Quantum Latin Squares

and Unitary Error Bases

Ben Musto   Jamie Vicary

Department of Computer Science
University of Oxford

26 November 2015

Latin squares

Definition

A *Latin square of order n* is an n-by-n array of integers in the range $\{0, \ldots, n-1\}$, such that every row and column contains each number exactly once.

Latin squares

Definition

A *Latin square of order n* is an n-by-n array of integers in the range $\{0, \ldots, n-1\}$, such that every row and column contains each number exactly once.

By sending $k \in \{0, \ldots, n-1\}$ to $|k\rangle \in \mathbb{C}^n$, we can turn a Latin square into an array of Hilbert space elements:

3	1	0	2
1	0	2	3
2	3	1	0
0	2	3	1

$\rightsquigarrow$

$\|3\rangle$	$\|1\rangle$	$\|0\rangle$	$\|2\rangle$
$\|1\rangle$	$\|0\rangle$	$\|2\rangle$	$\|3\rangle$
$\|2\rangle$	$\|3\rangle$	$\|1\rangle$	$\|0\rangle$
$\|0\rangle$	$\|2\rangle$	$\|3\rangle$	$\|1\rangle$

Main definition - quantum Latin squares

Definition

A *quantum Latin square of order n* is an n-by-n grid of elements of the Hilbert space $\mathbb{C}^n$, such that every row and column is an orthonormal basis.

Main definition - quantum Latin squares

Definition

A *quantum Latin square of order n* is an n-by-n grid of elements of the Hilbert space $\mathbb{C}^n$, such that every row and column is an orthonormal basis.

For example:

$\|0\rangle$	$\|1\rangle$	$\|2\rangle$	$\|3\rangle$
$\frac{1}{\sqrt{2}}(\|1\rangle - \|2\rangle)$	$\frac{1}{\sqrt{5}}(i\|0\rangle + 2\|3\rangle)$	$\frac{1}{\sqrt{5}}(2\|0\rangle + i\|3\rangle)$	$\frac{1}{\sqrt{2}}(\|1\rangle + \|2\rangle)$
$\frac{1}{\sqrt{2}}(\|1\rangle + \|2\rangle)$	$\frac{1}{\sqrt{5}}(2\|0\rangle + i\|3\rangle)$	$\frac{1}{\sqrt{5}}(i\|0\rangle + 2\|3\rangle)$	$\frac{1}{\sqrt{2}}(\|1\rangle - \|2\rangle)$
$\|3\rangle$	$\|2\rangle$	$\|1\rangle$	$\|0\rangle$

Here is our example quantum Latin square:

$\lvert 0\rangle$	$\lvert 1\rangle$	$\lvert 2\rangle$	$\lvert 3\rangle$
$\frac{1}{\sqrt{2}}(\lvert 1\rangle - \lvert 2\rangle)$	$\frac{1}{\sqrt{5}}(i\lvert 0\rangle + 2\lvert 3\rangle)$	$\frac{1}{\sqrt{5}}(2\lvert 0\rangle + i\lvert 3\rangle)$	$\frac{1}{\sqrt{2}}(\lvert 1\rangle + \lvert 2\rangle)$
$\frac{1}{\sqrt{2}}(\lvert 1\rangle + \lvert 2\rangle)$	$\frac{1}{\sqrt{5}}(2\lvert 0\rangle + i\lvert 3\rangle)$	$\frac{1}{\sqrt{5}}(i\lvert 0\rangle + 2\lvert 3\rangle)$	$\frac{1}{\sqrt{2}}(\lvert 1\rangle - \lvert 2\rangle)$
$\lvert 3\rangle$	$\lvert 2\rangle$	$\lvert 1\rangle$	$\lvert 0\rangle$

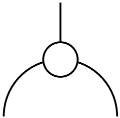
Here is our example quantum Latin square:

	$\|0\rangle$	$\|1\rangle$	$\|2\rangle$	$\|3\rangle$
$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|2\rangle$	$\|3\rangle$
$\|1\rangle$	$\frac{1}{\sqrt{2}}(\|1\rangle - \|2\rangle)$	$\frac{1}{\sqrt{5}}(i\|0\rangle + 2\|3\rangle)$	$\frac{1}{\sqrt{5}}(2\|0\rangle + i\|3\rangle)$	$\frac{1}{\sqrt{2}}(\|1\rangle + \|2\rangle)$
$\|2\rangle$	$\frac{1}{\sqrt{2}}(\|1\rangle + \|2\rangle)$	$\frac{1}{\sqrt{5}}(2\|0\rangle + i\|3\rangle)$	$\frac{1}{\sqrt{5}}(i\|0\rangle + 2\|3\rangle)$	$\frac{1}{\sqrt{2}}(\|1\rangle - \|2\rangle)$
$\|3\rangle$	$\|3\rangle$	$\|2\rangle$	$\|1\rangle$	$\|0\rangle$

Here is our example quantum Latin square:

	$\|0\rangle$	$\|1\rangle$	$\|2\rangle$	$\|3\rangle$
$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|2\rangle$	$\|3\rangle$
$\|1\rangle$	$\frac{1}{\sqrt{2}}(\|1\rangle - \|2\rangle)$	$\frac{1}{\sqrt{5}}(i\|0\rangle + 2\|3\rangle)$	$\frac{1}{\sqrt{5}}(2\|0\rangle + i\|3\rangle)$	$\frac{1}{\sqrt{2}}(\|1\rangle + \|2\rangle)$
$\|2\rangle$	$\frac{1}{\sqrt{2}}(\|1\rangle + \|2\rangle)$	$\frac{1}{\sqrt{5}}(2\|0\rangle + i\|3\rangle)$	$\frac{1}{\sqrt{5}}(i\|0\rangle + 2\|3\rangle)$	$\frac{1}{\sqrt{2}}(\|1\rangle - \|2\rangle)$
$\|3\rangle$	$\|3\rangle$	$\|2\rangle$	$\|1\rangle$	$\|0\rangle$

$\rightsquigarrow$



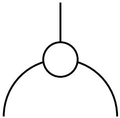
We can encode this data as a linear map.

Quantum Latin squares
as linear maps in Hilbert space

Here is our example quantum Latin square:

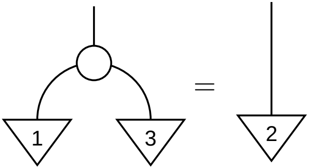
	$\vert 0\rangle$	$\vert 1\rangle$	$\vert 2\rangle$	$\vert 3\rangle$
$\vert 0\rangle$	$\vert 0\rangle$	$\vert 1\rangle$	$\vert 2\rangle$	$\vert 3\rangle$
$\vert 1\rangle$	$\frac{1}{\sqrt{2}}(\vert 1\rangle - \vert 2\rangle)$	$\frac{1}{\sqrt{5}}(i\vert 0\rangle + 2\vert 3\rangle)$	$\frac{1}{\sqrt{5}}(2\vert 0\rangle + i\vert 3\rangle)$	$\frac{1}{\sqrt{2}}(\vert 1\rangle + \vert 2\rangle)$
$\vert 2\rangle$	$\frac{1}{\sqrt{2}}(\vert 1\rangle + \vert 2\rangle)$	$\frac{1}{\sqrt{5}}(2\vert 0\rangle + i\vert 3\rangle)$	$\frac{1}{\sqrt{5}}(i\vert 0\rangle + 2\vert 3\rangle)$	$\frac{1}{\sqrt{2}}(\vert 1\rangle - \vert 2\rangle)$
$\vert 3\rangle$	$\vert 3\rangle$	$\vert 2\rangle$	$\vert 1\rangle$	$\vert 0\rangle$

$\rightsquigarrow$



We can encode this data as a linear map.

For example:



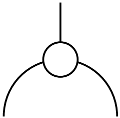
Quantum Latin squares

as linear maps in Hilbert space

Here is our example quantum Latin square:

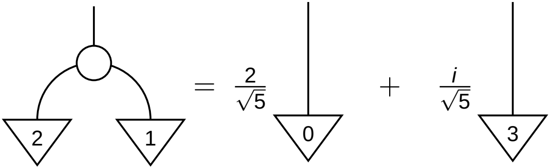
	$\|0\rangle$	$\|1\rangle$	$\|2\rangle$	$\|3\rangle$
$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|2\rangle$	$\|3\rangle$
$\|1\rangle$	$\frac{1}{\sqrt{2}}(\|1\rangle - \|2\rangle)$	$\frac{1}{\sqrt{5}}(i\|0\rangle + 2\|3\rangle)$	$\frac{1}{\sqrt{5}}(2\|0\rangle + i\|3\rangle)$	$\frac{1}{\sqrt{2}}(\|1\rangle + \|2\rangle)$
$\|2\rangle$	$\frac{1}{\sqrt{2}}(\|1\rangle + \|2\rangle)$	$\frac{1}{\sqrt{5}}(2\|0\rangle + i\|3\rangle)$	$\frac{1}{\sqrt{5}}(i\|0\rangle + 2\|3\rangle)$	$\frac{1}{\sqrt{2}}(\|1\rangle - \|2\rangle)$
$\|3\rangle$	$\|3\rangle$	$\|2\rangle$	$\|1\rangle$	$\|0\rangle$

$\rightsquigarrow$



We can encode this data as a linear map.

For example:

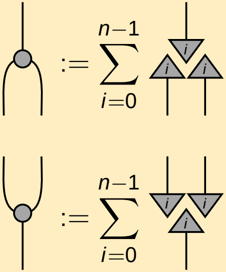


Definition (Basis tensors)

Given a basis for a Hilbert space, $|i\rangle, 0 \leq i < n-1$, we canonically define the following two linear maps:

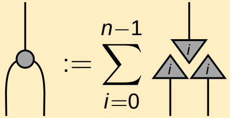
Definition (Basis tensors)

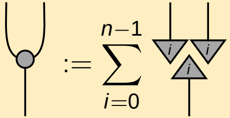
Given a basis for a Hilbert space, $|i\rangle, 0 \leq i < n-1$, we canonically define the following two linear maps:



Definition (Basis tensors)

Given a basis for a Hilbert space, $|i\rangle, 0 \leq i < n-1$, we canonically define the following two linear maps:



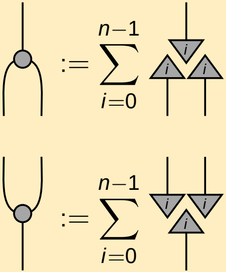


A grey dot will represent the computational basis.

Bases
as tensors

Definition (Basis tensors)

Given a basis for a Hilbert space, $|i\rangle, 0 \leq i < n-1$, we canonically define the following two linear maps:



Basis tensors are uniquely characterized by the property that connected composites with the same boundary are equal.

Mutually unbiased bases (MUBs)

as characterised through spider tensors

MUBs have a nice characterisation in terms of tensors.

MUBs have a nice characterisation in terms of tensors.

Definition (Mutually unbiased bases)

Given two orthonormal bases $|a_i\rangle$ and $|b_j\rangle$ for the n dimensional Hilbert space $\mathcal{H}$, they are mutually unbiased when:

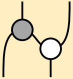
$$|\langle a_i|b_j\rangle|^2 = \frac{1}{n}$$

$\forall i,j\,,\ 0 \leq i,j < n-1$.

MUBs have a nice characterisation in terms of tensors.

Theorem

For orthonormal bases  *and* *, the following are equivalent:*

- *the bases are mutually unbiased;*
- *the composite*  *is unitary (up to a constant).*

Graphical characterisation

Let  be a linear map and  be a basis tensor;

Graphical characterisation

Let  be a linear map and  be a basis tensor;

Quantum Latin squares

Graphical characterisation

Let  be a linear map and  be a basis tensor;

Quantum Latin squares

 ,  are unitary

Graphical characterisation

Let  be a linear map and  be a basis tensor;

Quantum Latin squares   *Latin squares*

 ,  are unitary

Graphical characterisation

Let  be a linear map and  be a basis tensor;

Quantum Latin squares

 ,  are unitary

Latin squares

 ,  are unitary

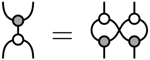
Let  be a linear map and  be a basis tensor;

Quantum Latin squares

 ,  are unitary

Latin squares

 ,  are unitary



Graphical characterisation

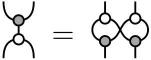
Let  be a linear map and  be a basis tensor;

Quantum Latin squares

 ,  are unitary

Latin squares

 ,  are unitary



Quantum Latin squares generalise Latin squares.

Graphical characterisation

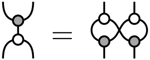
Let  be a linear map and  be a basis tensor;

Quantum Latin squares

 ,  are unitary

Latin squares

 ,  are unitary



Mutually unbiased bases

Graphical characterisation

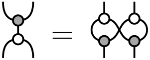
Let  be a linear map and  be a basis tensor;

Quantum Latin squares

 ,  are unitary

Latin squares

 ,  are unitary



Mutually unbiased bases

 ,  are unitary

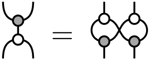
Let  be a linear map and  be a basis tensor;

Quantum Latin squares

 ,  are unitary

Latin squares

 ,  are unitary



Mutually unbiased bases

 ,  are unitary

 is a basis tensor

Graphical characterisation

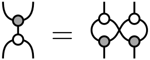
Let  be a linear map and  be a basis tensor;

Quantum Latin squares

 ,  are unitary

Latin squares

 ,  are unitary



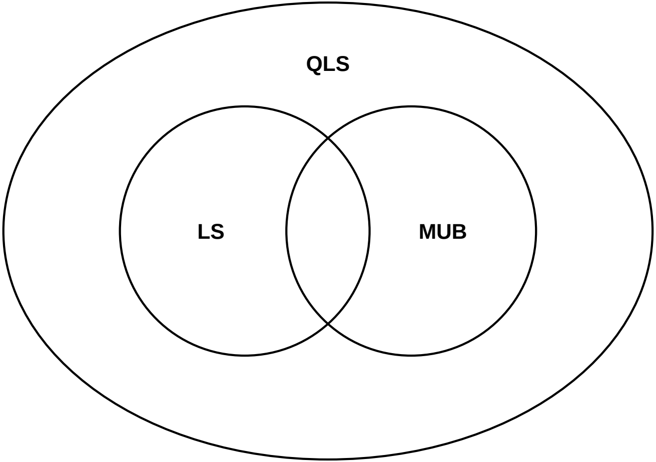
Mutually unbiased bases

 ,  are unitary

 is a basis tensor

Hence Quantum Latin squares generalise both Latin squares and mutually unbiased bases.

Venn Diagram 1



Unitary Error Bases

Definition

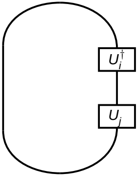
For a Hilbert space $\mathcal{H}$ of dimension n, a *unitary error basis* is an n^2 family of unitary operators which form an orthogonal basis.

$$\mathrm{Tr}(U_i^\dagger \circ U_j) = \delta_{ij} n$$

Unitary Error Bases

Definition

For a Hilbert space $\mathcal{H}$ of dimension n, a *unitary error basis* is an n^2 family of unitary operators which form an orthogonal basis.

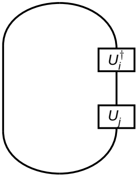


$= \delta_{ij} n$

Unitary Error Bases

Definition

For a Hilbert space $\mathcal{H}$ of dimension n, a *unitary error basis* is an n^2 family of unitary operators which form an orthogonal basis.



$= \delta_{ij} n$

Famous example: the Pauli matrices together with the identity.

Constructions of UEBs

How to construct a UEB for a Hilbert space of dimension n:

Constructions of UEBs

How to construct a UEB for a Hilbert space of dimension n:

- *LS construction* [Werner, 2001]
  Input: Latin square and n Hadamards (order n)

Constructions of UEBs

How to construct a UEB for a Hilbert space of dimension n:

- *LS construction* [Werner, 2001]
  Input: Latin square and n Hadamards (order n)
- *MUB construction* [folklore?]
  Input: Hadamard (order n)

Constructions of UEBs

How to construct a UEB for a Hilbert space of dimension n:

- *LS construction* [Werner, 2001]
  Input: Latin square and n Hadamards (order n)
- *MUB construction* [folklore?]
  Input: Hadamard (order n)
- *Algebraic construction* [Knill, 1996]
  Input: Group (order n^2) with nice representation

Constructions of UEBs

How to construct a UEB for a Hilbert space of dimension n:

- *LS construction* [Werner, 2001]
  Input: Latin square and n Hadamards (order n)
- *MUB construction* [folklore?]
  Input: Hadamard (order n)
- *Algebraic construction* [Knill, 1996]
  Input: Group (order n^2) with nice representation
- *QLS construction* [MV, 2015]
  Input: Quantum Latin square and n Hadamards (order n)

An example

Take our example quantum Latin square:

$\lvert 0\rangle$	$\lvert 1\rangle$	$\lvert 2\rangle$	$\lvert 3\rangle$
$\frac{1}{\sqrt{2}}(\lvert 1\rangle - \lvert 2\rangle)$	$\frac{1}{\sqrt{5}}(i\lvert 0\rangle + 2\lvert 3\rangle)$	$\frac{1}{\sqrt{5}}(2\lvert 0\rangle + i\lvert 3\rangle)$	$\frac{1}{\sqrt{2}}(\lvert 1\rangle + \lvert 2\rangle)$
$\frac{1}{\sqrt{2}}(\lvert 1\rangle + \lvert 2\rangle)$	$\frac{1}{\sqrt{5}}(2\lvert 0\rangle + i\lvert 3\rangle)$	$\frac{1}{\sqrt{5}}(i\lvert 0\rangle + 2\lvert 3\rangle)$	$\frac{1}{\sqrt{2}}(\lvert 1\rangle - \lvert 2\rangle)$
$\lvert 3\rangle$	$\lvert 2\rangle$	$\lvert 1\rangle$	$\lvert 0\rangle$

and the following family of Hadamard matrices:

$$H_0 = H_1 = H_2 = H_3 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$$

We get the following UEB, $\mathcal{M}$:

$$
\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}
\begin{pmatrix} 0 & \frac{i}{\sqrt{5}} & \frac{2}{\sqrt{5}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & \frac{2}{\sqrt{5}} & \frac{i}{\sqrt{5}} & 0 \end{pmatrix}
\begin{pmatrix} 0 & \frac{2}{\sqrt{5}} & \frac{i}{\sqrt{5}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}} \\ 0 & \frac{i}{\sqrt{5}} & \frac{2}{\sqrt{5}} & 0 \end{pmatrix}
\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}
$$

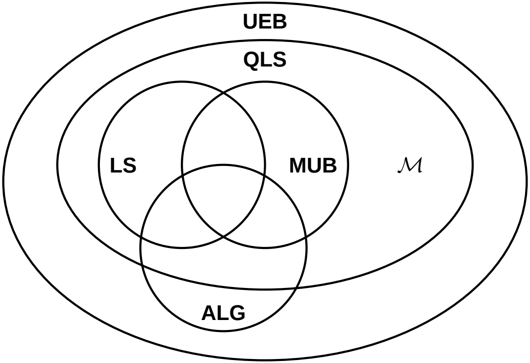
$$
\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -i \end{pmatrix}
\begin{pmatrix} 0 & -\frac{1}{\sqrt{5}} & -\frac{2}{\sqrt{5}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{i}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & 0 & 0 & -\frac{i}{\sqrt{2}} \\ 0 & \frac{2i}{\sqrt{5}} & -\frac{i}{\sqrt{5}} & 0 \end{pmatrix}
\begin{pmatrix} 0 & \frac{2i}{\sqrt{5}} & -\frac{i}{\sqrt{5}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{i}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 & 0 & \frac{i}{\sqrt{2}} \\ 0 & -\frac{1}{\sqrt{5}} & -\frac{2}{\sqrt{5}} & 0 \end{pmatrix}
\begin{pmatrix} 0 & 0 & 0 & -i \\ 0 & 0 & -1 & 0 \\ 0 & i & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}
$$

$$
\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}
\begin{pmatrix} 0 & -\frac{i}{\sqrt{5}} & \frac{2}{\sqrt{5}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}} \\ 0 & -\frac{2}{\sqrt{5}} & \frac{i}{\sqrt{5}} & 0 \end{pmatrix}
\begin{pmatrix} 0 & -\frac{2}{\sqrt{5}} & \frac{i}{\sqrt{5}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & -\frac{i}{\sqrt{5}} & \frac{2}{\sqrt{5}} & 0 \end{pmatrix}
\begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}
$$

$$
\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -i & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & i \end{pmatrix}
\begin{pmatrix} 0 & \frac{1}{\sqrt{5}} & -\frac{2}{\sqrt{5}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & \frac{i}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & 0 & 0 & \frac{i}{\sqrt{2}} \\ 0 & -\frac{2i}{\sqrt{5}} & -\frac{i}{\sqrt{5}} & 0 \end{pmatrix}
\begin{pmatrix} 0 & -\frac{2i}{\sqrt{5}} & -\frac{i}{\sqrt{5}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & \frac{i}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{i}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{5}} & -\frac{2}{\sqrt{5}} & 0 \end{pmatrix}
\begin{pmatrix} 0 & 0 & 0 & i \\ 0 & 0 & -1 & 0 \\ 0 & -i & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}
$$

Venn Diagram 2

Why our construction is great!



Theorem

The example UEB $\mathcal{M}$ is not in LS, MUB or ALG.

UEBs built from tensors

QLS UEB

UEBs built from tensors

QLS UEB

 - ONB

UEBs built from tensors

QLS UEB

 - ONB

H_j - n Hadamards

UEBs built from tensors

QLS UEB

 - ONB

H_j - *n* Hadamards

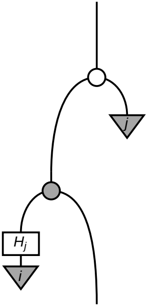
 - QLS

QLS UEB

 - ONB

H_j - n Hadamards

 - QLS



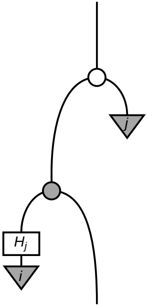
UEBs built from tensors

QLS UEB ***LS UEB***

 - ONB

H_j - n Hadamards

 - QLS



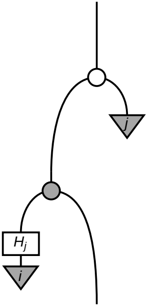
UEBs built from tensors

QLS UEB

 - ONB

H_j - n Hadamards

 - QLS



LS UEB

 - ONB

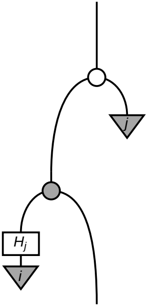
UEBs built from tensors

QLS UEB

 - ONB

H_j - n Hadamards

 - QLS



LS UEB

 - ONB

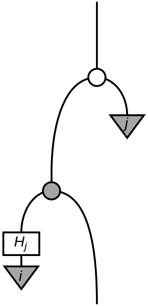
H_j - n Hadamards

QLS UEB

 - ONB

H_j - n Hadamards

 - QLS



LS UEB

 - ONB

H_j - n Hadamards

 - LS

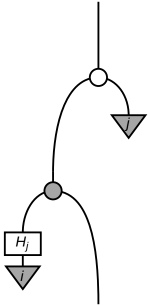
UEBs built from tensors

QLS UEB

- ONB

H_j - n Hadamards

- QLS

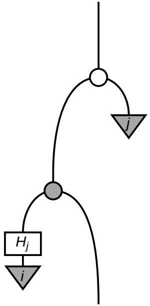


LS UEB

- ONB

H_j - n Hadamards

- LS

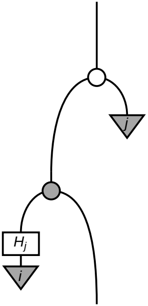


QLS UEB

 - ONB

H_j - n Hadamards

 - QLS

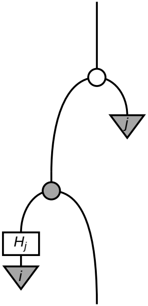


LS UEB

 - ONB

H_j - n Hadamards

 - LS



MUB UEB

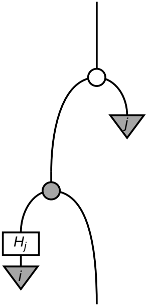
UEBs built from tensors

QLS UEB

 - ONB

H_j - n Hadamards

 - QLS

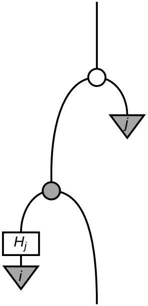


LS UEB

 - ONB

H_j - n Hadamards

 - LS



MUB UEB

 - ONB

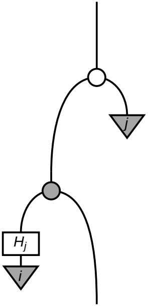
UEBs built from tensors

QLS UEB

 - ONB

H_j - n Hadamards

 - QLS

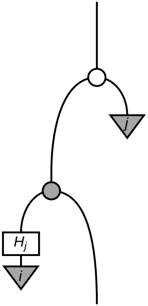


LS UEB

 - ONB

H_j - n Hadamards

 - LS



MUB UEB

 - ONB

H - Hadamard

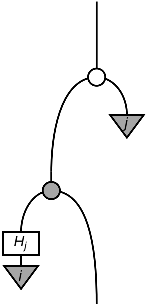
UEBs built from tensors

QLS UEB

 - ONB

H_j - *n* Hadamards

 - QLS

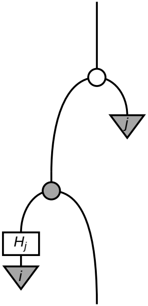


LS UEB

 - ONB

H_j - *n* Hadamards

 - LS



MUB UEB

 - ONB

H - Hadamard

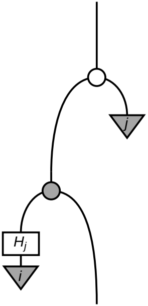
 - ONB

QLS UEB

- ONB

H_j - n Hadamards

- QLS

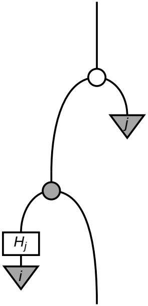


LS UEB

- ONB

H_j - n Hadamards

- LS

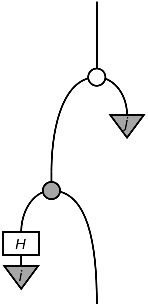


MUB UEB

- ONB

H - Hadamard

- ONB



Main Theorem

Theorem

Quantum Latin square bases are unitary error bases.

First we prove that the U_{ij} are unitary.

First we prove that the U_{ij} are unitary.

Proof.

Need to show that for all i, j: $U_{ij} \circ U_{ij}^{\dagger} = \mathbb{I}_n$.

First we prove that the U_{ij} are unitary.

Proof.

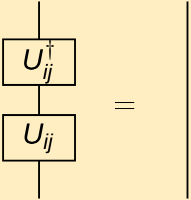
Need to show that for all i, j: $U_{ij} \circ U_{ij}^{\dagger} = \mathbb{I}_n$. Using tensor diagrams this condition becomes:

Main Theorem
Unitarity

First we prove that the U_{ij} are unitary.

Proof.

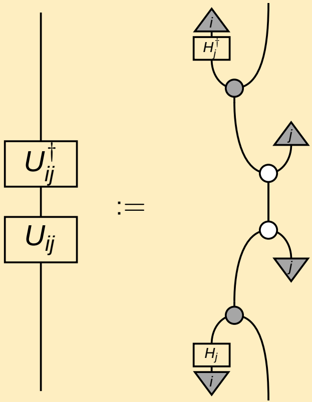
Need to show that for all i, j: $U_{ij} \circ U_{ij}^{\dagger} = \mathbb{I}_n$. Using tensor diagrams this condition becomes:



Main Theorem
Unitarity

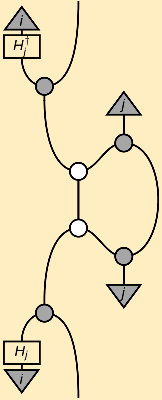
Proof.

By definition:



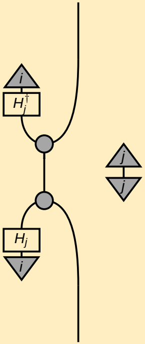
Proof.

$=$



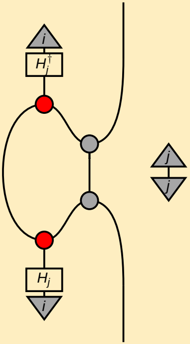
Proof.

$=$

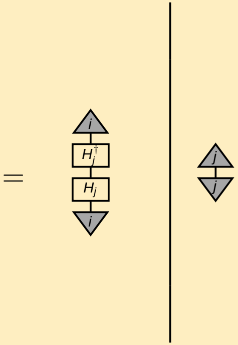


Proof.

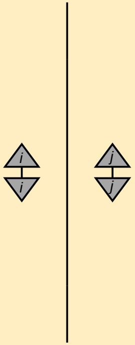
$=$



Proof.



Proof.

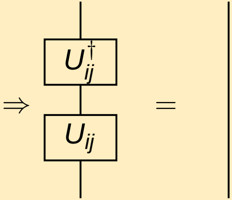
$=$ 

Proof.

$=$

Main Theorem
Unitarity

Proof.



Now we prove that the U_{ij} are an orthogonal basis.

Now we prove that the U_{ij} are an orthogonal basis.

Proof.

Need to show that for all i, j: $\mathrm{Tr}(U_{pq}^{\dagger} \circ U_{ij}) = \delta_{ip}\delta_{jq}n$.

Now we prove that the U_{ij} are an orthogonal basis.

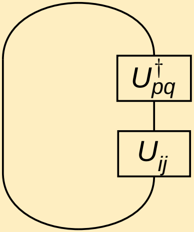
Proof.

Need to show that for all i, j: $\mathrm{Tr}(U_{pq}^{\dagger} \circ U_{ij}) = \delta_{ip}\delta_{jq}n$. Using tensor diagrams this becomes:

Now we prove that the U_{ij} are an orthogonal basis.

Proof.

Need to show that for all i, j: $\mathrm{Tr}(U_{pq}^{\dagger} \circ U_{ij}) = \delta_{ip}\delta_{jq}n$. Using tensor diagrams this becomes:

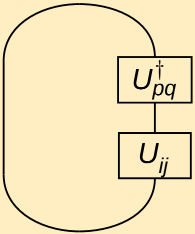


$$= \delta_{ip}\delta_{jq}n$$

Now we prove that the U_{ij} are an orthogonal basis.

Proof.

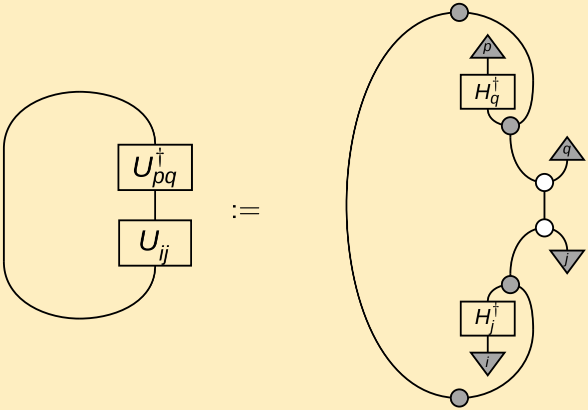
Or disregarding normalization:



$$= \delta_{ip}\delta_{jq}$$

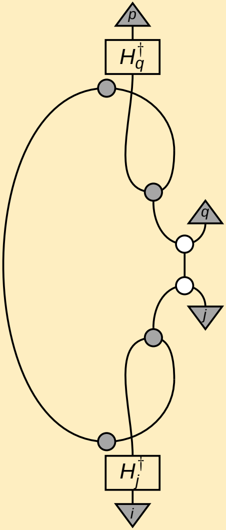
Proof.

By definition:



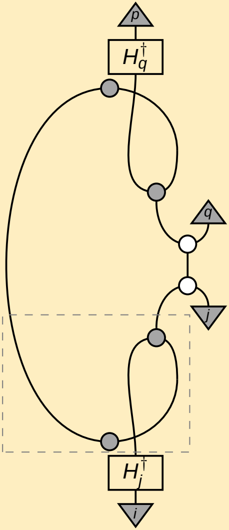
Proof.

$=$



Proof.

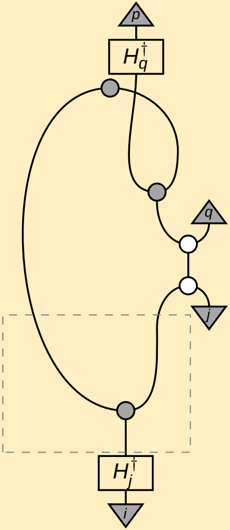
$=$



Proof.

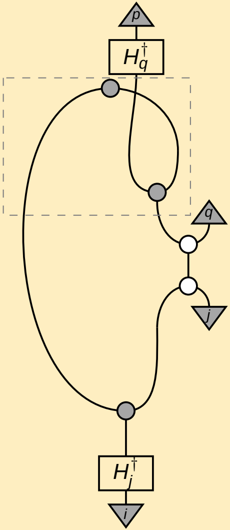
By spider merge

$=$



Proof.

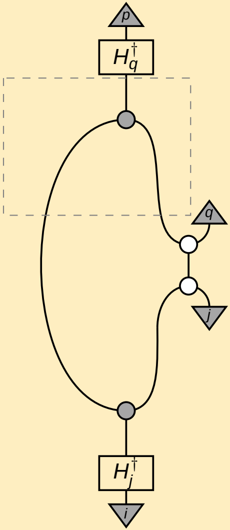
$=$



Proof.

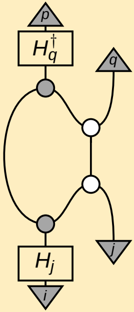
By spider merge

$=$



Proof.

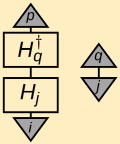
$=$



Main Theorem
Orthogonality

Proof.

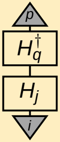
$$=$$



Main Theorem
Orthogonality

Proof.

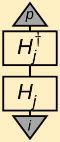
$=$



δ_{jq}

Proof.

$=$



δ_{jq}

Proof.

$=$ 

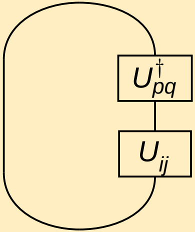
δ_{jq}

Proof.

$$= \delta_{ip}\delta_{jq}$$

Proof.

$\Rightarrow$



$= \delta_{ip}\delta_{jq}$

$\square$