**, **2**] for generalized Euclidean algorithms and proofs for all $n \geq 2$ (more complex than the present $\mathrm{Alg}(n, \mathbf{Z})$). Note that if $\mathrm{Alg}(n, \mathbf{Z})$ terminates, then a relation for x is a column of a $\mathrm{GL}(n, \mathbf{Z})$ matrix constructed by a previous iteration of $\mathrm{Alg}(n, \mathbf{Z})$.

THEOREM. *Either* $\mathrm{Alg}(n, \mathbf{Z})$ *will construct a relation* $x \in \mathbf{R}^n$ *after finitely many iterations or there is no relation for* x.

PROOF. The theorem is true for $n = 1$; in this case $\mathrm{Alg}(n, \mathbf{Z})$ simply distinguishes between $x = 0$ and $x \neq 0$. Suppose $x \neq 0$, $x \in \mathbf{R}^n$, and consider the pair x, P where $P = x\hat{x}I_n - \hat{x}x$. Then $P\hat{m} = (x\hat{x})m$ if m is any relation for x. Since $1 \leq |A\hat{m}|$ for any $A \in \mathrm{GL}(n, \mathbf{Z})$,

$$(*) \qquad 0 < x\hat{x} \leq |AP|\,|m|.$$

Assume $n > 1$ and that the theorem is true for $\mathrm{Alg}(n-1, \mathbf{Z})$, $\mathrm{Alg}(n-2, \mathbf{Z}), \ldots,$ $\mathrm{Alg}(1, \mathbf{Z})$. Perform one iteration of $\mathrm{Alg}(n, \mathbf{Z})$ upon x, P to construct the matrix $A \in \mathrm{GL}(n, \mathbf{Z})$. Then x, P is replaced by xA^{-1}, AP. The matrix of the first $n-1$ rows of the product AP is $BW + cv$. From the definition of Q in Step 2_n, $W = \hat{u}uW/u\hat{u} + QW/u\hat{u}$. Hence by this expansion of W in terms of Q and $uW = -v$,

$$BW + cv = B\hat{u}uW/u\hat{u} + BQW/u\hat{u} + cv = (c - B\hat{u}/u\hat{u})v + BQW/u\hat{u}.$$

Therefore by the inequality of Step 2_n,

$$\begin{aligned} |BW + cv| &\leq |c - B\hat{u}/u\hat{u}|\,|v| + |BQW/u\hat{u}| \\ &\leq (\sqrt{n-1} + 1/\sqrt{n+1})|v|/2. \end{aligned}$$

It is supposed that x, P are as after Step 1_n, so that $n|v|^2 \leq |P|^2$. Then

$$|AP|^2 = |BW + cv|^2 + |v|^2 < (n^2 + 6n + 4)|P|^2/4n(n+1).$$

Therefore

$$(**) \qquad |AP| < \tfrac{1}{2}\sqrt{1 + (5/n)}|P|.$$

Set $M_0 = I_n$ and iterate $\mathrm{Alg}(n, \mathbf{Z})$ k times upon x, P (initially $P = x\hat{x}I_n - \hat{x}x$). Let $M_k \in \mathrm{GL}(n, \mathbf{Z})$ be the product of the A and E matrices from Steps 3_n and 1_n up to and including the kth iteration, $k \geq 0$. If $\mathrm{Alg}(n, \mathbf{Z})$ terminates at the $(k+1)$st iteration, some entry of xM_k^{-1} is zero and a column of M_k^{-1} is a relation for x. Such a relation will consist of relatively prime integers. Similarly if any of $\mathrm{Alg}(n-1, \mathbf{Z})$, $\mathrm{Alg}(n-2, \mathbf{Z}), \ldots$ terminate, then a relation for x has been constructed. If $\mathrm{Alg}(n, \mathbf{Z})$ never terminates for x, then from the second inequality $(**)$ M_kP tends to zero as k increases without bound. Since the first inequality $(*)$ is true for any relation $m \in \mathbf{Z}^n$, $|m|$ cannot remain bounded and there are no relations for x.

COROLLARY 1. *If $x \in \mathbf{R}^n$ has no relation, then for every $\varepsilon > 0$ $\mathrm{Alg}(n, \mathbf{Z})$ constructs $A \in \mathrm{GL}(n, \mathbf{Z})$ with each row less than distance ε from the line $\mathbf{R}x$.*

PROOF. $(x\hat{x})A = (A\hat{x})x + AP$ is an orthogonal decomposition of A where $x\hat{x}I_n = \hat{x}x + P$. Set $A = M_k$ for the kth iteration of $\mathrm{Alg}(n, \mathbf{Z})$ on x. Since $\mathrm{Alg}(n, \mathbf{Z})$ never terminates then by the second inequality $(**)$ above, M_kP tends to zero as k increases. Specifically, if $k > (\log(|P|/\varepsilon))/(\log(2/\sqrt{1 + (5/n)}))$, then $|M_kP| < \varepsilon$.

COROLLARY 2. *The closure of the $\mathrm{GL}(n, \mathbf{Z})$ orbit of a rank $n-1$ matrix P contains the zero matrix if and only if the coordinates of any eigenvector corresponding to zero of P are $\mathbf{Z}$-linearly independent.*

PROOF. Let P have rank $n - 1$ and let x, $0 \neq x \in \mathbf{R}^n$, be an eigenvector of P so that $xP = 0$. The if direction: there is no relation for x. Hence the algorithm $\mathrm{Alg}(n, \mathbf{Z})$ applied to x, P never terminates. Then matrices $A \in \mathrm{GL}(n, \mathbf{Z})$ are constructed by iteration of $\mathrm{Alg}(n, \mathbf{Z})$ such that by the second inequality $(**)$ the norm $|AP|$ and hence AP is arbitrarily small. The only if direction: the zero matrix is in the closure of $\mathrm{GL}(n, \mathbf{Z})P$; i.e., there are $A \in \mathrm{GL}(n, \mathbf{Z})$ such that AP is arbitrarily small. By the first inequality $(*)$ this contradicts the existence of a relation for x.

REFERENCES

1. Helaman Ferguson and Rodney Forcade, *Generalization of the Euclidean algorithm for real numbers to all dimensions higher than two*, Bull. Amer. Math. Soc. (N.S.) **1** (1979), 912–914.
2. ———, *Multidimensional Euclidean algorithms*, J. Reine Angew. Math. **334** (1982), 171–181.

DEPARTMENT OF MATHEMATICS, BRIGHAM YOUNG UNIVERSITY, PROVO, UTAH 84602