QCrypt 2021

A Quantum–Prover Interactive Proof for Simon's Problem

Samuel Ducharme
Université de Montréal
samuel.ducharme@umontreal.ca

Simon's Problem

Let f be a function $f:\{0,1\}^n \to \{0,1\}^n$ given as a black-box and for which there exists $s \in \{0,1\}^n$ such that $x,y \in \{0,1\}^n$

$$f(x)=f(y) \text{ iff } x \oplus y \in \{0^n, s\}$$

Goal : Finding out if $s=0^n$ or $s \neq 0^n$

If $s=0^n$, we'll say that f is one-to-one

If $s \neq 0^n$, we'll say that f is two-to-one

Any classical algorithm attempting to solve Simon's problem with a good probability of success needs to make at least $\Omega(2^{(n/2)})$ calls to f.

There exists a quantum algorithm that can solve Simon's problem with a good probability of success that makes $O(n)$ calls to f.

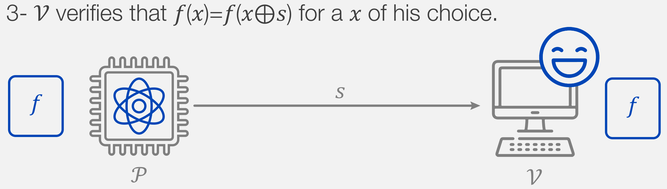
Daniel Simon : On the power of quantum computation. In Proceedings of the 35th Symposium on Foundations of Computer Science, page 116–123, 1994.

In 2010, Scott Aaronson asked the following question on his personal blog:
"Let f be a black-box function, which is promised either to satisfy the Simon promise or to be one-to-one. Can a prover with the power of BQP convince a BPP verifier that f is one-to-one."

Scott Aaronson : Research projects in quantum complexity theory, 2010. https://www.scottaaronson.com/blog/?p=471, Consulted on 2021-07-03.

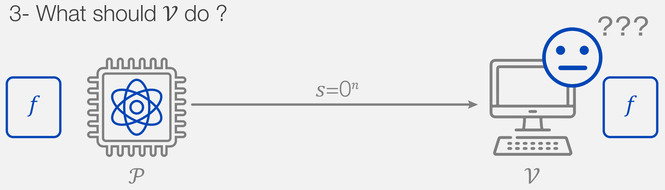
if f is two-to-one :

1- $\mathcal{P}$ finds s using Simon's algorithm
2- $\mathcal{P}$ sends s to $\mathcal{V}$.
3- $\mathcal{V}$ verifies that $f(x)=f(x \oplus s)$ for a x of his choice.



if f is one-to-one :

1- $\mathcal{P}$ finds that $s=0^n$ using Simon's algorithm.
2- $\mathcal{P}$ sends s to $\mathcal{V}$.
3- What should $\mathcal{V}$ do ?



Under the assumption that the verifier has access to a large enough constant-size quantum computer, it is known that for any non-black-box quantum circuit, there exists a protocol that will make the verifier differentiate between an honest and a cheating prover with good enough probability.

Dorit Aharonov, Michael Ben-Or, Elad Eban et Urmila Mahadev : Interactive proofs for quantum computations, 2017. https://arxiv.org/abs/1704.04487.

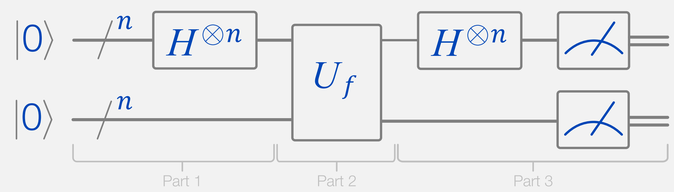
My Protocol

The verifier randomly choses if he wants to do a Simon's algorithm round or a trap round.

If a trap round is chosen and the final mesurement doesn't give all zeroes, the protocol aborts.

Repeat until enough Simon's algorithm rounds have been done.

Simon's Algorithm Round



Parts 1 and 3 will be done using the QAS-based technique
Between parts 1 and 2, the verifier will decode all of the qubits
Between parts 2 and 3, the verifier will re-encode all of the qubits

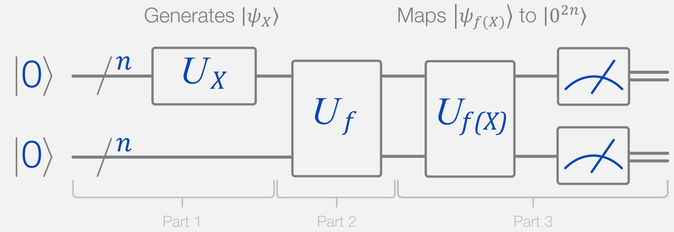
Trap Round

The verifier generates a random set $X \subseteq \{0,1\}^n$ such that $|X|$ is polynomial in n.

Let $|\psi_X\rangle = \frac{1}{\sqrt{|X|}} \sum_{x \in X} |x\rangle$.

The verifier calls f on each values of X. By doing that, he knows exactly the output state that calling U_f on $|\psi_X\rangle|0^n\rangle$ would produce, which is $|\psi_{f(X)}\rangle = \frac{1}{\sqrt{|X|}} \sum_{x \in X} |x\rangle|f(x)\rangle$.

The verifier does a round similar to Simon's, but where the circuit in part 1 is a circuit that generates $|\psi_X\rangle$, and where the circuit in part 3 is a circuit that mesures if the state is indeed $|\psi_{f(X)}\rangle$.



Open Questions

Is this protocol secure enough?

Could this be generalized to any black-box problem in BQP ?