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

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

This is a polynomial function in n^2 variables x_{ij}.
The function $\det : [-1,1]^{n^2} \to \mathbb{R}$ 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

$$\det : \{-1,1\}^{n^2} \to \mathbb{Z}.$$

$X \in \{-1,1\}^{n\times n}$

Let $G = XX^\top$. Then $G_{ii} = n$. Let

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

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

$$\begin{aligned}\det(X)^2 = \det G = \prod_{i=1}^{n} \lambda_i &\le \left(\frac{1}{n}\sum_{i=1}^{n}\lambda_i\right)^n \\ &= \left(\frac{1}{n}\operatorname{tr} G\right)^n = \left(\frac{1}{n}n^2\right)^n = n^n.\end{aligned}$$

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

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):

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

For $n = 3$:

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

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

$$4 \mid n \implies \exists \textit{Hadamard matrix of order } n.$$

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

Complex Hadamard matrices

Instead of

$$\det : \{-1,1\}^{n^2} \to \mathbb{Z},$$

consider

$$\det : (S^1)^{n^2} \to \mathbb{C},$$

where $S^1 = \{z \in \mathbb{C} \mid z\bar{z} = 1\}$.
With $G = XX^*$, $X \in (S^1)^{n \times n}$,

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

Equality holds iff rows of X are pairwise orthogonal.

Complex Hadamard matrices

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

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

for $n \geq 6$?
The 5th workshop on Real and Complex Hadamard Matrices and Applications, 10–14 July, 2017, Budapest.

Inverse orthogonal matrices and spin models

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

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

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).
Jaeger (1996), Jaeger-Matsumoto-Nomura (1998): spin models $\rightarrow$ association schemes

Back to real Hadamard matrices

Conjecture

$$4 \mid n \implies \exists \textit{Hadamard matrix of order } n.$$

- 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

$$\liminf_{N\to\infty} \frac{|\{n \mid 1 \le n \le N,\ \exists \text{Hadamard matrix of order } n\}|}{N} > 0.$$

Symmetric regular Hadamard matrices

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:

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

is a circulant Hadamard matrix.

Conjecture

There is no circulant Hadamard matrix of order $n > 4$.

2×2 block matrices, dihedral group

$$\begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \to \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \to \begin{bmatrix} A & B \\ -B & A \end{bmatrix}? \quad (A(-B)^\top + BA^\top = 0?)$$

$$\begin{bmatrix} A & BR \\ -BR & A \end{bmatrix}$$

$$\begin{aligned} & A(-BR)^\top + (BR)A^\top \\ &= -ARB^\top + BRA^\top && \text{if } R = R^\top, \\ &= -ABR + BAR && \text{if } BR = RB^\top,\ AR = RA^\top \\ &= 0 && \text{if } AB = BA. \end{aligned}$$

Goethals-Seidel (1970)

Let

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

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.

Quaterninons

Goethals-Seidel array:

$$\begin{bmatrix} \boldsymbol{A} & \boldsymbol{B}\boldsymbol{R} & \boldsymbol{C}\boldsymbol{R} & \boldsymbol{D}\boldsymbol{R} \\ -\boldsymbol{B}\boldsymbol{R} & \boldsymbol{A} & -\boldsymbol{D}^\top\boldsymbol{R} & \boldsymbol{C}^\top\boldsymbol{R} \\ -\boldsymbol{C}\boldsymbol{R} & \boldsymbol{D}^\top\boldsymbol{R} & \boldsymbol{A} & -\boldsymbol{B}^\top\boldsymbol{R} \\ -\boldsymbol{D}\boldsymbol{R} & -\boldsymbol{C}^\top\boldsymbol{R} & \boldsymbol{B}^\top\boldsymbol{R} & \boldsymbol{A} \end{bmatrix}$$

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

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

$$\det \boldsymbol{Y} = (a^2 + b^2 + c^2 + d^2)^2 = |a1 + bi + cj + dk|^4.$$

Quaterninons

$$\mathbb{H} = \{a1 + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}.$$

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

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)

$$\begin{aligned} Y &= a1 + bi + cj + dk, \\ Z &= e1 + fi + gj + hk, \\ YZ &= q1 + ri + sj + tk. \end{aligned}$$

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

$$\begin{aligned} q &= ae - bf - cg - dh, \\ r &= af + be + ch - dg, \\ s &= ag - bh + ce + df, \\ t &= ah + bg - cf + de. \end{aligned}$$

Every natural number is a sum of four integer squares.

Generalization of Lagrange identity by Yang (1983)

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

$$\begin{aligned} q &= ae - bf - cg - dh, \\ r &= af + be + ch - dg, \\ s &= ag - bh + ce + df, \\ t &= ah + bg - cf + de. \end{aligned}$$

In a commutative ring with automorphism $*$ satisfying $*^2 = \mathrm{id}$, replace x^2 by xx^* for $x \in \{a, b, \dots, t\}$, to get

$$\begin{aligned} &qq^* + rr^* + ss^* + tt^* \\ &= (aa^* + bb^* + cc^* + dd^*)(ee^* + ff^* + gg^* + hh^*). \end{aligned}$$

Generalization of Lagrange identity by Yang (1983)

$$\begin{aligned} &qq^* + rr^* + ss^* + tt^* \\ &= (aa^* + bb^* + cc^* + dd^*)(ee^* + ff^* + gg^* + hh^*) \end{aligned}$$

if

$$\begin{aligned} q &= ae - bf - cg - dh \to a^*e - bf^* - cg^* - dh^* \\ r &= af + be + ch - dg \to af^* + b^*e + ch - dg \\ s &= ag - bh + ce + df \to ag^* - bh + c^*e + df \\ t &= ah + bg - cf + de \to ah^* + bg - cf + d^*e \end{aligned}$$

Yang used this for the Laurent polynomial ring $\mathbb{Z}[x^{\pm 1}]$ with $* : x \mapsto x^{-1}$.

Yang (1989)

Composition of $\{\pm 1\}$-sequences: a method to produce long sequences from short ones.

$\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{d}, \boldsymbol{e}, \boldsymbol{f}, \boldsymbol{g}, \boldsymbol{h}$ are "nice" $\{\pm 1\}$-sequences
$\Longrightarrow$ $\boldsymbol{q}, \boldsymbol{r}, \boldsymbol{s}, \boldsymbol{t}$ can be used to build circulant matrices
$\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}, \boldsymbol{D}$ with $\boldsymbol{A}\boldsymbol{A}^\top + \boldsymbol{B}\boldsymbol{B}^\top + \boldsymbol{C}\boldsymbol{C}^\top + \boldsymbol{D}\boldsymbol{D}^\top = 4\boldsymbol{n}\boldsymbol{I}$
$\Longrightarrow$ (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.