**SCIENCE CHINA**
Information Sciences

• **Supplementary File** •

# Exact Quantum Query Complexity of Weight Decision Problems via Chebyshev Polynomials

Xiaoyu HE[1,2], Xiaoming SUN[1,2*], Guang YANG[1,2] & Pei YUAN[1,2]

[1]*Institute of Computing Technology, Chinese Academy of Sciences (CAS), Beijing* 100190*, China;*
[2]*University of Chinese Academy of Sciences, Beijing* 100049*, China*

## Appendix A Preliminary

An important and amazing feature of quantum mechanics is that we can only "read" a quantum state by measuring it, when the superposed quantum state collapses to a *random* sample according to a classical distribution. As a result, many quantum algorithms would make error if the final quantum state does not collapse to the desired sample corresponding to the correct answer. Although the error probability can be reduced through repetition, it remains natural to ask when and how such error can be completely eliminated.

*Exact quantum algorithms* are quantum algorithms that always give exactly the correct answer (decoded from the measurement result). The complexity of such algorithms can be measured in the number of queries to the input oracle. An example is the Deutsch-Jozsa algorithm [1] which shows an exponential speed-up of quantum computation over classical ones.

*Exact quantum query complexity* of a problem $\mathcal{P}$ is the necessary number of queries required by exact quantum algorithms to find the correct answer of $\mathcal{P}$. This is a quantum analog of the classical decision tree complexity, and it is also the exact version of quantum query complexity where bounded-error are allowed. Furthermore, the exact quantum query complexity turns out to be a good choice for demonstrating quantum advantages, since its classical counterpart, the exact query complexity of deterministic algorithms, is usually significantly greater than that of (classical) bounded-error algorithms. For example, a deterministic algorithm needs $\Omega(n)$ queries to solve Deutsch-Jozsa problem whereas a trivial $\varepsilon$-error BPP algorithm only needs $O\left(\log \frac{1}{\varepsilon}\right)$ queries.

The implementation of a quantum algorithm $\mathcal{A}$ in the query complexity model is described as follows: $\mathcal{A}$ starts with a fixed state $|\Psi_{start}\rangle$ and performs a sequence of operations $U_0, O_x, U_1, O_x, \ldots, O_x, U_t$, where every $O_x$ denotes an oracle query to the input $x$ and each $U_i$ is a unitary operator independent of $x$; the result $\mathcal{A}(x)$ is obtained from the measurement of the final state $|\Psi_{end}\rangle = U_t O_x U_{t-1} \cdots U_1 O_x U_0 |\Psi_{start}\rangle$. The quantum query complexity of $\mathcal{A}$ is $t$ since it makes $t$ queries to the input oracle. If furthermore $\mathcal{A}$ always give the correct answer, $\mathcal{A}$ is an exact quantum algorithm with exact quantum query complexity $Q_E(\mathcal{A}) = t$. The exact quantum query complexity of a function $f$, denoted by $Q_E(f)$, is the minimum query complexity of all quantum algorithms that compute $f$ exactly on all inputs, *i.e.*

$$Q_E(f) = \min_{\mathcal{A}:\forall x, \mathcal{A}(x)=f(x)} Q_E(\mathcal{A})$$

For any positive integer $t$, let $[t] := \{1, \ldots, t\}$ and $[t]_0 := \{0, 1, \ldots, t\}$. Let $f : D \to \{0,1\}$ denote a (partial) Boolean function whose domain is $D \subseteq \{0,1\}^n$. In the quantum query model, $O_x$ is the quantum (phase-flip) oracle query to the input $x$ defined as

$$O_x|i\rangle := \begin{cases} (-1)^{x_i}|i\rangle, & \text{if } i \in [n]; \\ |0\rangle, & \text{if } i = 0. \end{cases}$$

which can be obtained by conjugating the standard bit-flip oracle with Hadamard gates [2].

We say that a quantum algorithm computes $f$ exactly if for every $x \in D$ the algorithm outputs $f(x)$ with probability 1 in finite steps. The exact quantum query complexity $Q_E(f)$ is the minimum number of queries of all quantum algorithms computing $f$ exactly.

It is easy to show that every Boolean function can be represented by $n$-variate polynomials.

**Definition 1.** For a function $f : D \to \{0,1\}$ with domain $D \subseteq \{0,1\}^n$, an $n$-variate polynomial $p : \mathbb{R}^n \to \mathbb{R}$ is called a *real-valued multilinear polynomial representation* of $f$ if $f(x) = p(x)$ for all $x \in D$ and $0 \leqslant p(x) \leqslant 1$ for all $x \in \{0,1\}^n$. The *degree* of $f$, denoted by $\deg(f)$, is defined as the minimum degree of all real-valued multilinear polynomial representations of $f$.

A Boolean function is *symmetric* if permutating its inputs does not change its outputs. Namely, the value of $f(x)$ is fully determined by $|x|$. In fact, any real-valued multilinear polynomial representation of a symmetric function can be converted to a univariate polynomial of $|x|$ with the same degree [3]. We will make no distinction between these two polynomial representations of symmetric Boolean functions if the meaning is clear from the context.

The following lemma by Beals *et al.* establishes a connection between the degree of $f$ and its exact quantum query complexity $Q_E(f)$.

**Lemma 1** ( [4])**.** If $f$ is a (total) Boolean function, then $Q_E(f) \geqslant \deg(f)/2$.

According to the following Property 1, we will only investigate $f_n^{k,l}$ with $k < l$.

**Proposition 1** ( [5])**.** For every $n \in \mathbb{N}$ and $k, l \in [n]_0$, $Q_E(f_n^{k,l}) = Q_E(f_n^{n-l,n-k})$.

* Corresponding author (email: sunxiaoming@ict.ac.cn)

Suppose that $f_{n'}^{\kappa n',\lambda n'}$ is computed by a $d$-query exact quantum algorithm. To compute $f_n^{k,l}$, we can pad $a$ many zeros and $b$ many ones to the input of $f_n^{k,l}$ and hence reduce $f_n^{k,l}$ to $f_{n+a+b}^{k+b,l+b}$, where the latter is indeed $f_{n'}^{\kappa n',\lambda n'}$ when $a=\frac{l-k}{\lambda-\kappa}-\frac{l\kappa-k\lambda}{\lambda-\kappa}-n$ and $b=\frac{l\kappa-k\lambda}{\lambda-\kappa}$ (so that $k+b=\kappa n'$ and $l+b=\lambda n'$ for $n'=n+a+b$). As long as $a,b,k$ and $l$ are non-negative integers, the above reduction is straightforward and $f_n^{k,l}$ can be computed by a $d$-query exact quantum algorithm as well, *i.e.* $Q_E(f_n^{k,l})\leqslant Q_E(f_n^{\kappa n.\lambda n})$. However the naïve padding technique is very limited in the sense that we cannot pad a non-integer (or irrational, if we only care about $\frac{k}{n}$ and $\frac{l}{n}$) number of zeros or ones.

## Appendix B Related works

In this paper we study the exact quantum query complexity of weight decision problems. Such problems require to decide the Hamming weight $|x|$ of a vector $x$ drawn from $\{0,1\}^n$, with all possible weights of $x$ given in advance. In query complexity model this is equivalent to decide the output weight of a given Boolean function when interpreting $x$ as the truth table. Such weight analysis of Boolean functions may find applications, as a whole or building blocks of more sophisticated algorithms, in various areas such as cryptanalysis [6], coding theory [7], fault-tolerant circuit design [8], the built-in self-testing of circuits [9] and so on.

In particular, two well-known quantum speed-up examples are special cases of weight decision problems: the Deutsch-Jozsa problem [1] requires to distinguish $|x|=n/2$ from $|x|\in\{0,n\}$; and the (decision version of) Grover search problem [10] distinguishes $|x|=0$ from $|x|=1$ (see [11–13] for exact algorithms, and [14]) for a setting with prior knowledge of solution.

Many previous studies on weight decision problems generalized the above two famous problems. For example, Montanaro, Jozsa, and Mitchison [15] considered the discrimination of $|x|=\frac{n}{2}$ from $|x|\in\{0,1,n-1,n\}$. Qiu and Zheng [5, 16] proved that the exact quantum query complexity of distinguishing $|x|=\frac{n}{2}$ from $|x|\in\{0,1,\ldots,k,n-k,n-k+1,\ldots,n\}$ is $k+1$. The Grover search problem can be generalized as the discrimination of two specific weights $|x|=k$ and $|x|=l$, for $(k,l)$ other than $(0,1)$. Brassard *et al.* [11] introduced quantum amplitude amplification as a general and optimal solution for the case $k=0$, and with similar intuition Choi and Braunstein [17, 18] obtained asymptotically tight bounds for $l>k>0$.

The weight decision function $f_n^{k,l}$ studied in this paper is most relevant to the generalization of Grover search [10] and amplitude amplification [11] which distinguishes two specific weights $k$ and $l$. Along this line, Braunstein *et al.* [19] first proved that $Q_E(f_n^{k,n-k})=O(\frac{n}{|n-2k|})$. Later, Choi and Braunstein [17] showed $Q_E(f_n^{k,l})=O(\frac{n}{l-k})$ when $0\leqslant k<\frac{n}{2}<l\leqslant n$ via a reduction to the symmetric form $f_n^{k,n-k}$, and Choi [18] proved the asymptotic optimality of this upper bound (for $0\leqslant k<\frac{n}{2}<l\leqslant n$) with techniques from [20]. Qiu and Zheng [5] proved that $Q_E(f_n^{\frac{n}{4},\frac{3n}{4}})=2$ and characterized all cases reducible to $f_n^{\frac{n}{4},\frac{3n}{4}}$ via classical padding. This does save one query compared with [17], but it turns out just a special case of our algorithm and further requires $l-k$ to be even to apply a classical padding. [5] also proved $Q_E(f_n^{0,k})=2$ for $\frac{n}{4}\leqslant k<\frac{n}{2}$, extending the previous knowledge [21] that $Q_E(f_n^{0,l})=1$ for $l\geqslant\frac{n}{2}$. A very recent work by Scott Aaronson [22] studied the tradeoff between two kinds of quantum resources for computing $f_n^{k,2k}$ with bounded error, and proved the necessity of either $\Omega(\sqrt{n/k})$ queries or $\Omega(\min\{k^{1/4},\sqrt{n/k}\})$ copies of $|x\rangle=\frac{1}{\sqrt{|x|}}\sum_{x_i=1}|i\rangle$, which is technically orthogonal to our work. In summary, previous results on quantum query complexity of $f_n^{k,l}$ are either asymptotic or ad-hoc, and the crude padding technique only handles discrete parameters and sometimes requires divisibility. In this paper we not only propose a systemic solution that vastly extends the knowledge of (both upper and lower bounds of) $Q_E(f_n^{k,l})$, but also introduce a quantum padding technique that removes range and divisibility restrictions such as $k<\frac{n}{2}<l$ or $l-k$ must be even.

We remark that the bounded-error quantum query complexity of $f_n^{k,l}$ is $Q_2(f_n^{k,l})=\Omega\left(\frac{\sqrt{(n-k)l}}{l-k}\right)$ by [18], which matches our upper bound for $Q_E(f_n^{k,l})$ as in Corollary 1. Thus both exact and bounded-error quantum query complexity of $f_n^{k,l}$ are $\Theta\left(\frac{\sqrt{(n-k)l}}{l-k}\right)$, with an advantage over the deterministic query complexity $D(f_n^{k,l})=n-l+k+1$.

Total Boolean functions of similar forms are also studied but in a way technically orthogonal to our work. For example, Ambainis *et al.* [23] proved that $\max\{n-k,l\}-1\leqslant Q_E(\mathsf{EXACT}_{k,l}^n)\leqslant\max\{n-k,l\}+1$, where $0\leqslant k\leqslant l\leqslant n$, $\mathsf{EXACT}_{k,l}^n(x)=1$ on inputs of Hamming weight $|x|\in\{k,l\}$ and $\mathsf{EXACT}_{k,l}^n(x)=0$ otherwise. The quantum advantage of $\mathsf{EXACT}_{k,l}^n$ is much less than that of $f_n^{k,l}$ mainly because it is a total Boolean function. In general, the quantum speed-up for total Boolean functions are polynomially bounded: in the bounded-error setting, Beals *et al.* [4] proved that $Q_2(f)=\Omega\left(D(f)^{1/6}\right)$; and Midrijanis [24] proved that $Q_E(f)=\Omega\left(D(f)^{1/3}\right)$. However, the best separation from randomized query complexity was linear until 2013 when the first superlinear speed-up example with $Q_E(f)=O\left(R_2(f)^{0.86\cdots}\right)$ was discovered by Ambainis [25] (the current best separation is $Q_E(f)=\widetilde{O}\left(R_2(f)^{1/2}\right)$ by [26]). In [27], Ambainis *et al.* showed that almost all $n$-bit Boolean functions have exact quantum query complexity less than $n$ except $\mathsf{AND}_n$, up to isomorphism. Aaronson *et al.* [28] presented a total function $f$ with $R_2(f)=\widetilde{\Omega}(Q_2(f)^{2.5})$. Aaronson and Ambainis [29] together proved that $R_2(f)=O(Q_2(f)^7\mathrm{polylog}Q_2(f))$ for every symmetrically partial (not necessarily Boolean) function $f$.

## Appendix C Chebyshev polynomials

In this paper, we employ the mathematical tools *Chebyshev polynomials of the first kind* [30], which are denoted by $\{T_n\}_{n=1}^{\infty}$. More specifically, we use the following properties of the Chebyshev polynomials:

**Proposition 2** ( [30]). Let $T_n$ be the first kind Chebyshev polynomial of degree $n$, then

1. $|T_n(x)|\leqslant 1$ for $|x|\leqslant 1$, and $|T_n(x)|>1$ for $|x|>1$;
2. $T_n(\cos(\frac{k\pi}{n}))=(-1)^k$ for $k\in[n]_0$ and $T_n'(\cos(\frac{k\pi}{n}))=0$ for $k\in[n-1]$.

For convenience, we call the points in $\{x\in[-1,1]\mid|T_n(x)|=1\}$ *extrema* of $T_n$.

Now we explain the relation between Chebyshev polynomials and the weight decision problem. Noticing that the range of Chebyshev polynomials is $[-1,1]$, we consider another representation of Boolean functions on $\{-1,1\}$, *i.e.* $\hat{f}:\{-1,1\}^n\to\{-1,1\}$. The function $f_n^{k,l}:\{0,1\}^n\to\{0,1\}$ can be transformed into $\hat{f}_n^{k,l}$ defined on input $\hat{x}=(\hat{x}_1,\ldots,\hat{x}_n)\in\{-1,1\}^n$ by setting

$\hat{x}_i = (-1)^{x_i}$ for every $x_i \in \{0,1\}$ and $i \in [n]$:

$$\hat{f}_n^{k,l}(\hat{x}) = \begin{cases} 1, & \text{if } |\hat{x}| = n-2k; \\ -1, & \text{if } |\hat{x}| = n-2l; \\ undefined, & \text{otherwise.} \end{cases}$$

Note that $\hat{f}_n^{k,l}$ distinguishes $|\hat{x}| = n-2k$ from $|\hat{x}| = n-2l$ since $|\hat{x}| := \sum_{i=1}^n \hat{x}_i = n-2|x|$.

The bijection between $f_n^{k,l}(x)$ and $\hat{f}_n^{k,l}(\hat{x})$ also holds on their polynomial representations, *i.e.* if a polynomial $p(|x|)$ represents $f_n^{k,l}(x)$ then $\hat{p}(|\hat{x}|) = 1 - 2 \cdot p\left(\frac{n-|\hat{x}|}{2}\right)$ represents $\hat{f}_n^{k,l}(\hat{x})$ accordingly. And in particular, $\hat{p}(|\hat{x}|) = \hat{f}_n^{k,l}(\hat{x})$ for $|\hat{x}| = n-2k$ and $|\hat{x}| = n-2l$, and $-1 \leqslant \hat{p}(|\hat{x}|) \leqslant 1$ for every $\hat{x} \in \{-1,1\}^n$. However, the domain of $\hat{p}$ is $[-n,n]$ since $|\hat{x}| \leqslant n$ for $\hat{x} \in \{-1,1\}^n$. To fit the Chebyshev polynomials which are bounded on the domain $[-1,1]$, we introduce the polynomial $\hat{P}$ such that $\hat{P}(z) = \hat{p}(zn)$. Note that $\deg(\hat{P}) = \deg(\hat{p}) = \deg(p)$ since we only use linear transformations. In particular $\hat{P}(1-\frac{2k}{n}) = \hat{p}(n-2k) = 1$ corresponds to $p(k) = 0$, $\hat{P}(1-\frac{2l}{n}) = \hat{p}(n-2l) = -1$ corresponds to $p(l) = 1$.

Let $\hat{P}$ be the Chebyshev polynomial of degree $D = 2d$ or $2d-1$, *i.e.* $T_D = T_{2d}$ or $T_{2d-1}$. Then $\hat{P}$ should distinguish the two weights as $\hat{P}(1-\frac{2k}{n}) = (-1)^\gamma$ and $\hat{P}(1-\frac{2l}{n}) = (-1)^{\gamma+1}$, which turn out to be two extrema of the Chebyshev polynomial $T_D$. Recalling that padding is inherently limited in amplifying gaps, we consider consecutive extrema of $T_D$ in the form $(\eta_\gamma, \eta_{\gamma+1}) := \left(\cos(\frac{\gamma\pi}{D}), \cos(\frac{(\gamma+1)\pi}{D})\right)$ as boundary cases where $T_D(\eta_\gamma) = -T_D(\eta_{\gamma+1})$ and $T'_D(\eta_\gamma) = T'_D(\eta_{\gamma+1}) = 0$. Translating $(1-\frac{2k}{n}, 1-\frac{2l}{n}) \equiv (\eta_\gamma, \eta_{\gamma+1})$ back to the polynomial $p$ representing $f_n^{k,l}$, we get $\left(\frac{k}{n}, \frac{l}{n}\right)$ as a boundary case for the weight decision problem, where $\frac{k}{n} = \frac{1}{2}(1-\cos(\frac{\gamma\pi}{D}))$ and $\frac{l}{n} = \frac{1}{2}(1-\cos(\frac{(\gamma+1)\pi}{D}))$. The definition of $\{S_d\}_{d\in\mathbb{N}}$ before Theorem 1 consists of such boundary cases derived from extrema of both $T_{2d}$ and $T_{2d-1}$ for every $d$, after tailored[1)] for our upper and lower bound results.

## Appendix C.1 Extrema of Chebyshev polynomials and exact quantum algorithms

In this section, we will discuss the relationship between extrema of Chebyshev polynomials and exact quantum algorithms for $f_n^{k,l}$. In order to distinguish inputs with two different weights, we need a quantum algorithm that the final states are in two orthogonal subspaces corresponding to inputs of different weights. Let $\kappa = \frac{k}{n}$ and $\lambda = \frac{l}{n}$ for $n,k,l \in \mathbb{N}$. Suppose $\delta \in \{0,1\}$, $d \in [n]$ and $\gamma, \chi \in [2d-\delta-1]_0$. In what follows, we will show that if $1-2\kappa$ and $1-2\lambda$ are two extrema $\eta_\gamma := \cos\left(\frac{\gamma\pi}{2d-\delta}\right), \eta_\chi := \cos\left(\frac{\chi\pi}{2d-\delta}\right)$ of a Chebyshev polynomial $T_{2d-\delta}$ and $\gamma - \chi$ is odd, then $\{x \in \{0,1\}^n \mid |x| = k\}$ and $\{x \in \{0,1\}^n \mid |x| = l\}$ can be distinguished by a $d$-queries quantum algorithm. For simplicity we only consider the case $\gamma - \chi = 1$ in this subsection.

Let the initial state be $|\Psi_0\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^n |i\rangle$ and $\theta = \arcsin\sqrt{\frac{|x|}{n}}$, then $|\Psi_0\rangle$ can be interpreted as follows:

$$|\Psi_0\rangle = \cos\theta|\alpha_\perp\rangle + \sin\theta|\alpha\rangle$$

where $|\alpha_\perp\rangle := \frac{1}{\sqrt{n-|x|}} \sum_{i:x_i=0} |i\rangle$ and $|\alpha\rangle := \frac{1}{\sqrt{|x|}} \sum_{i:x_i=1} |i\rangle$. For the construction of our algorithm we define two unitary transformations $W$ and $U$ as follows.

(1) $W$ is a unitary transformation over a $n$-dimensional Hilbert space with basis vectors $\{|1\rangle, \ldots, |n\rangle\}$. It is a unitary transformation described as follows:

$$W|k\rangle = \frac{2}{n} \sum_{i=1}^n |i\rangle - |k\rangle, \ \forall k \in [n].$$

(2) $U$ denotes a unitary transformation over a $\left(n + \binom{n}{2}\right)$-dimensional Hilbert space with basis vectors $\{|k\rangle, |i,j\rangle \mid i,j,k \in [n], i < j\}$. It is a unitary completion of the following transformation:

$$U|k\rangle = \frac{1}{n} \sum_{i=1}^n |i\rangle + \frac{1}{\sqrt{n}} \left( \sum_{i:k<i\leqslant n} |k,i\rangle - \sum_{i:1\leqslant i<k} |i,k\rangle \right), \ \forall k \in [n].$$

It is easy to verify that both $W$ and $U$ are unitary transformations. For convenience, we further define two unitary transformations $G$ and $R$ such that $G := WO_x$ and $R := UO_x$. The operator $G$ is also known as the Grover operator [10] and $R$ is a rotation operator. After applying the operators $G$ and $R$ respectively, the initial state $|\Psi_0\rangle$ becomes

$$G|\Psi_0\rangle = \cos(3\theta)|\alpha_\perp\rangle + \sin(3\theta)|\alpha\rangle,$$

$$R|\Psi_0\rangle = \cos(2\theta)|\beta_\perp\rangle + \sin(2\theta)|\beta\rangle,$$

where $|\beta\rangle := \frac{1}{\sqrt{n}} \sum_{i=1}^n |i\rangle$ and $|\beta_\perp\rangle := \frac{1}{\sqrt{(n-|x|)|x|}} \sum_{i,j:x_i=0,x_j=1} |i,j\rangle$.

Next, we investigate the special cases of $k = \kappa n, l = \lambda n$ when $1-2\kappa$ and $1-2\lambda$ are two consecutive extrema of a Chebyshev polynomial (i.e. $\gamma - \chi = 1$). After applying Grover operators $G$ for $d-1$ times on $|\Psi_0\rangle$, the initial state becomes

$$|\Psi_{d-1}\rangle := G^{d-1}|\Psi_0\rangle = \cos((2d-1)\theta)|\alpha_\perp\rangle + \sin((2d-1)\theta)|\alpha\rangle,$$

Without loss of generality, we may assume $\gamma$ is odd and continue the discussion for $\delta = 0$ and $\delta = 1$. In the discussion we let $m \in \{\gamma, \gamma+1\}$ such that $\frac{m\pi}{2(2d-\delta)} = \theta = \arcsin\left(\sqrt{\frac{|x|}{n}}\right)$.

1) For $\gamma = 0$ the case $\left(0, \frac{1}{2}\left(1-\cos\left(\frac{\pi}{2d-1}\right)\right)\right)$ is excluded since it is dominated by $\left(0, \frac{1}{2}\left(1-\cos\left(\frac{\pi}{2d}\right)\right)\right)$ and does not affect the bounds. The symmetric case $\left(\frac{1}{2}\left(1-\cos\left(\frac{(2d-2)\pi}{2d-1}\right)\right), 1\right)$ is excluded as well.

(1) If $\delta = 1$, then $1-2\kappa = \cos\left(\frac{\gamma\pi}{2d-1}\right)$ and $1-2\lambda = \cos\left(\frac{(\gamma+1)\pi}{2d-1}\right)$ are two extrema of $T_{2d-1}(x)$. $|\Psi_{d-1}\rangle$ can be rewritten as

$$|\Psi_{d-1}\rangle = \cos\left(\frac{m\pi}{2}\right)|\alpha_\perp\rangle + \sin\left(\frac{m\pi}{2}\right)|\alpha\rangle.$$

Then we measure $|\Psi_{d-1}\rangle$ in computational basis, and make another query to $x_s$ if the measurement outcome is $s \in [n]$. Note that $x_s = 0$ implies $m$ is even, and $x_s = 1$ implies $m$ is not an even integer. Thus we can distinguish between $|x| = k$ and $|x| = l$ with certainty.

(2) If $\delta = 0$, then $1-2\kappa = \cos\left(\frac{\gamma\pi}{2d}\right)$ and $1-2\lambda = \cos\left(\frac{(\gamma+1)\pi}{2d}\right)$ are extrema of $T_{2d}(x)$. Apply operator $R$ to $|\Psi_{d-1}\rangle$ and obtain

$$\begin{aligned}|\Psi_d\rangle :&= R|\Psi_{d-1}\rangle = \cos(2d\theta)|\beta_\perp\rangle + \sin(2d\theta)|\beta\rangle\\ &= \cos\left(\frac{m\pi}{2}\right)|\beta_\perp\rangle + \sin\left(\frac{m\pi}{2}\right)|\beta\rangle.\end{aligned}$$

We now measure $|\Psi_d\rangle$ in orthogonal basis $\{|k\rangle, |i,j\rangle | k,i,j \in [n], i<j\}$. If the measurement result is $|k\rangle (k \in [n])$, then $m$ is even, otherwise $m$ is not an even integer. Thus we can distinguish between $|x| = k$ and $|x| = l$ with certainty.

From the above discussion, we conclude that if $1-2\kappa$ and $1-2\lambda$ are both extrema of a Chebyshev polynomial $T_{2d-\delta}(x)$ for some $d \in [n]$ where $\delta \in \{0,1\}$ and $T_{2d-\delta}(1-2\kappa)\cdot T_{2d-\delta}(1-2\kappa) = -1$, then $f_n^{k,l}$ can be computed by a $d$-queries exact quantum algorithm.

One may wonder that the above argument only makes sense when both $k = \kappa n$ and $l = \lambda n$ are integers for the input length $n \in \mathbb{N}$. For a general choice of parameters, the extrema of Chebyshev polynomials are likely to be irrational and hence $f_n^{k,l}$ turns out to be meaningless, *e.g.* for $T_4$ and $\gamma = 0$, the weight decision function $f_n^{0,(1-\sqrt{2})n/2}$ is constant on its domain since no $x \in \{0,1\}^n$ could have an irrational weight $|x| = (1-\sqrt{2})n/2$. However, we remark that although the above algorithm does not solve a meaningful weight decision problem, the essential power of the construction remains valid in amplifying the gap between two quantum states to be distinguished.

## Appendix D Asymptotically optimal upper bound

**Theorem 1** (Upper bounds)**.** For every $d \in \mathbb{N}$ and $0 \leqslant k < l \leqslant n$ with $k,l,n \in \mathbb{N}$, let $\kappa = \frac{k}{n}$ and $\lambda = \frac{l}{n}$. If $(\kappa,\lambda) \in \mathsf{UL}(S_d)$, then $Q_E(f_n^{k,l}) \leqslant d$.

The upper bound for $Q_E(f_n^{k,l})$ in Theorem 1 can be represented in terms of $k$ and $l$ as in Corollary 1. This is asymptotically optimal because there is a matching lower bound for the (bounded-error) quantum query complexity of $f_n^{k,l}$ by [18].

**Corollary 1.** If $k,l,n \in \mathbb{N}$ and $0 \leqslant k < l \leqslant n$, then $Q_E(f_n^{k,l}) = O\left(\frac{\sqrt{(n-k)l}}{l-k}\right)$.

*Proof.* Let $\mathsf{R}(x,y) = \left\{(\kappa,\lambda) \in I^2 | \kappa \leqslant x \wedge \lambda \geqslant y\right\}$ be the upper-left rectangle of $(x,y)$. It immediately follows that $\mathsf{R}(x,y) \subseteq \mathsf{UL}(x,y)$. By Theorem 1, if $(x,y) \in S_d$ and $(\frac{k}{n}, \frac{l}{n}) \in \mathsf{R}(x,y) \subseteq \mathsf{UL}(x,y)$, then there exists a $d$-query exact quantum algorithm for $f_n^{k,l}$, *i.e.* $Q_E(f_n^{k,l}) \leqslant d$. In what follows we will determine an upper bound for $d$.

In order to get $(\frac{k}{n}, \frac{l}{n}) \in \mathsf{R}(x,y)$ for some $d$ and $(x,y) \in S_d$, it suffices to find $\gamma \in [2d-1]_0$ such that $x = \frac{1}{2}\left(1-\cos\left(\frac{\gamma\pi}{2d}\right)\right)$ and $y = \frac{1}{2}\left(1-\cos\left(\frac{(\gamma+1)\pi}{2d}\right)\right)$ satisfy the following:

$$\begin{cases} \frac{k}{n} \leqslant x = \frac{1}{2}\left(1-\cos\left(\frac{\gamma\pi}{2d}\right)\right) = \sin^2\left(\frac{\gamma\pi}{4d}\right); \\ \frac{l}{n} \geqslant y = \frac{1}{2}\left(1-\cos\left(\frac{(\gamma+1)\pi}{2d}\right)\right) = \sin^2\left(\frac{(\gamma+1)\pi}{4d}\right). \end{cases}$$

Solving above inequalities for $\gamma$, we get

$$0 \leqslant \frac{4d}{\pi}\arcsin\sqrt{\frac{k}{n}} \leqslant \gamma \leqslant \frac{4d}{\pi}\arcsin\sqrt{\frac{l}{n}} - 1 \leqslant 2d-1.$$

Therefore, the desired integer $\gamma \in [2d-1]_0$ exists if $d$ is sufficiently large such that

$$\left(\frac{4d}{\pi}\arcsin\sqrt{\frac{l}{n}} - 1\right) - \frac{4d}{\pi}\arcsin\sqrt{\frac{k}{n}} \geqslant 1,$$

which is $d \geqslant \frac{\pi}{2}\Big/\left(\arcsin\sqrt{\frac{l}{n}} - \arcsin\sqrt{\frac{k}{n}}\right)$. Next we show that $d = O\left(\frac{\sqrt{(n-k)l}}{l-k}\right)$ suffices if $k < \frac{n}{2}$.

Notice that $g(z) = \arcsin(z) - z$ is monotonically increasing when $z \in [0,1]$. Thus we have $\arcsin\sqrt{\frac{l}{n}} - \arcsin\sqrt{\frac{k}{n}} > \sqrt{\frac{l}{n}} - \sqrt{\frac{k}{n}} > 0$ as long as $0 \leqslant k < l \leqslant n$, and hence

$$\frac{\pi}{2}\Big/\left(\arcsin\sqrt{\frac{l}{n}} - \arcsin\sqrt{\frac{k}{n}}\right) < \frac{\pi}{2}\Big/\left(\sqrt{\frac{l}{n}} - \sqrt{\frac{k}{n}}\right) = O\left(\frac{\sqrt{(n-k)l}}{l-k}\right)$$

where the last equality holds because $\sqrt{l} + \sqrt{k} < 2\sqrt{l}$ for $k < l$ and $\sqrt{n} < 2\sqrt{n-k}$ for $k < n/2$.

Therefore, for any $k < \frac{n}{2}$, there is $Q_E(f_n^{k,l}) \leqslant d = O\left(\frac{\sqrt{(n-k)l}}{l-k}\right)$. Exactly the same upper bound holds for $k \geqslant \frac{n}{2}$ since $Q_E(f_n^{k,l}) = Q_E(f_n^{n-l,n-k})$ and now $n-l < n-k \leqslant \frac{n}{2}$.

## Appendix E Proof of Theorem 2

In this section, we prove the lower bounds for exact quantum query complexity of weight decision problems. Our main result is described in Theorem 2 and its immediate corollary as follows.

**Theorem 2.** For every $d \in \mathbb{N}$ and $0 \leqslant k < l \leqslant n$ with $k, l, n \in \mathbb{N}$, let $\kappa = \frac{k}{n}$ and $\lambda = \frac{l}{n}$. If $(\kappa, \lambda) \in \mathsf{LR}(S_d)$, then $Q_E(f_n^{k,l}) \geqslant d+1$ for sufficiently large $n$.

**Corollary 2.** If $n$ is sufficiently large and integers $k, l$ satisfying $0 \leqslant k < l \leqslant n$, then $Q_E(f_n^{k,l}) \geqslant 1+\max\left\{d \mid (\frac{k}{n}, \frac{l}{n}) \in \mathsf{LR}(S_d)\right\}$.

In the quantum query complexity model, the degree of a Boolean function provides a lower bound for its exact quantum query complexity following Lemma 1. Therefore, in order to prove $Q_E(f_n^{k,l}) \geqslant d+1$, it suffices to show that $\deg(f_n^{k,l}) \geqslant 2d+1$. Let $p : \mathbb{R} \to \mathbb{R}$ denote the minimum degree univariate polynomial representing $f_n^{k,l}$ (see Definition 1), and let $q(x) = \pm(1-2p((1-x)n/2))$. Note that $\deg(p) = \deg(q)$, and it suffices to prove the lower bound for $\deg(q)$. The following two lemmas give lower bounds for $\deg(q)$ when $0 < k < l < n$ (Lemma 2) and $k = 0$ or $l = n$ (Lemma 3) respectively.

**Lemma 2.** For every integer $m \geqslant 3$ and $\gamma \in [m-2]$, let $\eta_\gamma = \cos(\frac{\gamma\pi}{m})$, $\eta_{\gamma+1} = \cos\left(\frac{(\gamma+1)\pi}{m}\right)$ and

$$D_\gamma := \left\{ (y_1, y_2) \in [-1,1]^2 \;\middle|\; \begin{array}{l} (1+\eta_{\gamma+1})(y_1+1) \leqslant (1+\eta_\gamma)(y_2+1) \\ (1-\eta_{\gamma+1})(y_1-1) \leqslant (1-\eta_\gamma)(y_2-1) \\ y_1 > y_2, (y_1, y_2) \neq (\eta_\gamma, \eta_{\gamma+1}) \end{array} \right\}.$$

For every real polynomial $p : \mathbb{R} \to \mathbb{R}$ satisfying $-1 \leqslant p(x) \leqslant 1$ for any $x \in \{1 - \frac{2k}{n} | k \in [n]_0\}$, if there exists $(x_1, x_2) \in D_\gamma$ such that $p(x_1) = (-1)^{\gamma+1}$ and $p(x_2) = (-1)^\gamma$, then $\deg(p) \geqslant m+2$ when $n$ is sufficiently large.

In Lemma 2, $\eta_\gamma$ and $\eta_{\gamma+1}$ are two consecutive extrema of the first kind Chebyshev polynomial $T_m$. $D_\gamma$ is the triangle region which is derived from $\mathsf{LR}\left(\frac{1-\eta_\gamma}{2}, \frac{1-\eta_{\gamma+1}}{2}\right)$ via a linear transformation.

Our proof is composed of two steps. First, we show that for any real polynomial $p$ proposed in Lemma 2: (i) there exist two different extreme point $x_1', x_2'$ of $p$ such that $(x_1', x_2') \in D_\gamma$ for sufficiently large $n$; (ii) $|p(x)| \leqslant 1+\varepsilon$ for any $\varepsilon \geqslant 0$ and $x \in [-1,1]$ when $n$ is sufficiently large. Second, we prove that $|p(-1)| > 1$ or $|p(1)| > 1$ for $\deg(p) \leqslant m+1$ based on the first step, which is contradicted with the fact that $|p(-1)| \leqslant 1$ and $|p(1)| \leqslant 1$.

*Proof.* [Proof of Lemma 2] For any $x \in [-1,1]$, there exists an integer $k = \lceil \frac{n-\lfloor nx \rfloor}{2} \rceil$ such that $0 \leqslant k \leqslant n$ and $x - \frac{n-2k}{n} \leqslant \frac{2}{n}$. Recalling that $-1 \leqslant p((n-2k)/n) \leqslant 1$, by Lagrange mean value theorem, there exists $x_0 \in [(n-2k)/n, x]$ such that

$$|p'(x_0)| \geqslant \frac{|p(x) - p((n-2k)/n)|}{x - \frac{n-2k}{n}} \geqslant \frac{(|p(x)|-1)n}{2}.$$

Therefore, let $|p| = \max_{|x|\leqslant 1} |p(x)|$,

$$\max_{|x|\leqslant 1} |p'(x)| \geqslant |p'(x_0)| \geqslant \frac{(|p|-1)n}{2}.$$

Let $d$ denote the degree of polynomial $p(x)$, and $p(x)$ has a property [31] that

$$d^2 \geqslant \frac{\max_{|x|\leqslant 1} |p'(x)|}{\max_{|x|\leqslant 1} |p(x)|}.$$

That is

$$d^2 \geqslant \frac{\max_{|x|\leqslant 1} |p'(x)|}{|p|} \geqslant \frac{(|p|-1)n}{2|p|},$$

and hence

$$|p| \leqslant 1 + \frac{2d^2}{n-2d^2}.$$

Namely, for any $\varepsilon \geqslant 0$ and sufficiently large $n$ we have

$$|p| \leqslant 1+\varepsilon.$$

Recall that $p(x_1) = (-1)^{\gamma+1}$ and $p(x_2) = (-1)^\gamma$. Without lose of generality, let $\gamma$ be odd. If $p'(x_1) \leqslant 0$, there exists $x_1' \in \left[\frac{n-2\lceil n(1-x_1)/2\rceil}{n}, x_1\right]$ such that $p'(x_1') = 0$ and $p(x_1') \geqslant 1$ because $p\left(\frac{n-2\lceil n(1-x_1)/2\rceil}{n}\right) \leqslant 1$ and $p(x_1) = 1$; If $p'(x_1) \geqslant 0$, there exists $x_1' \in \left[x_1, \frac{n-2\lfloor n(1-x_1)/2\rfloor}{n}\right]$ such that $p'(x_1') = 0$ and $p(x_1') \geqslant 1$ because $p\left(\frac{n-2\lfloor n(1-x_1)/2\rfloor}{n}\right) \leqslant 1$ and $p(x_1) = 1$. Namely, there exists $x_1' \in (x_1 - \frac{2}{n}, x_1 + \frac{2}{n})$ satisfying $p'(x_1') = 0$ and $p(x_1') \geqslant 1$. Similarly, there exists $x_2' \in (x_2 - \frac{2}{n}, x_2 + \frac{2}{n})$ satisfying $p'(x_2') = 0$ and $p(x_2') \leqslant -1$.

Note that $(x_1', x_2') \in D_\gamma$ when $n$ is sufficiently large and $(x_1, x_2) \in D_\gamma$ since $D_\gamma$ is an open set. Therefore, for any $\gamma \in [m-2]$,there exists $(x_1', x_2') \in D_\gamma$ such that

$$\begin{cases} (-1)^{\gamma+1} p(x_1') \geqslant 1, \\ (-1)^\gamma p(x_2') \geqslant 1, \\ p'(x_1') = 0, \\ p'(x_2') = 0. \end{cases}$$

We operate some linear transformation on polynomial $p(x)$ and get polynomial $g(x)$, let

$$g(x) = \frac{2(-1)^\gamma}{p(x_2') - p(x_1')} \left( \frac{p(x_1') + p(x_2')}{2} - p\left( \frac{(x_2' - x_1')x + x_1'\eta_{\gamma+1} - x_2'\eta_\gamma}{\eta_{\gamma+1} - \eta_\gamma} \right) \right).$$

In fact, $\deg(p)=\deg(g)$ and $g(x)$ satisfies

$$\begin{cases} g(\eta_\gamma)=(-1)^\gamma, \\ g(\eta_{\gamma+1})=(-1)^{\gamma+1}, \\ g'(\eta_\gamma)=0, \\ g'(\eta_{\gamma+1})=0, \\ |g(x)|\leqslant 1+\varepsilon, \forall x\in[-1,1], \end{cases}$$

for any $\varepsilon\geqslant 0$.

Since $(x_1',x_2')\in D_\gamma$, there exists $|\xi|>1$ such that

$$g(\xi)=\frac{2(-1)^\gamma}{p(x_2')-p(x_1')}\left(\frac{p(x_1')+p(x_2')}{2}-p(-1)\right)$$

for $\xi=\xi_1$ or

$$g(\xi)=\frac{2(-1)^\gamma}{p(x_2')-p(x_1')}\left(\frac{p(x_1')+p(x_2')}{2}-p(1)\right)$$

for $\xi=\xi_2$, where $\xi_1$ and $\xi_2$ are

$$\xi_1=\frac{\eta_{\gamma+1}-\eta_\gamma+x_1'\eta_{\gamma+1}-x_2'\eta_\gamma}{x_1'-x_2'},$$

$$\xi_2=\frac{\eta_\gamma-\eta_{\gamma+1}+x_1'\eta_{\gamma+1}-x_2'\eta_\gamma}{x_1'-x_2'}.$$

Next, we will prove that if $|g(\xi)|>1$, then $|p(1)|>1$ or $|p(-1)|>1$, which is a contradiction with $|p(1)|\leqslant 1$ or $|p(-1)|\leqslant 1$. Without loss of generality, we assume that $\gamma$ is odd. When $|g(\xi)|>1$ with $\xi=\xi_1$, we have $p(-1)>p(x_1')\geqslant 1$ or $p(-1)<p(x_2')\leqslant -1$, i.e., $|p(-1)|>1$. When $|g(\xi)|>1$ with $\xi=\xi_2$, we have $p(1)>p(x_1')\geqslant 1$ or $p(1)<p(x_2')\leqslant -1$, i.e., $|p(1)|>1$.

In the rest of this proof, we will show that if $\deg(p)\leqslant m+1$, then $|g(\xi)|>1$.

Let $T_m(x)$ denote the $m$-th Chebyshev polynomial of the first kind. Because $\deg(g)=\deg(p)\leqslant m+1$, let $h(x):=g(x)-T_m(x)=\sum_{i=0}^{m+1}a_i^*x^i$, where $a_i^*\in\mathbb{R}$ for all $i\in\{0,\dots,m+1\}$. According to Property 2, we have

$$\begin{cases} h(\eta_\gamma)=0, \\ h(\eta_{\gamma+1})=0, \\ h'(\eta_\gamma)=0, \\ h'(\eta_{\gamma+1})=0, \\ (-1)^k h\left(\cos\left(\frac{k\pi}{m}\right)\right)\leqslant\varepsilon, 0\leqslant k\leqslant m. \end{cases} \tag{E1}$$

Let $\mathbf{a}=[a_0,\dots,a_{m+1}]^{\mathrm{T}}\in\mathbb{R}^{m+2}$. For any $i\in\{0,\dots,m+1\}$, let $\mathbf{e_i}=[e_{i0},\dots,e_{i,m+1}]^{\mathrm{T}}\in\mathbb{R}^{m+2}$ where $e_{ii}=1$ if $a_i^*\geqslant 0$, $e_{ii}=-1$ if $a_i^*<0$ and $e_{ij}=0$ for all $i\neq j$. Let $\boldsymbol{\varepsilon}=[\varepsilon_0,\dots,\varepsilon_{m+8}]^{\mathrm{T}}$ in which $\varepsilon_i=\varepsilon$ for $0\leqslant i\leqslant m$ and $\varepsilon_j=0$ for $m+1\leqslant j\leqslant m+8$. Let $\mathbf{C}\in\mathbb{R}^{(m+9)\times(m+2)}$ where the row index set and column index set are $\{0,\dots,m+8\}$ and $\{0,\dots,m+1\}$ respectively. The matrix $\mathbf{C}$ can be defined as follows:

$$\mathbf{C}=\begin{cases} \mathbf{C}_{ij}=(-1)^i\cos^j(\frac{i\pi}{m}), & \text{if } 0\leqslant i\leqslant m, 0\leqslant j\leqslant m+1; \\ \mathbf{C}_{m+1+k,j}=(-1)^{\gamma+k}\cos^j\left(\frac{(\gamma+k)\pi}{m}\right), & \text{if } 0\leqslant j\leqslant m+1, k\in\{0,1\}; \\ \mathbf{C}_{m+3,0}=\mathbf{C}_{m+4,0}=0, & \\ \mathbf{C}_{m+3+k,j}=j\cos^{j-1}\left(\frac{(\gamma+k)\pi}{m}\right), & \text{if } 1\leqslant j\leqslant m+1, k\in\{0,1\}; \\ \mathbf{C}_{m+k+4,j}=-\mathbf{C}_{m+k,j}, & \text{if } 1\leqslant k\leqslant 4, 0\leqslant j\leqslant m+1. \end{cases}$$

Define a linear programming:

$$\begin{aligned} \max\quad & \mathbf{e_i}^{\mathrm{T}}\mathbf{a}; \\ s.t.\quad & \mathbf{C}\mathbf{a}\leqslant\boldsymbol{\varepsilon}; \end{aligned}$$

where $|a_i|=\mathbf{e_i}^{\mathrm{T}}\mathbf{a}$ for any $0\leqslant i\leqslant m+1$. Since $\mathbf{a}^*=[a_0^*,\dots,a_{m+1}^*]^{\mathrm{T}}$ satisfies linear constraints (E1), $\mathbf{a}^*$ is a feasible solution of linear programming. Let $\mathbf{b}=[b_0,\dots,b_{m+1}]^{\mathrm{T}}$. Then, the corresponding asymmetric dual problem is

$$\begin{aligned} \min\quad & \boldsymbol{\varepsilon}^{\mathrm{T}}\mathbf{b}; \\ s.t.\quad & \mathbf{C}^{\mathrm{T}}\mathbf{b}=\mathbf{e_i}; \\ & \mathbf{b}\geqslant 0. \end{aligned}$$

If $\varepsilon=0$, then $h(x)$ has at least $m+2$ roots based on linear constraints (E1). Since $\deg(h)\leqslant m+1$, $h(x)\equiv 0$. Namely, $[0,\dots,0]^{\mathrm{T}}\in\mathbb{R}^{m+2}$ is a feasible solution of primal problem. Hence, there exists a feasible solution $\mathbf{b}^*$ of dual problem where $\mathbf{C}^{\mathrm{T}}\mathbf{b}^*=\mathbf{e_i}$ and $\mathbf{b}^*$ is independent with $\boldsymbol{\varepsilon}$. Recall that $\mathbf{a}^*$ and $\mathbf{b}^*$ are feasible solutions of primal and dual problem, respectively. If $\varepsilon>0$, then $|a_i^*|=\mathbf{e_i}^{\mathrm{T}}\mathbf{a}^*\leqslant\boldsymbol{\varepsilon}^{\mathrm{T}}\mathbf{b}^*$ according to weak duality theorem [32]. Therefore, $|a_i^*|\leqslant\boldsymbol{\varepsilon}^{\mathrm{T}}\mathbf{b}^*\leqslant\varepsilon\|\mathbf{b}^*\|_1$ for any $0\leqslant i\leqslant m+1$. Then $|h(\xi)|=|\sum_{i=0}^{m+1}a_i^*\xi^i|\leqslant\sum_{i=0}^{m+1}|a_i^*||\xi|^i\leqslant\varepsilon\|\mathbf{b}^*\|_1\sum_{i=0}^{m+1}|\xi|^i$. If $|\xi|>1$, $|T_n(\xi)|>1$ due to Property 2. Let $\varepsilon=\frac{|T_m(\xi)|-1}{2\|\mathbf{b}^*\|_1\sum_{i=0}^{m+1}|\xi|^i}>0$, then $|g(\xi)|=|h(\xi)+T_m(\xi)|\geqslant|T_m(\xi)|-|h(\xi)|>(|T_m(\xi)|+1)/2>1$.

**Lemma 3.** For every polynomial $p:\mathbb{R}\to\mathbb{R}$ satisfying $-1\leqslant p(x)\leqslant 1$ for all $x\in\{1-\frac{2k}{n}|k\in[n]_0\}$. If there exists an $x_0$ satisfying either of the follows conditions:

1. $x_0\in(\cos(\frac{\pi}{m}),1)$ such that $p(x_0)=-1$ and $p(1)=1$;

2. $x_0 \in (-1, -\cos(\frac{\pi}{m}))$ such that $p(x_0) = 1$ and $p(-1) = -1$;

then $\deg(p) \geqslant m+1$ when $n$ is sufficiently large.

*Proof.* The proof sketch is the same with Lemma 2. Let $d$ denote the degree of $p(x)$. Similar with the proof of Lemma 2, when $n$ is sufficiently large, we have

$$\max_{|x|\leqslant 1} |p(x)| \leqslant 1+\varepsilon, \forall \varepsilon > 0.$$

Without loss of generality, we only discuss case (1). Recall that $p(x_0) = -1$ for $x_0 \in (\cos(\frac{\pi}{m}), 1)$ and $p(1) = 1$. If $p'(x_0) \leqslant 0$, there exists $x_0' \in \left[x_0, \frac{n-2\lfloor(1-x_0)n/2\rfloor}{n}\right]$ satisfying $p'(x_0') = 0$ and $p(x_0') \leqslant -1$; If $p'(x_0) \geqslant 0$, there exists $x_0' \in \left[\frac{n-2\lceil(1-x_0)n/2\rceil}{n}, x_0\right]$ satisfying $p'(x_0') = 0$ and $p(x_0') \leqslant -1$. Namely, there exists $x_0' \in (x_0 - \frac{2}{n}, x_0 + \frac{2}{n})$ satisfying $p'(x_0') = 0$ and $p(x_0') \leqslant -1$. If $n$ is sufficiently large, there exists $x_0' \in (\cos(\frac{\pi}{m}), 1)$ satisfying $p(x_0') \leqslant -1$, $p'(x_0') = 0$ since $x_0 \in (\cos(\frac{\pi}{m}), 1)$. Define a polynomial $g(x)$ by $p(x)$:

$$g(x) = \frac{2}{1-p(x_0')}\left(\frac{1+p(x_0')}{2} - p\left(\frac{(x_0'-1)x + \cos(\frac{\pi}{m}) - x_0'}{\cos(\frac{\pi}{m}) - 1}\right)\right).$$

In fact, $\deg(p) = \deg(g)$. Moreover, $g(1) = 1$, $g(\cos(\frac{\pi}{m})) = -1$, $g'(\cos(\frac{\pi}{m})) = 0$ and $-1-\varepsilon \leqslant g(x) \leqslant 1+\varepsilon$ for all $x \in [-1,1]$ and $\varepsilon > 0$. If $x_0' \in (\cos(\frac{\pi}{m}), 1)$, there exists $\xi = \frac{2\cos(\frac{\pi}{m}) - x_0' - 1}{1-x_0'} < -1$ such that $g(\xi) = \frac{2}{1-p(x_0')}\left(\frac{p(x_0')+1}{2} - p(-1)\right)$. If $|g(\xi)| > 1$, then $p(-1) \leqslant p(x_0') < -1$ or $p(-1) > 1$. In the rest of this proof, we will show that if $p(x)$ is a polynomial of degree at most $m$, then $|g(\xi)| > 1$. Namely, $|p(-1)| > 1$ holds when $\deg(p) \leqslant m$, which is a contradiction with $|p(-1)| \leqslant 1$. Therefore, $\deg(p) \geqslant m+1$.

Let $h(x) = g(x) - T_m(x) = \sum_{i=0}^m a_i^* x^i$, where $T_m(x)$ is the $m$-th Chebyshev polynomial of the first kind. Based on Lemma 2, we have

$$\begin{cases} h(1) = 0, \\ h\left(\cos\left(\frac{\pi}{m}\right)\right) = 0, \\ h'\left(\cos\left(\frac{\pi}{m}\right)\right) = 0, \\ (-1)^k h\left(\cos\left(\frac{k\pi}{m}\right)\right) \leqslant \varepsilon, 0 \leqslant k \leqslant m. \end{cases} \tag{E2}$$

Let $\mathbf{a} = [a_0, \ldots, a_m]^{\mathrm{T}} \in \mathbb{R}^{m+1}$. For any $i \in [m]_0$, let $\mathbf{e_i} = [e_{i0}, \ldots, e_{i,m}]^{\mathrm{T}} \in \mathbb{R}^{m+1}$ where $e_{ii} = 1$ if $a_i^* \geqslant 0$, $e_{ii} = -1$ if $a_i^* < 0$ and $e_{ij} = 0$ for all $i \neq j$. Let $\boldsymbol{\varepsilon} = [\varepsilon_0, \ldots, \varepsilon_{m+6}]^{\mathrm{T}}$ in which $\varepsilon_i = \varepsilon$ for $0 \leqslant i \leqslant m$ and $\varepsilon_j = 0$ for $m+1 \leqslant j \leqslant m+6$. Let $\mathbf{C} \in \mathbb{R}^{(m+7)\times(m+1)}$ where the row index set and column index set are $\{0, \ldots, m+6\}$ and $\{0, \ldots, m\}$ respectively. The matrix $\mathbf{C}$ can be defined as follows:

$$\mathbf{C} = \begin{cases} \mathbf{C}_{ij} = (-1)^i \cos^j\left(\frac{i\pi}{m}\right), & \text{if } 0 \leqslant i \leqslant m, 0 \leqslant j \leqslant m; \\ \mathbf{C}_{m+1+k,j} = (-1)^k \cos^j\left(\frac{k\pi}{m}\right), & \text{if } 0 \leqslant j \leqslant m, k \in \{0,1\}; \\ \mathbf{C}_{m+3,0} = 0, & \\ \mathbf{C}_{m+3,j} = j\cos^{j-1}\left(\frac{\pi}{m}\right), & \text{if } 1 \leqslant j \leqslant m; \\ \mathbf{C}_{m+k+3,j} = -\mathbf{C}_{m+k,j}, & \text{if } 1 \leqslant k \leqslant 3, 0 \leqslant j \leqslant m. \end{cases}$$

Define a linear programming:

$$\begin{aligned} \max \quad & \mathbf{e_i}^{\mathrm{T}}\mathbf{a}; \\ s.t. \quad & \mathbf{C}\mathbf{a} \leqslant \boldsymbol{\varepsilon}; \end{aligned}$$

where $|a_i| = \mathbf{e_i}^{\mathrm{T}}\mathbf{a}$ for any $0 \leqslant i \leqslant m+1$. Since $\mathbf{a}^* = [a_0^*, \ldots, a_m^*]^{\mathrm{T}}$ satisfies linear constraints (E2), $\mathbf{a}^*$ is a feasible solution of linear programming. Let $\mathbf{b} = [b_0, \ldots, b_m]^{\mathrm{T}}$. Then, the corresponding asymmetric dual problem is

$$\begin{aligned} \min \quad & \boldsymbol{\varepsilon}^{\mathrm{T}}\mathbf{b}; \\ s.t. \quad & \mathbf{C}^{\mathrm{T}}\mathbf{b} = \mathbf{e_i}; \\ & \mathbf{b} \geqslant 0. \end{aligned}$$

Similar discussion with Lemma 2, there exists a feasible solution $\mathbf{b}^*$ of dual problem which is independent with $\boldsymbol{\varepsilon}$. According to weak duality theorem, $|a_i^*| \leqslant \boldsymbol{\varepsilon}^{\mathrm{T}}\mathbf{b}^* \leqslant \varepsilon\|\mathbf{b}^*\|_1$ for any $0 \leqslant i \leqslant m$. Therefore, $|h(\xi)| = |\sum_{i=0}^m a_i\xi^i| \leqslant \sum_{i=0}^m |a_i||\xi|^i \leqslant \varepsilon\|\mathbf{b}^*\|_1 \sum_{i=0}^m |\xi|^i$. Because $|T_m(\xi)| > 1$ for $\xi < -1$ duo to Property 2, let $\varepsilon = \frac{|T_m(\xi)|-1}{2\|\mathbf{b}^*\|_1 \sum_{i=0}^m |\xi|^i} > 0$, then $|g(\xi)| = |h(\xi) + T_m(\xi)| \geqslant |T_m(\xi)| - |h(\xi)| > (|T_m(\xi)| + 1)/2 > 1$.

The proof of Theorem 2 combines Lemma 2, Lemma 3, together with Lemma 1.

*Proof.* [Proof of Theorem 2] Let polynomial $p : \mathbb{R} \to \mathbb{R}$ denote the minimum degree univariate polynomial representation of $f_n^{k,l}$. Then $p$ satisfies $p(k) = 0$, $p(l) = 1$ and $0 \leqslant p(i) \leqslant 1$ for all $i \in [n]$. For every $d \in \mathbb{N}$ and $(\kappa, \lambda) \in \mathsf{LR}(S_d)$, there exists $(s,t) \in S_d$ satisfying $(\kappa, \lambda) \in \mathsf{LR}(s,t)$. Suppose $s = \frac{1}{2}\left(1 - \cos\left(\frac{\gamma\pi}{2d-\delta}\right)\right)$ and $t = \frac{1}{2}\left(1 - \cos\left(\frac{(\gamma+1)\pi}{2d-\delta}\right)\right)$ where $\gamma \in [2d-1]_0$ if $\delta = 0$ and $\gamma \in [2d-3]$ if $\delta = 1$. Let $q(x) = (-1)^{\gamma+1}(1 - 2p((1-x)n/2))$, where $\deg(p) = \deg(q)$. It follows that $q(1-2k/n) = (-1)^{\gamma+1}$, $q(1-2l/n) = (-1)^{\gamma}$ and $-1 \leqslant q(1-2i/n) \leqslant 1$ for all $i \in [n]_0$. If $\delta \in \{0,1\}$ and $\gamma \in [2d-\delta-1]$, we have $Q_E(f_n^{k,l}) \geqslant d+1$ following Lemma 2 and Lemma 1; otherwise if $\delta = 0$ and $\gamma \in \{0, 2d-1\}$, we have $Q_E(f_n^{k,l}) \geqslant d+1$ following Lemma 3 and Lemma 1.

**Remark 1.** It may be observed in the proof of Theorem 2 that for $0 \leqslant k < \frac{n}{2}$, the minimum-degree polynomial computing $f_n^{k,\frac{n}{2}}$ also computes a symmetric partial Boolean function $g_n^k$ defined as follows:

$$g_n^k(x) = \begin{cases} 0, & |x| \in \{k, n-k\}; \\ 1, & |x| = \frac{n}{2}; \\ undefined, & \text{otherwise.} \end{cases}$$

Furthermore, we note that for $k = 0$, $g_n^0(x)$ is exactly the Deutsch-Jozsa function [1] and hence $Q_E(g_n^0) = 1$; whereas for $d > 1$ and $\frac{1}{2}\left(1 - \cos\left(\frac{(d-2)\pi}{2(d-1)}\right)\right) < \frac{k}{n} \leqslant \frac{1}{2}\left(1 - \cos\left(\frac{(d-1)\pi}{2d}\right)\right)$, $Q_E(g_n^k) = d$ if $n$ is sufficiently large. The proof is the same as Theorem 1 and Theorem 2.

**Remark 2.** There are two probable reasons why our upper and lower bounds are not perfectly matched: i) Theorem 2 only makes use of the degree of Chebyshev polynomials (indeed stretched Chebyshev polynomials after padding), whereas the best known lower bound Lemma 1 is not restricted to Chebyshev polynomials; ii) the lower bound by Lemma 1 may not be tight, given the recent result that degree-4 polynomials are not equivalent to 2-query quantum algorithms in the bounded-error model [33]. In what follows we elaborate on the reasons with three sets of $(\frac{k}{n}, \frac{l}{n})$ estimating the boundary of $Q_E(f_n^{k,l}) = d$ derived from Theorem 1, 2 and Lemma 1 respectively (for simplicity we assume both $k$ and $l$ are integers):

$$\begin{cases} \mathcal{A}_d := \mathsf{UL}(S_d); \\ \mathcal{B}_d := \mathsf{LR}(S_d); \\ \mathcal{C}_d := \left\{(\kappa,\lambda) \in I^2 \mid \exists \text{ polynomial } p:[0,1]\to[0,1], \text{ s.t. } \deg(f) \leqslant 2d, \right. \\ \qquad \left. f(\kappa) = 0, f(\lambda) = 1\right\}. \end{cases}$$

Specifically, $Q_E(f_n^{k,l}) \leqslant d$ for every $(\frac{k}{n}, \frac{l}{n}) \in \mathcal{A}_d$ by 1, while $Q_E(f_n^{k,l}) > d$ for $(\frac{k}{n}, \frac{l}{n}) \in \mathcal{B}_d$ by 2 and $Q_E(f_n^{k,l}) > d$ if $(\frac{k}{n}, \frac{l}{n}) \in \overline{\mathcal{C}_d}$ by Lemma 1 ($\overline{\mathcal{B}_d}$ and $\overline{\mathcal{C}_d}$ are the complementaries of $\mathcal{B}_d$ and $\mathcal{C}_d$). In fact there is $\mathcal{A}_d \subseteq \mathcal{C}_d \subsetneq \overline{\mathcal{B}_d}$ for $d > 1$ and furthermore it is likely $\mathcal{A}_d \subsetneq \mathcal{C}_d$. As a result $\mathcal{A}_d \bigcup \mathcal{B}_d$ does not cover all the choices of $(\kappa, \lambda)$, and hence we cannot determine from Theorem 1, 2 whether $Q_E(f_n^{k,l}) \leqslant d$ or $Q_E(f_n^{k,l}) > d$ as long as $(\frac{k}{n}, \frac{l}{n}) \in \overline{\mathcal{A}_d \bigcup \mathcal{B}_d}$, even if it is the case $(\frac{k}{n}, \frac{l}{n}) \in \overline{\mathcal{C}_d} \bigcap \overline{\mathcal{B}_d} = \overline{\mathcal{C}_d} \bigcap (\overline{\mathcal{A}_d \bigcup \mathcal{B}_d})$ when $Q_E(f_n^{k,l}) > d$ by Lemma 1.

Anyhow, upper and lower bounds for exact quantum query complexity of $f_n^{k,l}$ can still be derived from Theorem 1, 2 but with a larger gap, and fortunately the gap is no more than one in most cases as verified numerically, *i.e.* $\bigcup_{d\in\mathbb{N}} \left(\overline{\mathsf{A}_{d+1} \bigcup \mathcal{B}_d}\right)$ is small.

## References


1 David Deutsch and Richard Jozsa. Rapid solution of problems by quantum computation. *Proceedings of The Royal Society A: Mathematical, Physical and Engineering Sciences*, 439(1907):553–558, 1992.
2 Michael A Nielsen and Isaac Chuang. Quantum computation and quantum information, 2002.
3 Marvin L Minsky and S Papert. Perceptrons, expanded ed. *MIT Press, Cambridge, MA*, 15:767776, 1988.
4 Robert Beals, Harry Buhrman, Richard Cleve, Michele Mosca, and Ronald de Wolf. Quantum lower bounds by polynomials. *Journal of the ACM (JACM)*, 48(4):778–797, 2001. Earlier version in FOCS'1998. Also arXiv:quant-ph/9802049.
5 Daowen Qiu and Shenggen Zheng. Characterizations of symmetrically partial boolean functions with exact quantum query complexity. *arXiv preprint arXiv:1603.06505*, 2016.
6 Eric Filiol and Caroline Fontaine. Highly nonlinear balanced boolean functions with a good correlation-immunity. *theory and application of cryptographic techniques*, pages 475–488, 1998.
7 Florence Jessie MacWilliams and Neil James Alexander Sloane. *The theory of error-correcting codes*. Elsevier, 1977.
8 Krishnendu Chakrabarty and John P Hayes. Test response compaction using multiplexed parity trees. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 15(11):1399–1408, 1996.
9 Krishnendu Chakrabarty and John P Hayes. Cumulative balance testing of logic circuits. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 3(1):72–83, 1995.
10 Lov K Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing*, pages 212–219. ACM, 1996. Also arXiv:quant-ph/9605043.
11 Gilles Brassard, Peter Hoyer, Michele Mosca, and Alain Tapp. Quantum amplitude amplification and estimation. *Contemporary Mathematics*, 305:53–74, 2002. Also arXiv:quant-ph/0005055.
12 Peter Høyer. Arbitrary phases in quantum amplitude amplification. *Physical Review A*, 62(5):052304, 2000. Also arXiv:quant-ph/0006031.
13 Gui-Lu Long. Grover algorithm with zero theoretical failure rate. *Physical Review A*, 64(2):022307, 2001. Also arXiv:quant-ph/0106071.
14 Xiaoyu He, Jialin Zhang, and Xiaoming Sun. Quantum search with prior knowledge. *arXiv preprint arXiv:2009.08721*, 2020.
15 Ashley Montanaro, Richard Jozsa, and Graeme Mitchison. On exact quantum query complexity. *Algorithmica*, 71(4):775–796, 2015. Also arXiv:1111.0475.
16 Daowen Qiu and Shenggen Zheng. Generalized deutsch-jozsa problem and the optimal quantum algorithm. *Physical Review A*, 97(062331), 2018.
17 Byung-Soo Choi and Samuel L Braunstein. Quantum algorithm for the asymmetric weight decision problem and its generalization to multiple weights. *Quantum Information Processing*, 10(2):177–188, 2011.
18 Byung-Soo Choi. Optimality proofs of quantum weight decision algorithms. *Quantum Information Processing*, 11(1):123–136, 2012.
19 Samuel L Braunstein, Byung-Soo Choi, Subhroshekhar Ghosh, and Subhamoy Maitra. Exact quantum algorithm to distinguish boolean functions of different weights. *Journal of Physics A: Mathematical and Theoretical*, 40(29):8441, 2007. Also arXiv:quant-ph/0410043.
20 Andris Ambainis. Quantum lower bounds by quantum arguments. In *Proceedings of the 32nd annual ACM Symposium on Theory of Computing*, pages 636–643. ACM, 2000. Also arXiv:quant-ph/0002066.
21 Jozef Gruska, Daowen Qiu, and Shenggen Zheng. Generalizations of the distributed deutsch–jozsa promise problem. *Mathematical Structures in Computer Science*, 27(3):311–331, 2017. Also arXiv:1402.7254.
22 Scott Aaronson, Robin Kothari, William Kretschmer, and Justin Thaler. Quantum lower bounds for approximate counting via laurent polynomials. In *Proceedings of the 35th Computational Complexity Conference*, pages 1–47, 2020.
23 Andris Ambainis, Jānis Iraids, and Daniel Nagaj. Exact quantum query complexity of Exact $_n^{k,l}$. In *International Conference on Current Trends in Theory and Practice of Informatics*, pages 243–255. Springer, 2017.
24 Gatis Midrijanis. Exact quantum query complexity for total boolean functions. *arXiv preprint arXiv:quant-ph/0403168*, 2004.
25 Andris Ambainis. Superlinear advantage for exact quantum algorithms. *Proceedings of the 45th Annual ACM Symposium on Theory of Computing*, pages 891–900, 2013. Also arXiv:1211.0721.

26 Andris Ambainis, Kaspars Balodis, Aleksandrs Belovs, Troy Lee, Miklos Santha, and Juris Smotrovs. Separations in query complexity based on pointer functions. *Proceedings of the 48th Annual ACM Symposium on Theory of Computing*, pages 800–813, 2016. Also arXiv:1506.04719.

27 Andris Ambainis, Jozef Gruska, and Shenggen Zheng. Exact quantum algorithms have advantage for almost all boolean functions. *Quantum Information & Computation*, 15(5-6):435–452, 2015.

28 Scott Aaronson, Shalev Ben-David, and Robin Kothari. Separations in query complexity using cheat sheets. In *Proceedings of the 48th annual ACM symposium on Theory of Computing*, pages 863–876. ACM, 2016.

29 Scott Aaronson and Andris Ambainis. The need for structure in quantum speedups. *Theory of Computing*, 10(6):133–166, 2014.

30 Richard Askey. Chebyshev polynomials from approximation theory to algebra and number theory, 1991.

31 N.I. Achiezer. *Theory of approximation*. New York: Dover Publications, Inc., 1992.

32 Radu Ioan Bot, Sorin-Mihai Grad, and Gert Wanka. *Duality in vector optimization*. Springer Science & Business Media, 2009.

33 Srinivasan Arunachalam, Jop Briët, and Carlos Palazuelos. Quantum query algorithms are completely bounded forms. *SIAM Journal on Computing*, 48(3):903–925, 2019.