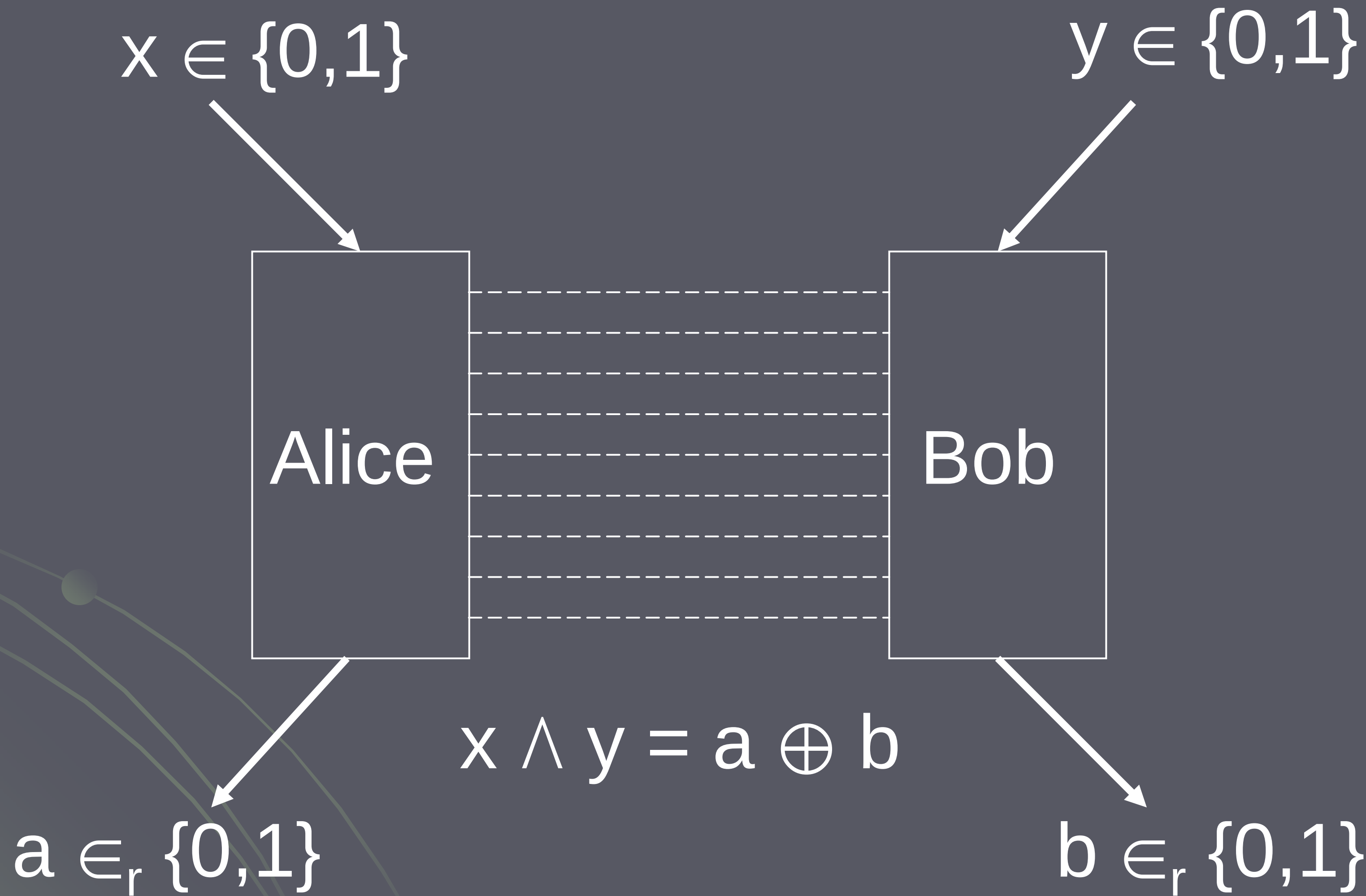
A limit on nonlocality in any world in which communication complexity is not trivial

André Allan Méthot

Université de Genève/Montréal

Work in collaboration with
G. Brassard, H. Buhrman, N. Linden
A.Tapp & F. Unger
quant-ph/0508042

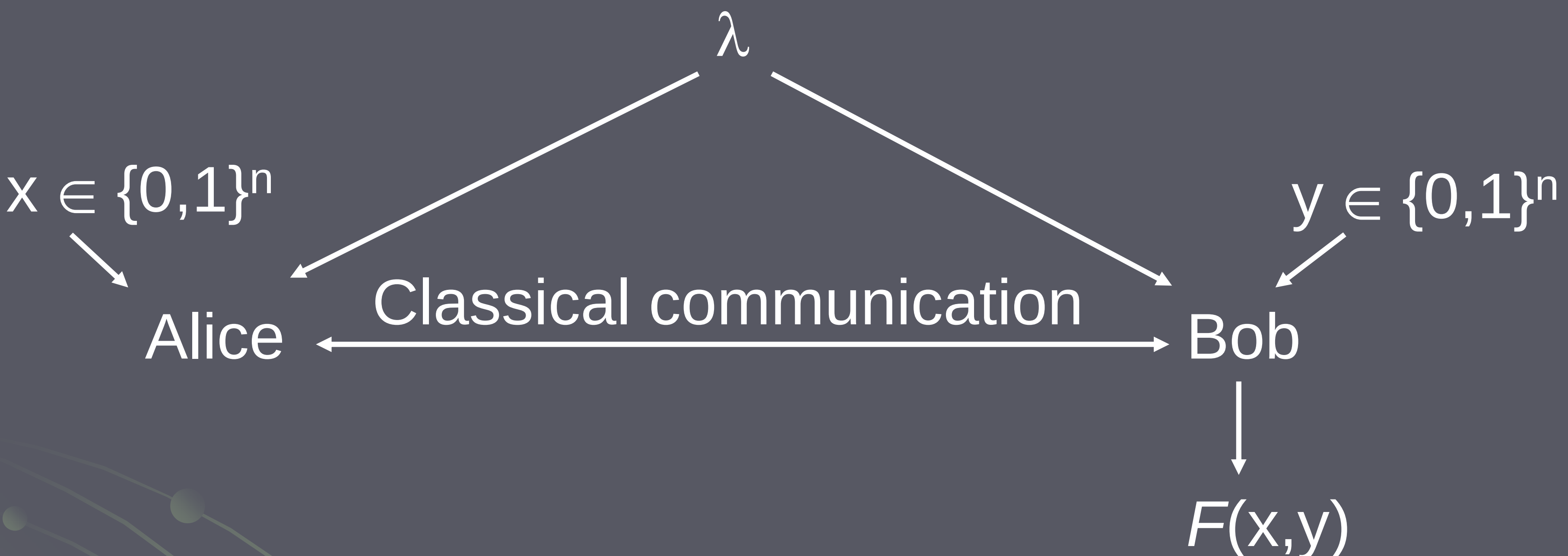
Non-local boxes



Simulating NLBs

- Local hidden variable theory (LHV):
  - 75%.
- Quantum :
  - $\cos^2(\pi/8) \approx 85\%$.
  - Known (in other terms) as the CHSH inequality.
- Why not 100% ?
  - Would not violate causality…

Communication complexity



Probabilistic communication complexity

A limit on non-locality

- Most functions : about n bits of communication.
- Simulating NLBs with an efficiency of 91%: all (boolean) functions can be computed with only *one* bit of communication!
  - Wim van Dam already had a similar result with 100%.
- Such a world would be unbelievable!

Distributed computing

- A bit x is said to be distributed between Alice and Bob if they have x^A and x^B respectively such that $x^A \oplus x^B = x$.
- A function *F* is computed distributively if Alice can output z^A and Bob z^B such that $z^A \oplus z^B = F(x,y)$.
  - WITHOUT COMMUNICATION.

Bias

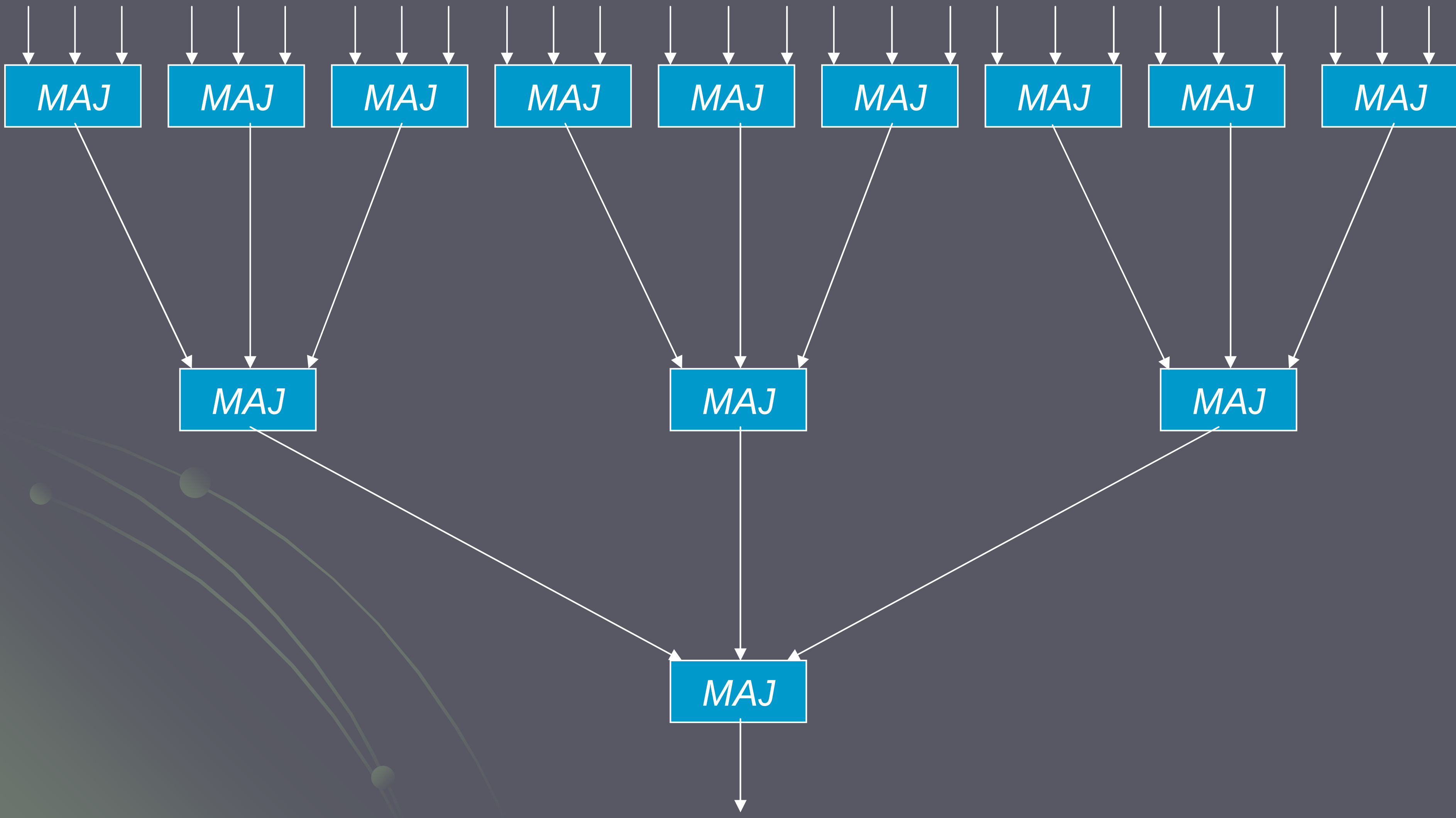
- *F* has a *bias*: Alice and Bob can produce a distributed bit *z* such that $z^A \oplus z^B = z = F(x,y)$ with probability $P[z = F(x,y)] > ½$.
- Every function has a bias.
- *F* has a *bounded* bias: …

  … $P[z = F(x,y)] > ½ + \delta$.

Idea

- We have a distributed bias.
- We want a bounded bias.
- Let’s amplify the bias.
- Repetition and Majority.
- Compute Majority distributively *(MAJ).*
- Use NLBs to implement *MAJ*.
- Calculate the effeciency of NLBs we need to for this to work.

Majority tree



MAJ > 5/6

- If *MAJ* can be computed with probability stricly greather than 5/6, than every fonction can be computed with a bounded bias.
- Below that treshold *MAJ* makes things worst.
- p = Pr[having the right answer].

  q = Pr[*MAJ* works properly].

$$q(p^3+3p^2(1-p))+(1-q)(3p(1-p)^2+(1-p)^3)> p$$

$$\Rightarrow q > 5/6$$

NLBs and *MAJ*

- We can implement the non-local majority with 2 NLBs.

$$
\begin{aligned}
MAJ = {} & [(x_1^{\mathsf{A}} \oplus x_2^{\mathsf{A}}) \vee (x_2^{\mathsf{A}} \oplus x_3^{\mathsf{A}})] \oplus x_1^{\mathsf{A}} \oplus x_2^{\mathsf{A}} \oplus x_3^{\mathsf{A}} \\
& \oplus [(x_1^{\mathsf{B}} \oplus x_2^{\mathsf{B}}) \vee (x_2^{\mathsf{B}} \oplus x_3^{\mathsf{B}})] \oplus x_1^{\mathsf{B}} \oplus x_2^{\mathsf{B}} \oplus x_3^{\mathsf{B}} \\
& \oplus [(x_1^{\mathsf{A}} \oplus x_2^{\mathsf{A}}) \wedge (x_2^{\mathsf{B}} \oplus x_3^{\mathsf{B}})] \\
& \oplus [(1 \oplus x_2^{\mathsf{A}} \oplus x_3^{\mathsf{A}}) \wedge (x_1^{\mathsf{B}} \oplus x_2^{\mathsf{B}})]
\end{aligned}
$$

$$\frac{5}{6} \Rightarrow \frac{1}{2} + \frac{1}{\sqrt{6}}$$

$$p^2 + (1-p)^2 > 5/6$$

$$\Rightarrow p > 1/2 + 1/\sqrt{6} \approx 91\%$$

I have left out the analysis of the convergence of the protocol to a value bounded from 1/2.

Conclusion

- If we take the *reasonable* assumption that communication complexity is *not* trivial, we have a bound on non-locality.
  - Take a look at the complexity zoo: http://qwiki.caltech.edu/wiki/Complexity_Zoo.
- Protocol:
  - Compute distributively *F* many times with tiny bias.
  - Use *MAJ* tree to amplify the bias.
    - *MAJ* uses 2 NLBs.
  - Bob sends his one bit of the shared output.
  - Need NLBs of 91%.
- Classical fault-tolerant computing < 25%

What else in physics can computer science give us insights into?