Group algebras and quantum Latin squares

Arnbjörg Soffía Árnadóttir
Universidade Federal de Minas Gerais

- Joint work with David Roberson

TerwilligerFest

Kranjska Gora, Slovenia
June, 2025

Outline

Outline

The isomorphism game

R

We need:

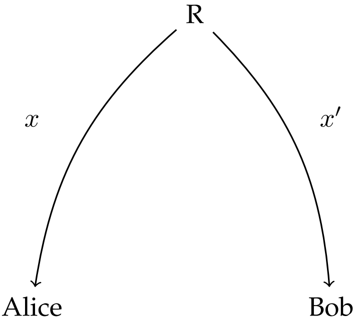
- Players: Alice & Bob
- Graphs: X & Y
- Referee: R

Alice Bob

The isomorphism game

We need:

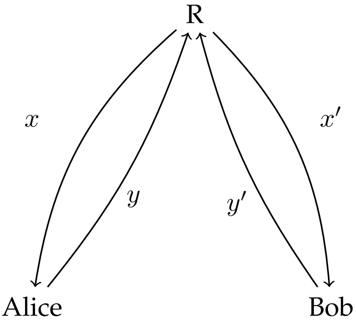
- Players: Alice & Bob
- Graphs: X & Y
- Referee: R



The isomorphism game

We need:

- Players: Alice & Bob
- Graphs: X & Y
- Referee: R



Winning the game

Alice and Bob win the game if their output vertices, y, y', have the same relation as their input vertices x, x'.

Winning the game

Alice and Bob win the game if their output vertices, y, y', have the same relation as their input vertices x, x'. In other words,

- if $x = x'$, then $y = y'$,

Winning the game

Alice and Bob win the game if their output vertices, y, y', have the same relation as their input vertices x, x'. In other words,

- if $x = x'$, then $y = y'$,
- if $x \sim x'$, then $y \sim y'$, and

Winning the game

Alice and Bob win the game if their output vertices, y, y', have the same relation as their input vertices x, x'. In other words,

- if $x = x'$, then $y = y'$,
- if $x \sim x'$, then $y \sim y'$, and
- if $x \neq x'$ and $x \not\sim x'$, then $y \neq y'$ and $y \not\sim y'$

Quantum isomorphic graphs

Classical:

$$\text{Alice \& Bob win} \iff X \cong Y$$

Quantum isomorphic graphs

Classical:

$$\text{Alice \& Bob win} \iff X \cong Y$$

Quantum:

If they have access to an entangled quantum state, they can win on non-isomorphic graphs.

Quantum isomorphic graphs

Classical:

$$\text{Alice \& Bob win} \iff X \cong Y$$

Quantum:

If they have access to an entangled quantum state, they can win on non-isomorphic graphs.

Definition

Graphs X and Y are *quantum isomorphic*, denoted $X \cong_q Y$, if Alice and Bob can win the isomorphism game using a quantum strategy.

Another definition

Definition

A *quantum permutation matrix* is an $n \times n$ matrix, $U = (u_{ij})_{i,j \in [n]}$ whose entries are elements of a C^*-algebra and satisfy

- $u_{i,j} = u_{i,j}^* = u_{i,j}^2$, for all $i, j \in [n]$ and
- $\sum_{i=1}^{n} u_{i,k} = \sum_{j=1}^{n} u_{\ell,j} = I$, for all $\ell, k \in [n]$.

Another definition

Definition

A *quantum permutation matrix* is an $n \times n$ matrix, $U = (u_{ij})_{i,j \in [n]}$ whose entries are elements of a C^*-algebra and satisfy

- $u_{i,j} = u_{i,j}^* = u_{i,j}^2$, for all $i, j \in [n]$ and
- $\sum_{i=1}^{n} u_{i,k} = \sum_{j=1}^{n} u_{\ell,j} = I$, for all $\ell, k \in [n]$.

- Permutation matrices.

Another definition

Definition

A *quantum permutation matrix* is an $n \times n$ matrix, $U = (u_{ij})_{i,j \in [n]}$ whose entries are elements of a C^*-algebra and satisfy

- $u_{i,j} = u_{i,j}^* = u_{i,j}^2$, for all $i, j \in [n]$ and
- $\sum_{i=1}^{n} u_{i,k} = \sum_{j=1}^{n} u_{\ell,j} = I$, for all $\ell, k \in [n]$.

- Permutation matrices.
- $\frac{1}{2}\begin{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} & \begin{pmatrix} 1 & - \\ - & 1 \end{pmatrix} \\ \begin{pmatrix} 1 & - \\ - & 1 \end{pmatrix} & \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \end{pmatrix}$

Another definition

Definition

Let X and Y be graphs with adjacency matrices A_X and A_Y, respectively. Then X and Y are *quantum isomorphic* if there exits a quantum permutation matrix U satisfying

$$A_X U = U A_Y\,.$$

Another definition

Definition

Let X and Y be graphs with adjacency matrices A_X and A_Y, respectively. Then X and Y are *quantum isomorphic* if there exits a quantum permutation matrix U satisfying

$$A_X U = U A_Y .$$

Remark

X and Y are isomorphic if and only if there exists a permutation matrix, P satisfying

$$A_X P = P A_Y .$$

Outline

Quantum Latin Squares

Definition

A *quantum Latin square (QLS)*, $\Psi = (\psi_{i,j})_{i,j \in [n]}$, is an $n \times n$ array of vectors from an n-dimensional complex vector space V such that the entries of each row and column form an orthonormal basis of V.

Quantum Latin Squares

Definition

A *quantum Latin square (QLS)*, $\Psi = (\psi_{i,j})_{i,j\in[n]}$, is an $n \times n$ array of vectors from an n-dimensional complex vector space V such that the entries of each row and column form an orthonormal basis of V.

$\frac{1}{\sqrt{3}}$

$(1,1,1)$	$(1,\omega,\omega^2)$	$(1,\omega^2,\omega)$
$(1,\omega,\omega^2)$	$(1,\omega^2,\omega)$	$(1,1,1)$
$(1,\omega^2,\omega)$	$(1,1,1)$	$(1,\omega,\omega^2)$

Quantum Latin Squares

Definition

A *quantum Latin square (QLS)*, $\Psi = (\psi_{i,j})_{i,j \in [n]}$, is an $n \times n$ array of vectors from an n-dimensional complex vector space V such that the entries of each row and column form an orthonormal basis of V.

$$\frac{1}{\sqrt{3}} \begin{array}{|c|c|c|} \hline (1,1,1) & (1,\omega,\omega^2) & (1,\omega^2,\omega) \\ \hline (1,\omega,\omega^2) & (1,\omega^2,\omega) & (1,1,1) \\ \hline (1,\omega^2,\omega) & (1,1,1) & (1,\omega,\omega^2) \\ \hline \end{array} \rightarrow \begin{array}{|c|c|c|} \hline 1 & 2 & 3 \\ \hline 2 & 3 & 1 \\ \hline 3 & 1 & 2 \\ \hline \end{array}$$

A quantum Latin square, where $\omega := e^{2\pi/3}$.

Quantum Latin squares

$\frac{1}{2}$

$(1,1,1,1)$	$(1,-1,1,-1)$	$(1,1,-1,-1)$	$(1,-1,-1,1)$
$(1,-i,-1,i)$	$(1,i,-1,-i)$	$(1,-i,1,-i)$	$(1,i,1,i)$
$(1,-1,1,-1)$	$(1,1,1,1)$	$(1,-1,-1,1)$	$(1,1,-1,-1)$
$(1,i,-1,-i)$	$(1,-i,-1,i)$	$(1,i,1,i)$	$(1,-i,1,-i)$

Quantum Latin squares

$$\frac{1}{2}\begin{array}{|c|c|c|c|}\hline (1,1,1,1) & (1,-1,1,-1) & (1,1,-1,-1) & (1,-1,-1,1) \\ \hline (1,-i,-1,i) & (1,i,-1,-i) & (1,-i,1,-i) & (1,i,1,i) \\ \hline (1,-1,1,-1) & (1,1,1,1) & (1,-1,-1,1) & (1,1,-1,-1) \\ \hline (1,i,-1,-i) & (1,-i,-1,i) & (1,i,1,i) & (1,-i,1,-i) \\ \hline \end{array}$$

Remark

Given a quantum Latin square, we can form a quantum permutation matrix by taking $u_{i,j}$ to be the projection onto the i, j-entry.

Outline

Group-invariant QLS

Definition

For finite groups G and H, we say that a quantum Latin square $\Psi = (\psi_{a,b})$ is (G, H)-*invariant* if its rows are indexed by G and its columns by H and the inner product $\langle \psi_{a,b} \mid \psi_{c,d} \rangle$ depends only on the values of $a^{-1}c \in G$ and $b^{-1}d \in H$.

Again this example

Let $G = \mathbb{Z}_4 = \langle g \rangle$ and $H = \mathbb{Z}_2^2 = \langle x, y \rangle$.

	e	x	y	xy
e	$(1,1,1,1)$	$(1,-1,1,-1)$	$(1,1,-1,-1)$	$(1,-1,-1,1)$
g	$(1,-i,-1,i)$	$(1,i,-1,-i)$	$(1,-i,1,-i)$	$(1,i,1,i)$
g^2	$(1,-1,1,-1)$	$(1,1,1,1)$	$(1,-1,-1,1)$	$(1,1,-1,-1)$
g^3	$(1,i,-1,-i)$	$(1,-i,-1,i)$	$(1,i,1,i)$	$(1,-i,1,-i)$

Take for example $\psi_{g,e}, \psi_{e,y}$ and $\psi_{g^2,x}, \psi_{g,xy}$.

Again this example

Let $G = \mathbb{Z}_4 = \langle g \rangle$ and $H = \mathbb{Z}_2^2 = \langle x, y \rangle$.

	e	x	y	xy
e	$(1,1,1,1)$	$(1,-1,1,-1)$	$(1,1,-1,-1)$	$(1,-1,-1,1)$
g	$(1,-i,-1,i)$	$(1,i,-1,-i)$	$(1,-i,1,-i)$	$(1,i,1,i)$
g^2	$(1,-1,1,-1)$	$(1,1,1,1)$	$(1,-1,-1,1)$	$(1,1,-1,-1)$
g^3	$(1,i,-1,-i)$	$(1,-i,-1,i)$	$(1,i,1,i)$	$(1,-i,1,-i)$

Take for example $\psi_{g,e}, \psi_{e,y}$ and $\psi_{g^2,x}, \psi_{g,xy}$. Then

$$g^{-1}e = g^{-1} = g^{-2}g \quad \text{and} \quad e^{-1}y = y = x^{-1}xy.$$

Again this example

Let $G = \mathbb{Z}_4 = \langle g \rangle$ and $H = \mathbb{Z}_2^2 = \langle x, y \rangle$.

	e	x	y	xy
e	$(1,1,1,1)$	$(1,-1,1,-1)$	$(1,1,-1,-1)$	$(1,-1,-1,1)$
g	$(1,-i,-1,i)$	$(1,i,-1,-i)$	$(1,-i,1,-i)$	$(1,i,1,i)$
g^2	$(1,-1,1,-1)$	$(1,1,1,1)$	$(1,-1,-1,1)$	$(1,1,-1,-1)$
g^3	$(1,i,-1,-i)$	$(1,-i,-1,i)$	$(1,i,1,i)$	$(1,-i,1,-i)$

Take for example $\psi_{g,e}, \psi_{e,y}$ and $\psi_{g^2,x}, \psi_{g,xy}$. Then

$$g^{-1}e = g^{-1} = g^{-2}g \quad \text{and} \quad e^{-1}y = y = x^{-1}xy.$$

Indeed we have

$$\langle \psi_{g,e} | \psi_{e,y} \rangle = \frac{1-i}{2} = \langle \psi_{g^2,x} | \psi_{g,xy} \rangle.$$

Transformation matrices

Definition

Suppose that $\Psi = (\psi_{a,b})$ is a (G, H)-invariant quantum Latin square. Define its *transformation matrix*, denoted U^{Ψ}, to be the $|G| \times |H|$ matrix defined entrywise as

$$U^{\Psi}_{g,h} = \langle \psi_{a,b} \mid \psi_{c,d} \rangle$$

for some $a, c \in G,\ b, d \in H$ such that $a^{-1}c = g$ and $b^{-1}d = h$.

Transformation matrices

Definition

Suppose that $\Psi = (\psi_{a,b})$ is a (G, H)-invariant quantum Latin square. Define its *transformation matrix*, denoted U^Ψ, to be the $|G| \times |H|$ matrix defined entrywise as

$$U^\Psi_{g,h} = \langle \psi_{a,b} \mid \psi_{c,d} \rangle$$

for some $a, c \in G,\ b, d \in H$ such that $a^{-1}c = g$ and $b^{-1}d = h$.

Our previous example is $(\mathbb{Z}_4, \mathbb{Z}_2^2)$-invariant with the following transformation matrix where $\alpha = \frac{1+i}{2}$ and $\beta = \frac{1-i}{2}$.

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & \alpha & \beta \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \beta & \alpha \end{pmatrix}$$

Properties

Let $U \in \mathbb{C}^{G \times H}$ be the transformation matrix for a (G, H)-invariant quantum Latin square. Then U satisfies the following:

Properties

Let $U \in \mathbb{C}^{G \times H}$ be the transformation matrix for a (G, H)-invariant quantum Latin square. Then U satisfies the following:

- It is unitary,

Properties

Let $U \in \mathbb{C}^{G \times H}$ be the transformation matrix for a (G, H)-invariant quantum Latin square. Then U satisfies the following:

- It is unitary,
- $\overline{U_{a,b}} = U_{a^{-1},b^{-1}}$, for all $a \in G$, $b \in H$, and

Properties

Let $U \in \mathbb{C}^{G \times H}$ be the transformation matrix for a (G, H)-invariant quantum Latin square. Then U satisfies the following:

- It is unitary,
- $\overline{U_{a,b}} = U_{a^{-1},b^{-1}}$, for all $a \in G$, $b \in H$, and
- $U_{ab,c} = \sum_{\substack{x,y \in H \\ xy = c}} U_{a,x} U_{b,y}$ for all $a, b \in G$ and $c \in H$.

Properties

Let $U \in \mathbb{C}^{G \times H}$ be the transformation matrix for a (G, H)-invariant quantum Latin square. Then U satisfies the following:

- It is unitary,
- $\overline{U_{a,b}} = U_{a^{-1},b^{-1}}$, for all $a \in G$, $b \in H$, and
- $U_{ab,c} = \sum_{\substack{x,y \in H \\ xy = c}} U_{a,x} U_{b,y}$ for all $a, b \in G$ and $c \in H$.

In fact, these three conditions are sufficient.

Theorem

A matrix, $U \in \mathbb{C}^{G\times H}$ is a transformation matrix for some (G,H)-invariant quantum Latin square if and only if

- *It is unitary,*
- $\overline{U_{a,b}} = U_{a^{-1},b^{-1}}$*, for all* $a \in G$*,* $b \in H$*, and*
- $U_{ab,c} = \sum_{\substack{x,y\in H\\ xy=c}} U_{a,x}U_{b,y}$ *for all* $a,b \in G$ *and* $c \in H$.

Outline

Cayley graphs

Definition

Let G be a group and $D \subseteq G \backslash \{e\}$ a subset with $D^{-1} = D$. The *Cayley graph*, $X := \mathrm{Cay}(G, D)$, has vertex set $V(X) := G$, and

$$g \sim h \quad \text{if} \quad hg^{-1} \in D.$$

The set D is called the *connection set* of the graph.

Cayley graphs

Definition

Let G be a group and $D \subseteq G \backslash \{e\}$ a subset with $D^{-1} = D$. The *Cayley graph*, $X := \mathrm{Cay}(G, D)$, has vertex set $V(X) := G$, and

$$g \sim h \quad \text{if} \quad hg^{-1} \in D.$$

The set D is called the *connection set* of the graph.

A vague and mostly useless statement

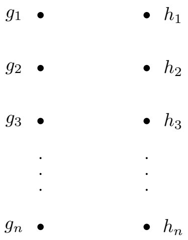
We can use a (G, H)-transformation matrix, to construct pairs, (X, Y) of quantum isomorphic graphs where $X = \mathrm{Cay}(G, D)$ and $Y = \mathrm{Cay}(H, D')$.

The construction

Let U be a (G, H)-transformation matrix. We construct an auxiliary graph with vertex set $G \cup H$:

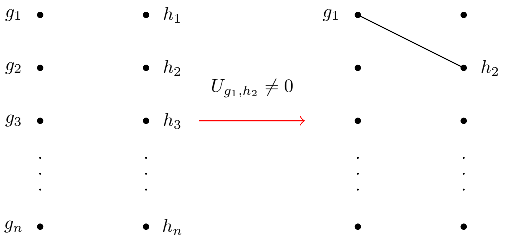
The construction

Let U be a (G, H)-transformation matrix. We construct an auxiliary graph with vertex set $G \cup H$:



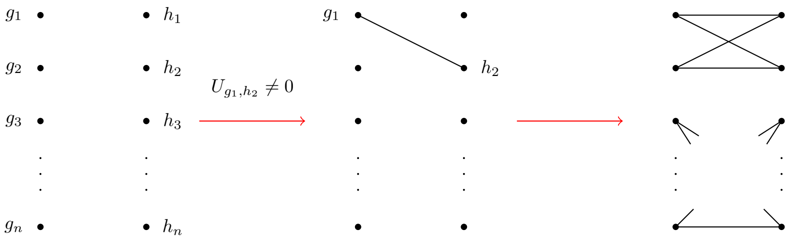
The construction

Let U be a (G, H)-transformation matrix. We construct an auxiliary graph with vertex set $G \cup H$:

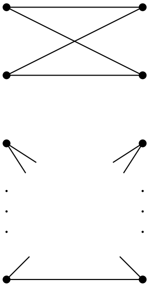


The construction

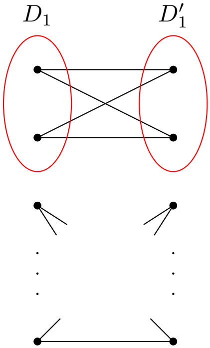
Let U be a (G, H)-transformation matrix. We construct an auxiliary graph with vertex set $G \cup H$:



The construction

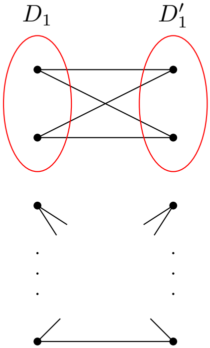


The construction



Let $C_1, \ldots, C_k$ be the connected components of this graph and define $D_i := C_i \cap G$ and $D'_i := C_i \cap H$.

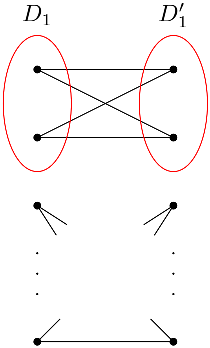
The construction



Let $C_1, \ldots, C_k$ be the connected components of this graph and define $D_i := C_i \cap G$ and $D'_i := C_i \cap H$.

Then the Cayley graphs $\mathrm{Cay}(G, D_i)$ and $\mathrm{Cay}(H, D'_i)$ are quantum isomorphic for all $i = 1, \ldots, k$.

The construction



Let $C_1, \dots, C_k$ be the connected components of this graph and define $D_i := C_i \cap G$ and $D'_i := C_i \cap H$.

Then the Cayley graphs $\mathrm{Cay}(G, D_i)$ and $\mathrm{Cay}(H, D'_i)$ are quantum isomorphic for all $i = 1, \dots, k$.

More generally, for any subset I of $[k]$, $\mathrm{Cay}\left(G, \sum_{i \in I} D_i\right)$ and $\mathrm{Cay}\left(H, \sum_{i \in I} D'_i\right)$ are quantum isomorphic.

Outline

Existence

For which groups G, H does a (G, H)-transformation matrix exist?

Existence

For which groups G, H does a (G, H)-transformation matrix exist?

Theorem (Árnadóttir & Roberson, 2025+)

Let G, H be finite groups. A (G, H)-invariant QLS exists if and only if the group algebras of G and H are isomorphic.

Existence

For which groups G, H does a (G, H)-transformation matrix exist?

Theorem (Árnadóttir & Roberson, 2025+)

Let G, H be finite groups. A (G, H)-invariant QLS exists if and only if the group algebras of G and H are isomorphic.

Remark

The group algebras of G and H being isomorphic is equivalent to the degrees of their irreducible characters being the same.

Proof - part 1

For a group G with left regular representation λ, the group algebra is given by $\Lambda_G := \mathrm{span}\{\lambda(g) : g \in G\}$.

Proof - part 1

For a group G with left regular representation λ, the group algebra is given by $\Lambda_G := \operatorname{span}\{\lambda(g) : g \in G\}$.

Lemma

Let G be a finite group with left regular representation λ and irreducible, unitary representations $\rho_1, \ldots, \rho_r$ with degrees $d_1 \ldots, d_r$. Then the map

$$\Phi_G : \Lambda_G \to \bigoplus_{i=1}^{r} \big(I_{d_i} \otimes M_{d_i}(\mathbb{C})\big), \quad \lambda(g) \mapsto \bigoplus_{i=1}^{r} \big(I_{d_i} \otimes \rho_i(g)\big)$$

(extended linearly) is an algebra isomorphism that preserves trace and commutes with the conjugate transpose.

Proof - part 2

Lemma

Let G and H be groups with isomorphic group algebras, Λ_G and Λ_H. Then there exists an isomorphism, $\Psi : \Lambda_G \to \Lambda_H$ that preserves trace and commutes with the conjugate transpose.

Proof - part 3

Lemma

Let G and H be finite groups with left regular representations λ and λ', respectively. Then $U \in \mathbb{C}^{G\times H}$ is a (G, H)-transformation matrix if and only if the linear map $\Psi_U : \Lambda_H \to \Lambda_G$ given by

$$\Psi_U(\lambda'(b)) = \sum_{a\in G} U_{a,b}\lambda(a)$$

is an algebra isomorphism preserving trace and conjugate transpose. Moreover, every such isomorphism from Λ_H to Λ_G is attained in this way.

Conclusion of proof

Proof. It follows from the previous lemmas that:

- There is one-to-one correspondence between (G, H)-transformation matrices and isomorphisms between the algebras that preserve trace and conjugate transpose.

Conclusion of proof

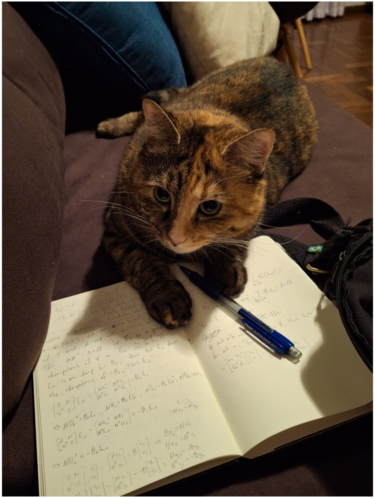
Proof. It follows from the previous lemmas that:

- There is one-to-one correspondence between (G, H)-transformation matrices and isomorphisms between the algebras that preserve trace and conjugate transpose.
- Such isomorphisms exists if and only if the algebras are isomorphic.

Thus the existence theorem follows. □

Thank you

My paper



My cat

Example

Let G and H be finite abelian groups with $|G| = |H| =: n$. Let $\chi_1, \ldots, \chi_n$ and $\chi'_1, \ldots, \chi'_n$ be the irreducible characters of G and H, respectively.

Example

Let G and H be finite abelian groups with $|G| = |H| =: n$. Let $\chi_1, \ldots, \chi_n$ and $\chi'_1, \ldots, \chi'_n$ be the irreducible characters of G and H, respectively. For $g \in G$ and $h \in H$, define

$$\psi_{g,h} := \frac{1}{n}\big(\chi_1(g^{-1})\chi'_1(h), \ldots, \chi_n(g^{-1})\chi'_n(h)\big).$$

Example

Let G and H be finite abelian groups with $|G| = |H| =: n$. Let $\chi_1, \ldots, \chi_n$ and $\chi'_1, \ldots, \chi'_n$ be the irreducible characters of G and H, respectively. For $g \in G$ and $h \in H$, define

$$\psi_{g,h} := \frac{1}{n}\big(\chi_1(g^{-1})\chi'_1(h), \ldots, \chi_n(g^{-1})\chi'_n(h)\big).$$

Then $\big(\psi_{g,h}\big)_{g \in G, h \in H}$ is a (G, H)-invariant quantum Latin square with inner product matrix

$$U = \frac{1}{n^2} M^* M'$$

where M and M' are the character tables of G and H, respectively, and M^* denotes the conjugate transpose of M.

Example

Take $G := \mathbb{Z}_4$ and $H := \mathbb{Z}_2^2$.

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} \quad \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

Example

Take $G := \mathbb{Z}_4$ and $H := \mathbb{Z}_2^2$.

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} \quad \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

We get the following (G, H)-invariant quantum Latin square:

$$\frac{1}{2}\begin{array}{|c|c|c|c|} \hline (1,1,1,1) & (1,-1,1,-1) & (1,1,-1,-1) & (1,-1,-1,1) \\ \hline (1,-i,-1,i) & (1,i,-1,-i) & (1,-i,1,-i) & (1,i,1,i) \\ \hline (1,-1,1,-1) & (1,1,1,1) & (1,-1,-1,1) & (1,1,-1,-1) \\ \hline (1,i,-1,-i) & (1,-i,-1,i) & (1,i,1,i) & (1,-i,1,-i) \\ \hline \end{array}$$