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, $\mathrm{row}_i M$ = ith row, $\mathrm{col}_j M$ = jth 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 $m \geqslant 1/$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.