A matrix approach to Yang multiplication

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

July 10, 2017
5th Workshop on Real and Complex
Hadamard Matrices and Applications
Alfréd Rényi Institute of Mathematics, Budapest

Sequence and real Hadamard matrices

Yang (1983,1983,1989) proved composition theorems for sequences. (Preserved property: complementarity).
A quadruple $(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{d})$ of complementary sequences of length $\boldsymbol{n}$ can be used to construct a Hadamard matrix of order $4\boldsymbol{n}$, via the Goethals-Seidel array:

$$\boldsymbol{H} = \begin{bmatrix} A & -BR & -CR & -DR \\ BR & A & -D^\top R & C^\top R \\ CR & D^\top R & A & -B^\top R \\ DR & -C^\top R & B^\top R & A \end{bmatrix}, \quad \boldsymbol{H}\boldsymbol{H}^\top = 4\boldsymbol{n}\boldsymbol{I},$$

where

$$A, B, C, D = \text{circulant matrix with first row } \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{d},$$
$$R = \text{back diagonal permutation matrix.}$$

Quadruple of complementary sequences

Kharaghani–Koukouvinos, Part V, Chapter 8 of CRC Handbook.

1. Base seq. $BS(m, n)$: length (m, m, n, n)
2. Near normal seq. $NN(n)$: a special case of $BS(n + 1, n)$
3. Nonperiodic complementary seq. $NCS(n)$: length (n, n, n, n)
4. Golay seq. $GCP(n)$: $(n, n, 0, 0)$

For $\{0, \pm 1\}$-sequences (ternary),

1. Normal seq. $NS(n)$: length $(n, n, n, 0)$, weight $2n$,
2. T-seq. $TS(n)$: length (n, n, n, n), weight n

(with some disjointness conditions).
Work done by Craigen, Doković, Kotsireas, Seberry,. . . .

From base sequences to 4 complementary sequences

Yang (1989), Theorem 4, states

$$\begin{aligned} & BS(m+1,m) \neq \emptyset,\ BS(n+1,n) \neq \emptyset \\ & \implies NCS((2m+1)(2n+1),4) \neq \emptyset \\ & (\implies \exists H(4(2m+1)(2n+1))). \end{aligned}$$

Conjecture $BS(n+1,n) \neq \emptyset$ for all n.
In this talk: a matrix approach to prove this theorem.
Is the proof difficult?
See the next page: only 9 lines.

$BS(m+1,m) \times BS(n+1,n) \to NCS((2m+1)(2n+1),4)$

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

$\Longrightarrow$

$$
\begin{aligned}
(q,r,s,t) &\in NCS((2m+1)(2n+1),4) \\
&\subset (\{\pm 1\}^{(2m+1)(2n+1)})^4.
\end{aligned}
$$

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

Our matrix approach:

$$(Q,R,S,T) \in (\{\pm 1\}^{(2n+1)\times(2m+1)})^4$$

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 Hall polynomial $f_a(x)$

Let $a = (a_0, \ldots, a_{n-1}) \in \mathbb{Z}^n$.
Define the *Hall polynomial* $f_a(x) \in \mathbb{Z}[x]$ of a by

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

It is more convenient to use

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

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

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

Complementary sequences

Define

$$*: \mathbb{Z}[x^{\pm 1}] \to \mathbb{Z}[x^{\pm 1}], \quad x \mapsto x^{-1}.$$

A k-tuple $(a_1, \dots, a_k)$ of sequences with all entries in $\{\pm 1\}$ is said to be complementary if

$$\sum_{i=1}^{k} f_{a_i}(x) f_{a_i}^*(x) \in \mathbb{Z}.$$

The constant term of the right-hand side is the sum of the lengths of $a_1, \dots, a_k$.

Example:

$$BS(m, n) : (a, b, c, d) \in \{\pm 1\}^m \times \{\pm 1\}^m \times \{\pm 1\}^n \times \{\pm 1\}^n,$$
$$NCS(n, 4) : (q, r, s, t) \in (\{\pm 1\}^n)^4.$$

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

Let

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

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

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

Our matrix approach:

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

$\psi_Q(x,y)$ 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 $\mathbf{seq}(Q)$ 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 f^* denotes the reverse of f. Note $\psi_f^*(y) = \psi_{f^*}(y)$.

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

Complementary sequences

Lemma

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

Thus

$$\begin{aligned} &a_1, \dots, a_k\text{: complementary} \\ \iff &\sum_{i=1}^{k} f_{a_i}(x)f_{a_i}^*(x) \in \mathbb{Z} \\ \iff &\sum_{i=1}^{k} \psi_{a_i}(x)\psi_{a_i}^*(x) \in \mathbb{Z}. \end{aligned}$$

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

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

Interleaving

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

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

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 $\{\pm 1\}$:

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

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

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

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

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

Another result of Yang (1983)

Theorem

Let $(a, b, c, d) \in BS(m, n)$. *Suppose* $f, g \in \{0, \pm 1\}^k$ *and* $e \in \{0, \pm 1\}^{k-1}$ *satisfy*

1. (e, f, g) *is complementary with weight* $2k + 1$,
2. $(0|f), (e|00) \in \{0, \pm 1\}^{k+1}$ *are disjoint,*
3. g *and* g^* *have the same support.*

Then $\exists (q, r, s, t) \in TS((2k + 1)(m + n))$.

Remarks:

1. Yang (1983) shows this only for $k = 6$ with e, f, g given.
2. This is different from better known Yang multiplication (1989): $NS(k) \neq \emptyset,\ BS(m, n) \neq \emptyset \implies TS((2k+1)(m+n))$.
3. Our proof is not as neat as the one presented here. The End.