Combinatorics and Quantum Non Locality

Harry Buhrman
CWI
Univ. of Amsterdam
The Netherlands
Joint work with:
Serge Massar
Hein Röhrig
overview

• EPR pairs
• Bell $\rightarrow$ non locality
• Quantum Computing
• Non locality $\rightarrow$
  Quantum Communication Complexity
• Quantum Communication Complexity $\rightarrow$ Non locality
non locality
Non locality

• k (>1) parties
• each party \( i \) has
  - part of an entangled state \( |\varphi\rangle \)
  - receives input \( x_i \)
  - performs measurement \( M_{x_i} \)
  - outputs measurement value \( o_i \)
• Induces correlations:
  - \( P_Q(o_1...o_k \mid x_1...x_k) \)
• no communication!
Quantum Setup

$|0\rangle + |1\rangle$

EPR-pair

Alice

$M_{x_1}$

$O_1$

$X_1$

Bob

$M_{x_2}$

$O_2$

$X_2$

induces correlations:

$P_Q(o_1o_2 \mid x_1x_2)$
Non locality

• Question:
  - Can these correlations be reproduced classically?
Local hidden var. model

• Classical setup
• Each party has:
  - copy of random bits (shared randomness)
  - input $x_i$
  - Performs computation (protocol)
  - Outputs $o_i$
• Induces correlations:
  - $P_c(o_1...o_k \mid x_1...x_k)$
Classical Setup

$r_1 r_2 \ldots r_k$ shared randomness

Alice

$x_1$ computation

$y_1$ induces correlations:

$P_C(y_1 y_2 \mid x_1 x_2)$

Bob

$x_2$ computation
Non locality

• If for every protocol:
  - \( P_c(o_1...o_k \mid x_1...x_k) \neq P_Q(o_1...o_k \mid x_1...x_k) \)
  - Non locality

• Requires
  - State + measurements to obtain \( P_Q \)
  - Prove that for every classical lhv protocol:
    \( P_c(o_1...o_k \mid x_1...x_k) \neq P_Q(o_1...o_k \mid x_1...x_k) \)
Examples

• 2 parties:
  - EPR pair: \( \frac{1}{\sqrt{2}}[|00\rangle + |11\rangle] \)
  - Bell inequalities

• 3 parties
  - GHZ state: \( \frac{1}{\sqrt{2}}[|000\rangle + |111\rangle] \)
  - Mermin state: \( \frac{1}{2}[|001\rangle + |010\rangle + |100\rangle + |111\rangle] \)

• n parties
  \( \frac{1}{\sqrt{2}}[\underbrace{|0\cdots 0\rangle}_{n} + \underbrace{|1\cdots 1\rangle}_{n}] \)
Communication Complexity
Communication Complexity

Goal: Compute some function $F(x_1,x_2)$ minimizing communication bits.
Equality

Classical bits

\[ F(x_1, x_1) = 1 \text{ iff } x_1 = x_2 \]
Equality

Classical bits

$F(x_1, x_1) = 1$ iff $x_1 = x_2$

$|x_2| = n$ bits necessary and sufficient:

$C(EQ) = n$
Quantum Com. Complexity

Goal: Compute some function $F(x_1, x_2) \rightarrow \{0, 1\}$ minimizing communication bits.
EPR-pairs can reduce Com. Cost

- **Mermin nonlocality (3 parties):** \[CB'97\]
  - classical cost 4 bits
  - quantum cost 3 bits

- **Improvements:**
  - \( k \) parties \( k \text{ vs } k \log(k) \) \[BvDHT'99\]
  - incorporating quantum algorithms: \[BCW'98\]
    - 2 parties \( \log(n) \text{ vs } n \) (Deutsch-Jozsa)
    - 2 parties \( n^{1/2} \text{ vs } n \) (Grover)
  - few rounds, randomness, quantum lower bounds
    ...[R'99,KNTZ'00,K'00,ANTVW'99,JVS'01,HdeW'02,R'02...\]
EPR-pairs Can Reduce Cost

exponential gap [BCW’98]

\[ \text{EQ}'(x_1, x_2) = 1 \text{ iff } x_1 = x_2 \]

Promise \( \Delta(x_1, x_2) = n/2 \text{ or } 0 \)

- need \( \Omega(n) \) classical bits.
- can be done with \( \log(n) \) bits +EPR-pairs.
- Protocol: distributed Deutsch-Jozsa
non locality experiments
Quantum Setup

\[ |0 \rangle + \]

EPR-pair

\[ |1 \rangle \]

induces correlations:

\[ P_Q(o_1o_2 \mid x_1x_2) \]
Quantum Setup

$|0\rangle \rightarrow 0\rangle +$

$|1\rangle \rightarrow 1\rangle$

induces correlations:

$P_Q(o_1 o_2 \mid x_1 x_2)$
Quantum Setup

\[ |0 \rangle \rightarrow EPR\text{-}pair \rightarrow |1 \rangle \]

\( x_1M_{x_1}o_1 \) induces correlations:

\[ P_Q(o_1o_2 \mid x_1x_2) \]
• sometimes detector(s) don’t click
  - Alice and/or Bob don’t have an output
  - can only test correlations when both Alice and Bob have an output
• Classical non clicking:
  - classical lhv protocol sometimes no output
  - only check whenever there is an output
• \( \eta = \text{detector efficiency} = \text{prob. of clicking} \)
  - small \( \eta \) allows for lhv protocols
example

shared randomness

\[ \eta = 2^{-k} \]

correlation

\[ P(o | xy) \]

- if \( y_1 \ldots y_k \neq r_{k+1} \ldots r_{2k} \) ➔ No Click
- if \( y_1 \ldots y_k = r_{k+1} \ldots r_{2k} \)
  assume \( x = r_1 \ldots r_k \)
  output \( P(o_1 | xy) \)

- if \( x_1 \ldots x_k \neq r_1 \ldots r_k \) ➔ No Click
- if \( x_1 \ldots x_k = r_1 \ldots r_k \)
  assume \( y = r_{k+1} \ldots r_{2k} \)
  output \( P(o_2 | xy) \)
detection loophole

- All experiments that show non locality have $\eta$ such that a lhv model exist!
- Solution:
  - Design tests that allow small $\eta$
  - Test also useful to test devices that claim to behave non local (eg quantum crypto)
- No good tests known
\( \eta^* \)

definition

\( \eta^* \) is the maximum detector efficiency for which a lhv model exists.

Goal:

- design correlation problem/test
- prove upper bounds on \( \eta^* \)
from quantum communication complexity back to non locality
Monochromatic rectangles

- $X_1, X_2$ set of inputs for Alice and Bob
- Rectangle $R = A \times B$, $A \subseteq X_1$ & $B \subseteq X_2$
- $R$ is $a$-monochromatic if
  - for all $(x_1, x_2) \in R : F(x_1, x_2) = a$

- $R_a = \max \{ R \mid R \text{ is } a\text{-monochr.}\}$
- $|R_a|$ yields lower bound on $C(F)$
Monochromatic rectangles

- \(X_1, X_2\) set of inputs for Alice and Bob
- Rectangle \(R = A \times B, A \subseteq X_1 \land B \subseteq X_2\)
- \(R\) is \(a\)-monochromatic if
  - for all \((x_1, x_2) \in R \cap D: F(x_1, x_2) = a\)
- \(D\) = set of promise inputs
- \(R_a = \max \{R \cap D \mid R\text{ is } a\text{-monochr.}\}\)
- \(|R_a|\) yields lower bound on \(C(F)\)
set of inputs that have \( a \) as output

\[
C(F) \geq \log \left( \frac{D_a}{R_a} \right)
\]
EPR-pairs Can Reduce Cost

exponential gap \([BCW'98]\)

\[ \text{EQ}'(x_1, x_2) = 1 \text{ iff } x_1 = x_2 \]

Promise \(\Delta(x_1, x_2) = n/2 \text{ or } 0\)

- need \(\Omega(n)\) classical bits.
- can be done with \(\log(n)\) bits +EPR-pairs.
- Protocol: distributed Deutsch-Jozsa
set of inputs that have 1 as output

\[ C(F) \geq \log \left( \frac{D_1}{R_1} \right) = .04n \]

\[ R_1 \leq 2^{0.96n} \]

\[ D_1 = 2^n \]

hard comb. theorem due to Frankl & Rödl
non-locality test

Promise $\Delta(x_1, x_2) = n/2 \ or \ 0$

- Alice outputs $\log(n)$ bits $o_1$
- Bob outputs $\log(n)$ bits $o_2$
- correlation:
  $$x_1 = x_2 \leftrightarrow o_1 = o_2$$

- D-J algorithm on EPR-pairs [BCT'99]

$$\eta_\star \leq \frac{\sqrt{n}}{20.02n}$$  [Massar’01]
DJ-test

\[ |0 \rangle \rightarrow 0 \rangle + \log(n) \text{ EPR-pairs} \]
\[ |1 \rangle \rightarrow 1 \rangle \]

promise $\Delta(x_1,x_2) = n/2$ or 0

Alice

$X_1$
$H + \text{ph-flip}$
$O_1$

$X_2$
$H + \text{ph-flip}$
$O_2$

$log(n) \text{ bits}$

$x_1 = x_2 \iff o_1 = o_2$
Monochromatic rectangles

- \(X_1, X_2\) set of inputs for Alice and Bob
- \(\text{Rectangle } R = A \times B, A \subseteq X_1 \& B \subseteq X_2\)
- \(R\) is \(a\)-monochromatic if
  - for all \((x_1, x_2) \in R \cap D: P(a|x_1 x_2) > 0\)
- \(D\) = set of promise inputs
- \(R_A = \max \{R \cap D | R\text{ is } a\text{-mon. } a \in A\}\)
- \(|R_A|\) yields upper bound on \(\eta^*\)
Bound on $\eta_*$

Number of possible outputs $= |A|$

$$\eta_* \leq \left(d \frac{R^A}{|D_a|}\right)^{\frac{1}{2}}$$

$A$ is set of other outputs

\{b | \exists x \ P(a|x) > 0 \& P(b|x) > 0\}

Set of inputs $x$ s.t.

$P(a|x) > 0$
proof

\[ \eta^* \leq \left( d \frac{R_A}{|D_a|} \right)^{\frac{1}{2}} \]

- **lhv protocol** is distribution of deterministic prot. \( Q_i \): for all \( x \)
  - Alice & Bob yield admissible outcome, or
  - at least one doesn’t click [prob. \( \eta \)]

- **exist** \( Q_j \) Alice & Bob yield admissible outcome on \( \eta^2 \) fraction of \( a \)-inputs

- **det. protocol** Alice & Bob yield outcome on at most \( dR_A \) of the inputs

- \( dR_A / |D_a| \geq \eta^2 \)
Application of bound
**DJ-test**

|0\rangle \rightarrow \text{log}(n) \text{ EPR-pairs} \rightarrow |0\rangle +

|1\rangle \rightarrow \Delta(x_1, x_2) = n/2 \text{ or } 0

\[ x_1 = x_2 \iff o_1 = o_2 \]

log(n) bits

**promise**

\[ \eta^* \leq \frac{\sqrt{n}}{20.02n} \]
Bound on $\eta_*$ for DJ-test

number of possible outputs

$$\eta_* \leq \left( d \frac{R_A}{|D_{aa}|} \right)^{\frac{1}{2}}$$

A = \{a_ia_i\}

d = n

$R_A \leq 2^{0.96n}$

$D_{aa} = 2^n$

set of inputs x s.t. $P(aa|x) > 0$
Bound on $\eta_*$ for DJ-test

number of possible outputs

$$\eta_* \leq \left( d \frac{R_A}{|D_{aa}|} \right)^{\frac{1}{2}} = \frac{\sqrt{n}}{2^{0.02n}}$$

set of inputs $x$ s.t. $P(aa|x) > 0$

$d = n$

$R_A \leq 2^{0.96n}$

$D_{aa} = 2^n$
n parties
n party test [BvDHT'99]

- input party i:
  \[ x_i \in \{0, \ldots, n - 1\} \]

- promise:
  \[ \sum_{i=1}^{n} x_i \mod \frac{n}{2} = 0 \]

- output a_i:
  \[ \sum_{i=1}^{n} a_i \mod 2 = \frac{1}{n/2} \sum_{i=1}^{n} x_i \mod n \]

- detector:
  \[ \eta_* \leq \frac{1}{n} \]
n-party bound

largest mon. rectangle

\[ \eta_* \leq \left( d \frac{R}{|D|} \right)^{\frac{1}{n}} \]

inputs

\[ d = 2^n \]
\[ R \leq (n-2/n)^n \]
\[ D = 2^{n \log(n)} \]

number of possible outputs
n-party bound

largest mon. rectangle

\[ \eta_* \leq \left( d \frac{R}{|D|} \right)^{\frac{1}{n}} = \frac{1}{n} \]

inputs

number of possible outputs

d = 2^n
R \leq (n-2/n)^n
D = 2^{n\log(n)}
error's

• DJ-test can be simulated classically with small error.

• n-party test is even robust against error! Can not be simulated classically with:
  - error prob. < $\frac{1}{2} - \frac{1}{n}$ and
  - $\eta_* \leq \frac{1}{n}$ [Hoyer’lastweek]
open problems

• construct 2 party test:
  - $\eta \leq \frac{1}{2^n}$ and
  - prob. of error $< \frac{1}{n}$
  - quantum gives perfect correlation

• Maybe can use Raz’s problem?
• Other applications of non-locality tests?
Thanks to the organizers!