

Interactive Proof = nonlocalゲーム

-- Interactive Proofと確率的証明 --

Interactive Proofの発展
第一部 Interactive Proofと複雑性 #1

nonlocal game と Interactive Proof

- CHSHゲームやMagic Squareゲーム等をnonlocal gameと呼ぶ。nonlocal というのは、これらのゲームでは、非局所的なエンタングルメントの性質を利用して、古典的な相関を超える高い勝率を実現しているからである。

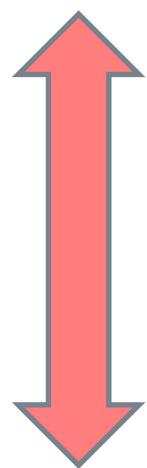
nonlocal game と Interactive Proof

- CHSHゲームやMagic Squareゲーム等をnonlocal gameと呼ぶ。nonlocal というのは、これらのゲームでは、非局所的なエンタングルメントの性質を利用して、古典的な相関を超える高い勝率を実現しているからである。
- nonlocalゲームは、量子論が古典論とは異なるものであることを、理論的・実験的に明らかにしようとする取り組みの中で生まれたものであるが、それは、Interactive Proofと、同じ構造をしていた。

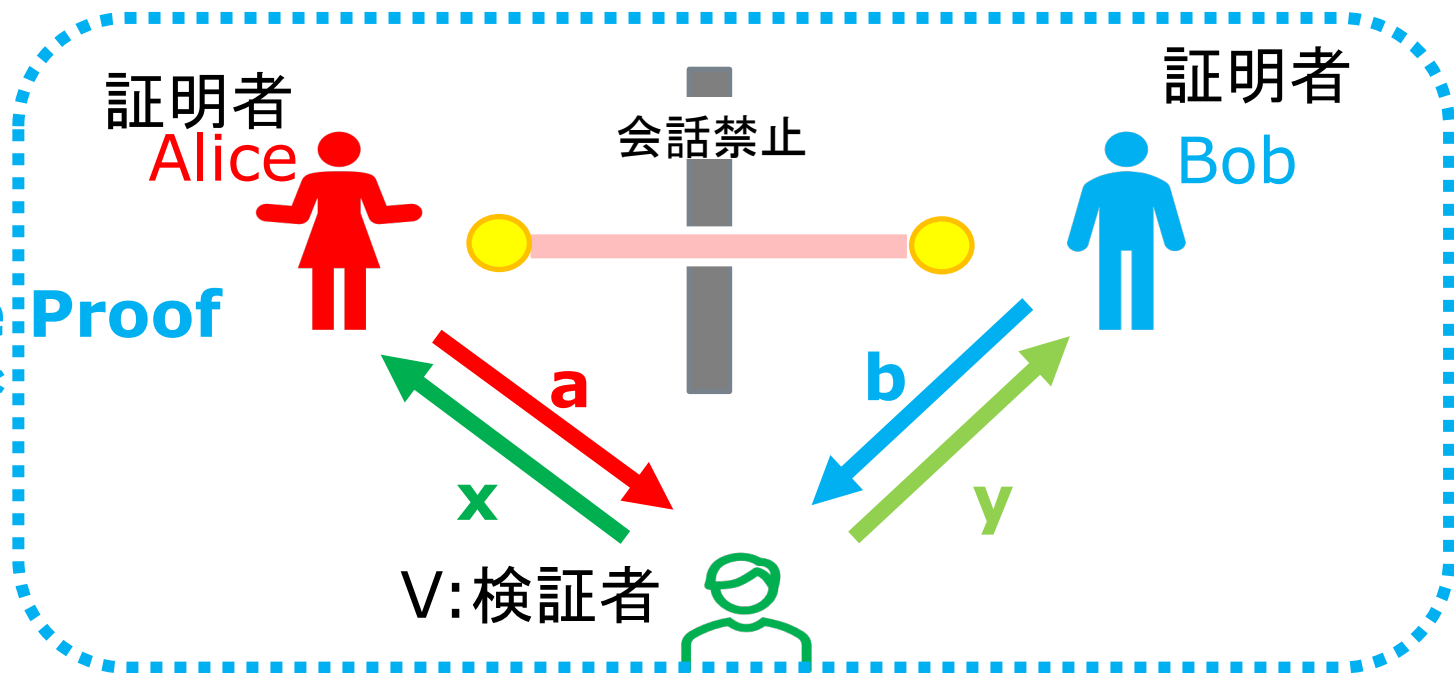
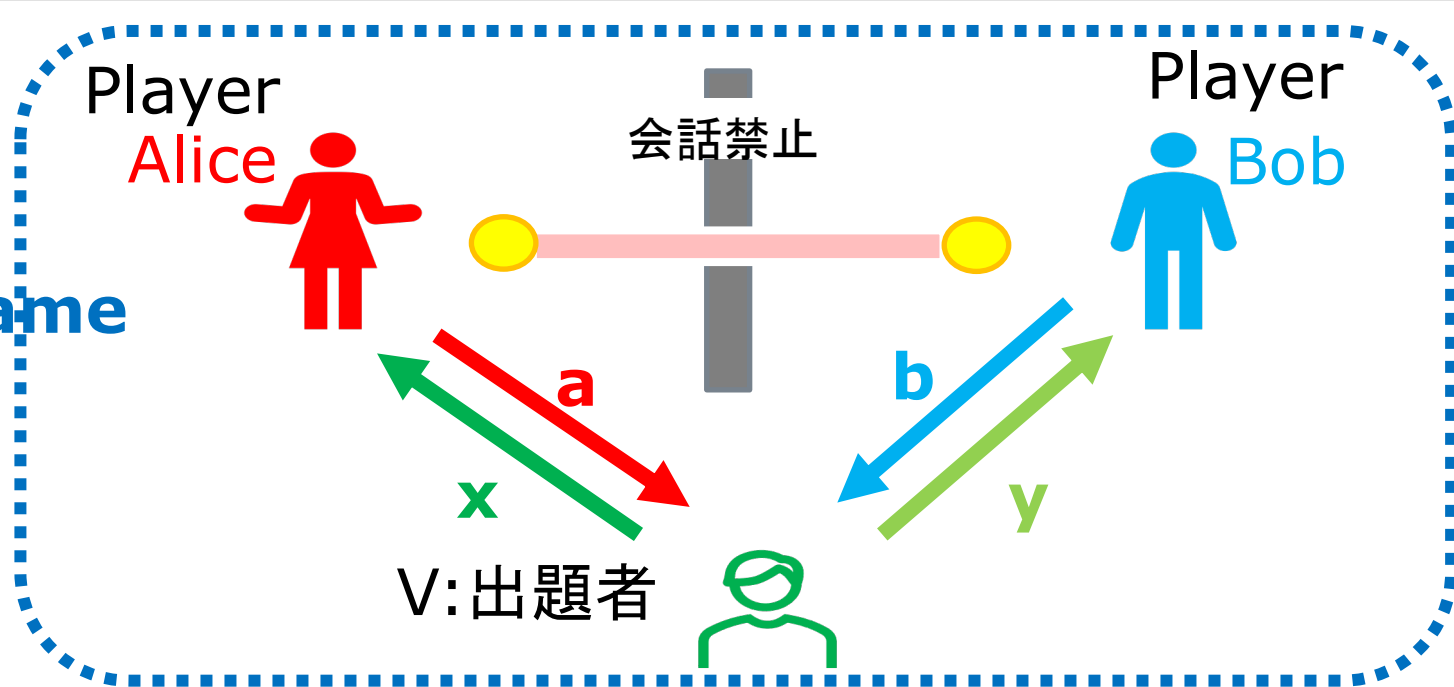
nonlocal game と Interactive Proof

- CHSHゲームやMagic Squareゲーム等をnonlocal gameと呼ぶ。nonlocal というのは、これらのゲームでは、非局所的なエンタングルメントの性質を利用して、古典的な相関を超える高い勝率を実現しているからである。
- nonlocalゲームは、量子論が古典論とは異なるものであることを、理論的・実験的に明らかにしようとする取り組みの中で生まれたものであるが、それは、Interactive Proofと、同じ構造をしていた。
- CHSHゲームは 1960年代に生まれ、Interactive Proofは1990年代に発展するのだが、両者が同一の構造を持つという認識は、21世紀に入ってから生まれたものだ。

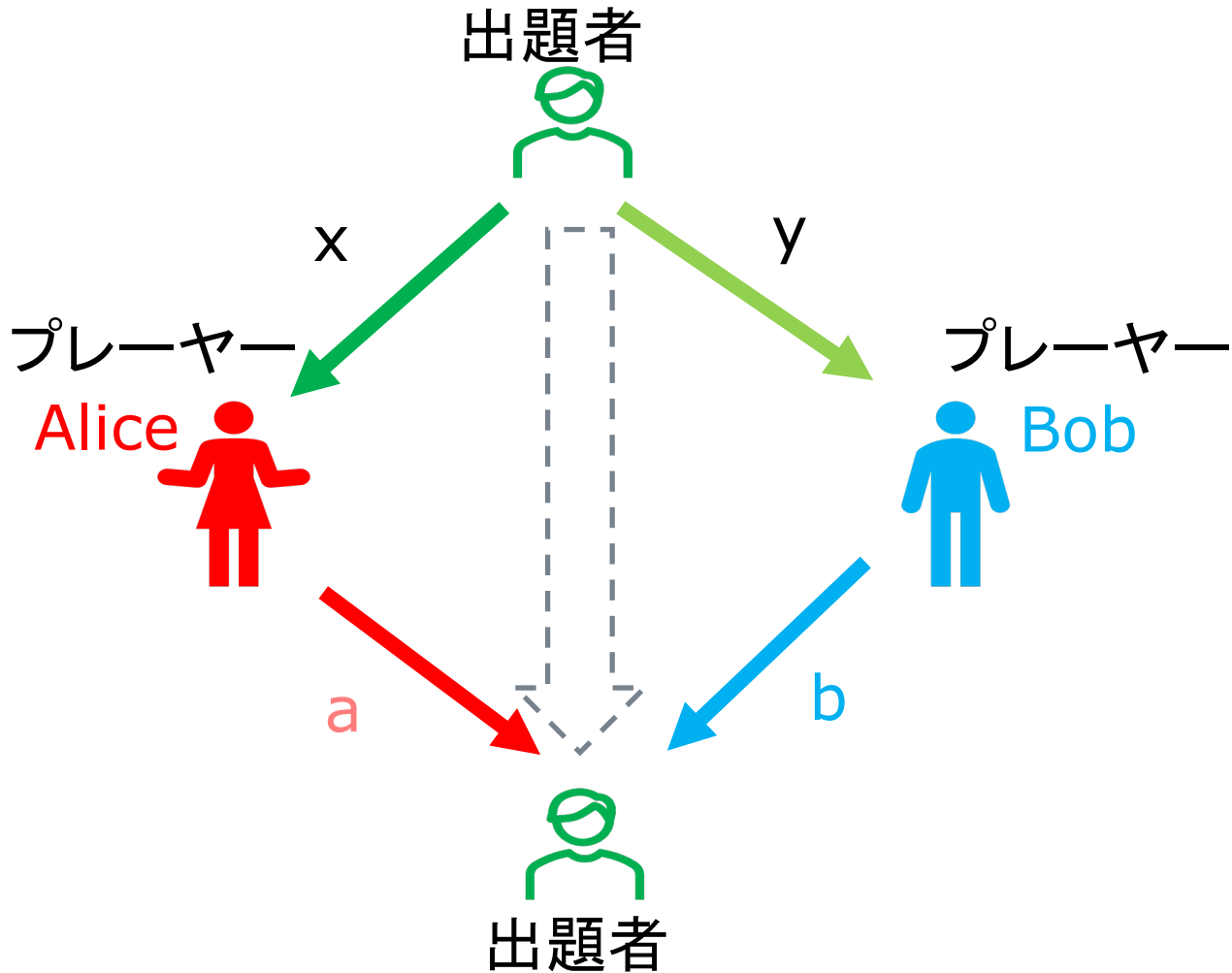
nonlocal game
CHSH



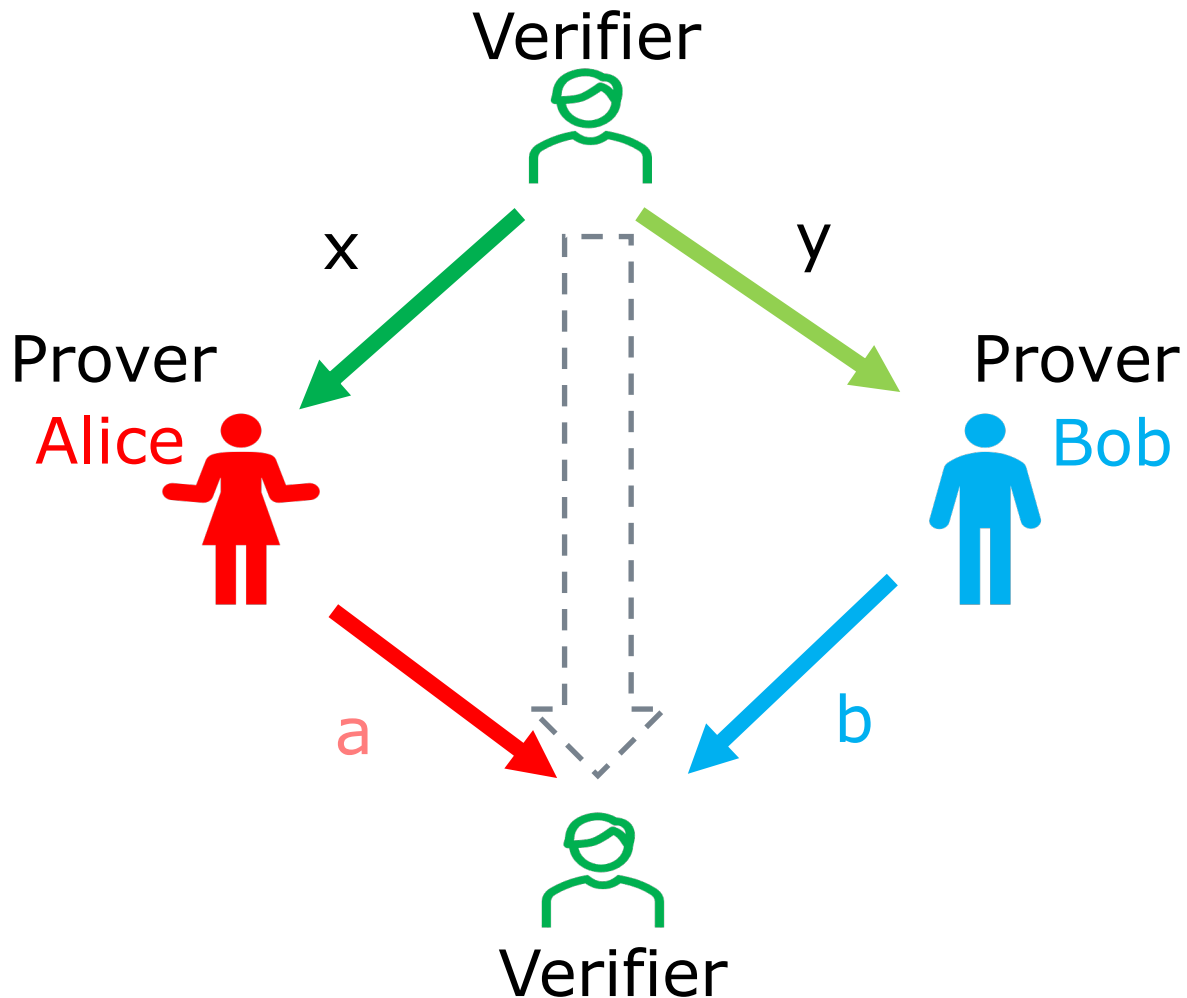
Interactive Proof
MIP*



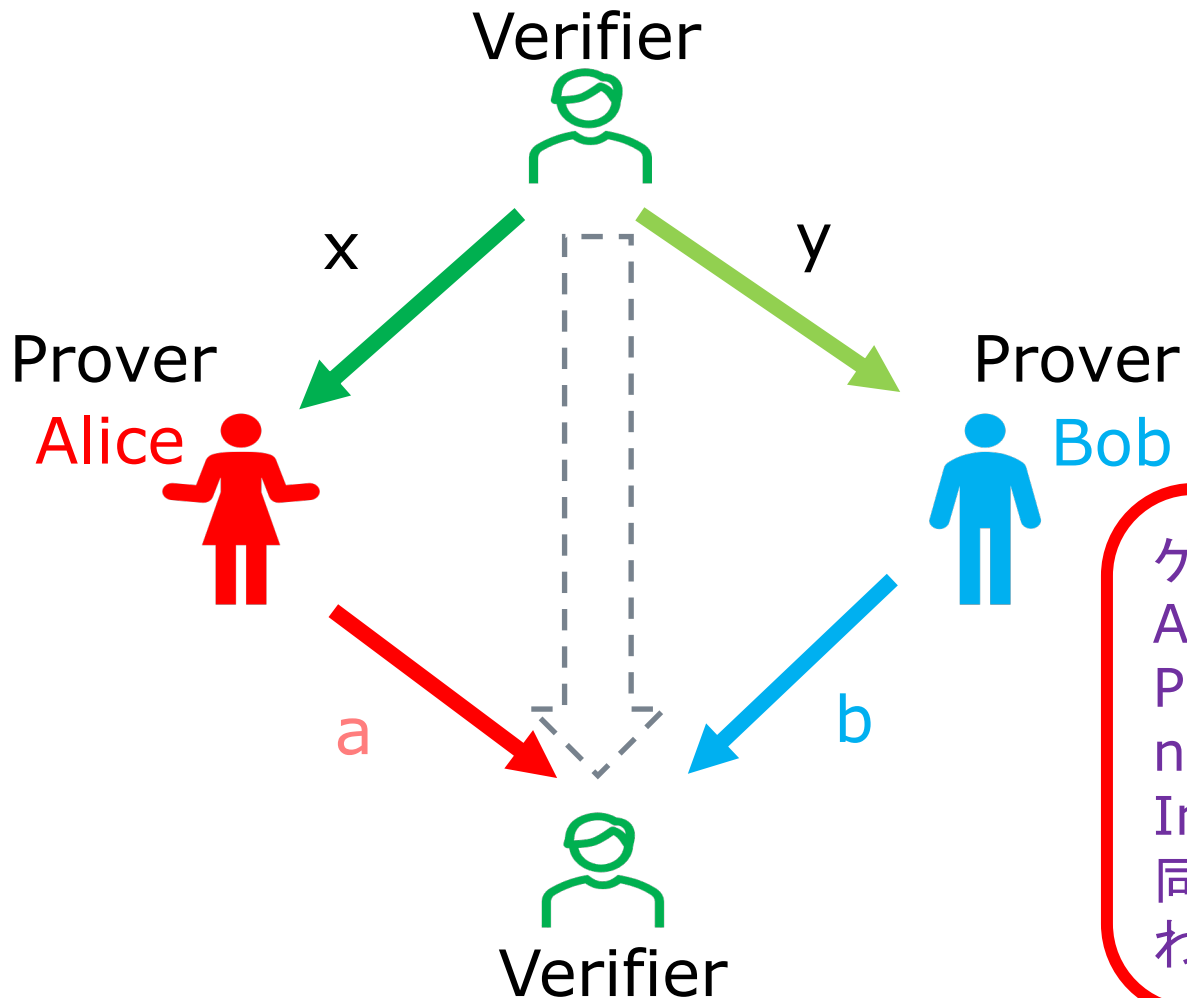
nonlocal ゲームは



nonlocal ゲームは、Interactive Proofである

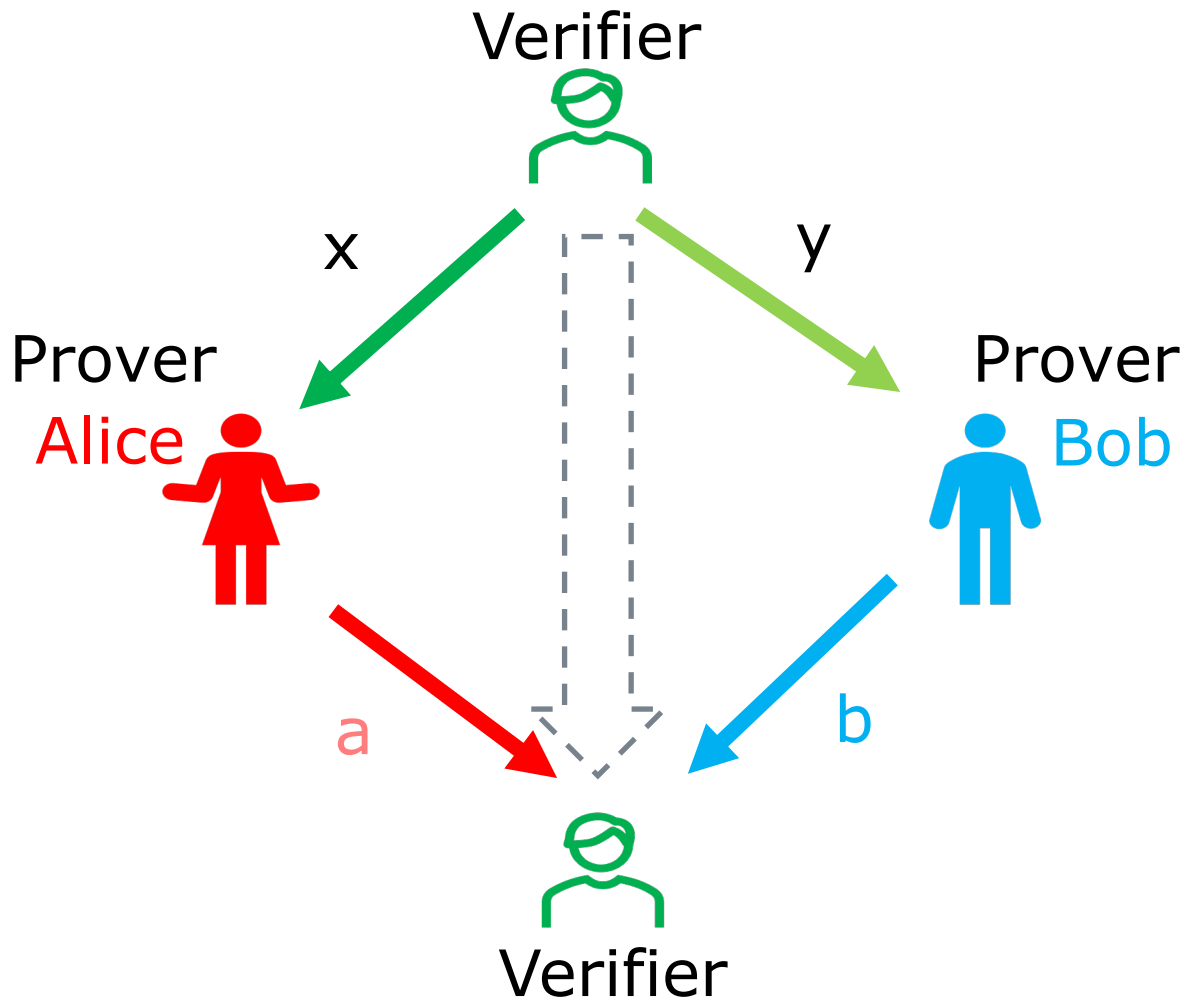


nonlocal ゲームは、Interactive Proofである

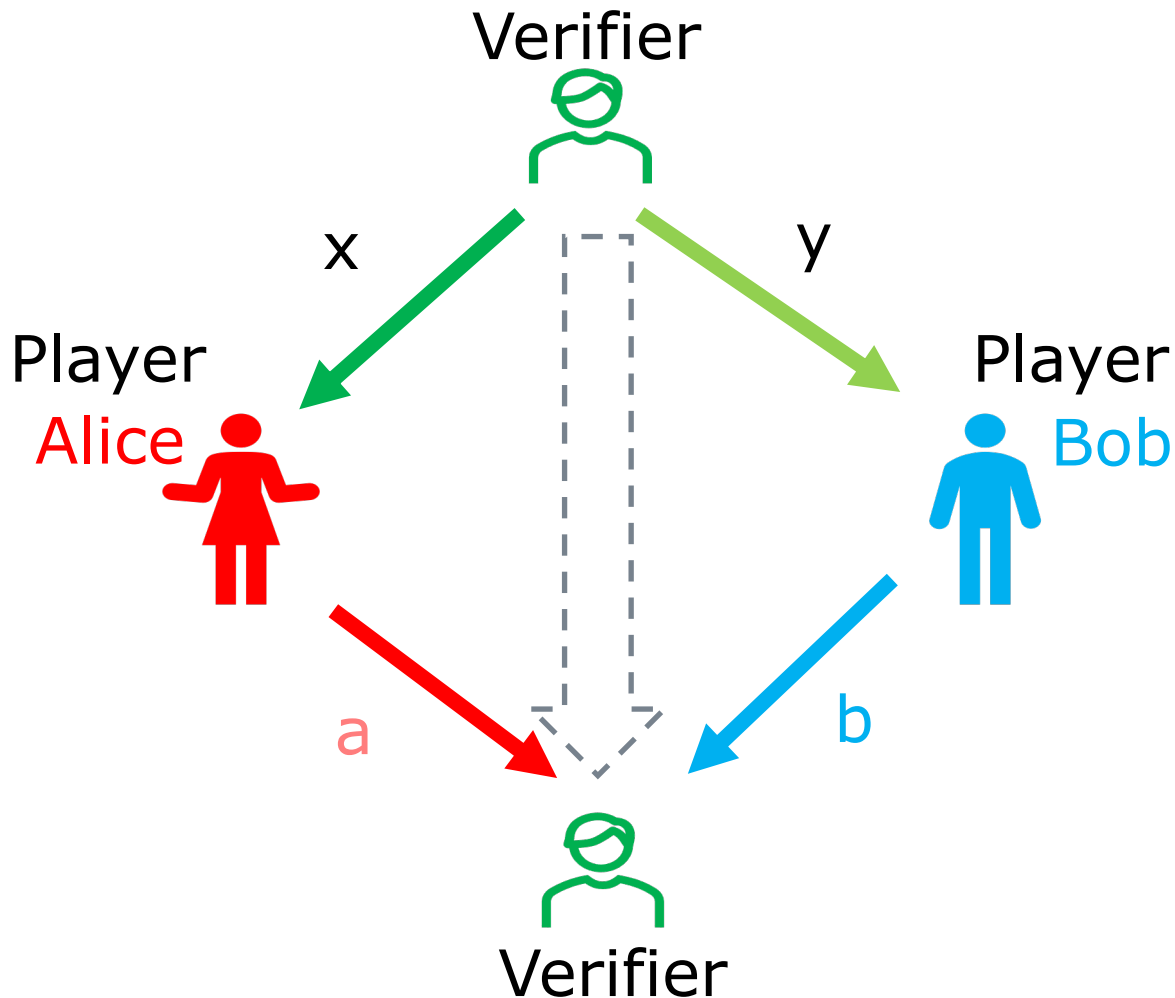


ゲームのプレイヤーの Alice と Bob を二人の Prover とみなせば、nonlocal ゲームは Interactive Proof と同じ構造をしていることがわかる。

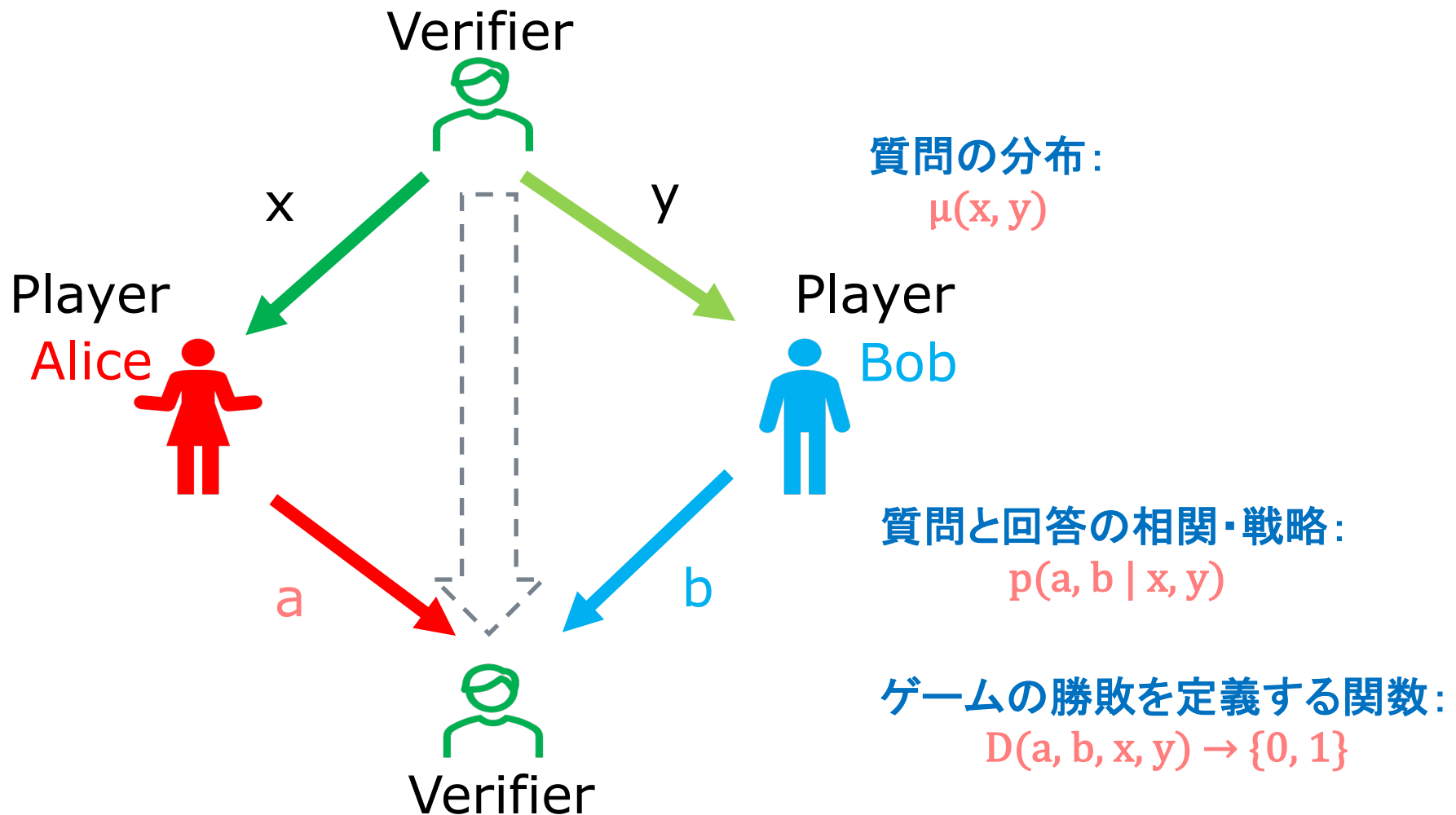
Interactive Proofは



Interactive Proofは、nonlocal ゲームである



Interactive Proofは、nonlocal ゲームである



nonlocalゲームの定式化

それぞれのゲームは、次の三つの式で特徴付けられる。

1. 質問の分布: $\mu(x, y)$
2. 質問と回答の相関: $p(a, b \mid x, y)$
入力 x, y が与えられた時 a, b を出力する、条件付き確率である
3. ゲームの勝敗を定義する関数: $D(a, b, x, y) \rightarrow \{0, 1\}$

nonlocalゲームの定式化

それぞれのゲームは、次の三つの式で特徴付けられる。

1. 質問の分布: $\mu(x, y)$
2. 質問と回答の相関: $p(a, b \mid x, y)$
入力 x, y が与えられた時 a, b を出力する、条件付き確率である
3. ゲームの勝敗を定義する関数: $D(a, b, x, y) \rightarrow \{0, 1\}$

CHSHゲームの場合、

- $\mu(x, y)$ は、0と1の一様にランダムな分布、
- $p(a, b \mid x, y)$
 $= p(a, b \mid 0, 0) + p(a, b \mid 0, 1) + p(a, b \mid 1, 0) + p(a, b \mid 1, 1)$ 、
- $D(a, b, x, y)$ は、
 $a + b = xy \pmod{2}$ の時に1を、それ以外の時に0を返す関数である。

相関 p が与えられた時のゲームの勝率

相関 p が与えられたときのゲーム G の勝率 $\omega(G, p)$ は、次の式で与えられる。

$$\omega(G, p) = \sum_{x,y,a,b} \mu(x, y) \cdot D(x, y, a, b) \cdot p(a, b|x, y)$$

古典論的なCHSHと、エンタングルメントを利用したCHSHとの違いは、相関 p が古典論的相関に属するか $p \in C_c$ 、量子論的相関に属するか $p \in C_q$ の違いに帰着する。

どのような相関を選択するかで勝率は変わる。こうして選択された相関をゲームの「戦略」という。

最適な戦略の元でのゲームGの最大勝率 $\omega(G)$

戦略 p の元でのゲーム G の勝率を $\omega(G, p)$ で表す。

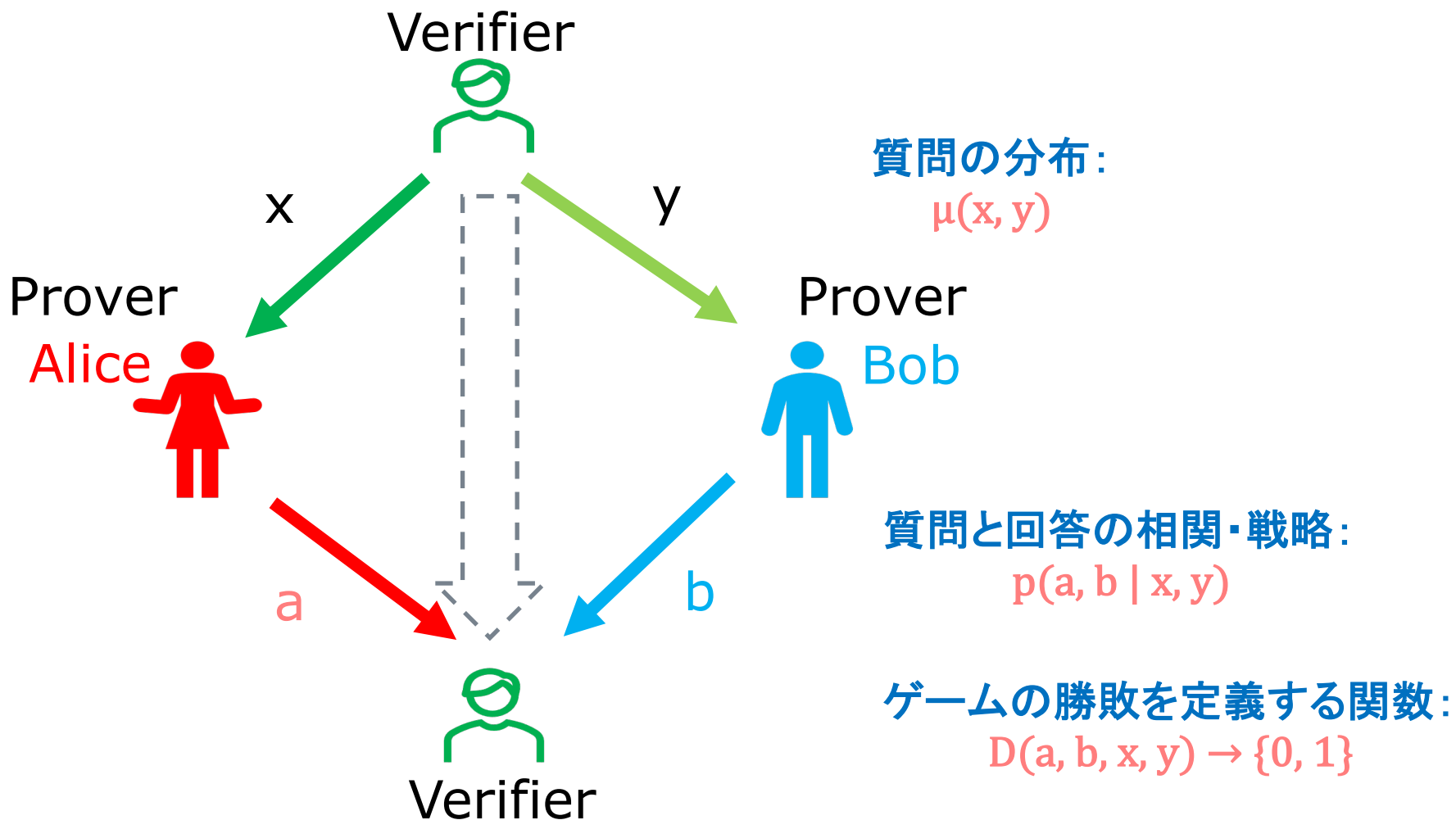
古典論的相関 C_c のもとでの最大勝率を $\omega_c(G)$ 、
量子論的相関 C_q のもとでの最大勝率を $\omega_q(G)$ と表すと

$$\omega_c(G) = \sup_{p \in C_c} \omega(G, p)$$

$$\omega_q(G) = \sup_{p \in C_q} \omega(G, p)$$

- $\omega_c(\text{CHSH}) = 3/4$
- $\omega_q(\text{CHSH}) = \cos^2(\pi/8)$
- $\omega_c(\text{Magic Square}) = 8/9$
- $\omega_q(\text{Magic Square}) = 1$

Interactive Proofでも、
 $\omega(G, p)$ や $\omega_q(G)$ を考えることができる



Interactive Proofとnonlocalゲームの対応は、
Interactive Proofに「確率的証明」の概念を
導入する