

Exploring a Quantum Theory with Graph Rewriting and Computer Algebra

Aleks Kissinger

Oxford University Computing Laboratory

Abstract. Graphical languages provide a powerful tool for describing the behaviour of quantum systems. While the use of graphs vastly reduces the complexity of many calculations [4,10], manual graphical manipulation quickly becomes untenable for large graphs or large numbers of graphs. To combat this issue, we are developing a tool called Quantomatic, which allows automated and semi-automated explorations of graph rewrite systems and their underlying semantics.

We emphasise in this paper the features of Quantomatic that interact with a computer algebra system to discover graphical relationships via the unification of matrix equations. Since these equations can grow exponentially with the size of the graph, we use this method to discover small identities and use those identities as graph rewrites to expand the theory.

1 Introduction

Quantomatic is a tool designed to use automated graph rewriting techniques in conjunction with a computer algebra system to expand and enrich graphical theories. The primary contribution of this paper is an exposition of the methods, features and limitations of this tool, as well as a detailed look at its application to a real problem.

Quantomatic was created to explore the theory of complementary classical structures (CCS), which witness in an abstract sense the interaction of non-commuting observables in quantum states and protocols [6]. The theory of CCS is primarily expressed in the language of monoidal categories and builds upon a large body of work concerned with formalising quantum information within category theory (see for example [1,5,17,18,19]). Certain kinds of monoidal categories lend themselves well to graphical representations [12,13], which often provide a simpler and more intuitive interpretation of concepts like entanglement and generalised information flow. In the interest of providing a minimal introduction to the motivating theory for Quantomatic, many of the results from this body of work are given in their concrete form, where the monoidal category is taken to be FdHilb , the category of finite-dimensional Hilbert spaces and linear maps.

In section 2, we provide an explicit construction of classical structures as linear maps and the concrete versions of the related notions of unbiased points, complementarity, and the spider theorem. In section 3 we provide a summarised definition of typed graph rewriting, as defined in [10,14]. We then introduce

a graphical notation for CCS using graphs of red and green dots and give a short exposition the theory in terms of a graph rewrite system. In section 4, we explain in more detail the current and future methods that Quantomatic employs to automatically apply rewrites and to communicate with a computer algebra system to deduce new rules in the theory. In section 5, we shall show these features in action with a simple example in which we use Quantomatic to deduce several new rewrites that better reflect the behaviour of certain entangled states in the graphical theory.

2 Classical Structures

In general, a *classical structure* is any triple $(A, \delta : A \rightarrow A \otimes A, \epsilon : A \rightarrow I)$ in a \dagger -symmetric monoidal category $(\mathcal{C}, \otimes, I, (-)^\dagger)$ that induces a *special commutative Frobenius algebra*. We shall omit the details of this construction here (see for example [6,8]) and proceed immediately to the concrete case, where $\mathcal{C} = \text{FdHilb}$, the category of finite-dimensional Hilbert spaces and linear maps.

In quantum mechanics, vectors in a Hilbert space are called *states*¹ and self-adjoint linear maps are called *observables*. The eigenvectors of an observable have a physical interpretation as classical data. For example, they could represent the possible outcomes of a measurement. For this reason, we call them *classical points*. A property that is unique to classical data (as opposed to quantum data) is that it can be copied and deleted, so we make the following definition.

Definition 1. *For any observable O , we can define a classical structure on its eigenbasis $\{|j\rangle\}_j$ as follows:*

$$\begin{aligned}\delta_O : \mathcal{H} &\rightarrow \mathcal{H} \otimes \mathcal{H} :: |j\rangle \mapsto |jj\rangle \\ \epsilon_O : \mathcal{H} &\rightarrow \mathbb{C} :: |j\rangle \mapsto 1\end{aligned}$$

Let $(-)^\dagger$ be the linear adjoint (conjugate-transpose) of a map. For a classical structure $(\mathcal{H}, \delta_O, \epsilon_O)$, vectors $|\psi\rangle$ induce a map $O_\psi : \mathcal{H} \rightarrow \mathcal{H} := \delta_O^\dagger \circ (1 \otimes |\psi\rangle)$.

Definition 2. *If O_ψ is unitary, we say $|\psi\rangle$ is unbiased with respect to O . If $\delta_O \circ |\psi\rangle = |\psi\rangle \otimes |\psi\rangle$, we say $|\psi\rangle$ is classical with respect to O .*

Proposition 1. *In FdHilb , unbiased points of dimension n with respect to O can be represented as $n - 1$ phase angles.*

For classical structures, we have a result called the “spider theorem.” This theorem exists in various guises in the literature [6,15,17]. Its statement for finite-dimensional Hilbert spaces is as follows.

¹ Throughout this paper, we shall use the terms *vector*, *state*, and *point* interchangeably.

Theorem 1. (*Spider in FdHilb*) For a classical structure $(\mathcal{H}, \delta, \epsilon)$, any map $f : \mathcal{H}^m \rightarrow \mathcal{H}^n$ containing only arbitrary compositions and tensor products of $(\delta, \epsilon, \delta^\dagger, \epsilon^\dagger)$ and swaps $\sigma : |jk\rangle \rightarrow |kj\rangle$ is the following map:

$$f(|\psi\rangle) = \begin{cases} |j\rangle^n & \text{if } |\psi\rangle = |j\rangle^m \text{ for some } |j\rangle \\ 0 & \text{otherwise} \end{cases}$$

The name spider is due to the graphical interpretation of classical structures, which we shall see shortly. In two dimensions, examples of observables are the Pauli X and Z matrices.

$$Z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Let $\{|0\rangle, |1\rangle\}$ be an orthonormal basis of eigenvectors of Z . We fix $\{|+\rangle, |-\rangle\}$ as an eigenbasis with respect to X , where

$$|+\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad \text{and} \quad |-\rangle := \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

For the two-dimensional Hilbert space \mathcal{Q} , we shall define the classical structures $(\mathcal{Q}, \delta_Z, \epsilon_Z)$ and $(\mathcal{Q}, \delta_X, \epsilon_X)$ as above. By proposition 1, we shall represent the unbiased points

$$z_\alpha = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\alpha}|1\rangle)$$

$$x_\beta = \frac{1}{\sqrt{2}}(|+\rangle + e^{i\beta}|-\rangle)$$

and their associated maps Z_α, X_β as above. Note that $X_0 = |0\rangle$, $X_\pi = |1\rangle$, $Z_0 = |+\rangle$, and $Z_\pi = |-\rangle$. This means that X and Z induce *complementary* classical structures.

Definition 3. Two classical structures $A = (\mathcal{H}, \delta_A, \epsilon_A)$ and $B = (\mathcal{H}, \delta_B, \epsilon_B)$ are called *complementary* if the classical points of A are unbiased with respect to B and the classical points of B are unbiased with respect to A .

Complementary classical structures (or CCS) have a rich set of identities, which are most easily explained graphically. To do this, we shall introduce graph rewrite systems.

3 Graph Rewrite Systems

Definition 4. For a partial order (T, \leq) , we define a T -graph as a pair (G, τ_G) , where G is a directed graph and $\tau_G : V_G \rightarrow T$ is called the *typing function* of G .

Definition 5. A T -graph homomorphism $f : G \rightarrow H$ is a graph homomorphism (f_V, f_E) with an additional component $f_T : T \rightarrow T$ that is monotone with respect to \leq and is consistent with the typing functions of G and H , i.e. $f_T \circ \tau_G = \tau_H \circ f_V$.

Remark 1. Defining T -graph isomorphisms in the usual way, we have by anti-symmetry that $f_T = id_T$. Therefore, as in the case of untyped graphs, it is natural to say that isomorphic T -graphs are “essentially” the same.

Remark 2. If we think of the elements of T as formal expressions, then it is useful to think of \leq as a unifiability or pattern-matching condition.

Definition 6. If T has a bottom element \perp , we call this the boundary type. We call vertices of this type boundary vertices and all other vertices internal vertices. We say a T -graph G is well-bounded if each of its boundary vertices is incident to exactly one edge. If the boundary vertex is the source of an edge, it is called an input, and if it is the destination of an edge, it is called an output.

Definition 7. For the set of well-bounded T -graphs \mathcal{G} , a graph rewrite system (GRS) is a set S of triples (L, R, ρ) , where $L, R \in \mathcal{G}$ and ρ is a bijection on the boundary vertices of L and R .

To see how we actually perform rewrites, we need the concept of a matching.

Definition 8. A T -graph homomorphism $f : G \rightarrow H$ is strict on a set of vertices $V' \subseteq V_G$ if for all vertices $v \in V'$ and all edges $e \in H$ that are incident to $f_V(v)$, e is in the image of f_E .

Definition 9. For L, G well-bounded, a T -graph matching $m : L \rightarrow G$ is a T -graph homomorphism such that m_E is injective and m_V is injective and strict on internal vertices.

For a well-bounded T -graph G , a rewrite rule (L, R, ρ) , and a matching $m : L \rightarrow G$ we perform a rewrite by replacing the sub-graph matched by L with R , “gluing” on ρ . For an explicit definition, see [14] or [10]. We let the resultant graph be called $G[(L, R, \rho), m]$ and make the following definition.

Definition 10. For a graph rewrite system (\mathcal{G}, S) , we define the reduction relation \rightarrow_S as follows.

$$G \rightarrow_S H \Leftrightarrow \exists (L, R, \rho) \in S, m : L \rightarrow G. G[(L, R, \rho), m] \cong H$$

It is often useful to describe infinite sets of graph rewrites using pattern graphs.

Definition 11. [10] A pattern graph is a well-bounded T -graph G with a pairwise disjoint family \mathcal{B} of subsets of V_G called !-boxes (bang-boxes). We introduce a refinement order \preceq on pattern graphs. $G \preceq H$ if and only if H can be obtained from G via the following !-box operations.

- copy:** copies a !-box $B \in \mathcal{B}$. For $v \in B$, add a new vertex v' of the same type, as well as a new e' for every edge incident to v' , including those connected to vertices outside of the !-box. Form a new !-box B' of all the new vertices.
- drop:** remove B from \mathcal{B} , leaving the vertices of G intact.

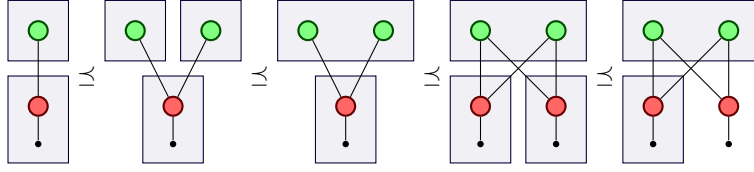


Fig. 1. Operations on !-boxes. Left to right: **copy**, **merge**, **copy**, **drop**.

- kill:** remove all $v \in B$ from G and remove B from \mathcal{B} .
merge: if the vertices of two !-boxes $B_1, B_2 \in \mathcal{B}$ share no edges, merge them into a new !-box $B_1 \cup B_2$.

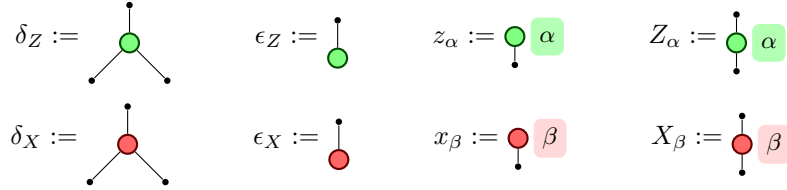
We represent !-boxes graphically by drawing a box around sets of vertices. We can extend this definition to rewrites in the obvious way. For a rewrite (L, R, ρ) , we can associate !-boxes \mathcal{B}_L and \mathcal{B}_R , subject to the following conditions.

- A bijection $\mu : \mathcal{B}_L \rightarrow \mathcal{B}_R$ exists
- For each $B \in \mathcal{B}_L$, the restriction of ρ to B is a bijection from the boundary vertices in B to the boundary vertices in $\mu(B)$.

Let $r = (L, R, \rho, \mathcal{B}_L, \mathcal{B}_R, \mu)$ be a pattern rewrite. For $B \in \mathcal{B}_L$ and some operation **op** from definition 11, obtain a new rewrite r' by applying **op**(B) to L and **op**($\mu(B)$) to R then applying the suitable restriction or extension of ρ . If we define pattern graph homomorphisms as T -graph homomorphisms $f : G \rightarrow H$ such that for each $B \in \mathcal{B}_G$, $f(B) \in \mathcal{B}_H$, we recover a suitable definition of pattern graph matching and rewriting.

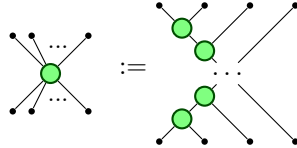
3.1 Classical structures as graph rewrites

We represent classical structures as the following graphs.



Since both δ_Z and δ_X are commutative, we can compose by “gluing” graphs together on the boundary nodes and we can tensor by simple juxtaposition. Taking the adjoint $(-)^{\dagger}$ of a map flips its graph upside-down and reverses the sign of all the phase angles.

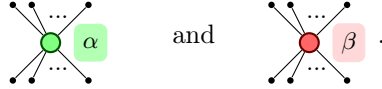
We employ *spiders* as a short-hand for trees of δ_Z .



As such, we have an equivalent statement of the spider theorem.

Theorem 2. (*Spider, graphical*) Any connected graph with m inputs and n outputs whose dots are all a single colour is equivalent to a spider with m inputs and n outputs.

Since unbiased maps commute through dots of the same colour, we often write the sum of all the phases contained in a spider on its vertex. Thus, our most general graph components are



We define the types of these vertices as follows. Let $\mathcal{LR}[F]$ be the set of linear polynomials with rational coefficients on a set of free variables F and a constant π . Then, for $B = \{X, Z\}$, our set of vertex types $T = (B \times \mathcal{LR}[F]) \cup \{\perp\}$. Type subsumption \leq is defined as:

$$(b_1, e_1(\bar{\alpha})) \leq (b_2, e_2(\bar{\beta})) \iff (b_1 = b_2) \wedge (\exists \sigma : F \rightarrow \mathcal{E}[F]. e_1(\sigma(\bar{\alpha})) = e_2(\bar{\beta}))$$

This means one vertex matches another if it is the same colour and there exists a substitution on F such that e_1 can be unified with e_2 . Using this typing, a vertex with m inputs, n outputs, and type (Z, e) has an interpretation as a linear map.

$$\begin{aligned} sp_Z(e, m, n) &:= sp'_Z(n) \circ Z_e \circ sp'_Z(m)^\dagger \\ sp'_Z(0) &:= \epsilon_Z \\ sp'_Z(1) &:= 1 \\ sp'_Z(n) &:= (\delta_Z \otimes 1) \circ sp'_Z(\alpha, n-1) \end{aligned}$$

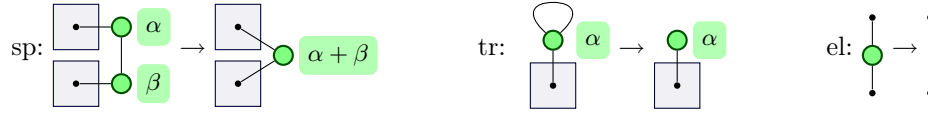
Unrolling the recursion, we get the map:

$$sp_Z(\alpha, m, n) :: \bigotimes_m |0\rangle \mapsto \bigotimes_n |0\rangle, \bigotimes_m |1\rangle \mapsto e^{i\alpha} \bigotimes_n |1\rangle, \text{ other} \mapsto 0$$

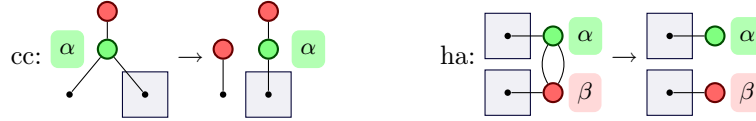
We define sp_X similarly, using δ_X , ϵ_X , and X_e . Note that sp_Z and sp_X both generate matrices that are sparse in their respective bases. This plays a key role in optimising matrix output from a graph.

Remark 3. Map-state duality (see Prop. 4) allows us to interpret arbitrary graphs of classical structures as compositions of matrices. Due to the spider theorem, we can also flip any internal edge in a graph of classical structures without changing the contents of its matrix representation. For details, see [9,8]. In the scope of this paper, we shall use this result to let graphs of classical structures be undirected when it is convenient.

It is useful to think of the spider theorem as a graph identity that lets us merge adjacent vertices of the same colour. By this philosophy, we can express the spider theorem as the following rewrite patterns.



From the complementarity of X and Z , we can derive several other rewrites [6]. In order to avoid expanding spiders, we use versions of these rules that are locally confluent with “sp.” Here are two examples.



4 Quantomatic

Quantomatic² was created to explore theories based on graph rewrite systems. It consists of a core written in ML and a GUI based on a Java graph library called JUNG [16]. We can describe the features of Quantomatic in terms of two operational components: a graphical component that operates on a rewrite theory, and an algebraic component that operates on the semantics of the theory. Using just the graphical component, a theory can be expanded with derived rewrites and completions as follows.

1. A potential LHS is constructed in Quantomatic.
2. Rewrites and converse rewrites are performed to yield a new RHS.
3. The rule “LHS \rightarrow RHS” can be included back into the theory as a derived rewrite if only rewrites were used and as a completion if rewrites and converse rewrites were used.

We can also use the graphical and algebraic components together to systematically develop a theory. In general, this process is as follows.

1. A graphical identity $G(\bar{\alpha}) = H(\bar{\beta})$ is conjectured, where $\bar{\alpha}$ and $\bar{\beta}$ are lists of free variables such as phase angles.
2. G and H are input into Quantomatic and potentially normalised with respect to a reduction strategy.
3. Quantomatic exports the interpretations of G and H as tensor terms (i.e. terms constructed with \otimes and \circ).
4. The CAS is used to search for a substitution $\sigma : \{\bar{\beta}\} \rightarrow \mathcal{LR}[\bar{\alpha}]$ and a scalar λ such that $G(\bar{\alpha}) = \lambda H(\sigma(\bar{\beta}))$.
5. If a substitution is found, a new rewrite $G(\bar{\alpha}) \rightarrow \lambda H(\sigma(\bar{\beta}))$ is incorporated into the theory.

² The Quantomatic source code is currently available for Subversion checkout. See <http://dream.inf.ed.ac.uk/projects/quantomatic> for details.

4.1 Dag-ification and tensor term export

By remark 3, we can choose an any ordering for the edges of a graph G .

Proposition 2. *For an (undirected) graph G , we can always form an equivalent directed acyclic graph G' , called the dag-ification.*

Proof. Remove all self-loops from G with the “tr” rewrite, then define a strict order $<$ on the vertices of G such that any two connected vertices are comparable. Such an order always exists because, for example, a strict linear order on the vertices of G will work. Form G' from G by directing all edges such that $u \rightarrow v$ iff $u < v$.

G' depends heavily on the choice of $<$ and is not unique in general. Once we have dag-ified a graph, we can reconstruct a term using *components*. A component is a triple (i, t, o) , where i and o are lists of edges and t is a tensor term generated by sp_X , sp_Z , 1 , and a tensor permutation function σ , defined as follows for a permutation p :

$$\sigma(p) :: |\psi_1\rangle \otimes |\psi_2\rangle \otimes \dots \otimes |\psi_n\rangle \mapsto |\psi_{p(1)}\rangle \otimes |\psi_{p(2)}\rangle \otimes \dots \otimes |\psi_{p(n)}\rangle$$

σ acts as a generalised swap function. We can recover the “normal” swap function as $\sigma((2\ 1))$. We construct components recursively as follows.

- For a single vertex v of type \perp , let $\llbracket v \rrbracket = ([e], 1, [e])$, where e is the unique edge connected to v . Otherwise, v has type (b, α) with in-edges in_v and out-edges out_v , let $\llbracket v \rrbracket$ be a component $(in_v, sp_b(\alpha, \#in_v, \#out_v), out_v)$.
- For components $c_1 = (i_1, t_1, o_1)$ and $c_2 = (i_2, t_2, o_2)$ that share no edges:

$$c_1 \otimes c_2 = (i_1 \cdot i_2, (t_1 \otimes t_2), o_1 \cdot o_2)$$

- For components c_1 and c_2 where o_1 and i_2 share some edges, we can make c'_1 and c'_2 be such that o'_1 and i'_2 share all edges by padding out c_1 and c_2 with identity components $([e], 1, [e])$. After finding a permutation p such that $p(o'_1) = i'_2$, we form composition as:

$$c_2 \circ c_1 = (i'_1, (t'_2 \circ \sigma(p) \circ t'_1), o'_2)$$

A component is *total* on G if it contains every vertex in G . Any total component will then represent a valid semantic interpretation of G . For a dag-ified graph G' , we can always chose a sequence of tensors and compositions that will construct a total component. Take, for instance, a ranking of G' . Tensoring together the vertices of each rank and composing the ranks yields a total component.

Given suitable definitions for the constructors, composition, and tensor product, we can import the generated tensor term into a computer algebra and evaluate it as a matrix.

4.2 Rewrite strategies

Quantomatic will implement a variety of different strategies for automatic graph rewrites. We describe two strategies here, both designed to reduce the graph complexity.

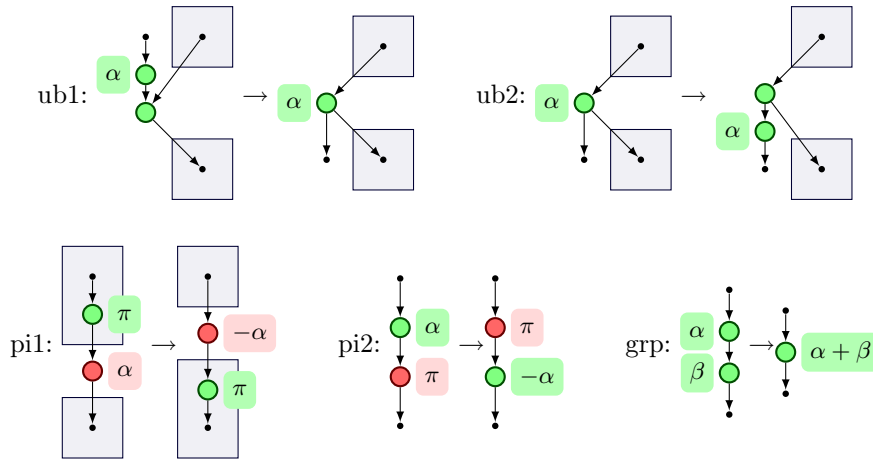
Strategy: CONV

Method: for $R = \{\text{sp}, \text{tr}, \text{el}, \text{ha}, \text{cc}\}$, do $G \downarrow R$

Termination: G is a normal form with respect to R

It was shown in [14] that R is confluent and terminating, so this strategy always terminates with unique normal forms with respect to R .

If we consider each undirected rewrite as a set of directed rewrites, one for each possible ordering, we can make a finer-grained choice of rewrites to apply in a strategy. We'll define an example of this kind of strategy to reduce phase angles.



Note that these rewrites move green angles strictly downward. If we take G to be a dag-ification of an undirected graph, normalising with respect to these rewrites will always terminate. Let A_1 be the above rewrites and A_2 be the same with the colours swapped. We define the *directed angle push* strategy as follows.

Strategy: DAP

Method: repeatedly normalise first with respect to A_1 , then A_2

Termination: G is a fixed point

Proposition 3. *DAP is a terminating strategy.*

Proof. A_1 and A_2 terminate individually for directed acyclic graphs. For each vertex $v \in V_G$, let $w(v)$ be the size of the longest directed walk from v . For all the

vertices $V' \subseteq V_G$ that are labeled with a non-zero angle, let $W = \sum_{v \in V'} w(v)$. All of the above rewrites are strictly non-increasing on W . If $G \downarrow A_1 \downarrow A_2$ preserves W , then all the angles are blocked and G is a fixed point, otherwise W decreases. Since $W \geq 0$, this procedure terminates.

5 Example: Exploring tripartite entanglement³

Two states are SLOCC-equivalent (see appendix A) if and only if they can be converted to one another using one-qubit invertible maps. We shall now show the use of Quantomatic to explore the behaviour and SLOCC-equivalence classes of 3-qubit states. If any part of the state is separable, the problem reduces to that of 2-qubit states, which is trivial. Therefore, we shall only consider true entangled states. From [11], we know that there are only two SLOCC-equivalence classes, represented by the following maps:

$$GHZ :: \{|0\rangle \mapsto |00\rangle, |1\rangle \mapsto |11\rangle\} \text{ and } W :: \{|0\rangle \mapsto |01\rangle + |10\rangle, |1\rangle \mapsto |00\rangle\}$$

Note that $GHZ = \delta_Z$. Figure 2 shows the W state, up to a scalar.

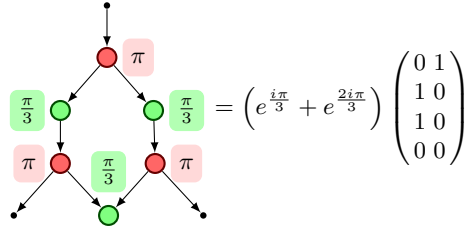


Fig. 2. The W state as a graph

For this example, we shall work mainly with the W state. We start by finding a more general form of W -like (SLOCC-equivalent) states. We shall then identify a rewrite rule for supplementary angles that induces a new kind of graphical behaviour for W -like states.

5.1 Finding a better representative for W -like states

We postulate that we can find an SLOCC-equivalence to the W state for any state of the form given by Fig. 3.

³ Much of this case study follows notes by Bob Coecke and Bill Edwards that were unpublished at the time of this writing. They should soon be available as [7].

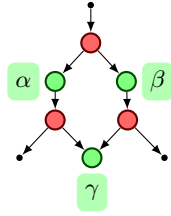


Fig. 3. A general form for the W state.

To help with our search, we narrow down the types of linear maps we will look for. Since we're trying to change the unbiased- Z angles, we'll look at various kinds of Z phase shifts. We try the standard, unitary shifts Z_α as well as the two "partial" shifts Zuc_α and Zdc_α .

$$Z_\alpha := \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix} \quad Zuc_\alpha := \begin{pmatrix} \cos \alpha & 0 \\ 0 & 1 \end{pmatrix} \quad Zdc_\alpha := \begin{pmatrix} 1 & 0 \\ 0 & \cos \alpha \end{pmatrix}$$

Using Quantomatic and Mathematica, we discovered that conjugation by Zuc_α yields a unification. To do this, we first define Zuc_α in graphical terms (Fig. 4). We then feed the equation in Fig. 5 into Quantomatic and export the matrix terms to Mathematica.

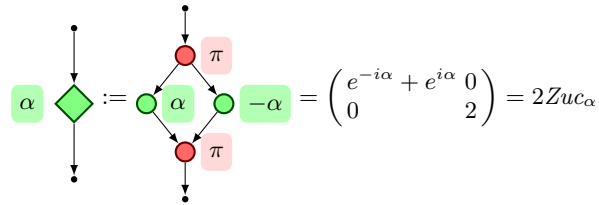


Fig. 4. The definition of Zuc_α

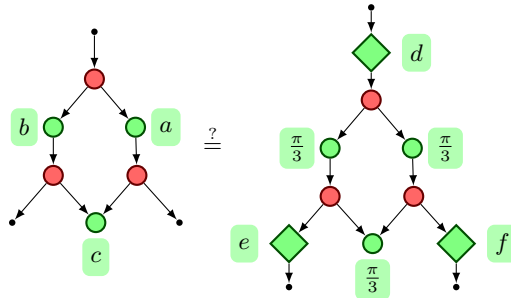


Fig. 5. Equation, conjugating by Zuc

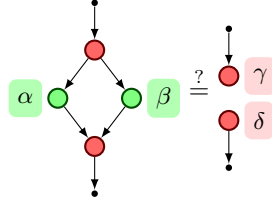
A first call to `Reduce []` yields the condition $(a + b + c = \pi) \wedge (\dots)$. So, letting $c = \pi - a - b$, and calling `Reduce []` again, we find a substitution

$$\sigma = \left\{ d \mapsto \frac{\pi}{2} - a - b, e \mapsto \frac{\pi}{2} - b, f \mapsto \frac{\pi}{2} - a \right\}$$

that satisfies the equation in Fig. 5. Therefore any state of the form given by (3) such that the angles sum to π is SLOCC-equivalent to the W state.

5.2 Supplementary angle condition

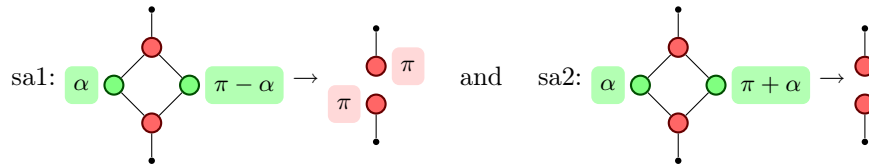
To aid in the reduction of entangled states, we'll search for angles that induce the following graph disconnect.



We use `Quantomatic` to export this identity as a matrix equation. We use `Mathematica` to solve for phase angles and a scaling factor k .

$$\left(\begin{array}{l} k = \frac{1}{e^{i\alpha} + e^{i\beta}} \\ \wedge \gamma = \pi \\ \wedge \delta = \pi \\ \wedge \pi = \alpha + \beta \\ \wedge \pi \neq \alpha - \beta \end{array} \right) \vee \left(\begin{array}{l} k = \frac{1}{1 + e^{i(\alpha + \beta)}} \\ \wedge \gamma = 0 \\ \wedge \delta = 0 \\ \wedge \pi = \alpha - \beta \\ \wedge \pi \neq \alpha + \beta \end{array} \right)$$

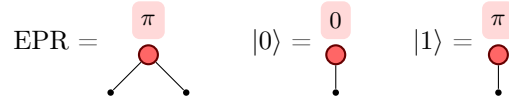
From these conditions, we can deduce that the angles α and β on the LHS are precisely those that are both non-zero and their sum or difference is π . Therefore, we call these identities supplementary angle identities. We can now introduce two new rewrite rules to the theory.



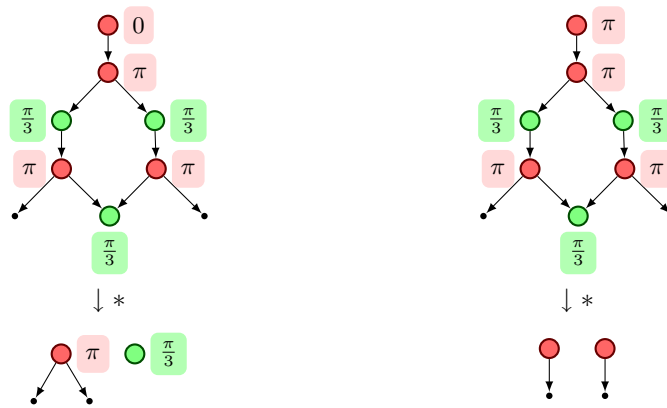
5.3 Emergent property

Let `CONV+SA` be the strategy `CONV`, but with rules $R' = R \cup \{\text{sa1}, \text{sa2}\}$. `CONV+SA` still terminates because all of the rules are strictly reductive on the graph complexity. If we consider the definition of the W state as a map, it is a sort of “controlled” two-qubit entanglement. That is, an input of $|0\rangle$ yields

$|01\rangle + |10\rangle$, which is a fully entangled state called the Einstein-Podolsky-Rosen (EPR) state. An input of $|1\rangle$ yields the separable state $|00\rangle$. If we note the following representations,



then alternate applications of CONV+SA and DAP, we get the following normalisations.



Taking any W -like state, we can apply the rewrite derived in section 5.1 in conjunction with the method above to prove that a $|1\rangle$ input yields a separable state and a $|0\rangle$ yields a state that is SLOCC-equivalent to the EPR state.

6 Conclusion and Future Work

We have shown that Quantomatic is already a useful tool for working with a graphical theory. The example in this paper expanded on some important properties of tripartite states that are W -like. To follow on from this, the natural next step is to give a similar treatment to tripartite states that are GHZ-like. We conjecture that when the angles in Fig. 3 do *not* add up to π , the state is SLOCC-equivalent to the GHZ state. We hope to find local linear maps that are easy to express in the graphical language to prove this identity. After this, the next step is to explore states involving more qubits or higher-dimensional generalisations of qubits such as qutrits for 3 dimensions and qudits for d dimensions.

Quantomatic itself also could benefit from a more flexible theory engine, better support for strategies and cleaner interaction with the computer algebra system. Also, the use of a general-purpose CAS can be limiting in the class of equations it can solve. A specialised CAS that can better cope with phase equations and periodic unknowns could reduce the amount of manual help that

is needed to push systems of equations through a reduction routine. Also, a better implementation of sparse matrices that takes into account the properties of classical structures and tensor products could drastically reduce the resource requirements and increase the effective size limits CAS-based methods.

A Appendix: Quantum Entanglement

Quantum states and state evolutions can be described in terms of a Hilbert space. For this, we shall use Dirac notation, where $|\psi\rangle$ is a vector in the Hilbert space \mathcal{H} and $\langle\psi| := |\psi\rangle^\dagger$, taking $(-)^\dagger$ to be the conjugate-transpose. Multiplication then recovers the usual notions of inner and outer product as $\langle\varphi|\psi\rangle$ and $|\varphi\rangle\langle\psi|$, respectively.

Let \mathcal{Q} be a two-dimensional vector space over the complex numbers. We call elements of \mathcal{Q} quantum bits, or *qubits*. We shall fix a basis called the *computational basis* as $\{|0\rangle, |1\rangle\}$. We can use the computational basis and the tensor product to generate bases for all 2^n dimensional spaces. As a useful shorthand, we write $|ij\rangle := |i\rangle \otimes |j\rangle$. For example the vectors $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ span a 4-dimensional space.

For a Hilbert space \mathcal{H} , the elements of $\mathcal{H} \otimes \mathcal{H}$ that can be represented as $|\psi\rangle \otimes |\varphi\rangle$ for $|\psi\rangle, |\varphi\rangle \in \mathcal{H}$ are called *separable*. Elements of $\mathcal{H} \otimes \mathcal{H}$ that are not separable are called *entangled* and can always be expressed as sums of separable elements.

If we fix a basis $\{|j\rangle\}_j$, we can represent an arbitrary linear map as a matrix $\sum_{ij} c_{ij} |j\rangle\langle i|$. This carries the same data as $\sum_{ij} c_{ij} (|i\rangle \otimes |j\rangle)$, so the space of maps from \mathcal{H} to \mathcal{H} is essentially the same space as $\mathcal{H} \otimes \mathcal{H}$. Letting \mathcal{H}^n be the n -fold tensor product of \mathcal{H} , we express the general result as follows.

Proposition 4. *Linear maps from \mathcal{H}^m to \mathcal{H}^n are in bijective correspondence to the elements of \mathcal{H}^{m+n} .*

This concept is called *map-state duality*. We shall often use it to discuss states as linear maps or vice-versa. In quantum computation, we often view information as passing through various kinds of entanglement. This interpretation is the basis of protocols such as quantum teleportation [2].

There are many different kinds of entanglement. Identifying the equivalence classes of entangled states with respect to certain relations is one of the most important open problems in quantum information theory. Two useful equivalence conditions are LOCC and SLOCC.

Definition 12. *Two states are said to be equivalent up to local operations with classical communication, or LOCC-equivalent if they can be made equal by applying one-qubit unitary corrections that can be chosen based on any classical data about the states. If two states can be made equivalent up to LOCC with some non-zero probability, they are said to be equivalent up to stochastic LOCC, or SLOCC-equivalent.*

Definition 13. Two states $|\psi\rangle, |\varphi\rangle \in \mathcal{H}^n$ are ILO-equivalent if there exist n invertible operators $L_i : \mathcal{H} \rightarrow \mathcal{H}$ such that $(L_1 \otimes \dots \otimes L_n) \circ |\psi\rangle = |\varphi\rangle$. If each L_i is unitary, $|\psi\rangle$ and $|\varphi\rangle$ are said to be LU-equivalent.

It can be shown that two states are LOCC-equivalent if and only if they are LU-equivalent [3], and two states are SLOCC-equivalent if and only if they are ILO-equivalent [11].

References

1. Samson Abramsky and Bob Coecke. A categorical semantics of quantum protocols. *Proceedings from LiCS*, quant-ph, Feb 2004.
2. C Bennett, G Brassard, C Crepeau, and R Jozsa. Teleporting an unknown quantum state via dual classical and epr channels. *Phys. Rev. Lett.*, Jan 1993.
3. Charles H Bennett, Sandu Popescu, Daniel Rohrlich, John A Smolin, and Ashish V Thapliyal. Exact and asymptotic measures of multipartite pure state entanglement. *arXiv*, quant-ph, Aug 1999.
4. Bob Coecke. Kindergarten quantum mechanics. *arXiv*, quant-ph, Oct 2005.
5. Bob Coecke. Introducing categories to the practicing physicist. page 29, Aug 2006.
6. Bob Coecke and Ross Duncan. Interacting quantum observables. *ICALP*, pages 298–310, Mar 2008.
7. Bob Coecke and Bill Edwards. Three qubit entanglement analysed with graphical calculus. *Research Report PRG-RR-09-03*, 2009.
8. Bob Coecke, Eric Oliver Paquette, and Dusko Pavlovic. Classical and quantum structuralism. *Semantic Techniques for Quantum Computation*, page 43, Oct 2008.
9. Bob Coecke, Eric Oliver Paquette, and Simon Perdrix. Bases in diagrammatic quantum protocols. *arXiv*, quant-ph, Aug 2008.
10. Lucas Dixon and Ross Duncan. Extending graphical representations for compact closed categories with applications to symbolic quantum computation. *AISC/MKM/Calcuemu*, pages 77–92, Jun 2008.
11. W Dür, G Vidal, and J. I Cirac. Three qubits can be entangled in two inequivalent ways. *Phys. Rev. A*, 62(6), Nov 2000.
12. Andre Joyal and Ross Street. The geometry of tensor calculus I. *Advances in Mathematics*, 88:55–113, 1991.
13. Max Kelly and Miguel L Laplaza. Coherence for compact closed categories. *Journal of Pure and Applied Algebra*, 19:193–213, 1980.
14. Aleks Kissinger. Graph rewrite systems for classical structures in dagger-symmetric monoidal categories. *Masters Thesis*, pages 1–54, Feb 2008.
15. Stephen Lack. Composing props. *Theory and Applications of Categories*, 13(9):147–163, 2004.
16. J O’Madadhain, D Fisher, and Tom Nelson. Jung: Java universal network/graph framework. <http://jung.sourceforge.net>.
17. Éric Oliver Paquette. Categorical quantum computation. *PhD Thesis*, pages 1–174, Feb 2008.
18. Peter Selinger. Dagger compact closed categories and completely positive maps (extended abstract). *Electronic Notes in Theoretical Computer Science*, 170:139–163, 2007.
19. Jamie Vicary. A categorical framework for the quantum harmonic oscillator. *arXiv*, quant-ph, Jun 2007. 44 pages, many figures.