Fooling One-Sided Quantum Protocols

Hartmut Klauck*
CQT and Nanyang Technological University
Singapore
hklauck@gmail.com

Ronald de Wolf†
CWI and University of Amsterdam
The Netherlands
rdewolf@cwi.nl

Abstract

We use the venerable "fooling set" method to prove new lower bounds on the quantum communication complexity of various functions. Let $f : X \times Y \to \{0,1\}$ be a Boolean function, $\mathrm{fool}^1(f)$ its maximal fooling set size among 1-inputs, $Q_1^*(f)$ its one-sided error quantum communication complexity with prior entanglement, and $NQ(f)$ its nondeterministic quantum communication complexity (without prior entanglement; this model is trivial with entanglement). Our main results are the following, where logs are to base 2:

- $Q_1^*(f) \geq \dfrac{\log \mathrm{fool}^1(f) - 1}{2}$. This result is tight via superdense coding, and gives optimal bounds for basic functions like equality and disjointness (for the former, no super-constant lower bound seems to follow from other known techniques).
- $NQ(f) \geq \frac{1}{2} \log \mathrm{fool}^1(f) + 1$. We do not know if the factor 1/2 is needed in this result, but it cannot be replaced by 1: we give an example where $NQ(f) \approx 0.613 \log \mathrm{fool}^1(f)$.

1 Introduction

1.1 Background: fooling classical communication protocols

Communication complexity [Yao79, KN97] is one of the most versatile computational models we have, and *lower bounds* on communication complexity are one of the main sources of lower bounds in many other areas, from circuits to data structures to data streams. One of the simplest and most intuitive ways to prove lower bounds on communication protocols is by exhibiting a large *fooling set*, which was first done in [Yao79, LS81]. Suppose Alice and Bob want to compute some function $f : X \times Y \to \{0,1\}$, given inputs $x \in X$ and $y \in Y$, respectively. A 1-fooling set for f is a set $F = \{(x,y)\}$ of input pairs with the following properties:

(1) If $(x,y) \in F$ then $f(x,y) = 1$
(2) If $(x,y), (x',y') \in F$ then $f(x,y') = 0$ or $f(x',y) = 0$

*Research at the Centre for Quantum Technologies is funded by the Singapore Ministry of Education and the National Research Foundation.

†Partially supported by a Vidi grant from the Netherlands Organization for Scientific Research (NWO), and by the European Commission under the project QCS (Grant No. 255961). Most of this work was done when RdW was visiting CQT, whose hospitality is gratefully acknowledged.

For example, consider the n-bit equality function EQ, defined on $x, y \in \{0,1\}^n$ as $\mathrm{EQ}(x,y) = 1$ iff $x = y$. This has a 1-fooling set $F = \{(x,x)\}$ of size 2^n, since $\mathrm{EQ}(x,x) = 1$ for all x by $\mathrm{EQ}(x,y) = 0$ for all distinct x, y. The n-bit disjointness function DISJ, defined as $\mathrm{DISJ}(x,y) = 1$ iff $|x \wedge y| = 0$, also has a 1-fooling set of size 2^n, which can be seen as follows: write its communication matrix as $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{\otimes n}$, and take the anti-diagonal as the 1-fooling set. All entries on the anti-diagonal are 1 (giving the first property) and all entries below the anti-diagonal are 0 (giving the second property).

Now consider for simplicity a deterministic protocol computing f. Suppose the last bit of the conversation is the output bit, so both parties end up knowing the output. Consider input pairs $(x,y), (x',y') \in F$. For both inputs, the first property of the fooling set says that the correct output value is 1. Suppose, by way of contradiction, that the conversation between Alice and Bob is the same on both input pairs. If we switch input pair (x,y) to (x,y') then nothing changes from Alice's perspective (neither her input nor the conversation changes), so the output will still be 1. Similarly, if we switch (x,y) to (x',y) then the output won't change from Bob's perspective. But by the second property of fooling sets, for at least one of (x,y') and (x',y), the correct output is 0! Hence the conversations on inputs (x,y) and (x',y') must have been different. Accordingly, the bigger our fooling set F is, the more distinct conversations we must allow and hence the more bits of communication are needed.

More precisely, the communication complexity is lower bounded by $\log|F|+1$. The formal proof of this fact is based on the notion of *monochromatic rectangles*. A rectangle is a set $R = A \times B$, where $A \subseteq X$ and $B \subseteq Y$. Such a rectangle is *1-monochromatic* if $f(x,y) = 1$ for all $(x,y) \in R$. Note that a rectangle containing 1-inputs $(x,y), (x',y') \in F$ cannot be 1-monochromatic, because by the rectangle property it also contains (x,y') and (x',y), at least one of which is a 0-input by the fooling set property. Accordingly, if we want to include F in a set of 1-rectangles, we need a separate 1-rectangle for each element of F, and hence need at least $|F|$ different rectangles. It is well-known that a deterministic c-bit communication protocol induces a partition of the set of all 1-inputs into 2^{c-1} 1-monochromatic rectangles, so the previous argument implies $2^{c-1} \geq |F|$; equivalently $c \geq \log|F| + 1$. In fact even *nondeterministic* communication complexity is lower bounded by $\log|F| + 1$, since a c-bit nondeterministic protocol gives rise to a *cover* (rather than partition) of the set of all 1-inputs by 2^{c-1} 1-monochromatic rectangles, and we still need a separate rectangle for each element of F.

In contrast, a *quantum* communication protocol does not naturally induce a partition or cover of the 1-inputs into rectangles[1], so the above way of reasoning fails. In fact, in contrast to the classical case, the number of monochromatic rectangles needed to partition the 1-inputs does not provide a lower bound on exact quantum protocols, as witnessed by the exponential separation in [BCW98]. Nevertheless, in this paper we show how fooling sets can still be used to lower bound quantum communication complexity. We do this in two settings: one-sided error quantum protocols with unlimited prior entanglement and nondeterministic quantum protocols without entanglement. These results also imply lower bound for quantum "Las Vegas" or "zero-error" protocols (i.e., quantum protocols that never err, but have probability $\leq 1/2$ of giving up without a result).

[1] It can be viewed as approximately producing rectangles *with signs* [Kla07, Section 3].

1.2 Our results: fooling one-sided error quantum protocols

First, we study one-sided error protocols: protocols that always output 0 on inputs x, y where $f(x, y) = 0$, and that output 1 with probability at least 1/2 on inputs where $f(x, y) = 1$. In Section 2 we show:

$$Q_1^*(f) \geq \frac{\log \mathrm{fool}^1(f) - 1}{2}.$$

We have $Q_1^*(f) \leq n/2 + 1$ for any Boolean function where $X \subseteq \{0,1\}^n$, because superdense coding [BW92] allows Alice to send 2 classical bits using one EPR-pair and one qubit of communication. Hence Theorem 1 is essentially tight for functions where $\mathrm{fool}^1(f) = 2^n$, for example for equality and disjointness we get $Q_1^*(f) = n/2 \pm 1$. (For the special case of *exact* quantum protocols, we get the same bound without the '-1'.)

Surprisingly for such basic functions, these bounds were not known before. While it is possible to use Razborov's technique [Raz03] combined with results about polynomial approximation with very small error [BCWZ99] to show $Q_1^*(\mathrm{DISJ}) = \Omega(n)$, no lower bound larger than 1 was known for $Q_1^*(\mathrm{EQ})$. This gap in our knowledge was due to the fact that other existing lower bound methods can't give good lower bounds for equality, as we explain now. General lower bound methods for quantum communication complexity can be grouped into rank-based methods and methods based on approximation norms (in particular based on the γ_2-norm [LS09c]).[2] The linearity of norms makes it possible to prove lower bounds for quantum protocols in which Alice and Bob share prior entanglement. Rank-based methods, however, do not seem to directly apply to protocols with entanglement: in the case of exact quantum protocols a direct sum-based construction in [BW01] shows that the logarithm of the rank is a lower bound even in the presence of entanglement.[3] In the case of two-sided error and entanglement Lee and Shraibman [LS09a] show that the approximation rank yields lower bounds by relating it to the γ_2-norm. Since the communication matrix of EQ is the identity matrix I, and $\gamma_2(I) = O(1)$ for I of any size, there is no hope to use a connection between a one-sided error version of approximation rank and the γ_2-norm to establish a large lower bound on $Q_1^*(\mathrm{EQ})$. Whether a one-sided error version of approximation rank gives lower bounds for Q_1^* remains open, but we note that the construction in [LS09a] cannot be adapted to the one-sided error scenario.

So neither of the two main approaches to quantum communication complexity lower bounds provides us with a lower bound for $Q_1^*(\mathrm{EQ})$. Hence in this paper we take a different approach. We first simulate a quantum protocol with entanglement by a game without communication, in which Alice and Bob share entanglement, and they need to compute a function f conditioned on postselection on their local measurements. This approach itself is not new, and can for instance be used to show that the γ_2-norm is a lower bound, see [LS09b]. We then analyze the impact of Alice's and Bob's measurements on the single entangled state used in the game. The one-sided error requirement places strong constraints on those measurements, which we exploit to derive our lower bound in terms of fooling sets.

In a quantum *Las Vegas* protocol Alice and Bob compute a function f without error, but they are allowed to give up without a result with probability 1/2. The quantum Las Vegas commu-

[2] Information-theoretic methods [JRS03] have also been used to lower bound quantum communication complexity. However, the notion is defined there for internal information cost, and in this case the information cost for equality is $O(1)$, even for classical protocols without error [Bra12, Proposition 3.21].

[3] Footnote 2 of [BW01] claims such a bound for *zero-error* quantum protocols for equality and disjointness without proof, but in retrospect they didn't seem to have a proof of this.

nication complexity with entanglement $Q_0^*(f)$ is the minimum worst-case communication of any protocol that computes f under these requirements.[4] Quantum Las Vegas protocols were investigated in [BCWZ99, Kla00, Wol03] in the case where no prior entanglement is available. Since $Q_0^*(f) \geq \max\{Q_1^*(f), Q_1^*(\neg f)\}$ we immediately get large lower bounds on the quantum Las Vegas complexity of DISJ and EQ, but also the following general lower bound:

$$Q_0^*(f) \geq \frac{\log \mathrm{fool}(f) - 1}{2},$$

where $\mathrm{fool}(f)$ is the standard maximum fooling set size, i.e., the maximum over the largest 1-fooling set and 0-fooling set.

1.3 Our results: fooling nondeterministic quantum protocols

As a second main result, just like in the classical world fooling sets lower bound *nondeterministic* protocols, our second result shows that they also lower bound nondeterministic *quantum* protocols. For our purposes, we can define a nondeterministic protocol (quantum as well as classical) for a Boolean function f as one that has positive acceptance probability on input x, y iff $f(x, y) = 1$. In other words, it's like a one-sided-error protocol with the requirement of *large* acceptance probability on 1-inputs relaxed to *positive* acceptance probability. This model was introduced in [Wol03], which also exhibits a total function with an exponential separation between quantum and classical nondeterministic communication complexities.

Note that allowing unlimited prior entanglement trivializes the nondeterministic model, for the same reason that unlimited shared randomness trivializes it in the classical case: Alice and Bob can share a random variable r uniformly distributed over the set X of Alice's inputs; Alice sends a bit indicating whether $x = r$; if 'yes' then Bob outputs $f(r, y) = f(x, y)$, and if 'no' then he outputs 0. Hence if we were to allow unlimited prior randomness or entanglement, any function has nondeterministic communication complexity at most 1. Accordingly, we will study nondeterministic protocols which don't share anything at the start. In Section 3 we show the following lower bound on nondeterministic quantum communication complexity in terms of fooling sets:

$$NQ(f) \geq \frac{1}{2} \log \mathrm{fool}^1(f) + 1.$$

We do not know if the factor 1/2 is needed in this result, but it cannot be replaced by 1: in Section 3 we give an example of a function where $NQ(f) \leq \frac{\log 3}{\log 6} \log \mathrm{fool}^1(f) + 1$, where $\log 3 / \log 6 \approx 0.613$.

2 Lower bound for one-sided bounded-error quantum protocols

We assume familiarity with communication complexity. See [KN97] for more details about classical communication complexity and [Wol02] for quantum communication complexity. Our key lemma is based on a reasonably well-known trick to replace quantum communication by the guessing of twice as many classical bits:

[4] It is possible to define Las Vegas protocols as protocols that never err and place bounds on *expected* communication. The corresponding complexity measure is always larger or equal to the one considered here, and is smaller than 2 times our measure.

Lemma 1. *Suppose there is a quantum protocol P with inputs from $X \times Y$ and output in $\{0,1\}$, that uses some fixed starting state (possibly entangled) and q qubits of communication, and where a measurement of the last qubit on the channel gives the output. Then there exists another quantum protocol Q with a fixed starting state and no communication at all, where Alice outputs $a \in \{0,1\}$ and Bob outputs $b \in \{0,1\}$, such that*

$$\text{for all inputs } x, y : \Pr[Q \text{ outputs } a = b = 1] = 2^{-2q} \Pr[P \text{ outputs } 1].$$

Proof. We assume without loss of generality that P communicates *exactly* q qubits on all possible inputs. By the well-known teleportation primitive [BBC+93], we can replace each qubit of communication in P by the use of one additional EPR-pair and two classical bits of communication. These 2 bits are the outcome of a measurement by the sending party, and indicate which of the 4 Pauli matrices the receiving party has to apply on their end of the EPR-pair in order to obtain the qubit that the sender wanted to send. If the bits happen to be 00 (which happens with probability 1/4), then the right Pauli is the identity matrix, so then they don't need to do anything. Call the resulting $2q$-bit protocol P_{clas}.

Protocol Q is now as follows. Alice and Bob run protocol P_{clas} *assuming* all messages are 0-bits (so they don't communicate anything). Alice checks if all her teleportation measurements gave outcome 00. If not then she outputs $a = 0$; if yes then she outputs P_{clas}'s output if she was the one supposed to output that, and otherwise she outputs $a = 1$. Bob does the same from his end, outputting $b \in \{0,1\}$. Note that $a = b = 1$ iff all q teleportation measurements gave outcome 00 *and* the output of P would have been 1. The first event happens with probability 4^{-q} and the second event with $\Pr[P \text{ outputs } 1]$. Since these two events are independent we can multiply their probabilities to obtain the lemma. □

Note that the starting state of Q is the starting state of P augmented with an additional q EPR-pairs. Using the above lemma, we can prove the main result of this section:

Theorem 1. $Q_1^*(f) \geq \dfrac{\log \mathrm{fool}^1(f) - 1}{2}$.

Proof. Let $q = Q_1^*(f)$ and let P be a q-qubit entanglement-assisted protocol for f, whose acceptance probability is 0 on inputs $(x,y) \in f^{-1}(0)$ and at least 1/2 on $(x,y) \in f^{-1}(1)$. Apply Lemma 1 to this protocol to obtain a new protocol Q without communication, where Alice outputs $a \in \{0,1\}$, Bob outputs $b \in \{0,1\}$, satisfying

$$\Pr[a = b = 1] \geq 2^{-2q-1} \text{ on inputs } (x,y) \in f^{-1}(1)$$
$$\Pr[a = b = 1] = 0 \text{ on inputs } (x,y) \in f^{-1}(0)$$

Let ρ be the entangled starting state of protocol Q. Assume without loss of generality that, on input x, Alice applies a projective measurement with operators $A_x, I - A_x$ corresponding to outputs 1 and 0, respectively. Similarly Bob uses projections $B_y, I - B_y$.

Now consider a 1-fooling set F of size $\mathrm{fool}^1(f)$. Assume without loss of generality that it is of the form $F = \{(x,x)\}$ (this is just a matter of relabeling Bob's inputs), and define $S = \{x : (x,x) \in F\}$. Then from the properties of a 1-fooling set we have that for all $x, y \in S$ with $x \neq y$:

$$\mathrm{Tr}(A_x \otimes B_x \rho) = \Pr[a = b = 1] \geq 2^{-2q-1}$$
$$\mathrm{Tr}(A_x \otimes B_y \rho) = \Pr[a = b = 1] = 0 \text{ or } \mathrm{Tr}(A_y \otimes B_x \rho) = \Pr[a = b = 1] = 0$$

To simplify notation we will identify a projector A with the subspace on which it projects. Let $A^\perp$ denote the subspace orthogonal to A. Define $A'_x = A_x \cap (\text{span}\{A_y : f(y,x) = 0\})^\perp$. Since $A'_x \subseteq A_x$, replacing A_x by A'_x doesn't increase $\text{Tr}(A_x \otimes B_x\rho)$. Also, the replacement doesn't *de*crease that value, informally speaking because the subspaces A_y that are "subtracted" from A_x were such that $\text{Tr}(A_y \otimes B_x\rho) = 0$. Hence $\text{Tr}(A'_x \otimes B_x\rho) = \text{Tr}(A_x \otimes B_x\rho)$. Note that the subspace A'_x is orthogonal to the subspace A'_y (denoted $A'_x \perp A'_y$) whenever $f(y,x) = 0$. Similarly define $B'_x = B_x \cap (\text{span}\{B_y : f(x,y) = 0\})^\perp$, and note that by the above argument we have $\text{Tr}(A'_x \otimes B'_x\rho) = \text{Tr}(A_x \otimes B_x\rho)$, and $B'_x \perp B'_y$ whenever $f(x,y) = 0$. Crucially, for every distinct pair $x, y \in S$ the subspaces $A'_x \otimes B'_x$ and $A'_y \otimes B'_y$ are orthogonal. That is because

(1) if $f(y,x) = 0$ then $A'_x \perp A'_y$ and hence $A'_x \otimes B'_x \perp A'_y \otimes B'_y$
(2) if $f(x,y) = 0$ then $B'_x \perp B'_y$ and hence $A'_x \otimes B'_x \perp A'_y \otimes B'_y$

and by the properties of a fooling set, for each x, y we have $f(x,y) = 0$ or $f(y,x) = 0$. It follows that $\sum_{x\in S} A'_x \otimes B'_x \leq I$. Now we have the following

$$\begin{aligned} |F|2^{-2q-1} &\leq \sum_{x\in S} \text{Tr}(A_x \otimes B_x\rho) = \sum_{x\in S} \text{Tr}(A'_x \otimes B'_x\rho) \\ &= \text{Tr}\left((\sum_{x\in S} A'_x \otimes B'_x)\rho \right) \leq \text{Tr}(\rho) = 1. \end{aligned}$$

Rearranging gives the theorem. □

3 Lower bound for nondeterministic quantum protocols

In this section we study nondeterministic quantum protocols. The following algebraic characterization of nondeterministic quantum communication complexity of f is known. The *communication matrix* M_f for f is the $|X| \times |Y|$ Boolean matrix $M_f(x,y) = f(x,y)$. A *nondeterministic matrix* for f is any real or complex matrix M with the same support as M_f, i.e., such that $M_{x,y} = 0$ iff $f(x,y) = 0$. The *nondeterministic rank* of f is the minimal rank (over the reals) among all such matrices. [Wol03, Theorem 3.3] shows that $NQ(f) = \lceil \log \text{nrank}(f) \rceil + 1$.

The key to using fooling sets for nondeterministic quantum lower bounds is the following simple lemma, which uses a trick similar to the proof that fooling set size is at most quadratically bigger than rank [KN97, Lemma 4.15]:

Lemma 2. *For every function* $f : X \times Y \to \{0,1\}$ *we have* $\text{nrank}(f)^2 \geq \text{fool}^1(f)$.

Proof. Define $g : X^2 \times Y^2 \to \{0,1\}$ as $g(xx', yy') = f(x,y) \cdot f(y',x')$, and note the reversed role of the two inputs in the second f. If M is a nondeterministic matrix for f, then $M \otimes M^T$ is a nondeterministic matrix for g. Hence, choosing M of minimal rank, we have $\text{nrank}(f)^2 = \text{rank}(M)^2 = \text{rank}(M \otimes M^T) \geq \text{nrank}(g)$.

Now consider a 1-fooling set F for f of size $\text{fool}^1(f)$. Again assume without loss of generality it is of the form $F = \{(x,x)\}$. Consider (x,x) and (x',x') in F. Since $f(x,x) = 1$, we have $g(xx,xx) = f(x,x)f(x,x) = 1$. On the other hand, if $x \neq x'$ then since F is a fooling set we have $f(x,x') = 0$ or $f(x',x) = 0$, hence $g(xx,x'x') = f(x,x')f(x',x) = 0$. This shows that the communication matrix of g restricted to entries $\{xx\} \times \{x'x'\}$ is the $|F| \times |F|$ identity matrix: 1s on the diagonal and 0s off the diagonal. It is easy to see that the nondeterministic rank of the identity matrix is its dimension, and hence $\mathrm{nrank}(g) \geq |F| = \mathrm{fool}^1(f)$. Putting together the two inequalities gives the lemma. □

Taking logarithms and using that $NQ(f) = \lceil \log \mathrm{nrank}(f) \rceil + 1$, we get

Corollary 1. $NQ(f) \geq \frac{1}{2} \log \mathrm{fool}^1(f) + 1$.

For example for the equality function, this shows $NQ(f) \geq n/2 + 1$. However, for the equality function we already knew $NQ(f) = n + 1$ since obviously $\mathrm{nrank}(f) = 2^n$ [Wol03]. Hence it is natural to ask whether the constant 1/2 in the above corollary is needed. We don't know, but at least we can show that it needs to be less than 1. Specifically, we give an example where $NQ(f) \leq \frac{\log 3}{\log 6} \log \mathrm{fool}^1(f) + 1$, where $\frac{\log 3}{\log 6} \approx 0.613$. Consider the following 6×6 matrix of rank 3:

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & -1 & -1 & 0 \\ -1 & 1 & 1 & 0 & -1 & 0 \\ -1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$$

The Boolean matrix obtained by dropping the minus signs corresponds to a communication complexity problem $g : [6] \times [6] \to \{0, 1\}$ with a 1-fooling set of size 6 (just take the diagonal). Now let $f : X \times Y \to \{0, 1\}$ be the AND of k independent instances of g (so $|X| = |Y| = 6^k$). Because 1-fooling set size is multiplicative under taking ANDs, we have $\mathrm{fool}^1(f) = 6^k$. On the other hand, taking the k-fold tensor product of the above rank-3 matrix gives a nondeterministic matrix for f of rank 3^k. Hence $NQ(f) = \lceil \log \mathrm{nrank}(f) \rceil + 1 \approx \frac{\log 3}{\log 6} \log \mathrm{fool}^1(f) \approx 0.613 \log \mathrm{fool}^1(f)$.

A simpler but slightly weaker separation can be obtained from the 3-input non-equality function. This has nrank $= 2$ vs $\mathrm{fool}^1 = 3$, hence taking a k-fold AND of this gives a function $f : X \times Y \to \{0, 1\}$ with $|X| = |Y| = 3^k$ and $\mathrm{nrank}(f) = 2^k$ vs $\mathrm{fool}^1(f) = 3^k$. Taking logarithms, we have $NQ(f) \approx 0.63 \log \mathrm{fool}^1(f)$.

4 Conclusion and open problems

Equality and disjointness are two of the most important functions considered in communication complexity. Prior to this paper no large lower bound on the one-sided error or Las Vegas quantum communication complexity of these problems was known for the case of protocols with prior entanglement. In particular, for EQ previous lower bound methods were not applicable. We have shown that the fooling set method is applicable to one-sided error protocols with entanglement, resolving the complexity of these problems.

It is interesting to note that for classical protocols there is essentially no need to consider fooling sets at all: the method is completely subsumed by the rectangle bound (i.e., bounding the size of the largest monochromatic rectangle under some distribution). However, for quantum protocols with one-sided error and entanglement, and for quantum nondeterministic communication complexity the rectangle bound is not applicable.

We conclude with some open problems:

- One goal would be to show that classical deterministic complexity $D(f)$ and quantum Las Vegas complexity $Q_0(f)$ are polynomially close for all total functions. This is a (possibly easier) variant of a general conjecture that for total functions quantum communication yields only polynomial improvements in communication complexity. Proving a linear lower bound in terms of classical nondeterministic complexity (i.e., $Q_0(f) = \Omega(N(f))$) would settle that, since it is known that $D(f) = O(N(f)^2)$. However, an example from [Wol03] refutes that hope. Let $f(x, y) = 0$ if $|x \wedge y| = 1$ and $f(x, y) = 1$ otherwise. This function as well as its complement have linear $N(f)$, but $NQ(f), NQ(\neg f) = O(\sqrt{n})$. This does not, however, preclude a bound like $Q_0(f) = \Omega(\sqrt{N(f)})$, which would still achieve the above goal.
- Another problem is to show that the factor 2 in Corollary 1 is necessary. It seems hard to come up with a matrix for which the nondeterministic rank is the square root of the rank, as would be required by a construction along the lines of our separation at the end of Section 3.

References

[BBC+93] C. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70:1895–1899, 1993.

[BCW98] H. Buhrman, R. Cleve, and A. Wigderson. Quantum vs. classical communication and computation. In *Proceedings of 30th ACM STOC*, pages 63–68, 1998. quant-ph/9802040.

[BCWZ99] H. Buhrman, R. Cleve, R. de Wolf, and Ch. Zalka. Bounds for small-error and zero-error quantum algorithms. In *Proceedings of 40th IEEE FOCS*, pages 358–368, 1999. cs.CC/9904019.

[Bra12] M. Braverman. Interactive information complexity. In *ECCC report No. 123 (2011), to appear in STOC*, 2012.

[BW92] C. Bennett and S. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Physical Review Letters*, 69:2881–2884, 1992.

[BW01] H. Buhrman and R. de Wolf. Communication complexity lower bounds by polynomials. In *Proceedings of 16th IEEE Conference on Computational Complexity*, pages 120–130, 2001. cs.CC/9910010.

[HW02] P. Høyer and R. de Wolf. Improved quantum communication complexity bounds for disjointness and equality. In *Proceedings of 19th Annual Symposium on Theoretical Aspects of Computer Science (STACS'2002)*, volume 2285 of *Lecture Notes in Computer Science*, pages 299–310. Springer, 2002. quant-ph/0109068.

[JRS03] R. Jain, J. Radhakrishnan, and P. Sen. A lower bound for the bounded round quantum communication complexity of set disjointness. In *Proceedings of 44th IEEE FOCS*, pages 220–229, 2003.

[Kla00] H. Klauck. On quantum and probabilistic communication: Las Vegas and one-way protocols. In *Proceedings of 32nd ACM STOC*, pages 644–651, 2000.

[Kla07] H. Klauck. Lower bounds for quantum communication complexity. *SIAM Journal on Computing*, 37(1):20–46, 2007. Earlier version in FOCS'01. quant-ph/0106160.

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

[LS81] R. J. Lipton and R. Sedgewick. Lower bounds for VLSI. In *Proceedings of 13th ACM STOC*, pages 300–307, 1981.

[LS09a] T. Lee and A. Shraibman. An approximation algorithm for approximation rank. In *Proceedings of 24th IEEE Conference on Computational Complexity*, pages 351–357, 2009.

[LS09b] T. Lee and A. Shraibman. Lower bounds in communication complexity. *Foundations and Trends in Theoretical Computer Science*, 3(4):263–398, 2009.

[LS09c] N. Linial and A. Shraibman. Lower bounds in communication complexity based on factorization norms. *Random Struct. Algorithms*, 34(3):368–394, 2009. Earlier version in STOC'07.

[Raz03] A. Razborov. Quantum communication complexity of symmetric predicates. *Izvestiya of the Russian Academy of Sciences, mathematics*, 67(1):159–176, 2003. quant-ph/0204025.

[Wol00] R. de Wolf. Characterization of non-deterministic quantum query and quantum communication complexity. In *Proceedings of 15th IEEE Conference on Computational Complexity*, pages 271–278, 2000. cs.CC/0001014.

[Wol02] R. de Wolf. Quantum communication and complexity. *Theoretical Computer Science*, 287(1):337–353, 2002.

[Wol03] R. de Wolf. Nondeterministic quantum query and quantum communication complexities. *SIAM Journal on Computing*, 32(3):681–699, 2003. Journal version of parts of [Wol00] and [HW02].

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