The Geometry of Single-Qubit Maps

Daniel Kuan Li Oi*
Centre for Quantum Computation, Clarendon Laboratory, University of Oxford, OX1 3PU, UK
(Dated: February 1, 2008)

The physically allowed quantum evolutions on a single qubit can be described in terms of their geometry. From a simple parameterisation of unital single-qubit channels, the canonical form of all such channels can be given. The related geometry can be used to understand how to approximate positive maps by completely-positive maps, such as in the case of optimal eavesdropping strategies. These quantum channels can be generated by the appropriate network or through dynamical means. The Strømer-Woronowisc result can also be understood in terms of this geometry.

PACS numbers: 03.67.-a

I. INTRODUCTION

An important consideration in the field of quantum information theory is what transformations to the state of a system are physically allowed. This guides us in the search for how we can manipulate quantum information as well as giving an insight into the nature of quantum theory. It is instructive to examine the simplest non-trivial case of a quantum system, the qubit, or two-level system, and study the possible evolutions of the state. Such transformations are called single-qubit channels and they play a vital role in the theory of quantum communication and computing. Recently, other workers have analysed the single-qubit channel [1] and characterised the extreme points for the most general qubit map [2]. The geometry of single-qubit channels provides a useful description of them. This simple structure of single qubit maps can be applied to other problems in quantum information theory.

II. IMPOSSIBLE QUBIT TRANSFORMATIONS

If we consider an arbitrary pure state of a qubit, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, what operations are physically allowed by quantum mechanics? If we require that the final state of the qubit be pure and non-degenerate, then the operation must be unitary. Therefore, seemingly innocuous operations such as,

$$\begin{array}{ll} |\psi\rangle \mapsto \alpha^*|0\rangle + \beta^*|1\rangle\,, & |\psi\rangle \mapsto \alpha^*|0\rangle - \beta^*|1\rangle\,, \\ |\psi\rangle \mapsto \beta^*|0\rangle + \alpha^*|1\rangle\,, & |\psi\rangle \mapsto \beta^*|0\rangle - \alpha^*|1\rangle\,, \end{array} \tag{1}$$

are not allowed. More generally, if the inital and final states are allowed to be mixed, then the states are represented by 2 by 2 density matrices and the allowed transformations are specific types of maps from density matrices to density matrices. These operations are precisely the trace-preserving completely positive (CP) linear maps. A map $\mathcal{S}$ is trace-preserving if $\mathrm{Tr}(\mathcal{S}(\rho)) = \mathrm{Tr}(\rho)$ for all density matrices ρ and positive if the eigenvalues of $\mathcal{S}(\rho)$ are nonnegative whenever the eigenvalues of ρ are non-negative. This ensures $\mathcal{S}$ always sends density matrices to density matrices.

The maps in (1) are trace-preserving and positive but they fail the final, more subtle, requirement, complete-positivity. A map $\mathcal{S}$ is said to be completely-positive (CP) if and only if the trivial extension, $\mathbb{1}_n \otimes \mathcal{S}$, is a positive map for all n where $\mathbb{1}_n$ is the identity map on n by n matrices. This requirement is physically very natural as it acknowledges that the mixed state ρ may be entangled with other quantum systems and that $\mathcal{S}$ extended to these other systems must still produce a physical state. Henceforth, we will refer to a trace-preserving completely-positive map as a quantum channel.

*daniel.oi@qubit.org

III. CP MAPS ON SINGLE-QUBITS

It will be convenient to work with the Bloch vector representation where the action of a quantum channel on a single-qubit is characterised by an affine map on the Bloch Sphere:

$$\vec{s}' = \mathcal{S}(\vec{s}) = \mathrm{A}\vec{s} + \vec{\mathrm{b}}, \tag{2}$$

where A is a 3×3 real matrix, $\vec{\mathrm{b}}$ is a 3-dimensional real vector and $\vec{s}$ and $\vec{s}'$ are the Bloch vectors representing the initial $\rho = \frac{1}{2}(\mathbb{1} + \vec{s}\cdot\vec{\sigma})$ and final state $\rho' = \frac{1}{2}(\mathbb{1} + \vec{s}'\cdot\vec{\sigma})$ of the qubit, respectively. Note that such maps are automatically trace-preserving. We can visualise the effect of these map, $\vec{s} \mapsto \vec{s}'$. First, physical states should be mapped onto physical states and thus $\mathcal{S}$ is a contraction. Since $\mathcal{S}$ is affine linear, it must map the Bloch sphere to an ellipsoid contained within the Bloch sphere. This gives 12 free parameters consisting of 6 parameters denoting the magnitude and axes of scaling of the Bloch sphere, 3 parameters specifying the axis and magnitude of a rotation and finally, 3 parameters specifying a translation of the ellipsoid. It was shown in [1] that not all ellipsoids in the Bloch sphere can be the image of a quantum channel.

If we restrict ourselves to the maps for which $\vec{\mathrm{b}} = 0$ (unital), and A diagonal with entries $(\eta_\mathrm{x}, \eta_\mathrm{y}, \eta_\mathrm{z}) = \vec{\eta}$, several groups [1, 3, 4] have found neccessary and sufficient conditions for complete positivity. This form is not a serious restriction as we shall see later. We denote the set of $\vec{\eta}$ corresponding to CP-maps as $\mathcal{D}$.

Property 1 *$\eta \in \mathcal{D}$ if and only if*

$$|\eta_x \pm \eta_y| \leq |1 \pm \eta_z| \tag{3}$$

These conditions specify a tetrahedron in the parameter space of $\{\eta_\mathrm{x}, \eta_\mathrm{y}, \eta_\mathrm{z}\}$.

A simple method of deriving these conditions for unital CP-maps on single-qubits is by examining the effect of a positive map extended to a maximally entangled system of two qubits, $|\Psi_+\rangle = \sum_i |i\rangle|i\rangle$. It can be shown (Appendix) that a necessary and sufficient condition for $\mathcal{S}$ to be a CP-map is that $\mathbb{1}\otimes\mathcal{S}(|\Psi_+\rangle\langle\Psi_+|) \geq 0$. For a unital diagonal map $\mathcal{S}$, this leads to,

$$\rho' = \frac{1}{2}\begin{pmatrix} 1+\eta_\mathrm{z} & 0 & 0 & \eta_\mathrm{x}+\eta_\mathrm{y} \\ 0 & 1-\eta_\mathrm{z} & \eta_\mathrm{x}-\eta_\mathrm{y} & 0 \\ 0 & \eta_\mathrm{x}-\eta_\mathrm{y} & 1-\eta_\mathrm{z} & 0 \\ \eta_\mathrm{x}+\eta_\mathrm{y} & 0 & 0 & 1+\eta_\mathrm{z} \end{pmatrix} \tag{4}$$

being positive when,

$$(1+\eta_\mathrm{z})^2 - (\eta_\mathrm{x}+\eta_\mathrm{y})^2 \;\geq\; 0 \tag{5a}$$

$$(1-\eta_\mathrm{z})^2 - (\eta_\mathrm{x}-\eta_\mathrm{y})^2 \;\geq\; 0. \tag{5b}$$

These are precisely the tetrahedron conditions for the unital single-qubit channel. The geometry of $\mathcal{D}$ in this representation will be the starting point for our investigations (Figure 1).

IV. SIMULATING QUANTUM CHANNELS

The set $\mathcal{D}$ is a regular tetrahedron with vertices I, $\mathrm{R_x}$, $\mathrm{R_y}$ and $\mathrm{R_z}$, where I is the identity tranformation and the R_is are rotations by π about the x, y, z axes. Since the tetrahedron is a convex polyhedron, $\mathcal{D}$ is the convex hull of the points representing I and the three rotations. Thus, every transformation corresponding to a point in $\mathcal{D}$ can be realised as a statistical mixture of those four extremal transformations. Such a transformation is sometimes referred to as a Pauli channel. Thus, we have

Property 2 *$\vec{\eta} \in \mathcal{D}$ if and only if $\vec{\eta}$ corresponds to a Pauli channel.*

Now, suppose $\mathcal{S}$ is a unital single-qubit quantum channel but A is not necessarily diagonal. A possesses a polar decomposition of the form $\mathrm{A} = \mathrm{sPR}$, where $\mathrm{s} = \det(\mathrm{A})$, $\mathrm{P} = \left(\mathrm{AA}^\mathrm{T}\right)^{\frac{1}{2}}$, and R is a rotation [5]. Since sP is symmetric, there exists a rotation Q and a diagonal Δ such that $\mathrm{sP} = \mathrm{Q}\Delta\mathrm{Q}^\mathrm{T}$, giving

$$\mathrm{A} = \mathrm{Q}\Delta\mathrm{Q}^\mathrm{T}\mathrm{R}. \tag{6}$$

Since both Q and $\mathrm{Q}^\mathrm{T}\mathrm{R}$ are rotations, a general unital CP map on a single qubit can be decomposed into a rotation, followed by a diagonal transformation, followed by another rotation. Thus, we can construct a quantum computational network to simulate an arbitrary single-qubit unital quantum channel (Figure 2).

V. CP MAP DYNAMICS

We can simulate a CP map dynamically by coupling the qubit to an ancilla with a time-independant Hamiltonian, evolving the whole system by the unitary, $\mathrm{U(t)} = \exp\left(\frac{-i\mathrm{Ht}}{\hbar}\right)$, and tracing over the ancilla. Thus, the final state of the qubit is a function of the interaction time. This gives us a class of maps on the single-qubit subsystem, parameterised by t, which depends on the coupling Hamiltonian. For unital maps, these classes corespond to paths in $\vec{\eta}$-space. It is again convenient to use a two-qubit ancilla. Consider the following Hamiltonians,

$$\mathrm{H_x} = \sigma_\mathrm{x} \otimes (|\mathrm{a_1}\rangle\langle\mathrm{a_2}| + |\mathrm{a_2}\rangle\langle\mathrm{a_1}|) \tag{7a}$$
$$\mathrm{H_y} = \sigma_\mathrm{y} \otimes (|\mathrm{a_1}\rangle\langle\mathrm{a_3}| + |\mathrm{a_3}\rangle\langle\mathrm{a_1}|) \tag{7b}$$
$$\mathrm{H_z} = \sigma_\mathrm{z} \otimes (|\mathrm{a_1}\rangle\langle\mathrm{a_4}| + |\mathrm{a_4}\rangle\langle\mathrm{a_1}|), \tag{7c}$$

where $\{|\mathrm{a}_i\rangle\}$ are othornormal states of the ancilla, and the initial state of the system is $\rho_0 \otimes |\mathrm{a_1}\rangle\langle\mathrm{a_1}|$. Each H_i induces a set of CP maps in $\vec{\eta}$-space which form a straight line from I to the other corners of the tetrahedron, $\mathrm{R_x}$, $\mathrm{R_y}$ or $\mathrm{R_z}$ respectively. If we combine these Hamiltonians together,

$$\begin{aligned}\mathrm{H_{total}} &= \alpha_\mathrm{x}\mathrm{H_x} + \alpha_\mathrm{y}\mathrm{H_y} + \alpha_\mathrm{z}\mathrm{H_z} \\ 1 &= \alpha_\mathrm{x}^2 + \alpha_\mathrm{y}^2 + \alpha_\mathrm{z}^2,\end{aligned} \tag{8}$$

the map induced by $\mathrm{H_{total}}$ is,

$$\vec{\eta}(\mathrm{t}) = (1,1,1)\cos^2\left(\frac{\mathrm{t}}{\hbar}\right) + \left(2\alpha_\mathrm{x}^2 - 1, 2\alpha_\mathrm{y}^2 - 1, 2\alpha_\mathrm{z}^2 - 1\right)\sin^2\left(\frac{\mathrm{t}}{\hbar}\right) \tag{9}$$

This resulting set of maps is a line in $\vec{\eta}$-space connecting I to the convex combination of $\mathrm{R_x}$, $\mathrm{R_y}$ and $\mathrm{R_z}$ weighted by the α_i^2. For example, if $\alpha_x^2 = \alpha_y^2 = \alpha_z^2 = \frac{1}{3}$, the resulting set of maps is a line from $(1,1,1)$ to $\left(-\frac{1}{3}, -\frac{1}{3}, -\frac{1}{3}\right)$. Thus, if we let the system evolve until $\mathrm{t} = \frac{\pi\hbar}{2}$, the induced map is the best approximation to the Universal-NOT, as we shall see later. At $\mathrm{t} = \frac{\pi\hbar}{3}, \frac{2\pi\hbar}{3}$, the qubit is maximally mixed. Conversely, any unital CP map can be expressed as the result of some combination of $\mathrm{H_x}$, $\mathrm{H_y}$ and $\mathrm{H_z}$ evolved for a particular time (Figures 3 and 4).

VI. APPROXIMATING POSITIVE MAPS

Now consider finding the CP map that best approximates a given positive map on a single qubit. We shall choose the metric on the space of positive maps induced by the inner product,

$$\langle \mathrm{A}, \mathrm{B}\rangle = \mathrm{Tr}(\mathrm{A}^\dagger \mathrm{B}) \tag{10}$$

For the unital diagonal maps, this is simply the Euclidean distance in $\vec{\eta}$-space. Thus, finding the best unital, diagonal CP approximation to a given transformation is simply a matter of minimising the distance to the tetrahedron $\mathcal{D}$, in effect, dropping a perpendicular to the nearest face of $\mathcal{D}$ (Figure 5). This simplification has wide applicability because symmetry requirements on the approximating maps often necessitate the restriction to unital, diagonal maps anyway.

A simple example is the best approximation to the universal NOT gate on a single qubit [6]. On the Bloch sphere, a perfect universal NOT corresponds to the transformation $\vec{\eta} = (-1,-1,-1)$. It is simply the map

$$|\psi\rangle \mapsto \beta^* |0\rangle - \alpha^* |1\rangle \tag{11}$$

that we observed was not physical in (1). Here, we need to drop a perpendicular to the plane

$$\eta_\mathrm{x} + \eta_\mathrm{y} + \eta_\mathrm{z} = -1. \tag{12}$$

This yields the best approximation, $\vec{\eta} = \left(-\frac{1}{3}, -\frac{1}{3}, -\frac{1}{3}\right)$ which was, of course, well-known. It is easy to check that this map can be constructed by selecting randomly from among the three options $\mathrm{R_x}$, $\mathrm{R_y}$, and $\mathrm{R_z}$, each with probability one third.

The technique, however, applies equally well to less symmetrical positive maps not as amenable to the techniques used in [6]. For example, the best approximation to the "pancake" map $\vec{\eta} = (1,1,0)$ is given by the map $\vec{\eta} = \left(\frac{2}{3}, \frac{2}{3}, \frac{1}{3}\right)$. It is also easy to verify that the best approximation of the type $(\eta_\mathrm{x}, \eta_\mathrm{y}, 0)$ is $\vec{\eta} = \left(\frac{1}{2}, \frac{1}{2}, 0\right)$.

VII. APPLICATION TO QUANTUM EAVESDROPPING

In the *four-state* [7] (resp. *six-state* [8]) quantum key-distribution protocol, Alice sends one by one to Bob, qubits in one of four (six) states, $\{|0\rangle_\theta, |1\rangle_\theta\}_\theta$ where $\theta \in \{\mathrm{x},\mathrm{z}\}$ ($\theta \in \{\mathrm{x},\mathrm{y},\mathrm{z}\}$) is a choice of basis and $|0\rangle_{\mathrm{z}} = |0\rangle$, $|1\rangle_{\mathrm{z}} = |1\rangle$, $|0\rangle_{\mathrm{x}} = (|0\rangle + |1\rangle)/2$, $|1\rangle_{\mathrm{x}} = (|0\rangle - |1\rangle)/2$, $|0\rangle_{\mathrm{y}} = (|0\rangle + i\,|1\rangle)/2$ and $|1\rangle_{\mathrm{y}} = (|0\rangle - i\,|1\rangle)/2$. Bob measures each qubit in a random basis $\theta' \in \{\mathrm{x},\mathrm{z}\}$ ($\theta' \in \{\mathrm{x},\mathrm{y},\mathrm{z}\}$) chosen independently of θ. After the quantum transmission, Alice and Bob compare their bases publicly. For each qubit, if their bases correspond, Alice and Bob should share the same bit value, provided the qubits were not tampered with during the transmission. They estimate the error rate or the disturbance of the quantum channel by comparing a sample of these bits. The key distribution is validated if this disturbance is smaller than a certain specified threshold.

Many eavesdropping scenerios against quantum cryptographic protocols have been studied. In particular, in an *incoherent* attack, a possible spy, Eve, interacts each qubit, sent by Alice to Bob, with a probe. One can assume, without loss of generality, that the probe is in a pure state $|\mathrm{E}\rangle$. The unitary operator that Eve uses to interact her probe with Alice's qubits is identical in each case. In the basis $\theta \in \{\mathrm{x},\mathrm{z}\}$ (or $\theta \in \{\mathrm{x},\mathrm{y},\mathrm{z}\}$)

$$\mathrm{U}\,|0\rangle_\theta\,|\mathrm{E}\rangle = |\mathrm{E}_{00}\rangle_\theta\,|0\rangle_\theta + |\mathrm{E}_{01}\rangle_\theta\,|1\rangle_\theta \tag{13}$$

$$\mathrm{U}\,|1\rangle_\theta\,|\mathrm{E}\rangle = |\mathrm{E}_{10}\rangle_\theta\,|0\rangle_\theta + |\mathrm{E}_{11}\rangle_\theta\,|1\rangle_\theta\,, \tag{14}$$

where the $|\mathrm{E}_{ij}\rangle_\theta$ are possibly not normalised nor orthogonal states for Eve's probe. After transmission of qubits, Eve stores her probes until the public announcement of the bases and measures them accordingly. However, Eve is limited to measuring her probes individually. In a *symmetric incoherent* attack, the quantum channel described above is a Pauli channel $(\eta_{\mathrm{x}}, \eta_{\mathrm{y}}, \eta_{\mathrm{z}})$ with $\eta_{\mathrm{x}} = \eta_{\mathrm{z}} = \eta$ for the four-state protocol and $\eta_{\mathrm{x}} = \eta_{\mathrm{y}} = \eta_{\mathrm{z}} = \eta$ for the six-state protocol. This implies that, for any basis θ,

$${}_\theta\langle \mathrm{E}_{01}|\mathrm{E}_{01}\rangle_\theta = {}_\theta\langle \mathrm{E}_{10}|\mathrm{E}_{10}\rangle_\theta = \frac{1-\eta}{2} = \mathrm{D} \tag{15}$$

$${}_\theta\langle \mathrm{E}_{00}|\mathrm{E}_{00}\rangle_\theta = {}_\theta\langle \mathrm{E}_{11}|\mathrm{E}_{11}\rangle_\theta = \frac{1+\eta}{2} = \mathrm{F} = 1 - \mathrm{D} \tag{16}$$

$${}_\theta\langle \mathrm{E}_{00}|\mathrm{E}_{11}\rangle_\theta = {}_\theta\langle \mathrm{E}_{11}|\mathrm{E}_{00}\rangle_\theta = \begin{cases} (\eta+\eta_{\mathrm{y}})/2 & \text{4-state} \\ \eta & \text{6-state} \end{cases} \tag{17}$$

The quantity D, called *disturbance*, is the probability, given that they choose the same basis, Alice and Bob get a different bit. Similarly, the quantity F is called *fidelity* since it is the probability, given Alice and Bob choose the same basis, they get the same bit. Let $\mathrm{p_c}$ be the probability that given Alice and Bob share the same basis and the same bit, Eve guesses correctly the value of this shared bit. When Alice and Bob share the same basis and the same bit, Eve has to guess whether her probe is in state $\frac{1}{\mathrm{F}}\,|\mathrm{E}_{00}\rangle_{\theta\,\theta}\,\langle \mathrm{E}_{00}|$ or in the state $\frac{1}{\mathrm{F}}\,|\mathrm{E}_{11}\rangle_{\theta\,\theta}\,\langle \mathrm{E}_{11}|$. If Eve uses the optimal measurement to guess this bit value,

$$\mathrm{p_c} = \frac{1}{2} + \frac{1}{2}\sqrt{1 - \frac{1}{\mathrm{F}}|\,{}_\theta\langle \mathrm{E}_{00}|\mathrm{E}_{11}\rangle_\theta|^2}. \tag{18}$$

Eve's objective is to maximise $\mathrm{p_c}$ given an allowed disturbance level. In other words, given $\eta \geq \eta_{min}$ where $(1-\eta_{\min})/2 = \mathrm{D}_{\max}$ is the maximum allowed disturbance, Eve has to minimise $|\,{}_\theta\langle \mathrm{E}_{00}|\mathrm{E}_{11}\rangle_\theta|$. Referring to the tetrahedron representing $\mathcal{D}$, it is easy to see that such a minimum is reached for $\vec{\eta} = (\eta_{\min}, 2\eta_{\min} - 1, \eta_{\min})$ for the four-state protocol (Figure 6) and $\vec{\eta} = (\eta_{\min}, \eta_{\min}, \eta_{\min})$ for the six-state protocol (Figure 7). This is precisely the results obtained by Cirac and Gisin in [9].

It should be noted that the same analysis can be applied to protocols involving distribution of EPR pairs between Alice and Bob [10] and, in essence, the same results apply.

VIII. STRØMER-WORONOWICZ RESULT

Horodecki's proof [11] of Peres' separability criterion [12] for 2 by 2 and 2 by 3 dimensional quantum systems relies crucially on an older result of Strømer and Woronowicz [13] stating that any positive map $\mathcal{P}$ from a 2 dimensional quantum system to a 2 or 3 dimensional quantum system can be decomposed in the form

$$\mathcal{P} = \mathcal{CP}_1 + \mathcal{CP}_2 \circ \mathcal{T}, \tag{19}$$

where $\mathcal{CP}_1$ and $\mathcal{CP}_2$ are completely positive maps and $\mathcal{T}$ is the transpose map. The geometry of $\mathcal{D}$ will again make the reason clear for the 2 by 2 dimensional, unital case.

The maps in (19) are not neccessarily trace preserving so it is convenient to consider an equivalent result,

$$\mathcal{P} = \mathrm{p}\mathcal{CP}_1 + (1-\mathrm{p})\mathcal{CP}_2 \circ \mathcal{T}, \tag{20}$$

where $0 \leq \mathrm{p} \leq 1$ and $\mathcal{CP}_1$ and $\mathcal{CP}_2$ are now trace preserving. Thus, $\mathcal{P}$ can be expressed as the convex combination of $\mathcal{CP}_1$ and $\mathcal{CP}_2 \circ \mathcal{T}$.

Furthermore, observe that $\mathcal{T}$ corresponds to the point $(1,-1,1)$ in Figure 1 and is equivalent to the points $(-1,-1,-1)$, $(-1,1,1)$ and $(1,1,-1)$ up to rotations of the tetrahedron. Since rotations correspond to unitary transformations, which are invertible CP maps, any of the above 3 transformations can be substituted for $\mathcal{T}$ in (19).

Now, given any point inside the cube of Figure 1 representing a positive map $\mathcal{P}$, it either lies within $\mathcal{D}$, or within one of the four pyramidal regions. If it lies within the tetrathedron, then the proof is trivial. If the map lies outside $\mathcal{D}$, the map is positive but not completely positive and we need to show that it can be decomposed into $\mathcal{CP}_1$ and $\mathcal{CP}_2 \circ \mathcal{T}$, where $\mathcal{CP}_1$ and $\mathcal{CP}_2$ both lie within $\mathcal{D}$.

To simplify the argument, let us consider the corner region of the U-NOT map $(-1,-1,-1)$. By symmetry, the following argument can be applied to the other three corners regions. By constructing a line between the map $(-1,-1,-1)$ and the face of the tetrahedron whose vertices are $\mathrm{R_x}$, $\mathrm{R_y}$ and $\mathrm{R_z}$, passing through the map $\mathcal{P}$, the proof is now apparent. Every $\mathcal{P}$ can be decomposed in this way as the non-CP pyramidal region is convex with extreme points, $(-1,-1,-1)$, $\mathrm{R_x}$, $\mathrm{R_y}$ and $\mathrm{R_z}$. Figure 8 illustrates the situation.

IX. CONCLUSION

We have seen how the tetrahedral geometry of the set of unital, diagonal single-qubit channels can be used to motivate solutions to a number of problems in quantum information theory. The question of whether the techniques can be extended to non-unital maps or to higher dimensions remains open.

Acknowledgments

I would like to thank Artur Ekert, Patrick Hayden and Hitoshi Inamori for illuminating discussions and valuable feedback on this work. I would also like to acknowledge the support of CESG, UK.

APPENDIX

The CP conditions (3) can be easily derived by ensuring that the trivial extension of a positive map to a maximally entangled state is positive. Let $\mathcal{S} : \mathcal{B}(C^d) \mapsto \mathcal{B}(C^d)$ be a linear operator and let $|\Psi_+\rangle = \mathrm{N}^{-\frac{1}{2}} \sum_i |i\rangle\,|i\rangle$ be a maximally entangled state. Then

$$(\mathbf{1} \otimes \mathcal{S})\,|\Psi_+\rangle\,\langle\Psi_+| \geq 0, \tag{21}$$

iff $\mathcal{S}$ is CP. To see this, if $\mathcal{S}$ is not CP, $\exists\,|\Phi\rangle \in \mathcal{H} \otimes \mathcal{H}$ such that $(\mathbf{1} \otimes \mathcal{S})\,|\Phi\rangle\,\langle\Phi| \not\geq 0$. We can express,

$$|\Phi\rangle = (\mathcal{A} \otimes \mathbf{1})\,|\Psi_+\rangle\,, \tag{22}$$

where $\mathcal{A}$ is CP and its components are,

$$\begin{aligned} \langle m|\,\mathrm{A}\,|n\rangle &= \sqrt{\mathrm{N}}a_{mn} \\ (\mathrm{A} \otimes \mathbf{1})\,|\Psi_+\rangle &= \sum_{m,n} a_{mn}\,|m\rangle\,|n\rangle \\ \rho &\mapsto \mathrm{A}\rho\mathrm{A}^\dagger. \end{aligned} \tag{23}$$

Thus, we have that,

$$\begin{aligned} (\mathbf{1} \otimes \mathcal{S})(\mathcal{A} \otimes \mathbf{1})\,|\Psi_+\rangle\,\langle\Psi_+| &\not\geq 0 \\ (\mathcal{A} \otimes \mathbf{1})(\mathbf{1} \otimes \mathcal{S})\,|\Psi_+\rangle\,\langle\Psi_+| &\not\geq 0 \\ \Rightarrow \quad (\mathbf{1} \otimes \mathcal{S})\,|\Psi_+\rangle\,\langle\Psi_+| &\not\geq 0, \end{aligned} \tag{24}$$

hence we only need look at the action of $\mathbf{1} \otimes \mathcal{S}$ on the maximally entangled state $|\Psi_+\rangle$ to ensure that $\mathcal{S}$ is CP.

[1] A. Fujiwara and P. Algoet, Physical Review **A59**(5), 3290 (1999).
[2] M. B. Ruskai, S. Szarek, and E. Werner (2001), LANL e-print quant-ph/0101003.
[3] M. B. Ruskai, *Minimal entropy of states emergy from noisy quantum channels* (1999), LANL e-print quant-ph/9911079.
[4] D. di Vincenzo and B. Terhal (1998), LANL e-print quant-ph/9806095.
[5] R. Horn and C. Johnson, *Topics in Matrix Analysis* (Cambridge University Press, 1985).
[6] V. Buzek, M. Hillery, and R. Werner, *Optimal manipulations with qubits: Universal not gate* (1997), LANL e-print quant-ph/9711070.
[7] C. Bennett and G. Brassard, eds., *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (Banglore, India, 1984).
[8] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).
[9] I. Cirac and N. Gisin, Phys. Lett. A **229**, 1 (1997).
[10] A. Ekert, in *Proceedings of the Conference in Commemoration of John Bell, "Quantum (Un)Speakables"* (University of Vienna, 2000).
[11] P. Horodecki, Phys. Lett. A **232**, 333 (1997).
[12] A. Peres, in *Proceedings of Nobel Symposium 104: Modern Studies of Basic Quantum Concepts and Phenomena* (1998), vol. 76.
[13] S. L. Woronowicz, Rep. Math. Phys. **10**, 165 (1976).

FIGURES

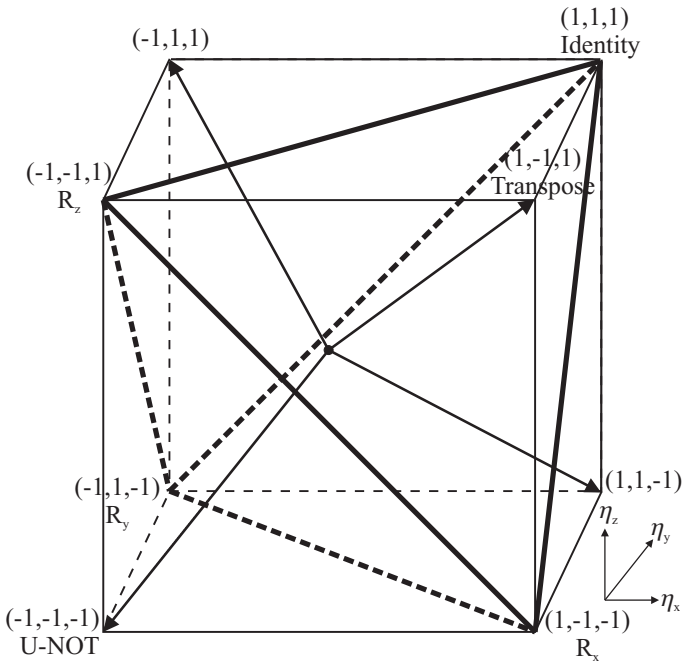

FIG. 1: The completely positive unital, diagonal single-qubit maps as a subset of the positive ones. The axes η_x, η_y, and η_z represent the diagonal "squeezing parameters". Some special transformations, including the matrix transpose, the universal NOT, and the identity are also marked.

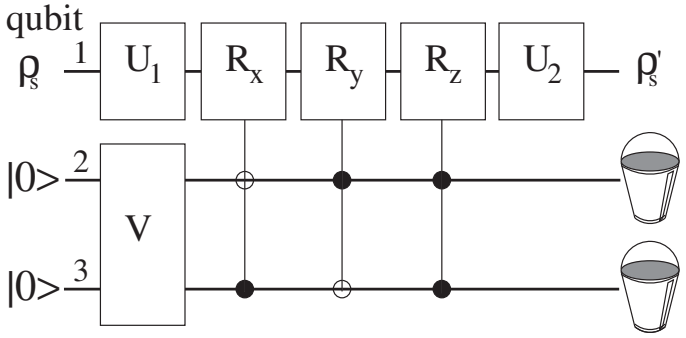

FIG. 2: A quantum computational network for simulating a unital single-qubit quantum channel. Transformations U_1 and U_2 are qubit rotations while V prepares arbitrary superpositions of the states $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ of the ancilla. After interacting with qubit 1, the ancilla is ignored. The controlled-controlled-R_i gates perform the Pauli rotations depending on the component amplitudes of the ancilla.

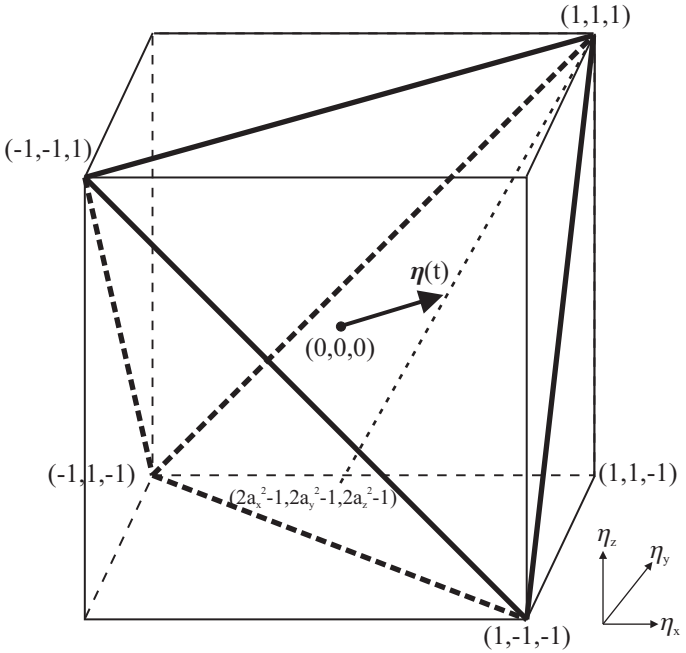

FIG. 3: Dynamical generation of a CP map by suitable combination of coupling Hamiltonians and evolution times.

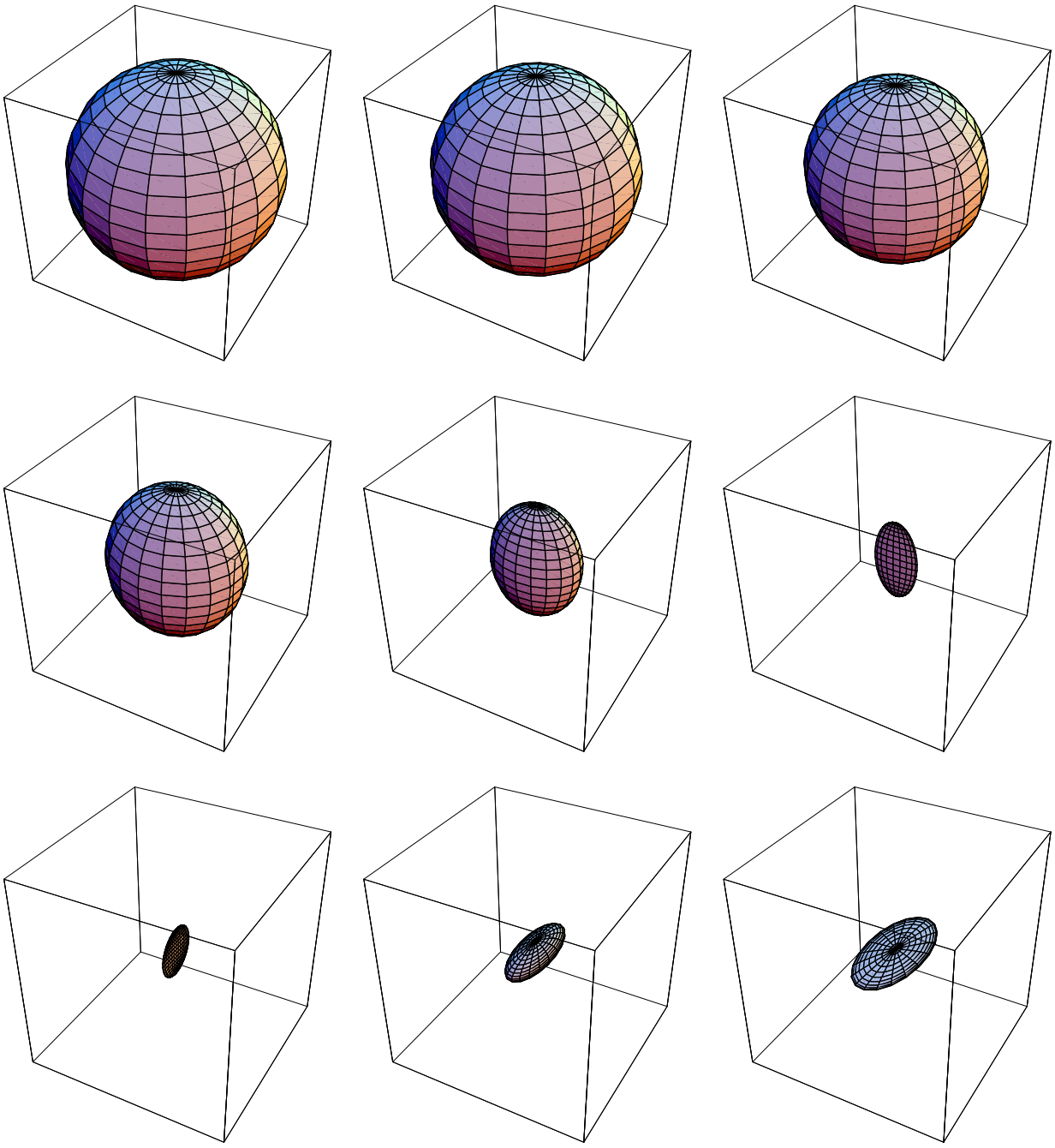

FIG. 4: The Bloch sphere of the reduced density operator of the single qubit evolving in time with $\alpha_{\rm x}^2 = \frac{1}{2}$, $\alpha_{\rm y}^2 = \frac{1}{3}$ and $\alpha_{\rm z}^2 = \frac{1}{6}$.

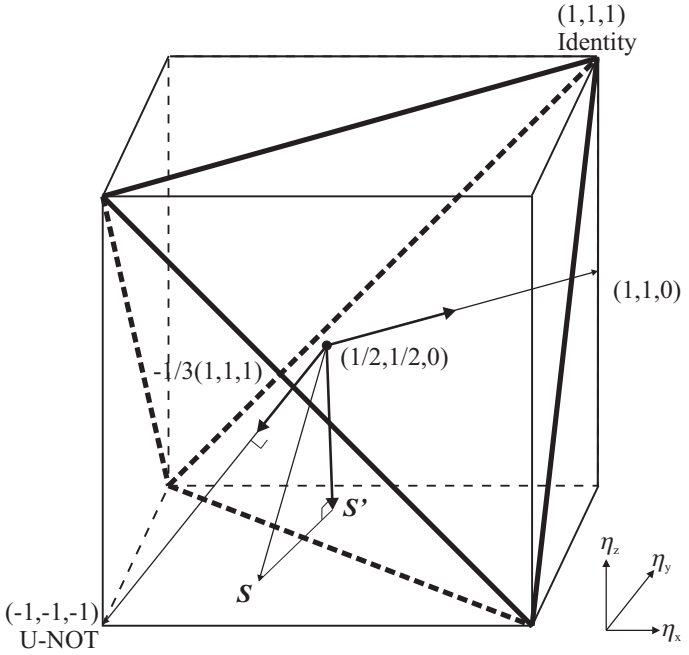

FIG. 5: Both the universal NOT and a generic positive map are approximated by dropping perpendiculars to the closest face of $\mathcal{D}$.

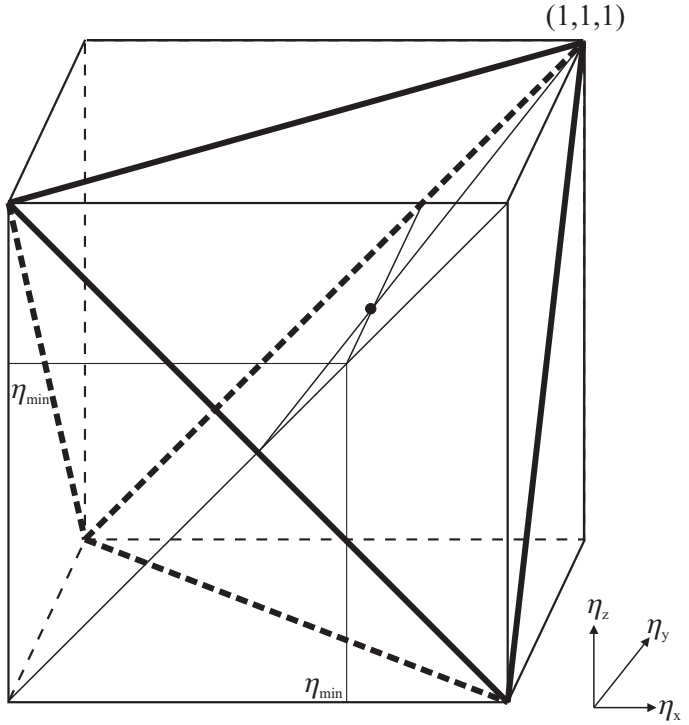

FIG. 6: For the four-state protocol with $\eta_x = \eta_z = \eta \geq \eta_{\min}$, Eve has to minimise η_y. When $\eta_{\min}$ is positive, the minimum lies on the plane $\{(1,1,1),(-1,-1,1),(1,-1,1)\}$.

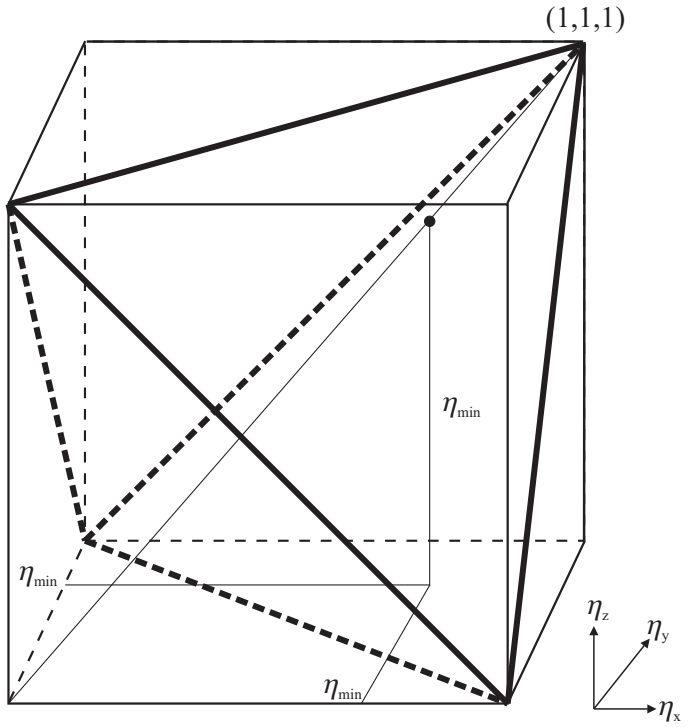

FIG. 7: For the six-state protocol, with $\eta_x = \eta_y = \eta_z = \eta \geq \eta_{\min}$, the minimum is reached for $\eta = \eta_{\min}$.

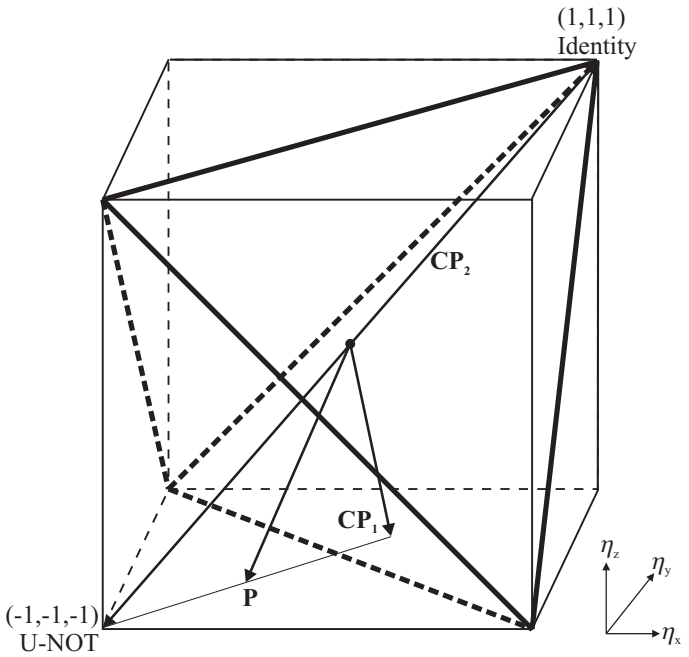

FIG. 8: The map $\mathcal{P}$ is decomposed into components $\mathcal{CP}_1$ and $\mathcal{CP}_2 \circ$ U-NOT lying entirely within $\mathcal{D}$.