Quantum communication complexity of symmetric predicates

A. A. Razborov

Abstract. We completely (that is, up to a logarithmic factor) characterize the bounded-error quantum communication complexity of every predicate \( f(x, y) \) \((x, y \subseteq [n])\) depending only on \(|x \cap y|\). More precisely, given a predicate \( D \) on \( \{0, 1, \ldots, n\} \), we put

\[
\begin{align*}
l_0(D) & \overset{\text{def}}{=} \max\{l \mid 1 \leq l \leq n/2 \land D(l) \neq D(l - 1)\}, \\
l_1(D) & \overset{\text{def}}{=} \max\{n - l \mid n/2 < l < n \land D(l) \neq D(l + 1)\}.
\end{align*}
\]

Then the bounded-error quantum communication complexity of \( f_D(x, y) = D(|x \cap y|) \) is equal to \( \sqrt{n} l_0(D) + l_1(D) \) (up to a logarithmic factor). In particular, the complexity of the set disjointness predicate is equal to \( \Omega(\sqrt{n}) \). This result holds both in the model with prior entanglement and in the model without it.

§ 1. Introduction

The model of communication complexity, originally introduced by Yao [25], has since evolved into a very intriguing and important branch of computational complexity. In particular, it links and unifies many different things. This model involves two players, traditionally called Alice and Bob. Alice holds an input \( x \in X \) (where \( X \) is a fixed finite set), Bob holds \( y \in Y \), and they exchange messages to evaluate a Boolean predicate \( f: X \times Y \to \{0, 1\} \). The complexity is measured by the number of bits exchanged and, as in many other areas of computational complexity, one distinguishes between deterministic and probabilistic modes.

Just as circuit complexity is often concerned with symmetric Boolean functions, the class of symmetric predicates attracts considerable interest in communication complexity. We define symmetric predicates to be those for which \( x, y \) are finite sets and \( f_D(x, y) = D(|x \cap y|) \) for some Boolean predicate \( D \) on integers. The most prominent members of this class are the disjointness predicate \( \text{DISJ}_n \) \((D(s) \equiv (s = 0))\) and the inner product function \( \text{IP}_n \) \((D(s) \equiv s \mod 2)\). The classical rank lower bound of Mehlhorn and Schmidt [19] immediately yields a tight \( \Omega(n) \)

Institute for Advanced Study, Princeton, US, on leave from the Steklov Mathematical Institute, Moscow, Russia. Supported by the von Neumann Fund.

AMS 2000 Mathematics Subject Classification. 03D15, 68Q15, 81P68.
lower bound\(^1\) on the deterministic communication complexity of both \(\text{DISJ}_n\) and \(\text{IP}_n\).

For randomized algorithms that allow an error with probability \(\varepsilon\), where \(\varepsilon < 1/2\) is an arbitrary absolute constant, an \(\Omega(n)\) lower bound on the complexity of the inner product \(\text{IP}_n\) was proved in [4], [10], [24]. The paper [4] also contains an \(\Omega(\sqrt{n})\) lower bound for \(\text{DISJ}_n\). This bound was improved to the optimal \(\Omega(n)\) in [18], and the proof of the last result was further simplified in [23].

The model of quantum communication complexity was also introduced by Yao [26]. Suppose that Alice and Bob can employ the laws of quantum mechanics and are allowed to exchange qubits instead of classical bits. Can this help them to reduce the amount of communication?

Buhrman, Cleve and Wigderson [3] observed that the rank lower bound for deterministic protocols extends to the quantum case. (So, after all, the answer can be “no” for such protocols.) In particular, both \(\text{DISJ}_n\) and \(\text{IP}_n\) require at least \(\Omega(n)\) qubits to be exchanged by quantum deterministic (=zero-error) protocols. The rank lower bound was extended in [7] to the stronger model with prior entanglement introduced in [8]. (In this model, before communication begins, Alice and Bob share an unlimited number of Einstein–Podolski–Rosen pairs which are “entangled” in the sense that the first component of each pair is available to Alice, and the second to Bob.)

The question of the complexity of protocols that allow a small error is by far the more interesting. Based on some ideas from the seminal paper [26], Kremer [17] proved an exact \(\Omega(n)\) lower bound for \(\text{IP}_n\). This result was extended to the model with prior entanglement in [9]. Klauck [14] looked at threshold predicates \(D(s) \equiv (s \geq l)\) and exact-\(l\) predicates \(D(s) \equiv (s = l)\) and proved an \(\Omega(l/\log l)\) lower bound in both cases (without entanglement). Prior to our work, the only general lower bound for \(\text{DISJ}_n\) (which corresponds to \(l = 0\)) was \(\Omega(\log n)\) [1], [7]. We also mention some partial results in this direction such as the bounds for constant-round protocols [15], protocols with exponentially small error [7], and some highly structured protocols [13].

On the upper bounds frontier, the elegant paper [3] established a close connection between quantum search and quantum communication by showing how to convert every quantum search algorithm for any Boolean function \(g\) into a quantum communication algorithm for the associated predicate \(f_g(x, y) = g(x \land y)\) with only a logarithmic delay. Plugging the Grover search algorithm [12] into this procedure, we immediately get an \(O(\sqrt{n} \log n)\) upper bound for the quantum bounded-error communication complexity of the disjointness predicate. (This estimate was slightly improved to \(O(\sqrt{n} \exp(\log^* n))\) in [13].) It was proved in [2] that the quantum query complexity of every symmetric Boolean function \(g\) is equal (up to a constant factor) to the approximate degree \(\widetilde{\deg}(g)\), which is defined as the minimal degree of a real polynomial that approximates \(g\) in the \(l_\infty\)-norm on \(\{0, 1\}^n\) within accuracy 1/3. Combined with the reduction in [3], this yields an \(O(\deg(g) \log n)\) upper bound for the quantum bounded-error communication complexity of \(f_g(x, y)\).

\(^1\)The notation \(\Omega(f(n))\) is widely used in computational complexity. It is dual to the usual notation \(O(f(n))\) and denotes any function \(g(n)\) such that for some absolute constant \(\varepsilon > 0\) we have \(g(n) \geq \varepsilon f(n)\) for all \(n\).
Quantum communication complexity of predicates

In this paper we prove that this communication algorithm is essentially optimal for every symmetric predicate \( f_D(x, y) \) provided that we take care of one “degenerate” case. More precisely, we put

\[
l_0(D) \overset{\text{def}}{=} \max\{l \mid 1 \leq l \leq n/2 \land D(l) \neq D(l - 1)\}
\]

and

\[
l_1(D) \overset{\text{def}}{=} \max\{n - l \mid n/2 \leq l < n \land D(l) \neq D(l + 1)\},
\]

and \( g_D(x_1, \ldots, x_n) = D(|x|) \). Then the classical result by Paturi [22] says that \( \deg(g_D) = \Theta(\sqrt{n (l_0(D) + l_1(D))}) \). By [3], this yields an upper bound \( O(\sqrt{nl_0(D) + l_1(D)}) \log n) \) for the quantum bounded-error communication complexity of \( f_D \).

This bound can easily be improved to \( O(\sqrt{nl_0(D) + l_1(D)}) \log n) \). (Large values of \(|x \cap y|\) are taken care of by the trivial algorithm in which Alice sends Bob the whole input \( x \).) We shall prove the lower bound \( \Omega(\sqrt{n l_0(D) + l_1(D)}) \), which matches the upper bound up to a logarithmic factor (Theorem 2.1). Our lower bound also holds in the model with prior entanglement.

To prove this result, we use a multi-dimensional version of the usual discrepancy method (§ 5.2). In other words, we measure the communication matrix against several probability distributions at the same time. This enables us to reduce our problem to a classical problem in discrete polynomial approximation, which (quite fortunately) is already solved in the paper [22] mentioned above (see § 5.3). Another specific feature of our approach is that we apply spectral methods (as opposed to combinatorial ones) more systematically than was done in previous papers on this subject. (This becomes especially important when handling prior entanglement.) In particular, we prove a general lower bound for the quantum communication complexity of a function in terms of the approximate trace norm of its communication matrix (§ 5.1).

In the rest of the paper we state and prove our main result. Whenever possible, we try to reach reasonable generality in the statements of those intermediate steps of the proof that might be of independent interest.

§ 2. The quantum communication model and the main result

There are several equivalent definitions of the quantum communication model. Our description follows [7], which seems to be the most convenient to work with.

Let \( X, Y \) be finite sets, and \( f : X \times Y \rightarrow \{0, 1\} \) a Boolean predicate. Let \( \mathcal{H}_A, \mathcal{C}, \mathcal{H}_B \) be finite-dimensional Hilbert spaces representing Alice’s part, the channel, and Bob’s part respectively. Following [7], we assume that \( \mathcal{C} \) consists of a single qubit, in other words, \( \dim(\mathcal{C}) = 2 \) and \( |0\rangle, |1\rangle \) is an orthonormal basis of \( \mathcal{C} \).

The models with or without prior entanglement differ only in the choice of a unitary vector \( \text{Input}(x,y) \in \mathcal{H}_A \otimes \mathcal{C} \otimes \mathcal{H}_B \), which is prepared at the beginning of communication. We postpone its definition and describe how the communication proceeds. A communication protocol of length \( c \) is completely determined by unitary operators \( U_1, U_2, \ldots, U_c \), where \( U_i \) acts on \( \mathcal{H}_A \otimes \mathcal{C} \) if \( i \) is odd, and on \( \mathcal{C} \otimes \mathcal{H}_B \) if \( i \) is even. The (unitary) output vector \( \text{Output}(x,y) \) is given by

\[
\text{Output}(x,y) \overset{\text{def}}{=} \ldots (U_3 \otimes I_B)(I_A \otimes U_2)(U_1 \otimes I_B) \text{Input}(x,y),
\]
where $I_A, I_B$ are the identity operators on $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively. The acceptance probability of this protocol on $(x, y)$ is the result of the measurement of $\text{Output}(x, y)$ with respect to $C$, that is, the squared $l_2$-norm of its orthogonal projection onto $\mathcal{H}_A \otimes \{|1\} \otimes \mathcal{H}_B$.

We now describe the vector $\text{Input}(x, y)$. In the model without prior entanglement, $\mathcal{H}_A$ has an orthonormal basis $\{|a, x\} | a \in W_A, x \in X\}$, where $W_A$ is a finite set (representing Alice's internal computations) with a distinguished element $0$ (the beginning state). Likewise, $\mathcal{H}_B$ has an orthonormal basis $\{|y, b\} | b \in W_B, y \in Y\}$, and $\text{Input}(x, y) \overset{\text{def}}{=} |0, x\rangle|0, y, 0\rangle$.

In the model with prior entanglement (see also Remark 2.4 below), $\mathcal{H}_A$ has a basis $\{|a, x, e\} | a \in W_A, x \in X, e \in E\}$, and $\mathcal{H}_B$ has a basis $\{|e, y, b\} | b \in W_B, y \in Y, e \in E\}$. Here $E$ is a new finite set, which corresponds to all possible pure states of entangled Einstein–Podolski–Rosen pairs. The beginning state in this case is given by

$$\text{Input}(x, y) \overset{\text{def}}{=} \frac{1}{|E|^{1/2}} \sum_{e \in E} |0, x, e\rangle|0, y, 0\rangle.$$ (2.2)

It is important that we have no control over $|E|$ in this model. In particular, this number must not appear in our final bounds.

A communication protocol computes $f(x, y)$ with error $\varepsilon$ if its acceptance probability on every $(x, y)$ is at most $\varepsilon$ whenever $f(x, y) = 0$, and at least $1 - \varepsilon$ whenever $f(x, y) = 1$. Let $Q_\varepsilon(f)$ (resp. $Q^*_\varepsilon(f)$) be the smallest $c$ for which there is a communication protocol of length $c$ without (resp. with) prior entanglement that computes $f$ with error $\varepsilon$. We put $Q(f) \overset{\text{def}}{=} Q_{1/3}(f)$ and $Q^*(f) \overset{\text{def}}{=} Q^*_{1/3}(f)$.

We now fix an integer $n$, and let $D: \{0, 1, \ldots, n\} \rightarrow \{0, 1\}$ be any Boolean predicate. We put $f_{n,D}(x, y) \overset{\text{def}}{=} D(\{x \cap y\})$, where $x, y \subseteq [n] \overset{\text{def}}{=} \{1, 2, \ldots, n\}$. Let $l_0(D)$ and $l_1(D)$ be given by (1.1), (1.2) (if no such $l$ exists, we naturally put $l_\varepsilon(D) \overset{\text{def}}{=} 0$). The main result of this paper is the following theorem.

**Theorem 2.1.** For every Boolean predicate $D: \{0, 1, \ldots, n\} \rightarrow \{0, 1\}$ we have

$$\Omega(\sqrt{n l_0(D)} + l_1(D)) \leq Q^*(f_{n,D}) \leq Q(f_{n,D}) \leq O((\sqrt{n l_0(D)} + l_1(D)) \log n).$$

Let $\text{DISJ}_n(x, y) \overset{\text{def}}{=} x \cap y = \varnothing$.

**Corollary 2.2.** $Q^*(\text{DISJ}_n) \geq \Omega(\sqrt{n})$.

Our proof of the lower bound essentially uses the high symmetry of the predicate $f_{n,D}$. In particular, we need $x, y$ to be of the same fixed cardinality $k$. We formulate the corresponding intermediate result since, although somewhat technical, it might still be of independent interest.

Take $k \leq n$ and $D: \{0, 1, \ldots, k\} \rightarrow \{0, 1\}$. Let $X = Y \overset{\text{def}}{=} [n]^k$ be the set of all $k$-element subsets of $[n]$, and $f_{n,k,D}: X \times Y \rightarrow \{0, 1\}$, $f_{n,k,D}(x, y) \overset{\text{def}}{=} D(\{x \cap y\})$. (Thus, $f_{n,D} = f_{n,n,D}$.)
Theorem 2.3. Suppose that $k \leq n/4$, $l \leq k/4$, and let $D: \{0, 1, \ldots, k\} \to \{0, 1\}$ be any predicate such that $D(l) \neq D(l-1)$. Then $Q^*(f_{n,k,D}) \geq \Omega(\sqrt{kl})$.

Remark 2.4. In a personal communication, Nayak and Shi have observed that Theorems 2.1, 2.3 can be extended to a more general model where the entanglement need not necessarily be given in the form of shared Einstein–Podolski–Rosen pairs. More precisely, the input vector of this model (which was considered, for example, in [21]) is given by

$$\text{Input}(x, y) \overset{\text{def}}{=} \sum_{e \in E} \lambda_e |0, x, e\rangle |0\rangle |e, y, 0\rangle,$$  \hspace{1cm} (2.3)

where $\{\lambda_e \mid e \in E\}$ is an arbitrary unitary vector. (The case (2.2) of Einstein–Podolski–Rosen pairs corresponds to the vector $\lambda_e = |E|^{1/2}$. By kind permission of A. Nayak and Ya. Shi, the adjustments to our basic proof needed for this generalization are included in §5.1 (see Remark 5.6).

§3. Preliminaries

In this section we compile some definitions and previously known results needed in our proof.

3.1. Quantum search versus quantum communication. A precise definition of a quantum decision tree can be found, for example, in [6]. Given a Boolean function $g(x_1, \ldots, x_n)$, we denote by $Q_{DT}(g)$ the minimal number of queries needed to compute $g$ by a quantum decision tree with error at most $1/3$ at any input $x \in \{0, 1\}^n$.

We denote by $f_g: \mathcal{P}([n]) \times \mathcal{P}([n]) \to \{0, 1\}$ the predicate $f_g(x, y) \overset{\text{def}}{=} g(x \cap y)$, where $x \cap y$ is identified with its characteristic function.

Proposition 3.1 [3]. For any Boolean function $g(x_1, \ldots, x_n)$ we have $Q(f_g) \leq O(Q_{DT}(g) \log n)$.

3.2. Matrix norms. All the material in this subsection is classical and can be found, for example, in the textbook [5].

If we discard the Dirac notation (see §5.2), then all vectors will be represented as columns. The conjugate transpose of a complex vector $\xi$ (resp. complex matrix $A$) is denoted by $x^* \overset{\text{def}}{=} (x)^\top$ (resp. $A^* \overset{\text{def}}{=} (A)^\top$). Let $||\xi|| \overset{\text{def}}{=} (\xi^* \xi)^{1/2}$ be the $l_2$-norm of $\xi$. For a complex matrix $A$ we define the operator norm $||A||$ by $||A|| \overset{\text{def}}{=} \max\{||Ax|| : ||x|| \leq 1\}$. Alternatively, $||A|| = \max\{||\eta^\top A\xi|| : ||\eta||, ||\xi|| \leq 1\}$.

Given two complex matrices $A, B$ of the same size $m \times n$, we denote by $(A, B)$ their entrywise scalar product, that is,

$$(A, B) \overset{\text{def}}{=} \text{Tr}(A^* B) = \sum_{i=1}^m \sum_{j=1}^n \bar{a}_{ij} b_{ij}.$$  

Let $||A||_F$ be the Frobenius norm corresponding to this scalar product, that is,

$$||A||_F \overset{\text{def}}{=} \left(\sum_{i=1}^m \sum_{j=1}^n |a_{ij}|^2\right)^{1/2}.$$
We also use the trace norm, which is given by
\[ \|A\|_{\text{tr}} \overset{\text{def}}{=} \max_B \{|\langle A, B \rangle| : \|B\| \leq 1\}, \]
where \( B \) runs over all (complex) matrices of the same size as \( A \).

The following proposition summarizes some properties of these norms.

**Proposition 3.2.** 1. Let \( \| \cdot \| \) be any of the norms \( \| \cdot \|, \| \cdot \|_F, \| \cdot \|_{\text{tr}} \). Let \( A \) be a complex \((m \times n)\)-matrix. Then the following assertions hold.
   
   (a) \( \|A^*\| = \|A\| \).
   
   (b) If \( B \) is a submatrix of \( A \), then \( \|B\| \leq \|A\| \).
   
   (c) \( \| \cdot \| \) is invariant under left and right unitary transformations. In other words, \( \|UAV\| = \|A\| \) for every unitary \((m \times m)\)-matrix \( U \) and every unitary \((n \times n)\)-matrix \( V \).

2. Now let \( B \) be another complex \((n \times k)\)-matrix, and \( AB \) the usual matrix multiplication. Then the following assertions hold.
   
   (a) \( \|AB\| \leq \|A\| \cdot \|B\| \).
   
   (b) \( \|AB\|_{\text{tr}} \leq \|A\|_F \cdot \|B\|_F \) (Hölder’s inequality; see, for example, [5], Corollary IV.2.6).

3. \( \|A\| \leq \|A\|_F \leq (\min\{m, n\})^{1/2} \cdot \|A\| \).

4. For every \((n \times n)\)-matrix \( A \) we have \( \|A\|_{\text{tr}} \geq \sum_{i=1}^n |a_{ii}| \).

**Remark 3.3.** Let \( \sigma_1(A) \geq \sigma_2(A) \geq \cdots \geq \sigma_p(A) \) be the singular values of \( A \), where \( p = \min\{m, n\} \). Then \( \|A\| = \sigma_1(A), \|A\|_F = (\sum_{i=1}^p \sigma_i^2(A))^{1/2} \), and \( \|A\|_{\text{tr}} = \sum_{i=1}^p \sigma_i(A) \). Combined with Proposition 3.2.1(c) and the theorem on singular value decomposition, this yields all non-trivial parts of Proposition 3.2. However, the singular value characterization is not used in our proof.

**Remark 3.4.** Assertion 1(c) of Proposition 3.2 also implies that we can speak unambiguously of the operator, Frobenius, or trace norm of an operator from one (finite-dimensional) Hilbert space to another.

We shall also use the \( l_1 \)-norm and \( l_\infty \)-norm, which are defined entrywise:
\[ l_1(A) \overset{\text{def}}{=} \sum_{1 \leq i \leq m} \sum_{1 \leq j \leq n} |a_{ij}|, \]
\[ l_\infty(A) \overset{\text{def}}{=} \max_{1 \leq i \leq m} \max_{1 \leq j \leq n} |a_{ij}|. \]

Of course, these norms are not invariant under unitary transformations. However, they are related to unitary invariant norms by the following (obvious) observation:
\[ |\langle A, B \rangle| \leq l_1(A) \cdot l_\infty(B). \]

3.3. Decomposition of quantum communication protocols.

**Proposition 3.5** (see [26], [17]). Let \( P \) be a quantum communication protocol of length \( c \), and let \( U_p \) be the unitary operator appearing in the right-hand side of (2.1).
Then there are linear operators $A_u$ on $H_A$ and $B_u$ on $H_B$ ($u \in \{0, 1\}^c$) such that the following decomposition holds for all vectors $a \in H_A$, $b \in H_B$:

$$U_p(|a\rangle|0\rangle|b\rangle) = \sum_{u \in \{0, 1\}^c} |A_u(a)|u_c\rangle|B_u(b)\rangle.$$  

Moreover, $\|A_u\|, \|B_u\| \leq 1$ for every $u \in \{0, 1\}^c$.

**Proof.** Only the last observation (on the operator norms) is apparently new. However, it is an immediate corollary of Proposition 3.2, 2(a) and the fact that $A_u, B_u$ are composites of unitary operators and orthogonal projections onto the subspaces $H_A \otimes |\epsilon\rangle \otimes H_B$, $\epsilon \in \{0, 1\}$.

### 3.4. Symmetric functions and predicates.

Given a Boolean predicate $D: \{0, 1, \ldots, n\} \rightarrow \{0, 1\}$, we denote by $\text{deg}(D)$ its approximate degree, which is defined as the minimal degree of a real polynomial $f(x)$ in one variable such that $|f(s) - D(s)| \leq 1/3$ for every $s \in \{0, 1, \ldots, n\}$. We define a symmetric Boolean function $g_D(x_1, \ldots, x_n)$ by

$$g_D(x) \overset{\text{def}}{=} D\left(\sum_{i=1}^{n} x_i\right)$$

(note that $f_{n,D}(x, y) = f_{g_D}(x, y)$). As observed in [20], we have $\widetilde{\text{deg}}(D) = \widetilde{\text{deg}}(g_D)$, where $\text{deg}(g)$ is the minimal degree of a real polynomial in $n$ variables that approximates $g$ in the $l_\infty$-norm on $\{0, 1\}^n$ within accuracy $1/3$.

**Proposition 3.6** [22]. $\widetilde{\text{deg}}(D) = \theta(\sqrt{n}\sqrt{l_0(D) + l_1(D)})$.

It is proved in [2] that $\Omega(\text{deg}(g))$ is a general lower bound on $Q_{DT}(g)$. As established in the same paper, this lower bound is tight for symmetric functions.

**Proposition 3.7** [2]. $Q_{DT}(g_D) \leq O(\widetilde{\text{deg}}(D))$.

We now assume that $X = Y \overset{\text{def}}{=} [n]^k$. For $0 \leq s \leq k$ let $J_{n,k,s}$ be the following $(0, 1)$-matrix of size $\binom{n}{k} \times \binom{n}{s}$, whose rows and columns are indexed by elements of $[n]^k$:

$$(J_{n,k,s})_{xy} \overset{\text{def}}{=} \begin{cases} 1 & \text{if } |x \cap y| = s, \\ 0 & \text{otherwise}. \end{cases}$$

The spectrum of these matrices is described by the so-called Hahn polynomials (see, for example, [11]). Being classical objects, these polynomials have been rediscovered many times in different contexts. Knuth [16] proposed the expression which is the most convenient for our purposes. Remarkably, it is based on a direct computation of eigenvalues.

**Proposition 3.8** [16]. Suppose that $k \leq n/2$. Then the matrices $J_{n,k,s}$ with $0 \leq s \leq k$ share the same eigenspaces $E_0, E_1, \ldots, E_k$. The eigenvalue of $J_{n,k,s}$ corresponding to the eigenspace $E_t$ is given by

$$\sum_{i=\max\{0, s+t-k\}}^{\min\{s,t\}} (-1)^{t-i} \binom{t}{i} \binom{k-i}{s-i} \binom{n-k-t+i}{k-s-t+i}.$$
§ 4. The upper bound

In this section we show that the upper bound

\[ Q(f_{n,D}) \leq O((\sqrt{nl_0(D)} + l_1(D)) \log n) \]

in Theorem 2.1 follows almost immediately from the known results cited in § 3.

Let \( D : \{0,1,\ldots,n\} \rightarrow \{0,1\} \) be any predicate. By definition, \( D \) is constant on the interval \( [l_0(D), n - l_1(D)] \). Negating \( D \) if necessary, we can assume without loss of generality that \( D \) is equal to 0 on this interval. Then \( D = D_0 \lor D_1 \), where \( D_0^{-1}(1) \subseteq [0, l_0(D) - 1] \) and \( D_1^{-1}(1) \subseteq [n - l_1(D) + 1, n] \). We also have \( f_D = f_{D_0} \lor f_{D_1} \), that is, Alice and Bob compute \( f_{D_0} \) and \( f_{D_1} \) separately.

To compute \( f_{D_0} \), they apply the BCW-reduction (Proposition 3.1) and Propositions 3.7, 3.6:

\[ Q(f_{D_0}) \leq O(Q_D(g_{D_0}) \log n) \leq O(\deg(D_0) \log n) \leq O(\sqrt{nl_0(D)} \log n). \]

To compute \( f_{D_1} \), Alice and Bob use the following trivial (classical) protocol. Alice first checks whether \( |x| \leq n - l_1(D) \). If \( |x| \leq n - l_1(D) \), then \( f_{D_1}(x,y) = 0 \), and Alice declares the result. Otherwise she sends the entire input \( x \) to Bob. This requires at most \( \log_2 \left( \sum_{k=n-l_1(D)+1}^{n} \binom{n}{k} \right) \) bits, which is \( O(l_1(D) \log n) \) since \( l_1(D) \leq n/2 \). Then Bob computes \( f_{D_1}(x,y) \).

§ 5. The lower bounds

In this section we prove the lower bounds in Theorems 2.1 and 2.3. Using a straightforward reduction, we first show that the latter implies the former.

**Definition 5.1.** Given a Boolean predicate \( D \) on \( \{0,1,\ldots,n\} \) and an integer \( 0 \leq r \leq n \), we define a predicate \( D - r : \{0,1,\ldots,n - r\} \rightarrow \{0,1\} \) by \( (D - r)(s) \equiv D(r + s) \). Also let \( D|_k \) be the restriction of \( D \) to \( \{0,1,\ldots,k\} \), \( k \leq n \).

**Lemma 5.2.** Suppose that \( D \) is a predicate on \( \{0,1,\ldots,n\} \), and integers \( k, r \) satisfy \( 0 \leq r \leq n \), \( k \leq n - r \). Then \( Q^*(f_{n,D}) \geq Q^*(f_{n-r,k,(D-r)|_k}) \).

**Proof.** Alice and Bob use the optimal protocol for \( f_{n,D} : \mathcal{P}(\{n\}) \times \mathcal{P}(\{n\}) \rightarrow \{0,1\} \) to compute \( f_{n-r,k,(D-r)|_k} : [n - r]^k \times [n - r]^k \rightarrow \{0,1\} \). To do this, they simply map their inputs \( x, y \in [n - r]^k \) to the inputs \( \phi(x), \phi(y) \in \mathcal{P}(\{n\}) \) by the map \( \phi(x) \equiv x \cup \{n - r + 1, \ldots, n\} \) and feed \( \phi(x), \phi(y) \) into the protocol for \( f_{n,D} \).

**Proof of the lower bound in Theorem 2.1 assuming Theorem 2.3.** We must establish two separate bounds: \( Q^*(f_{n,D}) \geq \Omega(\sqrt{nl_0(D)}) \) and \( Q^*(f_{n,D}) \geq \Omega(l_1(D)) \). Their proofs use the reduction described in Lemma 5.2 (with different \( r, k \)). The parameters \( r, k \) must satisfy the conditions

\[ k \leq (n - r)/4, \quad (l - r) \leq k/4 \quad (5.1) \]

(arising from the hypotheses of Theorem 2.3), where \( l \equiv l_0(D) \) for the first bound and \( l \equiv n - l_1(D) \) for the second. If these conditions hold, then Theorem 2.3 implies that \( Q^*(f_{n,D}) \geq \Omega(\sqrt{rl_1(D)} (l - r)) \).
If $l \leq n/16$ (and, in particular, $l = l_0(D)$), we simply put $r \overset{\text{def}}{=} 0$ and $k \overset{\text{def}}{=} n/4$. Then the bound of Theorem 2.3 becomes $\Omega(\sqrt{n}l)$, as required.

If $l \geq n/16$, then we put $r \overset{\text{def}}{=} \frac{\log l}{16l}$ and $k \overset{\text{def}}{=} \frac{1}{l}(n - l)$, and the conditions (5.1) hold with equality. Then $l - r \geq \Omega(n - l)$, and Theorem 2.3 again yields the required bound $Q^*(f_n, D) \geq \Omega(n - l)$.

In the rest of the paper we prove Theorem 2.3. The proof splits into three fairly independent blocks.

### 5.1. A lower bound in terms of the approximate trace norm.

**Definition 5.3.** The $\epsilon$-approximate trace norm of a real matrix $M$ is defined by

$$
\|M\|_{\text{tr}}^{\epsilon} \overset{\text{def}}{=} \min\{\|P\|_{\text{tr}} : l_{\infty}(M - P) \leq \epsilon\},
$$

where $P$ runs over all real matrices of the same size as $M$.

**Definition 5.4.** For a predicate $f : X \times Y \rightarrow \{0, 1\}$, let $M_f$ be its communication $(0, 1)$-matrix ($M_f)_{xy} \overset{\text{def}}{=} f(x, y)$.

**Theorem 5.5.** For any predicate $f : X \times Y \rightarrow \{0, 1\}$ with $|X| = |Y| = N$ and any $\epsilon > 0$ we have $Q^*_\epsilon(f) \geq \Omega(\log(\|M_f\|_{\text{tr}}^{\epsilon}/N))$.

**Proof.** We fix a communication protocol of length $c$ with prior entanglement computing $f$ with probability $\epsilon$. Let $p_{xy}$ be the acceptance probability of this protocol on the input $(x, y)$. We arrange these into an $(N \times N)$-matrix $P$. Then clearly $l_{\infty}(M_f - P) \leq \epsilon$, and it remains to prove that $\|P\|_{\text{tr}} \leq N \exp(O(c))$.

We apply the decomposition in Proposition 3.5 to the input string (2.2). We get

$$
\text{Output}(x, y) = \frac{1}{|E|^{1/2}} \sum_{e \in E} \sum_{u \in \{0, 1\}^c} A_u|0, x, e\rangle|u_c\rangle B_u|e, y, 0\rangle,
$$

and then

$$
p_{xy} = \frac{1}{|E|} \left\| \sum_{e \in E} \sum_{u \in \Pi} A_u|0, x, e\rangle B_u|e, y, 0\rangle \right\|^2
= \frac{1}{|E|} \sum_{e, f \in E} \sum_{u, v \in \Pi} \langle (f, x, 0|A_v|A_u|0, x, e\rangle \cdot (f, y, 0|B_u|B_v|0, y, e\rangle),
$$

where $\Pi \overset{\text{def}}{=} \{u \in \{0, 1\}^c | u_c = 1\}$.

We define $N \times (|E|^2 \times |\Pi|^2)$-matrices $A, B$ by $a_{x, (e|f|uv)} \overset{\text{def}}{=} \langle f, x, 0|A_v|A_u|0, x, e\rangle$ and $b_{y, (e|f|uv)} \overset{\text{def}}{=} \langle f, y, 0|B_u|B_v|0, y, e\rangle$. Then $P = \frac{1}{|E|} AB^\dagger$, and Proposition 3.2, 2(b) implies that

$$
\|P\|_{\text{tr}} \leq \frac{1}{|E|} \|A\|_F \|B\|_F.
$$

To estimate $\|A\|_F$ and $\|B\|_F$, we divide these matrices into $N|\Pi|^2$ blocks and interpret every block as a $|E| \times |E|$-matrix. More precisely, for any fixed $x \in X$
and \( u, v \in \Pi \) we denote by \( A^{xuv} \) the square \( |E| \times |E| \)-matrix given by \( a_{ef}^{xuv} \triangleq a_{x,(e|fuv)} = \langle f, x, 0|A_v|A_u|0, x, e \rangle \). Then

\[
\|A\|_F^2 \leq N|\Pi|^2 \max_{x,u,v} \|A^{xuv}\|_F^2. \tag{5.3}
\]

To estimate \( \|A^{xuv}\|_F \), we first use assertion 3 of Proposition 3.2:

\[
\|A^{xuv}\|_F \leq |E|^{1/2} \|A^{xuv}\|. \tag{5.4}
\]

We finally claim that \( \|A^{xuv}\| \leq 1 \). \( \tag{5.5} \)

Indeed, let \( \eta, \xi \) be any vectors of length \( |E| \) with \( \|\eta\|, \|\xi\| \leq 1 \). Then

\[
\eta^\top A^{xuv} \xi = \left\langle \sum_{f \in E} \eta_f f, x, 0|A_v|A_u|0, x, \sum_{e \in E} \xi_e e \right\rangle
\]

and, since \( \|A_u\|, \|A_v\| \leq 1 \), we have

\[
\|\eta^\top A^{xuv} \xi\| \leq \left\| A_u|0, x, \sum_{e \in E} \xi_e e \rangle \right\| \left\| A_u|0, x, \sum_{f \in E} \eta_f f \right\|
\leq \left\| 0, x, \sum_{e \in E} \xi_e e \rangle \right\| \left\| 0, x, \sum_{f \in E} \eta_f f \rangle \right\| = \|\xi\| \|\eta\| \leq 1.
\]

This proves (5.5). Together with (5.4) and (5.3), this inequality yields that \( \|A\|_F \leq N^{1/2}|\Pi| |E|^{1/2} \), and the same bound holds for \( \|B\|_F \). Substituting these into (5.2), we get \( \|P\|_F \leq N|\Pi|^2 \leq N \exp(O(c)) \), which completes the proof of Theorem 5.5.

**Remark 5.6** (Nayak, Shi). Theorem 5.5 (together with all the lower bounds obtained as its corollaries) extends to the case of a more general entanglement where the input vector is given by (2.3). To see this, we begin with the following generalization of the second inequality in Proposition 3.2, 3:

\[
\|LA\|_F \leq \|L\|_F \|A\|. \tag{5.6}
\]

(The original statement corresponds to \( L = I_{\min\{m,n\}} \).) If \( \hat{a}_{x,(e|fuv)} \triangleq \lambda_e a_{x,(e|fuv)} \) and \( \hat{b}_{y,(e|fuv)} \triangleq \lambda_f b_{y,(e|fuv)} \), then \( \hat{P} = \hat{A}\hat{B}^\top \), where \( \hat{P} \) is the matrix of acceptance probabilities with respect to the input vector (2.3), and \( \|\hat{P}\|_F \leq \|\hat{A}\| \|\hat{B}\|_F \). As before, \( \|\hat{A}\|_F^2 \leq N|\Pi|^2 \max_{x,u,v} \|\hat{A}^{xuv}\|_F^2 \). However, we know that \( \hat{A}^{xuv} = LA^{xuv} \), where \( L \) is the diagonal matrix with elements \( \{\lambda_e | e \in E\} \). Since the vector \( \lambda \) is unitary, we have \( \|L\|_F = 1 \), and (5.6) implies that \( \|\hat{A}^{xuv}\|_F \leq \|\hat{A}^{xuv}\| \leq 1 \). The remaining calculations are as in the original proof.
5.2. The multi-dimensional discrepancy bound. This subsection is central to our argument, so we begin with a brief overview of the usual (one-dimensional) discrepancy bound.

Suppose that we want to get a lower bound for the approximate trace norm (or any other approximate norm) of a matrix $M$. In other words, we want to rule out the existence of a decomposition $M = P + \Delta$, where $\|P\|_{\text{tr}}$ and $l_\infty(\Delta)$ are small. The usual discrepancy method [26], [17] proceeds as follows. We assume for simplicity that $M$ is a $(\pm 1)$-matrix, take any probability distribution $\mu$ on its entries, and form the Hadamard product $M \circ \mu$ $(\{(M \circ \mu)_{ij} \equiv M_{ij}\mu_{ij}\})$. Then $\langle M, M \circ \mu \rangle = 1$ and $\|\langle \Delta, M \circ \mu \rangle\| \leq l_1(M \circ \mu) \cdot l_\infty(\Delta) = l_\infty(\Delta)$. Therefore, if $\|\langle P, M \circ \mu \rangle\|$ is small for every matrix $P$ with small trace norm (in other words, if $M \circ \mu$ has low discrepancy relative to such matrices), then we are done.

The next logical step was taken by Klauk ([14], Theorem 4), who observed that the “testmatrix” need not be of the particular form $M$. However, our application requires that $\lambda_1(\mu) = 1$ and of low discrepancy, we can still establish the desired lower bound for all matrices $M$ such that $\langle \langle M, \mu \rangle \rangle$ is sufficiently large.

However, it is well known that even this generalized form of the discrepancy method does not work for the disjointness predicate. In this paper we take it one step further and, instead of considering the linear functional $X \mapsto \langle X, \mu \rangle$ for a single “test matrix” $\mu$, we consider the multi-dimensional “trace operator” $X \mapsto \langle \langle X, \mu_1 \rangle, \ldots, \langle X, \mu_r \rangle \rangle$ for a family of matrices $\mu_1, \ldots, \mu_r$, with $l_1(\mu_s) \leq 1$. To be able to apply spectral methods, we assume that $\mu_1, \ldots, \mu_r$ are real symmetric commuting matrices (although it would be sufficient to assume that they have singular value decompositions $U \lambda_1 V, \ldots, U \lambda_r V$ with common unitary matrices $U, V$).

**Definition 5.7.** An $r$-dimensional discrepancy test consists of real symmetric matrices $\mu_1, \ldots, \mu_r$ with $l_1(\mu_s) \leq 1$ (1 $\leq s \leq r$) that have the same size $N \times N$ and commute with each other, along with an orthogonal decomposition

$$\mathbb{R}^N = E_1 \oplus E_2 \oplus \cdots \oplus E_k$$

of $\mathbb{R}^N$ into their common eigenspaces $E_1, E_2, \ldots, E_k$.

We note that commutativity alone yields the existence of at least one decomposition (5.7). However, our application requires that $k \ll N$ (that is, the eigenvalues of $\mu_s$ must substantially repeat themselves). Therefore we prefer to fix the decomposition explicitly in the definition.

Given a discrepancy test $(\mu_1, \ldots, \mu_r, E_1, \ldots, E_k)$, we denote by $\lambda_{st}$ the eigenvalue of $\mu_s$ corresponding to the eigenspace $E_t$. The trace of $E_t$ is the $r$-dimensional vector $\lambda' \equiv \{\lambda'_{st} \equiv \lambda_{st} \in \mathbb{R}_+^r \ | \ 1 \leq t \leq k\}$ be the set of all such vectors.

**Definition 5.8.** Given a set $T \subseteq \mathbb{R}^r$ of vectors and $C > 0$, we denote by $\text{Conv}_C(T) \equiv \{\sum_{\lambda \in T} a_\lambda \lambda : \sum_{\lambda \in T} |a_\lambda| \leq C\}$ the convex hull of the segments $\{[-C, C] \lambda : \lambda \in T\}$. Given another vector $\xi \in \mathbb{R}^r$ in the same space and $\varepsilon > 0$, we put $\phi^\varepsilon(\xi, T) \equiv \min\{C \ | \ \rho_\infty(\xi, \text{Conv}_C(T)) \leq \varepsilon\}$, where $\rho_\infty$ is the distance in the $l_\infty$-norm.
Theorem 5.9. Let $M$ be a real square matrix, and $(\mu_1, \ldots, \mu_r, E_1, \ldots, E_k)$ an arbitrary $r$-dimensional test of the same size. We define $\xi_M \in \mathbb{R}^r$ by $(\xi_M)_s \triangleq \langle M, \mu_s \rangle$. Then

$$\|M\|_{\text{tr}}^c \geq \phi^c(\xi_M, \text{Trace}(\bar{\mu}, \mathcal{E})).$$

Proof. We put $\|M\|_{\text{tr}}^c = C$ and fix a decomposition $M = P + \Delta$, where $\|P\|_{\text{tr}} = C$ and $l_\infty(\Delta) \leq \varepsilon$. Then $\xi_M = \xi_P + \xi_\Delta$ and, moreover, $\|\xi_\Delta\| = \|\Delta, \mu_s\| \leq l_1(\mu_s)l_\infty(\Delta) \leq \varepsilon$ for every $s \in [r]$, whence $l_\infty(\xi_\Delta) \leq \varepsilon$. Thus it remains to show that $\xi_P \in \text{Conv}_C(\text{Trace}(\bar{\mu}, \mathcal{E}))$.

Let $U$ be an orthogonal matrix corresponding to the decomposition (5.7) such that all $(U^T \mu_s U)$ are diagonal. We consider the matrix $(U^T P U)$. For every $t \in [k]$ let $(U^T P U)_t$ be its principal submatrix corresponding to the eigenspace $E_t$. We put $a_t \equiv \text{Tr}((U^T P U)_t)$. Then the required property $\xi_P \in \text{Conv}_C(\text{Trace}(\bar{\mu}, \mathcal{E}))$ is a corollary of the following two facts:

$$\xi_P = \sum_{t=1}^{k} a_t \lambda_t^t$$

and

$$\sum_{t=1}^{k} |a_t| \leq C.$$ 

These facts are proved by easy matrix manipulations and estimates which make essential use of Proposition 3.2:

$$(\xi_P)_s = \langle P, \mu_s \rangle = \langle (U^T P U), (U^T \mu_s U) \rangle = \sum_{t=1}^{k} \text{Tr}((U^T P U)_t) \lambda_{st} = \sum_{t=1}^{k} a_t \lambda_{st}$$

and

$$\sum_{t=1}^{k} |a_t| \leq \sum_{i=1}^{N} |(U^T P U)_{i,i}| \leq \|(U^T P U)\|_{\text{tr}} = \|P\|_{\text{tr}} = C.$$ 

5.3. Completion of the proof of Theorem 2.3. We fix integers $n$ and $k \leq n/4$ and put $N \triangleq \binom{n}{k}$. Let $D: \{0, 1, \ldots, k\} \rightarrow \{0, 1\}$ be any predicate such that $D(l) \neq D(l-1)$ for some $l \leq k/4$. Applying Theorem 5.5 (and observing that the error probability can always be reduced from $1/3$ to $1/4$ with an increase in complexity by at most a constant factor), we get

$$Q^*(f_{n,k,D}) \geq \Omega(\log(\|M_{f_{n,k,D}}\|_{\text{tr}}^{1/4}/N)).$$

We now put $\mu_s \triangleq N^{-1}(k)^{-1}(n-k)^{-1}J_{n,k,s}$ and denote by $E_0, \ldots, E_k$ the common eigenspaces of these matrices as described in Proposition 3.8. We note that $l_1(\mu_s) = 1$ and $(M_{f_{n,k,D}}, \mu_s) = D(s)$. Applying Theorem 5.9 to the $(k/2 + 1)$-dimensional test $(\mu_0, \mu_1, \ldots, \mu_{k/2}, E_0, E_1, \ldots, E_k)$, we get

$$\|M_{f_{n,k,D}}\|_{\text{tr}}^{1/4} \geq \phi^{1/4}(D|_{k/2}, \text{Trace}(\bar{\mu}, \mathcal{E})).$$

(5.9)
Claim 5.10. Let $\lambda_{st}$ be the eigenvalue of the matrix $\mu_s$ corresponding to the eigenspace $E_t$. Then we have
1) $\lambda_{st} = F_t(s)$, where $F_t$ is a polynomial of degree $t$, which coincides with the Hahn polynomial up to a normalizing factor,
2) $|\lambda_{st}| \leq N^{-1} \exp(-\Omega(t))$ whenever $k \leq n/4$ and $s \leq k/2$.

Proof. By Proposition 3.8,

$$\lambda_{st} = N^{-1} \binom{k}{s}^{-1} \binom{n-k}{k-s}^{-1} \sum_{i=\max\{0, s+t-k\}}^{\min\{s,t\}} (-1)^{t-i} \binom{t}{i} \binom{k-i}{s-i} \binom{n-k-t+i}{k-s-t+i}.$$

Part 1) is already obvious from this expression. Part 2) is also easy:

$$|\lambda_{st}| \leq N^{-1} \sum_{i=0}^{t} \left( \frac{t}{i} \frac{s(s-1)\ldots(s-i+1)}{k(k-1)\ldots(k-i+1)} \frac{(k-s)(k-s-1)\ldots(k-s-t+i+1)}{(n-k)(n-k-1)\ldots(n-k-t+i+1)} \right).$$

This claim implies that for every $t_0 \leq k$ we have $\{\lambda^t \mid t \leq t_0\} \subseteq P(t_0)$, where $P(t_0)$ is the set of all real-valued functions on $\{0, 1, \ldots, k/2\}$ that are representable by (real) polynomials of degree $\leq t_0$. But $t_\infty(\lambda^t) \leq N^{-1} \exp(-\Omega(t_0))$ for all $t \geq t_0$. Hence,

$$\forall \xi \in \text{Conv}_C(\text{Trace}(\hat{\mu}, E)) \quad \rho_\infty(\xi, P(t_0)) \leq N^{-1} C \exp(-\Omega(t_0)). \quad (5.10)$$

We now put $t_0 \overset{\text{def}}{=} \deg(D|_{k/2}) - 1$ and $C \overset{\text{def}}{=} \phi^{1/4}(D|_{k/2}, \text{Trace}(\hat{\mu}, E))$. Since $l \leq k/4$, it follows by Proposition 3.6 that

$$t_0 \geq \Omega(\sqrt{kl}). \quad (5.11)$$
Also, \( \rho_\infty(D|_{k/2}, P(t_0)) > 1/3 \) by definition of the approximate degree. On the other hand, (5.10) implies that
\[
\rho_\infty(D|_{k/2}, P(t_0)) \leq N^{-1}C\exp(-\Omega(t_0)) + \rho_\infty(D|_{k/2}, \text{Conv}_C(\text{Trace}(\mu, E))) \\
\leq N^{-1}C\exp(-\Omega(t_0)) + 1/4.
\]
Combining these two bounds with (5.11), we get
\[
\phi^{1/4}(D|_{k/2}, \text{Trace}(\mu, E)) = C \geq N\exp(\Omega(\sqrt{k\ell})).
\]
(5.12)

Theorem 2.3 now follows from (5.8), (5.9) and (5.12).

I am grateful to Andris Ambainis and Avi Wigderson for several useful discussions, to Noga Alon for pointing out the reference [16], to Hartmut Klauk for pointing out an omission in the first draft of this paper, and to Ashwin Nayak and Yaoyun Shi for their permission to include Remark 5.6.

**Bibliography**

[1] A. Ambainis, L. Schulman, A. Ta-Shma, V. Vazirani, and A. Wigderson, “The quantum communication complexity of sampling”, Proc. 39th IEEE Symposium on Foundations of Computer Science, IEEE Computer Society, Los Alamitos 1998, pp. 342–351.

[2] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf, “Quantum lower bounds by polynomials”, Proc. 39th IEEE Symposium on Foundations of Computer Science, IEEE Computer Society, Los Alamitos 1998, pp. 352–361; preliminary version available at quant-ph/9802049.

[3] H. Buhrman, R. Cleve, and A. Wigderson, “Quantum vs. classical communication and computation”, Proc. 30th ACM Symposium on the Theory of Computing, ACM Press, New York 1998, pp. 63–86; preliminary version available at quant-ph/9802040.

[4] L. Babai, P. Frankl, and J. Simon, “Complexity classes in communication complexity theory”, Proc. 27th IEEE Symposium on Foundations of Computer Science, IEEE Computer Society, Los Alamitos 1986, pp. 337–347.

[5] R. Bhatia, *Matrix analysis*, Graduate Texts in Math, vol. 169, Springer-Verlag, Berlin–New York 1997.

[6] H. Buhrman and R. de Wolf, “Complexity measures and decision tree complexity: a survey”, *Theoret. Comput. Sci.* 288 (2000), 21–43.

[7] H. Buhrman and R. de Wolf, “Communication complexity lower bounds by polynomials”, Proc. 16th IEEE Conference on Computational Complexity, IEEE Computer Society, Los Alamitos 2001, pp. 120–130; preliminary version available at cs.CC/9910010.

[8] R. Cleve and H. Buhrman, “Substituting quantum entanglement for communication”, *Phys. Rev. A* 56 (1997), 1201–1204; preliminary version available at quant-ph/9704026.

[9] R. Cleve, W. van Dam, M. Nielsen, and A. Tapp, “Quantum entanglement and the communication complexity of the inner product function”, Proc. of the 1st NASA QCQC Conference, Lecture Notes in Computer Science, vol. 1509, Springer-Verlag, New York–Berlin 1998, pp. 61–74; preliminary version available at quant-ph/9708019.

[10] B. Chor and O. Goldreich, “Unbiased bits from sources of weak randomness and probabilistic communication complexity”, *SIAM J. Comput.*, 17 (1988), 230–261.

[11] P. Delsarte, “Hahnpolynomials, discrete harmonics and t-designs”, *SIAM J. Appl. Math.* 34:1 (1978), 157–166.

[12] L. K. Grover, “A fast quantum mechanical algorithm for database search”, Proc. 28th ACM Symposium on the Theory of Computing, ACM Press, New York 1996, pp. 212–219; preliminary version available at quant-ph/9605043.
Quantum communication complexity of predicates

[13] P. Høyer and R. de Wolf, “Improved quantum communication complexity bounds for disjointness and equality”, Proc. 19th Annual Symposium on Theoretical Aspects of Computer Science, Lecture Notes in Computer Science, vol. 2607, Springer-Verlag, Berlin–New York 2002, pp. 299–310; preliminary version available at quant-ph/0109068.

[14] H. Klauck, “Lower bounds for quantum communication complexity”, Proc. 42nd IEEE Symposium on Foundations of Computer Science, IEEE Computer Society, Los Alamitos 2001, pp. 288–297; preliminary version available at quant-ph/0106160.

[15] H. Klauck, A. Nayak, A. Ta-Shma, and D. Zuckerman, “Interaction in quantum communication and the complexity of set disjointness”, Proc. 33rd ACM Symposium on the Theory of Computing, ACM Press, New York 2001, pp. 124–133.

[16] D. Knuth, Combinatorial matrices, Manuscript available at http://www-cs-faculty.stanford.edu/~knuth/preprints.html#unpub, 1991.

[17] I. Kremer, Quantum communication, Master’s thesis, Hebrew University, Jerusalem 1995.

[18] B. Kalyanasundaram and G. Schnitger, “The probabilistic communication complexity of set intersection”, SIAM J. Discrete Math. 5 (1992), 545–557.

[19] K. Mehlhorn and E. M. Schmidt, “Las Vegas is better than determinism in VLSI and distributive computing”, Proc. 14th ACM Symposium on the Theory of Computing, ACM Press, New York 1982, pp. 330–337.

[20] N. Nisan and M. Szegedy, “On the degree of Boolean functions as real polynomials”, Comput. Complexity 4 (1994), 301–313.

[21] A. Nayak and J. Salzman, “On communication over an entanglement-assisted quantum channel”, Proc. 34th ACM Symposium on the Theory of Computing, ACM Press, New York 2002.

[22] R. Paturi, “On the degree of polynomials that approximate symmetric Boolean functions”, Proc. 24th ACM Symposium on the Theory of Computing, ACM Press, New York 1992, pp. 468–474.

[23] A. Razborov, “On the distributional complexity of disjointness”, Theoret. Comput. Sci. 106 (1992), 385–390.

[24] U. Vazirani, “Towards a strong communication complexity theory of generating quasi-random sequences from two communicating slightly-random sources”, Combinatorica 7 (1987), 375–392.

[25] A. Yao, “Some complexity questions related to distributive computing”, Proc. 11th ACM Symposium on the Theory of Computing, ACM Press, New York 1979, pp. 209–213.

[26] A. Yao, “Quantum circuit complexity”, Proc. 34th IEEE Symposium on Foundations of Computer Science, IEEE Computer Society, Los Alamitos 1993, pp. 352–361.

Steklov Math. Institute of RAS

Received 29/APR/02
Translated by THE AUTHOR

Typeset by AMS-\TeX