Quantum Protocols within Spekkens' Toy Model

Leonardo Disilvestro, Damian Markham

Telecom ParisTech, Paris

6th GRD IQFA colloquium,

Palaiseau, 18-20 November 2015

November 19, 2015

Quantum theory and information tasks

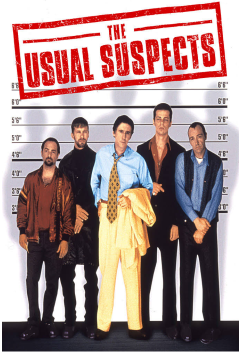
- Quantum protocols provide advantages over classical ones

---

[1] ⓒSpelling Films International

Quantum theory and information tasks

- Quantum protocols provide advantages over classical ones
- Responsibility given to '*the usual suspects*[1]':
    - non-locality or contextuality
    - superposition
    - existence of purifications
    - etc...

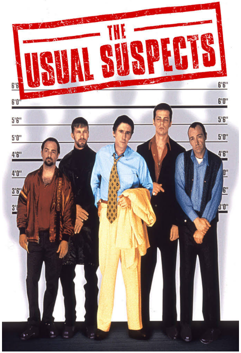


---

[1] ©Spelling Films International

Quantum theory and information tasks

- Quantum protocols provide advantages over classical ones
- Responsibility given to '*the usual suspects*[1]':
  - non-locality or contextuality
  - superposition
  - existence of purifications
  - etc...



- Only one responsible? Or many?
- Use '*toy theories*' to explore this kind of questions!

---

[1] ©Spelling Films International

Toy theories, why bother?

Foundational interest

- Toy theories are *epistemic*
- Explicitly separate local/non-local behaviors
- Some toy theories *are* physical restrictions of quantum theory (e.g quantum Gaussian optics)[2]
- Better characterize the 'usual suspects'

---

[2] Reconstruction of Gaussian quantum mechanics from Liouville mechanics with an epistemic restriction SD Bartlett, T Rudolph, RW Spekkens - Physical Review A, 2012

Toy theories, why bother?

Foundational interest

- Toy theories are *epistemic*
- Explicitly separate local/non-local behaviors
- Some toy theories *are* physical restrictions of quantum theory (e.g quantum Gaussian optics)[2]
- Better characterize the ‘usual suspects’

Computational interest

- Highlight structure of protocols
- Shows how far can we go without non locality
- Steering correlations → easier to implement in the lab

---

[2] Reconstruction of Gaussian quantum mechanics from Liouville mechanics with an epistemic restriction SD Bartlett, T Rudolph, RW Spekkens - Physical Review A, 2012

What is Spekkens toy model?

Spekkens Toy Model[3] is a *classical*, *realist*, and *local* theory:

1. Is a Local Hidden Variable theory,
2. No Bell inequalities, and non-contextual
3. Is an epistemic *(= of knowledge)* theory
4. Admits a stabilizer description (almost identical quantum case)

---

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

What is Spekkens toy model?

Spekkens Toy Model[3] is a *classical*, *realist*, and *local* theory:

1. Is a Local Hidden Variable theory,
2. No Bell inequalities, and non-contextual
3. Is an epistemic *(= of knowledge)* theory
4. Admits a stabilizer description (almost identical quantum case)
5. Toy phenomenology ≈ quantum phenomenology

---

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

What is Spekkens toy model?

Spekkens Toy Model[3] is a *classical*, *realist*, and *local* theory:

1. Is a Local Hidden Variable theory,
2. No Bell inequalities, and non-contextual
3. Is an epistemic *(= of knowledge)* theory
4. Admits a stabilizer description (almost identical quantum case)
5. Toy phenomenology ≈ quantum phenomenology

i.e. it reproduces many quantum behaviors:

- incompatibility of measurements,
- coherent superposition
- interference effects,
- remote steering,
- teleportation,
- no-cloning,
- etc...

---

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

Outline

- Review of Spekkens toy model
- How to translate quantum protocols
- Toy protocols:
    1. no-go bit commitment
    2. error correction & secret sharing
    3. measurement based toy computation
    4. blind and verified toy computation

Spekkens toy states [Spekkens '07]

I	II	III	IV

Ontic (= of existence) states
never directly accessed/prepared/measured

Spekkens toy states [Spekkens ‘07]

I	II	III	IV

Ontic (= of existence) states
never directly accessed/prepared/measured

Allowed epistemic states:

- $|0\rangle$: 🟦🟦⬜⬜
- $|1\rangle$: ⬜⬜🟦🟦
- $|+\rangle$: 🟦⬜🟦⬜
- $|-\rangle$: ⬜🟦⬜🟦
- $|i\rangle$: 🟦⬜⬜🟦
- $|-i\rangle$: ⬜🟦🟦⬜

E.g. of not allowed epistemic state:

- $I/2$: 🟦🟦🟦⬜

- Underlying states → *Ontic*
- Observable states → *Epistemic*

How to write a state: stabilizer notation [Pusey '12][4]

A toy state *n* toy systems is represented

$$S = \{s_1, \ldots, s_{2^l}\}\text{ , generated by }G_S = \{g_1, \ldots, g_l\}$$

---

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

How to write a state: stabilizer notation [Pusey '12][4]

A toy state *n* toy systems is represented

$$S = \{s_1, \ldots, s_{2^l}\} \text{ , generated by } G_S = \{g_1, \ldots, g_l\}$$

Can also be written as a *diagonal matrix*

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

Elements of ρ_S are *probabilities*

---

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

How to write a state: stabilizer notation [Pusey '12][4]

A toy state *n* toy systems is represented

$$S = \{s_1, \dots, s_{2^l}\}\text{ , generated by } G_S = \{g_1, \dots, g_l\}$$

Can also be written as a *diagonal matrix*

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

Elements of ρ_S are *probabilities*

e.g.

$$\longleftrightarrow \;\rho_{\mathcal{Z}} = \begin{pmatrix} 1/2 & 0 & 0 & 0 \\ 0 & 1/2 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \longleftrightarrow < \mathcal{Z} >$$

---

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

How to act on a state

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

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

2. **Measurements:** given a toy state ρ_S

$$\begin{aligned} Measurement: &\quad M = \sum_i \alpha_i P_i, \\ Probability\ outcome\ \alpha_i: &\quad prob(\alpha_i) = tr(P_i\rho_s), \\ Resulting\ state: &\quad \rho_s \xrightarrow{Measurement\ M} \rho_{s'} = \frac{P_i\rho_s P_i}{tr(P_i\rho_s)} \end{aligned}$$

How to act on a state

1. **Reversible transformations:** $4^n \times 4^n$ permutation matrices $\tilde{U}$ over ontic states
$$\rho_S' = \tilde{U} \rho_S \tilde{U}^T,$$

2. **Measurements:** given a toy state ρ_S

$$Measurement : \quad M = \sum_i \alpha_i P_i,$$

$$Probability\ outcome\ \alpha_i : \quad prob(\alpha_i) = tr(P_i \rho_s),$$

$$Resulting\ state : \quad \rho_s \xrightarrow{Measurement\ M} \rho_{s'} = \frac{P_i \rho_s P_i}{tr(P_i \rho_s)}$$

Only valid toy states are stabilizer states

Differences between toy and quantum stabilizers

Toy stabilizers vs quantum stabilizers (i)

Commutation relations		
	Quantum Theory	**Toy Theory**
	$XZ = -iY$	$\mathcal{X}\mathcal{Z} = \mathcal{Y}$ 'Stabilizers' $\tilde{X}\tilde{Z} = \tilde{Y}$ 'Permutations'
	$\{X, Z\} = 0$	$\{\mathcal{X}, \tilde{Z}\} = 0 = \{\tilde{X}, \mathcal{Z}\}$

Toy stabilizers vs quantum stabilizers (ii)

Map between toy and quantum states is **not** unique

Toy stabilizers vs quantum stabilizers (ii)

Map between toy and quantum states is **not** unique

Translation between S^Q and S^T (and vice versa) is an highly ambiguous operation:

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

Toy stabilizers vs quantum stabilizers (ii)

Map between toy and quantum states is **not** unique

Translation between S^Q and S^T (and vice versa) is an highly ambiguous operation:

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

However quantum $XZ = -iY$ while toy $\mathcal{X}\mathcal{Z} = \mathcal{Y}$

Toy stabilizers vs quantum stabilizers (ii)

Map between toy and quantum states is **not** unique

Translation between S^Q and S^T (and vice versa) is an highly ambiguous operation:

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

However quantum $XZ = -iY$ while toy $\mathcal{X}\mathcal{Z} = \mathcal{Y}$

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

Therefore S^Q state maps to 3 distinct toy states:

$S_1^T \neq S_2^T \neq S_3^T$ *Are all mutually orthogonal!*

Toy stabilizers vs quantum stabilizers (iii)

Operations are ambiguous too:

- Toy permutations $\approx$ Clifford unitaries
- Pauli operations $\{\sigma_x, \sigma_z, \sigma_y, I\}^{Quantum} \longleftrightarrow (\tilde{X}, \tilde{Z}, \tilde{Y}, \tilde{I})^{Toy}$
- Arbitrary permutation are not, e.g. ‘toy Hadamard’:

Toy	Quantum
$\tilde{H}\rho_{\mathcal{X}}\tilde{H}^T = \rho_{\mathcal{Z}}$	$H\rho_X H^\dagger = \rho_Z$
$\tilde{H}\rho_{\mathcal{Z}}\tilde{H}^T = \rho_{\mathcal{X}}$	$H\rho_Z H^\dagger = \rho_X$
$\tilde{H}\rho_{\mathcal{Y}}\tilde{H}^T = \rho_{\mathcal{Y}}$	$H\rho_Y H^\dagger = -\rho_Y$

Toy stabilizers vs quantum stabilizers (iii)

Operations are ambiguous too:

- Toy permutations $\approx$ Clifford unitaries
- Pauli operations $\{\sigma_x, \sigma_z, \sigma_y, I\}^{Quantum} \longleftrightarrow (\tilde{X}, \tilde{Z}, \tilde{Y}, \tilde{I})^{Toy}$
- Arbitrary permutation are not, e.g. 'toy Hadamard':

Toy	Quantum
$\tilde{H}\rho_{\mathcal{X}}\tilde{H}^T = \rho_{\mathcal{Z}}$	$H\rho_X H^\dagger = \rho_Z$
$\tilde{H}\rho_{\mathcal{Z}}\tilde{H}^T = \rho_{\mathcal{X}}$	$H\rho_Z H^\dagger = \rho_X$
$\tilde{H}\rho_{\mathcal{Y}}\tilde{H}^T = \rho_{\mathcal{Y}}$	$H\rho_Y H^\dagger = -\rho_Y$

- Spekkens toy model and Quantum theory are *genuinely* different
- Maps quantum-toy & toy-quantum are not unique

Consistent quantum-toy and toy-quantum maps

Translation criteria

Existence of a quantum protocol ⇒ existence of an '*equivalent*' toy protocol

- *Equivalent* := preserves some key figure of merit

Difficulties:

- Map cannot exists if quantum protocols are non-local (e.g. Mermin square)
- Maps and operations between quantum state and toy states are *not unique*

Need a way to ensure consistency

Purifications in the toy model

$\rho^{T}_{S_A}$ mixed over a system A

$$\begin{tikzcd}
\rho^{Q}_{S_A} \\
\rho^{T}_{S_A} \arrow[u]
\end{tikzcd}$$

Purifications in the toy model

$\rho^T_{S_A}$ mixed over a system A

$$\begin{tikzcd}
\rho^Q_{S_A} \arrow[r, "\rho^Q_{S_A}=tr_B(\rho^Q_{S_{AB}})"] & \rho^Q_{S_{AB}} \\
\rho^T_{S_A} \arrow[u] &
\end{tikzcd}$$

- $\rho^Q_{S_{AB}}$ is pure over systems AB

Purifications in the toy model

$\rho^T_{S_A}$ mixed over a system A

$$\begin{tikzcd}
\rho^Q_{S_A} \arrow[r, "\rho^Q_{S_A}=tr_B(\rho^Q_{S_{AB}})"] & \rho^Q_{S_{AB}} \arrow[d] \\
\rho^T_{S_A} \arrow[u] & \rho^T_{S_{AB}}
\end{tikzcd}$$

- $\rho^Q_{S_{AB}}$ is pure over systems AB
- Maps ↑ and ↓ can be always found

Purifications in the toy model

$\rho^T_{S_A}$ mixed over a system A

$$\begin{tikzcd}
\rho^Q_{S_A} \arrow[r, "\rho^Q_{S_A} = tr_B(\rho^Q_{S_{AB}})"] & \rho^Q_{S_{AB}} \arrow[d] \\
\rho^T_{S_A} \arrow[u] \arrow[r, red, "??"] & \rho^T_{S_{AB}}
\end{tikzcd}$$

- $\rho^Q_{S_{AB}}$ is pure over systems AB
- Maps $\uparrow$ and $\downarrow$ can be always found
- However must be taken such that toy map $\xrightarrow{??}$ is implied

Purifications in the toy model

$\rho^{T}_{S_A}$ mixed over a system A

$$\begin{tikzcd}
\rho^{Q}_{S_A} \arrow[r, "\rho^{Q}_{S_A}=tr_B(\rho^{Q}_{S_{AB}})"] & \rho^{Q}_{S_{AB}} \arrow[r, leftrightarrow] \arrow[d] & G^{Q}_{AB} \\
\rho^{T}_{S_A} \arrow[u] \arrow[r, "\rho^{T}_{S_A}=tr^{T}_B(\rho^{T}_{S_{AB}})"] & \rho^{T}_{S_{AB}} &
\end{tikzcd}$$

- $\rho^{Q}_{S_{AB}}$ is pure over systems AB
- Maps ↑ and ↓ can be always found
- However must be taken such that toy map $\xrightarrow{??}$ is implied
- $G^{Q}_{AB} =< \{g_i | g_i \in S_{AB} \ and \ g_i = g_a \otimes I_B\}, \cdots >$

Purifications in the toy model

$\rho^T_{S_A}$ mixed over a system A

$$\begin{tikzcd}
\rho^Q_{S_A} \arrow[r, "\rho^Q_{S_A} = tr_B(\rho^Q_{S_{AB}})"] & \rho^Q_{S_{AB}} \leftrightarrow G^Q_{AB} \arrow[d] \\
\rho^T_{S_A} \arrow[u] \arrow[r, "\rho^T_{S_A} = tr^T_B(\rho^T_{S_{AB}})"] & \rho^T_{S_{AB}}
\end{tikzcd}$$

- $\rho^Q_{S_{AB}}$ is pure over systems AB
- Maps ↑ and ↓ can be always found
- However must be taken such that toy map $\xrightarrow{??}$ is implied
- $G^Q_{AB} =< \{g_i | g_i \in S_{AB} \text{ and } g_i = g_a \otimes I_B\}, \cdots >$

$$\boxed{\text{Choice of } G^Q_{AB} \Rightarrow \text{consistency of } \uparrow \text{ and } \downarrow \text{ maps} \Rightarrow \text{toy map } tr^T_B(\cdot)}$$

Purificaitons & no-bit commitment

- Toy purifications
- Purifications equivalent up to permutation on B

We can prove

- no-go for perfect bit commitment
- no-go for ϵ-cheating bit commitment

Proofs then reduce to adaptations of the quantum proofs

Error correction (i)

Quantum error correction

1. Encode state k systems ρ_k into n system state ρ_{S_L}

$$\rho_k^Q \xrightarrow{\textit{Encoding}} \rho_{S_L}^Q$$

Error correction (i)

Quantum error correction

1. Encode state k systems ρ_k into n system state ρ_{S_L}
2. Noise map $\mathcal{F}(\rho^Q_{S_L})$ (CPTP map)

$$\rho^Q_k \xrightarrow{\textit{Encoding}} \rho^Q_{S_L} \xrightarrow{\textit{Noise}} \mathcal{F}(\rho^Q_{S_L})$$

Error correction (i)

Quantum error correction

1. Encode state k systems ρ_k into n system state ρ_{S_L}
2. Noise map $\mathcal{F}(\rho^Q_{S_L})$ (CPTP map)
3. Error Correction protocol $\mathfrak{E}$ (*syndrome* and *recovery*)

$$\rho^Q_k \xrightarrow{Encoding} \rho^Q_{S_L} \xrightarrow{Noise} \mathcal{F}(\rho^Q_{S_L}) \xrightarrow{E.C.} \mathfrak{E}(\mathcal{F}(\rho^Q_{S_L})) = \rho'^Q_{S_L}$$

Error correction (i)

Quantum error correction

1. Encode state k systems ρ_k into n system state ρ_{S_L}
2. Noise map $\mathcal{F}(\rho^Q_{S_L})$ (CPTP map)
3. Error Correction protocol $\mathfrak{E}$ (*syndrome* and *recovery*)
4. Decode corrected state

$$\rho^Q_k \xrightarrow{Encoding} \rho^Q_{S_L} \xrightarrow{Noise} \mathcal{F}(\rho^Q_{S_L}) \xrightarrow{E.C.} \mathfrak{E}(\mathcal{F}(\rho^Q_{S_L})) = \rho'^Q_{S_L} \xrightarrow{decoding} \rho'^Q_{S_k}$$

Error correction (i)

Quantum error correction

1. Encode state k systems ρ_k into n system state ρ_{S_L}
2. Noise map $\mathcal{F}(\rho^Q_{S_L})$ (CPTP map)
3. Error Correction protocol $\mathfrak{E}$ (*syndrome* and *recovery*)
4. Decode corrected state

$$\rho^Q_k \xrightarrow{Encoding} \rho^Q_{S_L} \xrightarrow{Noise} \mathcal{F}(\rho^Q_{S_L}) \xrightarrow{E.C.} \mathfrak{E}(\mathcal{F}(\rho^Q_{S_L})) = \rho'^Q_{S_L} \xrightarrow{decoding} \rho'^Q_{S_k}$$

$$\boxed{\rho'^Q_{S_L} = \rho^Q_{S_L} \Rightarrow \text{error } \mathcal{F} \text{ is } \textit{correctable}}$$

Error correction (ii)

$$\rho_{S_L}^{Q} \quad \xrightarrow{\textit{Noise}} \quad \mathcal{F}(\rho_{S_L}^{Q}) \quad \xrightarrow{\textit{Q.E.C.}} \quad \mathfrak{E}(\mathcal{F}(\rho_{S_L}^{Q})) = \rho_{S_L}'^{Q} \quad \Rightarrow \rho_{S_L}'^{Q} = \rho_{S_L}^{Q}$$

$$\rho_{S_L}^{T} \quad \xrightarrow{\textit{Noise}} \quad \mathcal{E}(\rho_{S_L}^{T}) \quad \xrightarrow{\textit{T.E.C.}} \quad \mathfrak{F}(\mathcal{E}(\rho_{S_L}^{Q})) = \rho_{S_L}'^{T} \quad \Rightarrow \rho_{S_L}'^{Q} = \rho_{S_L}^{T}$$

Error correction (ii)

$$\begin{tikzcd}
\rho^{Q}_{S_L} \arrow[r, "??"] \arrow[d] & (\bar{\rho}^{Q}_{S_L}) \arrow[r, "E.C."] & \mathfrak{E}(\bar{\rho}^{Q}_{S_L}) = \rho'^{Q}_{S_L} & \Rightarrow \rho'^{Q}_{S_L} = \rho^{Q}_{S_L} \\
\rho^{T}_{S_L} \arrow[r, "Noise"] & \mathcal{E}(\rho^{T}_{S_L}) \arrow[r, "??"] \arrow[u] & \mathfrak{F}(\mathcal{E}(\rho^{Q}_{S_L})) = \rho'^{T}_{S_L} & \overset{??}{\Longrightarrow} \rho'^{Q}_{S_L} = \rho^{T}_{S_L}
\end{tikzcd}$$

- Procedure must
  1. For all maps ↓ and toy noise $\text{Weight}(\mathcal{E}) \leq d^{Q}_{code}$
  2. imply $\xrightarrow{??}$ arrows and $\overset{??}{\Longrightarrow}$
  3. i.e. find some correctable $\mathcal{F}$ s.t. $\bar{\rho}^{Q}_{S_L} = \mathcal{F}(\rho^{Q}_{S_L})$

Error correction (ii)

$$\begin{tikzcd}
\rho^Q_{S_L} \arrow[r, "\mathcal{F}"] \arrow[d] & \mathcal{F}(\rho^Q_{S_L}) \arrow[r, "\mathit{E.C.}"] & \mathfrak{E}(\mathcal{F}(\rho^Q_{S_L})) = \rho'^Q_{S_L} & \Rightarrow \rho'^Q_{S_L} = \rho^Q_{S_L} \\
\rho^T_{S_L} \arrow[r, "\mathit{Noise}"] & \mathcal{E}(\rho^T_{S_L}) \leftrightarrow G_d \arrow[u] \arrow[r, "\mathfrak{F}\ \textbf{T.E.C}"] & \mathfrak{F}(\mathcal{E}(\rho^Q_{S_L})) = \rho'^T_{S_L} & \Rightarrow \rho'^Q_{S_L} = \rho^T_{S_L}
\end{tikzcd}$$

- Procedure must
  1. For all maps ↓ and toy noise Weight$(\mathcal{E}) \leq d^Q_{code}$
  2. imply $\xrightarrow{??}$ arrows and $\overset{??}{\Longrightarrow}$
  3. i.e. find some correctable $\mathcal{F}$ s.t. $\bar{\rho}^Q_{S_L} = \mathcal{F}(\rho^Q_{S_L})$

- Choice of generating map ↑

$$\mathcal{E}(\rho^T_{S_L}) \leftrightarrow G_d =< \{G_L\}, \{G_{Syndrome}\}, \cdots >$$

- $\{G_L\}$ preserves logical encoding — $\{G_{Syndrome}\}$ preserve syndrome extraction

Error correction (iii)

Despite

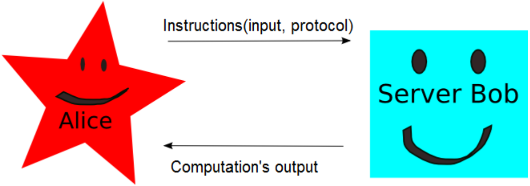
- Toy model being classical
- Featuring a no-cloning theorem [Spekkens' 07]

We find that

- Stabilizer based error correction is possible on the toy model
- Existence of toy error correction → toy secret sharing

Choice of generating set allows quantum figures of merit to be preserved by the $\uparrow$ and $\downarrow$ maps

Blind and verified computation (i)



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

Blind and verified computation (ii)

We considered two protocols which implement verification:

- RUV[5] uses Bell's tests
- FK[6] uses
  1. graph states [Pusey '12]
  2. measurement based quantum computation
  3. ...non-locality?

There are no classical verified protocols with the same properties

---

[5] B. Reichardt, R. Unger, U. Vazirani. Classical command of quantum systems. Nature, 2013.

[6] J. Fitzsimons, E. Kashefi. Unconditionally verifiable blind computation, arXiv:1203.5217 2012

Blind and verified computation (iii)

Protocol is hard to (formally!) describe and draw

Key ideas outline:

- MBQC computation
- Disentangled traps → deterministic outcome
- Figure of merit is the '*probability Bob has altered the computation without springing a trap*':

$$p_{fail} = tr((P_{inc}^{Output} \otimes |Acc\rangle \langle Acc|^{traps})\rho^{output}) < 1 \tag{1}$$

- Choice of generators must account for
  1. all possible toy computations
  2. all possible Bob's deviations

Considerations

Starting point

- Spekkens toy model reproduces quantum behaviors [Spekkens '12]
- Toy model admits a stabilizer notations [Pusey '12]

Our contribution

- Toy model reproduces many stabilizer protocols
- Despite classical and no-cloning → error correction
- Properties of the encoding → no bit commitment, secret sharing
- Despite locality → verified protocols

Conclusions

- Steering and commutation relations are key to our translations
- Looking for a steering-based version of FK
- Gaussian optics is a toy theory and can provide easier experimental setups where to test toy protocols
- Understanding when and where non-locality is truly necessary gives a better understanding of the protocols and a mean of simplification.

Conclusions

Thank you for listening!