The one-way communication complexity of the Boolean Hidden Matching Problem

Iordanis Kerenidis*
CNRS - LRI
Université Paris-Sud
jkeren@lri.fr

Ran Raz†
Faculty of Mathematics
Weizmann Institute
ran.raz@weizmann.ac.il

July 25, 2006

Abstract

We give a tight lower bound of $\Omega(\sqrt{n})$ for the randomized one-way communication complexity of the Boolean Hidden Matching Problem [BJK04]. Since there is a quantum one-way communication complexity protocol of $O(\log n)$ qubits for this problem, we obtain an exponential separation of quantum and classical one-way communication complexity for partial functions. A similar result was independently obtained by Gavinsky, Kempe, de Wolf [GKdW06].

Our lower bound is obtained by Fourier analysis, using the Fourier coefficients inequality of Kahn Kalai and Linial [KKL88].

1 Introduction

Communication complexity is a central model of computation, first defined by Yao in 1979 [Yao79]. It has found applications in many areas of theoretical computer science. Numerous examples of such applications can be found in the textbook of Kushilevitz and Nisan [KN97].

A communication complexity problem is defined by three sets X, Y, Z and a relation $\mathcal{R} \subseteq X \times Y \times Z$. There are two unconditionally powerful parties, Alice and Bob, who are given inputs $x \in X$ and $y \in Y$, respectively. Alice and Bob exchange messages according to a shared *protocol* over a channel, until Bob has sufficient information to announce an output $z \in Z$ s.t. $(x, y, z) \in \mathcal{R}$. The *communication cost* of a protocol is the sum of the lengths of

*Supported in part by ACI Securité Informatique SI/03 511 and ANR AlgoQP grants of hte French Ministry and in part by the European Commission under the Intergrated Project Qubit Applications (QAP) funded by the IST directorate as Contract Number 015848.

†Part of this work was done when the second author visited Microsoft Research, Redmond.

messages (in bits) Alice and Bob exchange on the worst-case choice of inputs x and y. The *communication complexity* of the problem $\mathcal{R}$ is the cost of the best protocol that computes $\mathcal{R}$ correctly.

In the *one-way* variant of the model [PS84, Abl96, KNR99], Alice is allowed to send a single message to Bob, after which he announces the outcome. Last, in the *Simultaneous Messages Passing (SMP)* model, Alice and Bob cannot communicate directly, but instead, each of them sends a single message to a third party called the "referee", who computes the outcome based on the two messages.

Another important distinction has to do with the type of problem that Alice and Bob try to solve. In the most natural setting, the problem is a total Boolean function, meaning that Alice and Bob receive inputs $x \in \{0,1\}^n$ and $y \in \{0,1\}^n$ and the goal is to compute a Boolean function $f(x,y)$, which is defined for all possible (x,y). In other cases, the problem is a partial function (or promise problem), meaning that Alice and Bob receive only inputs that satisfy some special property and compute a Boolean function $f(x,y)$. For example, Alice and Bob might receive sets S and T with the property that either they are disjoint or their intersection is half their size and the question is to figure out which of the two cases it is. Last, the communication problem could be a relation, meaning that for each input of Alice and Bob there could be more than one right answer. For example, on inputs $x \in \{0,1\}^n$ and $y \in \{0,1\}^n$ Alice and Bob need to output an index $i \in [n]$ such that $x_i = y_i$ (if such an i exists). Note that a total Boolean function is a special case of a promise problem, which is a special case of a relation.

We can define different measures of communication complexity for a problem $\mathcal{R}$ depending on the allowed protocols. In a *bounded-error randomized* protocol with error δ, we allow Alice and Bob to have access to *public* random coins. For any inputs x, y, the outcome z should be correct with probability at least $1-\delta$, where the probability is taken over the public random coins. The cost of a randomized protocol is the number of bits Alice and Bob exchange in the worst-case. The randomized communication complexity of $\mathcal{R}$ (w.r.t. δ) is the cost of the optimal randomized protocol for $\mathcal{R}$.

In the setting of *quantum communication complexity* [Yao93], Alice and Bob have qubits, some of which are initialized to their respective inputs. In a communication round, a player can perform a unitary operation on his/her part of the qubits and send some of them to the other player. At the end of the protocol Bob performs a measurement and decides on an outcome. The outcome of the protocol should be correct with probability of at least $1-\delta$ (for any inputs x, y). The quantum communication complexity of $\mathcal{R}$ is the number of qubits exchanged in the optimal bounded-error quantum protocol for $\mathcal{R}$.

The main question in the theory of quantum communication complexity is whether in the different communication models quantum channels can reduce significantly the amount of communication necessary to solve certain types of problems.

For total functions, we do not have any exponential gap between quantum communication and randomized communication with public coins in any of the abovementioned models. Buhrman *et al.* [BCWdW01] were able to solve the equality problem in the SMP model with a quantum protocol of complexity $O(\log n)$ rather than the $\Theta(\sqrt{n})$ bits necessary in any

bounded-error randomized SMP protocol with private coins [NS96, BK97]. However, if we allow the players to share random coins, then equality can be solved classically with $O(1)$ communication.

For promise problems, an exponential gap between the quantum and the (public-coins) randomized communication complexity models was proved in [Raz99]. This was obtained by describing a promise problem $\mathcal{P}_1$ with an efficient quantum protocol of complexity $O(\log n)$ and such that the bounded-error randomized communication complexity of $\mathcal{P}_1$ is $\Omega(n^{1/4})$.

For relations, Bar-Yossef *et. al.* [BJK04] defined the Hidden Matching Problem and proved an exponential gap between quantum and randomized communication in the one-way model and the SMP model.

In this paper we give a tight lower bound of $\Omega(\sqrt{n})$ for the bounded-error randomized one-way communication complexity of a Boolean version of the Hidden Matching Problem [BJK04]. Since there is a simple quantum one-way communication complexity protocol of $O(\log n)$ qubits for the problem, this provides an exponential separation for promise problems between the models of quantum and randomized one-way communication complexity. A similar result was independently obtained by Gavinsky, Kempe, de Wolf [GKdW06].

Our lower bound is obtained by Fourier analysis, using the Fourier coefficients inequality of Kahn Kalai and Linial [KKL88], which in turn was proved using the Bonami-Beckner inequality [Bon70, Bec75]. The KKL inequality was previously used in the context of communication complexity in [Raz95, Kla01].

2 Preliminaries

2.1 Fourier analysis

For a function $f : \{0,1\}^n \to \mathcal{R}$, we define the ℓ_1 and ℓ_2 norms as

$$||f||_1 = \sum_{x \in \{0,1\}^n} |f(x)| \quad , \quad ||f||_2 = \left(\sum_{x \in \{0,1\}^n} |f(x)|^2 \right)^{1/2}$$

It is a well known fact that for a function $f : \{0,1\}^n \to \mathcal{R}$

$$||f||_2^2 \geq \frac{||f||_1^2}{2^n}.$$

The Fourier transform of $f : \{0,1\}^n \to \mathcal{R}$ is defined as

$$f = \sum_{s \in \{0,1\}^n} \hat{f}(s) \chi_s,$$

where $\chi_s : \{0,1\}^n \to \mathcal{R}$ is the character $\chi_s(y) = (-1)^{y^T \cdot s}$ with " $\cdot$ " being the scalar product over $GF(2)$ and $\hat{f}(s)$ is the Fourier coefficient

$$\hat{f}(s) = \frac{1}{2^n} \sum_{y \in \{0,1\}^n} f(y) \chi_s(y).$$

One very useful fact about the Fourier coefficients of a function is Parseval's identity

Lemma 1. *(Parseval's Identity)*
For a function $f : \{0,1\}^n \to \mathcal{R}$ it holds that

$$||f||_2^2 = 2^n \sum_{s \in \{0,1\}^n} (\hat{f}(s))^2$$

Let $f : \{0,1\}^n \to \mathcal{R}$ and $g : \{0,1\}^n \to \mathcal{R}$ and " $+$ " denote the bitwise XOR of two strings. The convolution $f * g : \{0,1\}^n \to \mathcal{R}$ is defined as

$$f * g(w) = \sum_{y \in \{0,1\}^n} f(y+w)g(y)$$

For the Fourier coefficients of a convolution we have the following lemma

Lemma 2. *For functions $f : \{0,1\}^n \to \mathcal{R}$ and $g : \{0,1\}^n \to \mathcal{R}$ it holds that*

$$\widehat{f * g}(s) = 2^n \cdot \hat{f}(s) \cdot \hat{g}(s)$$

Let $h(\cdot,\cdot)$ be the hamming distance function and $h(\cdot)$ the hamming weight function. A final tool in our analysis is the KKL lemma

Lemma 3. *[KKL88] Let f be a function $f : \{0,1\}^n \to \{-1,0,1\}$. Let t be the probability that $f \neq 0$. Then for every $0 \leq \delta \leq 1$*

$$\sum_{s \in \{0,1\}^n} \delta^{h(s)} (\hat{f}(s))^2 \leq t^{\frac{2}{1+\delta}}$$

2.2 Quantum computation

We explain the standard notation of quantum computing and describe the basic notions that will be useful in this paper. For more details we refer the reader to the textbook of Nielsen and Chuang [NC00].

Let H denote a 2-dimensional complex vector space, equipped with the standard inner product. We pick an orthonormal basis for this space, label the two basis vectors $|0\rangle$ and $|1\rangle$, and for simplicity identify them with the vectors $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$, respectively. A *qubit* is a unit length vector in this space, and so can be expressed as a linear combination of the basis states:

$$\alpha_0|0\rangle + \alpha_1|1\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}.$$

Here α_0, α_1 are complex *amplitudes*, and $|\alpha_0|^2 + |\alpha_1|^2 = 1$.

An *m-qubit system* is a unit vector in the m-fold tensor space $H \otimes \cdots \otimes H$. The 2^m basis states of this space are the m-fold tensor products of the states $|0\rangle$ and $|1\rangle$. For example, the

basis states of a 2-qubit system are the four 4-dimensional unit vectors $|0\rangle \otimes |0\rangle$, $|0\rangle \otimes |1\rangle$, $|1\rangle \otimes |0\rangle$, and $|1\rangle \otimes |1\rangle$. We abbreviate, e.g., $|1\rangle \otimes |0\rangle$ to $|1\rangle|0\rangle$, or $|1,0\rangle$, or $|10\rangle$, or even $|2\rangle$ (since 2 is 10 in binary). With these basis states, an m-qubit state $|\phi\rangle$ is a 2^m-dimensional complex unit vector

$$|\phi\rangle = \sum_{i \in \{0,1\}^m} \alpha_i |i\rangle.$$

We use $\langle\phi| = |\phi\rangle^*$ to denote the conjugate transpose of the vector $|\phi\rangle$, and $\langle\phi|\psi\rangle = \langle\phi|\cdot|\psi\rangle$ for the inner product between states $|\phi\rangle$ and $|\psi\rangle$. These two states are *orthogonal* if $\langle\phi|\psi\rangle = 0$. The *norm* of $|\phi\rangle$ is $\||\phi\rangle\| = \sqrt{\langle\phi|\phi\rangle}$.

Let $|\phi\rangle$ be an m-qubit state and $B = \{|b_1\rangle, \ldots, |b_{2^m}\rangle\}$ an orthonormal basis of the m-qubit space. A measurement of the state $|\phi\rangle$ in the B basis means that we apply the projection operators $P_i = |b_i\rangle\langle b_i|$ to $|\phi\rangle$. The resulting quantum state is $|b_i\rangle$ with probability $p_i = |\langle\phi|b_i\rangle|^2$.

3 Definition of the Boolean Hidden Matching Problem

The relational version of the Hidden Matching Problem was defined in [BJK04]. There, they proved a $\Omega(\sqrt{n})$ lower bound for the randomized one-way communication complexity of it and also described a $O(\log n)$ quantum one-way protocol. This provided an exponential separation for a relation between the randomized and quantum one-way communication complexity models. [BJK04] also defined a Boolean version of the Hidden Matching Problem but did not provide a lower bound for the randomized communication complexity of it.

A version of the relational Hidden Matching Problem was also used by Gavinsky *et al* [GKRdW06] to show that in the model of Simultaneous Messages, shared entanglement can reduce the communication exponentially compared to shared randomness.

Here, we define a slightly different version of the Boolean Hidden Matching Problem and prove a tight lower bound for its randomized one-way communication complexity. We denote a perfect matching on $[2n]$ as a $(n \times 2n)$ binary matrix M where each column corresponds to a number in $[2n]$ and the i-th row corresponds to the i-th edge of the matching. In other words, if the i-th edge of the matching is (k, l), then the i-th row of the matrix contains two 1's at the positions k and l and 0's elsewhere.

Let $x \in \{0,1\}^{2n}$. Then the product Mx is an n-bit string w, where the i-th bit is equal to the parity of the two bits of x that correspond to the i-th edge of the matching, i.e. $w_i = x_k \oplus x_l$. Recall that we denote by $h(\cdot,\cdot)$ the hamming distance function and by $h(\cdot)$ the hamming weight function.

The Boolean Hidden Matching Problem ($\mathbf{BHM}_n$):

Alice gets as input a string $x \in \{0,1\}^{2n}$ and Bob gets as input a perfect matching M on $[2n]$ and a string $w \in \{0,1\}^n$. The promise is that either $h(Mx, w) \leq n/3$ ("0" instance) or $h(Mx, w) \geq 2n/3$ ("1" instance). The goal is for Bob to determine where the input corresponds to a "0" instance or to a "1" instance.

4 Quantum protocol for the Boolean Hidden Matching Problem

We present a quantum protocol for the Boolean Hidden Matching Problem with communication complexity of $O(\log n)$ qubits. Let $\mathbf{x} = x_1 \dots x_{2n}$ be Alice's input and M, w be Bob's input.

Quantum protocol for BHM_n

1. Alice sends the state $|\psi\rangle = \frac{1}{\sqrt{2n}} \sum_{i=1}^{2n} (-1)^{x_i} |i\rangle$.
2. Bob performs a measurement on the state $|\psi\rangle$ in the orthonormal basis $B = \{\frac{1}{\sqrt{2}}(|k\rangle \pm |\ell\rangle) \mid (k,\ell) \in M\}$.

The probability that the outcome of the measurement is a basis state $\frac{1}{\sqrt{2}}(|k\rangle + |\ell\rangle)$ is

$$|\langle\psi|\frac{1}{\sqrt{2}}(|k\rangle + |\ell\rangle)\rangle|^2 = \frac{1}{4n}((-1)^{x_k} + (-1)^{x_\ell})^2.$$

This equals to $1/n$ if $x_k \oplus x_\ell = 0$ and 0 otherwise. Similarly for the state $\frac{1}{\sqrt{2}}(|k\rangle - |\ell\rangle)$ we have that $|\langle\psi|\frac{1}{\sqrt{2}}(|k\rangle - |\ell\rangle)\rangle|^2$ is 0 if $x_k \oplus x_\ell = 0$ and $1/n$ if $x_k \oplus x_\ell = 1$. Hence, if the outcome of the measurement is a state $\frac{1}{\sqrt{2}}(|k\rangle + |\ell\rangle)$ then Bob knows with certainty that $x_k \oplus x_\ell = 0$. If the outcome is a state $\frac{1}{\sqrt{2}}(|k\rangle - |\ell\rangle)$ then Bob knows with certainty that $x_k \oplus x_\ell = 1$. Let (k,ℓ) be the j-th edge in the matching M, then Bob outputs $x_k \oplus x_\ell \oplus w_j$. The protocol is correct with probability at least $2/3$ and by repeating a constant number of times we can achieve correctness $1 - \epsilon$ for any small constant ϵ.

5 The randomized one-way communication complexity of the Boolean Hidden Matching Problem

Theorem 4. *The randomized one-way communication complexity of the Boolean Hidden Matching Problem is $\Omega(\sqrt{n})$.*

Proof. For $b \in \{0,1\}$ we denote by σ_b the distribution over $\{0,1\}$ such that $\text{Prob}_{\sigma_b}[b] = 3/4$ and define $\mu_b = (\sigma_b)^{\otimes n}$. In other words, μ_0 is the distribution over strings $\{0,1\}^n$ such that independently for every bit $i \in [n]$, $\text{Prob}_{\mu_0}[i\text{-th bit is } 0] = 3/4$ and μ_1 is the distribution over strings $\{0,1\}^n$ such that independently for every bit $i \in [n]$, $\text{Prob}_{\mu_1}[i\text{-th bit is } 1] = 3/4$.

We define the function $f : \{0,1\}^n \to \mathcal{R}$ as

$$f(y) = \text{Prob}_{\mu_0}[y] - \text{Prob}_{\mu_1}[y]$$

It is easy to see that the Fourier coefficients of f are

$$\hat{f}(s) = \begin{cases} \frac{2}{2^{n+k}} & \text{for } s \text{ with } h(s) = k \text{ and } k \text{ odd} \\ 0 & \text{otherwise} \end{cases}$$

Using Yao's Lemma [Yao83], in order to prove the lower bound, it suffices to construct a "hard" distribution over instances of BHM_n, and prove a lower bound for deterministic one-way protocols whose distributional error with respect to this distribution is at most ϵ. For every $x \in \{0,1\}^{2n}$ and matching M we define the following distributions:
$\mathcal{D}_0$ is the distribution over strings $w \in \{0,1\}^n$ such that independently for each $i \in [n]$, $\text{Prob}[w_i = (Mx)_i] = 3/4$ and $\mathcal{D}_1$ is the distribution over strings $w \in \{0,1\}^n$ such that independently for each $i \in [n]$, $\text{Prob}[w_i \neq (Mx)_i] = 3/4$.

The "hard" distribution $\mathcal{T}$ is defined as follows: The string $x \in \{0,1\}^{2n}$ and the matching M are picked uniformly at random. The string $w \in \{0,1\}^n$ is picked according to the distribution $\mathcal{D} = \frac{1}{2}\mathcal{D}_0 + \frac{1}{2}\mathcal{D}_1$, that is w is picked with probability $1/2$ from the distribution $\mathcal{D}_0$ and with probability $1/2$ from the distribution $\mathcal{D}_1$, where $\mathcal{D}_0, \mathcal{D}_1$ are the ones corresponding to x, M. The goal is now for Bob to determine whether w was drawn from the distribution $\mathcal{D}_0$ or $\mathcal{D}_1$.

Note that if (x, M, w) are picked according to the distribution $\mathcal{T}$, then the probability that $n/3 \leq h(Mx, w) \leq 2n/3$ is exponentially small. Hence, any probabilistic protocol for BHM_n with error ϵ' gives a deterministic protocol for the distribution $\mathcal{T}$ with distributional error $\epsilon' + o(1)$. Therefore, for the rest of the proof we use the distribution $\mathcal{T}$.

Let us assume that there exists a deterministic protocol P which is correct on the distribution $\mathcal{T}$ with probability $1 - \epsilon$, namely for uniformly random x, M and w drawn from $\mathcal{D}$, Bob can determine with probability $1 - \epsilon$ whether w was drawn from $\mathcal{D}_0$ or $\mathcal{D}_1$. Then, the protocol is correct for at least half of the x's, with probability at least $(1 - 2\epsilon)$ over the input of Bob. Let us denote by $S \subseteq \{0,1\}^{2n}$ the set of these "good" x's.

Let $A \subset S$ be a set of x's, for which Alice sends the same message. Note that since A is a subset of S, the protocol is correct with probability at least $(1 - 2\epsilon)$ over the inputs $x \in A$. We are going to show that the size of A cannot be too large.

Let $g : \{0,1\}^{2n} \to \mathcal{R}$ be the uniform distribution over the set A, i.e.

$$g(x) = \begin{cases} \frac{1}{|A|} & \text{for } x \in A \\ 0 & \text{for } x \notin A \end{cases}$$

For any matching M we define $g_M : \{0,1\}^n \to \mathcal{R}$ to be the distribution of Mx when x is picked uniformly from the set A, i.e.

$$g_M(y) = \frac{|\{x \in A | Mx = y\}|}{|A|}$$

For the ℓ_1 norm of $f * g_M$ we have

$$\begin{aligned} ||f * g_M||_1 &= \sum_{w\in\{0,1\}^n} |f * g_M(w)| = \sum_{w\in\{0,1\}^n} \left| \sum_{y\in\{0,1\}^n} f(y+w) g_M(y) \right| \\ &= \sum_{w\in\{0,1\}^n} \left| \frac{1}{|A|} \sum_{x\in A} f(Mx+w) \right| \end{aligned}$$

where the last equation follows from the definition of the function g_M. Since Alice's message is fixed for the set A and Bob's algorithm is deterministic, for every matching M we can split the set of w's into two sets $W_{b,M}$, where $b \in \{0,1\}$ is Bob's answer. Let $\mathcal{M}$ denote the set of all possible perfect matchings on $[2n]$ and $N = |\mathcal{M}|$. Then

$$\begin{aligned} &\frac{1}{N} \sum_{M\in\mathcal{M}} ||f * g_M||_1 \\ &= \frac{1}{N} \sum_{M\in\mathcal{M}} \sum_{w\in W_{0,M}} \left| \frac{1}{|A|} \sum_{x\in A} f(Mx+w) \right| + \frac{1}{N} \sum_{M\in\mathcal{M}} \sum_{w\in W_{1,M}} \left| \frac{1}{|A|} \sum_{x\in A} f(Mx+w) \right| \\ &\geq \frac{1}{N|A|} \left| \sum_{M\in\mathcal{M}} \sum_{w\in W_{0,M}} \sum_{x\in A} f(Mx+w) \right| + \frac{1}{N|A|} \left| \sum_{M\in\mathcal{M}} \sum_{w\in W_{1,M}} \sum_{x\in A} f(Mx+w) \right| \\ &= \frac{1}{N|A|} \left| \sum_{M\in\mathcal{M}} \sum_{w\in W_{0,M}} \sum_{x\in A} (\mathrm{Prob}_{\mu_0}[Mx+w] - \mathrm{Prob}_{\mu_1}[Mx+w]) \right| \\ &+ \frac{1}{N|A|} \left| \sum_{M\in\mathcal{M}} \sum_{w\in W_{1,M}} \sum_{x\in A} (\mathrm{Prob}_{\mu_0}[Mx+w] - \mathrm{Prob}_{\mu_1}[Mx+w]) \right| \\ &\geq \frac{1}{N|A|} \left| \sum_{M\in\mathcal{M}} \sum_{w\in W_{0,M}} \sum_{x\in A} \mathrm{Prob}_{\mu_0}[Mx+w] \right| - \frac{1}{N|A|} \left| \sum_{M\in\mathcal{M}} \sum_{w\in W_{0,M}} \sum_{x\in A} \mathrm{Prob}_{\mu_1}[Mx+w] \right| \\ &+ \frac{1}{N|A|} \left| \sum_{M\in\mathcal{M}} \sum_{w\in W_{1,M}} \sum_{x\in A} \mathrm{Prob}_{\mu_1}[Mx+w] \right| - \frac{1}{N|A|} \left| \sum_{M\in\mathcal{M}} \sum_{w\in W_{1,M}} \sum_{x\in A} \mathrm{Prob}_{\mu_0}[Mx+w] \right| \end{aligned}$$

The protocol is correct when Bob answers $b \in \{0,1\}$ and the string w was drawn from the distribution $\mathcal{D}_b$. Since the protocol is correct with probability at least $1-2\epsilon$ we have

$$\begin{aligned} \frac{1}{N} \sum_{M\in\mathcal{M}} \frac{1}{|A|} \sum_{x\in A} \sum_{w\in W_{0,M}} \frac{1}{2} \mathrm{Prob}_{\mathcal{D}_0}[w] + \frac{1}{N} \sum_{M\in\mathcal{M}} \frac{1}{|A|} \sum_{x\in A} \sum_{w\in W_{1,M}} \frac{1}{2} \mathrm{Prob}_{\mathcal{D}_1}[w] &\geq 1-2\epsilon \\ \frac{1}{N|A|} \sum_{M\in\mathcal{M}} \sum_{w\in W_{0,M}} \sum_{x\in A} \mathrm{Prob}_{\mu_0}[Mx+w] + \frac{1}{N|A|} \sum_{M\in\mathcal{M}} \sum_{w\in W_{1,M}} \sum_{x\in A} \mathrm{Prob}_{\mu_1}[Mx+w] &\geq 2-4\epsilon \end{aligned}$$

Similarly,

$$\frac{1}{N|A|}\sum_{M\in\mathcal{M}}\sum_{w\in W_{0,M}}\sum_{x\in A}\text{Prob}_{\mu_1}[Mx+w]+\frac{1}{N|A|}\sum_{M\in\mathcal{M}}\sum_{w\in W_{1,M}}\sum_{x\in A}\text{Prob}_{\mu_0}[Mx+w] \;\leq\; 4\epsilon$$

Hence, we conclude that

$$\frac{1}{N}\sum_{M\in\mathcal{M}}||f*g_M||_1 \;\geq\; 2(1-4\epsilon)$$

The ℓ_1 and ℓ_2 norms are related by the following inequality

$$||f*g_M||_2^2 \geq \frac{||f*g_M||_1^2}{2^n}$$

and hence for the ℓ_2 norm we have

$$\begin{aligned}\frac{1}{N}\sum_{M\in\mathcal{M}}||f*g_M||_2^2 &\geq \frac{1}{N}\sum_{M\in\mathcal{M}}\frac{||f*g_M||_1^2}{2^n}=\frac{1}{2^n}\frac{1}{N}\sum_{M\in\mathcal{M}}||f*g_M||_1^2\geq\frac{1}{2^n}\left(\frac{1}{N}\sum_{M\in\mathcal{M}}||f*g_M||_1\right)^2\\ &\geq \frac{1}{2^{n-2}}(1-4\epsilon)^2 \qquad (1)\end{aligned}$$

By Parseval's identity (lemma 1) and the convolution theorem (lemma 2) it holds that

$$||f*g_M||_2^2=2^n\sum_s(\widehat{f*g_M}(s))^2=2^{3n}\sum_s(\hat{f}(s))^2(\hat{g_M}(s))^2$$

Using the expression for the Fourier coefficients of f we have

$$\begin{aligned}\frac{1}{N}\sum_{M\in\mathcal{M}}||f*g_M||_2^2 &= \frac{1}{N}\sum_{M\in\mathcal{M}}2^{3n}\sum_s(\hat{f}(s))^2(\hat{g_M}(s))^2=\frac{2^{3n}}{N}\sum_{M\in\mathcal{M}}\sum_{\substack{s:h(s)=k\\ k\ odd}}\frac{4}{2^{2n+2k}}(\hat{g_M}(s))^2\\ &= 2^{n+2}\frac{1}{N}\sum_{M\in\mathcal{M}}\sum_{\substack{s:h(s)=k\\ k\ odd}}\frac{1}{2^{2k}}(\hat{g_M}(s))^2 \qquad (2)\end{aligned}$$

Putting (1) and (2) together we have

$$(1-4\epsilon)^2\leq 2^{2n}\frac{1}{N}\sum_{M\in\mathcal{M}}\sum_{\substack{s:h(s)=k\\ k\ odd}}\frac{1}{2^{2k}}(\hat{g_M}(s))^2 \qquad (3)$$

We now relate the Fourier coefficients of g_M with those of g. Note first that if M is an $(n\times 2n)$ matrix, $x\in\{0,1\}^{2n}$ and $s\in\{0,1\}^n$ then

$$(Mx)^T\cdot s=(x^TM^T)\cdot s=x^T\cdot(M^Ts)$$

By the definition of g_M, its Fourier coefficients are

$$\hat{g}_M(s) = \frac{1}{2^n}\sum_y g_M(y)(-1)^{y^T\cdot s} = \frac{1}{2^n|A|}\Big(|\{x\in A|(Mx)^T\cdot s=0\}| - |\{x\in A|(Mx)^T\cdot s=1\}|\Big).$$

Let $s_M = M^T s$ and note that $h(s_M) = 2h(s)$. Then,

$$\begin{aligned}
\hat{g}(s_M) &= \frac{1}{2^{2n}}\sum_{x\in\{0,1\}^{2n}} g(x)(-1)^{x^T\cdot s_M} = \frac{1}{2^{2n}|A|}\Big(|\{x\in A|\ x^T\cdot s_M=0\}| - |\{x\in A|\ x^T\cdot s_M=1\}|\Big)\\
&= \frac{1}{2^{2n}|A|}\Big(|\{x\in A|\ (Mx)^T\cdot s=0\}| - |\{x\in A|\ (Mx)^T\cdot s=1\}|\Big)\\
&= \frac{1}{2^n}\hat{g}_M(s)
\end{aligned}$$

Inequality (3) now becomes

$$\begin{aligned}
(1-4\epsilon)^2 &\le 2^{2n}\frac{1}{N}\sum_{M\in\mathcal{M}}\sum_{\substack{s:h(s)=k\\ k\ odd}}\frac{1}{2^{2k}}(\hat{g_M}(s))^2\\
&= 2^{2n}\frac{1}{N}\sum_{M\in\mathcal{M}}\sum_{\substack{s:h(s)=k\\ k\ odd}}\frac{1}{2^{2k}}\ 2^{2n}\ (\hat{g}(s_M))^2\\
&= 2^{4n}\frac{1}{N}\sum_{M\in\mathcal{M}}\sum_{\substack{s:h(s)=k\\ k\ odd}}\frac{1}{2^{2k}}(\hat{g}(s_M))^2 \qquad (4)
\end{aligned}$$

In the above expression we first sum over all matchings and then over the string s. In what follows we will try to change the order of the summation. Note that in the above expression when $h(s)$ is odd, $h(s_M) = 2 \mod 4$. For any $k = 2 \mod 4$ we define γ_k as follows:
Let $z \in \{0,1\}^{2n}$ be any string of hamming weight k and M be a random matching. Then

$$\gamma_k = \mathrm{Prob}_M[\exists s \text{ s.t. } z = s_M]$$

Note that this probability depends only on k and not on the specific string z. For any even number $t \ge 2$, let $N(t)$ be the number of perfect matchings on $[t]$. Then,

$$N(2) = 1,\ \ N(t) = (t-1)N(t-2).$$

It is not hard to see that the expression for γ_k is

$$\gamma_k = \frac{N(k)N(2n-k)}{N(2n)} = \frac{(k-1)(k-3)\cdot\ldots\cdot 1}{(2n-1)(2n-3)\cdot\ldots\cdot(2n-k+1)} \le \left(\frac{k}{2n}\right)^{k/2}$$

We now rewrite inequality (4) after changing the order of the summation

$$(1-4\epsilon)^2 \le 2^{4n}\sum_{\substack{z:h(z)=k\\ k=2(mod4)}}\frac{1}{2^k}\ \gamma_k\ (\hat{g}(z))^2$$

and hence

$$\begin{aligned} 1 &\leq \frac{1}{(1-4\epsilon)^2}\, 2^{4n} \sum_{\substack{z:h(z)=k \\ k=2(mod4)}} \frac{1}{2^k}\, \gamma_k\, (\hat{g}(z))^2 \\ &= \sum_{k=2(mod4)} \frac{1}{(1-4\epsilon)^2}\, 2^{4n} \sum_{z:h(z)=k} \frac{1}{2^k}\, \gamma_k\, (\hat{g}(z))^2 \end{aligned}$$

From the above inequality, it is easy to see that there exists a k such that

$$\frac{1}{(1-4\epsilon)^2}\, 2^{4n} \sum_{z:h(z)=k} \frac{1}{2^k} \gamma_k (\hat{g}(z))^2 \;\geq\; \frac{1}{2^{k/2}} \Big/ \sum_{r=2(mod4)} \frac{1}{2^{r/2}}$$

otherwise sum over $k = 2 \mod 4$ to get a contradiction. Moreover,

$$\sum_{r=2(mod4)} \frac{1}{2^{r/2}} \leq \frac{2}{3}$$

and hence for that k

$$2^{4n} \sum_{z:h(z)=k} \frac{1}{2^{k/2}} \gamma_k (\hat{g}(z))^2 \;\geq\; \frac{3(1-4\epsilon)^2}{2}.$$

We choose small enough ϵ such that $\frac{3(1-4\epsilon)^2}{2} \geq 1$ and then we rewrite the above inequality as

$$\frac{2^{4n}}{|A|^2} \sum_{z:h(z)=k} \gamma_k |A|^2 (\hat{g}(z))^2 \;\geq\; 2^{k/2} \tag{5}$$

Let $\delta = (\gamma_k)^{1/k}$. Note that $0 \leq \delta \leq 1$. By the KKL inequality (lemma 3) [KKL88], we know that

$$\sum_{z:h(z)=k} \delta^k |A|^2 (\hat{g}(z))^2 \leq \left(\frac{|A|}{2^{2n}}\right)^{\frac{2}{1+\delta}}.$$

Hence, inequality (5) becomes

$$2^{k/2} \;\leq\; \frac{2^{4n}}{|A|^2} \left(\frac{|A|}{2^{2n}}\right)^{\frac{2}{1+\delta}} = \left(\frac{|A|}{2^{2n}}\right)^{\frac{-2\delta}{1+\delta}} \leq \left(\frac{|A|}{2^{2n}}\right)^{-2\delta}$$

and therefore

$$\frac{|A|}{2^{2n}} \leq \left(2^{k/2}\right)^{-1/2\delta} = 2^{-k/4\delta} \tag{6}$$

We know that $\gamma_k \leq \left(\frac{k}{2n}\right)^{k/2}$ and $k \geq 2$, so

$$\frac{k}{4\delta} = \frac{k}{4(\gamma_k)^{1/k}} \geq \frac{k}{4\left(\frac{k}{2n}\right)^{1/2}} = \frac{\sqrt{2nk}}{4} \geq \frac{\sqrt{n}}{2}.$$

From inequality (6) we conclude that

$$\begin{aligned} \frac{|A|}{2^{2n}} &\leq 2^{\frac{-\sqrt{n}}{2}} \\ |A| &\leq 2^{2n-\Omega(\sqrt{n})} \end{aligned}$$

Since the size of any $|A|$ cannot be more than $2^{2n-\Omega(\sqrt{n})}$, it means that there are at least $2^{\Omega(\sqrt{n})}$ different sets A. In other words, there are at least $2^{\Omega(\sqrt{n})}$ different messages that Alice sends and therefore the length of her message is at least $\Omega(\sqrt{n})$. □

References

[Abl96] F. Ablayev. Lower bounds for one-way probabilistic communication complexity and their application to space complexity. *Theoretical Computer Science*, 157(2):139–159, 1996.

[Bec75] W. Beckner. Inequalities in Fourier Analysis. *Annals of Mathematics,* 102:159–182 , 1975.

[Bon70] A. Bonami. Etude des coefficients de Fourier des fonctions de Lp (G). *Annales de l'Instute Fourier*, 20(2):335–402 , 1970.

[BJK04] Ziv Bar-Yossef, T. S. Jayram, Iordanis Kerenidis Exponential separation of quantum and classical one-way communication complexity, *Proceedings of ACM STOC 2004*

[BCW98] H. Buhrman, R. Cleve, and A. Wigderson. Quantum vs. classical communication and computation. In *Proceedings of the 30th ACM Symposium on Theory of Computing (STOC)*, pages 63–68, 1998.

[BCWdW01] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf. Quantum fingerprinting. *Physical Review Letters*, 87(16), 2001.

[BK97] L. Babai and P. G. Kimmel. Randomized simultaneous messages: Solution of a problem of Yao in communication complexity. In *Proceedings of the 12th IEEE Conference on Computational Complexity (CCC)*, pages 239–246, 1997.

[GKRdW06] Dmitry Gavinsky, Julia Kempe, Oded Regev, and Ronald de Wolf. Bounded-error quantum state identification and exponential separations in communication complexity. *Proceedings of ACM Symposium on Theory of Computing (STOC)*, 2006.

[GKdW06] Dmitry Gavinsky, Julia Kempe and Ronald de Wolf. Exponential separation of quantum and classical one-way communication complexity for a boolean function. Manuscript, 2006.

[KKL88] J. Kahn, G. Kalai, N. Linial The influence of variables on Boolean functions. *Proceedings of 29th IEEE Symp. Foundations of Computer Science (FOCS), 1988*

[Kla01] H. Klauck. Lower Bounds for Quantum Communication Complexity. In *Proceedings of the 42th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 288–297, 2001.

[KN97] E. Kushilevitz and N. Nisan. *Communication Complexity*. Cambridge University Press, 1997.

[KNR99] I. Kremer, N. Nisan, and D. Ron. On randomized one-round communication complexity. *Computational Complexity*, 8(1):21–49, 1999.

[NC00] M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[NS96] I. Newman and M. Szegedy. Public vs. private coin flips in one round communication games. In *Proceedings of the 28th ACM Symposium on Theory of Computing (STOC)*, pages 561–570, 1996.

[PS84] C. H. Papadimitriou and M. Sipser. Communication complexity. *Journal of Computer and System Sciences*, 28(2):260–269, 1984.

[Raz95] R. Raz. Fourier analysis for probabilistic communication complexity. *Computational Complexity*, 5(3):205–221, 1995.

[Raz99] R. Raz. Exponential separation of quantum and classical communication complexity. In *Proceedings of the 31st ACM Symposium on Theory of Computing (STOC)*, pages 358–367, 1999.

[Yao79] A. C-C. Yao. Some complexity questions related to distributive computing. In *Proceedings of the 11th ACM Symposium on Theory of Computing (STOC)*, pages 209–213, 1979.

[Yao83] A. C-C. Yao. Lower bounds by probabilistic arguments. In *Proceedings of the 24th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 420–428, 1983.

[Yao93] A. C-C. Yao. Quantum circuit complexity. In *Proceedings of the 34th IEEE Annual Symposium on Foundations of Computer Science (FOCS)*, pages 352–361, Los Alamitos, CA, 1993.