Recent Progress in the Rational Factorisation of Integer Matrices

Matthew C. Lettington (Cardiff)

Joint with Nicholas J. Higham (Manchester) and Karl M. Schmidt (Cardiff)

Bohemian Matrices and Applications Minisymposium Part II
SIAM AN21, Spokane Washington 23rd July 2021
The Approach of Louis J. Mordell (1888-1972)

Mordell considered the similarity classes of $n \times n$ symmetric matrices with determinant 1.

He considered two such matrices $L$, $M$ to be in the same class if there exists a unimodular integral matrix $N$ such that $M = N^T LN$.

The number of such similarity classes is denoted by $h_n$.

Hence a matrix $M$ is in the similarity class of $I_n$ (the identity matrix) if and only if there exists a factorisation $M = N^T N$ with $N$ an integer matrix $N$. 

Historic Overview and Focus

Wilson's Matrix

The S+V Decomposition of Matrices

Some Theorems

Explicit Examples
The quadratic form classically associated with the symmetric matrix $M$, $q(x) = x^T M x$, can be written as

$$q(x) = x^T M x = x^T N^T N x = y^T y = \sum_{j=1}^{n} y_j^2,$$

where $y = Nx$, and $N$ has determinant 1. Thus, the factorisation can be used to write the quadratic form $q(x)$ as a sum of squares of $n$ linear factors.

When $n = 8$, such a factorisation may not exist.

Minkowski proved in 1911 that $h_n \geq [1 + n/8]$, so $h_n \geq 2$ if $n = 8$. Mordell showed (1938) that $h_8 = 2$, and Ko showed (1938) that $h_9 = 2$ as well.
In this talk, we revisit the question of integer matrix factorisation in the light of recent general results on matrix decompositions.

We establish that the existence of integer solutions to a certain quadratic equation is a necessary condition for a matrix factorisation of the type $M = N^T N$ (for symmetric positive definite $M$) to exist.

It is interesting to note that solutions to this new type of quadratic equation associated with a given integer matrix $M$ can also lead to rational matrix factors $N$ with entries in $\frac{1}{n^2} \mathbb{Z}$. 
Throughout this talk we use the classical example of the Wilson matrix

\[
W = \begin{pmatrix}
5 & 7 & 6 & 5 \\
7 & 10 & 8 & 7 \\
6 & 8 & 10 & 9 \\
5 & 7 & 9 & 10
\end{pmatrix}
\]  

(2)

This integer matrix has determinant 1 and hence an integer inverse matrix, but is moderately ill conditioned, despite its small size and entries. It has the integer factorisation \( W = Z^T Z \) discovered by the first two authors with

\[
Z = \begin{pmatrix}
2 & 3 & 2 & 2 \\
1 & 1 & 2 & 1 \\
0 & 0 & 1 & 2 \\
0 & 0 & 1 & 1
\end{pmatrix}
\]  

(3)

We note that the entries of \( Z \) are nonnegative and, although the matrix is not triangular, it has a block upper triangular structure and can be thought of as a block Cholesky factor of \( W \).
The Wilson Matrix II

The quadratic form associated with the Wilson matrix can be written, using (1) and (3), as a sum of four squares:

\[ q(x) = x^T W x = (2x_1 + 3x_2 + 2x_3 + 2x_4)^2 + (x_1 + x_2 + 2x_3 + x_4)^2 + (x_3 + 2x_4)^2 + (x_3 + x_4)^2 \]
\[ = y_1^2 + y_2^2 + y_3^2 + y_4^2. \]  

As \( Z \) is a unimodular integer matrix it has an integer inverse.

It follows by Lagrange’s four-square theorem that the quadratic form \( q \) generated by the Wilson matrix is universal in the sense that it generates all positive integers as \( x \) ranges over \( \mathbb{Z}^4 \).
Matrix Decompositions I

The following symmetries of $n \times n$ matrices were considered by the second two authors.

(S) A matrix $M = (m_{i,j})_{i,j=1}^n \in \mathbb{R}^{n \times n}$ has the constant sum property (or is of type S) if there is a number $w \in \mathbb{R}$, called the weight of the matrix, such that

$$\sum_{j=1}^n m_{i,j} = \sum_{j=1}^n m_{j,i} = nw \quad (i \in \{1, \ldots, n\}).$$

The vector subspace of $\mathbb{R}^{n \times n}$ of matrices having the constant sum property with some weight is denoted by $S_n$ and can be characterised as

$$S_n = \{ M \in \mathbb{R}^{n \times n} : 1_n^T M u = 0 = u^T M 1_n \ (u \in \{1_n\}^\perp) \},$$

where $1_n \in \mathbb{R}^n$ is the column vector with all entries equal to 1 and orthogonality is with respect to the standard inner product, $\{1_n\}^\perp = \{ u \in \mathbb{R}^n : u^T 1_n = 0 \}$. 
(V) A matrix $M = (m_{i,j})_{i,j=1}^n \in \mathbb{R}^{n \times n}$ has the vertex cross sum property (or is of type V) if

$$m_{i,j} + m_{k,l} = m_{i,l} + m_{k,j} \quad (i, j, k, l \in \{1, \ldots, n\})$$

and the matrix entries sum to zero, $\sum_{i,j=1}^n m_{i,j} = 0$. The vector subspace of $\mathbb{R}^{n \times n}$ of matrices having the vertex cross sum property is denoted by $V_n$ and can be characterised as

$$V_n = \{ M \in \mathbb{R}^{n \times n} : u^T M v = 0 \ (u, v \in \{1_n\}^\perp), \ 1_n^T M 1_n = 0 \} \quad (5)$$
Matrix Decompositions III

The decompositions are unique and the odd and even parts of the decomposition orthogonal w.r.t. the Frobenius norm.

For the integer factor $Z$ of the Wilson matrix we find that the $S \oplus V$ decomposition $Z = Z_V + Z_S + w_Z \mathcal{E}_4$ is given by

$$Z = Z_V + Z_S + w_Z \mathcal{E}_4$$

$$= \frac{1}{8} \begin{pmatrix} 5 & 7 & 11 & 11 \\ -3 & -1 & 3 & 3 \\ -7 & -5 & -1 & -1 \\ -9 & -7 & -3 & -3 \end{pmatrix} + \frac{1}{16} \begin{pmatrix} 3 & 15 & -9 & -9 \\ 3 & -1 & 7 & -9 \\ -5 & -9 & -1 & 15 \\ -1 & -5 & 3 & 3 \end{pmatrix} + \frac{19}{16} \mathcal{E}_4,$$

so that $Z$ has weight $w_Z = \frac{19}{16}$ and, the entries of $Z_V$ and $Z_S$ are in $\frac{1}{16} \mathbb{Z}$.

**Theorem 1**

A matrix $M \in \mathbb{R}^{n \times n}$ is an element of $V_n$ if and only if there exist vectors $a, b \in \{1_n\}^\perp$ such that $M = a1_n^T + 1_n b^T$. 
Main Results I

For the Wilson matrix $W$ this decomposition takes the form

$$16W = 14 \begin{pmatrix} -27 \\ 9 \\ 13 \\ 5 \end{pmatrix}^T + \begin{pmatrix} -27 \\ 9 \\ 13 \\ 5 \end{pmatrix} 1_4^T + \begin{pmatrix} 15 & 11 & -9 & -17 \\ 11 & 23 & -13 & -21 \\ -9 & -13 & 15 & 7 \\ -17 & -21 & 7 & 31 \end{pmatrix} + 119E_4$$

Theorem 2

Let $M = (m_{i,j}) \in \mathbb{R}^{n \times n}$. Then there is a unique decomposition

$$M = M_V + M_0 + (\text{wt } M) E_n,$$

where $M_0 \in S_n$ with weight 0 and $M_V = a1_n^T + 1_nb^T \in V_n$, and the entries of the vectors $a$ and $b$ are given by

$$a_i = \frac{1}{n} \sum_{j=1}^{n} m_{i,j} - \text{wt } M \quad (i \in \{1, \ldots, n\}),$$

$$b_j = \frac{1}{n} \sum_{i=1}^{n} m_{i,j} - \text{wt } M \quad (j \in \{1, \ldots, n\}).$$

In particular, if $M$ is an integer matrix then the vectors $n^2a$ and $n^2b$ have integer entries.
Main Results II

**Theorem 3**
Given a symmetric matrix $M \in \mathbb{Z}^{n \times n}$, it is necessary for the existence of a factorisation $M = N^T N$ with $N \in \mathbb{Z}^{n \times n}$ that $n^2 \text{wt} N \in \mathbb{Z}$ and that the vector components $n^2 a_j, n^2 b_j \in \mathbb{Z}$ ($j \in \{1, \ldots, n\}$), where $N = a1_n^T + 1_n b^T + N_0 + w_N \mathcal{E}_n$ is the decomposition of $N$, form a solution of the quadratic equation

$$n^4 \text{wt} M = n (n^2 \text{wt} N)^2 + \sum_{j=1}^{n} (n^2 a_j)^2.$$ 

**Theorem 4**
Using the decomposition $M = y 1_n^T + 1_n y^T + M_0 + (\text{wt} M) \mathcal{E}_n$, we have $b = \frac{1}{n \text{wt} N} (y - N_0^T a)$. Hence matrix factors correspond to solutions $N_0$ of the quadratic matrix equation

$$N_0^T (aa^T + n^2 w_N^2 \mathbb{I}_n) N_0 - N_0^T ay^T - ya^T N_0 = n^2 w_N^2 M_0 - yy^T. \quad (6)$$
The quadratic equation arising from balancing the weights in the assumed factorisation of the Wilson matrix $W = Z^T Z$ is

$$\text{wt } W = \frac{119}{16} = a_1^2 + a_2^2 + a_3^2 + a_4^2 + 4w_Z^2$$

$$= 2(a_1^2 + a_2^2 + a_3^2 + a_1a_2 + a_1a_3 + a_2a_3) + 4w_Z^2,$$

as $a_4 = -a_1 - a_2 - a_3$. Clearing fractions and setting $x_i = 16a_i$, $w = 16w_Z$, we find that a necessary condition for the integer factorisation of the Wilson matrix is that there are integer solutions to the quadratic equation

$$2w^2 + x_1^2 + x_1x_2 + x_1x_3 + x_2^2 + x_2x_3 + x_3^2 = 952.$$

Solving this equation for $w, x_1, x_2, x_3$ in Mathematica 11.0 on a PC with a Intel Core i7 6500CPU, gave the 1728 solutions in just under 6 seconds.
Exactly one third (576) of these solutions lead to rational matrix factorisations $W = Z^T Z$ with $Z \in \frac{1}{16} \mathbb{Z}^{4 \times 4}$.

The process of converting solutions into matrix factors, i.e. of finding suitable vectors $b$ and matrices $N_0$ satisfying the equations of Theorem 4, took considerably longer at 34 minutes.

The approach involved utilising (6), in which the vector $b$ is eliminated and the right-hand-side completely determined for a given factor weight $w_N$.

Substituting potential solutions for the vector $a$ and weight $w_N$ thus reduces the general problem of finding the matrix $N_0$ to that of an $(n - 1) \times (n - 1)$ unknown matrix.
For the Wilson matrix the 576 matrix factors split naturally into 3 classes, where any two elements in the same class are related by an integer orthogonal matrix.

If $M = N^T N$ and $U$ is an integer orthogonal matrix, then $UN$ is another solution of the factorisation problem.

Conversely, if $\det M = 1$ and $N$ and $N'$ are solutions with integer entries, then $N' = UN$, where $U = N' N^{-1}$ is an integer orthogonal matrix.

It can be shown that any integer orthogonal matrix is a signed permutation matrix, i.e. a matrix which has exactly one non-zero entry, either 1 or $-1$, in each row and in each column.
For the Wilson matrix the 3 classes of matrix factors with entries in $\frac{1}{16}\mathbb{Z}$, can be represented by the integer matrix factor $Z$ and the two rational matrix factors

$$Z' = \begin{pmatrix} \frac{1}{2} & 1 & 0 & 1 \\ \frac{3}{2} & 2 & 3 & 3 \\ \frac{1}{2} & 1 & 0 & 0 \\ \frac{3}{2} & 2 & 1 & 0 \end{pmatrix}, \quad Z'' = \begin{pmatrix} \frac{3}{2} & 2 & 2 & 2 \\ \frac{3}{2} & 2 & 2 & 1 \\ \frac{1}{2} & 1 & 1 & 2 \\ -\frac{1}{2} & -1 & 1 & 1 \end{pmatrix}, \quad (7)$$

where any two elements in the same class are related by an integer orthogonal matrix.

The three factorisations $W = Z^TZ = Z'^TZ' = Z''^TZ''$ correspond to the solutions $(w, x_1, x_2, x_3) = (19, 17, 1, -7)$, $(w, x_1, x_2, x_3) = (18, -8, 20, -12)$ and $(w, x_1, x_2, x_3) = (19, 11, 7, -1)$, respectively.

Note that $Z'$ and $Z''$ are not integer matrices, so the equivalence class of $Z$ comprises all integer factorisations of the Wilson matrix.
Thank you for listening!
Historic Overview and Focus

Wilson's Matrix

The S+V Decomposition of Matrices

Some Theorems

Explicit Examples


C. B. Moler, *Reviving Wilsons matrix*,