MFPS 2010

A free object in quantum information theory

Keye Martin[1] Johnny Feng[2] Sanjeevi Krishnan[3]

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

Abstract

We consider three examples of affine monoids. The first stems from information theory and provides a natural model of image distortion, as well as a higher-dimensional analogue of a binary symmetric channel. The second, from physics, describes the process of teleporting quantum information with a given entangled state. The third is purely a mathematical construction, the free affine monoid over the Klein four group. We prove that all three of these objects are isomorphic.

Keywords: Information Theory, Quantum Channel, Category, Teleportation, Free Object, Affine Monoid

1 Introduction

Here are some questions one can ask about the transfer of information:

(i) Is it possible to build a device capable of interrupting any form of quantum communication?

(ii) Is it possible to maximize the amount of information that can be transmitted with quantum states in a fixed but unknown environment?

(iii) Binary symmetric channels are some of the most useful models of noise in part because all of their information theoretic properties are easy to calculate. What are their higher dimensional analogues?

(iv) If we attempt to teleport quantum information using a state that is not maximally entangled, what happens?

(v) Is it possible to do quantum information theory using classical channels?

It turns out that the answer to all of these questions depends on a certain free object over a finite group.

[1] Email: keye.martin@nrl.navy.mil

[2] Email: johnny.feng@nrl.navy.mil (Visiting NRL from Tulane University, Department of Mathematics)

[3] Email: sanjeevi.krishnan.ctr@nrl.navy.mil

This paper is electronically published in
Electronic Notes in Theoretical Computer Science
URL: www.elsevier.nl/locate/entcs

In any collection of mathematical objects, *free objects* are those which satisfy the fewest laws. For instance, if one takes the set of finite words built from symbols in a set S, and uses concatenation to define a multiplication on it, they obtain the *free monoid* over S, since any other monoid over S can be thought of as the free monoid together with additional restrictions imposed on its multiplication. Computer scientists call the elements of the free monoid "lists." They are among the most fundamental objects in computation. In particular, the free monoid over a one element set is the set of natural numbers with addition.

This paper is about a free object whose elements are called "channels." From classical image distortion to quantum communication, and even recently in steganography, it plays a very important role when studying the transfer of information in a noisy environment.

2 Black and white

A simple way to represent a black and white image on a computer is as a set of pixels. A pixel represents a tiny rectangular region of the original image. The center of this rectangle is assigned a number representing its intensity or "grey level." For instance, black might be represented with 0, while white could be represented with 255. In general, let us assume that the intensity is represented by a number whose binary expansion can be given in n bits.

An image becomes distorted when environmental noise flips some of the bits in a pixel. This has the effect of altering the original intensity of a pixel. For instance, if all the bits in a white pixel are flipped, the pixel would become black, causing the image to appear dark in a place where it should be light. To model the distortion of an image, we will use a channel whose input is a pixel and whose output is a pixel that in general has been degraded in some manner.

Let us first consider the case $n = 1$, when the intensity is represented by a single bit. Then there are two things that can happen to this bit:

$$\mathrm{id} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \& \quad \mathrm{flip} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

That is, a bit is either left alone or it is flipped. This process is probabilistic, so the the possible forms of distortion are

$$(1-p)\cdot \mathrm{id} + p \cdot \mathrm{flip}$$

for $p \in [0,1]$. That is, with probability p the bit is flipped, and otherwise it is left alone. Channels of this form are called *binary symmetric channels* [3].

For the case of an n bit pixel, there are 2^n bit flipping operations possible, described inductively as follows:

$$V_1 := \{\mathrm{id}, \mathrm{flip}\}$$

$$V_{n+1} := \{\mathrm{id} \otimes g_i : g_i \in V_n\} \cup \{\mathrm{flip} \otimes g_i : g_i \in V_n\}$$

Once again, the process is probabilistic, so the possible forms of noise are

$$\langle V_n\rangle := \left\{\sum_{i=1}^{2^n} x_i g_i : x \in \Delta^{2^n}\right\}$$

where $V_n := \{g_1, \ldots, g_{2^n}\}$ and

$$\Delta^n := \left\{x \in [0,1]^n : \sum_{i=1}^{n} x_i = 1\right\}.$$

To measure the amount of distortion in an image caused by a form of noise $f \in \langle V_n\rangle$, we calculate its capacity:

$$C(f) = \sup_{x \in \Delta^{2^n}} \left\{H(xf) - \sum x_i H(e_i f)\right\}$$

where $e_i f$ denotes row i of the matrix f and $H(x) = -\sum x_i \log x_i$ is the base two Shannon entropy.

Theorem 2.1 *The capacity of $f \in \langle V_n\rangle$ is*

$$C(f) = n - H(x_1, \ldots, x_{2^n})$$

where $f = \sum x_i g_i$.

Proof. By induction, each row in f is a permutation of the first and the first is a permutation of $(x_1, \ldots, x_{2^n})$. Because entropy is invariant under permutations, the mutual information, which is the expression being maximized in the definition of capacity, reduces to

$$H(yf) - H(x_1, \ldots, x_{2^n})$$

where we sup over all $y \in \Delta^{2^n}$. Since f holds the uniform distribution $\perp \in \Delta^{2^n}$ fixed, the capacity is

$$H(\perp) - H(x_1, \ldots, x_{2^n}) = \log 2^n - H(x_1, \ldots, x_{2^n}) = n - H(x_1, \ldots, x_{2^n})$$

which is the desired expression. □

The channels in $\langle V_n\rangle$ provide a legitimate higher dimensional generalization of the binary symmetric channels $\langle V_1\rangle$: (i) there is a clear conceptual connection between $\langle V_1\rangle$ and $\langle V_n\rangle$, (ii) the important ease of calculation for $\langle V_1\rangle$ is inherited by $\langle V_n\rangle$, (iii) the class of channels is not ad-hoc i.e. it forms an affine monoid, for instance. To further illustrate (iii), a channel $f \in (2^n, 2^n)$ belongs to $\langle V_n\rangle$ iff $H_n f H_n$ is diagonal, where

$$H_1 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad H_{n+1} := H_1 \otimes H_n$$

are the Hadamard matrices. We are not sure if this implies a special connection between $\langle V_n\rangle$ and Hadamard codes, but are curious to find out.

3 Teleportation

3.1 Qubit channels

The fact that a binary channel $f : \Delta^2 \to \Delta^2$ operates on Δ^2 is indicative of the fact that only two symbols are being sent and that we have chosen a particular and fixed way of representing these two symbols. By contrast, in the case of a quantum channel, there are an infinite number of ways to represent bits: each basis of the state space $\mathcal{H}^2$, a two dimensional complex Hilbert space, offers a different possible representation.

Let us suppose that we choose a *particular* quantum representation for the classical bits '0' and '1', denoted by orthogonal unit vectors $|0\rangle$ and $|1\rangle$ in $\mathcal{H}^2$. In doing so, we are implicitly saying that we will use a quantum system to represent a classical bit. When the system is in state $|0\rangle$, it represents the classical bit '0'; when in state $|1\rangle$, it represents the classical bit '1'. There is a subtle but relevant caveat here though.

Physically, states are equal "to within a phase factor." So for example, the states $|0\rangle, -|0\rangle, i|0\rangle, -i|0\rangle, e^{i\theta}|0\rangle$ are all equivalent in the sense that quantum mechanics makes the same predictions about a system in any one of these states. Mathematically, though, we know that we cannot go around writing things like "$|0\rangle = -|0\rangle$," for the simple reason that in a vector space the only such element is the zero vector and the zero vector is not a unit vector. One way around this difficulty is to say that a 'state', specified by a unit vector $|\psi\rangle \in \mathcal{H}^2$, is mathematically represented by the operator $f : \mathcal{H}^2 \to \mathcal{H}^2$ given by

$$f(u) = \langle\psi|u\rangle \cdot |\psi\rangle$$

The operator f takes as input a vector u and returns as output the vector $|\psi\rangle$ multiplied by the complex number $\langle\psi|u\rangle$, which is the inner product of the vector u and the vector $|\psi\rangle$. For this reason, the operator f is traditionally denoted $f = |\psi\rangle\langle\psi|$. Such an operator is called a *pure state* since it refers to a state that the system can be in; pure states are the quantum analogues of $e_0 = (1, 0)$ and $e_1 = (0, 1)$ in Δ^2, the latter of which we think of as the classical representation of the bits '0' and '1'.

A classical binary channel $f : \Delta^2 \to \Delta^2$ takes an input distribution to an output distribution. In a similar way, a qubit channel will map input distributions to output distributions. But what is the quantum analogue of a distribution? Let us return to the classical case. Each distribution $x \in \Delta^2$ may be written

$$x = x_0 \cdot e_0 + x_1 \cdot e_1$$

i.e., as a convex sum of classical 'pure' states. The meaning of such an expression is that the system is in state e_0 with probability x_0 and in state e_1 with probability x_1. Thus, if a quantum system is in state $|\psi_i\rangle\langle\psi_i|$ with probability x_i, a natural way to represent this 'distribution' is given by the operator

$$\rho = \sum_{i=1}^{n} x_i \cdot |\psi_i\rangle\langle\psi_i|$$

where we assume $\sum x_i = 1$. Such an operator is called a *density operator*. A density operator is also called a *mixed state*. The set of all density operators on $\mathcal{H}^2$ is denoted by Ω^2. Thus, in analogy with the classical case, a qubit channel will be a function of the form $\varepsilon : \Omega^2 \to \Omega^2$. Specifically,

Definition 3.1 A *qubit channel* is a function $\varepsilon : \Omega^2 \to \Omega^2$ that is convex linear and completely positive[4].

To say that ε is convex linear means that ε preserves convex sums i.e. sums of the form $x \cdot \rho + (1-x) \cdot \sigma$. Complete positivity is a condition which ensures that the definition of a qubit channel is compatible with natural intuitions about joint systems. Now what we want to do is get rid of the Hilbert space formulation of qubit channels.

3.2 The Bloch representation

There is a 1-1 correspondence between density operators on a two dimensional state space and points on the unit ball $\mathbb{B}^3 = \{x \in \mathbb{R}^3 : |x| \leq 1\}$: each density operator $\rho : \mathcal{H}^2 \to \mathcal{H}^2$ can be written uniquely as

$$\rho = \frac{1}{2}(I + r_x\sigma_x + r_y\sigma_y + r_z\sigma_z) := \frac{1}{2}(I + r \cdot \boldsymbol{\sigma})$$

where $r = (r_x, r_y, r_z) \in \mathbb{R}^3$ satisfies $|r| = \sqrt{r_x^2 + r_y^2 + r_z^2} \leq 1$ and $\boldsymbol{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ is the vector of *spin operators*:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

The vector r is called the *Bloch vector* associated to ρ. Let us write $r = [\![\rho]\!]$ and denote the *bijection* between Ω^2 and $\mathbb{B}^3$ as $[\![\cdot]\!] : \Omega^2 \to \mathbb{B}^3$. Then:

- $[\![I/2]\!] = 0$
- $[\![x\rho + (1-x)\sigma]\!] = x[\![\rho]\!] + (1-x)[\![\sigma]\!]$

where $x \in [0,1]$ and ρ, σ are density operators. Notice here that $I/2$ is the completely mixed state i.e. the identity divided by two, which is the quantum analogue of the uniform distribution.

Since qubit channels map Ω^2 into itself, they also have Bloch representations. The Bloch representation of a qubit channel $\varepsilon : \Omega^2 \to \Omega^2$ is the map $f_\varepsilon = [\![\varepsilon]\!]$ that makes

$$\begin{tikzcd} \Omega^2 \arrow[r, "\varepsilon"] \arrow[d, "{[\![\cdot]\!]}"'] & \Omega^2 \arrow[d, "{[\![\cdot]\!]}"] \\ \mathbb{B}^3 \arrow[r, "f_\varepsilon"'] & \mathbb{B}^3 \end{tikzcd}$$

[4] Notice that such maps are implicitly trace preserving since every operator in Ω^2 has trace one.

commute. It satisfies

$$f_\varepsilon([\![\rho]\!]) = [\![\varepsilon(\rho)]\!].$$

The map $f_\varepsilon : \mathbb{B}^3 \to \mathbb{B}^3$ is an *affine transformation*: there is a 3×3 real matrix M and a vector $b \in \mathbb{R}^3$ such that $f_\varepsilon(x) = Mx + b$ for all x. Notice though that there are plenty of affine transformations that do not arise as the Bloch representation of a qubit channel. For instance, the antipodal map $a(x) = -x$ does not represent a qubit channel [6] i.e. ”universal bit flipping” is physically impossible.

The following equations [6] are helpful when calculating the Bloch representations of qubit channels:

- $[\![I]\!] = I$
- $[\![\rho \mapsto I/2]\!] = 0$
- $[\![f \circ g]\!] = [\![f]\!] \circ [\![g]\!]$
- $[\![pf + (1-p)g]\!] = p[\![f]\!] + (1-p)[\![g]\!]$

where $f, g : \Omega^2 \to \Omega^2$ are qubit channels and $p \in [0, 1]$. Because of the convex linear isomorphism between qubit channels and their Bloch representations, the Bloch representation $[\![\varepsilon]\!]$ of a qubit channel $\varepsilon : \Omega^2 \to \Omega^2$ will also be called a *qubit channel*.

3.3 Unitality

The classical channels f which increase entropy $(H(f(x)) \geq H(x))$ are exactly the *doubly stochastic* channels, i.e., those which hold the uniform distribution fixed. Part of the rationale for studying them is that they provide conservative models of noise when operating in an unknown environment [5]. The *unital channels* offer a quantum analogue of this idea: they are the quantum channels which hold the completely mixed state fixed, or equivalently, those which increase the von Neumann entropy for all input states.

Because a unital qubit channel will have to map the completely mixed state $I/2$ to itself, its Bloch representation, being affine, will have to be linear and thus defined by a 3×3 real matrix. The set of such matrices can be characterized inductively. Let $r_i(\theta)$ denote the principal rotation about the $i \in \{x, y, z\}$ axis by an angle of θ.

Theorem 3.2 **([6])** *The set of unital channels $\mathcal{U}$ is the smallest set of 3×3 real matrices such that*

- *For each angle θ,*

$$r_x(\theta), r_y(\theta), r_z(\theta) \in \mathcal{U},$$

- *If $f, g \in \mathcal{U}$, then $f \circ g \in \mathcal{U}$, and*
- *If $f, g \in \mathcal{U}$ and $p \in [0, 1]$, then $pf + (1-p)g \in \mathcal{U}$.*

A particularly important class of unital channels are the *diagonal channels*: the unital channels whose matrix representations are diagonal. An elementary proof of the following is given in [6]:

Proposition 3.3 *A diagonal matrix*

$$\begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{pmatrix}$$

is a unital qubit channel if and only if $|\lambda_i| \leq 1$ *for each* $i \in \{1,2,3\}$ *and if the following four inequalities are satisfied:*

(i) $1 + \lambda_1 + \lambda_2 + \lambda_3 \geq 0$

(ii) $1 + \lambda_1 - \lambda_2 - \lambda_3 \geq 0$

(iii) $1 - \lambda_1 + \lambda_2 - \lambda_3 \geq 0$

(iv) $1 - \lambda_1 - \lambda_2 + \lambda_3 \geq 0$

It is difficult to overstate the importance of diagonal qubit channels. Each unital channel f can be written in the form $f = udv$, where $u, v \in SO(3)$ and d is a *diagonal* unital channel. It turns out that the Holevo capacity of f is the same as that of the diagonal channel d. In a related way, the *scope* [6] of f is also systematically determined by a diagonal channel. This leads to a method for maximizing key generation rates in quantum cryptography in a fixed but unknown environment [6].

3.4 The teleportation channels

Teleportation allows a sender (Alice) to transmit a *qubit* $|\Psi\rangle$ to a receiver (Bob) as follows:

- At the start, Alice and Bob share a *maximally entangled* pair of qubits i.e. the composite system consisting of their individual subysystems is in the state

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

- Alice interacts $|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ with her half of the entangled pair, and then measures both of these qubits, obtaining one of four possible results: $m = 00$, $m = 01$, $m = 10$ or $m = 11$.
- The state of Bob's qubit is now determined by the result of the measurement Alice performed in the previous step; specifically, Bob's state is

$$\begin{cases} \alpha|0\rangle + \beta|1\rangle \text{ if } m = 00 \\ \alpha|1\rangle + \beta|0\rangle \text{ if } m = 01 \\ \alpha|0\rangle - \beta|1\rangle \text{ if } m = 10 \\ \alpha|1\rangle - \beta|0\rangle \text{ if } m = 11 \end{cases}$$

- Alice now sends the bit string $m = ij$ to Bob. He then applies the operator $\sigma_z^i \sigma_x^j$ to the qubit he holds, thereby completely recovering $|\Psi\rangle$.

However, no known experimental method is capable of generating maximally entangled states "on demand" – the most one can hope for currently is to generate entangled states that are subject to imperfection. Suppose then, that instead of Alice and Bob sharing the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, they share the imperfect state

$$|\Phi\rangle = a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle$$

where $a, b, c, d \in \mathbb{C}$ and $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$. How does teleportation function now? When Alice attempts to teleport a pure state to Bob, what does Bob receive if they no longer have access to maximal entanglement?

Intuitively, there is a "noisy channel" lurking: Alice attempts to teleport the pure state $|\Psi\rangle$ to Bob, and the state Bob receives is described by a mixed state $f_\Phi(|\Psi\rangle\langle\Psi|)$ that depends on the entangled state $|\Phi\rangle$. There is certainly a function f_Φ that maps pure states to mixed states, but is it a trace-preserving, convex linear *completely positive* map? That is, is this *intuitive channel* actually a channel in the formal sense of quantum information theory?

It was shown in [4] that the process of teleporting a qubit with a given entangled state does indeed define a qubit channel in the formal sense, so we refer to such channels as *teleportation channels.* In fact, much more is true:

Theorem 3.4 *The set of teleportation channels is equal to the set of diagonal channels.*

Proof. From [4], if a pure state with Bloch vector $(r_x, r_y, r_z) \in \mathbb{B}^3$ is teleported using the state

$$|\Phi\rangle = a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle\,,$$

then the Bloch vector of the mixed state describing the state received is

$$f_\Phi(r_x, r_y, r_z) = (\lambda_x r_x, \lambda_y r_y, \lambda_z r_z)$$

where

$$\begin{aligned}\lambda_x &= ad^* + bc^* + b^*c + a^*d\\ \lambda_y &= ad^* - bc^* - b^*c + a^*d\\ \lambda_z &= aa^* - bb^* - cc^* + dd^*.\end{aligned}$$

This correspondence defines a convex linear function $f_\Phi : \mathbb{B}^3 \to \mathbb{B}^3$ that is the Bloch representation of a diagonal qubit channel – in particular, the form of the λ_i guarantees that f_Φ represents a completely positive map. Thus, each teleportation channel is diagonal.

Conversely, each diagonal channel with entries $(\lambda_x, \lambda_y, \lambda_z)$ is an instance of teleportation through the entangled state $a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$, where

$$a = \frac{1}{2}\sqrt{1+\lambda_1+\lambda_2+\lambda_3} + \frac{1}{2}\sqrt{1-\lambda_1-\lambda_2+\lambda_3}$$

$$b = \frac{1}{2}\sqrt{1+\lambda_1-\lambda_2-\lambda_3} + \frac{1}{2}\sqrt{1-\lambda_1+\lambda_2-\lambda_3}$$

$$c = \frac{1}{2}\sqrt{1+\lambda_1-\lambda_2-\lambda_3} - \frac{1}{2}\sqrt{1-\lambda_1+\lambda_2-\lambda_3}$$

$$d = \frac{1}{2}\sqrt{1+\lambda_1+\lambda_2+\lambda_3} - \frac{1}{2}\sqrt{1-\lambda_1-\lambda_2+\lambda_3}$$

□

In particular, the set of teleportation channels is an affine monoid: it is *closed under composition and nondeterministic choice.* For instance, teleporting through one state and then teleporting through another is equivalent to teleporting through a fixed third state.

4 The free affine monoid over a finite group

By an *affine monoid*, we mean a convex subset of a real algebra that is closed under multiplication and contains the algebra's multiplicative identity, though more general definitions are possible [7]. In the category of affine monoids, the morphisms are the convex linear maps that preserve multiplication and identity.

Definition 4.1 A *free affine monoid* over a finite group G is an affine monoid $\langle G\rangle$ together with a homomorphism $i : G \to \langle G\rangle$ that has the following universal property:

$$\begin{tikzcd}
G \arrow[r, "\forall f"] \arrow[dr, "i"'] & \mathbb{A} \\
& \langle G\rangle \arrow[u, "\exists! \bar{f}"']
\end{tikzcd}$$

That is, each homomorphism $f : G \to \mathbb{A}$ into an affine monoid $\mathbb{A}$ has a unique convex linear extension to all of $\langle G\rangle$.

Free objects are unique up to isomorphism: if $\mathbb{A}$ and $\mathbb{B}$ are both free over G then we have the following implication of commutative diagrams:

$$\begin{tikzcd}
G \arrow[r, "i_{\mathbb{B}}"] \arrow[dr, "i_{\mathbb{A}}"'] & \mathbb{B} & \& & G \arrow[r, "i_{\mathbb{A}}"] \arrow[dr, "i_{\mathbb{B}}"'] & \mathbb{A} & \Longrightarrow & G \arrow[r, "i_{\mathbb{A}}"] \arrow[dr, "i_{\mathbb{A}}"'] & \mathbb{A} \\
& \mathbb{A} \arrow[u, "\overline{i}_{\mathbb{B}}"'] & & & & \mathbb{B} \arrow[u, "\overline{i}_{\mathbb{A}}"'] & & & \mathbb{A} \arrow[u, "\overline{i}_{\mathbb{A}}\overline{i}_{\mathbb{B}}"']
\end{tikzcd}$$

Since the identity also makes the rightmost diagram commute, and only one morphism can do so, $\overline{i}_{\mathbb{A}}\overline{i}_{\mathbb{B}} = 1_{\mathbb{A}}$. Interchanging $\mathbb{A}$ and $\mathbb{B}$ above gives $\overline{i}_{\mathbb{B}}\overline{i}_{\mathbb{A}} = 1_{\mathbb{B}}$, which means that $\mathbb{A}$ and $\mathbb{B}$ are isomorphic. Because of this uniqueness, we call any object satisfying the universal property in Definition 4.1 *the* free object over G.

Proposition 4.2 *An affine monoid $\mathbb{A}$ with a morphism $i_{\mathbb{A}} : G \to \mathbb{A}$ is the free object over a finite group $G = \{g_1, \ldots, g_n\}$ iff for each $a \in \mathbb{A}$, there is a unique $x \in \Delta^n$ such that*

$$a = \sum_{i=1}^{n} x_i \, i_{\mathbb{A}}(g_i).$$

In either case, the map $i_{\mathbb{A}}$ must be injective.

Proof. ($\Rightarrow$): Take an n-dimensional real vector space V with basis $\{e_i\}$ and using the correspondence $g_i \mapsto e_i$, first define a multiplication on $\{e_i\}$, and then take its unique extension to all of V, turning V into a real algebra. Define

$$\langle G\rangle := \left\{ \sum_{i=1}^{n} x_i e_i : x \in \Delta^n \right\}$$

to be the convex closure of $\{e_i\}$ within V and $i_V : G \to \langle G\rangle$ by $i_V(g_i) = e_i$. Then $(\langle G\rangle, i_V)$ satisfies the desired property since $i_V(G)$ is a basis for V.

($\Leftarrow$): Given a morphism $f : G \to \mathbb{B}$ into some affine $\mathbb{B}$, the conditions assumed enable us to define a function $\bar{f} : \mathbb{A} \to \mathbb{B}$ given by

$$\bar{f}\left(\sum_{i=1}^{n} x_i\, i_{\mathbb{A}}(g_i) \right) = \sum_{i=1}^{n} x_i f(g_i)$$

Since each $a \in \mathbb{A}$ is expressible as a convex sum of the form indicated above, $\bar{f}$ is defined on all elements on $\mathbb{A}$; since each $a \in \mathbb{A}$ is uniquely represented by an $x \in \Delta^n$, $\bar{f}$ is a well-defined function. In [5], it is shown that $\bar{f}$ is a convex-linear homomorphism whenever it is actually a function.

Finally, if we have a pair $(\mathbb{A}, i_{\mathbb{A}})$ satisfying the freeness condition, then we obtain a commutative diagram

$$\begin{tikzcd}
G \arrow[r, "i_{\mathbb{A}}"] \arrow[dr, "i_V"'] & \mathbb{A} \\
& \langle G\rangle \arrow[u, "\bar{i}_{\mathbb{A}}"]
\end{tikzcd}$$

As we saw earlier, because both $\mathbb{A}$ and $\langle G\rangle$ are free, the map $\bar{i}_{\mathbb{A}}$ is an isomorphism. Thus, $i_{\mathbb{A}}$ is also injective, as the composition of two injective maps. □

Corollary 4.3 *The free affine monoid over a finite group exists.*

Finally, we come to the case of the Klein four group i.e. the unique four element group $\{e, x, y, z\}$ in which every element is its own inverse.

Theorem 4.4 *The following affine monoids are isomorphic:*

(i) *The classical channels $\langle \mathrm{V}_2\rangle$ generated by flip operations on two bits,*

(ii) *The teleportation channels,*

(iii) *The free affine monoid over the Klein four group.*

Proof. In [5], it is shown that (i) satisfies the property

$$\sum_{i=1}^{2^n} x_i g_i = \sum_{i=1}^{2^n} y_i g_i \Rightarrow (\forall i)\, x_i = y_i$$

And since the flip operations on two bits form a copy of the Klein four group, Prop 4.2 gives that (i) is isomorphic to (iii). In the proof of Theorem 4.3 from [1], it is proven that the convex closure of

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

has the same property. But since this convex closure is the set of diagonal qubit channels, Prop. 4.2 and Theorem 3.4 give that (ii) is also isomorphic to (iii). Since both (i) and (ii) are free affine monoids over the Klein four group, the uniqueness of free objects implies that they must be isomorphic! And in fact,

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

is an explicit isomorphism between the two. □

Corollary 4.5 *$\langle V_n \rangle$ is the free affine monoid over the involution group of order 2^n.*

There are extremely natural examples of monoids that arise as the convex closure of the Klein four group, but nevertheless fail to be free. For instance, the monoid $[-1,1] \times [-1,1]$ with the pointwise multiplcation it inherits from $\mathbb{R}$ is not free since there are two ways to write $(0,0)$:

$$(0,0) = \frac{(-1,1)+(1,-1)}{2} = \frac{(-1,-1)+(1,1)}{2}.$$

5 Closing

We have seen the utility of the free affine monoid over the Klein four group:

(i) It can be used to design a device capable of interrupting any form of quantum communication, as first explained in [5];

(ii) It plays a crucial role in calculating both the Holevo capacity and the scope of a unital channel; in the first case, one is lead to an experimentally realizable protocol for achieving the Holevo capacity [2], while in the second we obtain a method for maximizing key generation rates in quantum cryptography [6];

(iii) It provides a higher dimensional analogue of binary symmetric channels in which some of the most crucial information theoretic properties are easy to calculate;

(iv) It can be understood as the process of teleportation when any state is allowed as the source of entanglement;

(v) It offers the possibility of doing quantum information theory with classical channels, since the isomorphism from $\langle V_2 \rangle$ to the diagonal channels assigns the nontrivial eigenvalues of a classical channel, and the largest of these in magnitude determines the Holevo capacity of the assigned diagonal channel.

But while we have established the utility of free objects in communication, what about freeness itself? To establish the importance of freeness in communication, we would like to begin with the universal property in the definition of “free,” and demonstrate clearly why in some cases it yields classes of channels that are easier to study from the point of view of calculating information theoretic quantities like capacity. We expect that this will only be the case for certain finite groups and it will be exciting to try and determine which ones.

As we have seen, the free affine monoid over the Klein four group has a quantum representation as well as a *stochastic representation* – one in terms of stochastic matrices with the usual operations of multiplication and convex sum. In fact, Tanner Crowder has recently shown that the free affine monoid over *any finite group* has a stochastic representation in an appropriate dimension. This is more subtle than it may sound: the stochastic representation of the symmetric group S_3 on three letters requires the use of 5×5 matrices [1]. This of course raises the question of a quantum representation.

Interestingly, the set of *single qubit* channels contains an infinite number of copies of the finite group $\mathbb{A}_4$, the alternating group on four letters, but not one of them has a convex closure that yields the free object over $\mathbb{A}_4$: the reason is that there is a copy of $\mathbb{A}_4$ in $SO(3)$ whose convex closure is not free [1] and that all copies of $\mathbb{A}_4$ in $SO(3)$ are conjugate. Thus, the free affine monoid over $\mathbb{A}_4$ has no quantum representation using *single qubit* channels. Whether the free affine monoid over a finite group always has a quantum representation in some higher dimension is an open question.

6 Black and gold

The first author wishes to express his gratitude to the organizers of this year’s meeting for the invitation to speak. All three thank the members of the IP group in DC for listening to several informal lectures on this topic.

http://neworleanscitypark.com/donate.html

Finally, congratulations to the **World Champion** New Orleans Saints and to the beautiful city they represent.

References

[1] T. Crowder and K. Martin. *Classical representations of qubit channels.* Proceedings of Quantum Physics and Logic 2009, Electronic Notes in Theoretical Computer Science, Elsevier Science, In press.

[2] J. Feng. *A domain of qubit channels.* In preparation.

[3] G. A. Jones and J. M. Jones. *Information and coding theory.* Springer-Verlag, 2000.

[4] M. Lanzagorta and K. Martin. *Teleportation with an imperfect state.* Theoretical Computer Science, Elsevier Science, submitted.

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

[6] K. Martin. *The scope of a quantum channel.* Submitted to Proceedings of the Clifford Lectures, American Mathematical Society.

[7] S. Krishnan. *Some notes on affine semigroups.* Unpublished notes from 2010.