COMP 598: Non-local Games and Communication Complexity

Eric Hanson[1]

[1] *McGill University, Montreal, Quebec, Canada*

(Dated: April 18, 2013)

Synthesizing some of the literature on non-local games and communication complexity scenarios provides a deeper understanding of the fundamental differences between classical mechanics and quantum mechanics, as exemplified by the quantum violation of Bell inequalities, which hold in classical mechanics. Quantum mechanical protocols are shown to provide significant advantages in certain tasks over classical protocols, and could create the first loophole-free demonstration of quantum non-locality. Non-local games are a scenario where two players attempt to perform a task without communication; communication complexity scenarios generalize non-local games by allowing but attempting to minimize communication. Completing the circle, communication complexity tasks naturally draw forth new non-locality scenarios.

Keywords: quantum information theory; non-local games; communication complexity scenarios; Bell inequalities; quantum mechanics

CONTENTS

I. INTRODUCTION

As forms of Bell inequalities, non-local games and communication complexity scenarios can be used to highlight the profound differences between quantum mechanics and classical theories. Non-local games, such as the odd-cycle game, use entanglement to accomplish otherwise-impossible tasks, or to perform them with a significantly better rate of success [1–3]. This quantum-classical separation could be used to provide the first loophole-free experimental demonstration of a Bell inequality [2] (even as of April 2013, such a demonstration has not been performed [4]; either the detectors used are too inefficient to rule out classical correlations, or are too close together to be non-local). For some classes of non-local games, upper bounds on the quantum success rate can be found in terms of the classical success rate; upper bounds below 1 are useful when games are interpreted as multi-prover interactive proof systems, in which case one wishes the verifier to be able to accurately reject invalid proofs [1].

For example, in the magic square game, the two players Alice and Bob attempt to convince a third-party verifier that there exists a three-by-three matrix with ± 1 entries such that the product of the entries of any row is $+1$ and any column is -1 (a "magic square"). Such a matrix cannot exist, as can be easily shown by computing the product of every entry by multiplying the product of the rows ($+1$) and by multiplying the product of the columns (-1). The verifier asks Alice for all three entries of a row or column of a purported magic square, and Bob for one of those entries; Alice's response must fulfill the parity constraints, and Bob's response must be consistent with Alice's. It can be shown that the best possible classical strategy (i.e. one that does not employ entanglement) can win with probability $17/18$, while a quantum strategy can win with probability 1 [1]. If implemented experimentally, the magic square game would provide convincing evidence of non-locality even to those unfamiliar of the details of quantum mechanics, and so succeeds as a *pseudo-telepathic* game [2]; that is, someone unacquainted with quantum mechanics would have as much reason to believe that Alice and Bob were telepathic as any other explanation. However, in the spirit of multi-prover interactive proof systems, as the quantum strategy succeeds with probability 1, the procedure of asking Alice for a row or column and Bob for an element of that row or column provides a poor method for proving that a magic square exists.

On the other hand, in the odd-cycle game, in which two parties attempt to convince a referee that an odd-cycle can be two-coloured (a similarly impossible task to creating a magic square), neither classical nor quantum strategies can achieve unity success rate. The odd-cycle game will be examined in detail in section II A, as it provides a concrete example of a type of non-local game for which upper bounds of the optimal success rate of quantum strategies can be determined (see section II D).

Similarly to non-local games, communication-complexity scenarios analyze how much communication is required between two parties to accomplish a task. Quantum communication can be used to provide an exponential advantage over classical strategies, as demonstrated by Raz's problem (featured in section III B), despite Holevo's bound (see section III A). Additionally, by formulating new non-locality scenarios from communication complexity scenarios, one can use entanglement to exponentially reduce the classical communication required to solve, for example, the hidden matching problem (see sections III C and III D).

II. NON-LOCAL GAMES AND PSEUDO-TELEPATHY

A non-local game is one in which two players Alice and Bob attempt to perform a task without communication; they are allowed shared randomness and local operations, as well as shared entanglement. Often the task is framed as an attempt to convince a third-party verifier of some fact.

A non-local game is called *pseudo-telepathic* in the spirit of [2] if there exists a quantum strategy (i.e. one using entanglement) which wins the game, but no classical strategy can win the game; the magic square game described in the introduction is an example of such a game. In such cases, a verifier who does not know quantum mechanics would not be able to distinguish Alice and Bob from telepaths via that non-local game.

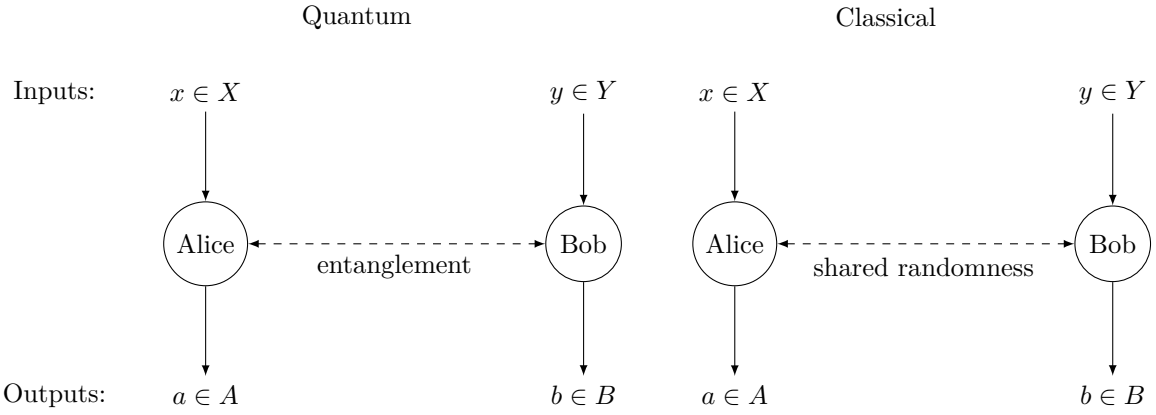


FIG. 1: Diagrams of a non-local game with quantum Alice and Bob (left) and classical Alice and Bob (right). In either situation, Alice and Bob receive an input, perform local operations, and respond with an output.

The following formal definition of a non-local game is adopted from [2]:

A two-party game is a sextuple of sets $G = \langle X, Y, A, B, P, W \rangle$. X and Y are input sets to Alice and Bob respectively and A and B are output sets from Alice and Bob respectively. $P \subseteq X \times Y$ is the *promise* which defines legitimate inputs for Alice and Bob, and $W \subseteq X \times Y \times A \times B$ is the *winning condition* which defines which combinations of outputs and inputs together constitute winning the game.

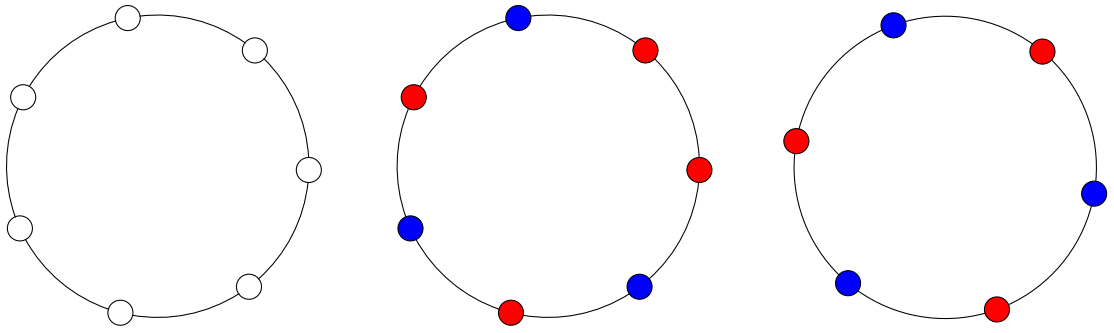
Before the game begins, Alice and Bob can decide on a strategy and exchange classical information. At the start of the game, Alice and Bob are separated and given an input, respectively $x \in X$ and $y \in Y$. Then, only using local operations, shared randomness, and, for quantum Alice and Bob, entanglement (which can simulate shared randomness), Alice and Bob each produce output $a \in A$ and $b \in B$, respectively.

If the promise is not fulfilled, Alice and Bob win by default; otherwise, they need to produce appropriate output defined by the winning condition, in order to win the game. The *probability of winning the game* for a given strategy is the probability that Alice and Bob win the game when they are given inputs uniformly randomly selected from the set of inputs which satisfy the promise.

A. The Odd-Cycle Game

In graph theory, graphs are described by vertices connected together by edges. An n-cycle graph is n vertices connected in a closed loop, where every vertex has two adjacent edges and there are the same number of edges as vertices. A 2-colourable graph is one in which each vertex is assigned one of two colours, and no two adjacent vertices are assigned the same color; see figure 2 for examples of odd-cycles and 2-colouring. Clearly, odd-cycles cannot be 2-coloured.

As presented and analyzed in [1], the odd-cycle game consists of Alice and Bob attempting to convince the verifier that they have done the impossible and 2-coloured an odd-cycle.



(a) (b) (c)

FIG. 2: (a): an example of an odd-cycle; here, the number of vertices $n = 7$. (b): an unsuccessful attempt to 2-colour the same 7-cycle. (c): a 2-coloured 6-cycle.

In the n-cycle game, for $n \geq 3$ odd, $X = Y = \{1, 2, \ldots, n\}$ and Alice and Bob are given an $x \in X$ and $y \in Y$ respectively (corresponding to a vertex). Alice and Bob are to each respond with a 0 or 1 corresponding to two possible colours. The promise is that either $y \equiv x + 1 \pmod{n}$ or $y = x$ (i.e. they were either given adjacent vertices or the same vertex). The winning condition is that, if the promise is fulfilled, Alice's output $a \in A = \{0, 1\}$ and Bob's output $b \in B = \{0, 1\}$ satisfies $a = b$ if $x = y$ and $a \neq b$ if $x \neq y$. In the language of cycle graphs, Alice and Bob win if they report back an appropriate colouring for their inputs: different colours for adjacent vertices and the same colour for the same vertex. Note that for legitimate inputs $(x, y) \in P$ then

$$W(x, y, a, b) = \begin{cases} 1 & \text{if } a \oplus b = [y + 1 \equiv x \pmod{n}] \\ 0 & \text{otherwise} \end{cases}$$

That is, $W(x, y, a, b) = 1$ if $a \oplus b = 1$ and $y + 1 \equiv x \pmod{n}$ or $a \oplus b = 0$ and $y + 1 \not\equiv x \pmod{n}$, and $W(x, y, a, b) = 0$ otherwise. This is because if x and y are adjacent, Alice and Bob win if their outputs differed, and if $x = y$, Alice and Bob win when their outputs are the same.

Any deterministic classical strategy amounts to attempting to 2-colour such an odd-cycle before the game starts, and then reading off the colours from that cycle. As an odd-cycle cannot be 2-coloured, no deterministic strategy can win every time, so the strategy must fail for one of the pairs (x, y) of legitimate x, y. There are $2n$ such pairs: n pairs of the form (x, x) and n of the form $(x, x + 1 \pmod{n})$. Hence, a classical strategy can win at best with probability $1 - \frac{1}{2n}$; such a strategy can be achieved by "2-colouring" all but one vertex, and assigning either colour to that one, just as in figure 2 (b). More formally, Alice and Bob share a 2-coloured $(n-1)$-cycle and then insert an additional vertex assigned one of the two colours; Alice and Bob then report back the colour of the vertex corresponding to their inputs to win with probability $1 - \frac{1}{2n}$. Any stochastic (non-deterministic) strategy is simply a probabilistic combination of deterministic strategies, and so cannot win with higher probability [1].

Using a quantum strategy, however, Alice and Bob can do quadratically better. They begin by sharing a maximally entangled state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

Motivated by the idea of Alice and Bob each rotating the shared state as in the proof of the optimal quantum strategy for the CSCH strategy presented in [3], define

$$|\varphi_0(\theta)\rangle := \cos(\theta)|0\rangle + \sin(\theta)|1\rangle$$
$$|\varphi_1(\theta)\rangle := -\sin(\theta)|0\rangle + \cos(\theta)|1\rangle$$

so that

$$R(\theta) = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} = \begin{pmatrix} |\varphi_0(\theta)\rangle & |\varphi_1(\theta)\rangle \end{pmatrix}$$

also define angles

$$\begin{aligned} \beta_y &:= \left(\tfrac{\pi}{2n} - \tfrac{\pi}{2}\right) y \\ \alpha_x &:= \beta_x + \tfrac{\pi}{4n} = \left(\tfrac{\pi}{2n} - \tfrac{\pi}{2}\right) x + \tfrac{\pi}{4n} \end{aligned}$$

and measurement operators

$$\begin{aligned} A_x^a &:= |\varphi_a(\alpha_x)\rangle\langle\varphi_a(\alpha_x)| \\ B_y^b &:= |\varphi_b(\beta_y)\rangle\langle\varphi_b(\beta_y)| \end{aligned}$$

Alice chooses the set of projective matrices corresponding to her input x: $\{A_x^a : a \in A\}$ and measures her half of the entangled state; she reports the outcome a. Similarly, Bob measures his half of the entangled state using $\{B_y^a : b \in B\}$ and reports the outcome b.

Exercises:

1. Show that if Alice and Bob receive the same vertex, they win the game with probability $\cos^2\left(\frac{\pi}{4n}\right)$ using this strategy.

2. Show that Alice and Bob always win the game with probability $\cos^2\left(\frac{\pi}{4n}\right)$ using this strategy.

See page 13 for solutions.

Note that $\cos^2\left(\frac{\pi}{4n}\right) \geq 1 - \left(\frac{\pi}{4n}\right)^2$, so this quantum strategy performs quadratically better than the best classical strategy. Below, in the section II D, it will be shown as the result of a more general theorem that this quantum success rate is optimal.

B. An Alternate Definition of Quantum Strategies for Non-local Games

Earlier, quantum strategies were unrestricted, as in [2]; Alice and Bob were allowed to do any local operations they wished. However, a (naively) more restrictive definition of quantum admits bounds on its performance as compared to an optimal classical strategy [1].

This definition (from [1]) is as follows: Alice and Bob each start with a copy of $\mathbb{C}^n$, called $\mathcal{A}$ and $\mathcal{B}$ respectively, and share a state $|\psi\rangle \in \mathcal{A}\otimes\mathcal{B}$. Alice has a set of measurement operators $\{A_x^a : a \in A\}$ for each input $x \in X$, and similarly Bob has a set of measurement operators $\{B_y^a : b \in B\}$ for each input $y \in Y$. Given input $(x, y) \in P$, Alice uses $\{A_x^a : a \in A\}$ to measure her half of $|\psi\rangle$ and reports back the outcome a; similarly, Bob uses $\{B_y^b : b \in B\}$ to measure his half of $|\psi\rangle$ and reports back the outcome b. Clearly, the strategy used above for the odd-cycle game fits this definition of a quantum strategy. However, this definition is actually equivalent to the original, unrestricted definition.

In a general quantum strategy, Alice and Bob are allowed any local operations. Consider a coherent implementation of such a strategy. Because Alice and Bob cannot communicate, any general strategy simply consists of Alice and Bob implementing a series of unitaries independently; the composition of unitaries is unitary, so Alice and Bob could equivalently simply each implement a single unitary. Thus, the seemingly more restrictively type of quantum strategy is actually equivalent to the general type.

C. Binary Games

A binary game is a non-local game in which Alice and Bob only output bits; that is, $A = B = \{0, 1\}$. For the case of binary games, quantum strategies can be assumed to only use projective measurements instead of general measurements [1]; adding ancillary spaces is not needed, so this result is nontrivial. Additionally, any binary game that has a perfect quantum strategy has a perfect classical strategy [1]. This fact is specific to binary games; for example, the magic square game has a perfect quantum strategy but imperfect optimal classical strategy. Hence, binary games cannot be pseudo-telepathic, at least in the sense of [2].

Of course, pseudo-telepathy is not the only property of interest; binary games are simpler than other games, in the sense that they have the minimal output set for Alice and Bob; they may also be experimentally easier to implement, and so could succeed in a major goal of pseudo-telepathic games - a loophole free demonstration of a Bell inequality - despite not being pseudo-telepathic. In fact, a recent proposal for such a demonstration is based on the CHSH inequality [4] which itself can be implemented as a binary game [1].

This relationship between classical and quantum maximal success rates is strengthened for a subset of binary games featured in the next section.

D. Binary XOR Games

A binary XOR game is a non-local game in which the winning condition $W(a, b, x, y)$ only depends on the bit $a \oplus b$ and not on a and b separately; $W(a, b, x, y)$ in this case is written as $W(a \oplus b, x, y)$ to emphasize its dependence on only three inputs. The odd-cycle game is an example of such a game. Upper bounds on the maximal success rate of quantum strategies for binary XOR games can be found in terms of the success rate of the optimal classical strategy.

First, define the trivial strategy to be the strategy where Alice and Bob report uniformly random bits to the verifier, regardless of their input; denote the success rate of the trivial strategy for a non-local game G by $\tau(G)$. Similarly, for a game G, call the maximal success rate of quantum strategies $\omega_q(G)$ and for classical strategies $\omega_c(G)$.

The bound in equation 4 uses Grothendieck's theorem [5]:

There exists a universal constant which is the smallest number K_G such that for all integers $N \geq 2$ and all $N \times N$ real matrices M which satisfy

$$\left| \sum_{i,j} M_{i,j} a_i b_j \right| \leq 1 \tag{1}$$

where $M_{i,j}$ are the entries of M, for all $a_1, \ldots, a_N, b_1, \ldots, b_N \in [-1, 1]$, the following holds:

$$\left| \sum_{i,j} M_{i,j} \langle u_i | v_j \rangle \right| \leq K_G \tag{2}$$

for all unit vectors $|u_1\rangle, \ldots, |u_N\rangle, |v_1\rangle, \ldots, |v_N\rangle$ in $\mathbb{R}^n$ (for any n).

Later work [6, 7] has shown that

$$1.6769 \leq K_G < \frac{\pi}{2 \log\left(1 + \sqrt{2}\right)} \approx 1.7822 \tag{3}$$

Cleve et al. [1] have shown that

$$\omega_q(G) - \tau(G) \leq K_G \left(\omega_c(G) - \tau(G)\right) \tag{4}$$

For any binary XOR game G.

Here's a (brief) sketch of the proof: Tsirelson's correspondence [8] establishes an equivalence between the existence of observables and the existence of collections of unit vectors. The collections of measurement operators of a quantum strategy (using the restricted definition discussed in section II B) are formulated as observables and associated with vectors according to Tsirelson's correspondence. The probability that Alice and Bob's answers are equal is calculated in terms of these unit vectors and the winning condition W is employed to form an expression for the probability of Alice and Bob winning the game (and the probability of the trivial strategy winning is subtracted). The maximum over vectors associated to observables of this expression gives the difference $\omega_q(G) - \tau(G)$.

Then a matrix satisfying equation 1 is constructed so that the maximization can be written as Grothendieck's inequality (equation 2), and the result is obtained.

This bound is most descriptive when $\omega_c(G)$ is close to $\tau(G)$; another bound is more useful for games with a strong classical strategy:

$$\omega_q(G) \leq \begin{cases} \gamma_1 \omega_c(G) & \text{if } \omega_c(G) \leq \gamma_2 \\ \sin^2\left(\frac{\pi}{2}\omega_c(G)\right) & \text{if } \omega_c(G) > \gamma_2 \end{cases} \tag{5}$$

where the constants γ_1 and γ_2 are defined implicitly by the relationship $\frac{\pi}{2}\sin(\pi\gamma_2) = \frac{\sin^2\left(\frac{\pi}{2}\gamma_2\right)}{\gamma_2} = \gamma_1$ which yields $\gamma_1 \approx 1.1382$ and $\gamma_2 \approx 0.74202$.

To prove the second bound, equation 5, a classical strategy is formulated in terms of the measurement operators of an optimal quantum strategy and a shared random vector (the orientation of which introduces the trigonometry that shows up in the final bound). A similar method was used in Grothendieck's proof of the existence of K_G [1].

Applying equation 5 to the odd-cycle game, we have $\omega_c = 1 - \frac{1}{2n}$, so for large n,

$$\omega_q = \sin^2\left(\frac{\pi}{2} - \frac{1}{4n}\right) = \cos^2\left(\frac{\pi}{4n}\right)$$

Thus, strategy in section II A is optimal.

III. COMMUNICATION COMPLEXITY

Communication complexity scenarios generalize non-local games by allowing Alice and Bob shared randomness and (depending on the situation) entanglement, as well as some communication; the goal of protocols in this setting is to minimize the amount of communication needed to compute a function dependent on the input to Alice and Bob. Note that quantum communication can simulate entanglement and shared randomness.

Buhrman et al. present a formal definition of a communication complexity scenario [3]:

Alice and Bob wish to compute a function $f : \mathcal{D} \to \{0, 1\}$, where $\mathcal{D} \subseteq X \times Y$; often, $X = Y = \{0, 1\}^n$. If the domain $\mathcal{D} = X \times Y$, f is called a total function; otherwise, f is a promise function. If f is a promise function, the scenario's promise is a predicate $P \subseteq X \times Y$ that determines which $(x, y) \in X \times Y$ are valid. Alice receives $x \in X$ and Bob receives $y \in Y$; in some scenarios, they also start with shared ebits or shared randomness. Then Alice and Bob execute a protocol by each performing local operations and communicating in order to compute f. In quantum protocols, Alice and Bob use quantum states and can access quantum channel; in classical protocols, Alice

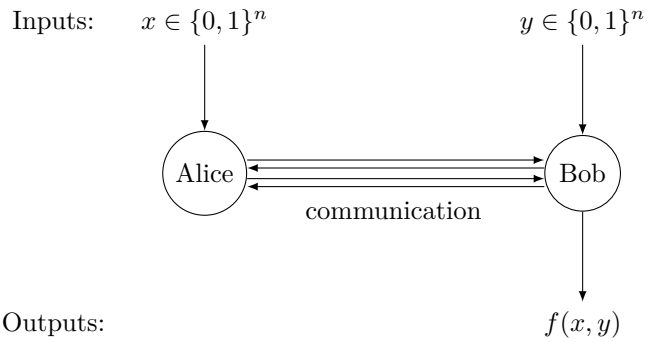


FIG. 3: Diagram of a communication complexity protocol as described by [3]. Alice receives an n-bit string input x, and Bob receives an n-bit string y. The players perform a sequence of local operations and transmissions (while attempting to minimize the amount of communication needed), until Bob can output the result $f(x, y)$.

and Bob are restricted to classical bits and a classical channel. The *cost* of the protocol is defined to be the number of bits communicated on the worst-case input. A *bounded-error* protocol outputs the right value $f(x, y)$ with probability at least $2/3$ for all $(x, y) \in \mathcal{D}$, while an *errorless* protocol must always output the correct value of $f(x, y)$ for all $(x, y) \in \mathcal{D}$.

A. Holevo's Bound

Holevo's Theorem states that the cost in qubits for transmitting a classical message from Alice to Bob costs the same using qubits as it does bits; that is, a $k-$bit classical message would take k qubits to transmit [9]; this situation is depicted in figure 4. Naively then, quantum channels wouldn't seem to provide a communication advantage, beyond perhaps a factor of two if Alice and Bob share entanglement and employ super-dense coding.

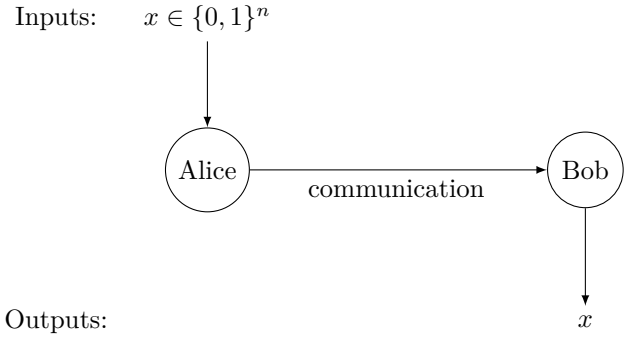


FIG. 4: The communication scenario to which Holevo's bound is applicable. Alice receives an n-bit input x; she is allowed one message to Bob before he must output x.

However, by instead setting the task to be for Bob to output a *function* of the inputs, quantum mechanics can be exploited for a significant advantage over classical protocols. This is nicely illustrated in Raz's problem below.

B. Raz's Problem

Raz's problem has the interesting property that the quantum protocol uses exponentially less communication than the classical protocol, even if the classical protocol is allowed to have bounded-error [3]. As presented in [3], in Raz's problem Alice receives a unit vector $v \in \mathbb{R}^m = H^{(0)} \oplus H^{(1)}$ where the $H^{(i)}$ are orthogonal subspaces. Bob receives an $m \times m$ unitary U. The promise in Raz's problem is that Uv is "close" to either $H^{(0)}$ or $H^{(1)}$; that is, if Π is the projector onto H, a vector u is close to H if $\|\Pi u\|^2 \geq 2/3$. Alice and Bob's task is to learn to which of the two subspaces Uv is close. In order to interpret the problem as involving finite input, every real number is approximated by $n = O(\log m)$ bits; then Alice and Bob's input is $O(m^2 \log m)$.

An efficient quantum protocol is to interpret v as $\log m-$qubits; that is, regard $v \in \mathbb{R}^m$ as $v \in \mathbb{C}^{\log m}$. Alice then sends the qubits v to Bob, who applies his unitary U, and sends the state back. Alice simply measures which subspace $H^{(i)}$ the state lies in, and outputs the result. This protocol only uses $2 \log m$ qubits of communication.

In contrast, classical protocols forgo access to such representations and need to almost send v literally; while the proof is beyond the scope of this document, Raz proved that any classical bounded-error protocol for the problem requires at least $\frac{n^{1/4}}{\log n}$ bits [10].

This protocol also demonstrates why Holevo's bound does not prevent quantum protocols having a communication complexity advantage (beyond the factor of two from super-dense coding): if Alice and Bob's task was to output the vector Uv, representing v as qubits would not help, because the general vector Uv can't be recovered from measurement. However, because Alice and Bob only need to output a single bit, "compressing" v as qubits becomes very useful.

C. Hidden Matching Problem

The hidden matching problem is interesting, because it demonstrates exponential separation between quantum and classical communication complexity as a one-way protocol [3]. So far, we have seen that although qubits can only simulate cbits generically in a $1-1$ ratio (as shown by Holevo's bound in section III A), in certain cases qubits can simulate exponentially more cbits, as in Raz's problem. However, by considering a non-local version of the hidden matching problem, we will see that ebits and cbits together can also non-trivially simulate exponentially more cbits. But to begin with, consider the hidden matching problem as a communication complexity scenario.

First, a definition: a perfect matching M on $\{1, \ldots, n\}$ (for n even) is a partition into $n/2$ disjoint pairs. Then, as stated in [3], the hidden matching problem is the following:

Alice receives a string $x^n \in \{0,1\}^n$ and Bob receives a perfect matching M on $\{1, \ldots, n\}$. The task is to output an ordered triplet $(i, j, x_i \oplus x_j)$ for some $(i, j) \in M$. Note that in this case there are $n/2$ correct responses, corresponding to each pair in M.

If two-way communication is allowed, as in Raz's problem, this can be solved classically easily: Bob simply sends Alice a pair $(i, j) \in M$, which would use $2 \log n$ bits. The problem is more interesting when communication is only allowed from Alice to Bob. As shown by [11], any such classical communication protocol requires at least $O(\sqrt{n})$ bits of communication, even if a small probability of error is allowed.

Exercise:

3. Show that there is a simple bounded-error classical strategy that achieves this lower bound.

See page 14 for the solution.

However, there's a simple quantum protocol that uses only $O(\log n)$ qubits of communication from Alice to Bob.

Alice encodes her string onto a $\log n$-qubit message

$$\frac{1}{\sqrt{n}}\sum_{i=1}^{n}(-1)^{x_i}|i\rangle$$

which she sends to Bob. Bob applies the projective measurement $\{P_{ij} = |i\rangle\langle i| + |j\rangle\langle j| : (i,j) \in M\}$ to project the state Alice sent him into $n/2$ 2-dimensional subspaces.

Bob is left with a specific $(i,j) \in M$ and the state

$$|\varphi\rangle := \frac{1}{\sqrt{2}}\left((-1)^{x_i}|i\rangle + (-1)^{x_j}|j\rangle\right)$$

Then Bob can use the measurement operators $M_0 = \frac{1}{2}(|i\rangle + |j\rangle)(\langle i| + \langle j|)$ and $M_1 = \frac{1}{2}(|i\rangle - |j\rangle)(\langle i| - \langle j|)$; Bob receives the outcome 0 or 1 corresponding to $x_i \oplus x_j$ with certainty:

$$\begin{aligned}|\langle\varphi|M_0|\varphi\rangle|^2 &= \tfrac{1}{4^2}|\left((-1)^{x_i}\langle i| + (-1)^{x_j}\langle j|\right)(|i\rangle + |j\rangle)((-1)^{x_i} + (-1)^{x_j})|^2 \\ &= \tfrac{1}{4^2}|((-1)^{x_i} + (-1)^{x_j})^2|^2 = 1 \iff x_i \oplus x_j = 0\end{aligned}$$

And so $|\langle\varphi|M_1|\varphi\rangle|^2 = 1 \iff x_i \oplus x_j = 1$.

Hence, Bob can output $(i, j, x_i \oplus x_j)$.

D. Non-local Hidden Matching Problem

Now, the non-local version of the hidden matching problem will be considered. While the problem as presented above cannot be solved non-locally, a task can be constructed such that Alice and send Bob $\log n$ cbits to solve the original hidden matching problem. The problem requires $O(\sqrt{n})$ cbits to solve without entanglement, so the addition of entanglement allows exponentially less classical communication.

To simplify the situation, take $n = 2^m$ so that $\log n = m$ is an integer. Then, as before, Alice receives a string $x^n \in \{0,1\}^n$ and Bob a perfect matching M on $\{1,\ldots,n\}$. The task is for Alice to output a shorter string $k \in \{0,1\}^m$ and Bob a pair $(i,j) \in M$ and a string $\ell \in \{0,1\}^m$ such that $i \cdot (k \oplus \ell) + j \cdot (k \oplus \ell) = x_i \oplus x_j$.

That way, Alice can send Bob k using m-cbits, and Bob can compute $x_i \oplus x_j$ to solve the communication complexity hidden matching problem.

This can be achieved by using only m-ebits:

Alice and Bob share

$$\frac{1}{\sqrt{n}}\sum_{i\in\{0,1\}^m}|i\rangle^A|i\rangle^B$$

where A is Alice's space and B, Bob's.

Alice applies the unitary $U = \sum_{i\in\{0,1\}^m}(-1)^{x_i}|i\rangle\langle i|^A \otimes I_B$ to add phases to the shared state, and Bob measures (as before) using $\{P_{ij} = |i\rangle\langle i| + |j\rangle\langle j| : (i,j) \in M\}$ to project the shared state into orthogonal subspaces. Bob is left with a specific $(i,j) \in M$ and the shared state becomes

$$|\varphi\rangle := \frac{1}{\sqrt{2}}\left((-1)^{x_i}|i\rangle^A|i\rangle^B + (-1)^{x_j}|j\rangle^A|j\rangle^B\right)$$

Then Alice and Bob each perform a Hadamard transformation, given by $(H)_{a,b} = \frac{1}{2^{m/2}}(-1)^{a\cdot b} = \frac{1}{\sqrt{n}}(-1)^{a\cdot b}$ (in the standard basis).

Hence,

$$H|i\rangle = \frac{1}{\sqrt{n}} \sum_{k\in\{0,1\}^m} (-1)^{k\cdot i}|k\rangle$$

Thus, the shared state becomes

$$\begin{aligned}&\frac{1}{\sqrt{2}}\left(\frac{(-1)^{x_i}}{n}\sum_{k,\ell\in\{0,1\}^m}(-1)^{i\cdot k+i\cdot\ell}|k\rangle^A|\ell\rangle^B + \frac{(-1)^{x_j}}{n}\sum_{k,\ell\in\{0,1\}^m}(-1)^{j\cdot k+j\cdot\ell}|k\rangle^A|\ell\rangle^B\right)\\ &= \frac{1}{\sqrt{2}n}\sum_{k,\ell\in\{0,1\}^m}\left((-1)^{x_i+i\cdot(k\oplus\ell)} + (-1)^{x_j+j\cdot(k\oplus\ell)}\right)|k\rangle^A|\ell\rangle^B\end{aligned}$$

Note that the non-zero terms in the sum have $x_i + i\cdot(k\oplus\ell) = x_j + j\cdot(k\oplus\ell) \pmod 2$. Then Alice and Bob each measure half of the shared state using $\{|i\rangle\langle i|\otimes I\}$. Then Alice has a k and Bob an ℓ such that $x_i + i\cdot(k\oplus\ell) = x_j + j\cdot(k\oplus\ell) \pmod 2$. Hence,

$$i\cdot(k\oplus\ell) - j\cdot(k\oplus\ell) = x_j - x_i \pmod 2 \implies i\cdot(k\oplus\ell) + j\cdot(k\oplus\ell) = x_i + x_j \pmod 2$$

Thus, Alice and Bob have completed the task using only $m = \log n$ ebits. So for this specific task, $\log n$ ebits and $\log n$ cbits simulated the $O(\sqrt{n})$ cbits which would be needed to solve the problem classically.

E. Mapping from Communication Complexity Scenarios to Non-locality Scenarios

In fact, the above relationship between a one-way quantum communication complexity scenario and a non-local game is a special case of a more general mapping created by Burhman et al. [3]:

For a communication complexity scenario that can be solved by Alice sending Bob q qubits, and can be solved if:

1. Alice starts with an arbitrary basis state $|k\rangle$, where k is known to both Alice and Bob

2. Alice performs a transformation $U_A(x)$ on $|k\rangle$ which does not depend on k, but can depend on Alice's input x

3. Alice sends the result to Bob

4. Bob performs a transformation $U_B(y)$ (again, independent of k, but dependent his input y) and measures in the computational basis to obtain a result ℓ

5. Bob is able to compute $f(x,y)$ using k, ℓ, y.

Then the scenario can be solved using q ebits and q cbits.

Note that, as the problem can be solved using q qubits, it can trivially be solved using q ebits and $2q$ cbits, via teleportation.

IV. DISCUSSION

Non-local games present "physical" Bell inequalities: situations where quantum mechanics can be used to do classically-impossible tasks, or complete tasks with a classically-impossible probability of success. The magic square game achieves the former, earning the designation pseudo-telepathic, while the odd-cycle game achieves the latter. Examination of the odd-cycle game leads to the natural question of optimality, which Cleve et al. [1] answer for a general binary XOR game. An open problem is to experimentally demonstrate, without any loopholes, a Bell inequality; perhaps, this can be achieved form of a non-local game.

Broadening the focus to allow communication, scenarios such as Raz's problem and the Hidden Matching problem are considered. Raz's problem demonstrates exponential separation between a quantum strategy and the best classical strategy, even when the classical strategies are allowed a slight probability of error (whereas other scenarios, such as the Distributed Deutsch-Jozsa problem, only exhibit such separations for errorless protocols [3]). Next, one-way communication scenarios are investigated, typified by the Hidden Matching problem. Again, a quantum communication strategy exhibits an exponential advantage over bounded-error classical protocols, but furthermore, ebits and cbits together can form a strategy, developed by the consideration of a non-local version of the problem, which uses exponentially fewer resources than cbits alone (and uses half the cbits as composing teleportation with the qubit strategy).

A. Further work

We have discussed quantum communication, entanglement, and classical communication, and compared the amount of these resources were required to solve different specific problems (while super-dense coding and teleportation give us general resource inequalities). Continuing this work, Degorre et al. [12] explore simulating entanglement. They have shown that a single non-local box, which can be simulated by 1 cbit, can simulate the results of the EPR experiment, using, however, infinite shared randomness. Buhrman et al. [3] investigate noisy non-local boxes and present an open problem: if Alice and Bob were given an unlimited supply of non-local boxes, what is the minimum level of noise p that can tolerated while being able to compute any function $f(x, y)$ with only a single cbit?[1]

---

[1] R. Cleve, P. Hoyer, B. Toner, and J. Watrous, "Consequences and Limits of Nonlocal Strategies," eprint arXiv:quant-ph/0404076 (2010).

[2] G. Brassard, A. Broadbent, and A. Tapp, "Quantum Pseudo-Telepathy," Foundations of Physics **35**, 1877–1907 (2005), arXiv:quant-ph/0407221.

[3] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf, "Nonlocality and communication complexity," Reviews of Modern Physics **82**, 665–698 (2010), arXiv:0907.3584 [quant-ph].

[4] J. Etesse, R. Blandino, B. Kanseri, and R. Tualle-Brouri, "Proposal for a loophole-free violation of Bell inequalities with a set of single photons and homodyne measurements," eprint arXiv: quant-ph/1304.2532 (2013).

[5] A. Grothendieck, "Résumé de la théorie métrique des produits tensoriels topologiques," Bol. Soc. Mat. São Paulo **8**, 1–79 (1953).

[6] James Reeds, "A New Lower Bound on the Real Grothendieck Constant," Unpublished; accessible at http://www.dtc.umn.edu/~reedsj/bound2.dvi.

[1] It has been narrowed down to $85.4\% \approx \frac{2+\sqrt{2}}{4} \leq p \leq \frac{3+\sqrt{6}}{6} \approx 90.8\%$ [3].

[7] M. Braverman, K. Makarychev, Y. Makarychev, and A. Naor, "The Grothendieck constant is strictly smaller than Krivine's bound," ArXiv e-prints (2011), arXiv:1103.6161 [math.FA].
[8] B.S. Tsirel'son, "Quantum analogues of the bell inequalities. the case of two spatially separated domains," Journal of Soviet Mathematics **36**, 557–570 (1987).
[9] A. S. Holevo, "Bounds for the quantity of information transmitted by a quantum communication channel," Problemy Peredachi Informatsii (1973).
[10] R. Raz, "Exponential separation of quantum and classical communication complexity," Proceedings of 31st ACM STOC (1999).
[11] Ziv Bar-Yossef, T. S. Jayram, and Iordanis Kerenidis, "Exponential separation of quantum and classical one-way communication complexity," in *STOC*, edited by László Babai (ACM, 2004) pp. 128–137.
[12] J. Degorre, S. Laplante, and J. Roland, "Simulating quantum correlations as a distributed sampling problem," Phys. Rev. A **72**, 062314 (2005), arXiv:quant-ph/0507120.

Appendix A: Exercise Solutions

1. Odd-cycle game

See page 3 for the context of this exercise.

1. Show that if Alice and Bob receive the same vertex, they win the game with probability $\cos^2\left(\frac{\pi}{4n}\right)$ using this strategy.
2. Show that Alice and Bob always win the game with probability $\cos^2\left(\frac{\pi}{4n}\right)$ using this strategy.

Solutions:

1. The probability that $a = b = j$ is

$$\langle\Phi^+|A_x^j \otimes B_y^j|\Phi^+\rangle = \tfrac{1}{2}\left(\langle 00| + \langle 11|\right)\left(|\varphi_j(\alpha_x)\rangle\langle\varphi_j(\alpha_x)| \otimes |\varphi_j(\beta_y)\rangle\langle\varphi_j(\beta_y)|\right)\left(|00\rangle + |11\rangle\right)$$

Expanding the right product,

$$\begin{aligned}= \tfrac{1}{2}\left(\langle 00| + \langle 11|\right)&\left(|\varphi_j(\alpha_x)\rangle\langle\varphi_j(\alpha_x)|0\rangle \otimes |\varphi_j(\beta_y)\rangle\langle\varphi_j(\beta_y)|0\rangle\right.\\ &\left.+ |\varphi_j(\alpha_x)\rangle\langle\varphi_j(\alpha_x)|1\rangle \otimes |\varphi_j(\beta_y)\rangle\langle\varphi_j(\beta_y)|1\rangle\right)\end{aligned}$$

Expanding the left product,

$$\begin{aligned}= \tfrac{1}{2}(&\langle 0|\varphi_j(\alpha_x)\rangle\langle\varphi_j(\alpha_x)|0\rangle\langle 0|\varphi_j(\beta_y)\rangle\langle\varphi_j(\beta_y)|0\rangle\\ &+ \langle 0|\varphi_j(\alpha_x)\rangle\langle\varphi_j(\alpha_x)|1\rangle\langle 0|\varphi_j(\beta_y)\rangle\langle\varphi_j(\beta_y)|1\rangle)\\ &+ (\langle 1|\varphi_j(\alpha_x)\rangle\langle\varphi_j(\alpha_x)|0\rangle\langle 1|\varphi_j(\beta_y)\rangle\langle\varphi_j(\beta_y)|0\rangle\\ &+ \langle 1|\varphi_j(\alpha_x)\rangle\langle\varphi_j(\alpha_x)|1\rangle\langle 1|\varphi_j(\beta_y)\rangle\langle\varphi_j(\beta_y)|1\rangle)\end{aligned}$$

Using $\langle\psi|\varphi\rangle\langle\varphi|\psi\rangle = |\langle\varphi|\psi\rangle|^2$:

$$\begin{aligned}= \tfrac{1}{2}&|\langle 0|\varphi_j(\alpha_x)\rangle|^2|\langle 0|\varphi_j(\beta_y)\rangle|^2\\ &+ \langle 0|\varphi_j(\alpha_x)\rangle\langle\varphi_j(\alpha_x)|1\rangle\langle 0|\varphi_j(\beta_y)\rangle\langle\varphi_j(\beta_y)|1\rangle)\\ &+ (\langle 1|\varphi_j(\alpha_x)\rangle\langle\varphi_j(\alpha_x)|0\rangle\langle 1|\varphi_j(\beta_y)\rangle\langle\varphi_j(\beta_y)|0\rangle\\ &+ |\langle 1|\varphi_j(\alpha_x)\rangle|^2|\langle 1|\varphi_j(\beta_y)\rangle|^2\end{aligned}$$

Using that all the inner products are real and that $a^2 + b^2 + 2ab = (a+b)^2$:

$$= \tfrac{1}{2}\left(\langle 0|\varphi_j(\alpha_x)\rangle\langle 0|\varphi_j(\beta_y)\rangle + \langle 1|\varphi_j(\alpha_x)\rangle\langle 1|\varphi_j(\beta_y)\rangle\right)^2$$

Substituting in either $|\varphi_0(\theta)\rangle$ or $|\varphi_1(\theta)\rangle$:

$$= \tfrac{1}{2}\left(\cos(\alpha_x)\cos(\beta_y) + \sin(\alpha_x)\sin(\beta_y)\right)^2$$

and, by a trigonometric identity,

$$= \tfrac{1}{2}\left(\cos(\alpha_x - \beta_y)\right)^2$$

Hence, the probability that $a = b = 0$ is $\frac{1}{2}\cos^2(\alpha_x - \beta_y)$ and the probability that $a = b = 1$ is $\frac{1}{2}\cos^2(\alpha_x - \beta_y)$. So the probability that $a = b$ is $\cos^2(\alpha_x - \beta_y)$.

So, if $x = y$, then $a = b$ with probability $\cos^2(\alpha_x - \beta_x) = \cos^2\left(\frac{\pi}{4n}\right)$; i.e., when Alice and Bob are given the same vertex, they output the same result (and thus win the game) with probability $\cos^2\left(\frac{\pi}{4n}\right)$. □

2. From the above result, the probability that $a \neq b$ is $1 - \cos^2(\alpha_x - \beta_y) = \sin^2(\alpha_x - \beta_y)$.

If $y \equiv x + 1 \pmod{n} \iff y - x = 1 + \ell n$ for $\ell \in \mathbb{N}$, then $a \neq b$ with probability

$$\begin{aligned}
\sin^2\left(\tfrac{\pi}{4n} + \tfrac{\pi}{2n}(x-y) + \tfrac{\pi}{2}(y-x)\right) &= \sin^2\left(\tfrac{\pi}{4n} + \tfrac{\pi}{2n}(-1-\ell n) + \tfrac{\pi}{2}(1+\ell n)\right)^2 \\
&= \sin^2\left(\tfrac{1}{2}\tfrac{\pi}{2n} - \tfrac{\pi}{2n} + \tfrac{\pi}{2} - \ell\tfrac{\pi}{2} + \ell n\tfrac{\pi}{2}\right)^2 \\
&= \sin^2\left(\tfrac{\pi}{2} - \tfrac{\pi}{4n} + \ell(n-1)\tfrac{\pi}{2}\right)
\end{aligned}$$

n is odd, so $\ell(n-1)$ is even, so for integer $k = \frac{\ell(n-1)}{2}$,

$$\begin{aligned}
&= \sin^2\left(\tfrac{\pi}{2} - \tfrac{\pi}{4n} + k\pi\right) \\
&= \sin^2\left(\tfrac{\pi}{2} - \tfrac{\pi}{4n}\right)^2 \\
&= \cos^2\left(\tfrac{\pi}{4n}\right)
\end{aligned}$$

Thus, for legitimate inputs, Alice and Bob win with probability $\cos^2\left(\frac{\pi}{4n}\right)$. □

2. Hidden Matching Problem

See page 9 for the context of this exercise.

3. Show that there is a simple bounded-error classical strategy that achieves this lower bound.

The strategy will be for Alice to simply send $O(\sqrt{n})$ pairs (i, x_i) randomly, and show that with probability at least ⅔ Bob will receive both points of at least one pair $(i, j) \in M$.

Assume Alice sends Bob m distinct sets (i, x_i) (to be referred to as elements from now on); assume she chooses them uniformly randomly, subject to the condition that she doesn't send the same element twice. Then it's easier to calculate the probability that Alice has not sent Bob a pair (a pair being two elements $(i, x_i), (j, x_j)$ with $(i, j) \in M$). This can be calculated sequentially, element by element:

When Alice sends the first element, she has probability 1 of not having sent any pairs (one element can't make a pair!).

Now one of the remaining $n - 1$ possible elements Alice could send is the matching element to the first such that sending this element would make a pair.

When Alice sends the second element then, there's 1 chance in $n - 1$ that she sent the corresponding element to the first; i.e., she has probability $1 - \frac{1}{n-1} = \frac{n-2}{n-1}$ of not forming a pair by sending the second element.

Now, two of the $n-2$ remaining elements are pairs to the two elements she already sent (assuming she has not sent any pairs yet), so when she sends the third element, she has probability $1-\frac{2}{n-2}=\frac{n-4}{n-2}$.

This argument can be repeated for all m elements she sends; the probability p that she sends no pairs after sending all of the elements is the product of all the conditional probabilities and 1:

$$\begin{aligned}
p &= \Pr\{\text{first element does not cause Bob to have a pair}\} \\
&\quad \times \Pr\{\text{second element does not cause Bob to have a pair} \mid \text{Bob has no pairs}\} \\
&\quad \vdots \\
&\quad \times \Pr\{\text{m}^{\text{th}} \text{ element does not cause Bob to have a pair} \mid \text{Bob has no pairs}\} \\
&= 1 \times \tfrac{n-2}{n-1} \times \tfrac{n-4}{n-2} \times \ldots \times \tfrac{n-2(m-1)}{n-(m-1)} \\
&= \prod_{k=1}^{m-1} \frac{n-2k}{n-k}
\end{aligned}$$

We hope to find $m=O(\sqrt{n})$, so consider when Alice sends Bob fewer than $\frac{n}{2}$ elements (besides, if Alice sends $\frac{n}{2}+1$ elements, she must have sent a pair by the pigeon hole principle, and we only want her to have likely sent Bob a pair).

Now, n is even, so set $n=2N$ and let $N-m=A$. Then we have

$$\begin{aligned}
p &= \frac{n(n-2)(n-4)\ldots(n-2(m-1))}{n(n-1)(n-2)\ldots(n-(m-1))} \\
&= \frac{2N(2N-2)(2N-4)\ldots(\overbrace{2N-2m}^{2A}+2)}{2N(2N-1)(2N-2)\ldots(N+\underbrace{N-m}_{A}+1)} \\
&= \frac{(2(A+1))(2(A+2))\ldots(2(A+m))}{(N+A+1)(N+A+2)\ldots(N+A+m)} \\
&= \frac{\frac{2\times4\times6\times\ldots\times2A}{2\times4\times6\times\ldots\times2A}(2(A+1))(2(A+2))\ldots(2(A+m))}{\frac{1\times2\times3\times\ldots\times(N+A)}{1\times2\times3\times\ldots\times(N+A)}(N+A+1)(N+A+2)\ldots(N+A+m)} \\
&= \frac{\frac{1}{2^A A!}2^{A+m}(A+m)!}{\frac{1}{(N+A)!}(N+A+m)!} \\
&= 2^m \frac{N!(2N-m)!}{(2N)!(N-m)!}
\end{aligned}$$

Taking the natural log,

$$\log p = m\log 2 + \log(N!) + \log((2N-m)!) - \log((2N)!) - \log((N-m)!)$$

applying Stirling's approximation (valid for large N, and $N-m$ large),

$$\begin{aligned}
&\approx m\log 2 + N\log N - N + (2N-m)\log(2N-m) - (2N-m) \\
&\qquad - 2N\log(2N) + 2N - (N-m)\log(N-m) + (N-m) \\
&= m\log 2 + N\log\left(\frac{N}{N-m}\right) + 2N\log\left(\frac{2N-m}{2N}\right) + m\log\left(\frac{N-m}{2N-m}\right) \\
&= N\log\left(\frac{N}{N-m}\left(\frac{2N-m}{2N}\right)^2\right) + m\log\left(\frac{2N-2m}{2N-m}\right) \\
&= N\log\left(1+\frac{Nm^2}{4N^3-4N^2m}\right) + m\log\left(1-\frac{m}{2N-m}\right)
\end{aligned}$$

Set $m = k\sqrt{N}$ to try to prove the result:

$$= N\log\left(1+\frac{N^2k^2}{4N^3-4kN^{5/2}}\right) + k\sqrt{N}\log\left(1-\frac{k\sqrt{N}}{2N-k\sqrt{N}}\right) \to \frac{k^2}{4} - \frac{k^2}{2} \text{ as } N\to\infty$$

So for sufficiently large n, $\log p \approx -\frac{k^2}{4}$. Choosing $p = 1/3$, we have $k = 2\sqrt{\log 3} \approx 2.1$. So for $m = k\sqrt{N} = O(\sqrt{N})$, we achieve at a $2/3$ probability of Alice sending Bob at least one pair. □