Theoretical Computer Science 412 (2011) 4619–4628

Contents lists available at ScienceDirect

Theoretical Computer Science

journal homepage: www.elsevier.com/locate/tcs

Unbounded-error quantum query complexity☆

Ashley Montanaro [a], Harumichi Nishimura [b], Rudy Raymond [c,*]

[a] Department of Applied Mathematics and Theoretical Physics, University of Cambridge, UK
[b] School of Science, Osaka Prefecture University, Japan
[c] IBM Research – Tokyo, 242-8502 Yamato-shi, Japan

ARTICLE INFO

Article history:
Received 30 July 2010
Received in revised form 7 April 2011
Accepted 25 April 2011
Communicated by G. Rozenberg

Keywords:
Quantum computing
Query complexity
Communication complexity

ABSTRACT

This work studies the quantum query complexity of Boolean functions in an *unbounded-error* scenario where it is only required that the query algorithm succeeds with a probability strictly greater than 1/2. We show that, just as in the communication complexity model, the unbounded-error quantum query complexity is exactly half of its classical counterpart for any (partial or total) Boolean function. Moreover, connecting the query and communication complexity results, we show that the "black-box" approach to convert quantum query algorithms into communication protocols by Buhrman–Cleve—Wigderson [STOC'98] is optimal even in the unbounded-error setting.

We also study a related setting, called the *weakly* unbounded-error setting, where the cost of a query algorithm is given by $q+\log(1/2(p-1/2))$, where q is the number of queries made and $p > 1/2$ is the success probability of the algorithm. In contrast to the case of communication complexity, we show a tight multiplicative $\Theta(\log n)$ separation between quantum and classical query complexity in this setting for a *partial* Boolean function. The asymptotic equivalence between them is also shown for some well-studied *total* Boolean functions.

1. Introduction

Many models in computational complexity have several settings where different restrictions are placed on the success probability to evaluate a Boolean function f. The most basic one is the *exact* setting: it requires that the computation of f is always correct. In the polynomial-time complexity model, this corresponds to the complexity class P. If we require the success probability to be only "high" (say, 2/3), such a setting is called a *bounded-error*. The corresponding polynomial-time complexity class is known as BPP. The *unbounded-error* setting is also standard. In this setting, it suffices to have a "positive hint", even infinitesimal, towards the right answer. That is, the unbounded-error setting requires that the success probability to compute Boolean functions is strictly larger than 1/2. The most famous model for this setting is also polynomial-time complexity, and PP is the corresponding complexity class. This setting also has connections with important concepts such as *polynomial threshold functions* in computational learning theory.

There are two major computing models which have been introduced to develop the lower bound method in complexity theory. The first one is the *communication complexity (CC)* model. The CC model measures the amount of communication for several parties, which have distributed inputs, to compute Boolean functions. The second one is the *query complexity (QC)* model. The QC model measures the amount of queries required for a machine with no input to compute a Boolean function

☆ An extended abstract of this article was presented in Proceedings of 19th ISAAC, Lecture Notes in Computer Science, vol. 5369, pp. 920–931, 2008.

* Corresponding author. Tel.: +81 46 215 4797.
E-mail addresses: am994@cam.ac.uk (A. Montanaro), hnishimura@mi.s.osakafu-u.ac.jp (H. Nishimura), raymond@jp.ibm.com, rraymondhp@gmail.com (R. Raymond).

0304-3975/$ – see front matter Crown Copyright © 2011 Published by Elsevier B.V. All rights reserved.
doi:10.1016/j.tcs.2011.04.043

by querying the input given in a black box. The CC and QC models are also studied in the *quantum* setting, and there are many results on the performance gaps between classical and quantum computation [32].

So far, the unbounded-error setting has also been studied in the CC and QC models. In the classical CC model, a large literature has developed since its introduction by Paturi and Simon [27]. In the quantum case, Iwama et al. [20] showed that the quantum CC of *any* Boolean function is almost half of its classical CC. Furthermore, a variant of the unbounded-error setting was studied, which is often called the *weakly unbounded-error* setting. Here the cost of a protocol is defined by $q + \log(1/2(p - 1/2))$, where q is the number of communication (qu)bits and $p > 1/2$ is the success probability.[1] This concept appeared in [5,17], and was later studied in [21]. Halstenberg and Reischuck [17] showed that weakly unbounded-error protocols correspond to so-called "majority nondeterministic" protocols, while Klauck [21] showed a close connection between this setting and the discrepancy method in communication complexity. Recently, Buhrman et al. [11] and Sherstov [30] independently showed that there is a Boolean function that exponentially separates the classical weakly unbounded-error CC and unbounded-error CC, which solves an open problem that remained from [5]. On the other hand, there can only be a constant gap between quantum and classical CCs for Boolean functions in the weakly unbounded-error setting [20,21].

The study of the QC model in the unbounded-error setting has been developed implicitly as the study of the sign-representing polynomial (say, [4,7]) since Beals et al. [6] gave the nice characterization of the (quantum) QC by polynomials. In fact, Buhrman et al. [11] mentioned the close relationship between sign-representing polynomials and QCs of Boolean functions. However, there is no explicit literature on unbounded-error quantum QCs, such as the relationship to classical QC and the weakly unbounded-error variants.

Our results. In this paper we deal with the unbounded-error quantum QC and study its relationship to the other unbounded-error concepts. First, we show that, as in the case of CC, the unbounded-error quantum QC of some (total/partial) Boolean function is always exactly half of its classical counterpart. Second, we discuss the relation between the unbounded-error quantum QC and CC. A powerful result by Buhrman, Cleve and Wigderson [10] is often used to "reduce" quantum CC to quantum QC, which is a "black-box" approach to convert quantum query algorithms into communication protocols with $O(\log n)$ overhead. It is a natural question whether their black-box approach is *optimal*, that is, $\Omega(\log n)$ overhead is inevitable. We show that the overhead of the black-box approach of [10] is optimal in the unbounded-error setting. Moreover, we show that this bound on overhead factor also holds under nondeterministic and exact settings. Third, we develop the weakly unbounded-error QC, which is a natural measure to trade-off queries and success probability, as the correspondence of the weakly unbounded-error CC. We show a multiplicative separation, $T(n)$ vs. $\Omega(T(n)\log(n/T(n)))$ for any monotone increasing function satisfying $T(n) \leq n$, between the weakly unbounded-error quantum and classical QCs of some *partial* function. This result contrasts with the only constant quantum-classical gaps of the weakly unbounded-error CC [20,21] as well as the unbounded-error QC. On the other hand, we show that the separation is only constant for some well-known *total* Boolean functions such as PARITY, AND, OR and threshold functions. Finally, we show that a weakly unbounded-error QC can be exponentially smaller than a well-studied complexity measure of Boolean functions, the average sensitivity.

Related work. In a similar direction, de Wolf [33] characterized the nondeterministic[2] quantum QC and CC by, respectively, *nondeterministic degree* of approximating polynomials and *nondeterministic rank* of communication matrices. When comparing classical and quantum complexities under these models, de Wolf showed strong separations; an unbounded gap for QC and an exponential gap for CC (the first unbounded gap for CC was shown before in [23]). Under a different (i.e., certificate based) type of nondeterminism, a quadratic separation between quantum and classical CC is known for some total function [22]. Quite recently under a different aspect, Zhang showed that the reduction in [10] is polynomially tight up to the choice of all AND or all OR inner functions and derived polynomial relations between quantum and classical communication complexity for composed functions [35].

Organization of the paper. We begin, in Section 2, by giving the formal definitions of the models that we discuss in this paper. Section 3 contains the relation between unbounded-error quantum and classical QCs. In Section 4, we show the optimality of the reduction of [10] from quantum CC to quantum QC. In Section 5, we compare the weakly unbounded-error quantum QC to other several QCs and to average sensitivity. The paper finishes with some concluding remarks.

2. Definition and models

We first list some useful definitions, starting with unbounded-error polynomials.

Definition 2.1. Let $f : \{0,1\}^n \to \{0,1\}$ be a Boolean function of n variables, and $q : \{0,1\}^n \to [0,1]$ be a real multilinear polynomial. We say that q is an *unbounded-error polynomial for* f if for any $x \in \{0,1\}^n$, $q(x) > 1/2$ if $f(x) = 1$ and $q(x) < 1/2$ if $f(x) = 0$. We denote the lowest degree among all unbounded-error polynomials for f as $udeg(f)$.

Note that this definition is given in terms of total Boolean functions, but we can naturally extend it to partial functions. Throughout this paper, we use the term "Boolean functions" for results that hold for both partial and total functions; if not, we mention it explicitly.

[1] Some previous work does not have the factor of 2 in the denominator; see Section 2 for a discussion.

[2] This could be called *one-sided unbounded-error* since the computation is required to be exact in one side of the output.

There have been many studies and extensive results in the literature on polynomials that *sign-represent* Boolean functions [4,7,24]. A polynomial $p : \{0,1\}^n \to \mathcal{R}$ is said to sign-represent f if $p(x) > 0$ whenever $f(x) = 1$, and $p(x) < 0$ whenever $f(x) = 0$.[3] If $|p(x)| \leq 1$ for all x, we say that p is *normalized*. The *bias* of a normalized polynomial p is defined as $\beta = \min_x |p(x)|$. Denoting the minimum degree of polynomials that sign-represent f as $sdeg(f)$, it is easy to see that $udeg(f) = sdeg(f)$, since an unbounded-error polynomial q for f can be obtained from a sign-representing polynomial p for f as follows: $q(x) = 1/2 + p(x)/2$. In the following, we will use some results about polynomials that sign-represent f to characterize the unbounded-error QC.

It is folklore that every real multilinear polynomial q of degree at most d can be represented in the so-called *Fourier basis*. Namely,

$$q(x) = \sum_{S \in S_d} \hat{q}(S)(-1)^{x_S}, \tag{1}$$

where S_d denotes the set of all index sets $S \subseteq [n]$ of at most d variables, and x_S denotes the XOR (or parity) of the bits of x on index set S, namely, $x_S = \oplus_{i \in S} x_i$.

Next, we give the definitions of unbounded-error QC and CC, as well as their weak counterparts.

Definition 2.2. Let $UQ(f)$ and $UC(f)$ be the unbounded-error quantum and classical, respectively, QCs of a Boolean function f. Namely, $UQ(f)$ (resp. $UC(f)$) is the minimum number of quantum (resp. classical) queries to a black box that holds the input $x \in \{0,1\}^n$ to f such that f can be computed with a success probability greater than $1/2$. Let $UQ_{cc}(g)$ and $UC_{cc}(g)$ be the unbounded-error quantum and classical, respectively, CCs of a distributed Boolean function $A \times B \to \{0,1\}$, where $A \subseteq \{0,1\}^{n_1}$ and $B \subseteq \{0,1\}^{n_2}$ denote the sets of inputs each given to Alice and Bob, respectively. Namely, $UQ_{cc}(g)$ (resp. $UC_{cc}(g)$) is the minimum number of quantum (resp. classical) bits exchanged between Alice and Bob to compute g with success probability greater than $1/2$.

Define the *bias* β of a quantum or classical query algorithm (resp. communication protocol) which succeeds with probability $p > 1/2$ as $p - 1/2$. Then the *weakly unbounded-error cost* of such an algorithm (resp. protocol) is equal to the number of queries (resp. communicated bits or qubits) plus $\log 1/2\beta$.[4] Let $WUQ(f)$, $WUC(f)$, $WUQ_{cc}(g)$ and $WUC_{cc}(g)$ be the *weakly* unbounded-error counterparts of the previous measures, given by the minimum weakly unbounded-error cost over all quantum or classical query algorithms and communication protocols, respectively.

Note that in the above definition UQ_{cc} and UC_{cc} refer to two-way CC. However, since two-way CC only differs from one-way CC by at most one qubit or bit [27,20], for simplicity we will mainly use results in one-way CC, which have been much studied in [27,19]. Also note that some previous work defines the weakly unbounded-error cost as the number of queries plus $\log 1/\beta$ [11,20]. However, we prefer the present definition, as it ensures that weakly unbounded-error QC or CC is never greater than its exact counterpart. For example, with the previous definition, a function f for which there exists an optimal classical algorithm that uses one query and succeeds with certainty would have $WUC(f) = 2$, whereas with the present definition $WUC(f) = 1$.

3. Unbounded-error quantum and classical QCs

In [19], it was shown that $UQ_{cc}(f)$ is always exactly half of $UC_{cc}(f)$ for any (partial or total) Boolean function f. We will show that in the unbounded-error QC model, the equivalent (and rather tight) result – that quantum QC is always *exactly* half of its classical counterpart – also holds for any Boolean function. For this purpose, we need the following lemmas.

The first lemma, shown by Beals et al. [6], gives a lower bound on the number of queries in terms of the minimum degree of representing polynomials.

Lemma 3.1 (*[6]*). *The amplitude of the final basis states of a quantum algorithm using T queries can be written as a multilinear polynomial of degree at most T.*

The second lemma, shown by Beals et al. [6] and Farhi et al. [15], gives an exact quantum algorithm for computing the parity of n variables with just $n/2$ queries.

Lemma 3.2 (*[6,15]*). *Let $S \subseteq [n]$ be a set of indices of variables. There exists a quantum algorithm for computing x_S with $\lceil |S|/2 \rceil$ queries. That is, there exists a unitary transformation U_f which needs exactly $\lceil |S|/2 \rceil$ queries: for any $b \in \{0,1\}$,*

$$U_f |S\rangle |0^m\rangle |b\rangle = |S\rangle |\psi_S\rangle |b \oplus x_S\rangle,$$

where $|0^m\rangle$ and $|\psi_S\rangle$ are the workspace quantum registers before and after the unitary transformation, respectively.

The third lemma was shown recently by Buhrman et al. [11]. It turns out to be very useful in characterizing the unbounded-error QC of Boolean functions.

[3] Note that in the literature, 0/1 is usually replaced by $1/-1$ for convenience.

[4] In this paper, log denotes the logarithm taken to base 2.

Lemma 3.3 ([11]). *Suppose that there exists a multilinear polynomial p of d-degree that sign-represents $f : \{0,1\}^n \to \{0,1\}$ with bias β. Define $N = \sum_{i=0}^{d} \binom{n}{i}$. Then there also exists a multilinear polynomial $q(x) = \sum_{S \in S_d} \hat{q}(S)(-1)^{x_S}$ of the same degree and bias $\beta/\sqrt{N}$ that sign-represents f such that $\sum_{S \in S_d} |\hat{q}(S)| = 1$.*

Now we are ready to prove the exact relation between UQ and UC.

Theorem 3.4. *For any Boolean function $f : X \to \{0,1\}$ such that $X \subseteq \{0,1\}^n$, it holds that:*

$$UQ(f) = \left\lceil \frac{UC(f)}{2} \right\rceil = \left\lceil \frac{udeg(f)}{2} \right\rceil.$$

Proof. $[UC(f) = udeg(f)]$ This follows from a result in Buhrman et al. [11]: an unbounded-error randomized algorithm for f using d queries is equivalent to a d-degree polynomial p that sign-represents f, and hence to a d-degree unbounded-error polynomial q for f.

$[UQ(f) \geq udeg(f)/2]$ Let $\mathcal{A}$ be an unbounded-error quantum algorithm for f using $UQ(f)$ queries. Note that the acceptance probabilities of quantum algorithms can be written as the sum of the absolute values squared of the amplitude magnitudes of the corresponding basis states. By Lemma 3.1, the acceptance probability of $\mathcal{A}$ can be written as a multilinear polynomial of degree at most $2UQ(f)$. Hence, $udeg(f) \leq 2UQ(f)$.

$[UQ(f) \leq \lceil udeg(f)/2 \rceil]$ This follows from Lemmas 3.2 and 3.3. First, let $\delta(y) = 1$ if $y > 0$, and $\delta(y) = 0$ otherwise. With regard to the Fourier representation of polynomial p that sign-represents f as in Eq. (1), and for a fixed $x \in \{0,1\}^n$, we can write

$$p(x) = \sum_{S \in S_{udeg(f)}} \hat{p}(S)(-1)^{x_S} = \sum_{S \in S_x^+} |\hat{p}(S)| - \sum_{S \in S_x^-} |\hat{p}(S)|$$

such that $S_x^+ = \{S | x_S \oplus \delta(\hat{p}(S)) = 1\}$, and $S_x^- = \{S | x_S \oplus \delta(\hat{p}(S)) = 0\}$. By Lemma 3.3, we can assume that $\sum_{S \in S_{udeg(f)}} |\hat{p}(S)| = 1$. Then, we have $\sum_{S \in S_x^+} |\hat{p}(S)| > 1/2$ if $f(x) = 1$, and $\sum_{S \in S_x^+} |\hat{p}(S)| < 1/2$ otherwise. Thus, the unbounded-error quantum algorithm for f can be obtained by computing the XOR of x_S and $\delta(\hat{p}(S))$: the former by applying Lemma 3.2 with $\lceil |S|/2 \rceil \leq \lceil udeg(f)/2 \rceil$ queries, and the latter without query cost, as summarized in the following steps.

1. Prepare quantum state $|\psi_p\rangle = \sum_{S \in S_{udeg(f)}} \sqrt{|\hat{p}(S)|} |S\rangle |0^m\rangle |\delta(\hat{p}(S))\rangle$.
2. Apply the unitary transformation U_f of Lemma 3.2 for obtaining the parity of x on index set S, whose result is stored in the last register. The quantum state after the transformation is:
$$U_f |\psi_p\rangle = \sum_{S \in S_{udeg(f)}} \sqrt{|\hat{p}(S)|} |S\rangle |\psi_S\rangle |\delta(\hat{p}(S)) \oplus x_S\rangle.$$
3. Measure the last register, and output the result of the measurement.

This completes the proof. □

From Theorem 3.4 and classical results in [26], we immediately obtain the following corollary, which implies that almost every function has unbounded-error quantum QC $n(1/4 + o(1))$. By contrast, there remains a gap in the bounded-error setting: Almost every function has bounded-error quantum QC between $n/4 + \Omega(\sqrt{n})$ [3,26] and $n/2 + O(\sqrt{n})$ [13].

Corollary 3.5. *Almost every function $f : \{0,1\}^n \to \{0,1\}$ has unbounded-error quantum QC bounded by $n/4 \leq UQ(f) \leq n/4 + O(\sqrt{n \log n})$.*

4. Tightness of reducing CC to QC

Buhrman et al. [10] gave a method for reducing a quantum communication protocol to a quantum query algorithm with $O(\log n)$ overhead, which we call the *BCW reduction*, as follows.

Theorem 4.1 ([10]). *Let $F : \{0,1\}^n \to \{0,1\}$, and $F^L : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ denote the distributed function of F induced by the bitwise function $L : \{0,1\} \times \{0,1\} \to \{0,1\}$, that is defined by $F^L(x,y) = F(z)$ such that each bit of z is $z_i = L(x_i, y_i)$. If there is a quantum algorithm that computes F using T queries with some success probability, then there is a $T(2 \log n + 4)$-qubit communication protocol for F^L, where Alice has input x and Bob has input y, with the same success probability.*

In the reverse direction, this implies that any lower bound C in the CC side is translated into a lower bound $\Omega(C/\log n)$ in the QC side. The BCW reduction is exact: the success probability of the communication protocol is the same as that of the query computation. In fact, [10] proved some interesting results using this reduction, such as the first non-trivial quantum protocol for the disjointness problem, which used $O(\sqrt{n} \log n)$ communication by a reduction from Grover's search algorithm. Later, this upper bound was improved to $O(\sqrt{n} \log^*(n))$ by [18], and finally to $O(\sqrt{n})$, which matches the lower bound shown in [28], by [1] with ingenious simulation techniques. However, unlike the results of [10], those techniques seem to be limited only to specific functions such as disjointness.

Thus, it is of interest to know whether there exists a universal reduction similar to the BCW reduction but with $o(\log n)$ overhead and preserving the success probability. This might be achieved by designing new reduction methods. In addition, a smaller overhead might be achieved by relaxing the success probability condition, that is, allowing the success probability of the resulting protocol to be significantly lower than that of the original algorithm. To look for the possibility of such a universal reduction, one can consider relations between quantum QC and CC by using such a reduction as a "black box" under various settings for the required success probability.

Our result in this section is the optimality of the BCW reduction in the exact, nondeterministic, and unbounded-error settings, as showed in the following theorem. Here, $\oplus$ and $\wedge$ denote the functions XOR and AND from $\{0,1\} \times \{0,1\}$ to $\{0,1\}$, respectively.

Theorem 4.2. *Let $T(n)$ be a nondecreasing function satisfying $T(n) \leq n$. The following hold:*

(1) *There is a Boolean function f whose nondeterministic (exact, respectively) quantum QC is $T(n)$, while the CC of its XOR distributed counterpart $f^{\oplus}$ is $\Omega(T(n)\log(n/T(n)))$.*

(2) *There is a Boolean function f whose unbounded-error quantum QC is $T(n)$, while the CC of its AND distributed counterpart $f^{\wedge}$ is $\Omega(T(n)\log(n/T(n)))$.*

We should remark that we do not know if the BCW reduction is also optimal, that is, the $\log n$ overhead by the reduction is inevitable, in the *bounded-error* setting. What we only know is that a $\log\log n$ overhead is inevitable, which can be shown by the same function for showing the optimality of BCW reduction in nondeterministic (exact) case.

4.1. Nondeterministic and exact cases

The following partial Boolean function, which is a variant of the Fourier Sampling problem of Bernstein and Vazirani [9], will be the base of the proof of the first part of Theorem 4.2.

Definition 4.3. For $x, r \in \{0,1\}^m$, let F^r be a bit string of length $n = 2^m$ whose x-th bit is $F^r_x = \sum_i x_i \cdot r_i \mod 2$. Let also g be another bit string of length n. The *Fourier Sampling* (FS) of F^r and g is defined by $\mathrm{FS}(F^r, g) = g_r$. When Alice and Bob are given (F^a, g) and (F^b, h), respectively, as their inputs where $a, b \in \{0,1\}^m$ and $g, h \in \{0,1\}^n$, the *Distributed Fourier Sampling* (DFS) on their inputs is $\mathrm{FS}^{\oplus}((F^a, g), (F^b, h)) = \mathrm{FS}(F^a \oplus F^b, g \oplus h)$.

Remark. FS can also be considered as a variant of the Goldreich–Levin problem in the cryptographic setting for *noisy* F^r and a bit string g such that $g_i = 1$ if and only if $i = r$, see, e.g., the lecture note by Bellare [8].

Now, let us consider the AND of $T = T(N)$ instances of FS, namely, $\mathrm{FS}(F^{r_1}, g^1) \wedge \cdots \wedge \mathrm{FS}(F^{r_T}, g^T)$ where $N = 2Tn$ is the length of the input string (note that n, the length of F^{r_i} and g^i, is a function of N). The proof of the first part of Theorem 4.2 is given in the following lemma.

Lemma 4.4. *The exact quantum QC of the AND of T instances of* FS *is $O(T)$, while the nondeterministic quantum CC of its distributed function induced by the bitwise XOR is $\Omega(T\log(N/T))$.*

Proof. For the QC part, note that for each instance of FS we can construct the following two-query quantum algorithm: Given input (F^r, g) (in a black box), (i) Determine r with one query to F^r with certainty by the quantum algorithm of [9]. (ii) Output $\mathrm{FS}(F^r, g) = g_r$ with one query to g. Thus, the exact quantum QC of the AND of T instances of FS is $O(T)$.

For the CC part, we first prove that the nondeterministic (and hence exact) CC of DFS is $\Omega(\log n)$, and use this result for showing the lower bound of the AND of T instances of DFS. For this purpose, let us consider the set of inputs $((F^a, g), (F^b, h)) \in (\{0,1\}^n)^2 \times (\{0,1\}^n)^2$ such that $g \oplus h = 10^{n-1}$. For such inputs, $\mathrm{FS}^{\oplus}((F^a, g), (F^b, h)) = 1$ (resp. 0) implies $a = b$ (resp. $a \neq b$) since $\mathrm{FS}^{\oplus}((F^a, g), (F^b, h)) = \mathrm{FS}(F^a \oplus F^b, g \oplus h) = \mathrm{FS}(F^{a\oplus b}, 10^{n-1}) = (10^{n-1})_{a\oplus b}$ (the $(a \oplus b)$-th bit of 10^{n-1}). This means that if the nondeterministic CC of DFS is $o(\log n)$, then that of $\mathrm{EQ}_{\log n}$ (the equality on two $\log n$ bits a and b) is also $o(\log n)$, which contradicts the fact that the nondeterministic quantum CC of $\mathrm{EQ}_{\log n}$ is $\Omega(\log n)$ [33]. Next, notice that any protocol for the AND of T instances of DFS problem can also be used for $\mathrm{EQ}_{T\log n}$. Thus, its nondeterministic quantum CC should be $\Omega(T\log(N/T))$, as claimed. □

4.2. Unbounded-error case

Here we show the proof of the second part of Theorem 4.2, that is, the impossibility of converting a quantum query algorithm into the corresponding communication protocol with $o(\log n)$ overhead, even if the success probability of the resulting protocol becomes very close to half. The base function is ODD-MAX-BIT function, a total Boolean function introduced in [7]. First, we recall the definition of ODD-MAX-BIT$_n$ (or OMB$_n$ for short).

Definition 4.5. For any $x \in \{0,1\}^n$, let us define $\mathrm{OMB}_n(x) = k \mod 2$, where k is the largest index of x such that $x_k = 1$ ($k = 0$ for $x = 0^n$).

The proof of the second part of Theorem 4.2 follows from the complexities of the XOR of T instances of OMB and OMB$^{\wedge}$, as given in the following lemma.

Lemma 4.6. *The unbounded-error quantum QC of the XOR of T instances of* OMB *is $O(T)$, while the unbounded-error quantum CC of* $\text{OMB}^\wedge$ *is $\Omega(T \log(N/T))$ where $N = Tn$ is the input length.*

Proof. The QC part is easy since one instance of OMB_n can be solved with only one query by the following classical algorithm: Query x_i with probability $p_i = \frac{2^i}{2^{n+1}-2}$. Then, output $i \mod 2$ if $x_i = 1$, and the result of a random coin flip if $x_i = 0$. It can be seen that the success probability is always bigger than $1/2$ for all positive integers n. It is not difficult to see that if each instance can be solved with probability more than half, so can the XOR of T instances.

For the CC part, we first show $UQ_{cc}(\text{OMB}_n^\wedge) \geq (\log n - 3)/2$, and use this result for proving the lower bound of the XOR of T instances of $\text{OMB}^\wedge$. The bound for $UQ_{cc}(\text{OMB}_n^\wedge) \geq (\log n - 3)/2$ follows from the lower bound on quantum random access coding (which is also known as the INDEX function) shown in [19]. For $a \in \{0,1\}^n$ and $b \in \{0,1\}^{\log n}$, $\text{INDEX}_n(a,b)$ is defined as the value of the b-th bit of a, or a_b. Then, we consider the case when Alice uses $x = a_1 0 a_2 0 \ldots a_n 0$, and Bob uses $y = y_1 y_2 y_3 \ldots y_{2n}$ such that $y_j = 1$ iff $j = 2b-1$, as inputs to the protocol for $\text{OMB}_{2n}^\wedge$. Clearly, $\text{OMB}_{2n}^\wedge(x,y) = \text{INDEX}_n(a,b)$. However, according to [19], $UQ_{cc}(\text{INDEX}_n) \geq \frac{1}{2}\log(n+1) - 1$ (Here, -1 comes from the difference between two-way and one-way CC [20]). Therefore, $UQ_{cc}(\text{OMB}_n^\wedge) \geq \frac{1}{2}\log(n/2+1) - 1 \geq (\log n - 3)/2$.

Next, we show that the XOR of T instances of $\text{OMB}_n^\wedge$ can be used to compute the inner product of two distributed $T\log(n/2)$ bits. Let Alice and Bob's inputs for the inner product be x and y, respectively. To compute the answer $\sum_{i=1}^{T\log(n/2)} x_i y_i \mod 2$, they divide their input strings into T parts, each of length $\log(n/2)$ bits, and for each part they compute the inner product, which is done by the reduction to $\text{INDEX}_{n/2}$ (and hence $\text{OMB}_n^\wedge$) as follows: Alice writes the inner product of her part with all possible Bob's parts, which results in a bit string of length $n/2$ as her input to $\text{INDEX}_{n/2}$. By setting the corresponding Bob's part as the other input to $\text{INDEX}_{n/2}$, they can compute the inner product for each part by applying the protocol for $\text{INDEX}_{n/2}$. Since the quantum CC lower bound of the inner product on distributed inputs of $T\log(n/2)$ bits is $\Omega(T\log(n/2)) = \Omega(T\log(N/T))$ [16,20], we obtain the desired result. □

5. Weakly unbounded-error quantum and classical QCs

In this section, we study the weakly unbounded-error QC (*WUQ*). There are two reasons why this model, which at first sight seems somewhat contrived, may be of interest: (i) The separation between quantum and classical QCs appears to be different for different success probability settings. For example, the best known separation for a total function is quadratic in the bounded-error setting, but we showed earlier that only a factor of two is possible in the unbounded-error setting. The *WUQ* model gives a natural way to trade-off queries and success probability. (ii) Weakly unbounded-error CC is closely related to the well-studied notion of *discrepancy* [21]. *WUQ* is thus a QC analogue of a natural CC quantity.

5.1. Unbounded gaps between UQ and WUQ

First, we observe a large gap, $O(1)$ vs. $\Omega(n^{1/3}/\log n)$, between unbounded-error and weakly unbounded-error quantum QCs. As mentioned in Section 1, an exponential gap between UQ_{cc} and WUQ_{cc} in the CC model was shown by Buhrman et al. [11] and Sherstov [30]. In [11] the function $\text{OMB}_n^\wedge$ was used to show the gap. We can easily see that by using OMB_n a similar gap is shown also in the QC model.

Lemma 5.1. *$UQ(\text{OMB}_n) = 1$ and $WUQ(\text{OMB}_n) = \Omega(n^{1/3}/\log n)$.*

Proof. $UQ(\text{OMB}_n) = 1$ was already shown in Lemma 4.6. The lower bound of $WUQ(\text{OMB}_n)$ follows from the result $WUQ_{cc}(\text{OMB}_n^\wedge) = \Omega(n^{1/3})$ in [11] combined with the BCW reduction. □

5.2. Tight gaps between WUQ and WUC for partial functions

In the CC model, Klauck [21] showed that weakly unbounded-error quantum and classical CCs are within some constant factor (see also [20]). It turns out that the gap is a bit different in the QC model: there exists a Boolean function f such that its classical weakly unbounded-error QC is $\Omega(\log n)$-times worse than its quantum correspondence. To show this, we will use a probabilistic method requiring the following Chernoff bound lemma from Appendix A of [2].

Lemma 5.2. *Let $S = \{X_i\}$ be a set of N independent random variables with $\Pr[X_i = 1] = \Pr[X_i = -1] = \frac{1}{2}$. Then, $\Pr\left[\left|\sum_{i=1}^N X_i\right| > a\right] < 2e^{-a^2/2N}$.*

Lemma 5.3. *There exists a partial Boolean function f such that $WUC(f) = \Omega(\log n)$ and $WUQ(f) = 2$.*

Proof. We will again consider the Fourier Sampling problem $\text{FS}(F^a, g) = g_a$, which (as shown in Section 4) can be solved exactly with two quantum queries for any choice of g. For the classical lower bound, we fix a string g (to be determined shortly), and assume that g is already known, so the algorithm need only make queries to F^a.

We use Yao's minimax principle [34] that the minimum number of queries required in the worst case for a randomized algorithm to compute some function f with success probability at least p for any input is equal to the maximum, over all

distributions on the inputs, of the minimum number of queries required for a *deterministic* algorithm to compute f correctly on a p fraction of the inputs. Thus, in order to show a lower bound on the number of queries used by any randomized algorithm that succeeds with probability $1/2+\beta$, it suffices to show a lower bound on the number of queries required for a deterministic algorithm to successfully output g_a for a $1/2+\beta$ fraction of the functions F^a (under some distribution). We will use the uniform distribution over all strings F^a – recall that $F^a_x = \sum_i x_i \cdot a_i \mod 2$ – which are also known as *Hadamard codewords*.

Now consider a fixed deterministic algorithm which makes an arbitrary sequence of $\frac{1}{3}\log n$ distinct queries to F^a, and then guesses the bit g_a. There are at most $2^{\frac{1}{3}\log n} = n^{1/3}$ possible answers to the queries (we assume without loss of generality that the algorithm makes exactly $\frac{1}{3}\log n$ queries on all inputs and that $n^{1/3}$ is an integer). Then, the set of n inner product functions $\{F^r \mid r \in \{0,1\}^{\log n}\}$ is divided into at most $k \leq n^{1/3}$ non-empty subsets $S_1, S_2, \ldots, S_k$ of functions compatible with the answers to previous queries. Notice that $|S_i| \geq n^{2/3}$ for all i because each query will either split the set of remaining functions exactly in half, or will do nothing. Each subset will contain between 0 and $|S_i|$ functions F^a such that $g_a = 0$, with the remainder of the functions having $g_a = 1$. For any i, define m^i_0 (resp. m^i_1) as the number of remaining functions $F^a \in S_i$ such that $g_a = 0$ (resp. $g_a = 1$). To succeed on the largest possible fraction of the inputs, the deterministic algorithm should guess the value with which the majority of the remaining bit strings in the subset S_i picked out by the answers to the queries are associated. It is thus easy to see that this deterministic algorithm can succeed on at most a p fraction of the inputs, where $p = \frac{1}{2} + \frac{1}{2n}\sum_{i=1}^{k} |m^i_0 - m^i_1|$. We now turn to finding a g such that this expression is close to $1/2$ for all possible deterministic algorithms.

Our string g will be picked uniformly at random from the set of all n-bit strings. This implies that, for an arbitrary *fixed* deterministic algorithm and for any i, m^i_0 and m^i_1 are random variables. Lemma 5.2 can thus be used to upper bound the fraction of the inputs on which this algorithm succeeds:

$$\Pr[p > 1/2+\beta] \leq \Pr\left[\frac{1}{2n^{2/3}}|m^1_0 - m^1_1| > \beta\right] < 2e^{-2\beta^2 n^{2/3}},$$

where it is sufficient for the bound to consider a fixed i with $|S_i| = n^{2/3}$, w.l.o.g. assuming that this is true for $i = 1$. The remainder of the proof is a simple counting argument. We find a rough upper bound on the number of deterministic algorithms using exactly q queries on every input by noting that such an algorithm is a complete binary tree with $q+1$ levels, where each leaf is labeled with 0 or 1 (corresponding to the output of the algorithm) and each internal node is labeled with a number from $[n]$ (corresponding to the input variable to query). There are thus fewer than $n^{2^{q+1}}$ deterministic algorithms using exactly q queries. For $q = \frac{1}{3}\log n$, there are fewer than $2^{2n^{1/3}\log n}$ algorithms. We can now use a union bound to determine an upper bound on the probability p', taken over random strings g, that *any* of these algorithms succeeds on a $1/2+\beta$ fraction of the inputs.

$$\Pr[p' > 1/2+\beta] < 2^{2n^{1/3}\log n + 1} e^{-2\beta^2 n^{2/3}} < 2e^{2n^{1/3}(\log n - \beta^2 n^{1/3})}.$$

Let us pick $\beta = n^{-1/7}$. It can easily be verified that $\Pr[p' > 1/2+\beta] < 1$ for sufficiently large n, so there exists *some* g such that no classical algorithm that uses at most $\frac{1}{3}\log n$ queries can succeed on more than $1/2 + n^{-1/7}$ of the inputs. By Yao's principle, this implies that for this g, no randomized algorithm that uses at most $\frac{1}{3}\log n$ queries can solve $\mathrm{FS}(F^a, g)$ with a bias greater than $n^{-1/7}$. Therefore, we have the desired separation: $WUQ(\mathrm{FS}) = 2$ (by the proof of Lemma 4.4) while $WUC(\mathrm{FS}) = \Omega(\log n)$. □

Indeed, we can use this function to obtain a more general multiplicative separation between WUC and WUQ.

Theorem 5.4. *Let $T(N)$ be any monotone increasing function satisfying $T(N) \leq N$. Then there exists a partial Boolean function g on N variables such that $WUC(g) = \Omega(T(N)\log(N/T(N)))$ and $WUQ(g) \leq T(N) + 2$.*

Proof. Let $k = T(N)$ and $n = N/T(N)$. For an arbitrary (partial/total) function $f(x_1, \ldots, x_n)$ on n bits, define a new function f^k on $N = nk$ bits by encoding each input bit x_i by the parity of k bits $(y_{i1}, \ldots, y_{ik})$, i.e. $f^k(y_{11}, \ldots, y_{nk}) = f(y_{11} \oplus \cdots \oplus y_{1k}, \ldots, y_{n1} \oplus \cdots \oplus y_{nk})$. By Lemma 3.2, $WUQ(f^k) \leq \lceil k/2 \rceil WUQ(f) \leq (k/2+1)WUQ(f)$. On the contrary, it is essentially immediate that $WUC(f^k) = k\,WUC(f)$ since no sequence of queries to fewer than k of the bits $(y_{i1}, \ldots, y_{ik})$ can guess the parity $(y_{i1} \oplus \cdots \oplus y_{ik})$ with probability $> 1/2$. Taking f to be the FS function, the theorem follows from Lemma 5.3. □

This gap is asymptotically almost optimal, as we show with the following lemma.

Lemma 5.5. *For any Boolean function $f : \{0,1\}^n \to \{0,1\}$, $WUC(f) \leq 2WUQ(f)\log n$.*

Proof. Let $\mathcal{A}$ be an algorithm achieving $WUQ(f)$, i.e., $\mathcal{A}$ uses d queries and has the success probability $1/2+\beta$ such that $WUQ(f) = d + \log(1/2\beta)$. By the result of [6], we know that there exists a polynomial that sign-represents f such that its degree is $2d$, and its bias is β. Now we can use Lemma 3.3, which says that given such a polynomial, we can produce a randomized algorithm using at most $2d$ queries with success probability at least $1/2 + \beta/\sqrt{n^d}$. This implies that $WUC(f) \leq 2d + \log(1/2\beta) + d\log n \leq 2WUQ(f)\log n$. □

By Lemmas 5.3 and 5.5, we obtain the following theorem.

Theorem 5.6. *There exists a partial Boolean function $f : \{0,1\}^n \to \{0,1\}$ such that $WUC(f) = \Theta(WUQ(f)\log n)$.*

5.3. Gaps between WUQ and WUC for Total Functions

In this subsection, we analyze the weakly unbounded-error QC of some specific total Boolean functions. In contrast to the case for partial Boolean functions, our examples have only constant gaps between quantum and classical QCs.

5.3.1. PARITY function

It is straightforward to characterize the unbounded-error QC of the function PARITY : $\{0,1\}^n \to \{0,1\}$, defined as $\mathrm{PARITY}(x) = \oplus_i x_i$. It is a famous result of Minsky and Papert [24] that $sdeg(\mathrm{PARITY}) = n$. With the algorithm of Lemma 3.2, we therefore have $UC(\mathrm{PARITY}) = WUC(\mathrm{PARITY}) = n$, $UQ(\mathrm{PARITY}) = WUQ(\mathrm{PARITY}) = \lceil n/2 \rceil$.

5.3.2. Threshold functions

First, let us consider the function OR : $\{0,1\}^n \to \{0,1\}$ which is defined as follows: $\mathrm{OR}(x) = 1$ iff $|x| \geq 1$, where $|x|$ is the Hamming weight of x. Consider the following single-query randomized algorithm for computing OR. Pick an input bit uniformly at random and query it. If the bit is 1, output 1. If the bit is 0, output 1 with probability $\frac{n-1}{2n-1}$, and 0 otherwise. It is easy to see that this algorithm achieves bias $\frac{1}{4n-2}$, so we have $UC(\mathrm{OR}) = 1$ and $WUC(\mathrm{OR}) \leq \log n + 2$.

In fact, by modifying the probability of outputting 1 properly, the above algorithm can also be used to compute threshold functions TH_k defined by $\mathrm{TH}_k(x) = 1$ if and only if $|x| > k$. Note that AND, OR, and MAJORITY are threshold functions. Without loss of generality, we can assume $k \leq n/2 - 1$, since when $k \geq n/2$ one can consider the threshold function on flipped x. Now, the modified algorithm will output 1 with probability q, or otherwise, with probability $1 - q$ query x at random position, say, i, and output the value of x_i. Therefore, choosing $q = (1/2 - r)/(1 - r)$ for $r = (k + 1/2)/n$, if $|x| \leq k$, then the probability of outputting 1 is at most $q + (1 - q)\frac{k}{n} < 1/2$. Otherwise, it is at least $q + (1 - q)\frac{k+1}{n} > 1/2$. Thus, we have an unbounded-error algorithm for TH_k. Moreover, it is easy to see that the bias is $\Omega(1/n)$, and therefore to conclude that $WUC(\mathrm{TH}_k) = O(\log n)$.

On the other hand, we can lower bound $WUQ(f)$ for *any* non-constant symmetric function f using the polynomial method. Let p be a degree d unbounded-error polynomial representing f with bias β and $0 \leq p(x) \leq 1$ for all $x \in \{0,1\}^n$. By Lemma 3.1, $WUQ(f)$ can be bounded in terms of a tradeoff between d and β, using techniques of [25], which are based on the following well-known lemma of Ehlich and Zeller [14] and Rivlin and Cheney [29]:

Lemma 5.7. *Let p be a degree d polynomial such that, for any integer $0 \leq i \leq n$, $b_1 \leq p(i) \leq b_2$, and for some real $0 \leq x \leq n$, $|p'(x)| \geq c$. Then $d \geq \sqrt{cn/(c + b_2 - b_1)}$.*

In order to use this lemma, we first note that p can be symmetrized [24,25] to produce a univariate polynomial q of degree at most d defined via the following mapping: $q(x) = (\sum_{y,|y|=x} p(y))/\binom{n}{x}$. Since f is not constant, there exists a $k \in \{0, 1, \ldots, n\}$ such that $q(k) \leq 1/2 - \beta$, and that either $q(k-1) \geq 1/2 + \beta$ or $q(k+1) \geq 1/2 + \beta$. Thus, there must exist some x in $[k-1, k]$ (or in $[k, k+1]$) such that $|q'(x)| \geq 2\beta$. By Lemma 5.7, $d \geq \sqrt{2\beta n/(2\beta + 1)}$, which implies that

$$WUQ(f) \geq \min_{\beta} \left(\sqrt{\frac{n\beta}{4\beta + 2}} + \log(1/\beta) \right).$$

To simplify this expression, we note that the elementary inequality $\sqrt{4 + 2/\beta} \leq 1 + 1/\beta$ (for $0 < \beta < 1/\sqrt{3}$) gives

$$WUQ(f) \geq \min_{\beta} \left(\frac{\sqrt{n}}{1 + 1/\beta} + \log(1/\beta) \right).$$

By minimizing this expression over β we see that the minimum is found at

$$\beta = \frac{1}{2} \left(\sqrt{n} \ln 2 - 2 - \sqrt{n(\ln 2)^2 - 4\sqrt{n} \ln 2} \right).$$

Now we can use the series expansion of the square root function to upper bound β as follows:

$$\begin{aligned} \beta &= \frac{1}{2} \left(\sqrt{n} \ln 2 - 2 - \sqrt{n} \ln 2 \sqrt{1 - 4/(\sqrt{n} \ln 2)} \right) \\ &= \frac{1}{2} \left(\sqrt{n} \ln 2 - 2 - \sqrt{n} \ln 2 \left(1 - \frac{2}{\sqrt{n} \ln 2} - \frac{2}{(\ln 2)^2 n} + O(n^{-3/2}) \right) \right) \\ &< \frac{1}{\sqrt{n} \ln 2}. \end{aligned}$$

Given this upper bound on β, it is immediate that $WUQ(f) \geq \log(1/2\beta) \geq (\log n)/2 - O(1)$.

Now we summarize the results on the unbounded-error and weakly unbounded-error QCs of the threshold function.

Theorem 5.8. *$UC(\mathrm{TH}_k) = UQ(\mathrm{TH}_k) = 1$ and $WUC(\mathrm{TH}_k) = WUQ(\mathrm{TH}_k) = \Theta(\log n)$.*

5.4. Other complexity measures

Can we relate UQ or WUQ to any other interesting complexity measures of Boolean functions [12]? One might hope to show that some well-studied property of Boolean functions gives a lower bound on UQ. One of the weakest such measures is *average sensitivity* (also known as *total influence*). The sensitivity of a function $f : \{0,1\}^n \to \{0,1\}$ at input x is defined as $s_x(f) = \sum_{i\in[n]} |f(x) - f(x \oplus e_i)|$, where e_i is the bit string with 1 at position i, and 0 elsewhere. The average sensitivity of f is the average over all x: $\bar{s}(f) = \left(\sum_x s_x(f)\right)/2^n$.

$\bar{s}(f)$ is a lower bound on many other interesting complexity measures, such as block sensitivity and certificate complexity [12]. In particular, Shi [31] has shown that $\bar{s}(f)$ is a lower bound on the bounded error quantum QC of f. However, we now show that $\bar{s}(f)$ can be exponentially larger than even $WUC(f)$. This implies that the unbounded-error complexity models studied in this paper are somehow too weak to be comparable with the usual complexity measures of Boolean functions. The example we use is simply the threshold function $\mathrm{TH}_{n/2}$, or in other words the MAJORITY function.

Lemma 5.9. *Assume n is even. Then $WUC(TH_{n/2}) = O(\log n)$ while $\bar{s}(TH_{n/2}) = \Omega(\sqrt{n})$.*

Proof. The first half follows from the discussion at the start of Section 5.3.2. The second half is folklore; for an explicit proof, note that $s_x(\mathrm{TH}_{n/2}) = 0$ unless $|x| = n/2$ or $|x| = n/2+1$. When $|x| = n/2$, $s_x(\mathrm{TH}_{n/2}) = n/2$, and when $|x| = n/2+1$, $s_x(\mathrm{TH}_{n/2}) = n/2+1$. Thus

$$\bar{s}(\mathrm{TH}_{n/2}) = \frac{1}{2^n}\left(\binom{n}{n/2}\frac{n}{2} + \binom{n}{n/2+1}\left(\frac{n}{2}+1\right)\right) \geq \frac{n}{2^{n+1}}\binom{n}{n/2} \geq \frac{\sqrt{n}}{2\sqrt{\pi}}$$

where we use Stirling's approximation. □

6. Concluding remarks

We have completely characterized the unbounded-error quantum QC as half of its classical counterpart, and have given a lower bound on the weakly unbounded-error quantum QC which is tight for partial functions. However, some open questions remain. For example, for total functions f, is it the case that $WUC(f) = O(WUQ(f))$? One might expect this to be true as total functions do not have big gaps between quantum and classical QCs in the bounded-error setting: there can be at most a polynomial separation between the quantum and classical QCs of total functions [6] while a partial function gives us an exponential gap between them. It is also intriguing to note that the factor of 2 separation between UQ and UC is the same as the maximal known separation between the exact quantum and classical QCs of total Boolean functions – perhaps the techniques here could provide insight into whether this is optimal.

Acknowledgements

AM was supported by the EC-FP6-STREP network QICS, and would like to thank Richard Low for helpful discussions, and in particular for help in simplifying the proof of Theorem 5.8. HN was supported in part by Scientific Research Grant, Ministry of Japan, 19700011.

References

[1] S. Aaronson, A. Ambainis, Quantum search of spatial regions, Theory of Computing 1 (2005) 47–79.
[2] N. Alon, J.H. Spencer, The probabilistic method, in: Wiley-Interscience Series in Discrete Mathematics and Optimization, John-Wiley & Sons, 2000.
[3] A. Ambainis, A note on quantum black-box complexity of almost all Boolean functions, Inform. Process. Lett. 71 (1999) 5–7.
[4] J. Aspnes, R. Beigel, M. Furst, S. Rudich, The expressive power of voting polynomials, Combinatorica 14 (1994) 1–14.
[5] L. Babai, P. Frankl, J. Simon, Complexity classes in communication complexity, in: Proc. 27th FOCS, 1986, pp. 303–312.
[6] R. Beals, H. Buhrman, R. Cleve, M. Mosca, R. de Wolf, Quantum lower bounds by polynomials, J. ACM 48 (2001) 778–797.
[7] R. Beigel, Perceptrons, PP, and the polynomial hierarchy, Comput. Complexity 4 (1994) 339–349.
[8] M. Bellare, The Goldreich–Levin Theorem, Lecture note, 1999. Available at: http://cseweb.ucsd.edu/users/mihir/papers/gl.pdf.
[9] E. Bernstein, U. Vazirani, Quantum complexity theory, SIAM J. Comput. 26 (1997) 1411–1473.
[10] H. Buhrman, R. Cleve, A. Wigderson, Quantum vs. classical communication and computation, in: Proc. 30th STOC, 1998, pp. 63–68.
[11] H. Buhrman, N. Vereshchagin, R. de Wolf, On computation and communication with small bias, in: Proc. 22nd CCC, 2007, pp. 24–32.
[12] H. Buhrman, R. de Wolf, Complexity measures and decision tree complexity: a survey, Theoret. Comput. Sci. 288 (2002) 21–43.
[13] W. van Dam, Quantum oracle interrogation: getting all information for almost half the price, in: Proc. 39th FOCS, 1998, pp. 362–367.
[14] H. Ehlich, K. Zeller, Schwankung von Polynomen zwischen Gitterpunkten, Mathematische Zeitschrift 86 (1964) 41–44.
[15] E. Farhi, J. Goldstone, S. Gutmann, M. Sipser, A limit on the speed of quantum computation in determining parity, Phys. Rev. Lett. 81 (1998) 5442–5444.
[16] J. Forster, A linear lower bound on the unbounded error probabilistic communication complexity, J. Comput. Syst. Sci. 65 (2002) 612–625.
[17] B. Halstenberg, R. Reischuk, Relations between communication complexity classes, J. Comput. Syst. Sci. 41 (1990) 402–429.
[18] P. Høyer, R. de Wolf, Improved quantum communication complexity bounds for disjointness and equality, in: Proc. 19th STACS, 2002, pp. 299–310.
[19] K. Iwama, H. Nishimura, R. Raymond, S. Yamashita, Unbounded-error one-way classical and quantum communication complexity, in: Proc. 34th ICALP, 4596, 2007 110–121.
[20] K. Iwama, H. Nishimura, R. Raymond, S. Yamashita, Unbounded-error classical and quantum communication complexity, in: Proc. 18th ISAAC, 4835, 2007, pp. 100–111.
[21] H. Klauck, Lower bounds for quantum communication complexity, SIAM J. Comput. 37 (2007) 20–46.
[22] F. Le Gall, Quantum Weakly nondeterministic communication complexity, Proc. 31st MFCS, 2006, pp. 658–669.
[23] S. Massar, D. Bacon, N. Cerf, R. Cleve, Classical simulation of quantum entanglement without local hidden variables, Phys. Rev. A 63 (2001) 052305.

[24] M. L. Minsky, S. A. Papert, Perceptrons, MIT Press, Cambridge, MA, 1988.
[25] N. Nisan, M. Szegedy, On the degree of Boolean functions as real polynomials, Comput. Complexity 4 (1994) 301–313.
[26] R. O'Donnell, R.A. Servedio, Extremal properties of polynomial threshold functions, J. Comput. Syst. Sci. 74 (2008) 298–312.
[27] R. Paturi, J. Simon, Probabilistic communication complexity, J. Comput. Syst. Sci. 33 (1986) 106–123.
[28] A. A. Razborov, Quantum communication complexity of symmetric predicates, Izvestiya Math. 67 (2003) 145–149 (English version).
[29] T.J. Rivlin, E.W. Cheney, A comparison of Uniform Approximations on an interval and a finite subset thereof, SIAM J. Numer. Anal. 3 (1966) 311–320.
[30] A. Sherstov, Halfspace matrices, Comput. Complexity 17 (2008) 149–178.
[31] Y. Shi, Lower bounds of quantum black-box complexity and degree of approximating polynomials by influence of Boolean variables, Inform. Process. Lett. 75 (2000) 79–83.
[32] R. de Wolf, Quantum Computing and Communication Complexity, University of Amsterdam, 2001.
[33] R. de Wolf, Nondeterministic quantum query and communication complexities, SIAM J. Comput. 32 (2003) 681–699.
[34] A.C-C. Yao, Probabilistic computations: toward a unified measure of complexity, in: Proc. 18th FOCS, 1977, pp. 222–227.
[35] S. Zhang, On the tightness of the Buhrman–Cleve–Wigderson simulation, in: Proc. 20th ISAAC, 2009, pp. 434–440.