BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 1, Number 6, November 1979

GENERALIZATION OF THE EUCLIDEAN ALGORITHM FOR REAL NUMBERS TO ALL DIMENSIONS HIGHER THAN TWO

BY H. R. P. FERGUSON AND R. W. FORCADE

ABSTRACT. A construction using integral matrices with determinant ± 1 is given which has as corollaries generalizations of classical theorems of Dirichlet and Kronecker. This construction yields a geometrically convergent algorithm successfully generalizing the Euclidean algorithm to finite sets of real numbers. Applied to such a set this algorithm terminates if and only if the set is integrally linearly dependent and the algorithm gives absolute simultaneous integral approximations if and only if the set is integrally linearly independent. This development applies to complex numbers, can be used to give proofs of irreducibility of polynomials and yields effective lower bounds on heights of integral relations.

Let $\mathbf{Z}$ = rational integers, $\mathbf{R}$ = real numbers, $\mathbf{Z}^n$ = lattice points $\subset \mathbf{R}^n$ as row vectors, $\mathrm{GL}_n(\mathbf{Z}) \subset \mathrm{GL}_n(\mathbf{R})$ are n by n matrices with entries and invertible determinants in $\mathbf{Z} \subset \mathbf{R}$ resp. For M = any matrix or vector, M^t = transpose, $\mathrm{row}_i M = i$th row, $\mathrm{col}_j M = j$th column, height (M) = max absolute values of entries of M. The entries of $x \in \mathbf{R}^n$ are $\mathbf{Z}$-linearly dependent iff there exists $0 \neq m \in \mathbf{Z}^n$ such that $xm^t = 0$, $m = \mathbf{Z}$-relation for x. For $0 \neq x \in \mathbf{R}^n$, x determines the line $x\mathbf{R}$ and orthogonal hyperplane $x^\perp = \{y \in \mathbf{R}^n : xy^t = 0\}$. A hyperplane matrix Q with respect to x is any matrix $xQ = 0$ such that the columns of Q transposed span $x^\perp$. The hyperplane matrix is a key idea here in three aspects: (I) it permits estimates of heights of relations (Theorem 1), (II) it measures how closely the rows of a $\mathrm{GL}_n(\mathbf{Z})$ matrix are to the line $x\mathbf{R}$ (Lemma 1), (III) it underlies the definition of a crucial injection $\mathrm{GL}_n(\mathbf{Z}) \hookrightarrow \mathrm{GL}_{n+1}(\mathbf{Z})$ (Lemma 2). We exploit the nonuniqueness of Q.

THEOREM 1. *Let $0 \neq x \in \mathbf{R}^n$. Then there exists a hyperplane matrix Q such that* height $m \geqslant 1/\mathrm{height}\, AQ$ *for m any $\mathbf{Z}$-relation for x and any $A \in \mathrm{GL}_n(\mathbf{Z})$.*

SKETCH OF PROOF. The parallelotope $/A/ = \{\Sigma f_j \mathrm{col}_j A : |f_j| \leqslant 1 \leqslant j \leqslant n\}$ has easily characterized lattice points if $A \in \mathrm{GL}_n(\mathbf{Z})$. Let I = identity matrix and define Q to be the hyperplane matrix whose columns transposed are the vertices of the convex polytope $/I/ \cap x^\perp$.

A $\mathrm{GL}_n(\mathbf{Z})$-algorithm is defined to be any construction (usually in response

Received by the editors March 26, 1979.
AMS (MOS) subject classifications (1970). Primary 10E45, 10F10, 10F20; Secondary 10F37, 12A10, 10H05, 02E10.

0002-9904/79/0000-0505/$01.75

to an x) of a sequence $\{M_k\}_{k\geq 1}$, $M_k \in \mathrm{GL}_n(\mathbf{Z})$. If xM_k has a zero entry for some k then the entries of x are $\mathbf{Z}$-linearly dependent: the algorithm *terminates.* If the height of $M_k^{-1}Q$ approaches zero as k increases to infinity then the entries of x are $\mathbf{Z}$-linearly independent: the algorithm *absolutely approximates* x. A $\mathrm{GL}_n(\mathbf{Z})$-algorithm is *split* iff the algorithm terminates or absolutely approximates for every $x \in \mathbf{R}^n$.

LEMMA 1. *If a* $\mathrm{GL}_n(\mathbf{Z})$ *algorithm is split and does not terminate for some* x *then the distance of the rows of* M_k^{-1} *to the line* $x\mathbf{R}$ *approaches zero as* k *increases.*

SKETCH OF PROOF. For $xx^t = 1$, set $Q = I - x^t x$ to get a line-hyperplane decomposition of any matrix $A = (Ax^t)x + AQ$.

Define the $\mathrm{GL}_2(\mathbf{Z})$ algorithm A_2 by the following iteration. For $x = (x_1, x_2)$, let x_i be of largest and x_j of next largest absolute value. Replace x_i by the $x_i \pm x_j$ of smaller absolute value. Then A_2 splits. We will give an uncountable collection of $\mathrm{GL}_n(\mathbf{Z})$ algorithms which split, $A_n(b)$, $n \geq 2 > 1/b > 1$. For brevity we describe them by induction on n by defining the injection J: $\mathrm{GL}_n(\mathbf{Z}) \subset\!\!\rightarrow \mathrm{GL}_{n+1}(\mathbf{Z})$, j is also an integer $1 \leq j \leq n+1$. Let $x_{(j)} \in \mathbf{R}^n$ be $x \in \mathbf{R}^{n+1}$ with the jth entry deleted. For $A \in \mathrm{GL}_n(\mathbf{Z})$ set $T_i = \mathrm{row}_i A$ if $i < j$ or $T_i = \mathrm{row}_{i-1} A$ if $i > j$, $c_i =$ *nearest* integer to $T_i x_{(j)}^t x_j / x_{(j)} x_{(j)}^t$. Define $J(A) \in \mathrm{GL}_{n+1}(\mathbf{Z})$ to have a 1 in the (j, j) position, zeros in that row, the c's in that column and A the minor matrix of the 1. Let $Q_{(j)}$ be Q without the jth row and $T_i = d_i x_{(j)} + v_i$ orthogonally.

LEMMA 2. *The injection map* $J: \mathrm{GL}_n(\mathbf{Z}) \hookrightarrow \mathrm{GL}_{n+1}(\mathbf{Z})$ *has the property that* $\mathrm{row}_i(J(A)Q) = \mathrm{row}_j Q$ *if* $i = j$ *and* $\delta_i \mathrm{row}_j Q + n_i Q_{(j)}$ *if* $i \neq j$ *where* $|\delta_i| \leq 1/2$.

To sketch the construction of $A_{n+1}(b)$ from $A_n(b)$ and the proof that A_n splits, select the map J by choosing j to be the number of the row of Q with least height. By induction A_n splits; if A_n does not terminate then for $0 < \epsilon < (b - 1/2)$ height $(\mathrm{row}_j Q)$ there exists a finite number of iterations of A_n acting on $x_{(j)}$ yielding $x_{(j)}A^{-1}$ for a certain $A \in \mathrm{GL}_n(\mathbf{Z})$ with height $(n_i) < \epsilon /$ height Q. By Lemma 2, height $(\mathrm{row}_i(J(A)Q)) < b$ height $(\mathrm{row}_j Q)$ if $i \neq j$. Define one iteration of A_{n+1} by $x \mapsto x(J(A))^{-1}$.

THEOREM 2. *For every integer* n *and real number* b, $n \geq 2 > 1/b > 1$, *the* $\mathrm{GL}_n(\mathbf{Z})$ *algorithm* $A_n(b)$ *splits, i.e., for every nonzero* $x \in \mathbf{R}^n$ *the sequence of matrices* M_k, $k \geq 1$ *is such that Termination) There exists a* k *such that a column of* M_k *is an integral relation among the entries of* x *OR Absolute approximation) For every* $\epsilon > 0$ *there exists an integer* $K \geq 1$ *such that for each* $k \geq K$ *the rows of* M_k^{-1} *give* n *linearly independent lattice points in* $\mathbf{Z}^n$, *each within a distance* ϵ *of the line determined by* x.

THEOREM 3. *Let* $x = (x_1, x_2, \ldots, x_n) \in \mathbf{R}^n$ *where* $x_1 = 1, x_2, \ldots, x_n$ *are* **Z***-linearly independent real numbers. Then for every* $\epsilon > 0$ *there exists an integral matrix* $P \in \mathrm{GL}_n(\mathbf{Z})$ *with first column* N, $N^t \in \mathbf{Z}^n$ *such that* height $(Nx - P) < \epsilon$.

THEOREM 4. *A finitely generated spanning* **Z***-module in* $\mathbf{R}^n$ *is dense in* $\mathbf{R}^n$ *if and only if every neighborhood of the origin contains a* **Z***-basis for the* **Z***-module.*

THEOREM 5. (a) *The height of any quintic polynomial with integer coefficients having Euler's constant as a zero must exceed* 10^{50}.

(b) *If* $\zeta(3)/\pi^3$ *satisfies an integral quadratic equation then at least two of the three coefficients exceed one hundred decimal digits in length.*

(c) *The first seven imaginary parts of the nontrivial zeros of the Riemann zeta function have no integral relations with heights* $\leqslant 65$.

The proof of Theorems 3 and 4 involve applications of the construction represented in Theorem 2. The proof of Theorem 5 is given by exhibiting three integral matrices, from $\mathrm{GL}_6(\mathbf{Z})$, $\mathrm{GL}_3(\mathbf{Z})$ and $\mathrm{GL}_7(\mathbf{Z})$ for parts (a), (b) and (c) respectively.

It is appropriate to give a very short historical commentary. The problem solved by the construction A_n is rather old. A_2 is essentially in Euclid [Book X, Proposition 2]. The question of generalizing the Euclidean algorithm with an iterative process is implicit in Euler [Acta Acad. Sci. Imp. Petro. (1) **14** (1771), 188–214] and Lagrange [Leçons à l'école norm., 1795]. Hermite [Crelle's J. **40** (1850), 261–315] raised a related circle of questions. Iterative responses to Hermite's letters were made by Jacobi [Crelle's J. **69** (1868), 29–64] and Poincare [C. R. Acad. Sci. Paris **99** (1884), 1014–1016] and also a noniterative development by Minkowski [Acta Math. **26** (1902), 333–351], the latter subsequently improved by Mahler [J. Austral. Math. Soc. **4** (1964), 425–448]. Perron [Math. Ann. **64** (1907), 1–76] and Bernstein [Lecture Notes in Math. **207** (1971), 1–161] followed the Jacobi line and Brun [Treizième Congr. Math. Scand. Helsinki (1957), 46–64] followed Poincaré with counterexamples and improvements. Rosser [Proc. Nat. Acad. Sci. **27** (1941), 309–311] gave counterexamples to his proposal for dimensions above four. Simple counterexamples show that the Jacobi-Perron algorithm applied to an n-tuple can terminate without a relation. We have counterexamples to show that Brun's algorithm does not split for $n \geqslant 4$. We have several examples that suggest Szekeres' [Ann. Univ. Sci. Budapest, Eötvös Sect. Math. **13** (1970), 113–140] algorithm does not split for $n \geqslant 5$.

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