Simon’s problem for linear functions

Joran van Apeldoorn*    Sander Gribling*

Abstract

Simon’s problem asks the following: determine if a function \( f : \{0,1\}^n \rightarrow \{0,1\}^n \) is one-to-one or if there exists a unique \( s \in \{0,1\}^n \) such that \( f(x) = f(x \oplus s) \) for all \( x \in \{0,1\}^n \), given the promise that exactly one of the two holds. A classical algorithm that can solve this problem for every \( f \) requires \( 2^{\Omega(n)} \) queries to \( f \). Simon \cite{Sim97} showed that there is a quantum algorithm that can solve this promise problem for every \( f \) using only \( O(n) \) quantum queries to \( f \). A matching lower bound on the number of quantum queries was given in \cite{KNP07}, even for functions \( f : \mathbb{F}_p^n \rightarrow \mathbb{F}_p^n \). We give a short proof that \( O(n) \) quantum queries is optimal even when we are additionally promised that \( f \) is linear. This is somewhat surprising because for linear functions there even exists a classical \( n \)-query algorithm.

1 Introduction

In 1994, Simon \cite{Sim97} showed the existence of a query problem where quantum algorithms offer an exponential improvement over the best randomized classical algorithms that have a bounded error probability of, say, at most 1/3. The problem he considers is the following:

\[ \text{Given a function } f : \{0,1\}^n \rightarrow \{0,1\}^n \text{ with the promise that it either (1) is one-to-one or (2) admits a unique } s \in \{0,1\}^n \text{ such that } f(x) = f(x \oplus s) \text{ for all } x \in \{0,1\}^n, \text{ decide which of the two holds.} \]

Simon showed that there is a quantum algorithm which can solve this promise problem for any \( f \) using \( O(n) \) quantum queries to \( f \), i.e., using \( O(n) \) applications of the unitary \( |x\rangle |b\rangle \rightarrow |x\rangle |b \oplus f(x)\rangle \). This offers an exponential improvement over classical algorithms, since Simon also showed that at least \( 2^{\Omega(n)} \) classical queries of the form \( x \mapsto f(x) \) are needed in order to succeed with probability at least 2/3. The question we are interested in is the optimality of Simon’s quantum algorithm and its generalization to finite fields. Let \( p \) be a prime power and let \( \mathbb{F}_p \) be the finite field with \( p \) elements. Simon’s problem over \( \mathbb{F}_p \) can be formulated as follows:

\[ \text{Given a function } f : \mathbb{F}_p^n \rightarrow \mathbb{F}_p^n \text{ with the promise that it either (1) is one-to-one or (2) admits a one-dimensional subspace } H \subset \mathbb{F}_p^n \text{ such that for all } x, y \in \mathbb{F}_p^n, f(x) = f(y) \iff x - y \in H, \text{ decide which of the two holds.} \]

Koiran et al. \cite{KNP07} (for an earlier version see \cite{KNP05}) showed that the quantum query complexity of Simon’s problem over \( \mathbb{F}_p \) is \( \Theta(n) \). Here we show that the lower bound of \( \Omega(n) \) quantum queries holds even when \( f \) is additionally promised to be linear. That is, a quantum algorithm which can solve Simon’s problem over \( \mathbb{F}_p \) for any linear function requires \( \Omega(n) \) quantum queries to \( f \). Interestingly, this shows that for the class of linear functions there is no quantum advantage: classically, one can also fully determine a linear function using \( n \) queries, by querying a basis.

*QuSoft, CWI, the Netherlands. Both authors are supported by the Netherlands Organization for Scientific Research, grant number 617.001.351. The first author is also partially supported by QuantERA, project QuantAlgo 680-91-034. {apeldoorn,gribling}@cwi.nl

1In fact, Simon considered the problem of finding the non-zero string \( s \), if it exists. Here we focus on the decision version of his problem. However, all upper bounds mentioned are derived from algorithms which also find \( s \).

2They even prove the analogous lower bound for the hidden subgroup problem over Abelian groups, see Section 4.
Definition (Linear Simon’s problem). Given a linear function \( f : \mathbb{F}_p^n \to \mathbb{F}_p^n \), with the promise that either \( |\ker(f)| = 1 \) or \( |\ker(f)| = p \), decide which of the two holds.

Our main result (proved in Section 2) is the following.

**Theorem 1.** Let \( A \) be a \( T \)-query quantum algorithm for the Linear Simon’s problem with success probability at least \( 2/3 \). Then \( T = \Omega(n) \).

We follow the same proof structure as [KNP07], using the polynomial method [BBC+01]. More specifically, we show that, averaged over a subset of functions, the acceptance probability of a \( T \)-query quantum algorithm is a polynomial of degree at most \( 2T \) in the size of the kernel. We then obtain the lower bound by appealing to [KNP07, Lemma 5] which states that any polynomial with the correct success probabilities has degree \( \Omega(n) \). However, where [KNP07] average over all functions, we only consider linear functions over \( \mathbb{F}_p^n \). Surprisingly this simplifies the proof substantially. We also give a slightly simplified proof of [KNP07, Lemma 5].

**Notation** For a set \( K \subseteq \mathbb{F}_p^n \) we call \( s : K \to \mathbb{F}_p^n \) a partial function and we say that \( f : \mathbb{F}_p^n \to \mathbb{F}_p^n \) extends \( s \) if \( f(x) = s(x) \) for all \( x \in K \). We write \( s \preceq f \) if \( f \) extends \( s \). Let \( S_k \) be the set of all partial functions defined on a domain of size at most \( k \). Let \( \deg_x(f) \) be the degree of \( f \) as a polynomial in the variable \( x \). We define \( F = \{ f : \mathbb{F}_p^n \to \mathbb{F}_p^n \mid f \text{ linear} \} \) as the set of all linear functions from \( \mathbb{F}_p^n \) to \( \mathbb{F}_p^n \). For each \( k \in \{0,1,\ldots,n\} \) and \( D = p^k \) let \( F_D \) be the subset of \( F \) consisting of linear functions whose kernel has size \( D \), i.e., \( F_D = \{ f \in F \mid |\ker(f)| = D \} \). Finally, we use \( i^2 = -1 \) and we use square brackets \([\cdot] : \{0,1\} \to \{0,1\}\) to denote the function that maps true to 1 and false to 0.

## 2 Proof of Theorem 1

The proof of Theorem 1 is based on a well-known method of lower bounding the quantum query complexity of a Boolean function \( G : \{0,1\}^n \to \{0,1\} \): the polynomial method introduced by Beals et al. [BBC+01]. Let us first sketch the polynomial method in the setting of their paper. A \( T \)-query quantum algorithm \( A \) for computing \( G(x) \) (for every \( x \in \{0,1\}^n \)) can be described by a Hilbert space \( \mathbb{C}^n \otimes \mathbb{C}^2 \otimes \mathbb{C}^m \), a sequence of \( T \) unitary matrices \( U_0, \ldots, U_T \) acting on the space, and an oracle \( O_x \) that is defined as

\[
O_x : |i\rangle|b\rangle|w\rangle \mapsto |i\rangle|b \oplus x_i\rangle|w\rangle.
\]

The definition of the oracle explains the tensor product structure of the Hilbert space \( \mathbb{C}^n \otimes \mathbb{C}^2 \otimes \mathbb{C}^m \); the first part corresponds with a query input, the second with a query output, and the last with extra work space. The quantum algorithm then works as follows. It starts in a fixed state, say \( |0\rangle|0\rangle|0\rangle \), and then alternates between applying the unitaries and queries before deciding on its output via a measurement to the second register of the final state. Concretely, the state of the algorithm before the final measurement is as follows:

\[
U_T O_x U_{T-1} O_x \cdots O_x U_1 O_x U_0 |0\rangle|0\rangle|0\rangle =: \sum_{(i,b,w) \in [n] \times \{0,1\} \times [m]} \alpha_{i,b,w}(x) |i\rangle|b\rangle|w\rangle
\]

where \( \alpha_{i,b,w}(x) \in \mathbb{C} \). The crucial observation is that the amplitudes \( \alpha_{i,b,w}(x) \) of the final state are polynomials in the input variables \( x_i \) of degree at most \( T \). Indeed, applying the oracle to, e.g., a state \( \alpha |i\rangle|0\rangle|w\rangle + \beta |i\rangle|1\rangle|w\rangle \) leads to the state

\[
[(1 - x_i)\alpha + x_i \beta] |i\rangle|0\rangle|w\rangle + [x_i \alpha + (1 - x_i) \beta] |i\rangle|1\rangle|w\rangle.
\]

This shows that applying the oracle once increases the degree by at most 1. Since the unitaries do not depend on \( x \) and are linear transformations, they do not increase the degree. Instead of viewing the amplitudes as polynomials in the variables \( x_i \), it will be more convenient to think of them as homogeneous (degree \( T \)) polynomials in the Kronecker delta variables \( \delta_{x_i,1} := x_i \) and \( \delta_{x_i,0} := (1 - x_i) \). The probability of measuring
a 1 in the second register of the final state, i.e., the acceptance probability \( P(x) \), is then given by the sum of the squared amplitudes of states with a 1 in the second register:

\[
P(x) = \sum_{i \in [n], w \in [m]} |\alpha_{i,1,w}(x)|^2 = \sum_{s \subseteq [n] \times \{0,1\}, |s| \leq 2T} \beta_s \prod_{(i,b) \in s} \delta_{x_i,b}
\]

where the real numbers \( \beta_s \) are the coefficients of the monomials \( \prod_{(i,b) \in s} \delta_{x_i,b} \) in \( P(x) \). If \( \mathcal{A} \) computes \( G \) with high success probability, then \( P(x) \) will be close to \( G(x) \) for every \( x \in \{0,1\}^n \) which may be used to prove a degree lower bound on \( P(x) \). However, proving lower bounds on the degree of \( P(x) \) directly is often complicated. A common technique is to average \( P(x) \) over multiple inputs in order to reduce the problem to studying a univariate polynomial. For example, for a symmetric function \( G : \{0,1\}^n \rightarrow \{0,1\} \) averaging \( P(x) \) over all permutations of \( n \) elements reduces the problem to studying univariate polynomials \( q(|x|) \) which approximate \( G(x) \) (for which tight degree bounds are known) [BBC^+01].

The above version of the polynomial method is easily generalized to inputs that are not Boolean (see, e.g., [AS04]). We will do so here for the setting corresponding to the Linear Simon’s problem.

Let \( \mathcal{A} \) be a \( T \)-query algorithm for the Linear Simon’s problem and let \( P(f) \) be the acceptance probability of \( \mathcal{A} \) on the input \( f \). As before, we can write

\[
P(f) = \sum_{s \subseteq \mathbb{F}_p \times \mathbb{F}_p, |s| \leq 2T} \beta_s \prod_{(x,y) \in s} \delta_{f(x),y}.
\]

When we view \( s \) as a partial function, this expression can be rewritten in terms of \( f \) extending \( s \):

\[
P(f) = \sum_{s \in S_{2T}} \beta_s [s \preceq f],
\]

where \( S_{2T} \) is the set of all partial functions \( s \) with \( |\text{dom}(s)| \leq 2T \). As above, it will turn out to be useful to average \( P(f) \) over all linear functions \( f \) with a kernel of size \( D \), i.e., we consider the average acceptance probability \( Q(D) \) over all functions with a kernel of size \( D \):

\[
Q(D) = \sum_{f \in F_D} \frac{1}{|F_D|} P(f) = \sum_{f \in F_D} \frac{1}{|F_D|} \sum_{s \in S} \beta_s [s \preceq f] = \sum_{s \in S} \beta_s \frac{1}{|F_D|} \sum_{f \in F_D} [s \preceq f] = \sum_{s \in S} \beta_s Q_s(D).
\]

Here \( Q_s(D) \) is the probability that a uniformly random \( f \in F_D \) extends \( s \):

\[
Q_s(D) = \frac{1}{|F_D|} \sum_{f \in F_D} [s \preceq f] = \Pr_{f \in F_D} [s \preceq f]
\]

In the next two sections we will prove that the degree of \( Q \) needs to be at least linear in \( n \), and that the degree of each \( Q_s \) (and hence of \( Q \)) is upper bounded by \( 2T \). Together these results implies Theorem I.

### 2.1 Lower bound on the degree

For \( k \in \{0,1,\ldots,n\} \), \( Q(p^k) \) represents an acceptance probability and therefore \( Q(p^k) \in [0,1] \). Moreover, if the algorithm succeeds with probability at least \( 2/3 \), then \( Q(1) \geq 2/3 \) and \( Q(p) \leq 1/3 \). The lemma below shows that such a \( Q \) has degree \( \Omega(n) \). We give a slightly simplified proof for completeness.

**Lemma 2** ([KNP07] Lemma 5). For every polynomial \( Q \) such that \( Q(1) \geq 2/3 \), \( Q(p) \leq 1/3 \) and \( Q(p^k) \in [0,1] \) for all \( k \in \{0,\ldots,n\} \), it holds that \( \deg(Q) \geq n/4 \).

\(^3\)A Boolean function \( G \) is symmetric if \( G(x) \) only depends on the Hamming weight \( |x| \) of \( x \).
Proof. Assume that $Q$ is a polynomial of degree $d \leq n/2$ (otherwise we are done), so that its derivative $Q'$ is of degree $d - 1$ and its second derivative $Q''$ is of degree $d - 2$. Consider the $2d - 2$ intervals of the form $(p^a, p^{a+1})$ where $a = n - (2d - 2), \ldots, n - 1$. Since together $Q'$ and $Q''$ have at most $2d - 3$ roots, there is such an interval for which both polynomials have no roots with real part in it; let $a \geq n - (2d - 2)$ be the integer corresponding to this interval and let $M := \frac{1 + \sqrt{2}}{2} p^n$ be the middle of this interval. By the mean value theorem we know that there is an $x_0 \in [1, p]$ for which $|Q'(x_0)| \geq \frac{1}{3(p - 1)}$. To show the degree lower bound it suffices to prove the following chain of inequalities:

\[
\frac{1}{p^{2d-2}} \leq \frac{Q'(M)}{Q'(x_0)} \leq \frac{3(p-1)}{p^n - 2d + 2}.
\]

Indeed, if the above chain of inequalities holds, then $6 \geq p^n - 4d + 4 \geq 2n - 4d + 4$ which implies that $n - 4d + 4 \leq 3$, i.e., $d \geq \frac{n+1}{4}$.

(*) For the lower bound we will use the following elementary fact:

\[
\text{if } 0 \leq v < w \text{ and } 0 \leq y, \text{ then } \frac{v + y}{w + y} \geq \frac{v}{w}.
\]

Denote the roots of $Q'$ by $b_j + c_j i$, for $j \in [d - 1]$. Then $Q'(x) = \lambda \prod_{j=1}^{d-1} (x - b_j - c_j i)$ for some $\lambda \in \mathbb{R}$ and hence

\[
\left| \frac{Q'(M)}{Q'(x_0)} \right| = \prod_{j=1}^{d-1} \frac{|M - b_j - c_j i|}{|x_0 - b_j - c_j i|} = \prod_{j=1}^{d-1} \frac{|M - b_j - c_j i|}{|x_0 - b_j - c_j i|} = \prod_{j=1}^{d-1} \left| \frac{(M - b_j)^2 + c_j^2}{(x_0 - b_j)^2 + c_j^2} \right|
\]

We will show that each factor in the product is bounded from below by $1/p^2$. Considering the $j$-th factor, if $|x_0 - b_j| \leq |M - b_j|$ then we are clearly done. Hence, assume $|x_0 - b_j| > |M - b_j|$, that is, $b_j > \frac{M-x_0}{2} \geq p^{a-1}$.

We use (I):

\[
\sqrt{\frac{(M - b_j)^2 + c_j^2}{(x_0 - b_j)^2 + c_j^2}} \geq \frac{|M - b_j|}{|x_0 - b_j|}
\]

Since we know that $b_j > p^{a-1}$ and $b_j \not\in (p^a, p^{a+1})$ there are two cases to consider:

- If $b_j \in (p^{a-1}, p^a]$, then $\frac{|M - b_j|}{|x_0 - b_j|} \geq \frac{1}{2} \geq \frac{1}{p^2}$

- If $b_j \in [p^{a+1}, \infty)$, then $\frac{|M - b_j|}{|x_0 - b_j|} = \frac{1}{\frac{1}{2}p^a - b_j} = \frac{p^a - b_j}{p^{a+1} - x_0 + (b_j - p^a)} \geq \frac{p^{a-1}}{p^{a+1} - x_0} \geq \frac{1}{2} \geq \frac{1}{p^2}$

where we use (I) and $\frac{1}{2} \geq \frac{1}{p}$ for the first inequality.

(**) By construction $|Q'(x_0)| \geq \frac{1}{3(p - 1)}$, so it remains to show that $|Q'(M)| \leq \frac{(\frac{p-1}{2})^{p^n-2d+2}}{p^n-2d+2}$. Assume towards a contradiction that $|Q'(M)| > (\frac{p-1}{2})^{p^n-2d+2}$. Since $Q''$ has no roots with real part in the interval $(p^a, p^{a+1})$, $Q'$ is either strictly increasing or strictly decreasing on the interval $(p^a, p^{a+1})$. Therefore, there is an interval $(\alpha, \beta)$ (with $\alpha, \beta \in (p^a, M, p^{a+1})$ of length $\frac{1}{2}p^a$ where $|Q'(x)| > (\frac{p-1}{2})^{p^n-2d+2}$. By the fundamental theorem of calculus this implies that $|Q(\alpha) - Q(\beta)| > 1$. This is a contradiction, since we have $1 \geq |Q(p^{a+1}) - Q(p^a)| \geq |Q(\alpha) - Q(\beta)|$, where the last inequality follows by monotonicity of $Q$ on the interval $(p^a, p^{a+1})$. It follows that

\[
|Q'(M)| \leq \left( \frac{p-1}{2} \right)^{p^n-2d+2} \leq \left( \frac{p-1}{2} \right)^{p^n-2d+2}.
\]

We conclude that $\frac{1}{p^{2d-2}} \leq \frac{Q'(M)}{Q'(x_0)} \leq \frac{3(p-1)}{p^n - 2d + 2}$ and hence that $d \geq n/4$. \qed
2.2 Upper bound on the degree

We now show that the degree of each $Q_s$ is upper bounded by $2T$.

Lemma 3. Given a partial linear function $s : \text{dom}(s) \rightarrow \mathbb{F}_p^n$, $\deg_D(Q_s) \leq \dim(\text{span}(\text{dom}(s)))$.

Proof. Let $K := \text{span}(\text{dom}(s))$ and $k := \dim(K)$. We can extend $s$ uniquely to a linear function on $K$. Define $Z := \ker(s) \subseteq K$ and $z := \dim(Z)$, and $Y := Z^\perp \cap K$. For a function $f : \mathbb{F}_p^n \rightarrow \mathbb{F}_p^n$ in $D$, we write $H := \ker(f)$, $h := \dim(H)$ and $D := |H| = p^h$. We show that $\Pr_{f \in R_D} [s \preceq f]$ has degree at most $k$ as a polynomial in $D$. We analyze this probability in three parts:

$$
\Pr_{f \in R_D} [s \preceq f] = \Pr_{f \in R_D} [Z \subseteq H \cap Y \cap H = \{0\}] - \Pr_{f \in R_D} [s \preceq f \mid Z \subseteq H \cap Y \cap H = \{0\}]
$$

$$
= \Pr_{f \in R_D} [Z \subseteq H] \Pr_{f \in R_D} [Y \cap H = \{0\} \mid Z \subseteq H] \Pr_{f \in R_D} [s \preceq f \mid Z \subseteq H \cap Y \cap H = \{0\}].
$$

We show that

1. $\Pr_{f \in R_D} [Z \subseteq H]$ is a polynomial in $D$ of degree at most $z$,
2. $\Pr_{f \in R_D} [Y \cap H = \{0\} \mid Z \subseteq H]$ is a polynomial in $D$ of degree at most $k - z$,
3. $\Pr_{f \in R_D} [s \preceq f \mid Z \subseteq H \cap Y \cap H = \{0\}]$ does not depend on $D$.

Together, this implies that $\Pr_{f \in R_D} [s \preceq f]$ is a polynomial in $D$ of degree at most $k$.

(1) The probability that $Z \subseteq H$ equals the fraction of $h$-dimensional subspaces of $\mathbb{F}_p^n$ that contain $Z$. There are $\alpha(n, h) = \prod_{i=0}^{n-1} (p^h - p^i)$ ways to pick $h$ linearly independent vectors in a space of dimension $n$, and hence there are $\beta(n, h) = \frac{\alpha(n, h)}{\alpha(n, n)}$ different subspaces of dimension $h$ in $\mathbb{F}_p^n$. The number of $h$-dimensional subspaces that contain $Z$ equals the number of $(h - z)$-dimensional subspaces in an $(n - z)$-dimensional space. Hence

$$
\Pr_{f \in R_D} [Z \subseteq H] = \frac{\beta(n - z, h - z)}{\beta(n, h)} = \prod_{i=0}^{n-1} \frac{p^h - p^i}{p^n - p^i},
$$

which is a degree-$z$ polynomial in terms of $D = p^h$.

(2) We have $\Pr_{f \in R_D} [Y \cap H = \{0\} \mid Z \subseteq H] = \Pr_{f \in R_D} [Y/Z \cap H/Z = \{0\}]$ where $Y/Z$ and $H/Z$ are subspaces of $\mathbb{F}_p^n / Z \simeq \mathbb{F}_p^{n - z}$. By construction we have that $\dim(Y/Z) = \dim(Y) = k - z$, $\dim(H/Z) = h - z$. The probability $\Pr_{f \in R_D} [Y/Z \cap H/Z = \{0\}]$ equals the number of $(h - z)$-dimensional bases of $\mathbb{F}_p^{n - z}$ which are linearly independent from $Y$, divided by $\beta(n - z, h - z)$. That is,

$$
\Pr_{f \in R_D} [Y/Z \cap H/Z = \{0\}] = \prod_{i=0}^{h-z-1} \frac{p^{n-z} - p^{k-z+i}}{\alpha(n - z, h - z)} = \prod_{i=0}^{h-z-1} \frac{p^{n-z} - p^{k-z+i}}{\alpha(n - z, k - z)}
$$

where the last equality is obtained using $\alpha(n - z, h - z) = \alpha(n - z, k - z) \prod_{i=k-z}^{h-z-1} p^n - p^{h-z+i}$. It follows that

$$
\Pr_{f \in R_D} [Y/Z \cap H/Z = \{0\}] = \prod_{i=0}^{h-z-1} \frac{p^{n-z} - p^{h-z+i}}{\alpha(n - z, k - z)}
$$

is a polynomial in $D = p^h$ of degree $k - z$.

We mention in passing that, alternatively, one can arrive at the same expression by looking at the probability that a random $Y$ is linearly independent from a fixed $H$.

(3) Finally we consider $\Pr_{f \in R_D} [s \preceq f \mid Z \subseteq H \cap Y \cap H = \{0\}]$. Since $Z \subseteq H$, we know that $f$ and $s$ agree on $Z$. Hence, $f$ extends $s$ if their values agree on $Y$. Let $b_1, \ldots, b_{k-z}$ be a basis for $Y$, then $f$ and $s$ agree on $Y$ if and only if they agree on $b_1, \ldots, b_{k-z}$. Since we condition on the event $Y \cap H = \{0\}$, the probability that this happens does not depend on $D = p^h$. 

\qed
3 Open problems

To conclude, we propose the following open problems:

- Koiran et al. [KNP07] lift the lower bound on Simon’s problem over $\mathbb{F}_p^n$ to the hidden subgroup problem over finite Abelian groups:

  Given a (finite Abelian) group $G$ and a function $f : G \to X$ with the promise that there is a subgroup $H \leq G$ of rank either 0 or 1 (i.e., either trivial, or generated by a single element), such that $f(g) = f(g')$ if and only if $g - g' \in H$, decide which of the two holds.

  One recovers Simon’s problem over $\mathbb{F}_p^n$ by taking $G = X = \mathbb{F}_p^n$. A natural question is whether or not the hidden subgroup problem over finite Abelian groups also remains equally hard when we are additionally promised that $f$ is an endomorphism. The reduction used by Koiran et al. combined with our result gives a smaller and more structured set of hard instances of the hidden subgroup problem over Abelian groups. However, the functions obtained from this reduction will only be endomorphisms on a subgroup of $G$, not on all of $G$.

- While the general Simon’s problem has no natural extension to $\mathbb{R}^n$, the linear Simon’s problem can possibly be extended to $\mathbb{R}^n$. For example: given matrix-vector multiplication queries $x \mapsto Ax$ for a symmetric matrix $A$ with $\|A\| \leq 1$, decide if $\lambda_{\min}(A) \leq \epsilon$ or $\lambda_{\min}(A) \geq 2\epsilon$. It remains an open question to prove a lower bound on this problem. An $\Omega(n)$ lower bound could have implications for quantum convex optimization. In particular this may resolve an open question posed in recent work [VAGGW18] regarding the number of queries needed to optimize a convex function.

- Aaronson and Ben-David [ABD16] introduced the idea of sculpting functions. They characterized the total Boolean functions for which there is a promise on the input such that restricted to that promise there is an exponential separation between quantum and classical query complexity. We propose the related idea of over-sculpting: bringing the classical query complexity down to the quantum query complexity. More specifically, for which (possibly partial) Boolean functions $f$ does there exist a promise $P$ such that:

  $$Q_{1/3}(f) \leq o(R_{1/3}(f))$$

  $$Q_{1/3}(f) = \Theta(Q_{1/3}(f|_P)) = \Theta(R_{1/3}(f|_P)).$$

  Simon’s problem does not correspond to a Boolean function since the input alphabet is not Boolean, but our results show that Simon’s problem can be over-sculpted in this slightly different setting.

References

[ABD16] S. Aaronson and S. Ben-David. Sculpting quantum speedups. In Proceedings of the 31st Conference on Computational Complexity, CCC ’16, pages 26:1–26:28, 2016.

[AS04] S. Aaronson and Y. Shi. Quantum lower bounds for the collision and the element distinctness problems. Journal of the ACM, 51(4):595–605, 2004.

[BBC+01] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf. Quantum lower bounds by polynomials. Journal of the ACM, 48(4):778–797, 2001. Earlier version in FOCS’98. quant-ph/9802049.

[KNP05] P. Koiran, V. Nesme, and N. Portier. A quantum lower bound for the query complexity of Simon’s problem. In Proceedings of the 32nd ICALP, volume 3580 of Lecture Notes in Computer Science, pages 1287–1298, 2005.

An input for Simon’s problem is a function $f : \mathbb{F}_p^n \to \mathbb{F}_p^n$, which can be viewed as a string of length $p^n$ over the input alphabet $\mathbb{F}_p^n$. 


[KNP07] P. Koiran, V. Nesme, and N. Portier. The quantum query complexity of the Abelian hidden subgroup problem. *Theoretical Computer Science*, 380:115–126, 2007.

[Sim97] D. Simon. On the power of quantum computation. *SIAM Journal on Computing*, 26(5):1474–1483, 1997. Earlier version in FOCS’94.

[vAGGdW18] J. van Apeldoorn, A. Gilyén, S. Gribling, and R. de Wolf. Convex optimization using quantum oracles, 2018. arXiv:1809.00643.