

Complexity Upper Bounds for Classical Locally Random Reductions Using a Quantum Computational Argument*

Rahul Tripathi

Department of Computer Science and Engineering, University of South Florida,
Tampa, FL 33620, USA (Email: tripathi@cse.usf.edu)

Abstract. We use a *quantum computational* argument to prove, for any integer $k \geq 2$, a complexity upper bound for nonadaptive k -query classical locally random reductions (LRRs) that allow bounded-errors. Extending and improving a recent result of Pavan and Vinodchandran [PV], we prove that if a set L has a nonadaptive 2-query classical LRR to functions g and h , where both g and h can output $O(\log n)$ bits, such that the reduction succeeds with probability at least $1/2 + 1/\text{poly}(n)$, then $L \in \text{PP}^{\text{NP}}/\text{poly}$. Previous complexity upper bound for nonadaptive 2-query classical LRRs was known only for much restricted LRRs: LRRs in which the target functions can only take values in $\{0, 1, 2\}$ and the error probability is zero [PV]. For $k > 2$, we prove that if a set L has a nonadaptive k -query classical LRR to *boolean* functions g_1, g_2, \dots, g_k such that the reduction succeeds with probability at least $2/3$ and the distribution on $(k/2 + \sqrt{k})$ -element subsets of queries depends only on the input length, then $L \in \text{PP}^{\text{NP}}/\text{poly}$. Previously, for no constant $k > 2$, complexity upper bound for nonadaptive k -query classical LRRs was known even for LRRs that do not make errors.

Our proofs follow a two stage argument: (1) simulate a nonadaptive k -query classical LRR by a 1-query quantum *weak* LRR, and (2) upper bound the complexity of this quantum weak LRR. To carry out the two stages, we formally define nonadaptive quantum weak LRRs, and prove that if a set L has a 1-query quantum weak LRR to a function g , where g can output *polynomial* number of bits, such that the reduction succeeds with probability at least $1/2 + 1/\text{poly}(n)$, then $L \in \text{PP}^{\text{NP}}/\text{poly}$.

1 Introduction

1.1 Background

A *locally random reduction* (LRR) of a set L to a database f is an efficient computational procedure that allows to determine the membership of any instance x in L by using random queries to the database. The concept of LRR is motivated from the standpoint of cryptographic security and can be understood from the following example. Suppose Alice holds an object (encoded as a binary string)

* Research supported by the New Researcher Grant of University of South Florida.

and wants to efficiently retrieve some information about the object by using queries to Bob (database f). However for security reasons, Alice cannot reveal her object to Bob. Therefore, she makes random queries to Bob so that Bob gets no clue about the object from the queries. An LRR is an efficient computational procedure that allows Alice to retrieve the information without leaking Bob anything more than the size of the object. (See Section 2.4 for a more general definition of LRR.) An LRR where the set L and the database f are the same, i.e., f is the characteristic function of L is called a *random self-reduction* (RSR).

In general, one can define an LRR of a set L to *several* databases f_1, f_2, \dots, f_k such that the reduction (1) is an efficient randomized procedure, (2) allows determining the membership of any instance x in L with bounded-error probability by using random queries $\alpha_1, \alpha_2, \dots, \alpha_k$ to f_1, f_2, \dots, f_k , respectively, and (3) leaks no detail more than $|x|$ to an adversary even if the adversary is revealed any subset of at most t queries, for some fixed $t \geq 1$. For the special case $f_1 = f_2 = \dots = f_k = f$, Beaver et al. [BFKR97] called this reduction a (t, k) -locally random reduction of L to f . This general notion of LRR subsumes earlier studied notions of random reductions known as *single-oracle* [AFK89] and *multioracle* [Riv86] instance-hiding schemes. Here “leaking no detail more than $|x|$ to an adversary even if the adversary is revealed any subset of t queries” has the following interpretation: If instances x and y are such that $|x| = |y|$, then for any i_1, i_2, \dots, i_t , the distribution on the t queries $\langle \alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_t} \rangle$ induced by the randomized reduction on input x is identical to the distribution induced by the randomized reduction on input y . Thus, from the viewpoint of an adversary who has access to some subset of t queries, any instance y of length $|x|$ is equally likely to be the input of the reduction.

Both LRR and RSR have proved to be useful at several places in computational complexity theory. They have found implicit or explicit applications in worst-case to average-case reductions [Lip91], random oracle separations [Bab87], interactive proof systems [BFL91,LFKN92,Sha92], program checkers and self-testing/correcting pairs [BK95,Lip91,BLR93], probabilistically checkable proof systems [AS98,ALM⁺98,FGL⁺96], cryptography [GM84,BM84], instance hiding schemes [Riv86,AFK89,BF90,BFKR97], zero knowledge proofs on committed bits [BFKR97], private information retrieval [BFG06], and locally decodable codes [PV].

1.2 Related Work

A direct consequence of a result of Beaver and Feigenbaum [BF90] is that for every set L , there is a function f such that L is $(n + 1)$ -query locally random reducible to f . Beaver, Feigenbaum, Kilian, and Rogaway [BFKR97] extended

and improved this result: For any constant $c > 0$ and any function $t : \mathbb{N} \rightarrow \mathbb{N}$, every set L is $t\lfloor n/c \log n \rfloor$ -query locally random reducible to some function f , where the distribution on t -element subsets of queries depends only on n and where the lengths of answers from f could be $\Theta(\log n + \log t)$.

There have been work on understanding the complexity of functions that can be locally random reduced via k queries to some function f , for constants $k \geq 1$. Abadi, Feigenbaum, and Kilian [AFK89] proved that if a set L is 1-query locally random reducible to some function, then L is in $\text{NP/poly} \cap \text{coNP/poly}$. Yao [Yao90] proved that if a set L is 2-query locally random reducible to some *boolean* function, then L is in PSPACE/poly . Fortnow and Szegedy [FS92] improved upon Yao's result and showed that any such set in fact belongs to $\text{NP/poly} \cap \text{coNP/poly}$. Pavan and Vinodchandran [PV] addressed the question whether the results of Yao, and Fortnow and Szegedy can be extended for LRRs where the reductions are to functions other than the boolean functions. Building on the work of Yao [Yao90] and Fortnow and Szegedy [FS92], they proved that if a set L is 2-query locally random reducible to functions g and h that take values in $\{0, 1, 2\}$, then L is in PSPACE/poly . The LRRs considered in the last three papers, i.e., in [Yao90,FS92,PV] do not allow errors.

1.3 Our Results

A comparison of our results with previously known results is summarized in Table 1. The notations “ (t, k, ℓ, ϵ) -clr” and “ (t, k, ℓ, ϵ) -qwlr,” used in Table 1, capture generalizations of previously studied notions of classical LRRs. They are defined as follows: (a) A nonadaptive (t, k, ℓ, ϵ) -clr is an LRR of a set L to some functions g_1, g_2, \dots, g_k such that (1) the reduction makes k nonadaptive queries $\alpha_1, \alpha_2, \dots, \alpha_k$ to g_1, g_2, \dots, g_k , respectively, (2) the distribution on t -element subsets of queries $\langle \alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_t} \rangle$ is dependent only on the input length n to the reduction, (3) each g_i returns $\ell(n)$ bits on input length n to the reduction, and (4) the reduction succeeds with probability at least $1/2 + \epsilon(n)$, and (b) A nonadaptive (t, k, ℓ, ϵ) -qwlr is a *quantum* analog of (t, k, ℓ, ϵ) -clr, where the reduction can be a bounded-error quantum polynomial-time algorithm that can make quantum queries. (See Definition 3 and Definition 4 for a formal definition of these notions.) For notational convenience, if the answers returned by the target functions in LRRs can only take values in $\{0, 1, 2\}$, then for such reductions we define the number of answer bits ℓ to be $3/2$ (see, for instance, the second column of Table 1 in the entry corresponding to [PV]).

Note that our proofs for classical LRRs use quantum computational arguments. The application of quantum arguments in proving results related to classical computing is a surprising phenomenon witnessed only in the last few years. See, for instance, the papers [KdW04,WdW05,AR03,AR05,Aar05,dW06,Ker05,LLS05,Aar06]

| Papers | Type of nonadaptive LRRs (t, k, ℓ, ϵ)-clr / (t, k, ℓ, ϵ)-qwlr | Complexity Upper Bound |
|-------------------|--|-----------------------------|
| [AFK89] | (1, 1, poly(n), 1/poly(n))-clr | NP/poly \cap coNP/poly |
| [Yao90] | (1, 2, 1, 1/2)-clr | PSPACE/poly |
| [FS92] | (1, 2, 1, 1/2)-clr | NP/poly \cap coNP/poly |
| [BFKR97] | ($t, t \lfloor n/O(\log n) \rfloor, O(\log n + \log t), 1/2$)-clr | None |
| [PV] | (1, 2, 3/2, 1/2)-clr | PSPACE/poly |
| This paper | (1, 2, $O(\log n)$, 1/poly(n))-clr | PP^{NP}/poly |
| This paper | ($k/2 + \sqrt{k}, k, 1, 1/6$)-clr | PP^{NP}/poly |
| This paper | (1, 1, poly(n), 1/poly(n))-qwlr | PP^{NP}/poly |

Table 1. Summary of results showing complexity upper bounds for various nonadaptive LRRs.

where quantum computational arguments have been used to prove classical complexity results.) This paper fits in this growing body of research on proving classical complexity results using quantum computational arguments. Our results also shed light on the role of quantum computational arguments in the understanding of classical computation.

2 Preliminaries

2.1 Notations

Let \mathbb{N} denote the set of all positive integers. Our alphabet is $\Sigma = \{0, 1\}$. For a binary string $b \in \Sigma^\ell$, we use b_i to denote its i 'th bit. We identify a binary string $b \in \Sigma^\ell$ alternatively as a bit vector $\mathbf{b} = (b_1, b_2, \dots, b_\ell)$. Given two binary strings $a, b \in \Sigma^\ell$, their *inner product* $\mathbf{a} \cdot \mathbf{b}$ is the integer $\mathbf{a} \cdot \mathbf{b} =_{df} \sum_{i=1}^{\ell} a_i \cdot b_i$, and their *xor* is the binary string $a \oplus b$ obtained by taking the xor of the individual bits of a and b , i.e., $a \oplus b =_{df} (a_1 \oplus b_1) \dots (a_\ell \oplus b_\ell)$. For a string $a \in \Sigma^\ell$, we use $|a|$ to denote the number of 1's in a and for a set A , we use $|A|$ to denote the cardinality of A (which sense is being used for " \cdot " will be clear from the context). For a binary string $b \in \Sigma^\ell$, let $\text{int}(b) \in \{0, 1, \dots, 2^\ell - 1\}$ denote the integer representation of b . Let $[n] =_{df} \{1, 2, \dots, n\}$ for all $n \in \mathbb{N}$.

2.2 Basics of Quantum Computing

Let \mathcal{H} denote a two-dimensional Hilbert space, i.e., a complex vector space equipped with an inner product $\langle \cdot | \cdot \rangle$ operation. A qubit $|u\rangle =_{df} (\alpha, \beta)^T$ represent the states $|0\rangle$ and $|1\rangle$, respectively, associated with a qubit. The states $|0\rangle$ and $|1\rangle$ are called the *computational basis* states. We can express the qubit $|u\rangle$

as a linear combination of the computational basis states: $|u\rangle = \alpha|0\rangle + \beta|1\rangle$. Here α and β are complex numbers, called the *amplitudes* of $|u\rangle$. Since $|u\rangle$ is a unit vector, the amplitudes (of $|u\rangle$) must satisfy $|\alpha|^2 + |\beta|^2 = 1$.

An m -qubit is a unit vector in the 2^m -dimensional Hilbert space $\mathcal{H}^{\otimes m} =_{df} \mathcal{H} \otimes \cdots \otimes \mathcal{H}$, the m -fold tensor product of \mathcal{H} with itself. A multiple qubit is an m -qubit for some integer $m > 1$. The computational basis states of $\mathcal{H}^{\otimes m}$ are the m -fold tensor product of the computational basis states of \mathcal{H} . That is, they are $|b_1\rangle \otimes \cdots \otimes |b_m\rangle$, where for each $1 \leq i \leq m$, b_i ranges over 0 and 1. The vector representation of a computational basis state $|b_1\rangle \otimes \cdots \otimes |b_m\rangle$ is the column vector with 2^m rows in which the only row containing 1 is at location $1 + \text{int}(b_1 b_2 \dots b_m)$ and all other rows contain 0. We sometimes use the standard abbreviation $|a\rangle|b\rangle$ for $|a\rangle \otimes |b\rangle$, where $|a\rangle$ and $|b\rangle$ can be arbitrary multiple qubits. An m -qubit $|u\rangle =_{df} (\alpha_{0^m}, \alpha_{0^{m-1}1}, \dots, \alpha_{1^m})^T$ can be expressed as a linear combination of the computation basis states of $\mathcal{H}^{\otimes m}$: $|u\rangle = \sum_{i \in \Sigma^m} \alpha_i |i\rangle$. Here, the complex numbers α_i s are the amplitudes of $|u\rangle$. These amplitudes satisfy $\sum_{i \in \Sigma^m} |\alpha_i|^2 = 1$ because $|u\rangle$ is a unit vector in $\mathcal{H}^{\otimes m}$.

The conjugate transpose of a vector $|u\rangle$, i.e., $|u\rangle^\dagger$, is denoted by $\langle u|$. The inner product $\langle \cdot | \cdot \rangle$ of vectors $|u\rangle$ and $|v\rangle$ can be expressed as: $\langle u|v\rangle = \langle u| \cdot |v\rangle$, i.e., the matrix product of $\langle u|$ and $|v\rangle$. The vectors $|u\rangle$ and $|v\rangle$ are orthogonal if their inner product $\langle u|v\rangle$ is zero. The norm of $|u\rangle$ is $\|u\| =_{df} \sqrt{\langle u|u\rangle}$.

A quantum system that can take one of a number of states $|\psi_i\rangle$ with respective probabilities p_i is said to be in a *mixed* state. A quantum system whose state is known exactly is said to be in *pure* state. (Thus, a pure quantum state is also a mixed quantum state, but not the vice-versa.) A mixed quantum state is described by an ensemble $\{p_i, |\psi_i\rangle\}$ of pure quantum states. We can equivalently describe this mixed quantum state in terms of the density operator ρ : $\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i|$. In particular, for a pure quantum state $|\psi\rangle$, the density operator is $|\psi\rangle \langle \psi|$.

Any operation on a quantum system is either a *unitary* operation or a measurement operation. A unitary operation is described by a linear transformation U , which preserves the ℓ_2 norm: for any state $|\psi\rangle$, $\| |\psi\rangle \| = \| U|\psi\rangle \|$. When a unitary operation U is performed on a state $|\psi\rangle$, the resulting state is $U|\psi\rangle$. In the terminology of density operators, U transforms the state ρ into state $U\rho U^\dagger$.

The most general measurement in quantum mechanics is the POVM measurement, which is described by a collection of positive semidefinite measurement operators $E_m = M_m^\dagger M_m$ satisfying $\sum_m E_m = I$. If a measurement described by the measurement operators E_m is performed on a quantum system in state $|\psi\rangle$, then the probability $p(m)$ of getting outcome m is given by $p(m) =_{df} \langle \psi | M_m^\dagger M_m | \psi \rangle = \langle \psi | E_m | \psi \rangle$ and the resulting state is $\frac{M_m |\psi\rangle}{\sqrt{p(m)}}$. In the terminology of density operators ρ , the probability $p(m)$ is given by $p(m) =_{df}$

$\text{Tr}(M_m \rho M_m^\dagger) = \text{Tr}(E_m \rho)$ and the resulting state is $\frac{M_m \rho M_m^\dagger}{p(m)}$. By *measuring in the computational basis* of a 2^m -dimensional Hilbert space $\mathcal{H}^{\otimes m}$, we mean that we perform a measurement whose measurement operators E_m are given by $E_m = M_m = |\psi_m\rangle\langle\psi_m|$, where $|\psi_m\rangle$ s are the computational basis states of $\mathcal{H}^{\otimes m}$.

A *bipartite* quantum system consists of two subsystems. Let \mathcal{H} and \mathcal{K} be Hilbert spaces and let ρ be the density operator of a bipartite quantum system over the Hilbert space $\mathcal{H} \otimes \mathcal{K}$. A *partial trace* $\text{Tr}_{\mathcal{K}}$ of ρ over \mathcal{K} is the following mapping: $\text{Tr}_{\mathcal{K}}(\rho) = \sum_{j=1}^n (I \otimes \langle e_j |) \rho (I \otimes |e_j\rangle)$, where $\{|e_1\rangle, |e_2\rangle, \dots, |e_n\rangle\}$ is any orthonormal basis of \mathcal{K} . Intuitively, the *partial trace* $\text{Tr}_{\mathcal{K}}(\rho)$ of a mixed state ρ of a bipartite system over the Hilbert space $\mathcal{H} \otimes \mathcal{K}$ is the density operator of the first part (i.e., \mathcal{H}) of the system obtained by discarding the second part (i.e., \mathcal{K}) of the system.

We will consider quantum queries whose answers are ℓ bits long, for some $\ell \geq 1$. A quantum query to an oracle $\mathcal{O} : \Sigma^m \rightarrow \Sigma^\ell$ is the unitary transformation given by $|s\rangle|z\rangle \rightarrow |s\rangle|z \oplus \mathcal{O}(s)\rangle$, where $z \in \Sigma^\ell$ is called the target register. For convenience, we store the query answer in the phase of the quantum state instead of storing it in the target register. To store the answer in the phase, define for any $R \in \Sigma^\ell$, the quantum state $|z_R\rangle = \frac{1}{\sqrt{2^\ell}} \bigotimes_{i=1}^\ell (|0\rangle + (-1)^{R_i} |1\rangle)$. A quantum query to an oracle $\mathcal{O} : \Sigma^m \rightarrow \Sigma^\ell$ then, for any $R \in \Sigma^\ell$, maps $|s\rangle|z_R\rangle$ to $(-1)^{R \cdot \mathcal{O}(s)} |s\rangle|z_R\rangle$.

Finally, we refer the reader to the excellent textbook [NC00] for any relevant concept in quantum computing that is not explained here.

2.3 Complexity Classes

The quantum complexity class BQP/qpoly is the class of all sets decidable by a polynomial-time quantum computer when given a polynomial-size quantum advice state, which depends only on the input length.

Definition 1. BQP/qpoly is the class of all sets L for which there exist a polynomial-size quantum circuit family $\{C_n\}_{n \in \mathbb{N}}$ and a polynomial-size family of quantum states $\{|\Psi_n\rangle\}_{n \in \mathbb{N}}$ such that for all $n \in \mathbb{N}$ and $x \in \Sigma^n$,

1. if $x \in L$, then C_n accepts $|x\rangle|\Psi_n\rangle$ with probability at least $2/3$, and
2. if $x \notin L$, then C_n accepts $|x\rangle|\Psi_n\rangle$ with probability at most $1/3$.

We will require the following result of Aaronson [Aar04] on the power of BQP/qpoly. This result holds in every relativized world.

Theorem 2. [Aar04] BQP/qpoly \subseteq PP/poly.

2.4 Locally Random Reduction

Beaver et al. [BFKR97] formally introduced the notion of LRRs. They defined LRRs that reduce a function f to a *single* function g using k random queries, succeed with probability at least $3/4$, and leak no detail more than $|x|$ even if any t -element subset of queries is revealed.

We present a more general definition of (nonadaptive) LRRs in Definition 3. This new definition also takes into account the number of answer bits returned by the target functions and the success probability of the reduction.

Definition 3 (Nonadaptive Classical Locally Random Reduction). *Let $t, k \in \mathbb{N}$, $\ell : \mathbb{N} \rightarrow \mathbb{N}$, and $\epsilon : \mathbb{N} \rightarrow (0, 1/2]$. A set L is nonadaptively (t, k, ℓ, ϵ) -classically-locally-random (or, “nonadaptively (t, k, ℓ, ϵ) -clr” in short) reducible to functions g_1, g_2, \dots, g_k , where each g_i outputs $\ell(n)$ bits on inputs of length n to the reduction, if there exist a classical bounded-error probabilistic polynomial-time algorithm A , a polynomial-time function σ , and a polynomial $p(\cdot)$ such that:*

1. **[Query Reduction]** *For all $n \in \mathbb{N}$, $x \in \Sigma^n$, and $r \in \Sigma^{p(n)}$, A makes k nonadaptive queries $\sigma(1, x, r), \sigma(2, x, r), \dots, \sigma(k, x, r)$ to g_1, g_2, \dots, g_k , respectively.*
2. **[Local Randomness]** *For all $n \in \mathbb{N}$ and $\{i_1, i_2, \dots, i_t\} \subseteq [k]$, if $r \in \Sigma^{p(n)}$ is chosen uniformly at random, then for any $x, y \in \Sigma^n$, the distribution on $\langle \sigma(i_1, x, r), \sigma(i_2, x, r), \dots, \sigma(i_t, x, r) \rangle$ is identical to that on $\langle \sigma(i_1, y, r), \sigma(i_2, y, r), \dots, \sigma(i_t, y, r) \rangle$.*
3. **[Correctness]** *For all $n \in \mathbb{N}$ and $x \in \Sigma^n$, it holds that*

$$\text{Prob}_r [A(x, r, g_1(\sigma(1, x, r)), \dots, g_k(\sigma(k, x, r))) = L(x)] \geq \frac{1}{2} + \epsilon,$$

where the probability is over the uniform random choice of $r \in \Sigma^{p(n)}$.

If the algorithm A receives $h(n)$ bits of advice on input length n , then we say that L is nonuniformly nonadaptively (t, k, ℓ, ϵ) -clr reducible to functions g_1, g_2, \dots, g_k with $h(n)$ bits of advice.

Our proofs of complexity upper bounds for nonadaptive classical LRRs use (as a tool) the notion of nonadaptive quantum *weak* LRRs, defined in Definition 4. We mention that our notion may not fully capture the most general notion of nonadaptive quantum LRRs.¹

¹ Definition 4 may not fully capture nonadaptive quantum LRRs in the most general way for the following two reasons: (1) In the *query reduction* property, we require the quantum algo-

Definition 4 (Nonadaptive Quantum Weak Locally Random Reduction).

Let $t, k \in \mathbb{N}$, $\ell : \mathbb{N} \rightarrow \mathbb{N}$, and $\epsilon : \mathbb{N} \rightarrow (0, 1/2]$. A set L is nonadaptively (t, k, ℓ, ϵ) -quantumly-weakly-locally-random (or, “nonadaptively (t, k, ℓ, ϵ) -qwlr” in short) reducible to functions g_1, g_2, \dots, g_k , where each g_i outputs $\ell(n)$ bits on inputs of length n to the reduction, if there exist a bounded-error quantum polynomial-time algorithm A , and polynomials $p(\cdot)$ and $q(\cdot)$ such that:

1. **[Query Reduction]** For all $n \in \mathbb{N}$, $x \in \Sigma^n$, A uniformly at random selects a string $r \in \Sigma^{p(n)}$, deterministically computes k sets of strings $T_{x,r}^1, T_{x,r}^2, \dots, T_{x,r}^k \subseteq \Sigma^{q(n)}$, and makes k quantum queries of the form: $|Q(x, r)\rangle =$

$$\frac{1}{\sqrt{\prod_{i=1}^k |T_{x,r}^i|}} \sum_{s_{j_1} \in T_{x,r}^1} \sum_{s_{j_2} \in T_{x,r}^2} \cdots \sum_{s_{j_k} \in T_{x,r}^k} |s_{j_1}, s_{j_2}, \dots, s_{j_k}\rangle \otimes |\psi\rangle^{\otimes k},$$

where $|\psi\rangle = \frac{1}{\sqrt{2^\ell}} \sum_{R \in \Sigma^\ell} |z_R\rangle$. Also, each $T_{x,r}^i \subseteq \Sigma^{q(n)}$ depends only on i , x , and r , and $|T_{x,r}^i|$ depends only on i and n .

2. **[Local Randomness]** For all $n \in \mathbb{N}$ and $\{i_1, i_2, \dots, i_t\} \subseteq [k]$, and for any $x \in \Sigma^n$, the distribution on strings at locations i_1, i_2, \dots, i_t induced by measuring the query state $\frac{1}{\sqrt{2^{p(n)}}} \sum_{r \in \Sigma^{p(n)}} |r\rangle |Q(x, r)\rangle$ in the computational basis is independent of x , but may perhaps depend on n . In other words, if $r \in \Sigma^{p(n)}$ is chosen uniformly at random, then for any $x, y \in \Sigma^n$ and for all $s_1, s_2, \dots, s_t \in \Sigma^{q(n)}$, it holds that

$$\text{Prob}_r [s_1 \in T_{x,r}^{i_1} \wedge \dots \wedge s_t \in T_{x,r}^{i_t}] = \text{Prob}_r [s_1 \in T_{y,r}^{i_1} \wedge \dots \wedge s_t \in T_{y,r}^{i_t}].$$

algorithm A , on input x , to randomly select $r \in \Sigma^{p(n)}$ and generate a superposition over strings belonging to the polynomial-time computable sets $T_{x,r}^i$, for $1 \leq i \leq k$. Meaning, the quantum state describing the quantum queries just before their answers are received is given by $|\Phi\rangle =_{df} \frac{1}{\sqrt{2^{p(n)}}} \sum_{r \in \Sigma^{p(n)}} |r\rangle |Q(x, r)\rangle$. While this requirement on the form of $|\Phi\rangle$ helps to serve our purpose, which is obtaining complexity upper bounds for nonadaptive classical LRRs, it may not be an essential requirement for the most general definition of quantum LRRs. (2) In the *local randomness* property, we consider measurements only in the *computational basis*. Again, we restrict to only such measurements because they suffice to obtain complexity upper bounds for nonadaptive classical LRRs. If we consider general (POVM) measurements, then the *local randomness* property may be stated as follows:

Let ρ_x denote the density operator describing the state $|\Phi\rangle$ of the quantum queries just before their answers are received, i.e., $\rho_x = |\Phi\rangle\langle\Phi|$.

[Local Randomness] For all $n \in \mathbb{N}$, $\{i_1, i_2, \dots, i_t\} \subseteq [k]$, and for any $x, y \in \Sigma^n$, it holds that

$$\text{Tr}_{r, [k] - \{i_1, i_2, \dots, i_t\}}(\rho_x) = \text{Tr}_{r, [k] - \{i_1, i_2, \dots, i_t\}}(\rho_y),$$

where $\text{Tr}_{r, [k] - \{i_1, i_2, \dots, i_t\}}(\rho_x)$ denotes the reduced density operator obtained by taking the partial trace of ρ_x over the qubits storing r and the qubits corresponding to the query locations $[k] - \{i_1, i_2, \dots, i_t\}$.

3. **[Correctness]** For all $n \in \mathbb{N}$ and $x \in \Sigma^n$, it holds that

$$\text{Prob}_{r,A} [A(x, r, g_1 \circ g_2 \circ \dots \circ g_k(|Q(x, r)\rangle)) = L(x)] \geq \frac{1}{2} + \epsilon,$$

where the probability is over the uniform random choice of $r \in \Sigma^{p(n)}$ and over the inherent randomness of A . Here $g_1 \circ g_2 \circ \dots \circ g_k(|Q(x, r)\rangle)$ denotes

$$\frac{1}{\sqrt{\prod_{i=1}^k |T_{x,r}^i|}} \sum_{s_{j_1} \in T_{x,r}^1} \dots \sum_{s_{j_k} \in T_{x,r}^k} |s_{j_1}, \dots, s_{j_k}\rangle \otimes \left(\bigotimes_{i=1}^k \frac{1}{\sqrt{2^\ell}} \sum_{R \in \Sigma^\ell} (-1)^{\mathbf{R} \cdot \mathbf{g}_i(s_{j_i})} |z_R\rangle \right),$$

i.e., the outcome of the queries to the functions g_1, \dots, g_k .

If the algorithm A receives $h(n)$ bits (qubits) of advice on input length n , then we say that L is nonuniformly nonadaptively (t, k, ℓ, ϵ) -qwlr reducible to functions g_1, g_2, \dots, g_k with $h(n)$ bits (respectively, qubits) of classical (respectively, quantum) advice.

3 Results

3.1 The Case of Two Queries

Theorem 5 shows that a nonadaptive 2-query classical LRR with answer length ℓ and success probability at least $1/2 + \epsilon$ can be simulated by a 1-query quantum weak LRR with success probability at least $1/2 + \epsilon/2^\ell$. This simulation of nonadaptive 2-query classical LRRs by 1-query quantum weak LRRs along with Theorem 6, which proves a complexity upper bound for 1-query quantum weak LRRs, allow us to obtain a complexity upper bound for nonadaptive 2-query classical LRRs.

The proofs of Theorem 5 and Theorem 6 are inspired from those in the papers by Kerenidis and de Wolf [KdW04] and Wehner and de Wolf [WdW05]. However, there are at least two technical features that indicate that our proofs are conceptually different from those in [KdW04, WdW05]. First, efficiency of algorithms is an issue in our proofs (since LRRs are required to be efficient algorithms), whereas efficiency is not an issue in the papers [KdW04, WdW05] (since algorithms in these papers are for information-theoretic LDCs and PIRs). Second, we do not require any major result from quantum information theory in our proofs, whereas the proofs in [KdW04, WdW05] use Nayak's [Nay99] linear lower bound on the length of quantum random access codes. Nayak's [Nay99] lower bound proof in turn requires some deep results from quantum information theory.

Theorem 5. *Let $\ell(n) = \text{poly}(n)$ and $\epsilon(n) \in (0, 1/2]$. If a set L is nonadaptively $(1, 2, \ell, \epsilon)$ -clr reducible to functions g_1 and g_2 , then L is $(1, 1, \ell, \frac{\epsilon}{2\ell})$ -qwlr reducible to some function g . Here, each of g_1 , g_2 , and g outputs $\ell(n)$ bits on inputs of length n to their corresponding reductions.*

Theorem 6 shows that any set that has a 1-query quantum weak LRR in which the target function outputs *polynomial* number of bits and the reduction succeeds with probability at least $1/2 + 1/\text{poly}(n)$ is in $\text{BQP}^{\text{NP}}/\text{qpoly}$.

Theorem 6. *Let $\ell(n) = \text{poly}(n)$ and $\epsilon(n) = 1/\text{poly}(n) \in (0, 1/2]$. If a set L is $(1, 1, \ell, \epsilon)$ -qwlr reducible to a function g , where g outputs $\ell(n)$ bits on inputs of length n to the reduction, then L is in $\text{BQP}^{\text{NP}}/\text{qpoly}$.*

Aaronson [Aar04] gave a relativizable proof of the inclusion $\text{BQP}/\text{qpoly} \subseteq \text{PP}/\text{poly}$. As a consequence, we obtain the following corollary of Theorem 5 and Theorem 6.

Corollary 7. *Let $\ell(n) = O(\log n)$ and $\epsilon(n) = 1/\text{poly}(n) \in (0, 1/2]$. If a set L is nonadaptively $(1, 2, \ell, \epsilon)$ -clr reducible to functions g_1, g_2 , where each g_i outputs $\ell(n)$ bits on inputs of length n to the reduction, then $L \in \text{PP}^{\text{NP}}/\text{poly}$.*

Note that Theorem 6 holds even if the reduction is nonuniform and requires a polynomial-size quantum advice state. Thus, we get the following strengthening of Theorem 6.

Theorem 8. *Let $\ell = \text{poly}(n)$ and $\epsilon(n) = 1/\text{poly}(n) \in (0, 1/2]$. If a set L is nonuniformly $(1, 1, \ell, \epsilon)$ -qwlr reducible to a function g with a polynomial-size quantum advice, then L is in $\text{BQP}^{\text{NP}}/\text{qpoly}$. Here g outputs $\ell(n)$ bits on inputs of length n to the reduction.*

3.2 The Case of More Than Two Queries and Binary Answers

Theorem 5 shows that a nonadaptive 2-query classical LRR can be simulated by a 1-query quantum weak LRR. We show in Theorem 9 that, for any constant $k > 2$, a nonadaptive k -query classical LRR can also be simulated by a 1-query quantum weak LRR provided that in the classical LRR, the target functions are boolean and the distribution on sufficiently large subsets of queries depends only on the input length.

Theorem 9. *Let $k > 2$ be some fixed integer and let $\epsilon \in (0, 1/2]$ be a fixed constant. If a set L is nonadaptively $(k/2 + O(\sqrt{k}), k, 1, \epsilon)$ -clr reducible to boolean functions g_1, g_2, \dots, g_k , then L is nonuniformly $(1, 1, 1, \epsilon/2)$ -qwlr reducible to some boolean function g with k qubits of quantum advice. (The constant inside the O -notation depends only on ϵ .)*

In the statement of Theorem 9, the constant inside the O -notation depends only on ϵ . In particular, it can be shown that for any $\epsilon \geq 0.055$ and integer $k > 2$, if a set L is nonadaptively $(k/2 + \sqrt{k}, k, 1, \epsilon)$ -clr reducible to boolean functions g_1, g_2, \dots, g_k , then L is nonuniformly $(1, 1, 1, \epsilon/2)$ -qwlr reducible to some boolean function g with k qubits of quantum advice.

The following corollary is an immediate consequence of Theorem 8 and Theorem 9.

Corollary 10. *Let $\epsilon \in (0, 1/2]$ be a fixed constant. If a set L is nonadaptively $(k/2 + O(\sqrt{k}), k, 1, \epsilon)$ -clr reducible to boolean functions g_1, g_2, \dots, g_k , then $L \in \text{PP}^{\text{NP}}/\text{poly}$.*

Acknowledgment We thank Aduri Pavan and Vinodchandran Variyam for several insightful comments during an early stage of this work.

References

- [Aar04] S. Aaronson. Limitations of quantum advice and one-way communication. In *Proceedings of the 19th Annual IEEE Conference on Computational Complexity*, pages 320–332, 2004.
- [Aar05] S. Aaronson. Quantum computing, postselection, and probabilistic polynomial-time. Technical Report 05-003, Electronic Colloquium on Computational Complexity (ECCC), <http://www.eccc.uni-trier.de/eccc/>, January 2005.
- [Aar06] S. Aaronson. Lower bounds for local search by quantum arguments. *SIAM Journal on Computing*, 35(4):804–824, 2006.
- [AFK89] M. Abadi, J. Feigenbaum, and J. Kilian. On hiding information from an oracle. *Journal of Computer and System Sciences*, 39(1):21–50, 1989.
- [ALM⁺98] S. Arora, C. Lund, R. Motwani, M. Sudan, and M. Szegedy. Proof verification and the hardness of approximation problems. *Journal of the ACM*, 45(3):501–555, 1998.
- [AR03] D. Aharonov and O. Regev. A lattice problem in quantum NP. In *Proceedings of the 44th IEEE Symposium on Foundations of Computer Science*, pages 210–219. IEEE Computer Society Press, 2003.
- [AR05] D. Aharonov and O. Regev. Lattice problems in $\text{NP} \cap \text{coNP}$. *Journal of the ACM*, 52(5):749–765, 2005.
- [AS98] S. Arora and S. Safra. Probabilistic checking of proofs: A new characterization of NP. *Journal of the ACM*, 45(1):70–122, 1998.
- [Bab87] L. Babai. A random oracle separates PSPACE from the Polynomial Hierarchy. *Information Processing Letters*, 26(1):51–53, 1987.
- [BF90] D. Beaver and J. Feigenbaum. Hiding instances in multioracle queries. In *Proceedings of the 7th Annual Symposium on Theoretical Aspects of Computer Science*, pages 37–48. Springer-Verlag *Lecture Notes in Computer Science #415*, 1990.
- [BFG06] R. Beigel, L. Fortnow, and W. Gasarch. A tight lower bound for restricted PIR protocols. *Computational Complexity*, 15:82–91, 2006.
- [BFKR97] D. Beaver, J. Feigenbaum, J. Kilian, and P. Rogaway. Locally random reductions: Improvements and applications. *Journal of Cryptology*, 10(1):17–36, Winter 1997.

- [BFL91] L. Babai, L. Fortnow, and C. Lund. Non-deterministic exponential time has two-prover interactive protocols. *Computational Complexity*, 1(1):3–40, 1991.
- [BK95] M. Blum and S. Kannan. Designing programs that check their work. *Journal of the ACM*, 42(1):269–291, 1995.
- [BLR93] M. Blum, M. Luby, and R. Rubinfeld. Self-testing/correcting with applications to numerical problems. *Journal of Computer and System Sciences*, 47(3):549–595, December 1993.
- [BM84] M. Blum and S. Micali. How to generate cryptographically strong sequences of pseudo-random bits. *SIAM Journal on Computing*, 13(4):850–864, November 1984.
- [dW06] R. de Wolf. Lower bounds on matrix rigidity via a quantum argument. In *Proceedings of the 33rd International Colloquium on Automata, Languages, and Programming*, pages 62–71, 2006.
- [FGL⁺96] U. Feige, S. Goldwasser, L. Lovász, S. Safra, and M. Szegedy. Interactive proofs and the hardness of approximating cliques. *Journal of the ACM*, 43:268–292, 1996.
- [FS92] L. Fortnow and M. Szegedy. On the power of two-local random reductions. *Information Processing Letters*, 44(6):303–306, 1992.
- [GM84] S. Goldwasser and S. Micali. Probabilistic encryption. *Journal of Computer Security*, 28:270–299, 1984.
- [KdW04] I. Kerenidis and R. de Wolf. Exponential lower bound for 2-query locally decodable codes via a quantum argument. *Journal of Computer and System Sciences*, 69(3):395–420, 2004.
- [Ker05] I. Kerenidis. Quantum multiparty communication complexity and circuit lower bounds. Technical Report quant-ph/0504087, Los Alamos e-Print Quantum Physics Technical Report Archive, April 12 2005.
- [LFKN92] C. Lund, L. Fortnow, H. Karloff, and N. Nisan. Algebraic methods for interactive proof systems. *Journal of the ACM*, 39(4):859–868, 1992.
- [Lip91] R. Lipton. New directions in testing. In J. Feigenbaum and M. Merritt, editors, *Distributed Computing and Cryptography*, pages 191–202. DIMACS series in Discrete Mathematics and Theoretical Computer Science, American Mathematical Society, 1991.
- [LLS05] S. Laplante, T. Lee, and M. Szegedy. The quantum adversary method and classical formula size lower bounds. In *Proceedings of the 20th Annual IEEE Conference on Computational Complexity*, pages 76–90, 2005.
- [Nay99] A. Nayak. Optimal lower bounds for quantum automata and random access codes. In *Proceedings of the 40th IEEE Symposium on Foundations of Computer Science*, pages 369–377, 1999.
- [NC00] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
- [PV] A. Pavan and N. Vinodchandran. 2-local random reductions to 3-valued functions. *Computational Complexity*. To appear.
- [Riv86] R. Rivest. Workshop on communication and computing. MIT, October 1986.
- [Sha92] A. Shamir. $IP=PSPACE$. *Journal of the ACM*, 39(4):869–877, 1992.
- [WdW05] S. Wehner and R. de Wolf. Improved lower bounds for locally decodable codes and private information retrieval. In *Proceedings of the 32nd International Colloquium on Automata, Languages, and Programming*, pages 1424–1436. Springer-Verlag *Lecture Notes in Computer Science*, July 2005.
- [Yao90] A. Yao. An application of communication complexity to cryptography. In *Lecture at DIMACS Workshop on Structural Complexity and Cryptography*, 1990.