Round Elimination in Exact Communication Complexity

Briët, J.; Buhrman, H.; Leung, D.; Piovesan, T.; Speelman, F.

DOI
10.4230/LIPIcs.TQC.2015.206

Publication date
2015

Document Version
Final published version

Published in
10th Conference on the Theory of Quantum Computation, Communication and Cryptography

Round Elimination in Exact Communication Complexity

Jop Briët[1], Harry Buhrman[2], Debbie Leung[3], Teresa Piovesan[2], and Florian Speelman[2]

1 **Courant Institute**
New York University, 251 Mercer Street, New York NY 10012, USA
jop.briet@cims.nyu.edu
2 **Centrum Wiskunde & Informatica (CWI)**
Science Park 123, 1098 XG Amsterdam, The Netherlands
{buhrman,piovesan,speelman}@cwi.nl
3 **University of Waterloo**
200 University Ave W, Waterloo, Ontario N2L3G1, Canada
wcleung@math.uwaterloo.ca

Abstract

We study two basic graph parameters, the chromatic number and the orthogonal rank, in the context of classical and quantum exact communication complexity. In particular, we consider two types of communication problems that we call *promise equality* and *list* problems. For both of these, it was already known that the one-round classical and one-round quantum complexities are characterized by the chromatic number and orthogonal rank of a certain graph, respectively.

In a promise equality problem, Alice and Bob must decide if their inputs are equal or not. We prove that classical protocols for such problems can always be reduced to one-round protocols with no extra communication. In contrast, we give an explicit instance of a promise problem that exhibits an exponential gap between the one- and two-round exact quantum communication complexities. Whereas the chromatic number thus captures the complete complexity of promise equality problems, the hierarchy of "quantum chromatic numbers" (starting with the orthogonal rank) giving the quantum communication complexity for every fixed number of communication rounds thus turns out to enjoy a much richer structure.

In a list problem, Bob gets a subset of some finite universe, Alice gets an element from Bob's subset, and their goal is for Bob to learn which element Alice was given. The best general lower bound (due to Orlitsky) and upper bound (due to Naor, Orlitsky, and Shor) on the classical communication complexity of such problems differ only by a constant factor. We exhibit an example showing that, somewhat surprisingly, the four-round protocol used in the bound of Naor et al. can in fact be optimal. Finally, we pose a conjecture on the orthogonality rank of a certain graph whose truth would imply an intriguing impossibility of *round elimination* in quantum protocols for list problems, something that works trivially in the classical case.

1998 ACM Subject Classification F.2 Analysis of Algorithms and Problem Complexity

Keywords and phrases Communication complexity, round elimination, quantum communication, protocols, chromatic numbers

Digital Object Identifier 10.4230/LIPIcs.TQC.2015.206

1 Introduction

The chromatic number $\chi(G)$ of a graph G is the minimum number of colors needed to color the vertices in such a way that adjacent vertices get different colors. This important graph

10th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2015).
Editors: Salman Beigi and Robert König; pp. 206–225

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

parameter appears frequently in computer science and mathematics; it is well-known to be NP-hard to compute and has recently found a number of meaningful generalizations in the context of non-local games and entanglement-assisted zero-error information theory. One of those generalizations is the *orthogonal rank* of a graph, denoted $\xi(G)$ and defined as follows. An orthogonal representation of a graph is an assignment of complex unit vectors to the vertices such that adjacent vertices receive orthogonal vectors. The orthogonal rank is the minimum dimension of such a representation. Similar to the chromatic number, the orthogonal rank is NP-hard to compute, which follows from a result of Peeters [29, Theorem 3.1]. In this paper, we study both of these graph parameters in the context of communication complexity.

Classical communication complexity. Since its introduction by Yao [34] communication complexity has become a standard model in computational complexity that enjoys a wide variety of connections to other areas in theoretical computer science [22]. Here two parties, Alice and Bob, receive inputs x, y from sets $\mathcal{X}, \mathcal{Y}$ (resp.) and need to compute the value $f(x, y)$ of a two-variable function f known to them in advance. Usually each party has insufficient information to solve the problem alone, meaning they have to exchange information about each others' inputs. The idea that communication is expensive motivates the study of the *communication complexity* of f, which counts the minimal number of bits that the parties must exchange on worst-case inputs. Throughout this paper, we consider only exact (deterministic) communication protocols, and we will omit the word *exact* from now on. Of particular importance to this paper is the distinction between *one-round* protocols, where all communication flows from Alice to Bob, and *multi-round* protocols, where they take turns in sending messages from one party to the other.

Quantum communication complexity. In yet another celebrated paper, Yao [35] introduced *quantum communication complexity*, where to compute the value $f(x, y)$ the parties are allowed to transmit *qubits* back and forth. The study of this model has also become a well-established discipline in theoretical computer science and quantum information theory. The most basic question that arises when considering the classical and quantum models is whether they are actually substantially different. An upper bound on the possible difference between these models was proved by Kremer [21, Theorem 4].[1]

▶ **Theorem 1.1** (Kremer). *Any quantum protocol that uses ℓ qubits of communication can be turned into a $2^{O(\ell)}$-bit one-round classical protocol for the same problem.*

The first large gap between exact classical and quantum communication complexity was demonstrated by Buhrman, Cleve, and Wigderson [7], who gave a problem admitting a one-round quantum protocol that is exponentially more efficient than any (one- or multi-round) classical protocol.

The chromatic number and orthogonal rank naturally show up in two types of communication problems that we call *promise equality* and *list* problems, discussed next.

1.1 Promise equality

In a *promise equality problem*, Alice and Bob are either given equal inputs or a pair of distinct inputs from a subset $\mathcal{D}$ of $\binom{\mathcal{X}}{2}$ ($\mathcal{D}$ is known to them in advance). Their goal is to decide whether they have equal or different inputs.

[1] The result stated here is actually a slight generalization of Kremer's result (which focuses on boolean functions) that can be proved in the same way; for completeness we give a proof in Appendix A.

Classical complexity of promise problems. It was shown by de Wolf [11, Theorem 8.5.1] that if $G = (\mathcal{X}, \mathcal{D})$ is the graph with vertex set $\mathcal{X}$ and edge set $\mathcal{D}$, then the one-round classical communication of the problem equals $\lceil \log \chi(G) \rceil$. Analogously, for each positive integer r one can define a "level-r" chromatic number of the graph corresponding to the communication complexity of protocols that proceed in r rounds or less. For general communication problems, using more rounds can decrease the total communication, as is the case for the general Pointer Jumping Problem for example, where for every positive integer m there is an instance for which any m-round protocol requires exponentially more communication than the best $(m+1)$-round protocol [22]. However, we show that this is not true for promise equality problems (Lemma 2.1 below), meaning that for such problems the chromatic number not only gives rise to the one-round complexity, but their overall communication complexity.

Quantum complexity of promise problems. The one-round quantum communication complexity of promise equality problems is characterized by the orthogonal rank. It is not difficult to see that a one-round quantum protocol of a promise equality problem is equivalent to an orthogonal representation of the associated graph $G = (\mathcal{X}, \mathcal{D})$; the vectors correspond to the states that Alice would send to Bob and orthogonality is required for Bob's measurement to tell whether they got equal inputs or not. Viewing the orthogonal rank as the "one-round quantum chromatic number" of the graph G naturally leads one to define a hierarchy of such numbers where the level-r quantum chromatic number corresponds to the communication complexity of r-round quantum protocols. One might expect that, as in the classical case, this hierarchy is redundant in that the levels all carry the same number. However, one of our main results shows that in the quantum setting, this is *not* the case.

▶ **Theorem 1.2.** *There exist absolute constants $c, C \in (0, \infty)$ and an infinite family of promise equality problems $(\mathcal{X}_n, \mathcal{D}_n)_{n \in \mathbb{N}}$ such that:*

- *The one-round quantum communication complexity of $(\mathcal{X}_n, \mathcal{D}_n)$ is at least cn.*
- *There is a two-round quantum protocol for $(\mathcal{X}_n, \mathcal{D}_n)$ using at most $C \log n$ qubits.*

During our analysis of the particular promise problem used for Theorem 1.2 we answer an open question of Gruska, Qiu, and Zheng [18]. To explain this, we briefly elaborate on what goes into our result. The problem we consider is simple: Let n be a positive integer multiple of 8. Alice and Bob are given n-bit strings x and y, respectively, that are either equal or differ in exactly $n/4$ coordinates and they must distinguish between the two cases. We denote this problem by EQ-$\binom{n}{n/4}$. Similar promise equality problems were studied before. Buhrman, Cleve, and Wigderson [7] showed the first exponential gap between classical and quantum communication with the problem EQ-$\binom{n}{n/2}$, where Alice and Bob get n-bit strings that are either equal or differ in exactly half of the entries (for n a multiple of 4). They used a distributed version of the Deutsch–Jozsa algorithm to give a one-round $O(\log n)$-qubit quantum protocol for this problem, while a celebrated graph-theoretic result of Frankl and Rödl [14] implies that the classical communication complexity is at least $\Omega(n)$. Similar results were shown (based on similar techniques) in the above-mentioned paper [18] for the analogous problem EQ-$\binom{n}{\alpha n}$ when $\alpha > 1/2$, and the authors pose as an open problem to determine the quantum communication complexity of EQ-$\binom{n}{\alpha n}$ when $\alpha < 1/2$.

We show that the one-round quantum communication complexity of EQ-$\binom{n}{n/4}$ is at least $\Omega(n)$ and we give a two-round protocol for it that uses at most $O(\log n)$ qubits. For the proof of the first bound we use the famous Lovász theta number, which lower bounds the orthogonal rank and therefore the one-round quantum communication complexity. We prove a lower bound on the theta number using the theory of association schemes and known

properties of the roots of the Krawtchouk polynomials. Our two-round protocol is based on a distributed version of Grover's algorithm. With a little extra technical work our results can be extended to any of the problems EQ-$\binom{n}{\alpha n}$ with constant $\alpha < 1/2$. In light of Kremer's Theorem and the obvious fact that the one-round classical communication complexity is at least its quantum counterpart, we thus settle the question of [18].

1.2 The list problem

In the *list problem*, inputs are picked from a subset $\mathcal{D} \subseteq \mathcal{X} \times \mathcal{Y}$ and the parties' goal is for Bob to learn Alice's input. The reason for the name "list problem" is that Bob's input y may just as well be given to him as the list (subset) of all of Alice's possible inputs x satisfying $(x, y) \in \mathcal{D}$. A list problem can thus equivalently be given by a family $\mathcal{L} \subseteq 2^{\mathcal{X}}$ of lists, where Bob gets a list $L \in \mathcal{L}$, Alice gets an element $x \in L$, and Bob must learn x. We refer to this communication problem as $\mathcal{L}$-LIST.

Classical complexity of list problems. Witsenhausen [33] observed that the one-round classical communication complexity of the list problem is characterized by the chromatic number of the graph with vertex set $\mathcal{X}$ and whose edge set consists of the pairs of distinct elements appearing together in some list $L \in \mathcal{L}$. Denoting this graph by $G_{\mathcal{L}}$, the one-round communication complexity equals $\lceil \log \chi(G_{\mathcal{L}}) \rceil$. The multi-round communication complexity of the list problem was also studied before. Orlitsky [28, Corollary 3 and Lemma 3] proved the following lower bound in terms of the chromatic number of $G_{\mathcal{L}}$, and the cardinality of the largest list, denoted $\omega(\mathcal{L}) = \max\{|L| : L \in \mathcal{L}\}$ (not to be confused with the cardinality of the largest clique $\omega(G_{\mathcal{L}})$ in the graph $G_{\mathcal{L}}$, which can be larger).

▶ **Theorem 1.3** (Orlitsky). *For every family $\mathcal{L} \subseteq 2^{\mathcal{X}}$, the classical communication complexity of $\mathcal{L}$-LIST is at least* $\max\{\log\log \chi(G_{\mathcal{L}}), \log \omega(\mathcal{L})\}$.

The basic idea behind the above result is that Alice must send sufficient information for Bob to be able to distinguish among $\omega(\mathcal{L})$ elements, and that any multi-round protocol can be simulated by a one-round protocol with at most an exponential difference in communication. In the same work, Orlitsky [28, Theorem 4] gave a two-round classical protocol based on perfect hashing functions that nearly achieves the above lower bound.

▶ **Theorem 1.4** (Orlitsky). *For every family $\mathcal{L} \subseteq 2^{\mathcal{X}}$, the two-round classical communication complexity of $\mathcal{L}$-LIST is at most* $\log\log \chi(G_{\mathcal{L}}) + 3\log \omega(\mathcal{L}) + 4$.

It thus follows from Witsenhausen's observation and Theorem 1.4 that list problems have exponentially more efficient two-round protocols than one-round protocols. But Theorem 1.3 shows that—in stark contrast with the Pointer Jumping Problem—using more than two rounds cannot decrease the total amount of communication by more than a factor of 4, since obviously $\log\log \chi(G_{\mathcal{L}}) + 3\log \omega(\mathcal{L}) \leq 4\max\{\log\log \chi(G_{\mathcal{L}}), \log \omega(\mathcal{L})\}$. The natural question that thus arises is if the lower bound of Theorem 1.3 can be attained by using more than two rounds of communication. Towards answering this question, Naor, Orlitsky, and Shor [27, Corollary 1] slightly improved on Theorem 1.4 and showed that the four-round communication complexity gets to within a factor of about 3 of the lower bound.

▶ **Theorem 1.5** (Naor–Orlitsky–Shor). *For every family $\mathcal{L} \subseteq 2^{\mathcal{X}}$, the four-round classical communication complexity of $\mathcal{L}$-LIST is at most* $\log\log \chi(G_{\mathcal{L}}) + 2\log \omega(\mathcal{L}) + 3\log\log \omega(\mathcal{L}) + 7$.

As our contribution to this line of work we show that, surprisingly, for some list problems the four-round protocol of Naor, Orlitsky, and Shor is in fact asymptotically optimal, thus answering the above question in the negative.

▶ **Theorem 1.6.** *For any $\varepsilon > 0$ there exists a set $\mathcal{X}$ and a family $\mathcal{L} \subseteq 2^{\mathcal{X}}$ such that the classical communication complexity of $\mathcal{L}$-LIST is at least $\log\log\chi(G_{\mathcal{L}}) + (2-\varepsilon)\log\omega(\mathcal{L})$. Moreover, there exists such an $(\mathcal{X}, \mathcal{L})$ pair for which $\omega(\mathcal{L}) = \log\chi(G_{\mathcal{L}})$.*

In particular, our result gives a family of list problems with communication complexity at least $(3-\varepsilon)\max\{\log\log\chi(G_{\mathcal{L}}), \log\omega(\mathcal{L})\}$ for any $\varepsilon > 0$.

Quantum complexity of list problems and quantum round elimination. The one-round quantum communication complexity of list problems is given by $\lceil\log\xi(G_{\mathcal{L}})\rceil$, which follows from the same considerations as for the promise equality problems (see Lemma 3.4). Based on a conjecture we make about the orthogonal rank of a certain family of graphs, we believe that in the context of quantum communication complexity, list problems may have the interesting property of resisting a quantum analogue of *round elimination*.

In classical communication complexity, round elimination reduces the number of rounds of a given protocol by having the parties send some extra information instead. Consider the following basic example, where we start with a two-round $(\log n + 1)$-bit protocol in which Bob starts by sending Alice a single bit and Alice replies with an $\log n$-bit string. This protocol can easily be turned into a *one-round* $2\log n$-bit protocol by having Alice directly send Bob two $\log n$-bit strings, one corresponding to the case where Bob sends a 0 in the two-round protocol and another for if he sends a 1. Then Bob can just pick the string corresponding to the bit he would have sent based on his input and solve the problem.

A quantum analogue of the above example would turn a two-round $(\log n + 1)$-qubit protocol into a one-round $2\log n$-qubit protocol. We conjecture that the following family of list problems is a counterexample to the existence of such an analogue. For an even positive integer n and $d \in [n]$, let $\mathcal{L}_d \subseteq 2^{\{0,1\}^n}$ be the family of all lists $L \subseteq \{0,1\}^n$ of maximal cardinality such that all strings in L have Hamming distance exactly d. The example we consider is given by the family $\mathcal{K} = \mathcal{L}_{n/2} \cup \cdots \cup \mathcal{L}_n$. Similar to the classical example above, we give a simple two-round protocol for $\mathcal{K}$-LIST.

▶ **Theorem 1.7.** *For $\mathcal{K} \subseteq 2^{\{0,1\}^n}$ as above, there exists a two-round protocol for $\mathcal{K}$-LIST where Bob sends Alice a single qubit and Alice replies with a $(1+\log n)$-qubit message.*

It is easy to see that the graph $G_{\mathcal{K}} = (\{0,1\}^n, E)$ associated with $\mathcal{K}$ has edge set E given by all pairs of strings with Hamming distance in $\{n/2, \ldots, n\}$.

▶ **Conjecture 1.8.** *The graph $G_{\mathcal{K}}$ as above satisfies $\xi(G_{\mathcal{K}}) \geq n^{\omega(1)}$.*

By the relation between the one-round quantum communication complexity of list problems and the orthogonal rank of their associated graphs, it follows that the validity of the above conjecture would imply that the exact one-round quantum communication complexity of the above problem is super-logarithmic in n, in marked contrast with the classical example of round elimination.

1.3 Connections to other work

Our work strengthens a link between communication complexity and graph theory established by de Wolf [11]. Orthogonal representations appear in the context of zero-error information theory. Indeed they were introduced by Lovász [26] to settle a famous problem of Shannon concerning the (classical) capacity of the 5-cycle and they serve as proxies for entanglement-assisted schemes [8, 9, 24, 5, 6, 10]. They also appear in the context of non-local games [8, 16, 31]. Nevertheless the orthogonal rank is poorly understood. To the best of our knowledge,

our result is the first time a *lower bound* on the dimension was used. The use of the Lovász theta number in the context of communication complexity problems also appears to be new and we hope that it may find further applications there in the future. Finally, quantum variants of the chromatic number that appeared in for example non-local games [8, 31] and zero-error information theory [6, 10] can be interpreted as quantum communication complexities of promise equality problems in various different communication models, which puts those parameters in a more unified framework.

Outline of the paper. In Section 2 we study the promise equality problem and in particular we prove Theorem 1.2. In Section 3 we discuss the list problem and prove Theorem 1.6 and Theorem 1.7.

2 Promise Equality

Recall that in a promise equality problem, Alice and Bob each receive an input from a set $\mathcal{X}$ with the promise that their inputs either are equal or come from a subset $\mathcal{D}$ of $\binom{\mathcal{X}}{2}$ (known to the players beforehand). The goal is to distinguish between the two cases. To any promise equality problem, we associate the graph $G = (\mathcal{X}, \mathcal{D})$.

2.1 General properties of promise equality

Recall that the one-round classical communication complexity of the problem equals $\lceil \log \chi(G) \rceil$. We begin by proving that the chromatic number of the associated graph actually gives the overall communication complexity.

▶ **Lemma 2.1.** *For any promise equality problem, the classical communication complexity is attained with a single round of communication.*

Proof. We show how to transform a k-round communication protocol into a one-round protocol that uses the same amount of bits. To summarize, the idea is that Alice mimics all the rounds of communication assuming that her input is equal to Bob's one, and sends them in one-round. He then checks whether the message received is consistent with his input. If this is not the case, then he knows that the two strings are different, otherwise he completes the protocol.

More formally, fix an optimal protocol P that requires k rounds, where $k \geq 2$. Suppose that Alice has input x and Bob has y. We assume that the first round of communication is from Alice to Bob, but the same reasoning applies in the other case. For i odd, let a_i be the message that Alice would send to Bob on the i-th round of communication if she followed protocol P and used the knowledge of the messages exchanged in the previous rounds and of her input x. Similarly, for i even, let $\hat{b}_i$ be the message that Bob would send to Alice on the i-th round of communication if he had $y = x$ as input, followed the protocol P and used the knowledge derived by the previous rounds. Using the protocol P, Alice can mimic Bob's rounds of communication under the assumption that Bob's input is equal to x. Alice uses her input x to produce the string $a_1\hat{b}_2a_3 \dots a_i\hat{b}_{i+1} \dots a_k$ and sends it to Bob in one round. From his input y, Bob constructs the messages b_i that he would have produced during the protocol P, with the knowledge of Alice's messages a_ℓ and his messages b_ℓ for all $\ell < i$. If there exists an index i such that $b_i \neq \hat{b}_i$, then x must be different from y. Otherwise, Bob uses the transcript $a_1\hat{b}_2a_3 \dots a_i\hat{b}_{i+1} \dots a_k$ to finish the protocol and either outputs $x = y$ or $x \neq y$. We have constructed a one-round communication protocol $\hat{P}$ whose worst-case

transcript length is at most as long as the one of the original protocol P. Since P is an optimal protocol so must be $\hat{P}$. ◀

As already mentioned, de Wolf [11, Theorem 8.5.2] showed that one-round quantum protocols are related to orthogonal representations. We include a proof here for completeness.

▶ **Theorem 2.2** (de Wolf). *Consider a promise equality problem defined by the sets $\mathcal{X}$ and $\mathcal{D}$, then its one-round quantum communication complexity is equal to $\lceil \log \xi(G) \rceil$, where $G = (\mathcal{X}, \mathcal{D})$.*

The proof of the above result uses the following standard lemma (see for example [6]).

▶ **Lemma 2.3** (Orthogonality Lemma). *Let $\rho_1, \ldots, \rho_\ell \in \mathbb{C}^{d \times d}$ be a collection of Hermitian positive semidefinite matrices. Then the following are equivalent:*

1. *We have $\rho_i \rho_j = 0$ for every $i \neq j \in [\ell]$.*
2. *There exists a measurement consisting of positive semidefinite matrices $P^1, \ldots, P^\ell$, $P^\perp \in \mathbb{C}^{d \times d}$ such that $\mathsf{Tr}(P^i \rho_j) = \delta_{ij} \mathsf{Tr}(\rho_j)$ and $\mathsf{Tr}(P^\perp \rho_j) = 0$ for every $i, j \in [\ell]$.*

In particular, a collection of pure states $|\phi_1\rangle, \ldots, |\phi_\ell\rangle \in \mathbb{C}^d$ can be perfectly distinguished with a quantum measurement if and only if they are pairwise orthogonal.

Proof of Theorem 2.2. Let P be an optimal one-round protocol for the considered promise equality problem. Without loss of generality, Alice sends pure state $|\phi_x\rangle \in \mathbb{C}^d$ on input $x \in \mathcal{X}$. For any pair $(x, y) \in \mathcal{D}$, $|\phi_x\rangle$ and $|\phi_y\rangle$ have to be perfectly distinguishable and therefore, in view of Lemma 2.3, they must be orthogonal. Hence, the map $\phi : \mathcal{X} \to \mathbb{C}^d$ where $\phi(x) = |\phi_x\rangle$ is a d-dimensional orthonormal representation of $G = (\mathcal{X}, \mathcal{D})$ and $\xi(G) \leq d$.

On the other hand, let ϕ be a d-dimensional orthonormal representation of the graph $G = (\mathcal{X}, \mathcal{D})$ and consider the one-round quantum protocol that transmits $\phi(x) \in \mathbb{C}^d$ on input $x \in \mathcal{X}$. This uses $\log d$-qubits of communication. From Lemma 2.3 we know that Bob can use his input y to perform a quantum measurement that allows him to learn whether his input is equal or not to Alice's one. Thus, the one-round quantum communication complexity of this equality problem is at most $\lceil \log \xi(G) \rceil$. ◀

2.2 Proof of Theorem 1.2

The rest of this section will be devoted to the proof of Theorem 1.2, which shows that there is a family of promise equality problems where allowing two rounds of quantum communication is exponentially more efficient than a single round. The problem that exhibits this separation is EQ-$\binom{n}{n/4}$, where Alice and Bob each receive a n-bit string that are either equal or differ in exactly $n/4$ positions (with n multiple of 8). We denote by $H(n, n/4)$ the graph associated with this problem. For any $n, d \in \mathbb{N}$, let $H(n, d)$ be the graph which has all the n-bit strings as vertex set, such that two vertices are adjacent if their Hamming distance is d. We split the proof in two parts: in Section 2.2.1 we bound the one-round quantum communication complexity and in Section 2.2.2 we give the two-round protocol.

2.2.1 One-round quantum communication complexity of EQ-$\binom{n}{n/4}$

The main result of this section is the following theorem.

▶ **Theorem 2.4.** *The one-round quantum communication complexity of* EQ-$\binom{n}{n/4}$ *is at least $\Omega(n)$.*

To prove Theorem 2.4, we use Theorem 2.2 and thus set out to bound the orthogonal rank of the graph $H(n, n/4)$. We prove the desired bound in three steps: first, we show that the Lovász theta number is a lower bound for the orthogonal rank; second, we use structural properties of $H(n, n/4)$ together with known properties of the theta number to reformulate this bound in terms of the eigenvalues of the adjacency matrix of this graph; third, we bound the eigenvalues to get the desired result.

We remark that in the following proofs we consider a more general situation than just the graph $H(n, n/4)$. Indeed, the statement of Theorem 2.4 holds for any problem EQ-$\binom{n}{\alpha n}$ where $\alpha \in (0, 1/2)$ and where both n and $\alpha \cdot n$ are even.

Step 1: The Lovász theta number. This parameter was introduced by Lovász [26] to upper bound the Shannon capacity of a graph. Among its many equivalent definitions, we will use the following primal and dual formulations:

$$\begin{aligned} \vartheta(G) &= \max \sum_{i,j \in V(G)} X_{ij} \quad \text{s.t.} \quad X \succeq 0, \quad \mathsf{Tr}(X) = 1, \quad X_{ij} = 0 \quad \forall ij \in E(G), \\ \vartheta(G) &= \min t \quad \text{s.t.} \quad X \succeq 0, \quad X_{ii} = t - 1 \quad \forall i \in V(G), \quad X_{ij} = -1 \quad \forall ij \in E(\overline{G}), \end{aligned} \tag{1}$$

where $X \succeq 0$ means that X is a symmetric positive semidefinite matrix. The graph $\overline{G}$, called the complement of a graph G, has the same vertex set as the original graph and a pair of vertices is adjacent if and only if it is non adjacent in G.

Lovász [26] proved that ϑ lower bounds the minimum dimension of an orthonormal representation where the vectors are real valued. Note that this is slightly different from our setting where we allow the vectors to have complex entries. However, we show that the Lovász theta number is also a lower bound for $\xi(G)$. The proof is an adaptation to the complex case of a known proof [23].

▶ **Lemma 2.5.** *For any graph G, we have $\xi(G) \geq \vartheta(\overline{G})$.*

Proof. Let $n = |V(G)|$ and label the vertices of the graph G by $\{1, 2, \ldots, n\}$. Suppose that the orthogonal rank of G is equal to d and that $u_1, \ldots, u_n \in \mathbb{C}^d$ are the unit vectors forming an orthogonal representation of G. For every vertex of the graph $i \in [n]$, define a matrix $U_i := u_i u_i^\dagger$ and $U_0 := I_d$. Let Z be a $(n+1) \times (n+1)$ matrix where the i, j-th entry $Z_{ij} := \langle U_i, U_j \rangle = \mathsf{Tr}(U_j^\dagger U_i)$ for every $i, j \in \{0\} \cup [n]$. Notice that Z is positive semidefinite since it is the Gram matrix of a set of complex vectors. Moreover, Z is real valued and we get that $Z_{00} = d$, $Z_{0i} = \langle I, u_i u_i^\dagger \rangle = 1$ and $Z_{ii} = \langle u_i u_i^\dagger, u_i u_i^\dagger \rangle = (u_i^\dagger u_i)^2 = 1$ for all $i \in V(G)$ and that $Z_{ij} = (u_i^\dagger u_j)(u_j^\dagger u_i) \geq 0$ for all $i, j \in V(G)$ with equality if $ij \in E(G)$. By taking the Schur complement[2] in Z with respect to the entry Z_{00}, we obtain a new symmetric positive semidefinite matrix X with $X_{ii} = 1 - 1/d$ for all $i \in V(G)$ and $X_{ij} = -1/d$ for all $ij \in E(G)$. Rescaling X by d, we get a feasible solution for the minimization program in (1) of $\vartheta(\overline{G})$ with value d. We conclude that $d = \xi(G) \geq \vartheta(\overline{G})$. ◀

Step 2: Eigenvalue bound on the theta number. In the second step we show the following useful bound on the theta number of the graph $H(n, d)$ in terms of the eigenvalues of its

[2] Let X be a symmetric matrix of the form $X = \left(\begin{smallmatrix} \alpha & b^T \\ b & A \end{smallmatrix}\right)$, where $b \in \mathbb{R}^{n-1}$ and $\alpha > 0$. X is positive semidefinite if and only if $A - bb^T/\alpha$ is positive semidefinite. The matrix $A - bb^T/\alpha$ is called the Schur complement in X with respect to the entry α.

adjacency matrix. For the remainder of this step, by the eigenvalues of a graph we mean the eigenvalues of its adjacency matrix.

▶ **Lemma 2.6.** *For every positive integer n and $d \in [n]$, we have $\vartheta(\overline{H(n,d)}) \geq 1 - \binom{n}{d}/\lambda_{\text{MIN}}$, where λ_{MIN} is the smallest eigenvalue of $H(n,d)$.*

The proof of the above lemma uses the fact that for graphs with certain structural properties, the Lovász theta number is characterized by their eigenvalues. Let us recall the following standard definitions. Let $G = (V, E)$ be a graph. A permutation $\pi : V \to V$ is *edge preserving* if for every edge $\{u, v\} \in E$, we have $\{\pi(u), \pi(v)\} \in E$. The graph G is *vertex-transitive* if for every pair of vertices $u, v \in V$ there is an edge-preserving permutation $\pi : V \to V$ such that $\pi(u) = v$. Moreover, G is *edge-transitive* if for every pair of edges $\{u_1, v_1\}, \{u_2, v_2\} \in E$, there is an edge-preserving permutation $\pi : V \to V$ such that $\pi(u_1) = u_2$ and $\pi(v_1) = v_2$. Lovász [26] showed that if a graph is both vertex- and edge-transitive, then the theta number is given by a simple formula involving its eigenvalues.

▶ **Lemma 2.7** (Lovász)**.** *For a positive integer n let G be an n-vertex graph with eigenvalues $\lambda_1 \geq \cdots \geq \lambda_n$. If G is both vertex- and edge-transitive, then $\vartheta(\overline{G}) = 1 - \lambda_1/\lambda_n$.*

Proof of Lemma 2.6. We start by showing that $H(n,d)$ is vertex-transitive. Given any pair of vertices $u, v \in \{0,1\}^n$ of $H(n,d)$, consider the automorphism of the graph $H(n,d)$ that maps $x \mapsto x \oplus u \oplus v$ where $\oplus$ is the bit-wise addition. This map preserves the Hamming distance, and therefore the adjacencies, between the vertices and sends $u \mapsto v$. Hence $H(n,d)$ is vertex-transitive.

To show that $H(n,d)$ is edge-transitive, fix any two edges uv and st and let $p = u \oplus v$, $q = s \oplus t$. Noting that the n-bit strings p and q have the same Hamming weight d, let π be a permutation of the indices such that $\pi(p) = q$. We define ν to be an automorphism that sends a vertex x to $\pi(x \oplus u) \oplus s$. The map ν preserves the edges of $H(n,d)$ and, since the permutation π maps the all-zero string to itself and p to q, we have that $\nu(u) = s$ and $\nu(v) = t$. Hence, $H(n,d)$ is edge-transitive.

Finally, since the largest eigenvalue of a vertex-transitive graph is equal to its degree, we clearly have $\lambda_1(H(n,d)) = \binom{n}{d}$. The result now follows from Lemma 2.7. ◀

Step 3: Bound on the smallest eigenvalue of $H(n,d)$. Finally, we prove an upper bound on the magnitude of the smallest eigenvalue of $H(n,d)$.

▶ **Lemma 2.8.** *Let d and n be even positive integers such that $d < n/2$. Then, the smallest eigenvalue λ_{MIN} of the graph $H(n,d)$ is a negative number such that*

$$|\lambda_{\text{MIN}}| \leq \sqrt{\frac{2^n \binom{n}{d}}{\binom{n}{n/2-\sqrt{d(n-d)}}}}.$$

The proof of the lemma uses the following facts from coding theory that can be found in the survey [12]. The eigenvalues of $H(n,d)$ play a fundamental role in the theory of Hamming association schemes, where they are expressed in terms of a set of orthogonal polynomials known as the (binary) *Krawtchouk polynomials*. For a positive integer n and $d = 0, 1, \ldots, n$, the Krawtchouk polynomial $K_d^n \in \mathbb{R}[x]$ is a degree-d polynomial that is uniquely defined by

$$K_d^n(x) = \sum_{j=0}^{d} (-1)^j \binom{x}{j}\binom{n-x}{d-j}, \qquad x = 0, 1, \ldots, n.$$

When n and d are even, then K_d^n is symmetric about the point $x = n/2$. Moreover, these polynomials satisfy the important orthogonality relation

$$\sum_{x=0}^{n} \binom{n}{x} K_d^n(x) K_{d'}^n(x) = \delta_{d,d'} \binom{n}{d} 2^n. \tag{2}$$

The set of distinct eigenvalues of $H(n,d)$ turns out to be $\{K_d^n(0), K_d^n(1), \ldots, K_d^n(n)\}$. Crucial to our proof of Lemma 2.8 then, is the following result of Levenshtein [25, Theorem 6.1] characterizing the smallest roots of the Krawtchouk polynomials.

▶ **Theorem 2.9** (Levenshtein). *Let n be a positive integer and $d \in [n]$. Then, K_d^n has exactly d distinct roots and its smallest root is given by*

$$n/2 - \max_z \Big(\sum_{i=0}^{d-2} z_i z_{i+1} \sqrt{(i+1)(n-i)} \Big), \tag{3}$$

where the maximum is over all vectors $z = (z_0, \ldots, z_{d-1})$ on the real Euclidean unit sphere.

This implies the following general bound on the location of the smallest root of K_d^n. The bound is stated for instance in [20], but since we were unable to find a published proof we include one here for completeness.

▶ **Corollary 2.10.** *Let n and d be positive integers such that $d < n/2$. Then, the smallest root of K_d^n lies in the interval $\big[n/2 - \sqrt{(n-d)d}, n/2\big]$.*

Proof. It is clear that (3) is trivially upper bounded by $n/2$. We focus on the lower bound. To this end, let $z = (z_0, \ldots, z_{d-1})$ be a real unit vector achieving the maximum in (3). For $i \in \{0, 1, \ldots, d-1\}$ define the numbers $a_i = z_i \sqrt{n-i}$ and $b_i = z_{i+1}\sqrt{i+1}$. By the Cauchy-Schwarz inequality,

$$\begin{aligned}
\Big(\sum_{i=0}^{d-2} z_i z_{i+1} \sqrt{(i+1)(n-i)} \Big)^2 &= \Big(\sum_{i=0}^{d-2} a_i b_i \Big)^2 \\
&\le \Big(\sum_{i=0}^{d-2} a_i^2 \Big) \Big(\sum_{j=0}^{d-2} b_j^2 \Big) \\
&= \Big(\sum_{i=0}^{d-2} a_i^2 \Big) \Big(\sum_{j=1}^{d-1} b_{j-1}^2 \Big) \\
&\le \Big(\sum_{i=0}^{d-1} a_i^2 \Big) \Big(\sum_{j=0}^{d-1} b_{j-1}^2 \Big) \\
&= \Big(\sum_{i=0}^{d-1} z_i^2 (n-i) \Big) \Big(\sum_{j=0}^{d-1} z_j^2 j \Big) \\
&= \Big(n - \sum_{i=0}^{d-1} z_i^2 i \Big) \Big(\sum_{j=0}^{d-1} z_j^2 j \Big),
\end{aligned} \tag{4}$$

where in the last equality we used the fact that z is a unit vector. Observe that the sum $\sum_{i=0}^{d-1} z_i^2 i$ lies in the interval $[0, d-1]$. Hence, since $d < n/2$, (4) is at most $\max\{(n-t)t : t \in [0, d-1]\} = (n-(d-1))(d-1) \le (n-d)d$. ◀

Proof of Lemma 2.8. Since the trace of a matrix equals the sum of its eigenvalues and the trace of an adjacency matrix is zero, it follows that $\lambda_{\text{MIN}} < 0$.

Recall that the eigenvalues of $H(n,d)$ belong to the set $\{K_d^n(x) : x = 0,1,\dots,n\}$. Moreover, since by our assumption n and d are even, the polynomial K_d^n is symmetric about the point $n/2$. Also observe that $K_d^n(0) > 0$ and hence the first time this polynomial assumes a negative value is somewhere beyond its smallest root, i.e. the smallest x for which $K_d^n(x) < 0$ lies in between the smallest root and $n/2$. It therefore follows from Corollary 2.10 and from the fact that K_d^n is symmetric about the point $n/2$ that $\lambda_{\text{MIN}} = K_d^n(x^\star)$ for some integer $x^\star \in [n/2 - \sqrt{(n-d)d}, n/2]$.

Clearly (2) implies that

$$\sum_{x=0}^{n} \binom{n}{x} K_d^n(x)^2 = \binom{n}{d} 2^n.$$

Hence,

$$\binom{n}{x^\star} K_d^n(x^\star)^2 \le \binom{n}{d} 2^n$$

and we can conclude that

$$|\lambda_{\text{MIN}}|^2 = |K_d^n(x^\star)|^2 \le \frac{2^n \binom{n}{d}}{\binom{n}{x^\star}} \le \frac{2^n \binom{n}{d}}{\binom{n}{n/2-\sqrt{(n-d)d}}}. \qquad \blacktriangleleft$$

Putting everything together. To conclude this section, we combine the main lemmas of the above three steps to prove Theorem 2.4.

Proof of Theorem 2.4. Combining Lemmas 2.5, 2.6, and 2.8 gives

$$\xi(H(n,d)) \ge \vartheta\big(\overline{H(n,d)}\big) \ge 1 - \binom{n}{d}/\lambda_{\text{MIN}} \ge 1 + \sqrt{\frac{\binom{n}{d}\binom{n}{n/2-\sqrt{(n-d)d}}}{2^n}}. \tag{5}$$

We take the logarithm and use Stirling's approximation: $\log \binom{n}{k} = \big(H(k/n) + o(1)\big)n$, where $H(\epsilon) = -\epsilon \log(\epsilon) - (1-\epsilon)\log(1-\epsilon)$ is the binary entropy function and the $o(1)$ term goes to zero as $n \to \infty$ (see for example [32, p. 64]). Then, for $\alpha = d/n$, logarithm of (5) is at least

$$\frac{1}{2} \log \left(\frac{\binom{n}{d}\binom{n}{n/2-\sqrt{(n-d)d}}}{2^n} \right) = \frac{n}{2} \left(H(\alpha) + H\left(1/2 - \sqrt{(1-\alpha)\alpha}\right) - 1 + o(1) \right).$$

A simple check gives that $H(\alpha) + H(1/2 - \sqrt{(1-\alpha)\alpha}) - 1 > 0$ for any $\alpha \in (0, 1/2)$. In particular, $\log \xi(H(n,n/4)) \ge \Omega(n)$. $\blacktriangleleft$

2.2.2 Two-round quantum communication

Using a distributed version of Grover's search algorithm, we find a quantum communication protocol that solves EQ-$\binom{n}{n/4}$ with a logarithmic number of qubits.

▶ **Theorem 2.11.** *The two-round quantum communication complexity of* EQ-$\binom{n}{n/4}$ *is at most* $2\lceil \log n \rceil + 1$ *qubits.*

Proof. Let x and y be the inputs of Alice and Bob, respectively, and $z = x \oplus y$ be their bit-wise addition. The promise ensures that either $|z| = 0$ if $x = y$ or $|z| = n/4$ in the case where $x \neq y$.

If a bit string $z \in \{0,1\}^n$ is known to contain exactly $n/4$ entries that are 1, Grover's algorithm [17] is able to find one of these entries without error [2], needing only a single query to the string z. For any string we define the query unitary $U_z = \sum_{i=1}^n (-1)^{z_i} |i\rangle\langle i|$ and we define $|s\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^n |i\rangle$ to be the uniform superposition of all basis states. Then $G = 2|s\rangle\langle s| - I$ is a unitary operation known as the Grover diffusion operator.

The quantum communication protocol can be viewed as combining Grover's algorithm with a special case of the simulation theorem given by Buhrman, Cleve and Wigderson [7, Theorem 2.1]. We want to perform the algorithm on the effective string $z = x \oplus y$, using the fact that performing a single query U_z is the same as performing the operations U_x and U_y in sequence, i.e., $U_z = U_x U_y = U_y U_x$.

At the start of the protocol, Bob first creates the state $U_y|s\rangle$ and sends this state over to Alice using $\lceil \log n \rceil$ qubits. Alice first applies U_x to the incoming state and then applies the Grover operator G. The final state of Grover's algorithm is $\frac{1}{\sqrt{n/4}} \sum_{i \text{ s.t. } z_i = 1} |i\rangle$ if $|z| = n/4$. That is, in the case that $x \neq y$ Grover's algorithm has produced a superposition over all indices i such that $x_i \neq y_i$. Alice measures the state, obtaining some index i^* such that $x_{i^*} \neq y_{i^*}$ if $x \neq y$. Then she sends i^* and the value x_{i^*} over to Bob using $\lceil \log n \rceil + 1$ qubits. He outputs 'equal' if and only if $x_{i^*} = y_{i^*}$. The total communication cost of the protocol is then $2\lceil \log n \rceil + 1$ qubits. ◀

This protocol can be extended to efficiently solve the equivalent problem for other distances than $n/4$ in constant rounds, by using a more general exact version of the Grover search algorithm. The construction is described in Appendix B.

3 The list problem

In this section, we consider the $\mathcal{L}$-LIST problem: Bob gets a list $L \in \mathcal{L}$ from a family $\mathcal{L} \subseteq 2^{\mathcal{X}}$ of lists, Alice gets an element $x \in L$, and Bob must learn x.

3.1 Classical communication complexity of the list problem

Here we prove Theorem 1.6. The list problem that gives the result is simple: For positive integers k, N such that $2 \leq k \leq N$, we consider the list problem $\mathcal{L} = \binom{[N]}{k}$, where the family of lists consists of all k-element subsets of $[N]$. Note that for this problem, Theorem 1.5 gives a four-round protocol using at most $\log\log N + 2\log k + O(\log\log k)$ bits of communication.

▶ **Theorem 3.1.** *The classical communication complexity of* $\binom{[N]}{k}$-LIST *is at least*

$$\log\log N + 2\log(k-1) - \log\log(k-1) - O(1).$$

To see that this implies Theorem 1.6 note that for $\mathcal{L}$ as above, we clearly have $\omega(\mathcal{L}) = k$ and that $G_{\mathcal{L}}$ is the complete graph on N vertices, giving $\chi(G_{\mathcal{L}}) = N$. Hence, the bound in the above theorem can be written as $\log\log\chi(G_{\mathcal{L}}) + (2 - o(1))\log\omega(\mathcal{L})$, where the term $o(1)$ goes to zero as $k \to \infty$. Choosing $k = \log N$ then gives the second part of the theorem.

To prove Theorem 3.1, we use a bound on the size of cover-free families due to Dýachkov and Rykov [13]; see [30, 15] for simplified proofs (in English).

▶ **Definition 3.2.** Let r be a positive integer and $\mathcal{S}$ be a finite set. A family $\mathcal{F} \subseteq 2^{\mathcal{S}}$ of at least $r+1$ subsets is *r-cover-free* if every subfamily of $r+1$ distinct sets $F_0, F_1, \ldots, F_r \in \mathcal{F}$ satisfies $F_0 \not\subseteq F_1 \cup \cdots \cup F_r$.

▶ **Theorem 3.3** (Dýachkov–Rykov)**.** *There exists an absolute constant $c > 0$ such that the following holds. Let N and r be positive integers such that $N \geq r+1$ and $r \geq 2$. Let $\mathcal{S}$ be a finite set. Let $\mathcal{F} \subseteq 2^{\mathcal{S}}$ be an r-cover free family consisting of N sets. Then,*

$$|\mathcal{S}| \geq \frac{cr^2 \log N}{\log r}.$$

Proof of Theorem 3.1. For a positive integer C, suppose that the communication complexity of $\binom{[N]}{k}$-LIST is C. Fix such a protocol and for every input pair (x, L) in the $\binom{[N]}{k}$-LIST problem, define the *transcript* $T_{x,L} \in \{0,1\} \cup \{0,1\}^2 \cup \cdots \cup \{0,1\}^C$ as the concatenation of the parties' messages in the order they are sent during their conversation on input (x, L). Let $\mathcal{T}$ be the set of said transcripts.

For each transcript $T \in \mathcal{T}$, denote by T^A the sequence of Alice's messages in T, to be understood as a sequence of strings indexed by her rounds in the conversation. Let $\mathcal{F} = \{F_x\}_{x \in \mathcal{X}} \subseteq 2^{\mathcal{T}}$ be the family where each F_x is the collection of transcripts $T \in \mathcal{T}$ that is consistent with x being Alice's input and that agrees on T^A. We claim that $\mathcal{F}$ is a $(k-1)$-cover free family. To see this, take any k sets of $\mathcal{F}$, say $F_{x_0}, \ldots, F_{x_{k-1}}$, and let L be the corresponding k-element list $\{x_0, \ldots, x_{k-1}\}$. Consider the transcript $T_{x_0,L}$ of the input pair (x_0, L). Clearly, $T_{x_0,L} \in F_{x_0}$. We show that $T_{x_0,L} \notin F_{x_i}$ for each $i \in \{1, \ldots, k-1\}$, which gives the claim as this implies that $F_{x_0} \not\subseteq F_{x_1} \cup \cdots \cup F_{x_{k-1}}$. Suppose that $T_{x_0,L} \in F_{x_i}$ holds for some $i \in \{1, \ldots, k-1\}$. This means that Alice sends identical message sequences on inputs x_0 and x_i and therefore that Bob is not able to distinguish between these two cases for the input pair (x_0, L), contradicting our assumption that we started with a functional protocol.

We also claim that $\mathcal{F}$ consists of at least N sets. Indeed, for every pair $x, y \in [N]$, there is a list $L \in \binom{[N]}{k}$ containing both x and y. Since we must have $T^A_{x,L} \neq T^A_{y,L}$ for Bob to be able to distinguish x and y on input L, the inputs x and y induce distinct transcript sets.

It thus follows from Theorem 3.3 that the total number of distinct transcripts is at least

$$|\mathcal{T}| \geq \frac{c(k-1)^2 \log N}{\log(k-1)}.$$

Hence, since $\mathcal{T} \subseteq \{0,1\} \cup \{0,1\}^2 \cup \cdots \cup \{0,1\}^C$, we have

$$\frac{2^{C+1}-1}{2-1} = \sum_{l=0}^{C} 2^l \geq \frac{c(k-1)^2 \log N}{\log(k-1)},$$

for some absolute constant $c > 0$. Taking logarithms now gives the claim. ◀

3.2 Quantum communication complexity of the list problem

Analogous to Witsenhausen's result, the one-round quantum communication complexity of a list problem is characterized in terms of the orthogonality dimension of its associated graph.

▶ **Lemma 3.4.** *For every family $\mathcal{L} \subseteq 2^{\mathcal{X}}$, the one-round quantum communication complexity of $\mathcal{L}$-LIST equals $\lceil \log \xi(G_{\mathcal{L}}) \rceil$.*

Proof. Consider an optimal one-round protocol. Without loss of generality, we can assume that Alice sends to Bob a pure state $|\phi_x\rangle \in \mathbb{C}^d$ on input $x \in \mathcal{X}$. Then, given a list $L \in \mathcal{L}$, Bob has a measurement that allows him to distinguish the states $\{|\phi_x\rangle : x \in L\}$. It thus follows from Lemma 2.3 that these states must be orthogonal. In particular, since for every list $L \in \mathcal{L}$, each pair of distinct elements $x, y \in L$ forms an edge in $G_{\mathcal{L}}$, the vectors $|\phi_x\rangle$, $x \in \mathcal{X}$, form a d-dimensional orthogonal representation. Hence, $\xi(G_{\mathcal{L}}) \leq d$.

Conversely, let $f : V(G_{\mathcal{L}}) \to \mathbb{C}^d$ be an orthogonal representation of $G_{\mathcal{L}}$. Then, for every list $L \in \mathcal{L}$, the vectors $\{f(x) : x \in L\}$ are pairwise orthogonal. If Bob gets a list $L \in \mathcal{L}$ and Alice gets an element $x \in L$, it follows from Lemma 2.3 that there is a quantum measurement allowing Bob to uniquely identify x when Alice sends $f(x)$ using $\log d$-qubits. Hence, the one-round quantum communication complexity is at most $\lceil \log \xi(G_{\mathcal{L}}) \rceil$. ◀

For multi-round protocols, a quantum analogue of Theorem 1.3 also holds.

▶ **Lemma 3.5.** *For every family $\mathcal{L} \subseteq 2^{\mathcal{X}}$, the quantum communication complexity of $\mathcal{L}$-*LIST *is at least* $\max\{\Omega(\log\log \chi(G_{\mathcal{L}})), \log \omega(\mathcal{L})\}$.

Proof. Kremer's Theorem (Theorem 1.1) shows that there is at most an exponential difference between the (multi-round) quantum and one-round classical communication complexity. Hence, by Witsenhausen's result, the former is at least $\Omega(\log\log \chi(G_{\mathcal{L}}))$. Moreover, on the worst input Bob has to be able to distinguish among $\omega(\mathcal{L})$ different elements. Hence, $\log \omega(\mathcal{L})$ bits of information must be communicated and Holevo's Theorem [19] says that to retrieve $\log \omega(\mathcal{L})$ bits of information $\log \omega(\mathcal{L})$ qubits are necessary. ◀

3.3 Proof of Theorem 1.7

Recall that we are considering the following family of lists. For an even positive integer n and $d \in [n]$, let $\mathcal{L}_d \subseteq 2^{\{0,1\}^n}$ be the family of all lists $L \subseteq \{0,1\}^n$ of maximal cardinality such that all strings in L have Hamming distance exactly d. We denote by $\mathcal{K}$ the union $\mathcal{L}_{n/2} \cup \cdots \cup \mathcal{L}_n$.

Proof of Theorem 1.7. Let $\ell = \lceil \log n \rceil$ and U be an $(\ell+1)$-qubit unitary matrix satisfying

$$U|0\rangle|0\rangle^{\otimes \ell} = |0\rangle|0\rangle^{\otimes \ell}$$
$$U|1\rangle|0\rangle^{\otimes \ell} = \frac{1}{\sqrt{n}}|1\rangle \sum_{i=1}^{n} |i\rangle.$$

Moreover, for any 2^ℓ-bit string z, we define the conditional query unitary U_z which acts on the computational basis states as $U_z|0\rangle|i\rangle = |0\rangle|i\rangle$ and $U_z|1\rangle|i\rangle = (-1)^{z_i}|1\rangle|i\rangle$. For a small technicality, if n is not a power of 2, i.e. $\ell > \log n$, we will map any n-bit string to a 2^ℓ-bit string obtained by padding zeros to the original string. We can now explain the protocol.

Suppose that Bob receives a list $L \in \mathcal{L}_d$ and Alice a string $x \in L$. From L, Bob computes the distance d and he sends to Alice a single qubit $\gamma|0\rangle + \sqrt{1-\gamma^2}|1\rangle$ where $\gamma^2 = 1 - \frac{n}{2d} > 0$. Alice pads ℓ zero qubits to the one she received and then applies in sequence the unitaries U

and U_x, obtaining the state

$$\begin{aligned}|\phi_x\rangle &:= U_x U\left(\gamma|0\rangle|0\rangle^{\otimes\ell} + \sqrt{1-\gamma^2}|1\rangle|0\rangle^{\otimes\ell}\right)\\ &= U_x\left(\gamma|0\rangle|0\rangle^{\otimes\ell} + \sqrt{\frac{1-\gamma^2}{n}}\sum_{i=1}^{n}|1\rangle|i\rangle\right)\\ &= \gamma|0\rangle|0\rangle^{\otimes\ell} + \sqrt{\frac{1-\gamma^2}{n}}\sum_{i=1}^{n}(-1)^{x_i}|1\rangle|i\rangle\end{aligned}$$

which she sends to Bob, using $\lceil \log n \rceil + 1$ qubits. Notice that if $x, y \in \{0,1\}^n$ differ in exactly d positions, then the states $|\phi_x\rangle$ and $|\phi_y\rangle$ are orthogonal to each other. Hence, by Lemma 2.3, using the list L Bob can perform a measurement that allows him to learn Alice's input x. This protocol requires a total communication of $\lceil \log n \rceil + 2$ qubits. ◀

Acknowledgements. Part of this work was conducted while H. B., D. L., T. P. and F. S. were at the Newton Institute of Mathematical Sciences in Cambridge, UK. J. B. was supported by a Rubicon grant from the Netherlands Organization for Scientific Research (NWO). H. B., T. P. and F. S. were funded in part by the EU project SIQS. D. L. is supported by NSERC, CRC, and CIFAR.

References

1 Andris Ambainis. Quantum search algorithms. *SIGACT News*, 35(2):22–35, June 2004.
2 M. Boyer, G. Brassard, P. Høyer, and A. Tapp. Tight bounds on quantum searching. *Fortschritte der Physik*, 46(4-5):493–505, 1998.
3 G. Brassard, P. Høyer, M. Mosca, and A. Tapp. Quantum amplitude amplification and estimation. In *Quantum computation and information (Washington, DC, 2000)*, volume 305 of *Contemp. Math.*, pages 53–74. Amer. Math. Soc., Providence, RI, 2002.
4 G. Brassard, P. Høyer, and A. Tapp. Quantum counting. In *Proceedings of the 25th International Colloquium on Automata, Languages and Programming*, ICALP'98, pages 820–831, London, UK, 1998. Springer-Verlag.
5 J. Briët, H. Buhrman, and D. Gijswijt. Violating the Shannon capacity of metric graphs with entanglement. *Proceedings of the National Academy of Sciences*, 2012.
6 J. Briët, H. Buhrman, M. Laurent, T. Piovesan, and G. Scarpa. Entanglement-assisted zero-error source-channel coding. *Information Theory, IEEE Transactions on*, 61(2):1124–1138, 2015. A previous version appeared in EuroComb 2014.
7 H. Buhrman, R. Cleve, and A. Wigderson. Quantum vs. classical communication and computation. In *Proceedings of the 30th Annual ACM Symposium on Theory of Computing (STOC 1998)*, pages 63–68, 1998.
8 P. J. Cameron, A. Montanaro, M. W. Newman, S. Severini, and A. Winter. On the quantum chromatic number of a graph. *The electronic journal of combinatorics*, 14(R81):1, 2007.
9 T. S. Cubitt, D. Leung, W. Matthews, and A. Winter. Improving zero-error classical communication with entanglement. *Physical Review Letters*, 104(23):230503, 2010.
10 T. S. Cubitt, L. Mančinska, D. E. Roberson, S. Severini, D. Stahlke, and A. Winter. Bounds on entanglement assisted source-channel coding via the lovasz theta number and its variants. *IEEE Transactions of Information Theory*, 60(11):7330–7344, 2014.
11 R. de Wolf. *Quantum Computing and Communication Complexity*. PhD thesis, Universiteit van Amsterdam, 2001.
12 P. Delsarte and V. I. Levenshtein. Association schemes and coding theory. *IEEE Transactions on Information Theory*, 44(6):2477–2504, 1998.

13 A. G. Dýachkov and V. V. Rykov. Bounds on the length of disjunctive codes. *Problemy Peredachi Informatsii*, 18(3):7–13, 1982. In Russian.

14 P. Frankl and V. Rödl. Forbidden intersections. *Transactions of the American Mathematical Society*, 300(1):259–286, 1987.

15 Z. Füredi. On r-cover-free families. *Journal of Combinatorial Theory, Series A*, 73(1):172–173, 1996.

16 C. D. Godsil and M. W. Newman. Coloring an orthogonality graph. *SIAM Journal on Discrete Mathematics*, 22(2):683–692, March 2008.

17 L. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of STOC'96*, pages 212–219, 1996.

18 J. Gruska, D. Qiu, and S. Zheng. Generalizations of the distributed deutsch-jozsa promise problem. *Preprint available at arXiv:1402.7254*, 2014.

19 A. S. Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problems of Information Transmission*, 9:177–183, 1973.

20 I. Krasikov and S. Litsyn. *Survey of binary Krawtchouk polynomials.*, pages 199–211. Providence, RI: AMS, American Mathematical Society, 2001.

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

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

23 M. Laurent. Private communications, 2014.

24 D. Leung, L. Mančinska, W. Matthews, M. Ozols, and A. Roy. Entanglement can increase asymptotic rates of zero-error classical communication over classical channels. *Communications in Mathematical Physics*, 311:97–111, 2012.

25 V. I. Levenshtein. Krawtchouk polynomials and universal bounds for codes and designs in hamming spaces. *IEEE Trans. Inf. Theor.*, 41(5):1303–1321, 1995.

26 L. Lovász. On the Shannon capacity of a graph. *IEEE Transactions on Information Theory*, 25(1):1–7, 1979.

27 M. Naor, A. Orlitsky, and P. Shor. Three results on interactive communication. *IEEE Transactions on Information Theory*, 39:1608–1615, 1993.

28 A. Orlitsky. Worst-case interactive communication i: Two messages are almost optimal. *IEEE Transactions on Information Theory*, 36:1111–1126, 1990.

29 M. J. P. Peeters. Orthogonal representations over finite fields and the chromatic number of graphs. *Combinatorica*, 16(3):417–431, 1996.

30 M. Ruszinkó. On the upper bound of the size of the r-cover-free families. *Journal of Combinatorial Theory, Series A*, 66(2):302–310, 1994.

31 G. Scarpa and S. Severini. Kochen-Specker Sets and the Rank-1 Quantum Chromatic Number. *IEEE Transactions on Information Theory*, 58(4):2524–2529, 2012.

32 Joel Spencer. *Asymptopia*, volume 71 of *Student Mathematical Library*. American Mathematical Society, Providence, RI, 2014. With Laura Florescu.

33 H. S. Witsenhausen. The zero-error side information problem and chromatic numbers. *IEEE Transactions on Information Theory*, 22(5):592–593, 1976.

34 A. C.-C. Yao. Some complexity questions related to distributive computing (preliminary report). In *Proceedings of the 11th annual ACM symposium on Theory of computing (STOC 1979)*, pages 209–213, 1979.

35 A. C.-C. Yao. Quantum circuit complexity. In *Proceedings of the 34th Annual Symposium on Foundations of Computer Science (FOCS 1993)*, pages 352–361, 1993.

A Kremer's Theorem

Here we prove Kremer's Theorem (Theorem 1.1), which we restate for convenience. The original proof by Kremer [21] applied to boolean functions; we give a slight generalization of the statement so that it applies to functions with arbitrary range. It is important to notice that the statements in this section hold for general communication protocols, not only exact ones.

▶ **Theorem A.1.** *Let ℓ be a positive integer, $X, Y, \mathcal{R}$ be finite sets and $\mathcal{D} \subseteq X \times Y$. Let $f : \mathcal{D} \to \mathcal{R}$ be a function and suppose that f admits an ℓ-qubit quantum protocol. Then, there exists a one-round $2^{O(\ell)}$-bit classical protocol for f.*

The proof uses the following lemma of Yao [35] and Kremer [21]. To reduce the amount of notation needed in the proof we assume that the parties use the following general protocol. At any point during the protocol, both Alice and Bob have a private quantum register. If it is Alice's turn to communicate, say ℓ-qubits, she appends a fresh ℓ-qubit register to her existing register, applies a unitary to both registers and sends the ℓ-qubit register over to Bob, who then absorbs the ℓ-qubit register into his private register. If it's his turn to communicate, Bob operates similarly. This assumption will allow us to deal more easily with protocols in which different numbers of qubits are sent in each round.

▶ **Lemma A.2** (Yao–Kremer). *Let ℓ be a positive integer, $X, Y, \mathcal{R}$ be finite sets and $\mathcal{D} \subseteq X \times Y$. Suppose that there exists an r-round quantum protocol for a function $f : \mathcal{D} \to \mathcal{R}$, where ℓ_i qubits are communicated in round $i \in [r]$. Then, the final state of the protocol on input $(x, y) \in \mathcal{D}$ can be written as*

$$\sum \alpha_{\mathbf{u}}(x)\beta_{\mathbf{u}}(y)|A_{\mathbf{u}}(x)\rangle|B_{\mathbf{u}}(y)\rangle,$$

where the sum is over all $\mathbf{u} \in \{0,1\}^{\ell_1} \times \cdots \times \{0,1\}^{\ell_r}$, the $\alpha_{\mathbf{u}}(x), \beta_{\mathbf{u}}(y)$ are complex numbers and the $|A_{\mathbf{u}}(x)\rangle, |B_{\mathbf{u}}(y)\rangle$ are complex unit vectors.

Proof. By induction on r. The base case $r = 1$ is trivial, since then Alice sends Bob an ℓ-qubit state. For some $i \in \{2, 3, \ldots, r\}$, suppose that after $i-1$ rounds the state is given by

$$\sum \alpha_{\mathbf{v}}(x)\beta_{\mathbf{v}}(y)|A_{\mathbf{v}}(x)\rangle|B_{\mathbf{v}}(y)\rangle,$$

where the sum is over all $\mathbf{v} \in \{0,1\}^{\ell_1} \times \cdots \times \{0,1\}^{\ell_{i-1}}$. Assume that the i-th round is Alice's turn (the case of Bob's turn is handled similarly). She appends a fresh ℓ_i-qubit register to her current register, causing the state to become

$$\sum \alpha_{\mathbf{v}}(x)\beta_{\mathbf{v}}(y)|A_{\mathbf{v}}(x)\rangle|0_1 \cdots 0_{\ell_i}\rangle|B_{\mathbf{v}}(y)\rangle.$$

Next, she applies a unitary over both of her registers, turning the state into

$$\sum \alpha_{\mathbf{v}}(x)\beta_{\mathbf{v}}(y) \left(\sum_{\mathbf{w} \in \{0,1\}^{\ell_i}} \gamma_{\mathbf{w}}|A_{\mathbf{v},\mathbf{w}}(x)\rangle|\mathbf{w}\rangle \right) |B_{\mathbf{v}}(y)\rangle,$$

where $\gamma_{\mathbf{w}}$ is a complex number (which might depend on x) and for some unit vectors $|A_{\mathbf{v},\mathbf{w}}(x)\rangle$. Now define

$$\alpha_{\mathbf{v},\mathbf{w}}(x) := \alpha_{\mathbf{v}}(x)\gamma_{\mathbf{w}}, \qquad \beta_{\mathbf{v},\mathbf{w}}(y) := \beta_{\mathbf{v}}(y) \qquad \text{and} \qquad |B_{\mathbf{v},\mathbf{w}}(y)\rangle := |\mathbf{w}\rangle|B_{\mathbf{v}}(y)\rangle,$$

so that after the ith round, after Alice has sent the ℓ_i-qubit register to Bob, the state equals

$$\sum_{\mathbf{v},\mathbf{w}} \alpha_{\mathbf{v},\mathbf{w}}(x)\beta_{\mathbf{v},\mathbf{w}}(y)|A_{\mathbf{v},\mathbf{w}}(x)\rangle|B_{\mathbf{v},\mathbf{w}}(y)\rangle.$$

After r rounds the state thus looks like as claimed in the lemma. ◀

Proof of Theorem 1.1. Assume that the protocol proceeds in r rounds and that ℓ_i qubits are communicated during round $i \in [r]$. By Lemma A.2 the final state of the protocol can be written as

$$\sum \alpha_{\mathbf{u}}(x)\beta_{\mathbf{u}}(y)|A_{\mathbf{u}}(x)\rangle|B_{\mathbf{u}}(y)\rangle,$$

To produce his output, Bob performs a measurement $\{M_1, \ldots, M_k\}$ on his register. For each pair $\mathbf{u}, \mathbf{v} \in \{0,1\}^{\ell_1} \times \cdots \times \{0,1\}^{\ell_r}$ and $j \in [k]$ we define the complex numbers

$$\begin{aligned} a_{\mathbf{u},\mathbf{v}}(x) &:= \overline{\alpha_{\mathbf{u}}(x)}\alpha_{\mathbf{v}}(x)\langle A_{\mathbf{u}}(x)|A_{\mathbf{v}}(x)\rangle \\ b^j_{\mathbf{u},\mathbf{v}}(x) &:= \overline{\beta_{\mathbf{u}}(y)}\beta_{\mathbf{v}}(y)\langle B_{\mathbf{u}}(y)|M_j|B_{\mathbf{v}}(y)\rangle. \end{aligned}$$

Then, the probability that Bob gets measurement outcome j equals

$$p_j(x,y) = \sum_{\mathbf{u},\mathbf{v}} a_{\mathbf{u},\mathbf{v}}(x)b^j_{\mathbf{u},\mathbf{v}}(y).$$

The classical one-round protocol works in the following way. Let ℓ be the total communication of the protocol and define $\tilde{a}_{\mathbf{u},\mathbf{v}}(x)$ as an approximation of $a_{\mathbf{u},\mathbf{v}}(x)$ using $2\ell+4$ bits for the real part and $2\ell+4$ bits for the imaginary part, so that $|\tilde{a}_{\mathbf{u},\mathbf{v}}(x) - a_{\mathbf{u},\mathbf{v}}(x)| \leq 2^{-2\ell-3}$. Alice's message consists of all $2^{2\ell}$ numbers $\tilde{a}_{\mathbf{u},\mathbf{v}}(x)$, making the total communication cost $O(\ell 2^{2\ell})$ bits. Bob calculates his approximation of the probability of getting outcome j as

$$\tilde{p}_j(x,y) = \sum_{\mathbf{u},\mathbf{v}} \tilde{a}_{\mathbf{u},\mathbf{v}}(x)b^j_{\mathbf{u},\mathbf{v}}(y).$$

We can bound the difference between this approximation and the acceptance probability of the original quantum protocol by

$$\begin{aligned} |\tilde{p}_j(x,y) - p_j(x,y)| &= \Big|\sum_{\mathbf{u},\mathbf{v}} \big(\tilde{a}_{\mathbf{u},\mathbf{v}}(x) - a_{\mathbf{u},\mathbf{v}}(x)\big)b^j_{\mathbf{u},\mathbf{v}}(y)\Big| \\ &\leq \sum_{\mathbf{u},\mathbf{v}} \big|\tilde{a}_{\mathbf{u},\mathbf{v}}(x) - a_{\mathbf{u},\mathbf{v}}(x)\big|\,\big|b^j_{\mathbf{u},\mathbf{v}}(y)\big| \\ &\leq 2^{-2\ell-3}2^{2\ell} \leq \frac{1}{8}. \end{aligned}$$

Therefore, given a quantum protocol with sufficiently high success probability, in this paper in particular probability 1, Bob can (deterministically) choose the unique outcome j for which $\tilde{p}_j(x,y)$ is strictly greater than $\frac{1}{2}$, and this outcome j is equal to the function value $f(x,y)$, by correctness of the original quantum protocol. ◀

B Multi-round quantum protocols for EQ-$\binom{n}{\alpha n}$ with $\alpha < 1/2$

Using distributed versions of Grover's search algorithm, we find multi-round quantum communication protocols that solve the EQ-$\binom{n}{\alpha n}$ problem for $\alpha < 1/2$ with a logarithmic number of qubits. For $\alpha = 1/4$, this statement is proven in Theorem 2.11.

When $d = \alpha \cdot n$ where $\alpha \in (1/4, 1/2)$, we can pad zeros to the inputs such that the new strings are either equal or differ in exactly 1/4-th of the positions and run the above two-rounds protocol on the new strings. This is the simple key idea behind the following theorem.

▶ **Theorem B.1.** *For $d = \alpha \cdot n$ with $\alpha \in (1/4, 1/2)$, the two-round quantum communication complexity of $\mathrm{EQ}\text{-}\binom{n}{\alpha n}$ is at most $2\lceil \log n \rceil + 2\lceil \log(4\alpha) \rceil + 1$ qubits.*

Proof. Let x and y be Alice's and Bob's inputs. They know that x and y are either equal or they differ in exactly $d = \alpha \cdot n$ positions where $d > n/4$. Suppose that Alice and Bob pad their respective inputs with k consecutive zeros with $k = 4d - n$. The new bit strings $\hat{x}$ and $\hat{y}$ have length $n' = n + k = 4d$ and they are either equal or differ in exactly $\alpha' \cdot n' = n'/4$ positions.

Alice and Bob can now run the distributed Grover's search protocol described in the proof of Theorem 2.11 on the new inputs $\hat{x}, \hat{y} \in \{0,1\}^{n'}$. The total communication cost is $2\lceil \log n' \rceil + 1 = 2\lceil \log(4\alpha \cdot n) \rceil + 1 \leq 2\lceil \log n \rceil + 2\lceil \log(4\alpha) \rceil + 1$ qubits. ◀

For $d = \alpha \cdot n$ where $\alpha \in (0, 1/4)$, we need to introduce some technicalities to ensure an exact version of Grover's search algorithm.

▶ **Theorem B.2.** *For $d = \alpha \cdot n$ with $\alpha \in (0, 1/4)$, the quantum communication complexity of $\mathrm{EQ}\text{-}\binom{n}{\alpha n}$ is at most $O(\log n)$ qubits. The quantum communication protocol uses $O(\frac{1}{\sqrt{\alpha}})$ rounds.*

Proof. If a n-bit string z is known to contain exactly d entries that are 1, Grover's algorithm can be modified such that it finds an index for one of them with certainty [3, Theorem 16] [4, 1]. The number of queries ℓ that the exact version of Grover's algorithm needs in this case is given by

$$\ell = \left\lceil \frac{\pi}{4 \arcsin \sqrt{\frac{d}{n}}} - \frac{1}{2} \right\rceil < \frac{\pi}{4}\sqrt{\frac{n}{d}} + 1\,.$$

The exact version of Grover's algorithm is the same as the original algorithm, except for an adapted final step, which uses a parametrized diffusion operator $G(\phi)$ and partial query $V_z(\varphi)$, where ϕ and φ are angles that depend on the Hamming distance d. As these angles do not have a nice closed formula, we refer the reader to [3, Equation (12)] for the relation that ϕ and φ must satisfy. Here

$$V_z(\varphi)|j\rangle = \begin{cases} |j\rangle & \text{if } z_j = 0 \\ e^{i\varphi}|j\rangle & \text{if } z_j = 1 \end{cases}$$

and

$$G(\phi) = F_n V_0(\phi) F_n^\dagger\,,$$

where F_n is the $n \times n$ discrete quantum Fourier transform.[3]

Take $x, y \in \{0,1\}^n$ to be the input strings of Alice and Bob and let $z = x \oplus y$. As in the proof of the $n/4$ case of Theorem 2.11, we turn this search algorithm into a quantum communication protocol by writing a single query $U_z = U_x U_y = U_y U_x$. We can use the

[3] Note that if n is a power of 2, it is also possible to use the $n \times n$ Hadamard transform.

commutativity of U_x and U_y to save rounds: The exact Grover's algorithm is performed by executing the operations

$$G(\phi)V_z(\varphi)\underbrace{GU_z\dots GU_z}_{\ell-1 \text{ times}}$$

on starting state $|s\rangle = \frac{1}{\sqrt{n}}\sum_{i=1}^{n}|i\rangle$. Since we can write two alternations as $GU_zGU_z = GU_xU_yGU_yU_x$, alternating whether Alice or Bob executes the query first that round, only $\ell-1$ rounds are needed for the $\ell-1$ ordinary Grover iterations. Alice starts the protocol if ℓ is even, and Bob sends the first message if ℓ is odd.

For the final step, the players need to simulate a query $V_z(\varphi)$ by local operations that depend only on x or y. At this point in the protocol it is Alice's turn to communicate. She currently holds the state

$$|\psi\rangle = \underbrace{GU_z\dots GU_z}_{\ell-1 \text{ times}}|s\rangle\,.$$

Now Alice adds an auxiliary qubit that starts in $|0\rangle$ state. Define the unitary operation Q_x by its action on the computational basis states as

$$Q_x|j\rangle|b\rangle = |j\rangle|b\oplus x_j\rangle$$

and the (diagonal) unitary matrix $R_y(\varphi)$ as

$$R_y(\varphi)|j\rangle|b\rangle = e^{i\varphi(b\oplus y_j)}|j\rangle|b\rangle\,.$$

Now Alice first applies Q_x on the state $|\psi\rangle|0\rangle$, sends this state to Bob who performs $R_y(\varphi)$, sending the state back to Alice who again performs Q_x. It is easy to check that $Q_xR_y(\varphi)Q_x|\psi\rangle|0\rangle = (V_z(\varphi)\otimes I)|\psi\rangle|0\rangle$, therefore Alice now discards the auxiliary qubit and applies $G(\phi)$ to finish the simulation of the exact version of Grover's algorithm.

The final state of the exact Grover's algorithm is $\frac{1}{\sqrt{d}}\sum_{i \text{ s.t. } z_i=1}|i\rangle$ if $|z| = d$. If Alice has this state in her possession, she performs a measurement in the computational basis, obtaining an index i^* such that $x_{i^*} \neq y_{i^*}$ if $x \neq y$. Then she sends i^* and the value x_{i^*} over to Bob, who outputs 'equal' if and only if $x_{i^*} = y_{i^*}$. This final message consists of $\lceil\log n\rceil + 1$ qubits. By the correctness of the exact Grover's algorithm, this protocol correctly outputs 'not equal' if the Hamming distance between x and y is the fixed value d. Therefore we turned a ℓ-query execution of the exact version of Grover's algorithm into a protocol that uses $(\ell+2)\lceil\log n\rceil + 2$ qubits of communication in $\ell+2$ rounds. ◀