# Combinatorics and Quantum Non Locality

Harry Buhrman
CWI
Univ. of Amsterdam
The Netherlands

Joint work with:
Serge Massar
Hein Röhrig

# overview

- EPR pairs
- Bell → non locality
- Quantum Computing
- Non locality →
  Quantum Communication Complexity
- Quantum Communication Complexity
  → Non locality

# non locality

# Non locality

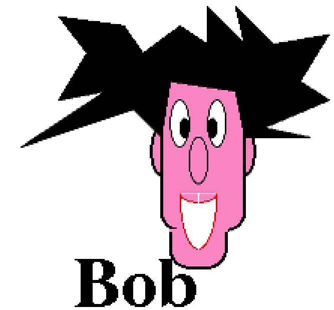
- k (>1) parties
- each party i has
  - part of an entangled state $|\varphi\rangle$
  - receives input $x_i$
  - performs measurent $M_{x_i}$
  - outputs measurement value $o_i$
- Induces correlations:
  - $P_Q(o_1 \ldots o_k \mid x_1 \ldots x_k)$
- no communication!

# Quantum Setup

$|0$ - - - - - - - - - - $0\rangle +$

EPR-pair

$|1$ - - - - - - - - - - $1\rangle$


| | |
|---|---|
| $x_1$ | $x_2$ |
| $M_{x1}$ | $M_{x2}$ |
| $o_1$ | $o_2$ |

induces correlations:

$P_Q(o_1 o_2 \mid x_1 x_2)$

# Non locality

- Question:
  - Can these correlations be reproduced classically?

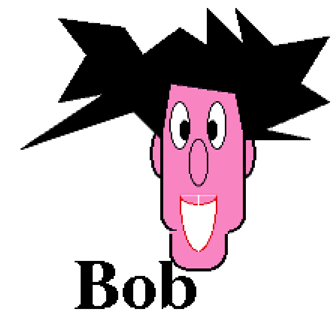
# Local hidden var. model

- Classical setup
- Each party has:
  - copy of random bits (shared randomness)
  - input $x_i$
  - Performs computation (protocol)
  - Oututs $o_i$
- Induces correlations:
  - $P_C(o_1 \ldots o_k \mid x_1 \ldots x_k)$

# Classical Setup

$r_1 r_2 .. r_k$ $r_1 r_2 .. r_k$

shared randomness


$x_1$ $x_2$

computation computation

$o_1$ $o_2$

induces correlations:

$$P_C(o_1 o_2 \mid x_1 x_2)$$

# Non locality

- If for every protocol:
  - $P_C(o_1 \ldots o_k \mid x_1 \ldots x_k) \neq P_Q(o_1 \ldots o_k \mid x_1 \ldots x_k)$
  - Non locality
- Requires
  - State + measurements to obtain $P_Q$
  - Prove that for every classical lhv protocol:

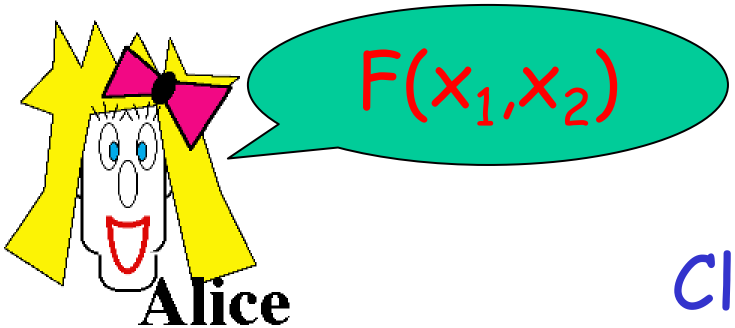
$$P_C(o_1 \ldots o_k \mid x_1 \ldots x_k) \neq P_Q(o_1 \ldots o_k \mid x_1 \ldots x_k)$$

# Examples

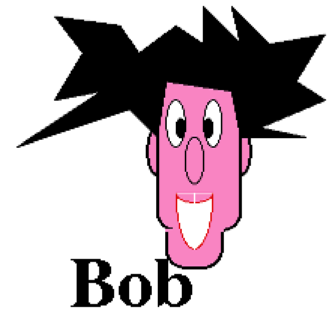
- 2 parties:
  - EPR pair: $\frac{1}{\sqrt{2}}[|00\rangle + |11\rangle]$
  - Bell inequalities
- 3 parties
  - GHZ state: $\frac{1}{\sqrt{2}}[|000\rangle + |111\rangle]$
  - Mermin state: $\frac{1}{2}[|001\rangle + |010\rangle + |100\rangle + |111\rangle]$
- n parties $\frac{1}{\sqrt{2}}[|\underbrace{0\cdots0}_{n}\rangle + |\underbrace{1\cdots1}_{n}\rangle]$

# Communication Complexity

# Communication Complexity




Classical bits

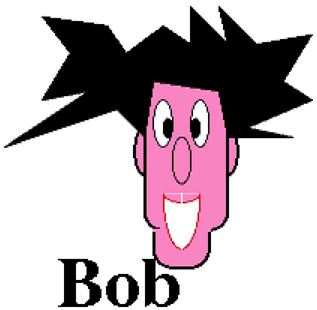



$x_1$ $x_2$

Goal: Compute some function $F(x_1,x_2) \longrightarrow \{0,1\}$ minimizing communication bits.

# Equality


Classical bits



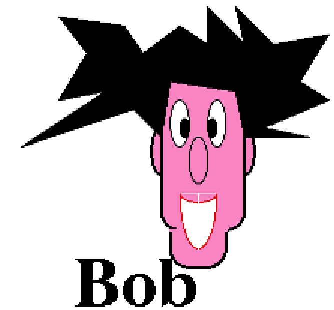

$x_1$

$x_2$

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

# Equality


Classical bits




$x_1$ $x_2$

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

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

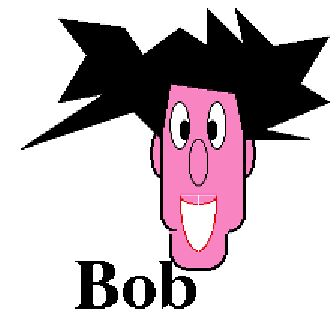
$C(EQ) = n$

# Quantum Com. Complexity


Classical bits

←

→




$x_1$ $x_2$

$$|0\rangle|0\rangle + |1\rangle|1\rangle$$

EPR-pair(s)

Goal: Compute some function $F(x_1, x_2) \longrightarrow \{0,1\}$
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 vs klog(k) [BvDHT'99]
  - incorporating quantum algorithms: [BCW'98]
    - 2 parties log(n) vs n (Deutsch-Jozsa)
    - 2 parties $n^{1/2}$ 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]

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

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

Hamming Distance

- need $\Omega(n)$ classical bits.
- can be done with log(n)) bits +EPR-pairs.
- Protocol: distributed Deutsch-Jozsa

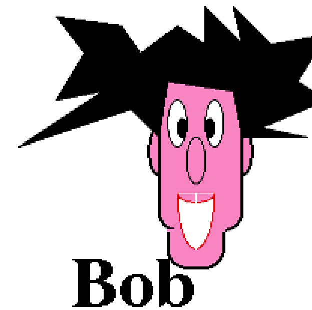
# non locality experiments

# Quantum Setup

$|0$ - - - - - - - - - - - - - - - - - - - - $0\rangle +$

EPR-pair

$|1$ - - - - - - - - - - - - - - - - - - - - $1\rangle$

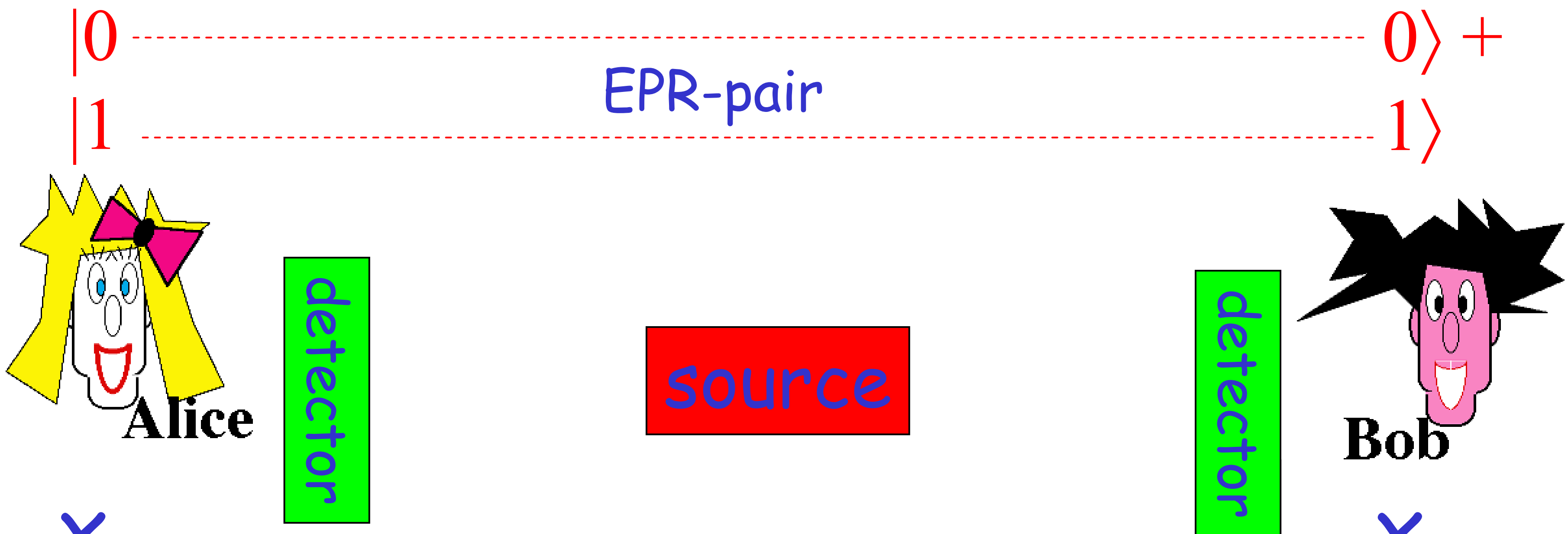

$x_1$ $\qquad$ $x_2$

$M_{x1}$ $\qquad$ $M_{x2}$

$o_1$ $\qquad$ induces correlations: $\qquad$ $o_2$

$P_Q(o_1 o_2 \mid x_1 x_2)$

# Quantum Setup




$x_1$ $x_2$

$M_{x1}$ $M_{x2}$

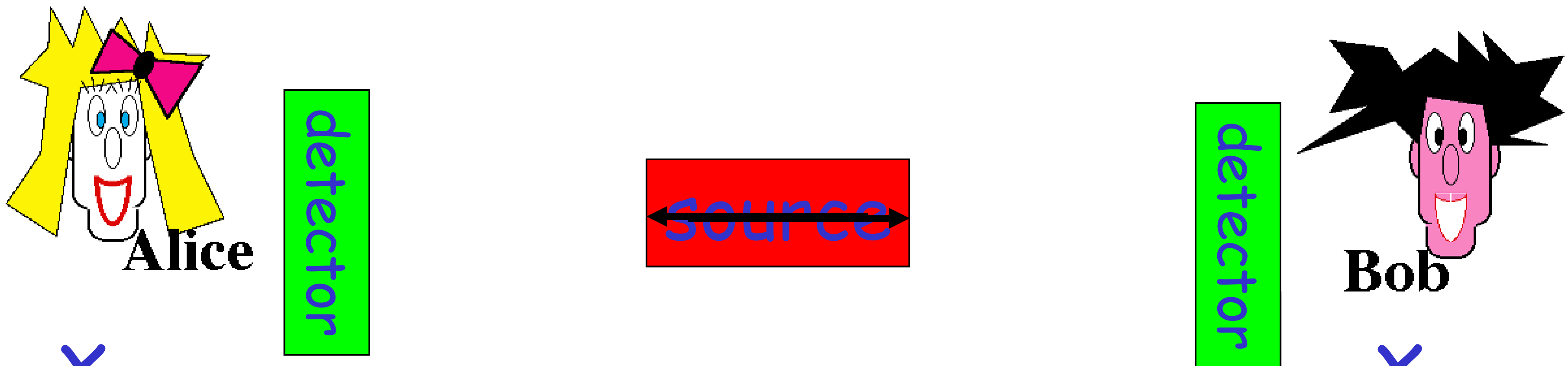
$o_1$ induces correlations: $o_2$

$P_Q(o_1 o_2 \mid x_1 x_2)$

# Quantum Setup

$|00\rangle + |11\rangle$

EPR-pair




$x_1$ $\quad$ $x_2$

$M_{x1}$ $\quad$ $M_{x2}$

$o_1$ $\quad$ $o_2$

induces correlations:

$P_Q(o_1 o_2 \mid x_1 x_2)$

# detection loophole

prob. $1-\eta$

- 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
- $\eta$ = detector efficiency = prob. of clicking
  - small $\eta$ allows for lhv protocols

prob. $\eta^2$

# example

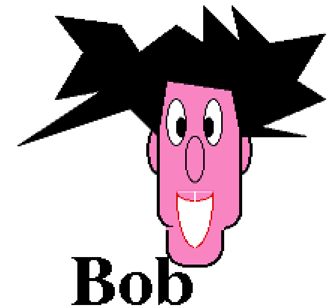
$r_1 \ldots r_k \; r_{k+1} \ldots r_{2k}$


shared randomness

correlation
$P(o|xy)$

$\eta = 2^{-k}$

$r_1 \ldots r_k \; r_{k+1} \ldots r_{2k}$




$x = x_1 \ldots x_k$

- 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 $P(o_1 \mid xy)$

$y = y_1 \ldots y_k$

- if $y_1 \ldots y_k \neq r_{k+1} \ldots r_{2k}$
  → No Click
- if $y_1 \ldots y_k = r_{k+1} \ldots r2_k$
  assume $x = r_1 \ldots r_k$
  output $P(o_2 \mid xy)$

# 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 = $A \times B$ , $A \subseteq X_1$ & $B \subseteq X_2$
- 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 {$R \cap D$ | R is a-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]

$EQ'(x_1,x_2) = 1$ iff $x_1=x_2$

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

Hamming Distance

- need $\Omega(n)$ classical bits.
- can be done with log(n)) bits +EPR-pairs.
- Protocol: distributed Deutsch-Jozsa

# EQ'

set of inputs that have 1 as output

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

$R_1 \leq 2^{0.96n}$ ← hard comb. theorem due to Frankl & Rödl

$D_1 = 2^n$

# 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]

$$\eta_* \leq \frac{\sqrt{n}}{2^{0.02n}}$$

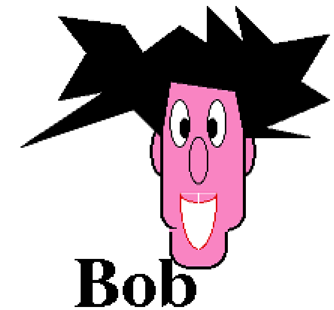
[Massar'01]

# DJ-test

$|0 \cdots\cdots 0\rangle + |1 \cdots\cdots 1\rangle$

log(n) EPR-pairs


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




$x_1$ | $x_2$
H+ph-flip | H+ph-flip
$o_1$ | $o_2$

$x_1=x_2 \leftrightarrow o_1=o_2$

log(n) bits

# 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 $(x_1,x_2) \in R \cap D$: $P(a|x_1 x_2)>0$
- $D$ = 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
$\{b \mid \exists x \; P(a|x)>0 \;\&\; P(b|x)>0\}$

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
- $dR_A/|D_a| \geq \eta^2$

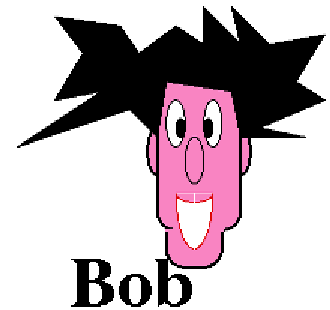
# Application of bound

# DJ-test

$|0 \cdots 0\rangle + |1 \cdots 1\rangle$

log(n) EPR-pairs


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




$x_1$ H+ph-flip $o_1$

$$\eta_* \leq \frac{\sqrt{n}}{2^{0.02n}}$$

$x_2$ H+ph-flip $o_2$

$x_1=x_2 \leftrightarrow o_1=o_2$

log(n) bits

# Bound on $\eta_*$ for DJ-test

number of possible outputs

$A = \{a_i a_i\}$

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

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

$d = n$
$R_A \leq 2^{0.96n}$
$D_{aa} = 2^n$

# Bound on $\eta_*$ for DJ-test

number of possible outputs

$A = \{a_i a_i\}$

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

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

$d = n$
$R_A \le 2^{0.96n}$
$D_{aa} = 2^n$

# n parties

# n party test

[BvDHT'99]

- input party i: $x_i \in \{0, \cdots, n-1\}$
- 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

number of possible outputs

$d = 2^n$

$R \leq (n\text{-}2/n)^n$

$D = 2^{n\log(n)}$

# n-party bound

largest mon. rectangle

$$\eta_* \le \left( d \, \frac{R}{|D|} \right)^{\frac{1}{n}} = \frac{1}{n}$$

inputs

number of possible outputs

$d = 2^n$

$R \le (n-2/n)^n$

$D = 2^{n\log(n)}$

# 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. < ½-1/n and
  - $\eta_* \leq 1/n$ [Hoyer'lastweek]

# open problems

- construct 2 party test:
  - $\eta_* \leq 1/2^n$ and
  - prob. of error < 1/n
  - quantum gives perfect correlation
- Maybe can use Raz's problem?
- Other applications of non-locality tests?

Thanks to the organizers!