SCIENCE CHINA
Information Sciences

• LETTER •

February 2023, Vol. 66 129503:1–129503:2
https://doi.org/10.1007/s11432-021-3468-x

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*

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 $f_n^{k,l}:\{0,1\}^n\to\{0,1\}$ as follows:

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

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

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 $|x|=\frac{n}{2}$ from $|x|\in\{0,1,n-1,n\}$. Qiu and Zheng [5] proved that the exact quantum query complexity of distinguishing $|x|=\frac{n}{2}$ 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 $\mathsf{UL}(x,y)$ and lower-right region $\mathsf{LR}(x,y)$ are as follows:

$$\begin{aligned}\mathsf{UL}(x,y):=&\big\{(\kappa,\lambda)\in I^2|(1-\kappa)(1-y)\geqslant(1-\lambda)(1-x),\\ &\lambda x\geqslant\kappa y,\kappa<\lambda\big\};\\ \mathsf{LR}(x,y):=&\big\{(\kappa,\lambda)\in I^2|(1-\kappa)(1-y)\leqslant(1-\lambda)(1-x),\\ &\lambda x\leqslant\kappa y,\kappa<\lambda,(\kappa,\lambda)\neq(x,y)\big\}.\end{aligned}$$

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

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:

$$\begin{aligned}S_d:=&\left\{\left(\frac{1-\cos\frac{\gamma\pi}{2d}}{2},\frac{1-\cos\frac{(\gamma+1)\pi}{2d}}{2}\right)\,\middle|\,\gamma\in\{0,\ldots,2d-1\}\right\},\\ &\bigcup\left\{\left(\frac{1-\cos\frac{\gamma\pi}{2d-1}}{2},\frac{1-\cos\frac{(\gamma+1)\pi}{2d-1}}{2}\right)\,\middle|\,\gamma\in\{1,\ldots,2d-3\}\right\}.\end{aligned}$$

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 $0\leqslant k<l\leqslant n$ 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 of $Q_E(f_n^{k,l})$ is determined by elements of S_d that $f_n^{k,l}$ can be reduced to via an enhanced "quantum

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

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 $(1-2\kappa, 1-2\lambda)$ to the extrema of a Chebyshev polynomial $(1-2s, 1-2t)$. Let $a, b \geqslant 0$ and $a^2 = \frac{l-k}{t-s} - \frac{ls-kt}{t-s} - n$, $b^2 = \frac{ls-kt}{t-s}$. The initial state is $|\Psi_0\rangle = \cos\theta|\alpha_\perp\rangle + \sin\theta|\alpha\rangle$, where $|\alpha_\perp\rangle := \frac{1}{\sqrt{n-|x|+a^2}}(\sum_{i:x_i=0}|i\rangle + a|\mathcal{L}\rangle)$, $|\alpha\rangle := \frac{1}{\sqrt{|x|+b^2}}(\sum_{i:x_i=1}|i\rangle - b|\mathcal{R}\rangle)$, and $\sin^2\theta = \frac{|x|+b^2}{n+a^2+b^2}$. Intuitively, we introduce $a|\mathcal{L}\rangle$ and $b|\mathcal{R}\rangle$ to represent the unnormalized superpositions of newly padded a^2 zeros and b^2 ones, respectively, which can translate k and l into $s(n+a^2+b^2)$ and $t(n+a^2+b^2)$, even if they are not integers. It is obvious that $a^2, b^2 \geqslant 0$ if $(\kappa, \lambda) \in \mathsf{UL}(S_d)$.

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

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

$$\begin{cases} W(a,b)|k\rangle &= \frac{2}{n+a^2+b^2}\left(\sum_{i=1}^n |i\rangle + a|\mathcal{L}\rangle - b|\mathcal{R}\rangle\right) - |k\rangle, \\ W(a,b)|\mathcal{L}\rangle &= \frac{2a}{n+a^2+b^2}\left(\sum_{i=1}^n |i\rangle + a|\mathcal{L}\rangle - b|\mathcal{R}\rangle\right) - |\mathcal{L}\rangle, \\ W(a,b)|\mathcal{R}\rangle &= \frac{-2b}{n+a^2+b^2}\left(\sum_{i=1}^n |i\rangle + a|\mathcal{L}\rangle - b|\mathcal{R}\rangle\right) - |\mathcal{R}\rangle. \end{cases}$$

(2) $U(a,b)$ is a unitary transformation over a Hilbert space of dimension $\binom{n}{2} + 3n + 3$ where the basis vectors are $\{|k\rangle, |\mathcal{L}\rangle, |\mathcal{R}\rangle, |i,j\rangle, |k,\mathcal{L}\rangle, |k,\mathcal{R}\rangle, |\mathcal{L},\mathcal{R}\rangle | k, i, j \in [n], i < j\}$. It is a unitary completion of the following form:

$$\begin{cases} U(a,b)|k\rangle &= \frac{1}{n+a^2+b^2}\left(\sum_{i=1}^n |i\rangle + a|\mathcal{L}\rangle + b|\mathcal{R}\rangle\right) \\ &\quad + \frac{1}{\sqrt{n+a^2+b^2}}\left(-\sum_{i:i<k}|i,k\rangle + \sum_{i:k<i}|k,i\rangle\right) \\ &\quad + \frac{1}{\sqrt{n+a^2+b^2}}\left(a|k,\mathcal{L}\rangle + b|k,\mathcal{R}\rangle\right),\ k \in [n], \\ U(a,b)|\mathcal{L}\rangle &= \frac{a}{n+a^2+b^2}\left(\sum_{i=1}^n |i\rangle + a|\mathcal{L}\rangle + b|\mathcal{R}\rangle\right) \\ &\quad + \frac{1}{\sqrt{n+a^2+b^2}}\left(-\sum_{i=1}^n |i,\mathcal{L}\rangle + b|\mathcal{L},\mathcal{R}\rangle\right), \\ U(a,b)|\mathcal{R}\rangle &= \frac{b}{n+a^2+b^2}\left(\sum_{i=1}^n |i\rangle + a|\mathcal{L}\rangle + b|\mathcal{R}\rangle\right) \\ &\quad + \frac{1}{\sqrt{n+a^2+b^2}}\left(-\sum_{i=1}^n |i,\mathcal{R}\rangle - a|\mathcal{L},\mathcal{R}\rangle\right). \end{cases}$$

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 $|\Psi_{d-1}\rangle := G(a,b)^{d-1}|\Psi_0\rangle$,

$$|\Psi_{d-1}\rangle = \cos((2d-1)\theta)|\alpha_\perp\rangle + \sin((2d-1)\theta)|\alpha\rangle.$$

Without loss of generality, we assume γ is odd.

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

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

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

where

$$\begin{cases} |\beta_\perp\rangle := \frac{1}{\sqrt{n+a^2+b^2}}\left(\sum_{i=1}^n |i\rangle + a|\mathcal{L}\rangle + b|\mathcal{R}\rangle\right), \\ |\beta\rangle := \frac{1}{\sqrt{(n-|x|+a^2)(|x|+b^2)}}\Bigg(\sum_{\substack{i:x_i=0 \\ j:x_j=1}} |i,j\rangle \\ \qquad -a\sum_{i:x_i=1}|i,\mathcal{L}\rangle + b\sum_{j:x_j=0}|i,\mathcal{R}\rangle + ab|\mathcal{L},\mathcal{R}\rangle\Bigg). \end{cases}$$

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

Unlike the classical padding, 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, $Q_E(f_n^{k,l})$ has an upper bound fully and smoothly determined by $\frac{k}{n}$ and $\frac{l}{n}$.

For the lower-bound part, we discover the relation between the weight decision function $f_n^{k,l}$ and extrema 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 $d \in \mathbb{N}$ 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 a sufficiently large n (see Appendix E for the proof).

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

Combining Theorems 1 and 2, we derive the upper and lower bounds for $Q_E(f_n^{k,l})$ by determining the corresponding S_{d_1} and S_{d_2}, such that $d_1 + 1 \leqslant Q_E(f_n^{k,l}) \leqslant d_2$. 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. XDB28000000).

Supporting information Appendixes A–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 Filiol 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, Espoo, 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, 1922. 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 Qiu D W, Zheng S G. Generalized Deutsch-Jozsa problem and the optimal quantum algorithm. Phys Rev A, 2018, 97: 062331