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 Alg(n, Z). An iteration of Alg(n, Z) is defined
by three steps. Given n real numbers Alg(n, 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
GL(n, Z) matrix or the simultaneous approximations will be rows of GL(n, Z)
matrices constructed by Alg(n, Z). This algorithm characterizes linear inde-
dependence of reals over rationals by GL(n, Z) orbits of rank n — 1 matrices.

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

The algorithm \( \text{Alg}(n, \mathbb{Z}) \) 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 \( A \in GL(n, \mathbb{Z}) \)
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 \( \text{Alg}(n, \mathbb{Z}) \), 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
\( t \in \mathbb{R} \) and \( t \neq 0 \), set \( x = (ut, t) \), \( u \in \mathbb{R}^{n-1} \). Set \( P = \begin{bmatrix} w \\ v \end{bmatrix} \) where \( v \) is the last row of
\( P \). Note that \( xP = 0 \) implies \( uW = —v \).

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

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

Step 3ₙ. Let \( c \) be a nearest integral vector to \( B\hat{u}/u\hat{u}, c \in \mathbb{Z}^{n-1} \). Set \( A = \begin{bmatrix} B & c \\ 0 & 1 \end{bmatrix} \in \text{GL}(n, \mathbb{Z}) \).

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

Case \( n = 2 \), \( \text{Alg}(2, \mathbb{Z}) \), 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 \( \text{Alg}(n, \mathbb{Z}) \)). Note that if \( \text{Alg}(n, \mathbb{Z}) \) terminates, then a relation for \( x \) is a column of a \( \text{GL}(n, \mathbb{Z}) \) matrix constructed by a previous iteration of \( \text{Alg}(n, \mathbb{Z}) \).

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

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

\[
(*) \quad 0 < x\hat{x} \leq |AP||m|.
\]

Assume \( n > 1 \) and that the theorem is true for \( \text{Alg}(n - 1, \mathbb{Z}), \text{Alg}(n - 2, \mathbb{Z}), \ldots, \text{Alg}(1, \mathbb{Z}) \). Perform one iteration of \( \text{Alg}(n, \mathbb{Z}) \) upon \( x, P \) to construct the matrix \( A \in \text{GL}(n, \mathbb{Z}) \). 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 2ₙ, \( W = \hat{u}W/u\hat{u} + QW/u\hat{u} \). Hence by this expansion of \( W \) in terms of \( Q \) and \( uW = -v \),

\[
BW + cv = B\hat{u}W/u\hat{u} + BQW/u\hat{u} + cv = (c - B\hat{u}/u\hat{u})v + BQW/u\hat{u}.
\]

Therefore by the inequality of Step 2ₙ,

\[
|BW + cv| \leq |c - B\hat{u}/u\hat{u}| |v| + |BQW/u\hat{u}|
\leq (\sqrt{n-1} + \sqrt{n+1})|v|/2.
\]

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

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

Therefore

\[
(**) \quad |AP| < \frac{1}{2}\sqrt{1 + (5/n)}|P|.
\]

Set \( M_0 = I_n \) and iterate \( \text{Alg}(n, \mathbb{Z}) \) \( k \) times upon \( x, P \) (initially \( P = x\hat{x}I_n - \hat{x}x \)). Let \( M_k \in \text{GL}(n, \mathbb{Z}) \) be the product of the \( A \) and \( E \) matrices from Steps 3ₙ and 1ₙ up to and including the \( k \)th iteration, \( k \geq 0 \). If \( \text{Alg}(n, \mathbb{Z}) \) 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 \( \text{Alg}(n - 1, \mathbb{Z}), \text{Alg}(n - 2, \mathbb{Z}), \ldots \) terminate, then a relation for \( x \) has been constructed. If \( \text{Alg}(n, \mathbb{Z}) \) 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 \( m \in \mathbb{Z}^n, |m| \) cannot remain bounded and there are no relations for \( x \).
COROLLARY 1. If \( x \in \mathbb{R}^n \) has no relation, then for every \( \varepsilon > 0 \) \( \text{Alg}(n, \mathbb{Z}) \) constructs \( A \in \text{GL}(n, \mathbb{Z}) \) with each row less than distance \( \varepsilon \) from the line \( \mathbb{R}x \).

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 \( k \)th iteration of \( \text{Alg}(n, \mathbb{Z}) \) on \( x \). Since \( \text{Alg}(n, \mathbb{Z}) \) 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 \( \text{GL}(n, \mathbb{Z}) \) 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 \( \mathbb{Z} \)-linearly independent.

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

REFERENCES