A Note About Claw Function with a Small Range

Andris Ambainis ✉
Center for Quantum Computer Science, Faculty of Computing, University of Latvia, Riga, Latvia

Kaspars Balodis ✉
Center for Quantum Computer Science, Faculty of Computing, University of Latvia, Riga, Latvia

Jānis Iraids ✉
Center for Quantum Computer Science, Faculty of Computing, University of Latvia, Riga, Latvia

Abstract

In the claw detection problem we are given two functions $f : D \to R$ and $g : D \to R$ ($|D| = n$, $|R| = k$), and we have to determine if there is exist $x, y \in D$ such that $f(x) = g(y)$. We show that the quantum query complexity of this problem is between $\Omega\left(n^{1/2}k^{1/6}\right)$ and $O\left(n^{1/2+\varepsilon}k^{1/4}\right)$ when $2 \leq k < n$.

2012 ACM Subject Classification Theory of computation → Quantum query complexity

Keywords and phrases collision, claw, quantum query complexity

Digital Object Identifier 10.4230/LIPIcs.TQC.2021.6

Funding Supported by the project "Quantum algorithms: from complexity theory to experiment" funded under ERDF programme 1.1.1.5.

1 Introduction

In this note we study the Claw problem in which given two discrete functions $f : D \to R$ and $g : D \to R$ ($|D| = n$, $|R| = k$) we have to determine if there is a collision, i.e., inputs $x, y \in D$ such that $f(x) = g(y)$. In contrast to the Element-Distinctness problem, where the input is a single function $f : D \to R$ and we have to determine if f is injective, Claw is non-trivial even when $k < n$. This is the setting we focus on.

Both Claw and Element-Distinctness have wide applications as useful subroutines in more complex algorithms [5, 12] and as a means of lower bounding complexity [10, 1].

Claw and Element-Distinctness were first tackled by Buhrman et al. in 2000 [8] where they gave an $O\left(n^{3/4}\right)$ algorithm and $\Omega\left(n^{1/2}\right)$ lower bound. In 2003 Ambainis, introducing a novel technique of quantum walks, improved the upper bound to $O\left(n^{2/3}\right)$ in the query model [4]. It was soon realized that a similar approach works for Claw [9, 13, 15]. Meanwhile Aaronson and Shi showed a lower bound $\Omega\left(n^{2/3}\right)$ that holds if the range $k = \Omega\left(n^2\right)$ [2]. Eventually Ambainis showed that the $\Omega\left(n^{2/3}\right)$ bound holds even if $k = n$ [3]. The same lower bound has since been reproved using the adversary method [14]. Until now, only the $\Omega\left(n^{1/2}\right)$ bound based on reduction of searching was known for Claw with $k = o(n)$ [8].

We consider quantum query complexity of Claw where the input functions are given as a list of their values in black box. Let $Q(f)$ denote the bounded error quantum query complexity of f. For a short overview of black box model refer to Buhrman and de Wolf's survey [7]. Let $[n]$ denote $\{1, 2, \ldots, n\}$. Let $\textsc{Claw}_{n\to k} : [k]^{2n} \to \{0, 1\}$ be defined as

$$\textsc{Claw}_{n\to k}(x_1, \ldots, x_n, y_1, \ldots, y_n) = \begin{cases} 1, & \text{if } \exists i, j\; x_i = y_j \\ 0, & \text{otherwise} \end{cases}.$$

Our contribution is a quantum algorithm for $\textsc{Claw}_{n\to k}$ with quantum query complexity $Q(\textsc{Claw}_{n\to k}) = O\left(n^{1/2+\varepsilon}k^{1/4}\right)$ and a lower bound $Q(\textsc{Claw}_{n\to k}) = \Omega\left(n^{1/2}k^{1/6}\right)$. In section 2 we describe the algorithm, and in section 3 we give the lower bound.

2 Results

▶ **Theorem 1.** *For all $\varepsilon > 0$, we have $Q(\textsc{Claw}_{n\to k}) = O\big(n^{1/2+\varepsilon}k^{1/4}\big)$.*

Proof. Let $X = (x_1, \dots, x_n)$, $Y = (y_1, \dots, y_n)$ be the inputs of the function. We denote $k = n^{\varkappa}$.

Consider the following algorithm parametrized by $\alpha \in [0, 1]$.

1. **a.** Select a random sample $A = \{a_1, \dots, a_\ell\} \subseteq [n]$ of size $\ell = 4 \cdot n^\alpha \cdot \ln n$ and query the variables $x_{a_1}, \dots, x_{a_\ell}$.
   Denote by $X_A = \{x_a \mid a \in A\}$ the set containing their values. Do a Grover search for an element $y \in Y$ such that $y \in X_A$. If found, output 1.

   b. Select a random sample $A' = \{a'_1, \dots, a'_\ell\} \subseteq Y$ of size ℓ and query the variables $y_{a'_1}, \dots, y_{a'_\ell}$.
   Denote by $Y_{A'} = \{y_{a'} \mid a' \in A'\}$ the set containing their values. Do a Grover search for an element $x \in X$ such that $x \in Y_{A'}$. If found, output 1.
2. Run $\textsc{Claw}_{4b\ln n\to k}$ algorithm (with the value of b specified below) with the following oracle:
   a. To get x_i: do a pseudorandom permutation on $x_1, \dots, x_n$ using seed i and using Grover's minimum search return the first value x_j such that $x_j \notin X_A$.
   b. To get y_i: do a pseudorandom permutation on $y_1, \dots, y_n$ using seed i and using Grover's minimum search return the first value y_j such that $y_j \notin X_{A'}$.

Let $B = \{i \in [n] \mid x_i \notin X_A\}$, $B' = \{i \in [n] \mid y_i \notin Y_{A'}\}$ be the sets containing the indices of the variables which have values not seen in the steps 1a and 1b. We denote $|B| = b = n^\beta$.

Let us calculate the probability that after step 1a there exists an unseen value v which is represented in at least $n^{1-\alpha}$ variables, i.e., $v \notin X_A \wedge |\{i \in [n] \mid x_i = v\}| \geq n^{1-\alpha}$. Consider an arbitrary value $v^* \in [k]$ such that $|\{i \mid x_i = v^*\}| \geq n^{1-\alpha}$. For $i \in [\ell]$, let Z_i be the event that $x_{a_i} = v^*$. $\forall i \in [\ell]$ $\Pr[Z_i] \geq \frac{n^{1-\alpha}}{n}$. Let $Z = \sum_{i\in[\ell]} Z_i$. Then $\mathbb{E}[Z] = \ell \cdot \mathbb{E}[Z_1] \geq 4 \cdot n^\alpha \cdot \ln n \cdot \frac{n^{1-\alpha}}{n} = 4 \ln n$. Using Chernoff inequality (see e.g. [11]),

$$\Pr[Z = 0] \leq \exp\left(-\frac{1}{2}\,\mathbb{E}[Z]\right) \leq \exp(-2\ln n) = \frac{1}{n^2}.$$

The probability that there exists such $v^* \in [k]$ is at most $\frac{n^\varkappa}{n^2} = o(1)$. Therefore, with probability $1 - o(1)$ after step 1a, every value $v \in X_B$ is represented in the input less than $n^{1-\alpha}$ times. The same reasoning can be applied to step 1b and the set B'. Therefore, with probability $1 - o(1)$ both b and b' are at most $k \cdot n^{1-\alpha} = n^{\varkappa+1-\alpha}$.

Similarly, we show that with probability $1 - o(1)$ each $x \in B$ appears as the first element from B in at least one of the permutations of the oracle in step 2. Let W_i^x be the event that $x \in B$ appears in the i-th permutation as the first element from B. $\mathbb{E}[W_i^x] = \frac{1}{b}$. Let $W^x = \sum_{i\in[4b\ln n]} W_i^x$. $\mathbb{E}[W^x] = 4b\ln n \cdot \frac{1}{b} = 4\ln n$. $\Pr[W^x = 0] \leq \exp(-2\ln n) = \frac{1}{n^2}$. $\Pr[\exists x \in B : W^x = 0] \leq \frac{n}{n^2} = \frac{1}{n} = o(1)$. The same argument works for B'. Therefore, if there is a collision, it will be found by the algorithm with probability $1 - o(1)$.

We also show that with probability $1 - o(1)$, in all permutations the first element from B appears no further than in position $4\frac{n}{b}\ln n$ (and similarly for B'). We denote by $P_{i,j}$ the event that in the i-th permutation in the j-th position is an element from B. $\mathbb{E}[P_{i,j}] = \frac{b}{n}$. We denote $P_i = \sum_{j\in[4\cdot\frac{n}{b}\cdot\ln n]} P_{i,j}$. $\mathbb{E}[P_i] = 4 \cdot \ln n$. $\Pr[P_i = 0] \leq \exp(-2\ln n) = \frac{1}{n^2}$. $\Pr[\exists i \in [4b\ln n] : P_i = 0] \leq \frac{4b\ln n}{n^2} \leq \frac{4n\ln n}{n^2} = o(1)$. Therefore, the Grover's minimum search will use at most $\tilde{O}\big(\sqrt{\frac{n}{n^\beta}}\big)$ queries.

The steps 1a and 1b use $\tilde{O}(n^{\alpha})$ queries to obtain the random sample, and $O(\sqrt{n})$ queries to check if there is a colliding element on the other side of the input. The oracle in step 2 uses $\tilde{O}(\sqrt{\frac{n}{n^{\beta}}})$ queries to obtain one value of x_i or y_i.

Therefore the total complexity of the algorithm is

$$\tilde{O}\left(n^{\alpha} + n^{\frac{1}{2}} + Q(\textsc{Claw}_{4b\ln n \to k}) \cdot n^{\frac{1}{2}-\frac{1}{2}\beta}\right).$$

By using the $O(n^{2/3})$ algorithm in step 2,

$$\begin{aligned} Q(\textsc{Claw}_{4b\ln n \to k}) \cdot n^{\frac{1}{2}-\frac{1}{2}\beta} &= n^{\frac{2}{3}\beta+\frac{1}{2}-\frac{1}{2}\beta} \\ &= n^{\frac{1}{2}+\frac{1}{6}\beta} \\ &\leq n^{\frac{1}{2}+\frac{1}{6}(\varkappa+1-\alpha)} \\ &= n^{\frac{4+\varkappa-\alpha}{6}}, \end{aligned}$$

and the total complexity is minimized by setting $\alpha = \frac{4+\varkappa}{7}$. However, we can do better than that. Notice that the $O(n^{2/3})$ algorithm might not be the best choice for solving $\textsc{Claw}_{4b\ln n \to k}$ in step 2.

Let $\mathcal{A}_0$ denote the regular $O(n^{2/3})$ $\textsc{Claw}_{n \to k}$ algorithm. For $i > 0$, let $\mathcal{A}_i$ denote a version of algorithm from Theorem 1 that in step 2 calls $\mathcal{A}_{i-1}$. Then we show that for all n and all $0 \leq \varkappa \leq \frac{2}{3}$,

$$Q(\mathcal{A}_i) = \tilde{O}\left(n^{T_i(\varkappa)}\right),$$

where $T_i(\varkappa) = \frac{(2^i-1)\varkappa+2^{i+1}}{2^{i+2}-1}$.

The proof is by induction on i. For $i = 0$, we trivially have that $Q(\mathcal{A}_0) = \tilde{O}(n^{2/3})$. For the inductive step, consider the analysis of our algorithm. Let us set $\alpha = T_i(\varkappa)$. First, notice that $T_i(\varkappa)$ is non-decreasing in $\varkappa$ and $T_i(\frac{2}{3}) = \frac{2}{3}$ for all i. Thus for all $\varkappa \leq \frac{2}{3}$, we have $T_i(\varkappa) \leq \frac{2}{3}$, hence $\alpha \leq \frac{2}{3}$ and $\frac{\varkappa}{1-\alpha+\varkappa} \leq \frac{2}{3}$. Second, since the coefficient of $\varkappa$ is $\frac{2^i-1}{2^{i+2}-1} \leq 1$ the function $T_i(\varkappa)$ is above $\varkappa$ for $\varkappa \leq \frac{2}{3}$, establishing $\alpha - \varkappa \geq 0$. This confirms that $\alpha = T_i(\varkappa)$ is a valid choice of α.

It remains to show that the complexity of step 2 does not exceed $\tilde{O}(n^{T_i(\varkappa)})$. By the inductive assumption and analysis of the algorithm, the complexity (up to logarithmic factors) of the second step is n to the power of $(1-\alpha+\varkappa) \cdot T_{i-1}\left(\frac{\varkappa}{1-\alpha+\varkappa}\right) + \frac{\alpha-\varkappa}{2}$. Finally, we have to show that

$$(1 - T_i(\varkappa) + \varkappa) \cdot T_{i-1}\left(\frac{\varkappa}{1 - T_i(\varkappa) + \varkappa}\right) + \frac{T_i(\varkappa) - \varkappa}{2} \leq T_i(\varkappa).$$

By expanding $T_{i-1}(\varkappa)$ and with a slight rearrangement, we obtain

$$\frac{(2^{i-1}-1)\varkappa + 2^i(1 - T_i(\varkappa) + \varkappa)}{2^{i+1}-1} \leq \frac{T_i(\varkappa) + \varkappa}{2}.$$

We can further rearrange the required inequality by bringing $T_i(\varkappa)$ to right hand side and everything else to the other. Then we get

$$\frac{(2^{i-1} - 1 + 2^i - \frac{2^{i+1}-1}{2})\varkappa + 2^i}{2^{i+1}-1} \leq T_i(\varkappa)\left(\frac{1}{2} + \frac{2^i}{2^{i+1}-1}\right).$$

After simplification we obtain $\frac{(2^i-1)\varkappa+2^{i+1}}{2^{i+2}-1} \leq T_i(\varkappa)$, which is true.

Since $\lim_{i\to\infty} \frac{2^i-1}{2^{i+2}-1} = \frac{1}{4}$ and $\lim_{i\to\infty} \frac{2^{i+1}}{2^{i+2}-1} = \frac{1}{2}$, the result follows. ◀

3 Lower Bound

We show a $\Omega(n^{1/2}k^{1/6})$ quantum query complexity lower bound for $\textsc{Claw}_{n\to k}$.

▶ **Theorem 2.** *For all $k \geq 2$, we have $Q(\textsc{Claw}_{n\to k}) = \Omega(n^{1/2}k^{1/6})$.*

Proof. Let $\textsc{pSearch}_m : (* \cup [k])^m \to [k]$ be the partial function defined as

$$\textsc{pSearch}_m(x_1, x_2, \ldots, x_m) = \begin{cases} x_i, & \text{if } x_i \neq *, \forall j \neq i : x_j = * \\ \text{undefined}, & \text{otherwise} \end{cases}.$$

Consider the function $f_{n,k} = \textsc{Claw}_{k\to k} \circ \textsc{pSearch}_{\lfloor n/k \rfloor}$. One can straightforwardly reduce $f_{n,k}(x, y)$ to $\textsc{Claw}_{n\to k+2}(x', y')$ by setting

$$x'_i = \begin{cases} x_i, & \text{if } x_i \neq * \\ k+1, & \text{if } x_i = * \end{cases}$$

and

$$y'_i = \begin{cases} y_i, & \text{if } y_i \neq * \\ k+2, & \text{if } y_i = * \end{cases}.$$

Now we show that $Q(f_{n,k}) = \Omega\left(k^{2/3}\sqrt{n/k}\right) = \Omega(n^{1/2}k^{1/6})$. The fact that $Q(\textsc{Claw}_{k\to k}) = \Omega(k^{2/3})$ has been established by Zhang [16]. Furthermore, thanks to the work done by Brassard et al. in [6, Theorem 13] we know that for $\textsc{pSearch}_m$ a composition theorem holds: $Q(h \circ \textsc{pSearch}_m) = \Omega(Q(h) \cdot Q(\textsc{pSearch}_m)) = \Omega(Q(h) \cdot \sqrt{m})$. Therefore,

$$Q(\textsc{Claw}_{n\to k}) \geq Q\left(\textsc{Claw}_{k-2\to k-2} \circ \textsc{pSearch}_{\lfloor \frac{n}{k-2} \rfloor}\right) = \Omega\left(k^{2/3}\sqrt{\frac{n}{k}}\right) = \Omega\left(n^{1/2}k^{1/6}\right).$$

◀

4 Open Problems

Can we show that $Q(\textsc{Claw}_{n\to n^{2/3}}) = \Omega(n^{2/3})$? In particular, our algorithm struggles with instances where there are $\frac{n^{2/3}}{2}$ singletons only two (or none) of which are matching and the remaining variables are evenly distributed with $\Theta(n^{1/3})$ copies each, such that none are matching. Thus our algorithm then either has to waste time sampling all the high-frequency decoy values or have most variables not sampled by step 2. If this lower bound held, it would imply a better lower bound for evaluating constant depth formulas and Boolean matrix product verification [10, Theorem 5].

References

1 Scott Aaronson, Nai-Hui Chia, Han-Hsuan Lin, Chunhao Wang, and Ruizhe Zhang. On the Quantum Complexity of Closest Pair and Related Problems. In Shubhangi Saraf, editor, *35th Computational Complexity Conference (CCC 2020)*, volume 169 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 16:1–16:43, Dagstuhl, Germany, 2020. Schloss Dagstuhl–Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.CCC.2020.16.

2 Scott Aaronson and Yaoyun Shi. Quantum lower bounds for the collision and the element distinctness problems. *Journal of the ACM (JACM)*, 51(4):595–605, 2004.

3 Andris Ambainis. Polynomial degree and lower bounds in quantum complexity: Collision and element distinctness with small range. *Theory of Computing*, 1(1):37–46, 2005.
4 Andris Ambainis. Quantum walk algorithm for element distinctness. *SIAM Journal on Computing*, 37(1):210–239, 2007.
5 Daniel J. Bernstein, Stacey Jeffery, Tanja Lange, and Alexander Meurer. Quantum algorithms for the subset-sum problem. In Philippe Gaborit, editor, *Post-Quantum Cryptography*, pages 16–33, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.
6 Gilles Brassard, Peter Høyer, Kassem Kalach, Marc Kaplan, Sophie Laplante, and Louis Salvail. Key establishment à la merkle in a quantum world. *Journal of Cryptology*, 32(3):601–634, 2019. doi:10.1007/s00145-019-09317-z.
7 Harry Buhrman and Ronald de Wolf. Complexity measures and decision tree complexity: a survey. *Theoretical Computer Science*, 288(1):21–43, 2002. Complexity and Logic. doi:10.1016/S0304-3975(01)00144-X.
8 Harry Buhrman, Christoph Dürr, Mark Heiligman, Peter Høyer, Frédéric Magniez, Miklos Santha, and Ronald de Wolf. Quantum algorithms for element distinctness. *SIAM Journal on Computing*, 34(6):1324–1330, 2005. doi:10.1137/S0097539702402780.
9 Andrew M. Childs and Jason M. Eisenberg. Quantum algorithms for subset finding. *Quantum Info. Comput.*, 5(7):593–604, 2005.
10 Andrew M. Childs, Shelby Kimmel, and Robin Kothari. The quantum query complexity of read-many formulas. In *Proceedings of the 20th Annual European Conference on Algorithms*, ESA'12, pages 337–348, Berlin, Heidelberg, 2012. Springer-Verlag. doi:10.1007/978-3-642-33090-2_30.
11 Fan Chung and Linyuan Lu. Concentration inequalities and martingale inequalities: a survey. *Internet Mathematics*, 3(1):79–127, 2006.
12 François Le Gall and Saeed Seddighin. Quantum meets fine-grained complexity: Sublinear time quantum algorithms for string problems, 2020. arXiv:2010.12122.
13 Frédéric Magniez, Miklos Santha, and Mario Szegedy. Quantum algorithms for the triangle problem. *SIAM Journal on Computing*, 37(2):413–424, 2007. doi:10.1137/050643684.
14 Ansis Rosmanis. Adversary lower bound for element distinctness with small range, 2014. arXiv:1401.3826.
15 Seiichiro Tani. Claw finding algorithms using quantum walk. *Theoretical Computer Science*, 410(50):5285–5297, 2009. Mathematical Foundations of Computer Science (MFCS 2007). doi:10.1016/j.tcs.2009.08.030.
16 Shengyu Zhang. Promised and distributed quantum search. In Lusheng Wang, editor, *Computing and Combinatorics*, pages 430–439, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg.