On Non-Locality Distillation

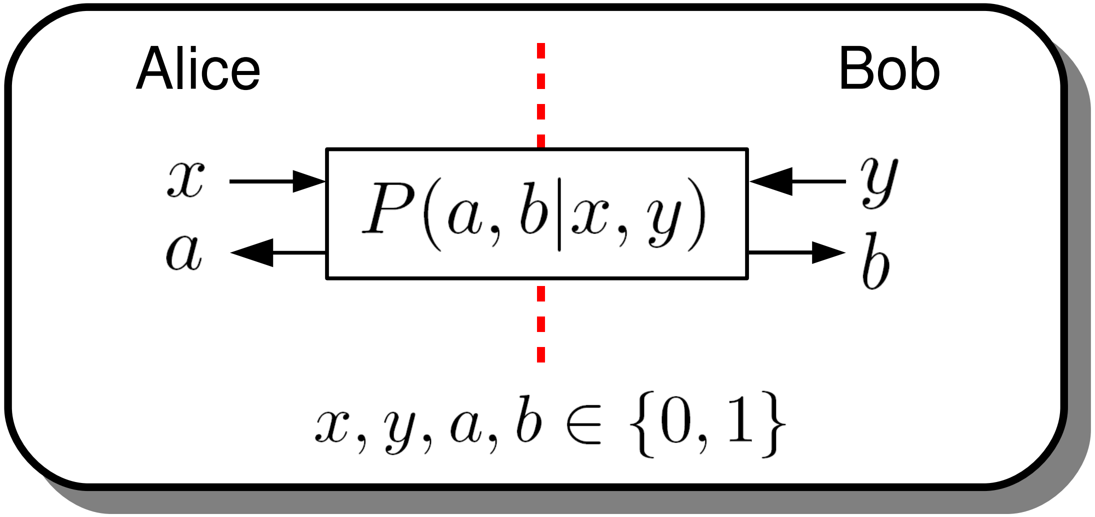
Dejan D. Dukaric, ETH Zurich

joint work with

Manuel Forster, ETH Zurich
Severin Winkler, ETH Zurich
Stefan Wolf, ETH Zurich

QIP, January 16, 2009, Santa Fe

Non-Signalling Systems



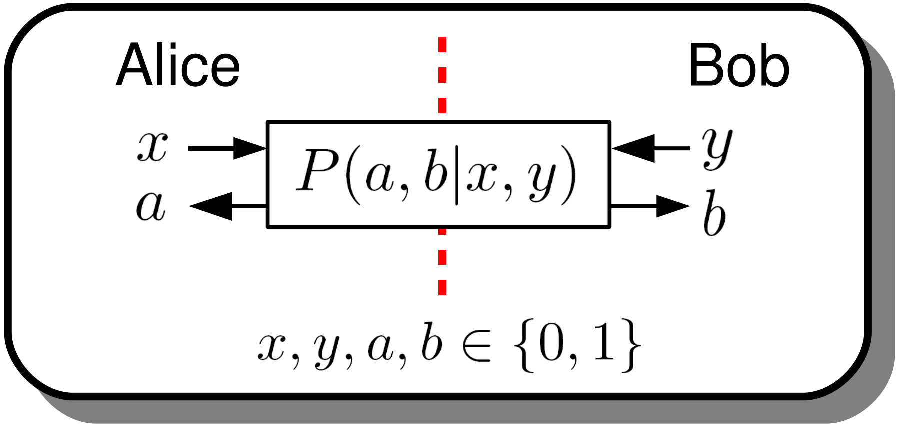
A system $P(a,b|x,y)$ is ....

- ... **local** if it can be simulated with shared randomness
- ... **non-signalling** if

$$\sum_{b\in\{0,1\}} P(a,b|x,y) \quad = \quad P(a|x) \ , \ \forall a,x,y \in \{0,1\}$$

$$\sum_{a\in\{0,1\}} P(a,b|x,y) \quad = \quad P(b|y) \ , \ \forall b,x,y \in \{0,1\}$$

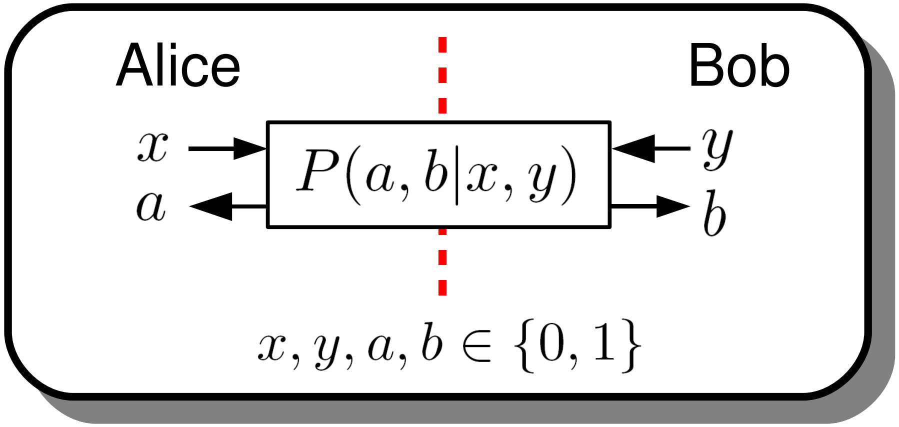
CHSH Non-Locality



Non-locality of $P(a,b|x,y)$: $NL[P] := \sum_{x,y\in\{0,1\}} \frac{1}{4} \cdot \Pr[x \wedge y = A \oplus B]$

$NL[P] :=$ “how well Alice and Bob can compute $x \wedge y = a \oplus b$ using $P(a,b|x,y)$, local operations and shared randomness, given the input is uniformly distributed”

CHSH Non-Locality

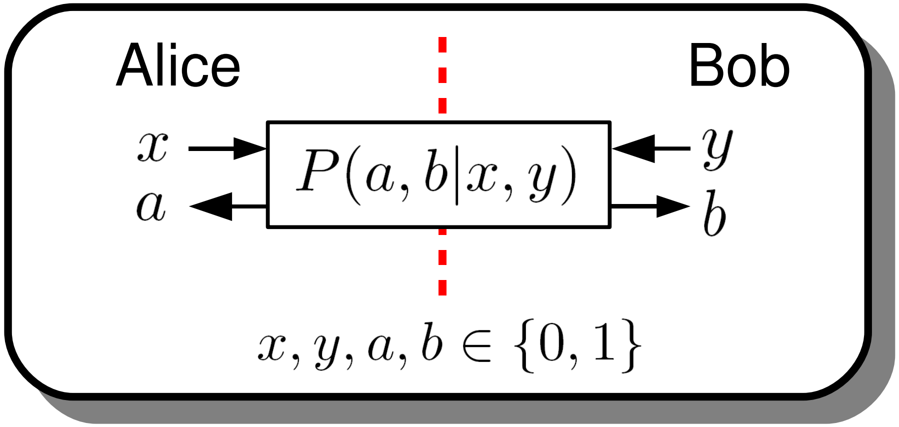


Non-locality of $P(a,b|x,y)$: $NL[P] := \sum_{x,y\in\{0,1\}} \frac{1}{4} \cdot \Pr[x \wedge y = A \oplus B]$

P **non-local** $\Leftrightarrow NL[P] > 3/4$

(Bell, 1964 / CHSH, 1969)

CHSH Non-Locality



Non-locality of $P(a,b|x,y)$: $NL[P] := \sum_{x,y\in\{0,1\}} \frac{1}{4} \cdot \Pr[x \wedge y = A \oplus B]$

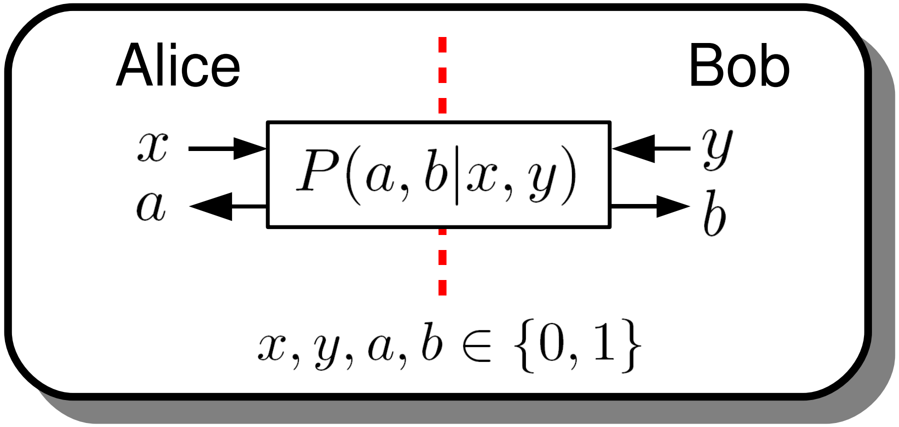
P **non-local** $\Leftrightarrow NL[P] > 3/4$

(Bell, 1964 / CHSH, 1969)

Achieving $NL[P] = 3/4$ **locally**:

- Alice sets $a = 0$ independent of input
- Bob sets $b = 0$ independent of input
- They compute with **certainty** the right relation ($x \wedge y = a \oplus b$) for inputs $x = 0, y = 0$ | $x = 0, y = 1$ | $x = 1, y = 0$

CHSH Non-Locality



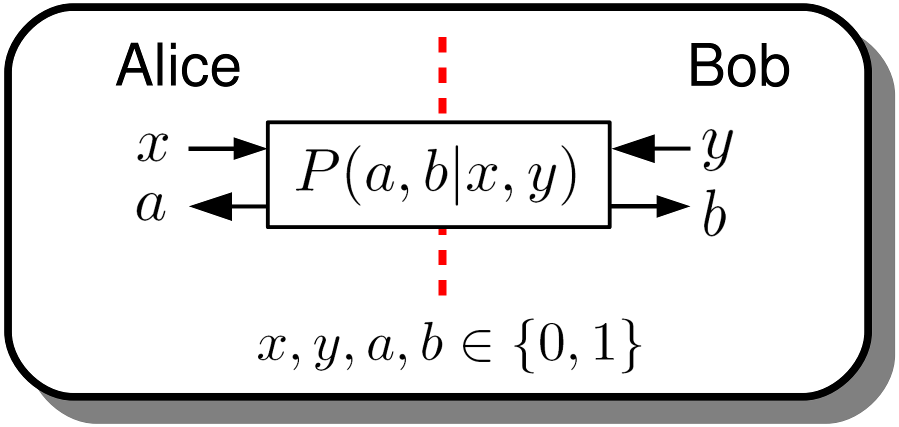
Non-locality of $P(a,b|x,y)$: $NL[P] := \sum_{x,y \in \{0,1\}} \frac{1}{4} \cdot \Pr[x \wedge y = A \oplus B]$

P **non-local** $\Leftrightarrow NL[P] > 3/4$

P **quantum** $\Rightarrow NL[P] \lessapprox 0.85$

(Tsirelson, 1980)

CHSH Non-Locality



Alice

Bob

x a $P(a,b|x,y)$ y b

$x, y, a, b \in \{0,1\}$

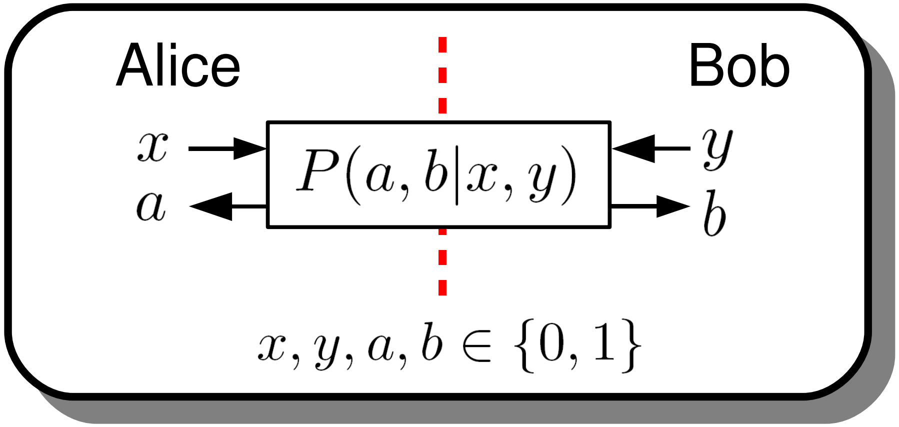
Non-locality of $P(a,b|x,y)$: $NL[P] := \sum_{x,y\in\{0,1\}} \frac{1}{4} \cdot \Pr[x \wedge y = A \oplus B]$

P **non-local** $\Leftrightarrow NL[P] > 3/4$

P **PR-box** $\Leftrightarrow NL[P] = 1$

P **quantum** $\Rightarrow NL[P] \lessapprox 0.85$

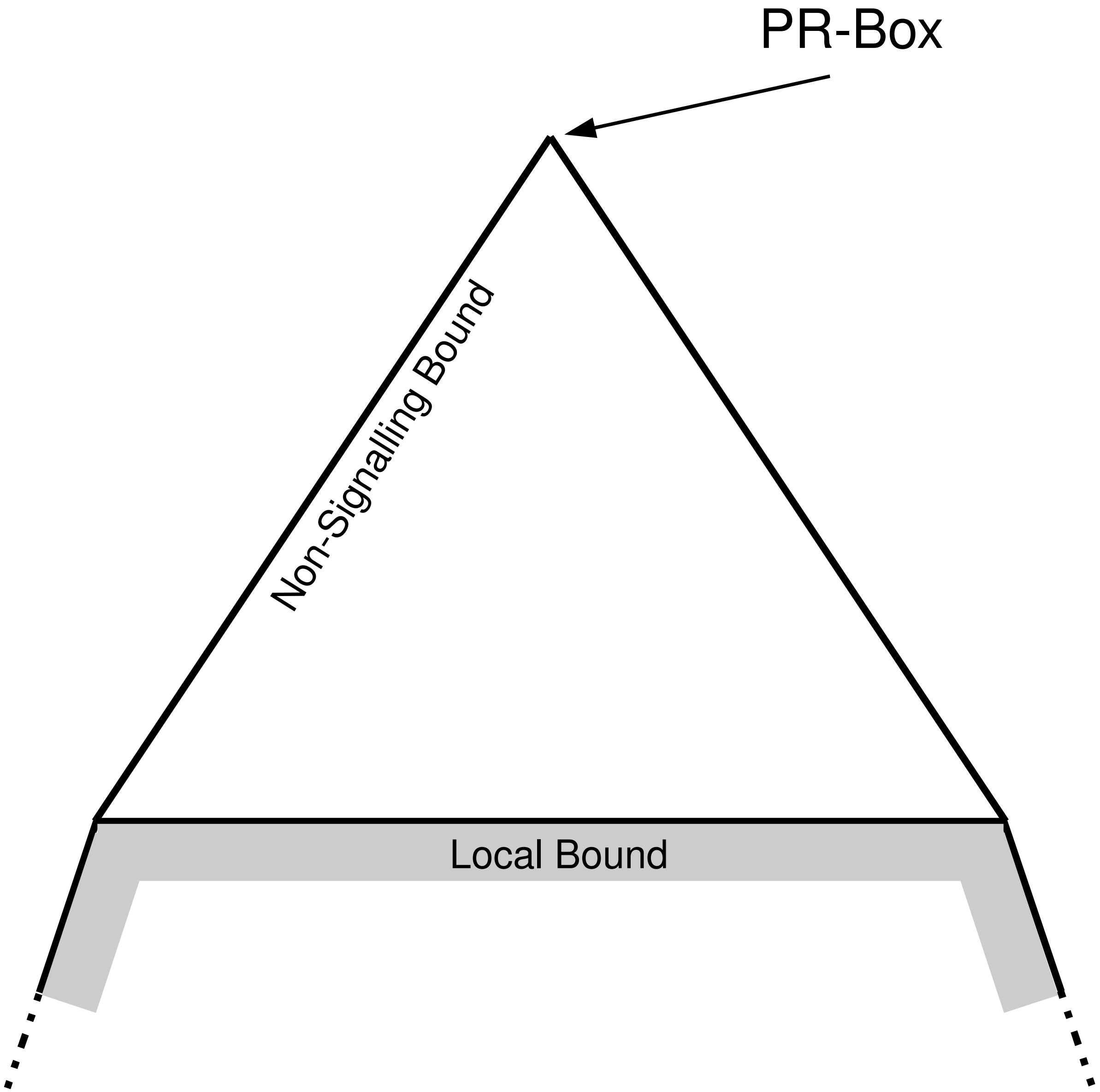
CHSH Non-Locality



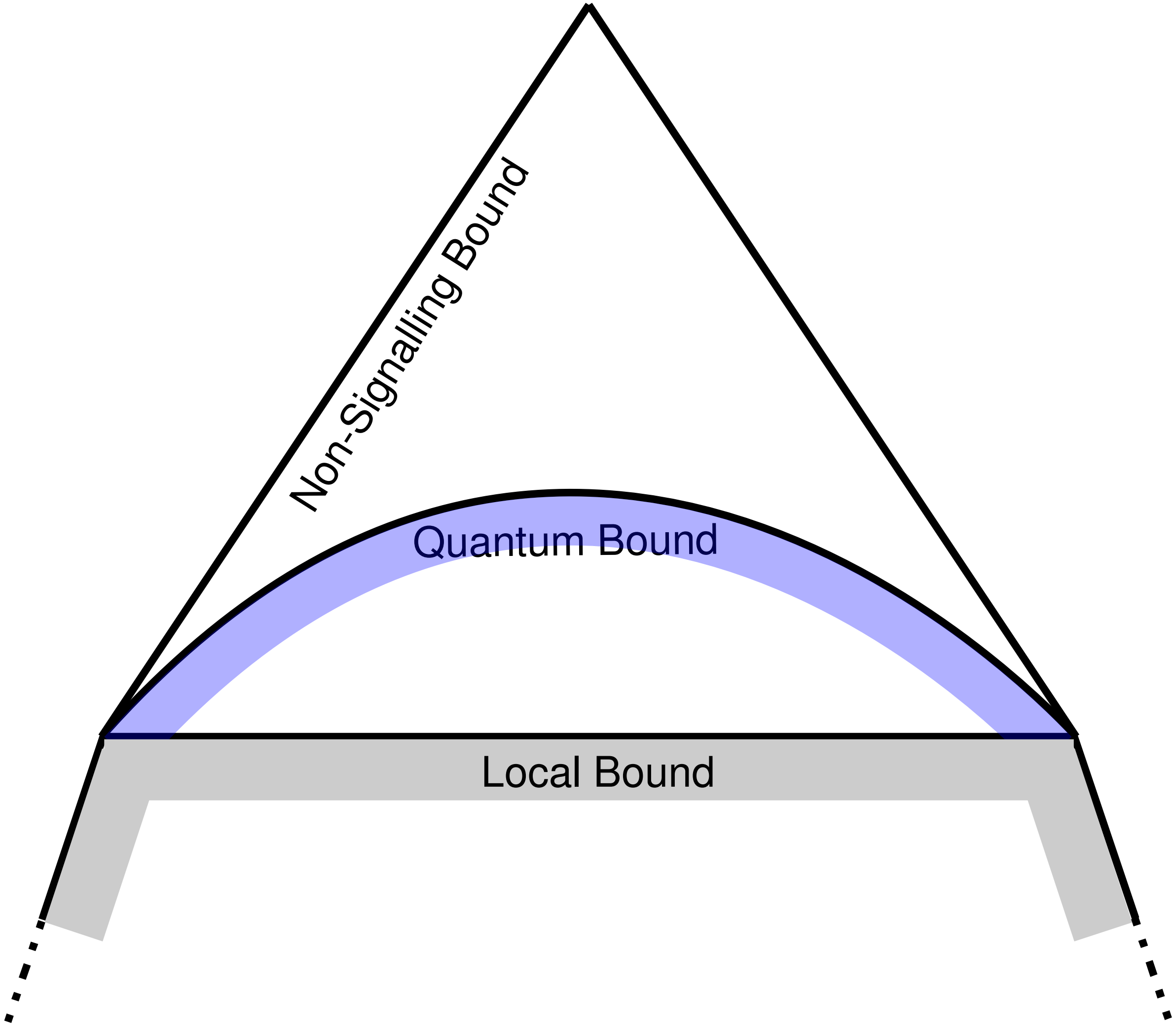
Non-locality of $P(a,b|x,y)$: $NL[P] := \sum_{x,y\in\{0,1\}} \frac{1}{4} \cdot \Pr[x \wedge y = A \oplus B]$

P **non-local** $\Leftrightarrow NL[P] > 3/4$	P **PR-box** $\Leftrightarrow NL[P] = 1$
P **quantum** $\Rightarrow NL[P] \lessapprox 0.85$	P **isotropic** $\Leftrightarrow$ $\Pr[x \wedge y = A \oplus B] = p\ ,\ \forall x,y \in \{0,1\}$ and $P(a|x) = P(b|y) = 1/2$

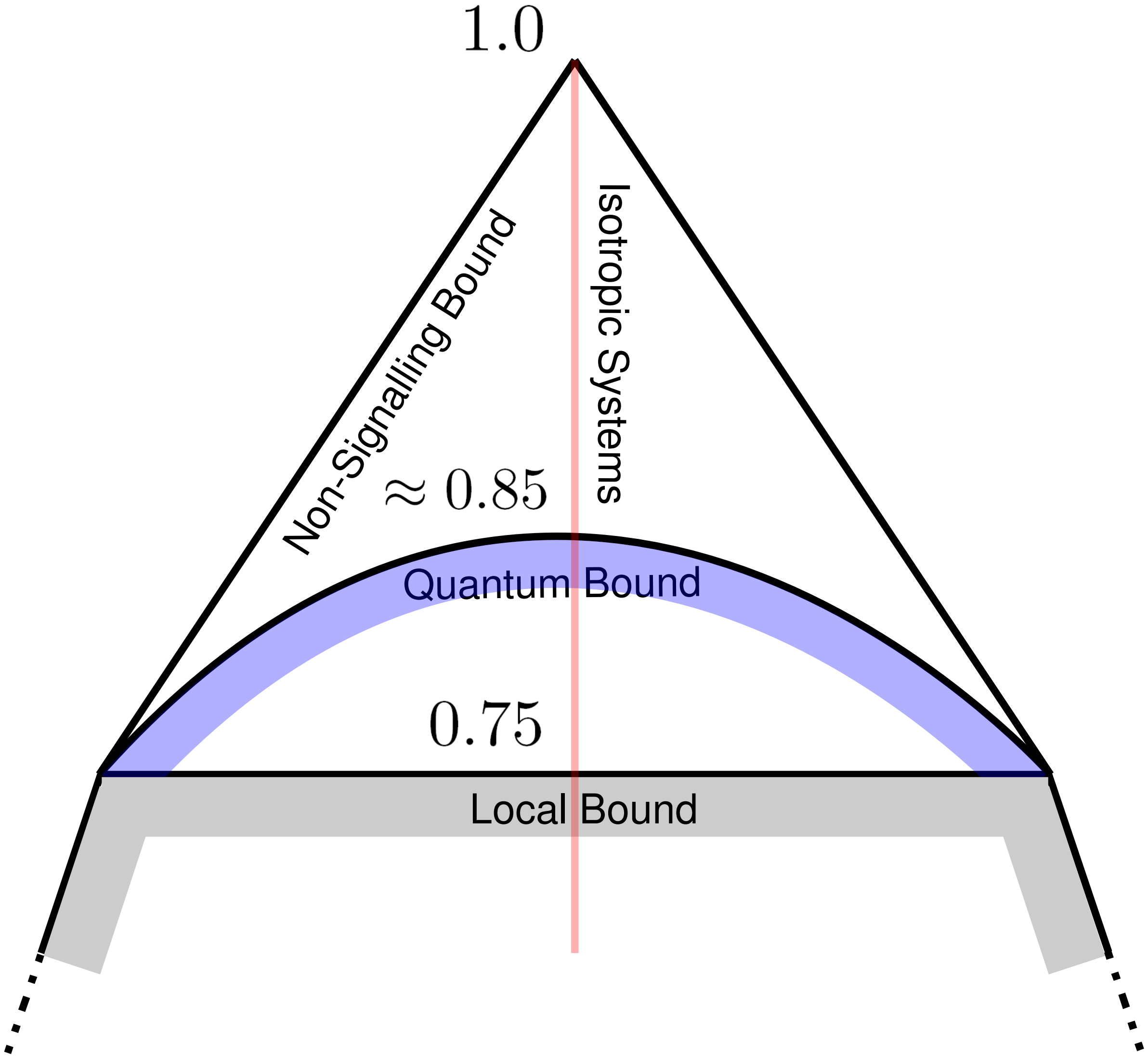
Non-Signalling Polytope



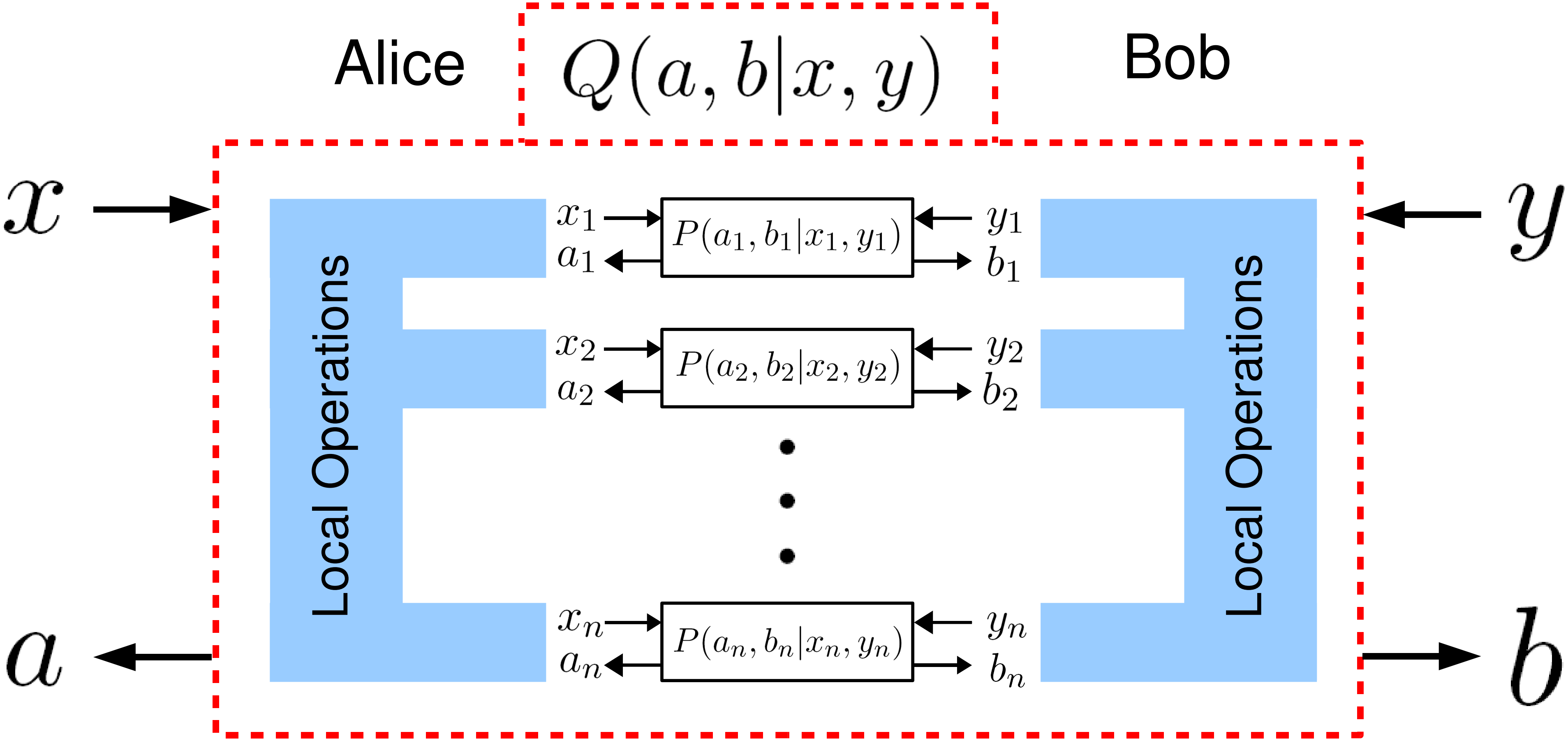
Non-Signalling Polytope



Non-Signalling Polytope

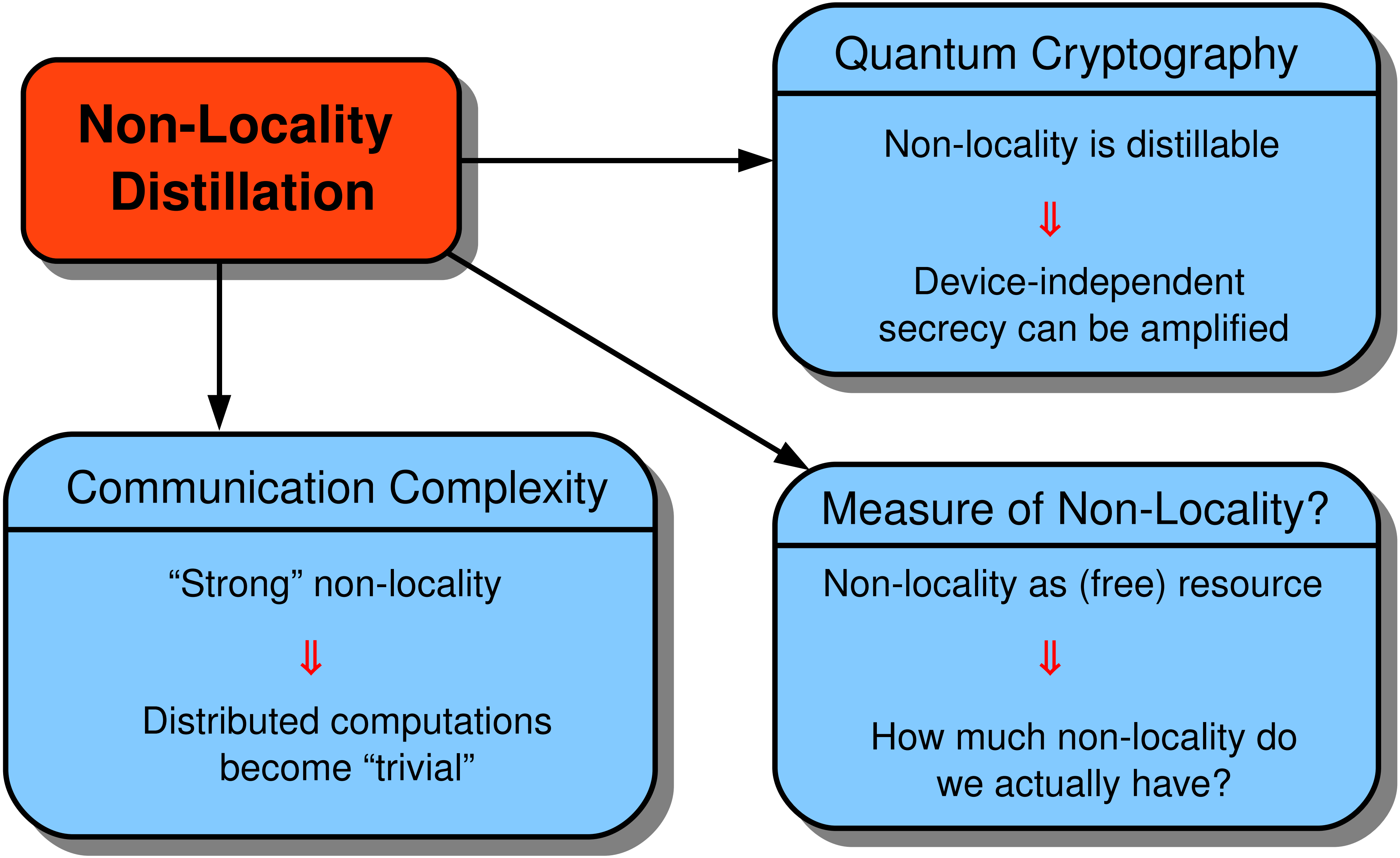


Non-Locality Distillation



Goal: $NL[Q] > NL[P]$

Motivation: Why considering non-locality distillation?



Non-Locality Distillation

Quantum Cryptography

Non-locality is distillable

⇓

Device-independent
secrecy can be amplified

Communication Complexity

“Strong” non-locality

⇓

Distributed computations
become “trivial”

Measure of Non-Locality?

Non-locality as (free) resource

⇓

How much non-locality do
we actually have?

Known Results about Non-Locality Distillation

Impossibility Results

⇒ Bell's bound (“no non-locality from locality”)

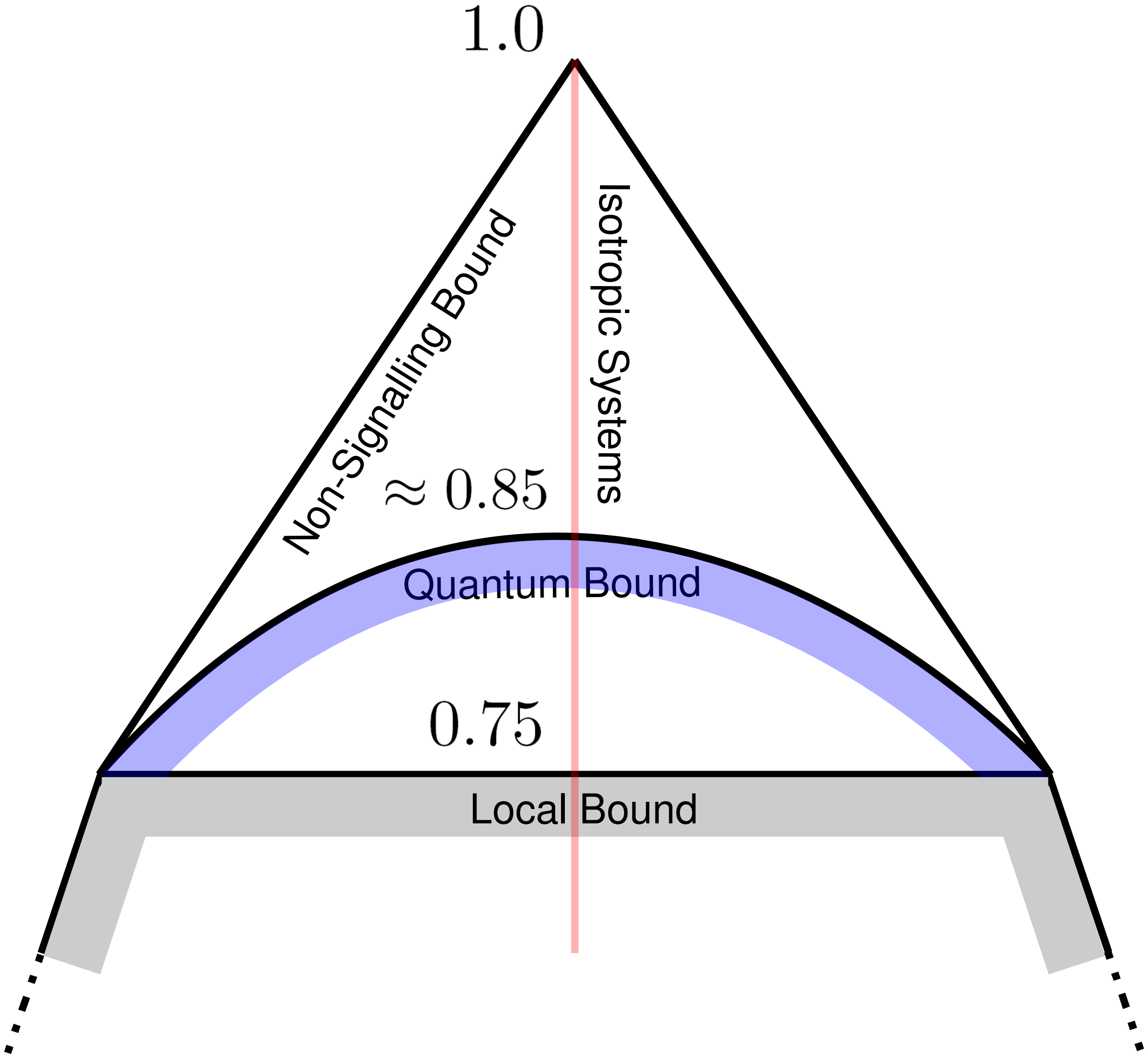
⇒ Tsirelson's bound (“no non-quantum from quantum”)

⇒ No non-locality distillation from two isotropic systems (Short, 2008)

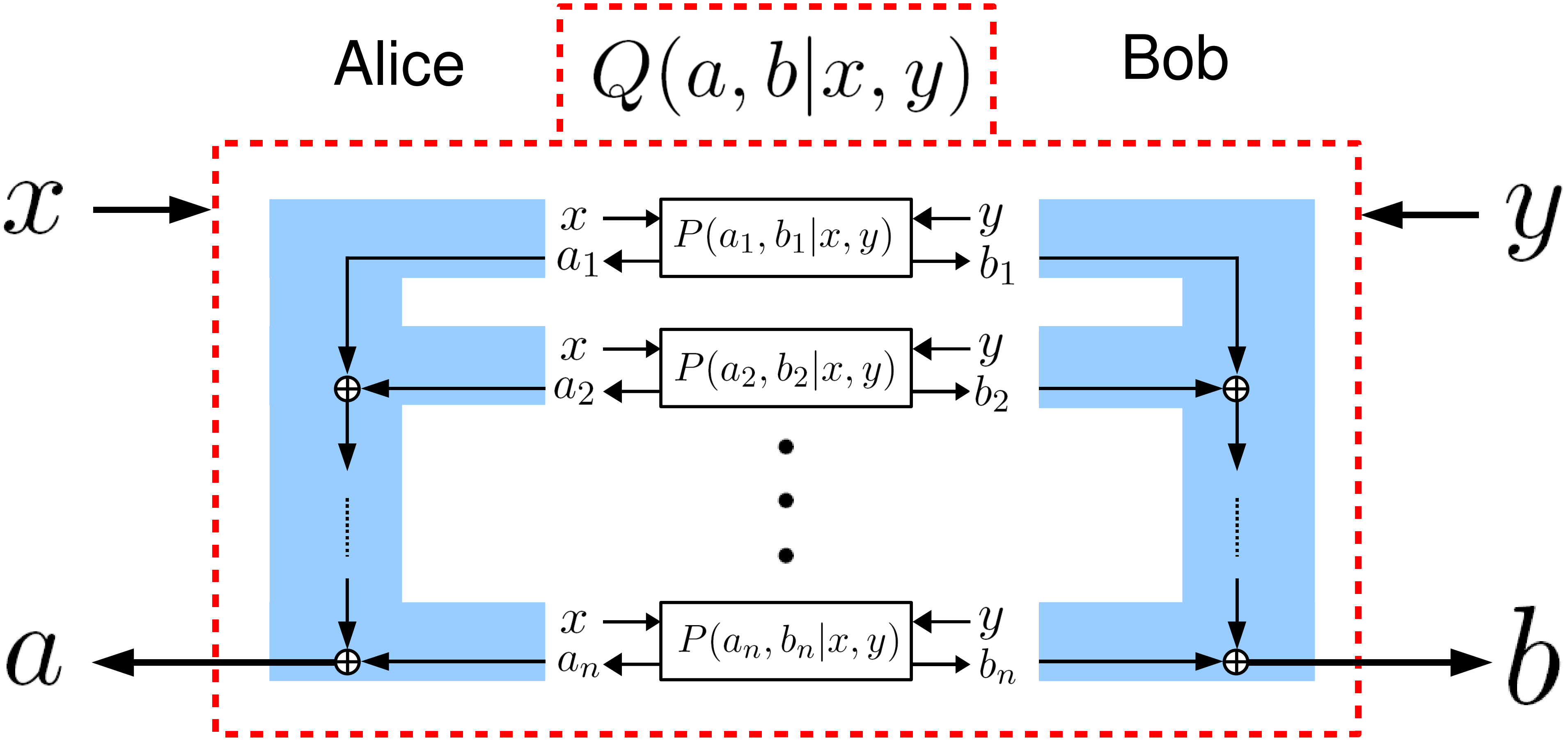
Possibility Results

⇒ none!

Non-Signalling Polytope

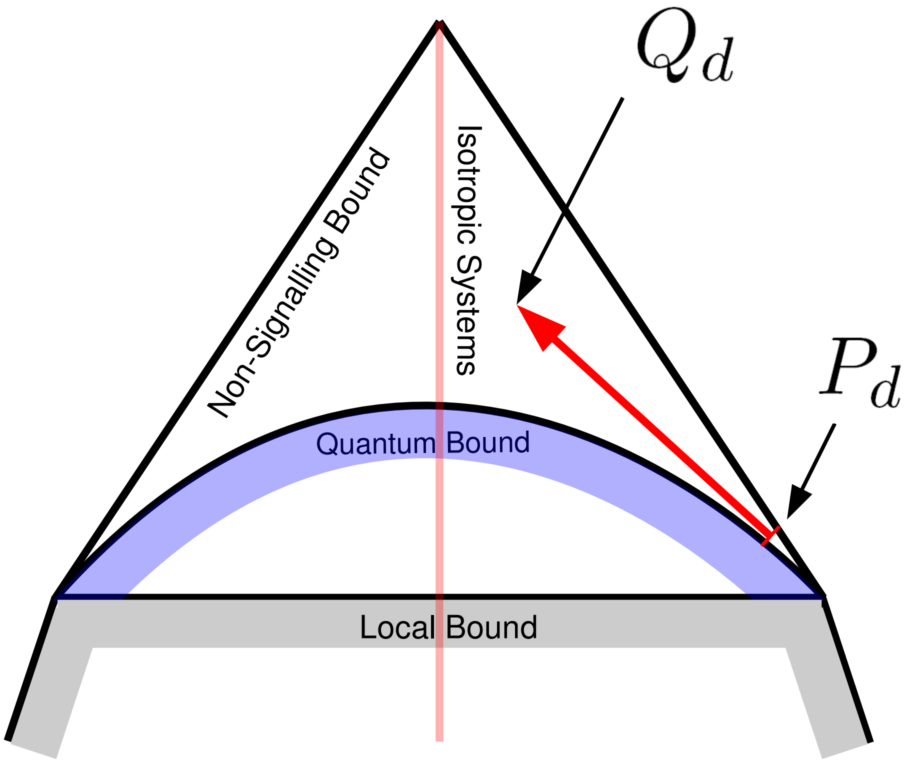


Non-Locality Distillation Protocol



Claim: There exists P such that $NL[Q] > NL[P]$

Distillable System



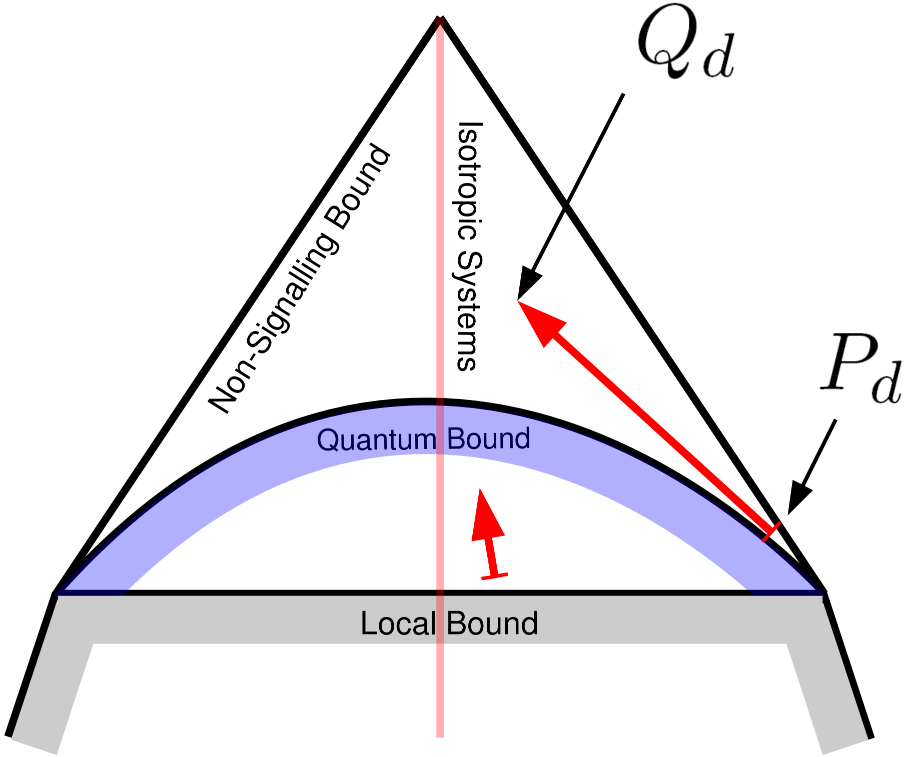
P_d		a, b			
		$0, 0$	$0, 1$	$1, 0$	$1, 1$
x, y	$0, 0$	$1/2$	0	0	$1/2$
	$0, 1$	$1/2$	0	0	$1/2$
	$1, 0$	$1/2$	0	0	$1/2$
	$1, 1$	$1/2 - \varepsilon$	ε	ε	$1/2 - \varepsilon$

Q_d		a, b			
		$0, 0$	$0, 1$	$1, 0$	$1, 1$
x, y	$0, 0$	$1/2$	0	0	$1/2$
	$0, 1$	$1/2$	0	0	$1/2$
	$1, 0$	$1/2$	0	0	$1/2$
	$1, 1$	$1/4$	$1/4$	$1/4$	$1/4$

$$NL[P_d] = 0.75 + \varepsilon/2$$

$$NL[Q_d] = 0.875$$

Distillable System



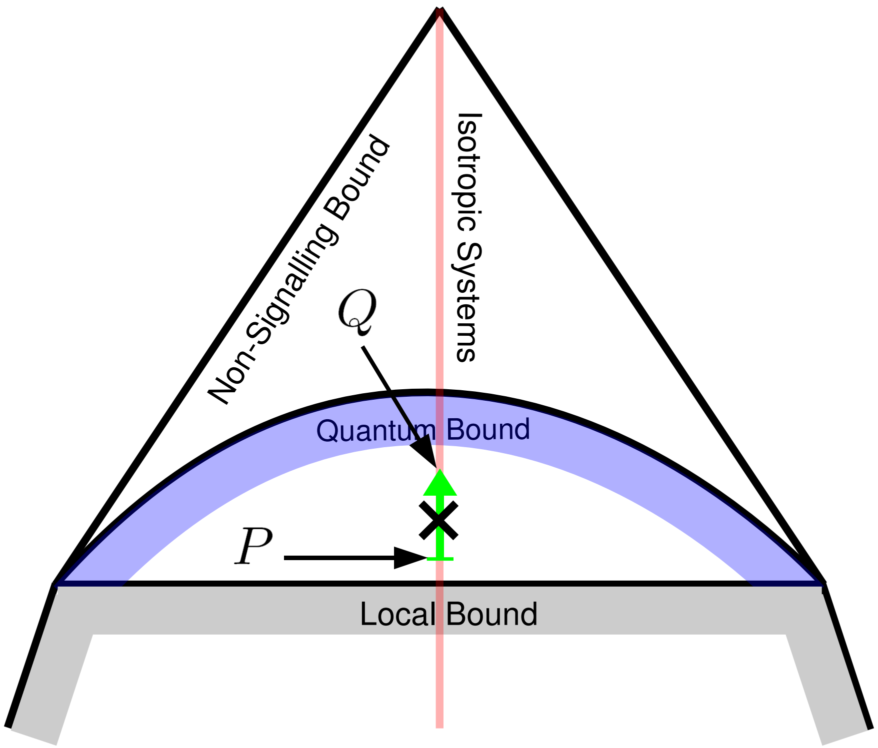
$$NL[P_d] = 0.75 + \varepsilon/2$$

$$NL[Q_d] = 0.875$$

		a, b			
P_d		$0, 0$	$0, 1$	$1, 0$	$1, 1$
x, y	$0, 0$	$1/2$	0	0	$1/2$
	$0, 1$	$1/2$	0	0	$1/2$
	$1, 0$	$1/2$	0	0	$1/2$
	$1, 1$	$1/2 - \varepsilon$	ε	ε	$1/2 - \varepsilon$

		a, b			
Q_d		$0, 0$	$0, 1$	$1, 0$	$1, 1$
x, y	$0, 0$	$1/2$	0	0	$1/2$
	$0, 1$	$1/2$	0	0	$1/2$
	$1, 0$	$1/2$	0	0	$1/2$
	$1, 1$	$1/4$	$1/4$	$1/4$	$1/4$

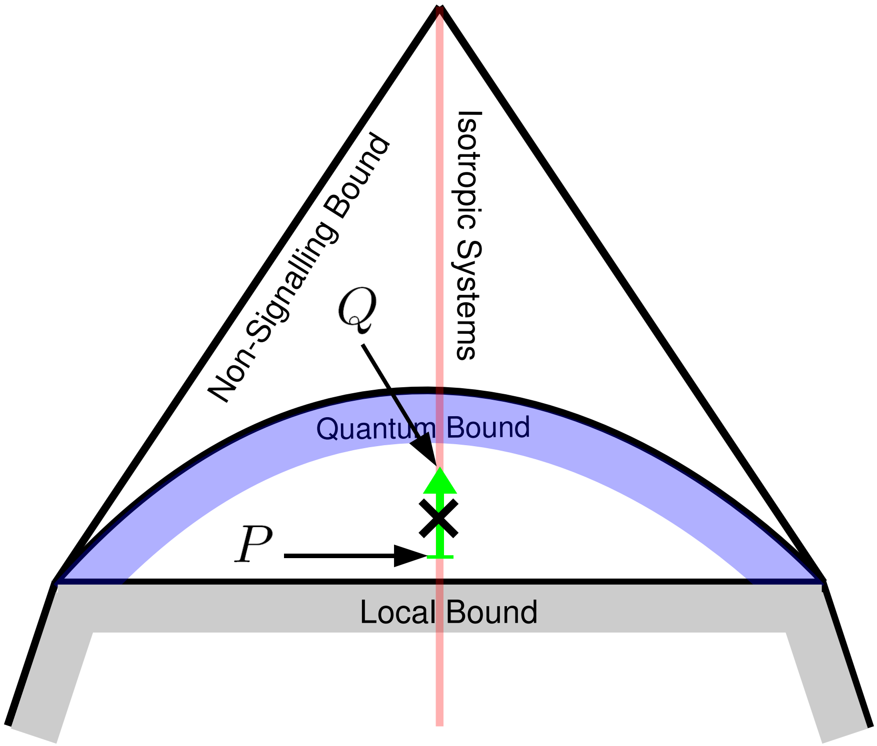
Limited Distillability for Isotropic Quantum Systems

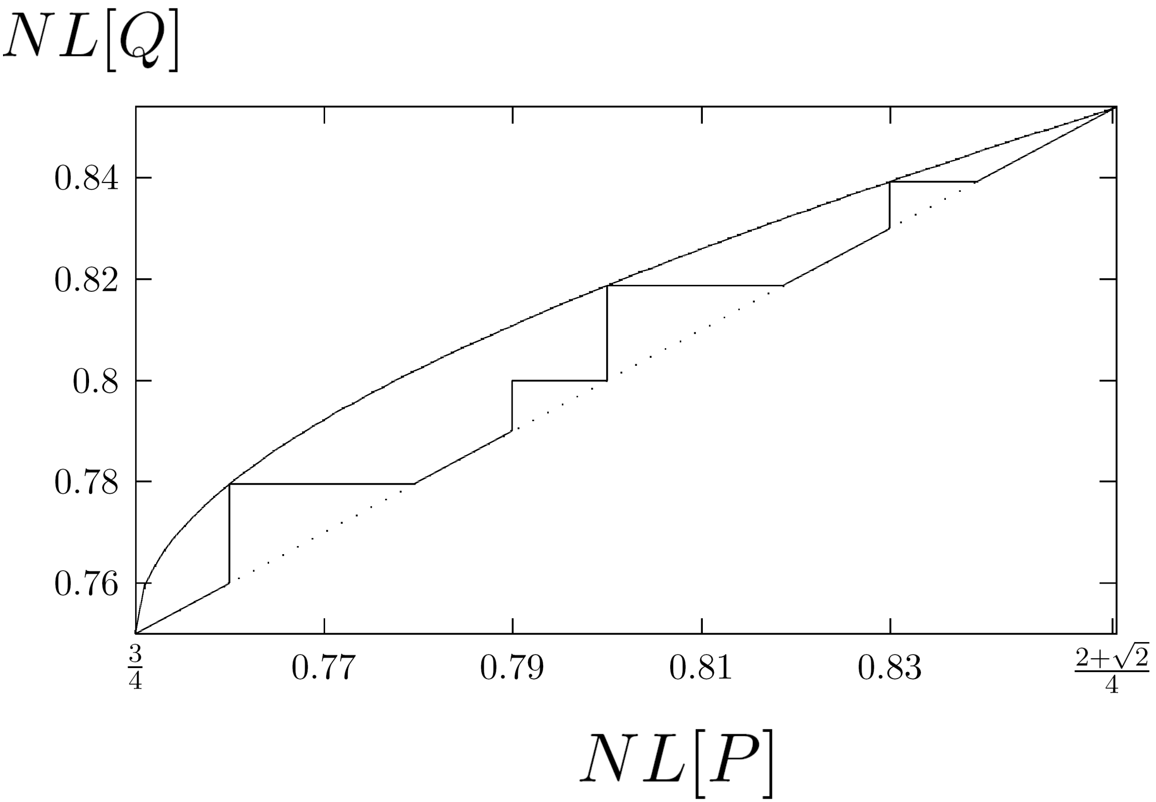


<u>Proof Idea</u>:

1. Simulate distillation circuit by quantum circuit by measuring certain mixed entangled states.
2. Show that there is **no** non-interactive entanglement distillation protocol for these mixed entangled states.
3. As non-locality and entanglement are different resources we lose something, the “gap”.

Limited Distillability for Isotropic Quantum Systems





Proof Idea:

1. Simulate distillation circuit by quantum circuit by measuring certain mixed entangled states.
2. Show that there is **no** non-interactive entanglement distillation protocol for these mixed entangled states.
3. As non-locality and entanglement are different resources we lose something, the “gap”.

Conclusions and Open Problems

- There exists distillable quantum and non-quantum non-locality
- Isotropic quantum non-locality at most limitedly distillable
- Infinite number of non-distillable isotropic systems

- Can isotropic systems be distilled at all?
- CHSH non-locality “right” measure of non-locality?

Any Questions?

For more information see: arXiv:0808.3317 + arXiv:0809.3173