Orthogonal Quantum Latin Squares and Mutually Unbiased Bases

Ben Musto

Department of Computer Science
University of Oxford

9 June 2016
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.
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:

\[
\begin{array}{cccc}
|0\rangle & |1\rangle & |2\rangle & |3\rangle \\
|1\rangle & |0\rangle & |3\rangle & |2\rangle \\
|2\rangle & |3\rangle & |0\rangle & |1\rangle \\
|3\rangle & |2\rangle & |1\rangle & |0\rangle \\
\end{array}
\]
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:

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

\[
\begin{array}{cccc}
|0\rangle & |1\rangle & |2\rangle & |3\rangle \\
|1\rangle & |0\rangle & |3\rangle & |2\rangle \\
|2\rangle & |3\rangle & |0\rangle & |1\rangle \\
|3\rangle & |2\rangle & |1\rangle & |0\rangle \\
\end{array}
\]

\[
\begin{array}{cccc}
|0\rangle & |2\rangle & |3\rangle & |1\rangle \\
|1\rangle & |3\rangle & |2\rangle & |0\rangle \\
|2\rangle & |0\rangle & |1\rangle & |3\rangle \\
|3\rangle & |1\rangle & |0\rangle & |2\rangle \\
\end{array}
\]
Let $\mathcal{P} := \mathcal{P}$, $\mathcal{Q} := \mathcal{Q}$ be a pair of orthogonal quantum Latin squares, $\mathcal{Q}$ be the computational basis spider and $H_j$ and $G_q$ be indexed families of Hadamard matrices.
Let $\mathcal{P} := \begin{array}{c}
\end{array}$, $\mathcal{Q} := \begin{array}{c}
\end{array}$ be a pair of orthogonal quantum Latin squares, $\otimes$ 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.
Let $\mathcal{P} := \bigotimes_i$, $\mathcal{Q} := \bigotimes_j$ be a pair of orthogonal quantum Latin squares, $\mathcal{X}$ 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.

\[ A_{ij} := \frac{1}{\sqrt{n}} \]

\[ B_{pq} := \frac{1}{\sqrt{n}} \]
The condition that $\uparrow$ and $\downarrow$ are orthogonal is equivalent to the following linear map being a function on the computational basis states:
The condition that $\otimes$ and $\otimes$ are orthogonal is equivalent to the following linear map being a function on the computational basis states:
Proof

\[ |\langle B_{pq} | A_{ij} \rangle|^2 = \frac{1}{n} \]
Proof

\[
\frac{1}{n^2}
\]
\[ \frac{1}{n^2} \]
Proof

\[
\frac{1}{n^2}
\]
Proof

\[
\frac{1}{n^2}
\]
Proof

\[ \frac{1}{n^2} \]
\[ \frac{1}{n^2} \begin{vmatrix} H_j & G_q \\ i & i_{jq} \end{vmatrix}^2 \]
Proof

\[
= \frac{1}{n^2} \left| \frac{\Gamma_{jq}^{i} \Gamma_{jq}^{p}}{\Gamma_{ij}^{q} \Gamma_{i}^{q}} \right|^2

= \frac{1}{n^2} \left| (H_j)_{it} (G_q^\dagger)_{tp} \right|^2
\]
\[
\begin{align*}
&= \frac{1}{n^2} \left| \begin{array}{c}
\begin{array}{c}
\text{up triangle}\n\text{middle triangle}
\end{array}
\end{array} \right|^2 \\
&= \frac{1}{n^2} \left| (H_j)_{it} (G_q^\dagger)_{tp} \right|^2 \\
&= \frac{1}{n^2} \cdot 1^2
\end{align*}
\]
Proof

\[ \frac{1}{n^2} \left| \begin{array}{c}
\text{\includegraphics[width=2cm]{H_j}} \\
\text{\includegraphics[width=2cm]{G_q}} \\
\text{\includegraphics[width=2cm]{t_i_q}} \\
\text{\includegraphics[width=2cm]{t_p}} \\
\end{array} \right|^2 \\
= \frac{1}{n^2} \left| (H_{j})_{it} (G_{q}^\dagger)_{tp} \right|^2 \\
= \frac{1}{n^2} \left( \frac{1}{n^2} \right)^2 \\
= \frac{1}{n^2} \\
= \frac{1}{n^2} \]