Quantum Period Finding is Compression Robust

Alexander May, Lars Schlieper
Ruhr-University Bochum

arXiv:1905.10074

Simon's Institute – Feb 2020

Compression and Error Tolerance

Current status: Quantum devices

- have low qubit numbers,
- are noisy.

Research challenges:

- Can we design low qubit algorithms?
- Are noisy quantum devices useful without error correction?

Simon's problem

Simon problem

Given: $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ with $f(x) = f(y) \Leftrightarrow y \in \{x, x+s\}$

Find: period $s \in \mathbb{F}_2^n \setminus \vec{0}$

- Classically: Requires collision, $\Omega(2^{n/2})$.
- Many applications in symmetric cryptanalysis.

Quantum circuit

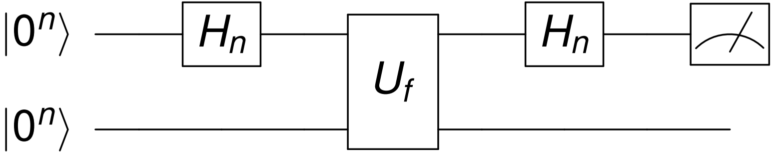


Figure: Simon's circuit

- After $U_f : |x\rangle |y\rangle \to |x\rangle |y + f(x)\rangle$, we obtain

$$\sum_{x \in \{0,1\}^n} (|x\rangle + |x + s\rangle) |f(x)\rangle$$

- Eventually:

$$\sum_{x \in \{0,1\}^n} \sum_{\langle y,s \rangle = 0} |y\rangle |f(x)\rangle$$

- After $\mathcal{O}(n)$ measurements: basis of the subspace $s^{\perp}$.
- Requires $2n$ qubits. (but we measure only n)

Example Simon

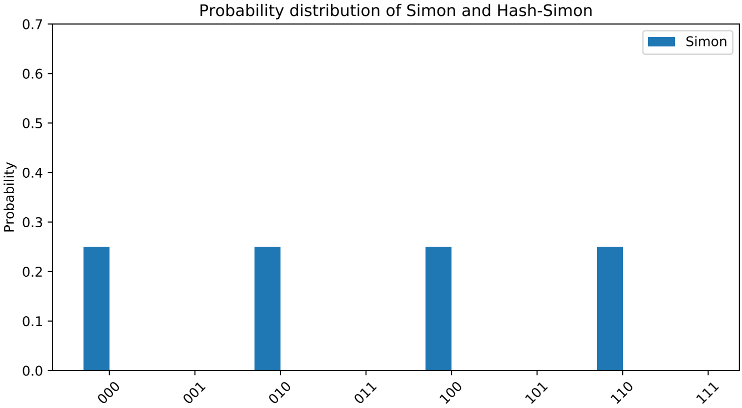
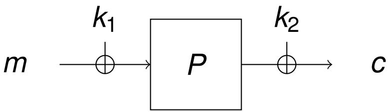


Figure: Period $s = 001$.

Even-Mansour application



Attacking Even-Mansour

- Idea of Kuwakado, Morii ('12):

$$f(x) = \mathrm{EM}(x) + P(x) = P(x + k_1) + k_2 + P(x)$$

- Observation:

$$f(x + k_1) = f(x)$$

- Period k_1, but no Simon promise

$$f(x) = f(y) \not\Rightarrow y \in \{x, x + k_1\}.$$

- Kaplan, Leurent, Leverrier, Naya-Plasencia ('16), Santoli, Schaffner ('17), Leander, May ('17):

Missing promise (only) implies (some) more measurements.

Our idea

Main idea for saving output qubits.

- Let us hash $f(x)$ downto some bits, e.g. to a single bit. Take

$$h : \mathbb{F}_2^n \to \mathbb{F}_2, f(x) \mapsto h(f(x))$$

  from some universal hash function family $\mathcal{H}$.
- Observation:

$$f(x) = f(y) \Rightarrow h(f(x)) = h(f(y)).$$

- **But many** undesired collisions!

Our Oracle Model (for now):

- We get $U_{h \circ f}$ for many h.
- Not clear that $h \circ f : \mathbb{F}_2^n \to \mathbb{F}_2$ can be realized memory efficient.
- **Not sufficient:** Compute first f, then compute h.

Hashing Simon's algorithm

Hashed Simon

Input: $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$, $\mathcal{H} := \{h : \mathbb{F}_2^n \to \mathbb{F}_2\}$
Output: s

1. Set $Y = \emptyset$.
2. **Repeat**
   1. $y \leftarrow$ Measure $Q_{h\circ f}^{Simon}$ on $|0^n\rangle\,|0\rangle$ for some freshly chosen $h \in_R \mathcal{H}$.
   2. If $y \notin \mathrm{span}(Y)$, then include y in Y.
3. **Until** Y contains $n-1$ linearly independent vectors
4. Compute $\{s\}$ as $Y^\perp$ via Gaussian elimination.

Hashed Simon

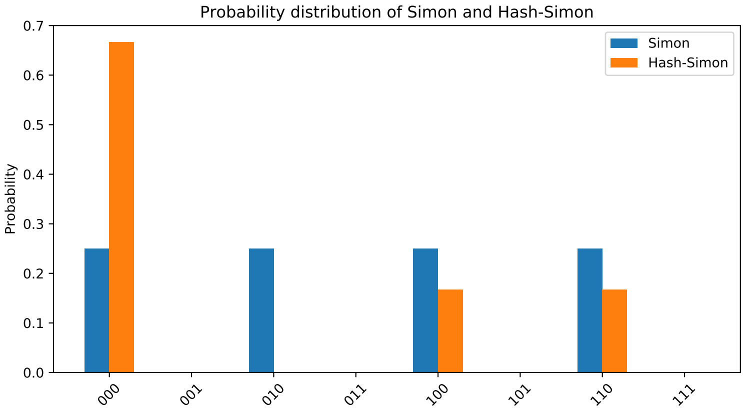


Figure: Period $s = 001$.

Hashed Simon

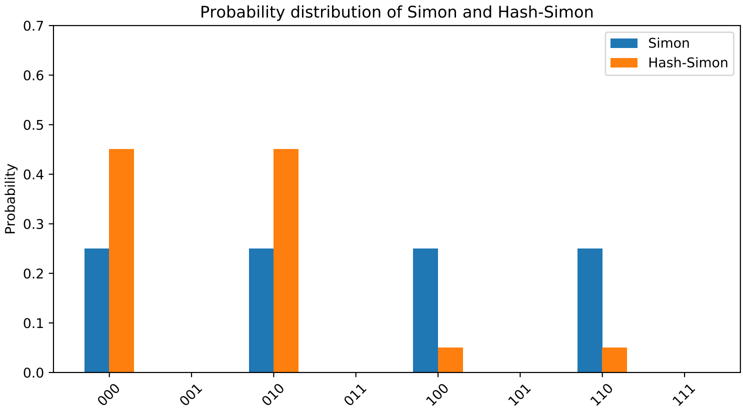


Figure: Period $s = 001$.

Hashed Simon

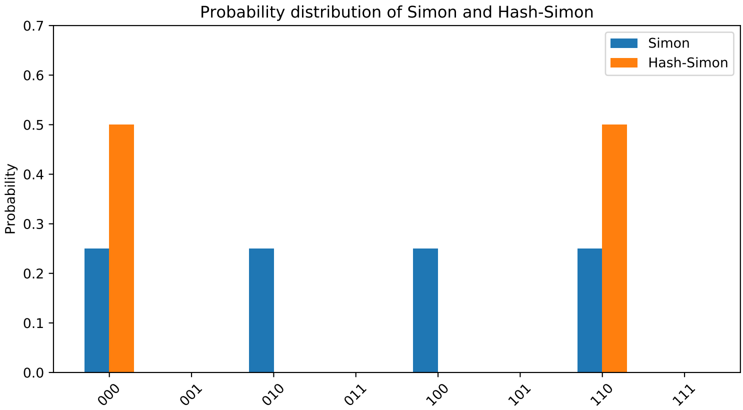


Figure: Period $s = 001$.

Hashed Simon

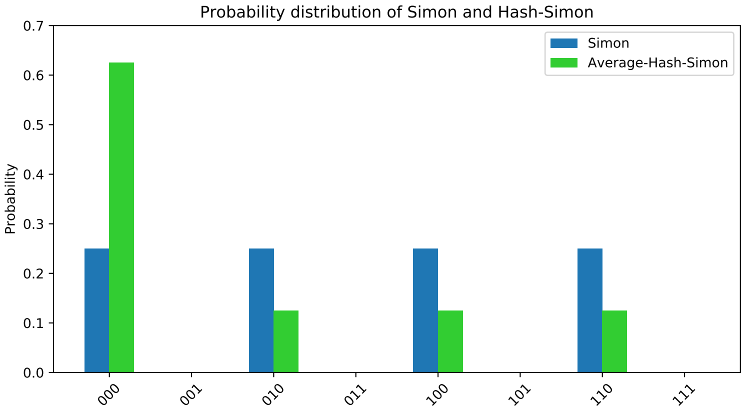


Figure: Period $s = 001$.

Theorems

Theorem (Orthogonality)

Only states y with $\langle y, s \rangle = 0$ *have non-zero amplitude.*

As in Simon.

Theorem (Amplitudes)

We measure each $y \neq 0$ *with probability* $\frac{1}{2^n}$.

Compared to $\frac{1}{2^{n-1}}$.

Theorem (Measurements)

Hashed-Simon succeeds with $2(n+1)$ *measurements.*

Compared to $n+1$, but we reduce qubits from $2n$ to $n+1$.

Even-Mansour Application

Recall Even-Mansour function

$$f(x) = P(x) + \mathrm{EM}(x).$$

We use a linear hash function family

$$\mathcal{H} : x \mapsto \langle x, r \rangle \text{ for } r \in \mathbb{F}_2^n.$$

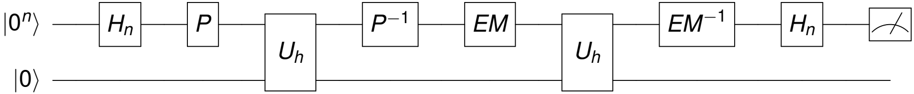


Figure: HASHED-SIMON on Even-Mansour with $n + 1$ qubits

Correctness:

$$h(P(x)) + h(EM(x)) = h(f(x))$$

What about factoring?

Let $f(x) = a^x \bmod N$ with $n = \log_2 N$.

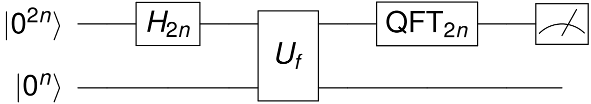


Figure: Shor's circuit

Input bit size:

Shor (1994):	$2n$	
Seifert (2001):	$(1 + o(1))n$	
Ekerå, Håstad (2017):	$(\frac{1}{2} + o(1))n$	(for RSA moduli)
Mosca, Ekert (1998):	1	

Shor Unhashed

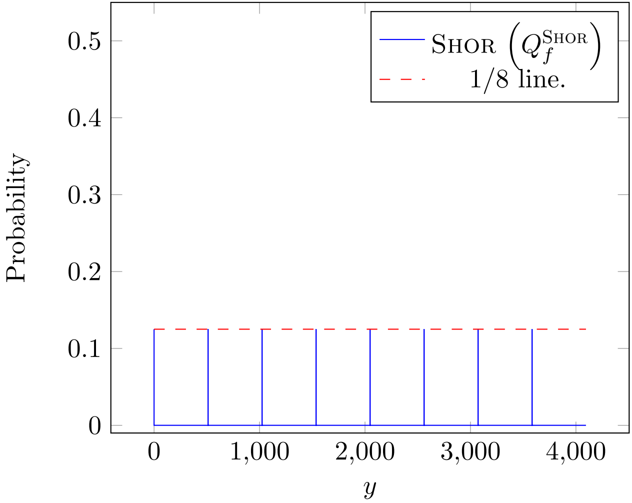


Figure: Period $s = 8$, $q = 12$ qubits.

Hashed Shor

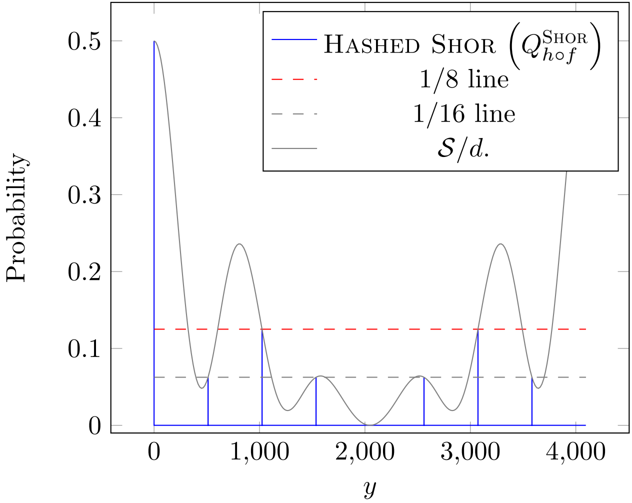


Figure: Period $s = 8$, $q = 12$ qubits.

Theorems

Theorem (Orthogonality)

Only y that are multiples of $\frac{2^q}{s}$ have non-zero amplitude.

Just as before.

Theorem (Amplitudes)

We measure each $y \neq 0$ with probability $\frac{1}{2s}$.

Instead of $\frac{1}{s}$.

Theorem (Measurements)

Hashed-Shor succeeds with 4 measurements.

Instead of 2.

Question: Can we also instantiate $U_{h \circ f}$?

Mosca-Ekert 1998

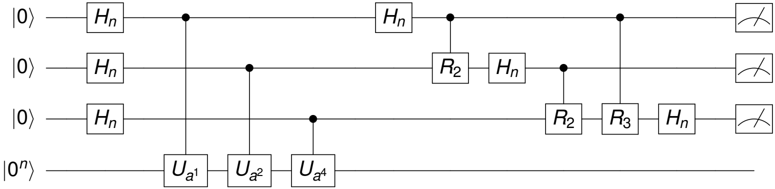


Figure: Shor's circuit.

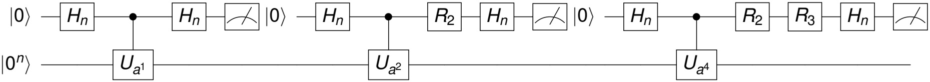


Figure: Mosca-Ekert circuit.

Why not only 2 qubits?

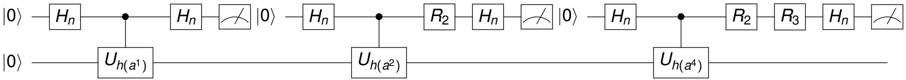


Figure: Quantum circuit with two bit.

- Requires $h(a^1) \cdot h(a^2) \cdot h(a^4) = h(a^1 \cdot a^2 \cdot a^4)$.
- Well, take for instance

$$h : \mathbb{Z}_N^* \to \{-1, 1\}, a^x \mapsto \left(\frac{a^x}{N}\right).$$

(Warning: Does not work!)

Theorem

If there exists an efficiently computable universal homomorphic hash function family $h : \mathbb{Z}_N^* \to \{0,1\}^t$ then we can factor with $t+1$ qubits. (in the oracle model only)

Summary

- Hashing preserves probability distribution (conditioned on $y \neq 0$).
- Reduces output qubits significantly, basically at no cost.
- Leads to clean results in oracle model for period finding.
- Is useful for problems of interest (Even-Mansour).
- Leads to interesting open problems (factoring, dlog).