Quantum Protocols within Spekkens' Toy Model

Leonardo Disilvestro, Damian Markham

Paris Center for Quantum Computing (Telecom ParisTech), Paris

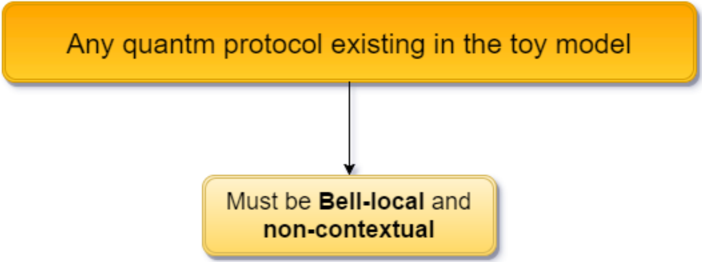
QPL, Glasgow

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

[1] R. W. Spekkens, Phys. Rev. A, 75, 032110 (2007)

- 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



[1] R. W. Spekkens, Phys. Rev. A, 75, 032110 (2007)

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

[2] B. Coecke, B. Edwards, R. Spekkens, *Phase groups and the origin of non-locality for qubits (2011)*

A few remarks on the toy model

States

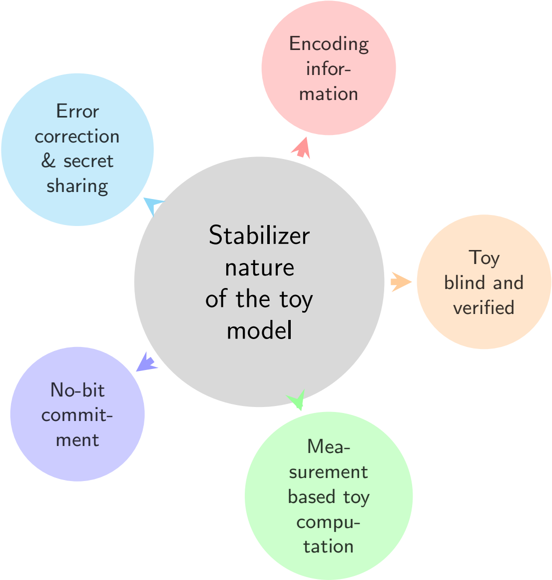
- Underlying states $\rightarrow$ *Ontic (= of reality/existence)* — (*i.e. the LHV*)
- Observable states $\rightarrow$ *Epistemic (= of knowledge)*
- Epistemic restriction: 'Knowledge Balance Principle' (KBP)
- KBP $\Rightarrow$ uniform distributions over the ontic states

Stabilizer structure

- Qubit stabilizer $\approx$ Toy stabilizer
- Difference between quantum and toy well understood[2]
- However stabilizer formalism generalize the protocol more straightforwardly
- Toy model is local but steerable
- Computationally very weak model, i.e. $\oplus L$ (Gottesman-Knill)

[2] B. Coecke, B. Edwards, R. Spekkens, *Phase groups and the origin of non-locality for qubits (2011)*

Summary of our results



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

$$\text{the stabilizer group } S = \{s_1, \ldots, s_{|S|}\} = \overbrace{< g_1, \ldots, g_l >}^{\textit{Generators}},$$

S identifies a *diagonal* matrix

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

where the elements of ρ_S are *probabilities* of each ontic state

[3] M. Pusey, Found. Phys. 42, 688 (2012)

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 ρ_S

$$\textit{Measurement}: \quad M = \sum_i \alpha_i P_{T_i}, \ \textit{where} \sum_i P_{T_i} = \mathcal{I}^n$$
$$\textit{Probability outcome } \alpha_i: \quad \textit{prob}(\alpha_i) = \textit{Tr}(P_{T_i} \rho_s),$$
$$\textit{Resulting state}: \quad \rho_{S'} = < T_i, \{\textit{generators of } S \textit{ compatible with } T_i\} >$$

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 ρ_S

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

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

$$\textit{Resulting state}: \quad \rho_{S'} =< T_i, \{\textit{generators of } S \textit{ compatible with } T_i\} >$$

3. **Generalized Transformation** : 'Toy CPTP'

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

$$\textit{Ancilla Measurement} \ : \quad M = \sum_i q_i I^A \otimes P^R_{T_i}$$

$$\textit{Ensamble}: \quad \{\textit{prob}(q_i), \ \chi^A_{S''_i} = Tr_R(\chi^{AR}_{S'_i})\}, \}$$

Toy stabilizers vs quantum stabilizers

$$\boxed{\text{toy states} \not\longleftrightarrow \text{quantum states}}$$

- $S^Q = \{XX, ZZ, -YY, II\} \not\rightarrow S^T = \{\mathcal{X}\mathcal{X}, \mathcal{Z}\mathcal{Z}, -\mathcal{Y}\mathcal{Y}, \mathcal{I}\mathcal{I}\}$ not a toy state

  (quantum-ly $XZ = -iY$, while toy-ly $\mathcal{X}\mathcal{Z} = \mathcal{Y}$)

Toy stabilizers vs quantum stabilizers

$$\boxed{\text{toy states} \not\leftrightarrow \text{quantum states}}$$

- $S^Q = \{XX, ZZ, -YY, II\} \not\to S^T = \{\mathcal{X}\mathcal{X}, \mathcal{Z}\mathcal{Z}, -\mathcal{Y}\mathcal{Y}, \mathcal{I}\mathcal{I}\}$ not a toy state
  (quantum-ly $XZ = -iY$, while toy-ly $\mathcal{X}\mathcal{Z} = \mathcal{Y}$)
- However, we can use the generators:

$$S^Q = \{XX, ZZ, -YY, II\} \text{ is generated by } \begin{cases} G_1^Q = < XX, ZZ >, \\ G_2^Q = < XX, -YY >, \\ G_3^Q = < ZZ, -YY >, \end{cases}$$

Toy stabilizers vs quantum stabilizers

$$\boxed{\text{toy states} \not\leftrightarrow \text{quantum states}}$$

- $S^Q = \{XX, ZZ, -YY, II\} \not\rightarrow S^T = \{\mathcal{X}\mathcal{X}, \mathcal{Z}\mathcal{Z}, -\mathcal{Y}\mathcal{Y}, \mathcal{I}\mathcal{I}\}$ not a toy state
  (quantum-ly $XZ = -iY$, while toy-ly $\mathcal{X}\mathcal{Z} = \mathcal{Y}$)
- However, we can use the generators:

$$S^Q = \{XX, ZZ, -YY, II\} \text{ is generated by } \begin{cases} G_1^Q =< XX, ZZ >, \\ G_2^Q =< XX, -YY >, \\ G_3^Q =< ZZ, -YY >, \end{cases}$$

- implying

$$G_1^Q \rightarrow G_1^T = \{\mathcal{X}\mathcal{X}, \mathcal{Z}\mathcal{Z}\} \text{ generates } S_1^T = \{\mathcal{X}\mathcal{X}, \mathcal{Z}\mathcal{Z}, \mathcal{Y}\mathcal{Y}, \mathcal{I}\mathcal{I}\}$$
$$G_2^Q \rightarrow G_2^T = \{\mathcal{X}\mathcal{X}, -\mathcal{Y}\mathcal{Y}\} \text{ generates } S_2^T = \{\mathcal{X}\mathcal{X}, -\mathcal{Z}\mathcal{Z}, -\mathcal{Y}\mathcal{Y}, \mathcal{I}\mathcal{I}\},$$
$$G_3^Q \rightarrow G_3^T = \{\mathcal{Z}\mathcal{Z}, -\mathcal{Y}\mathcal{Y}\} \text{ generates } S_3^T = \{-\mathcal{X}\mathcal{X}, \mathcal{Z}\mathcal{Z}, -\mathcal{Y}\mathcal{Y}, \mathcal{I}\mathcal{I}\},$$

Toy stabilizers vs quantum stabilizers

$$\boxed{\text{toy states} \not\leftrightarrow \text{quantum states}}$$

- $S^Q = \{XX, ZZ, -YY, II\} \not\rightarrow S^T = \{\mathcal{X}\mathcal{X}, \mathcal{Z}\mathcal{Z}, -\mathcal{Y}\mathcal{Y}, \mathcal{I}\mathcal{I}\}$ not a toy state
  (quantum-ly $XZ = -iY$, while toy-ly $\mathcal{X}\mathcal{Z} = \mathcal{Y}$)
- However, we can use the generators:

$$S^Q = \{XX, ZZ, -YY, II\} \text{ is generated by } \begin{cases} G_1^Q =< XX, ZZ >, \\ G_2^Q =< XX, -YY >, \\ G_3^Q =< ZZ, -YY >, \end{cases}$$

- implying

$$G_1^Q \rightarrow G_1^T = \{\mathcal{X}\mathcal{X}, \mathcal{Z}\mathcal{Z}\} \text{ generates } S_1^T = \{\mathcal{X}\mathcal{X}, \mathcal{Z}\mathcal{Z}, \mathcal{Y}\mathcal{Y}, \mathcal{I}\mathcal{I}\}$$
$$G_2^Q \rightarrow G_2^T = \{\mathcal{X}\mathcal{X}, -\mathcal{Y}\mathcal{Y}\} \text{ generates } S_2^T = \{\mathcal{X}\mathcal{X}, -\mathcal{Z}\mathcal{Z}, -\mathcal{Y}\mathcal{Y}, \mathcal{I}\mathcal{I}\},$$
$$G_3^Q \rightarrow G_3^T = \{\mathcal{Z}\mathcal{Z}, -\mathcal{Y}\mathcal{Y}\} \text{ generates } S_3^T = \{-\mathcal{X}\mathcal{X}, \mathcal{Z}\mathcal{Z}, -\mathcal{Y}\mathcal{Y}, \mathcal{I}\mathcal{I}\},$$

- Note quantum-ly $[X, Z] = 0$, while toy-ly $[\mathcal{X}, \tilde{Z}] = 0 = [\tilde{X}, \mathcal{Z}]$

Translation criteria

Equivalent $\equiv$ preserves some key figure of merit

<u>Difficulties</u>:

1. Criteria fails when quantum protocol is non-local (e.g. Mermin square)
2. Ambiguity due to different group structure

   i.e. quantum: $\boxed{XZ = -iY}$, toy: $\boxed{\mathcal{X}\mathcal{Z} = \mathcal{Y}}$

$\boxed{\text{Need a way to ensure consistency}}$

Toy purifications

Proof sketch:

Idea: use the stabilizer nature of the toy model

Mixed state *Purification*

$$\rho_T^A \xleftrightarrow{\;\;?\;\;} \rho_T^{AR} \text{ , s.t. } Tr_R(\rho_T^{AR}) = \rho_T^A$$

Toy purifications

Proof sketch:

Idea: use the stabilizer nature of the toy model

Mixed state *Purification*

$$\rho_T^A \xleftrightarrow{\quad ? \quad} \rho_T^{AR} \text{ , s.t. } Tr_R(\rho_T^{AR}) = \rho_T^A$$

$$\rho_Q^A \xleftrightarrow{\quad Tr_R \quad} \rho_Q^{AR}$$

Toy purifications

Proof sketch:

Idea: use the stabilizer nature of the toy model

Mixed state *Purification*

$$
\begin{tikzcd}
\rho_T^A \arrow[d] & \arrow[l] \rho_T^{AR} \arrow[l, leftrightarrow, "Tr_R"] \\
\rho_Q^A & \rho_Q^{AR} \arrow[l, leftrightarrow, "Tr_R"] \arrow[u]
\end{tikzcd}
$$

ρ_T^{AR} , s.t. $Tr_R(\rho_T^{AR}) = \rho_T^A$

Toy purifications

Proof sketch:

Idea: use the stabilizer nature of the toy model

Mixed state *Purification*

$$
\begin{tikzcd}
\rho_T^A \arrow[r, leftrightarrow, "Tr_R"] \arrow[d] & \rho_T^{AR} \text{ , s.t. } Tr_R(\rho_T^{AR}) = \rho_T^A \\
\rho_Q^A \arrow[r, leftrightarrow, "Tr_R"] & \rho_Q^{AR} \arrow[u]
\end{tikzcd}
$$

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

$$
Tr_R(s^A \otimes s^R) = \begin{cases} 0 & \text{if } s^R \neq \mathcal{I}^R, \\ s^A & \text{if } s^R = \mathcal{I}^R. \end{cases}
$$

Toy purifications

Proof sketch:

Idea: use the stabilizer nature of the toy model

Mixed state *Purification*

$$
\begin{tikzcd}
\rho_T^A \arrow[rr, leftrightarrow, "Tr_R"] \arrow[d] & & \rho_T^{AR} \\
\rho_Q^A \arrow[rr, leftrightarrow, "Tr_R"] & & \rho_Q^{AR} \arrow[u]
\end{tikzcd}
$$

ρ_T^{AR}, s.t. $Tr_R(\rho_T^{AR}) = \rho_T^A$

$$
\begin{tikzcd}
G_T^A \arrow[r, leftrightarrow, "Tr_R"] \arrow[d] & G_T^{AR} =< \{G_T^A\}, \cdots > \\
G_Q^A \arrow[r, leftrightarrow, "Tr_R"] & G_Q^{AR} =< \{G_Q^A\}, \cdots > \arrow[u]
\end{tikzcd}
$$

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

$$
Tr_R(s^A \otimes s^R) = \begin{cases} 0 & \text{if } s^R \neq \mathcal{I}^R, \\ s^A & \text{if } s^R = \mathcal{I}^R. \end{cases}
$$

Toy purifications

Proof sketch:

Idea: use the stabilizer nature of the toy model

Mixed state *Purification*

$$\begin{array}{ccc} \rho_T^A & \xleftrightarrow{\quad Tr_R \quad} & \rho_T^{AR} \text{ , s.t. } Tr_R(\rho_T^{AR}) = \rho_T^A \\ \downarrow & & \uparrow \\ \rho_Q^A & \xleftrightarrow{\quad Tr_R \quad} & \rho_Q^{AR} \end{array}$$

$$\begin{array}{ccc} G_T^A & \xleftrightarrow{\quad Tr_R \quad} & G_T^{AR} =< \{G_T^A\}, \cdots > \\ \downarrow & & \uparrow \\ G_Q^A & \xleftrightarrow{\quad Tr_R \quad} & G_Q^{AR} =< \{G_Q^A\}, \cdots > \end{array}$$

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

$$Tr_R(s^A \otimes s^R) = \begin{cases} 0 & \text{if } s^R \neq \mathcal{I}^R, \\ s^A & \text{if } s^R = \mathcal{I}^R. \end{cases}$$

$\boxed{\text{Toy-Quantum ambiguity is pushed where it doesn't matter}}$

Purifications & no-bit commitment

Thm.1 Existence of toy purifications

Thm.2 Local equivalence:
if σ^{AR} and ρ^{AR} are purifications of ρ^{A}
then $\sigma^{AR} = (\tilde{A} \otimes \tilde{U}^{R})\rho^{AR}(\tilde{A} \otimes \tilde{U}^{R})^{T}$

Imply

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

Proof: exactly as in the quantum case!

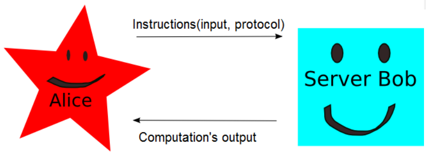
Error correction

- We show $\forall\ [n, k, d]^{Q} \longrightarrow [n, k, d]^{toy}$, with same correcting properties
- Any toy $[2k1, 1, k]^{toy}$ 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

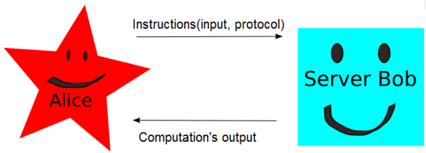
Blind and verified computation (i)



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

[4] B. Reichardt, R. Unger, U. Vazirani. Classical command of quantum systems. Nature, 2013.
[5] J. Fitzsimons, E. Kashefi. Unconditionally verifiable blind computation, arXiv:1203.5217 2012

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

[4] B. Reichardt, R. Unger, U. Vazirani. Classical command of quantum systems. Nature, 2013.
[5] J. Fitzsimons, E. Kashefi. Unconditionally verifiable blind computation, arXiv:1203.5217 2012

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 $p_{fail} < 1 - \frac{1}{2n}$

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 $p_{fail} < 1 - \frac{1}{2n}$

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!