Quantum, a look through nonlocality

Alexandre Nolin [1]

[1]IRIF, algocomp group

03/05/2017

Defining quantumness

Disclaimer

This is in no way a real introduction to quantum theory.

Defining quantumness

Disclaimer

This is in no way a real introduction to quantum theory.

However ...

I will try to give all the basic notation and ideas necessary to understand most quantum computing talks.

Defining quantumness

Disclaimer

This is in no way a real introduction to quantum theory.

However ...

I will try to give all the basic notation and ideas necessary to understand most quantum computing talks.
And talk about my own research.

Defining quantumness: the basic idea

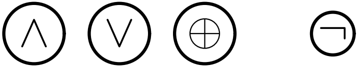
Quantum computing is what you get when you move from the usual theory of probability to a similar theory based on the ℓ_2-norm.

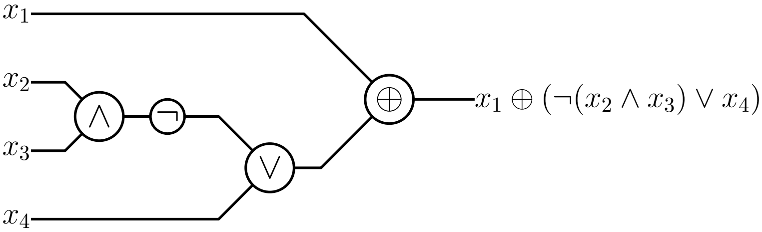
Defining quantumness: the basic idea

Quantum computing is what you get when you move from the usual theory of probability to a similar theory based on the ℓ_2-norm.

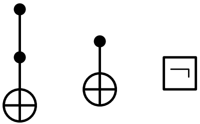
ok ... but precisely ?

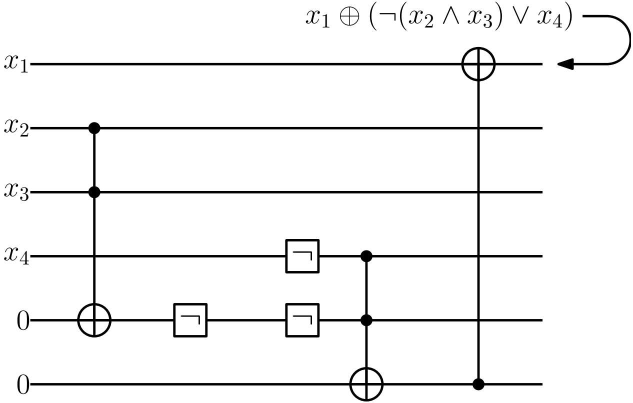
Classical circuits



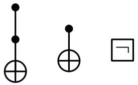


Reversibility

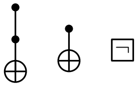




Matrix form

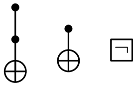


Matrix form



$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} : \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} : \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

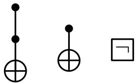
Matrix form



$$\begin{pmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0 \end{pmatrix} : \begin{pmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&0&1\\ 0&0&1&0 \end{pmatrix} : \begin{pmatrix} 0&1\\ 1&0 \end{pmatrix}$$

$$|0\rangle = \begin{pmatrix} 1\\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0\\ 1 \end{pmatrix}, |01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 1\cdot|1\rangle\\ 0\cdot|1\rangle \end{pmatrix} = \begin{pmatrix} 0\\ 1\\ 0\\ 0 \end{pmatrix}$$

Matrix form

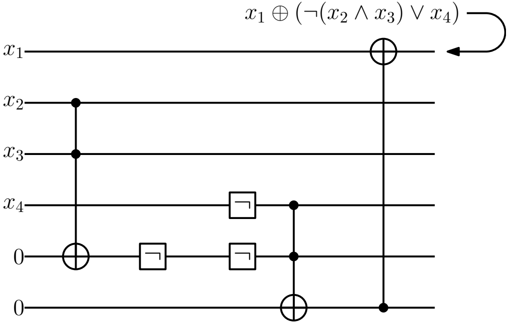


$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} : \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} : \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, |01\rangle = |0\rangle\ |1\rangle = \begin{pmatrix} 1 \cdot |1\rangle \\ 0 \cdot |1\rangle \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

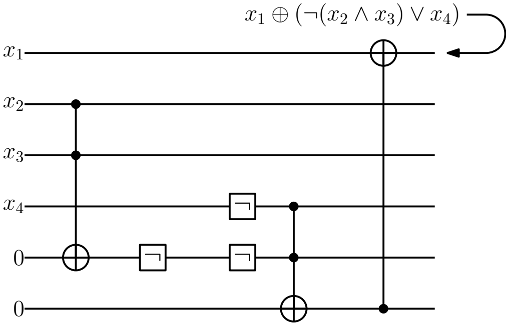
Combining parts

If S_1 and S_2 are the sets of states of two circuits, the states of the two circuits combined are $S_1 \times S_2$.

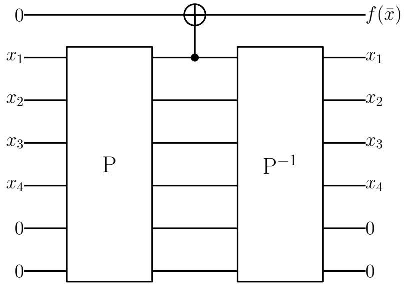


Combining parts

If S_1 and S_2 are the sets of states of two circuits, the states of the two circuits combined are $S_1 \times S_2$.
The matrix representing how a small-dimensional operator is applied to the whole space is obtained with a tensor product $\mathbf{1} \otimes M$

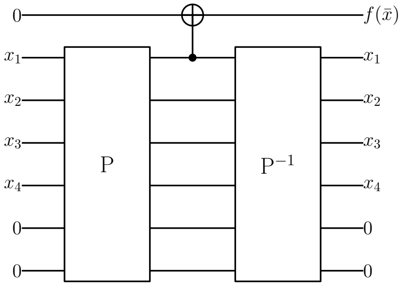


Uncomputation



Reversible circuit correspond to a *permutation matrix* over the 2^n states of the system.
As every gate is its own inverse, taking the circuit from the other side *reverses the computation*.

Uncomputation



Reversible circuit correspond to a *permutation matrix* over the 2^n states of the system.
As every gate is its own inverse, taking the circuit from the other side *reverses the computation*.
Every permutation is achievable with the previous gates.

Moving to probabilities

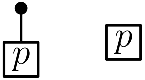
With reversible circuits and permutation matrices, we have a bijective map of the 2^n possible states of a n-wire circuit.

Moving to probabilities

With reversible circuits and permutation matrices, we have a bijective map of the 2^n possible states of a n-wire circuit.

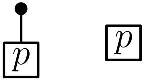
Can we do the same with *probability distributions* over such states, that is *convex combinations* of the previous states ?

What can we add ?



$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & p & 1-p \\ 0 & 0 & 1-p & p \end{pmatrix} \quad : \quad \begin{pmatrix} p & 1-p \\ 1-p & p \end{pmatrix}$$

What can we add ?



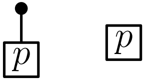
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & p & 1-p \\ 0 & 0 & 1-p & p \end{pmatrix} \; : \; \begin{pmatrix} p & 1-p \\ 1-p & p \end{pmatrix}$$

In contrast to deterministic reversible circuits ...

... it is *very different* !

The sets of ℓ_1-norm-preserving matrices, the *stochastic* matrices, are not necessarily inversible.

What can we add ?



$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & p & 1-p \\ 0 & 0 & 1-p & p \end{pmatrix} \; : \; \begin{pmatrix} p & 1-p \\ 1-p & p \end{pmatrix}$$

In contrast to deterministic reversible circuits ...

... it is *very different* !
The sets of ℓ_1-norm-preserving matrices, the *stochastic* matrices, are not necessarily inversible.
And their inverse are not necessarily norm-preserving !

Quantum

A message from the past

Quantum computing is what you get when you move from the usual theory of probability to a similar theory based on the ℓ_2-norm.

Quantum

A message from the past

Quantum computing is what you get when you move from the usual theory of probability to a similar theory based on the ℓ_2-norm.

Instead of ℓ_1-unit, positive vectors of $\{\ |0\rangle, \ |1\rangle\ \}^{\otimes n}$ taken as a $\mathbb{R}$-vector space, we now consider ℓ_2-unit vectors of $\{\ |0\rangle, \ |1\rangle\ \}^{\otimes n}$ taken as a $\mathbb{C}$-vector space.

Quantum

A message from the past

Quantum computing is what you get when you move from the usual theory of probability to a similar theory based on the ℓ_2-norm.

Instead of ℓ_1-unit, positive vectors of $\{ \mid 0\rangle, \mid 1\rangle \}^{\otimes n}$ taken as a $\mathbb{R}$-vector space, we now consider ℓ_2-unit vectors of $\{ \mid 0\rangle, \mid 1\rangle \}^{\otimes n}$ taken as a $\mathbb{C}$-vector space.

Superposition and observation

In the presence of a state $\sum_i \alpha_i \,|i\rangle$, the probability of observing $|i\rangle$ is $|\alpha_i|^2$

Quantum gates

$\boxed{\mathrm{X}}\ \boxed{\mathrm{Y}}\ \boxed{\mathrm{Z}}\quad \boxed{\mathrm{H}}\quad \boxed{\mathrm{R}_\theta}$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \;:\; \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \;:\; \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

Quantum gates

$\boxed{\mathrm{X}}\ \boxed{\mathrm{Y}}\ \boxed{\mathrm{Z}}\quad \boxed{\mathrm{H}}\quad \boxed{\mathrm{R}_\theta}$

$$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\ \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\ \begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}\ :\ \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\ :\ \begin{pmatrix}1 & 0\\ 0 & e^{i\theta}\end{pmatrix}$$

The set of ℓ_2-norm-preserving matrices is the *unitary* matrices (U s.t $UU^\dagger = I$).

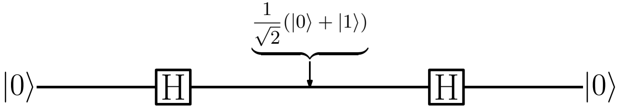
Quantum gates

$\boxed{\mathrm{X}}\ \boxed{\mathrm{Y}}\ \boxed{\mathrm{Z}}\quad \boxed{\mathrm{H}}\quad \boxed{\mathrm{R}_\theta}$

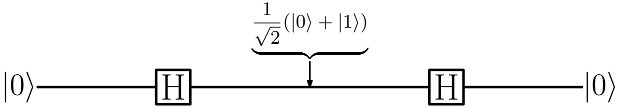
$$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\ \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\ \begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}\ :\ \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\ :\ \begin{pmatrix}1 & 0\\ 0 & e^{i\theta}\end{pmatrix}$$

The set of ℓ_2-norm-preserving matrices is the *unitary* matrices (U s.t $UU^\dagger = I$).
This makes all quantum circuits invertible in the same sense than classical reversible circuits.

Example

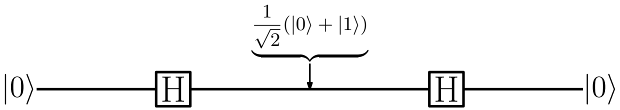


Example



$$HH\,|0\rangle = \frac{1}{\sqrt{2}} H \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = H \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} = H \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle\right) = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

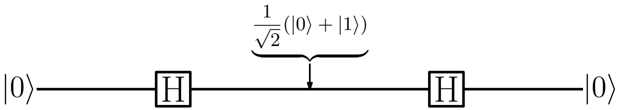
Example



$$HH\,|0\rangle = \frac{1}{\sqrt{2}} H \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = H \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} = H \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

In this example, if we were to observe the circuit in the middle, we would see $|0\rangle$ w.p $1/2$, $|1\rangle$ w.p $1/2$.

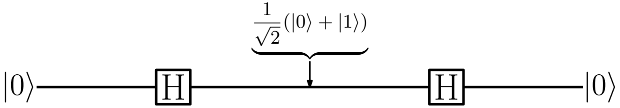
Example



$$HH|0\rangle = \frac{1}{\sqrt{2}} H \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = H \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} = H \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

In this example, if we were to observe the circuit in the middle, we would see $|0\rangle$ w.p $1/2$, $|1\rangle$ w.p $1/2$.
But after a second Hadamard gate, we go back to the state $|0\rangle$.

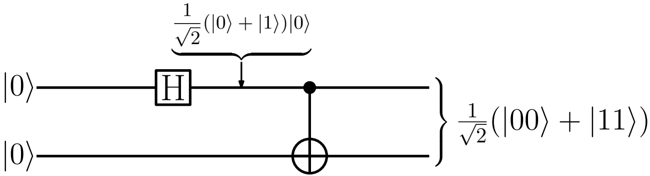
Example



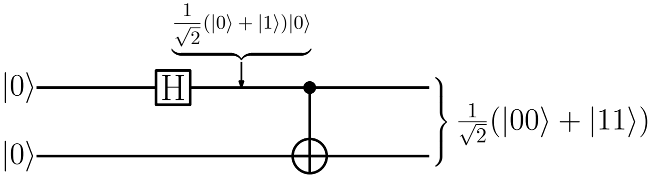
$$HH|0\rangle = \frac{1}{\sqrt{2}} H \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = H \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} = H \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

In this example, if we were to observe the circuit in the middle, we would see $|0\rangle$ w.p $1/2$, $|1\rangle$ w.p $1/2$.
But after a second Hadamard gate, we go back to the state $|0\rangle$.
This is definitely *not possible* with probabilistic gates as described before.

EPR pairs

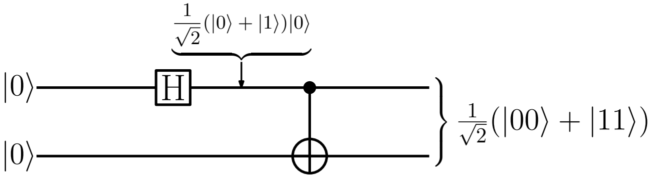

$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle$
$|0\rangle$
H
$|0\rangle$
$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

EPR pairs



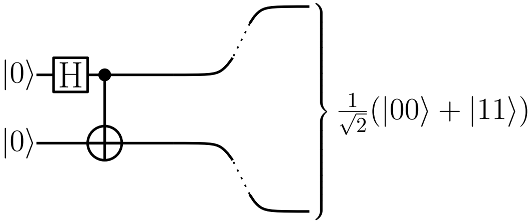
In this example, the two wires are *entangled*, because the state $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ *cannot* be factored as $|a\rangle \otimes |b\rangle$

EPR pairs



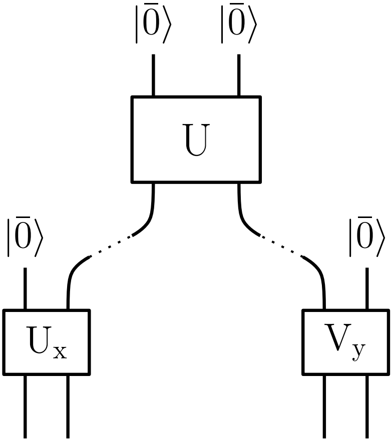
In this example, the two wires are *entangled*, because the state $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ *cannot* be factored as $|a\rangle \otimes |b\rangle$
An observer that measures a wire can get both $|0\rangle$ and $|1\rangle$ w.p $1/2$ and learns what is on the other wire.

EPR pairs

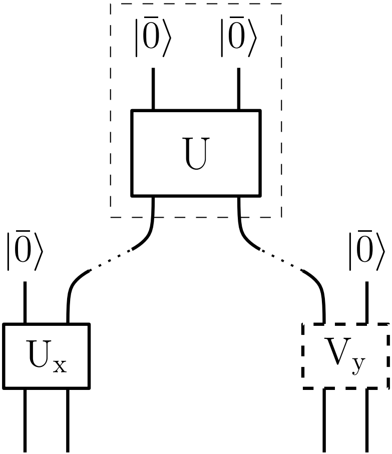


In this example, the two wires are *entangled*, because the state $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ *cannot* be factored as $|a\rangle \otimes |b\rangle$
An observer that measures a wire can get both $|0\rangle$ and $|1\rangle$ w.p $1/2$ and learns what is on the other wire.
This is even true if the wires are far away from each other.

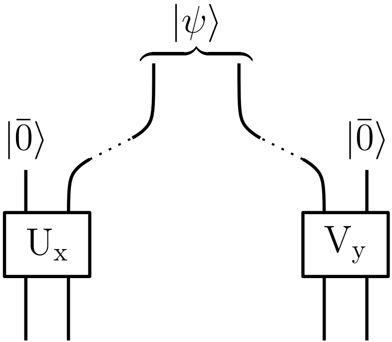
Moving to the Bell setup



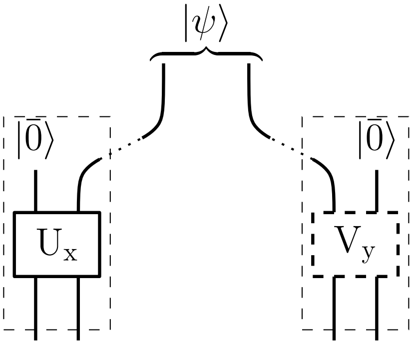
Moving to the Bell setup



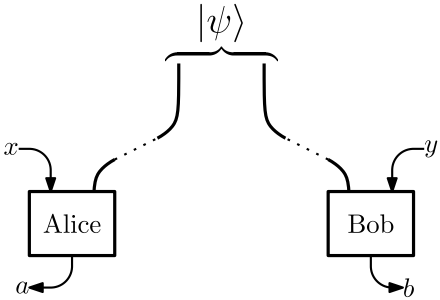
Moving to the Bell setup



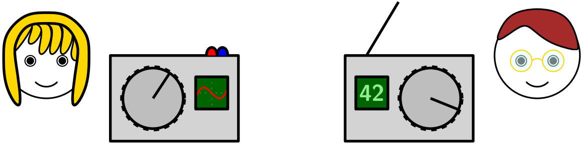
Moving to the Bell setup

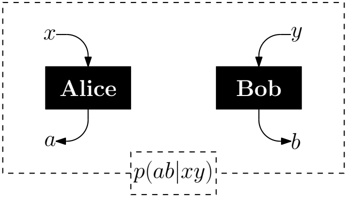


Moving to the Bell setup

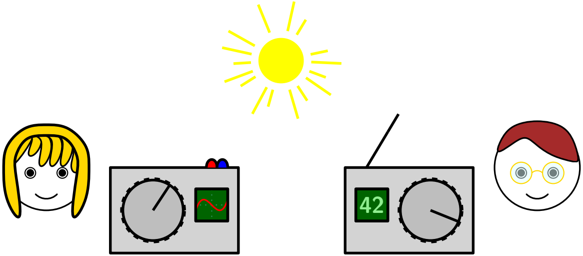


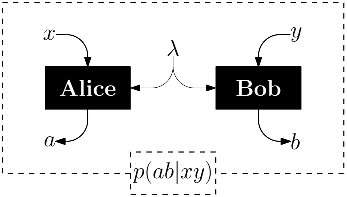
Bell tests : The basic setup

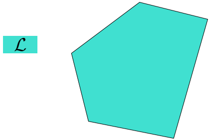




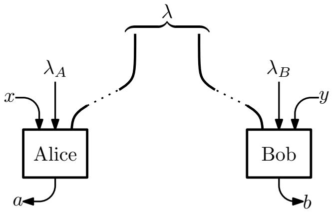
Bell tests : Players using only local hidden variables



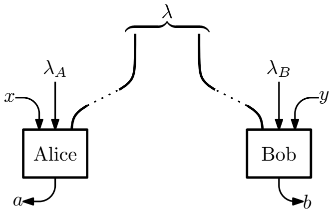


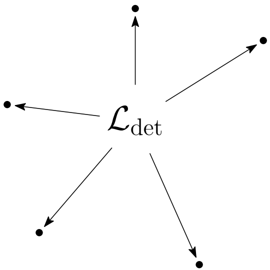


Local hidden variables ? Probabilistic circuits !

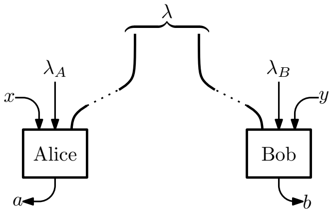


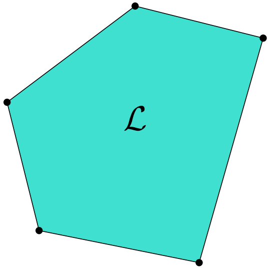
Local hidden variables ? Probabilistic circuits !



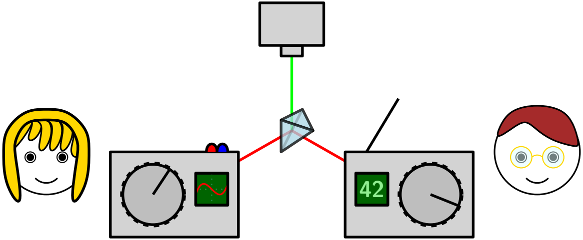


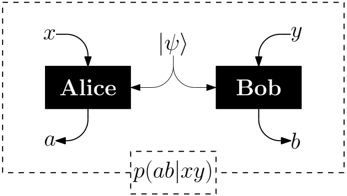
Local hidden variables ? Probabilistic circuits !

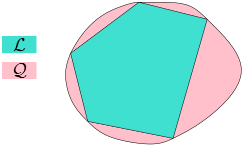




Bell tests : Players with access to a quantum state



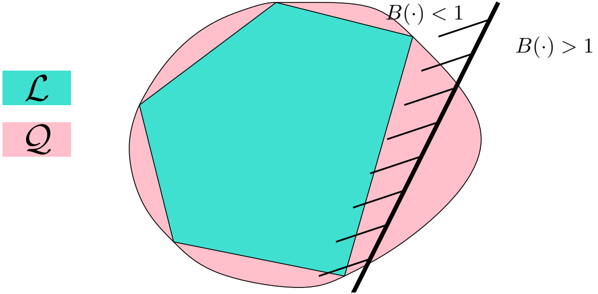




Bell tests : Bell inequalities

Bell functionals $\Leftrightarrow$ linear forms over $\mathbb{R}^{\mathcal{A}\times\mathcal{B}\times\mathcal{X}\times\mathcal{Y}}$

Bell inequalities $\Leftrightarrow$ Inequalities involving a Bell functional that are satisfied by all local distributions



$B : (B_{abxy})_{\mathcal{A}\times\mathcal{B}\times\mathcal{X}\times\mathcal{Y}}$ $\qquad$ $B(\mathbf{p}) = \sum_{abxy} B_{abxy}\, p(ab|xy)$

An example : CHSH

The CHSH game

Alice gets an $x \in \{0, 1\}$, Bob gets an $y \in \{0, 1\}$ (u.a.r).

An example : CHSH

The CHSH game

Alice gets an $x \in \{0,1\}$, Bob gets an $y \in \{0,1\}$ (u.a.r).
Goal : output a and b s.t. $a \oplus b = x \wedge y$

An example : CHSH

The CHSH game

Alice gets an $x \in \{0, 1\}$, Bob gets an $y \in \{0, 1\}$ (u.a.r).
Goal : output a and b s.t. $a \oplus b = x \wedge y$

Claim

It is impossible to win this game with probability higher than 3/4 classically.

An example : CHSH

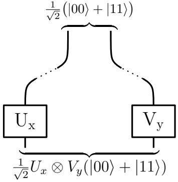
The CHSH game

Alice gets an $x \in \{0, 1\}$, Bob gets an $y \in \{0, 1\}$ (u.a.r).
Goal : output a and b s.t. $a \oplus b = x \wedge y$

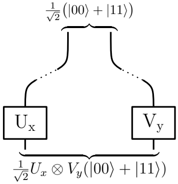
Claim

It is impossible to win this game with probability higher than 3/4 classically.
However, with quantum ressources, it is possible to achieve $\frac{1+\sqrt{2}}{2\sqrt{2}} \approx 0.85\ldots$

CHSH : winning with $p = 0.85\ldots$



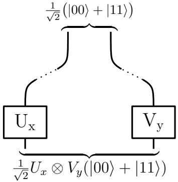
CHSH : winning with $p = 0.85\ldots$



$$U_x = R_{\alpha_x} \qquad V_y = R_{\beta_y}$$
$$\alpha_0 = 0, \alpha_1 = \pi/4 \qquad \beta_0 = \pi/8, \beta_1 = -\pi/8$$

$$\textit{where } R_\alpha = \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix}$$

CHSH : winning with $p = 0.85\ldots$



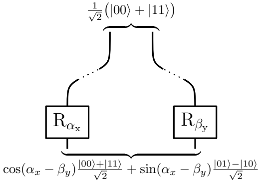
$$U_x = R_{\alpha_x} \qquad V_y = R_{\beta_y}$$

$$\alpha_0 = 0, \alpha_1 = \pi/4 \qquad \beta_0 = \pi/8, \beta_1 = -\pi/8$$

$$\textit{where } R_\alpha = \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix}$$

$$\begin{aligned}
& U_x \otimes V_y \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
= \quad & R_{\alpha_x} \otimes R_{\beta_y} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
= \quad & \frac{1}{\sqrt{2}} \mathbb{1} \otimes R_{\beta_y} (\cos\alpha_x |00\rangle - \sin\alpha_x |10\rangle + \sin\alpha_x |01\rangle + \cos\alpha_x |11\rangle) \\
= \quad & \frac{1}{\sqrt{2}} \Big[(\cos\alpha_x \cos\beta_y + \sin\alpha_x \sin\beta_y)(|00\rangle + |11\rangle) \\
& +(\sin\alpha_x \cos\beta_y - \cos\alpha_x \sin\beta_y)(|01\rangle - |10\rangle) \Big] \\
= \quad & \cos(\alpha_x - \beta_y) \frac{|00\rangle + |11\rangle}{\sqrt{2}} + \sin(\alpha_x - \beta_y) \frac{|01\rangle - |10\rangle}{\sqrt{2}}
\end{aligned}$$

CHSH : winning with $p = 0.85\ldots$



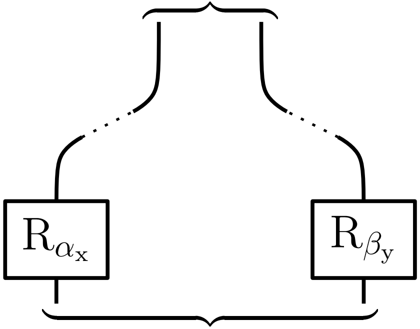
$$U_x = R_{\alpha_x} \qquad V_y = R_{\beta_y}$$
$$\alpha_0 = 0, \alpha_1 = \pi/4 \qquad \beta_0 = \pi/8, \beta_1 = -\pi/8$$

$$\textit{where } R_\alpha = \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix}$$

$$\begin{aligned}
& U_x \otimes V_y \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
= \quad & R_{\alpha_x} \otimes R_{\beta_y} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
= \quad & \frac{1}{\sqrt{2}} \mathbb{1} \otimes R_{\beta_y} (\cos\alpha_x |00\rangle - \sin\alpha_x |10\rangle + \sin\alpha_x |01\rangle + \cos\alpha_x |11\rangle) \\
= \quad & \frac{1}{\sqrt{2}} \Big[(\cos\alpha_x \cos\beta_y + \sin\alpha_x \sin\beta_y)(|00\rangle + |11\rangle) \\
& +(\sin\alpha_x \cos\beta_y - \cos\alpha_x \sin\beta_y)(|01\rangle - |10\rangle) \Big] \\
= \quad & \cos(\alpha_x - \beta_y)\frac{|00\rangle + |11\rangle}{\sqrt{2}} + \sin(\alpha_x - \beta_y)\frac{|01\rangle - |10\rangle}{\sqrt{2}}
\end{aligned}$$

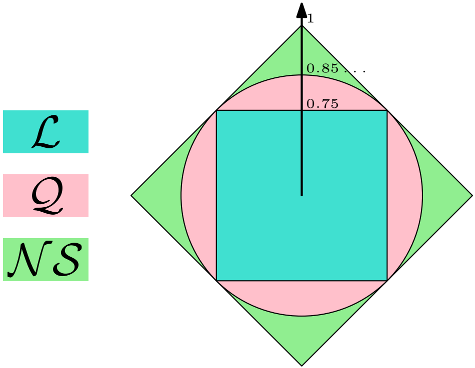
CHSH : winning with $p = 0.85\ldots$

$$\frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big)$$

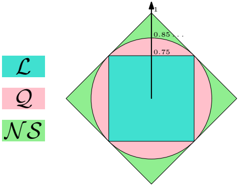


$$\cos(\alpha_x - \beta_y)\frac{|00\rangle+|11\rangle}{\sqrt{2}} + \sin(\alpha_x - \beta_y)\frac{|01\rangle-|10\rangle}{\sqrt{2}}$$

CHSH as bipartite distributions and a Bell inequality

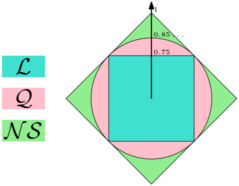


CHSH as bipartite distributions and a Bell inequality



$$B_{abxy} = \mathbb{1}_{\{a \oplus b = x \wedge y\}}$$

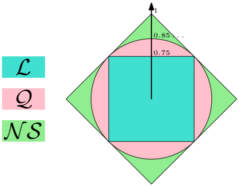
CHSH as bipartite distributions and a Bell inequality



$$B_{abxy} = \mathbb{1}_{\{a \oplus b = x \wedge y\}}$$

$$B(\ell) \leq 0.75, \forall \ell \in \mathcal{L}$$

CHSH as bipartite distributions and a Bell inequality



$$B_{abxy} = \mathbb{1}_{\{a \oplus b = x \wedge y\}}$$

$$B(\ell) \leq 0.75, \forall \ell \in \mathcal{L}$$

$$\exists \mathbf{q}, B(\mathbf{q}) = \cos^2 \frac{\pi}{8} = \frac{1}{2} + \frac{1}{2\sqrt{2}}$$

Fun related stuff

Fun related stuff

- Non-local boxes (NLBs) of success probability $p > \frac{1}{2} + \frac{1}{\sqrt{6}} \approx 0.91$ trivializes communication complexity [van Dam'00,BBL+'06]

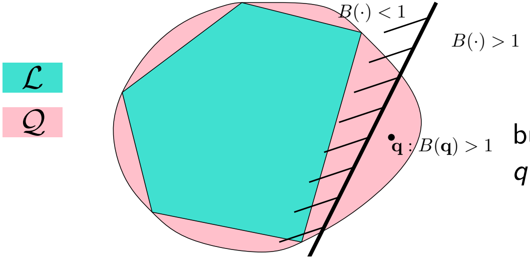
Fun related stuff

- Non-local boxes (NLBs) of success probability $p > \frac{1}{2} + \frac{1}{\sqrt{6}} \approx 0.91$ trivializes communication complexity [van Dam'00,BBL+'06]
- Because quantum is inherently random, and because deterministic strategies cannot violate Bell inequalities, one can *certify* random bits using Bell inequalities.[PAM'10]

Fun related stuff

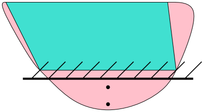
- Non-local boxes (NLBs) of success probability $p > \frac{1}{2} + \frac{1}{\sqrt{6}} \approx 0.91$ trivializes communication complexity [van Dam'00,BBL+'06]
- Because quantum is inherently random, and because deterministic strategies cannot violate Bell inequalities, one can *certify* random bits using Bell inequalities.[PAM'10]
- Such proofs can be *device independent*.

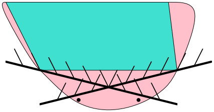
Bell tests : Bell inequality violations

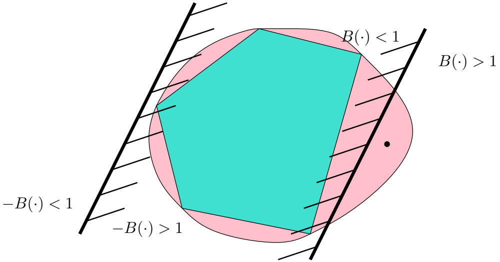


but can we
quantify nonlocality ?

Bell inequality violations : Quantifying nonlocality



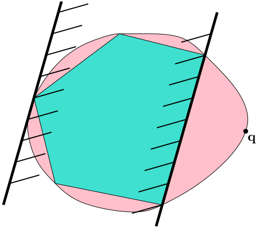




Normalisation constraint : $|B(\cdot)| \leq 1$ on $\mathcal{L}$

$$\nu(\mathbf{p}) := \max B(\mathbf{p}), \qquad |B(\ell)| \leq 1, \; \forall \ell \in \mathcal{L}$$

Maximal violations : Known bounds

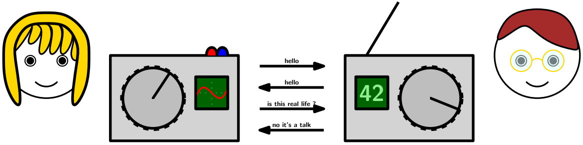


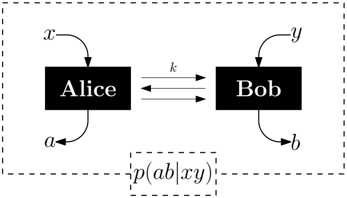
max $B(\mathbf{q})$ over $\mathbf{q} \in \mathcal{Q}$ and
B s.t $|B(\ell)| \leq 1$, $\forall \ell \in \mathcal{L}$?

Parameter	Upper bound	Ad hoc lower bounds	
# inputs N	$2^c \leq N$ [234]	$\frac{\sqrt{N}}{\log(N)}$ [5]	
# outputs K	$O(K)$ [5]	$\Omega\left(\frac{K}{(\log(K))^2}\right)$ [6]	
Dimension d	$O(d)$ [4]	$\Omega\left(\frac{d}{(\log(d))^2}\right)$ [6]	

[1] BCG+'16 [2] LS'09 [3] DKLR'11 [4] JPP+'10 [5] JP'11 [6] BRSdW'12

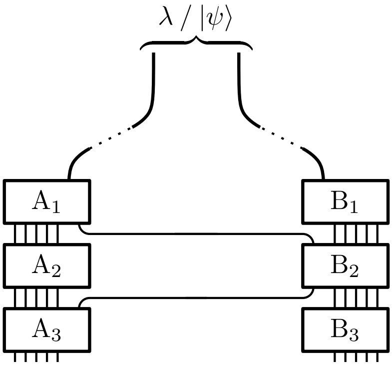
Communication complexity : Definition



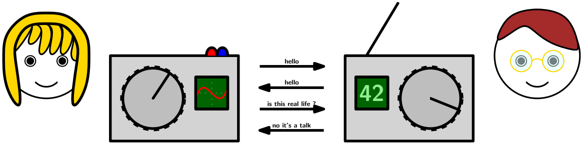


Communication complexity : min k
Classical messages : $\mathrm{CC}(\mathbf{p})$
Quantum messages : $\mathrm{QCC}(\mathbf{p})$

Communication complexity : traveling wires



Communication complexity : Upper and lower bounds



Upper bounds	$\leftrightarrow$	protocols
Lower bounds	$\leftrightarrow$	combinatorial or algebraic measures (ν, γ_2, $\mathrm{disc}\ldots$)

Theorem (DKLR'11)

ν (LS'08) is a lower bound on simulating probability distributions : $\log \nu(\mathbf{p}) \leq \mathrm{CC}(\mathbf{p})$.

Communication complexity : Recent general link to Bell inequalities

Theorem (BCG+'16)

For any communication problem f there exists a normalized Bell inequality B and a quantum distribution $\mathbf{q}$ such that :

$$B(\mathbf{q}) = \Omega\left(\frac{\sqrt{\mathrm{CC}(f)}}{\mathrm{QCC}(f)}\right)$$

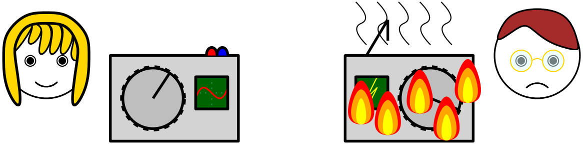
Techniques : protocol tree, port-based teleportation, bias amplification (+Chernoff bound) . . .

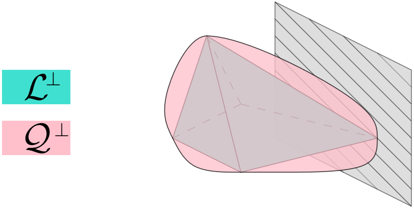
Maximal violations : Known bounds

Parameter	Upper bound	Ad hoc lower bounds	Best possible lower bound from [1]
# inputs N	$2^c \leq N$ [234]	$\frac{\sqrt{N}}{\log(N)}$ [5]	$\frac{\sqrt{c}}{q} \leq \log(N)$
# outputs K	$O(K)$ [5]	$\Omega\left(\frac{K}{(\log(K))^2}\right)$ [6]	$\leq \log(K)$
Dimension d	$O(d)$ [4]	$\Omega\left(\frac{d}{(\log(d))^2}\right)$ [6]	$\leq \log\log(d)$

[1] BCG+'16 [2] LS'09 [3] DKLR'11 [4] JPP+'10 [5] JP'11 [6] BRSdW'12

Efficiency and distributions with abort events

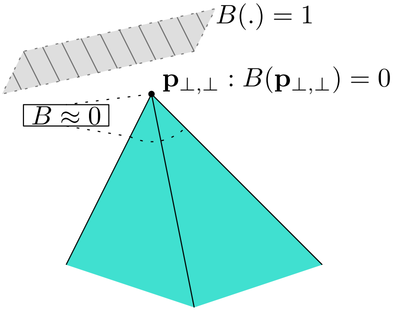




We add a new event $\perp$ (abort) to the outputs
We get new sets $\mathcal{L}^{\perp}$ and $\mathcal{Q}^{\perp}$

Inefficiency-resistant Bell inequalities

Bell inequalities over the larger space $\{\mathcal{A} \cup \perp\} \times \{\mathcal{B} \cup \perp\} \times \mathcal{X} \times \mathcal{Y}$:



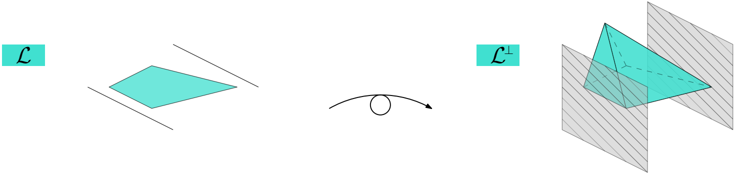
No weights on abort events.
Normalized over a larger set $\mathcal{L}^{\perp}$.
Weaker constraints :

$$B(\ell) \leq 1, \ \forall \ell \in \mathcal{L}^{\perp}.$$

eff$(\mathbf{p}) := \max B(\mathbf{p}), B(\ell) \leq 1, \forall \ell \in \mathcal{L}^{\perp}$ (LLR'12) still well-defined.
It is equivalent to the partition bound of (JK'10).

Theorem (1, this work)

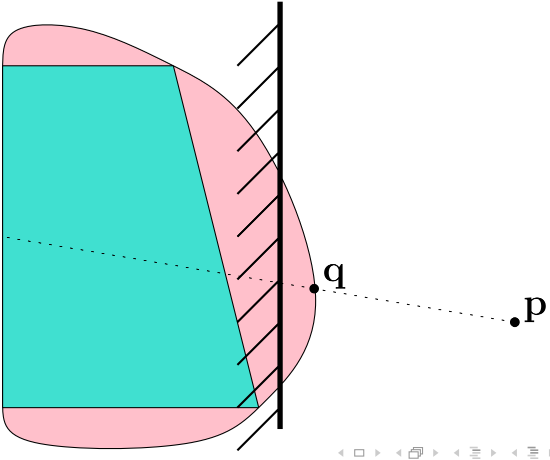
For B such that $|B(\ell)| \leq 1$ over $\mathcal{L}$ There exists B^* such that for all $\mathbf{p} \in \mathcal{C}$ such that $B(\mathbf{p}) \geq 1$, $B^*(\mathbf{p}) \geq \frac{1}{3}B(\mathbf{p}) - \frac{2}{3}$ and $|B(\ell)| \leq 1$ over $\mathcal{L}^\perp$



Ideas : replace aborts by local strategies (preserving locality), make corresponding Bell inequality with weights on aborts, remove aborts from said Bell inequality (MPRG'02)

Theorem (2, this work)

If a distribution $\mathbf{p} \in \mathcal{P}$ *is such that* $CC(\mathbf{p}) \geq \log(B(\mathbf{p})) = C$ *and* $QCC(\mathbf{p}) \leq Q$. *Then there exists* $\mathbf{q} \in \mathcal{Q}$ *with one additional output per player compared to the distribution* $\mathbf{p}$ *such that* $B(\mathbf{q}) \geq 2^{C-2Q}$



Application to some communication problems

Problem	Normalized Bell violations [1]	Inefficiency-resistant Bell violations (this work)
VSP [23]	$\Omega\left(\sqrt[6]{n}/\sqrt{\log n}\right)$	$2^{\Omega(\sqrt[3]{n})-O(\log n)}$
DISJ [456]	N/A	$2^{\Omega(n)-O(\sqrt{n})}$
TRIBES [78]	N/A	$2^{\Omega(n)-O(\sqrt{n}\log^2 n)}$
ORT [98]	N/A	$2^{\Omega(n)-O(\sqrt{n}\log n)}$

[1] BCG'16 [2] Raz'99 [3] KR'11 [4] Razb'92 [5] Razb'03 [6] AA'05 [7] JKS'03 [8] BCW'98 [9] She'12

Maximal violations for inefficiency-resistant Bell inequalities

Parameter	Upper bound	Lower bounds
# inputs N	N	$\Omega(N)$
# outputs K	$2^{O(\frac{K^4}{\epsilon^2}\log^2(K))}$	$\infty(\epsilon = 0)$
Dimension d	$2^{O((\frac{Kd}{\epsilon})^2\log^2(K))}$	?

Very sensitive to arbitrary noise, less so to other noise models.
Uses much less entanglement than (BCG'+16).
Results are quantitatively incomparable.

Thank you !

Why inefficiency-resistant Bell inequalities are normalized

How to get arbitrary violations with normalized Bell inequalities

$\tilde{B} = M \cdot B + \frac{M-1}{\#\mathcal{X}\mathcal{Y}}$

A simple example where this fails for inefficiency-resistant Bell inequalities

- $B_{0,0,0,0} = 1$
- $B_{a,b,x,y} = 0$ for $(a, b, x, y) \neq (0, 0, 0, 0)$

$\forall \mathbf{p} \in \mathcal{P},\ |B(\mathbf{p})| \leq 1$ $\tilde{B}(\ell_{(0,0)\to(0,0)}) = M - \frac{M-1}{\#\mathcal{X}\mathcal{Y}}$