# Quantum vs. Classical Communication and Computation

Harry Buhrman* CWI

Richard Cleve† University of Calgary

Avi Wigderson‡ Hebrew University


### Abstract

We present a simple and general simulation technique that transforms any black-box quantum algorithm (*à la* Grover's database search algorithm) to a quantum communication protocol for a related problem, in a way that fully exploits the quantum parallelism. This allows us to obtain new positive and negative results.

The positive results are novel quantum communication protocols that are built from nontrivial quantum algorithms via this simulation. These protocols, combined with (old and new) classical lower bounds, are shown to provide the first asymptotic separation results between the quantum and classical (probabilistic) two-party communication complexity models. In particular, we obtain a quadratic separation for the bounded-error model, and an exponential separation for the zero-error model.

The negative results transform known quantum communication lower bounds to computational lower bounds in the black-box model. In particular, we show that the quadratic speed-up achieved by Grover for the *OR* function is impossible for the *PARITY* function or the *MAJORITY* function in the bounded-error model, nor is it possible for the *OR* function itself in the exact case. This dichotomy naturally suggests a study of bounded-depth predicates (i.e. those in the polynomial hierarchy) between *OR* and *MAJORITY*. We present black-box algorithms that achieve near quadratic speed up for all such predicates.


*Research supported in part by the Dutch foundation for scientific research (NWO) by SION project 612-34-002, and by the European Union through NeuroCOLT ESPRIT Working Group Nr. 8556, and HC&M grant nr. ERB4050PL93-0516. Address: CWI, Quantum Computing and Advanced Systems Research, P.O. Box 94079, Amsterdam, The Netherlands. E-mail: `buhrman@cwi.nl`.

†Research supported in part by Canada's NSERC. Address: Department of Computer Science, University of Calgary, Calgary, Alberta, Canada T2N 1N4. E-mail: `cleve@cpsc.ucalgary.ca`.

‡Work partially supported by grant 032-7736 from the Israel Academy of Sciences. Part of this work was done during a visit to the Institute for Advanced Study, Princeton, supported by a Sloan Foundation grant number 96-6-2. Address: Hebrew University Jerusalem, Israel. E-mail: `avi@cs.huji.ac.il`.

## 1 Introduction and summary of results

We discuss our results about quantum communication complexity and quantum black-box algorithms in separate subsections. Regarding quantum communication complexity, Subsection 1.1 contains a background discussion and Subsection 1.2 states our results. Regarding quantum black-box algorithms, Subsection 1.3 contains a background discussion and Subsection 1.4 states our results. The results are all proven in Sections 2 and 3.

### 1.1 Quantum communication complexity

The recent book by Kushilevitz and Nisan [KN97] is an excellent text on communication complexity. As usual, two parties, Alice and Bob, wish to compute a boolean function on their $N$-bit inputs using a communication protocol. It will be convenient to let $N = 2^n$ and think of Alice and Bob's $N$-bit inputs as functions $f, g : \{0,1\}^n \to \{0,1\}$ (e.g., when $n = 2$, $f$ represents the four-bit string $f(00)f(01)f(10)f(11)$). Examples of well-studied communication problems are:

- Equality: *EQ*$(f,g) = \bigwedge_{x\in\{0,1\}^n}(f(x) = g(x))$
- Inner product: *IP*$(f,g) = \bigoplus_{x\in\{0,1\}^n}(f(x) \wedge g(x))$
- Disjointness[1]: *DISJ*$(f,g) = \bigvee_{x\in\{0,1\}^n}(f(x) \wedge g(x))$.

Classical communication protocols were defined by Yao [Ya79]. In an $m$-bit deterministic protocol, the players exchange $m$ (classical) bits according to their individual inputs and then decide on an answer, which must be correct. In an $m$-bit probabilistic protocol, the players are allowed to flip coins to decide their moves, but they still must exchange at most $m$ bits in any run. The answer becomes a random variable, and we demand that the answer be correct with probability at least $1-\varepsilon$ (for some $\varepsilon \geq 0$) for every input pair. Note that if $\varepsilon$ is set to 0 then probabilistic protocols are not more powerful than deterministic ones.

An alternative measure of the communication cost of a probabilistic protocol is to take the *expected* communication cost of a run, with respect to the outcomes of the coin flips (rather than the worst-case communication cost of a run). In this case, probabilistic protocols with error probability zero may be more powerful than deterministic protocols. Another alternate definition for probabilistic protocols is where the players share a random string. This model has been shown to have the same power as the above

[1] In fact this defines the *complement* of the set disjointness problem. Since for the models we study the communication complexity of *DISJ* and its complement are equal our results hold for both.

bounded-error model whenever the communication complexity is above $\log N$ [Ne91].

For a communication problem $P$, and $\varepsilon \geq 0$, let $C_\varepsilon(P)$ denote the minimum $m$ such that there is a (probabilistic) protocol that requires at most $m$ bits of communication and determines the correct answer with probability at least $1-\varepsilon$. Then $C_0(P)$ can be taken as the *deterministic* communication complexity of $P$ (sometimes denoted as $D(P)$). Also, let $C(P)$ denote $C_{1/3}(P)$, the *bounded-error* communication complexity of $P$. Clearly, $C(P) \leq C_0(P)$, and there are instances where there are exponential gaps between them. Furthermore, let $C_0^E(P)$ denote the minimum *expected* communication for probabilistic errorless protocols, frequently called the *zero-error* communication complexity. According to our definitions, $\frac{2}{3}C(P) \leq C_0^E(P) \leq C_0(P)$.

For the aforementioned problems, the following is known.

**Theorem 1.1:** *[Ya79] $C_0(EQ) = C_0^E(EQ) = N$, but $C(EQ) \in O(\log N)$.*

**Theorem 1.2:** *[CG88] $C(IP) \in \Omega(N)$.*

**Theorem 1.3:** *[KS87, Raz90] $C(DISJ) \in \Omega(N)$.*

Yao [Ya93] also introduced a *quantum* communication complexity model, where Alice and Bob are allowed to communicate with qubits rather than bits. It is not immediately clear whether using qubits can reduce communication because a fundamental result in quantum information theory by Holevo [Hol73] (see also [FC94]) implies that by sending $m$ qubits one cannot convey more than $m$ classical bits of information. Yao's motivation was to prove lower bounds on the size of particular kinds of quantum circuits that compute the *MAJORITY* function, and he accomplished this via a qubit communication complexity lower bound. The MSc thesis of Kremer [Kr95] includes several important definitions and basic results.

Denote by $Q_\varepsilon(P)$ the minimum $m$ for which there is a protocol for $P$ involving $m$ qubits of communication with error probability bounded by $\varepsilon$. Let $Q(P)$ denote $Q_{1/3}(P)$, the *bounded-error* communication complexity of $P$. Also, call $Q_0(P)$ the *exact* communication complexity of $P$. It turns out that one of the differences between the quantum scenario and the classical probabilistic scenario is that $Q_0(P)$ is not the same as the deterministic communication complexity of $P$ (see Theorem 1.7 below), whereas $C_0(P)$ is.

A basic result is that quantum protocols are at least as powerful as probabilistic ones.

**Fact 1.4:** *[Kr95] For every problem $P$ on $n$-bit inputs, $Q(P) \leq C(P)$ and $Q_0(P) \leq C_0(P)$.*

Kremer also presents the following lower bound (whose origin he attributes to Yao).

**Theorem 1.5:** *[Kr95] (see also [CDNT97]) $Q(IP) \in \Omega(N)$.*

Kremer leaves open the question of whether the quantum (qubit) model is ever more powerful than the classical bit model for any communication problem.

Cleve and Buhrman [CB97] (see also [BCD97]) showed the first example where quantum information reduces communication complexity. They considered a different model than that of Yao, the *entanglement* model, where the communication is restricted to classical bits; however, the parties have an *a priori* set of qubits in an entangled quantum state. As with the qubit model, there are no trivial communication advantages in the entanglement model, because a prior entanglement cannot reduce the communication cost of conveying $m$ bits. In this model, they demonstrated a three-party communication problem where the prior entanglement reduces the required communication complexity by one bit. Buhrman [Bu97] showed that, in this model, the separation between quantum vs. classical communication costs can be as large as $2n$ vs. $3n$. Also, van Dam, Høyer, and Tapp [DHT97] showed the first instance where the reduction in communication can be asymptotically large in a multi-party setting. They showed that, for a particular $k$-party scenario, the quantum vs. classical communication cost is roughly $k$ vs. $k \log k$ (note that this falls short of an asymptotic separation when the number of parties is fixed).

### 1.2 Our results in quantum communication complexity

We prove some asymptotic gap theorems between quantum and classical two-party communication. The first is a near quadratic gap for the bounded-error models (and also happens to be a near quadratic gap between $Q$ and $Q_0$).

**Theorem 1.6:** *$Q(DISJ) \in O(\sqrt{N}\log N)$ and $Q_0(DISJ) \in \Omega(N)$.*

This, combined with Theorem 1.3, results in a near quadratic separation between classical bounded-error communication complexity and quantum bounded-error communication complexity.

Our second theorem is an exponential gap between the exact quantum and the zero-error classical model. For this, we need to define a *partial* function. Let $\Delta(f,g)$ denote the hamming distance between the two functions $f, g$ (viewed as binary strings of length $N = 2^n$). Define the partial function $EQ'$ as

$$EQ'(f,g) = \begin{cases} 1 & \text{if } \Delta(f,g) = 0 \\ 0 & \text{if } \Delta(f,g) = 2^{n-1}. \end{cases}$$

For a partial function all communication definitions above extend in the natural way, demanding correct (or approximately correct) answers only for pairs on which the partial function is defined.

**Theorem 1.7:** *$Q_0(EQ') \in O(\log N)$, but $C_0(EQ'), C_0^E(EQ') \in \Omega(N)$.*

Finally, we generalize Theorem 1.6 to balanced, constant depth formulae.

**Theorem 1.8:** *Let $F$ be any balanced depth-$d$ $AC^0$ formula (i.e. formula with unbounded fan-in $\wedge$ and $\vee$ gates) with $N$ leaves, and $L : \{0,1\}^2 \rightarrow \{0,1\}$. Then the communication problem $P(f,g) = F(L(f,g))$ has complexity $O(\sqrt{N}\log^{d-1}(N))$.*

The classical lower bounds will appeal to known techniques and results in communication complexity and combinatorics. The quantum upper bounds will follow from a reduction from communication problems to computational problems where the input is given as a black-box, in conjunction with known quantum algorithms for these problems—and a new quantum algorithm in the case of Theorem 1.8. The reduction is presented in Theorem 2.1, Section 2. Applying this reduction in its reverse direction enables us to translate lower bounds for quantum communication problems into lower bounds for black-box computations.

### 1.3 Black-box quantum computations

All the upper bounds on communication complexity will come from a simulation of quantum circuits whose inputs are functions that can be queried as black-boxes. Relevant definitions (and some lower bound techniques) may be found in [BV93, BB94, BBBV97, Ya93].

For $f : \{0,1\}^n \to \{0,1\}$, define an *$f$-gate* as the unitary mapping such that

$$U_f : |x\rangle|y\rangle \mapsto |x\rangle|f(x) \oplus y\rangle, \quad (1)$$

for all $x \in \{0,1\}^n$, $y \in \{0,1\}$. For the initial state with $x \in \{0,1\}^n$ and $y = 0$, this mapping simply writes the value of $f(x)$ on the $n+1^{\text{st}}$ qubit; however, for this gate to make sense when evaluated in quantum superposition, it must also be defined for the $y = 1$ case as well as be reversible.

A *quantum circuit* (or *gate array*) $G$ with input given as a black-box operates as follows. It begins with a set of qubits in some initial state (say, $|0,\ldots,0\rangle$) and performs a sequence of unitary transformations to this state. These unitary transformations are from a designated set of "basis" operations (say, the set of all operations corresponding to "two-qubit gates"), as well as $f$-gates. At the end of the computation, the state is measured (in the *standard* basis, consisting of states of the form $|x_1,\ldots,x_m\rangle$, for $x_1,\ldots,x_m \in \{0,1\}$), and some designated bit (or set of bits) is taken as the *output*. Denote the output of $G$ on *input* $f$ as $G(f)$ (which is a random variable).

Let $\mathcal{H}$ be a collection of functions. We say that a quantum circuit $G$ *computes* a function $F : \mathcal{H} \to S$ *with error* $\varepsilon$ if, for every $h \in \mathcal{H}$, $\Pr[G(h) = F(h)] \geq 1 - \varepsilon$. We denote by $T_\varepsilon(F)$ the minimum $t$ (time, or, more accurately, number of black-box accesses) for which there is a quantum circuit that computes $F$ with error $\varepsilon$. We call $T_0(F)$ the *exact* quantum complexity of $F$, and we call $T(F) = T_{1/3}(F)$ the *bounded-error* quantum complexity of $F$.

Here are three well-known examples of nontrivial quantum algorithms (and precious few others are known). For these problems, classical (probabilistic) computations require $\Theta(2^n)$, $\Theta(\sqrt{2^n})$, and $\Theta(2^n)$ black-box queries (respectively) to achieve the same error probability as the quantum algorithm.

- **Half or None** Here $\mathcal{H}$ consists of the constant 0 function and all "balanced" functions (i.e. $h$'s which take on an equal number of 0s and 1s). The function *BAL* takes the value 1 if $h$ is balanced and 0 otherwise.

  **Theorem 1.9:** *[DJ92]* $T_0(\mathit{BAL}) = 1$.

- **Abelian Subgroups** Here $\mathcal{H}$ are all functions $h : \{0,1\}^n \to \{0,1\}$ for which there exists a subgroup $K$ of $Z_2^n$ (represented by $\{0,1\}^n$) such that $h(x) = h(y)$ iff $x + y \in K$. *STAB*$(h)$ is a specification of $K$.

  **Theorem 1.10:** *[Si97]* $T(\mathit{STAB}) \in O(n)$.

  This theorem has been generalized (appropriately) to other Abelian groups by Kitaev [Ki95].

- **Database Search** Here $\mathcal{H}$ contains *all* possible functions $h : \{0,1\}^n \to \{0,1\}$ and

  $$\mathit{OR}(f) = \bigvee_{x \in \{0,1\}^n} f(x).$$

  Based on a technique introduced by Grover and later refined by Boyer *et al.*, it is straightforward to construct a quantum algorithm that solves *OR* with the following efficiency.

  **Theorem 1.11:** *[Gr96, BBHT96]* $T(\mathit{OR}) \in O(\sqrt{2^n})$.

### 1.4 Our results about black-box quantum computations

Define

$$\mathit{PARITY}(f) = \bigoplus_{x \in \{0,1\}^n} f(x).$$

*PARITY* is at least as hard as *OR* (in the bounded-error case) by a result of Valiant and Vazirani [VV86]. In view of Theorem 1.11, it is natural to ask whether Grover's technique can somehow be adapted to solve *PARITY* with quadratic speedup—or at least to solve *PARITY* in $O((2^n)^r)$ steps for some $r < 1$. We show that this is not possible by the following.

**Theorem 1.12:** $T(\mathit{PARITY}) \in \Omega(2^n/n)$.

Also, define

$$\mathit{MAJORITY}(f) = \begin{cases} 1 & \text{if } \sum_{x \in \{0,1\}^n} f(x) > 2^{n-1} \\ 0 & \text{otherwise.} \end{cases}$$

**Theorem 1.13:** $T(\mathit{MAJORITY}) \in \Omega(2^n/n^2 \log(n))$.

Considering this dichotomy among Theorems 1.11 to 1.13, we investigate the bounded-depth predicates (i.e. the polynomial-time hierarchy). First, define *SIGMA*$_2$, on functions $f : \{0,1\}^n \to \{0,1\}$ as

$$\mathit{SIGMA}_2(f) = \bigvee_{x \in \{0,1\}^{n-m}} \left( \bigwedge_{y \in \{0,1\}^m} f(x_1,\ldots,x_{n-m},y_1,\ldots,y_m) \right) \quad (2)$$

(where $m \in \{0,\ldots,n\}$ is an implicit parameter of *SIGMA*$_2$). Let *PI*$_2$ be the negation of *SIGMA*$_2$. Both *PI*$_2$ and *SIGMA*$_2$ have classical complexity $\Theta(2^n)$. Is a near square root speed up possible for these problems? We shall show

**Theorem 1.14:** $T(\mathit{SIGMA}_2) \in O(\sqrt{2^n}\, n)$.

More generally, for the appropriate generalization to higher levels of the polynomial-hierarchy, define for $d$ alternations

$$\mathit{SIGMA}_d(f) = \bigvee_{x^{(1)} \in \{0,1\}^{m_1}} \left( \cdots \left( \bigwedge_{x^{(d)} \in \{0,1\}^{m_d}} f(x^{(1)},\ldots,x^{(d)}) \right) \cdots \right) \quad (3)$$

(where $m_1,\ldots,m_d$ are implicit parameters with $m_1 + m_2 + \cdots + m_d = n$), and *PI*$_d$ is the negation of *SIGMA*$_d$. Note that *SIGMA*$_1$ = *OR* and *PI*$_1$ is equivalent to *AND*.

**Theorem 1.15:** $T(\mathit{SIGMA}_d) \in O(\sqrt{2^n}\, n^{d-1})$ *and* $T(\mathit{PI}_d) \in O(\sqrt{2^n}\, n^{d-1})$.

This is a near square root speed up for any fixed value of $d$.

Moreover, if we are willing to settle for speed up by a root slightly worse that square, such as $O((2^n)^{1/2+\delta})$ steps (for some fixed $\delta > 0$), then the error probability can be *double exponentially* small!

**Theorem 1.16:** *For* $\varepsilon = 1/2^{2^{(n/\delta d)-1}}$, $T_\varepsilon(\mathit{SIGMA}_d) \in O((2^n)^{1/2+\delta})$.

Finally, in sharp contrast with Theorem 1.11 and Theorem 1.16, we have

**Theorem 1.17:** $T_0(\mathit{OR}) \in \Omega(2^n/n)$.

## 2 Reducing communication to computation problems

In this section, we prove a central theorem of this paper, which is essentially a simulation technique that transforms quantum algorithms for black-box computation to quantum communication protocols. While the idea of the simulation is extremely simple, we stress that it utilizes quantum parallelism in full.

This enables us to obtain new quantum communication protocols by applying the simulation to known quantum algorithms. We can also apply this technique in the reverse direction to use lower bounds for quantum communication protocols to derive lower bounds for quantum computation.

Let $\mathcal{F}_n$ denote the set of all functions $f : \{0,1\}^n \to \{0,1\}$.

**Theorem 2.1:** *Let $F : \mathcal{F}_n \to \{0,1\}$ and $L : \{0,1\} \times \{0,1\} \to \{0,1\}$. $L$ induces a mapping $\mathcal{F}_n \times \mathcal{F}_n \to \mathcal{F}_n$ by pointwise application: $L(g,h)(x) = L(g(x),h(x))$, for all $x \in \{0,1\}^n$. If there is a quantum algorithm that computes $F(f)$ for input $f$ using $t$ $f$-gate calls then there is a $t(2n+4)$ qubit communication protocol for the following problem. Alice gets $g$, Bob gets $h$ and the goal is for Alice to determine $F(L(g,h))$. Furthermore, if the algorithm succeeds with a certain probability then the corresponding protocol succeeds with the same probability.*

**Proof:** Consider the quantum circuit $G$ that computes $F(f)$, with $t$ $f$-gate calls. In the communication protocol, Alice simulates the quantum circuit $G$ with $f$ set to $L(g,h)$. She communicates with Bob only when an $L(g,h)$-gate call is made (for which she needs Bob's help, since she does not know $h$). Note that Alice has sufficient information to simulate a $g$-gate and Bob has enough information to simulate an $h$-gate. Each $L(g,h)$-gate call is simulated by the following procedure for the state $|x\rangle|y\rangle$ (for each $x \in \{0,1\}^n$ and $y \in \{0,1\}$).

1. Alice sets an "ancilla" qubit to state $|0\rangle$.
2. Alice applies the mapping $|x\rangle|y\rangle|0\rangle \mapsto |x\rangle|y\rangle|g(x)\rangle$, and then sends the $n+2$ qubits to Bob.
3. Bob applies $|x\rangle|y\rangle|g(x)\rangle \mapsto |x\rangle|L(g(x),h(x)) \oplus y\rangle|g(x)\rangle$, and then sends the $n+2$ qubits back to Alice.
4. Alice applies $|x\rangle|L(g(x),h(x)) \oplus y\rangle|g(x)\rangle \mapsto |x\rangle|L(g(x),h(x)) \oplus y\rangle|0\rangle$.

This involves $2n+4$ qubits of communication. Therefore, the total amount of communication is $t(2n+4)$ qubits. ∎

Note that it is simple to generalize Theorem 2.1 to functions whose range is an arbitrary set $S$ instead of $\{0,1\}$, and any $L : S \times S \to \{0,1\}$.

## 3 Proofs of upper and lower bounds

**Proof of Theorem 1.6**

The upper bounds follows directly from the simulation result Theorem 2.1 with $L$ being the binary *AND* function and $F$ the $2^n$-ary *OR* function, together with the quantum algorithm for *OR* referred to in Theorem 1.11.

The lower bound on $Q(DISJ)$ is the well known result of Kalyanasundaram and Schnitger [KS87] (see also [Raz90]), stated in Theorem 1.3.

It remains to prove the linear lower bound on $Q_0$. By results in [Kr95], it is straightforward to see that see that a zero-error $m$-qubit quantum protocol for a communication problem $P$ puts an upper bound of $2^{O(m)}$ on the rank (over the reals) of the matrix describing $P$ (more details will be provided in the final version). It is well known that the set disjointness matrix has full rank over the reals, which gives $m = \Omega(n)$.

**Proof of Theorem 1.7**

The upper bound follows directly from the simulation result Theorem 2.1 with $L$ being the binary XOR function and $F$ the $N$-way *OR* function (restricted to balanced or zero inputs), together with the Deutsch-Jozsa algorithm for $F$ [DJ92] stated in Theorem 1.9. We observe that the algorithm accesses the $F$-gate only once, and in fact a *1-way* communication protocol of $O(\log N)$ qubits can be obtained in this case.

For the lower bound we need the following strong result of Frankl and Rödl [FR87], which seems tailor-made for our needs.

**Theorem 3.1:** *[FR87] Let $n$ be divisible by 4. Let $S, T \subseteq \{0,1\}^n$ be two families of $n$-bit vectors, such that for every pair $s \in S, t \in T$ we have $\Delta(s,t) \neq n/2$. Then $|S| \times |T| \leq 4^{.96n}$.*

Consider any deterministic protocol for *EQ'* of complexity less than $n/100$. Take the largest rectangle answering 1, and let its sides be the subsets $S, T$. Since there are $2^n$ 1 answers, and they lie on the diagonal, we must have $|S| \times |T| \geq 4^{.98n}$. On the other hand, since this algorithm makes no error, this rectangle has no 0 entry, which means that for every pair $s \in S, t \in T$ we have $\Delta(s,t) \neq n/2$, which is a contradiction.

For the probabilistic, zero-error lower bound, it suffices to give a distribution which is hard on average for deterministic protocols. Observe that the argument above shows that the depth of *every* 1-leaf of any protocol which is always correct, is at least $n/100$. By considering an input distribution which places half the weight on each of the two output values, and then uniformly on the input pairs for each output, requires average communication $n/100 - 1$ in every such protocol.

**Proof of Theorem 1.8**

The upper bound follows directly from the simulation result Theorem 2.1 with $L$ being the binary *AND* function and $F$ the $AC^0$ formula corresponding a $SIGMA_d$ or $PI_d$ predicate, together with Theorem 1.15.

**Proof of Theorem 1.12**

Let $F(f)$ be *PARITY*$(f)$. Suppose we have a quantum algorithm for $F$ that makes $t$ $f$-gate calls. Apply Theorem 2.1. Let $L$ be the *AND* function and observe that $F(L(g,h))$ is the inner product communication problem. An application of the lower bound for *Q(IP)*, Theorem 1.5 yields that $t \in \Omega(2^n/n)$.

**Proof of Theorem 1.13**

The problem of computing *PARITY* with error $\frac{1}{3}$ can be reduced to $n$ instances of computing *MAJORITY* with error $O(\frac{1}{n})$. The latter problem reduces to $O(\log n)$ instances of computing *MAJORITY* with error $\frac{1}{3}$. Therefore, in the bounded-error model, *PARITY* is reducible to $n \log n$ instances of *MAJORITY*. The result now follows from Theorem 1.12.

**Proof of Theorem 1.14**

The basic approach is to define

$$g(x_1, \ldots, x_{n-m}) = \bigwedge_{y \in \{0,1\}^m} f(x_1, \ldots, x_{n-m}, y_1, \ldots, y_m) \tag{4}$$

and then first use Boyer *et al.*'s [BBHT96] extension of Grover's technique [Gr96] (in a way that does not involve measurements) to simulate an *approximate* $g$-gate within accuracy $\varepsilon/\sqrt{2^{n-m}}$. More precisely, a $g$-gate is a unitary transformation

$$U_g : |x_1, \ldots, x_{n-m}\rangle|z\rangle \mapsto |x_1, \ldots, x_{n-m}\rangle|z \oplus g(x)\rangle, \tag{5}$$

and we'll simulate a unitary transformation $V$ such that $\|U_g - V\|_2 \leq \varepsilon/\sqrt{2^{n-m}}$ (where $\|\cdot\|_2$ is the norm induced by Euclidean distance). We'll see that this can be accomplished unitarily with $O(\sqrt{2^m}\, n)$ accesses to the $f$-gate.

Then the Grover technique is applied to compute

$$\bigvee_{x \in \{0,1\}^{n-m}} g(x_1, \ldots, x_{n-m}) \qquad (6)$$

with $O(\sqrt{2^{n-m}})$ calls to the $g$-gate. Due to the accuracy of our simulated approximate $g$-gate calls, they can be used in place of the true $g$-gate calls, and the resulting total accumulated error in the final state will be bounded by $\varepsilon$. This follows from the unitarity of the operations (see [BBBV97]). This inaccuracy affects the correctness probability of the final measured answer by at most $2\varepsilon$.

It remains to show how to compute the approximate $g$-gates. In [BBHT96], it is shown that the Grover search procedure can be implemented so as to find a satisfying assignment (whenever one exists) of an $m$-variable function with an expected number of $O(\sqrt{2^m})$ calls to that function (and this holds without knowing anything about the number of satisfying assignments). Their procedure essentially involves a sequence of independent runs of Grover's original procedure for various carefully chosen run lengths. By stopping this after an appropriate number of runs, we obtain a procedure that, with $c\sqrt{2^m}$ black-box calls, decides the satisfiability of the function with error probability at most $\frac{1}{2}$ (and only errs in the case of satisfiability). By repeating this $k$ times, we obtain a procedure that, with $ck\sqrt{2^m}$ queries, decides the satisfiability of the function with error probability at most $2^{-k}$. This procedure will involve several intermediate measurements; however, by standard quantum computing techniques, the procedure can be modified so that it runs for a purely unitary stage, $G$, followed by a single measurement step.

In our context, $G$ can be thought of as being applied on an initial quantum state of the form $|x_1, \ldots, x_{n-m}\rangle|0, \ldots, 0\rangle$, (for some $x_1, \ldots, x_{n-m} \in \{0,1\}$) and making calls to $f$-gates, with the first $n-m$ inputs of $f$ always set to state $|x_1, \ldots, x_{n-m}\rangle$. What we know about the state after applying $G$ is that, if its first qubit (say) is measured, the result will be $g(x)$ with probability at least $1 - 2^{-k}$. This means that, after applying $G$ to $|x_1, \ldots, x_{n-m}\rangle|0, \ldots, 0\rangle$, but prior to any measurements, the state must be of the form

$$\alpha|g(x)\rangle|A\rangle + \beta|\overline{g(x)}\rangle|B\rangle, \qquad (7)$$

where $|\alpha|^2 \geq 1 - 2^{-k}$ and $|\beta|^2 \leq 2^{-k}$.

Now, consider the following construction. Introduce a new qubit, in initial state $|z\rangle$ (for some $z \in \{0,1\}$) and apply the following steps to the state $|z\rangle|x_1, \ldots, x_{n-m}\rangle|0, \ldots, 0\rangle$:

1. Apply $G$.
2. Perform a controlled-NOT with the first qubit as target and the second qubit as control (recall that here the second qubit contains the "answer" $g(x)$).
3. Apply $G^\dagger$.

(We'll show that this approximates the $g$-gate.) Let us trace through the evolution of a *basis* state $|z\rangle|x_1, \ldots, x_{n-m}\rangle|0, \ldots, 0\rangle$. After the $G$ operation, the state is

$$|z\rangle\left(\alpha|g(x)\rangle|A\rangle + \beta|\overline{g(x)}\rangle|B\rangle\right). \qquad (8)$$

After the controlled-NOT gate, the state is

$$\begin{aligned}
&\alpha|z \oplus g(x)\rangle|g(x)\rangle|A\rangle + \beta|\overline{z \oplus g(x)}\rangle|\overline{g(x)}\rangle|B\rangle \\
&= \alpha|z \oplus g(x)\rangle|g(x)\rangle|A\rangle + \beta|z \oplus g(x)\rangle|\overline{g(x)}\rangle|B\rangle - \\
&\quad \beta|z \oplus g(x)\rangle|\overline{g(x)}\rangle|B\rangle + \beta|\overline{z \oplus g(x)}\rangle|\overline{g(x)}\rangle|B\rangle \\
&= |z \oplus g(x)\rangle\left(\alpha|g(x)\rangle|A\rangle + \beta|\overline{g(x)}\rangle|B\rangle\right) + \qquad (9) \\
&\quad \sqrt{2}\beta\left(\tfrac{1}{\sqrt{2}}|\overline{z \oplus g(x)}\rangle - \tfrac{1}{\sqrt{2}}|z \oplus g(x)\rangle\right)|\overline{g(x)}\rangle|B\rangle.
\end{aligned}$$

In this form, it's easy to see that, after applying $G^\dagger$, the state is

$$\begin{aligned}
&|z \oplus g(x)\rangle|x_1, \ldots, x_{n-m}\rangle|0, \ldots, 0\rangle + \qquad (10) \\
&\sqrt{2}\beta\left(\tfrac{1}{\sqrt{2}}|\overline{z \oplus g(x)}\rangle - \tfrac{1}{\sqrt{2}}|z \oplus g(x)\rangle\right) G^\dagger|\overline{g(x)}\rangle|B\rangle.
\end{aligned}$$

The Euclidean distance between this state and the state that a true $g$-gate would produce is $\sqrt{2}|\beta| \leq \sqrt{2}\cdot 2^{-k/2}$. The above distance holds for any initial basis state $|z\rangle|x_1, \ldots, x_{n-m}\rangle|0, \ldots, 0\rangle$; however, the distance might be larger for non-basis states. In general, the input to a $g$-gate is of the form

$$\sum_{\substack{z \in \{0,1\} \\ x \in \{0,1\}^{n-m}}} \lambda_{z,x}|z\rangle|x_1, \ldots, x_{n-m}\rangle|0, \ldots, 0\rangle, \qquad (11)$$

where $\sum_{z \in \{0,1\}, x \in \{0,1\}^{n-m}} |\lambda_{z,x}|^2 = 1$. In this case, the difference between the output state of the true $g$-gate and our approximation to it is still bounded by

$$\begin{aligned}
\sum_{\substack{z \in \{0,1\} \\ x \in \{0,1\}^{n-m}}} |\lambda_{z,x}|\sqrt{2}\cdot 2^{-k/2} &\leq \sqrt{2^{n-m+1}}\cdot\sqrt{2}\cdot 2^{-k/2} \\
&= 2^{\frac{n-m}{2}+1-\frac{k}{2}}. \qquad (12)
\end{aligned}$$

Now, in order to make this quantity bounded by $\varepsilon/\sqrt{2^{n-m}}$, it suffices to set $k \geq 2(n-m) + 2\log(2/\varepsilon)$.

Thus, the total number of $f$-gate calls is $O(\sqrt{2^{n-m}}\cdot 2\cdot c\cdot (2(n-m) + 2\log(2/\varepsilon))\cdot\sqrt{2^m}) \subseteq O(\sqrt{2^n}\, n)$, as claimed.

**Proof of Theorem 1.15** This is a straightforward generalization of Theorem 1.14. For each $i \in \{1, \ldots, d\}$, define

$$\begin{aligned}
&g^{(i)}(x^{(1)}, x^{(2)}, \ldots, x^{(i-1)}) = \\
&\bigvee_{x^{(i)} \in \{0,1\}^{m_i}} \cdots \left(\bigwedge_{x^{(d)} \in \{0,1\}^{m_d}} f(x^{(1)}, \ldots, x^{(d)})\right) \qquad (13)
\end{aligned}$$

(where the $\wedge$ and $\vee$ quantifiers are appropriately placed). As in the proof of Theorem 1.14, an approximation of $g^{(d)}$ is first constructed at a cost of $ck_d\sqrt{2^{m_d}}$. Then this is used to approximate $g^{(d-1)}$ with cost $(ck_{d-1}\sqrt{2^{m_{d-1}}})(ck_d\sqrt{2^{m_d}})$, and so on, up to $g^{(1)}$, whose value is the required answer. It suffices to set $k_2, \ldots, k_d$ to $5n$ and to set $k_1$ to a constant.

**Proof of Theorem 1.16**

This is similar to the proof of Theorem 1.15, except that the parameters $k_1, \ldots, k_d$ are all set to $2^{n/\delta d}$.

**Proof of Theorem 1.8**

This follows from the zero-error part of Theorem 1.6 in conjunction with Theorem 2.1.

## 4 Conclusions and open problems

We have constructed a reductions from quantum communication problems to quantum black-box computations. Using known quantum algorithms, this reduction enabled us to prove a near quadratic gap between bounded error classical communication complexity and bounded error quantum communication complexity. Using a partial function we also showed an exponential gap between zero-error classical communication complexity and exact quantum communication complexity. Kremer [Kr95] shows that the gap between the two models can never be bigger than exponential, so this result is optimal. Several problems however remain:

- Is there an exponential gap between the exact and the zero-error model with a total instead of a partial function? A recent result by [BBCMW98] shows that for any total black-box problem if there is a quantum algorithm that computes this problem with $T$ oracle calls then there is a deterministic classical algorithm that computes it with $O(T^6)$ oracle calls. This results shows that the approach taken here (reduce a communication problem to a black-box problem) will for total functions never yield more than a polynomial (sixth root) gap.
- Is the upper bound for *DISJ* optimal?
- Is there a bigger than quadratic gap for the bounded-error models (with total or partial functions)?

We used the reduction from communication problems to black-box computation in the reverse order to obtain non-trivial lower bounds for *PARITY* and *MAJORITY*. These bounds have recently been improved to optimal for *PARITY* [BBCMW98, FGGS98] and *MAJORITY* [BBCMW98].

**Acknowledgements**

We would like to thank Gilles Brassard, Wim van Dam, Peter Høyer, Tal Mor, and Alain Tapp for helpful discussions. A.W. would like to thank Dorit Aharonov, who taught him almost all he knows about quantum computing. This is the ultimate student-advisor relationship!

**References**

[BBCMW98] R. Beals, H. Buhrman, R. Cleve, M. Mosca, R. de Wolf, "Quantum Lower Bounds by Polynomials", preprint available from the LANL quant-ph archive 9802049, 1998.

[BBBV97] C.H. Bennett, E. Bernstein, G. Brassard and U.V. Vazirani, "Strengths and weaknesses of quantum computing" *SIAM J. on Computing*, Vol. 26, No. 5, pp. 1510–1523, 1997.

[BV93] E. Bernstein and U.V. Vazirani, "Quantum complexity theory", *Proc. of the 25th STOC*, pp. 11–20, 1993.

[BB94] A. Berthiaume and G. Brassard, "Oracle quantum computing", *Journal of Modern Optics*, 41, 12, pp. 2521–2535, 1994.

[BBHT96] M. Boyer, M., G. Brassard, P. Høyer, and A. Tapp, "Tight bounds on quantum searching", *Proc. 4th Workshop on Physics and Computation*, pp. 36–43, 1996.

[Bu97] H. Buhrman, untitled manuscript, 1997.

[BCD97] H. Buhrman, R. Cleve, and W. van Dam, "Quantum entanglement and communication complexity", preprint available from the LANL quant-ph archive 9705033, 1997.

[CG88] B. Chor and O. Goldreich, "Unbiased bits from sources of weak randomness and probabilistic communication complexity", *SIAM J. Comput.* 17(2), pp. 230–261, 1988.

[CB97] R. Cleve and H. Buhrman, "Substituting quantum entanglement for communication", *Physical Review A*, Vol. 56, No. 2, pp. 1201–1204, 1997. Preprint available from the LANL quant-ph archive 9704026.

[CDNT97] R. Cleve, W. van Dam, M. Nielsen, and A. Tapp, "Quantum entanglement and the communication complexity of the inner product function", preprint available from the LANL quant-ph archive 9708019, 1997.

[DHT97] W. van Dam, P. Høyer, and A. Tapp, "Multiparty quantum communication complexity", preprint available from the LANL quant-ph archive 9710054, 1997.

[DJ92] D. Deutsch and R. Jozsa, Proc. R. Soc. Lond. A 439, pp. 553–558, 1992.

[FGGS98] E. Fahri, J. Goldstone, S. Gutmann, M. Sipser, "A Limit on the Speed of Quantum Computation in Determining Parity", preprint available from the LANL quant-ph archive 9802045, 1998.

[FR87] P. Frankl and V. Rödl, "Forbidden intersections", *Trans. Amer. Math. Soc.* 300, 1, pp. 259–286, 1987.

[FC94] C. Fuchs and C. Caves, "Ensemble-dependent bounds for accessible information in quantum mechanics", *Physical Rev. Lett.*, Vol. 73, pp. 3047–3050, 1994.

[Gr96] L.K. Grover, "A fast quantum mechanical algorithm for database search", *Proc. of the 28th STOC*, pp. 212–219, 1996.

[Hol73] A.S. Holevo, "Some estimates of the information transmitted by quantum communication channels", *Problemy Peredachi Informatsii*, Vol. 9, 1973, pp. 3–11. English translation in *Problems of Information Transmission (USSR)*, Vol. 9, pp. 177–183, 1973.

[KS87] B. Kalyanasundaram and G. Schnitger, "The probabilistic communication complexity of set intersection", 2*nd Structure in Complexity Theory Conference*, pages 41–49, 1987.

[Ki95] A. Kitaev, "Quantum measurements and the abelian stabilizer problem", Preprint available from the LANL quant-ph archive 9511026.

[Kr95] I. Kremer, *Quantum Communication*, MSc Thesis, Computer Science Department, The Hebrew University, 1995.

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

[Ne91] I. Newman, "Private vs. common random bits in communication complexity", *Information Processing Letters*, 39, pp. 67–71, 1991.

[Raz95] R. Raz, "Fourier analysis for probabilistic communication complexity", *Comput. Complexity*, Vol. 5, pp. 205–221, 1995.

[Raz90] A. Razborov, "On the distributional complexity of disjointness", *Proceedings of the ICALP*, pp. 249–253, 1990. To appear in *Theoretical Computer Science*.

[Sh97] P.W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", *SIAM J. on Computing*, Vol. 26, No. 5, pp. 1484–1509, 1997. Preliminary version appeared as "Algorithms for quantum computation: discrete logarithms and factoring" in *Proc. of the 35th FOCS*, pp. 124–134, 1994.

[Si97] D. Simon, "On the power of quantum computation", *SIAM J. on Computing*, Vol. 26, No. 5, pp. 1474–1483, 1997. Preliminary version appeared in *Proc. of the 35th FOCS*, pp. 116–123, 1994.

[VV86] L.G. Valiant and V.V. Vazirani, "NP is as easy as detecting unique solutions", *Theoret. Comput. Sci.*, Vol. 47, pp. 85–93, 1986.

[Va87] U.V. Vazirani, "Strong communication complexity or generating quasi-random sequences from two communicating slightly-random sources", *Combinatorica*, Vol. 7, No. 4, pp. 375–392, 1987.

[Ya79] A. C.-C. Yao, "Some complexity questions related to distributive computing", *Proceedings of* $11^{\text{th}}$ *STOC*, pp. 209-213, 1979.

[Ya93] A. C.-C. Yao, "Quantum circuit complexity", *Proc. of the 34th FOCS*, pp. 352–361, 1993.