Quantum speedups for stochastic optimization

Aaron Sidford and Chenyi Zhang
{sidford, chenyiz}@stanford.edu

Abstract

We consider the problem of minimizing a continuous function given given access to a natural quantum generalization of a stochastic gradient oracle. We provide two new methods for the special case of minimizing a Lipschitz convex function. Each method obtains a dimension versus accuracy trade-off which is provably unachievable classically and we prove that one method is asymptotically optimal in low-dimensional settings. Additionally, we provide quantum algorithms for computing a critical point of a smooth non-convex function at rates not known to be achievable classically. To obtain these results we build upon the quantum multivariate mean estimation result of Cornelissen et al. [25] and provide a general quantum variance reduction technique of independent interest.

1 Introduction

Stochastic optimization is central to modern machine learning. Stochastic gradient descent (SGD), and its many variants, are used broadly for solving challenges in data science and learning theory. In theory, SGD and stochastic optimization, have been the subject of decades of extensive study. [19, 68, 27] established that SGD achieves optimal rates for minimizing Lipschitz convex functions (even in one dimension) and stochastic optimization methods have been established for a range of problems [72, 70, 73, 74]. More recently, the complexity of stochastic gradient methods for smooth non-convex optimization, e.g., critical point computation, were established [3, 29, 30, 49, 50].

Given the foundational nature of stochastic optimization and the potential promise and increased study of quantum algorithms, it is natural to ask whether quantum computation could enable improved rates for solving these problems. There has been work studying whether access to quantum counterparts of classic optimization oracle can yield faster rates for semidefinite programs [13, 12, 43, 75, 76, 54], convex optimization [21, 5, 20], and non-convex optimization [23, 63, 80]. Notably, [52] showed that with just access to the quantum analog of a zeroth-order oracle, i.e., an oracle that when queried at a point outputs the value of the function at that point, it is possible to simulate access to a classic gradient oracle with a single query. This tool immediately yields improved rates for, e.g., convex function minimization, with a zeroth-order oracle.

Unfortunately, despite this progress and the established power of quantum evaluation oracles, obtaining further improvements has been challenging. A line of work established a variety of striking lower bounds ruling out quantum speedups for fundamental optimization problems [31, 32, 82]. For example, [31] showed that when given access to the quantum analog of a first-order oracle, i.e., an oracle that when queried at a point outputs the value of the function as well as the gradient at that point, quantum algorithms have no improved rates for non-smooth convex optimization over GD and SGD when the dimension is large. [82] extended this result to the non-convex setting and

---

1We assume all objective functions are differentiable. Similar to related work, see e.g., [15], our results can be generalized to non-differentiable settings since convex functions are almost everywhere differentiable and our algorithms and corresponding convergence analysis are robust to polynomially small numerical errors.
showed that given access to the quantum analog of a stochastic gradient oracle, quantum algorithms have no improved rates for finding critical points over SGD when the dimension is large.

In spite of these negative results, we nevertheless ask, for stochastic optimization are quantum-speedups obtainable? Our main result is an answer to this question in the affirmative for dimension-dependent algorithms. We provide two different quantum algorithms for stochastic convex optimization (SCO) which provably outperform optimal classic algorithms. Furthermore, we provide a quantum algorithm for computing the critical point of a smooth non-convex function which improves upon the state-of-the-art. We obtain these results through a new general quantum-variance reduction technique built upon the quantum multivariate mean estimation result of Cornelsen et al. [25] and the multilevel Monte Carlo (MLMC) technique [41, 10, 7]. We complement these results with lower bounds showing that one of them is asymptotically optimal in low-dimensional settings.

**General notation.** We use $\| \cdot \|$ to denote the Euclidean norm and let $\mathbb{R}_d(X) := \{ y \in \mathbb{R}^d : \| y - x \| \leq R \}$ and $|T| := \{1, \ldots, T \}$. We use bold letters, e.g., $x, y$, to denote vectors and capital letters, e.g., $A, B$, to denote matrices. For a $d$-dimensional random variable $X$, we refer to the trace of the covariance matrix of $X$ as its variance, denoted by $\text{Var}[X]$. For $f : \mathbb{R}^d \rightarrow \mathbb{R}$, we let $f^* := \inf_x f(x)$ and call $x \in \mathbb{R}^d$ $\epsilon$-(sub)optimal if $f(x) \leq f^* + \epsilon$ and $\epsilon$-critical if $\| \nabla f(x) \| \leq \epsilon$. Moreover, we call a random point $x \in \mathbb{R}^d$ expected $\epsilon$-(sub)optimal if $E[f(x)] \leq f^* + \epsilon$ and expected $\epsilon$-critical if $E[\| \nabla f(x) \|] \leq \epsilon$. If $f : \mathbb{R}^d \rightarrow \mathbb{R}$ is $L$-Lipschitz if $f(x) - f(y) \leq L \| x - y \|$ for all $x, y \in \mathbb{R}^d$ and $\ell$-smooth if $\| \nabla f(x) - \nabla f(y) \| \leq \ell \| x - y \|$ for all $x, y \in \mathbb{R}^d$. For two matrices $A, B \in \mathbb{R}^{d \times d}$, $A \preceq B$ denotes that $x^T A x \leq x^T B x$ for all $x \in \mathbb{R}^d$. We use $O$ to denote the big-$O$ notation omitting poly-logarithmic factors in $\epsilon, \epsilon', d, \sigma, R$, and $L$. When applicable, we use $|\text{garbage}(\cdot)|$ to denote possible garbage states\(^2\) that arise during the implementation of a quantum oracle (e.g., in Definitions (1) and (2)).

### 1.1 Quantum stochastic optimization oracles

Here we formally define quantum stochastic optimization oracles that we study in this work.

**Qubit notation.** We use $\cdot | \cdot$ to represent input or output registers made of qubits that could be in superpositions. In particular, given $m$ points $x_1, \ldots, x_m \in \mathbb{R}^d$ and a coefficient vector $c \in \mathbb{C}^m$ with $\sum_{i \in [m]} |c_i|^2 = 1$, the quantum register could be in the quantum state $|\psi\rangle = \sum_{i \in [m]} c_i |x_i\rangle$, which is superposition over all these $m$ points at the same time. If we measure this state, we will get each $x_i$ with probability $|c_i|^2$. Furthermore, to model a classical probability distribution $p$ over $\mathbb{R}^d$ quantumly, we can prepare the quantum state $\int_{x \in \mathbb{R}^d} \sqrt{p(x)} dx |x\rangle$. If we measure this state, the measurement outcome would follow the probability density function $p$.

**Quantum random variable access.** We say that we have quantum access to a $d$-dimensional random variable $X$ if we can query the following quantum sampling oracle of $X$ that returns a quantum superposition over the probability distribution of $X$ defined as follows.\(^3\)

**Definition 1 (Quantum sampling oracle).** For a $d$-dimensional random variable $X$, its quantum sampling oracle $O_X$ is defined as

$$O_X |0\rangle \rightarrow \int_{x \in \mathbb{R}^d} \sqrt{p_X(x)} dx |x\rangle \otimes |\text{garbage}(x)\rangle ,$$

where $p_X(\cdot)$ represents the probability density function of $X$.

The garbage state in Definition 1 is a quantum analogue of classical garbage information that arises when preparing the classical sampling oracle of $X$. When implementing the quantum sampling

\(^2\)The garbage state is a quantum analogue of classical garbage information that arises when preparing the classical stochastic gradient oracle which cannot be erased or uncomputed in general. In this work, we consider a general model where we make no assumption on the garbage state. See e.g., [42] for a similar discussion of this standard use of garbage quantum states.

\(^3\)Throughout this paper, whenever we have access to a quantum oracle $O$, we assume that it is a unitary operation and that we also have access to its corresponding inverse operation, denoted as $O^{-1}$, that satisfies $O^{-1} O = O O^{-1} = I$. These are a standard assumption, either explicitly or implicitly, in prior work on quantum algorithms, see e.g., [14, 44, 25].
oracle in quantum superpositions however, this garbage information will appear in a quantum state and cannot be erased or uncomputed in general. In this work, we consider a general model where we make no assumption on the garbage state. See e.g., [42] for a similar discussion of this standard use of garbage quantum states.

Observe that if we directly measure the output of \( O_X \), it will collapse to a classical sampling access to \( X \) that returns random vectors with respect to the probability distribution \( p_X \).

**Quantum stochastic gradient oracle.** When considering the problem of optimizing a function \( f : \mathbb{R}^d \to \mathbb{R} \), we are often given access to a stochastic gradient oracle that returns a random vector from the probability distribution of the stochastic gradient.

**Definition 2 (Stochastic gradient oracle (SGO)).** For \( f : \mathbb{R}^d \to \mathbb{R} \), its stochastic gradient oracle (SGO) \( C_g \) is defined as a random function that when queried at \( x \), samples a vector \( g(x) \) from a probability distribution \( p_f, x(\cdot) \) over \( \mathbb{R}^d \) that satisfies

\[
E_{g(x) \sim p_f, x} g(x) = \nabla f(x), \quad \forall x \in \mathbb{R}^d.
\]

We say the oracle is \( L \)-bounded if

\[
E_{g(x) \sim p_f, x} \|g(x)\|^2 \leq L^2, \quad \forall x \in \mathbb{R}^d,
\]

and we say the oracle has variance \( \sigma^2 \) if

\[
E_{g(x) \sim p_f, x} \|g(x) - \nabla f(x)\|^2 \leq \sigma^2, \quad \forall x \in \mathbb{R}^d.
\]

In this paper, we further assume quantum access to a stochastic gradient oracle, or access to a quantum stochastic gradient oracle for brevity, that upon query returns a quantum superposition over the probability distribution \( p_f, x(v) \).

**Definition 3 (Quantum stochastic gradient oracle (QSGO)).** For \( f : \mathbb{R}^d \to \mathbb{R} \), its quantum stochastic gradient oracle (QSGO) is defined as

\[
O_g |x\rangle \otimes |0\rangle \to |x\rangle \otimes \int_{v \in \mathbb{R}^d} \sqrt{p_f, x(v)} d v |v\rangle \otimes |\text{garbage}(v)\rangle,
\]

where \( p_f, x(\cdot) \) is as defined in Definition 2.

Observe that if we directly measure the output of \( O_g \), it will collapse to a classical stochastic gradient oracle that randomly returns a stochastic gradient at \( x \).

Another standard assumption in previous works [1, 29, 30, 50] that the stochastic gradient can be queried simultaneously, which means that the algorithm can choose the random seed \( \omega \) that is being queried. We assume that in such setting there is an explicit probability distribution \( \omega \) such that \( E[|g(x, \omega)\rangle] = \nabla f(x) \). Similarly, we define the quantum access to stochastic gradients allowing simultaneous queries, or access to a quantum stochastic gradient oracle with simultaneous queries for brevity, that upon query returns \( g(x, \omega) \) in a quantum state.

**Definition 4 (\( \sigma \)-SQ-QSGO).** For \( f : \mathbb{R}^d \to \mathbb{R} \) with its stochastic gradient \( g(x, \omega) \) indexed by random seed \( \omega \) that satisfies

\[
E_{\omega} g(x, \omega) = \nabla f(x), \quad E_{\omega} \|g(x, \omega) - \nabla f(x)\|^2 \leq \sigma^2, \quad \forall x \in \mathbb{R}^d,
\]

its simultaneously queryable, \( \sigma \)-mean-squared smooth quantum stochastic gradient oracle (\( \sigma \)-SQ-QSGO) is defined as

\[
O_{g}^\sigma |x\rangle \otimes |\omega\rangle \otimes |0\rangle \to |x\rangle \otimes |\omega\rangle \otimes |g(x, \omega)\rangle \otimes |\text{garbage}(x, \omega)\rangle.
\]
1.2 Results

Here we present our main results on new quantum algorithms for stochastic optimization. Our results and the prior state-of-the-art are summarized in Table 1. Further, we discuss new quantum lower bounds that we establish for quantum variance reduction and stochastic convex optimization. Our algorithmic results leverage a common technique for quantum variance reduction introduced in the next Section 2. This technique uses a combination of the quantum multivariate mean estimation result of Cornelissen et al. [25] and multilevel Monte Carlo (MLMC) [41, 10, 7].

Table 1: Comparison between our quantum algorithms and state-of-the-art classical algorithms for Problem 1 (the convex setting) and Problem 2 (the non-convex setting) where, for simplicity, we assume $R$ and multilevel Monte Carlo (MLMC) [41, 10, 7].

Stochastic convex optimization. In this work we consider the quantum analog of the standard stochastic convex optimization (SCO) problem defined as follows.

**Problem 1 (Quantum stochastic convex optimization (QSCO)).** In the quantum stochastic convex optimization (QSCO) problem we are given query access to an $L$-bounded QSGO $O_g$ (see Definition 3) for a convex function $f : \mathbb{R}^d \to \mathbb{R}$ whose minimum is achieved at $x^*$ with $\|x^*\| \leq R$ and must output an expected $\epsilon$-optimal point.

Classically, it is known that simple stochastic gradient descent, e.g. $x_{t+1} = x_t - \eta g_t$, can solve QSCO with $O(\epsilon^{-2})$ queries. Further, this bound is known to be optimal in the worst case [69, 77]. Nevertheless, we develop two quantum algorithms for Problem 1 in Section 3 and Section 4, respectively. The query complexities of these algorithms are summarized in the following Theorem 1. In comparison to the optimal classical query complexity of $O(\epsilon^{-2})$ queries, our algorithms obtain an improved dependence in terms of $\epsilon$ at the cost of a worse dependence on the dimension, $d$; Theorem 1 shows that a quadratic speedup is achievable when $d$ is constant.

**Theorem 1** (Informal version of Theorem 5 and Corollary 1). Problem 1 can be solved using an expected $\tilde{O}(\min\{d^{5/8}(LR/\epsilon)^{3/2}, d^{3/2}LR/\epsilon\})$ queries.

We complement Theorem 1 with the following lower bound on the query complexity for QSCO.

**Theorem 2** (Informal version of Theorem 8). For any $\epsilon \leq O(d^{-1/2})$, any quantum algorithm that solve Problem 1 with probability at least $2/3$ makes at least $\Omega(d^{1/2}\epsilon^{-1})$ queries in the worst case. For any $\Omega(d^{-1/2}) \leq \epsilon \leq 1$, any quantum algorithm that solves Problem 1 with success probability at least $2/3$ must make at least $\Omega(\epsilon^{-2})$ queries in the worst case.

Theorem 2 shows that the $\tilde{O}(d^{3/2}LR/\epsilon)$ rate that we obtain is asymptotically optimal for $d = \tilde{O}(1)$. A key open problem is whether the dimension dependence in either our upper bounds (Theorem 5 and Corollary 1) or our lower bound (Theorem 8) can be improved.

Stochastic critical point computation. We also develop quantum algorithms for finding critical points, i.e., points with small gradients, of (possibly) non-convex functions.
Quantum zeroth-order oracles. Throughout the paper, we focus on stochastic gradient oracles optimal \[6\]. In comparison, our algorithm improves in terms of \(\epsilon\) algorithms on the problem dimension, below we provide several supplementary points of context.

Regarding potential concerns regarding the dependence of our quantum Dimension dependence. In the bounded variance setting, Problem 2 can be solved using an expected \(\mathcal{O} (\Delta \sigma d^{1/2}/\epsilon^{-3})\) queries. In the mean-squared smoothness setting, Problem 2 can be solved using an expected \(\mathcal{O} ((\Delta (d\sigma))^{1/2}/\epsilon^{-5/2})\) queries.

Theorem 3 (Informal version of Theorem 6 and Theorem 7). In the bounded variance setting, Problem 2 can be solved using an expected \(\mathcal{O} (\Delta \sigma d^{1/2}/\epsilon^{-3})\) queries. In the mean-squared smoothness setting, Problem 2 can be solved using an expected \(\mathcal{O} ((\Delta (d\sigma))^{1/2}/\epsilon^{-5/2})\) queries.

Quantum zeroth-order oracles. Throughout the paper, we focus on stochastic gradient oracles in correspondence with classical work on stochastic optimization. However, it is worth noting that in certain cases our results extend gracefully to quantum stochastic zeroth order oracles. For example, when the objective function exhibits a finite-sum structure and we have access each component function individually through a quantum zeroth-order oracle, we can achieve an SQ-QSGO (Definition 4) with just a single query, utilizing quantum gradient estimation \[52\]. However, in other cases, the correspondence is less clear. For instance, if we are given a quantum stochastic zeroth-order oracle where the function value is obfuscated by some external noise, quantum gradient estimation \[52\] is not directly applicable. Further study could be an interesting direction for future work.

Practicality. Regarding the utility of our algorithm in practical situations, note that our quantum oracles in Definition 3 and Definition 4 are defined as direct, natural generalizations of the corresponding classical oracles. Considering such quantum generalizations of classical oracles is standard in the literature, see e.g., \[21, 81\]. There are standard techniques for implementing such quantum analogs of classical oracles (in theory for now given the current state-of-the-art in implementing quantum algorithms in practice). In particular, if there is a classical circuit for the classical oracle, there is a standard technique to obtain a quantum circuit of the same size which implement the corresponding quantum oracle and its inverse. Hence, our quantum algorithms have the potential to surpass blackbox classical algorithms in low dimensional settings where the oracle is given as an explicit circuit.

Dimension dependence. Regarding potential concerns regarding the dependence of our quantum algorithms on the problem dimension, below we provide several supplementary points of context.

- As discussed, in the classical setting, prior research \[27\] demonstrated that when optimizing an 1-Lipschitz convex function, SGD has a query complexity of \(\mathcal{O}(\epsilon^{-2})\) which is optimal, even in the one-dimensional case. In the quantum setting, we showed that, theoretically, quantum speedups which offer a different tradeoff between \(\epsilon\) and \(d\) dependencies are possible. Additionally, from our lower bound presented in Theorem 2 we know that some dimension dependence is inherent in obtaining an improvement.
- Classically, the complexity of dimension dependent optimization methods is well studied. In particular, there are parallel and private stochastic convex settings where the dimension dependencies are discussed, see e.g., \[15, 18\], and there exists works on critical point computation in low dimension settings, see e.g., \[22\].
• Even for high-dimensional problems, our algorithms can potentially be used as subroutines for low-dimensional subproblems. For instance, in this paper we apply these method to the approximately best point problem (Problem 5), wherein we utilize our algorithm repeatedly within a one-dimensional setting.

1.3 Paper organization

In the next Section 2 we propose and develop a new algorithm for a new problem quantum variance reduction; this algorithm is the basis of our quantum speedups for stochastic optimization problems. We then discuss the application of quantum variance reduction for stochastic convex optimization by presenting two quantum algorithms in Section 3 and Section 4, respectively. Technically, it is possible to obtain our result in Section 4 just using the quantum mean estimation routine of [25] rather than quantum variance reduction, however our use of quantum variance reduction facilitates our presentation. Furthermore, we present quantum algorithms for non-convex optimization based on quantum variance reduction in Section 5. Finally, in Section 6 we prove quantum lower bounds for quantum variance reduction and quantum stochastic convex optimization that establish the optimality of our algorithms, and conclude the paper in Section 7.

2 Quantum variance reduction

We obtain our quantum speedups for stochastic optimization problems by proposing and developing new algorithms for a new problem which we call the quantum variance reduction problem.

Problem 3 (Variance reduction). For a d-dimensional random variable $X$ with $\text{Var}[X] \leq L^2$ and some $\hat{\sigma} \geq 0$, suppose we are given access to its quantum sampling oracle $O_X$ defined in Definition 1. The goal is to output an unbiased estimate $\hat{\mu}$ of $\mu := \mathbb{E}[X]$ satisfying $\mathbb{E}||\hat{\mu} - \mu||^2 \leq \hat{\sigma}^2$.

Classically, Problem 3 can be solved by averaging $\tilde{O}(L^2/\hat{\sigma})$ samples of $X$; this query complexity is optimal among classical algorithms [64]. However, if we have access to the quantum sampling oracle defined in Definition 1, [25] showed that a (possibly) biased estimate $\hat{\mu}$ with error $||\hat{\mu} - \mu|| \leq \hat{\sigma}$ can be computed using $\tilde{O}(L\sqrt{\hat{\sigma}^{-1}})$ queries.

Lemma 1 ([25, Theorem 3.5]). Given access to the quantum sampling oracle $O_X$, for any $\hat{\sigma}, \delta > 0$ there is a procedure QuantumMeanEstimation($X, \hat{\sigma}, \delta$) that uses $\tilde{O}(L\sqrt{\hat{\sigma}}\log(1/\delta)/\hat{\sigma})$ queries and outputs an estimate $\hat{\mu}$ of the expectation $\mu$ of any d-dimensional random variable $X$ satisfying $\text{Var}[X] \leq L^2$ with error $||\hat{\mu} - \mu|| \leq \hat{\sigma} \leq L$ and success probability $1 - \delta$.

QuantumMeanEstimation [25] proceeds by introducing a directional mean function that reduces a multivariate mean estimation problem to a series of univariate mean estimation problem through quantum Fourier transform, which in the bounded norm case can be solved by quantum algorithms with a quadratic speedup using phase estimation. In terms of error rate, QuantumMeanEstimation in Lemma 1 improves over any classical sub-Gaussian estimator when $\frac{\hat{\sigma}}{\sigma} \geq \frac{1}{\sqrt{d}}$. However, its bias hinders its combination with various optimization algorithms assuming unbiased inputs, see e.g., [57, 2, 29, 30]. In this work we show how to carefully combine their algorithm with a classic multi-level Monte-Carlo (MLMC) technique from [10, 7] to obtain an unbiased estimate $\hat{\mu}$ and success probability 1 with the same rate as [25] and prove the following theorem.

Theorem 4. Algorithm 1 solves Problem 3 using an expected $\tilde{O}(Ld^{3/2}/\hat{\sigma})$ queries.

In the following Table 2 we provide a comparison between our result and previous works and in Section 6 we prove that our algorithm is optimal up to a poly-logarithmic factor. Notably, our algorithm does not depend on the detailed implementation of QuantumMeanEstimation but only its query complexity. Hence, we believe that our approach may also be useful in removing the bias of other quantum mean estimation algorithms with similar expressions of query complexities, e.g., quantum phase estimation [55, 24] and quantum amplitude estimation [14].

Our algorithm consists of two components. First, we show that we can obtain a variant of the quantum mean estimation algorithm, denoted as QuantumMeanEstimation$^+ (X, \hat{\sigma})$, that outputs a low variance estimate with probability 1. This procedure compares the outcomes of the quantum estimator and a classical estimate, and in the event of significant disparity, generates a new independent classical estimate.
Second, we use the MLMC technique [41], specifically a variant of the methods described in [10, 7], to carefully invoke the biased subroutine QuantumMeanEstimation$^+$ and compute the unbiased estimate. The algorithm, Algorithm 1, simply invokes QuantumMeanEstimation$^+$ for three randomly chosen accuracies and combines them to obtain the result. Though there are an infinite number of possible accuracies chosen, we show that the expectation, the variance, and expected number of queries are all suitable to prove Theorem 4, whose proof is deferred to Appendix B.

Algorithm 1: Quantum variance reduction

Input: Random variable $X$, target variance $\tilde{\sigma}^2$
Output: An unbiased estimate $\hat{\mu}$ of $\mathbb{E}[X]$ with variance at most $\tilde{\sigma}^2$
1 Set $\hat{\mu}_0 \leftarrow$ QuantumMeanEstimation$^+(X, \tilde{\sigma}/10)$
2 Randomly sample $j \sim \text{Geom}(\frac{1}{2}) \in \mathbb{N}$
3 $\hat{\mu}_j \leftarrow$ QuantumMeanEstimation$^+(X, 2^{-3j/4}\tilde{\sigma}/10)$
4 $\hat{\mu}_{j-1} \leftarrow$ QuantumMeanEstimation$^+(X, 2^{-3(j-1)/4}\tilde{\sigma}/10)$
5 $\hat{\mu} \leftarrow \hat{\mu}_0 + 2^j (\hat{\mu}_j - \hat{\mu}_{j-1})$
6 return $\hat{\mu}$

Table 2: Comparison between different methods for variance reduction in the case of $L=1$ and $\tilde{\sigma} \in (0, 1)$. The $\tilde{O}$ symbol was omitted in the “Queries” column.

<table>
<thead>
<tr>
<th></th>
<th>Queries</th>
<th>Bias</th>
<th>Variance</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\hat{\sigma}^{-2}$</td>
<td>$O(1)$</td>
<td>$0$</td>
<td>$\hat{\sigma}^2$</td>
<td>Classical Variance Reduction</td>
</tr>
<tr>
<td>$d^{1/2}\hat{\sigma}^{-1}$</td>
<td>$\tilde{O}(1)$</td>
<td>$\hat{\sigma}$</td>
<td>$\hat{\sigma}^2$</td>
<td>Quantum Multivariate Mean estimation [25]</td>
</tr>
<tr>
<td>$\log^2(1/\gamma)\hat{\sigma}^{-1}$</td>
<td>$O(1)$</td>
<td>$\gamma$</td>
<td>$\hat{\sigma}^2$</td>
<td>One-dimensional Quantum Mean estimation [24]</td>
</tr>
<tr>
<td>$d^{1/2}\hat{\sigma}^{-1}$</td>
<td>$\tilde{O}(1)$</td>
<td>$0$</td>
<td>$\hat{\sigma}^2$</td>
<td>Our Result (Theorem 4)</td>
</tr>
</tbody>
</table>

3 Quantum accelerated stochastic approximation

In this section, we present our $\tilde{O}(d^{5/8} \epsilon^{-3/2})$ query quantum algorithm for Problem 1. Our approach builds upon the framework proposed by Duchi et al. [28, 15], which involves performing a Gaussian convolution on the objective function $f$ and then optimizing the resulting smooth convoluted function. Compared to their algorithm, our algorithm differs by replacing the variance reduction step by our quantum variance reduction technique (Algorithm 1).

As with a variety of prior work on parallel and private SCO [28, 33, 15], we consider the smooth function $F_r$ that is the Gaussian convolution of the objective function $f$:

$$F_r(x) := \int_{\mathbb{R}^d} g_r(y)f(x-y)dy, \quad \text{where} \quad g_r(y) := \frac{1}{(\sqrt{2\pi r})^d} \exp \left( -\frac{\|y\|^2}{2r^2} \right).$$

(5)

As shown in Lemma 4, when the radius $r$ of the convolution is sufficiently small, $F_r$ closely approximates $f$ pointwise. Consequently, to find an $\epsilon$-optimal point of $f$ it suffices to find an $\epsilon/4$-optimal point of $F_r$ for $r = \frac{2\epsilon}{4\sqrt{2L}}$. Moreover, Lemma 4 shows that the stochastic gradient $g_{F_r}$ of $F_r$ can be defined and obtained based on the stochastic gradient $g$ of $f$ as follows:

$$g_{F_r}(x) = g(x - y), \quad y \sim g_r,$$

(6)

which satisfies

$$\mathbb{E}_{y \sim g_r} g_{F_r}(x) = \nabla F_r(x) \quad \text{and} \quad \|g_{F_r}(x)\| \leq L, \quad \forall x.$$

Hence,

$$\|\nabla F_r(x)\| \leq \int_{y \sim g_r} \|g_{F_r}(x)\|dy \leq L,$$

indicating that $F_r$ is also $L$-Lipschitz.
To optimize this smooth convex function \( F_0 \), we leverage the accelerated stochastic approximation (AC-SA) algorithm introduced in [57], which applies an accelerated proximal descent method on the objective function using unbiased estimates of gradients. Our algorithm given in Algorithm 2 is a specialization of the AC-SA algorithm, where we implement those unbiased estimates of gradients using quantum variance reduction (Algorithm 1). In the classical setting, one query to the stochastic gradient \( g_0 (x) \) of \( F_0 \) can be implemented by a random sampling a vector \( y \in \mathbb{R}^d \) from the Gaussian \( \gamma_r \) followed by a query to the SGO \( C_g \) (Definition 2) at \( x - y \). Similarly, we can show that one query to a QSGO of \( F_0 \) (Definition 3) can also be implemented by one query to the QSGO of \( f \). The subsequent theorem presents the query complexity of Algorithm 2.

Algorithm 2: Quantum accelerated stochastic approximation (Q-AC-SA)

Input: Function \( f : \mathbb{R}^d \to \mathbb{R} \), precision \( \epsilon \)

Parameters: Domain Size \( \mathcal{D} \), total iteration budget \( T = \frac{4d^{3/4}L\sqrt{R}}{\epsilon} \), target variance \( \hat{\sigma} = \frac{d^{3/8}R^{3/4}}{\sqrt{LR} \epsilon} \), convolution radius \( r = \frac{\epsilon}{4\sqrt{d} \hat{\sigma}} \), \( \gamma = \frac{R\sqrt{\pi} \hat{\sigma}}{(T + 2)^{3/2}} \)

Output: an \( \epsilon \)-optimal point of \( F_0 \)

1. Denote \( F'_0 (x) := \int_{\mathbb{R}^d} \gamma_r (y) f(x - y) \) as in (5)
2. Set \( x_1 \leftarrow 0 \), \( x^a_1 \leftarrow x_1 \)
3. For \( t = 1, 2, \ldots, T \) do
   4. \( \beta_t \leftarrow \frac{t + 1}{2}, \gamma_t \leftarrow \frac{t + 1}{2} \gamma \)
   5. \( x^m_t \leftarrow \frac{1}{\beta_t} x_t + (1 - \beta_t^{-1}) x^a_t \)
   6. Call Algorithm 1 for an unbiased estimate \( \hat{g}_t \) of \( \nabla F_0 (x^m_t) \) with variance at most \( \hat{\sigma}^2 \)
   7. \( x_{t+1} \leftarrow \arg \min_{z \in \mathbb{R}^d} \{ \gamma_t (\hat{g}_t, z - x^m_t) + L\|x^m_t - z\|^2 / (2r) \} \)
   8. \( x^a_{t+1} \leftarrow \beta_t^{-1} x_{t+1} + (1 - \beta_t^{-1}) x^a_t \)
8. return \( x^a_T \)

Theorem 5 (Formal version of Theorem 1, Part 1). Algorithm 2 solves Problem 1 using an expected \( \tilde{O}(d^{3/8}(LR/\epsilon)^{3/2}) \) queries.

The proof of Theorem 5 is deferred to Appendix C.

4 Quantum stochastic cutting plane method (Q-SCP)

In this section, we develop our \( \tilde{O}(d^{3/2}LR/\epsilon) \) query algorithm for Problem 1 which is based on a stochastic version of the cutting plane method. We introduce the key properties and related concepts of cutting plane methods, and then provide a procedure for efficiently post-processing the outcomes obtained from the stochastic cutting plane method using quantum variance reduction (Algorithm 1). Then, we analyze the overall query complexity for solving Problem 1. Technically, it is possible to obtain the results of this section using the quantum mean estimation routine of [25], rather than quantum variance reduction, however using quantum variance reduction facilitates our presentation.

We begin by introducing some notation and concepts on cutting plane methods. Cutting plane methods solve the feasibility problem defined as follows. Note that this problem is slightly easier to solve than the one in, e.g., [48], however it is simple suffices for our purposes.

Problem 4 (Feasibility Problem). We are given query access to a separation oracle for a set \( K \subset \mathbb{R}^d \) such that on query \( x \in \mathbb{R}^d \) the oracle outputs a vector \( c \) and either \( c = 0 \), in which case \( x \in K \), or \( c \neq 0 \), in which case \( H := \{ z : c^\top z \leq c^\top x \} \supset K \). The goal is to query a point \( x \in K \).

[48] showed that Problem 4 can be solved by cutting plane method using \( O(d \log (dR/r)) \) queries to a separation oracle where \( R \) and \( r \) denote bounds on \( K \).

Lemma 2 ([48, Theorem 1.1]). There is a cutting plane method which solves Problem 4 using at most \( C \cdot d \log (dR/r) \) queries for some constant \( C \), given that the set \( K \) is contained in the ball of radius \( R \) centered at the origin and it contains a ball of radius \( r \).
[67, 58] demonstrated that, running cutting plane method on a convex function $f$ with the separation oracle being its gradient yields a sequence of points where at least one of them is an $\epsilon$-optimal point of $f$. This follows from the fact that there exists a ball of radius $O(\epsilon)$ around $x^*$ such that every point in this ball is $\epsilon$-optimal. In the stochastic setting, although we cannot access the precise gradient, we show that it suffices to use an $O(\epsilon/R)$-approximate gradient oracle of $f$ (formally defined in Appendix D.1) as the separation oracle. Specifically, we prove the following result.

**Proposition 1.** For any $0 \leq \epsilon \leq LR$, with success probability at least $5/6$ we can obtain $T = O(d\log(dLR/\epsilon))$ points $x_1, \ldots, x_T \in B_R(0)$ such that one of the $x_i$ is $\epsilon$-optimal using $\tilde{O} \left( d^{3/2}LR/\epsilon \right)$ queries to the QSGO $O_g$ defined in Definition 3.

The proof of Proposition 1 is deferred to Appendix D.1. After applying Proposition 1, it is not clear which query $x_i$ is an $O(\epsilon)$-optimal point. This difficulty arises because we lack access to the function value of $f$, which sets our problem apart from the feasibility problem discussed in [48], where there is a clear indication when a query successfully lies within the feasible region. Consequently, we next focus on identifying the optimal solution within the finite set $\Gamma$ of points using access to the QSGO. We conceptualize this task as the *approximately best point* problem, formulated as follows.

**Problem 5** (Approximately best point). For a $L$-Lipschitz convex function $f : \mathbb{R}^d \rightarrow \mathbb{R}$ and $T$ points $x_1, \ldots, x_T \in B_R(0)$, find a convex combination $x \in \mathbb{R}^d$ of the points satisfying

$$f(x) \leq \min_{i \in T} f(x_i) + \epsilon.$$

In this work, we develop an algorithm that solves Problem 5 by making pairwise comparisons in a hierarchical order, where each pairwise comparison is computed by running binary search on the segment along the segment between the two points. Formally, we prove the following result.

**Proposition 2.** For any accuracy parameter $\epsilon > 0$, with success probability at least $5/6$ Algorithm 5 solves Problem 5 using $\tilde{O} \left( RL/\epsilon \right)$ queries to an $L$-bounded QSGO $O_g$ defined in Definition 3.

The proof of Proposition 2 and the corresponding quantum algorithm can be found in Appendix D.2. Next, we present the main result of this section, which describes the query complexity of solving Problem 1 using quantum stochastic cutting plane method.

**Corollary 1** (Formal version of Theorem 1, Part 2). With success probability at least $2/3$, Problem 1 can be solved using an expected $\tilde{O} \left( d^{3/2}LR/\epsilon \right)$ queries.

The proof of Corollary 1 is deferred to Appendix D.3.

## 5 Quantum stochastic non-convex optimization

In this section, we present our quantum algorithms for Problem 2 in the bounded-variance setting and the mean-squared smoothness setting, respectively, using our quantum variance reduction technique.

To solve Problem 2 in the bounded variance setting, we leverage the randomized SGD method introduced in [40], which is a variant of SGD where the number of iterations is randomized. Our algorithm is a specialization of the randomized stochastic gradient algorithm, where we replace the classical variance reduction step by quantum variance reduction (Algorithm 1). The query complexity of our quantum algorithm is given in the following theorem.

**Theorem 6** (Formal version of Theorem 3, bounded variance setting). For any $\epsilon > 0$, Algorithm 6 solves Problem 2 in the bounded variance setting using an expected $\tilde{O}(\Delta/\sigma \sqrt{d} e^{-3})$ queries.

The proof of Theorem 6 and the corresponding quantum algorithm can be found in Appendix E.

To solve Problem 2 in the mean-squared smoothness setting, we leverage the SPIDER algorithm introduced in [29], which is a variance reduction technique that allows us to estimate the gradient of a function with lower cost by utilizing the smoothness structure and reuse the stochastic gradient samples at nearby points. Our algorithm is a specialization of the SPIDER algorithm, where we replace the classical variance reduction step by quantum variance reduction (Algorithm 1). The query complexity of our quantum algorithm is given in the following theorem.

**Theorem 7** (Formal version of Theorem 3, mean-squared smoothness setting). For any $0 \leq \epsilon \leq \sigma$, Algorithm 7 solves Problem 2 in the mean-squared smoothness setting using an expected $\tilde{O} \left( \ell\Delta/\sigma \epsilon^{-2.5} \right)$ number of queries.
The proof of Theorem 7 and the corresponding quantum algorithm can be found in Appendix F.

6 Lower bounds

In this section we present two quantum lower bounds for solving quantum variance reduction (Problem 3) and stochastic convex optimization (Problem 1), respectively.

We first establish the following quantum lower bound for the variance reduction problem (Problem 3) which shows that our Algorithm 1 is optimal up to a poly-logarithmic factor when $\hat{\sigma} = O (d^{-1/2})$. By Markov’s inequality, Proposition 3 equivalently states that any quantum algorithm that solves Problem 3 must make an expected $\Omega(L\sqrt{d} \hat{\sigma}^{-1})$ queries. This matches our algorithmic result provided in Theorem 4, up to a poly-logarithmic factor.

**Proposition 3.** There is a constant $\alpha$ such that for any $\hat{\sigma} \leq \sigma \alpha \sqrt{d}$, any quantum algorithm that solves Problem 3 with success probability at least $2/3$ must make at least $\Omega(L \sqrt{d} \hat{\sigma}^{-1})$ queries in the worst case.

The proof of Proposition 3 is deferred to Appendix G.1

Next, we establish the following quantum lower bounds for stochastic convex optimization (Problem 1) in the low-dimension regime and the high-dimension regime, respectively, which show that our quantum stochastic cutting plane method in Section 4 is optimal up to a poly-logarithmic factor when the dimension $d$ is a constant, and there is no quantum speedup over SGD when $d \geq \Omega(\epsilon^{-2})$.

**Theorem 8.** For any $\epsilon \leq \frac{RL}{100\sqrt{d}}$, any quantum algorithm that solves Problem 1 with success probability at least $2/3$ must make at least $\Omega(L \sqrt{d} / \epsilon)$ queries in the worst case. For any $\frac{RL}{100\sqrt{d}} \leq \epsilon \leq 1$, any quantum algorithm that solves Problem 1 with success probability at least $2/3$ must make at least $\Omega(R^2L^2 / \epsilon^2)$ queries in the worst case.

The proof of Theorem 8 is deferred to Appendix G.2.

7 Conclusion

We presented improved quantum algorithms for stochastic optimization. We developed a new technical tool which we call quantum variance reduction and show how to use it to improve upon the query complexity for stochastic convex optimization and for critical point computation in smooth, stochastic, non-convex functions. Further, we provided lower bounds which establish both the optimality of our quantum variance reduction technique and of one of our stochastic convex optimization algorithms in low dimensions. A natural open problem suggested by our work is to establish the optimal complexity of the problems we study, e.g., stochastic convex optimization and stochastic non-convex optimization with quantum oracle access, in higher dimensions. We hope this paper fuels further study of these problems.

Acknowledgement

We thank Adam Bouland, Yair Carmon, András Gilyén, Yujia Jin, and Tongyang Li for helpful discussions. A.S. was supported in part by a Microsoft Research Faculty Fellowship, NSF CAREER Award CCF-1844855, NSF Grant CCF-1955039, a PayPal research award, and a Sloan Research Fellowship. C.Z. was supported in part by the Shoucheng Zhang Graduate Fellowship.

References


[73] Shai Shalev-Shwartz, *Online learning: Theory, algorithms, and applications*, Hebrew University, 2007.


A Additional related work

Stochastic convex optimization. Stochastic convex optimization is a broad, well-studied area of research. Beyond the works mentioned in the introduction, for additional references and discussion of research in the area, see [11, 47, 68] for detailed overviews of stochastic convex optimization methods and [19] for a presentation of convex optimization in the online learning setting. Additionally, see [26, 51] for a discussion of the closely related problem of finite-sum optimization.

Non-convex optimization. Non-convex optimization is a rapidly advancing research area in optimization theory. These advances are motivated in part by the fact that the landscapes of various modern machine learning problems are typically non-convex, including deep neural networks, principal component analysis, tensor decomposition, etc. In general, finding a global optimum of a non-convex function is NP-hard [66, 69]. Hence, many theoretical works instead focus on finding local minima rather than a global one, given existing empirical and theoretical evidence that local minima can be as good as global minima in certain machine learning problems [8, 34, 36, 37, 39, 46]. The first step of finding local minima would be to find stationary points, which has been discussed in many previous works [1, 9, 17, 16, 70, 71]. An important line of work focuses on first-order, (stochastic) gradient-based algorithms for finding critical points and local minima since higher-order derivatives are often not accessible in practical scenarios [3, 17, 30, 34, 49, 50, 62, 78, 81]. There are also results on non-convex optimization that study different settings [38, 61, 79, 85, 35, 83, 84].

Quantum Monte Carlo methods. Since [65], quantum Monte Carlo methods have been broadly investigated. In particular, [59] discussed quantum Monte-Carlo methods for entropy estimation, and [45] initiated the study of quantum mean estimation problem with multiplicative error, which is followed by [44, 25, 24, 56]. Multilevel Monte Carlo methods are also widely used in quantum algorithms, see e.g., [4, 60]. Specifically, the particular multilevel Monte Carlo strategies we use for quantum variance reduction have roots in the classic computation work of [10, 7].

B Proof of Theorem 4

Algorithm 3: Quantum Mean Estimation

Input: Random variable $X$, target variance $\hat{\sigma}^2 \leq L^2$

Parameters: $\delta = \hat{\sigma}^6/(4L)^6$, $D = \frac{\hat{\sigma}}{2} + \frac{4L^2}{\hat{\sigma}^4}$

Output: An estimate $\hat{\mu}$ of $\mu = E[X]$ satisfying $E[|\hat{\mu} - \mu|^2] \leq \hat{\sigma}^2$

1. Set $X_1 \leftarrow \text{QuantumMeanEstimation}(X, \hat{\sigma}/4, \delta)$
2. Randomly draw one classical sample $X_2$ of $X$
3. if $\|X_1 - X_2\| \leq D$ then return $X_1$
4. else
5. Randomly draw one classical sample $X_3$ of $X$
6. return $X_3$

We begin by presenting a lemma showing how two unbiased, bounded variance random variables ($X_2$ and $X_3$ in the lemma) can be used to control the expected $\ell_2$ error of a random variable ($X_1$ in the lemma) that is close to the expectation of $X_2$ and $X_3$ with some probability. In Algorithm 3 $X_1$ corresponds to the output of QuantumMeanEstimation and then $X_2$ and $X_3$ are obtained by classic sampling.

Lemma 3. Let $X_1, X_2, X_3 \in \mathbb{R}^d$ be independent random variables where $E[X_2] = E[X_3] = \mu$, $\text{Var}[X_2] \leq L^2$, and $\text{Var}[X_1] \leq L^2$, and $\|X_1 - \mu\| \leq \hat{\sigma}$ with probability at least $1 - \delta$. Further, let $Z$ be the random variable that is $X_1$ if $\|X_1 - X_2\| \leq D$ and $X_3$ otherwise where $D > \hat{\sigma}$. Then,

$$E[\|Z - \mu\|^2] \leq \hat{\sigma}^2 + L \left( \frac{L^2 - \hat{\sigma}^2}{D - \hat{\sigma}} \right) + \delta(2D^2 + 3L^2).$$

Consequently, $E[\|Z - \mu\|^2] \leq 13\sigma^2$ when $D = \hat{\sigma} + L^3/\hat{\sigma}^2$ and $\delta \leq \hat{\sigma}^6/L^6$. 


Proof. Let $S$ denote the event that $\|X_1 - \mu\|_2 \leq \sigma$ and let $T$ denote the event that $\|X_1 - X_2\|_2 \leq D$. Then by the law of total expectation

$$E[\|Z - \mu\|_2^2] = Pr[S]E[\|Z - \mu\|_2^2 | S] + Pr[\text{not } S]E[\|Z - \mu\|_2^2 | \text{not } S]$$

$$\leq E[\|Z - \mu\|_2^2 | S] + \delta \cdot E[\|Z - \mu\|_2^2 | \text{not } S]$$

Where we used that $Pr[S] \leq 1$ and $Pr[\text{not } S] \leq \delta$. We will prove the lemma by leveraging this inequality and upper bounding both $E[\|Z - \mu\|_2^2 | S]$ and $E[\|Z - \mu\|_2^2 | \text{not } S]$.

First, we upper bound $E[\|Z - \mu\|_2^2 | S]$. Again by the law of total expectation and the definition of $Z$ we have that

$$E[\|Z - \mu\|_2^2 | S] = Pr[T | S]E[\|Z - \mu\|_2^2 | T \text{ and } S]$$

$$+ Pr[\text{not } T | S]E[\|Z - \mu\|_2^2 | T \text{ and } \text{not } S]$$

$$\leq Pr[T | S] \cdot \hat{\sigma}^2 + Pr[\text{not } T | S] L^2.$$

Here we use that if $T$ and $S$ both hold then $Z = X_1$ and $\|X_1 - \mu\| \leq \hat{\sigma}$ and that if $S$ holds and not $T$ then $Z = X_3$ and $X_3$ is independent of $T$ and $S$ with variance $L^2$. Now, if $\|X_2 - \mu\|_2 \leq D - \hat{\sigma}$ then when $S$ holds by triangle inequality

$$\|X_1 - X_2\| \leq \|X_1 - \mu\| + \|X_2 - \mu\| \leq D.$$

Applying this bound and Chebyshev inequality to $X_2$ (and using that $X_2$ is independent of $S$) we have that

$$Pr[T | S] \geq Pr[\|X_2 - \mu\|_2 \leq D - \hat{\sigma} | S] = Pr[\|X_2 - \mu\|_2 \leq D - \hat{\sigma}] \geq 1 - \frac{L}{D - \hat{\sigma}}.$$

Since $\hat{\sigma} < L$, combined with (7) this implies that

$$E[\|Z - \mu\|_2^2 | S] \leq \left(1 - \frac{L}{D - \hat{\sigma}}\right) \hat{\sigma}^2 + \frac{L^3}{D - \hat{\sigma}} = \hat{\sigma}^2 + \frac{L^2}{D - \hat{\sigma}}.$$

Next, we upper bound $E[\|Z - \mu\|_2^2 | \text{not } S]$. Note that if $T$ holds then

$$\|Z - \mu\|^2 \leq 2\|Z - X_2\|^2 + 2\|X_2 - \mu\|^2 \leq 2D^2 + 2\|X_2 - \mu\|^2.$$

Since $Z = X_3$ if $T$ does not hold, we then see that in either case

$$\|Z - \mu\|^2 \leq 2D^2 + 2\|X_2 - \mu\|^2 + \|X_3 - \mu\|^2.$$

Since, $X_2$ and $X_3$ are independent of $S$ with variance $L$ this therefore implies that

$$E[\|Z - \mu\|_2^2 | \text{not } S] \leq E[2D^2 + 2\|X_2 - \mu\|^2 + \|X_3 - \mu\|^2] = 2D^2 + 3L^2,$$

which leads to

$$E[\|Z - \mu\|_2^2] \leq E[\|Z - \mu\|_2^2 | S] + \delta \cdot E[\|Z - \mu\|_2^2 | \text{not } S]$$

$$\leq \hat{\sigma}^2 + L \left(\frac{L^2 - \hat{\sigma}^2}{D - \hat{\sigma}}\right) + \delta(2D^2 + 3L^2).$$

\[\square\]

Corollary 2. Given access to the quantum sampling oracle $O_X$ of a $d$-dimensional random variable $X$, for any $\sigma, \delta \geq 0$, the procedure QuantumMeanEstimation$^+$ ($X, \sigma$) (Algorithm 3) uses $\tilde{O}(L\sqrt{d}\sigma^{-1})$ queries and outputs an estimate $\hat{\mu}$ of the expectation $\mu = E[X]$ satisfying $E[\|\hat{\mu} - \mu\|^2] \leq \hat{\sigma}^2$.4

4At Line 2 and Line 5 of Algorithm 3, we can further refine our approach to obtain $X_2$ and $X_4$ by taking the same number of classical samples as we would have used in the QuantumMeanEstimation procedure, which can reduce the poly-logarithmic factor in the overall query complexity.
Proof. By Lemma 3, the output $\hat{\mu}$ of QuantumMeanEstimation$^+$ $(X, \hat{\sigma})$ (Algorithm 3) satisfies
\[ \mathbb{E}[\|\hat{\mu} - \mu\|^2] \leq \hat{\sigma}^2. \] (9)
As for the number of queries to $O_X$, note that it uses
\[ \mathcal{O}\left(\frac{L\sqrt{d}\log(1/\delta)}{\hat{\sigma}}\right) = \mathcal{O}\left(\frac{L\sqrt{d}}{\hat{\sigma}}\log\left(\frac{L^6}{\hat{\sigma}}\right)\right) = \mathcal{O}\left(\frac{L\sqrt{d}}{\hat{\sigma}}\right) \]
queries to prepare $X_1$. Moreover, we can prepare the classical samples $X_2$ and $X_3$ by measuring the quantum state $O_X\ket{0}$ in the computational basis, which takes 1 query to $O_X$. Hence, the overall query complexity equals $\mathcal{O}(L\sqrt{d}\hat{\sigma}^{-1})$.

Equipped with Corollary 2, we are ready to prove Theorem 4.

Proof of Theorem 4. The structure of our proof is similar to the proof of [7, Proposition 1]. Observe that the output $\hat{\mu}$ of Algorithm 1 can be expressed as
\[ \hat{\mu} = \hat{\mu}_0 + 2^j(\hat{\mu}_j - \hat{\mu}_{j-1}), \quad J \sim \text{Geom}\left(\frac{1}{2}\right) \in \mathbb{N}. \] (10)
Then we have
\[ \mathbb{E}[\hat{\mu}] = \mathbb{E}[\hat{\mu}_0] + \sum_{j=1}^{\infty} \Pr\{J = j\} 2^j(\mathbb{E}[\hat{\mu}_j] - \mathbb{E}[\hat{\mu}_{j-1}]) = \mathbb{E}[\hat{\mu}_\infty] = \mu, \]
given that $\Pr\{J = j\} = 2^{-j}$. As for the variance, we have
\[ \mathbb{E}[\|\hat{\mu} - \mu\|^2] \leq 2\mathbb{E}[\|\hat{\mu} - \hat{\mu}_0\|^2] + 2\mathbb{E}[\|\hat{\mu}_0 - \mu\|^2], \]
where
\[ \mathbb{E}[\|\hat{\mu} - \hat{\mu}_0\|^2] = \sum_{j=1}^{\infty} \Pr\{J = j\} 2^{2j} \mathbb{E}[\|\hat{\mu}_j - \hat{\mu}_{j-1}\|^2] = \sum_{j=1}^{\infty} 2^{2j} \mathbb{E}[\|\hat{\mu}_j - \hat{\mu}_{j-1}\|^2], \]
and for each $j$ we have
\[ \mathbb{E}[\|\hat{\mu}_j - \hat{\mu}_{j-1}\|^2] \leq 2\mathbb{E}[\|\hat{\mu}_j - \mu\|^2] + 2\mathbb{E}[\|\hat{\mu}_{j-1} - \mu\|^2]. \]
By Corollary 2,
\[ \mathbb{E}[\|\hat{\mu}_j - \mu\|^2] \leq \frac{\hat{\sigma}^2}{100 \cdot 2^{3j/2}}, \quad \forall j \geq 0, \]
which leads to
\[ \mathbb{E}[\|\hat{\mu}_j - \hat{\mu}_{j-1}\|^2] \leq \frac{\sigma^2}{50 \cdot 2^{3(j-1)/2}} + \frac{\sigma^2}{50 \cdot 2^{3j/2}} \leq \frac{\hat{\sigma}^2}{10 \cdot 2^{3j/2}}, \]
and
\[ \mathbb{E}[\|\hat{\mu} - \hat{\mu}_0\|^2] = \frac{\hat{\sigma}^2}{10} \sum_{j=1}^{\infty} \frac{1}{2^{j/2}} \leq \frac{1}{3} \hat{\sigma}^2. \]
Hence,
\[ \mathbb{E}[\|\hat{\mu} - \mu\|^2] \leq 2\mathbb{E}[\|\hat{\mu} - \hat{\mu}_0\|^2] + 2\mathbb{E}[\|\hat{\mu}_0 - \mu\|^2] \leq \hat{\sigma}^2, \]
given that $\mathbb{E}[\|\hat{\mu}_0 - \mu\|^2] \leq \hat{\sigma}^2/100$ by Corollary 2. Moreover, the expected number of queries is
\[ \mathcal{O}\left(\frac{L\sqrt{d}\log d}{\hat{\sigma}}\right) \cdot \left(1 + \sum_{j=1}^{\infty} \Pr\{J = j\} \cdot (2^{3j/4} + 2^{3(j-1)/4})\right) = \mathcal{O}\left(\frac{L\sqrt{d}}{\hat{\sigma}}\right). \]
C Proof of Theorem 5

We first state a result from [15] which bounds properties of $F$ defined in (5). The lemma states that, provided the radius $r$ of the convolution is sufficiently small, $F$ is pointwise close to $f$ and hence finding an $O(\epsilon)$-minimum of $f$ is equivalent to finding an $\epsilon$-minimum of $F$. Further the lemma shows that $F$ is Lipschitz and smooth.

**Lemma 4 ([15, Lemma 8]).** For any $L$-Lipschitz convex function $f : \mathbb{R}^d \rightarrow \mathbb{R}$, its Gaussian convolution $g$ defined in Eq. (5) is convex, $L$-Lipschitz, and satisfies

$$|f(x) - g(x)| \leq \sqrt{d} \cdot Lr \quad \text{and} \quad \nabla^2 g(x) \leq (L/r) \cdot I_d, \quad \forall x \in \mathbb{R}^d,$$

where $I_d$ is the $d$-dimensional identity matrix.

Prior to proving Theorem 5, we show that one query to a QSGO $O_{g,F}$ (Definition 3) of $F_r$ satisfying

$$O_{g,F} |x \rangle \otimes |0 \rangle \otimes |0 \rangle \rightarrow |x \rangle \otimes \int_{v \in \mathbb{R}^d} \sqrt{p_{F,x}(v)} |v \rangle \otimes |\text{garbage}(v)\rangle,$$

(11) can be implemented by one query to $O_g$ of $f$ defined in Definition 3.

**Lemma 5.** The QSGO $O_{g,F}$ of $F_r$ defined in (11) can be implemented with one query to the QSGO $O_g$ of $f$.

**Proof.** We first prepare the following quantum state

$$|\psi\rangle = |x \rangle \otimes \left( \int_{y \in \mathbb{R}^d} \sqrt{\gamma_r(y)}dy \right) |x - y \rangle \otimes |0 \rangle, \quad \forall x \in \mathbb{R}^d.$$

Applying $O_g$ to the last two registers yields

$$(\mathbb{I} \otimes O_g) |\psi\rangle = |x \rangle \otimes \left( \int_{y \in \mathbb{R}^d} \sqrt{\gamma_r(y)}dy \right) \otimes \int_{v \in \mathbb{R}^d} \sqrt{p_{f,x-y}(v)} |v \rangle \otimes |\text{garbage}(v)\rangle = |x \rangle \otimes \int_{y, v \in \mathbb{R}^d} \sqrt{\gamma_r(y) p_{f,x-y}(v)} dy dv |x - y\rangle |v\rangle.$$

(12)

Given that

$$p_{F,x}(v) = \int_{y \in \mathbb{R}^d} \gamma_r(y) p_{f,x-y}(v) dy, \quad \forall v \in \mathbb{R}^d,$$

if we measure the last register, the probability density function of the outcome would be exactly $p_{F,x}$. Hence, the quantum state $(\mathbb{I} \otimes O_g) |\psi\rangle$ in (12) can also be written as

$$(\mathbb{I} \otimes O_g) |\psi\rangle = |x \rangle \otimes \int_{v \in \mathbb{R}^d} \sqrt{p_{F,x}(v)} |\text{garbage}(v)\rangle \otimes |v\rangle.$$

By swapping the last two quantum registers, we can obtain the desired output state of $O_{g,F}$.

The following result from [57] bounds the rate at which Algorithm 2 decreases the function error of $F_r$. Note that validity of this result relies solely on the fact that, at Line 6, the variance of the unbiased gradient estimate $\hat{g}_t$ does not exceed $\tilde{d}^2$, irrespective of its implementation.

**Lemma 6.** The output $x^g_{T+1}$ of Algorithm 2 satisfies

$$\mathbb{E}[F_r(x^g_{T+1}) - F_r^*] \leq \frac{4LR^2}{rT(T + 2)} + \frac{4R\tilde{d}}{\sqrt{T}},$$

where $F_r$ is the convoluted function defined in Line 1 of Algorithm 2 and $F_r^*$ is its minimum.

**Proof.** This lemma follows from [57, Corollary 1], which shows that

$$\mathbb{E}[F_r(x^g_{T+1}) - F_r^*] \leq \frac{4\ell_F R^2}{T(T + 2)} + \frac{4R\tilde{d}}{\sqrt{T}},$$

where $\ell_F$ is the Lipschitz parameter of $F_r$, which equals $L/r$ by Lemma 4.
Equipped with above results, we are now ready to present the proof of Theorem 5.

Proof of Theorem 5. By Lemma 6, the output $x_{\text{out}}$ of Algorithm 2 satisfies

$$
E[F(x_{\text{out}}) - F^*] \leq \frac{4R^2}{R(T + 2)} + \frac{4R\sigma}{\sqrt{T}} \leq \epsilon.
$$  
(13)

Moreover, by Lemma 4 we can derive that

$$
E[f(x_{\text{out}}) - f^*] \leq E[f(x_{\text{out}}) - F(x_{\text{out}})] + (f^* - F^*) + E[F(x_{\text{out}}) - F^*] = \epsilon.
$$

Finally we bound the expected number of queries to $O_g$ used in the algorithm. Since $\|g_F(x)\| \leq L$ for any $x \in \mathbb{R}^d$, by Theorem 4 we know that Algorithm 1 can output an estimate $\hat{g}_F(x_{\text{mid}})$ of $\nabla F(x_{\text{mid}})$ with variance at most $\delta^2$ using $\mathcal{O}(L\sqrt{d}/\delta)$ queries to the oracle $O_F$, and hence the same number of queries to $O_g$ by Lemma 5. Then, the total number of queries to $O_g$ equals

$$
T \cdot \mathcal{O} \left( \frac{L\sqrt{d}}{\delta} \right) = \frac{d^{1/4}LR}{\epsilon} \cdot \mathcal{O} \left( \frac{L\sqrt{d}}{\delta} \cdot \sqrt{\frac{R}{L\epsilon}} \right) = \mathcal{O} \left( d^{5/8} \cdot \left( \frac{LR}{\epsilon} \right)^{3/2} \right).
$$

\[ \square \]

D Proof of quantum stochastic cutting plane method

D.1 Proof of Proposition 1

Definition 5 ($\delta$-approximate gradient oracle ($\delta$-AGO)). For $f : \mathbb{R}^d \to \mathbb{R}$, its $\delta$-approximate gradient oracle, $\delta$-AGO, is defined as a random function that when queried at $x$, returns a vector $\hat{g}(x)$ that satisfies $\|\hat{g}(x) - \nabla f(x)\| \leq \delta$.

We show that a $\delta$-AGO can be efficiently implemented using our quantum variance reduction algorithm. To obtain this result we can also use [53, Claim 1] by changing some parameters. Nevertheless, compared to their deterministic implementation, our approach has a lower expected time complexity (though is randomized).

Lemma 7. For any $\delta, \xi \geq 0$, with success probability at least $1 - \xi$, the $\delta$-AGO of a Lipschitz function $f$ can be implemented using $\mathcal{O}(\log(1/\xi))$ calls to Algorithm 1 with in total $\mathcal{O}(L\sqrt{d}\log(1/\xi)/\delta)$ queries to the QSGO.

Proof. We implement the $\delta$-AGO using the following procedure. First, we obtain $k = \log(1/\xi) + 10$ independent unbiased estimates $g_1, \ldots, g_k$ of $\nabla f(x)$ with variance $\delta^2/16$ by Algorithm 1, using

$$
k \cdot \frac{L\sqrt{d}}{\delta} = \mathcal{O}(L\sqrt{d}\log(1/\xi)/\delta)
$$

queries in total to the QSGO $O_g$, by Theorem 4. Note that any individual sample $g_i$ satisfies

$$
Pr \left[ \|g_i - \nabla f(x)\| \geq \frac{\delta}{2} \right] \leq \frac{1}{4}.
$$

Hence, if we let $S$ denote the subset of $[k]$ where each $i \in S$ have $\ell_2$ distance to $\nabla f(x)$ at most $\delta/2$, then by Hoeffding’s inequality, $|S| \geq 2k/3$ with probability at least

$$
1 - \exp \left( -\frac{2(k/3 - k/4)^2}{k} \right) \geq 1 - \xi.
$$

Observe that for any sample $g_i$ satisfying $\|g_i - g_j\| \leq \delta/2$ for at least $2k/3$ of $g_i$’s, there must exist at least some $g_{j'} \in S$ such that $\|g_i - g_{j'}\| \leq \delta/2$, and therefore $\|g_i - \nabla f(x)\| \leq \delta$ by triangle inequality. Consequently, we just need to find and output any such $g_i$ as a $\delta$-AGO, which is guaranteed to exist given that any sample in $S$ satisfies this property. This can be done in expected $\mathcal{O}(k)$ time by picking a random estimate and checking whether it is close to at least $2k/3$ of other estimates. \[ \square \]
Next, we establish that we can query an $\epsilon$-optimal point by applying the cutting plane method with the separation oracle being an $O(\epsilon/R)$-approximate gradient oracle, as provided by Lemma 7.

**Proof of Proposition 1.** Define $K_{\epsilon/2}$ as the set of $\epsilon/2$-optimal points of the function $f$, and $K_{\epsilon}$ as the set of $\epsilon$-optimal points of $f$. We know that $K_{\epsilon/2}$ contains a ball of radius at least $r_K = \epsilon/(2L)$ since for any $x$ with $\|x - x^*\| \leq r_K$ we have

$$f(x) - f(x^*) \leq L\|x - x^*\| \leq \frac{\epsilon}{2}.$$  

(14)

We apply the cutting plane method, as described in Lemma 7, to query a point in $K_{\epsilon/2}$, which is a subset of the ball $B_{2R}(0)$. To achieve this, we use an $\epsilon/(10R)$-approximate gradient oracle ($\epsilon/(10R)$-AGO) of $f$, implemented using Lemma 7, as the separation oracle for the cutting plane method. Throughout this process, we assume each query to the $\epsilon/(10R)$-AGO is successfully executed, and we will later discuss the error probability associated with this assumption. In this case, we show that any query outside of $K_{\epsilon}$ to the $\epsilon/(10R)$-AGO will be a valid separation oracle for $K_{\epsilon/2}$. In particular, if we ever queried the $\epsilon/(10R)$-AGO at any $x \in B_{2R}(0) \setminus K_{\epsilon}$ with output being $\tilde{g}$, for any $y \in K_{\epsilon/2}$ we have

$$\langle \tilde{g}, y - x \rangle \leq \langle \nabla f(x), y - x \rangle + \|\tilde{g} - \nabla f(x)\| \cdot \|y - x\|$$

$$\leq f(y) - f(x) + \|\tilde{g} - \nabla f(x)\| \cdot \|y - x\|$$

$$\leq -\frac{\epsilon}{2} + \frac{\epsilon}{10R} \cdot 4R < 0,$$

where the second inequality is due to the convexity of $f$, indicating that $\tilde{g}$ is a valid separation oracle for the set $K_{\epsilon/2}$. Consequently, upon applying Lemma 2, we can deduce that after $Cd\log(dR/r_K)$ iterations, at least one of the queries must lie within $K_{\epsilon}$.

To ensure an overall success probability of at least $5/6$, we employ the union bound, which necessitates that each query to the $\epsilon/(10R)$-AGO be implemented with a failure probability of no more than $(6Cd\log(dR/r_K))^{-1}$, which by Lemma 7 requires

$$O \left( \frac{10LR\sqrt{d}}{\epsilon} \log(6Cd\log(dR/r_K)) \right) = \tilde{O} \left( \frac{L\sqrt{d}}{\epsilon} \right)$$

queries to the QSGO $O_{\tilde{g}}$, and the overall query complexity equals

$$\tilde{O} \left( \frac{L\sqrt{d}}{\epsilon} \right) \cdot C d\log(dR/r_K) = \tilde{O} \left( \frac{d^{3/2}LR}{\epsilon} \right).$$

□

**D.2 Proof of Proposition 2**

We first present the following algorithm that makes pairwise comparison using queries to the QSGO (Definition 3).

Note that in Line 7 of Algorithm 4 the estimation step is carried out in a projected space along the vector $\hat{e}$. This is motivated by the fact that we are specifically interested in the information of the gradient $\nabla f$ within this projected space, which effectively reduces to a one-dimensional variable. As a result, the mean estimation can be performed without introducing an additional factor of $\sqrt{d}$ in the query complexity as given in Theorem 4.

**Lemma 8.** For any $y_{10}, y_{r0} \in B_R(0)$ and any $\epsilon' > 0$, with success probability at least $1/(6T)$ Algorithm 4 returns a point $\hat{y} \in \mathbb{R}^d$ satisfying

$$f(\hat{y}) \leq \min_{\lambda \in [0,1]} f(\lambda y_{10} + (1 - \lambda)y_{r0}) + \epsilon'$$

using $\tilde{O} (RL/\epsilon')$ queries to an $L$-bounded QSGO $O_{\tilde{g}}$ defined in Definition 3.
Algorithm 4: StochasticLineSearch($y_{l0}, y_{r0}, \epsilon'$)

**Input:** Endpoints $y_l, y_r \in \mathbb{R}(0)$, accuracy $\epsilon'$

**Output:** $\hat{y}$ such that $f(\hat{y}) \leq \min_{\lambda \in [0,1]} f(\lambda y_l + (1-\lambda)y_r) + \epsilon'$.

1. $y_l \leftarrow y_{l0}, y_r \leftarrow y_{r0}$
2. if $y_l = y_r$ then return $y_l$
3. else
4.     $\hat{e} \leftarrow \frac{y_r - y_l}{\|y_r - y_l\|}$
5.     repeat
6.         $y_m \leftarrow (y_l + y_r)/2$
7.         Obtain an estimate $\hat{g}_e(y_m)$ of $\nabla f(y_m)\hat{e}$ with error at most $\epsilon'/(4R)$
8.         if $|\hat{g}_e(y_m)| \leq \epsilon'/(4R)$ then return $y \leftarrow y_m$
9.         else
10.        if $\hat{g}_e(y_m) > 0$ then $y_r \leftarrow y_m$ else $y_l \leftarrow y_m$
11. until $\|y_r - y_l\| \leq \epsilon'/L$
12. return $\bar{y} \leftarrow y_l$

**Proof.** Observe that in each iteration the value $\|y_r - y_l\|$ is decreased by at least $1/2$. Hence, the total number of iterations is at most

$$\log_2 \left( \frac{\|y_{r0} - y_{l0}\|}{\epsilon'/L} \right) \leq \log_2 \left( \frac{2RL}{\epsilon'} \right).$$

Within each iteration, we need to estimate the value $\nabla f(y_m)^\top \hat{e}$, which is the component of $\nabla f(y_m)$ along $\hat{e}$. Note that this is essentially a univariate mean estimation problem, given that $\hat{e}$ is fixed in this iteration we can define an 1-dimensional random variable $\nabla f(y_m)^\top \hat{e}$ whose variance is at most

$$\text{Var}[\nabla f(y_m)^\top \hat{e}] \leq \mathbb{E}|\nabla f(y_m)^\top \hat{e}|^2 \leq \mathbb{E}\|\nabla f(y_m)\|^2 \leq L^2.$$ 

Then by Lemma 7, with success probability at least

$$1 - \left(6T \log_2 \left( \frac{2RL}{\epsilon'} \right) \right)^{-1}, \quad (15)$$

an estimate of $\nabla f(y_m)^\top \hat{e}$ with error at most $\epsilon'/(4R)$ can be obtained using

$$\frac{L}{\epsilon'/(4R)} \cdot \log \left(6T \log_2 \left( \frac{2RL}{\epsilon'} \right) \right) = \tilde{O}(\frac{RL}{\epsilon'})$$

queries to the quantum stochastic gradient oracle $O_y$, given that we can prepare the following quantum oracle

$$O_{\hat{e}}^\dagger |x\rangle \otimes |0\rangle \rightarrow |x\rangle \otimes \int_{v \in \mathbb{R}^d} \sqrt{p_{f,x}(v)} dv |v^\top \hat{e}\rangle \otimes |\text{garbage}(v)\rangle,$$

using one query to $O_y$. Hence, Algorithm 4 uses $\tilde{O}(RL/\epsilon')$ queries to the quantum stochastic gradient oracle $O_y$, with failure probability at most

$$\log_2 \left( \frac{\|y_{r0} - y_{l0}\|}{\epsilon'/L} \right) \cdot \left(6T \log_2 \left( \frac{2RL}{\epsilon'} \right) \right)^{-1} \leq \frac{1}{6T} \quad (16)$$

by union bound. Next, we show that the output $\hat{y}$ of Algorithm 4 has a relatively small function value as desired. We denote

$$\lambda^* := \arg\min_{\lambda \in [0,1]} f(\lambda y_{l0} + (1-\lambda)y_{r0}) \quad \text{and} \quad y^* := \lambda^* y_{l0} + (1-\lambda^*)y_{r0}.$$ 

If the algorithm terminates at a point $\hat{y}$ satisfying $|\hat{g}_e(\hat{y})| \leq \epsilon'/(4R)$, by convexity and the Cauchy Schwarz inequality we have

$$f(\hat{y}) - f(y^*) \leq |\nabla f(\hat{y})^\top \hat{e}| : ||\hat{y} - y^*|| \leq \frac{\epsilon'}{2R} \cdot 2R \leq \epsilon'.$$
Otherwise, by induction we can demonstrate that in each iteration of the algorithm, $y^*$ resides within the segment bounded by $y_t$ and $y_r$. Assume that this assertion holds true for the $t$-th iteration. If $g_e(y_m) > \epsilon'/(4R)$, we have
\[
\langle \nabla f(y_m), y_t - y_m \rangle = -\langle \nabla f(y_m), \hat{e} \rangle \cdot \|y_t - y_m\| \\
\leq -\left( g_e(y_m) - \frac{\epsilon'}{4R} \right) \|y_t - y_m\| < 0,
\]
indicating that the value of $f$ will decrease along the direction $y_t - y_m$. Hence, $y^*$ lies in the segment between $y_t$ and $y_m$ of the $t$-th iteration, or equivalently, the segment between $y_t$ and $y_m$ of the $(t + 1)$-th iteration, given that $f$ is convex. A symmetric argument applies in the case of $g_e(y_m) < \epsilon'/(4R)$. Then, we have
\[
\|y_t - y^*\| \leq \|y_t - y_r\|
\]
for every iteration, which leads to
\[
\|\hat{y} - y^*\| \leq \frac{\epsilon'}{L}
\]
when the algorithm terminates. Hence,
\[
f(\hat{y}) - f(y^*) \leq L \cdot \|\hat{y} - y^*\| = \epsilon'
\]
considering that $f$ is $L$-Lipschitz. \qed

Using Algorithm 4 as a subroutine, we develop the following Algorithm 5 that solves Problem 5.

**Algorithm 5**: Stochastic Approximately best point among finite number of points

**Input**: A set of points $\{x_1, \ldots, x_T\} \subset \mathbb{R}(0)$ where $T$ is a power of 2, accuracy $\epsilon$

**Output**: $\mathbf{x}$ such that $f(\mathbf{x}) \leq \min_i f(x_i) + \epsilon$

1. $y_0,1 \leftarrow x_t$ for all $t \in [T]$
2. for $\tau = 1, \ldots, \log_2 T$
3. for $j = 1, \ldots, T/2^\tau$ do $y_{\tau,j} = \text{StochasticLineSearch}(y_{\tau-1,2^j-1}, y_{\tau-1,2^j}, \epsilon / \log_2 T)$
4. return $y_{\log_2 T, 1}$

**Proof of Proposition 2**. We start by demonstrating that without loss of generality we can assume $T$ to be a power of 2. If $T$ is not already a power of 2, we can simply augment the set with at most $T$ points, each being $x_1$, without changing the algorithm’s output.

Next, we show that Algorithm 5 makes $T - 1$ calls to the StochasticLineSearch($\cdot$) subroutine (Algorithm 4) with an accuracy of $\epsilon' = \epsilon / \log_2 T$ to solve the Problem 5 problem. The algorithm exhibits a hierarchical structure, as illustrated in Figure 1, where each non-leaf node invokes the StochasticLineSearch($\cdot$) subroutine once. Consequently, the total number of calls is $T - 1$.

By Lemma 8, each call to StochasticLineSearch($\cdot$) is executed successfully with probability at least $1 - 1/(6T)$. Then by union bound, we can deduce that the likelihood of all calls to StochasticLineSearch($\cdot$) being successful is at least $5/6$. In this case, for any node $y_{\tau,j}$ in the tree with $\tau \in [\log_2 T]$ and $j \in [T/2^\tau]$, by convexity and the guarantee of Lemma 8 we have
\[
f(y_{\tau,j}) \leq \min_{\lambda \in [0,1]} f(\lambda y_{\tau-1,2^j-1} + (1 - \lambda)y_{\tau-1,2^j}) + \epsilon / \log_2 T
\]
\[
\leq \min\{f(y_{\tau-1,2^j-1}), f(y_{\tau-1,2^j})\} + \epsilon / \log_2 T.
\]
Therefore for any leaf node $x_j$ with $j \in [T]$ by summing over the path between the root $y_{1,1}$ and $x_j$ we have
\[
f(y_{1,1}) \leq f(x_j) + t \cdot \frac{\epsilon}{\log_2 T} = f(x_j) + \epsilon,
\]
which leads to
\[
f(y_{1,1}) \leq \min_{j \in [T]} f(x_j) + \epsilon.
\]
indicating \( y_{t,1} \) is a valid solution of Problem 5. Note that there are in total \( T - 1 \) non-leaf nodes in Figure 1, and the value of each non-leaf node is computed by one call to the subroutine StochasticLineSearch(\cdot). Hence, the total number of calls to StochasticLineSearch(\cdot) equals \( T - 1 \), and the overall failure probability of Algorithm 5 is at most

\[
(T - 1) \cdot \frac{1}{6T} \leq \frac{1}{6} \tag{17}
\]

by union bound, as the failure probability of Algorithm 4 is at most \( 1/(6T) \). Since each call to Algorithm 4 takes

\[ O(RL/\epsilon) \]

queries to the quantum stochastic gradient oracle \( O_g \) defined in (2), the total number of queries to the quantum stochastic gradient oracle \( O_g \) is then \( O(RL/T) \).

D.3 Proof of Corollary 1

Proof of Corollary 1. We first run cutting plane method with the separation oracle being an \( \epsilon_{\text{BBR}} \)-approximate gradient of \( f \) implemented by Algorithm 1, which by Proposition 1 outputs a set \( \Gamma \) of \( T = O(d \log(L/\epsilon)) \) points containing at least one \( O(\epsilon) \)-optimal point of \( f \) using \( O(d^{3/2}LR/\epsilon) \) queries to \( O_g \) with success probability at least 5/6. Then by running Algorithm 5 on \( \Gamma \), with success probability at least 5/6 we can find a point \( \hat{x} \in \mathbb{R}^d \) satisfying

\[ f(\hat{x}) = \min_{x \in \Gamma} f(x) + \epsilon \leq f(x^*) + O(\epsilon), \]

which takes \( \tilde{O}(RLT/\epsilon) = O(dRL/\epsilon) \) queries to \( O_g \) by Proposition 2. Hence, the overall number of queries to \( O_g \) equals \( O(d^{3/2}LR/\epsilon) \), and the overall success probability is at least 2/3.

E Proof of Theorem 6

The proof of Theorem 6 is based on the following result from [40].

**Theorem 9** ([40, Theorem 1]). Consider the bounded variance setting in Problem 2, the output \( x_{\text{out}} \) of Algorithm 6 is an expected \( \frac{2\Delta \epsilon}{T} + \hat{\sigma}^2 \)-critical point.

**Proof of Theorem 6.** By Theorem 9 and the associated parameter setting, the output \( x_{\text{out}} \) of Algorithm 6 satisfies

\[
\mathbb{E} \| \nabla f(x_{\text{out}}) \|^2 \leq \frac{2\Delta \epsilon}{T} + \hat{\sigma}^2 \leq \epsilon^2,
\]
Algorithm 6: Quantum randomized SGD (Q-SGD)

**Input:** Function $f : \mathbb{R}^d \rightarrow \mathbb{R}$, precision $\epsilon$, variance $\sigma$, smoothness $\ell$

**Parameters:** $\hat{\sigma} = \epsilon/3$, total iteration budget $T = 12\Delta \ell \epsilon^{-2}$

**Output:** $\epsilon$-critical point of $f$

1. Uniformly randomly select $N$ from $1, \ldots, T$
2. Set $x_0 \leftarrow 0$
3. for $t = 0, 1, 2, \ldots, N - 1$
   4. Call Algorithm 1 for an unbiased estimate $\tilde{g}_t$ of $\nabla f(x_t)$ with variance at most $\hat{\sigma}^2$
   5. $x_{t+1} \leftarrow x_t - \tilde{g}_t / \ell$
6. return $x_N$

implying that Algorithm 6 solves Problem 2 with probability at least $2/3$ under the bounded variance setting, and the remaining thing would be to analyze the number of queries it makes to $O_g$. By Theorem 4, at each iteration one can run Algorithm 1 to obtain an unbiased estimate $\tilde{g}_t$ of $\nabla f(x_t)$ with variance at most $\hat{\sigma}^2$ using

$$\tilde{O} \left( \frac{\sigma \sqrt{d}}{\sigma} \right) = \tilde{O} \left( \frac{\sigma \sqrt{d}}{\epsilon} \right).$$

queries to $O_g$. Then, the total number of queries to $O_g$ is at most

$$T \cdot \tilde{O} \left( \frac{\sigma \sqrt{d}}{\epsilon} \right) = \tilde{O} \left( \frac{\sigma \Delta \ell \sqrt{d}}{\epsilon^3} \right).$$

□

F Proof of Theorem 7

Algorithm 7: Q-SPIDER

**Input:** Function $f : \mathbb{R}^d \rightarrow \mathbb{R}$, precision $\epsilon$, variance $\sigma$, smoothness $\ell$

**Parameters:** $q = \frac{20\sigma}{\epsilon^2}, \hat{\sigma}_1 = \frac{\epsilon}{20}, \hat{\sigma}_2 = \frac{\epsilon}{40} \sqrt{\frac{d}{100}},$ total iteration budget $T = \frac{1600\Delta}{\sigma^2}$

**Output:** An $\epsilon$-critical point of $f$

1. Set $x_0 \leftarrow 0$
2. for $t = 0, 1, 2, \ldots, T$
   3. if $\text{mod}(t, q) = 0$ then
      4. Call Algorithm 1 to obtain an unbiased estimate $\tilde{g}_t$ of $\nabla f(x_t)$ with variance $\hat{\sigma}_1^2$
      5. $v_t \leftarrow \tilde{g}_t$
   else
      6. Call Algorithm 1 to obtain an unbiased estimate $\tilde{g}_t$ of $\nabla f(x_t) - \nabla f(x_{t-1})$ with variance $\hat{\sigma}_2^2$
      7. $v_t \leftarrow \tilde{g}_t + v_{t-1}$
   8. if $\|v_t\| \leq 2\epsilon$ then return $x_t$;
   9. else $x_{t+1} \leftarrow x_t - \frac{\epsilon}{\ell} \cdot \frac{v_t}{\|v_t\|}$
10. return $x_T$

The proof of Theorem 7 is based on the following result from [29].

**Theorem 10** ([29, Theorem 1]). Consider the mean-squared smoothness setting in Problem 2, the output $x_{\text{out}}$ of Algorithm 7 is an expected $\epsilon$-critical point.

**Proof of Theorem 7.** Theorem 10 shows that Algorithm 7 can solve Problem 2 under the mean-squared smoothness setting and the remaining thing would be to analyze the number of queries it makes to $O_g$. }

25
For each iteration $t$ with $\text{mod}(t, q) = 0$ such that Line 5 is executed, note that we can prepare the following quantum oracle
\[
\hat{O}_g |x⟩ \otimes |0⟩ \rightarrow |x⟩ \otimes \int_\omega \sqrt{p(\omega) d\omega} |g(x, \omega)⟩ \otimes |\text{garbage}(x, \omega)⟩,
\]
where $p(\omega)$ is the probability distribution of the random seed $\omega$, by first applying $O^S_g$ to the state
\[
|x⟩ \otimes \left( \int_\omega \sqrt{p(\omega) d\omega} |\omega⟩ \otimes |0⟩ \right)
\]
and then uncompute the second register. This procedure uses one query to the $\sigma$-SQ-QSGO $O^S_g$ (Definition 4). By Theorem 4, one can run Algorithm 1 to obtain an unbiased estimate $\tilde{g}_t$ of $\nabla f(x_t)$ with variance at most $\hat{\sigma}_t^2$ using
\[
\tilde{\tilde{O}} \left( \frac{\sigma \sqrt{d}}{\hat{\sigma}_1} \right) = \tilde{\tilde{O}} \left( \frac{\sigma \sqrt{d}}{\epsilon} \right)
\]
queries to $\hat{O}_g$ and thus the same number of queries to $O^S_g$.

Similarly, for each iteration $t$ with $\text{mod}(t, q) = 0$ such that Line 7 is executed, note that one can prepare the following quantum oracle
\[
\hat{O}^t_g |x_t⟩ \otimes |x_{t-1}⟩ \otimes |0⟩ \rightarrow |x_t⟩ \otimes |x_{t-1}⟩ \otimes \int_\omega \sqrt{p(\omega) d\omega} |g(x_t, \omega) - g(x_{t-1}, \omega)⟩ \otimes |\text{garbage}(x_t, x_{t-1}, \omega)⟩
\]
by first applying $O^S_g$ twice to obtain the state
\[
|x⟩ \otimes |x_{t-1}⟩ \otimes \int_\omega \sqrt{p(\omega) d\omega} |\omega⟩ \otimes |g(x_t, \omega)⟩ \otimes |g(x_{t-1}, \omega)⟩ \otimes |g(x_t, x_{t-1}, \omega)⟩ \otimes |\text{garbage}(x_t, x_{t-1}, \omega)⟩
\]
and then uncompute the fourth and the fifth register. Observe that
\[
\mathbb{E}_\omega ||g(x_t, \omega) - g(x_{t-1}, \omega)||^2 \leq \ell^2 ||x_t - x_{t-1}|| \leq \epsilon^2,
\]
then by Theorem 4, one can run Algorithm 1 to obtain an unbiased estimate $\tilde{g}_t$ of $\nabla f(x_t) - \nabla f(x_{t-1})$ with variance at most $\hat{\sigma}_t^2$ using
\[
\tilde{\tilde{O}} \left( \frac{\epsilon \sqrt{d}}{\hat{\sigma}_2} \right) = \tilde{\tilde{O}} \left( \frac{\epsilon d}{\sqrt{\epsilon}} \right)
\]
queries to $\hat{O}^t_g$ and thus twice the number of queries to $O^S_g$. Then, the total number of queries to $O^S_g$ can be expressed as
\[
\frac{T}{q} \cdot \tilde{\tilde{O}} \left( \frac{\sigma \sqrt{d}}{\epsilon} \right) + T \cdot \tilde{\tilde{O}} \left( \frac{\sqrt{d} \sigma}{\epsilon} \right) = \tilde{\tilde{O}} \left( \frac{\ell \Delta \sqrt{d}}{\epsilon^2} \left( 1 + \sqrt{\frac{\sigma}{\epsilon}} \right) \right).
\]

\[\Box\]

G Proof of lower bounds

G.1 Proof of Proposition 3

Note that Problem 3 is strictly harder than the multivariate mean estimation problem considered in [25]. In the latter, the objective is to produce an estimate of the expected value within a bounded $\ell_2$ error, without the requirement of unbiasedness. A query lower bound for solving quantum mean estimation was established in [25].
Lemma 9 ([25, Theorem 3.8]). Let $\sigma \geq 0$ and denote $P_{\sigma}$ to be the set of all $d$-dimensional quantum random variables with covariance matrix $\Sigma$ such that $\text{Tr}(\Sigma) = \sigma^2$. Suppose every $X \in P_{\sigma}$ is indexed by some random seeds $\omega$, i.e.,

$$X = X(\omega), \quad \omega \sim p_{\Omega},$$

where $p_{\Omega}$ denotes the probability distribution of the random seed $\omega$. Then there exists a constant $\alpha$ such that for any $n > \alpha d$ and any quantum algorithm that uses at most $n$ queries to the following two oracles

$$O_{\Omega} |0\rangle \rightarrow \int_{\omega} \sqrt{p_{\Omega}(\omega)} d\omega |\omega\rangle \quad \text{and} \quad B_{X} |\omega\rangle |0\rangle \rightarrow |\omega\rangle |X(\omega)\rangle,$$

there exists an instance $X \in P_{\sigma}$ such that the quantum algorithm returns a mean estimate $\tilde{\mu}$ of the mean $\mu$ of $X$ that satisfies

$$\|\tilde{\mu} - \mu\| \geq \Omega\left(\frac{\sigma \sqrt{d}}{n}\right)$$

with probability at least $2/3$.

By employing an oracle reduction argument, we obtain our lower bound result based on Lemma 9.

Proof of Proposition 3. We first show that one query to the quantum sampling oracle $O_X$ defined in Definition 1 can be implemented using one query to $O_{\Omega}$ and one query to $B_X$. In particular, observe that

$$B_X O_{\Omega} |0\rangle \otimes |0\rangle = \int_{\omega} \sqrt{p_{\Omega}(\omega)} d\omega \otimes |X(\omega)\rangle.$$

By measuring the first register in the computational basis spanned by all the random seeds $\{|\omega\rangle\}$, we can obtain the desired output of $O_X$. Hence, if there exists a quantum algorithm making at most $O(L \sqrt{d}/\sigma)$ queries to the oracle $O_X$ that solves Problem 3 with success probability at least $2/3$, there also exists a quantum mean estimation algorithm that uses at most $O(L \sqrt{d}/\sigma)$ queries to $O_{\Omega}$ and $B_X$ and for any $X \in P_{\sigma}$ it outputs an estimate $\tilde{\mu}$ of the mean $\mu$ of $X$ that satisfies $\|\tilde{\mu} - \mu\| \leq O(\sigma)$ with probability at least $2/3$, which contradicts to Lemma 9. \hfill \Box

G.2 Proof of Theorem 8

Our proof follow a similar approach to the previous proof of the quantum mean estimation lower bound [25]. Specifically, our results are derived through a reduction to a specific multivariate mean estimation problem. In this problem, all vectors are sampled from a set of orthonormal bases and there might be duplicated vectors. We choose to reduce to this particular problem instead of directly reducing to mean estimation problem because the construction of our hard instances require a tighter control over the norm of the vectors as well as the norm of their expected value. This problem can be equivalently represented as the following composition problem, as defined in [25].

Problem 6 (Search$^N \circ$ Parity$^M$). Let $N, M \geq 1$ be two integers. Let $A_{N, M}$ denote the set of matrices $A \in \{0, 1\}^{N \times M}$ such that $\lfloor N/2 \rfloor$ rows have Hamming weights $\lfloor M/2 \rfloor$, and the other rows have Hamming weights $\lceil M/2 \rceil + 1$. Define the vector $b^{(A)}$ such that,

$$b^{(A)}_i = \begin{cases} 0, & \text{if the } i\text{-th row of } A \text{ has Hamming weight } \lfloor M/2 \rfloor, \\ 1, & \text{if the } i\text{-th row of } A \text{ has Hamming weight } \lceil M/2 \rceil + 1, \end{cases}$$

for each $i \in [N]$. Then, the Search$^N \circ$ Parity$^M$ problem consists of finding a vector $\tilde{b} \in \mathbb{R}^N$ that minimizes $\|\tilde{b} - b^{(A)}\|_1$ given a quantum oracle

$$O_A |i, j\rangle \rightarrow (-1)^{A_{ij}} |i, j\rangle.$$  

[25] showed that $\Omega(NM)$ queries are needed to approximate the vector $b^{(A)}$ with small error.
Lemma 10 ([25, Lemma 3.6]). There exists a constant $\alpha > 1$ such that, for any quantum algorithm for the $\text{Search}^N \circ \text{Parity}^M$ problem that uses at most $NM/\alpha$ queries there exists an $A \in \mathcal{A}_{N,M}$ such that this algorithm returns a vector $\mathbf{b}$ satisfying $\|\mathbf{b} - \mathbf{b}^{(A)}\| \geq \sqrt{N}/2$ with probability at least $2/3$.

We establish our quantum lower bounds for stochastic convex optimization by establishing a correspondence between the $\text{Search}^N \circ \text{Parity}^M$ problem and Problem 1. Specifically, for any input $A \in \mathcal{A}_{N \times M}$ to the $\text{Search}^N \circ \text{Parity}^M$ problem, we design the following convex function whose optimal point corresponds to the solution of the $\text{Search}^N \circ \text{Parity}^M$ problem under certain sets of parameters,

$$\bar{f}^A(x) := \mathbb{E}_{i,j} [f_{i,j}(x)],$$

where

$$f_{i,j}^A(x) := -\frac{1}{3} \langle x, g_{i,j} \rangle + 2L \cdot \max \left\{ 0, \|x\| - \frac{R}{2} \right\}$$

for some $g_{i,j} \in \mathbb{R}^d$ satisfying $\|g_{i,j}\| \leq L$ for all $i \in [N]$ and $j \in [M]$.

**Lemma 11.** Denote $\bar{g} := \mathbb{E}_{i,j} [g_{i,j}]$. Then, the function $\bar{f}^A$ defined in (20) has the following properties if $\bar{g}$ is a non-zero vector.

1. $\bar{f}^A$ is convex.
2. $\bar{f}^A$ is minimized at $x^* = \frac{R}{2} \frac{\bar{g}}{\|\bar{g}\|}$.
3. Every $\epsilon$-optimum $x$ of $\bar{f}^A$ satisfies

$$\left\langle \frac{R}{2}, \frac{x}{\|x\|}, x^* \right\rangle \geq 1 - \frac{R\epsilon}{2\|\bar{g}\|}$$

4. For

$$g_{i,j}(x) := -\frac{1}{3} \cdot g_{i,j} + 2L \cdot \max \left\{ \|x\| - \frac{R}{2}, 0 \right\} \cdot \frac{x}{\|x\|}$$

it is the case that

$$\mathbb{E}_{i,j} [g_{i,j}(x)] \in \partial \bar{f}^A(x) \quad \text{and} \quad \|g_{i,j}(x)\| \leq L, \quad \forall x \in \mathbb{R}^d.$$

**Proof.** Since $\bar{f}^A$ is the sum of a linear function and a maximum function, both of which are convex, $\bar{f}^A$ itself is convex.

Observe that the minimum of $\bar{f}^A$ cannot be achieved when $\|x\| > R/2$ for otherwise the function value can be further decreased when moving towards $0$ given that

$$\|\bar{g}\| = \left\| \sum_{i,j} g_{i,j} \right\| = \sum_{i,j} \|g_{i,j}\| \leq \sum_{i,j} \frac{\|g_{i,j}\|}{NM} \leq L.$$

When $\|x\| \leq R/2$, $\bar{f}^A$ can be expressed as

$$\bar{f}^A(x) = -\frac{1}{3} \langle x, \bar{g} \rangle,$$

which is minimized at

$$\frac{R}{2} \frac{\bar{g}}{\|\bar{g}\|} = \frac{R\mathbf{b}^{(A)}}{\sqrt{2d}}.$$

For any $x$ that is an $\epsilon$-optimum of $\bar{f}^A$, we define

$$x' = \begin{cases} x, & \|x\| \leq \frac{R}{2}, \\ \frac{R}{2} \frac{x}{\|x\|}, & \text{otherwise}, \end{cases}$$
which satisfies $f(x') \leq f(x)$ and is thus also an $\epsilon$-optimum of $f$. Then we can derive that
\[
-\frac{1}{3} \langle x', g \rangle + \frac{1}{3} \langle x^*, g \rangle \leq \epsilon,
\]
and
\[
\langle x', x^* \rangle \geq \langle x^*, x^* \rangle - \epsilon \cdot \frac{\|x^*\|}{\|g\|} \geq 1 - \frac{R \epsilon}{2\|g\|},
\]
which leads to
\[
\frac{R}{2} \cdot \frac{x}{\|x\|} \cdot x^* \geq 1 - \frac{R \epsilon}{2\|g\|},
\]
given that $\frac{R}{2} \cdot \frac{x}{\|x\|} \geq \|x'\|$. As for the last entry, note that
\[
E_{i,j} [\hat{g}_{i,j}(x)] = -\frac{1}{3} \cdot E_{i,j} g_{i,j} + \frac{2L}{3} \cdot \max \left\{ \|x\| - \frac{R}{2} \right\} \cdot \frac{x}{\|x\|}
\]
\[
= -\frac{1}{3} \cdot g + \frac{2L}{3} \cdot \max \left\{ \|x\| - \frac{R}{2} \right\} \cdot \frac{x}{\|x\|},
\]
which is the (sub-)gradient of $\bar{f}^A$ at $x$. Moreover, for any $i,j$ we have
\[
\|\hat{g}_{i,j}(x)\| \leq \frac{1}{3} \|g_{i,j}\| + \frac{2L}{3} \leq L.
\]

Equipped with Lemma 11, we first prove our quantum lower bound for Problem 1 in the low-dimensional regime by encoding the Search $\circ$ Parity problem into the task of finding an $\epsilon$-optimal point of $\bar{f}^A$ defined in (20).

**Proof of Theorem 8 when $\epsilon \leq \frac{RL}{100\sqrt{d}}$.** Our proof proceeds by contradiction. Denote $n = \frac{RL\sqrt{d}}{100\alpha\epsilon}$. Assume for simplicity that $d$ is even, and $\alpha n$ is an even multiple of $d$ (the other cases can be handled by padding arguments). Then, we show that Search$^d \circ$ Parity$^{\alpha n/d}$ on this instance $A$ can be solved by finding an $\epsilon$-optimal of $\bar{f}^A$ defined in (20). In particular, we define the set of vectors $\{g_{i,j}\}$ to be
\[
g_{i,j} = \frac{\alpha Ln}{\sqrt{(2\alpha n)^2 - d^2}} (-1)^{1+A_{i,j}} e_i,
\]
where $i \in [d], j \in [\alpha n/d], \text{ and } e_i \in \mathbb{R}^d$ is the $i$-th indicator vector. Consider the function $\bar{f}^A$ defined in (20) with the set of vectors $\{g_{i,j}\}$ having the values in (22), we have
\[
\bar{g} = \mathbb{E}_{i,j} [g_{i,j}] = \frac{1}{\alpha n} \cdot \frac{\alpha Ln}{\sqrt{(2\alpha n)^2 - d^2}} \sum_{i=1}^d e_i \sum_{j=1}^{\alpha n/d} (-1)^{1+A_{i,j}}
\]
\[
= \frac{2L}{\sqrt{(2\alpha n)^2 - d^2}} \sum_{i=1}^d b_i^{(A)} = \frac{2L}{\sqrt{(2\alpha n)^2 - d^2}} b^{(A)},
\]
where the vector $b^{(A)}$ is defined in (18). By Lemma 11, every $\epsilon$-optimal point $x$ of $\bar{f}^A$ satisfies
\[
\frac{R}{2} \cdot \frac{x}{\|x\|} \cdot x^* \geq 1 - \frac{R \epsilon}{2\|g\|},
\]
by which we can derive that
\[
\frac{R}{2} \cdot \frac{x}{\|x\|} \cdot b^{(A)} \geq \frac{\|b^{(A)}\|}{\|x^*\|} \cdot \left( 1 - \frac{R \epsilon}{2\|g\|} \right)
\]
\[
\geq \frac{R}{2} \sqrt{\frac{d}{2} - 3\alpha n} = \frac{R \sqrt{d}}{L},
\]

29
which leads to
\[ \left\langle \sqrt{\frac{d}{2}} \cdot \frac{x}{\|x\|}, b^{(A)} \right\rangle \geq \frac{d}{2\sqrt{2}}. \]
Given that
\[ \left\| \sqrt{\frac{d}{2}} \cdot \frac{x}{\|x\|} \right\| = \left\| b^{(A)} \right\| = \sqrt{\frac{d}{2}}, \]
we have
\[ \left\| \sqrt{\frac{d}{2}} \cdot \frac{x}{\|x\|} - b^{(A)} \right\| \leq \frac{\sqrt{d}}{2}, \]
indicating that we can obtain an estimate \( \tilde{b} = \sqrt{\frac{d}{2}} \frac{x}{\|x\|} \) of \( b^{(A)} \) with \( \ell_2 \)-error at most \( \sqrt{d}/2 \) by obtaining an \( \epsilon \)-optimal point of \( \tilde{f}^A \).

Next, we show that we can implement a quantum stochastic gradient oracle of \( \bar{f}^A \) using only one query to the oracle \( O_A \), given that one can use one query to \( O_A \) to implement the following oracle
\[ O_A \left| i \right\rangle \left| j \right\rangle \left| 0 \right\rangle \rightarrow \left| i \right\rangle \left| j \right\rangle \left| g_{i,j}(x) \right\rangle, \]
and use one query to \( O_g^A \) to implement
\[ O_g^A \left| i \right\rangle \left| j \right\rangle \left| 0 \right\rangle \rightarrow \left| i \right\rangle \left| j \right\rangle \left| \tilde{g}_{i,j}(x) \right\rangle, \]
where \( g_{i,j}(x) \) is defined in (21). Then by applying \( O_g^A \) to the state
\[ \frac{1}{\sqrt{\alpha n}} \sum_{i \in [d]} \sum_{j \in \left[ \alpha n/d \right]} |i \rangle |j \rangle |0 \rangle \]
and uncompute the second and the third register, we construct the following stochastic gradient oracle \( O_{g}^A \) of \( f^A \).
\[ O_{g}^A \left| x \right\rangle \otimes \left| 0 \right\rangle \rightarrow \frac{1}{\sqrt{\alpha n}} \left| x \right\rangle \otimes \sum_{i \in [d]} \sum_{j \in \left[ \alpha n/d \right]} |i \rangle |j \rangle \left| \tilde{g}_{i,j}(x) \right\rangle. \]
Hence, any quantum algorithm that can find an \( \epsilon \)-optimum of \( f^A \) using \( T \) queries to \( O_{g}^A \) can be transformed into a quantum algorithm for the \( \text{Search}^d \circ \text{Parity}^{\alpha n/d} \) problem that uses \( T \) queries to the oracle \( O_A \) defined in (19) and returns an estimate \( \tilde{b} \) with \( \ell_2 \)-error at most \( \sqrt{d}/2 \). Then by Lemma 10, for any quantum algorithm making less than
\[ d \cdot \frac{\alpha n}{d} \cdot 1 = \frac{R L}{2 \alpha n} \sqrt{\frac{d}{2}} \]
queries to the quantum stochastic gradient oracle \( O_{g}^A \), there exists an \( A \in \mathcal{A}_{d,\alpha n/d} \) and corresponding \( \bar{f}^A \) such that the output of the algorithm is not an \( \epsilon \)-optimum of \( f^A \) with probability at least \( 2/3 \). □

Similarly, we can obtain our quantum lower bound in the high-dimensional regime by encoding the \( \text{Search} \circ \text{Parity} \) problem into the task of finding an \( \epsilon \)-optimal point of \( \bar{f}^A \) defined in (20).

**Proof of Theorem 8 when** \( \frac{RL}{100 \sqrt{d}} \leq \epsilon \leq 1 \). Our proof proceeds by contradiction. Denote \( n = \frac{R L^2}{10 \sqrt{\alpha n}} \). Consider an instance \( A \in \mathcal{A}_{\alpha n,1} \) of the \( \text{Search}^{\alpha n} \circ \text{Parity}^1 \) problem where \( d \) is a power of 2 and \( \alpha \) is even. Then, we show that \( \text{Search}^d \circ \text{Parity}^{\alpha n/d} \) on this instance \( A \) can be solved by finding an \( \epsilon \)-optimum of \( \bar{f}^A \) defined in (20). In particular, we define the set of vectors \( \{g_{i,j}\} \) where \( j \equiv 1 \) to be
\[ g_{i,1} = \alpha LA_{i,1} \sqrt{\frac{n}{2\alpha^2 n - 2\alpha}} e_i, \]  
(23)
where \( i \in [\alpha n] \) and \( e_i \in \mathbb{R}^d \) is the \( i \)-th indicator vector. Consider the function \( \bar{f}^A \) defined in (20) with the set of vectors \( \{g_{i,1}\} \) having the values in (23), we have

\[
\bar{g} = \mathbb{E}[g_{i,1}] = \frac{\alpha L}{\alpha n} \sqrt{\frac{n}{2\alpha^2 n - 2\alpha}} \sum_{i=1}^{d} A_{1,i} e_i = \frac{L}{n} \sqrt{\frac{n}{2\alpha^2 n - 2\alpha}} b^{(A)},
\]

where the vector \( b^{(A)} \) is defined in (18). By Lemma 11, every \( \epsilon \)-optimal point \( x \) of \( \bar{f}^A \) satisfies

\[
\langle \frac{R}{2} \cdot \frac{x}{\|x\|}, x^* \rangle \geq 1 - \frac{R\epsilon}{2\|g\|},
\]

by which we can derive that

\[
\langle \frac{R}{2} \cdot \frac{x}{\|x\|}, b^{(A)} \rangle \geq \frac{\|b^{(A)}\|}{\|x^*\|} \cdot \left( 1 - \frac{R\epsilon}{2\|g\|} \right) \geq \frac{R}{2} \sqrt{\frac{\alpha n}{2} - \frac{6\alpha n}{L}} = \frac{R\sqrt{\alpha n}}{4},
\]

which leads to

\[
\langle \sqrt{\frac{\alpha n}{2}} \cdot \frac{x}{\|x\|}, b^{(A)} \rangle \geq \frac{\alpha n}{2\sqrt{2}}.
\]

Given that

\[
\left\| \sqrt{\frac{\alpha n}{2}} \cdot \frac{x}{\|x\|} \right\| = \frac{\|b^{(A)}\|}{\|x^*\|} = \frac{\sqrt{\alpha n}}{2},
\]

we have

\[
\left\| \sqrt{\frac{\alpha n}{2}} \cdot \frac{x}{\|x\|} - b^{(A)} \right\| \leq \frac{\sqrt{\alpha n}}{2},
\]

indicating that we can obtain an estimate \( \hat{b} = \sqrt{\frac{\alpha n}{2}} \cdot \frac{x}{\|x\|} \) of \( b^{(A)} \) with \( \ell_2 \)-error at most \( \sqrt{d}/2 \) by obtaining an \( \epsilon \)-optimal point of \( \bar{f}^A \).

Next, we show that we can implement a quantum stochastic gradient oracle of \( \bar{f}^A \) using only one query to the oracle \( O_A \), given that one can use one query to \( O_A \) to implement the following oracle

\[
O^A_{g} \ | i \rangle \ | 0 \rangle \rightarrow \ | i \rangle \ | g_{i,1} \rangle
\]

and use one query to \( O^A_{g} \) to implement

\[
O^A_{g} \ | x \rangle \ | i \rangle \ | 0 \rangle \rightarrow \ | x \rangle \ | i \rangle \ | g_{i,1}(x) \rangle ,
\]

where \( g_{i,1}(x) \) is defined in (21). Then by applying \( O^A_{g} \) to the state

\[
\frac{1}{\sqrt{\alpha n}} \ | x \rangle \sum_{i \in [\alpha n]} \ | i \rangle \ | 0 \rangle
\]

and uncompute the second and the third register, we construct the following stochastic gradient oracle \( O^A_{g} \) of \( f^A \).

\[
O^A_{g} \ | x \rangle \otimes | 0 \rangle \rightarrow \frac{1}{\sqrt{\alpha n}} \ | x \rangle \otimes \sum_{i \in [\alpha n]} \ | g_{i,1}(x) \rangle .
\]

Hence, any quantum algorithm that can find an \( \epsilon \)-optimum of \( f^A \) using \( T \) queries to \( O^A_{g} \) can be transformed into a quantum algorithm for the Search\( \alpha n \circ \text{Parity}^1 \) problem that uses \( T \) queries to the oracle \( O_A \) defined in (19) and returns an estimate \( \hat{b} \) with \( \ell_2 \)-error at most \( \sqrt{d}/2 \). Then by Lemma 10, for any quantum algorithm making less than

\[
\alpha n = \frac{R^2 L^2}{100 \epsilon^2}
\]

queries to the quantum stochastic gradient oracle \( O^A_{g} \), there exists an \( A \in A_{\alpha n,1} \) and corresponding \( \bar{f}^A \) such that the output of the algorithm is not an \( \epsilon \)-optimum of \( f^A \) with probability at least \( 2/3 \). \( \square \)