On the Hadamard multiary quasigroup product

Lorenzo Mella
University of Modena and Reggio Emilia
Joint work with Raúl M. Falcón and Petr Vojtěchovský

CODESCO'24, Sevilla

Let $\mathcal{A}(n)$ be the set of $n \times n$ arrays with elements in $[n] := \{1, \ldots, n\}$.

Definition

A *Latin square of order n* is an $n \times n$ array filled with elements in $[n]$, such that every row and every column contains every element of $[n]$ exactly once.
We denote by $\mathcal{L}(n)$ the set of Latin squares of order n.

1	2	3	4
4	1	2	3
3	4	1	2
2	3	4	1

Definition

Two Latin squares L and L' in $\mathcal{L}(n)$ are *orthogonal* if when superimposed each of the possible n^2 ordered pairs of symbols occurs exactly once (denoted as $L \perp L'$).

1	2	3	4
4	3	2	1
2	1	4	3
3	4	1	2

1	2	3	4
3	4	1	2
4	3	2	1
2	1	4	3

Definition

Two Latin squares L and L' in $\mathcal{L}(n)$ are *orthogonal* if when superimposed each of the possible n^2 ordered pairs of symbols occurs exactly once (denoted as $L \perp L'$).

1	2	3	4
4	3	2	1
2	1	4	3
3	4	1	2

1	2	3	4
3	4	1	2
4	3	2	1
2	1	4	3

$\Rightarrow$

11	22	33	44
43	34	21	12
24	13	42	31
32	41	14	23

Definition

Two Latin squares L and L' in $\mathcal{L}(n)$ are *orthogonal* if when superimposed each of the possible n^2 ordered pairs of symbols occurs exactly once (denoted as $L \perp L'$).

1	2	3	4
4	3	2	1
2	1	4	3
3	4	1	2

1	2	3	4
3	4	1	2
4	3	2	1
2	1	4	3

$\Rightarrow$

11	22	33	44
43	34	21	12
24	13	42	31
32	41	14	23

Definition

Two Latin squares L and L' in $\mathcal{L}(n)$ are *orthogonal* if when superimposed each of the possible n^2 ordered pairs of symbols occurs exactly once (denoted as $L \perp L'$).

Definition

Two Latin squares L and L' in $\mathcal{L}(n)$ are *orthogonal* if when superimposed each of the possible n^2 ordered pairs of symbols occurs exactly once (denoted as $L \perp L'$).

Definition

Two arrays A and B in $\mathcal{A}(n)$ are *orthogonal* if when superimposed each of the possible n^2 ordered pairs of symbols occurs exactly once (denoted as $A \perp B$).

Definition

Let $A, B \in \mathcal{A}(n)$, $L \in \mathcal{L}(n)$. Then, the *Hadamard quasigroup product* $A \odot_L B$ is the array defined as:

$$(A \odot_L B)[i,j] = L[A[i,j], B[i,j]].$$

R. M. Falcón, V. Álvarez, J. A. Armario, M. D. Frau, F. Gudiel, M. B. Güemes, *A computational approach to analyze the Hadamard quasigroup product*, Electron. res. arch. **31** (2023), 3245–3263.

Definition

Let $A, B \in \mathcal{A}(n)$, $L \in \mathcal{L}(n)$. Then, the *Hadamard quasigroup product* $A \odot_L B$ is the array defined as:

$$(A \odot_L B)[i,j] = L[A[i,j], B[i,j]].$$

$$L = \begin{array}{|c|c|c|c|}\hline 1 & 2 & 3 & 4 \\ \hline 2 & 1 & 4 & 3 \\ \hline 3 & 4 & 1 & 2 \\ \hline 4 & 3 & 2 & 1 \\ \hline \end{array} \Rightarrow \quad \begin{array}{|c|c|c|c|}\hline 1 & 2 & 3 & 4 \\ \hline 4 & 3 & 2 & 1 \\ \hline 2 & 1 & 4 & 3 \\ \hline 3 & 4 & 1 & 2 \\ \hline \end{array} \odot_L \begin{array}{|c|c|c|c|}\hline 1 & 2 & 3 & 4 \\ \hline 3 & 4 & 1 & 2 \\ \hline 4 & 3 & 2 & 1 \\ \hline 2 & 1 & 4 & 3 \\ \hline \end{array} = \begin{array}{|c|c|c|c|}\hline 1 & 1 & 1 & 1 \\ \hline 2 & 2 & 2 & 2 \\ \hline 3 & 3 & 3 & 3 \\ \hline 4 & 4 & 4 & 4 \\ \hline \end{array}$$

R. M. Falcón, V. Álvarez, J. A. Armario, M. D. Frau, F. Gudiel, M. B. Güemes, *A computational approach to analyze the Hadamard quasigroup product*, Electron. res. arch. **31** (2023), 3245–3263.

Under which conditions $A \odot_L B \in \mathcal{L}(n)$?

Under which conditions $A \odot_L B \in \mathcal{L}(n)$?

Lemma

$A \odot_L B \in \mathcal{L}(n)$ if for each $i \in [n]$ it holds:

$$\{L(A[i,j], B[i,j]) : j \in [n]\} = \{L(A[j,i], B[j,i]) : j \in [n]\} = [n].$$

$$L = \begin{array}{|c|c|c|c|}\hline 1 & 2 & 3 & 4 \\ \hline 2 & 1 & 4 & 3 \\ \hline 3 & 4 & 1 & 2 \\ \hline 4 & 3 & 2 & 1 \\ \hline \end{array} \Rightarrow \begin{array}{|c|c|c|c|}\hline 1 & 2 & 3 & 4 \\ \hline 3 & 4 & 1 & 2 \\ \hline 4 & 3 & 2 & 1 \\ \hline 2 & 1 & 4 & 3 \\ \hline \end{array} \odot_L \begin{array}{|c|c|c|c|}\hline 1 & 1 & 1 & 1 \\ \hline 2 & 2 & 2 & 2 \\ \hline 3 & 3 & 3 & 3 \\ \hline 4 & 4 & 4 & 4 \\ \hline \end{array} = \begin{array}{|c|c|c|c|}\hline 1 & 2 & 3 & 4 \\ \hline 4 & 3 & 2 & 1 \\ \hline 2 & 1 & 4 & 3 \\ \hline 3 & 4 & 1 & 2 \\ \hline \end{array}$$

For each $i \in [n]$:

$$\{L(A[i,j], B[i,j]) : j \in [n]\} = [n]$$

$i = 1$:

1	2	3	4
3	4	1	2
4	3	2	1
2	1	4	3

1	1	1	1
2	2	2	2
3	3	3	3
4	4	4	4

$L =$

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

For each $i \in [n]$:

$$\{L(A[i,j], B[i,j]) : j \in [n]\} = [n]$$

$i = 2$:

1	2	3	4
3	4	1	2
4	3	2	1
2	1	4	3

1	1	1	1
2	2	2	2
3	3	3	3
4	4	4	4

$L =$

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

And so on for the first set...

For each $i \in [n]$:

$$\{L(A[j,i], B[j,i]) : j \in [n]\} = [n]$$

$i = 1$:

1	2	3	4
3	4	1	2
4	3	2	1
2	1	4	3

1	1	1	1
2	2	2	2
3	3	3	3
4	4	4	4

$L =$

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

For each $i \in [n]$:

$$\{L(A[j,i], B[j,i]) : j \in [n]\} = [n]$$

$i = 2$:

1	2	3	4
3	4	1	2
4	3	2	1
2	1	4	3

1	1	1	1
2	2	2	2
3	3	3	3
4	4	4	4

$L =$

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

For each $i \in [n]$:

$$\{L(A[j,i], B[j,i]) : j \in [n]\} = [n]$$

$i = 3$:

1	2	3	4
3	4	1	2
4	3	2	1
2	1	4	3

1	1	1	1
2	2	2	2
3	3	3	3
4	4	4	4

$L =$

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

For each $i \in [n]$:

$$\{L(A[j,i], B[j,i]) : j \in [n]\} = [n]$$

$i = 4$:

1	2	3	4
3	4	1	2
4	3	2	1
2	1	4	3

1	1	1	1
2	2	2	2
3	3	3	3
4	4	4	4

$L =$

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

Lemma

$A \odot_L B \in \mathcal{L}(n)$ if for each $i \in [n]$ it holds:

$$\{L(A[i,j], B[i,j]) : j \in [n]\} = \{L(A[j,i], B[j,i]) : j \in [n]\} = [n]. \tag{1}$$

- Construct the arrays $U[A[i,j], B[i,j]] = i$ and $V[A[j,i], B[j,i]] = i$.

Lemma

$A \odot_L B \in \mathcal{L}(n)$ if for each $i \in [n]$ it holds:

$$\{L(A[i,j], B[i,j]) : j \in [n]\} = \{L(A[j,i], B[j,i]) : j \in [n]\} = [n]. \tag{1}$$

- Construct the arrays $U[A[i,j], B[i,j]] = i$ and $V[A[j,i], B[j,i]] = i$.
- If $A \perp B$, then U and V are completely filled.

Lemma

$A \odot_L B \in \mathcal{L}(n)$ if for each $i \in [n]$ it holds:

$$\{L(A[i,j], B[i,j]) : j \in [n]\} = \{L(A[j,i], B[j,i]) : j \in [n]\} = [n]. \tag{1}$$

- Construct the arrays $U[A[i,j], B[i,j]] = i$ and $V[A[j,i], B[j,i]] = i$.
- If $A \perp B$, then U and V are completely filled.
- Equation (1) is equivalent to ask that $U, V \perp L$!

For each $i \in [n]$:

$$\{L(A[j,i], B[j,i]) : j \in [n]\} = [n]$$

$i = 1$:

1	2	3	4
3	4	1	2
4	3	2	1
2	1	4	3

1	1	1	1
2	2	2	2
3	3	3	3
4	4	4	4

$L =$

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

$\Rightarrow V =$

1	•	•	•
•	•	•	1
•	1	•	•
•	•	1	•

For each $i \in [n]$:

$$\{L(A[j,i], B[j,i]) : j \in [n]\} = [n]$$

$i = 2$:

1	2	3	4
3	4	1	2
4	3	2	1
2	1	4	3

1	1	1	1
2	2	2	2
3	3	3	3
4	4	4	4

$L =$

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

$\Rightarrow V =$

1	•	•	2
2	•	•	1
•	1	2	•
•	2	1	•

For each $i \in [n]$:

$$\{L(A[j,i], B[j,i]) : j \in [n]\} = [n]$$

$i = 3$:

1	2	3	4
3	4	1	2
4	3	2	1
2	1	4	3

1	1	1	1
2	2	2	2
3	3	3	3
4	4	4	4

$L =$

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

$\Rightarrow V =$

1	3	•	2
2	•	3	1
3	1	2	•
•	2	1	3

For each $i \in [n]$:

$$\{L(A[j,i], B[j,i]) : j \in [n]\} = [n]$$

$i = 4$:

1	2	3	4
3	4	1	2
4	3	2	1
2	1	4	3

1	1	1	1
2	2	2	2
3	3	3	3
4	4	4	4

$L =$

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

$\Rightarrow V =$

1	3	4	2
2	4	3	1
3	1	2	4
4	2	1	3

Proposition

If $A \perp B$, then $\odot_{A,B} : C \mapsto A \odot_C B$ is a bijection between $\mathcal{A}(n)$ and itself.

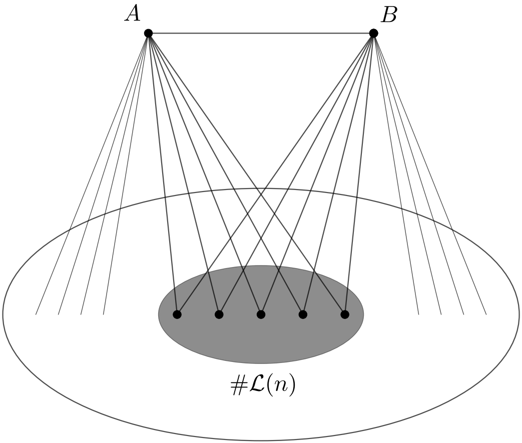
Proposition

If $A \perp B$, then $\odot_{A,B} : L \mapsto A \odot_L B$ is a bijection between $\mathcal{L}(n)$ and $\{C \in \mathcal{A}(n) : A, B \perp C\}$.

Proposition

If $A \perp B$, then $\odot_{A,B} : L \mapsto A \odot_L B$ is a bijection between $\mathcal{L}(n)$ and $\{C \in \mathcal{A}(n) : A, B \perp C\}$.

- Let $\Gamma = (V, E)$ be the graph having $\mathcal{A}(n)$ as vertex set, $\{A, B\} \in E \Leftrightarrow A \perp B$.



Proposition

If $A \perp B$, then $\odot_{A,B} : L \mapsto A \odot_L B$ is a bijection between $\mathcal{L}(n)$ and $\{C \in \mathcal{A}(n) : A, B \perp C\}$.

- Let $\Gamma = (V, E)$ be the graph having $\mathcal{A}(n)$ as vertex set, $\{A, B\} \in E \Leftrightarrow A \perp B$.
- If

$$A = \begin{array}{|c|c|c|c|} \hline 1 & 1 & \dots & 1 \\ \hline 2 & 2 & \dots & 2 \\ \hline \vdots & \vdots & \vdots & \vdots \\ \hline n & n & \dots & n \\ \hline \end{array} \quad B = \begin{array}{|c|c|c|c|} \hline 1 & 2 & \dots & n \\ \hline 1 & 2 & \dots & n \\ \hline \vdots & \vdots & \vdots & \vdots \\ \hline 1 & 2 & \dots & n \\ \hline \end{array},$$

then $\{C \in \mathcal{A}(n) : A, B \perp C\} = \mathcal{L}(n)$.

The Hadamard multiary Quasigroup product

R.M. Falcón, L. Mella and P. Vojtěchovský, *The Hadamard multiary quasigroup product*

Definition

- Denote by $\Omega_m(X)$ the set of m-ary operations on a set X.
- An *m-ary groupoid over X* is a pair (X, f), with $f \in \Omega_m(X)$.
- (X, f) is a *m-ary quasigroup* if for $i \in [m]$, for every $(a_1, \ldots, a_{i-1}, a_{i+1}, ..., a_m) \in X^{m-1}$ and every $b \in X$, $f(a_1, \ldots, a_{i-1}, a_i, a_{i+1}, \ldots, a_m) = b$ has an unique solution $a_i \in X$ (*Latin hypercube property*).
- We denote by $\mathcal{Q}_m(X)$ the set of m-ary quasigroups defined on X.

Definition

Let $f \in \Omega_m(X)$, $g_1, \ldots, g_m \in \Omega_n(X)$. The *superposition operator* $\odot_f(g_1, \ldots, g_m) \in \Omega_n(X)$ is defined as:

$$\odot_f(g_1, \ldots, g_m)(\bar{a}) = f(g_1(\bar{a}), \ldots, g_m(\bar{a})) \quad \text{for all } \bar{a} \in X^n.$$

Definition

Let $f \in \Omega_m(X)$, $g_1, \ldots, g_m \in \Omega_n(X)$. The *superposition operator* $\odot_f(g_1, \ldots, g_m) \in \Omega_n(X)$ is defined as:

$$\odot_f(g_1, \ldots, g_m)(\bar{a}) = f(g_1(\bar{a}), \ldots, g_m(\bar{a})) \quad \text{for all } \bar{a} \in X^n.$$

What properties does this operator have?

Proposition

The m-ary groupoid (X, f) satisfied the algebraic identity $\psi = \phi$ if and only if it is satisfied by $(\Omega_n(X), \odot_f)$.

Proposition

The m-ary groupoid (X, f) satisfied the algebraic identity $\psi = \phi$ if and only if it is satisfied by $(\Omega_n(X), \odot_f)$.

Example

Commutativity

- The m-ary groupoids $(X, \star)$ and $(\Omega(X), \odot_\star)$ are commutative if and only if they satisfy $x_1x_2 = x_2x_1$.
- In $(X, \star) \to a \star b = b \star a$ for all $a, b \in X$.
- In $(\Omega(X), \odot_\star) \to \odot_\star(g_1, g_2) = \odot_\star(g_2, g_1)$, i.e.

$$g_1(\bar{a}) \star g_2(\bar{a}) = g_2(\bar{a}) \star g_1(\bar{a}).$$

Example

- $X = \{1, 2\}$, then $\Omega_2(X)$ is the set:

1	1
1	1

g_1

1	1
1	2

g_2

1	1
2	1

g_3

1	1
2	2

g_4

1	2
1	1

g_5

1	2
1	2

g_6

1	2
2	1

g_7

1	2
2	2

g_8

2	1
1	1

g_9

2	1
1	2

g_{10}

2	1
2	1

g_{11}

2	1
2	2

g_{12}

2	2
1	1

g_{13}

2	2
1	2

g_{14}

2	2
2	1

g_{15}

2	2
2	2

g_{16}

Example

- $X = \{1,2\}$, then $\Omega_2(X)$ is the set:

$$\underset{g_1}{\begin{array}{|c|c|}\hline 1 & 1 \\ \hline 1 & 1 \\ \hline\end{array}} \quad \underset{g_2}{\begin{array}{|c|c|}\hline 1 & 1 \\ \hline 1 & 2 \\ \hline\end{array}} \quad \underset{g_3}{\begin{array}{|c|c|}\hline 1 & 1 \\ \hline 2 & 1 \\ \hline\end{array}} \quad \underset{g_4}{\begin{array}{|c|c|}\hline 1 & 1 \\ \hline 2 & 2 \\ \hline\end{array}}$$

$$\underset{g_5}{\begin{array}{|c|c|}\hline 1 & 2 \\ \hline 1 & 1 \\ \hline\end{array}} \quad \underset{g_6}{\begin{array}{|c|c|}\hline 1 & 2 \\ \hline 1 & 2 \\ \hline\end{array}} \quad \underset{\boldsymbol{g_7}}{\begin{array}{|c|c|}\hline \mathbf{1} & \mathbf{2} \\ \hline \mathbf{2} & \mathbf{1} \\ \hline\end{array}} \quad \underset{g_8}{\begin{array}{|c|c|}\hline 1 & 2 \\ \hline 2 & 2 \\ \hline\end{array}}$$

$$\underset{g_9}{\begin{array}{|c|c|}\hline 2 & 1 \\ \hline 1 & 1 \\ \hline\end{array}} \quad \underset{g_{10}}{\begin{array}{|c|c|}\hline 2 & 1 \\ \hline 1 & 2 \\ \hline\end{array}} \quad \underset{g_{11}}{\begin{array}{|c|c|}\hline 2 & 1 \\ \hline 2 & 1 \\ \hline\end{array}} \quad \underset{g_{12}}{\begin{array}{|c|c|}\hline 2 & 1 \\ \hline 2 & 2 \\ \hline\end{array}}$$

$$\underset{g_{13}}{\begin{array}{|c|c|}\hline 2 & 2 \\ \hline 1 & 1 \\ \hline\end{array}} \quad \underset{g_{14}}{\begin{array}{|c|c|}\hline 2 & 2 \\ \hline 1 & 2 \\ \hline\end{array}} \quad \underset{g_{15}}{\begin{array}{|c|c|}\hline 2 & 2 \\ \hline 2 & 1 \\ \hline\end{array}} \quad \underset{g_{16}}{\begin{array}{|c|c|}\hline 2 & 2 \\ \hline 2 & 2 \\ \hline\end{array}}$$

Example

- $X = \{1, 2\}$, then $\Omega_2(X)$ is the set:

$$
\underset{g_1}{\begin{array}{|c|c|}\hline 1 & 1 \\ \hline 1 & 1 \\ \hline\end{array}} \quad
\underset{g_2}{\begin{array}{|c|c|}\hline 1 & 1 \\ \hline 1 & 2 \\ \hline\end{array}} \quad
\underset{g_3}{\begin{array}{|c|c|}\hline 1 & 1 \\ \hline 2 & 1 \\ \hline\end{array}} \quad
\underset{g_4}{\begin{array}{|c|c|}\hline 1 & 1 \\ \hline 2 & 2 \\ \hline\end{array}}
$$

$$
\underset{g_5}{\begin{array}{|c|c|}\hline 1 & 2 \\ \hline 1 & 1 \\ \hline\end{array}} \quad
\underset{g_6}{\begin{array}{|c|c|}\hline 1 & 2 \\ \hline 1 & 2 \\ \hline\end{array}} \quad
\underset{\mathbf{g_7}}{\begin{array}{|c|c|}\hline \mathbf{1} & \mathbf{2} \\ \hline \mathbf{2} & \mathbf{1} \\ \hline\end{array}} \quad
\underset{g_8}{\begin{array}{|c|c|}\hline 1 & 2 \\ \hline 2 & 2 \\ \hline\end{array}}
$$

$$
\underset{g_9}{\begin{array}{|c|c|}\hline 2 & 1 \\ \hline 1 & 1 \\ \hline\end{array}} \quad
\underset{g_{10}}{\begin{array}{|c|c|}\hline 2 & 1 \\ \hline 1 & 2 \\ \hline\end{array}} \quad
\underset{g_{11}}{\begin{array}{|c|c|}\hline 2 & 1 \\ \hline 2 & 1 \\ \hline\end{array}} \quad
\underset{g_{12}}{\begin{array}{|c|c|}\hline 2 & 1 \\ \hline 2 & 2 \\ \hline\end{array}}
$$

$$
\underset{g_{13}}{\begin{array}{|c|c|}\hline 2 & 2 \\ \hline 1 & 1 \\ \hline\end{array}} \quad
\underset{g_{14}}{\begin{array}{|c|c|}\hline 2 & 2 \\ \hline 1 & 2 \\ \hline\end{array}} \quad
\underset{g_{15}}{\begin{array}{|c|c|}\hline 2 & 2 \\ \hline 2 & 1 \\ \hline\end{array}} \quad
\underset{g_{16}}{\begin{array}{|c|c|}\hline 2 & 2 \\ \hline 2 & 2 \\ \hline\end{array}}
$$

- (X, g_7) is isomorphic to $(\mathbb{Z}_2, +)$ (commutative, associative, neutral and inverse).

$(\Omega_2(X), \odot_{g_7})$

g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8	g_9	g_{10}	g_{11}	g_{12}	g_{13}	g_{14}	g_{15}	g_{16}
g_2	g_1	g_4	g_3	g_6	g_5	g_8	g_7	g_{10}	g_9	g_{12}	g_{11}	g_{14}	g_{13}	g_{16}	g_{15}
g_3	g_4	g_1	g_2	g_7	g_8	g_5	g_6	g_{11}	g_{12}	g_9	g_{10}	g_{15}	g_{16}	g_{13}	g_{14}
g_4	g_3	g_2	g_1	g_8	g_7	g_6	g_5	g_{12}	g_{11}	g_{10}	g_9	g_{16}	g_{15}	g_{14}	g_{13}
g_5	g_6	g_7	g_8	g_1	g_2	g_3	g_4	g_{13}	g_{14}	g_{15}	g_{16}	g_9	g_{10}	g_{11}	g_{12}
g_6	g_5	g_8	g_7	g_2	g_1	g_4	g_3	g_{14}	g_{13}	g_{16}	g_{15}	g_{10}	g_9	g_{12}	g_{11}
g_7	g_8	g_5	g_6	g_3	g_4	g_1	g_2	g_{15}	g_{16}	g_{13}	g_{14}	g_{11}	g_{12}	g_9	g_{10}
g_8	g_7	g_6	g_5	g_4	g_3	g_2	g_1	g_{16}	g_{15}	g_{14}	g_{13}	g_{12}	g_{11}	g_{10}	g_9
g_9	g_{10}	g_{11}	g_{12}	g_{13}	g_{14}	g_{15}	g_{16}	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8
g_{10}	g_9	g_{12}	g_{11}	g_{14}	g_{13}	g_{16}	g_{15}	g_2	g_1	g_4	g_3	g_6	g_5	g_8	g_7
g_{11}	g_{12}	g_9	g_{10}	g_{15}	g_{16}	g_{13}	g_{14}	g_3	g_4	g_1	g_2	g_7	g_8	g_5	g_6
g_{12}	g_{11}	g_{10}	g_9	g_{16}	g_{15}	g_{14}	g_{13}	g_4	g_3	g_2	g_1	g_8	g_7	g_6	g_5
g_{13}	g_{14}	g_{15}	g_{16}	g_9	g_{10}	g_{11}	g_{12}	g_5	g_6	g_7	g_8	g_1	g_2	g_3	g_4
g_{14}	g_{13}	g_{16}	g_{15}	g_{10}	g_9	g_{12}	g_{11}	g_6	g_5	g_8	g_7	g_2	g_1	g_4	g_3
g_{15}	g_{16}	g_{13}	g_{14}	g_{11}	g_{12}	g_9	g_{10}	g_7	g_8	g_5	g_6	g_3	g_4	g_1	g_2
g_{16}	g_{15}	g_{14}	g_{13}	g_{12}	g_{11}	g_{10}	g_9	g_8	g_7	g_6	g_5	g_4	g_3	g_2	g_1

$(\Omega_2(X), \odot_{g_7})$ commutative

g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8	g_9	g_{10}	g_{11}	g_{12}	g_{13}	g_{14}	g_{15}	g_{16}
g_2	g_1	g_4	g_3	g_6	g_5	g_8	g_7	g_{10}	g_9	g_{12}	g_{11}	g_{14}	g_{13}	g_{16}	g_{15}
g_3	g_4	g_1	g_2	g_7	g_8	g_5	g_6	g_{11}	g_{12}	g_9	g_{10}	g_{15}	g_{16}	g_{13}	g_{14}
g_4	g_3	g_2	g_1	g_8	g_7	g_6	g_5	g_{12}	g_{11}	g_{10}	g_9	g_{16}	g_{15}	g_{14}	g_{13}
g_5	g_6	g_7	g_8	g_1	g_2	g_3	g_4	g_{13}	g_{14}	g_{15}	g_{16}	g_9	g_{10}	g_{11}	g_{12}
g_6	g_5	g_8	g_7	g_2	g_1	g_4	g_3	g_{14}	g_{13}	g_{16}	g_{15}	g_{10}	g_9	g_{12}	g_{11}
g_7	g_8	g_5	g_6	g_3	g_4	g_1	g_2	g_{15}	g_{16}	g_{13}	g_{14}	g_{11}	g_{12}	g_9	g_{10}
g_8	g_7	g_6	g_5	g_4	g_3	g_2	g_1	g_{16}	g_{15}	g_{14}	g_{13}	g_{12}	g_{11}	g_{10}	g_9
g_9	g_{10}	g_{11}	g_{12}	g_{13}	g_{14}	g_{15}	g_{16}	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8
g_{10}	g_9	g_{12}	g_{11}	g_{14}	g_{13}	g_{16}	g_{15}	g_2	g_1	g_4	g_3	g_6	g_5	g_8	g_7
g_{11}	g_{12}	g_9	g_{10}	g_{15}	g_{16}	g_{13}	g_{14}	g_3	g_4	g_1	g_2	g_7	g_8	g_5	g_6
g_{12}	g_{11}	g_{10}	g_9	g_{16}	g_{15}	g_{14}	g_{13}	g_4	g_3	g_2	g_1	g_8	g_7	g_6	g_5
g_{13}	g_{14}	g_{15}	g_{16}	g_9	g_{10}	g_{11}	g_{12}	g_5	g_6	g_7	g_8	g_1	g_2	g_3	g_4
g_{14}	g_{13}	g_{16}	g_{15}	g_{10}	g_9	g_{12}	g_{11}	g_6	g_5	g_8	g_7	g_2	g_1	g_4	g_3
g_{15}	g_{16}	g_{13}	g_{14}	g_{11}	g_{12}	g_9	g_{10}	g_7	g_8	g_5	g_6	g_3	g_4	g_1	g_2
g_{16}	g_{15}	g_{14}	g_{13}	g_{12}	g_{11}	g_{10}	g_9	g_8	g_7	g_6	g_5	g_4	g_3	g_2	g_1

$(\Omega_2(X), \odot_{g_7})$ commutative, g_1 neutral element

g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8	g_9	g_{10}	g_{11}	g_{12}	g_{13}	g_{14}	g_{15}	g_{16}
g_2	g_1	g_4	g_3	g_6	g_5	g_8	g_7	g_{10}	g_9	g_{12}	g_{11}	g_{14}	g_{13}	g_{16}	g_{15}
g_3	g_4	g_1	g_2	g_7	g_8	g_5	g_6	g_{11}	g_{12}	g_9	g_{10}	g_{15}	g_{16}	g_{13}	g_{14}
g_4	g_3	g_2	g_1	g_8	g_7	g_6	g_5	g_{12}	g_{11}	g_{10}	g_9	g_{16}	g_{15}	g_{14}	g_{13}
g_5	g_6	g_7	g_8	g_1	g_2	g_3	g_4	g_{13}	g_{14}	g_{15}	g_{16}	g_9	g_{10}	g_{11}	g_{12}
g_6	g_5	g_8	g_7	g_2	g_1	g_4	g_3	g_{14}	g_{13}	g_{16}	g_{15}	g_{10}	g_9	g_{12}	g_{11}
g_7	g_8	g_5	g_6	g_3	g_4	g_1	g_2	g_{15}	g_{16}	g_{13}	g_{14}	g_{11}	g_{12}	g_9	g_{10}
g_8	g_7	g_6	g_5	g_4	g_3	g_2	g_1	g_{16}	g_{15}	g_{14}	g_{13}	g_{12}	g_{11}	g_{10}	g_9
g_9	g_{10}	g_{11}	g_{12}	g_{13}	g_{14}	g_{15}	g_{16}	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8
g_{10}	g_9	g_{12}	g_{11}	g_{14}	g_{13}	g_{16}	g_{15}	g_2	g_1	g_4	g_3	g_6	g_5	g_8	g_7
g_{11}	g_{12}	g_9	g_{10}	g_{15}	g_{16}	g_{13}	g_{14}	g_3	g_4	g_1	g_2	g_7	g_8	g_5	g_6
g_{12}	g_{11}	g_{10}	g_9	g_{16}	g_{15}	g_{14}	g_{13}	g_4	g_3	g_2	g_1	g_8	g_7	g_6	g_5
g_{13}	g_{14}	g_{15}	g_{16}	g_9	g_{10}	g_{11}	g_{12}	g_5	g_6	g_7	g_8	g_1	g_2	g_3	g_4
g_{14}	g_{13}	g_{16}	g_{15}	g_{10}	g_9	g_{12}	g_{11}	g_6	g_5	g_8	g_7	g_2	g_1	g_4	g_3
g_{15}	g_{16}	g_{13}	g_{14}	g_{11}	g_{12}	g_9	g_{10}	g_7	g_8	g_5	g_6	g_3	g_4	g_1	g_2
g_{16}	g_{15}	g_{14}	g_{13}	g_{12}	g_{11}	g_{10}	g_9	g_8	g_7	g_6	g_5	g_4	g_3	g_2	g_1

$(\Omega_2(X), \odot_{g_7})$ commutative, g_1 neutral element, $g_i = g_i^{-1}$

g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8	g_9	g_{10}	g_{11}	g_{12}	g_{13}	g_{14}	g_{15}	g_{16}
g_2	g_1	g_4	g_3	g_6	g_5	g_8	g_7	g_{10}	g_9	g_{12}	g_{11}	g_{14}	g_{13}	g_{16}	g_{15}
g_3	g_4	g_1	g_2	g_7	g_8	g_5	g_6	g_{11}	g_{12}	g_9	g_{10}	g_{15}	g_{16}	g_{13}	g_{14}
g_4	g_3	g_2	g_1	g_8	g_7	g_6	g_5	g_{12}	g_{11}	g_{10}	g_9	g_{16}	g_{15}	g_{14}	g_{13}
g_5	g_6	g_7	g_8	g_1	g_2	g_3	g_4	g_{13}	g_{14}	g_{15}	g_{16}	g_9	g_{10}	g_{11}	g_{12}
g_6	g_5	g_8	g_7	g_2	g_1	g_4	g_3	g_{14}	g_{13}	g_{16}	g_{15}	g_{10}	g_9	g_{12}	g_{11}
g_7	g_8	g_5	g_6	g_3	g_4	g_1	g_2	g_{15}	g_{16}	g_{13}	g_{14}	g_{11}	g_{12}	g_9	g_{10}
g_8	g_7	g_6	g_5	g_4	g_3	g_2	g_1	g_{16}	g_{15}	g_{14}	g_{13}	g_{12}	g_{11}	g_{10}	g_9
g_9	g_{10}	g_{11}	g_{12}	g_{13}	g_{14}	g_{15}	g_{16}	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8
g_{10}	g_9	g_{12}	g_{11}	g_{14}	g_{13}	g_{16}	g_{15}	g_2	g_1	g_4	g_3	g_6	g_5	g_8	g_7
g_{11}	g_{12}	g_9	g_{10}	g_{15}	g_{16}	g_{13}	g_{14}	g_3	g_4	g_1	g_2	g_7	g_8	g_5	g_6
g_{12}	g_{11}	g_{10}	g_9	g_{16}	g_{15}	g_{14}	g_{13}	g_4	g_3	g_2	g_1	g_8	g_7	g_6	g_5
g_{13}	g_{14}	g_{15}	g_{16}	g_9	g_{10}	g_{11}	g_{12}	g_5	g_6	g_7	g_8	g_1	g_2	g_3	g_4
g_{14}	g_{13}	g_{16}	g_{15}	g_{10}	g_9	g_{12}	g_{11}	g_6	g_5	g_8	g_7	g_2	g_1	g_4	g_3
g_{15}	g_{16}	g_{13}	g_{14}	g_{11}	g_{12}	g_9	g_{10}	g_7	g_8	g_5	g_6	g_3	g_4	g_1	g_2
g_{16}	g_{15}	g_{14}	g_{13}	g_{12}	g_{11}	g_{10}	g_9	g_8	g_7	g_6	g_5	g_4	g_3	g_2	g_1

$(\Omega_2(X), \odot_{g_7})$ commutative, g_1 neutral element, $g_i = g_i^{-1}$, associative

g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8	g_9	g_{10}	g_{11}	g_{12}	g_{13}	g_{14}	g_{15}	g_{16}
g_2	g_1	g_4	g_3	g_6	g_5	g_8	g_7	g_{10}	g_9	g_{12}	g_{11}	g_{14}	g_{13}	g_{16}	g_{15}
g_3	g_4	g_1	g_2	g_7	g_8	g_5	g_6	g_{11}	g_{12}	g_9	g_{10}	g_{15}	g_{16}	g_{13}	g_{14}
g_4	g_3	g_2	g_1	g_8	g_7	g_6	g_5	g_{12}	g_{11}	g_{10}	g_9	g_{16}	g_{15}	g_{14}	g_{13}
g_5	g_6	g_7	g_8	g_1	g_2	g_3	g_4	g_{13}	g_{14}	g_{15}	g_{16}	g_9	g_{10}	g_{11}	g_{12}
g_6	g_5	g_8	g_7	g_2	g_1	g_4	g_3	g_{14}	g_{13}	g_{16}	g_{15}	g_{10}	g_9	g_{12}	g_{11}
g_7	g_8	g_5	g_6	g_3	g_4	g_1	g_2	g_{15}	g_{16}	g_{13}	g_{14}	g_{11}	g_{12}	g_9	g_{10}
g_8	g_7	g_6	g_5	g_4	g_3	g_2	g_1	g_{16}	g_{15}	g_{14}	g_{13}	g_{12}	g_{11}	g_{10}	g_9
g_9	g_{10}	g_{11}	g_{12}	g_{13}	g_{14}	g_{15}	g_{16}	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8
g_{10}	g_9	g_{12}	g_{11}	g_{14}	g_{13}	g_{16}	g_{15}	g_2	g_1	g_4	g_3	g_6	g_5	g_8	g_7
g_{11}	g_{12}	g_9	g_{10}	g_{15}	g_{16}	g_{13}	g_{14}	g_3	g_4	g_1	g_2	g_7	g_8	g_5	g_6
g_{12}	g_{11}	g_{10}	g_9	g_{16}	g_{15}	g_{14}	g_{13}	g_4	g_3	g_2	g_1	g_8	g_7	g_6	g_5
g_{13}	g_{14}	g_{15}	g_{16}	g_9	g_{10}	g_{11}	g_{12}	g_5	g_6	g_7	g_8	g_1	g_2	g_3	g_4
g_{14}	g_{13}	g_{16}	g_{15}	g_{10}	g_9	g_{12}	g_{11}	g_6	g_5	g_8	g_7	g_2	g_1	g_4	g_3
g_{15}	g_{16}	g_{13}	g_{14}	g_{11}	g_{12}	g_9	g_{10}	g_7	g_8	g_5	g_6	g_3	g_4	g_1	g_2
g_{16}	g_{15}	g_{14}	g_{13}	g_{12}	g_{11}	g_{10}	g_9	g_8	g_7	g_6	g_5	g_4	g_3	g_2	g_1

$(\Omega_2(X), \odot_{g_7}) \quad \cong (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, +)$

g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8	g_9	g_{10}	g_{11}	g_{12}	g_{13}	g_{14}	g_{15}	g_{16}
g_2	g_1	g_4	g_3	g_6	g_5	g_8	g_7	g_{10}	g_9	g_{12}	g_{11}	g_{14}	g_{13}	g_{16}	g_{15}
g_3	g_4	g_1	g_2	g_7	g_8	g_5	g_6	g_{11}	g_{12}	g_9	g_{10}	g_{15}	g_{16}	g_{13}	g_{14}
g_4	g_3	g_2	g_1	g_8	g_7	g_6	g_5	g_{12}	g_{11}	g_{10}	g_9	g_{16}	g_{15}	g_{14}	g_{13}
g_5	g_6	g_7	g_8	g_1	g_2	g_3	g_4	g_{13}	g_{14}	g_{15}	g_{16}	g_9	g_{10}	g_{11}	g_{12}
g_6	g_5	g_8	g_7	g_2	g_1	g_4	g_3	g_{14}	g_{13}	g_{16}	g_{15}	g_{10}	g_9	g_{12}	g_{11}
g_7	g_8	g_5	g_6	g_3	g_4	g_1	g_2	g_{15}	g_{16}	g_{13}	g_{14}	g_{11}	g_{12}	g_9	g_{10}
g_8	g_7	g_6	g_5	g_4	g_3	g_2	g_1	g_{16}	g_{15}	g_{14}	g_{13}	g_{12}	g_{11}	g_{10}	g_9
g_9	g_{10}	g_{11}	g_{12}	g_{13}	g_{14}	g_{15}	g_{16}	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8
g_{10}	g_9	g_{12}	g_{11}	g_{14}	g_{13}	g_{16}	g_{15}	g_2	g_1	g_4	g_3	g_6	g_5	g_8	g_7
g_{11}	g_{12}	g_9	g_{10}	g_{15}	g_{16}	g_{13}	g_{14}	g_3	g_4	g_1	g_2	g_7	g_8	g_5	g_6
g_{12}	g_{11}	g_{10}	g_9	g_{16}	g_{15}	g_{14}	g_{13}	g_4	g_3	g_2	g_1	g_8	g_7	g_6	g_5
g_{13}	g_{14}	g_{15}	g_{16}	g_9	g_{10}	g_{11}	g_{12}	g_5	g_6	g_7	g_8	g_1	g_2	g_3	g_4
g_{14}	g_{13}	g_{16}	g_{15}	g_{10}	g_9	g_{12}	g_{11}	g_6	g_5	g_8	g_7	g_2	g_1	g_4	g_3
g_{15}	g_{16}	g_{13}	g_{14}	g_{11}	g_{12}	g_9	g_{10}	g_7	g_8	g_5	g_6	g_3	g_4	g_1	g_2
g_{16}	g_{15}	g_{14}	g_{13}	g_{12}	g_{11}	g_{10}	g_9	g_8	g_7	g_6	g_5	g_4	g_3	g_2	g_1

Definition

A set of *orthogonal* m-ary operations is any subset $\{g_1, \ldots, g_m\} \subseteq \Omega_m(X)$ such that the map

$$\begin{array}{ccc} X^m & \to & X^m \\ \bar{a} & \mapsto & \left(g_1\left(\bar{a}\right), \ldots, g_m\left(\bar{a}\right)\right) \end{array}$$

is a bijection.

Definition

A set of *orthogonal* m-ary operations is any subset $\{g_1, \ldots, g_m\} \subseteq \Omega_m(X)$ such that the map

$$\begin{array}{ccc} X^m & \to & X^m \\ \overline{a} & \mapsto & \left(g_1\left(\overline{a}\right), \ldots, g_m\left(\overline{a}\right)\right) \end{array}$$

is a bijection.

Example

- if $m = 2$, then g_1, g_2 are 2-ary operations $\rightarrow$ $|X| \times |X|$ arrays G_1, G_2;
- $\overline{a} \mapsto \left(g_1\left(\overline{a}\right), g_2\left(\overline{a}\right)\right)$ is a bijection, with $\overline{a} \in X^2$ $\rightarrow$ G_1 and G_2 are orthogonal in the sense given before.

Proposition

If $A \perp B$, then $\odot_{A,B} : C \mapsto A \odot_C B$ is a bijection between $\mathcal{A}(n)$ and itself.

Proposition

$\{g_1, \ldots, g_m\} \subseteq \Omega_m(X)$ is a set of orthogonal m-ary operations if and only if the map

$$\begin{array}{ccc} \Omega_m(X) & \to & \Omega_m(X) \\ f & \mapsto & \odot_f(g_1, \ldots, g_m) \end{array}$$

is a bijection.

Proposition

$\{g_1, \dots, g_m\} \subseteq \Omega_m(X)$ is a set of orthogonal m-ary operations if and only if the map

$$\begin{array}{ccc} \Omega_m(X) & \to & \Omega_m(X) \\ f & \mapsto & \odot_f(g_1, \dots, g_m) \end{array}$$

is a bijection.

Example

- if $m = 2$, then f, and g_1, g_2 are 2-ary operations $\to |X| \times |X|$ arrays F, and G_1, G_2;
- G_1 and G_2 are orthogonal $\to$ every array is of the form $G_1 \odot_F G_2$, for some array F.

Proposition

Let $S = \{g_1, \ldots, g_m\} \subset \Omega_m(X)$, define:

$$\mathrm{Ort}(S) = \{g \in \Omega_m(X) : (S \setminus \{g_i\}) \cup \{g\} \text{ are orthogonal operations } \forall i \leq m\}$$

Proposition

Let $S = \{g_1, \ldots, g_m\} \subset \Omega_m(X)$, define:

$$\mathrm{Ort}(S) = \{g \in \Omega_m(X) : (S \setminus \{g_i\}) \cup \{g\} \text{ are orthogonal operations } \forall i \leq m\}$$

Then, the map

$$\begin{array}{ccc} \mathcal{Q}_m(X) & \to & \mathrm{Ort}(S) \\ f & \to & \odot_f(g_1, \ldots, g_m) \end{array} \tag{2}$$

is a bijection.

Proposition

Let $S = \{g_1, \dots, g_m\} \subset \Omega_m(X)$, define:

$$\mathrm{Ort}(S) = \{g \in \Omega_m(X) : (S \setminus \{g_i\}) \cup \{g\} \text{ are orthogonal operations } \forall i \leq m\}$$

Then, the map

$$\begin{array}{ccc} \mathcal{Q}_m(X) & \to & \mathrm{Ort}(S) \\ f & \to & \odot_f(g_1, \dots, g_m) \end{array} \qquad (2)$$

is a bijection.

Proposition

If $A \perp B$, then $\odot_{A,B} : L \mapsto A \odot_L B$ is a bijection between $\mathcal{L}(n)$ and $\{C \in \mathcal{A}(n) : A, B \perp C\}$.

Consider the following operations in $\Omega_2([5])$:

$A_\star \equiv$

1	5	4	3	2
3	2	1	5	4
5	4	3	2	1
2	1	5	4	3
4	3	2	1	5

$A_\circ \equiv$

1	2	3	4	5
1	2	3	4	5
1	2	3	4	5
1	2	3	4	5
1	2	3	4	5

$A_* \equiv$

1	4	2	5	3
4	2	5	3	1
2	5	3	1	4
5	3	1	4	2
3	1	4	2	5

and $A_{\star^t} = A_\star^t$, $A_{\circ^t} = A_\circ^t$. Then $\odot_\star$ applied to $\{A_\star, A_{\star^t}, A_\circ, A_{\circ^t}, A_*\}$ gives the following table:

$\odot_\star$	$\star$	$\star^t$	$\circ$	$\circ^t$	$*$
$\star$	$\star$	$\circ$	$\star^t$	$*$	$\circ^t$
$\star^t$	$\circ^t$	$\star^t$	$*$	$\star$	$\circ$
$\circ$	$*$	$\circ^t$	$\circ$	$\star^t$	$\star$
$\circ^t$	$\circ$	$*$	$\star$	$\circ^t$	$\star^t$
$*$	$\star^t$	$\star$	$\circ^t$	$\circ$	$*$

$\odot_\star$	$\star$	$\star^t$	$\circ$	$\circ^t$	$*$
$\star$	$\star$	$\circ$	$\star^t$	$*$	$\circ^t$
$\star^t$	$\circ^t$	$\star^t$	$*$	$\star$	$\circ$
$\circ$	$*$	$\circ^t$	$\circ$	$\star^t$	$\star$
$\circ^t$	$\circ$	$*$	$\star$	$\circ^t$	$\star^t$
$*$	$\star^t$	$\star$	$\circ^t$	$\circ$	$*$

$\equiv$

$\bullet$	1	2	3	4	5
1	1	3	2	5	4
2	4	2	5	1	3
3	5	4	3	2	1
4	3	5	1	4	2
5	2	1	4	3	5

$\bullet$	1	2	3	4	5
1	1	3	2	5	4
2	4	2	5	1	3
3	5	4	3	2	1
4	3	5	1	4	2
5	2	1	4	3	5

$\equiv_{(235)}$

$\star$	1	2	3	4	5
1	1	4	2	5	3
2	4	2	5	3	1
3	2	5	3	1	4
4	5	3	1	4	2
5	3	1	4	2	5

Thank you for your attention!