Extending an orthonormal rational set of vectors into an orthonormal rational basis

Calvin Lin Zhiwei

August 17, 2006

Abstract

This paper was developed as an answer to a question posed at The University of Chicago's Research Experience for Undergraduates (REU) about the behaviour of rational matrices. The results here have direct application to questions about the volumes of lattice hypercubes in $4k + 2$ dimensions. The initial results about orthonormal basis in vector spaces over fields of characteristic zero have independent interest.

Definition. A rational vector is a vector whose coordinates are all rational. The vector is normal if the sum of the squares of its coordinates is equal to one. Two different vectors are orthonormal if their standard dot product is zero.

If we were working in $\mathbb{R}^n$, then the Gram-Schmidt procedure would extend any orthogonal set of vectors. However, this procedure requires division by the norm of the vector. It is not immediately obvious how this procedure can be adapted to work in $\mathbb{Q}^n$. In this paper, all vectors will be treated as column vectors. In particular, $\mathbf{e_j}$ refers to the j^{th} standard basis vector, 1 in the j^{th} entry and 0 otherwise.

Lemma. *Given a rational vector* $\mathbf{a}$ *with norm one, there exists a matrix* $A \in GL_n(\mathbb{Q})$ *such that the first column of the matrix is* $\mathbf{a}$ ($A\mathbf{e_1} = \mathbf{a}$) *and the columns of* A *are orthonormal.*

Proof. If $\mathbf{a} = \mathbf{e_1}$, take $A = I$. Now suppose $\mathbf{a} \neq \mathbf{e_1}$. Let the i^{th} coordinate of this vector be a_i. Consider the linear transformation that leaves the

vector $\mathbf{e_1} + \mathbf{a}$ fixed and reverses the direction of all other vectors orthogonal to $\mathbf{e_1} + \mathbf{a}$. The geometric interpretation of this linear transformation is a reflection through the vector $\mathbf{e_1} + \mathbf{a}$.

From the reflection, $A\mathbf{e_1} = \mathbf{a}$. Moreover, for all $i \neq 1$

$$A\mathbf{e_i} = 2\frac{\mathbf{e_i} \cdot (\mathbf{e_1} + \mathbf{a})}{||\mathbf{e_1} + \mathbf{a}||^2}(\mathbf{e_1} + \mathbf{a}) - \mathbf{e_i} = 2\frac{a_i}{2 + 2a_1}(\mathbf{e_1} + \mathbf{a}) - \mathbf{e_i}.$$

Since these vectors have rational coordinates, the entries of this matrix are rational. Also, this reflection preserves orthogonality and distance, hence the columns of A are orthonormal and thus form a basis for our space.

Note that $A^2 = AA^T = I$. □

Comment. *It can be verified that the following matrix in explicit form satisfies the conditions in the lemma.*

$$A = \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ a_2 & \frac{a_2^2 - a_1 - 1}{a_1 + 1} & \frac{a_2 a_3}{a_1 + 1} & \dots & \frac{a_2 a_n}{a_1 + 1} \\ a_3 & \frac{a_3 a_2}{a_1 + 1} & \frac{a_3^2 - a_1 - 1}{a_1 + 1} & \dots & \frac{a_3 a_n}{a_1 + 1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_n & \frac{a_n a_2}{a_1 + 1} & \frac{a_n a_3}{a_1 + 1} & \dots & \frac{a_n^2 - a_1 - 1}{a_1 + 1} \end{pmatrix}$$

Theorem. *In the vector space $\mathbb{Q}^n$, any set of orthonormal rational vectors can be extended to an orthonormal rational basis.*

Proof. We will prove this theorem by induction on n. The base case $n = 1$ is obvious.

For all n, if the set contains exactly one vector, the result follows from the previous lemma. Assume that the statement is true for $n-1$ and that our set contains two or more vectors. Take the k orthonormal vectors in $\mathbb{Q}^n$ labeled $\mathbf{v_1}, \mathbf{v_2}, \dots, \mathbf{v_k}$. Use $\mathbf{v_1}$ as vector $\mathbf{a}$ in the lemma to construct the matrix A and consider $A^{-1}\mathbf{v_1}, A^{-1}\mathbf{v_2}, \dots, A^{-1}\mathbf{v_k}$. Since $A^{-1}\mathbf{v_1} = \mathbf{e_1}$, the other $k - 1$ vectors lie in the subspace spanned by $\mathbf{e_2}, \mathbf{e_3}, \dots, \mathbf{e_n}$

By our induction hypothesis, in this subspace of $n - 1$ dimensions, the $k - 1$ rational vectors can be extended to an orthonormal rational basis. If we augment the vectors in this basis with 0 as the first entry and transform them by A, we get an extension of our n dimensional orthonormal rational vectors into an orthonormal rational basis. □

Comment. *This proof can be extended to any field of characteristic zero such as* $\mathbb{R}$ *and* $\mathbb{Q}_p$ *by replacing the word 'rational'.*

We will use this theorem to solve a problem posted by Dr. Paul Sally at the start of the REU.

Corollary. *Given* $M \in GL_n(\mathbb{Q}), M = \begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ a_{2,1} & a_{2,2} & \dots & a_{2,n} \\ a_{3,1} & a_{3,2} & \dots & a_{3,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n_2} & \dots & a_{n_n} \end{pmatrix}$, *such that* $M^T \cdot M = \operatorname{diag}(1, 1, \dots, 1, x, x)$. *Then,* x *can be written as the sum of squares of two rational numbers.*

Proof. Since x is the length of a vector and the determinant of $M^T M$ is not zero, we have $x > 0$.

Consider $L = \operatorname{diag}(1, 1, \dots, 1, \frac{1}{\sqrt{x}}, \frac{1}{\sqrt{x}})$. Since $L^T M^T M L = I$ and ML is in the orthogonal group $O_n(\mathbb{R})$, we have $LMM^T L^T = I$ and the sum of the squares of the entries of each row of ML equals 1. Thus,

$$a_{j,1}^2 + a_{j,2}^2 + \ldots + a_{j,n-2}^2 + \frac{1}{x} a_{j,n-1}^2 + \frac{1}{x} a_{j,n}^2 = 1$$

Given the first $n-2$ orthonormal rational column vectors in the matrix M, they can be extended to include two more orthonormal rational vectors b_1 and b_2 to form an orthonormal basis. Let $b_{j,i}$ refer to the j^{th} coordinate of the vector b_i. Since this is an orthonormal basis,

$$a_{j,1}^2 + a_{j,2}^2 + \ldots + a_{j,n-2}^2 + b_{j,1}^2 + b_{j,2}^2 = 1$$

Since the norm of b_1 is 1, it is non-zero in some coordinate k. Then,

$$\begin{aligned} x &= \frac{a_{k,n-1}^2 + a_{k,n}^2}{1 - a_{k,1}^2 - a_{k,2}^2 - \ldots - a_{k,n-2}^2} = \frac{a_{k,n-1}^2 + a_{k,n}^2}{b_{k,1}^2 + b_{k,2}^2} \\ &= \left(\frac{a_{k,n-1} b_{k,1} + a_{k,n} b_{k,2}}{b_{k,1}^2 + b_{k,2}^2} \right)^2 + \left(\frac{a_{k,n-1} b_{k,2} - a_{k,n} b_{k,1}}{b_{k,1}^2 + b_{k,2}^2} \right)^2 \end{aligned}$$

can be written as the sum of 2 rational squares. □

I would like to thank Robert Young, Jonathon Nieder and Nicholas Longo for helpful comments. Information about the volumes of lattice hypercubes in $\mathbb{R}^n$ can be found in [1].

References

[1] Judith Sally and Paul J. Sally Jr., *Developing Mathematics Vertically*, To be published.