Quantum query complexity of decision problems with small 1-certificates

Arjan Cornelissen

Department of Computer Science, Cambridge University

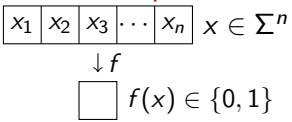
November 16th, 2026



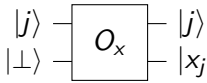
Quantum query complexity of decision problems

1. *Decision problem:* $f : \Sigma^n \to \{0,1\}$.
   1. Σ "alphabet".
   2. $f(x) = 0 \Leftrightarrow x$ is a NO-instance.
   3. $f(y) = 1 \Leftrightarrow y$ is a YES-instance.
2. *Oracle:* For all $x \in \Sigma^n$,
   1. $O_x \in \mathcal{U}(\mathbb{C}^n \otimes \mathbb{C}^\Sigma)$
   2. $O_x : |j\rangle\,|\perp\rangle \mapsto |j\rangle\,|x_j\rangle$.
3. *Quantum query algorithm:*
   1. Only depends on x through the oracle.
   2. $\mathcal{A}$ computes f with high probability, if: $\mathbb{P}[f(x) = b] \geq 2/3$.
4. *Quantum query complexity:*
   $$\mathrm{Q}(f) := \min_{\mathcal{A} \text{ comp. } f \text{ whp.}} T(\mathcal{A}).$$
   1. *Trivial:* $1 \leq \mathrm{Q}(f) \leq n$.

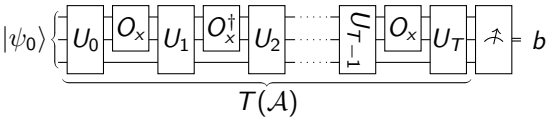
Decision problem:



Oracle:



Quantum query algorithm: $\mathcal{A}$



Certificates

Decision problem: $f : \Sigma^n \to \{0,1\}$.

1. *Certificate:*
   1. *Dfn:* $S \subseteq [n]$ is a certificate for x if: $\forall x' \in \Sigma^n, x'|_S = x|_S \Rightarrow f(x) = f(x')$.
   2. *Intuition:* "Sufficient set of characters in x to be convinced of the function value $f(x)$."
2. *Minimum certificate size:* $C(f;x) := \min_{S \subseteq [n] \text{ cert. for } x} |S|$.
3. 0- *and* 1*-certificate complexity:*
   1. $C_0(f) := \max_{x \in f^{-1}(0)} C(f;x)$.
   2. $C_1(f) := \max_{y \in f^{-1}(1)} C(f;y)$.
4. *Trivial:* $1 \leq \{C_0(f), C_1(f)\} \leq n$.

Example: the *OR*-function:

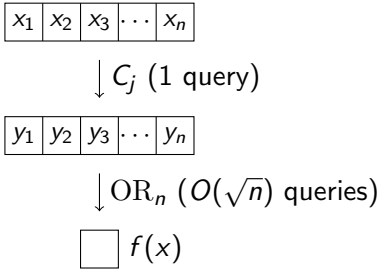
1. $\mathrm{OR}_n : \{0,1\}^n \to \{0,1\}$, $\mathrm{OR}_n(x) = 1 \Leftrightarrow |x| \geq 1$.
2. $C_1(\mathrm{OR}_n) = 1$.
3. $C_0(\mathrm{OR}_n) = n$.

Example: Element-distinctness:

1. $\mathrm{ED}_n : \Sigma^n \to \{0,1\}$, $(|\Sigma| \geq n)$, $\mathrm{ED}_n(x) = 1 \Leftrightarrow \exists \{i,j\} \subseteq [n] : x_i = x_j$.
2. $C_1(\mathrm{ED}_n) = 2$.
3. $C_0(\mathrm{ED}_n) = n$.

Grover's algorithm and consequences

1. *Grover's algorithm:* $\mathrm{Q}(\mathrm{OR}_n) \in O(\sqrt{n})$.
2. *More generally:*
   $C_1(f) = 1 \Rightarrow \mathrm{Q}(f) \in O(\sqrt{n})$.
   1. *Checking routine:* For any $j \in [n]$:
      1. Query x_j.
      2. Set $y_j = 1$ if this is a 1-certificate, else $y_j = 0$.
   2. Run Grover's algorithm over all $j \in [n]$.
3. *Natural question:*
   $C_1(f) = 2 \Rightarrow \mathrm{Q}(f) \in O(n^{\alpha})$?
4. *More generally:*
   $C_1(f) = k \Rightarrow \mathrm{Q}(f) \in O(n^{\alpha_k})$?
5. *Answer:* $C_1(f) = k \Rightarrow \mathrm{Q}(f) \in O(n^{\frac{k}{k+1}})$.

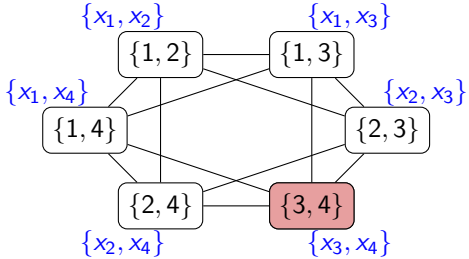


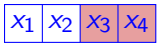
Quantum walk search (1/2)

Decision problem: $f : \Sigma^n \to \{0,1\}$, $C_1(f) = 2$.

1. *Johnson graph:* $J(n,r) = (V,E)$, where
   1. $V = \binom{[n]}{r}$, $1 \le r \le n$.
   2. $\{A,B\} \in E \Leftrightarrow |A \,\Delta\, B| = 2$.
2. *Database:* for $x \in \Sigma^n$, $A \in V$, keep track of x_A.
   1. *Setup:* $\mathrm{S} \in O(r)$ queries.
   2. *Update:* $\mathrm{U} \in O(1)$ queries.
3. *Marked set:* $A \in V$ is marked if x_A contains a 1-certificate.
   1. *Check:* $\mathrm{C} = 0$ queries.
4. *Statistics:*
   1. *Marked fraction:* $\geq \frac{\binom{n-2}{r-2}}{\binom{n}{r}} =: \varepsilon \in \Theta((\frac{r}{n})^2)$.
   2. *Mixing time:* $\mathrm{MT} \in \Theta(r)$.

Johnson graph: $J(4,2)$





$x \in \Sigma^n$

Classical query complexity:

$O(\mathrm{S} + \frac{1}{\varepsilon}(\mathrm{MT} \cdot \mathrm{U} + \mathrm{C}))$.

Quantum query complexity:

$\mathrm{Q}(f) \in O(\mathrm{S} + \frac{1}{\sqrt{\varepsilon}}(\sqrt{\mathrm{MT}} \cdot \mathrm{U} + \mathrm{C}))$.

Quantum walk search (2/2)

Decision problem: $f : \Sigma^n \to \{0,1\}$, $C_1(f) = 2$.

1. *Properties:*
   1. *Setup:* $\mathsf{S} \in O(r)$.
   2. *Update:* $\mathsf{U} \in O(1)$.
   3. *Check:* $\mathsf{C} = 0$.
   4. *Marked fraction:* $\varepsilon \in \Theta((\frac{r}{n})^2)$.
   5. *Mixing time:* $\mathrm{MT} \in \Theta(r)$.
2. *Total cost:*
   $$\mathsf{Q}(f) \in O(\mathsf{S} + \tfrac{1}{\sqrt{\varepsilon}}(\sqrt{\mathrm{MT}} \cdot U + \mathsf{C})) = O(r + \tfrac{n}{\sqrt{r}}).$$
3. *Optimal choice:*
   $r \in \Theta(n^{2/3}) \Rightarrow \mathsf{Q}(f) \in O(n^{2/3})$.

Decision problem: $f : \Sigma^n \to \{0,1\}$, $C_1(f) = k$.

1. *Properties:*
   1. *Setup:* $\mathsf{S} \in O(r)$.
   2. *Update:* $\mathsf{U} \in O(1)$.
   3. *Check:* $\mathsf{C} = 0$.
   4. *Marked fraction:* $\varepsilon \in \Theta((\frac{r}{n})^k)$.
   5. *Mixing time:* $\mathrm{MT} \in \Theta(r)$.
2. *Total cost:*
   $$\mathsf{Q}(f) \in O(\mathsf{S} + \tfrac{1}{\sqrt{\varepsilon}}(\sqrt{\mathrm{MT}} \cdot U + \mathsf{C})) = O(r + \tfrac{n^{k/2}}{r^{(k-1)/2}}).$$
3. *Optimal choice:*
   $r \in \Theta(n^{\frac{k}{k+1}}) \Rightarrow \mathsf{Q}(f) \in O(n^{\frac{k}{k+1}})$.

Summary & further insights

Decision problem: $f : \Sigma^n \to \{0,1\}$

1. *Grover's algorithm:* $C_1(f) = 1 \Rightarrow \mathrm{Q}(f) \in O(\sqrt{n})$.
2. *Quantum random walk:* $C_1(f) = k \Rightarrow \mathrm{Q}(f) \in O(n^{\frac{k}{k+1}})$.

Optimal for large alphabets: let $k \geq 2$,

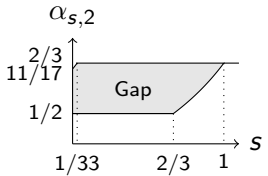
1. Let Σ an Abelian group, with $|\Sigma| \geq n^k$,
2. $k\text{−}\mathtt{SUM} : \Sigma^n \to \{0,1\}$, $k\text{−}\mathtt{SUM}(x) = 1 \Leftrightarrow \exists S \subseteq [n] : |S| = k, \sum_{j \in S} x_j = 0$.
3. $C_1(k\text{−}\mathtt{SUM}) = k$ and $\mathrm{Q}(k\text{−}\mathtt{SUM}) \in \Omega(n^{\frac{k}{k+1}})$.

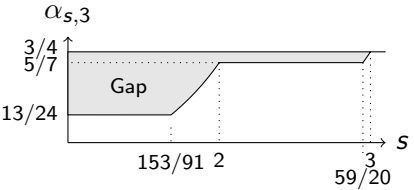
Recent results:

1. $|\Sigma| \in O(1) \wedge C_1(f) = 2 \Rightarrow \mathrm{Q}(f) \in O(n^{11/17})$.
2. $\exists f : |\Sigma| = 2, C_1(f) = 2, \mathrm{Q}(f) \in \Omega(\sqrt{n \log(n)})$
3. $\exists f : |\Sigma| = 2, C_1(f) = 3, \mathrm{Q}(f) \in \Omega(n^{13/24})$.

Pictorial overview:

$$\alpha_{s,k} := \limsup_{n \to \infty} \max_{\substack{f:\Sigma^n \to \{0,1\} \\ C_1(f)=k, |\Sigma| \leq 2n^s}} \frac{\log \mathrm{Q}(f)}{\log n}.$$





Thanks!

ajcornelissen@outlook.com