A matrix approach to Yang multiplication, I

Akihiro Munemasa
Tohoku University

July 24, 2017
International Conference and PhD-Master Summer School
“Groups and Graphs, Metrics and Manifolds”
Ural Federal University
About this talk

Part I:

- Hadamard’s inequality
- Hadamard matrices and generalizations
- Constructions of Hadamard matrices
- Quaternions and Lagrange’s identity
- Yang’s generalization of Lagrange’s identity
- Yang’s theorem

Part II:

- Complementary sequences
- A Laurent polynomial associated to a sequence
- A two-variable Laurent polynomial associated to a matrix
- A new proof of Yang’s theorem using matrices
Hadamard’s inequality for an $n \times n$ matrix $X$

$$\det(X) = \sum_{\sigma \in S_n} \text{sgn}(\sigma) \prod_{i=1}^{n} x_{i,\sigma(i)}.$$

This is a polynomial function in $n^2$ variables $x_{ij}$.

The function $\det : [-1, 1]^{n^2} \rightarrow \mathbb{R}$ takes maxima and minima, but they are not fully understood.

This is not a problem in multivariable calculus, rather, a combinatorial problem.

$\det$ is linear in each variable,

$\implies$ maxima and minima occur at end points

$\implies$ enough to consider

$$\det : \{-1, 1\}^{n^2} \rightarrow \mathbb{Z}.$$
Let $G = XX^\top$. Then $G_{ii} = n$. Let

$$\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n \geq 0.$$ 

be the eigenvalues of $G$. Then by the arithmetic-geometric mean,

$$\det(X)^2 = \det G = \prod_{i=1}^{n} \lambda_i \leq \left( \frac{1}{n} \sum_{i=1}^{n} \lambda_i \right)^n = \left( \frac{1}{n} \text{tr } G \right)^n = \left( \frac{1}{n} n^2 \right)^n = n^n.$$

$$|\det X| \leq n^{n/2} \text{ with equality iff } G = nI,$$

or equivalently, rows of $X$ are pairwise orthogonal.
Hadamard matrices

A matrix $H \in \{-1, 1\}^{n \times n}$ is called a Hadamard matrix if $HH^\top = nI$.

Examples (Sylvester matrices):

$$[1], \quad \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \ldots$$

For $n = 3$:

$$\begin{bmatrix} 1 & 1 & 1 \\ \pm1 & \pm1 & \pm1 \end{bmatrix}$$

impossible. In fact, $4 \mid n$ is necessary:

$$\begin{bmatrix} 1 \cdots 1 & 1 \cdots 1 & 1 \cdots 1 & 1 \cdots 1 \\ 1 \cdots 1 & 1 \cdots 1 & -1 \cdots -1 & -1 \cdots -1 \\ 1 \cdots 1 & -1 \cdots -1 & 1 \cdots 1 & -1 \cdots -1 \end{bmatrix}$$
The Hadamard conjecture

If a Hadamard matrix of order $n$ exists, then $n = 1, 2$ or $4 \mid n$. Conversely,

Conjecture

\[ 4 \mid n \implies \exists \text{Hadamard matrix of order } n. \]

Before proceeding further into this combinatorial problem, let me digress into topology.
Complex Hadamard matrices

Instead of
\[ \det : \{-1, 1\}^{n^2} \rightarrow \mathbb{Z}, \]
consider
\[ \det : (S^1)^{n^2} \rightarrow \mathbb{C}, \]
where \( S^1 = \{ z \in \mathbb{C} \mid z\overline{z} = 1 \} \).
With \( G = XX^*, \ X \in (S^1)^{n \times n}, \)

\[ |\det(X)|^2 = \det G = \prod_{i=1}^{n} \lambda_i \leq \left( \frac{1}{n} \sum_{i=1}^{n} \lambda_i \right)^n \]

\[ = \left( \frac{1}{n} \text{tr} \ G \right)^n = \left( \frac{1}{n} n^2 \right)^n = n^n. \]

Equality holds iff rows of \( X \) are pairwise orthogonal.
A matrix $H \in (S^1)^{n \times n}$ is called a complex Hadamard matrix if $HH^* = nI$.

Examples: (ordinary) Hadamard matrices, the character tables of abelian groups.

What is

$$\{H \in (S^1)^{n \times n} \mid HH^* = nI\}/\left(\text{left and right multiplication by monomial matrices}\right),$$

for $n \geq 6$?

A matrix $H \in (\mathbb{C}^\times)^{n \times n}$ is called an inverse-orthogonal matrix if $H(H^{(-1)})^\top = nI$, where 

$$H^{(-1)} = \text{elementwise inverse of } H.$$ 

Complex Hadamard $\implies$ inverse-orthogonal.
Jones (1989) defined a “spin model” which is a special class of inverse-orthogonal matrices. 
Jaeger (1992) “Strongly regular graphs and spin models...”:
Higman-Sims (sporadic finite simple group $\rightarrow$ strongly regular graph $\rightarrow$ spin model).
Back to real Hadamard matrices

**Conjecture**

\[ 4 \mid n \implies \exists \text{Hadamard matrix of order } n. \]

- If \( H_1 \) and \( H_2 \) are Hadamard matrices, then so is \( H_1 \otimes H_2 \).
- In particular, for every \( n \in \mathbb{N} \), there exists a Hadamard matrix of order \( 2^n \).
- Paley (1933): if \( p \equiv 3 \pmod{4} \) is a prime, then there exists a skew Hadamard matrix \( H \) of order \( p + 1 \) such that \( H + H^\top = 2I \).

Yet we do not know

\[
\liminf_{N \to \infty} \left\{ \frac{|\{n \mid 1 \leq n \leq N, \exists \text{Hadamard matrix of order } n\}|}{N} \right\} > 0.
\]
A Hadamard matrix is said to be regular if it has constant row and column sums.

**Theorem (Goethals-Seidel (1970))**

Symmetric regular Hadamard matrices with constant diagonal are equivalent to strongly regular graphs with Latin square or negative Latin square parameters:

\[(v, k, \lambda, \mu) = (4m^2, m(2m \pm 1), (m \pm 1)(m \pm 2) \mp 2m - 2, m(m \pm 1)).\]
Circulant Hadamard matrices

Cyclic symmetry:

\[
\begin{pmatrix}
-1 & 1 & 1 & 1 \\
1 & -1 & 1 & 1 \\
1 & 1 & -1 & 1 \\
1 & 1 & 1 & -1 \\
\end{pmatrix}
\]

is a circulant Hadamard matrix.

Conjecture

There is no circulant Hadamard matrix of order \( n > 4 \).
\[
\begin{bmatrix}
1 & 1 \\
-1 & 1
\end{bmatrix} \to \begin{bmatrix}
a & b \\
b & a
\end{bmatrix} \to \begin{bmatrix}
A & B \\
-B & A
\end{bmatrix}
\]

\[
A(-BR)\top + (BR)A\top = 0?
\]

\[
\begin{bmatrix}
A & BR \\
- BR & A
\end{bmatrix}
\]

\[
A(-BR)\top + (BR)A\top = -ARB\top + BRA\top \quad \text{if } R = R\top,
\]

\[
= -ABR + BAR \quad \text{if } BR = RB\top, \ AR = RA\top
\]

\[
= 0 \quad \text{if } AB = BA.
\]
Let

\[
H = \begin{bmatrix}
A & BR & CR & DR \\
- BR & A & -D^\top R & C^\top R \\
- CR & D^\top R & A & -B^\top R \\
- DR & -C^\top R & B^\top R & A
\end{bmatrix}, \quad R = \begin{bmatrix}
1 & \cdot \\
\cdot & \cdot \\
\cdot & \cdot \\
1 & \cdot
\end{bmatrix}
\]

If \(A, B, C, D\) are circulant and

\[
AA^\top + BB^\top + CC^\top + DD^\top = 4nI,
\]

then rows of \(H\) are pairwise orthogonal.

A Hadamard matrix of order \(4n\) has \((4n)^2\) entries, while four circulant matrices \(A, B, C, D\) can be specified only by a total of \(4n\) entries.
Quaternions

Goethals-Seidel array:

\[
\begin{bmatrix}
A & BR & CR & DR \\
-BR & A & -D^\top R & C^\top R \\
-CR & D^\top R & A & -B^\top R \\
-DR & -C^\top R & B^\top R & A \\
\end{bmatrix}
\]

\[
Y = \begin{bmatrix}
a & b & c & d \\
-b & a & -d & c \\
-c & d & a & -b \\
-d & -c & b & a \\
\end{bmatrix} = a1 + bi + cj + dk
\]

\[
i^2 = j^2 = k^2 = -1,
\]

\[
ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j.
\]

\[
\det Y = (a^2 + b^2 + c^2 + d^2)^2 = |a1 + bi + cj + dk|^4.
\]
\[ \mathbb{H} = \{ a1 + bi + cj + dk \mid a, b, c, d \in \mathbb{R} \} . \]

\[ i^2 = j^2 = k^2 = -1, \]
\[ ij = -ji = k, \ jk = -kj = i, \ ki = -ik = j. \]

For \( Y = a1 + bi + cj + dk \in \mathbb{H} \), define the norm by
\[ |Y| = \sqrt{a^2 + b^2 + c^2 + d^2} . \]

Then
\[ |YZ| = |Y||Z| \quad (Y, Z \in \mathbb{H}) . \]

\[ Y = a1 + bi + cj + dk, \]
\[ Z = e1 + fi + gj + hk, \]
\[ YZ = q1 + ri + sj + tk, \]
\[ q^2 + r^2 + s^2 + t^2 = (a^2 + b^2 + c^2 + d^2)(e^2 + f^2 + g^2 + h^2) . \]
Lagrange’s identity

Hamilton (1843); Lagrange (1770)

\[ Y = a_1 + b_1 + c_1 + d_1, \]
\[ Z = e_1 + f_1 + g_1 + h_1, \]
\[ YZ = q_1 + r_1 + s_1 + t_1. \]

\[ q^2 + r^2 + s^2 + t^2 = (a^2 + b^2 + c^2 + d^2)(e^2 + f^2 + g^2 + h^2). \]

\[ q = ae - bf - cg - dh, \]
\[ r = af + be + ch - dg, \]
\[ s = ag - bh + ce + df, \]
\[ t = ah + bg - cf + de. \]

Every natural number is a sum of four integer squares.
Generalization of Lagrange identity by Yang (1983)

\[ q^2 + r^2 + s^2 + t^2 = (a^2 + b^2 + c^2 + d^2)(e^2 + f^2 + g^2 + h^2). \]

\[ q = ae - bf - cg - dh, \]
\[ r = af + be + ch - dg, \]
\[ s = ag - bh + ce + df, \]
\[ t = ah + bg - cf + de. \]

In a commutative ring with automorphism \( \ast \) satisfying \( \ast^2 = \text{id} \), replace \( x^2 \) by \( xx^\ast \) for \( x \in \{a, b, \ldots, t\} \), to get

\[ qq^\ast + rr^\ast + ss^\ast + tt^\ast \]
\[ = (aa^\ast + bb^\ast + cc^\ast + dd^\ast)(ee^\ast + ff^\ast + gg^\ast + hh^\ast). \]
Generalization of Lagrange identity by Yang (1983)

\[ qq^* + rr^* + ss^* + tt^* = (aa^* + bb^* + cc^* + dd^*)(ee^* + ff^* + gg^* + hh^*) \]

if

\[ q = ae - bf - cg - dh \rightarrow a^*e - b^*f - c^*g - d^*h \]
\[ r = af + be + ch - dg \rightarrow a^*f + b^*e + c^*h - d^*g \]
\[ s = ag - bh + ce + df \rightarrow a^*g - b^*h + c^*e + d^*f \]
\[ t = ah + bg - cf + de \rightarrow a^*h + b^*g - c^*f + d^*e \]

Yang used this for the Laurent polynomial ring \( \mathbb{Z}[x^{\pm 1}] \) with
\[ * : x \mapsto x^{-1}. \]
Composition of $\{\pm 1\}$-sequences: a method to produce long sequences from short ones.

$a, b, c, d, e, f, g, h$ are “nice” $\{\pm 1\}$-sequences

$\implies q, r, s, t$ can be used to build circulant matrices

$A, B, C, D$ with $AA^\top + BB^\top + CC^\top + DD^\top = 4nI$

$\implies$ (Goethals-Seidel array) Hadamard matrix

The proof is constructive but it has no explanation. We expanded the original proof (9 lines) to a 9 page paper (arXiv:1705.05062v2), which will be explained in detail in my second talk.