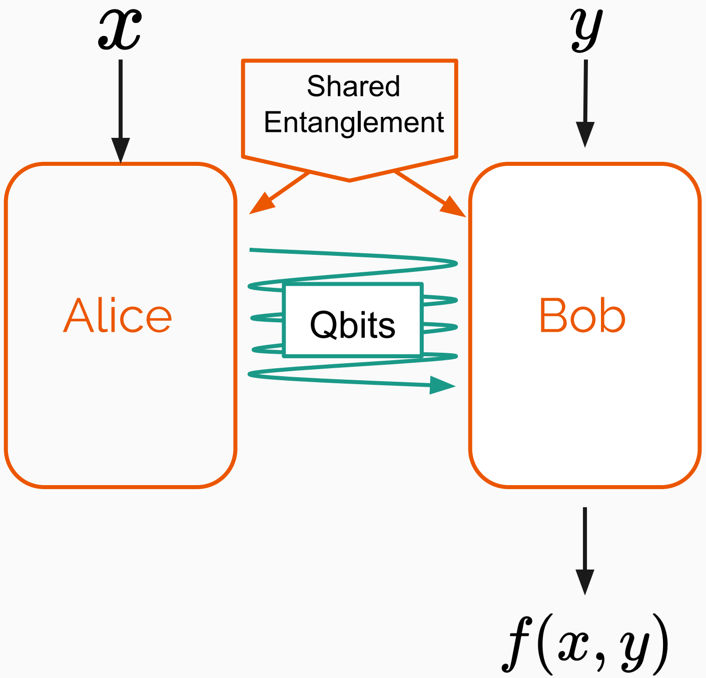
An adversary method for quantum communication complexity

QuIC-meets

Mathieu Brandeho

Motivation



Σ : an alphabet

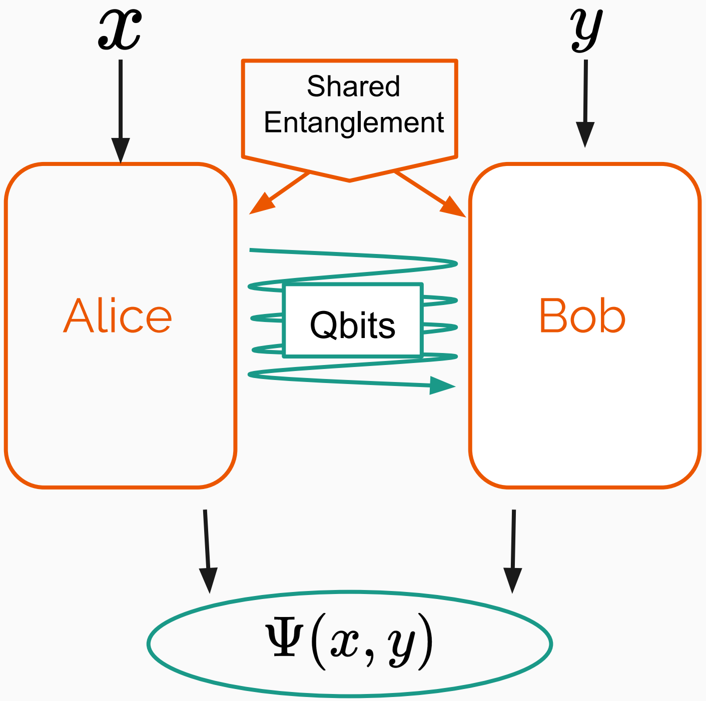
X, Y : subsets of the set Σ^n

$x \in X, y \in Y$

$f : X \times Y \to Z$

$\mathrm{QCC}(f)$: the minimum number of qbits needed to compute f

Motivation



Σ : an alphabet

X, Y : subsets of the set Σ^n

$x \in X, y \in Y$

$f : X \times Y \to Z$

$\mathrm{QCC}(f)$: the minimum number of qbits needed to generate $\Psi(x, y)$

How we construct our new lower bound method?

We use a $\underbrace{\text{lower bound method}}_{\textbf{Adversary method}}$ of $\underbrace{\text{another model}}_{\textbf{Query model}}$.

Quantum communication model

Protocols $\mathcal{P}$

(communication cost QCC)

Reduction

Quantum query model

Query algorithm $\mathcal{A}$

(query cost Q)

Reduction with this property

Adversary method

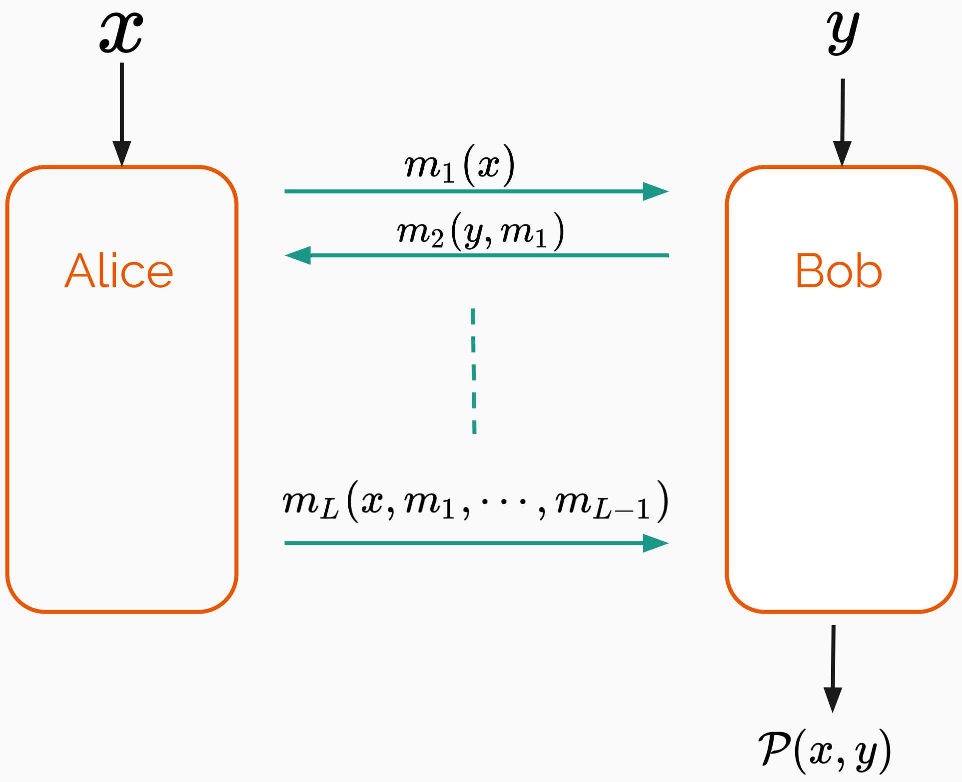
$$\left.\begin{array}{r} \mathrm{QCC}(\mathcal{P}) \geq \mathrm{Q}(R(\mathcal{P})) \\ \mathrm{Q}(\mathcal{A}) \geq \mathrm{Adv}(\mathcal{A}) \end{array}\right\} \quad \mathrm{QCC}(\mathcal{P}) \geq \mathrm{Adv}(R(\mathcal{P}))$$

Can we construct the reduction R?

Between classical models: **Yes**

Between quantum models: **I don't know**

Communication model and protocol



A **protocol** *P* is defined by a set of functions

$$\{m_i\}_{i=0}^{L}$$

Such that

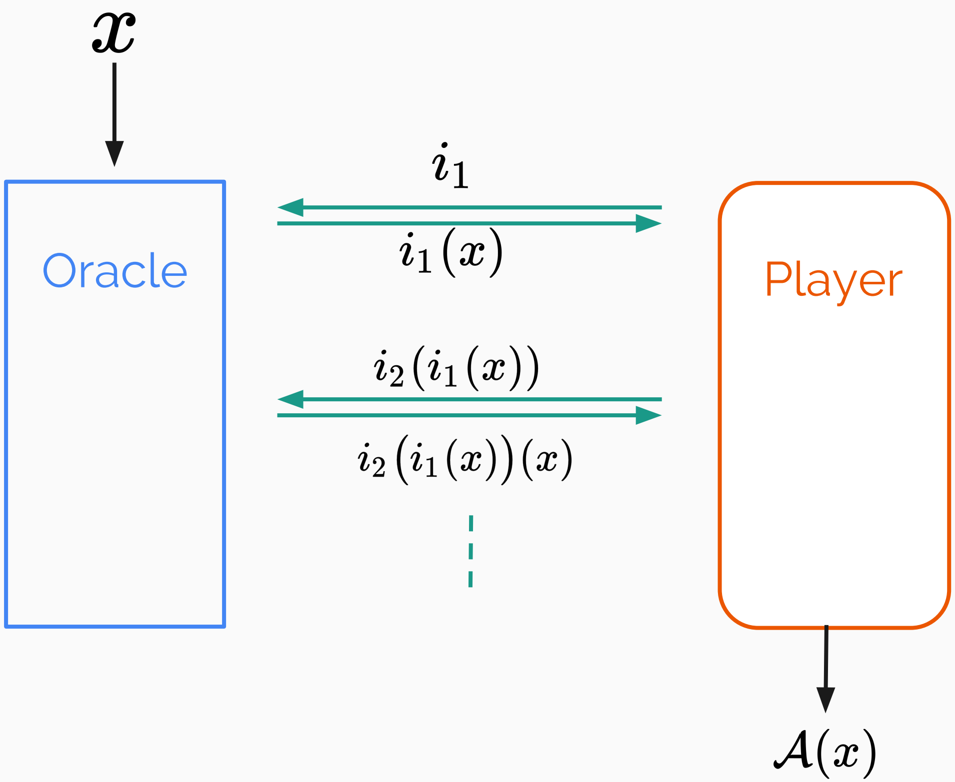
m_{2k+1} only depends of *x and previous messages*

m_{2k+2} only depends of *y and previous messages*

Communication cost

$$\mathrm{CC}(\mathcal{P}) = \sum_{i=1}^{L} |m_i|$$

Query model and query algorithm



Projection functions

$$i : \Sigma^n \to \Sigma$$
$$x \mapsto x_i$$

A **query algorithm** *A* is defined by a set of functions

$$\{i_k\}_{k=1}^{L}$$

Such that each function only depends of x and previous queries

Query cost $\quad R(\mathcal{A}) = L$

Looking for similarities

Communication model

A **protocol** *P* is defined by a set of functions

$$\{m_i\}_{i=0}^{L}$$

Such that

m_{2k+1} only depends of *x and previous messages*

m_{2k+2} only depends of *y and previous messages*

Communication cost

$$\mathrm{CC}(\mathcal{P}) = \sum_{i=1}^{L} |m_i|$$

Query model

A **query algorithm** *A* is defined by a set of functions

$$\{i_k\}_{k=1}^{L}$$

Such that

each function only depends of x and previous queries

Query cost $R(\mathcal{A}) = L$

Generalization of the oracle

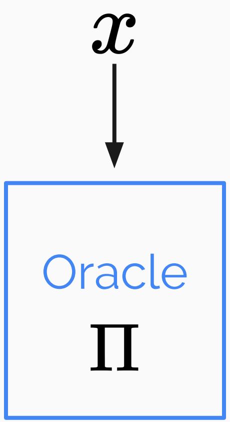
We precise which functions we can query to the oracle

$$\Pi = \{\text{All projection functions}\}$$

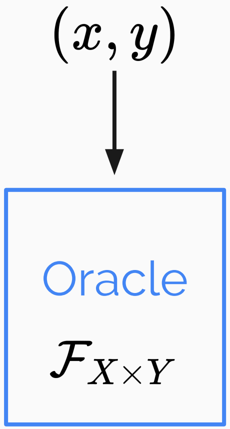
$$\mathcal{F}_X = \{f : X \to \Sigma\}$$

$$\mathcal{F}_Y = \{f : Y \to \Sigma\}$$

$$\mathcal{F}_{X \times Y} = \mathcal{F}_X \uplus \mathcal{F}_Y$$

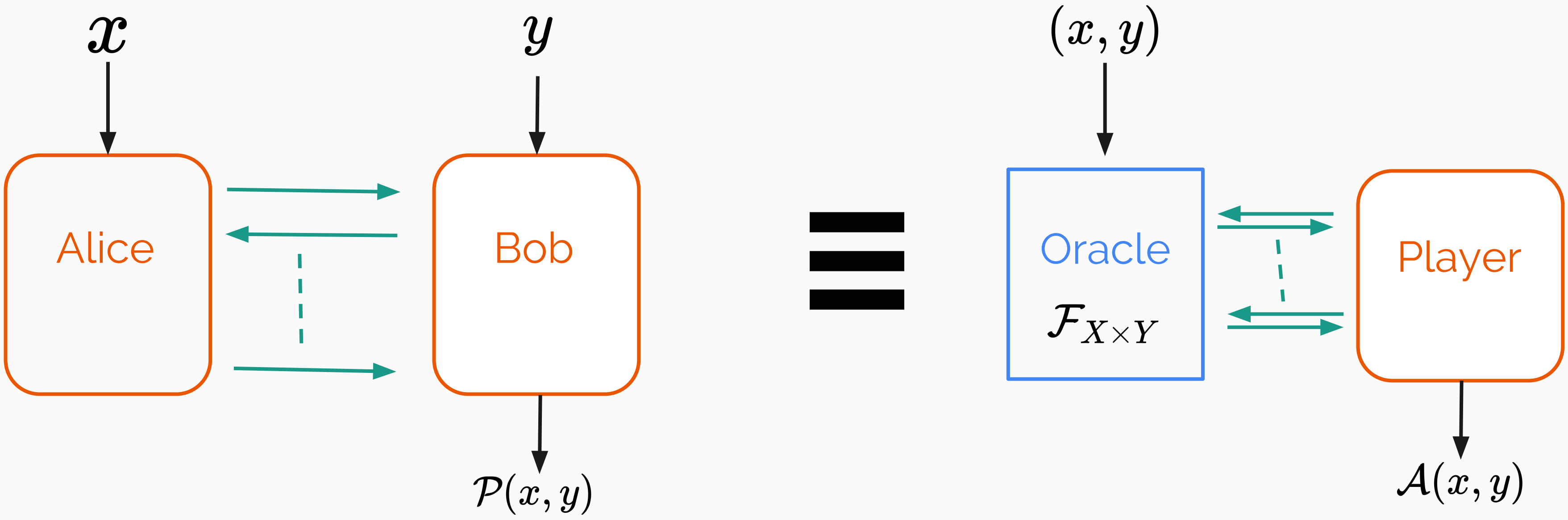


Initial oracle



Generalized oracle

Equivalence

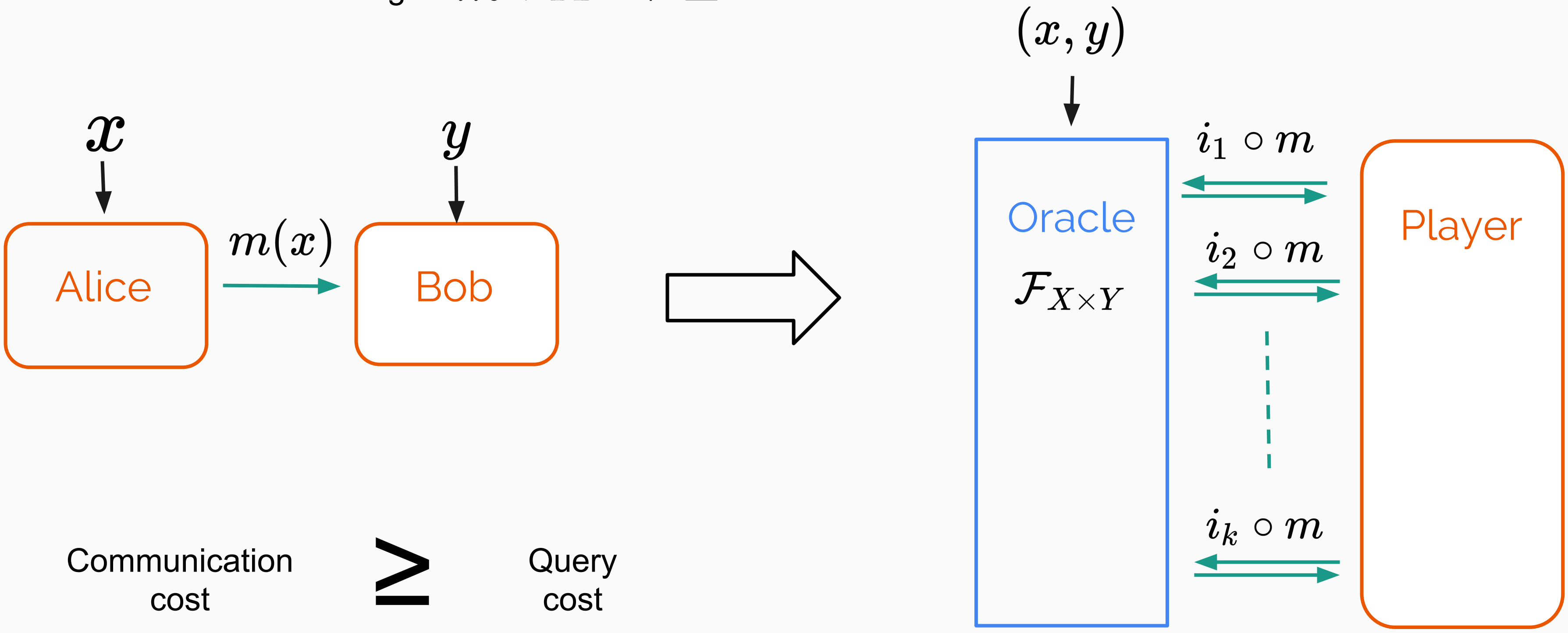


Communication model

Generalized query model

Proof: communication to query

Simulate a message $m : X \to \Sigma^k$

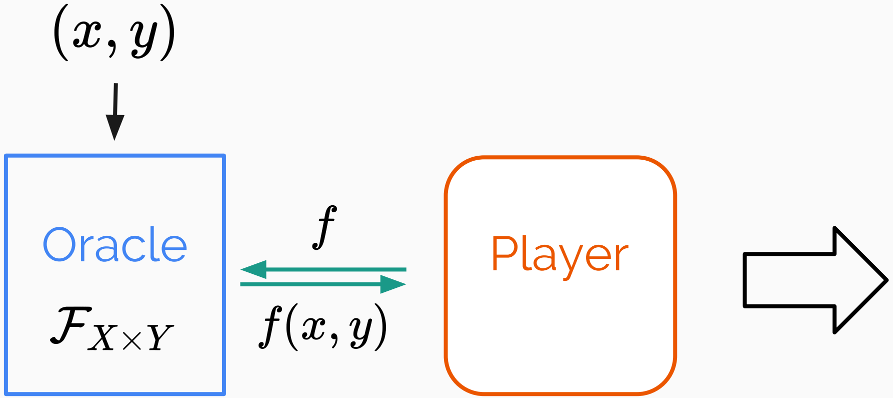


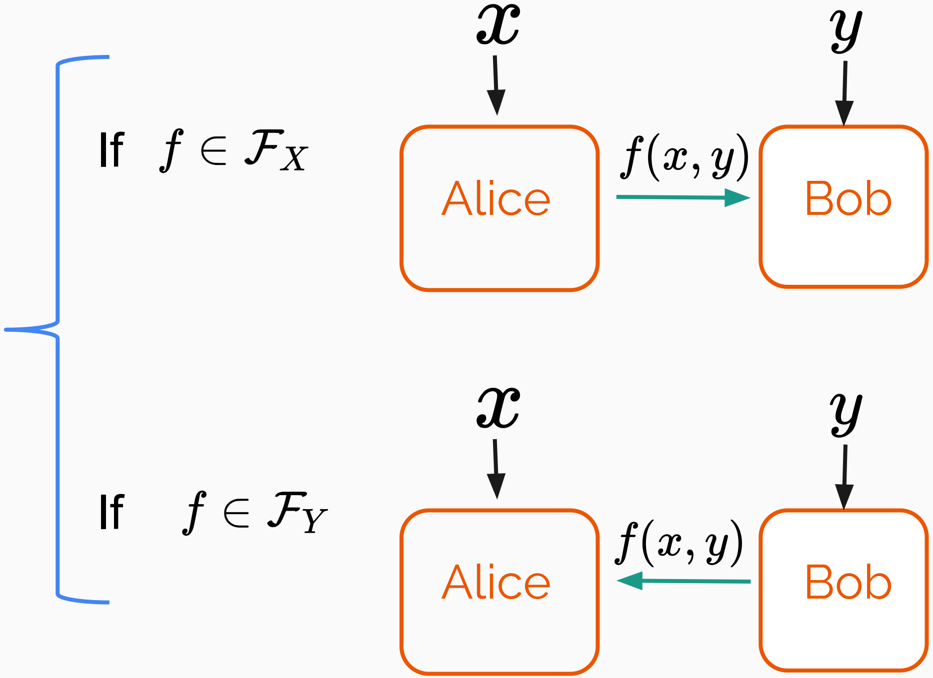
Communication cost $\geq$ Query cost

$\forall k \quad i_k \circ m \in \mathcal{F}_X$

Proof: query to communication

Simulate a query $f : X \times Y \to \Sigma$





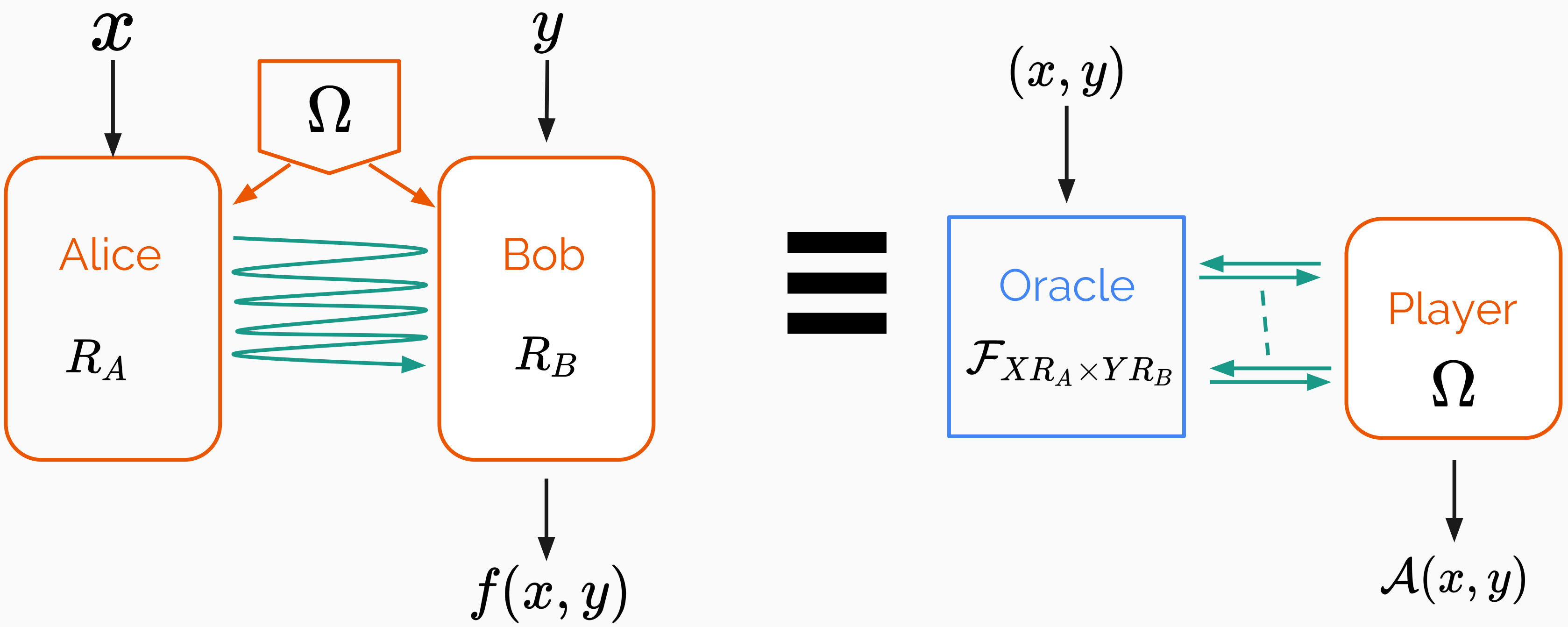
Communication cost $\leq$ Query cost

Extend to the equivalence to randomized models

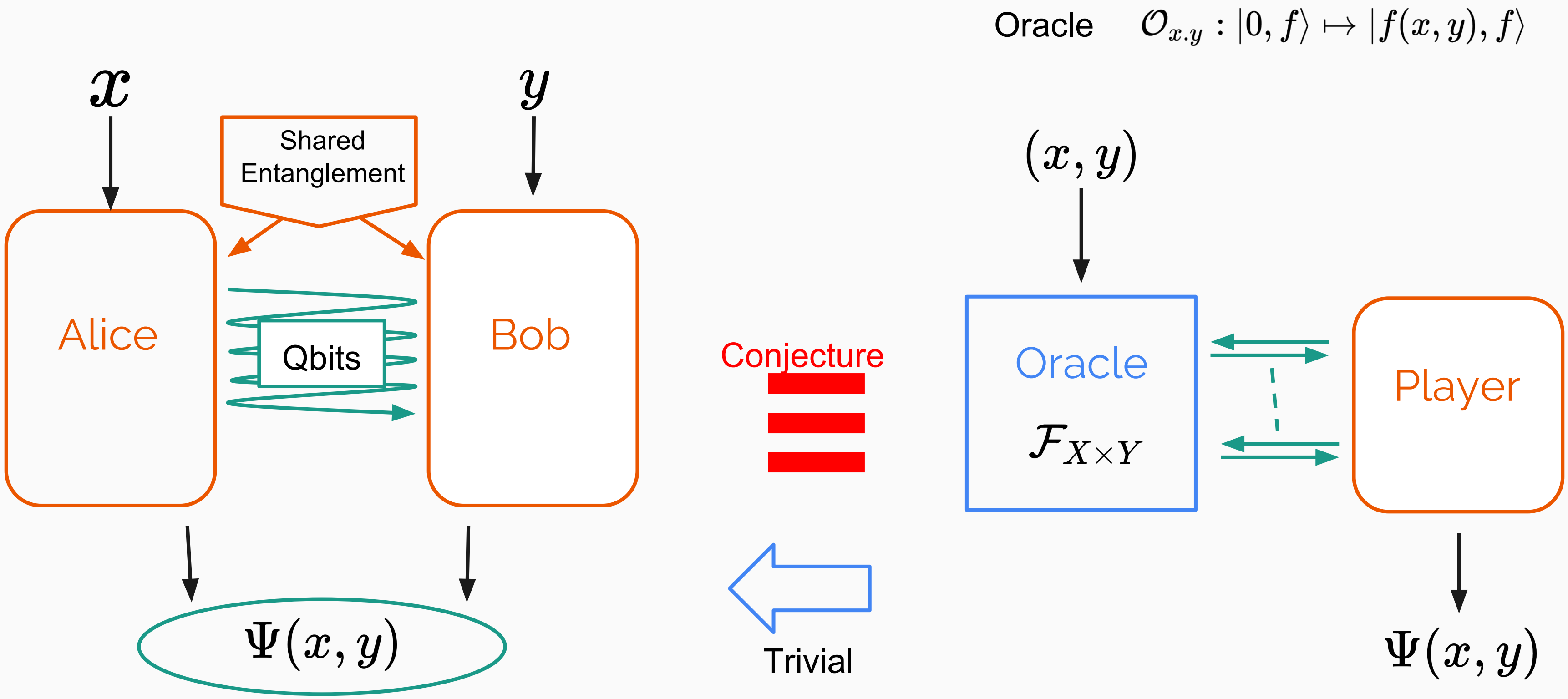
Ω : Shared randomness

R_A, R_B : Private randomness

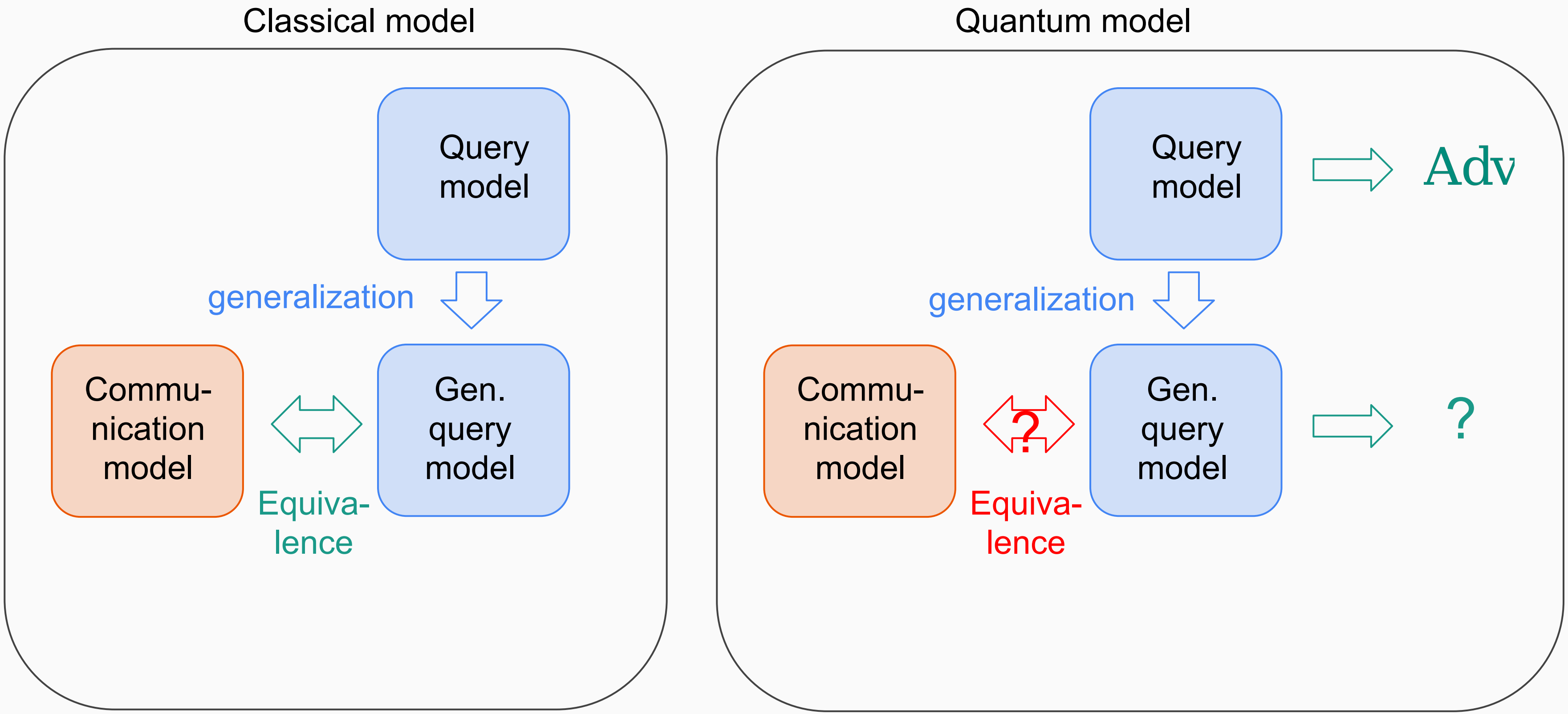
$$\mathcal{F}_{X,R_A} = \{f : X \times R_A \to \Sigma\}$$
$$\mathcal{F}_{Y,R_B} = \{f : Y \times R_B \to \Sigma\}$$
$$\mathcal{F}_{XR_A \times YR_B} = \mathcal{F}_{X,R_A} \uplus \mathcal{F}_{YR_B}$$



Extend the equivalence to quantum models?



Summary



Classical model
Query model
generalization
Commu-nication model
Gen. query model
Equiva-lence
Quantum model
Query model
Adv
generalization
Commu-nication model
?
Gen. query model
Equiva-lence
?

Adapt the Adversary method to generalized oracle

Adversary method

$$\mathrm{Adv}(f) = \max_{\Gamma,u} \mathrm{tr}([\Gamma \circ uu^*]F)$$

such that

$$\begin{cases} F(z,z') = 1 - \delta_{f(z),f(z')} \\ u \text{ is a unit vector} \\ \forall i \in \Pi, \quad \Gamma \circ \Delta_i \le Id \pm \Gamma \\ \text{where} \quad \Delta_i(z,z') = \delta_{i(z),i(z')} \end{cases}$$

Reminder $\Pi = \{\text{All projection functions}\}$

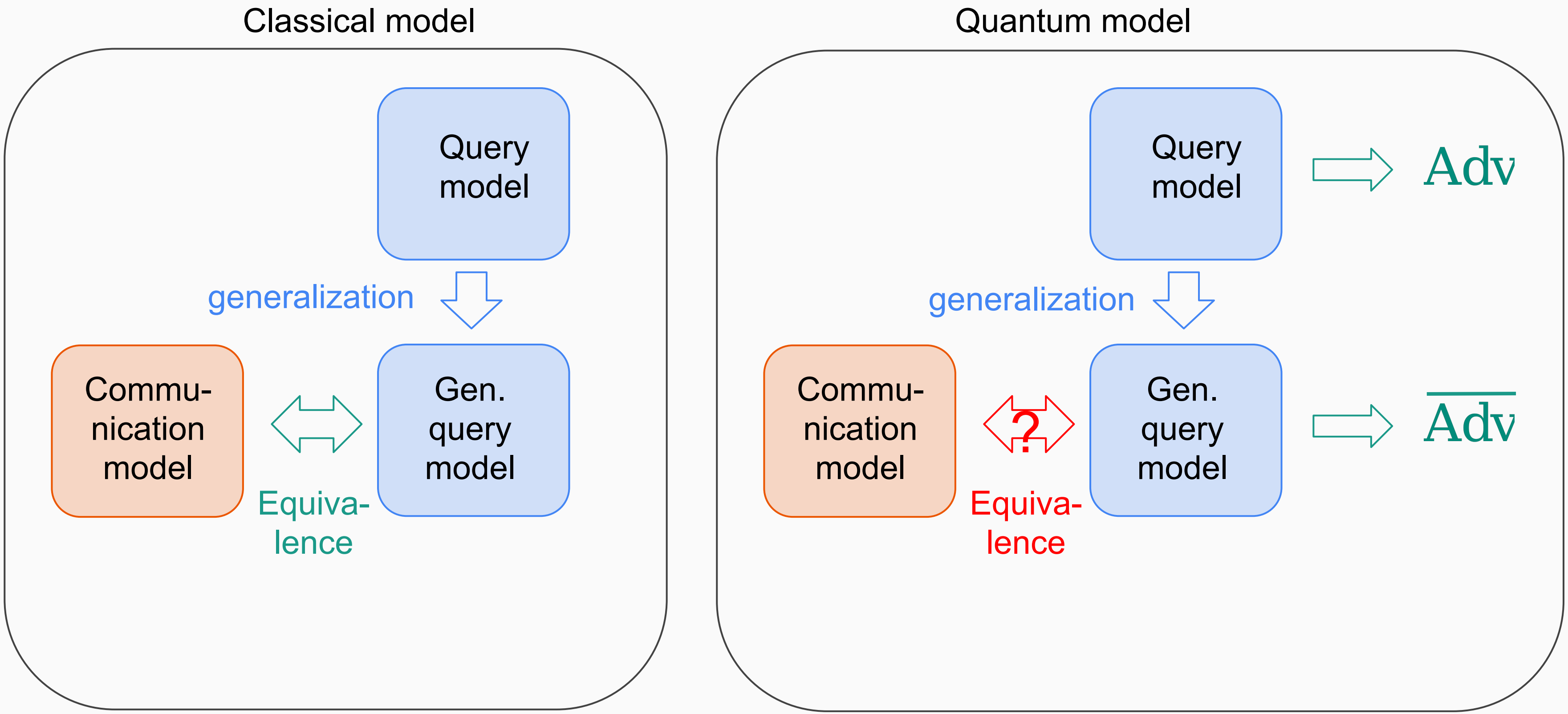
Generalized adversary method

$$\overline{\mathrm{Adv}}(f) = \max_{\Gamma,u} \mathrm{tr}([\Gamma \circ uu^*]F)$$

such that

$$\begin{cases} F(z,z') = 1 - \delta_{f(z),f(z')} \\ u \text{ is a unit vector} \\ \underline{\forall m \in \mathcal{F}_{X\times Y},} \quad \Gamma \circ \Delta_m \le Id \pm \Gamma \\ \text{where} \quad \boxed{\Delta_m(z,z') = \delta_{m(z),m(z')}} \end{cases}$$

Summary


Classical model
Query model
generalization
Commu-nication model
Gen. query model
Equiva-lence
Quantum model
Query model
Adv
generalization
Commu-nication model
?
Gen. query model
$\overline{\mathrm{Adv}}$
Equiva-lence