The Complexity of Quantum Disjointness*

Hartmut Klauck

Centre for Quantum Technologies and Nanyang Technological University, Singapore
hklauck@gmail.com

Abstract

We introduce the communication problem QNDISJ, short for *Quantum (Unique) Non-Disjointness*, and study its complexity under different modes of communication complexity. The main motivation for the problem is that it is a candidate for the separation of the quantum communication complexity classes QMA and QCMA. The problem generalizes the Vector-in-Subspace and Non-Disjointness problems. We give tight bounds for the QMA, quantum, randomized communication complexities of the problem. We show polynomially related upper and lower bounds for the MA complexity. We also show an upper bound for QCMA protocols, and show that the bound is tight for a natural class of QCMA protocols for the problem. The latter lower bound is based on a geometric lemma, that states that every subset of the n-dimensional sphere of measure 2^{-p} must contain an ortho-normal set of points of size $\Omega(n/p)$.

We also study a “small-spaces“ version of the problem, and give upper and lower bounds for its randomized complexity that show that the QNDISJ problem is harder than Non-disjointness for randomized protocols. Interestingly, for quantum modes the complexity depends only on the dimension of the smaller space, whereas for classical modes the dimension of the larger space matters.

1998 ACM Subject Classification F.1.2 Modes of Computation, F.1.3 Complexity Measures and Classes

Keywords and phrases Communication Complexity, Quantum Proof Systems

Digital Object Identifier 10.4230/LIPIcs.MFCS.2017.15

1 Introduction

Communication complexity [30, 23] is a central area in computational complexity and the source of many lower bounds for other computational (nonuniform) models. Because of this much of the research in communication complexity is focused on lower bounds. Most of these lower bound applications employ the lower bound to the Disjointness problem shown by Kalyanasundaram and Schnitger [14] (see also [26, 7] for simpler proofs), or, in the quantum case the lower bound by Razborov [27] (see also [28]).

The present paper is mainly motivated by the following open problem. The complexity class QMA (in the Turing machine world) is the quantum analogue of NP (or rather of MA), namely the class of problems, that can be verified efficiently given a (non-interactive) quantum proof (by a quantum verifier). Similarly, QCMA is the class of problems where a *classical* proof can be verified efficiently by a quantum verifier. Obviously, the relationship between the two classes is highly interesting. This relates to the problem of whether more

[*] This work is funded by the Singapore Ministry of Education (partly through the Academic Research Fund Tier 3 MOE2012-T3-1-009) and by the Singapore National Research Foundation. Also supported by Majulab UMI 3654.

42nd International Symposium on Mathematical Foundations of Computer Science (MFCS 2017).
Editors: Kim G. Larsen, Hans L. Bodlaender, and Jean-Francois Raskin; Article No. 15; pp. 15:1–15:13
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

information can be present in a quantum state than in a classical state (of the same size), in this case based on the capacity to function as a proof. This problem was first suggested by Aharonov and Naveh [5].

Aharonov and Naveh have conjectured that $QCMA = QMA$, because the local Hamiltonian problem is complete for QMA (Turing machine model, [15]), and hence in some sense only a constant number of qubits in a quantum proof need to be touched by the verifier at once, so only localized entanglement seems necessary. Nevertheless such a result has not been established since. On the other hand, obviously we are far away from proving such separations as $QCMA \neq QMA$ for the Turing machine model (one implication would be $P \neq PSPACE$). Aaronson and Kuperberg [3] have shown a separation of the classes relative to a *quantum* oracle, a result that does not imply the usual relativization obstacle to showing that the classes are equal. It remains open whether $QCMA \neq QMA$ relative to some *classical oracle* (which would imply that anyone who wants to show that $QMA = QCMA$ must use non-relativizing techniques). Aaronson and Wigderson [4] have proposed the stronger *algebrization* obstacle to showing complexity theoretic results, and give many examples of such results requiring non-algebrizing techniques. One of their methods is to use separations of complexity classes in communication complexity (see [6]) in order to show algebrization separations. This motivates trying to separate QCMA and QMA in communication complexity (besides the power of quantum proofs being interesting in any model). The main reason why this is preferable over trying to solve the (usually easier) separation in the query complexity model (which would give an oracle separation) is that we have a proper candidate problem for the separation, namely the problem Linear-Space-Distance (LSD) introduced by Raz and Shpilka [25], who show that LSD is QMA-complete (for the communication complexity model).

Due the QMA-completeness of LSD, if there is a separation of QMA from QCMA (in communication complexity), then there is one using LSD. However, the problem is awkward in the sense that the 1-inputs (resp. the 0-inputs) do not form a manifold. This complicates reasoning about the problem, which is of a geometrical nature, and is best studied in its non-discretized version. We propose a subproblem of LSD that has the following nice properties: its input sets are Riemannian manifolds and there are nontrivial protocols for various modes of communication for the problem, exhibiting limits on lower bounds that can be shown, guiding our intuition.

The problem we propose is called Quantum (Unique) Non-Disjointness (short QNDISJ). Informally, the 0-inputs of QNDISJ are pairs (W_A, W_B) of subspaces of $\mathbb{R}^n$ that are orthogonal to each other, while the 1-inputs are pairs such that $W_A \cap W_B$ has dimension 1, and the spaces are orthogonal outside of their intersection.

We view QNDISJ as a natural quantum analogue of the Disjointness problem. This works as follows: For a fixed ortho-normal basis of $\mathbb{R}^n$ a subset $x \subseteq \{1, \ldots, n\}$ can be identified with a subspace (by taking the span of the basis vectors indexed by x). Hence, if Alice and Bob have sets of size s, t respectively that are disjoint, then their inputs correspond to two orthogonal subspaces, i.e., a 0-inputs of QNDISJ. If the sets intersect on 1 element, then the two subspaces have a 1-dimensional intersection, and they are (also) a 1-input. The difference between (the complement) of Disjointness and QNDISJ is then that there is no fixed basis for the latter problem, but rather that Alice and Bob know their own subspaces, but no good basis of the whole space, in which the intersecting (unit) vector is a basis vector.

Another problem of which QNDISJ is a generalization is the Vector-in-Subspace problem [22, 24, 16], which is the same problem, only that Alice has a 1-dimensional subspace, and Bob an $n/2$-dimensional subspace. For this problem Klartag and Regev give a $\Omega(n^{1/3})$ lower bound on the randomized communication complexity and Raz gives a randomized $O(\sqrt{n})$ upper bound, with the upper bound likely tight. The quantum complexity of this problem is $O(\log n)$.

We explore the communication complexity of QNDISJ for the following modes of communication: QMA, QCMA, MA, randomized, quantum. We also consider the version of the problem, where the dimensions of the subspaces are s, t with $s \leq t \leq n/2$. We give (almost) matching upper and lower bounds for randomized, quantum, QMA-protocols in the case $s = t = n/4$. We give non-trivial bounds for smaller spaces as well (see the table later on). One interesting conclusion is that for the quantum modes (Q, QCMA, QMA) the complexity depends (up to small factors) only on s, the dimension of the smaller space, whereas for the classical modes (R, MA) the complexity of the larger space matters. We also give a lower bound for QCMA protocols for QNDISJ under a restriction on the protocols. This restriction is that the proof (sent by Merlin, who sees both subspaces) depends on the intersection of the subspaces *only* (and can hence be viewed as an (arbitrary) subset of the sphere). We prove a geometric lemma about large subsets of the sphere that allows us to reduce a smaller instance of Disjointness to the "leftover" problem of QNDISJ, once one of the classical proofs is fixed (namely the problem of accepting all 1-inputs for which this proof is good, while rejecting all 0-inputs).

Our restriction seems natural, because it is difficult to imagine how other information from Merlin could be useful to Alice (who knows her space, just not the intersection) or Bob. So our conditional bound can be seen as some evidence that quantum proofs are really more powerful than classical proofs. We note that a separation between QMA- and QCMA-communication complexity in the one-way model is known [21], but that result has no bearing on algebrization and the analogous problem for Turing machines.

2 Organization of the Paper

This is an extended abstract. In the next section we give a formal definition of $QNDISJ_{s,t}$. In Section 4 we have a table describing our results and define the property under which our conditional QCMA lower bound holds. In Section 5 we have preliminaries, and in Section 6 a rough overview of our main techniques. See the full paper for more formal statements and for proofs.

3 Definition of the Problem

Denote by $S^{n-1} = \{x \in \mathbb{R}^n : ||x|| = 1\}$ the sphere. The Grassmannian is $G_{n,m} = \{V : V \subseteq \mathbb{R}^n$ and V is an m-dimensional subspace$\}$. We define our main problem on two manifolds. Throughout the paper we will fix n as the dimension of the underlying space when talking about our problem. s, t are the dimensions of Alice's and Bob's subspace and we will always have $s \leq t \leq n/2$.

▶ **Definition 1.** The *orthogonal manifold* $O_{s,t}$ is the set of pairs of subspaces W_A, W_B, where W_A is an s-dimensional subspace of $\mathbb{R}^n$, W_B a t-dimensional subspace of $\mathbb{R}^n$, and $W_A \perp W_B$.

▶ **Definition 2.** The *intersection manifold* $I_{s,t}$ is the set of pairs of subspaces W_A, W_B, where W_B is an s-dimensional subspace of $\mathbb{R}^n$, W_B a t-dimensional subspace of $\mathbb{R}^n$, and W_A, W_B intersect in a 1-dimensional subspace spanned by some vector z. Furthermore $(W_A \cap z^\perp) \perp (W_B \cap z^\perp)$.

Table 1 Complexity of $QNDISJ_{s,t}$ for $s \leq t$.

Mode	Upper Bound	Lower Bound
QMA	$O(\log n)$	$\Omega(\sqrt{\log t})$ 1)
R	$O(\min\{s\sqrt{t}, n \log n\})$	$\Omega(s(t/s)^{1/3})$
Q	$O(\sqrt{s}\log n)$	$\Omega(\sqrt{s})$
MA	$O(\sqrt{s\sqrt{t}})$	$\Omega(t^{1/6})$
QCMA	$O(s^{1/3}\log n)$	$\Omega(s^{1/3})$ (*)

1) The lower bound becomes $\Omega(\log t)$, if Alice and Bob do not share entanglement.

(*) This lower bound is conditional on assumption (*) about protocols (see below).

▶ **Definition 3.** The problem $QNDISJ_{s,t}$ is a partial function. The set of 1-inputs is $I_{s,t}$. The set of 0-inputs is $O_{s,t}$. For all other pairs of subspaces the function is undefined.

When we don't indicate s, t, then $s = t = \frac{n}{4}$. We leave n, the dimension of the underlying space, implicit.

To provide some insight as to the name of the problem, consider Razborov's hard distribution for the Disjointness problem [26]: disjoint inputs are disjoint pairs of sets of size $n/4$, intersecting inputs are pairs of sets of size $n/4$ that have intersection size 1. If we fix an ortho-normal basis of $\mathbb{R}^n$, we can view each set as picking $n/4$ basis vectors and hence consider Alice and Bob's inputs as subspaces of dimension $n/4$. The subspaces are orthogonal for disjoint sets and are in the intersection manifold for intersecting inputs.

The difference between Non-disjointness and $QNDISJ$ is that Alice and Bob *do not know a good basis* for the whole space. Alice knows her space, and she can find a basis for her space, but the intersecting vector is a basis vector only in a hidden basis neither she nor Bob know. The situation is as if someone would take the Non-disjointness example above, and apply a secret unitary transformation to the bases of the subspaces, and then only hand the transformed basis of W_A to Alice and only the transformed basis of W_B to Bob.

The Vector-in-Subspace problem is $QNDISJ_{1,n/2}$. Similar to the reduction from Non-Disjointness above, there is a reduction from $INDEX_n$ (see Section 5.1) to this problem. Furthermore note that $QNDISJ_{1,1}$ is a somewhat natural real version of the Equality problem.

We don't explicitly consider discretized versions of QNDISJ in this paper. Obviously one can easily encode an approximation of the problem by providing Alice and Bob with a basis of their subspaces rounded to precision $1/poly(n)$.

4 Results

Our results concerning the communication complexity of $QNDISJ_{s,t}$ are collected in the following table. Alice receives the s-dimensional subspace, Bob the t-dimensional subspace, and $s \leq t$. The bounds for QMA, Q, R are tight up to logarithmic factors in the case $s = t = n/4$. Note that unless mentioned, we allow entanglement shared by Alice and Bob for the lower bounds (but don't use entanglement in our protocols).

We now explain the lower bound for QCMA protocols which holds under a certain assumption on the protocols. It is natural to assume that the prover should send information about the intersection to one of the players. The intersection (in the case of a 1-input) is a 1-dimensional subspace, and hence the prover should probably send some information about the (normalized) vector that spans it. A message from the prover would then correspond to a subset of the unit sphere, e.g. could be a spherical cap (or something else).

Our assumption about Merlin's proof is hence that the prover sends messages that correspond to subsets P of the unit sphere. All 1-inputs, where $W_A \cap W_B \in P$ should be accepted on such a proof with high probability.

What this means is that the prover communicates arbitrary information about the intersection, *but nothing more.* One more point is: which sphere? There are 3 possibilities: the sphere in $\mathbb{R}^n$, the sphere in W_A, and the sphere in W_B. Each of these is fine regarding our assumption. Indeed in the case of $s = t = n/4$ this difference does not matter much. For smaller spaces it is more convenient to use the sphere in W_A (assuming that Merlin sends his message to Alice).

We now make the assumption formal. in a QCMA-protocol the prover Merlin sends a classical message (the proof) to Alice, after which Alice and Bob verify the proof, using quantum communication. See Section 5.1 for the definition. We can identify Merlin's proof message with the subset of 1-inputs, which will be accepted with probability at least 2/3 by the verifier(s) when given this proof. So besides the actual message, we also refer to said subset of the 1-inputs as a proof. Hence, with a proof length of p we get a set of at most 2^p proofs that cover the set of 1-inputs. In particular, under any given distribution, the average proof must have measure at least 2^{-p} on the 1-inputs. For QNDISJ, the set of 1-inputs is the intersection manifold $I_{n/4,n/4}$.

A proof that satisfies our assumption also corresponds to a subset of the sphere S^{n-1}.

▶ **Definition 4.** A subset P' of the intersection manifold $I_{n/4,n/4}$ is called *intersectional*, if there is a subset $P \subseteq S^{n-1}$ such that $P' = \{(W_A, W_B) : (W_A, W_B) \in I_{n/4,n/4}$ and $(W_A \cap W_B)$ is spanned by some $z \in P\}$.

▶ **Definition 5.** A QCMA-protocol for a function f satisfies assumption (*), if it is a valid QCMA protocol, and if there is a strategy for Merlin, in which he can convince Alice and Bob to accept with probability at least 2/3 for every 1-input by using intersectional proofs only.

5 Preliminaries

5.1 Communication Complexity

We assume familiarity with the standard modes of communication complexity, and use $R(f)$ to denote the randomized communication complexity (for simplicity we choose public coin randomness), and $Q(f)$ to denote the (entanglement assisted) quantum communication complexity, with error 1/3 in each case. For details we refer to [29].

Proof systems have been introduced into communication complexity in [6], and studied further in e.g. [18, 25, 1, 4, 19, 20, 10, 12]. We now define the main models involving a prover that we use.

▶ **Definition 6.** In a Merlin Arthur protocol a prover (Merlin) sends a string to Alice, who then communicates with Bob. Merlin sees both inputs x, y while Alice sees only x and Bob only y. The goal is to compute a Boolean function $f(x, y)$. Alice and Bob have shared randomness that is invisible to Merlin. Such a protocol is *sound*, if all 0-inputs are accepted with probability at most 1/3 given any message of Merlin, and *complete*, if all 1-inputs are accepted with probability at least 2/3 for some message of Merlin.

The cost of the protocol is the total communication length used, in the worst case, i.e., the total length of the messages sent by Merlin, Alice and Bob. The Merlin Arthur communication complexity of f is the minimum complexity over all sound and complete protocols for f. It is denoted by $MA(f)$.

If we fix the proof length to some parameter p, then it is natural to only count the length of the communication among Alice and Bob. We denote the MA complexity with fixed proof length p by $MA^p(f)$.

It is easy to see that for all $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ we have $MA^n(f) = O(1)$. One can also establish easily by a counting argument that for most such f we have $MA(f) = \Theta(n)$. It is open to prove a larger lower bound than $\Omega(\sqrt{n})$ for any explicit function.

We now turn to quantum versions of this model.

▶ **Definition 7.** In a QCMA protocol Merlin sends a classical message to Alice, while Alice and Bob can communicate using quantum messages and may hold parts of an arbitrary entangled state (not accessible by Merlin). The remaining description is as for MA-protocols. The QCMA-complexity of f is denoted by $QCMA(f)$. If we restrict the length of the proof to p, then we count only the length of the communication between Alice and Bob. The corresponding complexity measure is denoted by $QCMA^p(f)$.

In a QMA protocol Merlin may send a quantum message to Alice. Otherwise the definition is as above. The notations are $QMA(f)$ and $QMA^p(f)$.

Finally, we consider the model where Merlin, Alice, Bob additionally share a classical public coin. Merlin then sends a quantum message to Alice, and Alice and Bob communicate with quantum messages (but have no shared entanglement). This can be called Arthur Quantum Merlin Arthur, because the shared public coin could be seen as a challenge to Merlin. The complexity is denoted $AQMA(f)$.

We define AQMA protocols because we can precisely capture the complexity of $QNDISJ_{s,t}$ in this model (see the full paper, the bound is $\Theta(\log t)$).

Besides the problem $QNDISJ_{s,t}$, and Vector-in-Subspace= $QNDISJ_{1,n/2}$ we also consider the following problems:

▶ **Definition 8.** The disjointness problem $DISJ_{s,t}$, or short DISJ in case $s = t = n/4$, is the problem where Alice gets $x \in \{0,1\}^n$, Bob gets $y \in \{0,1\}^n$, and they should accept if and only if $\vee_i(x_i \wedge y_i) = 0$ (and we have $|x| = s$ and $|y| = t$). The complement of this problem is NDISJ.

In the problem $INDEX_n$ Alice receives $x \in \{0,1\}^n$, Bob receives $i \in [n]$, and the required output is x_i. This is (more or less) equivalent to $NDISJ_{n/2,1}$.

In the problem IP_n Alice and Bob receive $x, y \in \{0,1\}^n$, and the required output is $\bigoplus_i x_i \wedge y_i$.

One of the main techniques of quantum computing is amplitude amplification, a generalization of Grover search [8, 13].

▶ **Fact 9.** *Suppose we are given a quantum protocol that, depending on the input x, y, either accepts with probability δ, or never accepts, with communication c, and hence computes a function $f(x, y)$ with large, but one-sided error.*

Then there is a quantum protocol for f with communication $O(\sqrt{1/\delta} \cdot c)$ and constant (one-sided) error.

▶ **Definition 10.** A *reduction* from a problem $f : X \times Y \to \{0,1\}$ to a problem $g : U \times V \to \{0,1\}$ consists of two mappings $\rho : X \to U$ and $\tau : Y \to V$ such that

$$g(\rho(x), \tau(y)) = f(x, y) \text{ for all } x, y.$$

Clearly, when there is a reduction from f to g, then for every mode of communication complexity g is at least as hard as f, because Alice and Bob can perform arbitrary local computations for free.

Finally, we note that by standard techniques we may assume that all amplitudes in all our quantum protocols are real.

5.2 Spherical Caps

Let S^{n-1} denote the $(n-1)$-dimensional sphere (i.e., the set of unit vectors in $\mathbb{R}^n$). By μ we usually denote the uniform distribution on a manifold, i.e., the Haar measure. A *spherical cap* centered on a unit vector c is the set $C^c_\epsilon = \{w \in S^{n-1} : \langle v, c\rangle \geq \epsilon\}$, where we leave n implicit and $\epsilon \geq 0$. If we care only about the area or measure of a cap, we drop the center c, because the caps are isomorphic to each other.

We are interested in the measure $\mu(C_\epsilon)$. For this we should know the area of both the sphere and a spherical cap. Let A_{n-1} denote the area of S^{n-1}. An explicit formula is $A_{n-1} = \frac{2\pi^{\frac{n}{2}}}{\Gamma(\frac{n}{2})}$. This is maximized (over integers) at $n = 7$. It can be shown that $A_{n-2}/A_{n-1} \geq \frac{\sqrt{n}}{4}$ for all $n \geq 2$.

Next we state upper and lower bounds on the area or measure of a cap C_ϵ in S^{n-1}.

▶ **Lemma 11.** *Let $\epsilon \leq 1/2$.*

1. *The measure $\mu(C_\epsilon)$ is at most $e^{-n\epsilon^2/2}$.*
2. *The area of C_ϵ is at least $A_{n-2}e^{-n\epsilon^2}/(8n\epsilon)$.*
3. *$\mu(C_\epsilon) \geq e^{-n\epsilon^2}/(32\epsilon\sqrt{n})$.*
4. *If $v \in S^{n-1}$ is a fixed vector, and w is randomly drawn from S^{n-1} under μ, then the probability that $\langle v, w\rangle^2 \geq \frac{k}{n}$ is $\leq 2e^{-k/2}$ and $\geq e^{-k}/(16\sqrt{k})$ for all $1 \leq k \leq n/4$.*

5.3 Concentration of Measure

We now consider projecting random unit vectors on larger subspaces. Unsurprisingly, the larger the subspace gets, the better the concentration of measure is. First note, that when a random unit vector from $\mathbb{R}^n$ is projected onto a fixed subspace of dimension t, then the expected squared projection length is t/n. The following bounds can be found in [11].

▶ **Fact 12.** *Let v be a uniformly random vector from S^{n-1}, W a fixed t-dimensional subspace of $\mathbb{R}^n$, and L denote $||Proj_W v||^2$.*

1. *For $0 < \beta < 1 : Prob(L \leq (1-\beta)\frac{t}{n}) \leq e^{-t\beta^2/4}$.*
2. *For $0 < \beta < 1 : Prob(L \geq (1+\beta)\frac{t}{n}) \leq e^{-t\beta^2/8}$.*

We also state a version of the Johnson-Lindenstrauss Theorem, for inner products, see [11].

▶ **Fact 13.** *Let $0 < \epsilon < 0.5$, $n, m > 0$ integers and k such that $k \geq 64/\epsilon^2 \cdot \ln m$. Then for any set $\{v_1, \ldots v_m\} \subseteq \mathbb{R}^n \cap S^{n-1}$ a random projection $g : \mathbb{R}^n \to \mathbb{R}^k$ plus re-normalization (together a mapping f) has the property that for all i, j*

$$\langle v_i|v_j\rangle - \epsilon \leq \langle f(v_i)|f(v_j)\rangle \leq \langle v_i|v_g\rangle + \epsilon.$$

5.4 Sampling by Equators

This is the core technical result from [16].

▶ **Fact 14.** *Let $A \subseteq S^{n-1}$ be a set of measure $\mu(A) \geq 2^{-p}$. Let $v \in S^{n-1}$ be a uniformly random vector from the unit sphere, and $v^{\perp} \subseteq \mathbb{R}^n$ the corresponding uniformly random subspace of dimension $n-1$ orthogonal to v. For any $\frac{p+1}{n} < k < 1$ we have*

$$Prob[|\frac{\mu_{v^{\perp}}(v^{\perp} \cap A)}{2^{-p}} - 1| \geq k] \leq e^{-\gamma nk/(p+1)},$$

where $\gamma > 0$ is a constant, and $\mu_{v^{\perp}}$ is the uniform measure on $S^{n-1} \cap v^{\perp}$.

5.5 Nets on the Sphere

A reasonable short proof of intersection for QNDISJ is the nearest center (to the intersection) of a cap in an ϵ-net consisting of spherical caps on the sphere. For us ϵ (usually the maximum distance between any vector and the nearest cap center) will be much larger than in the standard literature about ϵ-nets, i.e., ϵ will be close to $\sqrt{2}$. Therefore we prefer to simply call a set of vectors such that the union of caps around them covers the sphere a *net*. For the matter of quantum measurements, one can also allow the union of caps and corresponding anti-caps as elements of a net. An anti-cap is simple the set $\{-v : v \in C_{\epsilon}^{c}\}$. Recall that for C_{ϵ} we use the inner product between the cap center and the vectors in the cap as the defining closeness parameter.

▶ **Lemma 15.** *For $1 \leq p \leq n/4$ there is a set M of $20e^{2p}n^2$ vectors such that for every vector $v \in S^{n-1}$ there is a vector $w \in M$ with $\langle v, w\rangle^2 \geq \frac{p}{n}$.*

6 Techniques

Here we briefly sketch the main ideas in the paper.

6.1 QMA

There is a simple protocol with complexity $O(\log n)$: For a 1-input (W_A, W_B) Merlin sends a unit vector in the intersection $W_A \cap W_B$ as a quantum state to Alice. Alice measures this with an observable containing W_A. If the measurement does not yield W_A as the result, she rejects. Otherwise she sends the measured state to Bob, who measures with an observable containing W_B, and accepts iff the result is W_B.

We explore lower bounds, and are able to show a lower bound of $\Omega(\sqrt{\log t})$ via a reduction from the inner product function $IP_{\log t}$ to $QNDISJ_{1,t}$. We can get rid of the square root if we don't allow entanglement between Alice and Bob via a reduction from a random function $f : \{0,1\}^m \times \{0,1\}^m \to \{0,1\}$ for $m = \log t$ together with a proof that $QMA(f)$ is $\Theta(m)$ with high probability.

The $\log t$ upper bound is tight, if we allow a public coin to be shared by Alice, Bob, and Merlin. This holds via dimension reduction with the Johnson-Lindenstrauss Theorem (Fact 13). Without the public coin it remains open whether there is a better upper bound than $\log n$. For very small s, t we can use the randomized protocol (described below) to beat this bound.

6.2 Randomized

For $s = t = n/4$ the complexity is $\widetilde{\Theta}(n)$, with the lower bound inherited from the standard disjointness problem DISJ and the upper bound by Alice sending a uniformly random unit vector $v \in W_A \cap S^{n-1}$ encoded with additive error $1/poly(n)$ for each position. Bob then checks if this vector has projection $\approx 4/n$ or only $1/poly(n)$ onto W_B.

For smaller $s \leq t$ things become interesting. We give a protocol of complexity $O(s\sqrt{t})$ extending the protocol of [24] for the Vector-in-Subspace problem. In that protocol one tries to communicate a vector by using a public coin containing a lot of random unit vectors, and indicating which of them has the largest inner product with the vector one tries to communicate.

The extension is to do this for vectors that have a small overlap with the desired vector only, and to the case of differently sized spaces. This extension is like trying to run the mentioned protocol twice, and a careful analysis is needed using concentration of measure on the sphere and for random projections on subspaces. Basically, Alice has a vector with a given projection onto Bob's space, and tries to communicate the overlap, by pointing out the random vector (in the public coin) that has the best overlap with her vector. For the part of her vector that is in Bob's space to be 'visible' it must be larger than the 'noise', namely the usual deviation of a random vector from its expected projection onto the space. Furthermore it is also important for larger values of s, t to communicate the inner product between her vector and the chosen random vector, because otherwise the noise makes the signal useless. We note that for $s\sqrt{t} \geq n \log n$ our protocol becomes useless.

We also show a lower bound. This builds on the lower bound for the Vector-in-Subspace problem in [16]. The idea is to use a direct sum argument. The conditional external information cost [7] has a direct sum property for the OR of s instances of a problem. It is easy to embed an OR of s instances of $QNDISJ_{1,t/s}$ into one instance of $QNDISJ_{s,t}$. We then extend the result of [16] about $QNDISJ_{1,n/2}$ to conditional external information cost. Originally, this result uses the rectangle/corruption bound. The difficulty is that for the direct sum argument we must lower bound the *conditional* information cost. For this we define a partition (a random subspace V of dimension $n/3$ is drawn, then $W_A \in S^{n-1} \cap V$ and $W_B \subseteq V^{\perp}$ are chosen randomly and independently). We then have to bound the information cost conditioned on V.

Overall we get a lower bond of $\Omega(s(t/s)^{1/3})$. This approach might be improved to $\Omega(\sqrt{st})$ by improving the lower bound for $QNDISJ_{1,t}$.

We note some special cases in the following corollary.

▶ **Corollary 16.**

1. *$R(QNDISJ)$ is between $\Omega(n)$ and $O(n \log n)$.*
2. *$R(QNDISJ_{\sqrt{n},n/2})$ is between $\Omega(n^{2/3})$ and $O(n)$.*
3. *$R(QNDISJ_{\sqrt{n},\sqrt{n}})$ is between $\Omega(n^{1/2})$ and $O(n^{3/4})$.*
4. *$R(QNDISJ_{O(1),O(1)})$ is $\Theta(1)$.*

6.3 Quantum

The upper bound $O(\sqrt{s} \log n)$ is by amplitude amplification (see Fact 9): if Alice sends the uniform superposition over a basis of her space W_A to Bob, who measures with an observable containing W_B as an element, then for 1-inputs the probability of acceptance is $1/s$. Note that for 0-inputs this protocol never accepts.

The lower bound of $\Omega(\sqrt{s})$ is by reduction from the classical disjointness problem DISJ and Razborov's lower bound for the latter [27].

It remains open, whether the log-factor can be shaved off of the upper bound (compare [2]).

The protocol in our upper bound uses many rounds. Round-dependant lower bounds can be derived from the corresponding Disjointness lower bounds, see [9]. In particular, the one-way quantum complexity of $QNDISJ_{s,t}$ (Alice to Bob) is $\Omega(s)$ (by a reduction from $INDEX_s$, see [17]).

▶ **Theorem 17.** *There is a quantum protocol with k rounds (Alice starting) that computes $QNDISJ_{s,t}$ with communication $O(s/k \cdot \log n)$ as long as $k \le \sqrt{s}$. The protocol is optimal up to poly-logarithmic factors.*

Proof. The lower bound is by reduction from Disjointness and the main result in [9]. For the upper bounds we use amplitude amplification on the following protocol: Alice sends s/k^2 copies of the state used in our quantum protocol above. Bob measures those copies, and accepts with probability $1/k^2$. ◀

6.4 QCMA

We give a protocol of complexity $O(s^{1/3} \log n)$ in which Merlin can use caps on the sphere are his proofs. The verification is via amplitude amplification.

Merlin and Alice agree beforehand on a net of spherical caps on the sphere in W_A for all subspaces W_A of dimension s. This net has 2^p centers. On a 1-input (W_A, W_B) Merlin sends Alice the closest center to an intersecting unit vector in $W_A \cap W_B$ from the agreed upon net. Alice and Bob then use the same amplitude amplification protocol as in the prover-less case. Since the cap-center is better than a uniform superposition we get a better upper bound. The reason is that the cap center $|c\rangle$ satisfies $\langle c|x\rangle^2 \ge p/s$ for the intersection $|x\rangle$, whereas a uniform superposition $|u\rangle$ over some ortho-normal basis guarantees only $\langle u|x\rangle^2 \ge 1/s$.

▶ **Theorem 18.**
1. *For all $\log s \le p \le s$: $QCMA^p(QNDISJ_{s,t}) \le O(\sqrt{s/p} \log n)$.*
2. *$QCMA(QNDISJ_{s,t}) \le O(s^{1/3} \log n)$*

We give a conditional lower bound, for protocols with property (*). Such protocols need communication $\Omega(s^{1/3})$. It is enough to show that $QCMA(QNDISJ) = \Omega(n^{1/3})$ by padding.

The idea is that under the condition (*) an (intersectional) proof corresponds to a large subset of the sphere, and we can then, by a new geometrical lemma, find an ortho-normal set of size $\Omega(n/p)$ in any subset of the sphere of measure 2^{-p}. This result can be used to give a reduction from $DISJ_{n/p,n/p}$ to the subfunction of $QNDISJ$ that accepts all 1-inputs in the proof and rejects all 0-inputs.

For this we fix one large, intersectional proof. We then have a quantum protocol that accepts all 1-inputs in the proof, while rejecting all 0-inputs. We find our large ortho-normal set inside the proof, and then embed the classical $DISJ_{n/p,n/p}$ instance. The lower bound follows via the quantum lower bound for $DISJ_{n/p,n/p}$ [27].

This is the geometric lemma mentioned above.

▶ **Lemma 19.** *Let $A \subseteq S^{n-1}$ be a set of measure at least $\mu(A) \ge 2^{-p}$ for $o(\sqrt{n}) \ge p \ge \omega(1)$. Then A contains a set of $\ell = n/(40p)$ vectors $v_1, \dots, v_\ell$ such the x_i form an ortho-normal system (i.e., every v_i is orthogonal to the span of the other vectors).*

The lower bound statement is as follows.

▶ **Theorem 20.** *Under the condition (*)*
1. *$QCMA^p(QNDISJ_{n/4,n/4}) \ge \Omega(\sqrt{n/p})$ for $p \le o(\sqrt{n})$.*
2. *$QCMA(QNDISJ_{s,t}) \ge \Omega(s^{1/3})$.*

6.5 MA

We "Merlinize" our randomized protocol (proofs are still spherical caps as in the QCMA case). The result is an upper bound that is the square root of the randomized upper bound.

▶ **Theorem 21.**
1. *For all* $\log s \leq p \leq s$*:* $MA^p(QNDISJ_{s,t}) \leq O(s\sqrt{t}/p)$.
2. $MA(QNDISJ_{s,t}) \leq O(\sqrt{s\sqrt{t}})$.

Lower bounds for MA-communication complexity can be shown by using the rectangle bound [18]. [16] give such a lower bound, and we get a lower bound that depends polynomially on t. Sadly, no direct sum result is known for the rectangle bound, and our bound is simply a lower bound for $QNDISJ_{1,t}$. We note that the Grassmannian manifold is much harder to handle than the sphere, and so going for an improved rectangle bound heads on seems difficult.

▶ **Fact 22.** $MA(QNDISJ_{1,t}) = \Omega(t^{1/6})$.

It is interesting that this lower bound depends polynomially on the dimension of the *larger* subspace, whereas our QCMA upper bound depends only on the dimension of the smaller subspace.

7 Open Problems

We list a number of interesting open problems.
1. Show an unconditional, large lower bound on $QCMA(QNDISJ)$.
2. Give better bounds for the randomized and MA complexities of $QNDISJ_{s,t}$.
3. Since the randomized and MA protocols we give are one-way protocols, it might be interesting to also get one-way lower bounds.
4. Is $Q(QNDISJ_{s,t}) = O(\sqrt{s})$?
5. Our QMA upper and lower bounds are not close for small dimensional subspaces. For instance we only know that $QMA(QNDISJ_{\log n,\log n})$ is between $\sqrt{\log\log n}$ and $\log n$.
6. Raz and Shpilka [25] show that QMA protocols can be made one-way, but in general only at a polynomial blowup in communication. Can a gap be shown (for instance for Disjointness)?
7. We show that $AQMA(INDEX_n) \geq \Omega(\log n)$. Larger lower bounds for any explicit functions for even AM-complexity are wide open.
8. There is still a gap between the best lower and upper bound known for $QMA(DISJ)$ [20].
9. What is the QMA communication complexity (with entanglement) of a random function?
10. It would be nice if applications of our bounds could be found. Most applications of communication complexity employ Disjointness, so it is quite likely that the 'hidden basis" version of the problem (in particular also the Vector-in-Subspace problem) has interesting applications, e.g. in data-streaming.

References

1 S. Aaronson. Qma/qpoly $\subseteq$ pspace/poly: De-merlinizing quantum protocols. In *Proceedings of 21st IEEE Conference on Computational Complexity*, 2006.

2 S. Aaronson and A. Ambainis. Quantum search of spatial regions. In *Proceedings of 44th IEEE FOCS*, pages 200–209, 2003.

3 S. Aaronson and G. Kuperberg. Quantum versus classical proofs and advice. *Theory of Computing*, 3(1):129–157, 2007.

4 S. Aaronson and A. Wigderson. Algebrization: A New Barrier in Complexity Theory. *ACM Transactions on Computation Theory*, 1(1), 2009.

5 D. Aharonov and T. Naveh. Quantum np - a survey. quant-ph/0210077, 2002.

6 L. Babai, P. Frankl, and J. Simon. Complexity classes in communication complexity theory. In *Proceedings of 27th IEEE FOCS*, pages 337–347, 1986.

7 Z. Bar-Yossef, T. S. Jayram, R. Kumar, and D. Sivakumar. Information theory methods in communication complexity. In *Proceedings of 17th IEEE Conference on Computational Complexity*, pages 93–102, 2002.

8 G. Brassard, P. Høyer, M. Mosca, and A. Tapp. Quantum amplitude amplification and estimation. In *Quantum Computation and Quantum Information: A Millennium Volume*, volume 305 of *AMS Contemporary Mathematics Series*, pages 53–74. AMS, 2002. quant-ph/0005055.

9 M. Braverman, A. Garg, Young K.K., J. Mao, and D. Touchette. Near-optimal bounds on bounded-round quantum communication complexity of disjointness. In *IEEE 56th Annual Symposium on Foundations of Computer Science*, pages 773–791, 2015.

10 A. Chakrabarti, G. Cormode, A. McGregor, J. Thaler, and S. Venkatasubramanian. Verifiable stream computation and arthur-merlin communication. In *30th Conference on Computational Complexity*, pages 217–243, 2015.

11 S. Dasgupta and A. Gupta. An elementary proof of a theorem of johnson and lindenstrauss. *Random Structures & Algorithms*, 22(1):60–65, 2003.

12 M. Göös, T. Pitassi, and T. Watson. Zero-information protocols and unambiguity in arthur-merlin communication. *Algorithmica*, 76(3):684–719, 2016.

13 L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of 28th ACM STOC*, pages 212–219, 1996.

14 B. Kalyanasundaram and G. Schnitger. The probabilistic communication complexity of set intersection. *SIAM Journal on Discrete Mathematics*, 5(4):545–557, 1992. Earlier version in Structures'87.

15 A. Yu. Kitaev. Quantum NP, January 1999. Talk given at AQIP'99, DePaul University, Chicago.

16 B. Klartag and O. Regev. Quantum one-way communication is exponentially stronger than classical communication. In *Proceedings of 43rd ACM STOC*, 2011.

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

18 H. Klauck. Rectangle size bounds and threshold covers in communication complexity. In *18th Annual IEEE Conference on Computational Complexity*, pages 118–134, 2003.

19 H. Klauck. A strong direct product theorem for disjointness. In *Proceedings of the 42nd ACM Symposium on Theory of Computing, STOC*, pages 77–86, 2010.

20 H. Klauck. On arthur merlin games in communication complexity. In *Proceedings of the 26th Annual IEEE Conference on Computational Complexity*, pages 189–199, 2011.

21 H. Klauck and S. Podder. Two Results about Quantum Messages. In *Proceedings of MFCS*, 2014.

22 I. Kremer. Quantum communication. Master's thesis, Hebrew University, Computer Science Department, 1995.

23 E. Kushilevitz and N. Nisan. *Communication Complexity.* Cambridge University Press, 1997.

24 R. Raz. Exponential separation of quantum and classical communication complexity. In *Proceedings of 31st ACM STOC*, pages 358–367, 1999.

25 R. Raz and A. Shpilka. On the power of quantum proofs. In *19th Annual IEEE Conference on Computational Complexity*, pages 260–274, 2004.

26 A. Razborov. On the distributional complexity of disjointness. *Theoretical Computer Science*, 106(2):385–390, 1992.

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

28 A. Sherstov. The pattern matrix method for lower bounds on quantum communication. In *Proceedings of 40th ACM STOC*, pages 85–94, 2008.

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

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