Biunitary constructions in quantum information

David Reutter
Department of Computer Science
University of Oxford
david.reutter@cs.ox.ac.uk

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

September 27, 2016

Abstract

We present an infinite number of constructions involving unitary error bases, Hadamard matrices, quantum Latin squares and controlled families, many of which have not previously been described. Our results rely on biunitary connections, algebraic objects which play a central role in the theory of planar algebras. They have an attractive graphical calculus which allows simple correctness proofs for the constructions we present. We apply these techniques to construct a unitary error basis that cannot be built using any previously known method.

This is an extended abstract for arXiv:1609.07775

Biunitaries. *Biunitary connections* (or simply *biunitaries*) have been widely studied by Jones and others [7, 8, 14, 17] as a central tool in the classification of subfactors, part of the theory of von Neumann algebras. They have an attractive graphical calculus, usually expressed in the language of *planar algebras*, which describes the linear representation theory of algebraic structures in the plane. In this calculus, a biunitary can be presented informally as a planar algebra element U with two inputs and two outputs, which is *vertically unitary* (1), and which is *horizontally unitary* up to a scalar factor λ (2):

(1)

(2)

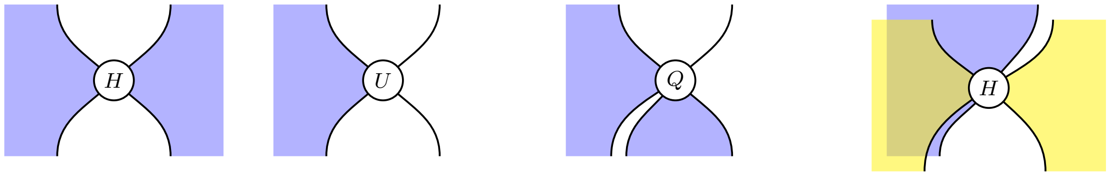
In this paper, diagrams of this sort denote linear algebraic data, in a simple way. Regions are labelled with finite indexing sets, with blank regions corresponding to the trivial indexing set. Wires and vertices correspond to families of Hilbert spaces or linear maps, respectively, indexed by the parameters of regions adjacent to the wire or vertex. In concrete terms, a biunitary therefore simply corresponds to a family of linear maps satisfying some algebraic equations.

Characterizing quantum structures. It has been shown by Jones [7] that Hadamard matrices[1] can be exactly characterized in terms of biunitaries of the form given in Figure 1(a). The second author has shown [25, 26] that unitary error bases[2] can be characterized similarly, in terms of biunitaries of the form given in Figure 1(b). In this paper we show that a similar approach can be used to characterize quantum Latin squares[3], as biunitaries of the form

[1] A *Hadamard matrix* is a square complex matrix with all entries of modulus 1, which is proportional to a unitary matrix.

[2] A *unitary error basis* is a basis of unitary operators on a finite-dimensional Hilbert space, orthogonal with respect to the trace inner product.

[3] A *quantum Latin square* [16] is a square grid of vectors in a finite-dimensional Hilbert space, such that every row and every column is an orthonormal basis.



(a) Hadamard matrix (Had) (b) Unitary error basis (UEB) (c) Quantum Latin square (QLS) (d) Controlled family of Hadamards (Had*)

Figure 1: Biunitary characterizations of quantum structures.

illustrated in Figure 1(c). We also show that controlled families of biunitaries can be described by attaching additional regions in certain ways; we illustrate one example in Figure 1(d), a controlled family of Hadamard matrices. These images are 3-dimensional; for example, in the last image, the blue sheet lies beneath the yellow sheet. The colours do not convey mathematical information, but rather make the geometry easier to understand. Rotations by a quarter-turn, and reflections about the horizontal or vertical axes, preserve the given interpretations of the pictures in terms of quantum structures.

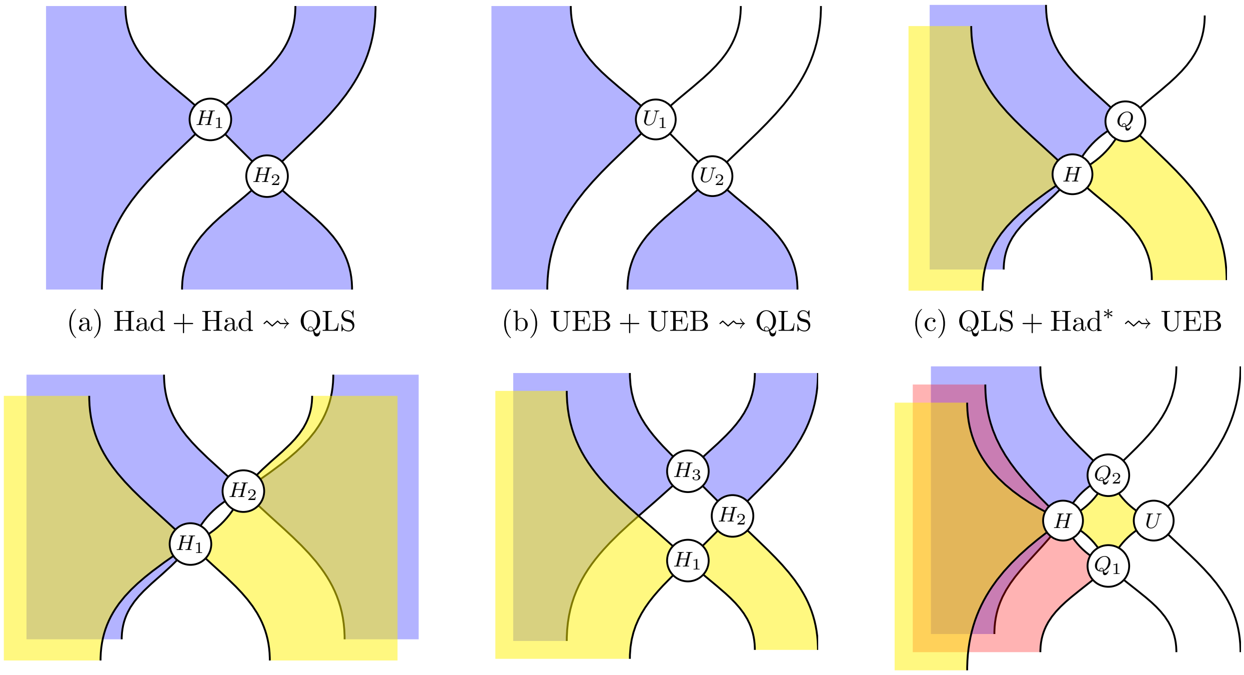
Composing biunitaries. Our main results are based on the simple fact that the *diagonal* composite of two biunitaries is again biunitary. Given the description of quantum structures in terms of biunitaries as summarized above, one can immediately write down a large number of schemes for the construction of certain quantum structures from others, many of which are not previously known. We give some examples in Figure 2 (only a subset of the constructions we consider in the full paper), which we briefly explore here. Note that the biunitaries are connected diagonally in each case, as required.

- Figure 2(a). Two Hadamards give a quantum Latin square, generalizing a known construction [16] in which one Hadamard gives a quantum Latin square.
- Figure 2(b). Two unitary error bases give a quantum Latin square, a new construction.
- Figure 2(c). A controlled family of Hadamards and a quantum Latin square give a unitary error basis, recovering the quantum shift-and-multiply construction [16] which generalizes Werner's shift-and-multiply construction [27].
- Figure 2(d). Two controlled families of Hadamards give a single Hadamard, recovering a construction of Hosoya and Suzuki [6] which generalizes a construction of Diţă [3].
- Figure 2(e). Three Hadamards give a unitary error basis, generalizing a known construction [16] in which one Hadamard gives a unitary error basis.
- Figure 2(f). A double-controlled family of Hadamards (H), two quantum Latin squares (Q_1, Q_2) and a unitary error basis (U) give a unitary error basis, a new construction.

Correctness of these constructions follows immediately from diagonality of the composition; no further details need to be checked. Our approach therefore offers advantages even for those constructions that are already known, since the traditional proofs of correctness are nontrivial.

Of course, these constructions can be iterated; for example, the schemes of Figure 2(a) and Figure 2(c) give a way to combine two Hadamards and a further list of Hadamards to produce a unitary error basis (and in fact Figure 2(e) is the special case when this list is of length one).

Further results. In the main paper, we further show that an infinite number of independent constructions of the sort shown in Figure 2 can be obtained. We use construction Figure 2(f) to produce an explicit unitary error basis on an 8-dimensional Hilbert space which we prove cannot be obtained from any previously-known construction method, yielding a proof of principle that our biunitary methods give rise to genuinely new concrete structures.



(a) Had + Had ⇝ QLS (b) UEB + UEB ⇝ QLS (c) QLS + Had* ⇝ UEB

(d) Had* + Had* ⇝ Had (e) Had + Had + Had ⇝ UEB (f) Had** + QLS + QLS + UEB ⇝ UEB

Figure 2: A variety of biunitary constructions of quantum structures.

Importance and relevance. Hadamard matrices and unitary error bases provide the mathematical foundation for a variety of quantum informatic phenomena, amongst them the study of mutually unbiased bases, quantum key distribution, quantum teleportation, dense coding and quantum error correction [4, 9, 11, 21, 27]. Nevertheless their general structure is notoriously difficult to understand; in dimension n, Hadamard matrices have only been classified up to $n = 5$ [22, 24], and the general structure of unitary error bases is virtually unknown for $n > 2$. Quantum Latin squares have been introduced much more recently [1, 15, 16], generalizing classical Latin squares which have a wide range of applications in classical and quantum information [2, 13, 20].

By unifying these quantum structures as special cases of the single notion of biunitary, and providing simple graphical tools to understand the intricate interplay between them, we unify several already-known and seemingly-unrelated constructions [1, 3, 6, 16, 27], uncover an infinite number of new constructions, and produce novel, concrete examples. These new tools may lead to further progress in questions of classification and applications of Hadamard matrices, unitary error bases and quantum Latin squares.

On the other hand, biunitaries are central tools in the study and classification of subfactors [7, 8, 14, 17, 19], a highly significant activity in the theory of von Neumann algebras. We hope that our work leads to the development of further connections between subfactor theory and quantum information theory.

Criticisms. There are many constructions of quantum structures which we cannot capture using our biunitary techniques. For unitary error bases, there is the nice error basis construction of Knill [10]. For Hadamard matrices, an analogue of Knill's construction are the Fourier matrices arising from finite abelian groups. Other examples include Petrescu's construction of continuous families of Hadamard matrices in prime dimension [18], Wocjan's and Beth's construction [28] and its generalization by Musto [15], or several other less-general constructions which only work in specific dimensions [5, 12, 22, 23]. In all of these cases, the methods are not purely compositional; they make use of some additional group-theoretic or algebraic structure which is out of reach of the biunitary approach.

References

[1] Teodor Banica and Remus Nicoară. Quantum groups and Hadamard matrices. *Panamer. Math. J.*, 17:1–24, 2007. `arXiv:math/0610529`.

[2] Tristan Benoist and Ion Nechita. On bipartite unitary matrices generating subalgebra-preserving quantum operations. 2016. `arXiv:1608.05811`.

[3] Petre Diţă. Some results on the parametrization of complex Hadamard matrices. *J. Phys. A: Math. Gen.*, 37(20):5355–5374, 2004. `doi:10.1088/0305-4470/37/20/008`.

[4] Thomas Durt, Berthold-Georg Englert, Ingemar Bengtsson, and Karol Życzkowski. On mutually unbiased bases. *International Journal of Quantum Information*, 08(04):535–640, 2010. `arXiv:1004.3348`, `doi:10.1142/s0219749910006502`.

[5] Uffe Haagerup. Orthogonal maximal abelian *-subalgebras of the n× n matrices and cyclic n-roots. *Institut for Matematik, U. of Southern Denmark*, 29:296–322, 1996.

[6] Rie Hosoya and Hiroshi Suzuki. Type II matrices and their Bose-Mesner algebras. *Journal of Algebraic Combinatorics*, 17(1):19–37, 2003. `doi:10.1023/a:1021960623533`.

[7] Vaughan F. R. Jones. Planar algebras, I. 1999. `arXiv:math/9909027`.

[8] Vaughan F. R. Jones, Scott Morrison, and Noah Snyder. The classification of subfactors of index at most 5. *Bull. Amer. Math. Soc.*, 51(2):277–327, 2013. `arXiv:1304.6141`, `doi:10.1090/s0273-0979-2013-01442-3`.

[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. *Los Alamos National Laboratory Report LAUR-96-2807*, 1996. `arXiv:quant-ph/9608049`, `doi:10.2172/378680`.

[11] Emanuel Knill. Non-binary unitary error bases and quantum codes. *Los Alamos National Laboratory Report LAUR-96-2717*, 1996. `arXiv:quant-ph/9608048`, `doi:10.2172/373768`.

[12] Máté Matolcsi, Júlia Réffy, and Ferenc Szöllősi. Constructions of complex Hadamard matrices via tiling abelian groups. *Open Syst. Inf. Dyn.*, 14(03):247–263, 2007. `arXiv:quant-ph/0607073`, `doi:10.1007/s11080-007-9050-6`.

[13] David A. Meyer and Thomas G. Wong. Connectivity is a poor indicator of fast quantum search. *Phys. Rev. Lett.*, 114(11), 2015. `arXiv:1409.5876`, `doi:10.1103/physrevlett.114.110503`.

[14] Scott Morrison and Emily Peters. The little desert? Some subfactors with index in the interval $(5, 3+\sqrt{5})$. *International Journal of Mathematics*, 25(08):1450080, 2014. `arXiv:1205.2742`, `doi:10.1142/s0129167x14500803`.

[15] Benjamin Musto. Constructing mutually unbiased bases from quantum Latin squares. 2016. `arXiv:1605.08919`.

[16] Benjamin Musto and Jamie Vicary. Quantum Latin squares and unitary error bases. *Quantum Information and Computation*, 2016. to appear. `arXiv:1504.02715`.

[17] Adrian Ocneanu. Quantized groups, string algebras, and Galois theory for algebras. In David E. Evans and Masamichi Takesaki, editors, *Operator Algebras and Applications*, pages 119–172. Cambridge University Press (CUP), 1989. doi:10.1017/cbo9780511662287.008.

[18] Mihai Petrescu. *Existence of Continuous Families of Complex Hadamard Matrices of Certain Prime Dimensions and Related Results.* PhD thesis, University of California, Los Angeles, 1997.

[19] Sorin Popa. Orthogonal pairs of *-subalgebras in finite von Neumann algebras. *J. Operator Theory*, 9(2):253–268, 1983.

[20] Claude E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4):656–715, 1949. doi:10.1002/j.1538-7305.1949.tb00928.x.

[21] Peter W. Shor. Fault-tolerant quantum computation. In *Proceedings of 37th Conference on Foundations of Computer Science*, pages 56–65. IEEE Computer Society Press, 1996. arXiv:quant-ph/9605011, doi:10.1109/sfcs.1996.548464.

[22] Ferenc Szöllősi. *Construction, classification and parametrization of complex Hadamard matrices.* PhD thesis, Central European University, Budapest, Hungary, 2011. arXiv:1110.5590.

[23] Ferenc Szöllősi. Complex Hadamard matrices of order 6: a four-parameter family. *Journal of the London Mathematical Society*, 85(3):616–632, 2012. arXiv:1008.0632, doi:10.1112/jlms/jdr052.

[24] Wojciech Tadej and Karol Życzkowski. A concise guide to complex Hadamard matrices. *Open Syst. Inf. Dyn.*, 13(02):133–177, 2006. arXiv:quant-ph/0512154, doi:10.1007/s11080-006-8220-2.

[25] Jamie Vicary. Higher quantum theory. 2012. arXiv:1207.4563.

[26] Jamie Vicary. Higher semantics of quantum protocols. In *2012 27th Annual IEEE Symposium on Logic in Computer Science*. Institute of Electrical & Electronics Engineers (IEEE), 2012. doi:10.1109/lics.2012.70.

[27] Reinhard F. Werner. All teleportation and dense coding schemes. *J. Phys. A: Math. Gen.*, 34(35):7081–7094, 2001. doi:10.1088/0305-4470/34/35/332.

[28] Pawel Wocjan and Thomas Beth. New construction of mutually unbiased bases in square dimension. 2004. arXiv:quant-ph/0407081.