Cost estimates for quantum preimage attacks

Matt Amy, Olivia Di Matteo, Vlad Gheorghiu, Michele Mosca,
Alex Parent, John Schanck

Institute for Quantum Computing
University of Waterloo

February 26, 2016

Given a bijection

$$\mathsf{H} : \{0,1\}^k \to \{0,1\}^k,$$

Grover's algorithm finds the preimage of

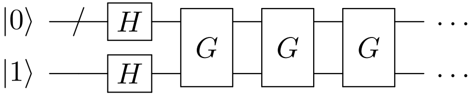
$$y \in \{0,1\}^k$$

using $\Theta(\sqrt{2^k})$ queries to an oracle that computes

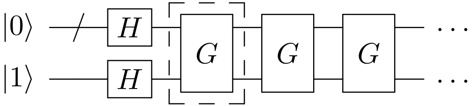
$$\begin{aligned} f : \{0,1\}^k &\to \{0,1\} \\ x &\mapsto \delta(\mathsf{H}(x), y). \end{aligned}$$

To estimate the cost of Grover's algorithm. . .

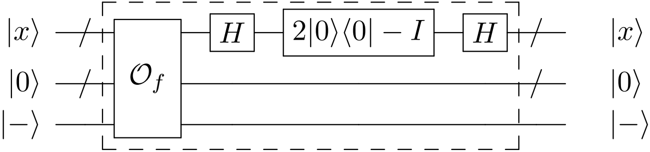
Write down a circuit.



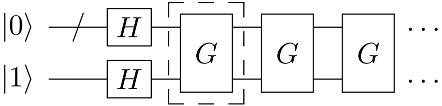
To estimate the cost of Grover's algorithm...



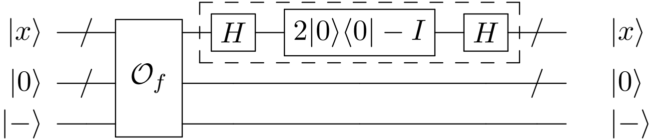
You'll need the cost of one Grover iteration



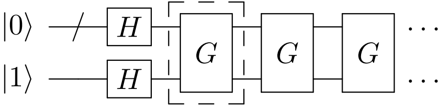
To estimate the cost of Grover's algorithm...



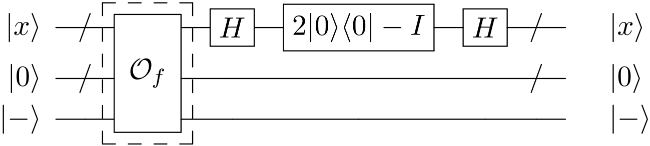
i.e. the diffusion operator



To estimate the cost of Grover's algorithm...

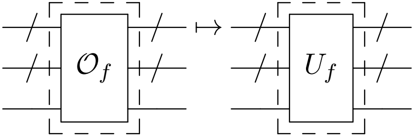


and the oracle.



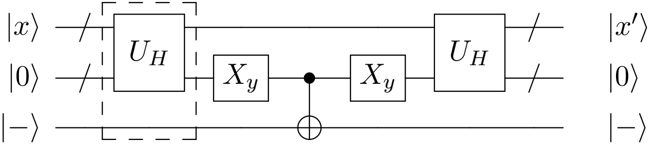
To estimate the cost of Grover's algorithm. . .

The oracle needs to be instantiated

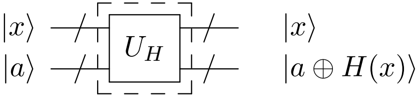


To estimate the cost of Grover's algorithm...

The oracle needs to be instantiated



with a reversible implementation of H.



The logical layer

1. Compile to a universal gate set (Clifford+T)
2. Optimize the circuit (minimize T-count)

Our contribution:

1. T-count optimized reversible implementations of SHA-2 and SHA-3 functions.

	#gates		depth		#qubits
	T	Clifford	T	overall	
SHA-256	193,280	4,510,960	88,256	830,720	2,337
SHAKE-256	499,200	34,030,165	576	9,112	3,200

The fault-tolerant layer

> *Without significant future effort, the classical processing will almost certainly limit the speed of any quantum computer, particularly one with intrinsically fast quantum gates.*

[1] Fowler, Whiteside, Hollenberg. "Towards practical classical processing for the surface code: timing analysis." 2012

The fault-tolerant layer

Our contribution:

2. Cost model for comparing Grover against classical brute force search.

The fault-tolerant layer

1. Assume surface code quantum computing.
2. Estimate additional resources required by fault tolerance layer, e.g. magic state distillation factories.
3. Cost only the classical resources.
4. Assume 1 classical core per logical qubit.
5. Assume 1 surface code cycle ≈ 1 application of H.
6. Compute cost as surface code cycles $\times$ logical qubits.

The fault-tolerant layer

See our forthcoming paper for details.

Thanks!