Quantum Protocols within Spekkens’ Toy Model

Leonardo Disilvestro, Damian Markham

Paris Center for Quantum Computing (Telecom ParisTech), Paris

QPL, Glasgow

June 8, 2016
Contextuality and non-locality are ubiquitous in quantum theory

We study quantum protocols within Spekkens’ toy model\(^1\) — a **classical**, **realist**, and **local** theory phenomenologically very close to quantum theory

---

Contextuality and non-locality are ubiquitous in quantum theory.

We study quantum protocols within Spekkens' toy model\(^1\) — a **classical**, **realist**, and **local** theory phenomenologically very close to quantum theory.

---

A few remarks on the toy model

**States**

- Underlying states $\rightarrow$ **Ontic** ($= \text{of reality/existence}$) --- (i.e. the LHV)
- Observable states $\rightarrow$ **Epistemic** ($= \text{of knowledge}$)
- Epistemic restriction: ‘Knowledge Balance Principle’ (KBP)
- KBP $\Rightarrow$ uniform distributions over the ontic states

---

A few remarks on the toy model

**States**
- Underlying states $\rightarrow$ **Ontic** ($=$ of reality/existence) — *(i.e. the LHV)*
- Observable states $\rightarrow$ **Epistemic** ($=$ of knowledge)
- Epistemic restriction: ‘Knowledge Balance Principle’ (KBP)
- KBP $\Rightarrow$ uniform distributions over the ontic states

**Stabilizer structure**
- Qubit stabilizer $\approx$ Toy stabilizer
- Difference between quantum and toy well understood
- However stabilizer formalism generalize the protocol more straightforwardly
- Toy model is local but steerable
- Computationally very weak model, i.e. $\oplus L$ (Gottesman-Knill)

---

Summary of our results

Stabilizer nature of the toy model

- Error correction & secret sharing
- Toy blind and verified
- Measurement based toy computation
- Encoding information
- No-bit commitment
Toy stabilizer notation [Pusey ‘12]\(^3\)

For a single system define a group composed by

\[
G_1 = \left\{ \mathcal{I} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \mathcal{X} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \mathcal{Z} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \mathcal{Y} = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \right\}
\]

\(^3\)M. Pusey, Found. Phys. 42, 688 (2012)
Toy stabilizer notation [Pusey ‘12]$^3$

For a single system define a group composed by

$$G_1 = \left\{ \mathcal{I} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \mathcal{X} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \mathcal{Z} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \mathcal{Y} = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \right\}$$

Analogously to quantum, all states over $n$ toy systems are described by

the stabilizer group $S = \{s_1, \ldots, s_{|S|}\} = \langle g_1, \ldots, g_l \rangle$,

$S$ identifies a diagonal matrix

$$\rho_S = \frac{1}{4^n} \prod_{g \in \text{Gen}(S)} (\mathcal{I} + g)$$

where the elements of $\rho_S$ are probabilities of each ontic state

Toy state evolution

1. **Reversible transformations** [Pusey'12]: $4^n \times 4^n$ permutation matrices $\tilde{U}$ over ontic states

\[ \rho'_S = \tilde{U} \rho_S \tilde{U}^T, \]
Toy state evolution

1. **Reversible transformations** [Pusey’12]: $4^n \times 4^n$ permutation matrices $\tilde{U}$ over ontic states
   \[ \rho'_S = \tilde{U}\rho_S\tilde{U}^T, \]

2. **Measurements** [Pusey’12]: given a toy state $\rho_S$
   \[ M = \sum_i \alpha_i P_{T_i}, \text{ where } \sum_i P_{T_i} = I^n \]
   Probability outcome $\alpha_i$:
   \[ \text{prob}(\alpha_i) = Tr(P_{T_i}\rho_s), \]
   Resulting state:
   \[ \rho'_S = \langle T_i, \{ \text{generators of } S \text{ compatible with } T_i \} > \]
Toy state evolution

1. **Reversible transformations** [Pusey’12]: $4^n \times 4^n$ permutation matrices $\tilde{U}$ over ontic states

$$\rho_S' = \tilde{U} \rho_S \tilde{U}^T,$$

2. **Measurements** [Pusey’12]: given a toy state $\rho_S$

Measurement: $M = \sum_i \alpha_i P_{T_i}$, where $\sum_i P_{T_i} = I^n$

Probability outcome $\alpha_i$: $\text{prob}(\alpha_i) = \text{Tr}(P_{T_i} \rho_s)$,

Resulting state: $\rho_S' = <T_i, \{\text{generators of } S \text{ compatible with } T_i\}>$

3. **Generalized Transformation** : ‘Toy CPTP’

  Global permutation: $\sigma_{S}^{AR} = \tilde{U}^{AR}(\rho^A \otimes \sigma^R) \tilde{U}^{AR T}$

  Ancilla Measurement: $M = \sum_i q_i I^A \otimes P_{T_i}^R$

  Ensemble: $\{\text{prob}(q_i), \chi_{S'_i}^A = \text{Tr}_R(\chi_{S'_i}^{AR})\}, \}$
Toy stabilizers vs quantum stabilizers

Toy states ↔ quantum states

\[ S^Q = \{XX, ZZ, -YY, II\} \not\leftrightarrow S^T = \{XX, ZZ, -YY, II\} \] not a toy state

(quantum-ly \( XZ = -iY \), while toy-ly \( XZ = Y \))
Toy stabilizers vs quantum stabilizers

- $S^Q = \{XX, ZZ, -YY, II\} \not\leftrightarrow S^T = \{XX, ZZ, -YY, II\}$ not a toy state
  
  (quantum-ly $XZ = -iY$, while toy-ly $XZ = Y$)

- However, we can use the generators:

  $S^Q = \{XX, ZZ, -YY, II\}$ is generated by

  \[
  \begin{cases}
  G_1^Q = \langle XX, ZZ \rangle, \\
  G_2^Q = \langle XX, -YY \rangle, \\
  G_3^Q = \langle ZZ, -YY \rangle,
  \end{cases}
  \]
Toy stabilizers vs quantum stabilizers

Toy states $\leftrightarrow$ quantum states

- $S^Q = \{XX, ZZ, -YY, II\} \nleftrightarrow S^T = \{XX, ZZ, -YY, II\}$ not a toy state
  
  (quantum-ly $XZ = -iY$, while toy-ly $XZ = Y$)

- However, we can use the generators:

  $$S^Q = \{XX, ZZ, -YY, II\} \text{ is generated by } \begin{cases} 
  G^Q_1 = \langle XX, ZZ \rangle, \\
  G^Q_2 = \langle XX, -YY \rangle, \\
  G^Q_3 = \langle ZZ, -YY \rangle, 
\end{cases}$$

- implying

  $$G^Q_1 \rightarrow G^T_1 = \{XX, ZZ\} \text{ generates } S^T_1 = \{XX, ZZ, YY, II\},$$
  $$G^Q_2 \rightarrow G^T_2 = \{XX, -YY\} \text{ generates } S^T_2 = \{XX, -ZZ, -YY, II\},$$
  $$G^Q_3 \rightarrow G^T_3 = \{ZZ, -YY\} \text{ generates } S^T_3 = \{-XX, ZZ, -YY, II\},$$
Toy stabilizers vs quantum stabilizers

\[ S^Q = \{XX, ZZ, -YY, II\} \not\rightarrow S^T = \{XX, ZZ, -YY, II\} \text{ not a toy state} \]

\( \text{quantum-ly } XZ = -iY, \text{ while toy-ly } XZ = Y \)

However, we can use the generators:

\[ S^Q = \{XX, ZZ, -YY, II\} \text{ is generated by} \]

\[ \begin{align*}
G^Q_1 &= \langle XX, ZZ \rangle, \\
G^Q_2 &= \langle XX, -YY \rangle, \\
G^Q_3 &= \langle ZZ, -YY \rangle,
\end{align*} \]

implying

\[ G^Q_1 \rightarrow G^T_1 = \{XX, ZZ\} \text{ generates } S^T_1 = \{XX, ZZ, YY, II\} \]
\[ G^Q_2 \rightarrow G^T_2 = \{XX, -YY\} \text{ generates } S^T_2 = \{XX, -ZZ, -YY, II\}, \]
\[ G^Q_3 \rightarrow G^T_3 = \{ZZ, -YY\} \text{ generates } S^T_3 = \{-XX, ZZ, -YY, II\}, \]

Note quantum-ly \([X, Z] = 0\), while toy-ly \([X, \tilde{Z}] = 0 = [\tilde{X}, Z] \)
Translation criteria

**Existence of a quantum stabilizer protocol** ➞ **Toy protocol with equivalent properties**

\[ Equivalent \equiv \text{preserves some key figure of merit} \]

**Difficulties:**

1. Criteria fails when quantum protocol is non-local (e.g. Mermin square)
2. Ambiguity due to different group structure
   
   i.e. quantum: \[ XZ = -iY \]
   
   toy: \[ xz = y \]

   Need a way to ensure consistency
Toy purifications

Proof sketch:

Idea: use the stabilizer nature of the toy model

Mixed state \( \rho_T^A \) \( \rightarrow \) Purification \( \rho_T^{AR} \), s.t. \( \text{Tr}_R(\rho_T^{AR}) = \rho_T^A \)
Toy purifications

Proof sketch:

Idea: use the stabilizer nature of the toy model

Mixed state

\[ \rho_T^A \] 

\[ ? \]

\[ \rho_T^{AR} , \text{s.t. } Tr_R(\rho_T^{AR}) = \rho_T^A \]

Purification

\[ \rho_Q^A \]

\[ Tr_R \]

\[ \rho_Q^{AR} \]
Toy purifications

Proof sketch:

Idea: use the stabilizer nature of the toy model

Mixed state

\[ \rho_T^A \xrightarrow{\text{Tr}_R} \rho_T^{AR}, \text{s.t. } \text{Tr}_R(\rho_T^{AR}) = \rho_T^A \]

Purification

\[ \rho_Q^A \xleftarrow{\text{Tr}_R} \rho_Q^{AR} \]

Toy-Quantum ambiguity is pushed where it doesn’t matter
Toy purifications

Proof sketch:

Idea: use the stabilizer nature of the toy model

Mixed state

\[ \rho_T^A \leftrightarrow \text{Tr}_R \rightarrow \rho_T^{AR} \text{, s.t. } \text{Tr}_R(\rho_T^{AR}) = \rho_T^A \]

Purification

\[ \rho_Q^A \leftrightarrow \text{Tr}_R \rightarrow \rho_Q^{AR} \]

note \( \forall s = s^A \otimes s^R \in S_Q^{AR} \)

\[ \text{Tr}_R(s^A \otimes s^R) = \begin{cases} 0 & \text{if } s^R \neq I^R, \\ s^A & \text{if } s^R = I^R. \end{cases} \]
Toy purifications

Proof sketch:

Idea: use the stabilizer nature of the toy model

Mixed state

\[ \rho_T^A \xleftarrow{\text{Tr}_R} \rho_T^{AR} \text{, s.t. } \text{Tr}_R(\rho_T^{AR}) = \rho_T^A \]

\[ \rho_Q^A \xleftarrow{\text{Tr}_R} \rho_Q^{AR} \]

Purification

\[ G_T^A \xleftarrow{\text{Tr}_R} G_T^{AR} = \langle \{ G_T^A \}, \cdots \rangle \]

\[ G_Q^A \xleftarrow{\text{Tr}_R} G_Q^{AR} = \langle \{ G_Q^A \}, \cdots \rangle \]

\text{note } \forall \ s = s^A \otimes s^R \in S_Q^{AR}

\[ \text{Tr}_R(s^A \otimes s^R) = \begin{cases} 0 & \text{if } s^R \neq I^R, \\ s^A & \text{if } s^R = I^R. \end{cases} \]
Toy purifications

**Proof sketch:**

Idea: use the stabilizer nature of the toy model

**Mixed state**

\[
\rho_T^A \xrightarrow{\text{Tr}_R} \rho_T^{AR}, \text{s.t. } \text{Tr}_R(\rho_T^{AR}) = \rho_T^A
\]

\[
\rho_Q^A \xrightarrow{\text{Tr}_R} \rho_Q^{AR}
\]

**Purification**

\[
G_T^A \xleftarrow{\text{Tr}_R} G_T^{AR} = \langle \{ G_T^A \}, \cdots >
\]

\[
G_Q^A \xleftarrow{\text{Tr}_R} G_Q^{AR} = \langle \{ G_Q^A \}, \cdots >
\]

**Note**

\[
\forall s = s^A \otimes s^R \in S_Q^{AR}
\]

\[
\text{Tr}_R(s^A \otimes s^R) = \begin{cases} 
0 & \text{if } s^R \neq \mathcal{I}^R, \\
\rho_Q^A & \text{if } s^R = \mathcal{I}^R.
\end{cases}
\]

Toy-Quantum ambiguity is pushed where it doesn't matter
Purifications & no-bit commitment

Thm.1: Existence of toy purifications

Thm.2: Local equivalence:

\[ \sigma_{AR} = (\tilde{A} \otimes \tilde{U}_R) \rho_{AR} (\tilde{A} \otimes \tilde{U}_R)^T \]

Imply

- No-go theorem for perfect and imperfect toy bit commitment

Proof: exactly as in the quantum case!
Error correction

- We show $\forall [n, k, d]^Q \rightarrow [n, k, d]^\text{toy}$, with same correcting properties
- Any toy $[2k1, 1, k]^\text{toy}$ E.C. code is equivalent to a $(k, 2k1)$ secret sharing code

Key remarks

- Cloning is impossible in the toy model
- Information is spread through the resource
- Syndrome/errors is recovered through permutations/stabilizer interplay
- Choice of generators
Blind and verified computation (i)

1. (Blindness) Bob gains no info about the computation he performs
2. (Verified) Bob's cheats or deviations from the agreed instruction are discovered with high probability

---

Blind and verified computation (i)

1. **(Blindness)** Bob gains no info about the computation he performs
2. **(Verified)** Bob's cheats or deviations from the agreed instruction are discovered with high probability

**Big open question:** can quantum computation be verified classically...?

**Our question:** are contextual resources needed?

- [RUV]$^4$ explicitly uses Bell’s tests
- [FK]$^5$
  1. graph states [toy version, Pusey ’12]
  2. measurement based quantum computation
  3. trapification & randomness

---


Blind and verified computation (ii)

Outline

- Client weaker than server (no ‘toy entanglement’ and bounded computational power)
- Slight extension of the toy model to allow for classical control
  - Needed to define the protocol
  - Not a key issue
  - Gaussian motivated
- Probability accepting an incorrect computation $p_{\text{fail}} < 1 - \frac{1}{2n}$

What does it imply?

- Suggest that structure of FK is Bell-local
- Therefore steering correlations should be enough
Blind and verified computation (ii)

Outline

- Client weaker than server (no ‘toy entanglement’ and bounded computational power)
- Slight extension of the toy model to allow for classical control
  - Needed to define the protocol
  - Not a key issue
  - Gaussian motivated
- Probability accepting an incorrect computation $p_{\text{fail}} < 1 - \frac{1}{2^n}$

What does it imply?

- Suggest that structure of FK is Bell-local
- Therefore steering correlations should be enough

Recent work\(^2\) provides a FK version based on steering

\(^2\)A. Cheorghiu, P. Wallden and E. Kashefi, Rigidity of quantum steering and one-sided device independent verifiable quantum computation, arXiv:1512.04401
Considerations

Our contribution

- A framework where toy protocols can be analyzed
- Despite classical and no-cloning $\rightarrow$ error correction
- Properties of the encoding $\rightarrow$ no bit commitment, secret sharing
- Despite locality $\rightarrow$ can perform toy blind and verified

Perspective

- Define a Gaussian blind and verified protocol
- Provide a generalized translation criteria

Take home message

- Toy stabilizer protocols are non-trivial
- Steering correlations suffice for many interesting protocols
Considerations

Our contribution

- A framework where toy protocols can be analyzed
- Despite classical and no-cloning $\rightarrow$ error correction
- Properties of the encoding $\rightarrow$ no bit commitment, secret sharing
- Despite locality $\rightarrow$ can perform toy blind and verified

Perspective

- Define a Gaussian blind and verified protocol
- Provide a generalized translation criteria

Take home message

- Toy stabilizer protocols are non-trivial
- Steering correlations suffice for many interesting protocols

Thank you for listening!