Orthogonal Quantum Latin Squares

and Mutually Unbiased Bases

Ben Musto

Department of Computer Science
University of Oxford

9 June 2016

Latin square

Definition

A *Latin square of order n* is an n-by-n array of computational basis vectors of $\mathbb{C}^n$ such that every row and column is an orthonormal basis.

Latin square

Definition

A *Latin square of order n* is an n-by-n array of computational basis vectors of $\mathbb{C}^n$ such that every row and column is an orthonormal basis.

For example:

$\lvert 0\rangle$	$\lvert 1\rangle$	$\lvert 2\rangle$	$\lvert 3\rangle$
$\lvert 1\rangle$	$\lvert 0\rangle$	$\lvert 3\rangle$	$\lvert 2\rangle$
$\lvert 2\rangle$	$\lvert 3\rangle$	$\lvert 0\rangle$	$\lvert 1\rangle$
$\lvert 3\rangle$	$\lvert 2\rangle$	$\lvert 1\rangle$	$\lvert 0\rangle$

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.

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:

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

Orthogonal quantum Latin squares

Definition

A pair of quantum Latin squares are orthogonal when the pointwise inner product of any row from one with any row from the other yielding a single 1 and with the rest being 0.

Orthogonal quantum Latin squares

Definition

A pair of quantum Latin squares are orthogonal when the pointwise inner product of any row from one with any row from the other yielding a single 1 and with the rest being 0.

For example:

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

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

MUBs from orthogonal quantum Latin squares

Let $\mathcal{P} :=$ , $\mathcal{Q} :=$  be a pair of orthogonal quantum Latin squares,  be the computational basis spider and H_j and G_q be indexed families of Hadamard matrices.

MUBs from orthogonal quantum Latin squares

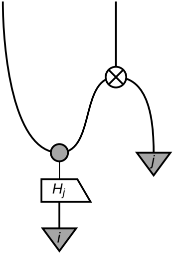
Let $\mathcal{P} :=$ , $\mathcal{Q} :=$  be a pair of orthogonal quantum Latin squares,  be the computational basis spider and H_j and G_q be indexed families of Hadamard matrices.

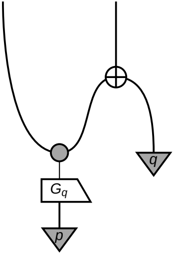
Then A_{ij} and B_{pq} as defined below are mutually unbiased.

MUBs from orthogonal quantum Latin squares

Let $\mathcal{P} :=$ , $\mathcal{Q} :=$  be a pair of orthogonal quantum Latin squares,  be the computational basis spider and H_j and G_q be indexed families of Hadamard matrices.

Then A_{ij} and B_{pq} as defined below are mutually unbiased.

$A_{ij} := \frac{1}{\sqrt{n}}$ 

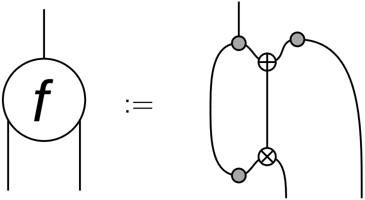
$B_{pq} := \frac{1}{\sqrt{n}}$ 

Proof

The condition that  and  are orthogonal is equivalent to the following linear map being a function on the computational basis states:

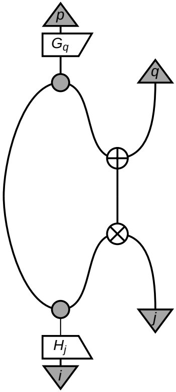
Proof

The condition that  and  are orthogonal is equivalent to the following linear map being a function on the computational basis states:



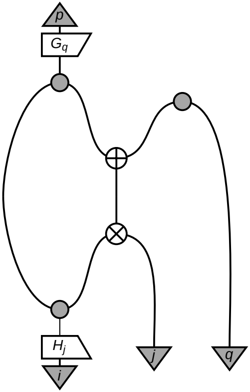
Proof

$$|\langle B_{pq}|A_{ij}\rangle|^2 \quad = \quad \left| \frac{1}{n} \quad \cdots \quad \right|^2$$

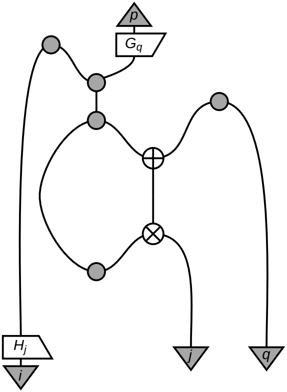


Proof

$$= \frac{1}{n^2} \left| \quad \right|^2$$

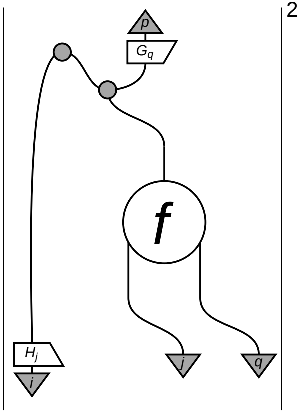


Proof

$$= \frac{1}{n^2} \left| \vphantom{\int} \right.$$  $$\left. \vphantom{\int} \right|^2$$

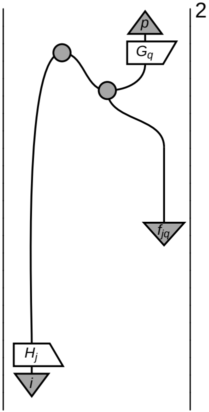
Proof

$$= \frac{1}{n^2}$$



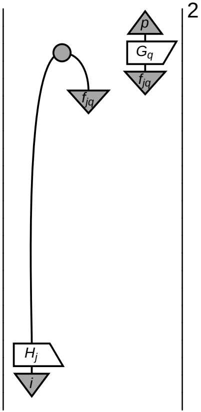
Proof

$$= \frac{1}{n^2}$$

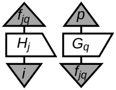


Proof

$$= \frac{1}{n^2}$$

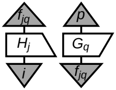


Proof

$= \frac{1}{n^2} \Bigg|$  $\Bigg|^2$

□

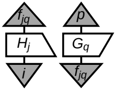
Proof

$$= \frac{1}{n^2} \left| \right.$$  $$\left. \right|^2$$

$$= \frac{1}{n^2} \left| (H_j)_{it} (G_q^\dagger)_{tp} \right|^2$$

$\square$

Proof

$$= \frac{1}{n^2} \left| \right.$$  $$\left. \right|^2$$

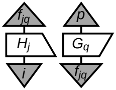
$$= \frac{1}{n^2} |(H_j)_{it}(G_q^\dagger)_{tp}|^2$$

$$= \frac{1}{n^2} 1^2$$

$\square$

Proof

$$= \frac{1}{n^2} \left| \right.$$



$$\left. \right|^2$$

$$= \frac{1}{n^2} |(H_j)_{it} (G_q^\dagger)_{tp}|^2$$

$$= \frac{1}{n^2} 1^2$$

$$= \frac{1}{n^2}$$

□