

Quantum Latin squares and unitary error bases

Benjamin Musto

Department of Computer Science, University of Oxford
benjamin.musto@cs.ox.ac.uk

Jamie Vicary

Department of Computer Science, University of Oxford
jamie.vicary@cs.ox.ac.uk

We introduce quantum Latin squares, combinatorial quantum objects which generalize classical Latin squares. We show that quantum Latin squares can be seen as weakened versions of mutually-unbiased bases (MUBs). Our main results use quantum Latin squares to give a new construction of unitary error bases (UEBs), basic structures in quantum information which lie at the heart of procedures such as teleportation, dense coding and error correction.

This is an extended abstract for arXiv:1504.02715

1 Quantum Latin squares

We begin with the definition of a quantum Latin square.

Definition 1. A *quantum Latin square of order n* is an n -by- n array of elements of the Hilbert space \mathbb{C}^n , such that every row and every column is an orthonormal basis.

Example 2. Here is a quantum Latin square given in terms of the computational basis elements $\{|0\rangle, |1\rangle, |2\rangle, |3\rangle\} \subset \mathbb{C}^4$:

$ 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$

It can readily be checked that along each row, and along each column, the elements form an orthonormal basis for \mathbb{C}^4 . We can compare this to the classical notion of Latin square [6].

Definition 3. A *classical Latin square of order n* is an n -by- n array of integers in the range $\{0, \dots, n-1\}$, such that every row and column contains each number exactly once.

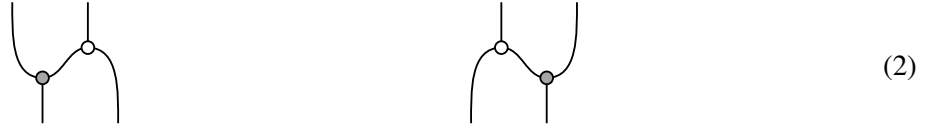
By interpreting a number $k \in \{0, \dots, n-1\}$ as a computational basis element $|k\rangle \in \mathbb{C}^n$, we can turn an array of numbers into an array of Hilbert space elements:

3	1	0	2	\rightsquigarrow	$ 3\rangle$	$ 1\rangle$	$ 0\rangle$	$ 2\rangle$	(1)
1	0	2	3		$ 1\rangle$	$ 0\rangle$	$ 2\rangle$	$ 3\rangle$	
2	3	1	0		$ 2\rangle$	$ 3\rangle$	$ 1\rangle$	$ 0\rangle$	
0	2	3	1		$ 0\rangle$	$ 2\rangle$	$ 3\rangle$	$ 1\rangle$	

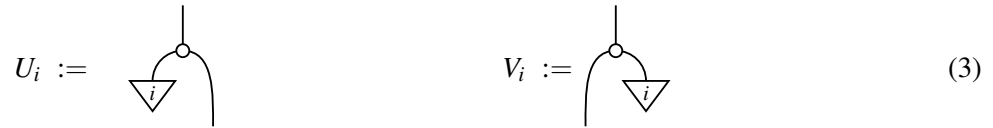
It is easy to see that the original array of numbers is a classical Latin square if and only if the corresponding grid of Hilbert space elements is a quantum Latin square. However, as Example 2 makes clear, not every quantum Latin square is of this form.

Quantum Latin squares have an elegant description in terms of *categorical quantum mechanics* [1, 2, 5, 11], a research programme in which techniques of monoidal category theory are used to understand quantum computational phenomena. For this theorem, note that an n -by- n grid of elements of \mathbb{C}^n corresponds exactly to a linear map $\mathbb{C}^n \otimes \mathbb{C}^n \rightarrow \mathbb{C}^n$, which acts on $|i\rangle \otimes |j\rangle$ to give the grid element in the i th row and j th column. This theorem will be included in a future version of our main paper.

Theorem 4. *In \mathbf{FHilb} , a linear map $\rho_{\blacktriangleright} : \mathbb{C}^n \otimes \mathbb{C}^n \rightarrow \mathbb{C}^n$ gives a quantum Latin square just when the following morphisms are both unitary, where the black vertex is the canonical classical structure on \mathbb{C}^n :*



Proof sketch. By expanding the black vertex as a sum over its classical points, we see these composites are unitary just when the following morphisms are unitary for all i indexing the computational basis states:



Encode the map $\rho_{\blacktriangleright}$ as an n -by- n grid of elements of \mathbb{C}^n . Then the i th row of this grid gives the columns of U_i , and the i th column of this grid gives the columns of V_i . So then the matrices U_i and V_i will be unitary just when the rows and columns of the grid form orthonormal bases, which is precisely the quantum Latin square condition. \square

Note that we do not require the white vertex to satisfy any additional axioms; in particular, it is not necessarily an algebra. In [14], it was shown that the basis defined by two commutative dagger-Frobenius structures in \mathbf{FHilb} are mutually unbiased precisely when the composites (2) are unitary, up to a scalar factor. Hence we see that quantum Latin squares are a *weak* form of unbiased basis.

2 Outline of main results

The main results of our paper are on using quantum Latin squares to construct *unitary error bases* (UEBs) [9], also known as unitary operator bases. These are basic structures in quantum information which play a central role in quantum teleportation [4], dense coding [8] and error correction [12]. Construction techniques for UEBs have been widely studied [7, 9, 10, 13]. We propose a new method for construction of UEBs:

- Quantum shift-and-multiply method (**QSM**). Requires a quantum Latin square and a family of Hadamard matrices.¹ (See paper Definition 17.)

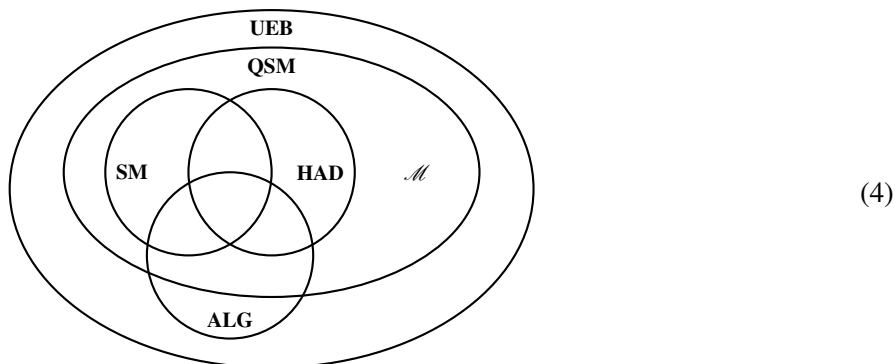
We compare this to the other methods that have been proposed in the literature:

- Shift-and-multiply method (**SM**). Requires a classical Latin square and a family of Hadamard matrices. (See paper Definition 20.)
- Hadamard method (**HAD**). Requires a pair of MUBs. (See paper Definition 32.)

¹A *Hadamard matrix* is a unitary matrix whose entries have constant norm. It is mathematically equivalent to the data for a pair of MUBs.

- Algebraic method (**ALG**). Requires a finite group equipped with a projective representation, satisfying certain properties. (See paper Definition 41.)

Our theorems concern the relationships between these constructions. We prove that **QSM** contains **SM** and **HAD** as special cases. We also use **QSM** to construct a concrete unitary error basis \mathcal{M} , and prove that it is not equivalent to one arising from **SM**, **HAD** or **ALG**. The relationships between these constructions, up to a standard notion of equivalence of UEBs, are indicated by the following Venn diagram:



Our work strongly extends previous results, in an area that has not seen progress since 2003 [9]. But there is much still to be settled: in particular, we do not know whether **ALG** is a subset of **QSM**, or whether **QSM** equals **UEB**.

There are interesting connections between MUBs, unitary error bases and quantum Latin squares. Our main result is that UEBs can be built from quantum Latin squares. We noted above that quantum Latin squares are weak forms of MUBs. Also, it has been shown MUBs can be extracted from a UEB [3]. So quantum Latin squares arise from MUBs, which arise from UEBs, which arise from quantum Latin squares; an interesting tapestry of results for which we currently lack a good intuition.

Acknowledgements. The authors are grateful to Dominic Verdon for useful discussions, and to the EPSRC for financial support.

References

- [1] Samson Abramsky and Bob Coecke. A categorical semantics of quantum protocols. In *Proceedings of the 19th Annual IEEE Symposium on Logic in Computer Science*, pages 415–425. IEEE, 2004. arXiv:quant-ph/0402130. doi:10.1109/LICS.2004.1319636.
- [2] Samson Abramsky and Bob Coecke. Categorical quantum mechanics. *Handbook of quantum logic and quantum structures: quantum logic*, pages 261–324, 2008.
- [3] Somshubhro Bandyopadhyay, Oscar P. Boykin, Vwani Roychowdhury, and Farrokh Vatan. A new proof for the existence of mutually unbiased bases. *Algorithmica*, 34(4):512–528, 2002. arXiv:quant-ph/0103162. doi:10.1007/s00453-002-0980-7.
- [4] Charles H Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70(13):1895, 1993. doi:10.1103/PhysRevLett.70.1895.
- [5] Bob Coecke and Aleks Kissinger. Quantum computer science, lecture notes, 2013.
- [6] Ronald Aylmer Fisher and Frank Yates. The 6×6 Latin squares. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 30.04, pages 492–507. Cambridge Univ Press, 1934. doi:10.1017/s0305004100012731.

- [7] Sibasish Ghosh and Ajit Iqbal Singh. Invariants for maximally entangled vectors and unitary bases. arXiv:1401.0099, 2014.
- [8] Mile Gu, Helen M Chrzanowski, Syed M Assad, Thomas Symul, Kavan Modi, Timothy C Ralph, Vlatko Vedral, and Ping Koy Lam. Observing the operational significance of discord consumption. *Nature Physics*, 8(9):671–675, 2012. arXiv:1203.0011. doi:10.1038/NPHYS2376.
- [9] Andreas Klappenecker and Martin Rötteler. Unitary error bases: Constructions, equivalence, and applications. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, pages 139–149. Springer, 2003. doi:10.1007/3-540-44828-4_16.
- [10] Emanuel Knill. Group representations, error bases and quantum codes. Technical Report LAUR-96-2807, LANL, 1996. arXiv:quant-ph/9608049. doi:10.2172/373768.
- [11] Benjamin Musto. Exploring quantum teleportation through unitary error bases. Master’s thesis, Department of Computer Science, University of Oxford, 2014. Download.
- [12] Peter Shor. Fault-tolerant quantum computation. In *Proceedings of 37th Symposium on Foundations of Computing*, pages 56–65. IEEE Computer Society Press, 1996. arXiv:quant-ph/9605011. doi:10.1007/978-0-387-30162-4_143.
- [13] Reinhard Werner. All teleportation and dense coding schemes. *Journal of Physics A: Mathematical and General*, 34(35):7081, 2001. arXiv:quant-ph/0003070. doi:10.1088/0305-4470/34/35/332.
- [14] Will Zeng and Jamie Vicary. Abstract structure of unitary oracles for quantum algorithms. In *Proceedings of QPL 2014*. arXiv:1406.1278.