Exact quantum query complexity of weight decision problems via Chebyshev polynomials

Xiaoyu HE1,2, Xiaoming SUN1,2*, Guang YANG1,2 & Pei YUAN1,2

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

Received 1 December 2021/Revised 6 February 2022/Accepted 30 March 2022/Published online 11 January 2023

Citation He X Y, Sun X M, Yang G, et al. Exact quantum query complexity of weight decision problems via Chebyshev polynomials. Sci China Inf Sci, 2023, 66(2): 129503, https://doi.org/10.1007/s11432-021-3468-x

The weight decision problem, which requires determining the Hamming weight of a given binary string, is a natural and important problem with lots of applications, such as cryptanalysis [1] and coding theory. In this study, we investigate the exact quantum query complexity of weight decision problems, where the exact quantum algorithm must always output the correct answer within finite steps (see Appendix A for a detailed explanation). Specifically we consider a partial Boolean function $f^{k,l}_{n}: \{0,1\}^n \rightarrow \{0,1\}$ as follows:

$$f^{k,l}_{n}(x) = \begin{cases} 0, & \text{if } |x| = k, \\ 1, & \text{if } |x| = l, \\ \text{undefined, otherwise}, \end{cases}$$

which distinguishes the Hamming weight of the length-$n$ input between $k$ and $l$. In the definition of $f^{k,l}_{n}$, we put no further restrictions on $n,k$ and $l$, except assuming that they are integers satisfying $0 \leq k < l \leq n$.

In particular, the Deutsch-Jozsa problem [2] and Grover search problem [3] can be interpreted as the special cases of this problem. Many previous studies on weight decision problems generalized the above mentioned problems. For example, Montanaro, Jozsa, and Mitchison [4] considered the discrimination of $|x| = \frac{k}{n}$ from $|x| \in \{0,1, \ldots, n-1\}$. Qin and Zheng [5] proved that the exact quantum query complexity of distinguishing $|x| = \frac{k}{n}$ from $|x| \in \{0, \ldots, k, n-k, \ldots, n\}$ is $k+1$ (see Appendix B for more related work).

Our contributions include upper and lower bounds for a precise number of queries. For most choices of $(k,l)$ and sufficiently large $n$, the gap between the upper and lower bounds is at most one. To obtain the results, we build the connection between the Chebyshev polynomials and our problem. We determine all the boundary cases of $(\frac{k}{n}, \frac{l}{n})$ with matching upper and lower bounds. We generalize the boundary cases via a new quantum padding technique. This quantum padding technique can be of independent interest in designing other quantum algorithms.

To characterize the effect of the quantum padding technique, we introduce the notion of upper-left region and lower-right region for every $(x,y) \in I^2$, where $x < y$ and $I := [0,1]$. The upper-left region $UL(x,y)$ and lower-right region $LR(x,y)$ are as follows:

$$UL(x,y) := \{(\kappa,\lambda) \in I^2 | (1-\kappa)(1-y) \geq (1-\lambda)(1-x), \lambda x \geq \kappa y, \kappa < \lambda \};$$

$$LR(x,y) := \{(\kappa,\lambda) \in I^2 | (1-\kappa)(1-y) \leq (1-\lambda)(1-x), \lambda x \leq \kappa y, \kappa < \lambda, (\kappa,\lambda) \neq (x,y) \}.$$ 

Then we extend the definition of $UL$ and $LR$ to every set $S \subseteq I^2$ as $UL(S) := \bigcup_{(x,y) \in S} UL(x,y)$ and $LR(S) := \bigcup_{(x,y) \in S} LR(x,y)$. Intuitively, for integers $0 \leq k < l \leq n$ and $\kappa = \frac{k}{n}$, $\lambda = \frac{l}{n}$, if $(\kappa,\lambda) \in UL(x,y)$, then any exact quantum algorithm which solves $f^{k,l}_{n}$ for $(\frac{k}{n}, \frac{l}{n}) = (x,y)$ will induce an exact quantum algorithm solving $f^{k,l}_{n}$ after padding some zeros and ones to the input of $f^{k,l}_{n}$. Therefore, $Q_{UL}(f^{k,l}_{n}) \leq Q_{UL}(f^{k,l}_{n})$. Similar reduction holds for $(\kappa,\lambda) \in LR(x,y)$, when $(x,y) \in UL(\kappa,\lambda)$.

Now, we introduce the definition of $S_d$ composed of the boundary cases, which we can solve with $d$-query exact quantum algorithms. Indeed, every element in $S_d$ corresponds to a pair of the consecutive extrema of degree-$D$ Chebyshev polynomial, where $D = 2d$ or $D = 2d - 1$. For every $d \in \mathbb{N}$, we define $S_d$ as below:

$$S_d := \left\{ \left( 1 - \frac{\cos \frac{\pi}{2d} \gamma}{2}, \frac{\cos \frac{\gamma}{2}}{2} \right), \left( 1 - \frac{\cos \frac{\gamma (2d-1)}{2}}{2}, \frac{\cos \frac{\gamma}{2}}{2} \right) \right\}, \gamma \in \{0, \ldots, 2d - 1\} \cup \left\{ \left( 1 - \frac{\cos \frac{\gamma}{2d}}{2}, \frac{\cos \frac{\gamma (2d-3)}{2}}{2} \right), \left( 1 - \frac{\cos \frac{\gamma (2d-1)}{2}}{2}, \frac{\cos \frac{\gamma}{2}}{2} \right) \right\}, \gamma \in \{1, \ldots, 2d - 3\}.$$ 

A major contribution of this study is the construction of a family of exact quantum algorithms that immediately implies the following theorem.

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

The upper bound of $Q_{UL}(f^{k,l}_{n})$ is determined by elements of $S_d$ that $f^{k,l}_{n}$ can be reduced to via an enhanced “quantum
padding" technique, since every case in $S_d$ can be solved exactly with $d$ quantum queries (see Appendix C for details). We expect to translate general $(1 - 2a, 1 - 2\lambda)$ to the extremum of a Chebyshev polynomial $(1 - 2x, 1 - 2t)$. Let $a, b > 0$ and $a^2 = \frac{1 - \lambda}{2 - \lambda} - \frac{1 - \lambda t}{2 - \lambda t}$. The initial state is $|\Psi_0\rangle = \cos\theta|\alpha\rangle + \sin\theta|\beta\rangle$, where $|\alpha\rangle := \frac{1}{\sqrt{n - |a|^2}} \sum_{i = 0}^{n - 1} |i\rangle + a|L\rangle$, $|\beta\rangle := \frac{1}{\sqrt{n + |b|^2}} \sum_{i = 0}^{n + 1} |i\rangle - b|R\rangle$, and $\sin^2 \theta = \frac{|a|^2 + b^2}{n + a^2 + b^2}$. Intuitively, we introduce $a|\lambda\rangle$ and $b|R\rangle$ to represent the unnormalized superpositions of newly padded $a^2$ zeros and $b^2$ ones, respectively, which can translate $k$ and $l$ into $n(n + a^2 + b^2)$ and $(n + a^2 + b^2)$, or if they are not integers. It is obvious that $a^2, b^2 \geq 0$ if $(\alpha, \lambda) \in \mathbb{UL}(S_d)$.

Our algorithm will utilize two unitary transformations $W(a, b)$ and $U(a, b)$, with parameters $a, b > 0$.

1. $(a, b)$ is a unitary transformation over a Hilbert space of dimension $n + 2$ with basis vectors $\{|k\rangle | k \in \{n\}\}$ and $\{|\lambda\rangle, |\beta\rangle\}$. It is a unitary transform described as follows:

$$
W(a, b) = \frac{1}{\sqrt{n + a^2 + b^2}} \left( \sum_{i = 0}^{n - 1} |i\rangle + a|L\rangle - b|R\rangle - |k\rangle \right),
$$

$$
W(a, b)|\lambda\rangle = \frac{1}{\sqrt{n + a^2 + b^2}} \left( \sum_{i = 0}^{n - 1} |i\rangle + a|L\rangle - b|R\rangle - |\lambda\rangle \right),
$$

$$
W(a, b)|R\rangle = \frac{1}{\sqrt{n + a^2 + b^2}} \left( \sum_{i = 0}^{n - 1} |i\rangle + a|L\rangle - b|R\rangle - |\beta\rangle \right).
$$

2. $(a, b)$ is a unitary transformation over a Hilbert space of dimension $n + 2$ with basis vectors $\{|k\rangle, |\lambda\rangle, |\beta\rangle, |i, j\rangle, |L\rangle, |R\rangle, |k, i\rangle, |k, j\rangle, |i, j\rangle, |n, i, j\rangle\}$. It is a unitary completion of the above form:

$$
U(a, b) = \frac{1}{\sqrt{n + a^2 + b^2}} \left( \sum_{i = 0}^{n - 1} |i\rangle + a|L\rangle + b|R\rangle \right)
$$

$$
+ \frac{1}{\sqrt{n + a^2 + b^2}} \left( \sum_{i = 0}^{n - 1} |i\rangle + a|L\rangle - b|R\rangle \right), \quad k \in [n],
$$

$$
U(a, b)|\lambda\rangle = \frac{1}{\sqrt{n + a^2 + b^2}} \left( \sum_{i = 0}^{n - 1} |i\rangle + a|L\rangle - b|R\rangle \right),
$$

$$
U(a, b)|R\rangle = \frac{1}{\sqrt{n + a^2 + b^2}} \left( \sum_{i = 0}^{n - 1} |i\rangle + a|L\rangle + b|R\rangle \right)
$$

$$
+ \frac{1}{\sqrt{n + a^2 + b^2}} \left( \sum_{i = 0}^{n - 1} |i\rangle + a|L\rangle + b|R\rangle \right), \quad k \in [n],
$$

Let $G(a, b) := W(a, b)O_x$ and $R(a, b) := U(a, b)O_x$. In particular, $G(a, b)$ degenerates into the standard Grover operator when $a = b = 0$. After $d - 1$ applications of $G(a, b)$, the initial state $|\Psi_0\rangle$ transforms into $|\Psi_{d-1}\rangle := G(a, b)^{d-1}|\Psi_0\rangle$.

Without loss of generality, we assume $\gamma$ is odd.

(1) $s = \frac{1}{4}(1 - \cos\frac{n(\gamma + 1)}{2d})$ and $t = \frac{1}{4}(1 - \cos\frac{n(\gamma - 1)}{2d})$. Now measure the final state $|\Psi_{d-1}\rangle$ and get a measurement result $m$. If $m = |\lambda\rangle$, return $|x\rangle = l$ if $m = |R\rangle$, return $|x\rangle = k$; otherwise, $m \in [n]$ and we need a query to $x_m$. Similarly, if $x_m = 0$, return $|x\rangle = l$; otherwise, $|x\rangle = k$.

(2) $s = \frac{1}{4}(1 - \cos\frac{n}{2d})$ and $t = \frac{1}{4}(1 - \cos\frac{n}{2d})$. Applying $R(a, b)$ to $|\Psi_{d-1}\rangle$ gives us

$$
|\Psi_d\rangle := R(a, b)|\Psi_{d-1}\rangle = \cos(2k\theta)|\beta\rangle + \sin(2k\theta)|\beta\rangle,
$$

where

$$
|\beta\rangle := \frac{1}{\sqrt{n + a^2 + b^2}} \left( \sum_{i = 0}^{n - 1} |i\rangle + a|L\rangle + b|R\rangle \right),
$$

$$
|\beta\rangle := \frac{1}{\sqrt{n + a^2 + b^2}} \left( \sum_{i = 0}^{n - 1} |i\rangle + a|L\rangle + b|R\rangle \right).
$$

Finally, we measure the final state $|\Psi_d\rangle$ and get a measurement result. If $m \in \{k, L, R|k \in [n]\}$, $|x\rangle = l$; else, $|x\rangle = k$.

Unlike the classical problem, where the number of padded zeros and ones must be nonnegative integers, our quantum padding technique can effectively pad an arbitrary (even real numbers such as $2/3$ or $\sqrt{2}$) non-negative number of zeros and ones to the input $0/1$ string to reduce the general problem in some special cases. Therefore, $Q_E(j, k)$ has an upper bound fully and smoothly determined by $\frac{n}{2}$ and $\frac{k}{2}$.

For the lower-bound part, we discover the relation between the weight decision function $j, k$ and extremum of the Chebyshev polynomials and prove the exact quantum query lower bound for elements in $S_d$ via a degree analysis. Finally, we apply the same padding technique as before (but in the other direction) for generalization. We have the following theorem.

**Theorem 2** (Lower bounds). For every $d \in N$ and $0 \leq k \leq l \leq n$ with $k, l, n \in N$, let $\kappa = \frac{n}{2}$ and $\lambda = \frac{l}{2}$. If $(\alpha, \lambda) \in \mathbb{LR}(S_d)$, then $Q_E(j, k) \geq d + 1$ for a sufficiently large $n$ (see Appendix E for the proof).

The lower bound of $Q_E(j, k)$ is fully determined by $\kappa = \frac{n}{2}$ and $\lambda = \frac{l}{2}$ when $n$ is sufficiently large.

Combining Theorems 1 and 2, we derive the upper and lower bounds for $Q_E(j, k)$ by determining the corresponding $S_d$ and $S_d^\prime$, such that $d_1 + 1 \leq Q_E(j, k) \leq d_2$. Using a numerical calculation, we find that our upper and lower bounds are nearly optimal — the bounds exactly match for $> 56\%$ area of $[0, 1]^2$, and the gap is no more than one for $> 97\%$ area.

**Acknowledgements**

This work was supported in part by National Natural Science Foundation of China (Grant Nos. 61832003, 61872334, 61801459) and Strategic Priority Research Program of Chinese Academy of Sciences (Grant No. XDB26000000).

**Supporting information**

Appendix E. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

**References**

1. Filion E, Fontaine C. Highly nonlinear balanced boolean functions with a good correlation-immunity. In: Proceedings of International Conference on the Theory and Application of Cryptographic Techniques, Epano, 1998. 475–488
2. Deutsch D, Jozsa R. Rapid solution of problems by quantum computation. In: Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences, London, 1996. 553–558
3. Grover L K. A fast quantum mechanical algorithm for database search. In: Proceedings of the 28th Annual ACM Symposium on the Theory of Computing, Philadelphia, 1996. 212–219
4. Montanaro A, Jozsa R, Mitchison G. On exact quantum query complexity. Algorithmica, 2015, 71: 775–796
5. Qui D W, Zheng S G. Generalized Deutsch-Jozsa problem and the optimal quantum algorithm. Phys Rev A, 2018, 97: 062331