

[Electronic Notes in Theoretical Computer Science 270 (2) (2011) 37–58](http://dx.doi.org/10.1016/j.entcs.2011.01.022)

[www.elsevier.com/locate/entcs](http://www.elsevier.com/locate/entcs)

Classical Representations of Qubit Channels

## Tanner Crowder[1](#_bookmark1) Keye Martin[2](#_bookmark0)

*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.

# Introduction

In [[7](#_bookmark21)], the Klein four group Z2 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?

2

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 A4, 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](mailto:crowder@chacs.nrl.navy.mil)

2 Email: [kmartin@itd.nrl.navy.mil](mailto:kmartin@itd.nrl.navy.mil)

1571-0661 Published by Elsevier B.V. Open access under [CC BY-NC-ND license](http://creativecommons.org/licenses/by-nc-nd/3.0/).

[doi:10.1016/j.entcs.2011.01.022](http://dx.doi.org/10.1016/j.entcs.2011.01.022)

channels represented by the convex closure of *S*3 and A4 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?

# 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 *Q* con- sists of all affine transformations of the unit ball in R3 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 *×X⟩*.

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 *×G⟩* into *Q* is a function *ϕ* : *×G⟩→Q* such that for all *x, y ∈ ×G⟩*,

* + *ϕ*(*I*)= *I*,
  + *ϕ*(*xy*)= *ϕ*(*x*)*ϕ*(*y*),
  + *ϕ*(*px* + (1 *− p*)*y*)= *pϕ*(*x*)+ (1 *− p*)*ϕ*(*y*) whenever *p ∈* [0*,* 1], and
  + *ϕ*(*x*)= *ϕ*(*y*) *⇒ x* = *y*.

That is, an *embedding* is an injective, convex-linear homomorphism. The set of qubit channels *ϕ*(*×G⟩*) is then said to have a *classical representation*.

**Proposition 2.2** *Let G be a subgroup of* (*m, n*)*. If there is an embedding ϕ* : *×G⟩→ Q, then n* = *m, G is ﬁnite and the image of ϕ is isomorphic to a convex subset of ×SO*(3)*⟩.*

**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 permuta- tion 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 B3 into itself. By algebraic topology, *f* must take the boundary of the unit ball into itself:

(*∀x ∈* B3) *|x|* =1 *⇒ |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 ∈* R3 such that *Mx* = *e*1. Writing *x* as a linear combination of the *ei*, we have

3

Σ

(*e*1*, b*)= (*Mx, b*)= *xi*(*Mei, b*)= 0*.*

*i*=1

Similarly, (*ei, 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](#_bookmark22)], *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 Theo- rem 2.1 of [[9](#_bookmark23)] 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](#_bookmark22)]).

Either way, the image of *ϕ* is isomorphic to a convex subset of *×SO*(3)*⟩*, where

*SO*(3) is the group of orthogonal matrices with determinant +1. *2*

# Cyclic groups

By the result of the last section, we know that any group whose convex closure may be embedded into *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

,1 0 0 ⎞

*rx*(*θ*) := 0 cos *θ* sin *θ*

⎝ ⎠

0 *−* sin *θ* cos *θ*

for some angle *θ ∈* (0*,* 2*π*]. Notice that *rx*(*α*)*rx*(*β*)= *rx*(*α* + *β*).

**Lemma 3.2** *If f ∈ SO*(3) *then there is r ∈ SO*(3) *such that*

*rfrt* = *rx*(*θ*)

*for some angle θ ∈* (0*,* 2*π*]*.*

**Proof**. Each 3 *×* 3 rotation *f* is a normal matrix, so by Theorem 3.3 of [[12](#_bookmark25)], we can find an orthogonal matrix *r* such that *rfrt* 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 *a b* . If det(*r*)= *−*1, we replace *r* by *−r* since det(*−r*)= (*−*1)3 det(*r*) and

*−b a*

thus we assume that *r ∈ SO*(3). Again because we are in dimension three, only two cases are possible: either *rfrt* is a diagonal matrix or it has the form

,*c* 0 0 ⎞

*rfrt* = ⎝0 *a b* ⎠

0 *−b a*

where *c* = *±*1 is a real eigenvalue of *f* . Using det(*r*)= 1*/* det(*rt*) since *rt* = *r−*1, det(*rfrt*)= det(*r*) det(*f* ) det(*rt*)= 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

*rfrt* is diagonal, we see that *rfrt* must be either the identity or one of the matrices

,1 0 0 ⎞ ,*−*1 0 0 ⎞ ,*−*1 0 0⎞

*sx* = ⎝0 *−*1 0 ⎠ *, sy* = ⎝ 0 1 0 ⎠ *, sz* = ⎝ 0 *−*1 0⎠ *.*

0 0 *−*1

0 0 *−*1

0 0 1

The identity and *sx* have the desired form. In the case *rfrt* = *sy*, we conjugate by the rotation

,0 1 0⎞

*a* = ⎝0 0 1⎠

1 0 0

to obtain *arf* (*ar*)*t* = *sx* which again has the desired form. In the case *rfrt* = *sz*, we conjugate by *at*.

Finally, because (*a, b*) is a point on the unit circle, there is an angle *θ ∈* (0*,* 2*π*] such that *a* = cos *θ* and *b* = sin *θ*. Thus, in all cases, we have *rfrt* = *rx*(*θ*). *2*

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

**Lemma 3.3** *Let f ∈ SO*(3) *have order n ≥* 2 *and let G* = *{fi* :1 *≤ i ≤ n}* Z*n be the cyclic group that it generates. Then there is a nonzero integer x ∈* Z *and an r ∈ SO*(3) *such that*

*rfxrt* = *rx*(2*π/n*)*.*

*Thus, G is also generated by an element fx ∈ G that is conjugate to rx*(2*π/n*)*.*

**Proof**. Let *a* = *rx*(2*π/n*). It is routine to show that *a* has order *n* and thus generates Z*n*. By Lemma [3.2](#_bookmark2), take *r ∈ SO*(3) with *rfrt* = *rx*(*θ*). Since *f* has order *n*, so does *rx*(*θ*) and thus *rx*(*θ*)*n* = *rx*(*nθ*) = *I*. Then *θ ∈* (0*,* 2*π*] has the form *θ* = 2*πk/n* for an integer 0 *< k < n*. But

*rx*(*θ*)= *rx*

2*πk*

*n*

= *rx*

2*π* *k*

*n*

= *ak*

and by standard group theory, since *a* has order *n*, the order of *ak* is *n/*(*k, n*), where (*k, n*) is the greatest common divisor of *k* and *n*. But we know that *ak* = *rx*(*θ*) 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 /*=0 since *n ≥* 2. Now we calculate as follows:

*rfxrt* = (*ak*)*x* = *akx* = *a*1*−yn* = *a*1*a−yn* = *a*(*an*)*−y* = *a*(*I*)*−y* = *a* (1) and since *a* has order *n*, so does *fx*. Then the fact that (*fx*)*n* = *I* implies

*{*(*fx*)*i* :1 *≤ i ≤ n}⊆ {fi* :1 *≤ i ≤ 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 *rx*(2*π/n*). *2* In particular, a finite cyclic subgroup of *SO*(3) is conjugate to the one generated

by *rx*(2*π/n*), so any two finite cyclic subgroups of *SO*(3) with the same order are conjugate. We now classify the cyclic subgroups of *Q* that have classical represen- tations. This requires a few lemmas in advance.

**Lemma 3.4** *For all n ≥* 4*, there is an integer k ≥* 1 *such that n <* 2*k <* 3*n .*

4 4

**Proof**. First, log2(3*n*) *−* log2(*n*) = log2(3) *>* log2(2) = 1, so the interval [log2 *n,* log2 3*n*] contains at least one integer, call it *m*. Then log2(*n*) *≤ m <* log2(3*n*) where the strict inequality on the right holds because 3*n* is never a power of two.

If *m* = log2(*n*), then because the length of [log2 *n,* log2 3*n*] is strictly greater than 1, it must also contain *m* + 1, so set *p* := *m* + 1. If not, set *p* := *m*. Either way,

log2(*n*) *< p <* log2(3*n*) =*⇒ n <* 2*p <* 3*n.*

Dividing by 4, we get *n/*4 *<* 2*p−*2 *<* 3*n/*4. Because *p >* log2(*n*) *≥* log2(4) = 2,

*p ≥* 3 so the desired integer is *k* := *p −* 2 *≥* 1. *2*

Recall that the element in position (*i, j*) of a matrix *a* is denoted by *aij*.

**Lemma 3.5** *Let a ∈* (*n, n*) *and let m ∈* N *be divisible by 2. If am*

*ii*

= 0 *then*

*am/*2 = 0*.*

*ii*

**Proof**. If *A* and *B* are two *n × n* matrices, their product *AB* satisfies (*AB*)*ii* =

Σ

*n r*=1

*Ai,rBr,i*. Since *am* = *am/*2*am/*2, we have

0= *am* = Σ *am/*2*am/*2*.*

*n*

*ii*

*i,r*

*r,i*

*r*=1

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 *am/*2*am/*2 is zero, which means *am/*2 = 0. *2*

*ii ii* *ii*

**Proposition 3.6** *The convex closure of* Z*n ⊆* (*m, m*) *cannot be embedded into Q*

*when n ≥* 4*.*

**Proof**. Let *G* = *{gi* : 1 *≤ i ≤ n} ⊆ SO*(3) be a cyclic group of order *n* with generator *g*. By Lemma [3.3](#_bookmark3), we can assume that there is *r ∈ SO*(3) with *rgrt* = *rx*(*θ*) and *θ* = 2*π/n*. For the remainder of this proof, *rx*(*θ*) will be denoted by *rx*. The average of all elements in *rGrt*,

*n i*

Σ

*⊥* := *rx , n*

*i*=1

is the unique algebraic zero of the monoid *×rGrt⟩*: the only element *⊥∈ ×rGrt⟩* such that *⊥· x* = *x ·⊥* for all *x ∈ ×rGrt⟩*. We will now show that there are *x, y ∈* [0*,* 1] with *x* + *y* = 1 and

*r* + *rt* *rj* + (*rj* )*t*

*x*

*x*

*x*

+ *y*

*x*

*x*

= *⊥.* (2)

2

2

Using Lemma [3.4](#_bookmark4), let *j* be a power of two such that *n < j <* 3*n* . Then because

4

4

*π/*2 *< jθ <* 3*π/*2, we have cos(*jθ*) *<* 0, while 0 *< θ ≤ π/*2 gives cos *θ ≥* 0. Defining

*x* :=

cos *jθ*

cos *jθ −* cos *θ*

*∈* (0*,* 1]

and setting *y* =1 *− x ∈* [0*,* 1) we have

*r* + *rt* *rj* + (*rj* )*t*

,1 0 0

⎞ ,1 0 0⎞

*x x x* +*y x* *x*

2 2

= ⎝0 *x* cos *θ* + *y* cos *jθ* 0

⎠ = ⎝0 0 0⎠ *.*

0 0 0

This projection belongs to *×rGrt⟩* since we have written it as a convex sum of elements belonging to *×rGrt⟩*. To see that equation ([2](#_bookmark6)) holds in *×rGrt⟩*, notice that

0 0 *x* cos *θ* + *y* cos *jθ*

,1 0 0⎞ ,1 0 0⎞ ,1 0 0⎞

*rx*(*α*) ⎝0 0 0⎠ = ⎝0 0 0⎠ *rx*(*α*)= ⎝0 0 0⎠

0 0 0

0 0 0

0 0 0

for any *α*; thus, this projection is the algebraic zero for *×rGrt⟩* and thus equal to *⊥*.

Multiplying equation ([2](#_bookmark6)) on the left by *rt* and on the right by *r*, the analogous equation holds in *×G⟩*:

*g* + *gt*

*x*

2

*gj* + (*gj*)*t*

+ *y* =

2

Σ*i*=1

*gi*

*n*

*n* = *⊥G.* (3)

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

*a ∈* (*m, m*) be a generator for a copy of Z*n*. If

*a* + *at*

*x*

2

*aj* + (*aj*)*t*

+ *y*

2

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

*a*2 + *I*

*x*

2

*aj*+1 + *an−j*+1

+ *y*

2

*a* + *at*

= *x*

2

*aj* + (*aj*)*t*

+ *y .*

2

Rearranging terms we can see that

*xI* = *xa* + *xat* + *yaj* + *y*(*aj*)*t − xa*2 *− yaj*+1 *− yan−j*+1*.* (4) Since *a* generates Z*n* and *j <* 3*n/*4 *< n*, *aj /*= *I*. Because *a* and hence *aj* is a

permutation, there is an entry *aj* on the diagonal of *aj* which is equal to zero.

*ii*

Since *j* = 2*k* with *k ≥* 1, *j* is divisible by 2, so by Lemma [3.5](#_bookmark5), *a*2

*ii*

= 0 and thus

*aii* = 0 as well. Since transposes do not alter diagonals, *at*

*ii*

=0 and (*aj*)*t*

= 0. For

the (*i, i*) entry of the matrix in equation ([4](#_bookmark8)), we have

*ii*

*x* = *−y*(*aj*+1 + *an−j*+1)*.*

*ii* *ii*

Since the powers of *a* are permutations, *aj*+1+*an−j*+1 is either 0, 1 or 2, contradicting

*x >* 0.

*ii* *ii*

Since equation ([3](#_bookmark7)) holds for any quantum generator of Z*n* but never holds for a classical generator of Z*n*, the convex closure of Z*n ⊆* (*m, m*) can never be embedded into *Q* when *n ≥* 4. *2*

An interesting consequence of the last proof is that for an integer *n ≥* 4,

*n n*

Σ cos(2*π/n · k*)=0= Σ sin(2*π/n · k*)*.*

*k*=1

*k*=1

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

flip = 0 1

1 0

,0 1 0⎞ 1 0 0

denote generators for Z2 and Z3 respectively.

*∈* (2*,* 2) & *c* = ⎝0 0 1⎠ *∈* (3*,* 3)

### Theorem 3.7

* *If G ⊆* (*m, m*) *is a cyclic group and ϕ* : *×G⟩ → Q is an embedding, then G* Z2

*or G* Z3*.*

* *The convex closure of the groups* Z2 *{I,* flip*} and* Z3 *{I, c, c*2*} can be embed- ded into Q.*

**Proof**. For Z2, we map *I,* flip *∈* (2*,* 2) onto the spin channels

,1 0 0⎞ ,1 0 0 ⎞

*I* = ⎝0 1 0⎠ & *sx* = ⎝0 *−*1 0 ⎠

0 0 1

0 0 *−*1

and then extend linearly to obtain an embedding

*x*1 *x*2

,*x*1 + *x*2 0 0 ⎞

*ϕ x*2 *x*1 = ⎝

⎠

0 *x*1 *− x*2 0 *.*

0 0 *x*1 *− x*2

For Z3, *c* is a classical channel that generates Z3. However, it is also a qubit channel: as a permutation, it is orthogonal, and direct calculation shows that det(*c*)= 1, so that *c ∈ SO*(3). Thus, its convex closure embeds into *Q* via the identity map! *2*

# Finite abelian groups

**Lemma 4.1** *If Q contains a copy of the group* Z*n, then n* =1 *or n* = 2*.*

2

**Proof**. Any involution *f ∈ Q* must be a rotation and hence symmetric since *f* = *f−*1 = *ft*. Thus, there is a rotation *r ∈ SO*(3) such that *rfrt* is diagonal. However, *rfrt ∈ SO*(3) is also an involution, but the only diagonal involutions in *SO*(3) are the *spin channels*:

,1 0 0⎞ ,1 0 0 ⎞ ,*−*1 0 0 ⎞ ,*−*1 0 0⎞

*I* = ⎝0 1 0⎠ *, sx* = ⎝0 *−*1 0 ⎠ *, sy* = ⎝ 0 1 0 ⎠ *, sz* = ⎝ 0 *−*1 0⎠ *.*

0 0 1

0 0 *−*1

0 0 *−*1

0 0 1

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 *Q* contains a copy of Z*n*, then it contains 2*n* commutative involutions.

Because all the elements of Z*n* commute, they diagonalize in a common basis. Thus, there is *r ∈ SO*(3) such that *rfrt ∈ SO*(3) is a diagonal involution for each *f ∈* Z*n*. Then *r* (Z*n*) *rt ⊆ {I, sx, sy, sz}.* And since the number of elements in the group *r* (Z*n*) *rt* is 2*n*, we have that either *n* =1 or *n* = 2. *2*

2

2

2

2

2

Let *rz*(*θ*) denote the principal rotation about the *z*-axis:

,cos *θ −* sin *θ* 0⎞

*rz*(*θ*)= ⎝sin *θ* cos *θ* 0⎠ *.*

0 0 1

From annoying arithmetic, it follows that *rx*(*θ*) and *rz*(*α*) commute iff they are both diagonal.

**Lemma 4.2** *If Q contains a copy of the group* Z*n, then n* = 1*.*

3

**Proof**. Suppose *Q* contains a copy of Z2. Let *f, g ∈* Z2 *⊆ SO*(3) be elements of

3 3

order 3 such that

*{fi* :1 *≤* 3*}∩ {gi* :1 *≤ i ≤* 3*}* = *{I}.*

Notice that Z2 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.

3

Because *f, g ∈ SO*(3) are commutative normal matrices, by Theorem 2.5.15 of [[5](#_bookmark19)], there is a single orthogonal matrix *r* such that *rfrt* and *rgrt* are block diagonal, each block being either a 1 *×* 1 matrix consisting of a real eigenvalue or a 2 *×* 2 matrix of the form *a b* .

*−b a*

Because *f* and *g* have order 3, so do *rfrt* and *rgrt*, 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

,*c* 0 0 ⎞

⎝0 *a b* ⎠ &

0 *−b a*

, *a b* 0 ⎞

0 0 *c*

⎝*−b a* 0 ⎠ *.*

Because *c* refers to a real eigenvalue of an orthogonal matrix, *c* = *±*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 *rx*(*θ*) for *θ ∈* (0*,* 2*π*] and the second has the form *rz*(*α*) for some *α ∈* (0*,* 2*π*].

However, because *f* and *g* commute, *rfrt* and *rgrt* also commute, and this means that both have the form *rx*(*θ*) or both have the form *rz*(*α*), since *rx*(*θ*) and *rz*(*α*) only commute when they are diagonal (which as we have seen, is impossible because *rfrt* and *rgrt* have order three). Thus, without loss of generality,

*rfrt* = *rx*(*θ*) & *rgrt* = *rx*(*α*)

where *θ* = 2*πk/*3 and *α* = 2*πm/*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 /*= *m*, then without loss of generality, *k* = 1 and *m* = 2. This gives

*fg* = *rt rx*(2*π/*3)*r rt rx*(4*π/*3)*r* = *rtrx*(6*π/*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 Z2.

3

If *Q* contains a copy of Z*n ⊆ SO*(3) for *n >* 1, then it contains a copy of Z2,

3 3

which as we have seen, is impossible. *2*

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:

*n*

*p*

*G* Z *ri i*

*i*=1

where the *pi* are primes, not necessarily distinct, and each *ri ≥* 1. We will now classify the abelian groups that can be used to represent qubit channels. Let

*{I ⊗ I, I ⊗* flip*,* flip *⊗ I,* flip *⊗* flip*}⊆* (4*,* 4) denote the natural copy of the Klein four group studied in [[7](#_bookmark21)].

### Theorem 4.3

* *If G ⊆* (*m, m*) *is an abelian group and ϕ* : *×G⟩ → Q is an embedding, then G is isomorphic to* Z2*,* Z3 *or* Z2*.*

2

* *The convex closure of the groups* Z2 *{I ⊗ I, I ⊗* flip*,* flip *⊗ I,* flip *⊗* flip*},* Z3

2

*{I, c, c*2*} and* Z2 *{I,* flip*} can be embedded into Q.*

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

*n*

*p*

*G* Z *ri i*

*i*=1

where the *pi* are primes, not necessarily distinct, and each *ri ≥* 1. If one of these primes *pi ≥* 5, then because *pi* divides the order of *G*,

*n n*

*|G|* = *|*Z *ri |* = *pri ,*

*i*=1

*i*=1

*pi*

*i*

the converse of Lagrange’s theorem for finite abelian groups implies that *G* must have a subgroup of order *pi*. But the only finite abelian group of order *pi* is Z*pi* , a cyclic group having order greater than 3. Since the convex closure of Z*pi* cannot be embedded in *Q* by Theorem [3.7](#_bookmark9), neither can the convex closure of *G*. Thus, there are three possibilities for *G*:

*n i*=1 *n*

(2) *G*

*i*=1

Z2*ri* with *n ≥* 1 and each *ri ≥* 1,

Z3*ri* with *n ≥* 1 and each *ri ≥* 1, or

(1) *G*

(3) *G* *n* Z2*ri ×* *m* Z3*si* with *n, m ≥* 1 and each *ri, si ≥* 1.

*i*=1

*i*=1

In case (1), each *ri* = 1 or else *G* has a cyclic subgroup of order *≥* 4, contradicting Theorem [3.7](#_bookmark9). Thus, *G* is simply a product of copies of Z2. By Lemma [4.1](#_bookmark10), the only possibilities are Z2, whose convex closure can be embedded by Theorem [3.7](#_bookmark9), and Z2, the latter of which we will show later in this proof has a convex closure that can be embedded.

2

In case (2), each *ri* = 1 or else *G* has a cyclic subgroup of order *≥* 4, contradicting Theorem [3.7](#_bookmark9). Thus, *G* is simply a product of copies of Z3. By Lemma [4.2](#_bookmark11), the only possibility is Z3, whose convex closure can be embedded by Theorem [3.7](#_bookmark9).

In case (3), *G* has a subgroup *H* Z2*r*1 *×* Z3*s*1 where *r*1*, s*1 *≥* 1. Because *H* is a product of cyclic groups whose orders are relatively prime, by Theorem 6.1 of [[11](#_bookmark24)], we have *H* Z2*r*1 3*s*1 , a cyclic group of order *|H|* = 2*ri* 3*si ≥* 6 *≥* 4, which is impossible by Theorem [3.7](#_bookmark9).

Now let us prove that the convex closure of Z2 = *{I⊗I, I⊗*flip*,* flip*⊗I,* flip*⊗*flip*}* can be embedded into *Q*. Using the spin channels from Lemma [4.1](#_bookmark10), we extend the natural isomorphism

2

*I ⊗ I '→ I, I ⊗* flip *'→ sx,* flip *⊗ I '→ sy,* flip *⊗* flip *'→ sz*

convex linearly to obtain

,*x*1 *x*2 *x*3 *x*4⎞

,*x*1 + *x*2 *− x*3 *− x*4 0 0 ⎞

*x*2 *x*1 *x*4 *x*3

⎜⎝ ⎟⎠ ⎝

*ϕ x*3 *x*4 *x*1 *x*2 =

⎠

*x*4 *x*3 *x*2 *x*1

0 *x*1 *− x*2 + *x*3 *− x*4 0 *.*

0 0 *x*1 *− x*2 *− x*3 + *x*4

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 ∈ ×*Z2*⟩* be defined by a convex sum involving probabilities *xi* and *yi* respectively. If *ϕ*(*f* )= *ϕ*(*g*), then

2

*ϕ*(*f* ) *− ϕ*(*g*)= *c*1*I* + *c*2*sx* + *c*3*sy* + *c*4*sz* =0

where each *ci* = *xi − yi* so that Σ4 *ci* = 0. Then the *ci* satisfy the following four

*i*=1

equations:

*c*1 + *c*2 + *c*3 + *c*4 =0 (5)

*c*1 + *c*2 *− c*3 *− c*4 =0 (6)

*c*1 *− c*2 + *c*3 *− c*4 =0 (7)

*c*1 *− c*2 *− c*3 + *c*4 = 0*.* (8)

Adding ([7](#_bookmark12)) and ([8](#_bookmark12)) gives *c*1 = *c*2. Substituting this into ([7](#_bookmark12)) gives *c*3 = *c*4. Substi- tuting both of these into ([6](#_bookmark12)) gives *c*1 = *c*3. Then *c*1 = *c*2 = *c*3 = *c*4. By ([5](#_bookmark12)), each *ci* = 0 and thus *xi* = *yi* for all *i*. This proves *f* = *g* so that *ϕ* is injective. *2*

# Finite groups

In this section, we show that there are at most two nonabelian groups that can be used to represent qubit channels. Let A4 denote the alternating group on four letters and let *S*3 denote the symmetric group on three letters.

**Theorem 5.1** *If G ⊆* (*n, n*) *is a nonabelian group whose convex closure can be embedded into Q, then G is either isomorphic to* A4 *or to S*3*.*

**Proof**. If *|G|* is divisible by a prime *p ≥* 5, then by Theorem 5.2 of [[6](#_bookmark20)], *G* contains an element of order *p* and thus a subgroup isomorphic to Z*p*. By Theorem [3.7](#_bookmark9), *×G⟩* cannot be embedded into *Q*. Then let us factor *|G|* into a product of its possible prime powers as *|G|* = 2*p*3*q* where *p, q ≥* 0.

If *q ≥* 2, then *G* contains a subgroup of order 32 by the first Sylow theorem, Theorem 5.7 of [[6](#_bookmark20)], but then by Exercise 13 on page 98 of [[6](#_bookmark20)], this subgroup must be abelian, which is impossible by Theorem [3.7](#_bookmark9). Thus, 0 *≤ q ≤* 1.

Write *|G|* = 2*p*3*q*, where *p ≥* 0 and 0 *≤ q ≤* 1. If *p ≥* 3, then by the first Sylow theorem, *G* contains a subgroup of order 23 = 8. By Theorem [4.3](#_bookmark12), 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](#_bookmark20)], so *G* contains a copy of Z4, which is impossible by Theorem [3.7](#_bookmark9). Thus, 0 *≤ p ≤* 2.

Write *|G|* = 2*p*3*q* with 0 *≤ p ≤* 2 and 0 *≤ q ≤* 1. If *p* = 0, then *G* is either the trivial group (*q* = 0) or Z3 (*q* = 1), using the table on page 98 of [[6](#_bookmark20)]. Similarly, if *q* = 0, then by the same table, the only nontrivial groups are Z2, Z4 and Z2, all of

2

which are abelian. Thus, *q* =1 and 1 *≤ p ≤* 2.

Write *|G|* = 2*p*3 with1 *≤ p ≤* 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](#_bookmark20)]. If *p* = 2, then *|G|* = 12, and using the same table, the only nonabelian groups of order 12 are *D*6, *T* and A4. Both of the groups *D*6 and *T* contain elements of order 6, by remarks (i) and (ii) on page 98 of [[6](#_bookmark20)], and thus contain a copy of Z6, in contrast to Theorem [3.7](#_bookmark9).

Thus, the only two nonabelian groups capable of being embedded into *Q* are A4

and *S*3. *2*

By Lagrange’s theorem, any subgroup of a finite group must divide the order of the group. Because *|S*3*|* = 6 and *|*A4*|* = 12, any proper subgroup of *S*3 must have order 2 or 3, while any proper subgroup of A4 must have order 2*,* 3*,* 4 or 6. However, by Exercise 8 on Page 51 of [[6](#_bookmark20)], A4 does not have a subgroup of order 6. The only groups of order 2 and 3 are Z2 and Z3, while the only groups of order four are Z4 and Z2. Thus, all the proper subgroups of A4 and *S*3 have convex closures that can be embedded into *Q*, so there is no obvious way to rule either case out. In addition, *S*3 is not a subgroup of A4, so the cases A4 and *S*3 must be considered separately.

2

## A4

The set of even permutations in (4*,* 4) comprises a group A4 called the *alternating group on four letters*. Explicitly, its involutions are

,1 0 0 0⎞ ,0 1 0 0⎞ ,0 0 1 0⎞ ,0 0 0 1⎞

0 1 0 0 1 0 0 0 0 0 0 1 0 0 1 0

⎜ ⎟ ⎜ ⎟ ⎜ ⎟ ⎜ ⎟

*I* = *, x* = *, y* = *, z* = *,*

⎝ ⎠

⎝ ⎠

⎝ ⎠

⎝ ⎠

0 0 1 0

0 0 0 1

0 0 0 1

0 0 1 0

1 0 0 0

0 1 0 0

0 1 0 0

1 0 0 0

its order three elements are

,0 0 0 1⎞ ,0 1 0 0⎞ ,1 0 0 0⎞ ,0 0 1 0⎞

0 1 0 0 0 0 0 1 0 0 1 0 1 0 0 0

⎜ ⎟ ⎜ ⎟ ⎜ ⎟ ⎜ ⎟

*a* = *, b* = *, c* = *, d* = *,*

⎝ ⎠

⎝ ⎠

⎝ ⎠

⎝ ⎠

1 0 0 0

0 0 1 0

0 0 1 0

1 0 0 0

0 0 0 1

0 1 0 0

0 1 0 0

0 0 0 1

together with their squares:

,0 0 1 0⎞ ,0 0 0 1⎞ ,1 0 0 0⎞ ,0 1 0 0⎞

2 0 1 0 0 2 1 0 0 0 2 0 0 0 1 2 0 0 1 0

*a* = ⎜ ⎟ *, b* = ⎜ ⎟ *, c* = ⎜ ⎟ *, d* = ⎜ ⎟ *.*

⎝ ⎠

⎝ ⎠

⎝ ⎠

⎝ ⎠

0 0 0 1

1 0 0 0

0 0 1 0

0 1 0 0

0 1 0 0

0 0 1 0

1 0 0 0

0 0 0 1

A quick proof that the matrices above give a copy of A4 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 A4:

**Definition 6.1** A4 := *{I, x, y, z, a, b, c, d, a*2*, b*2*, c*2*, d*2*}⊆* (4*,* 4).

Notice that any copy of A4 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 A4 within *SO*(3). Starting with the involutions of Lemma [4.1](#_bookmark10), we take

,1 0 0⎞ ,1 0 0 ⎞ ,*−*1 0 0 ⎞ ,*−*1 0 0⎞

*I* = ⎝0 1 0⎠ *, sx* = ⎝0 *−*1 0 ⎠ *, sy* = ⎝ 0 1 0 ⎠ *, sz* = ⎝ 0 *−*1 0⎠ *,*

0 0 1

0 0 *−*1

0 0 *−*1

0 0 1

and we choose our order three generator to be

, 0 *−*1 0⎞

*f* = ⎝ 0 0 1⎠ *.*

*−*1 0 0

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

,0 *−*1 0 ⎞ ,0 1 0⎞ , 0 1 0 ⎞

*g* = *sxf* = ⎝0 0 *−*1⎠ *, h* = *gsx* = ⎝0 0 1⎠ *, j* = *sxh* = ⎝ 0 0 *−*1⎠ *.*

1 0 0

1 0 0

*−*1 0 0

along with their squares:

, 0 0 *−*1⎞

, 0 0 1⎞

⎝ ⎠

,0 0 1⎞

⎝ ⎠

2

,0 0 *−*1⎞

⎝ ⎠

2

*f* = *−*1 0 0 *, g*

2

⎝ ⎠

2

0 1 0

= *−*1 0 0 *, h*

0 *−*1 0

= 1 0 0 *, j*

0 1 0

= 1 0 0 *.*

0 *−*1 0

**Definition 6.2** *G* := *{I, sx, sy, sz, f, g, h, j,f* 2*, g*2*, h*2*, j*2*}⊆ SO*(3).

The set *G* forms a group isomorphic to A4 in a natural way. Let us prove this:

**Lemma 6.3** *The set G ⊆ SO*(3) *is a group isomorphic to* A4 *⊆* (4*,* 4)*. An isomor- phism ϕ is*

* *ϕ*(*I*)= *I, ϕ*(*x*)= *sx, ϕ*(*y*)= *sy, ϕ*(*z*)= *sz,*
* *ϕ*(*a*)= *f, ϕ*(*b*)= *g, ϕ*(*c*)= *h, ϕ*(*d*)= *j,*
* *ϕ*(*a*2)= *f* 2*, ϕ*(*b*2)= *g*2*, ϕ*(*c*2)= *h*2*, ϕ*(*d*2)= *j*2*.*

**Proof**. By page 225 of [[1](#_bookmark18)], a presentation of the alternating group on four letters is given by generators *α* and *β* and relations *α*3 = *β*3 = (*αβ*)2 = *I*. Within *G*, the elements *j* and *h*2 satisfy such relations. Thus, the group they generate is isomorphic to A4. We define *ϕ* on these generators

*ϕ*(*d*)= *j* & *ϕ*(*c*2)= *h*2

and then extend *ϕ* homomorphically. By [[1](#_bookmark18)], *c*2 and *d* generate A4, so *ϕ* is an isomorphism between A4 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 = *sx* and

*dc*2 = *x*,

* *ϕ*(*x*)= *ϕ*(*dc*2)= *ϕ*(*d*)*ϕ*(*c*2)= *jh*2 = *sx*,
* *ϕ*(*I*)= *ϕ*(*x*2)= *ϕ*(*x*)*ϕ*(*x*)= *sxsx* = *I*.

Using the equations mentioned before the definition of A4, as well as those mentioned during the definition of *G*, we can now calculate it on *a, b* and *c*:

* *ϕ*(*c*)= *ϕ*(*xd*)= *ϕ*(*x*)*ϕ*(*d*)= *sxj* = *h*
* *ϕ*(*b*)= *ϕ*(*cx*)= *ϕ*(*c*)*ϕ*(*x*)= *hsx* = *g*
* *ϕ*(*a*)= *ϕ*(*xb*)= *ϕ*(*x*)*ϕ*(*b*)= *sxg* = *f.*

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

*ϕ*(*y*)= *ϕ*(*a*)*ϕ*(*c*2)= *fh*2 = *sy*

while the fact that *z* = *xy* gives

*ϕ*(*z*)= *ϕ*(*x*)*ϕ*(*y*)= *sxsy* = *sz*

finishing the proof. *2*

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

**Theorem 6.4** *The convex closure of* A4 *can be embedded into Q.*

**Proof**. Let *ϕ* : *×*A4*⟩ → ×G⟩* 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](#_bookmark21)] that it must actually be an embedding. An

arbitrary *f ∈ ×*A4*⟩* can be written

*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

⎜⎝ ⎟⎠

, ⎞

*f* = *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

where we have written a general element *f ∈ ×*A4*⟩* as a convex sum

*f* = *e · I* + *x· x* + *y · y* + *z · z* + *a · a* + *b · b* + *c · c* + *d · d* + *a*2 *· a*2 + *b*2 *· b*2 + *c*2 *· c*2 + *d*2 *· d*2

of elements of the group A4 *⊆* (4*,* 4). Notice that each probability in a general convex sum *f ∈ ×*A4*⟩* has the same name as its associated group element except in cases where this would create clear inconsistencies [3](#_bookmark13) . The element *ϕ*(*f* ) is thus

, *e* + *x − y − z −a − b* + *c* + *d −a*2 + *b*2 + *c*2 *− d*2⎞

*ϕ*(*f* )= *−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*

Let *fij* and *ϕ*(*f* )*ij* denote the entries of *f* and *ϕ*(*f* ) located at position (*i, j*). Then

*f* and *ϕ*(*f* ) are related by:

* *φ*(*f* )11 = +*f*11 + *f*21 *− f*42 *− f*32, *φ*(*f* )12 = *−f*14 *− f*24 + *f*42 + *f*32, *φ*(*f* )13 = *−f*13 *− f*23 + *f*32 + *f*42;
* *φ*(*f* )21 = *−f*13 + *f*24 *− f*33 + *f*44, *φ*(*f* )22 = +*f*11 *− f*43 + *f*31 *− f*23, *φ*(*f* )23 = +*f*14 *− f*41 *− f*21 + *f*34;
* *φ*(*f* )31 = *−f*14 + *f*23 + *f*33 *− f*44, *φ*(*f* )32 = +*f*13 *− f*21 + *f*43 *− f*31, *φ*(*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 *ϕ*(*f* ) = *ϕ*(*g*) where *f* is written as a convex sum using probabilities *e, x, y, z*, etc, *g* is written using probabilities *ej, xj, yj, zj*, etc and we set *ci* = *i − ij* for each *i ∈ {e, x, y, z, a, b, c, d, a*2*, b*2*, c*2*, d*2*}*. Because *ϕ*(*f* ) *− ϕ*(*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 ap- plied to Z2 in the proof of Theorem [4.3](#_bookmark12) applies to each of these sets allowing us to conclude that

2

* *ce* = *cx* = *cy* = *cz*,
* *ca* = *cb* = *cc* = *cd*,
* *ca*2 = *cb*2 = *cc*2 = *cd*2 .

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

However, because *ci* = 0, we then have *ci* + *cj* + *ck* = 0 for any *i ∈ {e, x, y, z}*, *j ∈ {a, b, c, d}* and *k ∈ {a*2*, b*2*, c*2*, d*2*}*. This implies that *f − g* = 0 so that *f* = *g* and hence that *ϕ* is injective.

Σ

Because the convex linear extension of the isomorphism *ϕ* is a well-defined in- jective function, it is an embedding by the proof of Theorem 2 in [[7](#_bookmark21)]. *2*

1. *S*3

We denote by *S*3 *⊆* (3*,* 3) the natural copy of the symmetric group on three letters:

, ,0 1 0!

0 0 1 *, a* =

1 0 0

*S*3 =

*I, a* =

2 ,0 0 1!

,1 0 0!

,0 0 1!

,0 1 0!,

1 0 0

0 0 1

*.*

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:

1 0 0 *,b* =

0 1 0

0 0 1 *, c* =

0 1 0

0 1 0 *, d* =

1 0 0

*I* + *a* + *a*2

3

*I* + *a* + *a*2 + *b* + *c* + *d*

=

6

*.* (9)

We will now show that this equation is *impossible* quantum mechanically: **Lemma 7.1** *The convex closure of S*3 *⊆* (3*,* 3) *cannot be embedded into Q.* **Proof**. If a copy *{I, a, a*2*, b, c, d}⊆ SO*(3) of *S*3 satisfies equation ([9](#_bookmark14)), then

*I* + *a* + *a*2 = *b* + *c* + *d.*

So taking the trace of both sides gives

3+ tr(*a*)+ tr(*a*2)= *−*3

where we note that each nontrivial involution is conjugate to one of the spin channels in Lemma [4.1](#_bookmark10), and that conjugate matrices always have the same trace: in this case, tr(*b*) = tr(*c*) = tr(*c*) = *−*1. However, each rotation is conjugate to some *rx*(*θ*) by Lemma [3.2](#_bookmark2), so tr(*a*) *≥ −*1 and tr(*a*2) *≥ −*1, contradicting the fact that their sum is -6. *2*

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

* *a*1 is the permutation 1234 *→* 1342
* *a*2 is the permutation 1234 *→* 3241
* *a*3 is the permutation 1234 *→* 2431
* *a*4 is the permutation 1234 *→* 2314.

Notice that *ai* 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*2*, a*2*, a*2*,*

*and a*2*.*

4

1 2 3

* + *For each i ∈ {*1*,* 2*,* 3*,* 4*}, there is an involution x ∈* (4*,* 4) *such that ai* = *xa*1*x.*

**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 *→* 2413, 1234 *→* 2341 and 1234 *→* 2143. They have orders four, four and two, respec- tively.
  + The fixed point free permutations that ‘begin’ in 3 are: 1234 *→* 3412, 1234 *→* 3421 and 1234 *→* 3142. They have orders two, four and four, respec- tively.
  + The fixed point free permutations that ‘begin’ in 4 are: 1234 *→* 4123, 1234 *→* 4321 and 1234 *→* 4312. They have orders four, two and four, respec- tively.

Thus, any *x ∈* (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 *→* 231 and *a*2 = 123 *→* 312. Then for each *i ∈ {*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: *{ai, a*2 :1 *≤ i ≤* 4*}*.

*i*

To see that each *ai* is conjugate to *a*1 by an involution:

* + *a*1 = *xa*1*x* where *x* is the involution 1234 *→* 1234
  + *a*2 = *xa*1*x* where *x* is the involution 1234 *→* 2134
  + *a*3 = *xa*1*x* where *x* is the involution 1234 *→* 3412
  + *a*4 = *xa*1*x* where *x* is the involution 1234 *→* 4231. This finishes the proof. *2*

**Proposition 7.3** *If G ⊆* (4*,* 4) *is a copy of S*3*, then its convex closure cannot be embedded into Q.*

**Proof**. Let *H ⊆* (4*,* 4) be the copy of *S*3 generated by the elements

*a*¯ = 1 0 & ¯*b* = 1 0 where *a, b ∈ S*3 *⊆* (3*,* 3). We claim that *G* is conjugate to *H*.

0 *a*

0 *b*

Since *G* is isomorphic to *S*3, it contains an element *x* of order three. By

Lemma [7.2](#_bookmark16), *x* belongs to *{a*1*, a*2*, a*3*, a*4*, a*2*, a*2*, a*2*, a*2*}*. If *x* = *a*2 *∈ G*, then since

1 2 3 4 *i*

*G* is a group,

*x*2 = (*a*2)(*a*2)= *aia*3 = *ai · I* = *ai ∈ G.*

*i i* *i*

Thus, *G* contains one of the elements *a*1*, a*2*, a*3*, a*4.

Suppose first that *a*1 *∈ G* and let *b*1 *∈ G* be any nontrivial involution. Then *f* = *a*1*b*1 is an nontrivial involution since *G S*3. Thinking of *b*1 as the bijection *b*1 : *{*1*,* 2*,* 3*,* 4*}→ {*1*,* 2*,* 3*,* 4*}* given by 1234 *→ b*1(1)*b*1(2)*b*1(3)*b*1(4) and *f* as the bi-

jection *f* : *{*1*,* 2*,* 3*,* 4*}→ {*1*,* 2*,* 3*,* 4*}* given by 1234 *→ 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

¯*b* = 1 0 *∈ H,*

0 *b*

*c*¯ = 1 0 *∈ H,*

0 *c*

*d*¯ = 1 0 *∈ H.*

0 *d*

Then *G* contains *a*1 = *a*¯ *∈ 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 *ai ∈ G*. Then by Lemma [7.2](#_bookmark16), there is an involution *x ∈* (4*,* 4) such that *xa*1*x* = *ai*. Then *xGx G S*3 is a subgroup that contains *a*1, so by the above argument, *xGx* = *H*. Since *H* = *xGx*, *×H⟩* = *×xGx⟩ ×G⟩*. But *×H⟩* satisfies equation ([9](#_bookmark14)), which means that *×G⟩* does as well. As seen in Lemma [7.1](#_bookmark15), no copy of *S*3 *⊆ SO*(3) can satisfy equation ([9](#_bookmark14)). Thus, *×G⟩* cannot be embedded into *Q*. *2*

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

**Definition 7.4** Let *U*3 *⊆* (5*,* 5) denote the copy of *S*3 given by

*U*3 = *I, a*¯ = *I* 0 *, a*¯2 = *I* 0 *,* ¯*b* = *f* 0 *, c*¯ = *f* 0 *, d*¯ = *f* 0

0 *a*

0 *a*2

0 *b*

0 *c*

0 *d*

where *S*3 = *{I, a, a*2*, b, c, d} ⊆* (3*,* 3) is the natural copy of *S*3 and *f* = flip *∈* (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 invo- lution (*b, c, d*) with either *a* or *a*2 is a nontrivial involution.

In order to construct a copy of *S*3 *⊆ SO*(3), we notice that in *S*3 =

*{I, a, a*2*, b, c, d} ⊆* (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 *⊆ SO*(3) is

*G* = *{I, a, a*2*, −b, −c, −d}⊆ SO*(3)*.*

Let us prove that this is in fact a copy of *S*3:

**Lemma 7.5** *The set G ⊆ SO*(3) *is a group isomorphic to S*3*. An isomorphism is given by*

* *ϕ*(*I*)= *I, ϕ*(*a*)= *a, ϕ*(*a*2)= *a*2*,*
* *ϕ*(*b*)= *−b, ϕ*(*c*)= *−c, ϕ*(*d*)= *−d.*

**Proof**. By Theorem 6.13 on page 50 of [[6](#_bookmark20)], a presentation of the symmetric group on three letters is given by generators *α, β* with relations *α*3 = *β*2 = *I* and *αβα* = *β*. Within *G*, the elements *a* and *−b* satisfy such relations, a property they inherit from *S*3 *⊆* (3*,* 3). Thus, the group they generate is isomorphic to *S*3. We define *ϕ* on these generators

*ϕ*(*a*)= *a* & *ϕ*(*b*)= *−b*

and then extend it homomorphically. Because *a* and *b* generate *S*3, *ϕ* is an isomor- phism 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*:

* *ϕ*(*I*)= *ϕ*(*b*2)= *ϕ*(*b*)*ϕ*(*b*)= (*−b*)(*−b*)= *b*2 = *I*,
* *ϕ*(*c*)= *ϕ*(*ab*)= *ϕ*(*a*)*ϕ*(*b*)= *a*(*−b*)= *−*(*ab*)= *c*,
* *ϕ*(*a*2)= *ϕ*(*a*)*ϕ*(*a*)= *a*2,
* *ϕ*(*d*)= *ϕ*(*a*2*b*)= *ϕ*(*a*2)*ϕ*(*b*)= *a*2(*−b*)= *−*(*a*2*b*)= *d. 2*

Consequently, the homomorphism specified on generators by *ϕ*(*a*¯) = *a* and *ϕ*(¯*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 *⊆* (5*,* 5) *can be embedded into 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*a*¯ + *x*2*a*¯2 + *x*3¯*b* + *x*4*c*¯ + *x*5*d*¯ *∈ ×U*3*⟩* we have

,*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

⎜ ⎟

*f* = 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

while the corresponding element *ϕ*(*f* ) *∈ ×G⟩* is then

,*x*0 *− x*3 *x*1 *− x*5 *x*2 *− x*4⎞ *x*1 *− x*4 *x*2 *− x*3 *x*0 *− x*5

*ϕ*(*f* )= ⎝*x*2 *− x*5 *x*0 *− x*4 *x*1 *− x*3⎠ *.*

Let us first prove that *ϕ* is a well-defined function. If *f* = *g ∈ ×U*3*⟩*, where *f* is

written as a convex sum using (*xi*) and *g* is written using (*yi*), set *ci* = *xi −yi*. Since

*f − g* = 0, we have the equations:

* *c*0 + *c*3 = 0*, c*0 + *c*4 = 0*, c*0 + *c*5 = 0*, c*2 + *c*3 = 0*, c*1 + *c*4 = 0, and
* *c*3 + *c*4 + *c*5 = 0.

From these equations, it easily follows that *ci* =0 for all *i*, which means *xi* = *yi* for all *i* and thus that *ϕ*(*f* )= *ϕ*(*g*).

To see that *ϕ* is injective, if *ϕ*(*f* ) = *ϕ*(*g*), we again set *ci* = *xi − yi* and from

*ϕ*(*f* ) *− ϕ*(*g*) = 0 derive equations that are even easier to solve:

*c*0 *− c*3 = 0*, c*0 *− c*4 = 0*, c*0 *− c*5 = 0*, c*2 *− c*4 = 0*, c*1 *− c*4 = 0*.*

So *ci* = *c*0 for all *i*. But *ci* =0 since both (*xi*) and (*yi*) sum to one. Thus, *ci* =0 for all *i*, which means *f* = *g*, and so *ϕ* is injective. By the proof of Theorem 2 in [[7](#_bookmark21)], *ϕ* is thus an embedding. *2*

Σ

# 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 A4 or a subgroup of *S*3:

**Theorem 8.1** *Let* A4 *⊆* (4*,* 4) *denote the alternating group on four letters and*

*S*3 *⊆* (5*,* 5) *denote the unorthodox copy of the symmetric group on three letters.*

*Then*

1. *For each subgroup G of* A4*, there is an embedding ϕ* : *×G⟩→ Q.*
2. *For each subgroup G of S*3*, there is an embedding ϕ* : *×G⟩→ Q.*
3. *If G ⊆* (*m, n*) *is a group for which such an embedding exists, then G is either a subgroup of* A4 *or a subgroup of S*3*. That is, G must be isomorphic to either* Z2*,* Z3*,* Z2*, S*3 *or* A4*.*

2

**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 A4 or *S*3. If *G* is abelian, then it is either Z2, Z3 or Z2, each of which is a subgroup of A4. Thus, *G* is either a subgroup of A4 or a subgroup of *S*3. *2*

2

As *S*3 shows, it is not true that the convex closure of *any* copy of the five groups above can be embedded into *Q*. However, the converse does hold: if *G ⊆ SO*(3) is one of the five groups above, then its convex closure *is* isomorphic to a subset of either *×*A4*⟩ ⊆* (4*,* 4) or *×S*3*⟩ ⊆* (5*,* 5). The reason is that all finite isomorphic subgroups of *SO*(3) are conjugate [[1](#_bookmark18)]. Thus, the particular representations of A4 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 *ϕ* : (3*,* 3) *→Q* by

,*x*1 *x*2 *x*3⎞

1 ,*x*1 *x*2 *x*3⎞

*ϕ* ⎝*y*1 *y*2 *y*3⎠ = 3 ⎝*y*1 *y*2 *y*3⎠ *.*

*z*1 *z*2 *z*3

*z*1 *z*2 *z*3

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](#_bookmark15). Similarly, there is no embedding of (*n, n*) into

*Q* when *n ≥* 3.

Thus, Theorem [8.1](#_bookmark17) is about the interaction between convexity and group theo- retic structure.

# 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 for- mer is that they express multiple experiments for achieving the same task. For instance, if *f ∈ SO*(3) is a generator for Z4, we can have an equation like

*f* + *f* 3

*f* 2 + *f* 4

,1 0 0⎞

2 = 2 = 0 0 0

⎝ ⎠

0 0 0

which is never true classically. This tells us that generators of Z4 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}⊆*

*SO*(3), where we can write

*e* + *x* + *y* + *z* = *e* + *x* *e* + *y* = 0*.*

4

2

2

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](#_bookmark21)].

# 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 *×SO*(*n*)*⟩*, 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 Z2, the channels described are bit flipping channels with respect to a particular spin matrix. For Z3, 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

A4 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>

1. M. Nielsen and I. Chuang, Quantum computation and quantum information. Cambridge University Press, 2000.
2. D. Saracino. *Abstract algebra: a first course.* Addison-Wesley, 1980.
3. D. Serre. *Matrices: Theory and applications.* Springer-Verlag, Graduate Texts in Mathematics, 2000.