A matrix approach to Yang multiplication, II

Akihiro Munemasa
Tohoku University
(joint work with Pritta Etriana Putri)

July 25, 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 matrices

A matrix $\boldsymbol{H} \in \{-1,1\}^{n\times n}$ is called a Hadamard matrix if $\boldsymbol{H}\boldsymbol{H}^\top = n\boldsymbol{I}$.
Examples (Sylvester matrices):

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

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

Conjecture

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

Goethals-Seidel (1970)

Let A, B, C, D be circulant matrices of order n, and

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

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

then

$$HH^\top = 4nI,$$

because

$$R^{-1} = R^\top,\ XR = RX^\top,\ XY = YX$$

for $X, Y \in \{A, B, C, D\}$.

$AA^\top + BB^\top + CC^\top + DD^\top = 4nI$

$$\begin{aligned}
&\{n \times n \text{ Circulant matrices with entries in } \mathbb{Z}\} \\
&= \text{Group algebra of the cyclic group } C_n \text{ over } \mathbb{Z} \\
&= \mathbb{Z}[x]/(x^n - 1) \leftarrow \mathbb{Z}[x, x^{-1}]
\end{aligned}$$

If A is the circulant matrix with first row

$$a = (a_0, a_1, \dots, a_{n-1}) \in \{\pm 1\}^n, \quad A \leftarrow\!\!\shortmid \sum_{i=0}^{n-1} a_i x^i = f_a(x)$$

Then $A^\top \leftarrow\!\!\shortmid f_a(x^{-1})$, so

$$\begin{aligned}
AA^\top &\iff f_a(x) f_a(x^{-1}) \bmod (x^n - 1) \\
&\Longleftarrow f_a(x) f_a(x^{-1}).
\end{aligned}$$

$AA^\top + BB^\top + CC^\top + DD^\top = 4nI$

Given $a, b, c, d \in \{\pm 1\}^n$, form circulant matrices A, B, C, D with first row a, b, c, d, respectively. Then

$$AA^\top + BB^\top + CC^\top + DD^\top = 4nI$$

is equivalent to

$$f_a(x)f_a(x^{-1}) + f_b(x)f_b(x^{-1}) + f_c(x)f_c(x^{-1}) + f_d(x)f_d(x^{-1}) \equiv 4n \pmod{(x^n - 1)}$$

which will follow if

$$f_a(x)f_a^*(x) + f_b(x)f_b^*(x) + f_c(x)f_c^*(x) + f_d(x)f_d^*(x) = 4n,$$

where $f^*(x) = f(x^{-1})$ for $f(x) \in \mathbb{Z}[x, x^{-1}]$.

Complementary sequences

A quadruple (a, b, c, d) of sequences of integers is said to be complementary if

$$f_a(x)f_a^*(x) + f_b(x)f_b^*(x) + f_c(x)f_c^*(x) + f_d(x)f_d^*(x) \in \mathbb{Z}.$$

We do not assume, a, b, c, d have the same length, nor entries are in $\{\pm 1\}$. But if $a, b, c, d \in \{\pm 1\}^n$, then the constant term of the left-hand side is $4n$.

Example (base seq. and non-periodic complementary seq.):

$$BS(m, n) \subset \{\pm 1\}^m \times \{\pm 1\}^m \times \{\pm 1\}^n \times \{\pm 1\}^n,$$
$$NCS(n) \subset (\{\pm 1\}^n)^4.$$

Recall $NCS(n) \neq \emptyset \implies \exists$Hadamard matrix of order $4n$

From BS to NCS

C.H. Yang (Proc. A.M.S., 1989), Theorem 4, states

$$\begin{aligned} & BS(m+1,m) \neq \emptyset,\ BS(n+1,n) \neq \emptyset \\ & \implies NCS((2m+1)(2n+1)) \neq \emptyset \\ & (\implies \exists \text{Hadamard matrix}). \end{aligned}$$

Conjecture $BS(n+1,n) \neq \emptyset$ for all n.
In this talk: a matrix approach to prove this theorem.
Is the proof difficult?
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 I now explain in detail.

Yang Multiplication Theorem

$$
\begin{aligned}
(a, b, c, d) &\in BS(m+1, m) \\
&\subset \{\pm 1\}^{m+1} \times \{\pm 1\}^{m+1} \times \{\pm 1\}^{m} \times \{\pm 1\}^{m}, \\
(f, g, h, e) &\in BS(n+1, n) \\
&\subset \{\pm 1\}^{n+1} \times \{\pm 1\}^{n+1} \times \{\pm 1\}^{n} \times \{\pm 1\}^{n},
\end{aligned}
$$

$$
\begin{aligned}
(a', b', c', d') &\in (\{0, \pm 1\}^{2m+1})^4, \\
(f', g', h', e') &\in (\{0, \pm 1\}^{2n+1})^4.
\end{aligned}
$$

Our matrix approach:

$$
\begin{aligned}
(Q, R, S, T) &\in (\{\pm 1\}^{(2n+1)\times(2m+1)})^4, \\
(q, r, s, t) &\in NCS((2m+1)(2n+1)), \\
Q &= {f'^*}^{\top} a' + {g'}^{\top} c' - {e'}^{\top} b'^* + {h'}^{\top} d'.
\end{aligned}
$$

Lagrange identity

Let $\mathcal{R}$ be a commutative ring with involutive automorphism $*$. Let $a, b, c, d, f, g, h, e \in \mathcal{R}$. Set

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

Then

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

We use this with

$$\mathcal{R} = \mathbb{Z}[x^{\pm 1}, y^{\pm 1}],\ * : x \mapsto x^{-1},\ y \mapsto y^{-1}.$$

The polynomials $f_a(x)$ and $\psi_a(x)$

For $a = (a_0, \dots, a_{n-1}) \in \mathbb{Z}^n$.
recall

$$f_a(x) = \sum_{i=0}^{n-1} a_i x^i.$$

It is more convenient to use

$$\psi_a(x) = x^{1-n} f_a(x^2).$$

Example: $a = (a_0, a_1, a_2, a_3)$, $b = (b_0, b_1, b_2)$

$$\begin{aligned} f_a(x) &= a_0 + a_1 x + a_2 x^2 + a_3 x^3, \\ \psi_a(x) &= a_0 x^{-3} + a_1 x^{-1} + a_2 x^{1} + a_3 x^{3}, \\ f_b(x) &= b_0 + b_1 x + b_2 x^2, \\ \psi_b(x) &= b_0 x^{-2} + b_1 x^{0} + b_2 x^{2}. \end{aligned}$$

Yang Multiplication Theorem (C.H. Yang, 1989)

$$(a, b, c, d) \in BS(m+1, m), \quad (f, g, h, e) \in BS(n+1, n).$$

Then $\exists(q, r, s, t) \in NCS((2m+1)(2n+1))$.
Yang's approach: produce a sequence q with

$$\begin{aligned} f_q(x) = {} & f_a(x^2) f_{f^*}(x^{2(2m+1)}) + x f_c(x^2) f_g(x^{2(2m+1)}) \\ & - x^{2m+1} f_{b^*}(x^2) f_e(x^{2(2m+1)}) \\ & + x^{2m+2} f_d(x^2) f_h(x^{2(2m+1)}). \end{aligned}$$

Our matrix approach: produce a matrix Q with (see the next slide for definition of ψ_Q)

$$\begin{aligned} \psi_Q(x, y) = {} & \psi_a(x)\psi_f^*(y) + \psi_c(x)\psi_g(y) \\ & - \psi_b^*(x)\psi_e(y) + \psi_d(x)\psi_h(y). \end{aligned}$$

$\psi_Q(x,y)$ for an $n \times m$ matrix Q

Let $q_0, \dots, q_{n-1}$ denote the row vector of Q:

$$Q = \begin{bmatrix} q_0 \\ q_1 \\ \vdots \\ q_{n-1} \end{bmatrix}.$$

Define

$$\psi_Q(x,y) = \sum_{i=0}^{n-1} y^{2i+1-n} \psi_{q_i}(x) \in \mathbb{Z}[x^{\pm 1}, y^{\pm 1}].$$

Example: Let $Q = (q_{ij})$ be a 3×4 matrix. Then $\psi_Q(x,y)$ is

$$\sum \text{ of } \begin{bmatrix} q_{00}x^{-3}y^{-2} & q_{01}x^{-1}y^{-2} & q_{02}x^{1}y^{-2} & q_{03}x^{3}y^{-2} \\ q_{10}x^{-3}y^{0} & q_{11}x^{-1}y^{0} & q_{12}x^{1}y^{0} & q_{13}x^{3}y^{0} \\ q_{20}x^{-3}y^{2} & q_{21}x^{-1}y^{2} & q_{22}x^{1}y^{2} & q_{23}x^{3}y^{2} \end{bmatrix}.$$

$\psi_{\boldsymbol{a}}(x)$ and $\psi_Q(x, y)$

Lemma

For sequences $\boldsymbol{a}, \boldsymbol{b}$ *regarded as row vectors,*

$$\psi_{\boldsymbol{b}^\top \boldsymbol{a}}(x, y) = \psi_{\boldsymbol{a}}(x)\psi_{\boldsymbol{b}}(y).$$

For a matrix Q, denote by $\mathrm{seq}(Q)$ the sequence obtained by concatenating the rows of Q.

Lemma

If Q *has* m *columns, then*

$$\psi_{\mathrm{seq}(Q)}(x) = \psi_Q(x, x^m).$$

Our approach

Recall that our matrix approach was:

$$\psi_Q(x, y) = \psi_a(x)\psi_f^*(y) + \psi_c(x)\psi_g(y) - \psi_b^*(x)\psi_e(y) + \psi_d(x)\psi_h(y).$$

This is achieved by defining

$$Q = f^{*\top}a + g^\top c - e^\top b^* + h^\top d,$$

where b^* denotes the reverse of b. Note $\psi_b^*(x) = \psi_{b^*}(x)$.

$$\psi_{\mathrm{seq}(Q)}(x) = \psi_a(x)\psi_f^*(x^m) + \psi_c(x)\psi_g(x^m) - \psi_b^*(x)\psi_e(x^m) + \psi_d(x)\psi_h(x^m).$$

Complementary sequences

Lemma

$$f_a(x^2)f_a^*(x^2) = \psi_a(x)\psi_a^*(x).$$

Thus

$$\begin{aligned} & a, b, c, d\text{: complementary} \\ \iff & f_a f_a^* + f_b f_b^* + f_c f_c^* + f_d f_d^* \in \mathbb{Z} \\ \iff & \psi_a \psi_a^* + \psi_b \psi_b^* + \psi_c \psi_c^* + \psi_d \psi_d^* \in \mathbb{Z} \end{aligned}$$

Recall the Lagrange identity

Let $a, b, c, d, f, g, h, e \in \mathbb{Z}[x^{\pm 1}, y^{\pm 1}]$. Set

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

Then

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

The Lagrange identity (consequence)

Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{d} \in \mathbb{Z}^m$, $\boldsymbol{f}, \boldsymbol{g}, \boldsymbol{h}, \boldsymbol{e} \in \mathbb{Z}^n$,

$$\begin{aligned} \boldsymbol{Q} &= \boldsymbol{f}^{*t}\boldsymbol{a} + \boldsymbol{g}^t\boldsymbol{c} - \boldsymbol{e}^t\boldsymbol{b}^* + \boldsymbol{h}^t\boldsymbol{d}, \\ \boldsymbol{R} &= \boldsymbol{f}^{*t}\boldsymbol{b} + \boldsymbol{g}^{*t}\boldsymbol{d} - \boldsymbol{e}^t\boldsymbol{a}^* - \boldsymbol{h}^{*t}\boldsymbol{c}, \\ \boldsymbol{S} &= \boldsymbol{g}^{*t}\boldsymbol{a} - \boldsymbol{f}^t\boldsymbol{c} - \boldsymbol{h}^t\boldsymbol{b} + \boldsymbol{e}^t\boldsymbol{d}^*, \\ \boldsymbol{T} &= \boldsymbol{g}^t\boldsymbol{b} - \boldsymbol{f}^t\boldsymbol{d} - \boldsymbol{h}^{*t}\boldsymbol{a} + \boldsymbol{e}^t\boldsymbol{c}^*. \end{aligned}$$

Then $\boldsymbol{Q}, \boldsymbol{R}, \boldsymbol{S}, \boldsymbol{T} \in \mathbb{Z}^{n \times m}$.

$$\begin{aligned} &(\psi_{\boldsymbol{Q}}\psi_{\boldsymbol{Q}}^* + \psi_{\boldsymbol{R}}\psi_{\boldsymbol{R}}^* + \psi_{\boldsymbol{S}}\psi_{\boldsymbol{S}}^* + \psi_{\boldsymbol{T}}\psi_{\boldsymbol{T}}^*)(\boldsymbol{x}, \boldsymbol{y}) \\ &= (\psi_{\boldsymbol{a}}\psi_{\boldsymbol{a}}^* + \psi_{\boldsymbol{b}}\psi_{\boldsymbol{b}}^* + \psi_{\boldsymbol{c}}\psi_{\boldsymbol{c}}^* + \psi_{\boldsymbol{d}}\psi_{\boldsymbol{d}}^*)(\boldsymbol{x}) \\ &\quad \times (\psi_{\boldsymbol{e}}\psi_{\boldsymbol{e}}^* + \psi_{\boldsymbol{f}}\psi_{\boldsymbol{f}}^* + \psi_{\boldsymbol{g}}\psi_{\boldsymbol{g}}^* + \psi_{\boldsymbol{h}}\psi_{\boldsymbol{h}}^*)(\boldsymbol{y}). \end{aligned}$$

The Lagrange identity (consequence)

Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{d} \in \mathbb{Z}^m$, $\boldsymbol{f}, \boldsymbol{g}, \boldsymbol{h}, \boldsymbol{e} \in \mathbb{Z}^n$,

$$\begin{aligned}
\boldsymbol{Q} &= \boldsymbol{f}^{*t}\boldsymbol{a} + \boldsymbol{g}^t\boldsymbol{c} - \boldsymbol{e}^t\boldsymbol{b}^* + \boldsymbol{h}^t\boldsymbol{d}, \\
\boldsymbol{R} &= \boldsymbol{f}^{*t}\boldsymbol{b} + \boldsymbol{g}^{*t}\boldsymbol{d} - \boldsymbol{e}^t\boldsymbol{a}^* - \boldsymbol{h}^{*t}\boldsymbol{c}, \\
\boldsymbol{S} &= \boldsymbol{g}^{*t}\boldsymbol{a} - \boldsymbol{f}^t\boldsymbol{c} - \boldsymbol{h}^t\boldsymbol{b} + \boldsymbol{e}^t\boldsymbol{d}^*, \\
\boldsymbol{T} &= \boldsymbol{g}^t\boldsymbol{b} - \boldsymbol{f}^t\boldsymbol{d} - \boldsymbol{h}^{*t}\boldsymbol{a} + \boldsymbol{e}^t\boldsymbol{c}^*.
\end{aligned}$$

Then for $\boldsymbol{q} = \mathrm{seq}(\boldsymbol{Q})$, $\boldsymbol{r} = \mathrm{seq}(\boldsymbol{R})$, $\boldsymbol{s} = \mathrm{seq}(\boldsymbol{S})$, $\boldsymbol{t} = \mathrm{seq}(\boldsymbol{T})$,

$$\begin{aligned}
&(\psi_{\boldsymbol{q}}\psi_{\boldsymbol{q}}^* + \psi_{\boldsymbol{r}}\psi_{\boldsymbol{r}}^* + \psi_{\boldsymbol{s}}\psi_{\boldsymbol{s}}^* + \psi_{\boldsymbol{t}}\psi_{\boldsymbol{t}}^*)(\boldsymbol{x}) \\
&= (\psi_{\boldsymbol{a}}\psi_{\boldsymbol{a}}^* + \psi_{\boldsymbol{b}}\psi_{\boldsymbol{b}}^* + \psi_{\boldsymbol{c}}\psi_{\boldsymbol{c}}^* + \psi_{\boldsymbol{d}}\psi_{\boldsymbol{d}}^*)(\boldsymbol{x}) \\
&\quad \times (\psi_{\boldsymbol{e}}\psi_{\boldsymbol{e}}^* + \psi_{\boldsymbol{f}}\psi_{\boldsymbol{f}}^* + \psi_{\boldsymbol{g}}\psi_{\boldsymbol{g}}^* + \psi_{\boldsymbol{h}}\psi_{\boldsymbol{h}}^*)(\boldsymbol{x}^{\boldsymbol{m}}).
\end{aligned}$$

Interleaving

For $a = (a_0, \ldots, a_{m-1})$, define

$$\begin{aligned} a/0 &= (a_0, 0, a_1, 0, \ldots, 0, a_{m-1}) \quad \text{(length } 2m-1\text{)}, \\ 0/a &= (0, a_0, 0, \ldots, 0, a_{m-1}, 0) \quad \text{(length } 2m+1\text{)}. \end{aligned}$$

Lemma

$$\psi_{a/0}(x) = \psi_{0/a}(x) = \psi_a(x^2).$$

Yang's Theorem

Theorem

Let $(a, b, c, d) \in BS(m+1, m)$, $(f, g, h, e) \in BS(n+1, n)$. *Then there exists* $(q, r, s, t) \in NCS((2n+1)(2m+1))$.

Construction of the matrices Q, R, S, T

Let $(a, b, c, d) \in BS(m+1, m)$, $(f, g, h, e) \in BS(n+1, n)$. Then

$$a, b \in \{\pm 1\}^{m+1}, c, d \in \{\pm 1\}^{m}, f, g \in \{\pm 1\}^{n+1}, h, e \in \{\pm 1\}^{n}.$$

Set

$$a' = a/0,\ b' = b/0,\ c' = 0/c,\ d' = 0/d \in \{0, \pm 1\}^{2m+1},$$
$$f' = f/0,\ g' = g/0,\ h' = 0/h,\ e' = 0/e \in \{0, \pm 1\}^{2n+1}.$$

Define $(2n+1) \times (2m+1)$ matrices with entries in $\{\pm 1\}$:

$$\begin{aligned}
Q &= f'^{*t}a' + g'^{t}c' - e'^{t}b'^{*} + h'^{t}d', \\
R &= f'^{*t}b' + g'^{*t}d' - e'^{t}a'^{*} - h'^{*t}c', \\
S &= g'^{*t}a' - f'^{t}c' - h'^{t}b' + e'^{t}d'^{*}, \\
T &= g'^{t}b' - f'^{t}d' - h'^{*t}a' + e'^{t}c'^{*}.
\end{aligned}$$

$(a,b,c,d),(f,g,h,e) \to (Q,R,S,T) \to$

Set $q=\mathrm{seq}(Q),\ r=\mathrm{seq}(R),\ s=\mathrm{seq}(S),\ t=\mathrm{seq}(T)$. Then

$$\begin{aligned}
&(\psi_q\psi_q^* + \psi_r\psi_r^* + \psi_s\psi_s^* + \psi_t\psi_t^*)(x)\\
&= (\psi_{a'}\psi_{a'}^* + \psi_{b'}\psi_{b'}^* + \psi_{c'}\psi_{c'}^* + \psi_{d'}\psi_{d'}^*)(x)\\
&\quad \times (\psi_{e'}\psi_{e'}^* + \psi_{f'}\psi_{f'}^* + \psi_{g'}\psi_{g'}^* + \psi_{h'}\psi_{h'}^*)(x^{2m+1})\\
&= (\psi_a\psi_a^* + \psi_b\psi_b^* + \psi_c\psi_c^* + \psi_d\psi_d^*)(x^2)\\
&\quad \times (\psi_e\psi_e^* + \psi_f\psi_f^* + \psi_g\psi_g^* + \psi_h\psi_h^*)(x^{2(2m+1)})\\
&\in \mathbb{Z}.
\end{aligned}$$

Thus $(q,r,s,t) \in NCS((2m+1)(2n+1))$. This proves Yang's theorem (see arXiv:1705.05062 for details).