Quantum Computing based on Tensor Products
Communication Complexity

Guillermo Morales Luna

Computer Science Section
CINVESTAV-IPN

E-mail: gmorales@cs.cinvestav.mx

5-th International Workshop on Applied Category Theory
Graph-Operad Logic

Agenda

1. Quantum Cryptography
   - Channels without Noise
   - Channels with Noise

2. Communication Complexity
   - Parities Addition
   - Congruent Functions with the Hamming Weight Map
   - Identity Checking
   - Inner Product
   - Deutsch-Josza Relation

Agenda

1. Quantum Cryptography
   - Channels without Noise
   - Channels with Noise
2. Communication Complexity
   - Parities Addition
   - Congruent Functions with the Hamming Weight Map
   - Identity Checking
   - Inner Product
   - Deutsch-Josza Relation

Quantum Cryptography: Key Agreement Protocols

$E^0 = \{\mathbf{e}^0_0 = (1,0), \mathbf{e}^0_1 = (0,1)\}$: canonical basis of $\mathbb{H}_1$
$H(E^0) = E^1 = \{\mathbf{e}^1_0, \mathbf{e}^1_1\}$: basis of $\mathbb{H}_1$ obtained by applying Hadamard's operator to E^0.
E^0 corresponds to a spin with vertical–horizontal polarization, $E^0 = \{\uparrow, \rightarrow\}$, while
E^1 corresponds to a spin with oblique or NW–NE polarization, $E^1 = \{\nwarrow, \nearrow\}$.

Two entities, Alice and Bob, should agree in private a common key. They may use two transmission channels

Quantum channel Transmits just one-way, say from Alice to Bob.

Classical channel Transmits bidirectionally.

We will present the BB84 Protocol, without and with noise.

Channels without Noise

Protocol over the quantum channel

1. Alice generates randomly two bit sequences $\delta = [\delta_i]_{i=1}^N$ and $\varepsilon = [\varepsilon_i]_{i=1}^N$.
   She transmits through the quantum channel the state sequence $S = \left[\mathbf{s}_i = \mathbf{e}_{\delta_i}^{\varepsilon_i}\right]_{i=1}^N$.
2. Bob generates a bit sequence $\eta = [\eta_i]_{i=1}^N$ and measures each qubit $\mathbf{s}_i$ w.r.t. E^{η_i} to obtain a bit sequence $\zeta = [\zeta_i]_{i=1}^N$.
   Whenever $\varepsilon_i = \eta_i$, $\delta_i = \zeta_i$.
   He may expect around $N/2$ entries at δ and ζ to coincide.

Protocol over the classic channel

1. Bob transmits his sequence ζ to Alice.
2. Alice calculates $J = \{i \leq N | \zeta_i = \varepsilon_i\}$ corresponding to correct "guessings" of Bob, and she sends it back to Bob.
3. The restrictions $\delta|_J$ and $\zeta|_J$ shall coincide. That sequence, or just a portion of it, can be taken as the common key. The only way for δ and ζ to differ should be due to a third part, Eve, eavesdropping.

In order to check whether there has been an eavesdropping, Alice and Bob may exchange segments of their respective $\delta|_J$ and $\zeta|_J$. Whenever a segment has been exchanged, it is suppressed from the remaining sequences. If a difference appears in an exchange then Eve's eavesdropping is detected. Otherwise, it can be trusted with a higher probability that the common key has been agreed.

Channels with Noise

Protocol over the quantum channel

It is identical to the case before:

1. Alice generates randomly two sequences $\delta = [\delta_i]_{i=1}^N$ and $\varepsilon = [\varepsilon_i]_{i=1}^N$. She transmits through the quantum channel the state sequence $S = \left[\mathbf{s}_i = \mathbf{e}_{\delta_i}^{\varepsilon_i}\right]_{i=1}^N$, which may be altered by noise in quantum channel.
2. Bob generates a bit sequence $\eta = [\eta_i]_{i=1}^N$ and measures each qubit $\mathbf{s}_i$ w.r.t. E^{η_i} to obtain a bit sequence $\zeta = [\zeta_i]_{i=1}^N$.

Protocol over the classic channel

1. Bob transmits his sequence ζ to Alice.
2. Alice calculates the set $J = \{i \leq N | \zeta_i = \varepsilon_i\}$ corresponding to correct basis "guessings" of Bob, and she sends it back to Bob.
3. Bob calculates the set $K \subset J$ of indexes in which he could measure ζ_k. Bob sends K to Alice. Up to Eve's eavesdropping or channel noise, the current sequences should coincide, $\delta|_K = \zeta|_K$.
4. Thus, Bob and Alice communicate among themselves portions of $\delta|_K$ and $\zeta|_K$ and they calculate the rate R of discrepancies. If R is above a fixed threshold, the protocol is finished, with a failure condition, and it is reset to the very beginning.

5. Otherwise, a phase of reconciled key extraction is initiated: while the probability of a discrepancy occurrence is high, repeat the following:
    1. Alice and Bob agree, using a public channel, a permutation $\pi \in S_K$ and they apply it to their current sequences: $\delta|_K := \pi\left(\delta|_K\right)$ and $\zeta|_K := \pi\left(\zeta|_K\right)$.
    2. Alice and Bob cut their corresponding current sequences in blocks with uniform length, $\delta|_K = [\delta_\ell]_\ell$, $\zeta|_K = [\zeta_\ell]_\ell$, such that with a high probability each pair $\{\delta_\ell, \zeta_\ell\}$ contains at most one discrepancy.
    3. For each ℓ, the discrepancy at each pair $\{\delta_\ell, \zeta_\ell\}$ is found and the bit in that position is suppressed. In order to find the discrepancy at $\{\delta_\ell, \zeta_\ell\}$ a form of binary partition is applied:

        Initially, the parities of the current subsequences δ_c, ζ_c should differ. While the discrepancy bit has not been found, each of the current subsequence is divided at the middle entry and the corresponding halves with different parities are kept which will serve as the current subsequences in a new iteration.

6. Alice and Bob have corresponding sequences, of equal lengths, say k, which for practical purposes may coincide, even though this common reconciled key may also be partially known by Eve. Alice and Bob should start now a phase of privacy amplification:
    1. From the discrepancy rate R obtained at point 4., Alice and Bob calculate an upper bound of the number k_l of bits known by Eve.
    2. They fix a security parameter s and they agree to select $k - k_l - s$ segments of their reconciled key. The contents of these segments are kept in secret, and their parities will give a string of length $k - k_l - s$ to be assumed as the common key.

The Privacy Amplification Theorem states that after this protocol the number of bits in the common key, effectively known by Eve, will be upper bounded by $2^{-s} / \ln 2$.

Agenda

1. Quantum Cryptography
   - Channels without Noise
   - Channels with Noise

2. Communication Complexity
   - Parities Addition
   - Congruent Functions with the Hamming Weight Map
   - Identity Checking
   - Inner Product
   - Deutsch-Josza Relation

Communication Complexity

The complexity of a communication process is determined by the minimum information quantity that should be transmitted, in order that the total information can be recovered by the receiving part, within a given context.

Optimal Transmission

Let us assume that three sets X, Y, Z are given and a function $f : X \times Y \to Z$. At some moment, Alice, who is a communicating part, possesses a point $x \in X$, Bob, who is a second part, possesses a point $y \in Y$ and both parts should calculate $z = f(x, y)$, by interchanging the minimum information quantity.

In what follows $X = \{0, 1\}^n = Y$.

Parities Addition

Suppose

$$f:(x,y)\mapsto\left(\sum_i x_i+\sum_i y_i\right)\bmod 2$$

then it will be enough that Alice and Bob interchange two bits: the parities of x and y, in order that both be able to calculate $f(x,y)$.

Congruent Functions with the Hamming Weight Map

Suppose that for a map $g : \mathbb{N}^2 \to Z$, known by both Alice and Bob, $f = g \circ (H_n, H_n)$, where $H_n : \{0,1\}^n \to \mathbb{N}$ is the Hamming weight map. Then it will be enough that

- Alice sends the weight of x to Bob,
- Bob calculates $f(x, y)$ and
- Bob sends the result back to Alice.

In this case the transmission of the order of $\log_2 n$ bits of information is enough to complete the common task.

Identity Checking

Exact and obvious method

If $f : (x, y) \mapsto \chi_=(x, y)$ is the characteristic function of the identity relation:

$$f(x, y) = 1 \text{ if and only if } x = y,$$

then Alice and Bob should interchange n bits to calculate $f(x, y)$.

n is exponential with respect to its size!

Approximating solution requiring $O(\log_2 n)$ bits

Given $\varepsilon > 0$,

- let p be a prime number such that $n/\varepsilon > p$,
- let $\mathbb{F}_p$ be the prime field of characteristic p.
- Given her point x, Alice considers $A(X) = \sum_{i=0}^{n-1} x_i X_i \in \mathbb{F}_p[X]$, and
- Bob considers $B(X) = \sum_{i=0}^{n-1} y_i X_i \in \mathbb{F}_p[X]$.
- Alice chooses a random element $a \in \mathbb{F}_p$,
- she calculates $b = A(a)$ and sends the pair (a, b) to Bob,
- Bob proceeds to calculate $c = B(a)$.
- If $c \neq b$ then Bob will know for sure that $x \neq y$ and $f(x, y) = 0$. Otherwise he assumes $f(x, y) = 1$.
- Bob communicates his value of $f(x, y)$ to Alice.

If $c = b$, then either $x = y$ or Alice has chosen a root of the difference $(A - B)(x)$.
The probability of this last event is n/p, which is lower than ε.
Consequently Bob claims $f(x, y) = 1$ with an error probability lower than ε.
Besides, it is possible to choose the prime integer p such that

$$\frac{n}{\varepsilon} < p \leq \frac{2n}{\varepsilon}.$$

In this case, a and b are written with $2 + \log_2 n - \log_2 \varepsilon$ bits and this is the number of bits to be transmitted.

An alternative procedure

- Alice and Bob select a common set of m vectors $a_1, \dots, a_m \in \{0,1\}^n$, with $2^{-m} < \varepsilon$.
- Alice calculates $\overline{x} = (a_i \cdot x)_{i=1}^m \in \{0,1\}^m$ and transmits it to Bob
- Bob calculates $\overline{y} = (a_i \cdot y)_{i=1}^m$.
- If for some entry $i \leq m$ there is a discrepancy $(\overline{x})_i \neq (\overline{y})_i$ then Bob knows that for sure $x \neq y$.

  Otherwise Bob may decide that $x = y$ and the error probability is at most $2^{-m} < \varepsilon$.

An interesting question is whether an exact algorithm can be obtained with logarithmic complexity.
The following theorem excludes the possibility to communicate more than k (classical) bits of information by transmitting k qubits.

Holevo's Theorem

The information quantity recovered from a register of qubits is upperly bounded by the value of von Neumann's entropy, which is bounded by Shannon's entropy. Both entropies coincide whenever the qubits are pairwise orthogonal.

However, in Quantum Computing the use of the notion of entangled states improves the communication complexities of several procedures.

Inner Product

Let us consider the inner product of two vectors modulo 2,

$$(x, y) \mapsto \langle x|y\rangle = \left(\sum_i x_i y_i\right) \bmod 2$$

and let us assume that

$$P : \mathbb{H}_1 \otimes \mathbb{H}_n \otimes \mathbb{H}_n \to \mathbb{H}_1 \otimes \mathbb{H}_n \otimes \mathbb{H}_n \ , \ \ \mathbf{e}_a \otimes \mathbf{e}_x \otimes \mathbf{e}_y \mapsto \mathbf{e}_{a+\langle x|y\rangle} \otimes \mathbf{e}_x \otimes \mathbf{e}_y,$$

is a quantum algorithm to calculate this product.
Then it is possible to transform it to get a quantum algorithm to transmit a sequence of n bits, say from Alice to Bob.

Let as before $H : \mathbb{H}_1 \to \mathbb{H}_1$ be Hadamard's operator.

Tranforming an inner product calculator into an identitiy checker

1. Bob considers, initially, $\mathbf{y}_0 = \mathbf{e}_1 \otimes \mathbf{e}_{0^{(n)}}$.
2. Bob applies $H^{\otimes(n+1)}$:
$$\mathbf{y}_1 := H^{\otimes(n+1)}(\mathbf{y}_0) = \sqrt{2^{-(n+1)}} \sum_{a\in\{0,1\},\boldsymbol{\varepsilon}\in\{0,1\}^n} (-1)^a \mathbf{e}_a \otimes \mathbf{e}_{\boldsymbol{\varepsilon}}.$$
3. Alice and Bob apply the protocol P to obtain:

$$\begin{aligned}
\mathbf{y}_2 &:= P(\mathbf{e}_x, \mathbf{y}_1) \\
&= \sqrt{2^{-(n+1)}} \sum_{a\in\{0,1\},\boldsymbol{\varepsilon}\in\{0,1\}^n} (-1)^a \mathbf{e}_{a+\langle x|\boldsymbol{\varepsilon}\rangle} \otimes \mathbf{e}_{\boldsymbol{\varepsilon}} \\
&= \sqrt{2^{-(n+1)}} \sum_{c\in\{0,1\},\boldsymbol{\varepsilon}\in\{0,1\}^n} (-1)^{c+\langle x|\boldsymbol{\varepsilon}\rangle} \mathbf{e}_c \otimes \mathbf{e}_{\boldsymbol{\varepsilon}}
\end{aligned}$$

4. Bob applies again $H^{\otimes(n+1)}$ to obtain $\mathbf{y}_3 := H^{\otimes(n+1)}(\mathbf{y}_2) = \mathbf{e}_1 \otimes \mathbf{e}_x$.

Thus by measuring his last n qubits, Bob recovers the sequence x.
The transmission cost in this algorithm is the cost of its step 3. which is the cost of protocol P.

Protocol P

Since n is even,

$$\langle x|y\rangle = \sum_{j=0}^{n-1} x_j y_j = \sum_{j=0}^{n/2-1} \left(x_{2j}y_{2j} + x_{2j+1}y_{2j+1}\right) = \sum_{j=0}^{n/2-1} \Big\langle (x_{2j}, x_{2j+1}) | (y_{2j}, y_{2j+1}) \Big\rangle$$

thus it is enough to consider the inner product in $\mathbb{H}_1$.
If Alice possesses (x_0, x_1) and Bob (y_0, y_1), then they will be able to calculate directly $x_0y_0 + x_1y_1$ by transmitting 3 bits:

- say two from Alice to Bob, x_0 and x_1, and
- then a bit from Bob to Alice, which is the result $(x_0y_0 + x_1y_1) \bmod 2$.

However, it is possible to make the same calculation with a transmission of at most two qubits.
We will introduce two quantum algorithms, with and without entanglement.

Using an Entangled Pair of Qubits

In $\mathbb{H}_2$, registers of two qubits, the first qubit is proper of the transmitter, say Alice, and the second of the receiver, Bob.

Alice's 4 rotations, depending on possible configurations of her point $x = (x_0, x_1)$

$$A_{00} = \begin{bmatrix} \sqrt{\frac{2}{5}} & -i\,\sqrt{\frac{3}{5}} \\ -i\,\sqrt{\frac{3}{5}} & \sqrt{\frac{2}{5}} \end{bmatrix} \qquad A_{01} = \begin{bmatrix} \frac{2}{\sqrt{5}} & \frac{\sqrt{3}}{4} + i\,\frac{1}{4\sqrt{5}} \\ \frac{-\sqrt{3}}{4} + i\,\frac{1}{4\sqrt{5}} & \frac{2}{\sqrt{5}} \end{bmatrix}$$

$$A_{10} = \begin{bmatrix} \frac{2}{\sqrt{5}} & \frac{-\sqrt{3}}{4} + i\,\frac{1}{4\sqrt{5}} \\ \frac{\sqrt{3}}{4} + i\,\frac{1}{4\sqrt{5}} & \frac{2}{\sqrt{5}} \end{bmatrix} \qquad A_{11} = \begin{bmatrix} \frac{1}{\sqrt{5}} & i\,\frac{2}{\sqrt{5}} \\ i\,\frac{2}{\sqrt{5}} & \frac{1}{\sqrt{5}} \end{bmatrix}$$

Bob's 4 rotations, depending on possible configurations of his vector $y = (y_0, y_1)$

$$B_{00} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \qquad B_{01} = \begin{bmatrix} \sqrt{\frac{3}{5}} & -\frac{1}{2} + i\,\frac{1}{2}\,\sqrt{\frac{3}{5}} \\ -\frac{1}{2} - i\,\frac{1}{2}\,\sqrt{\frac{3}{5}} & -\sqrt{\frac{3}{5}} \end{bmatrix}$$

$$B_{10} = \begin{bmatrix} \sqrt{\frac{3}{5}} & \frac{1}{2} + i\,\frac{1}{2}\,\sqrt{\frac{3}{5}} \\ -\frac{1}{2} + i\,\frac{1}{2}\,\sqrt{\frac{3}{5}} & \sqrt{\frac{3}{5}} \end{bmatrix} \quad B_{11} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

(B_{00} is not a rotation: if Bob knows that his vector y is null, he knows that the protocol should output the value 0, independently of Alice's vector).

Procedure with entanglement

1. Alice and Bob share the entangled state

$$\mathbf{z}_0 = \frac{1}{\sqrt{2}}(\mathbf{e}_{00} + \mathbf{e}_{11}) = \frac{1}{\sqrt{2}}(\mathbf{e}_0 \otimes \mathbf{e}_0 + \mathbf{e}_1 \otimes \mathbf{e}_1)$$

and both have access to it (this is a form of teleportation due to the so called Einstein-Podolsky-Rosen (EPR) paradox.)

2. Alice applies in her qubit the corresponding rotation $A_{x_0 x_1}$:

$$\mathbf{z}_1 = \begin{bmatrix} A_{x_0 x_1} & \mathbf{0} \\ \mathbf{0} & \mathbf{1}_2 \end{bmatrix} \mathbf{z}_0 .$$

3. Alice makes a measurement of her qubit, she obtains the bit m_0 and sends it to Bob.

4. If Bob sees that $y = (0,0)$ then he knows that the ending value should be $v = 0$, otherwise
    1. he applies in his qubit the corresponding rotation $B_{y_0 y_1}$:

    $$\mathbf{z}_2 = \left[\begin{array}{cc} \mathbf{1}_2 & \mathbf{0} \\ \mathbf{0} & B_{y_0 y_1} \end{array}\right] \mathbf{z}_0,$$

    2. he makes a measurement of his qubit to obtain the bit m_1, and
    3. he calculates $v = (m_0 + m_1) \bmod 2$.
5. Bob sends to Alice the value v which is the alleged inner product value.

This procedure transmits two (classic) bits, requires an entangled pair of qubits and produces the correct value with a probability no lesser than $\frac{4}{5}$.

Algorithm without Entangled States

Alice's initial qubit, depending on her vector $x = (x_0, x_1)$

$$\mathbf{z}_{00} = \sqrt{\tfrac{2}{5}}\mathbf{e}_0 - i\,\sqrt{\tfrac{3}{5}}\mathbf{e}_1 \qquad \mathbf{z}_{01} = \sqrt{\tfrac{4}{5}}\mathbf{e}_0 + \left(\frac{\sqrt{3}}{4} + i\,\frac{1}{4\,\sqrt{5}}\right)\mathbf{e}_1$$

$$\mathbf{z}_{10} = \sqrt{\tfrac{4}{5}}\mathbf{e}_0 + \left(-\frac{\sqrt{3}}{4} + i\,\frac{1}{4\,\sqrt{5}}\right)\mathbf{e}_1 \quad \mathbf{z}_{11} = \sqrt{\tfrac{1}{5}}\mathbf{e}_0 - i\,\sqrt{\tfrac{4}{5}}\mathbf{e}_1$$

Procedure

1. Alice sends to Bob her qubit $\mathbf{z}_{x_0 x_1}$.
2. If Bob sees that $y = (0,0)$ then he knows that the ending inner product value is $v = 0$, otherwise
    1. he applies his corresponding rotation $B_{y_0 y_1} : \mathbf{z} = B_{y_0 y_1} \mathbf{z}_{x_0 x_1}$, and
    2. he makes a measurement to obtain the bit v.
3. Bob sends to Alice the value v which is the alleged inner product value.

This procedure transmits one qubit and one classic bit and has the same correctness rate $\frac{4}{5}$.

Deutsch-Josza Relation

Pseudotelepathy Game

Given four sets X, Y, A and B, a relation $R \subset X \times and \times A \times B$, and the fact that Alice and Bob are separated, far from each other, at a given moment Alice receives a point $x \in X$, Bob a $y \in Y$ and they, trying to interchange the minimum information, should produce, respectively, $a \in A$ and $b \in B$ such that $(x, y, a, b) \in R$.

In particular, for $n = 2^k$ a power of 2, $X = \{0,1\}^n = Y$, $A = \{0,1\}^k = B$

R is Deutsch-Josza relation

$$
\begin{aligned}
&(x, y, a, b) \in R \;\; \Leftrightarrow \\
&\left[(H_n(x,y) = 0 \;\wedge\; a = b) \;\vee\; \left(H_n(x,y) = \frac{n}{2} \;\wedge\; a \neq b\right) \;\vee\right. \\
&\left. H_n(x,y) \notin \left\{0, \frac{n}{2}\right\}\right]
\end{aligned}
\qquad (1)
$$

- If the points x and y of Alice and Bob coincide, then the sequences that they produce should coincide
- If x and y differ exactly in half of the bits, then the produced sequences should differ
- In any other case no restrictions on produced sequences

In the space $\mathbb{H}_{2n}$, Alice and Bob create the entangled register of $2n$-qubits

$$\mathbf{z} = \sum_{(\varepsilon_{k-1},\ldots,\varepsilon_1,\varepsilon_0)\in\{0,1\}^k} 2^{-\frac{k}{2}} \mathbf{e}_{\varepsilon_{k-1}\cdots\varepsilon_1\varepsilon_0} \otimes \mathbf{e}_{\varepsilon_{k-1}\cdots\varepsilon_1\varepsilon_0}. \tag{2}$$

Clearly, in $\mathbb{H}_{2n}$:

$$\begin{aligned}\mathbf{z} &= \sum_{(\varepsilon_{k-1},\ldots,\varepsilon_1,\varepsilon_0)\in\{0,1\}^k} 2^{-\frac{k}{2}} \bigotimes_{i=0}^{k-1} (\mathbf{e}_{\varepsilon_i} \otimes \mathbf{e}_{\varepsilon_i}) \\ &= \bigotimes_{i=0}^{k-1} \left(\frac{1}{\sqrt{2}} \mathbf{e}_0 \otimes \mathbf{e}_0 + \frac{1}{\sqrt{2}} \mathbf{e}_1 \otimes \mathbf{e}_1 \right) \\ &= \bigotimes_{i=0}^{k-1} \left(\frac{1}{\sqrt{2}} \mathbf{e}_{00} + \frac{1}{\sqrt{2}} \mathbf{e}_{11} \right) \end{aligned} \tag{3}$$

or equivalently, $\mathbf{z} = \mathbf{z}_0^{\otimes k}$, where $\mathbf{z}_0 = \frac{1}{\sqrt{2}}\mathbf{e}_{00} + \frac{1}{\sqrt{2}}\mathbf{e}_{11} = \frac{1}{\sqrt{2}}\left(\mathbf{e}_{00} + \mathbf{e}_{11}\right)$ is an entangled pair of qubits.

Given $x = (x_i)_{i=0}^{n-1}$, $y = (y_i)_{i=0}^{n-1} \in \{0,1\}^n$ to Alice and Bob

- Identify $[\![0, n-1]\!]$ with $\{0,1\}^k$, $i = (\varepsilon_{k-1}\cdots\varepsilon_1\varepsilon_0)_2 = (\varepsilon)_2$.
- Alice calculates $M : \mathbb{H}_k \to \mathbb{H}_k$, $\mathbf{e}_{\boldsymbol{\varepsilon}} \mapsto (-1)^{x_i}\mathbf{e}_{\boldsymbol{\varepsilon}}$, and
- Bob, calculates the map $N : \mathbf{e}_{\boldsymbol{\varepsilon}} \mapsto (-1)^{y_i}\mathbf{e}_{\boldsymbol{\varepsilon}}$.
- Thus, the result of both maps over the entangled state $\mathbf{z}$ is

$$\mathbf{w} = (M,N)(\mathbf{z}) = \sum_{(\varepsilon_{k-1},\ldots,\varepsilon_1,\varepsilon_0)\in\{0,1\}^k} 2^{-\frac{k}{2}}(-1)^{x_i+y_i}\mathbf{e}_{\varepsilon_{k-1}\cdots\varepsilon_1\varepsilon_0}\otimes\mathbf{e}_{\varepsilon_{k-1}\cdots\varepsilon_1\varepsilon_0}.$$

- Alice applies Hadamard's operator H to each of her qubits: $\mathbf{v}_A = H^{\oplus k}(\Pi_1(\mathbf{w}))$; and
- Bob proceeds similarly: $\mathbf{v}_B = H^{\oplus k}(\Pi_2(\mathbf{w}))$.
- Alice makes measurements on her k-qubits to get $a \in \{0,1\}^k$.
- Bob proceeds similarly and obtains $b \in \{0,1\}^k$.

One can see that the tuple (x, y, a, b) satisfies relation R.