Noisy Simon Period Finding

Alexander May Lars Schlieper Jonathan Schwinger

Horst Görtz Institute for IT Security, Ruhr University Bochum, Germany

download the full paper

Introduction

We show that even noisy quantum period finding computations lead to speedups in comparison to purely classical computations. For this purpose, we implemented Simon's quantum period finding circuit on the 15-qubit quantum device IBM-Q16 Melbourne. Our experiments show that with a certain probability $\tau(n)$ we measure erroneous vectors that are not orthogonal to $\mathbf{s}$ and do not follow the expected distribution. To mitigate this, we propose new, simple, but very effective smoothing techniques to classically mitigate physical noise effects, which leads to a distribution similar to the LPN distribution (referred to as LSN in the following). We then use well-known LPN algorithms to solve the problem.

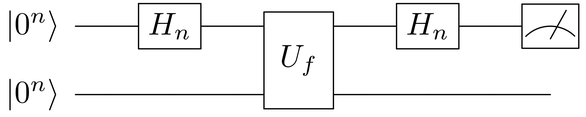
Simon's problem

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$. We call f a *Simon function* if there exists some period $\mathbf{s} \in \mathbb{F}_2^n \setminus \mathbf{0}$ such that for all $\mathbf{x} \neq \mathbf{y} \in \mathbb{F}_2^n$ we have

$$f(\mathbf{x}) = f(\mathbf{y}) \Leftrightarrow \mathbf{y} = \mathbf{x} + \mathbf{s}.$$

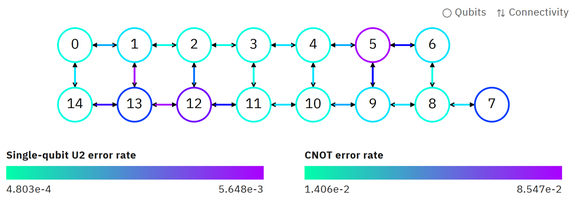
In *Simon's problem* we have to find $\mathbf{s}$ given oracle access to f.

It is well-known that Simon's algorithm finds $\mathbf{s}$ in time polynomial in n on quantum devices that are capable of performing error-correction.



IBM-Q16

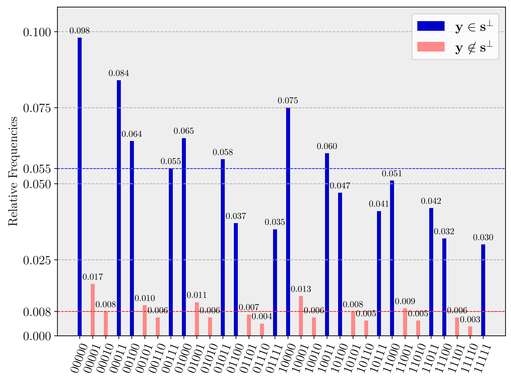
We ran our experiments on the IBM-Q16 Melbourne device, which (despite its name) realizes 15-qubit circuits. Further IBM-Q16 can only process 2-qubit gates on qubits that are adjacent in its topology graph. We adjusted our implementation of the Simon circuit accordingly.



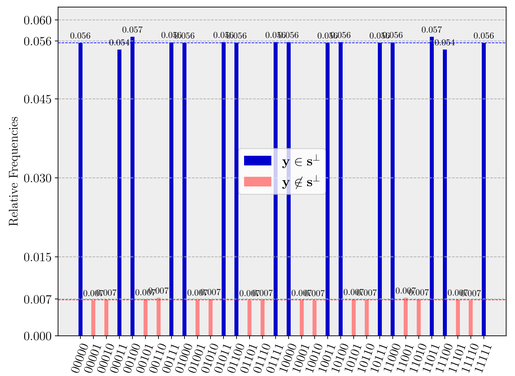
Conclusion

After smoothing, our noisy quantum device provides us a statistical distribution that we can easily transform into an LPN instance. Hence, in the noisy case we may not hope to find periods in time polynomial in n. However, we still obtain quantum advantage even for large errors $\tau(n)$ close to $\frac{1}{2}$. Thus, period finding does not necessarily require full quantum error correction capability.

Measurements



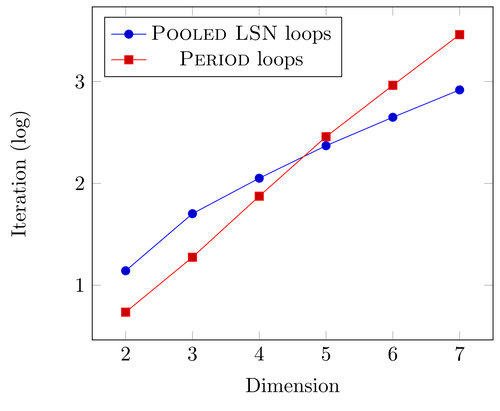
(a) Unsmoothed measurements, dim=5.



(b) Smoothed measurements, dim=5.

In the error free case, Simon's circuit produces vectors that are uniformly distributed. However, on IBM-Q16 this is not the case. First, IBM-Q16's qubits have different noise level, hence different reliability. Second, we experimentally observe vectors with small Hamming weight more frequently, the measured qubits have a bias towards 0. To mitigate both effects we introduce simple, but effective *smoothing techniques*. First, the quality of qubits can be averaged by introducing permutations that preserve the overall error probability τ. Second, the 0-bias can be removed by suitable addition of vectors, both quantumly and classically. In combination, our smoothing methods are effective in the sense that they provide a distribution where vectors orthogonal to $\mathbf{s}$ appear uniformly distributed with probability $1 - \tau$, and vectors not orthogonal to $\mathbf{s}$ appear uniformly distributed with probability τ, as seen above.

Runtime



We show that Pooled Gauss solves LSN for $\tau \leq 0.292$ faster than classical period finding algorithms. Well-Pooled Gauss even improves on any classical period finding algorithm for all errors $\tau < \frac{1}{2}$.
This indicates that we achieve *quantum advantage* for the Simon period finding problem on sufficiently large computers, even in the presence of errors: Our quantum oracle helps us in speeding up computation! But as opposed to the exponential speedup from the (unrealistic) error-free Simon setting $\tau = 0$, we obtain in the practically relevant noisy Simon setting $0 < \tau < \frac{1}{2}$ only a *polynomial speedup*.
The diagram (left) compares the runtime of an optimal classical algorithm (red) and a quantum-supported algorithm (blue) with smoothed measurements. In both cases, the iteration number of the main loop was measured, which determines the asymptotic runtime, ignoring all polynomial factors (the polynomial factors actually dominate in practice for our small considered dimensions).

As expected, the experimental runtime exponent of the classical algorithm (red) is $\frac{n}{2}$. For the quantum-supported algorithm (blue), we obtain an experimental regression line of roughly $\frac{n}{3}$, where the slope seems to decrease with n. This results in a cut-off point for the loop numbers between $n = 4$ and $n = 5$. So experimentally, IBM-Q16 's error rate $\tau(n)$ increases slowly enough to allow for quantum advantage, at least for our loop cost measure. We expect a real quantum advantage around dimension 50.

LSN∼LPN

We show that solving LSN with parameters n, τ is tightly polynomial time equivalent to solving the famous *Learning Parity with Noise* (LPN) problem with the same parameters n, τ. The core of our reduction shows that LSN samples coming from smoothed quantum measurements of Simon's circuit can be turned into perfectly distributed LPN samples, and vice versa.

Example

Let us illustrate the quantum advantage with an example. Assume that one could build a quantum device with 486 qubits performing Simon's circuit on a 243-bit periodic function with error $\tau = \frac{1}{8}$. Then our classical error handling of the noisy quantum data would translate into an LPN-instance with $(n, \tau) = (243, \frac{1}{8})$. Such an LPN instance was solved in [3] on 64 threads in only 15 days, whereas classically period finding would require 2^{121} steps.

References

[1] 15-qubit backend: IBM Q team, "IBM Q 16 Melbourne backend specification V2.0.1," (2020). Retrieved from https://quantum-computing.ibm.com. Accessed 14. January 2020.

[2] All measurements, configurations, backend properties and used mappings can be found in https://github.com/Quantum-Research/Advantage-for-Period-Finding-even-on-Noisy-Intermediate-Scale-Quantum-Devices in the format provided by Qiskit.

[3] Esser, A., Kübler, R., May, A.: LPN decoded. pp. 486--514 (2017)

[4] May, A., Schlieper, L., Schwinger, J.: Noisy simon period finding (2019), https://arxiv.org/abs/1910.00802

Acknowledgements

We acknowledge use of the IBM Q for this work. The views expressed are those of the authors and do not reflect the official policy or position of IBM or the IBM Q team.

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES