Available online at www.sciencedirect.com
ScienceDirect
Electronic Notes in Theoretical Computer Science
ELSEVIER
Electronic Notes in Theoretical Computer Science 270 (2) (2011) 37–58
www.elsevier.com/locate/entcs

Classical Representations of Qubit Channels

Tanner Crowder[1] Keye Martin[2]

Naval Research Laboratory
Center for High Assurance Computer Systems
Washington DC 20375

Abstract

A set of qubit channels has a *classical representation* when it is isomorphic to the convex closure of a group of classical channels. We prove that there are five such groups, each being either a subgroup of the alternating group on four letters, or a subgroup of the symmetric group on three letters.

Keywords: Group theory, quantum channels, convexity.

1 Introduction

In [7], the Klein four group $\mathbb{Z}_2^2$ is represented as a collection of classical channels with four inputs and four outputs, and it is shown that its convex closure can be embedded into the set of qubit channels. The qubit channels which result from this embedding can be studied, both qualitatively and quantitatively, as though they were classical channels. This has a surprising consequence: by working with classical channels, we can develop a method for completely interrupting quantum communication that only requires us to act in a *deterministic* manner, despite the fact that the end result of this process is purely random. Stepping back for a minute, a natural question emerges: are there any other classes of qubit channels that have classical representations?

In this paper, we completely answer this question by showing that there are five such classes and no others. Each class corresponds to either a subgroup of $\mathbb{A}_4$, the alternating group on four letters, or to a subgroup of S_3, the symmetric group on three letters. Let us briefly explain why we find this to be a very surprising result. If we take the stance that classical and quantum channels are very different, then we would expect them to have only trivial structure in common. But the

[1] Email: crowder@chacs.nrl.navy.mil
[2] Email: kmartin@itd.nrl.navy.mil

1571-0661 Published by Elsevier B.V.
doi:10.1016/j.entcs.2011.01.022

channels represented by the convex closure of S_3 and $\mathbb{A}_4$ have structure that is far from trivial. If, on the other hand, we try to dismiss this commonality on the grounds that the definition of a classical representation forces all qubit channels to be unital and that unital channels 'seem' classical, then why aren't there more than five groups capable of providing a classical representation, especially when the set of unital qubit channels contains arbitrarily large groups?

2 Classical representations

Let (m, n) denote the set of stochastic matrices with m rows and n columns, the classical channels with m inputs and n outputs. The set of qubit channels $\mathcal{Q}$ consists of all affine transformations of the unit ball in $\mathbb{R}^3$ which arise as the Bloch representations of the convex linear, completely positive, trace preserving maps on 2×2 density matrices. The convex closure of a set X is denoted as $\langle X \rangle$.

All subgroups of matrices are assumed to have the identity matrix I as the group identity and to be nontrivial.

Definition 2.1 Let G be a subgroup of (m, n). An *embedding* of $\langle G \rangle$ into $\mathcal{Q}$ is a function $\varphi : \langle G \rangle \to \mathcal{Q}$ such that for all $x, y \in \langle G \rangle$,

- $\varphi(I) = I$,
- $\varphi(xy) = \varphi(x)\varphi(y)$,
- $\varphi(px + (1-p)y) = p\varphi(x) + (1-p)\varphi(y)$ whenever $p \in [0, 1]$, and
- $\varphi(x) = \varphi(y) \Rightarrow x = y$.

That is, an *embedding* is an injective, convex-linear homomorphism. The set of qubit channels $\varphi(\langle G \rangle)$ is then said to have a *classical representation.*

Proposition 2.2 *Let G be a subgroup of (m, n). If there is an embedding $\varphi : \langle G \rangle \to \mathcal{Q}$, then $n = m$, G is finite and the image of φ is isomorphic to a convex subset of $\langle SO(3) \rangle$.*

Proof. Since every element of G is an invertible matrix, we have $m = n$. The only classical channels in which the inverses are also classical channels are the permutation matrices, so G is finite. To prove that the image of G under φ is contained in $SO(3)$, let us give a new and elementary proof of the fact that any qubit channel with an inverse that is also a qubit channel must be a rotation of the Bloch sphere.

Let $f(x) = Mx + b$ be a qubit channel with an inverse. Because f is injective, the equation $Mx = 0$ has a unique solution ($x = 0$), which means M is invertible. Then the inverse of f

$$f^{-1}(x) = M^{-1}x - M^{-1}b$$

is also affine. Thus, f and f^{-1} are both continuous, and so f is a homeomorphism of the unit ball $\mathbb{B}^3$ into itself. By algebraic topology, f must take the boundary of the unit ball into itself:

$$(\forall x \in \mathbb{B}^3)\ |x| = 1 \Rightarrow |f(x)| = 1.$$

We now claim that $(Mx, b) = 0$ for all $|x| = 1$. Let $|x| = 1$. Then $|-x| = 1$, and since f takes boundaries to boundaries, we have $|f(x)| = 1 = |f(-x)|$. Then

$$|f(x)|^2 = (Mx + b, Mx + b) = (Mx - b, Mx - b) = |f(-x)|^2.$$

The equation in the middle reduces to $(Mx, b) = 0$.

Now we show $b = 0$. Since M is invertible, it is surjective and thus contains the standard basis e_1, e_2, e_3 in its image, so we can find an $x \in \mathbb{R}^3$ such that $Mx = e_1$. Writing x as a linear combination of the e_i, we have

$$(e_1, b) = (Mx, b) = \sum_{i=1}^{3} x_i (Me_i, b) = 0.$$

Similarly, $(e_i, b) = 0$ for all i. So $b = 0$ and any affine homeomorphism of the unit ball onto itself will have to take the center to the center. However, this means any such qubit channel must be *unital*, and as shown by elementary means in [8], M must then be an orthogonal matrix with determinant $+1$, i.e., it must belong to $SO(3)$.

For those who find elementary proofs distasteful, it is also possible to use Theorem 2.1 of [9] and then appeal to the fact that all unitary channels induce rotations of the Bloch sphere (a complete proof of the latter is given in [8]).

Either way, the image of φ is isomorphic to a convex subset of $\langle SO(3) \rangle$, where $SO(3)$ is the group of orthogonal matrices with determinant $+1$. □

3 Cyclic groups

By the result of the last section, we know that any group whose convex closure may be embedded into $\mathcal{Q}$ has to be a finite subgroup of $SO(3)$. Our first lemma, which we shall refer back to often, tells us that *any* rotation is conjugate to a principal rotation about the x-axis:

Definition 3.1 A principal rotation about the x-axis is denoted

$$r_x(\theta) := \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & \sin\theta \\ 0 & -\sin\theta & \cos\theta \end{pmatrix}$$

for some angle $\theta \in (0, 2\pi]$. Notice that $r_x(\alpha) r_x(\beta) = r_x(\alpha + \beta)$.

Lemma 3.2 *If $f \in SO(3)$ then there is $r \in SO(3)$ such that*

$$r f r^t = r_x(\theta)$$

for some angle $\theta \in (0, 2\pi]$.

Proof. Each 3×3 rotation f is a normal matrix, so by Theorem 3.3 of [12], we can find an orthogonal matrix r such that rfr^t is block diagonal, each block being

either a 1×1 matrix consisting of a real eigenvalue of f or a 2×2 matrix of the form $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$. If $\det(r) = -1$, we replace r by $-r$ since $\det(-r) = (-1)^3 \det(r)$ and thus we assume that $r \in SO(3)$. Again because we are in dimension three, only two cases are possible: either rfr^t is a diagonal matrix or it has the form

$$rfr^t = \begin{pmatrix} c & 0 & 0 \\ 0 & a & b \\ 0 & -b & a \end{pmatrix}$$

where $c = \pm 1$ is a real eigenvalue of f. Using $\det(r) = 1/\det(r^t)$ since $r^t = r^{-1}$,

$$\det(rfr^t) = \det(r)\det(f)\det(r^t) = \det(f) = 1 = c(a^2 + b^2)$$

so we see that $c = 1$ and that (a, b) is a point on the unit circle. In the case that rfr^t is diagonal, we see that rfr^t must be either the identity or one of the matrices

$$s_x = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad s_y = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad s_z = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

The identity and s_x have the desired form. In the case $rfr^t = s_y$, we conjugate by the rotation

$$a = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

to obtain $arf(ar)^t = s_x$ which again has the desired form. In the case $rfr^t = s_z$, we conjugate by a^t.

Finally, because (a, b) is a point on the unit circle, there is an angle $\theta \in (0, 2\pi]$ such that $a = \cos\theta$ and $b = \sin\theta$. Thus, in all cases, we have $rfr^t = r_x(\theta)$. □

Recall that an element x in a group G is said to have order n if n is the smallest positive integer for which $x^n = I$.

Lemma 3.3 *Let $f \in SO(3)$ have order $n \geq 2$ and let $G = \{f^i : 1 \leq i \leq n\} \simeq \mathbb{Z}_n$ be the cyclic group that it generates. Then there is a nonzero integer $x \in \mathbb{Z}$ and an $r \in SO(3)$ such that*

$$rf^x r^t = r_x(2\pi/n).$$

Thus, G is also generated by an element $f^x \in G$ that is conjugate to $r_x(2\pi/n)$.

Proof. Let $a = r_x(2\pi/n)$. It is routine to show that a has order n and thus generates $\mathbb{Z}_n$. By Lemma 3.2, take $r \in SO(3)$ with $rfr^t = r_x(\theta)$. Since f has order n, so does $r_x(\theta)$ and thus $r_x(\theta)^n = r_x(n\theta) = I$. Then $\theta \in (0, 2\pi]$ has the form $\theta = 2\pi k/n$ for an integer $0 < k < n$. But

$$r_x(\theta) = r_x\left(\frac{2\pi k}{n}\right) = r_x\left(\frac{2\pi}{n}\right)^k = a^k$$

and by standard group theory, since a has order n, the order of a^k is $n/(k,n)$, where (k,n) is the greatest common divisor of k and n. But we know that $a^k = r_x(\theta)$ has order n, so $(k,n) = 1$. By the Euclidean algorithm, there are integers x and y, not both zero, such that

$$xk + yn = (k,n) = 1.$$

In addition, notice that $x \neq 0$ since $n \geq 2$. Now we calculate as follows:

$$rf^x r^t = (a^k)^x = a^{kx} = a^{1-yn} = a^1 a^{-yn} = a(a^n)^{-y} = a(I)^{-y} = a \tag{1}$$

and since a has order n, so does f^x. Then the fact that $(f^x)^n = I$ implies

$$\{(f^x)^i : 1 \leq i \leq n\} \subseteq \{f^i : 1 \leq i \leq n\},$$

and because n is the *least such positive integer*, both of these sets have exactly n elements and so are equal. Then G contains a generator conjugate to $r_x(2\pi/n)$. □

In particular, a finite cyclic subgroup of $SO(3)$ is conjugate to the one generated by $r_x(2\pi/n)$, so any two finite cyclic subgroups of $SO(3)$ with the same order are conjugate. We now classify the cyclic subgroups of $\mathcal{Q}$ that have classical representations. This requires a few lemmas in advance.

Lemma 3.4 *For all $n \geq 4$, there is an integer $k \geq 1$ such that $\frac{n}{4} < 2^k < \frac{3n}{4}$.*

Proof. First, $\log_2(3n) - \log_2(n) = \log_2(3) > \log_2(2) = 1$, so the interval $[\log_2 n, \log_2 3n]$ contains at least one integer, call it m. Then $\log_2(n) \leq m < \log_2(3n)$ where the strict inequality on the right holds because $3n$ is never a power of two.

If $m = \log_2(n)$, then because the length of $[\log_2 n, \log_2 3n]$ is strictly greater than 1, it must also contain $m+1$, so set $p := m+1$. If not, set $p := m$. Either way,

$$\log_2(n) < p < \log_2(3n) \Longrightarrow n < 2^p < 3n.$$

Dividing by 4, we get $n/4 < 2^{p-2} < 3n/4$. Because $p > \log_2(n) \geq \log_2(4) = 2$, $p \geq 3$ so the desired integer is $k := p - 2 \geq 1$. □

Recall that the element in position (i,j) of a matrix a is denoted by a_{ij}.

Lemma 3.5 *Let $a \in (n,n)$ and let $m \in \mathbb{N}$ be divisible by 2. If $a_{ii}^m = 0$ then $a_{ii}^{m/2} = 0$.*

Proof. If A and B are two $n \times n$ matrices, their product AB satisfies $(AB)_{ii} = \sum_{r=1}^n A_{i,r} B_{r,i}$. Since $a^m = a^{m/2} a^{m/2}$, we have

$$0 = a_{ii}^m = \sum_{r=1}^n a_{i,r}^{m/2} a_{r,i}^{m/2}.$$

The entries in a classical channel are nonnegative, so this means we have written zero as the sum of n nonnegative products. Then each product must be zero. In particular, for $r = i$, the product $a_{ii}^{m/2} a_{ii}^{m/2}$ is zero, which means $a_{ii}^{m/2} = 0$. □

Proposition 3.6 *The convex closure of $\mathbb{Z}_n \subseteq (m,m)$ cannot be embedded into $\mathcal{Q}$ when $n \geq 4$.*

Proof. Let $G = \{g^i : 1 \leq i \leq n\} \subseteq SO(3)$ be a cyclic group of order n with generator g. By Lemma 3.3, we can assume that there is $r \in SO(3)$ with $rgr^t = r_x(\theta)$ and $\theta = 2\pi/n$. For the remainder of this proof, $r_x(\theta)$ will be denoted by r_x. The average of all elements in rGr^t,

$$\perp := \sum_{i=1}^{n} \frac{r_x^i}{n},$$

is the unique algebraic zero of the monoid $\langle rGr^t \rangle$: the only element $\perp \in \langle rGr^t \rangle$ such that $\perp \cdot x = x \cdot \perp$ for all $x \in \langle rGr^t \rangle$. We will now show that there are $x, y \in [0,1]$ with $x + y = 1$ and

$$x\left(\frac{r_x + r_x^t}{2}\right) + y\left(\frac{r_x^j + (r_x^j)^t}{2}\right) = \perp. \tag{2}$$

Using Lemma 3.4, let j be a power of two such that $\frac{n}{4} < j < \frac{3n}{4}$. Then because $\pi/2 < j\theta < 3\pi/2$, we have $\cos(j\theta) < 0$, while $0 < \theta \leq \pi/2$ gives $\cos\theta \geq 0$. Defining

$$x := \frac{\cos j\theta}{\cos j\theta - \cos\theta} \in (0,1]$$

and setting $y = 1 - x \in [0,1)$ we have

$$x\left(\frac{r_x + r_x^t}{2}\right) + y\left(\frac{r_x^j + (r_x^j)^t}{2}\right) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & x\cos\theta + y\cos j\theta & 0 \\ 0 & 0 & x\cos\theta + y\cos j\theta \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

This projection belongs to $\langle rGr^t \rangle$ since we have written it as a convex sum of elements belonging to $\langle rGr^t \rangle$. To see that equation (2) holds in $\langle rGr^t \rangle$, notice that

$$r_x(\alpha)\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} r_x(\alpha) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

for any α; thus, this projection is the algebraic zero for $\langle rGr^t \rangle$ and thus equal to $\perp$.

Multiplying equation (2) on the left by r^t and on the right by r, the analogous equation holds in $\langle G \rangle$:

$$x\left(\frac{g + g^t}{2}\right) + y\left(\frac{g^j + (g^j)^t}{2}\right) = \sum_{i=1}^{n} \frac{g^i}{n} = \perp_G. \tag{3}$$

We will now show that this equation is *impossible* for classical (m,m) channels. Let

$a \in (m,m)$ be a generator for a copy of $\mathbb{Z}_n$. If

$$x\left(\frac{a+a^t}{2}\right)+y\left(\frac{a^j+(a^j)^t}{2}\right)$$

is the algebraic zero then multiplying it by a leaves it unchanged:

$$x\left(\frac{a^2+I}{2}\right)+y\left(\frac{a^{j+1}+a^{n-j+1}}{2}\right)=x\left(\frac{a+a^t}{2}\right)+y\left(\frac{a^j+(a^j)^t}{2}\right).$$

Rearranging terms we can see that

$$xI = xa + xa^t + ya^j + y(a^j)^t - xa^2 - ya^{j+1} - ya^{n-j+1}. \tag{4}$$

Since a generates $\mathbb{Z}_n$ and $j < 3n/4 < n$, $a^j \neq I$. Because a and hence a^j is a permutation, there is an entry a^j_{ii} on the diagonal of a^j which is equal to zero. Since $j = 2^k$ with $k \geq 1$, j is divisible by 2, so by Lemma 3.5, $a^2_{ii} = 0$ and thus $a_{ii} = 0$ as well. Since transposes do not alter diagonals, $a^t_{ii} = 0$ and $(a^j)^t_{ii} = 0$. For the (i,i) entry of the matrix in equation (4), we have

$$x = -y(a^{j+1}_{ii} + a^{n-j+1}_{ii}).$$

Since the powers of a are permutations, $a^{j+1}_{ii}+a^{n-j+1}_{ii}$ is either 0, 1 or 2, contradicting $x > 0$.

Since equation (3) holds for any quantum generator of $\mathbb{Z}_n$ but never holds for a classical generator of $\mathbb{Z}_n$, the convex closure of $\mathbb{Z}_n \subseteq (m,m)$ can never be embedded into $\mathcal{Q}$ when $n \geq 4$. □

An interesting consequence of the last proof is that for an integer $n \geq 4$,

$$\sum_{k=1}^{n} \cos(2\pi/n \cdot k) = 0 = \sum_{k=1}^{n} \sin(2\pi/n \cdot k).$$

The last result permits a solution of the classification problem for cyclic groups: let

$$\text{flip} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in (2,2) \quad \& \quad c = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \in (3,3)$$

denote generators for $\mathbb{Z}_2$ and $\mathbb{Z}_3$ respectively.

Theorem 3.7

- *If $G \subseteq (m,m)$ is a cyclic group and $\varphi : \langle G \rangle \to \mathcal{Q}$ is an embedding, then $G \simeq \mathbb{Z}_2$ or $G \simeq \mathbb{Z}_3$.*
- *The convex closure of the groups $\mathbb{Z}_2 \simeq \{I, \text{flip}\}$ and $\mathbb{Z}_3 \simeq \{I, c, c^2\}$ can be embedded into $\mathcal{Q}$.*

Proof. For $\mathbb{Z}_2$, we map $I, \text{flip} \in (2,2)$ onto the spin channels

$$I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \& \quad s_x = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

and then extend linearly to obtain an embedding

$$\varphi \begin{pmatrix} x_1 & x_2 \\ x_2 & x_1 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 & 0 & 0 \\ 0 & x_1 - x_2 & 0 \\ 0 & 0 & x_1 - x_2 \end{pmatrix}.$$

For $\mathbb{Z}_3$, c is a classical channel that generates $\mathbb{Z}_3$. However, it is also a qubit channel: as a permutation, it is orthogonal, and direct calculation shows that $\det(c) = 1$, so that $c \in SO(3)$. Thus, its convex closure embeds into $\mathcal{Q}$ via the identity map! □

4 Finite abelian groups

Lemma 4.1 *If $\mathcal{Q}$ contains a copy of the group $\mathbb{Z}_2^n$, then $n = 1$ or $n = 2$.*

Proof. Any involution $f \in \mathcal{Q}$ must be a rotation and hence symmetric since $f = f^{-1} = f^t$. Thus, there is a rotation $r \in SO(3)$ such that rfr^t is diagonal. However, $rfr^t \in SO(3)$ is also an involution, but the only diagonal involutions in $SO(3)$ are the *spin channels*:

$$I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad s_x = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad s_y = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad s_z = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

The reason is: being symmetric, each has three real eigenvalues; being orthogonal, each eigenvalue is ± 1; being a rotation, the product of these eigenvalues must be 1.

Now if $\mathcal{Q}$ contains a copy of $\mathbb{Z}_2^n$, then it contains 2^n commutative involutions. Because all the elements of $\mathbb{Z}_2^n$ commute, they diagonalize in a common basis. Thus, there is $r \in SO(3)$ such that $rfr^t \in SO(3)$ is a diagonal involution for each $f \in \mathbb{Z}_2^n$. Then $r\,(\mathbb{Z}_2^n)\,r^t \subseteq \{I, s_x, s_y, s_z\}$. And since the number of elements in the group $r\,(\mathbb{Z}_2^n)\,r^t$ is 2^n, we have that either $n = 1$ or $n = 2$. □

Let $r_z(\theta)$ denote the principal rotation about the z-axis:

$$r_z(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

From annoying arithmetic, it follows that $r_x(\theta)$ and $r_z(\alpha)$ commute iff they are both diagonal.

Lemma 4.2 *If $\mathcal{Q}$ contains a copy of the group $\mathbb{Z}_3^n$, then $n = 1$.*

Proof. Suppose $\mathcal{Q}$ contains a copy of $\mathbb{Z}_3^2$. Let $f, g \in \mathbb{Z}_3^2 \subseteq SO(3)$ be elements of order 3 such that

$$\{f^i : 1 \leq 3\} \cap \{g^i : 1 \leq i \leq 3\} = \{I\}.$$

Notice that $\mathbb{Z}_3^2$ contains elements of order three that generate distinct subgroups: intuitively, in additive notation, $f = (0,1)$ and $g = (1,0)$ are examples of such elements.

Because $f, g \in SO(3)$ are commutative normal matrices, by Theorem 2.5.15 of [5], there is a single orthogonal matrix r such that rfr^t and rgr^t are block diagonal, each block being either a 1×1 matrix consisting of a real eigenvalue or a 2×2 matrix of the form $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$.

Because f and g have order 3, so do rfr^t and rgr^t, so neither can have blocks consisting solely of eigenvalues, or they would be diagonal and then have order 1 or 2. Thus, the only possible forms are

$$\begin{pmatrix} c & 0 & 0 \\ 0 & a & b \\ 0 & -b & a \end{pmatrix} \quad \& \quad \begin{pmatrix} a & b & 0 \\ -b & a & 0 \\ 0 & 0 & c \end{pmatrix}.$$

Because c refers to a real eigenvalue of an orthogonal matrix, $c = \pm 1$, but since the determinant of each is $c(a^2 + b^2) = 1$, being the determinant of the rotations f and g respectively, $c = 1$ and $a^2 + b^2 = 1$. Thus, the first matrix has the form $r_x(\theta)$ for $\theta \in (0, 2\pi]$ and the second has the form $r_z(\alpha)$ for some $\alpha \in (0, 2\pi]$.

However, because f and g commute, rfr^t and rgr^t also commute, and this means that both have the form $r_x(\theta)$ or both have the form $r_z(\alpha)$, since $r_x(\theta)$ and $r_z(\alpha)$ only commute when they are diagonal (which as we have seen, is impossible because rfr^t and rgr^t have order three). Thus, without loss of generality,

$$rfr^t = r_x(\theta) \quad \& \quad rgr^t = r_x(\alpha)$$

where $\theta = 2\pi k/3$ and $\alpha = 2\pi m/3$ for integers $0 < k, m < 3$. If $k = m$, then $f = g$, contradicting the fact that f and g generate distinct subgroups. If $k \neq m$, then without loss of generality, $k = 1$ and $m = 2$. This gives

$$fg = \left(r^t\, r_x(2\pi/3) r\right)\left(r^t\, r_x(4\pi/3) r\right) = r^t r_x(6\pi/3) r = I$$

which means $f^{-1} = g$. However, f has order 3, so $g = f^{-1} = f^2$, which again contradicts the fact that f and g generate distinct subgroups. Thus, $SO(3)$ does not contain a copy of $\mathbb{Z}_3^2$.

If $\mathcal{Q}$ contains a copy of $\mathbb{Z}_3^n \subseteq SO(3)$ for $n > 1$, then it contains a copy of $\mathbb{Z}_3^2$, which as we have seen, is impossible. □

The fundamental theorem on finite abelian groups states that any finite abelian group G is isomorphic to a direct product of cyclic groups whose orders are powers of primes:

$$G \simeq \prod_{i=1}^{n} \mathbb{Z}_{p_i^{r_i}}$$

where the p_i are primes, not necessarily distinct, and each $r_i \geq 1$. We will now classify the abelian groups that can be used to represent qubit channels. Let

$$\{I \otimes I, I \otimes \text{flip}, \text{flip} \otimes I, \text{flip} \otimes \text{flip}\} \subseteq (4,4)$$

denote the natural copy of the Klein four group studied in [7].

Theorem 4.3

- *If $G \subseteq (m,m)$ is an abelian group and $\varphi : \langle G \rangle \to \mathcal{Q}$ is an embedding, then G is isomorphic to $\mathbb{Z}_2^2$, $\mathbb{Z}_3$ or $\mathbb{Z}_2$.*
- *The convex closure of the groups $\mathbb{Z}_2^2 \simeq \{I \otimes I, I \otimes \text{flip}, \text{flip} \otimes I, \text{flip} \otimes \text{flip}\}$, $\mathbb{Z}_3 \simeq \{I, c, c^2\}$ and $\mathbb{Z}_2 \simeq \{I, \text{flip}\}$ can be embedded into $\mathcal{Q}$.*

Proof. Let G be an abelian group in (m,m) whose convex closure can be embedded into $\mathcal{Q}$. By the fundamental theorem on finite abelian groups, we can write it as a product of cyclic groups

$$G \simeq \prod_{i=1}^{n} \mathbb{Z}_{p_i^{r_i}}$$

where the p_i are primes, not necessarily distinct, and each $r_i \geq 1$. If one of these primes $p_i \geq 5$, then because p_i divides the order of G,

$$|G| = \prod_{i=1}^{n} |\mathbb{Z}_{p_i^{r_i}}| = \prod_{i=1}^{n} p_i^{r_i},$$

the converse of Lagrange's theorem for finite abelian groups implies that G must have a subgroup of order p_i. But the only finite abelian group of order p_i is $\mathbb{Z}_{p_i}$, a cyclic group having order greater than 3. Since the convex closure of $\mathbb{Z}_{p_i}$ cannot be embedded in $\mathcal{Q}$ by Theorem 3.7, neither can the convex closure of G. Thus, there are three possibilities for G:

(1) $G \simeq \prod_{i=1}^{n} \mathbb{Z}_{2^{r_i}}$ with $n \geq 1$ and each $r_i \geq 1$,

(2) $G \simeq \prod_{i=1}^{n} \mathbb{Z}_{3^{r_i}}$ with $n \geq 1$ and each $r_i \geq 1$, or

(3) $G \simeq \prod_{i=1}^{n} \mathbb{Z}_{2^{r_i}} \times \prod_{i=1}^{m} \mathbb{Z}_{3^{s_i}}$ with $n, m \geq 1$ and each $r_i, s_i \geq 1$.

In case (1), each $r_i = 1$ or else G has a cyclic subgroup of order ≥ 4, contradicting Theorem 3.7. Thus, G is simply a product of copies of $\mathbb{Z}_2$. By Lemma 4.1, the only possibilities are $\mathbb{Z}_2$, whose convex closure can be embedded by Theorem 3.7, and $\mathbb{Z}_2^2$, the latter of which we will show later in this proof has a convex closure that can be embedded.

In case (2), each $r_i = 1$ or else G has a cyclic subgroup of order ≥ 4, contradicting Theorem 3.7. Thus, G is simply a product of copies of $\mathbb{Z}_3$. By Lemma 4.2, the only possibility is $\mathbb{Z}_3$, whose convex closure can be embedded by Theorem 3.7.

In case (3), G has a subgroup $H \simeq \mathbb{Z}_{2^{r_1}} \times \mathbb{Z}_{3^{s_1}}$ where $r_1, s_1 \geq 1$. Because H is a product of cyclic groups whose orders are relatively prime, by Theorem 6.1 of [11], we have $H \simeq \mathbb{Z}_{2^{r_1} 3^{s_1}}$, a cyclic group of order $|H| = 2^{r_i} 3^{s_i} \geq 6 \geq 4$, which is impossible by Theorem 3.7.

Now let us prove that the convex closure of $\mathbb{Z}_2^2 = \{I\otimes I, I\otimes\text{flip}, \text{flip}\otimes I, \text{flip}\otimes\text{flip}\}$ can be embedded into $\mathcal{Q}$. Using the spin channels from Lemma 4.1, we extend the natural isomorphism

$$I \otimes I \mapsto I, \quad I \otimes \text{flip} \mapsto s_x, \quad \text{flip} \otimes I \mapsto s_y, \quad \text{flip} \otimes \text{flip} \mapsto s_z$$

convex linearly to obtain

$$\varphi\begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_2 & x_1 & x_4 & x_3 \\ x_3 & x_4 & x_1 & x_2 \\ x_4 & x_3 & x_2 & x_1 \end{pmatrix} = \begin{pmatrix} x_1+x_2-x_3-x_4 & 0 & 0 \\ 0 & x_1-x_2+x_3-x_4 & 0 \\ 0 & 0 & x_1-x_2-x_3+x_4 \end{pmatrix}.$$

This clearly defines a function. As a convex linear extension of an isomorphism, it preserves the identity, convex sums and products. We need to prove that it is *injective*. Let $f, g \in \langle\mathbb{Z}_2^2\rangle$ be defined by a convex sum involving probabilities x_i and y_i respectively. If $\varphi(f) = \varphi(g)$, then

$$\varphi(f) - \varphi(g) = c_1 I + c_2 s_x + c_3 s_y + c_4 s_z = 0$$

where each $c_i = x_i - y_i$ so that $\sum_{i=1}^4 c_i = 0$. Then the c_i satisfy the following four equations:

$$c_1 + c_2 + c_3 + c_4 = 0 \tag{5}$$
$$c_1 + c_2 - c_3 - c_4 = 0 \tag{6}$$
$$c_1 - c_2 + c_3 - c_4 = 0 \tag{7}$$
$$c_1 - c_2 - c_3 + c_4 = 0. \tag{8}$$

Adding (7) and (8) gives $c_1 = c_2$. Substituting this into (7) gives $c_3 = c_4$. Substituting both of these into (6) gives $c_1 = c_3$. Then $c_1 = c_2 = c_3 = c_4$. By (5), each $c_i = 0$ and thus $x_i = y_i$ for all i. This proves $f = g$ so that φ is injective. □

5 Finite groups

In this section, we show that there are at most two nonabelian groups that can be used to represent qubit channels. Let $\mathbb{A}_4$ denote the alternating group on four letters and let S_3 denote the symmetric group on three letters.

Theorem 5.1 *If $G \subseteq (n, n)$ is a nonabelian group whose convex closure can be embedded into $\mathcal{Q}$, then G is either isomorphic to $\mathbb{A}_4$ or to S_3.*

Proof. If $|G|$ is divisible by a prime $p \geq 5$, then by Theorem 5.2 of [6], G contains an element of order p and thus a subgroup isomorphic to $\mathbb{Z}_p$. By Theorem 3.7, $\langle G\rangle$ cannot be embedded into $\mathcal{Q}$. Then let us factor $|G|$ into a product of its possible prime powers as $|G| = 2^p 3^q$ where $p, q \geq 0$.

If $q \geq 2$, then G contains a subgroup of order 3^2 by the first Sylow theorem, Theorem 5.7 of [6], but then by Exercise 13 on page 98 of [6], this subgroup must be abelian, which is impossible by Theorem 3.7. Thus, $0 \leq q \leq 1$.

Write $|G| = 2^p 3^q$, where $p \geq 0$ and $0 \leq q \leq 1$. If $p \geq 3$, then by the first Sylow theorem, G contains a subgroup of order $2^3 = 8$. By Theorem 4.3, this subgroup cannot be abelian. But if it is nonabelian, it must contain an element of order 4, by the proof of Prop. 6.3 in [6], so G contains a copy of $\mathbb{Z}_4$, which is impossible by Theorem 3.7. Thus, $0 \leq p \leq 2$.

Write $|G| = 2^p 3^q$ with $0 \leq p \leq 2$ and $0 \leq q \leq 1$. If $p = 0$, then G is either the trivial group ($q = 0$) or $\mathbb{Z}_3$ ($q = 1$), using the table on page 98 of [6]. Similarly, if $q = 0$, then by the same table, the only nontrivial groups are $\mathbb{Z}_2$, $\mathbb{Z}_4$ and $\mathbb{Z}_2^2$, all of which are abelian. Thus, $q = 1$ and $1 \leq p \leq 2$.

Write $|G| = 2^p 3$ with $1 \leq p \leq 2$. If $p = 1$, then $|G| = 6$, and the only nonabelian group of order 6 is S_3, using the table on page 98 of [6]. If $p = 2$, then $|G| = 12$, and using the same table, the only nonabelian groups of order 12 are D_6, T and $\mathbb{A}_4$. Both of the groups D_6 and T contain elements of order 6, by remarks (i) and (ii) on page 98 of [6], and thus contain a copy of $\mathbb{Z}_6$, in contrast to Theorem 3.7.

Thus, the only two nonabelian groups capable of being embedded into $\mathcal{Q}$ are $\mathbb{A}_4$ and S_3. □

By Lagrange's theorem, any subgroup of a finite group must divide the order of the group. Because $|S_3| = 6$ and $|\mathbb{A}_4| = 12$, any proper subgroup of S_3 must have order 2 or 3, while any proper subgroup of $\mathbb{A}_4$ must have order $2, 3, 4$ or 6. However, by Exercise 8 on Page 51 of [6], $\mathbb{A}_4$ does not have a subgroup of order 6. The only groups of order 2 and 3 are $\mathbb{Z}_2$ and $\mathbb{Z}_3$, while the only groups of order four are $\mathbb{Z}_4$ and $\mathbb{Z}_2^2$. Thus, all the proper subgroups of $\mathbb{A}_4$ and S_3 have convex closures that can be embedded into $\mathcal{Q}$, so there is no obvious way to rule either case out. In addition, S_3 is not a subgroup of $\mathbb{A}_4$, so the cases $\mathbb{A}_4$ and S_3 must be considered separately.

6 $\mathbb{A}_4$

The set of even permutations in $(4, 4)$ comprises a group $\mathbb{A}_4$ called the *alternating group on four letters*. Explicitly, its involutions are

$$I = \begin{pmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&1&0\\ 0&0&0&1 \end{pmatrix}, \; x = \begin{pmatrix} 0&1&0&0\\ 1&0&0&0\\ 0&0&0&1\\ 0&0&1&0 \end{pmatrix}, \; y = \begin{pmatrix} 0&0&1&0\\ 0&0&0&1\\ 1&0&0&0\\ 0&1&0&0 \end{pmatrix}, \; z = \begin{pmatrix} 0&0&0&1\\ 0&0&1&0\\ 0&1&0&0\\ 1&0&0&0 \end{pmatrix},$$

its order three elements are

$$a = \begin{pmatrix} 0&0&0&1\\ 0&1&0&0\\ 1&0&0&0\\ 0&0&1&0 \end{pmatrix}, \; b = \begin{pmatrix} 0&1&0&0\\ 0&0&0&1\\ 0&0&1&0\\ 1&0&0&0 \end{pmatrix}, \; c = \begin{pmatrix} 1&0&0&0\\ 0&0&1&0\\ 0&0&0&1\\ 0&1&0&0 \end{pmatrix}, \; d = \begin{pmatrix} 0&0&1&0\\ 1&0&0&0\\ 0&1&0&0\\ 0&0&0&1 \end{pmatrix},$$

together with their squares:

$$a^2 = \begin{pmatrix} 0&0&1&0\\ 0&1&0&0\\ 0&0&0&1\\ 1&0&0&0 \end{pmatrix},\ b^2 = \begin{pmatrix} 0&0&0&1\\ 1&0&0&0\\ 0&0&1&0\\ 0&1&0&0 \end{pmatrix},\ c^2 = \begin{pmatrix} 1&0&0&0\\ 0&0&0&1\\ 0&1&0&0\\ 0&0&1&0 \end{pmatrix},\ d^2 = \begin{pmatrix} 0&1&0&0\\ 0&0&1&0\\ 1&0&0&0\\ 0&0&0&1 \end{pmatrix}.$$

A quick proof that the matrices above give a copy of $\mathbb{A}_4$ is to first notice that a is even because it can be written as the product of two transpositions $a = fg$, where f swaps the first and third elements and g swaps the third and fourth. Similarly, x is also even. Thus, $xa = b$, $bx = c$ and $xc = d$ are even as the product of evens, as are their squares. Finally, $y = ac^2$, $z = xy$ and $x^2 = I$ are even. Since we have generated twelve distinct even permutations and a four element set only has $4!/2 = 12$ even permutations, this set of matrices forms a copy of $\mathbb{A}_4$:

Definition 6.1 $\mathbb{A}_4 := \{I, x, y, z, a, b, c, d, a^2, b^2, c^2, d^2\} \subseteq (4, 4)$.

Notice that any copy of $\mathbb{A}_4$ can be generated from an order three element and an *even* involution. Let us use this intuition to generate a likely candidate for a copy of $\mathbb{A}_4$ within $SO(3)$. Starting with the involutions of Lemma 4.1, we take

$$I = \begin{pmatrix} 1&0&0\\ 0&1&0\\ 0&0&1 \end{pmatrix}, s_x = \begin{pmatrix} 1&0&0\\ 0&-1&0\\ 0&0&-1 \end{pmatrix}, s_y = \begin{pmatrix} -1&0&0\\ 0&1&0\\ 0&0&-1 \end{pmatrix}, s_z = \begin{pmatrix} -1&0&0\\ 0&-1&0\\ 0&0&1 \end{pmatrix},$$

and we choose our order three generator to be

$$f = \begin{pmatrix} 0&-1&0\\ 0&0&1\\ -1&0&0 \end{pmatrix}.$$

Now multiplying s_x and f in various ways gives other order three elements

$$g = s_x f = \begin{pmatrix} 0&-1&0\\ 0&0&-1\\ 1&0&0 \end{pmatrix},\ h = g s_x = \begin{pmatrix} 0&1&0\\ 0&0&1\\ 1&0&0 \end{pmatrix},\ j = s_x h = \begin{pmatrix} 0&1&0\\ 0&0&-1\\ -1&0&0 \end{pmatrix}.$$

along with their squares:

$$f^2 = \begin{pmatrix} 0&0&-1\\ -1&0&0\\ 0&1&0 \end{pmatrix},\ g^2 = \begin{pmatrix} 0&0&1\\ -1&0&0\\ 0&-1&0 \end{pmatrix},\ h^2 = \begin{pmatrix} 0&0&1\\ 1&0&0\\ 0&1&0 \end{pmatrix},\ j^2 = \begin{pmatrix} 0&0&-1\\ 1&0&0\\ 0&-1&0 \end{pmatrix}.$$

Definition 6.2 $G := \{I, s_x, s_y, s_z, f, g, h, j, f^2, g^2, h^2, j^2\} \subseteq SO(3)$.

The set G forms a group isomorphic to $\mathbb{A}_4$ in a natural way. Let us prove this:

Lemma 6.3 *The set $G \subseteq SO(3)$ is a group isomorphic to $\mathbb{A}_4 \subseteq (4, 4)$. An isomorphism φ is*

- $\varphi(I) = I, \quad \varphi(x) = s_x, \quad \varphi(y) = s_y, \quad \varphi(z) = s_z,$
- $\varphi(a) = f, \quad \varphi(b) = g, \quad \varphi(c) = h, \quad \varphi(d) = j,$
- $\varphi(a^2) = f^2, \ \varphi(b^2) = g^2, \ \varphi(c^2) = h^2, \ \varphi(d^2) = j^2.$

Proof. By page 225 of [1], a presentation of the alternating group on four letters is given by generators α and β and relations $\alpha^3 = \beta^3 = (\alpha\beta)^2 = I$. Within G, the elements j and h^2 satisfy such relations. Thus, the group they generate is isomorphic to $\mathbb{A}_4$. We define φ on these generators

$$\varphi(d) = j \quad \& \quad \varphi(c^2) = h^2$$

and then extend φ homomorphically. By [1], c^2 and d generate $\mathbb{A}_4$, so φ is an isomorphism between $\mathbb{A}_4$ and the group generated by j and h^2. What we have to prove is that the latter group is G. We do so by explicitly calculating φ on the remaining ten elements.

Let us calculate the value of φ on the involutions I and x. Using $jh^2 = s_x$ and $dc^2 = x$,

- $\varphi(x) = \varphi(dc^2) = \varphi(d)\varphi(c^2) = jh^2 = s_x,$
- $\varphi(I) = \varphi(x^2) = \varphi(x)\varphi(x) = s_x s_x = I.$

Using the equations mentioned before the definition of $\mathbb{A}_4$, as well as those mentioned during the definition of G, we can now calculate it on a, b and c:

- $\varphi(c) = \varphi(xd) = \varphi(x)\varphi(d) = s_x j = h$
- $\varphi(b) = \varphi(cx) = \varphi(c)\varphi(x) = hs_x = g$
- $\varphi(a) = \varphi(xb) = \varphi(x)\varphi(b) = s_x g = f.$

Then the equations $\varphi(a^2) = f^2$, $\varphi(b^2) = g^2$, $\varphi(c^2) = h^2$ and $\varphi(d^2) = j^2$ follow. Finally, we calculate the value of φ on y and z. Using $y = ac^2$ and $fh^2 = s_y$,

$$\varphi(y) = \varphi(a)\varphi(c^2) = fh^2 = s_y$$

while the fact that $z = xy$ gives

$$\varphi(z) = \varphi(x)\varphi(y) = s_x s_y = s_z$$

finishing the proof. □

We now show that this isomorphism extends to the convex closures of both groups.

Theorem 6.4 *The convex closure of $\mathbb{A}_4$ can be embedded into $\mathcal{Q}$.*

Proof. Let $\varphi : \langle \mathbb{A}_4 \rangle \to \langle G \rangle$ be defined on group elements in the natural way and then extended convex linearly. If we show that φ is a function and that it is injective, then it follows from [7] that it must actually be an embedding. An

arbitrary $f \in \langle \mathbb{A}_4 \rangle$ can be written

$$f = \begin{pmatrix} e+c+c_2 & x+b+d_2 & y+d+a_2 & z+a+b_2 \\ x+d+b_2 & e+a+a_2 & z+c+d_2 & y+b+c_2 \\ y+a+d_2 & z+d+c_2 & e+b+b_2 & x+c+a_2 \\ z+b+a_2 & y+c+b_2 & x+a+c_2 & e+d+d_2 \end{pmatrix},$$

where we have written a general element $f \in \langle \mathbb{A}_4 \rangle$ as a convex sum

$$f = e \cdot I + x \cdot x + y \cdot y + z \cdot z + a \cdot a + b \cdot b + c \cdot c + d \cdot d + a_2 \cdot a^2 + b_2 \cdot b^2 + c_2 \cdot c^2 + d_2 \cdot d^2$$

of elements of the group $\mathbb{A}_4 \subseteq (4,4)$. Notice that each probability in a general convex sum $f \in \langle \mathbb{A}_4 \rangle$ has the same name as its associated group element except in cases where this would create clear inconsistencies [3]. The element $\varphi(f)$ is thus

$$\varphi(f) = \begin{pmatrix} e+x-y-z & -a-b+c+d & -a_2+b_2+c_2-d_2 \\ -a_2-b_2+c_2+d_2 & e-x+y-z & a-b+c-d \\ -a+b+c-d & a_2-b_2+c_2-d_2 & e-x-y+z \end{pmatrix}.$$

Let f_{ij} and $\varphi(f)_{ij}$ denote the entries of f and $\varphi(f)$ located at position (i,j). Then f and $\varphi(f)$ are related by:

- $\phi(f)_{11} = +f_{11} + f_{21} - f_{42} - f_{32}$,
  $\phi(f)_{12} = -f_{14} - f_{24} + f_{42} + f_{32}$,
  $\phi(f)_{13} = -f_{13} - f_{23} + f_{32} + f_{42}$;
- $\phi(f)_{21} = -f_{13} + f_{24} - f_{33} + f_{44}$,
  $\phi(f)_{22} = +f_{11} - f_{43} + f_{31} - f_{23}$,
  $\phi(f)_{23} = +f_{14} - f_{41} - f_{21} + f_{34}$;
- $\phi(f)_{31} = -f_{14} + f_{23} + f_{33} - f_{44}$,
  $\phi(f)_{32} = +f_{13} - f_{21} + f_{43} - f_{31}$,
  $\phi(f)_{33} = +f_{11} - f_{43} - f_{42} - f_{14}$.

Thus, φ is a well-defined function. To see that it is injective, suppose that $\varphi(f) = \varphi(g)$ where f is written as a convex sum using probabilities e, x, y, z, etc, g is written using probabilities e', x', y', z', etc and we set $c_i = i - i'$ for each $i \in \{e, x, y, z, a, b, c, d, a_2, b_2, c_2, d_2\}$. Because $\varphi(f) - \varphi(g) = 0$, we get three sets of three different equations: the first set involves only variables e, x, y, z, the second involves only a, b, c, d and the third involves only a_2, b_2, c_2, d_2. The argument applied to $\mathbb{Z}_2^2$ in the proof of Theorem 4.3 applies to each of these sets allowing us to conclude that

- $c_e = c_x = c_y = c_z$,
- $c_a = c_b = c_c = c_d$,
- $c_{a_2} = c_{b_2} = c_{c_2} = c_{d_2}$.

[3] This unorthodox notation is necessitated by the complexity of working with φ

However, because $\sum c_i = 0$, we then have $c_i + c_j + c_k = 0$ for any $i \in \{e, x, y, z\}$, $j \in \{a, b, c, d\}$ and $k \in \{a_2, b_2, c_2, d_2\}$. This implies that $f - g = 0$ so that $f = g$ and hence that φ is injective.

Because the convex linear extension of the isomorphism φ is a well-defined injective function, it is an embedding by the proof of Theorem 2 in [7]. □

7 S_3

We denote by $S_3 \subseteq (3, 3)$ the natural copy of the symmetric group on three letters:

$$S_3 = \left\{ I,\ a = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},\ a^2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, b = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},\ c = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix},\ d = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\}.$$

The elements b, c and d are all involutions and the entire group is determined by a and and *any* of its nontrivial involutions since $c = ab$ and $d = a^2 b$. Notice too that $aba = a$. Let us point out that this group has the following property:

$$\frac{I + a + a^2}{3} = \frac{I + a + a^2 + b + c + d}{6}. \tag{9}$$

We will now show that this equation is *impossible* quantum mechanically:

Lemma 7.1 *The convex closure of $S_3 \subseteq (3, 3)$ cannot be embedded into $\mathcal{Q}$.*

Proof. If a copy $\{I, a, a^2, b, c, d\} \subseteq SO(3)$ of S_3 satisfies equation (9), then

$$I + a + a^2 = b + c + d.$$

So taking the trace of both sides gives

$$3 + \mathrm{tr}(a) + \mathrm{tr}(a^2) = -3$$

where we note that each nontrivial involution is conjugate to one of the spin channels in Lemma 4.1, and that conjugate matrices always have the same trace: in this case, $\mathrm{tr}(b) = \mathrm{tr}(c) = \mathrm{tr}(c) = -1$. However, each rotation is conjugate to some $r_x(\theta)$ by Lemma 3.2, so $\mathrm{tr}(a) \geq -1$ and $\mathrm{tr}(a^2) \geq -1$, contradicting the fact that their sum is -6. □

Thus, the convex closure of the *natural copy* of S_3 cannot be embedded into $\mathcal{Q}$. Let us now look to $(4, 4)$. For the sake of simplicity, we introduce some new notation for permutations $\pi \in (4, 4)$. Let $v = (1, 2, 3, 4)$. Then $\pi v = (p, q, r, s)$ arises from rearranging the elements of v. We can thus denote π by $1234 \to pqrs$. We define the following permutations of order three:

- a_1 is the permutation $1234 \to 1342$
- a_2 is the permutation $1234 \to 3241$
- a_3 is the permutation $1234 \to 2431$
- a_4 is the permutation $1234 \to 2314$.

Notice that a_i keeps element i fixed.

Lemma 7.2

- *There are eight permutations in* $(4,4)$ *of order three:* a_1, a_2, a_3, a_4, a_1^2, a_2^2, a_3^2, *and* a_4^2.
- *For each* $i \in \{1,2,3,4\}$, *there is an involution* $x \in (4,4)$ *such that* $a_i = xa_1x$.

Proof.First, we claim that a permutation of order three must keep one element fixed. To see why, let us enumerate the fixed-point free permutations of $(4,4)$ and notice that none of them have order three:

- The fixed point free permutations that 'begin' in 2 are: $1234 \to 2413$, $1234 \to 2341$ and $1234 \to 2143$. They have orders four, four and two, respectively.
- The fixed point free permutations that 'begin' in 3 are: $1234 \to 3412$, $1234 \to 3421$ and $1234 \to 3142$. They have orders two, four and four, respectively.
- The fixed point free permutations that 'begin' in 4 are: $1234 \to 4123$, $1234 \to 4321$ and $1234 \to 4312$. They have orders four, two and four, respectively.

Thus, any $x \in (4,4)$ of order three keeps one element fixed and permutes the other three. By writing out the six permutations on a three element set, we see that there are only two that have order three: $a = 123 \to 231$ and $a^2 = 123 \to 312$. Then for each $i \in \{1,2,3,4\}$, there are two permutations of order three that have i as a fixed point: the first acts as a on the other three elements, the second acts as a^2 on the other three elements. Thus, there are a total of eight permutations in $(4,4)$ of order three: $\{a_i, a_i^2 : 1 \leq i \leq 4\}$.

To see that each a_i is conjugate to a_1 by an involution:

- $a_1 = xa_1x$ where x is the involution $1234 \to 1234$
- $a_2 = xa_1x$ where x is the involution $1234 \to 2134$
- $a_3 = xa_1x$ where x is the involution $1234 \to 3412$
- $a_4 = xa_1x$ where x is the involution $1234 \to 4231$.

This finishes the proof. □

Proposition 7.3 *If* $G \subseteq (4,4)$ *is a copy of* S_3, *then its convex closure cannot be embedded into* $\mathcal{Q}$.

Proof. Let $H \subseteq (4,4)$ be the copy of S_3 generated by the elements

$$\bar{a} = \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} \quad \& \quad \bar{b} = \begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix}$$

where $a, b \in S_3 \subseteq (3,3)$. We claim that G is conjugate to H.

Since G is isomorphic to S_3, it contains an element x of order three. By Lemma 7.2, x belongs to $\{a_1, a_2, a_3, a_4, a_1^2, a_2^2, a_3^2, a_4^2\}$. If $x = a_i^2 \in G$, then since

G is a group,

$$x^2 = (a_i^2)(a_i^2) = a_i a_i^3 = a_i \cdot I = a_i \in G.$$

Thus, G contains one of the elements a_1, a_2, a_3, a_4.

Suppose first that $a_1 \in G$ and let $b_1 \in G$ be any nontrivial involution. Then $f = a_1 b_1$ is an nontrivial involution since $G \simeq S_3$. Thinking of b_1 as the bijection $b_1 : \{1,2,3,4\} \to \{1,2,3,4\}$ given by $1234 \to b_1(1)b_1(2)b_1(3)b_1(4)$ and f as the bijection $f : \{1,2,3,4\} \to \{1,2,3,4\}$ given by $1234 \to f(1)f(2)f(3)f(4)$, we see that $b_1(1) = 1$:

- If $b_1(1) = 2$, then $f^2(3) = 1$, contradicting the fact that f is an involution,
- If $b_1(1) = 3$, then $f^2(4) = 1$, contradicting the fact that f is an involution,
- If $b_1(1) = 4$, then $f^2(2) = 1$, contradicting the fact that f is an involution.

Thus, $b_1(1) = 1$, so b_1 is determined by an involutive permutation of the last three elements. Then b_1 is one of

$$\bar{b} = \begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix} \in H, \qquad \bar{c} = \begin{pmatrix} 1 & 0 \\ 0 & c \end{pmatrix} \in H, \qquad \bar{d} = \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} \in H.$$

Then G contains $a_1 = \bar{a} \in H$ and also contains one of the nontrivial involutions of H. Since S_3 is determined by an element of order three and a nontrivial involution, $G = H$.

Now suppose that some $a_i \in G$. Then by Lemma 7.2, there is an involution $x \in (4,4)$ such that $xa_1x = a_i$. Then $xGx \simeq G \simeq S_3$ is a subgroup that contains a_1, so by the above argument, $xGx = H$. Since $H = xGx$, $\langle H \rangle = \langle xGx \rangle \simeq \langle G \rangle$. But $\langle H \rangle$ satisfies equation (9), which means that $\langle G \rangle$ does as well. As seen in Lemma 7.1, no copy of $S_3 \subseteq SO(3)$ can satisfy equation (9). Thus, $\langle G \rangle$ cannot be embedded into $\mathcal{Q}$. □

We now look to $(5,5)$.

Definition 7.4 Let $U_3 \subseteq (5,5)$ denote the copy of S_3 given by

$$U_3 = \left\{ I,\ \bar{a} = \begin{pmatrix} I & 0 \\ 0 & a \end{pmatrix},\ \bar{a}^2 = \begin{pmatrix} I & 0 \\ 0 & a^2 \end{pmatrix},\ \bar{b} = \begin{pmatrix} f & 0 \\ 0 & b \end{pmatrix},\ \bar{c} = \begin{pmatrix} f & 0 \\ 0 & c \end{pmatrix},\ \bar{d} = \begin{pmatrix} f & 0 \\ 0 & d \end{pmatrix} \right\}$$

where $S_3 = \{I, a, a^2, b, c, d\} \subseteq (3,3)$ is the natural copy of S_3 and $f = \text{flip} \in (2,2)$. U_3 is called the *unorthodox copy of* S_3.

A simple proof that U_3 is a copy of S_3 is that the product of a nontrivial involution (b, c, d) with either a or a^2 is a nontrivial involution.

In order to construct a copy of $S_3 \subseteq SO(3)$, we notice that in $S_3 = \{I, a, a^2, b, c, d\} \subseteq (3,3)$, each of the matrices I, a, a^2 have a determinant of $+1$, and so are rotations, while b, c, d have a determinant of -1. Thus, a candidate for $S_3 \subseteq SO(3)$ is

$$G = \{I, a, a^2, -b, -c, -d\} \subseteq SO(3).$$

Let us prove that this is in fact a copy of S_3:

Lemma 7.5 *The set $G \subseteq SO(3)$ is a group isomorphic to S_3. An isomorphism is given by*

- $\varphi(I) = I,\ \ \varphi(a) = a, \quad \varphi(a^2) = a^2,$
- $\varphi(b) = -b,\ \varphi(c) = -c,\ \varphi(d) = -d.$

Proof. By Theorem 6.13 on page 50 of [6], a presentation of the symmetric group on three letters is given by generators α, β with relations $\alpha^3 = \beta^2 = I$ and $\alpha\beta\alpha = \beta$. Within G, the elements a and $-b$ satisfy such relations, a property they inherit from $S_3 \subseteq (3,3)$. Thus, the group they generate is isomorphic to S_3. We define φ on these generators

$$\varphi(a) = a \quad \& \quad \varphi(b) = -b$$

and then extend it homomorphically. Because a and b generate S_3, φ is an isomorphism between S_3 and the group generated by a and $-b$. What we have to prove is that the latter group is G. We do so by explicitly calculating φ:

- $\varphi(I) = \varphi(b^2) = \varphi(b)\varphi(b) = (-b)(-b) = b^2 = I,$
- $\varphi(c) = \varphi(ab) = \varphi(a)\varphi(b) = a(-b) = -(ab) = c,$
- $\varphi(a^2) = \varphi(a)\varphi(a) = a^2,$
- $\varphi(d) = \varphi(a^2b) = \varphi(a^2)\varphi(b) = a^2(-b) = -(a^2b) = d.$ □

Consequently, the homomorphism specified on generators by $\varphi(\bar{a}) = a$ and $\varphi(\bar{b}) = -b$ is an isomorphism between U_3 and G. Its convex linear extension is an embedding:

Theorem 7.6 *The convex closure of $U_3 \subseteq (5,5)$ can be embedded into $\mathcal{Q}$.*

Proof. Let φ denote the natural isomorphism from U_3 to G and extend it convex linearly. For $f = x_0 I + x_1\bar{a} + x_2\bar{a}^2 + x_3\bar{b} + x_4\bar{c} + x_5\bar{d} \in \langle U_3 \rangle$ we have

$$f = \begin{pmatrix} x_0+x_1+x_2 & x_3+x_4+x_5 & 0 & 0 & 0 \\ x_3+x_4+x_5 & x_0+x_1+x_2 & 0 & 0 & 0 \\ 0 & 0 & x_0+x_3 & x_1+x_5 & x_2+x_4 \\ 0 & 0 & x_2+x_5 & x_0+x_4 & x_1+x_3 \\ 0 & 0 & x_1+x_4 & x_2+x_3 & x_0+x_5 \end{pmatrix},$$

while the corresponding element $\varphi(f) \in \langle G \rangle$ is then

$$\varphi(f) = \begin{pmatrix} x_0-x_3 & x_1-x_5 & x_2-x_4 \\ x_2-x_5 & x_0-x_4 & x_1-x_3 \\ x_1-x_4 & x_2-x_3 & x_0-x_5 \end{pmatrix}.$$

Let us first prove that φ is a well-defined function. If $f = g \in \langle U_3 \rangle$, where f is written as a convex sum using (x_i) and g is written using (y_i), set $c_i = x_i - y_i$. Since $f - g = 0$, we have the equations:

- $c_0 + c_3 = 0, \quad c_0 + c_4 = 0, \quad c_0 + c_5 = 0, \quad c_2 + c_3 = 0, \quad c_1 + c_4 = 0,$ and
- $c_3 + c_4 + c_5 = 0.$

From these equations, it easily follows that $c_i = 0$ for all i, which means $x_i = y_i$ for all i and thus that $\varphi(f) = \varphi(g)$.

To see that φ is injective, if $\varphi(f) = \varphi(g)$, we again set $c_i = x_i - y_i$ and from $\varphi(f) - \varphi(g) = 0$ derive equations that are even easier to solve:

$$c_0 - c_3 = 0, \quad c_0 - c_4 = 0, \quad c_0 - c_5 = 0, \quad c_2 - c_4 = 0, \quad c_1 - c_4 = 0.$$

So $c_i = c_0$ for all i. But $\sum c_i = 0$ since both (x_i) and (y_i) sum to one. Thus, $c_i = 0$ for all i, which means $f = g$, and so φ is injective. By the proof of Theorem 2 in [7], φ is thus an embedding. □

8 Classification

We now state in final form the collections of qubit channels that have a classical representation: there are five of them, each one being either a subgroup of $\mathbb{A}_4$ or a subgroup of S_3:

Theorem 8.1 *Let $\mathbb{A}_4 \subseteq (4,4)$ denote the alternating group on four letters and $S_3 \subseteq (5,5)$ denote the unorthodox copy of the symmetric group on three letters. Then*

(i) *For each subgroup G of $\mathbb{A}_4$, there is an embedding $\varphi : \langle G \rangle \to \mathcal{Q}$.*

(ii) *For each subgroup G of S_3, there is an embedding $\varphi : \langle G \rangle \to \mathcal{Q}$.*

(iii) *If $G \subseteq (m,n)$ is a group for which such an embedding exists, then G is either a subgroup of $\mathbb{A}_4$ or a subgroup of S_3. That is, G must be isomorphic to either $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_2^2$, S_3 or $\mathbb{A}_4$.*

Proof. (i) and (ii) follow from the fact that an embedding restricts to the convex closure of a subgroup. (iii) If G is nonabelian, then it is either $\mathbb{A}_4$ or S_3. If G is abelian, then it is either $\mathbb{Z}_2$, $\mathbb{Z}_3$ or $\mathbb{Z}_2^2$, each of which is a subgroup of $\mathbb{A}_4$. Thus, G is either a subgroup of $\mathbb{A}_4$ or a subgroup of S_3. □

As S_3 shows, it is not true that the convex closure of *any* copy of the five groups above can be embedded into $\mathcal{Q}$. However, the converse does hold: if $G \subseteq SO(3)$ is one of the five groups above, then its convex closure *is* isomorphic to a subset of either $\langle \mathbb{A}_4 \rangle \subseteq (4,4)$ or $\langle S_3 \rangle \subseteq (5,5)$. The reason is that all finite isomorphic subgroups of $SO(3)$ are conjugate [1]. Thus, the particular representations of $\mathbb{A}_4$ and S_3 considered in this paper capture a certain type of *quantum structure*.

Let us consider an example that will help to clarify the precise nature of the theorem above:

Example 8.2 *A convex linear injection that is not an embedding.* Define $\varphi : (3,3) \to \mathcal{Q}$ by

$$\varphi \begin{pmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ z_1 & z_2 & z_3 \end{pmatrix} = \frac{1}{3} \begin{pmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ z_1 & z_2 & z_3 \end{pmatrix}.$$

This is a convex linear injection that does not preserve products. Notice that there is no convex linear injection of $(3,3)$ that preserves products and the identity: if there were, it would restrict to an embedding of the convex closure of S_3 in $(3,3)$,

which is impossible by Lemma 7.1. Similarly, there is no embedding of (n, n) into $\mathcal{Q}$ when $n \geq 3$.

Thus, Theorem 8.1 is about the interaction between convexity and group theoretic structure.

9 Interpretation

Each time we rule out a group in the classification, we are identifying a difference between classical and quantum, by writing down an equation that holds quantum mechanically but not classically or vice-versa. The physical significance of the former is that they express multiple experiments for achieving the same task. For instance, if $f \in SO(3)$ is a generator for $\mathbb{Z}_4$, we can have an equation like

$$\frac{f + f^3}{2} = \frac{f^2 + f^4}{2} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

which is never true classically. This tells us that generators of $\mathbb{Z}_4$ and coin flips can be used to perform projective measurements in at least two different ways – depending on the context, one of these ways may be better than the other. This equation also makes the randomness in a projective measurement explicit.

Another interesting equation arises with the Klein four group $V = \{e, x, y, z\} \subseteq SO(3)$, where we can write

$$\frac{e + x + y + z}{4} = \left(\frac{e + x}{2}\right)\left(\frac{e + y}{2}\right) = 0.$$

This gives us multiple methods for completely disrupting the correlation between sender and receiver, with the second expression leaving the problem of randomness to nature. This is the quantum analogue of randomly flipping a classical bit [7].

10 Closing

It's natural now to wonder about the classical representation of quantum channels in higher dimensions. Other than the fact that involution groups of all orders can now be used and the fact that all such classes of channels arise as a convex subset of some $\langle SO(n) \rangle$, we do not know much else about the question.

However, even in the case of qubit channels, there is still much to be understood. For instance, while we have classified the groups that can be used to classically represent qubit channels, what are the classes of qubit channels which result? In the case of the Klein four group, the class represented is any maximal commutative collection of symmetric channels (for instance, the diagonal matrices). In the case of $\mathbb{Z}_2$, the channels described are bit flipping channels with respect to a particular spin matrix. For $\mathbb{Z}_3$, we know the channels described are those that are both stochastic and circulant, though we are not sure of what this means physically yet. Finally,

and most importantly, we have no idea which classes of channels are represented by $\mathbb{A}_4$ and S_3, be we suspect the answer is interesting.

Acknowledgement

We thank Alan Aspuru-Guzik for a helpful discussion about this work when it was still ongoing, Chris Fuchs for helping us navigate the literature and Sanjeevi Krishnan for help with algebraic topology (which is needed in the proof of (ii)(a)).

References

[1] M. Artin. *Algebra.* Prentice Hall, New Jersey, 1991.

[2] T.M. Cover and J.A. Thomas. *Elements of information theory.* Wiley, 1991.

[3] H. S. M. Coxeter. *Introduction to Geometry.* John Wiley and Sons, Inc. (1961), New York.

[4] H. S. M. Coxeter and W. O. J. Moser. *Generators and Relations for Discrete Groups.* Springer-Verlag (1965), Germany.

[5] R.A. Horn and C.R. Johnson. *Matrix Analysis.* Cambridge University Press, New York, 1985.

[6] T. Hungerford. *Algebra.* Springer-Verlag, New York, 1974.

[7] K. Martin. *How to randomly flip a quantum bit.* Proceedings of Quantum Physics and Logic 2008, Electronic Notes in Theoretical Computer Science, to appear.

[8] K. Martin. *The scope of a quantum channel.* Mathematical Structures in Computer Science, Cambridge University Press, to appear.

[9] A. Nayak and P. Sen. *Invertible quantum operations and perfect encryption of quantum states.* `http://arxiv.org/abs/quant-ph/0605041v4`

[10] M. Nielsen and I. Chuang, Quantum computation and quantum information. Cambridge University Press, 2000.

[11] D. Saracino. *Abstract algebra: a first course.* Addison-Wesley, 1980.

[12] D. Serre. *Matrices: Theory and applications.* Springer-Verlag, Graduate Texts in Mathematics, 2000.