Tight reference frame-independent quantum teleportation

Dominic Verdon & Jamie Vicary

Department of Computer Science
University of Oxford

June 9, 2016

Our result

- Teleportation is possible between parties that do not share a reference frame (RF).

Our result

- Teleportation is possible between parties that do not share a reference frame (RF).
- Requires communication of unspeakable information.
  The classical channel we use is very important.

Our result

- Teleportation is possible between parties that do not share a reference frame (RF).
- Requires communication of unspeakable information.
  The classical channel we use is very important.
- No transfer of information about the RF configuration.
  No prior communication or additional resources.

Our result

- Teleportation is possible between parties that do not share a reference frame (RF).
- Requires communication of unspeakable information.
  The classical channel we use is very important.
- No transfer of information about the RF configuration.
  No prior communication or additional resources.
- Depends on the action of the group of RF transformations.
  The group must be finite.

Our result

- Teleportation is possible between parties that do not share a reference frame (RF).
- Requires communication of unspeakable information.
  The classical channel we use is very important.
- No transfer of information about the RF configuration.
  No prior communication or additional resources.
- Depends on the action of the group of RF transformations.
  The group must be finite.
- Constructions of reference frame–independent (RFI) teleportation protocols.

How it fits in

- Hidden assumption of shared RF in teleportation first noted in [Enk, 2001].

How it fits in

- Hidden assumption of shared RF in teleportation first noted in [Enk, 2001].
- When the group of RF transformations contains $U(1)$, perfect teleportation is impossible. [Chiribella et al., 2012]
  Does not apply to finite groups.

How it fits in

- Hidden assumption of shared RF in teleportation first noted in [Enk, 2001].
- When the group of RF transformations contains $U(1)$, perfect teleportation is impossible. [Chiribella et al., 2012]
  Does not apply to finite groups.
- Work has been done on imperfect protocols in the infinite case. [Marzolino and Buchleitner, 2015]

How it fits in

- Hidden assumption of shared RF in teleportation first noted in [Enk, 2001].
- When the group of RF transformations contains $U(1)$, perfect teleportation is impossible. [Chiribella et al., 2012]
  Does not apply to finite groups.
- Work has been done on imperfect protocols in the infinite case. [Marzolino and Buchleitner, 2015]
- We deal with the case of a finite group of RF transformations.

Applications

- *Reference frame uncertainty.*

Applications

- *Reference frame uncertainty.*
  - Two parties with different RF alignments can perform teleportation.

Applications

- *Reference frame uncertainty.*
  - Two parties with different RF alignments can perform teleportation.
  - Works even with dynamic frame alignments.

Applications

- *Reference frame uncertainty.*
  - Two parties with different RF alignments can perform teleportation.
  - Works even with dynamic frame alignments.
- *Reference frame hiding.*

Applications

- *Reference frame uncertainty.*
  - Two parties with different RF alignments can perform teleportation.
  - Works even with dynamic frame alignments.
- *Reference frame hiding.*
  - RF configurations may be of cryptographic importance. [Kitaev et al., 2004]

Applications

- *Reference frame uncertainty.*
  - Two parties with different RF alignments can perform teleportation.
  - Works even with dynamic frame alignments.
- *Reference frame hiding.*
  - RF configurations may be of cryptographic importance. [Kitaev et al., 2004]
  - Can teleport without exchanging any RF information.

Applications

- *Reference frame uncertainty.*
  - Two parties with different RF alignments can perform teleportation.
  - Works even with dynamic frame alignments.
- *Reference frame hiding.*
  - RF configurations may be of cryptographic importance. [Kitaev et al., 2004]
  - Can teleport without exchanging any RF information.
- *Infinite reference frames.*

Applications

- *Reference frame uncertainty.*
  - Two parties with different RF alignments can perform teleportation.
  - Works even with dynamic frame alignments.
- *Reference frame hiding.*
  - RF configurations may be of cryptographic importance. [Kitaev et al., 2004]
  - Can teleport without exchanging any RF information.
- *Infinite reference frames.*
  - Discretise the group of RF transformations using limited prior communication.

Applications

- *Reference frame uncertainty.*
  - Two parties with different RF alignments can perform teleportation.
  - Works even with dynamic frame alignments.
- *Reference frame hiding.*
  - RF configurations may be of cryptographic importance. [Kitaev et al., 2004]
  - Can teleport without exchanging any RF information.
- *Infinite reference frames.*
  - Discretise the group of RF transformations using limited prior communication.
  - Imperfect protocols as limits of perfect finite-group schemes?

Applications

- *Reference frame uncertainty.*
  - Two parties with different RF alignments can perform teleportation.
  - Works even with dynamic frame alignments.
- *Reference frame hiding.*
  - RF configurations may be of cryptographic importance. [Kitaev et al., 2004]
  - Can teleport without exchanging any RF information.
- *Infinite reference frames.*
  - Discretise the group of RF transformations using limited prior communication.
  - Imperfect protocols as limits of perfect finite-group schemes?
- CQM as a way to work with RFs in quantum information.

Table of contents

Reference frames: I

- RFs are implicit in the description of quantum states.

Reference frames: I

- RFs are implicit in the description of quantum states.
  - Angular momentum eigenstates of a spin 1/2 particle: *along which axis?*

Reference frames: I

- RFs are implicit in the description of quantum states.
  - Angular momentum eigenstates of a spin 1/2 particle: *along which axis?*
  - Eigenstates of photon number: *what is time t_0?*

Reference frames: I

- RFs are implicit in the description of quantum states.
  - Angular momentum eigenstates of a spin 1/2 particle: *along which axis?*
  - Eigenstates of photon number: *what is time* t_0*?*
  - Degenerate energy eigenstates of a particle in a cuboidal box: *which way round is the box?*

Reference frames: I

- RFs are implicit in the description of quantum states.
  - Angular momentum eigenstates of a spin 1/2 particle: *along which axis?*
  - Eigenstates of photon number: *what is time* t_0*?*
  - Degenerate energy eigenstates of a particle in a cuboidal box: *which way round is the box?*
- Each RF has an associated group G of RF transformations.

Reference frames: I

- RFs are implicit in the description of quantum states.
  - Angular momentum eigenstates of a spin 1/2 particle: *along which axis?* $G = SO(3)$.
  - Eigenstates of photon number: *what is time* t_0*?*
  - Degenerate energy eigenstates of a particle in a cuboidal box: *which way round is the box?*
- Each RF has an associated group G of RF transformations.

Reference frames: I

- RFs are implicit in the description of quantum states.
  - Angular momentum eigenstates of a spin 1/2 particle: *along which axis?* $G = SO(3)$.
  - Eigenstates of photon number: *what is time* t_0*?* $G = U(1)$.
  - Degenerate energy eigenstates of a particle in a cuboidal box: *which way round is the box?*
- Each RF has an associated group G of RF transformations.

Reference frames: I

- RFs are implicit in the description of quantum states.
  - Angular momentum eigenstates of a spin 1/2 particle: *along which axis?* $G = SO(3)$.
  - Eigenstates of photon number: *what is time* t_0*?* $G = U(1)$.
  - Degenerate energy eigenstates of a particle in a cuboidal box: *which way round is the box?* $G = \mathfrak{S}_4$.
- Each RF has an associated group G of RF transformations.

Reference frames: II

- H carries a unitary representation $\pi : G \to \text{End}(H)$ of G.

Reference frames: II

- H carries a unitary representation $\pi : G \to \text{End}(H)$ of G.
- When RF configuration transforms by $g^{-1} \in G$:

	Old frame	New frame
State	$\|\psi\rangle$	$\pi(g)\,\|\psi\rangle$
Operations	$L \in \text{End}(H)$	$\pi(g) L \pi(g)^\dagger$

A classification of teleportation protocols

- For a Hilbert space H, a *unitary error basis* is a basis $\{U_i\}$ of $End(H)$ such that:

A classification of teleportation protocols

- For a Hilbert space H, a *unitary error basis* is a basis $\{U_i\}$ of $End(H)$ such that:
  1. U_i are all unitary.

A classification of teleportation protocols

- For a Hilbert space H, a *unitary error basis* is a basis $\{U_i\}$ of $End(H)$ such that:
  1. U_i are all unitary.
  2. U_i are orthonormal under the Hilbert-Schmidt inner product.

A classification of teleportation protocols

- For a Hilbert space H, a *unitary error basis* is a basis $\{U_i\}$ of $End(H)$ such that:
  1. U_i are all unitary.
  2. U_i are orthonormal under the Hilbert-Schmidt inner product.
- When Hilbert spaces have minimal dimension, teleportation protocols correspond to UEBs:

Shared entangled state	$\sum_i \|i\rangle \otimes \|i\rangle$
Alice's measurement basis	$\|\phi_x\rangle := \sum_i \|i\rangle \otimes U_x \|i\rangle$
Bob's unitary correction	$C_x := U_x^T$

Example: I

- Alice and Bob are in labs with different orientations in space, related by $g \in SO(3)$.
  They share the entangled state $\sum_i |i\rangle \otimes |i\rangle$.

Example: I

- Alice and Bob are in labs with different orientations in space, related by $g \in SO(3)$.
  They share the entangled state $\sum_i |i\rangle \otimes |i\rangle$.
- There exists finite $G \subset SO(3)$ such that $g \in G$.
  This subgroup and its action are known by both parties.

Example: I

- Alice and Bob are in labs with different orientations in space, related by $g \in SO(3)$.
  They share the entangled state $\sum_i |i\rangle \otimes |i\rangle$.
- There exists finite $G \subset SO(3)$ such that $g \in G$.
  This subgroup and its action are known by both parties.
- Their task: perform teleportation of a quantum state without revealing their orientation.

Example: I

- Alice and Bob are in labs with different orientations in space, related by $g \in SO(3)$.
  They share the entangled state $\sum_i |i\rangle \otimes |i\rangle$.
- There exists finite $G \subset SO(3)$ such that $g \in G$.
  This subgroup and its action are known by both parties.
- Their task: perform teleportation of a quantum state without revealing their orientation.

Example: II

- Take $G = \mathbb{Z}^2$, where the nontrivial element $a \in G$ acts as

$$\pi(a) = \begin{pmatrix} \sqrt{3}/2 & 1/2 \\ 1/2 & -\sqrt{3}/2 \end{pmatrix}.$$

Example: II

- Take $G = \mathbb{Z}^2$, where the nontrivial element $a \in G$ acts as

$$\pi(a) = \begin{pmatrix} \sqrt{3}/2 & 1/2 \\ 1/2 & -\sqrt{3}/2 \end{pmatrix}.$$

- They agree to use the following UEB:

$$U_0 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \qquad U_2 = \frac{1}{4} \begin{pmatrix} -\sqrt{2} - \sqrt{6} & -\sqrt{2} + \sqrt{6} \\ -\sqrt{2} + \sqrt{6} & \sqrt{2} + \sqrt{6} \end{pmatrix}$$

$$U_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \qquad U_3 = \frac{1}{4} \begin{pmatrix} \sqrt{2} - \sqrt{6} & -\sqrt{2} - \sqrt{6} \\ -\sqrt{2} - \sqrt{6} & -\sqrt{2} + \sqrt{6} \end{pmatrix}$$

Example: III - failure of speakable communication

- Suppose Alice communicates the measurement result to Bob as speakable information. There are two cases.

Example: III - failure of speakable communication

- Suppose Alice communicates the measurement result to Bob as speakable information. There are two cases.
- If Bob's RF is correctly aligned with Alice's, the procedure will be successful.

Example: III - failure of speakable communication

- Suppose Alice communicates the measurement result to Bob as speakable information. There are two cases.
- If Bob's RF is correctly aligned with Alice's, the procedure will be successful.
- If Bob's RF is upside-down wrt Alice's, teleportation fails.

Example: III - failure of speakable communication

- Suppose Alice communicates the measurement result to Bob as speakable information. There are two cases.
- If Bob's RF is correctly aligned with Alice's, the procedure will be successful.
- If Bob's RF is upside-down wrt Alice's, teleportation fails.
  - Alice's perspective: Bob's correction was *not* U_i^T but rather $\pi(a)^\dagger U_i^T \pi(a)$.

Example: III - failure of speakable communication

- Suppose Alice communicates the measurement result to Bob as speakable information. There are two cases.
- If Bob's RF is correctly aligned with Alice's, the procedure will be successful.
- If Bob's RF is upside-down wrt Alice's, teleportation fails.
  - Alice's perspective: Bob's correction was *not* U_i^T but rather $\pi(a)^\dagger U_i^T \pi(a)$.
  - Bob's perspective: the measurement result i Alice communicated did not correspond to the state $(\mathbb{1} \otimes \pi(a)) |\phi_i\rangle$ she measured.

The failure of speakable communication: a theorem

Theorem (VV)

If Alice sends her measurement result to Bob as speakable information, the procedure only succeeds for all RF alignments when G acts by a global phase.

The failure of speakable communication: a theorem

Theorem (VV)

If Alice sends her measurement result to Bob as speakable information, the procedure only succeeds for all RF alignments when G acts by a global phase.

Proof.

- Teleportation is possible if and only if $\pi(g)^\dagger U_i^T \pi(g) = U_i^T$ for all i and $g \in G$.

The failure of speakable communication: a theorem

Theorem (VV)

If Alice sends her measurement result to Bob as speakable information, the procedure only succeeds for all RF alignments when G acts by a global phase.

Proof.

- Teleportation is possible if and only if $\pi(g)^\dagger U_i^T \pi(g) = U_i^T$ for all i and $g \in G$.
- If the G-action is trivial on a basis of $End(H)$, it must be trivial on $End(H)$. So $H \otimes H^* \simeq d^2 \cdot \mathbb{1}$.

The failure of speakable communication: a theorem

Theorem (VV)

If Alice sends her measurement result to Bob as speakable information, the procedure only succeeds for all RF alignments when G acts by a global phase.

Proof.

- Teleportation is possible if and only if $\pi(g)^\dagger U_i^T \pi(g) = U_i^T$ for all i and $g \in G$.
- If the G-action is trivial on a basis of $End(H)$, it must be trivial on $End(H)$. So $H \otimes H^* \simeq d^2 \cdot \mathbb{1}$.
- Therefore all irreducible factors of H are identical and 1D.

□

Example: IV - unspeakable communication

- We now present the solution. Alice communicates her measurement result by sending two *arrows* to Bob.

Example: IV - unspeakable communication

- We now present the solution. Alice communicates her measurement result by sending two *arrows* to Bob.
- Her reference direction is $\uparrow$. She uses the following encoding:

$$0 \mapsto \{\uparrow\uparrow\} \qquad 1 \mapsto \{\downarrow\downarrow\} \qquad 2 \mapsto \{\uparrow\downarrow\} \qquad 3 \mapsto \{\downarrow\uparrow\}$$

Bob knows the encoding and infers the measurement result using his own reference direction.

Example: IV - unspeakable communication

- We now present the solution. Alice communicates her measurement result by sending two *arrows* to Bob.
- Her reference direction is $\uparrow$. She uses the following encoding:

$$0 \mapsto \{\uparrow\uparrow\} \qquad 1 \mapsto \{\downarrow\downarrow\} \qquad 2 \mapsto \{\uparrow\downarrow\} \qquad 3 \mapsto \{\downarrow\uparrow\}$$

  Bob knows the encoding and infers the measurement result using his own reference direction.
- Suppose Bob's lab is aligned upside-down wrt Alice's. 0, 1, 2 or 3 will be received as 1, 0, 3 or 2 respectively.

Example: IV - unspeakable communication (cont.)

- 0, 1, 2 or 3 will be received as 1, 0, 3 or 2 respectively.

Example: IV - unspeakable communication (cont.)

- 0, 1, 2 or 3 will be received as 1, 0, 3 or 2 respectively.
- But the UEB is such that the communication error cancels with his correction error:

$$\pi(a)^\dagger U_1 \pi(a) = U_0 \qquad \pi(a)^\dagger U_3 \pi(a) = U_2$$
$$\pi(a)^\dagger U_0 \pi(a) = U_1 \qquad \pi(a)^\dagger U_2 \pi(a) = U_3$$

Example: IV - unspeakable communication (cont.)

- 0, 1, 2 or 3 will be received as 1, 0, 3 or 2 respectively.
- But the UEB is such that the communication error cancels with his correction error:

$$\pi(a)^\dagger U_1 \pi(a) = U_0 \qquad \pi(a)^\dagger U_3 \pi(a) = U_2$$
$$\pi(a)^\dagger U_0 \pi(a) = U_1 \qquad \pi(a)^\dagger U_2 \pi(a) = U_3$$

- So teleportation is successful regardless of RF alignment!

Remarks

- Two crucial elements in the successful protocol:

Remarks

- Two crucial elements in the successful protocol:
  1. $\{U_i\}$ is permuted under the conjugation action of G. We call such a UEB *G-equivariant*.

Remarks

- Two crucial elements in the successful protocol:
  1. $\{U_i\}$ is permuted under the conjugation action of G. We call such a UEB *G-equivariant*.
  2. The classical channel carried a G-action, so we could encode the measurement results to carry the inverse permutation to the UEB.

Remarks

- Two crucial elements in the successful protocol:
  1. $\{U_i\}$ is permuted under the conjugation action of G. We call such a UEB *G-equivariant*.
  2. The classical channel carried a G-action, so we could encode the measurement results to carry the inverse permutation to the UEB.
- If we can find a suitable classical channel and a G-equivariant UEB, we can perform RFI teleportation.

A classical channel always exists

- Given a G-equivariant UEB, a suitable classical channel can always be found.

A classical channel always exists

- Given a G-equivariant UEB, a suitable classical channel can always be found.
- Alice decoheres in the basis corresponding to the UEB and sends the decohered system itself to Bob.

A classical channel always exists

- Given a G-equivariant UEB, a suitable classical channel can always be found.
- Alice decoheres in the basis corresponding to the UEB and sends the decohered system itself to Bob.
- Bob then measures the system and performs the correction corresponding to his own measurement.

A classical channel always exists

- Given a G-equivariant UEB, a suitable classical channel can always be found.
- Alice decoheres in the basis corresponding to the UEB and sends the decohered system itself to Bob.
- Bob then measures the system and performs the correction corresponding to his own measurement.

Theorem (VV)

This procedure is RF–independent exactly when the UEB is G-equivariant.

Alternative channels: another example

- May be more practical to use an alternative classical channel.

Alternative channels: another example

- May be more practical to use an alternative classical channel.
- The arrows channel could be generalised to any finite $G < SO(3)$.

Alternative channels: another example

- May be more practical to use an alternative classical channel.
- The arrows channel could be generalised to any finite $G < SO(3)$.
- What about a time reference frame, $G < U(1)$?

Alternative channels: another example

- May be more practical to use an alternative classical channel.
- The arrows channel could be generalised to any finite $G < SO(3)$.
- What about a time reference frame, $G < U(1)$?
- Suppose we have some cyclic subgroup $G \simeq \mathbb{Z}_n$ of translations by $\frac{T}{n}$.

Alternative channels: another example

- May be more practical to use an alternative classical channel.
- The arrows channel could be generalised to any finite $G < SO(3)$.
- What about a time reference frame, $G < U(1)$?
- Suppose we have some cyclic subgroup $G \simeq \mathbb{Z}_n$ of translations by $\frac{T}{n}$.
- Signals sent by Alice to Bob which arrive, according to her, at time $\frac{m_A T}{n}$, arrive for Bob at a different time $\frac{m_B T}{n}$.

Alternative channels: another example

- May be more practical to use an alternative classical channel.
- The arrows channel could be generalised to any finite $G < SO(3)$.
- What about a time reference frame, $G < U(1)$?
- Suppose we have some cyclic subgroup $G \simeq \mathbb{Z}_n$ of translations by $\frac{T}{n}$.
- Signals sent by Alice to Bob which arrive, according to her, at time $\frac{m_A T}{n}$, arrive for Bob at a different time $\frac{m_B T}{n}$.
- Alice can encode her measurement result in the time of arrival of signals.

Finding G-equivariant UEBs

- We cannot hope for a general classification of G-equivariant UEBs. (Not even when the G-action is trivial!)

Finding G-equivariant UEBs

- We cannot hope for a general classification of G-equivariant UEBs. (Not even when the G-action is trivial!)
- We provide a method for showing non-existence.

Finding G-equivariant UEBs

- We cannot hope for a general classification of G-equivariant UEBs. (Not even when the G-action is trivial!)
- We provide a method for showing non-existence.
- We provide methods for constructing them when they do.

G-equivariant orthonormal bases

- A *G-equivariant orthonormal basis* for H is an orthonormal basis of H whose elements are permuted by the action of G.

G-equivariant orthonormal bases

- A *G-equivariant orthonormal basis* for H is an orthonormal basis of H whose elements are permuted by the action of G.
- Every G-equivariant UEB is a G-equivariant orthonormal basis (of $End(H) \simeq H \otimes H^*$).

G-equivariant orthonormal bases

- A *G-equivariant orthonormal basis* for H is an orthonormal basis of H whose elements are permuted by the action of G.
- Every G-equivariant UEB is a G-equivariant orthonormal basis (of $End(H) \simeq H \otimes H^*$).
- G-equivariant orthonormal bases can be easily classified!

Classification of *G*-equivariant orthonormal bases

- There is a functor $\mathcal{M}$:G$-$*Set* $\rightarrow$ $\mathbf{Rep}(G)$.

Classification of *G*-equivariant orthonormal bases

- There is a functor $\mathcal{M}$:G$-$*Set* $\rightarrow$ **Rep(**G**)**.
- It takes a G-set to the free Hilbert space on its elements, extending the G-action linearly.

Classification of G-equivariant orthonormal bases

- There is a functor $\mathcal{M}$:G$-$*Set* $\to$ $\mathbf{Rep}(G)$.
- It takes a G-set to the free Hilbert space on its elements, extending the G-action linearly.
- G-equivariant orthonormal bases exist only on representations in $Im(\mathcal{M})$.

Classification of G-equivariant orthonormal bases

- There is a functor $\mathcal{M}$:G$-$*Set* $\to$ $\mathbf{Rep}(G)$.
- It takes a G-set to the free Hilbert space on its elements, extending the G-action linearly.
- G-equivariant orthonormal bases exist only on representations in $Im(\mathcal{M})$.
- Every G-set is a disjoint union of coset spaces G/H.
  Two coset spaces are isomorphic
  $\iff$ they correspond to conjugate subgroups.

Classification of G-equivariant orthonormal bases

- There is a functor $\mathcal{M}$:G$-$*Set* $\to$ $\mathbf{Rep}(G)$.
- It takes a G-set to the free Hilbert space on its elements, extending the G-action linearly.
- G-equivariant orthonormal bases exist only on representations in $Im(\mathcal{M})$.
- Every G-set is a disjoint union of coset spaces G/H.
  Two coset spaces are isomorphic
  $\iff$ they correspond to conjugate subgroups.
- $\mathcal{M}$ is additive ($\sqcup \to \oplus$).

Classification of G-equivariant orthonormal bases

- There is a functor $\mathcal{M}$:G$-$*Set* $\rightarrow$ **Rep(G)**.
- It takes a G-set to the free Hilbert space on its elements, extending the G-action linearly.
- G-equivariant orthonormal bases exist only on representations in $Im(\mathcal{M})$.
- Every G-set is a disjoint union of coset spaces G/H.
  Two coset spaces are isomorphic
  $\iff$ they correspond to conjugate subgroups.
- $\mathcal{M}$ is additive ($\sqcup \rightarrow \oplus$).
- So in order to classify all objects in $Im(\mathcal{M})$, it is sufficient to find the images of the coset spaces G/H under $\mathcal{M}$ - the basic permutation representations.

A representation on which no G-equivariant UEBs exist

Theorem (VV)

There is no G-equivariant UEB for the 2-dimensional irreducible representation V of S_3.

A representation on which no G-equivariant UEBs exist

Theorem (VV)

There is no G-equivariant UEB for the 2-dimensional irreducible representation V of S_3.

Proof.

Use characters to show that the representation $V \otimes V^*$ cannot be decomposed into basic permutation representations. □

A representation on which no G-equivariant UEBs exist

Theorem (VV)

There is no G-equivariant UEB for the 2-dimensional irreducible representation V of S_3.

Proof.

Use characters to show that the representation $V \otimes V^*$ cannot be decomposed into basic permutation representations. □

- This does not work for all irreps! (2D irrep of D_8.)

Constructing G-equivariant UEBs

- Sufficient condition to find a G-equivariant UEB for V:
  1. A G-equivariant orthonormal basis of V.

Constructing G-equivariant UEBs

- Sufficient condition to find a G-equivariant UEB for V:
  1. A G-equivariant orthonormal basis of V.
  2. A Hadamard matrix that commutes with all $\pi(g)$ expressed in that basis.

Constructing G-equivariant UEBs

- Sufficient condition to find a G-equivariant UEB for V:
  1. A G-equivariant orthonormal basis of V.
  2. A Hadamard matrix that commutes with all $\pi(g)$ expressed in that basis.

Theorem (VV)

Let $|v_i\rangle$ be the G-equivariant orthonormal basis, and H be the Hadamard matrix. Then the G-equivariant UEB is:

$$(U_H)_{ij} = \frac{1}{N} H \circ diag(H, j)^{\dagger} \circ H^{\dagger} \circ diag(H^T, i) \qquad (1)$$

A sufficient condition for dim < 5

Theorem (VV)

Suppose H admits a G-equivariant orthonormal basis, and has dimension $d < 5$. Then we can find G-equivariant UEB for H.

A sufficient condition for dim < 5

Theorem (VV)

Suppose H admits a G-equivariant orthonormal basis, and has dimension $d < 5$. Then we can find G-equivariant UEB for H.

Proof.

- Dimensions 1 and 2 can be proved immediately.

A sufficient condition for dim < 5

Theorem (VV)

Suppose H admits a G-equivariant orthonormal basis, and has dimension $d < 5$. Then we can find G-equivariant UEB for H.

Proof.

- Dimensions 1 and 2 can be proved immediately.
- For dimensions 3 and 4, we need H commuting with all $\pi(g)$ in the G-equivariant orthonormal basis.

A sufficient condition for dim < 5

Theorem (VV)

Suppose H admits a G-equivariant orthonormal basis, and has dimension $d < 5$. Then we can find G-equivariant UEB for H.

Proof.

- Dimensions 1 and 2 can be proved immediately.
- For dimensions 3 and 4, we need H commuting with all $\pi(g)$ in the G-equivariant orthonormal basis.
- $\pi(G) < S_d$ so the worst case is $\pi(G) = S_d$.

A sufficient condition for dim < 5

Theorem (VV)

Suppose H admits a G-equivariant orthonormal basis, and has dimension $d < 5$. Then we can find G-equivariant UEB for H.

Proof.

- Dimensions 1 and 2 can be proved immediately.
- For dimensions 3 and 4, we need H commuting with all $\pi(g)$ in the G-equivariant orthonormal basis.
- $\pi(G) < S_d$ so the worst case is $\pi(G) = S_d$.
- Any $M < C(S_d)$ has identical entries on the diagonal and identical entries everywhere else.

A sufficient condition for dim < 5 (cont.)

Proof (Cont.)

Unitarity of such a matrix is equivalent to

$$|b|^2 = \frac{1 - |a|^2}{d - 1} \tag{2}$$

$$\Re(a^* b) = \frac{2 - d}{2} |b|^2. \tag{3}$$

These equations can be satisfied for $|a|, |b| = \frac{1}{\sqrt{d}}$ iff $d < 5$. □

Teleportation in CQM

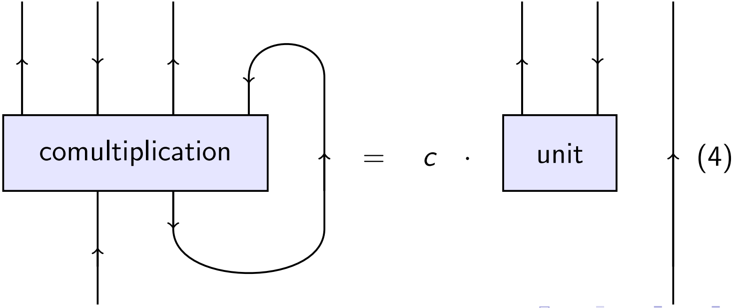
- In CQM we consider QI concepts in terms of their algebraic structure.

Teleportation in CQM

- In CQM we consider QI concepts in terms of their algebraic structure.
- Classical structures corrrespond to orthonormal bases.

Teleportation in CQM

- In CQM we consider QI concepts in terms of their algebraic structure.
- Classical structures corrrespond to orthonormal bases.
- In a dagger-compact category, a *quantum teleportation procedure* is a classical structure on $A \otimes A^*$ satisfying:



Teleportation in **Rep**(G)

- In **FHilb** these are exactly the unitary error bases.

Teleportation in **Rep**(G)

- In **FHilb** these are exactly the unitary error bases.
- In **Rel** these correspond to one-time pads.

Teleportation in **Rep**(G)

- In **FHilb** these are exactly the unitary error bases.
- In **Rel** these correspond to one-time pads.
- **Rep**(G) has obects unitary representations and morphisms intertwiners.

Teleportation in **Rep**(G)

- In **FHilb** these are exactly the unitary error bases.
- In **Rel** these correspond to one-time pads.
- **Rep**(G) has obects unitary representations and morphisms intertwiners.
- In **Rep**(G) these are exactly the G-equivariant unitary error bases.

Teleportation in **Rep**(G)

- In **FHilb** these are exactly the unitary error bases.
- In **Rel** these correspond to one-time pads.
- **Rep**(G) has obects unitary representations and morphisms intertwiners.
- In **Rep**(G) these are exactly the G-equivariant unitary error bases.
- All categorical constructions of UEBs carry over to **Rep**(G).

Teleportation in Rep(G)

- In **FHilb** these are exactly the unitary error bases.
- In **Rel** these correspond to one-time pads.
- **Rep**(G) has obects unitary representations and morphisms intertwiners.
- In **Rep**(G) these are exactly the G-equivariant unitary error bases.
- All categorical constructions of UEBs carry over to **Rep(**G**)**.
- Unclear how to generalise non-categorical constructions to the G-equivariant setting.

Future work

- Constructing G-equivariant UEBs.

Future work

- Constructing G-equivariant UEBs.
- Applications to cryptography.

Future work

- Constructing G-equivariant UEBs.
- Applications to cryptography.
- Infinite limits of RFI protocols.

Future work

- Constructing G-equivariant UEBs.
- Applications to cryptography.
- Infinite limits of RFI protocols.
- Teleportation of anyons.

Chiribella, G., Giovannetti, V., Maccone, L., and Perinotti, P. (2012).
Teleportation transfers only speakable quantum information.
Phys. Rev. A, 86:010304.

Enk, S. J. V. (2001).
The physical meaning of phase and its importance for quantum teleportation.
Journal of Modern Optics, 48(13):2049–2054.

Kitaev, A., Mayers, D., and Preskill, J. (2004).
Superselection rules and quantum protocols.
Phys. Rev. A, 69:052326.

Marzolino, U. and Buchleitner, A. (2015).
Quantum teleportation with identical particles.
Phys. Rev. A, 91:032316.