Implausible Consequences

of Superstrong Nonlocality

Daniel Busch

July 4, 2016

Review

- CHSH inequality tells us, that $\langle \mathcal{B} \rangle \leq 2$ for realistic and local theories

Review

- CHSH inequality tells us, that $\langle \mathcal{B} \rangle \leq 2$ for realistic and local theories
- Violated by a value of $2\sqrt{2}$ in quantum mechanics

Review

- CHSH inequality tells us, that $\langle \mathcal{B} \rangle \leq 2$ for realistic and local theories
- Violated by a value of $2\sqrt{2}$ in quantum mechanics
- This is the maximal theoretical violation (Cirel'son's bound) and also proven by experiments

Review

- CHSH inequality tells us, that $\langle \mathcal{B} \rangle \leq 2$ for realistic and local theories
- Violated by a value of $2\sqrt{2}$ in quantum mechanics
- This is the maximal theoretical violation (Cirel'son's bound) and also proven by experiments
- Question: Why is the violation of CHSH not bigger, although a value of 4 would be perfectly possible without permitting signaling (nonlocal boxes)?

Nonlocal boxes

Definition: nonlocal boxes

Let a and b be uniformly distributed bits. Let further x and y be arbitrary bits. A nonlocal box then is a theoretical device (one-shot) having input and output ports at two spacelike separated locations A and B with $A(x) = a$ and $B(y) = b$ such that $a + b \equiv_2 x \cdot y$ ($\Leftrightarrow a \oplus b = x \wedge y$). ($\equiv_2$ denotes congruency modulo 2)

This definition of nonlocal boxes is equivalent to the nonlocal boxes contstructed by Popescu and Rohrlich. One can see this by interpreting the observables A_1, B_1 as logic 0 respectively A_2, B_2 as logic 1 at each location and the measurement outcomes -1 as a logic 0 respectively $+1$ as a logic 1 in the table below.

Nonlocal boxes

		A_1		A_2	
		-1	$+1$	-1	$+1$
B_1	-1	$1/2$	0	$1/2$	0
	$+1$	0	$1/2$	0	$1/2$
B_2	-1	$1/2$	0	0	$1/2$
	$+1$	0	$1/2$	$1/2$	0

We also see here, that the CHSH inequality reaches its algebraic maximum in terms of nonlocal boxes:

$$\begin{aligned}\langle \mathcal{B} \rangle &= \langle A_1 \otimes B_1 \rangle + \langle A_1 \otimes B_2 \rangle + \langle A_2 \otimes B_1 \rangle - \langle A_2 \otimes B_2 \rangle \\ &= 1 + 1 + 1 - (-1) = 4 \nleq 2\end{aligned}$$

Communication complexity

Definition: communication complexity

The communication complexity of a function $f : \{0,1\}^n \times \{0,1\}^n \to 0,1$ is defined as the worst case amount of bits needed to distributively compute $f(x,y)$. More formal:

$$C(f) = \min_{\text{Protocol } P} \max_{x,y \in \{0,1\}^n} f(x,y)$$

Note that $C(f) \leq n$, because Bob can always send his complete input to Alice and let her calculate the result.

Communication complexity

Definition: trivial communication complexity

We call the communication complexity of f trivial, if $C(f) \leq 1$.

Boolean functions as multi-variable polynomials

Definition: inner product

The inner product function $\mathrm{IP}_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ is defined by

$$\mathrm{IP}_n(x_1 \cdots x_n, y_1 \cdots y_n) = \sum_{i=1}^{n} x_i \cdot y_i.$$

As there is no possible way of omitting a single bit when calculating the result of this function, we have $C(\mathrm{IP}_n) = n$.

Remark

Given quantum entanglement, the communication complexity of IP_n remains the same, while there are other functions, that can be computed with less classical communication.

Boolean functions as multi-variable polynomials

Lemma

Every boolean function can be represented as a multi-variable polynomial $f(x_1 \cdots x_n, y_1 \cdots y_n)$ in $\mathbb{F}_2[x]$.

Because we construct every boolean function with the compositions $\wedge$ and $\vee$, it is sufficient to show, that we can express these basic compositions by polynomials. This can be easily done in the following way:

$$x \wedge y \equiv_2 x \cdot y \text{ and}$$
$$x \vee y \equiv_2 x + y + x \cdot y$$

Boolean functions as multi-variable polynomials

Lemma

Every multi-variable polynomial $f(x_1 \cdots x_n, y_1 \cdots y_n) \in \mathbb{F}_2[x]$ can be written as

$$\sum_{i=1}^{2^n} P_i(x_1 \cdots x_n) Q_i(y_1 \cdots y_n),$$

where $P_i, Q_i \in \mathbb{F}_2[x]$ and Q_i are monomials, hence

$$Q_i(y_1 \cdots y_n) = \prod_{j \in S_i} y_j \text{ with } S_i \subseteq \{1, \dots, n\}.$$

Of course we can factor out all monomials in $y_1, \dots, y_n$ such that $f(x_1 \cdots x_n, y_1 \cdots y_n) = P_1(x_1 \cdots x_n) y_1 + \cdots + P_{2^n}(x_1 \cdots x_n) y_1 \cdots y_n$, which essentially is the statement given above, because the amount of possible monomials is bounded by the amount of subsets S_i, thus 2^n.

Boolean functions as multi-variable polynomials

Example: Let's have a look at the 2-bit equality function.

$$\mathrm{EQ}(x_1 x_2, y_1 y_2) = \ (x_1 \Leftrightarrow y_1) \wedge (x_2 \Leftrightarrow y_2)$$

Boolean functions as multi-variable polynomials

Example: Let's have a look at the 2-bit equality function.

$$\begin{aligned}\mathrm{EQ}(x_1x_2, y_1y_2) &= (x_1 \Leftrightarrow y_1) \wedge (x_2 \Leftrightarrow y_2) \\ &\equiv_2 (1 + x_1 + y_1) \cdot (1 + x_2 + y_2)\end{aligned}$$

Boolean functions as multi-variable polynomials

Example: Let's have a look at the 2-bit equality function.

$$
\begin{aligned}
\mathrm{EQ}(x_1x_2, y_1y_2) &= \ (x_1 \Leftrightarrow y_1) \wedge (x_2 \Leftrightarrow y_2) \\
&\equiv_2 (1 + x_1 + y_1) \cdot (1 + x_2 + y_2) \\
&\equiv_2 1 + x_2 + y_2 + x_1 + x_1x_2 + x_1y_2 + y_1 + y_1x_2 + y_1y_2
\end{aligned}
$$

Boolean functions as multi-variable polynomials

Example: Let's have a look at the 2-bit equality function.

$$
\begin{aligned}
\mathrm{EQ}(x_1x_2, y_1y_2) = \; & (x_1 \Leftrightarrow y_1) \wedge (x_2 \Leftrightarrow y_2) \\
\equiv_2 \; & (1 + x_1 + y_1) \cdot (1 + x_2 + y_2) \\
\equiv_2 \; & 1 + x_2 + y_2 + x_1 + x_1x_2 + x_1y_2 + y_1 + y_1x_2 + y_1y_2 \\
\equiv_2 \; & (1 + x_1 + x_2 + x_1x_2) \cdot 1 + (1 + x_2) \cdot y_1 + \\
& (1 + x_1) \cdot y_2 + 1 \cdot y_1y_2
\end{aligned}
$$

Boolean functions as multi-variable polynomials

Corollary

Regarding communication complexity, we can reduce every boolean function to the inner product.

Let $x_i' = P_i(x_1 \cdots x_n)$ and $y_i' = Q_i(y_1 \cdots y_n)$. This is possible, because Alice can precalculate P_i on her side and Bob Q_i respectively on his side. We then have, as desired:

$$g(x_1' \cdots x_{2^n}', y_1' \cdots y_{2^n}') = \sum_{i=1}^{2^n} x_i' \cdot y_i'$$

Consequences of superstrong nonlocality

Theorem

Assuming a theory, in which we can simulate (perfect) nonlocal boxes, the communication complexity of every boolean function becomes trivial.

As shown above, we can express every boolean function as an inner product:

$$\mathrm{IP}_n(x_1 \cdot x_n, y_1 \cdot y_n) = \sum_{i=1}^{n} x_i \cdot y_i .$$

Consequences of superstrong nonlocality

The correlation $a \oplus b = x \wedge y \iff a + b \equiv_2 x \cdot y$ now yields:

$$\begin{aligned} \mathrm{IP}_n(a_1 \cdots a_n, b_1 \cdots b_n) &= \sum_{i=1}^{n} a_i + b_i \\ &= \underbrace{\sum_{i=1}^{n} a_i}_{\substack{Alice's \\ part}} + \underbrace{\sum_{i=1}^{n} b_i}_{\substack{Bob's \\ part}} \\ &= \alpha + \beta \end{aligned}$$

To get the final result, Bob just has to transmit his bit β to Alice, so she can compute $\alpha + \beta$.

Conclusion

- Availability of perfect nonlocal boxes would cause every boolean function to have trivial communication complexity

Conclusion

- Availability of perfect nonlocal boxes would cause every boolean function to have trivial communication complexity
- Not conflicting with physical intuition, but...

Conclusion

- Availability of perfect nonlocal boxes would cause every boolean function to have trivial communication complexity
- Not conflicting with physical intuition, but...
- Implausible according to the experiences in complexity theory and general intuition of what computational complexity means

Conclusion

- Availability of perfect nonlocal boxes would cause every boolean function to have trivial communication complexity
- Not conflicting with physical intuition, but...
- Implausible according to the experiences in complexity theory and general intuition of what computational complexity means
- One interpretation of the fact, that quantum mechanics does not go beyond the value $\langle \mathcal{B} \rangle = 2\sqrt{2}$

Even stronger results

- Even with imperfect nonlocal boxes we can reach trivial communication complexity in a probabilistic sense

Even stronger results

- Even with imperfect nonlocal boxes we can reach trivial communication complexity in a probabilistic sense
- With nonlocal boxes of a success probability of $p = 90,8\%$ every boolean function can be computed correctly with $q > \frac{1}{2}$

Even stronger results

- Even with imperfect nonlocal boxes we can reach trivial communication complexity in a probabilistic sense
- With nonlocal boxes of a success probability of $p = 90,8\%$ every boolean function can be computed correctly with $q > \frac{1}{2}$
- This is the case for $\langle B \rangle > 2\sqrt{\frac{8}{3}}$

Even stronger results

- Even with imperfect nonlocal boxes we can reach trivial communication complexity in a probabilistic sense
- With nonlocal boxes of a success probability of $p = 90,8\%$ every boolean function can be computed correctly with $q > \frac{1}{2}$
- This is the case for $\langle B \rangle > 2\sqrt{\frac{8}{3}}$
- Proven by Brassard et al in 2006

Questions?

References I

[1] Sanjeev Arora. *Seminar in Algorithms and Complexity*. http://www.cs.princeton.edu/courses/archive/spr05/cos598B/.

[2] Gilles Brassard et al. "Limit on Nonlocality in Any World in Which Communication Complexity Is Not Trivial". In: *Physical Review Letters* (2006).

[3] Wim van Dam. "Implausible Consequences of Superstrong Nonlocality". In: *Natural Computing* (2005).