How to combine three quantum states

Maris Ozols

Department of Applied Mathematics and Theoretical Physics, University of Cambridge, Cambridge, CB3 0WA, U.K.
February 27, 2017

We devise a ternary operation for combining three quantum states: it consists of permuting the input systems in a continuous fashion and then discarding all but one of them. This generalizes a binary operation recently studied by Audenaert et al. [ADO16] in the context of entropy power inequalities. Our ternary operation continuously interpolates between all such nested binary operations. Our construction is based on a unitary version of Cayley’s theorem: using representation theory we show that any finite group can be naturally embedded into a continuous subgroup of the unitary group. Formally, this amounts to characterizing when a linear combination of certain permutations is unitary.

1 Introduction

A basic result in group theory known as Cayley’s theorem states that every finite group $G$ is isomorphic to a subgroup of the symmetric group. In other words, the elements of $G$ can be faithfully represented by permutation matrices of size $|G| \times |G|$. This gives a natural embedding of $G$ in the symmetric group $S_n$ on $n = |G|$ elements, known as the regular representation of $G$.

Since permutation matrices are unitary, one might ask whether the resulting subgroup of $S_{|G|}$ can be further extended to a continuous subgroup of the unitary group $U(|G|)$. Such extension would allow to treat the otherwise discrete group $G$ as continuous (e.g., it would allow to perturb the elements of $G$ and continuously interpolate between them in a meaningful sense).

To illustrate this, consider the simplest non-trivial example, namely, the finite group $\mathbb{Z}_2$. This group has two elements which, according to Cayley’s theorem, can be represented by $2 \times 2$ permutation matrices as $I := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Interestingly, the complex linear combination

$$U(\varphi, \alpha) := e^{i\varphi} \begin{pmatrix} \cos \alpha & i \sin \alpha \\ i \sin \alpha & \cos \alpha \end{pmatrix}$$

(1)

of $I$ and $X$ is unitary for any $\varphi, \alpha \in [0, 2\pi)$. Note that $U(0, 0) = I$ and $U(3\pi/2, \pi/2) = X$, so by changing $\varphi$ and $\alpha$ we can continuously interpolate between the two original matrices $I$ and $X$ that represent $\mathbb{Z}_2$. In fact, $U(\varphi, \alpha)U(\varphi', \alpha') = U(\varphi + \varphi', \alpha + \alpha')$, so the matrices $U(\varphi, \alpha)$ themselves form a group—a continuous two-parameter subgroup of $U(2)$.

1.1 Summary and main contributions

One of our main mathematical contributions is a generalization of the above idea to any finite group $G$: using representation theory, we characterize when a complex linear combination of matrices from the regular representation of $G$ is unitary (see Theorem 7). Equivalently, this characterizes the intersection of $U(|G|)$ and $\mathbb{C}[G]$, where $\mathbb{C}[G]$—also known as the group algebra of $G$—consists of all formal complex linear combinations of elements of $G$. As a consequence, any finite group $G$ can be naturally embedded into a continuous subgroup of the unitary group $U(|G|)$. This subgroup is isomorphic to a direct sum

Maris Ozols: marozols@gmail.com, http://marozols.com
of smaller unitary groups—one copy of \( U(d_r) \) for each irreducible representation \( \tau \) of \( G \), where \( d_r \) is the dimension of \( \tau \) (see Corollary 8).

We apply this result in quantum information theory by introducing a ternary operation that combines three quantum states. Our operation generalizes a similar binary operation studied recently in the context of entropy power inequalities [ADO16] and quantum algorithms [LMR14, KLL+16]. This binary operation can be regarded as a qudit analogue of a beam splitter with two input and two output ports (with one of the outputs immediately discarded). Similarly, our ternary operation is an analogue of a three-input and three-output beam splitter (with two of the outputs discarded).

More formally, the general operation consists of applying a joint unitary transformation \( U \) on all three input states, followed by discarding all output systems except the first. We require the unitary \( U \) to be a complex linear combination of three-qudit permutations, thus guaranteeing that the overall operation is covariant, i.e., commutes with any local basis change that is applied simultaneously to all three systems. To characterize such unitaries \( U \), we use the above group-theoretic result with \( G = S_3 \) where \( S_3 \) denotes the symmetric group on three elements (see Corollary 9).

By employing graphical tensor network notation, we derive a general expression for the output state in Section 2.4, and then explicitly parametrize it in Section 4.2 using the irreducible representations of \( S_3 \). In Section 4.4, we derive alternative parametrizations that provide further insight into our operation.

In particular, in Section 5.3 we relate the parameters to those of a four-bar linkage mechanism.

Using these insights, we show how nested binary operations (i.e., ones that combine the input states, two at a time) are special cases of our ternary operation (see Lemma 11). We also characterize the number of output state orbits when the output weights are fixed (there can be either 1 or 2 continuous one-parameter orbits, see Proposition 12). Finally, in Section 5.4 we investigate the uniform combination where all states appear with equal weights in the output.

### 1.2 The partial swap operation

Ability to make discrete groups continuous has an interesting application to quantum information. If we apply our construction to the symmetric group \( S_n \) (see Corollary 8), \( S_3 \) is the identity matrix and \( S_2 \) is a \( d \times d \) permutation matrices \( I \) and \( S \), where \( I \) is the identity matrix and \( S(i)|j\rangle := |j|\rangle |i\rangle \), for all \( i,j \in \{1,\ldots,d\} \), is the swap operation. Making this representation continuous would allow to interpolate between these two operations and thus swap two quantum systems in a continuous fashion. This idea was exactly the starting point of [ADO16] (see also [LMR14, KLL+16] where it has been explored in the context of quantum algorithms).

Following [ADO16], we define the partial swap operation \( U_\lambda \in U(d^2) \) for \( \lambda \in [0,1] \) as the following linear combination of the identity \( I \) and the two-qudit swap \( S \):

\[
U_\lambda := \sqrt{\lambda} I + i \sqrt{1-\lambda} S
\]

(2)

This can easily be verified to be unitary. In fact, \( U_\lambda \) is very similar to \( U(\varphi,\alpha) \) in eq. (1), except we ignore the global phase \( e^{i\varphi} \) and take only one sector of the unit circle corresponding to \( \alpha \in [0,\pi/2] \). Note also that \( U_0 = i S \) rather than \( S \); however, this global phase mismatch will be unimportant.

Let \( D(d) \) denote the set of all \( d \times d \) density matrices or qudit states. Given two states \( \rho_1, \rho_2 \in D(d) \), we can combine them using the partial swap as follows:

\[
\rho_1 \boxplus_\lambda \rho_2 := \text{Tr}_2 \left[ U_\lambda (\rho_1 \otimes \rho_2) U_\lambda^\dagger \right]
\]

(3)

where \( \lambda \in [0,1] \) and \( \text{Tr}_2 \) denotes the partial trace over the second system. With some tricks (see Section 2.4), eq. (3) can be expanded as

\[
\rho_1 \boxplus_\lambda \rho_2 := \lambda \rho_1 + (1-\lambda) \rho_2 + \sqrt{\lambda(1-\lambda)} i [\rho_2, \rho_1]
\]

(4)
where \([A, B] := AB - BA\) denotes the commutator of \(A\) and \(B\). Note that \(\rho_1 \boxplus \rho_2 = \rho_2\) and \(\rho_1 \boxplus \rho_2 = \rho_1\). Moreover, if the two states commute, i.e., \([\rho_2, \rho_1] = 0\), then \(\rho_1 \boxplus \rho_2 = \lambda \rho_1 + (1 - \lambda) \rho_2\) is just a convex combination of the two states.

The operation for combining two states obeys some interesting properties. For example, it is covariant under any unitary change of basis. That is, for any covariant \(U\),

\[
(V \rho_1 V^\dagger) \boxplus (V \rho_2 V^\dagger) = V(\rho_1 \boxplus \rho_2) V^\dagger.
\]

Another, less obvious property is a quantum analogue of the entropy power inequality [ADO16]. To state it in full generality, consider a function \(f : \mathcal{D}(d) \rightarrow \mathbb{R}\). We say that \(f\) is concave if

\[
f(\lambda \rho + (1 - \lambda) \sigma) \geq \lambda f(\rho) + (1 - \lambda) f(\sigma)
\]

for any \(\lambda \in [0, 1]\) and \(\rho, \sigma \in \mathcal{D}(d)\), and symmetric if \(f(\rho)\) depends only on the eigenvalues of \(\rho\) and is symmetric in them (a simple example of a function \(f\) satisfying these properties is the von Neumann entropy). The following result was originally obtained in [ADO16] (see also [CLL16] for a very elegant alternative proof).

**Theorem 1** ([ADO16]). Let \(d \geq 2\), \(\rho, \sigma \in \mathcal{D}(d)\), \(\lambda \in [0, 1]\), and \(\rho \boxplus \lambda \sigma\) be as in eq. (4). If \(f\) is concave and symmetric then

\[
f(\rho \boxplus \lambda \sigma) \geq \lambda f(\rho) + (1 - \lambda) f(\sigma).
\]

Motivated by this result, our goal is to generalize the partial swap operation to any number of systems. The rest of this paper is devoted to obtaining such generalization and using it to derive an analogue of eq. (4) for three states. Proving an analogue of Theorem 1 for this generalization is left as an open problem.

### 1.3 The most general way of combining two states

Before we attempt to generalize eq. (4), it is worthwhile first checking whether \(U_\lambda\) in eq. (2) is actually the most general unitary matrix that can be expressed as a complex linear combination of \(I\) and \(S\). As it turns out, up to an overall global phase and the sign of \(i\), this is indeed the case.

**Proposition 2.** Let \(z_1, z_2 \in \mathbb{C}\) and \(U := z_1 I + z_2 S\) where \(S\) swaps two qudits \((d \geq 2)\). Then \(U\) is unitary if and only if \(z_1 = e^{i\varphi} \sqrt{\lambda}\) and \(z_2 = \pm i e^{i\varphi} \sqrt{1 - \lambda}\) for some \(\lambda \in [0, 1]\) and \(\varphi \in [0, 2\pi]\). In other words,

\[
U = e^{i\varphi} (\sqrt{\lambda} I \pm i \sqrt{1 - \lambda} S).
\]

**Proof.** If \(U := z_1 I + z_2 S\) for some \(z_1, z_2 \in \mathbb{C}\) then

\[
UU^\dagger = (z_1 \bar{z}_1 + z_2 \bar{z}_2) I + (z_1 \overline{z}_2 + \bar{z}_1 z_2) S.
\]

Since \(I\) and \(S\) are linearly independent and we want \(UU^\dagger = I\), we equate the two coefficients to 1 and 0, respectively. This gives us

\[
|z_1|^2 + |z_2|^2 = 1 \quad \text{and} \quad z_1 \overline{z}_2 = -\overline{z}_1 z_2.
\]

From the first equation, \(z_1 = e^{i\varphi_1} \sqrt{\lambda}\) and \(z_2 = e^{i\varphi_2} \sqrt{1 - \lambda}\) for some \(\lambda \in [0, 1]\) and \(\varphi_1, \varphi_2 \in [0, 2\pi]\). The second equation says that \(z_1 \overline{z}_2\) is purely imaginary. Thus \(e^{i(\varphi_1 - \varphi_2)} = \pm i\), which is equivalent to \(e^{i\varphi_2} = \pm i e^{-i\varphi_1}\). In other words, we can take \(e^{i\varphi_1} := e^{i\varphi}\) and \(e^{i\varphi_2} := \pm i e^{i\varphi}\) for some \(\varphi \in [0, 2\pi]\). The reverse direction follows trivially by plugging in the values of \(z_1\) and \(z_2\) in eq. (10). \(\square\)

Since the map in eq. (3) involves conjugation by \(U\), the global phase \(e^{i\varphi}\) in eq. (8) is irrelevant and we only have the freedom of choosing the sign in front of \(i\). Up to the sign, eq. (2) indeed provides the most general unitary for our purpose. To account for the two possible signs, we define

\[
\rho_1 \boxplus \lambda \rho_2 := \lambda \rho_1 + (1 - \lambda) \rho_2 + \sqrt{\lambda(1 - \lambda)} i [\rho_2, \rho_1],
\]

\[
\rho_1 \boxplus \lambda \rho_2 := \lambda \rho_1 + (1 - \lambda) \rho_2 - \sqrt{\lambda(1 - \lambda)} i [\rho_2, \rho_1].
\]
These two operations are related as follows:

\[ \rho_1 \boxplus_\lambda \rho_2 = \rho_2 \boxplus_{1-\lambda} \rho_1. \]  

(13)

Alternatively, one can introduce a parameter \( t \in [0, \pi] \) such that \(|\cos t| = \sqrt{\lambda}\) and \(|\sin t| = \sqrt{1-\lambda}\). Then the two branches given by eqs. (11) and (12) can be combined into a single expression:

\[ (\cos t)^2 \rho_1 + (\sin t)^2 \rho_2 + \cos t \sin t \, i[\rho_2, \rho_1]. \]

(14)

2 Generalization to three states

Now that we fully understand the case of two states, let us investigate how to combine three states. While it is not immediately obvious how to proceed, one simple idea is to combine them in an iterative manner by nesting the original operation. This turns out to preserve some of the nice properties of the original operation. But it is not fully satisfying, since different nesting orders generally lead to different outputs. This ambiguity motivates the introduction of a more general ternary operation that combines all three states at once in a more symmetric fashion. However, before we do this, it is still worthwhile to work out nesting in more detail—this will highlight some of the issues that will appear later and will also serve as a useful reference to come back to once we have the general operation.

2.1 A nested generalization

A straightforward way of generalizing eq. (4) to more systems is by feeding the output state into another operation of the same kind. For example, take \( a, a' \in [0, 1] \) and consider

\[ \rho_1 \boxplus_a (\rho_2 \boxplus_{a'} \rho_3) = a \rho_1 + (1-a) (\rho_2 \boxplus_{a'} \rho_3) + \sqrt{a(1-a)} \, i[\rho_2 \boxplus_{a'} \rho_3, \rho_1] \]

(15)

\[ = a \rho_1 + (1-a) \left( a' \rho_2 + (1-a') \rho_3 + \sqrt{a'(1-a')} \, i[\rho_3, \rho_2] \right) \]

(16)

\[ + \sqrt{a(1-a)} \, i \left[ a' \rho_2 + (1-a') \rho_3 + \sqrt{a'(1-a')} \, i[\rho_3, \rho_2], \rho_1 \right] \]

(17)

\[ = a \rho_1 + (1-a) a' \rho_2 + (1-a)(1-a') \rho_3 \]

(18)

\[ + (1-a) \sqrt{a'(1-a')} \, i[\rho_3, \rho_2] \]

(19)

\[ + \sqrt{a(1-a)} \, a \rho_1 \]

(20)

\[ + \sqrt{a(1-a)} \, a' \rho_2 \]

(21)

\[ + \sqrt{a(1-a)} \, \sqrt{a'(1-a')} \, i[i[\rho_3, \rho_2], \rho_1]. \]

(22)

One can easily check that this nested operation inherits the covariance property (see eq. (5)) of the original operation. Moreover, it also obeys a simple generalization of inequality (7). Indeed, it follows trivially from Theorem 1 that

\[ f(\rho_1 \boxplus_a (\rho_2 \boxplus_{a'} \rho_3)) \geq a f(\rho_1) + (1-a) f(\rho_2 \boxplus_{a'} \rho_3) \]

(23)

\[ \geq a f(\rho_1) + (1-a) a' f(\rho_2) + (1-a)(1-a') f(\rho_3), \]

(24)

for any symmetric and concave function \( f : \mathcal{D}(d) \to \mathbb{R} \).

However, there is no reason why one should single out this particular way of combining three states. Indeed, there are other nested combinations, such as

\[ (\rho_1 \boxplus_b \rho_2) \boxplus_{b'} \rho_3 = b' b \rho_1 + b'(1-b) \rho_2 + (1-b') \rho_3 + \cdots \]

(25)

for some \( b, b' \in [0, 1] \). Here the omitted terms are similar to eqs. (19) to (22), except for the double commutator which in this case is \( i[\rho_3, i[\rho_2, \rho_1]] \), thus making the expression different from the one

---

4
above. Since there are several other nested ways of combining three states, it is not clear which of them, if any, should be preferred.

Considering this, it is desirable to have a ternary operation that treats each of the input states in the same way and combines them all at once. Note that the coefficients

\[(a, (1 - a)a', (1 - a)(1 - a')) \quad \text{and} \quad (b'b', b'(1 - b), 1 - b')\]  

in front of the states \(\rho_1, \rho_2, \rho_3\) in eqs. (18) and (25) are probability distributions. It is thus natural to demand the combined state to be of the form

\[p_1\rho_1 + p_2\rho_2 + p_3\rho_3 + \cdots\]  

for some probability distribution \((p_1, p_2, p_3)\), where—unlike in eq. (22)—all three states are treated symmetrically in the omitted higher-order terms (in particular, the third-order terms).

### 2.2 Twelve nested ways of combining three states

We can use eqs. (11) and (12) to work out all possible nested ways of combining three states. Because of relation (13), there are exactly 12 different nested combinations:

\[
\begin{align*}
\rho_1 \Box_a (\rho_2 \Box_{a'} \rho_3) \\
\rho_2 \Box_b (\rho_3 \Box_{b'} \rho_1) \\
\rho_3 \Box_c (\rho_1 \Box_{c'} \rho_2)
\end{align*}
\]

where each \(\Box\) can independently be replaced by either \(\Box\) or \(\Box\). In general, these all twelve expressions are different. However, if we choose the parameters so that

\[
(p_1, p_2, p_3) = (a, a'(1 - a), (1 - a')(1 - a)) = ((1 - b')(1 - b), b', b'(1 - b)) = (c'(1 - c), (1 - c')(1 - c), c),
\]

for some probability distribution \((p_1, p_2, p_3)\), we can at least guarantee that all twelve expressions begin with the same convex combination \(p_1\rho_1 + p_2\rho_2 + p_3\rho_3 + \cdots\). Our goal is to obtain a more general ternary operation that continuously interpolates between these twelve expressions.

### 2.3 Combining \(n\) states at once

Recall from eq. (2) that \(U_\lambda\) is a linear combination of two-qudit permutation matrices. One way of generalizing this to \(n\) systems is as follows:

\[
(p_1, \ldots, p_n) \mapsto \text{Tr}_{2,\ldots,n} [U(p_1 \otimes \cdots \otimes p_n)U^\dagger],
\]

where \(p_1, \ldots, p_n \in D(d)\) are qudit states, \(\text{Tr}_{2,\ldots,n}\) denotes the partial trace over all systems but the first, and the unitary matrix \(U \in U(d^n)\) is a linear combination of all \(n!\) permutations that act on \(n\) qudits. The goal of this paper is to develop a better understanding of this special type of unitaries and the corresponding map resulting from eq. (34). Here we particularly focus on the \(n = 3\) case and leave it as an open problem to work out the details for general \(n\).

### 2.4 Graphical notation for evaluating partial traces

Let us work out the details of eq. (34) for \(n = 3\). Let \(\rho_1, \rho_2, \rho_3 \in D(d)\) and define

\[
\rho := \text{Tr}_{2,3} [U(\rho_1 \otimes \rho_2 \otimes \rho_3)U^\dagger]
\]
for some unitary matrix $U \in U(d^3)$ such that

$$U := \sum_{i=1}^{6} z_i Q_i,$$

(36)

where $z_i \in \mathbb{C}$ and each $Q_i \in U(d^3)$ is one of the six permutations that act on three qudits. We can represent them using the following graphical notation (see [WBC15] for more details):

$$Q_1 := \begin{array}{c} \infty \end{array}, \quad Q_2 := \begin{array}{c} \infty \end{array}, \quad Q_3 := \begin{array}{c} \infty \end{array}, \quad Q_4 := \begin{array}{c} \infty \end{array}, \quad Q_5 := \begin{array}{c} \infty \end{array}, \quad Q_6 := \begin{array}{c} \infty \end{array}$$

(37)

One can easily recover the matrix representation of each $Q_i$ from this pictorial notation. For example,

$$Q_2(|\psi_1\rangle \otimes |\psi_2\rangle \otimes |\psi_3\rangle) = \begin{array}{c} \infty \end{array} = |\psi_2\rangle \otimes |\psi_3\rangle \otimes |\psi_1\rangle,$$

(38)

for any $|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle \in \mathbb{C}^d$, which is enough to determine all $d^3 \times d^3$ entries of the matrix $Q_2$.

The diagrams of $Q_i$ can be composed in a natural way and this operation is compatible with matrix multiplication (in fact, the diagrams as well as the matrices form a group). For example,

$$Q_4 Q_5 = \begin{array}{c} \infty \end{array} = Q_2.$$

(39)

Inverse permutations can be found by reversing the diagram:

$$Q_2^\dagger = \begin{array}{c} \infty \end{array} = Q_3.$$

(40)

Except for $Q_2$ and $Q_3$, which are inverses of each other, all other $Q_i$’s are self-inverse, i.e., $Q_i^\dagger = Q_i$ when $i \notin \{2, 3\}$. Equation (38) extends easily to mixed states too—the subsystems of a product state are now permuted under the conjugation by $Q_i$. For example,

$$Q_2(\rho_1 \otimes \rho_2 \otimes \rho_3) Q_2^\dagger = \begin{array}{c} \infty \end{array} = \begin{array}{c} \infty \end{array} = \rho_2 \otimes \rho_3 \otimes \rho_1.$$

(41)

Using this pictorial representation, we would like to expand $U$ on both sides of eq. (35) and obtain an explicit formula for the output state $\rho$ in terms of the input states $\rho_k$ and the coefficients $z_i$. This requires computing the matrices

$$\xi_{ij} := \text{Tr}_{2,3}[z_i Q_i (\rho_1 \otimes \rho_2 \otimes \rho_3) \tilde{z}_j Q_j^\dagger],$$

(42)

for each combination of $i, j \in \{1, \ldots, 6\}$. This daunting task becomes much more straightforward using the graphical notation for the partial trace [WBC15]. For example,

$$\xi_{11} = z_1 \tilde{z}_1 \text{Tr}_{2,3} \left[ \begin{array}{c} 1 \end{array} \right] = z_1 \tilde{z}_1 \left[ \begin{array}{c} 1 \end{array} \right] = z_1 \tilde{z}_1 \rho_1 \text{Tr} \rho_2 \text{Tr} \rho_3,$$

(43)

$$\xi_{41} = z_4 \tilde{z}_1 \text{Tr}_{2,3} \left[ \begin{array}{c} 1 \end{array} \right] = z_4 \tilde{z}_1 \left[ \begin{array}{c} 1 \end{array} \right] = z_4 \tilde{z}_1 \rho_1 \text{Tr} (\rho_2 \rho_3),$$

(44)

$$\xi_{51} = z_5 \tilde{z}_1 \text{Tr}_{2,3} \left[ \begin{array}{c} 1 \end{array} \right] = z_5 \tilde{z}_1 \left[ \begin{array}{c} 1 \end{array} \right] = z_5 \tilde{z}_1 \rho_2 \rho_1 \text{Tr} \rho_3,$$

(45)

$$\xi_{21} = z_2 \tilde{z}_1 \text{Tr}_{2,3} \left[ \begin{array}{c} 1 \end{array} \right] = z_2 \tilde{z}_1 \left[ \begin{array}{c} 1 \end{array} \right] = z_2 \tilde{z}_1 \rho_2 \rho_3 \rho_1.$$
We begin by first answering Q1, which will require some representation theory. Particularly relevant to us is reference [Chi13] that provides a very concise introduction to representation theory and Fourier analysis of non-abelian groups. For more background on representation theory of finite groups, see the standard reference [Ser12].

The remaining cases are similar and are summarized in Fig. 1.

We can find the resulting state \( \rho = \sum_{i,j=1}^{6} \xi_{ij} \), defined in eq. (35), by putting all 36 terms together:

\[
\begin{align*}
\rho = & \left( |z_1|^2 + |z_4|^2 + 2 \Re(z_1z_4) \Tr(\rho_3\rho_3) \right) \rho_1 \\
& + \left( |z_2|^2 + |z_5|^2 + 2 \Re(z_2z_5) \Tr(\rho_3\rho_1) \right) \rho_2 \\
& + \left( |z_3|^2 + |z_6|^2 + 2 \Re(z_3z_6) \Tr(\rho_1\rho_2) \right) \rho_3 \\
& + (z_1\z_3 + z_4\z_2) \rho_1\rho_2 + \text{c.t.} \\
& + (z_2\z_6 + z_3\z_3) \rho_2\rho_3 + \text{c.t.} \\
& + (z_3\z_4 + z_6\z_1) \rho_3\rho_1 + \text{c.t.} \\
& + (z_2\z_1 + z_5\z_4) \rho_2\rho_3\rho_1 + \text{c.t.} \\
& + (z_3\z_2 + z_6\z_5) \rho_3\rho_1\rho_2 + \text{c.t.} \\
& + (z_1\z_3 + z_4\z_6) \rho_1\rho_2\rho_3 + \text{c.t.} \\
\end{align*}
\]

where \text{c.t.} stands for the conjugate transpose of the previous term.

### 2.5 Unitarity and independence constraints

Before we can call eq. (47) a generalization of eq. (4), we need to answer the following two questions:

Q1. **Unitarity:** Under what constraints on the coefficients \( z_i \in \mathbb{C} \) is the matrix \( U \) in eq. (36) unitary?

Q2. **Independence:** Are additional constraints needed to make the \( \Tr(\rho_i\rho_j) \) terms in eq. (47) vanish?

We need to demand the unitarity of \( U \) since we want \( \rho \) to be a valid quantum state—this is very natural considering eq. (35). Note that Proposition 2 already answers Q1 for \( n = 2 \). We will answer Q1 in full generality using representation theory: Corollary 9 characterizes, for any \( n \geq 1 \), when a linear combination \( U := \sum_{\pi \in S_n} z_{i \pi} Q_{\pi} \) is unitary.

The reason for asking Q2 is because we would like to control the “amount” of each \( \rho_i \) in the output state. This is important in the context of inequality (7), which borrows the coefficients \( \lambda \) and \( 1 - \lambda \) directly from eq. (4). Inspired by this, we would also like the coefficients in eq. (47)—especially, those of the first-order terms \( \rho_i \)—to be independent of the states themselves. When \( n = 2 \), this happens automatically, see eq. (4), and leads to the particularly simple form of inequality (7). For \( n = 3 \), however, eq. (47) has an additional \( \Tr(\rho_i\rho_j) \) term within each coefficient of \( \rho_i \). As we will see, these terms survive the unitarity constraint from Q1, so we can remove them only by demanding directly that

\[
\text{Re}(z_1z_4) = \text{Re}(z_2z_5) = \text{Re}(z_3z_6) = 0.
\]

This turns the first-order terms of eq. (47) into a linear (in fact, a convex) combination of \( \rho_i \), just like in eq. (4) for \( n = 2 \). While eq. (48) might seem a bit arbitrary, it can be imposed in a fairly natural way (see Section 4.3) and leads to some further nice structure in eq. (47) (see Section 5.1).

### 3 When is a linear combination of permutations unitary?

We begin by first answering Q1, which will require some representation theory.
Figure 1: Tensor contraction diagrams for computing $\xi_{ij} := \text{Tr}_{2,3}[Q_i(\rho_1 \otimes \rho_2 \otimes \rho_3)Q_j^\dagger]$ for each pair of three qudit permutations $Q_i$ (rows) and $Q_j^\dagger$ (columns), for $i \geq j$. By combining all 36 terms we obtain eq. (47).
3.1 Background on representation theory

Let $U(d)$ denote the set of all $d \times d$ unitary matrices. A $d$-dimensional representation of a finite group $G$ is a map $\tau : G \to U(d)$ such that $\tau(gh) = \tau(g)\tau(h)$ for all $g, h \in G$. We will always use $e$ to denote the identity element of $G$. Note that $\tau(e) = I_d$, the $d \times d$ identity matrix, and $\tau(g^{-1}) = \tau(g)\dagger$. We call $d$ the dimension of the representation $\tau$.

Let $S_n$ denote the symmetric group consisting of all $n!$ permutations acting on $n$ elements. We write $\pi(i) = j$ to mean that permutation $\pi \in S_n$ maps $i$ to $j$, and we write $\pi^{-1}$ to denote the inverse permutation of $\pi$. The following are four different representations of the symmetric group (two of them, $Q_\pi$ and $L_\pi$, will play an important role later in the paper).

**Example (Representations of $S_n$).** The symmetric group $S_n$ can be represented by permutation matrices in several different ways. In each case we write down how the matrix associated to permutation $\pi \in S_n$ acts in the standard basis:

- **natural representation** $P_\pi \in U(n)$:
  $$P_\pi : |i\rangle \mapsto |\pi(i)\rangle, \quad \forall i \in \{1, \ldots, n\};$$

- **tensor representation** $Q_\pi \in U(d^n)$:
  $$Q_\pi : |i_1\rangle \otimes \cdots \otimes |i_n\rangle \mapsto |\pi^{-1}(i_1)\rangle \otimes \cdots \otimes |\pi^{-1}(i_n)\rangle, \quad \forall i_1, \ldots, i_n \in \{1, \ldots, d\};$$

- **left regular and right regular representations** $L_\pi, R_\pi \in U(|S_n|)$:
  $$L_\pi : |\sigma\rangle \mapsto |\pi\sigma\rangle, \quad \forall \sigma \in S_n, \quad (51)$$
  $$R_\pi : |\sigma\rangle \mapsto |\sigma\pi^{-1}\rangle, \quad \forall \sigma \in S_n. \quad (52)$$

We call $d$ the local dimension of the tensor representation (we will typically require that $d \geq n$).

Note that for the regular representations, the standard basis of the underlying space is labeled by permutations themselves, so the space has $n!$ dimensions: $\mathbb{C}^{S_n} \cong \mathbb{C}^{n!}$. Finally, note that the regular representations can be defined for any finite group $G$ in a similar manner.

Since $Q_\pi$ will play an important role later, let us verify that it is indeed a representation of $S_n$. First, note that

$$Q_\pi \bigotimes_{i=1}^{n} |\psi_i\rangle = \bigotimes_{i=1}^{n} |\psi_{\pi^{-1}(i)}\rangle = \bigotimes_{i=1}^{n} |\phi_i\rangle$$

where $|\phi_i\rangle := |\psi_{\pi^{-1}(i)}\rangle$. Following the same rule, we see that

$$Q_\sigma \bigotimes_{i=1}^{n} |\phi_i\rangle = \bigotimes_{i=1}^{n} |\phi_{\sigma^{-1}(i)}\rangle = \bigotimes_{i=1}^{n} |\psi_{\pi^{-1}(\sigma^{-1}(i))}\rangle = \bigotimes_{i=1}^{n} |\psi_{(\sigma\pi)^{-1}(i)}\rangle. \quad (54)$$

In other words, $Q_\sigma Q_\pi$ acts in exactly the same way as $Q_{\sigma\pi}$.

3.2 From permutations to unitaries: the importance of the left regular representation

Consider the following linear combination:

$$U := \sum_{\pi \in S_n} z_\pi Q_\pi, \quad (55)$$

where $z_\pi \in \mathbb{C}$ and $Q_\pi$ are the matrices from the tensor representation of $S_n$. Can we parametrize in some simple way all coefficient tuples $z := (z_\pi : \pi \in S_n) \in \mathbb{C}^{S_n}$ such that $U$ is unitary simultaneously for all local dimensions $d \geq 1$? We will provide an answer to this question using representation theory.

Let us start by first reducing this problem from the tensor representation $Q_\pi$ to the left regular representation $L_\pi$. As a first step, we need to show that the matrices $L_\pi$ are linearly independent (this holds more generally, i.e., not just for $S_n$ but for any finite group $G$).

\footnote{It would not be a representation if we would use $\pi$ instead of $\pi^{-1}$ on the RHS of eq. (50).}
Proposition 3. For any finite group \( G \), the matrices \( \{L_g : g \in G\} \) have disjoint supports (i.e., locations of non-zero entries) and thus are linearly independent.

Proof. For any \( x, y, g \in G \),

\[
\langle x|L_g|y \rangle = \langle x|gy \rangle = \begin{cases} 1 & \text{if } g = xy^{-1}, \\ 0 & \text{otherwise.} \end{cases}
\] (56)

So, for any fixed \( x \) and \( y \), there is exactly one matrix, namely \( L_{xy^{-1}} \), with a non-zero entry in row \( x \) and column \( y \). Hence, the matrices \( L_g \) have disjoint supports and thus are linearly independent. \( \square \)

Remark. The matrices \( L_g \) form a (non-commutative) association scheme [Ban93]. Their linear span is known as the Bose–Mesner algebra of this scheme. In representation theory, it goes by the name of the group algebra of \( G \) and is denoted by \( \mathbb{C}[G] \). Our Theorem 7 (see below) characterizes all unitary matrices within this algebra.

Example \((G = S_3)\). Because of Proposition 3, any linear combination of the matrices \( L_g \) has a particularly nice structure. For example, if \( G = S_3 \) and we order the permutations according to eq. (37) then

\[
\sum_{k=1}^{6} kL_k = \begin{pmatrix} 1 & 3 & 2 & 4 & 5 & 6 \\ 2 & 1 & 3 & 6 & 4 & 5 \\ 3 & 2 & 1 & 5 & 6 & 4 \\ 4 & 6 & 5 & 1 & 2 & 3 \\ 5 & 4 & 6 & 3 & 1 & 2 \\ 6 & 5 & 4 & 2 & 3 & 1 \end{pmatrix}.
\] (57)

One can easily read off the matrix representation of each \( L_i \) from this.

Let us now show that the matrices \( Q_\pi \) are also linearly independent, when \( d \) is sufficiently large.

Lemma 4. If \( d \geq n \) then \( Q_\pi \cong L_\pi \oplus \tau(\pi) \) for some representation \( \tau \) of \( S_n \), so the matrices \( \{Q_\pi : \pi \in S_n\} \) are linearly independent.

Proof. It suffices to show that \( Q_\pi \) are linearly independent even when restricted to some invariant subspace of \( \mathbb{C}^{dn} \). Let \( |\Psi_\pi\rangle := Q_\pi \otimes_{i=1}^n |i\rangle = \otimes_{i=1}^n |\pi^{-1}(i)\rangle \) (we need \( d \geq n \) for this to make sense). Note that \( Q_\sigma|\Psi_\pi\rangle = Q_\sigma \otimes_{i=1}^n |\pi^{-1}(i)\rangle = \otimes_{i=1}^n |\pi^{-1}(\sigma^{-1}(i))\rangle = \otimes_{i=1}^n |(\pi \sigma)^{-1}(i)\rangle = |\Psi_{\sigma \pi}\rangle \), just like in eq. (54). So \( \mathcal{L} := \text{span}\{|\Psi_\pi\rangle : \pi \in S_n\} \) is an invariant subspace of \( \mathbb{C}^{dn} \) under the action of the tensor representation. The vectors \( |\Psi_\pi\rangle \) have disjoint supports and hence form an orthonormal basis of the subspace \( \mathcal{L} \). Moreover, the tensor representation \( Q_\pi \) acts as the left regular representation \( L_\pi \) in this subspace. In other words,

\[
Q_\pi \cong L_\pi \oplus \tau(\pi)
\] (58)

for some (reducible) representation \( \tau \) acting on the orthogonal complement of \( \mathcal{L} \) in \( \mathbb{C}^{dn} \). According to Proposition 3, the matrices \( \{L_\pi : \pi \in S_n\} \) are linearly independent, so the result follows. \( \square \)

Lemma 5. Let \( z_\pi \in \mathcal{C} \), for each \( \pi \in S_n \). If \( d \geq n \) then \( \sum_{\pi \in S_n} z_\pi Q_\pi \) is unitary if and only if \( \sum_{\pi \in S_n} z_\pi L_\pi \) is unitary (the reverse implication holds for any \( d \geq 1 \)).

Proof. As we noted in the proof of Lemma 4, for \( d \geq n \) there is a subspace \( \mathcal{L} \) of \( \mathbb{C}^{dn} \) where \( Q_\pi \) acts as \( L_\pi \), see eq. (58); this immediately gives the forward implication. For the reverse implication, note that we can decompose any representation of a finite group into a direct sum of its irreducible representations or irreps [Ser12]. If we obtain such decomposition for the left regular representation, a standard result from representation theory says that each irrep will appear at least once in this decomposition [Ser12]. Thus, the unitarity of \( \sum_{\pi \in S_n} z_\pi L_\pi \) is equivalent to the simultaneous unitarity of \( \sum_{\pi \in S_n} z_\pi \tau(\pi) \) for all irreps \( \tau \) of \( S_n \). Since the tensor representation \( Q_\pi \) can also be decomposed as a direct sum of irreps, for any \( d \geq 1 \), we conclude that \( \sum_{\pi \in S_n} z_\pi Q_\pi \) must therefore be unitary. \( \square \)
According to Lemma 5, our problem now reduces to analyzing the left regular representation of $S_n$ and characterizing when $U := \sum_{\pi \in S_n} z_{\pi} L_{\pi}$ is unitary. We will analyze this in the Fourier basis, where the left regular representation decomposes as a direct sum of irreducible representations. This strategy does not rely on any special properties of $S_n$, so we might as well work with an arbitrary finite group $G$ for the sake of generality.

3.3 Fourier transform over finite groups

Recall from [Chi13] that the Fourier transform over a finite group $G$ is the unitary matrix

$$F := \sum_{g \in G} \sum_{\tau \in \hat{G}} \sqrt{\frac{d_{\tau}}{|G|}} \sum_{j,k=1}^{d_{\tau}} \tau(g)_{j,k} \langle \tau, j, k \rangle \langle g |,$$

where $\hat{G}$ denotes the set of irreducible representations of $G$, $d_{\tau}$ is the dimension of irrep $\tau$, and $\tau(g)_{j,k}$ are the matrix elements of $\tau(g)$. The output space of $F$ is labeled by triples $(\tau, j, k)$ and has the same dimension as the input space—indeed, it is a standard result in representation theory that

$$\sum_{\tau \in \hat{G}} d_{\tau}^2 = |G|. \quad (60)$$

One can easily check that $F$ is unitary using the orthogonality of characters [Chi13].

We will need the following standard result from representation theory [Chi13, Ser12]. Let $\hat{L}_g := F L_g F^\dagger$ denote $L_g$ in the Fourier basis. Then

$$\hat{L}_g = \bigoplus_{\tau \in \hat{G}} [\tau(g) \otimes I_{d_{\tau}}] \quad (61)$$

where $I_{d_{\tau}}$ is the $d_{\tau} \times d_{\tau}$ identity matrix. In other words, $\hat{L}_g$ is block-diagonal and contains each irrep $\tau$ the number of times equal to its dimension $d_{\tau}$.

3.4 Characterization of unitary linear combinations

Let us first show a simple preliminary fact. Recall from Proposition 3 that \{\text{\textit{L}}_g : \text{\textit{g}} \in G\} is a linearly independent set. In fact, when properly normalized, these matrices are orthonormal.

**Proposition 6.** For any finite group $G$, the matrices \{\text{\textit{L}}_g/\sqrt{|G|} : \text{\textit{g}} \in G\} are orthonormal with respect to the Hilbert–Schmidt inner product $\langle A, B \rangle := \text{Tr}(A^\dagger B)$.

**Proof.** First, note from eq. (56) that, for any $g \in G$,

$$\text{Tr} L_g = \sum_{h \in G} \langle h | L_g | h \rangle = \sum_{h \in G} \delta_{g, e} = |G| \delta_{g, e}. \quad (62)$$

Thus, for any $a, b \in G$, the corresponding Hilbert–Schmidt inner product is

$$\frac{1}{|G|} \langle L_a, L_b \rangle = \frac{1}{|G|} \text{Tr}(L_a^\dagger L_b) = \frac{1}{|G|} \text{Tr} L_{a^{-1} b} = \delta_{a,b}. \quad (63)$$

Hence the normalized matrices $L_g/\sqrt{|G|}$ are orthonormal. \hfill $\Box$

**Theorem 7.** Let $G$ be a finite group, $L_g$ be its left regular representation, and $z_{\text{\textit{g}}} \in \mathbb{C}$, for each $g \in G$. Then $\sum_{g \in G} z_{\text{\textit{g}}} L_{\text{\textit{g}}}$ is unitary if and only if

$$z_g = \sum_{\tau \in \hat{G}} \frac{d_{\tau}}{|G|} \text{Tr}(\tau(g)^\dagger U_{\tau}), \quad (64)$$

for some choice of $U_{\tau} \in \text{U}(d_{\tau})$, one for each irrep $\tau$ of $G$. 

Proof. Clearly, \( \sum_{g \in G} z_g L_g \) is unitary if and only if \( \sum_{g \in G} z_g \hat{L}_g \) is unitary where

\[
\hat{L}_g = FL_g F^\dagger = \bigoplus_{\tau \in \hat{G}} [\tau(g) \otimes I_{d_{\tau}}] \tag{65}
\]

according to eq. (61). We prefer to work in the Fourier basis, since then all \( \hat{L}_g \) become simultaneously block diagonal and we can write

\[
\sum_{g \in G} z_g \hat{L}_g = \bigoplus_{\tau \in \hat{G}} \left[ \left( \sum_{g \in G} z_g \tau(g) \right) \otimes I_{d_{\tau}} \right]. \tag{66}
\]

This matrix is unitary if and only if each of its blocks is unitary, i.e.,

\[
\sum_{g \in G} z_g \hat{L}_g = \bigoplus_{\tau \in \hat{G}} [U_{\tau} \otimes I_{d_{\tau}}] =: U \tag{67}
\]

for some set of unitaries \( U_{\tau} \in U(d_{\tau}) \). Since \( \mathcal{B} := \{ L_g / \sqrt{|G|} : g \in G \} \) is an orthonormal set, see Proposition 6, so is \( \hat{\mathcal{B}} := \{ FBF^\dagger : B \in \mathcal{B} \} = \{ \hat{L}_g / \sqrt{|G|} : g \in G \} \). Since \( |\hat{\mathcal{B}}| = |G| = \sum_{\tau \in \hat{G}} d_{\tau}^2 \) according to eq. (60), \( \hat{\mathcal{B}} \) is in fact an orthonormal basis for the set of all block matrices that have the same block structure as \( U \) in eq. (67). Thus, we can obtain the coefficients \( z_g \) in the expansion

\[
\frac{U}{\sqrt{|G|}} = \sum_{g \in G} z_g \hat{L}_g \frac{1}{\sqrt{|G|}} \tag{68}
\]

simply by projecting on the corresponding basis vector:

\[
z_g = \left\langle \hat{L}_g \frac{1}{\sqrt{|G|}} , U \frac{1}{\sqrt{|G|}} \right\rangle = \frac{1}{|G|} \text{Tr} \left( \bigoplus_{\tau \in \hat{G}} \left[ (\tau(g))^\dagger U_{\tau} \right] \otimes I_{d_{\tau}} \right) = \sum_{\tau \in \hat{G}} \frac{d_{\tau}}{|G|} \text{Tr}(\tau(g))^\dagger U_{\tau}, \tag{69}
\]

where we substituted eqs. (65) and (67). The reverse implication follows by applying all steps in the reverse order.

As a byproduct of our proof, we observe that all unitary linear combinations \( \sum_{g \in G} z_g L_g \) form a group of their own. According to eq. (67), this group is isomorphic to the direct sum of unitary groups,

\[
\bigoplus_{\tau \in \hat{G}} U(d_{\tau}), \tag{70}
\]

and it contains \( G \) as a subgroup (as represented by the matrices \( L_g \)). Indeed, if we take any \( g \in G \) and, for all irreps \( \tau \in \hat{G} \), set \( U_{\tau} := \tau(g) \) in eq. (64), then \( z_g = 1 \) while all other coefficients vanish (see Proposition 6), reducing the linear combination to \( L_g \). Considering this, we can intuitively think of

\[
\left\{ \sum_{g \in G} z_g L_g \in U(|G|) : z_g \in \mathbb{C} \right\} \tag{71}
\]

as a natural continuous extension of the discrete finite group \( G \).

**Corollary 8** (Unitary version of Cayley’s theorem). Every finite group \( G \) can be extended to a continuous subgroup of the unitary group \( U(|G|) \). This subgroup is isomorphic to \( \bigoplus_{\tau \in \hat{G}} U(d_{\tau}) \), where \( \hat{G} \) is the set of all irreps of \( G \) and \( d_{\tau} \) is the dimension of irrep \( \tau \).

If we specialize Theorem 7 to \( G = S_n \) and apply Lemma 5, we get the following result.

**Corollary 9.** Let \( z_\pi \in \mathbb{C} \), for each \( \pi \in S_n \). If \( d \geq n \) then \( \sum_{\pi \in S_n} z_\pi Q_{\pi} \) is unitary if and only if

\[
z_\pi = \sum_{\tau \in S_n} \frac{d_{\tau}}{n!} \text{Tr}(\tau(\pi))^\dagger U_{\tau}, \tag{72}
\]

for some choice of \( U_{\tau} \in U(d_{\tau}) \), one for each irrep \( \tau \) of \( S_n \) (the reverse implication holds for any \( d \geq 1 \)).
Table 1: All irreducible representations of $S_3$. The matrix elements of $\tau_3$ are not unique but depend on the choice of basis—we provide two simple choices (irreps $\tau_3$ and $\tau'_3$ are isomorphic).

4 How to combine three quantum states?

Let $Q_\pi \in U(d^3)$ denote the matrix that permutes three qudits according to permutation $\pi \in S_3$, see eq. (37). We will now use Corollary 9 to parametrize all tuples of complex coefficients $(z_\pi : \pi \in S_3) \in \mathbb{C}^6$, such that $\sum_{\pi \in S_3} z_\pi Q_\pi$ is a unitary matrix (for all $d \geq 1$). First, we need to work out all irreps of $S_3$.

4.1 The irreducible representations of $S_3$

The symmetric group $S_3$ has three irreducible representations [Ser12]: two 1-dimensional representations (the trivial representation $\tau_1$ and the sign representation $\tau_2$) and a 2-dimensional representation $\tau_3$. Recall that $S_3 \cong D_3$ (the dihedral group), so geometrically $\tau_3$ corresponds to rotations and reflections in 2D that preserve an equilateral triangle (centered at the origin and with one corner pointing along the $x$ axis). These representations are written out explicitly in Table 1. One can easily verify that $\tau_k(\pi\sigma) = \tau_k(\pi)\tau_k(\sigma)$ for all $\pi, \sigma \in S_3$ and $k \in \{1, 2, 3\}$. For example,

$$\tau_3\left(\begin{array}{c} 1 \\ \sqrt{3} \\ 0 \end{array}\right) = \tau_3\left(\begin{array}{c} 1 \\ \sqrt{3} \\ 0 \end{array}\right) \tau_3\left(\begin{array}{c} 1 \\ \sqrt{3} \\ 0 \end{array}\right) = \frac{1}{2}\left(\begin{array}{c} -1 & 0 \\ 0 & 1 \end{array}\right) = \frac{1}{2}\left(\begin{array}{c} -1 & \sqrt{3} \\ \sqrt{3} & 1 \end{array}\right) = \tau_3\left(\begin{array}{c} 0 \\ \omega \sqrt{3} \\ \omega \end{array}\right).$$

\[
\begin{array}{c|cccccc}
\pi & \tau_1(\pi) & \tau_2(\pi) & \tau_3(\pi) & \tau'_3(\pi) \\
\hline
\tau_1(\pi) & 1 & 1 & \chi & \chi & \chi & \chi \\
\tau_2(\pi) & 1 & 1 & 1 & -1 & -1 & -1 \\
\tau_3(\pi) & \left(\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array}\right) & \left(\begin{array}{cc} \frac{1}{2} & -1 \\ \sqrt{3} & -1 \end{array}\right) & \left(\begin{array}{cc} 1 & 0 \\ 0 & -1 \end{array}\right) & \left(\begin{array}{cc} \frac{1}{2} & -1 \\ -\sqrt{3} & 1 \end{array}\right) & \left(\begin{array}{cc} \frac{1}{2} & \sqrt{3} \\ \sqrt{3} & 1 \end{array}\right) \\
\tau'_3(\pi) & \left(\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array}\right) & \left(\begin{array}{cc} \omega & 0 \\ 0 & \omega^2 \end{array}\right) & \left(\begin{array}{cc} \omega^2 & 0 \\ 0 & \omega \end{array}\right) & \left(\begin{array}{cc} 0 & \omega^2 \\ \omega & 0 \end{array}\right) & \left(\begin{array}{cc} 0 & \omega \\ \omega^2 & 0 \end{array}\right) \\
\end{array}
\]

4.2 Parametrizing the general solution for $S_3$

According to Corollary 9, we need to assign one unitary matrix $U_k \in U(d_{\tau_k})$ to each irrep $\tau_k$ of $S_3$. Since the global phase of $\sum_{i=1}^{d-1} z_i Q_i$ has no effect on the output state, we can assume without loss of generality that one of the unitaries $U_k$ is in the special unitary group. We take $U_1, U_2 \in U(1)$ and $U_3 \in SU(2)$, and parametrize these unitaries as follows:

$$U_1 := \left( e^{i\varphi_1} \right), \quad U_2 := \left( e^{i\varphi_2} \right), \quad U_3 := \left( \begin{array}{cc} a & c \\ -\overline{c} & \overline{a} \end{array} \right)$$

where $\varphi_1, \varphi_2 \in [0, 2\pi)$ and $a, c \in \mathbb{C}$ are such that $|a|^2 + |c|^2 = 1$. 

13
We can now use eq. (72) and irreps \( \tau_1, \tau_2, \tau_3 \) from Table 1 to compute the coefficients \( z_1, \ldots, z_6 \):

\[
\begin{align*}
z_1 &= \frac{1}{6} \left[ e^{i\varphi_1} + e^{i\varphi_2} + 4 \Re(a) \right], \\
z_2 &= \frac{1}{6} \left[ e^{i\varphi_1} + e^{i\varphi_2} - 2 \Re(a + \sqrt{3}c) \right], \\
z_3 &= \frac{1}{6} \left[ e^{i\varphi_1} + e^{i\varphi_2} - 2 \Re(a - \sqrt{3}c) \right], \\
z_4 &= \frac{1}{6} \left[ e^{i\varphi_1} - e^{i\varphi_2} + 4i \Im(a) \right], \\
z_5 &= \frac{1}{6} \left[ e^{i\varphi_1} - e^{i\varphi_2} - 2i \Im(a + \sqrt{3}c) \right], \\
z_6 &= \frac{1}{6} \left[ e^{i\varphi_1} - e^{i\varphi_2} - 2i \Im(a - \sqrt{3}c) \right].
\end{align*}
\]

(74) \( \quad \) (75) \( \quad \) (76) \( \quad \) (77) \( \quad \) (78) \( \quad \) (79)

Up to an overall global phase, this parametrizes precisely the set of coefficients for which the following matrix, cf. eq. (57), is unitary:

\[
\sum_{i=1}^{6} z_i L_i = \begin{pmatrix}
z_1 & z_3 & z_2 & z_4 & z_5 & z_6 \\
z_2 & z_1 & z_3 & z_6 & z_4 & z_5 \\
z_3 & z_2 & z_1 & z_6 & z_5 & z_4 \\
z_4 & z_6 & z_5 & z_2 & z_3 & z_1 \\
z_5 & z_4 & z_6 & z_3 & z_1 & z_2 \\
z_6 & z_5 & z_4 & z_2 & z_3 & z_1
\end{pmatrix}.
\]

(80)

Remark. If we insist, in addition to eqs. (74) to (79), that \( |z_1| = \cdots = |z_6| = 1/\sqrt{6} \), we get a 6 × 6 flat unitary—this is also known as a complex Hadamard matrix [TZ06]. Such matrices are relevant to the MUB problem in six dimensions [BBE+07]. Using a computer, one can find a total of 72 discrete solutions \((z_1, \ldots, z_6)\) under the flatness constraint. Unfortunately, the corresponding unitaries appear to be equivalent to the 6 × 6 Fourier matrix. Nevertheless, this method can in principle be used to find flat unitaries of size \(|G| \times |G|\), for any finite group \(G\). It would be interesting to know whether this construction can yield anything beyond what is already known [TZ06].

4.3 Imposing the independence constraints

Recall that eq. (47) involves terms with coefficients \( \Re(z_1 \bar{z}_4), \Re(z_2 \bar{z}_5), \) and \( \Re(z_3 \bar{z}_6) \). We would like to understand when these terms vanish (see Q2 in Section 2.4), since this would ensure that the coefficients are independent of the states.

**Proposition 10.** \( \Re(z_1 \bar{z}_4) = \Re(z_2 \bar{z}_5) = \Re(z_3 \bar{z}_6) = 0 \) if \( \varphi_1 = -\varphi_2 \).

**Proof.** Note from eqs. (74) to (79) that (up to an overall constant of 1/6) each coefficient \( z_i \) has one of the following two forms:

\[
\begin{align*}
u &:= e^{i\varphi_1} + e^{i\varphi_2} + r \cos \alpha, \\
v &:= e^{i\varphi_1} - e^{i\varphi_2} + ir \sin \alpha
\end{align*}
\]

(81) \( \quad \) (82)

for some \( \varphi_1, \varphi_2, \alpha \in [0, 2\pi) \) and \( r \geq 0 \). Furthermore, each \( u \)-type coefficient is paired up with a
corresponding $v$-type coefficient. A straightforward calculation gives

\[
\text{Re}(u\bar{v}) = \text{Re}(u)\text{Re}(v) + \text{Im}(u)\text{Im}(v) \\
= (\cos \varphi_1 + \cos \varphi_2 + r \cos \alpha)(\cos \varphi_1 - \cos \varphi_2) \\
+ (\sin \varphi_1 + \sin \varphi_2)(\sin \varphi_1 - \sin \varphi_2 + r \sin \alpha) \\
= (\cos \varphi_1)^2 - (\cos \varphi_2)^2 + (\cos \varphi_1 - \cos \varphi_2)r \cos \alpha \\
+ (\sin \varphi_1)^2 - (\sin \varphi_2)^2 + (\sin \varphi_1 + \sin \varphi_2)r \sin \alpha \\
= r(\cos(\alpha - \varphi_1) - \cos(\alpha + \varphi_2)).
\]

We can guarantee that $\text{Re}(u\bar{v}) = 0$ irrespectively of the values of $r$ and $\alpha$ by choosing $-\varphi_1 = \varphi_2$. This makes all three terms vanish simultaneously.

Following Proposition 10, we define $\varphi := \varphi_1 = -\varphi_2$. Then eqs. (74) to (79) become:

\[
\begin{align*}
z_1 &= \frac{1}{3} \left[ \cos \varphi + 2 \text{Re}(a) \right], \\
z_2 &= \frac{1}{3} \left[ \cos \varphi - \text{Re}(a + \sqrt{3}c) \right], \\
z_3 &= \frac{1}{3} \left[ \cos \varphi - \text{Re}(a - \sqrt{3}c) \right], \\
z_4 &= \frac{i}{3} \left[ \sin \varphi + 2 \text{Im}(a) \right], \\
z_5 &= \frac{i}{3} \left[ \sin \varphi - \text{Im}(a + \sqrt{3}c) \right], \\
z_6 &= \frac{i}{3} \left[ \sin \varphi - \text{Im}(a - \sqrt{3}c) \right].
\end{align*}
\]

Here we can choose any $\varphi \in [0, 2\pi)$ and $a, c \in \mathbb{C}$ such that $|a|^2 + |c|^2 = 1$. The output state is then obtained by substituting eqs. (88) to (93) in eq. (47).

Unfortunately, the parametrization in eqs. (88) to (93) is somewhat cumbersome. In addition, it has another, more serious drawback: it appears as if there are four degrees of freedom—one from $\varphi$ and three from $a$ and $c$. While it is not obvious from eqs. (88) to (93), one of these degrees of freedom is redundant, since it has no affect on the output state.

4.4 Alternative parametrizations

Due to the shortcomings just discussed, in this section we derive two alternative parametrizations that are much simpler and more insightful. Our derivation is based on eqs. (88) to (93). With an educated guess, however, the same alternative parametrizations can also be derived from scratch without invoking the irreps of $S_3$ at all (see Appendix A).

4.4.1 Parametrization by $\mathbb{C}^3$

It is natural to pair up the coefficients $z_i$ as follows:

\[
\begin{align*}
q_1 &:= z_1 + z_4 = \frac{1}{3}(e^{i\varphi} + 2a), \\
q_2 &:= z_2 + z_5 = \frac{1}{3}(e^{i\varphi} - a - \sqrt{3}c), \\
q_3 &:= z_3 + z_6 = \frac{1}{3}(e^{i\varphi} - a + \sqrt{3}c).
\end{align*}
\]
The coefficients $z_i$ in terms of the new parameters $q_1, q_2, q_3 \in \mathbb{C}$ are expressed as follows:

$$(z_1, z_2, z_3, z_4, z_5, z_6) := (\Re q_1, \Re q_2, \Re q_3, i \Im q_1, i \Im q_2, i \Im q_3).$$  \hfill (95)

With this parametrization, the output state $\rho$ from eq. (47) looks as follows:

$$\rho = |q_1|^2 \rho_1 + |q_2|^2 \rho_2 + |q_3|^2 \rho_3$$ \hfill (96)

$$+ \Im(q_1 \bar{q}_2) i[\rho_1, \rho_2]$$ \hfill (97)

$$+ \Im(q_2 \bar{q}_3) i[\rho_2, \rho_3]$$ \hfill (97)

$$+ \Im(q_3 \bar{q}_1) i[\rho_3, \rho_1]$$ \hfill (97)

$$+ \Re(q_1 \bar{q}_2)(\rho_2 \rho_3 \rho_1 + \rho_1 \rho_3 \rho_2)$$ \hfill (98)

$$+ \Re(q_2 \bar{q}_3)(\rho_3 \rho_1 \rho_2 + \rho_2 \rho_1 \rho_3)$$ \hfill (98)

$$+ \Re(q_3 \bar{q}_1)(\rho_1 \rho_2 \rho_3 + \rho_3 \rho_2 \rho_1)$$ \hfill (98)

where $q_1, q_2, q_3 \in \mathbb{C}$ are subject to the following constraints:

$$|q_1|^2 + |q_2|^2 + |q_3|^2 = 1, \quad |q_1 + q_2 + q_3|^2 = 1.$$  \hfill (99)

To derive these constraints, we solve eq. (94) for the original parameters:

$$e^{i\varphi} = q_1 + q_2 + q_3,$$ \hfill (100)

$$a = q_1 - \frac{1}{2}(q_2 + q_3),$$ \hfill (100)

$$c = \frac{\sqrt{3}}{2}(q_3 - q_2).$$ \hfill (100)

From the first equation we immediately get the second constraint in eq. (99). From the next two equations we get:

$$|a|^2 = |q_1|^2 + \frac{1}{4}(|q_2|^2 + |q_3|^2) - \Re(q_1 \bar{q}_2) - \Re(q_2 \bar{q}_3) + \frac{1}{2} \Re(q_2 \bar{q}_3),$$ \hfill (101)

$$|c|^2 = \frac{3}{4}(|q_2|^2 + |q_3|^2) - \frac{3}{2} \Re(q_2 \bar{q}_3).$$ \hfill (102)

Adding these together gives:

$$1 = |a|^2 + |c|^2 = |q_1|^2 + |q_2|^2 + |q_3|^2 - \Re(q_1 \bar{q}_2) - \Re(q_2 \bar{q}_3) - \Re(q_3 \bar{q}_1).$$ \hfill (103)

However, we already know from the second constraint in eq. (99) that

$$1 = |q_1 + q_2 + q_3|^2 = |q_1|^2 + |q_2|^2 + |q_3|^2 + 2 \Re(q_1 \bar{q}_2) + 2 \Re(q_2 \bar{q}_3) + 2 \Re(q_3 \bar{q}_1).$$ \hfill (104)

Comparing eqs. (103) and (104) we conclude that

$$\Re(q_1 \bar{q}_2) + \Re(q_2 \bar{q}_3) + \Re(q_3 \bar{q}_1) = 0.$$ \hfill (105)

Consequently, constraints (104) and (103) are equivalent to eq. (99). These constraints are also equivalent to unitarity of the three matrices in eq. (73), assuming $\varphi_1 = -\varphi_2 =: \varphi$. Indeed, if we substitute eq. (94) in eq. (99), we recover $|e^{i\varphi}|^2 = 1$ and $|a|^2 + |c|^2 = 1$.

Another way of writing constraints (99) is as follows. If we let

$$|q\rangle := \begin{pmatrix} q_1 \\ q_2 \\ q_3 \end{pmatrix}, \quad |u\rangle := \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$ \hfill (106)

then eq. (99) is equivalent to

$$|\langle q|q\rangle|^2 = 1, \quad |\langle q|u\rangle|^2 = 1/3.$$ \hfill (107)
i.e., \(|q| \in \mathbb{C}^3\) is a unit vector that is mutually unbiased to the uniform superposition \(|u|\).

One advantage of this parametrization is that it makes it more apparent that neither the constraints (107) nor the output state \(\rho\) in eqs. (96) to (98) depend on the global phase of \(|q|\); this feature was not obvious at all from the original parametrization in eqs. (88) to (93). In fact, we can always adjust the global phase of \(|q|\) so that the \(|q_1 + q_2 + q_3|^2 = 1\) constraint from eq. (99) turns into \(q_1 + q_2 + q_3 = 1\). A simplified version of eq. (99) is then
\[
|q_1|^2 + |q_2|^2 + |q_3|^2 = 1,
\]
which makes it very clear that \(|q|\) has only three relevant degrees of freedom. We will explore these constraints further in Section 5.3 and relate them to the so-called four-bar linkage mechanism.

We can make some further observations:

- Due to the first constraint in eq. (108), the first-order terms in eq. (96) form a convex combination of \(\rho_1, \rho_2, \rho_3\). This is analogous to eq. (4) for \(n = 2\).
- If \(|q|\) satisfies eq. (108) then so does its complex conjugate \(|q|^*\). Complex conjugation of \(q_i\)’s preserves eqs. (96) and (98) but flips the signs of the second-order terms in eq. (97).
- Because of eq. (105), the coefficients of the third-order terms in eq. (98) sum to zero. Hence, the third-order terms themselves can be expressed as a linear combination of double commutators (see Section 5.1 for more details).
- If the input states \(\rho_i\) and the coefficients \(q_i\) are permuted according to the same permutation, the output state in eqs. (96) to (98) remains invariant. For cyclic permutations, this is evident form symmetry; it is straightforward to check for transpositions.

4.4.2 Parametrization by a probability distribution and phases

As we just noted, eq. (108) implies that \((|q_1|^2, |q_2|^2, |q_3|^2)\) is a probability distribution. We can highlight this by setting
\[
q_k := e^{i\phi_k} \sqrt{p_k},
\]
for some probability distribution \((p_1, p_2, p_3)\) and some phases \(\phi_1, \phi_2, \phi_3 \in [0, 2\pi)\). Note that
\[
\text{Re}(q_ik_i) = \sqrt{p_ip_j}\cos(\phi_i - \phi_j),
\]
\[
\text{Im}(q_ik_i) = \sqrt{p_ip_j}\sin(\phi_i - \phi_j).
\]

If we further denote the differences between consecutive phases by
\[
\delta_{12} := \phi_1 - \phi_2,
\]
\[
\delta_{23} := \phi_2 - \phi_3,
\]
\[
\delta_{31} := \phi_3 - \phi_1,
\]
we can rewrite eqs. (96) to (98) as follows:
\[
\rho = p_1\rho_1 + p_2\rho_2 + p_3\rho_3
\]
\[
+ \sqrt{p_1p_2} \sin \delta_{12} i[\rho_1, \rho_2]
\]
\[
+ \sqrt{p_2p_3} \sin \delta_{23} i[\rho_2, \rho_3]
\]
\[
+ \sqrt{p_3p_1} \sin \delta_{31} i[\rho_3, \rho_1]
\]
\[
+ \sqrt{p_1p_2} \cos \delta_{12} (p_3\rho_3\rho_1 + \rho_1\rho_3\rho_2)
\]
\[
+ \sqrt{p_2p_3} \cos \delta_{23} (p_3\rho_1\rho_2 + \rho_2\rho_1\rho_3)
\]
\[
+ \sqrt{p_3p_1} \cos \delta_{31} (p_1\rho_2\rho_3 + \rho_3\rho_2\rho_1).
\]
Parameters $p_i$ and $\delta_{ij}$ are subject to the following constraints: $(p_1, p_2, p_3)$ is a probability distribution (i.e., $p_i \geq 0$ and $p_1 + p_2 + p_3 = 1$) and the angles $\delta_{ij}$ satisfy

$$\delta_{12} + \delta_{23} + \delta_{31} = 0, \quad \sqrt{p_1 p_2} \cos \delta_{12} + \sqrt{p_2 p_3} \cos \delta_{23} + \sqrt{p_3 p_1} \cos \delta_{31} = 0. \quad (118)$$

The first constraint is apparent from eqs. (112) to (114), while the second constraint is equivalent to eq. (105). In total, there are three degrees of freedom: two for the distribution $(p_1, p_2, p_3)$ and one for the angles $(\delta_{12}, \delta_{23}, \delta_{31})$. If the distribution $(p_1, p_2, p_3)$ is fixed (and not deterministic), the constraints in eq. (118) yield a one-parameter family of angles $(\delta_{12}, \delta_{23}, \delta_{31})$. This is qualitatively different from the $n = 2$ case where the coefficients of the first-order terms are completely determined by $\lambda$, see eq. (4). Once the parameter $\lambda$ is fixed, only a discrete degree of freedom remains corresponding to the sign in front of the commutator, see Section 1.3.

5 Further observations

In this section we highlight some further features of the operation that combines three states. In particular, we show that the third-order terms can be expressed as a linear combination of double commutators. We also show that the twelve nested compositions discussed in Section 2.2 are special cases of the general operation.

5.1 Double commutators

Let us elaborate more on the meaning of the constraint (105). As mentioned earlier, it has to do with double commutators, i.e., expressions of the form $[1, [2, 3]]$. In what follows, we do not specify the states $\rho_i$ but rather treat them as abstract non-commutative variables. With this convention, for example, $\rho_1$ and $\rho_2$ are always considered to be linearly independent.

Note that there are 6 ways of ordering three states and 2 ways of putting brackets, so there are twelve double commutators in total. However, many of them are identical (such as $[1, [2, 3]]$ and $[[3, 2], 1]$) or differ only by a sign (such as $[1, [2, 3]]$ and $[1, [3, 2]]$). Furthermore, we know from the Jacobi identity that

$$[1, [2, 3]] + [2, [3, 1]] + [3, [1, 2]] = 0. \quad (119)$$

This leaves us with only two linearly independent double commutators. Somewhat arbitrarily, we can choose them as $[1, [2, 3]]$ and $[[1, 2], 3]$. After expanding both of them, we get the following coefficients in front of the six different products of the states $1, 2, 3$:

|     | 123 | 132 | 213 | 231 | 312 | 321 |
|-----|-----|-----|-----|-----|-----|-----|
| $[1, [2, 3]]$ | 1   | -1  | 0   | -1  | 0   | 1   |
| $[[1, 2], 3]$ | 1   | 0   | -1  | 0   | -1  | 1   |
| $x i[1, i[2, 3]] + y i[i[1, 2], 3]$ | $z$ | $x$ | $y$ | $x$ | $y$ | $z$ |

where the last row is a linear combination of the first two rows and $z := -x - y$. In other words,

$$x(213 + 132) + y(312 + 213) + z(123 + 321) = x i[1, i[2, 3]] + y i[i[1, 2], 3] \quad (121)$$

whenever $x + y + z = 0$.

We can use this to simply the third-order terms in eqs. (98) and (117). Indeed, since the coefficients in (98) sum to zero, see eq. (105), we can rewrite (98) as a linear combination of two double commutators:

$$+ \text{Re}(q_1 q_2) i[p_1, i[p_2, p_3]] \quad (122)$$

$$+ \text{Re}(q_2 q_3) i[i[p_1, p_2], p_3].$$

We write $i$ instead of $\rho_i$ for brevity.
Since expression (117) is symmetric, one can also use the above expression with all subscripts cyclically shifted by one or by two (i.e., according to $1 \to 2 \to 3 \to 1$ or its inverse). Alternatively, if we use the parametrization in terms of $p_i$ and $\delta_{ij}$ from Section 4.4.2, we can restate (117) as

$$
\begin{align*}
+ \sqrt{p_1 p_2} \cos \delta_{12} [i[p_1, i[p_2, p_3]]] \\
+ \sqrt{p_2 p_3} \cos \delta_{23} i[i[p_1, p_2], p_3].
\end{align*}
$$

Again, because of the second condition in eq. (118), this expression is invariant under cyclic shifts.

5.2 Relation to nested expressions

It is interesting to know whether the ternary operation can reproduce the 12 nested expressions discussed in Section 2.2 as special cases. More precisely, we would like to know whether, for fixed distribution $(p_1, p_2, p_3)$, the one-parameter family of states described by eqs. (115) to (117), under constraints (118), contains all 12 nested expressions with first-order terms $p_1 \rho_1 + p_2 \rho_2 + p_3 \rho_3$.

For example, consider nested expressions of the form $\rho_1 \Box_a (\rho_2 \Box_{a'} \rho_3)$ where each $\Box$ is either $\bigboxdot$ or $\Box$, see eqs. (11) and (12). Recall from eqs. (16) and (17) that

$$
\rho_1 \Box_a (\rho_2 \Box_{a'} \rho_3) = a \rho_1 \rho_2 \rho_3 + (-1)^s \sqrt{a(1-a)} i[\rho_3, \rho_2], \quad \rho_1 \Box_{a'} (\rho_2 \Box_{a} \rho_3) = a' \rho_1 \rho_2 \rho_3 + (-1)^{s'} \sqrt{a'(1-a')} i[\rho_3, \rho_2],
$$

where $s, s' \in \{0, 1\}$ depend on the signs of the two $\Box$ operations (0 stands for $\bigboxdot$ while 1 stands for $\Box$). Importantly, this expression has only one double commutator, namely $i[\rho_1, i[\rho_2, \rho_3]]$, while a general expression involves two, see eq. (123).

To get only one double commutator, we can set $\cos \delta_{ij} = 0$ for some $ij \in \{12, 23, 31\}$. However, we must also be able to solve eq. (118) for the remaining two angles. For example, to get only $i[\rho_1, i[\rho_2, \rho_3]]$, we can set $\cos \delta_{23} = 0$ and solve eq. (118) for $\delta_{12}$ and $\delta_{31}$. Similarly, $\cos \delta_{31} = 0$ would yield $i[\rho_2, i[\rho_3, \rho_1]]$ via eq. (118) and the Jacobi identity. The following lemma establishes that we can indeed get all 12 nested expressions in this way. Recall that throughout this section we treat $\rho_i$ as abstract non-commutative variables.

**Lemma 11.** Let $\rho$ be given by eqs. (115) to (117) and assume $p_1, p_2, p_3 \neq 0$. Then $\rho$ admits a nested expression if and only if $\cos \delta_{ij} = 0$ for some $ij \in \{12, 23, 31\}$.

**Proof.** We have already proved the forward implication. Indeed, nested expressions have only one double commutator, so we get $\cos \delta_{ij} = 0$ for some $ij \in \{12, 23, 31\}$.

For the reverse implication, we assume $\cos \delta_{23} = 0$ (the other cases follow similarly due to symmetry). Under this assumption, let us argue that eq. (118) has only four discrete solutions, and that these solutions correspond to the four nested expressions

$$
\rho_1 \Box_{p_1} \left( \rho_2 \Box_{p_2} \rho_3 \right)
$$

with arbitrary signs $s, s' \in \{0, 1\}$ for the two $\Box$ operations.

First, we can write

$$
\cos \delta_{23} = 0 \quad \text{and} \quad \sin \delta_{23} = -(-1)^{s'}
$$

for some $s' \in \{0, 1\}$. In other words, $\delta_{23} := -(-1)^{s'} \pi/2$. From the first half of eq. (118), $\delta_{12} = -\delta_{23} - \delta_{31} = -(-1)^{s'} \pi/2 - \delta_{31}$. Hence

$$
\cos \delta_{12} = (-1)^{s'} \sin \delta_{31} \quad \text{and} \quad \sin \delta_{12} = (-1)^{s'} \cos \delta_{31}.
$$

19
From the second half of eq. (118), \( \sqrt{p_2} \cos \delta_1 + \sqrt{p_3} \cos \delta_3 = 0 \). If we substitute \( \cos \delta_1 \) from eq. (128), this becomes \( \sqrt{p_2} (-1)^{s'} \sin \delta_3 + \sqrt{p_3} \cos \delta_3 = 0 \) and we get
\[
\sin \delta_3 = (-1)^s \sqrt{\frac{p_3}{p_2 + p_3}} \quad \text{and} \quad \cos \delta_3 = (-1)^{s'+1} \sqrt{\frac{p_2}{p_2 + p_3}}
\] (129)
for some \( s \in \{0, 1\} \). We can then find \( \delta_1 \) by substituting eq. (129) back in eq. (128):
\[
\sin \delta_1 = (-1)^s \sqrt{\frac{p_2}{p_2 + p_3}} \quad \text{and} \quad \cos \delta_1 = (-1)^{s'+1} \sqrt{\frac{p_3}{p_2 + p_3}}
\] (130)
Equations (127), (129) and (130) with \( s, s' \in \{0, 1\} \) give us the four states. It remains to argue that these solutions produce the four states in eq. (126).

We begin by restating eqs. (115) to (117) when \( \cos \delta_3 = 0 \):
\[
\rho = p_1 \rho_1 + p_2 \rho_2 + p_3 \rho_3
\] (131)
\[
+ \sqrt{p_1 p_2} \sin \delta_1 [\rho_1, \rho_2]
\]
\[
+ \sqrt{p_2 p_3} \sin \delta_2 [\rho_2, \rho_3]
\] (132)
\[
+ \sqrt{p_3 p_1} \sin \delta_3 [\rho_3, \rho_1]
\]
\[
+ \sqrt{p_1 p_2} \cos \delta_1 [\rho_1, i[\rho_2, \rho_3]].
\] (133)
Let us group the terms together to make this appear more similar to eqs. (124) and (125):
\[
\rho = p_1 \rho_1 + (p_2 \rho_2 + p_3 \rho_3 - \sqrt{p_2 p_3} \sin \delta_3 [\rho_3, \rho_2])
\]
\[
+ i[-\sqrt{p_1 p_2} \sin \delta_1 \rho_2 + \sqrt{p_3 p_1} \sin \delta_3 \rho_3 + \sqrt{p_1 p_2} \cos \delta_1 [\rho_3, \rho_2], \rho_1].
\] (134)
If we pull out the desired prefactors, we get
\[
\rho = p_1 \rho_1 + (1 - p_1) \left( \frac{p_2}{p_2 + p_3} \rho_2 + \frac{p_3}{p_2 + p_3} \rho_3 - \frac{\sqrt{p_2 p_3}}{p_2 + p_3} \sin \delta_3 [\rho_3, \rho_2] \right)
\]
\[
+ \sqrt{p_1 (1 - p_1)} i \left[ -\frac{\sqrt{p_2}}{p_2 + p_3} \sin \delta_2 \rho_2 + \frac{\sqrt{p_3}}{p_2 + p_3} \sin \delta_3 \rho_3 + \frac{\sqrt{p_2}}{p_2 + p_3} \cos \delta_2 [\rho_3, \rho_2], \rho_1 \right].
\] (135)
This becomes one of the four states in eq. (126) once we substitute the values of all \( \sin \delta_{ij} \) and \( \cos \delta_{ij} \) from eqs. (127), (129) and (130).

\[\Box\]

5.3 The four-bar linkage and its number of orbits

Recall from eqs. (96) to (98) in Section 4.4.1 that the output state can be parametrized by \( q_1, q_2, q_3 \in \mathbb{C} \), subject to eq. (108), i.e.,
\[
|q_1|^2 + |q_2|^2 + |q_3|^2 = 1, \quad q_1 + q_2 + q_3 = 1.
\] (138)
If we fix the absolute values \( |q_1|, |q_2|, |q_3| \) (and hence also the coefficients of the first-order terms in the output state), the set of possible solutions \( (q_1, q_2, q_3) \) coincides with the configuration space of a four-bar linkage, with bars of lengths \( |q_1|, |q_2|, |q_3| \), and a fourth (immobile) bar of length 1 (see Fig. 2). This simple mechanism played an important role in the invention of the steam engine and the bicycle in the 18th and 19th century, respectively, and it has found many other practical applications since. Interestingly, it also occurs in nature, such as in the human knee joint and the jaw of a parrotfish.

The four-bar linkage can have several different modes of operation, depending on the lengths of its bars (see [Gra83, p. 111] or [MS10, Sections 2.3 and 2.4] for more details). These modes are classified into two broad classes, based on the so-called Grashof condition [Gra83]:
\[
a + d < b + c,
\] (139)
where \(0 \leq a \leq b \leq c \leq d\) are the lengths of the four bars. Under this condition, for example, the shortest bar \(a\) can rotate fully. More importantly, under this condition the mechanism has two disjoint orbits, while it has a single orbit otherwise.\(^3\) The two orbits are related to each other by a reflection around the real axis (or by complex conjugation of all \(q_i\)’s). They also correspond to two different ways of assembling the mechanism.\(^4\)

In the context of combining quantum states, the longest bar \(d\) is always fixed since otherwise we would violate the first condition in eq. (138). In other words, we have \(d = 1\) and \(a^2 + b^2 + c^2 = 1\). Hence the number of orbits formed by possible output states, when the coefficients \(|q_1|, |q_2|, |q_3|\) in eq. (96) are fixed, can be determined as follows.

**Proposition 12.** Let \(a, b, c, d\) be as above, i.e., \(0 \leq a \leq b \leq c \leq d = 1\) and \(a^2 + b^2 + c^2 = 1\). Then the corresponding four-bar linkage has one orbit, unless \(b > b_0(c)\), in which case it has two; here

\[
b_0(c) := \frac{1}{2} \left(1 - c + \sqrt{1 + (2 - 3c)c}\right).
\]

(140)

In particular, if \(c \leq 2/3\) then \(b_0(c) \geq c \geq b\) and there is just one orbit irrespective of the value of \(b\).

**Proof.** If \(c \leq 2/3\) then \(b + c \leq 2c \leq 4/3\) and \(a^2 = 1 - b^2 - c^2 \geq 1 - 2c^2 \geq 1 - 8/9 = 1/9\), so \(1 + a \geq 4/3 \geq b + c\) violates the Grashof condition (139) and there is only one orbit irrespective of \(b\). If \(c > 2/3\), we find the critical value \(b_0(c)\) by solving \(a + 1 = b + c\) and \(a^2 + b^2 + c^2 = 1\).

Intuitively, if \(b\) and \(c\) are both sufficiently large, there are two orbits. In particular, in the extreme case when \(a = 0\) we have \(b = \sqrt{1 - c^2} > b_0(c)\) (assuming \(c \neq 1\)), meaning that there are two orbits for all choices of \(b\) (except for \(b = 0\), of course). This is consistent with the fact that the \(n = 2\) case has two discrete solutions, see eqs. (11) and (12).

### 5.4 The uniform combination

Let us consider the special case when \(p_1 = p_2 = p_3 = 1/3\) (or when \(|q_1| = |q_2| = |q_3| = 1/\sqrt{3}\)), i.e., the uniform combination. Using eqs. (115) to (117), the output state \(\rho\) can be written as

\[
3\rho = \rho_1 + \rho_2 + \rho_3 + \sin \delta_{12} i[\rho_1, \rho_2] + \sin \delta_{23} i[\rho_2, \rho_3] + \sin \delta_{31} i[\rho_3, \rho_1] + \cos \delta_{12} (\rho_2 \rho_3 p_1 + \rho_1 \rho_3 p_2) + \cos \delta_{23} (\rho_3 \rho_1 p_2 + \rho_2 \rho_1 p_3) + \cos \delta_{31} (\rho_1 \rho_2 p_3 + \rho_3 \rho_2 p_1),
\]

(143)

\(^3\)If eq. (139) holds with equality, the two disjoint orbits touch, thus merging into a single orbit.

\(^4\)By changing the angle between, say, \(q_1\) and \(q_2\) from reflex to non-reflex (and vice versa), one can obtain two configurations that belong to different orbits and are otherwise not reachable from one another.
where the angles $\delta_{ij}$ are subject to the following relations, see eq. (118):
\[ \delta_{12} + \delta_{23} + \delta_{31} = 0, \quad \cos \delta_{12} + \cos \delta_{23} + \cos \delta_{31} = 0. \] (144)

The corresponding four-bar linkage in this case has $a = b = c = 1/\sqrt{3}$, i.e., all non-stationary bars are of the same length. Proposition 12 implies that such mechanism has a single orbit. In other words, eqs. (141) to (143) describe a single one-parameter orbit of states. As proved in Lemma 11, this orbit contains all twelve nested combinations (they are illustrated in Fig. 3, together with the corresponding configurations of the four-bar linkage).

Recall from Lemma 11 that nested combinations correspond to $\cos \delta_{ij} = 0$, for some $ij \in \{12, 23, 31\}$. In terms of the complex parameters $q_i$ (see Section 4.4.1), this is equivalent to $\text{Re}(q_i \bar{q}_j) = 0$, meaning that $q_i$ and $q_j$ are orthogonal as vectors in the complex plane. Indeed, Fig. 3 illustrates exactly those configurations of the four-bar linkage where two of the three bars are orthogonal. Moreover, the sign of the angle $\arg(q_i \bar{q}_j) = \pm \pi/2$ between $q_i$ and $q_j$ determines the sign of the inner $\sqcap$ operation in the nested combination. The sign of the outer $\sqcap$ operation can be determined from the sign of the angle
the remaining bar forms with either of the other two bars (both signs coincide).

As a side node, if the parameters \( q_i \) are such that the four-bar linkage has two orbits (see Proposition 12), the output state cannot continuously pass through all twelve nested combinations, but only through those six for which either \( \arg q_1 > 0 \) or \( \arg q_1 < 0 \), depending on the initial configuration of the linkage. To pass from one orbit to the other, one can simultaneously take the complex conjugate of all three parameters \( q_i \). In the extreme case when one of the \( q_i \)'s is zero, the two orbits degenerate to two points. If two of the \( q_i \)'s are zero, the two points merge into one.

**Example** (Uniform combination of three mutually unbiased qubit states). Let \( I, \sigma_x, \sigma_y, \sigma_z \) be the Pauli matrices and \( \rho(x, y, z) := \frac{1}{2}(I + x\sigma_x + y\sigma_y + z\sigma_z) \) be an arbitrary single-qubit state. Let \( \rho_1 := \rho(1, 0, 0), \rho_2 := \rho(0, 1, 0), \rho_3 := \rho(0, 0, 1) \), and \( p_1 = p_2 = p_3 = 1/3 \). (Note that \( \rho_1 = |+\rangle\langle+|, \rho_2 = |+i\rangle\langle+i|, \rho_3 = |0\rangle\langle0| \), i.e., these are mutually unbiased pure states pointing along the three axes of the Bloch sphere.) According to eqs. (141) to (143), the combined state is given by

\[
\rho \left( \frac{1}{3} \left(1 - \sin \delta_{23}\right), \frac{1}{3} \left(1 - \sin \delta_{31}\right), \frac{1}{3} \left(1 - \sin \delta_{12}\right) \right),
\]

where the angles \( \delta_{ij} \) are subject to relations (144):

\[
\delta_{12} + \delta_{23} + \delta_{31} = 0, \quad \cos \delta_{12} + \cos \delta_{23} + \cos \delta_{31} = 0.
\]

The resulting one-parameter orbit is shown in Fig. 4. According to Lemma 11, this orbit contains all twelve nested uniform combinations of \( \rho_1, \rho_2, \rho_3 \), also illustrated in Fig. 4.
6 Open problems

The main open problem is generalizing Theorem 1 (originally from [ADO16]) to three states. Here is a formal statement of this conjecture.

**Conjecture** (ADO inequality for three states). For any concave and symmetric function $f : D(d) \to \mathbb{R}$, any states $\rho_1, \rho_2, \rho_3 \in D(d)$, and any probability distribution $(p_1, p_2, p_3)$,

$$f(\rho) \geq p_1 f(\rho_1) + p_2 f(\rho_2) + p_3 f(\rho_3)$$

(147)

where $\rho$ is given by eqs. (115) to (117) with $p_i$ and $\delta_{ij}$ subject to eq. (118).

It would also be interesting to understand how an arbitrary number of states can be combined. Towards this goal, the two main steps are:

1. **Finding a generalization of eq. (47).** For general $n$, the expression of the output state $\rho$ has $(n!)^2$ terms, so we need a more efficient way of contracting tensor diagrams to compute it.

2. **Answering Q2 for any $n$.** While for $n = 3$ it was sufficient to adjust the global phases of the unitaries $U_k$ in eq. (73), for general $n$ it is not clear at all how to turn the first-order terms of $\rho$ into a convex combination of $\rho_i$, with coefficients depending only on the parameters $z_\pi$ but not the input states $\rho_i$ themselves.

It is also worthwhile investigating when higher-order terms of $\rho$ can be written as a linear combination of nested commutators. Perhaps, as suggested by the $n = 3$ case, better understanding of the second problem might make it possible to deal with both problems simultaneously, since many terms are likely to drop out simultaneously.

Acknowledgements

I would like to thank Johannes Bausch, Andrew Childs, Toby Cubitt, Nilanjana Datta, Stephen Jordan, and Will Matthews for very helpful discussions. This work was supported by the European Union under project QALGO (Grant Agreement No. 600700) and by a Leverhulme Trust Early Career Fellowship (ECF-2015-256). In loving memory of L.O.V. Coffeebean.

References

[ADO16] Koenraad Audenaert, Nilanjana Datta, and Maris Ozols. Entropy power inequalities for qudits. *Journal of Mathematical Physics*, 57(5):052202, 2016. arXiv:1503.04213, doi:10.1063/1.4950785.

[Ban93] Eiichi Bannai. Association schemes and fusion algebras (an introduction). *Journal of Algebraic Combinatorics*, 2(4):327–344, 1993. doi:10.1023/A:1022489416433.

[BBE+07] Ingemar Bengtsson, Wojciech Bruzda, Åsa Ericsson, Jan-Åke Larsson, Wojciech Tadej, and Karol Życzkowski. Mutually unbiased bases and Hadamard matrices of order six. *Journal of Mathematical Physics*, 48(5):052106, 2007. arXiv:quant-ph/0610161, doi:10.1063/1.2716990.

[Chi13] Andrew M. Childs. Fourier analysis in nonabelian groups. Lecture notes at University of Waterloo, 2013. URL: [http://www.cs.umd.edu/~amchilds/teaching/w13/106.pdf](http://www.cs.umd.edu/~amchilds/teaching/w13/106.pdf).

[CLL16] Eric A. Carlen, Elliott H. Lieb, and Michael Loss. On a quantum entropy power inequality of Audenaert, Datta, and Ozols. *Journal of Mathematical Physics*, 57(6):062203, 2016. arXiv:1603.07043, doi:10.1063/1.4953638.
A Deriving the parametrization from scratch

In this appendix we derive from scratch (namely, without using the irreps of $S_3$) the parametrization of $\rho$ obtained in Section 4.4.1. The only assumption that goes into our derivation is that $z_1, z_2, z_3$ are real while $z_4, z_5, z_6$ are imaginary—this is something we observed in Section 4.3, eqs. (88) to (93). This assumption is in fact sufficient for deriving eqs. (96) to (98) and the constraints in eq. (99).

Following eq. (95), we choose the coefficients $z_i$ as

$$ (z_1, z_2, z_3, z_4, z_5, z_6) := (a_1, a_2, a_3, ib_1, ib_2, ib_3) $$

(148)

for some $a_1, a_2, a_3, b_1, b_2, b_3 \in \mathbb{R}$. Without any additional constraints, this can potentially capture only more than eqs. (88) to (93). At the same time, $z_i$ chosen according to eq. (148) still satisfy the constraints imposed in Proposition 10. In other words, this choice automatically takes care of Q2.

Let us rewrite the output state $\rho$ from eq. (47) in terms of the new parameters $a_i$ and $b_i$:

$$ \rho = (a_1^2 + b_1^2) \rho_1 + (a_2^2 + b_2^2) \rho_2 + (a_3^2 + b_3^2) \rho_3 + (a_1 b_2 - a_2 b_1) i [\rho_2, \rho_1] + (a_2 b_3 - a_3 b_2) i [\rho_3, \rho_2] + (a_3 b_1 - a_1 b_3) i [\rho_1, \rho_3] + (a_1 a_2 + b_1 b_2) (\rho_2 \rho_3 \rho_1 + \rho_1 \rho_3 \rho_2) + (a_2 a_3 + b_2 b_3) (\rho_3 \rho_1 \rho_2 + \rho_2 \rho_1 \rho_3) + (a_3 a_1 + b_3 b_1) (\rho_1 \rho_2 \rho_3 + \rho_3 \rho_2 \rho_1). $$

(149) (150) (151)

Clearly, this is identical to eqs. (96) to (98) if we let $q_k := a_k + i b_k$.

Let us now work backwards to find what extra constraints should be imposed on the coefficients $a_i$ and $b_i$ to satisfy the unitarity requirement Q1. Recall from Lemma 5 that we want the following
matrix, see eq. (80), to be unitary:
\[
\sum_{k=1}^{6} z_k L_k = \begin{pmatrix}
  a_1 & a_3 & a_2 & ib_1 & ib_2 & ib_3 \\
  a_2 & a_1 & a_3 & ib_3 & ib_1 & ib_2 \\
  a_3 & a_2 & a_1 & ib_2 & ib_3 & ib_1 \\
  ib_1 & ib_3 & ib_2 & a_1 & a_2 & a_3 \\
  ib_2 & ib_1 & ib_3 & a_3 & a_1 & a_2 \\
  ib_3 & ib_2 & ib_1 & a_2 & a_3 & a_1 \\
\end{pmatrix}
= \begin{pmatrix}
  A & iB^T \\
  iB & A^T \\
\end{pmatrix} =: U 
\] (152)

where
\[
A := \begin{pmatrix}
  a_1 & a_3 & a_2 \\
  a_2 & a_1 & a_3 \\
  a_3 & a_2 & a_1 \\
\end{pmatrix}, \quad B := \begin{pmatrix}
  b_1 & b_3 & b_2 \\
  b_2 & b_1 & b_3 \\
  b_3 & b_2 & b_1 \\
\end{pmatrix}. \tag{153}
\]

We can write the unitarity condition as
\[
UU^\dagger = \begin{pmatrix}
  A & iB^T \\
  iB & A^T \\
\end{pmatrix} \begin{pmatrix}
  A^T & -iB^T \\
  -iB & A \\
\end{pmatrix} = \begin{pmatrix}
  AA^T + B^T B & i[B^T, A] \\
  i[B, A^T] & A^T A + BB^T \\
\end{pmatrix} = I. \tag{154}
\]

Note that \([B^T, A] = 0\) holds automatically, so the remaining constraints follow solely from the diagonal blocks: \(AA^T + B^T B = A^T A + BB^T = I\). These constraints are:
\[
a_1^2 + a_2^2 + a_3^2 + b_1^2 + b_2^2 + b_3^2 = 1, \tag{155}
\]
\[
a_1 a_2 + a_2 a_3 + a_3 a_1 + b_1 b_2 + b_2 b_3 + b_3 b_1 = 0. \tag{156}
\]

It is not hard to see that these constraints are equivalent to eq. (99).