Unordered Tuples in Quantum Computation

Robert Furber
Radboud Universiteit Nijmegen
rfurber@cs.ru.nl

Bas Westerbaan
Radboud Universiteit Nijmegen
bwesterb@cs.ru.nl

It is well known that the C*-algebra of an ordered pair of qubits is $M_2 \otimes M_2$. What about *unordered* pairs? We show in detail that $M_3 \oplus \mathbb{C}$ is the C*-algebra of an *unordered* pair of qubits. Then we use Schur-Weyl duality to characterize the C*-algebra of an unordered n-tuple of d-level quantum systems. Using some further elementary representation theory and number theory, we characterize the quantum cycles. We finish with a characterization of the von Neumann algebra for unordered words.

Finite dimensional quantum computation is naturally viewed as occurring in the category of finite dimensional C*-algebras together with completely positive unital maps, in the opposite of their usual direction. The C*-algebras are the types (systems). For instance:

a single qubit	M_2	an ordered pair of qutrits	$M_3 \otimes M_3$
a single qutrit	M_3	a bit	$\mathbb{C}^2$
a qubit or a qutrit	$M_2 \oplus M_3$	a trit or a qubit	$\mathbb{C}^3 \oplus M_2$

More generally, writing $[\![\text{type}]\!]$ for the C*-algebra for the type, we have:

$$[\![d\text{-level quantum system}]\!] = M_d \qquad [\![d\text{-level classical system}]\!] = \mathbb{C}^d$$

$$[\![\text{(ordered) pair of } t \text{ and } s]\!] = [\![t]\!] \otimes [\![s]\!] \qquad [\![t \text{ (classical) or } s]\!] = [\![t]\!] \oplus [\![s]\!].$$

The completely positive unital maps are the programs (operations) in the opposite direction. For example:

1. *Measure a qubit in the standard basis*
   $m\colon M_2 \leftarrow \mathbb{C}^2$ (qubit $\to$ bit)
   $(\lambda,\mu) \mapsto \lambda\,|0\rangle\langle 0| + \mu\,|1\rangle\langle 1|$
2. *Apply Hadamard gate to a qubit*
   $h\colon M_2 \leftarrow M_2$ (qubit $\to$ qubit)
   $a \mapsto H^\dagger a H$, where $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
3. *Initialize a qutrit as 0*
   $i\colon \mathbb{C} \leftarrow M_3$ (empty $\to$ qutrit)
   $a \mapsto \langle 0|\,a\,|0\rangle$
4. *Forget about a qubit*
   $d\colon M_2 \leftarrow \mathbb{C}$ (qubit $\to$ empty)
   $\lambda \mapsto \lambda 1$

These basic quantum types are well known, but what about an unordered pair of qubits? An unordered pair of bits is simply a trit (00, 01 = 10 or 11). However, we will see an unordered pair of qubits is not a qutrit, but rather its C*-algebra is $M_3 \oplus \mathbb{C}$.

In Section 1, we prove this in detail to get a feel for this surprising result. Then in Section 2, we characterize the C*-algebras of unordered n-tuples of d-level quantum systems using Schur-Weyl duality, which dates back to the early 20th century. Applying some elementary representation theory, we characterize the C*-algebra for qubit 3-cycles in Section 3. Then, using some number theory, we characterize arbitrary quantum cycles in Section 4. We finish with a characterization of the von Neumann algebra for the quantum unordered words in Section 5.

Chris Heunen, Peter Selinger, and Jamie Vicary (Eds.):
12th International Workshop on Quantum Physics and Logic (QPL 2015).
EPTCS 195, 2015, pp. 196–207, doi:10.4204/EPTCS.195.15

Unordered quantum types have been considered before. For instance in [5] they are used to give denotational semantics to a quantum lambda calculus.[1] A concrete description, however, has to our knowledge not been published before.

At the end of the paper we will have demonstrated the following.

System	Algebra
unordered pair of qubits	$M_3 \oplus \mathbb{C}$
unordered n-tuple of d-level quantum systems	$\bigoplus_{\lambda \in Y_n} M_{m_\lambda}$
words of qubits	$B(\ell^2)$
unordered words of d-level quantum systems	$B(\ell^2) \oplus \bigoplus_{\lambda \in Y^*} M_{m_\lambda}$
3-cycle of qubits	$M_4 \oplus M_2 \oplus M_2$
n-cycle of d-level quantum systems	$\bigoplus_{0 \le k < n} M_{c_k}$

$$Y_n = \left\{\lambda;\ \lambda \in \mathbb{N}^n;\ \begin{bmatrix} \lambda_1 \ge \ldots \ge \lambda_d \ge 0 \\ \lambda_1 + \ldots + \lambda_d = n \end{bmatrix}\right\}$$ (n-block Young diagrams of height at most d)

$$Y^* = \bigcup_{n \ge 2} \{\lambda;\ \lambda \in Y_n;\ \lambda_2 \ne 0\}$$

$$m_\lambda = \prod_{1 \le i < j \le d} \frac{\lambda_i - \lambda_j + j - i}{j - i}$$ (Dimension corresponding representation $\mathrm{GL}(d)$)

$$c_k = \frac{1}{n} \sum_{l \mid n} d^{\frac{n}{l}} \mu\left(\frac{l}{\gcd(l,k)}\right) \frac{\phi(l)}{\phi\left(\frac{l}{\gcd(l,k)}\right)}$$ (Ramanujan sum)

φ : Euler's totient

μ : Möbius function

See appendix A for some decompositions computed using these formulae.

1 An Unordered Pair of Qubits

The Hilbert space of a pair of qubits is $\mathbb{C}^2 \otimes \mathbb{C}^2$. Write $\mathscr{H} = \mathbb{C}^2 \otimes \mathbb{C}^2$. Let $\sigma \colon \mathscr{H} \to \mathscr{H}$ denote the unitary map that exchanges the two qubits:

$$\sigma\colon \begin{array}{ll} |00\rangle \mapsto |00\rangle & |01\rangle \mapsto |10\rangle \\ |10\rangle \mapsto |01\rangle & |11\rangle \mapsto |11\rangle \end{array}$$

An important category to study semantics of finite-dimensional quantum computation is $\mathbf{Star}^{\mathrm{op}}_{\mathrm{cPU}}$, which we will define in a moment. It is important as every object corresponds to a type of finite-dimensional quantum system and every arrow to a program of the corresponding type. Conversely, every physical

[1] The type $[\![\mathbf{qubit}]\!]^{\odot 2}$ from [5, Example 23] corresponds to an unordered pair of qubits and thus has as C*-algebra $M_3 \oplus \mathbb{C}$.

finite dimensional quantum type and program corresponds to an object and arrow (respectively) in this category.

The objects are finite-dimensional C*-algebras[2]. As the norm plays no rôle in this paper, these are equivalently semisimple $*$-algebras over $\mathbb{C}$, and are also equivalently finite dimensional W*-algebras. Accordingly, we refer to them as $*$-algebras in the rest of the paper. We remark, however, that there are finite-dimensional $*$-algebras in the axiomatic sense that are not C*-algebras and these are excluded. The arrows in $\mathbf{Star}_{\mathrm{cPU}}$ are completely positive unital linear maps, and in $\mathbf{Star}_{\mathrm{cPU}}^{\mathrm{op}}$ they are in the opposite direction. [3]

The $*$-algebra of a pair of qubits is $B(\mathscr{H}) \cong M_4$. The map that exchanges the two qubits is given by:

$$B(\sigma)\colon M_4 \leftarrow M_4, \quad a \mapsto \sigma^{-1} a \sigma = \sigma a \sigma.$$

We claim the $*$-algebra of an unordered pair of qubits must be the coequalizer of $B(\sigma)$ and id. This is the equalizer in $\mathbf{Star}_{\mathrm{cPU}}$, which is the following subalgebra of M_4

$$E = \{a;\ a \in M_4;\ \sigma a \sigma = a\} \subseteq M_4.$$

First note the analogy with the classical case: to form an unordered pair of bits, one takes the quotient with respect to the equivalence relation defined by permuting the bits, which identifies 01 and 10. This is a coequalizer in the category **Set**. Why is the coequalizer used? The definition gives the following rule: for every program $f\colon M_4 \leftarrow \mathscr{A}$ invariant under swapping ($\sigma \circ f = f$) there is a unique lift $f'\colon E \leftarrow \mathscr{A}$ such that $e \circ f' = f$, where $e\colon E \subseteq M_4$ is the coequalizer map.

What $*$-algebra is E? We write $\mathscr{S}$ for the *symmetric part* of $\mathscr{H}$:

$$\mathscr{S} = \{v;\ v \in \mathscr{H};\ \sigma v = v\}.$$

One might expect $E = B(\mathscr{S})$, but this is not the case. There is another summand of E. First, we must take a small detour. It is easy to verify that the projection onto $\mathscr{S}$ is given by

$$P_{\mathscr{S}}\colon v \mapsto \frac{v + \sigma v}{2},$$

which is called the *symmetrizer*. The complementary projection $P_{\mathscr{A}} = I - P_{\mathscr{S}}$

$$P_{\mathscr{A}}\colon v \mapsto \frac{v - \sigma v}{2}$$

projects onto the antisymmetric subspace of $\mathscr{H}$, which is given by

$$\mathscr{A} = \{v;\ v \in \mathscr{H};\ \sigma v = -v\}.$$

By considering the images of the standard basis vectors under $P_{\mathscr{A}}$ and $P_{\mathscr{S}}$, it is easy to determine that

$$\{|00\rangle, |11\rangle, \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle\} \quad \text{and} \quad \{\frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle\}$$

are orthonormal bases for $\mathscr{S}$ and respectively $\mathscr{A}$.

---

[2] Which are automatically unital.

[3] The category $\mathbf{Star}_{\mathrm{cPU}}^{\mathrm{op}}$ and its variations occur under different names in the literature. The category $\mathbf{Star}_{\mathrm{cP}}^{\mathrm{op}}$ of finite dimensional C*-algebras with c.p. maps in the opposite direction is equivalent to the category $\mathbf{CP}^*[\mathbf{FHilb}]$ from [1]. If we restrict to subunital maps, we call the category $\mathbf{Star}_{\mathrm{cPsU}}^{\mathrm{op}}$, which is equivalent to the category $\mathbf{Q}$ from [7] and the category CPM_s from [5].

There is a map $i\colon B(\mathscr{S}) \oplus B(\mathscr{A}) \to B(\mathscr{S} \oplus \mathscr{A}) \cong B(\mathscr{H})$, given by

$$(s,a) \mapsto s \oplus a = \begin{pmatrix} s & 0 \\ 0 & a \end{pmatrix}.$$

Its image, $\mathrm{Im}\, i$, is actually the equalizer E. We have to show both inclusions.

First, suppose $a \in \mathrm{Im}\, i$. Then $a = P_{\mathscr{S}} a P_{\mathscr{S}} + P_{\mathscr{A}} a P_{\mathscr{A}}$. Note that $\sigma P_{\mathscr{S}} = P_{\mathscr{S}} \sigma = P_{\mathscr{S}}$ and $\sigma P_{\mathscr{A}} = P_{\mathscr{A}} \sigma = -P_{\mathscr{A}}$. Thus:

$$\sigma a \sigma = \sigma P_{\mathscr{S}} a P_{\mathscr{S}} \sigma + \sigma P_{\mathscr{A}} a P_{\mathscr{A}} \sigma = P_{\mathscr{S}} a P_{\mathscr{S}} + P_{\mathscr{A}} a P_{\mathscr{A}} = a.$$

Hence $a \in E$.

Conversely, suppose $a \in E$. First note that $a = P_{\mathscr{S}} a P_{\mathscr{S}} + P_{\mathscr{A}} a P_{\mathscr{A}} + P_{\mathscr{S}} a P_{\mathscr{A}} + P_{\mathscr{A}} a P_{\mathscr{S}}$. Now since $\sigma a \sigma = a$, we have:

$$P_{\mathscr{S}} a P_{\mathscr{S}} + P_{\mathscr{A}} a P_{\mathscr{A}} + P_{\mathscr{S}} a P_{\mathscr{A}} + P_{\mathscr{A}} a P_{\mathscr{S}} = P_{\mathscr{S}} a P_{\mathscr{S}} + P_{\mathscr{A}} a P_{\mathscr{A}} - P_{\mathscr{S}} a P_{\mathscr{A}} - P_{\mathscr{A}} a P_{\mathscr{S}}.$$

Thus $P_{\mathscr{S}} a P_{\mathscr{A}} = -P_{\mathscr{A}} a P_{\mathscr{S}}$. Their images are orthogonal, hence $P_{\mathscr{S}} a P_{\mathscr{A}} = P_{\mathscr{A}} a P_{\mathscr{S}} = 0$. So $a = P_{\mathscr{S}} a P_{\mathscr{S}} + P_{\mathscr{A}} a P_{\mathscr{A}}$, and hence $a \in \mathrm{Im}\, i$.

Thus $E \cong B(\mathscr{S}) \oplus B(\mathscr{A}) \cong M_3 \oplus \mathbb{C}$. At first one might be surprised that the antisymmetric vector $\frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle$ of $\mathscr{H}$ is a possible state of an unordered pair of qubits, since σ changes its sign. The explanation is simple: in $*$-algebras, two states that differ only by global phase are identified. Thus the antisymmetric vector is symmetric up to global phase -1.

An astute reader might note that we have proven a bit more: the $*$-algebra associated to an unordered pair of d-level quantum systems is given by $B(\mathscr{A}) \oplus B(\mathscr{S})$ as well, where $\mathscr{A}, \mathscr{S} \subseteq \mathbb{C}^d \otimes \mathbb{C}^d$ are defined similarly.

2 Unordered Tuples

In the previous section, we have shown how to characterize the $*$-algebra for a pair of qubits. In this section, we will generalize to arbitrary tuples. We define an unordered n-tuple of d-level quantum systems as follows. Consider the Hilbert space $(\mathbb{C}^d)^{\otimes n}$. A permutation of n elements $\pi \in S_n$ acts on it in an obvious way, by permuting the basis vectors as follows:

$$\pi\colon \ |i_1 i_2 \ldots i_n\rangle \mapsto |i_{\pi^{-1}(1)} \ldots i_{\pi^{-1}(n)}\rangle. \tag{1}$$

The equalizer of all $\pi \in S_n$ in $\mathbf{Star}_{\mathrm{cPU}}$ is the $*$-algebra for unordered n-tuples of d-level quantum systems. It is given by the following subalgebra of $B((\mathbb{C}^d)^{\otimes n})$

$$E = \{a;\ \pi^{-1} a \pi = a \text{ for all } \pi \in S_n\} \subseteq B((\mathbb{C}^d)^{\otimes n}).$$

The final result is:

$$E \cong \bigoplus_{\substack{\lambda_1 \geq \ldots \geq \lambda_d \geq 0 \\ \lambda_1 + \ldots + \lambda_d = n \\ \lambda_1, \ldots, \lambda_d \in \mathbb{N}}} M_{m_\lambda} \quad \text{where} \quad m_\lambda = \prod_{1 \leq i < j \leq d} \frac{\lambda_i - \lambda_j + j - i}{j - i}.$$

To prove this, we will first review some of the basics of representation theory of finite groups. Then we will introduce Schur-Weyl duality to prove the result.

A representation of a group is a pair (V,ρ), where V is a vector space and $\rho : G \to \mathrm{GL}(V)$ is a group homomorphism. Often, one refers to the vector space V as the representation instead of the group homomorphism. When considering the action of $g \in G$ on vectors $v \in V$ it is common to leave out the ρ and write gv instead of $\rho(g)v$.

We now give some examples of representations. The vector space $(\mathbb{C}^d)^{\otimes n}$ is a representation of S_n, by the action given in equation (1). Another one is that for any group G, we can consider $\rho_{\text{trivial}} \colon G \to \mathrm{GL}(\mathbb{C})$ given by $\rho_{\text{trivial}}(g) = I$. This is called the *trivial representation*.

Given two representations $\rho \colon G \to \mathrm{GL}(V)$ and $\sigma \colon G \to \mathrm{GL}(W)$ a morphism f from ρ to σ is a linear map $f \colon U \to V$ such that $\sigma(g)f = f\rho(g)$ for every $g \in G$. That is: linear maps that commute with the group actions of the representations.

We can relate morphisms of representations to the equalizer that we want to calculate as follows.

$$\begin{aligned}\mathbf{Rep}(S_n)((\mathbb{C}^d)^{\otimes n},(\mathbb{C}^d)^{\otimes n}) &= \{a;\ a \in B((\mathbb{C}^d)^{\otimes n});\ \pi a = a\pi \text{ for all } \pi \in S_n\} \\ &= \{a;\ a \in B((\mathbb{C}^d)^{\otimes n});\ \pi^{-1}a\pi = a \text{ for all } \pi \in S_n\} \\ &= E.\end{aligned}$$

Given two representations $\rho \colon G \to \mathrm{GL}(V), \sigma : G \to \mathrm{GL}(W)$, one can define the direct sum representation on $V \oplus W$ by $(\rho,\sigma)(g)(v,w) = (\rho(g)(v), \sigma(g)(w))$. A representation is called indecomposable if it is not the direct sum in this way of two other representations.

Given a representation on a vector space V and a subspace U, one calls U invariant (under G) if for every $u \in U$ and $g \in G$ we have $gu \in U$. A representation on V is called irreducible if the only invariant subspaces are $\{0\}$ and V itself. This intentionally implies that the unique representation on the zero-dimensional vector space is not irreducible, for the same reason that 1 is not prime and $\emptyset$ is not connected as a topological space.

A slightly surprising, but welcome, theorem is that a representation of a finite group is indecomposable if and only if it is irreducible. Furthermore, every representation is uniquely the direct sum of irreducible representations (up to isomorphism). See [2, Proposition 1.5].

Thus there are distinct irreducible representations U_λ and natural numbers m_λ, called multiplicities, such that $(\mathbb{C}^d)^{\otimes n} \cong \bigoplus U_\lambda^{\oplus m_\lambda}$ and hence

$$E \cong \bigoplus_{\lambda,\mu} \mathbf{Rep}(S_n)(U_\lambda^{m_\lambda}, U_\mu^{m_\mu}).$$

Now, given a morphism between representations, it is easy to see that its kernel and image are invariant. Thus, the only morphisms between irreducible representations are invertible or zero maps. This is the first part of Schur's lemma. Consequently the maps between non-isomorphic irreducible representations are 0 and do not contribute to the direct sum, giving

$$E \cong \bigoplus_{\lambda} \mathbf{Rep}(S_n)(U_\lambda^{m_\lambda}, U_\lambda^{m_\lambda}).$$

The second part of Schur's lemma is the following observation. Suppose we have an endomorphism f of an irreducible representation V. Since the base field $\mathbb{C}$ is algebraically closed, f must have an eigenvalue λ, which is to say that $f - \lambda I$ has non-trivial kernel. The map $f - \lambda I$ is itself a morphism of representations, and since V is irreducible, $\ker(f - \lambda I) = V$ and so $f - \lambda I = 0$. That is to say: $f = \lambda I$. Thus endomorphisms of irreducible representations are scalar multiples of the identity. We deduce

$$E \cong \bigoplus_{\lambda} M_{m_\lambda}.$$

Thus, if we know the irreducible representations of S_n and their multiplicities in $(\mathbb{C}^d)^{\otimes n}$, then we know E. Schur-Weyl duality solves this problem for us. It gives a correspondence between the irreducible representations of S_n in $(\mathbb{C}^d)^{\otimes n}$ and of $\mathrm{GL}(d)$ in $(\mathbb{C}^d)^{\otimes n}$. The space $(\mathbb{C}^d)^{\otimes n}$ is a representation of $\mathrm{GL}(d)$, via the following action

$$gv_1 \otimes \ldots \otimes v_n = (gv_1) \otimes \ldots \otimes (gv_d).$$

Schur-Weyl duality asserts

$$(\mathbb{C}^d)^{\otimes n} \cong \bigoplus_{\substack{\lambda_1 \geq \ldots \geq \lambda_d \geq 0 \\ \lambda_1 + \ldots + \lambda_d = n \\ \lambda_1, \ldots, \lambda_d \in \mathbb{N}}} U_\lambda \otimes V_\lambda \equiv \bigoplus_{\substack{\lambda_1 \geq \ldots \geq \lambda_d \geq 0 \\ \lambda_1 + \ldots + \lambda_d = n \\ \lambda_1, \ldots, \lambda_d \in \mathbb{N}}} U_\lambda^{\oplus \dim V_\lambda}$$

where U_λ are irreducible representations of S_n and V_λ are irreducible representations of $\mathrm{GL}(d)$. See [2, Exercise 6.30]. Thus $m_\lambda = \dim V_\lambda$. Together with the duality statement, we are given explicit constructions for U_λ and V_λ. See [2, Theorem 4.3] and [2, §6.1]. From this one can derive[2, Theorem 6.3 (1)] that

$$\dim V_\lambda = \prod_{1 \leq i < j \leq d} \frac{\lambda_i - \lambda_j + j - i}{j - i}.$$

In particular, in the case of unordered n-tuples of qubits, we see $\dim V_\lambda = \lambda_i - \lambda_j + j - i$ and hence

$$E \cong \begin{cases} \bigoplus_{1 \leq i \leq \frac{n}{2}+1} M_{2i-1} & n \text{ even} \\ \bigoplus_{1 \leq i \leq \frac{n+1}{2}} M_{2i} & n \text{ odd.} \end{cases}$$

3 A 3-cycle of Qubits

Unordered tuples are defined by quotienting out the action of the symmetric group. Similarly, we can define other types by quotienting out the action of a subgroup of the symmetric group. The methods of the previous section can be adapted to this situation as well. We will consider cycles, which are not as interesting a type as unordered tuples, but they serve as an example easily related to regular combinatorics.

A 3-cycle of qubits is given by the equalizer

$$E = \{a;\ a \in M_8;\ \pi^{-1} a \pi = a;\ \pi \in C_3 \leq S_3\} \subseteq M_8.$$

The cyclic subgroup C_3 of S_3 contains $\{(), (1\ 2\ 3), (1\ 3\ 2)\}$. We can use the same argument as before to derive that $E \cong \bigoplus_i M_{m_i}$, where m_i is the multiplicity of the ith irreducible representation of C_3 in $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$. However, Schur-Weyl duality will not help this time. We need to determine the multiplicities m_i in another way.

To this end, we recall the theory of characters. Given a representation $\rho\colon G \to \mathrm{GL}(V)$. For each $g \in G$ we can consider the trace $\mathrm{Tr}\,\rho(g)$. This yields a map $\chi_V = \mathrm{Tr} \circ \rho\colon G \to \mathbb{C}$, which is called the *character* of ρ.

By the cyclic property of the trace, we have for any character χ that $\chi(h^{-1}gh) = \chi(ghh^{-1}) = \chi(g)$. Thus on the same conjugacy class, a character will give the same value. Such a function is called a *class function*.

Using Schur's lemma one can work out that

$$\dim \mathbf{Rep}(G)(V,W) = \frac{1}{\#G} \sum_{g \in G} \overline{\chi_V(g)} \chi_W(g) = \begin{cases} 1 & V \cong W \\ 0 & V \ncong W. \end{cases}$$

Also, using spectral decomposition, we can derive $\chi_{V\oplus W} = \chi_V + \chi_W$. Thus, for two such class functions $\alpha, \beta\colon G \to \mathbb{C}$, one is lead to define

$$(\alpha,\beta) = \frac{1}{\#G}\sum_{g\in G}\overline{\alpha(g)}\beta(g).$$

This is an Hermitian inner product on the class functions. In fact, with respect to this inner product

1. the characters of irreducible representations are an orthonormal basis of the class functions;
2. a representation V is irreducible if and only if $(\chi_V,\chi_V) = 1$;
3. there are as many irreducible representations as conjugacy classes *and*
4. the multiplicity of V in W is (χ_V,χ_W).

See [2, §2.2 and Proposition 2.30].

Thus, to determine the multiplicities of the irreducible representations of C_3 in $\mathbb{C}^2\otimes\mathbb{C}^2\otimes\mathbb{C}^2$, it is sufficient to determine the character of $\mathbb{C}^2\otimes\mathbb{C}^2\otimes\mathbb{C}^2$ and the characters of the irreducible representations of C_3.

We determine the irreducible representations of C_3 as follows. As C_3 is Abelian, its conjugacy classes are trivial. Write π for the generator of C_3 such that $C_3 = \{1,\pi,\pi^2\}$. Thus, we are looking for $\#C_3 = 3$ irreducible representations. The trivial representation maps every group element to the identity matrix. It has character $(1,1,1)$. Then we have two 1-dimensional representations given by $\pi\mapsto(\omega)$ and $\pi\mapsto(\omega^2)$, where $\omega = e^{\frac{2}{3}i\pi}$. Using the inner product, we can compute that these are distinct irreducible representations. We summarize these results in a character table:

$C_3 \le S_3$	1	π	π^2
trivial	1	1	1
first	1	ω	ω^2
second	1	ω^2	ω

Now we compute the character χ of $\mathbb{C}^2\otimes\mathbb{C}^2\otimes\mathbb{C}^2$. This is particularly easy because of the way the action is defined: the value of the character on g is the number of basis vectors fixed by g. Thus:

$C_3 \le S_3$	1	π	π^2
$\mathbb{C}^2\otimes\mathbb{C}^2\otimes\mathbb{C}^2$	8	2	2

We compute

$$(\chi_{\text{trivial}},\chi) = 4 \qquad (\chi_{\text{first}},\chi) = 2 \qquad (\chi_{\text{second}},\chi) = 2.$$

Thus the $*$-algebra for a 3-cycle of qubits is given by $E = M_4\oplus M_2\oplus M_2$.

4 Cycles

Now we characterize arbitrary cycles: a n-cycle of d-level quantum systems is given by the equalizer

$$E = \{a;\ a\in B((\mathbb{C}^d)^{\otimes n});\ g^{-1}ag = a;\ g\in C_n\le S_n\}\subseteq B((\mathbb{C}^d)^{\otimes n}).$$

First, we compute the irreducible representation of C_n. Let $\pi\in C_n$ be such that $C_n = \{1,\pi,\pi^2,\ldots,\pi^n\}$. Note that by commutativity, the conjugacy classes are trivial. For any $0\le k\le n$, define a 1-dimensional representation ρ_k by

$$\rho_k\colon C_n\to \mathrm{GL}(\mathbb{C}) \qquad \pi^i\mapsto(\omega^{ki}),$$

where $\omega = e^{2\pi i/n}$. Note that ρ_0 is the trivial representation. Now, observe

$$(\rho_i, \rho_i) = \frac{1}{n} \sum_{0 \leq i < n} |\omega^{ik}|^2 = 1$$

and $\operatorname{Tr} \rho_j(\pi) \neq \operatorname{Tr} \rho_i(\pi)$ whenever $i \neq j$, so these are k distinct irreducible representations. The character table is given by

$C_n \leq S_m$	1	π	π^2	$\ldots$	π^{n-1}
ρ_0	1	1	1	$\ldots$	1
ρ_1	1	ω	ω^2	$\ldots$	ω^{n-1}
ρ_2	1	ω^2	ω^4	$\ldots$	$\omega^{2(n-1)}$
		$\vdots$			$\vdots$
ρ_{n-1}	1	ω^{n-1}	$\omega^{2(n-1)}$	$\ldots$	$\omega^{(n-1)^2}$

Now we will compute that character χ of the representation on $(\mathbb{C}^d)^{\otimes n}$. The value of $\chi(\pi^i)$ is the number of basis vectors that are fixed by π^i.

All of the basis vectors are fixed by $1 = \pi^0$, so $\chi(1) = d^n$. The only basis vectors fixed by π are of the form $|vv\ldots v\rangle$. The general case is more subtle. For instance, suppose $n = 4$ and $d = 2$. Then $|0101\rangle$ is fixed by π^2.

Given $0 \leq i < n$. If a basis vector $|v_1 \ldots v_n\rangle$ is fixed by π^i, then we must have $v_j = v_{\pi^i(j)} = v_{\pi^{2i}(j)} = \ldots$ for any $0 \leq j < n$. If i is coprime to n, then $\{0, \pi^i(0), \pi^{2i}(0), \ldots\}$ (the orbit of the subgroup generated by π^i) ranges over all indices and thus the basis vector must be of the form $|vv\ldots v\rangle$. If j is not coprime to n, then $\{1, 2, \ldots, n\}$ splits into several equally sized orbits. The size of each of them is the order of π^i, which equals $\frac{n}{\gcd(i,n)}$. Thus the number of orbits is $\gcd(i,n)$. On each of the orbits, the basis vector has the same value, but is otherwise unrestricted. Thus there are $d^{\gcd(i,n)}$ basis vectors fixed by π^i. Thus $\chi(\pi^i) = d^{\gcd(i,n)}$.

Now, we will compute the multiplicity of the kth irreducible representation in ρ, which is given by (χ_k, χ):

$$\begin{aligned} (\chi_k, \chi) &= \frac{1}{n} \sum_{0 \leq j < n} \omega^{jk} d^{\gcd(j,n)} \\ &= \frac{1}{n} \sum_{l \mid n} \sum_{\substack{1 \leq j \leq n \\ \gcd(j,n) = l}} \omega^{jk} d^l \\ &= \frac{1}{n} \sum_{l \mid n} d^l \sum_{\substack{1 \leq j \leq n \\ \gcd(j,n) = l}} \omega^{jk}. \end{aligned} \tag{2}$$

As l divides j, we may substitute jl for j and get:

$$(\chi_k, \chi) = \frac{1}{n} \sum_{l \mid n} d^l \sum_{\substack{1 \leq jl \leq n \\ \gcd(jl,n) = l}} \omega^{jlk} = \frac{1}{n} \sum_{l \mid n} d^l \sum_{\substack{1 \leq j \leq \frac{n}{l} \\ \gcd(j, \frac{n}{l}) = 1}} \omega^{jlk}.$$

In [6], Ramanujan introduced (what are now called) *Ramanujan sums*:

$$c_n(m) = \sum_{\substack{1 \leq h \leq n \\ \gcd(h,n) = 1}} e\left(\frac{hm}{n}\right),$$

where $e(x) = e^{2\pi ix}$. Note that $\omega^{jlk} = e\left(\frac{jlk}{n}\right)$. Consequently

$$(\chi_k, \chi) = \frac{1}{n}\sum_{l|n} d^l c_{\frac{n}{l}}(k) = \frac{1}{n}\sum_{l|n} d^{\frac{n}{l}} c_l(k).$$

Hölder gave a simple expression for $c_l(k)$, see [4, Theorem 272]:

$$c_l(k) = \mu\left(\frac{l}{\gcd(l,k)}\right)\frac{\phi(l)}{\phi\left(\frac{l}{\gcd(l,k)}\right)},$$

where μ is the Möbius function and ϕ is Euler's totient. Therefore:

$$(\chi_k, \chi) = \frac{1}{n}\sum_{l|n} d^{\frac{n}{l}} \mu\left(\frac{l}{\gcd(l,k)}\right)\frac{\phi(l)}{\phi\left(\frac{l}{\gcd(l,k)}\right)}.$$

There are two cases of particular interest, which can be proven directly from (2):

- If n is a prime number, then:

$$(\chi_k, \chi) = \begin{cases} \frac{d^n+(n-1)d}{n} & k = 0 \\ \frac{d^n-d}{n} & k > 0. \end{cases}$$

- The multiplicity corresponding to the trivial representation is

$$(\chi_0, \chi) = \frac{1}{n}\sum_{l|n} d^{\frac{n}{l}} \mu(1)\phi(l) = \frac{1}{n}\sum_{l|n} d^l \phi\left(\frac{n}{l}\right).$$

  This is MacMahon's formula for counting the number of possible necklaces with n beads, where we may choose from d different colors of beads. See [3, 4.63].

5 Unordered Words

Classically, a word is just a n-tuple for some n. To work out what should be an unordered word, we simply work out what is an unordered n-tuple. In the quantum analogue, such a reduction does not work. Again, we need to tune our methods to work out a suitable equalizer.

The Hilbert space for quantum words over a d-level quantum system is the infinite dimensional Hilbert space

$$\mathscr{H} := \bigoplus_{n\in\mathbb{N}} (\mathbb{C}^d)^{\otimes n}.$$

Note that it only contains sequences that are square summable. The corresponding von Neumann algebra is the set of all bounded operators $B(\mathscr{H})$.

We will define an action $\rho_{\mathscr{H}}$ of $\prod_{n\in\mathbb{N}} S_n$ on $\mathscr{H}$ as follows.

$$\rho_{\mathscr{H}}(\pi_1, \pi_2, \ldots)(|i_1 \ldots i_m\rangle) = |i_{\pi_m^{-1}(1)} \ldots i_{\pi_m^{-1}(m)}\rangle$$

We wish to compute the equalizer of the actions, which is simply given by

$$\begin{aligned} E &= \{a;\ a \in B(\mathscr{H});\ \pi^{-1}a\pi = a \text{ for all } \pi \in \prod_{n\in\mathbb{N}} S_n\} \\ &= \mathbf{BRep}(\textstyle\prod_n S_n)(\mathscr{H}, \mathscr{H}), \end{aligned} \tag{3}$$

where $\mathbf{BRep}(\prod_n S_n)(\mathscr{H},\mathscr{H})$ denotes the morphisms of representations that are bounded (as linear maps between Hilbert spaces).

We cannot simply apply the same techniques as in Section 2. There are various difficulties. First, $\mathscr{H}$ is infinite dimensional and the group $\prod_n S_n$ is not finite so it does not follow from the theory we used previously that H splits into irreducible representations of $\prod_n S_n$. Secondly, the infinite product $\bigoplus$ is not a coproduct anymore. We will work around these issues *ad hoc*. It is possible to give $\prod_n S_n$ a compact topology using Tychonoff's theorem and use the representation theory of compact groups, but we do not pursue that direction.

Let $i_n \colon S_n \to \prod_{n\in\mathbb{N}} S_n$ denote the obvious inclusion and $p_n \colon B(H) \to B((\mathbb{C}^d)^{\otimes n})$ the obvious projection. Then $p_n \circ \rho_H \circ i_n$ is the action we considered in (1). Recall that

$$(\mathbb{C}^d)^{\otimes n} \cong \bigoplus_{\lambda\in Y_n} U_\lambda^{\oplus m_\lambda} \quad \text{where} \quad m_\lambda = \prod_{1\le i<j\le d} \frac{\lambda_i-\lambda_j+j-i}{j-i}$$

and U_λ are distinct irreducible representations for S_n indexed by

$$Y_n = \left\{\lambda;\ \lambda\in\mathbb{N}^n;\ \begin{bmatrix}\lambda_1\ge\ldots\ge\lambda_d\ge 0\\ \lambda_1+\ldots+\lambda_d = n\end{bmatrix}\right\},$$

which are called n-block Young diagrams of height at most d. The diagram λ is often depicted as a row of λ_1 blocks, then a row of λ_2 blocks beneath it and so on. All blocks are left justified. For instance, $(4,2,0)$ is written as $\begin{smallmatrix}\square&\square&\square&\square\\ \square&\square\end{smallmatrix}$.

Note that U_λ for any $\lambda\in Y_n$ is an irreducible representation for $\prod_{n\in\mathbb{N}} S_n$ as well, since S_m acts trivially on U_λ if $m\ne n$. However, not all U_λ are distinct.

For each $n\in\mathbb{N}$, there is the trivial representation of S_n. They correspond to the Young diagrams of height 1 ($\square$, $\square\square$, $\square\square\square$, $\ldots$). They are all isomorphic as representations of $\prod_{n\in\mathbb{N}} S_n$. The representation isomorphism between any two, is the unique non-zero map between the 1-dimensional subspaces. We will show all other representations are distinct.

The *kernel* of a representation (V,ρ), is the subgroup of elements that map to the identity operator, equivalently the kernel of ρ as a group homomorphism. If two representations are isomorphic then their kernels and dimensions are the same.

Given $n,m\in\mathbb{N}$ and $\lambda\in Y_n$ and $\mu\in Y_m$ with $\lambda\ne\mu$ such that, without loss of generality, U_λ is not a trivial representation. Suppose $n=m$ and U_λ is isomorphic to U_μ as representation of $\prod_{n\in\mathbb{N}} S_n$. Then it is also isomorphic via the same isomorphism as representation of $S_n = S_m$, which is a contradiction. Thus U_λ and U_μ are distinct.

For the remaining case, suppose $n\ne m$. Because U_λ is not a trivial representation, there is an element $\pi\in S_n$ that is not in its kernel. If U_μ is a trivial representation, then U_λ and U_μ must be distinct as they have different kernels. If U_μ is not a trivial representation, then there is an element $\pi'\in S_m$ that is not in its kernel. By definition of the action on $\mathscr{H}$, every element of S_n is in the kernel of U_μ. Thus U_λ and U_μ have different kernel. Hence they are distinct.

We have a direct sum decomposition of $\mathscr{H}$ into irreducible representations of $\prod_{n\in\mathbb{N}} S_n$:

$$\mathscr{H} = \bigoplus_{n\in\mathbb{N}} (\mathbb{C}^d)^{\otimes n} \cong U_{\text{trivial}}^{\oplus\omega} \oplus \bigoplus_{\substack{n\in\mathbb{N}\\ \lambda\in Y_n\\ h(\lambda)\ne 1}} U_\lambda^{\oplus m_\lambda},$$

where $U_{\text{trivial}} = U_{\square} = U_{\square\square} = \ldots$ is the trivial representation. Write

$$Y^* = \bigcup_{n\in\mathbb{N}} \{\lambda;\ \lambda\in Y_n;\ h(\lambda)\ne 1\}.$$

Now recall (3):

$$
\begin{aligned}
E &= \mathbf{BRep}(\textstyle\prod_n S_n)(\mathscr{H},\mathscr{H}) \\
&\cong \mathbf{BRep}(\textstyle\prod_n S_n)(U_{\text{trivial}}^{\oplus\omega} \oplus \bigoplus_{\substack{n\in\mathbb{N}\\ \lambda\in Y_n\\ h(\lambda)\neq 1}} U_\lambda^{\oplus m_\lambda}, U_{\text{trivial}}^{\oplus\omega} \oplus \bigoplus_{\substack{n\in\mathbb{N}\\ \lambda\in Y_n\\ h(\lambda)\neq 1}} U_\lambda^{\oplus m_\lambda}).
\end{aligned}
$$

Using Schur's lemma and the fact that $\oplus$ is a biproduct, we derive

$$
\begin{aligned}
E &\cong \mathbf{BRep}(\textstyle\prod_n S_n)(U_{\text{trivial}}^{\oplus\omega}, U_{\text{trivial}}^{\oplus\omega}) \\
&\qquad \oplus \mathbf{BRep}(\textstyle\prod_n S_n)(\bigoplus_{\lambda\in Y^*} U_\lambda^{\oplus m_\lambda}, \bigoplus_{\lambda\in Y^*} U_\lambda^{\oplus m_\lambda}) \\
&\cong B(\ell^2) \oplus \mathbf{BRep}(\textstyle\prod_n S_n)(\bigoplus_{\lambda\in Y^*} U_\lambda^{\oplus m_\lambda}, \bigoplus_{\lambda\in Y^*} U_\lambda^{\oplus m_\lambda}).
\end{aligned}
$$

We have to be a bit more careful for the right-hand summand, since $\bigoplus$ is not a countable biproduct.

$$
\begin{aligned}
&\mathbf{BRep}(\textstyle\prod_n S_n)(\bigoplus_{\lambda\in Y^*} U_\lambda^{\oplus m_\lambda}, \bigoplus_{\lambda\in Y^*} U_\lambda^{\oplus m_\lambda}) \\
&= \left\{ (a_{\lambda\mu});\ \begin{bmatrix} a_{\lambda\mu} \in \mathbf{BRep}(\prod_n S_n)(U_\lambda^{\oplus m_\lambda}, U_\mu^{\oplus m_\mu}); \\ (a_{\lambda\mu}) \in B(\bigoplus_{\lambda\in Y^*} U_\lambda^{\oplus m_\lambda});\ \lambda,\mu \in Y^* \end{bmatrix} \right\} \quad \text{(dfn.)} \\
&= \left\{ (a_{\lambda\lambda});\ \begin{bmatrix} a_{\lambda\lambda} \in \mathbf{BRep}(\prod_n S_n)(U_\lambda^{\oplus m_\lambda}, U_\lambda^{\oplus m_\lambda}); \\ (a_{\lambda\lambda}) \in B(\bigoplus_{\lambda\in Y^*} U_\lambda^{\oplus m_\lambda});\ \lambda \in Y^* \end{bmatrix} \right\} \quad \text{(Schur's lemma)} \\
&= \left\{ (a_{\lambda\lambda});\ \begin{bmatrix} a_{\lambda\lambda} \in \mathbf{BRep}(\prod_n S_n)(U_\lambda^{\oplus m_\lambda}, U_\lambda^{\oplus m_\lambda}); \\ \sup_\lambda \|a_{\lambda\lambda}\| < \infty;\ \lambda \in Y^* \end{bmatrix} \right\} \quad (*\text{, see below}) \\
&\cong \left\{ (a_\lambda);\ \begin{bmatrix} a_\lambda \in M_{m_\lambda} \\ \sup_\lambda \|a_\lambda\| < \infty;\ \lambda \in Y^* \end{bmatrix} \right\} \quad \text{(reindexing)} \\
&\cong \prod_{\lambda\in Y^*} M_{m_\lambda}.
\end{aligned}
$$

Consequently

$$
E \cong B(\ell^2) \oplus \prod_{\lambda\in Y^*} M_{m_\lambda}.
$$

For step $*$, note that the inclusion $\subseteq$ is easy, and the other inclusion is can be carefully checked using the definition of the direct sum and noting the cross terms are zero. We also emphasize that the infinite product should be interpreted for C* or W*-algebras, with the norm bounded (the C*-sum). This is, in general, a strict subalgebra of the infinite product in $\mathbb{C}$-algebras or rings.

Acknowledgments

We would like to thank Sam Staton for suggesting the problem.

The first author has been financially supported by the Netherlands Organisation for Scientific Research (NWO) under TOP-GO grant no. 613.001.013 (The logic of composite quantum systems).

References

[1] Bob Coecke, Chris Heunen & Aleks Kissinger (2014): *Categories of Quantum and Classical Channels*. Quantum Information Processing, pp. 1–31, doi:10.1007/s11128-014-0837-4.

[2] William Fulton & Joe Harris (1991): *Representation Theory*. Graduate Texts in Mathematics 129, Springer Science & Business Media, doi:10.1007/978-1-4612-0979-9.

[3] Ronald L. Graham, Donald E. Knuth & Oren Patashnik (1989): *Concrete Mathematics*. Massachusetts: Addison-Wesley.

[4] G. H. Hardy & E. M. Wright (1999): *An Introduction to the Theory of Numbers*. Oxford.

[5] Michele Pagani, Peter Selinger & Benoit Valiron (2014): *Applying Quantitative Semantics to Higher-order Quantum Computing*. ACM SIGPLAN Notices 49(1), pp. 647–658, doi:10.1145/2535838.2535879.

[6] Srinivasa Ramanujan (1918): *On Certain Trigonometrical Sums and their Applications in the Theory of Numbers*. Trans. Cambridge Philos. Soc 22(13), pp. 259–276.

[7] Peter Selinger (2004): *Towards a Quantum Programming Language*. Mathematical Structures in Computer Science 14(04), pp. 527–586, doi:10.1017/s0960129504004256.

A Computed decompositions

For easy reference, we have computed[4]. the decompositions into matrix algebras of the C*-algebras for unordered pairs, triples and quads for various types.

d	$\yng(2)$	$\yng(1,1)$
2	M_3	$\mathbb{C}$
3	M_6	M_3
4	M_{10}	M_6
5	M_{15}	M_{10}
6	M_{21}	M_{15}
7	M_{28}	M_{21}
8	M_{36}	M_{28}
9	M_{45}	M_{36}
10	M_{55}	M_{45}

(a) unordered pairs

d	$\yng(3)$	$\yng(2,1)$	$\yng(1,1,1)$
2	M_4	M_2	
3	M_{10}	M_8	$\mathbb{C}$
4	M_{20}	M_{20}	M_4
5	M_{35}	M_{40}	M_{10}
6	M_{56}	M_{70}	M_{20}
7	M_{84}	M_{112}	M_{35}
8	M_{120}	M_{168}	M_{56}
9	M_{165}	M_{240}	M_{84}
10	M_{220}	M_{330}	M_{120}

(b) unordered triples

d	$\yng(4)$	$\yng(3,1)$	$\yng(2,2)$	$\yng(2,1,1)$	$\yng(1,1,1,1)$
2	M_5	M_3	$\mathbb{C}$		
3	M_{15}	M_{15}	M_6	M_3	
4	M_{35}	M_{45}	M_{20}	M_{15}	$\mathbb{C}$
5	M_{70}	M_{105}	M_{50}	M_{45}	M_5
6	M_{126}	M_{210}	M_{105}	M_{105}	M_{15}
7	M_{210}	M_{378}	M_{196}	M_{210}	M_{35}
8	M_{330}	M_{630}	M_{336}	M_{378}	M_{70}
9	M_{495}	M_{990}	M_{540}	M_{630}	M_{126}
10	M_{715}	M_{1485}	M_{825}	M_{990}	M_{210}

(c) unordered quads

Table 1: Decompositions into matrix algebras of unordered pairs, triples and quads of various types.

[4] The script used for the computation can be found here: `https://westerbaan.name/~bas/math/bags.py`