The communication complexity of non-signaling distributions

Julien Degorre[1,2] Marc Kaplan[2] Sophie Laplante[2]
Jérémie Roland[3]

[1]Laboratoire d'Informatique de Grenoble

[2]Université Paris-Sud - LRI

[3]NEC Laboratories America

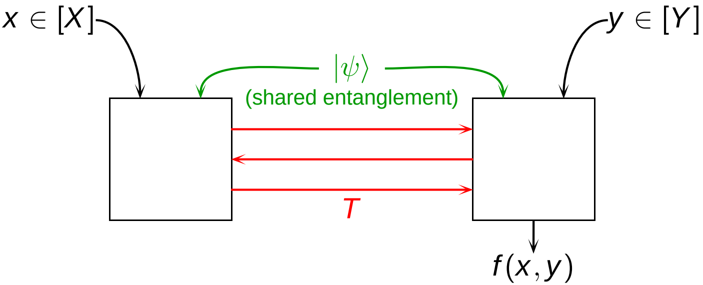
June 26, 2009

Plan

1. The problem
   - Communication complexity
   - Non-signaling distributions
   - Bell inequalities and EPR experiment
2. Affine combinations / quasi-probabilities
3. Lower bounds on communication complexity
4. Upper bounds on communication complexity
5. Conclusion

Communication complexity: Boolean functions

Boolean function $f : [X] \times [Y] \mapsto \{0, 1\}$

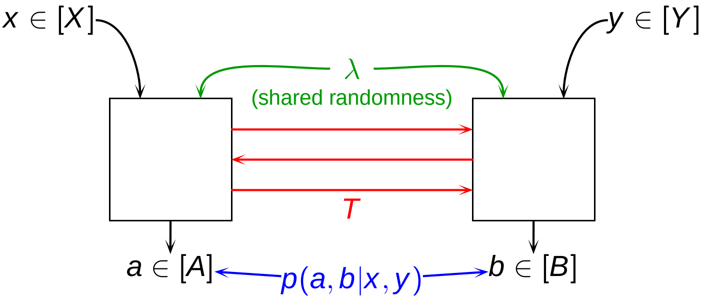


How much communication is needed?

- Assisted with shared randomness: $R_\epsilon(f)$
- Assisted with shared entanglement: $Q_\epsilon(f)$

Communication complexity: distributions

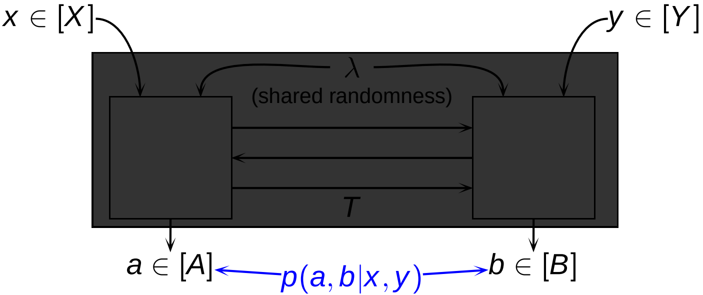
Probability distribution $p(a, b|x, y)$



How much communication is needed?

- Assisted with shared randomness: $R_\epsilon(\mathbf{p})$
- Assisted with shared entanglement: $Q_\epsilon(\mathbf{p})$

We consider non-signaling distributions **p**:



- a contains no information about y:

$$p(a|x, y) = p(a|x, y')$$

- b contains no information about x:

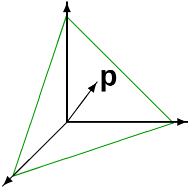
$$p(b|x, y) = p(b|x', y)$$

Set of non-signaling distributions $\mathcal{N}$

- Distribution $\mathbf{p} \longrightarrow$ vector in $\mathbb{R}^n$, for $n = ABXY$
- Coordinates $\mathbf{p}[a,b,x,y] = p(a,b|x,y)$
- $\mathbf{p} \in \mathcal{N}$ iff

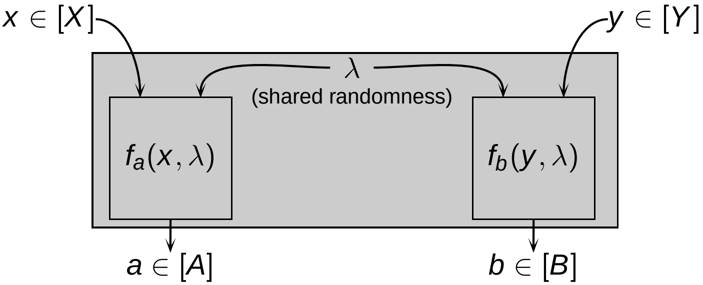
Positivity:	$p(a,b\|x,y) \geq 0$	$\forall a,b,x,y$
Normalization:	$\sum_{a,b} p(a,b\|x,y) = 1$	$\forall x,y$
Non-signaling:	$\sum_b p(a,b\|x,y) = \sum_b p(a,b\|x,y')$	$\forall a,y,y'$
	$\sum_a p(a,b\|x,y) = \sum_a p(a,b\|x',y)$	$\forall b,y,y'$

- Set of linear (in)equations $\Longrightarrow \mathcal{N}$ is a polytope in $\mathbb{R}^n$



Local distributions

No communication but shared randomness:



- No shared randomness (fixed λ) $\longrightarrow$ Deterministic protocol:

$$p(a,b|x,y,\lambda) = \delta_{a=f_a(x,\lambda)}\ \delta_{b=f_b(y,\lambda)}$$

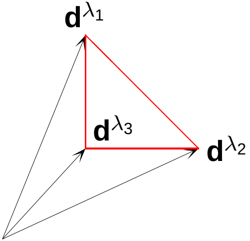
- Shared randomness $\longrightarrow$ Mixture of deterministic protocols:

$$p(a,b|x,y) = \sum_\lambda p(\lambda)\, p(a,b|x,y,\lambda)$$

Set of local distributions $\mathcal{L}$

- Deterministic protocols $\mathbf{d}^\lambda \longrightarrow$ vectors in $\mathbb{R}^n$
- Coordinates: $\mathbf{d}^\lambda[a, b, x, y] = \delta_{a=f_a(x,\lambda)}\ \delta_{b=f_b(y,\lambda)}$
- Set $\mathcal{L} \longrightarrow$ convex hull of these vectors

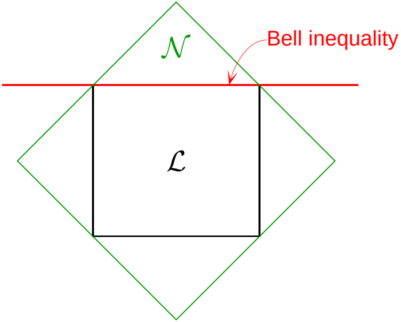
$\Longrightarrow$ $\mathcal{L}$ is also a polytope



Bell inequalities

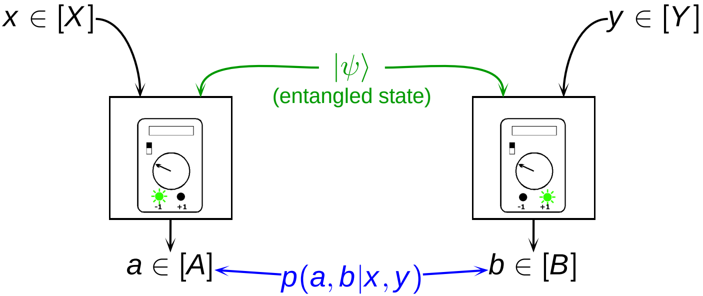
"Local" polytope $\mathcal{L}$ defined by:

- Extremal vertices: deterministic protocols $\mathbf{d}^\lambda$
- Facets: Bell inequalities $B(\mathbf{p}) \leq B_0$ for all $\mathbf{p} \in \mathcal{L}$
  where $B : \mathcal{H}(\mathcal{N}) \mapsto \mathbb{R}$ is a linear functional over distributions



Quantum distributions

No communication but shared entanglement $\longrightarrow$ EPR Experiment

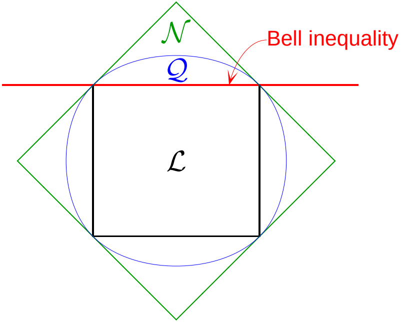


- $p(a,b|x,y)$ is non-signaling $\longrightarrow \mathcal{Q} \subseteq \mathcal{N}$
- BUT may violate Bell inequality $\longrightarrow \mathcal{L} \subset \mathcal{Q}$

Bell inequalities

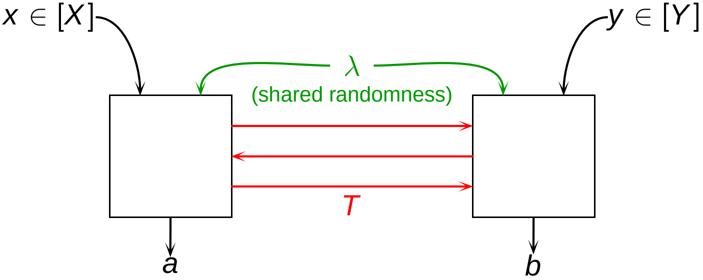
"Local" polytope $\mathcal{L}$ defined by:

- Extremal vertices: deterministic protocols $\mathbf{d}^{\lambda}$
- Facets: Bell inequalities $B(\mathbf{p}) \leq B_0$ for all $\mathbf{p} \in \mathcal{L}$
  where $B : \mathcal{H}(\mathcal{N}) \mapsto \mathbb{R}$ is a linear functional over distributions



Boolean functions

Function $f : [X] \times [Y] \mapsto \{0, 1\}$



$$p_f(a, b|x, y) = \begin{cases} \frac{1}{2} & \text{if } a \oplus b = f(x, y) \\ 0 & \text{otherwise} \end{cases}$$

Communication complexities of f and $\mathbf{p}_f$

$$R_\epsilon(\mathbf{p}_f) \leq R_\epsilon(f) \leq R_\epsilon(\mathbf{p}_f) + 1$$

Quasi-probabilities

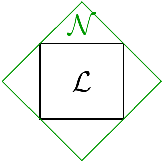
Set of local distributions defined as

$$\mathbf{p} \in \mathcal{L} \iff \exists\, p_\lambda \text{ s.t. } \begin{cases} \sum_\lambda p_\lambda \mathbf{d}^\lambda & = & \mathbf{p} \\ \sum_\lambda p_\lambda & = & 1 \\ p_\lambda & \geq & 0 \;\forall \lambda \end{cases}$$

Set of local distributions with quasi-probabilities defined as

$$\mathbf{p} \in \tilde{\mathcal{L}} \iff \exists\, q_\lambda \text{ s.t. } \begin{cases} \sum_\lambda q_\lambda \mathbf{d}^\lambda & = & \mathbf{p} \\ \sum_\lambda q_\lambda & = & 1 \\ p(a,b|x,y) & \geq & 0 \;\forall a,b,x,y \end{cases}$$

$$\mathcal{L} \subseteq \tilde{\mathcal{L}} \subseteq \mathcal{N}$$



Non-signaling distributions and quasi-probabilities

Theorem

The set of non-signaling distributions coincides with the set of LHV with quasi-probabilities

$$\tilde{\mathcal{L}} = \mathcal{N}$$

Proof sketch:

- Affine hulls:

$$\left.\begin{array}{rcl} \mathcal{H}(\tilde{\mathcal{L}}) & \subseteq & \mathcal{H}(\mathcal{N}) \\ \dim \mathcal{H}(\tilde{\mathcal{L}}) & \geq & \dim \mathcal{H}(\mathcal{N}) \end{array}\right\} \Longrightarrow \mathcal{H}(\tilde{\mathcal{L}}) = \mathcal{H}(\mathcal{N})$$

- Build $\tilde{\mathcal{L}}$ from $\mathcal{H}(\tilde{\mathcal{L}})$ by restricting to $p(a, b|x, y) \geq 0$
- Similarly for $\mathcal{N}$

$\Longrightarrow$ $\tilde{\mathcal{L}} = \mathcal{N}$

Affine combinations

Intuitively:

- Distance from $\mathcal{L} \rightarrow$ bound on classical communication complexity
- Distance from $\mathcal{Q} \rightarrow$ bound on quantum communication complexity

How well may **p** be described as an affine combination?

We define:

- $\nu(\mathbf{p}) = \min\{\sum_i |q_i| : \exists \mathbf{p}_i \in \mathcal{L}, q_i \in \mathbb{R}, \mathbf{p} = \sum_i q_i \mathbf{p}_i\}$, (LP)
- $\gamma_2(\mathbf{p}) = \min\{\sum_i |q_i| : \exists \mathbf{p}_i \in \mathcal{Q}, q_i \in \mathbb{R}, \mathbf{p} = \sum_i q_i \mathbf{p}_i\}$, (SDP relax.)
- $\nu^\epsilon(\mathbf{p}) = \min\{\nu(\mathbf{p}') : \delta(\mathbf{p}, \mathbf{p}') \leq \epsilon\}$, (LP)
- $\gamma_2^\epsilon(\mathbf{p}) = \min\{\gamma_2(\mathbf{p}') : \delta(\mathbf{p}, \mathbf{p}') \leq \epsilon\}$. (SDP relax.)

Extension of factorization norms [Linial,Shraibman STOC'07]

Lower bounds

Theorem

$$R_\epsilon(\mathbf{p}) \geq \log(\nu^\epsilon(\mathbf{p})) - 1 \qquad \text{and} \qquad Q_\epsilon(\mathbf{p}) \geq \frac{1}{2}\log(\gamma_2^\epsilon(\mathbf{p})) - 1$$

Proof sketch:

- Protocol for $\mathbf{p}$ with c bits.
- Replace communication by random transcript $T \in \{0,1\}^c$,
- Alice outputs random $a \sim p(a|x)$ if T not consistent with x,
- Similarly for Bob

$\longrightarrow$ 0 bit protocol for $\mathbf{p}_\pi$

$$p_\pi(a,b|x,y) \quad = \quad \pi\, p(a,b|x,y) + (1-\pi)\, p(a|x)p(b|y),$$

where $\pi = 2^{-c}$

Lower bounds

Theorem

$$R_\epsilon(\mathbf{p}) \geq \log(\nu^\epsilon(\mathbf{p})) - 1 \qquad \text{and} \qquad Q_\epsilon(\mathbf{p}) \geq \frac{1}{2}\log(\gamma_2^\epsilon(\mathbf{p})) - 1$$

Proof sketch (continued):

- 0 bit protocol for $\mathbf{p}_\pi$,

$\rightarrow$ $\mathbf{p}_\pi \in \mathcal{L}$,

$\rightarrow$ $\nu(\mathbf{p}) \leq 2^{c+1} - 1$ since

$$p(a,b|x,y) = \tfrac{1}{\pi}\, p_\pi(a,b|x,y) - (\tfrac{1}{\pi} - 1)\, p(a|x)p(b|y).$$

and $|\frac{1}{\pi}| + |\frac{1}{\pi} - 1| = \frac{2}{\pi} - 1$

Bell inequalities

By (LP or SDP) duality,
$\rightarrow$ We turn the minimization problem into a maximization problem.

Theorem

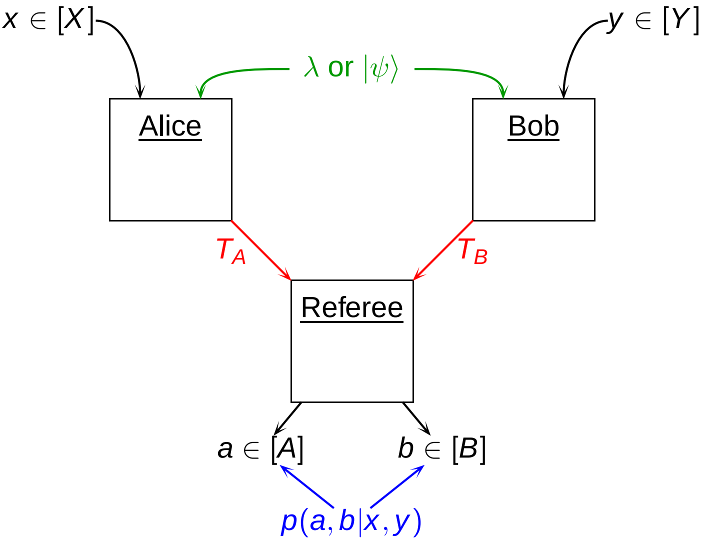
For any distribution $\mathbf{p} \in \mathcal{N}$,

- $\nu(\mathbf{p}) = \max\{B(\mathbf{p}) : \forall \mathbf{p}' \in \mathcal{L},\ |B(\mathbf{p}')| \leq 1\}$, and
- $\gamma_2(\mathbf{p}) = \max\{B(\mathbf{p}) : \forall \mathbf{p}' \in \mathcal{Q},\ |B(\mathbf{p}')| \leq 1\}$,

where the maximization is over linear functionals $B : \mathcal{H}(\mathcal{N}) \mapsto \mathbb{R}$

Intuition: The bounds consist in maximizing the violation of a Bell (or Tsirelson) inequality.

Simultaneous message passing (SMP)



Upper bounds in the SMP model

Theorem

- $R^{\mathrm{SMP}}_{\epsilon+\delta}(\mathbf{p}) \leq 16 \left[\frac{AB\nu^{\epsilon}(p)}{\delta}\right]^2 \ln\left[\frac{4AB}{\delta}\right] \log(AB)$
- $Q^{\mathrm{SMP}}_{\epsilon+\delta}(\mathbf{p}) \leq 16 \left[\frac{AB\gamma_2^{\epsilon}(p)}{\delta}\right]^2 \ln\left[\frac{4AB}{\delta}\right] \log(AB)$

Proof sketch:

- Let $\mathbf{p} = q_+\mathbf{p}^+ - q_-\mathbf{p}^-$, where $|q_+| + |q_-| = \nu(\mathbf{p})$.
- Alice and Bob send samples of $\mathbf{p}^+, \mathbf{p}^- \in \mathcal{L}$ to the referee.
- The referee estimates $p(a,b|x,y)\ \forall a,b$ (without knowing x,y).

Comparing ν and γ_2

- Special case
  - Binary outputs: $a, b = \pm 1$
  - Uniform marginals: $E(a|x) = E(b|y) = 0$
  - $\longrightarrow$ Correlations $E(a \cdot b|x, y) = C_{xy}$ (in particular Boolean functions)
  - $\longrightarrow$ Grothendieck's inequality: $\gamma_2(\mathbf{p}) \leq \nu(\mathbf{p}) \leq K_G\, \gamma_2(\mathbf{p})$
  - $\longrightarrow$ Tsirelson's bound
- General case

Theorem

$$\gamma_2(\mathbf{p}) \leq \nu(\mathbf{p}) \leq O(AB\, \gamma_2(\mathbf{p}))$$

The proof uses affine combinations and Grothendieck's inequality.

Simulating quantum protocols

From

- Upper bound: $R^{\mathrm{SMP}}_{\epsilon+\delta}(\mathbf{p}) \leq 16 \left[\frac{AB\nu^{\epsilon}(p)}{\delta}\right]^2 \ln\left[\frac{4AB}{\delta}\right] \log(AB)$
- Comparison: $\nu^{\epsilon}(\mathbf{p}) \leq O(AB\ \gamma_2^{\epsilon}(\mathbf{p}))$
- Lower bound: $\gamma_2^{\epsilon}(\mathbf{p}) \leq 2^{2Q_{\epsilon}(\mathbf{p})+1} - 1$

Corollary

Any quantum protocol may be simulated with classical messages in the SMP model with exponential blowup: For $Q_{\epsilon}(\mathbf{p}) \leq q$

- $R^{\mathrm{SMP}}_{\epsilon+\delta}(\mathbf{p}) \leq O\left(2^{4q}\frac{(AB)^3}{\delta^2}\ln^2\left[\frac{AB}{\delta}\right]\right)$

In particular, for $\mathbf{p} \in \mathcal{Q}$, that is, $Q_{\epsilon}(\mathbf{p}) = 0$

- $R^{\mathrm{SMP}}_{\epsilon+\delta}(\mathbf{p}) \leq O\left(\frac{(AB)^3}{\delta^2}\ln^2\left[\frac{AB}{\delta}\right]\right)$ [Shi,Zhu STOC'05]

Conclusion

Summary

- non-signaling distributions $\longleftrightarrow$ LHV with quasi-probabilities
- New intuition for studying non-locality
- Bounds for communication complexity
  $\longrightarrow$ Extension of [Linial,Shraibman STOC'07]
- Relation: communication complexity $\longleftrightarrow$ Bell inequalities

Further work

- Extension to multipartite model (number-on-the-forehead)
- New lower bounds (non-Boolean, partial functions, relations)

The End

Thank you !