Dealing with unknown quantum operations

Filippo Miatto*

SUPA and Department of Physics, University of Strathclyde, Glasgow G4 0NG, Scotland, U.K.
and
Current address: Dept. of Physics, University of Ottawa,
150 Louis Pasteur, Ottawa, Ontario, K1N 6N5 Canada
(Dated: May 2, 2014)

In the context of quantum communications between two parties (here Alice and Bob), Bob’s lack of knowledge about which channel Alice might be using. We indicate this operation by $T_w$, with the subscript reminding us that it depends on the probability density $w(g)$.

We have two limiting cases: the case of complete knowledge, where $w(g) = \delta(g - \hat{g})$ for some $\hat{g} \in G$, and the case of minimal knowledge, where $w(g) = 1$. In these limiting cases Bob receives either the pure state $T_\delta[\hat{\rho}] = U_\delta[\hat{\rho}]$, or the completely incoherent mixture $T[\hat{\rho}] = \int_G U_g[\hat{\rho}] dg$. In the general case of partial knowledge, Bob receives a partially mixed state, effectively obtained from the initial state by multiplying its off-diagonal entries by numbers of modulus not larger than 1: the representation of $G$ on the state space, being unitary, induces a Fourier transform, or a Fourier series, of $w(g)$ on the manifold that underlies $G$.

As a simple example consider $G = U(1)$, the twirling of a density matrix in the eigenbasis of some selfadjoint operator $L$ is

$$T_w[\hat{\rho}] = \frac{1}{2\pi} \sum_{m,n} r_{m,n} \int_0^{2\pi} d\phi \, w(\phi) e^{i\phi L} |m\rangle \langle n| e^{-i\phi L}$$

$$= \frac{1}{2\pi} \sum_{m,n} r_{m,n} \int_0^{2\pi} d\phi \, w(\phi) e^{i\phi (m-n)} |m\rangle \langle n|$$

$$= \sum_{m,n} r_{m,n} \hat{w}_{m-n} |m\rangle \langle n|. \quad (2)$$

The numbers $\hat{w}_{m-n}$ are the Fourier coefficients of $w(g)$, so only the diagonal is always safe from alteration, as $w_0 = 1$. The net effect is that in general the purity of the state that Alice sends, which initially is $\sum_{m,n} |r_{m,n}|^2$ becomes $\sum_{m,n} |r_{m,n}|^2 |\hat{w}_{m-n}|^2$, so as $|\hat{w}_{m-n}|^2 \leq 1$, it cannot increase, and in general it is reduced.

We now show some properties satisfied by twirling. The first property is that sequential twirlings can be composed. The second property is that twirling behaves in an associative way, i.e. $(T_w T_w') T_w = T_w (T_w' T_w)$. To avoid clutter in the equations, we omit the symbol “◦”, with the rule that the writing $AB$ means “$A$ after $B$”.

Let’s consider the composition of two twirlings $T_w T_{w'}$ and check if it still corresponds to a twirling $T_v$ for some
probability distribution \( v(g) \). Using the properties of the Haar measure, it is easy to see that it is the case, by explicitly calculating \( v(g) \):

\[
(\mathcal{T}_w' \mathcal{T}_w)[\hat{\rho}] = \int_G dg \, dh \, w'(h) w(g) \mathcal{U}_{h g} [\hat{\rho}] \tag{3}
\]

\[
= \int_G dg \, dh \, w'(h) w(h^{-1} g) \mathcal{U}_g [\hat{\rho}]. \tag{4}
\]

So the composition of the two initial twirlings is equivalent to a twirling with respect to the probability distribution

\[
v(g) = \int_G dh \, w'(h) w(h^{-1} g) := (w' \ast w)(g). \tag{5}
\]

Eq. (5) is the definition of convolution on a group, and it always yields an allowed probability distribution. Therefore we have the composition rule

\[
\mathcal{T}_w \mathcal{T}_w' = \mathcal{T}_{w' \ast w'}, \tag{6}
\]

where the symbol "\( \ast \)" means convolution on the group \( G \). Now we can easily prove associativity:

\[
(\mathcal{T}_w' \mathcal{T}_w') \mathcal{T}_w = \mathcal{T}_{w' \ast w' \ast w} = \mathcal{T}_{(w' \ast w') \ast w} \tag{7}
\]

\[
= \mathcal{T}_{w' \ast (w' \ast w)} = \mathcal{T}_{w' \ast w'} \tag{8}
\]

\[
= \mathcal{T}_{(w' \ast w) \ast w} \tag{9}
\]

where we used the composition rule (5) and the fact that convolution is associative, so as a consequence also twirling is.

**TWIRLING OF OPERATIONS**

Alice now modifies a copy of her state via a quantum operation \( \mathcal{O} \) before sending it to Bob: \( \hat{\rho}' = \mathcal{O}[\hat{\rho}] \), so Bob receives the states \( \hat{\sigma} = \mathcal{T}_w[\hat{\rho}] \) and \( \hat{\sigma}' = (\mathcal{T}_w \mathcal{O})[\hat{\rho}] \):

\[
\begin{array}{ccc}
\hat{\rho} & \xrightarrow{\mathcal{O}} & \hat{\rho}' \\
\mathcal{T}_w & & \mathcal{T}_w \\
\hat{\sigma} & \xrightarrow{\mathcal{O}'} & \hat{\sigma}'
\end{array} \tag{10}
\]

The natural question to ask is: what is the operation \( \mathcal{O}' \) (if there is any) that transforms \( \hat{\sigma} \) into \( \hat{\sigma}' \)? In other terms, how does Bob perceive Alice’s operation \( \mathcal{O} \)? This question is equivalent to the problem of finding a map \( \mathcal{O}' \) that, given \( \mathcal{O} \) and \( \mathcal{T}_w \), makes the diagram commute: \( \mathcal{O}' \mathcal{T}_w = \mathcal{T}_w \mathcal{O} \).

If Bob knew the channel employed, \( w(g) \) would be a delta function centred on a specific \( \hat{g} \), and it would be one of the limiting cases, \( \mathcal{T}_\delta = \mathcal{U}_\delta \). In this case applying \( \mathcal{O}' \) would be equivalent to applying the following sequence:

\( \mathcal{U}_{\delta^{-1}} \) to turn \( \hat{\sigma} \) into \( \hat{\rho} \), then \( \mathcal{O} \) to obtain \( \hat{\rho}' \) and finally \( \mathcal{U}_\delta \) to obtain \( \hat{\sigma}' \). Put simply,

\[
\mathcal{O}' = \mathcal{T}_\delta \mathcal{O} \mathcal{T}_\delta^{-1} = \mathcal{U}_\delta \mathcal{O} \mathcal{U}_{\delta^{-1}}. \tag{11}
\]

This is rather trivial, as \( \mathcal{T}_\delta \), corresponding to a unitary transformation, is invertible. The real issue that we want to explore is the assignment \( \mathcal{O} \rightarrow \mathcal{O}' \) for a general probability distribution \( w(g) \).

To go through the discussion, we employ a decomposition of Alice’s operation into four parts, exploiting the matrix representation of the density operator. A quantum operation can be written in terms of Kraus operators:

\[
\mathcal{O}[\hat{\rho}] = \sum_i K_i \hat{\rho} K_i^\dagger. \tag{12}
\]

The linearity of the Kraus representation allows us to split the density matrix into a diagonal matrix, \( \hat{d} \), and a vanishing-diagonal matrix \( \hat{f} \) via two operations \( \mathcal{D} \) and \( \mathcal{F} \) (for instance \((\frac{1}{2} 0\frac{1}{2}) = (\frac{1}{2} 0\frac{1}{2}) + (0 \frac{1}{2} 0)\). Equivalently, we have two contributions to the final result:

\[
\mathcal{O} = \mathcal{O} \mathcal{D} + \mathcal{O} \mathcal{F}, \tag{13}
\]

where \( \mathcal{O} \mathcal{D}[\hat{\rho}] \) and \( \mathcal{O} \mathcal{F}[\hat{\rho}] \) produce, respectively, the matrices \( m_1 \) and \( m_2 \), such that \( m_1 + m_2 = \mathcal{O} (\mathcal{D} + \mathcal{F})[\hat{\rho}] = \mathcal{O}[\hat{\rho}] = \hat{\rho}' \). Note that in general neither of \( m_1 \) or \( m_2 \) are proper quantum states, but this is not of our concern as their sum is always the proper quantum state at the output of \( \mathcal{O} \).

The reason for this decomposition is that it allows us to study the effect of twirling on the two contributions separately:

\[
\begin{array}{ccc}
\mathcal{T}_w \bigcirc \mathcal{D} & \xrightarrow{\mathcal{O}} & m_1 \\
\mathcal{T}_w & \xrightarrow{\mathcal{O}'} & \mathcal{T}_w [m_1] \\
\mathcal{T}_w \bigcirc \mathcal{D} & \xrightarrow{\mathcal{O}'} & \mathcal{T}_w [m_2]
\end{array} \tag{14}
\]

A diagonal matrix is left unchanged under any twirling, i.e. \( \mathcal{T}_w \mathcal{D} = \mathcal{D} \), so we can represent the twirling of a diagonal matrix with an arrow on itself.

**The \( \mathcal{O} \rightarrow \mathcal{O}' \) assignment**

With reference to the first diagram in (14), obtained by applying the map \( \mathcal{D} \) to the initial state \( \hat{\rho} \), we immediately obtain the commutativity relation \( \mathcal{O}' \mathcal{T}_w \mathcal{D} = \mathcal{T}_w \mathcal{O} \mathcal{D} \), with no additional restrictions on \( \hat{\rho}' \) or on \( \mathcal{O} \). The second diagram, instead, obtained by applying the map \( \mathcal{F} \) to the initial state \( \hat{\rho} \), induces a restriction on the kind of operations \( \mathcal{O} \) that allow commutativity: here the twirling has to be at least partially invertible.
If we consider the twirling action on the entries of a density matrix, eq. (2), we see that we can retrieve individual off-diagonal entries where \( \tilde{w}_{m-n} \neq 0 \) by entry-wise multiplication by the inverse \( \tilde{w}_{m-n}^{-1} \). We refer to the action of inverting the twirling where \( \tilde{w}_{m-n} \neq 0 \) as partial twirling inversion and we indicate it as \( \tilde{T}_w^{-1} \). In a non-ideal situation, the condition should be generalised to \( |\tilde{w}_{m-n}| \geq b \) where \( b \) is a lower bound determined by the experimental conditions. Note that twirling is generally not invertible, and that partial twirling inversion is not a positive operation.

From the points raised above, we see that the second diagram in (14) commutes if the final result \( T_w[m_2] \) is independent of the entries of \( \tilde{f} \) that are irreducibly lost after the twirling \( T_w \). We can annihilate only those entries by applying the map \( (\tilde{T}_w^{-1}T_w) \), and create the requirement for commutativity: \( T_wO\tilde{F} = T_wO(\tilde{T}_w^{-1}T_w)\tilde{F} \). Comparison with the commutativity expression \( O'\tilde{T}_w\tilde{F} = T_wO\tilde{F} \) immediately gives \( O' = T_wO\tilde{T}_w^{-1} \). We can confirm that commutativity of the first diagram does not imply any restriction, as \( T_wOD = T_wO(\tilde{T}_w^{-1}T_w)D \) is always satisfied. This means that the commutativity requirement of the second diagram is equivalent to \( T_wO = T_wO(\tilde{T}_w^{-1}T_w) \).

The other consequence is that the commutativity of both diagrams in (14), together, imply commutativity of the diagram (10): \( O'\tilde{T}_wD + O'\tilde{T}_wF = T_wO\tilde{D} + T_wO\tilde{F} \Rightarrow O'\tilde{T}_w = T_wO \), as it should be, and our proof is complete. We are now ready to state the following theorem:

**Theorem 1.** With reference to the definitions of twirling \( T_w \) and of its partial inversion \( \tilde{T}_w^{-1} \), the operations \( O \) that satisfy \( T_wO = T_wO(\tilde{T}_w^{-1}T_w) \) make the diagram (10) commutative, with

\[
O' = T_wO\tilde{T}_w^{-1}.
\]

**Proof.** See above discussion. \( \Box \)

We point out that the matter of distinguishability of operations is an interesting and closely related issue: the assignment \( O \mapsto O' \) in general is not injective, so there might well be a many-to-one assignment, in which case Bob identifies operations that are different for Alice. This is an issue that has to be addressed in matters regarding superselection.

Another issue that we should mention regards the state-dependence of the commutativity condition: one could just consider states that already lack enough coherence so that partial inversion of twirling is enough to retrieve the initial state. We have that for those states \( (\tilde{T}_w^{-1}T_w) = \text{id} \), so the representability condition is always satisfied, which means that whatever \( O \) Alice chooses, there will be an allowed choice of \( O' \) for Bob. However, one should be careful, as the states that make this possible can be quite dull (an example could be randomly rotating a state to make it rotationally invariant). On the other hand, particular instances of this issue might still be interesting: for instance if \( w(g) \) is such that twirling affects coherences between particular sets of eigenstates, employing states that do not exhibit such coherences can be beneficial, as they can still maintain coherence between all the other eigenstates, in a decoherence-free subspace fashion.

**Example**

As an example, we work out the representation of an operation in case of minimal knowledge \( w(g) = 1 \), inducing a total twirling \( T \) and compare it to a previous result [11]. In this extreme case, all Fourier coefficients are zero apart from the zeroth one (which acts on the diagonal elements and its value is 1), so \( T \) is the least locally invertible twirling, and it’s equivalent to \( D \), so we can conveniently replace any occurrence of \( D \) with \( T \). Commutativity of the first diagram in (14) means \( O'T = TOT \). Then, notice that as \( (\tilde{T}_w^{-1}T_w) = T \), the commutativity requirement is \( TO = TOT \), so the commutativity of the first diagram implies commutativity of the total diagram (10): \( O' = TOT = TO \). Finally, we have \( O' = TO = TOT \), because total twirling is not invertible.

This result is exactly the same that would be reached by applying the prescription in [11, 12]. In that reference, in case of total twirling, an operation \( O \) is prescribed to be mapped to

\[
O' = \int_G dg U_gOU_{g^{-1}}.
\]

However, we aim now at showing that this prescription is not as universal as it was intended. Considering the following diagram

\[
\begin{array}{c}
\tilde{T} \downarrow O' \downarrow \tilde{T} \\
\sigma \leftarrow \rightarrow \sigma' \leftarrow \rightarrow \sigma''
\end{array}
\]

we can look for the requirement that makes \( \tilde{\sigma}'' = \tilde{\sigma}' \), i.e. that \( (O'T)|\tilde{\rho} = (TO)|\tilde{\rho} \):

\[
\tilde{\sigma}'' = (O'T)|\tilde{\rho} = \int_G dg dh U_gOU_{g^{-1}}h|\tilde{\rho} = \int_G dg U_gOT|\tilde{\rho} = (TO)|\tilde{\rho}.
\]

So \( \tilde{\sigma}' = \tilde{\sigma}'' \) and the diagram commutes if \( TOT = TO \).
However, in the reference [11], the authors omit it, and one is lead to believe that any operation $O$ that Alice performs always has a corresponding operation $O'$ for Bob.

It is even more instructive to explicitly show a counterexample to the operation assignment (16). Consider a qubit state, and a total twirling generated by rotations around the $\hat{z}$ axis. The operation that we use as counterexample needs to violate the requirement $\mathcal{T} O \mathcal{T} = \mathcal{T} O$. An example is a rotation about $\hat{x}$ (of an angle $\theta \neq k\pi$). With reference to diagram (17), we have (remember that $\mathcal{T}$ annihilates the off-diagonal values)

$$\sigma' = \mathcal{T} [e^{-i\frac{\pi}{2} \hat{x}} \hat{\rho} e^{i\frac{\pi}{2} \hat{x}}] \quad (19)$$

$$= \frac{1}{2} \begin{pmatrix} 1 + (2p - 1) \cos \theta - 23(b) \sin \theta & 0 \\ 0 & 1 - (2p - 1) \cos \theta + 23(b) \sin \theta \end{pmatrix}$$

for some angle $\theta$. Instead, if we proceed through the diagram the other way, we obtain

$$\sigma'' = O' \mathcal{T} \left[ \begin{pmatrix} p & b \\ b^* & 1 - p \end{pmatrix} \right] = O' \left[ \begin{pmatrix} p & 0 \\ 0 & 1 - p \end{pmatrix} \right]$$

$$= \frac{1}{2} \begin{pmatrix} 1 + (2p - 1) \cos \theta & 0 \\ 0 & 1 - (2p - 1) \cos \theta \end{pmatrix} \quad (20)$$

So the prescription (16) fails in this case, i.e. $\sigma' \neq \sigma''$, because the operation that we chose is not representable after the twirling, as it does not satisfy the commutativity requirement. We also see that a general rotation about $\hat{x}$ is representable after a total $\hat{z}$-twirling only for states that have $\Im(b) = 0$, and this is an example of state-dependent representability.

**CONCLUSION**

We have shown the composition rule and the associativity property of generalised twirling. Then, we have found the requirement for an operation $O$ to be faithfully mapped to an operation $O'$ under a generalised twirling. We have also shown that the results in [11, 12] which inspired our study, lack a way of telling which operations can be represented under a twirling. Under the framework established in this work, the same operations would instead be correctly identified as non-representable. These results can help characterise quantum communication schemes, or understand the resources needed to lift a superselection rule, or study implementations of data hiding protocols, and similar issues that are affected by or rely on a lack of knowledge.

**ACKNOWLEDGEMENTS**

The author thanks Stephen Barnett, Daniel Oi and Davide Rinaldi for discussions. This work was supported by the UK EPSRC and the Canada Excellence Research Chairs (CERC) Program.

* fmiatto@uottawa.ca

[1] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. 76, 722 (1996).
[2] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A 54, 3824 (1996).
[3] K. G. H. Vollbrecht and R. F. Werner, Phys. Rev. A 64, 062307 (2001).
[4] S. Lee, D. P. Chi, S. D. Oh, and J. Kim, Phys. Rev. A 68, 062304 (2003).
[5] M. Hayashi, D. Markham, M. Murao, M. Owari, and S. Virmani, Phys. Rev. A 77, 012104 (2008).
[6] W. Dür, J. I. Cirac, M. Lewenstein, and D. Bruß, Phys. Rev. A 61, 062313 (2000).
[7] V. Gheorghiu, arXiv:1204.1072 [quant-ph] (2012).
[8] M. Skotiniotis and G. Gour, arXiv:1202.3163v2 [quant-ph] (2012).
[9] I. Marvian and R. W. Spekkens, arXiv:1104.0018v1 [quant-ph] (2011).
[10] S. D. Bartlett, T. Rudolph, R. W. Spekkens, and P. S. Turner, New Journal of Physics 11, 063013 (2009).
[11] S. D. Bartlett, T. Rudolph, and R. W. Spekkens, Rev. Mod. Phys. 79, 555 (2007).
[12] G. Gour and R. W. Spekkens, arXiv:0711.0043v2 [quant-ph] (2007).