Developing a quantum circuit for efficiently identifying D-optimal sequences

by Scott King
supervised by Shohini Ghose and Ilias Kotsireas, Wilfrid Laurier University
25th March 2018

Department of Physics and Computer Science
Wilfrid Laurier University
Waterloo, Ontario, Canada

CARGO Research Lab
Wilfrid Laurier University
Waterloo, Ontario, Canada

Abstract

Quantum computing provides a computation model, based on quantum mechanics, that changes the way we process and interpret information. By utilizing the rules and phenomena of quantum mechanics, algorithms have been developed to solve problems faster and more efficiently than they have been done before.

Specifically, I will investigate **Grover's search algorithm** [2], which performs a sublinear-time search.

This research aims to define a quantum algorithm and corresponding circuit that is able to more efficiently find D-optimal sequences.

1 Introduction

1.1 Quantum computing fundamentals

Classical computing, as we know it, is built on a system of bits, that, at any given time are 0 or 1 and act as the basis of states within the system.

What about quantum computing?

- A quantum computer operates on a set of quantum bits, are known as *qubits*
- A qubit can be denoted as: $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$
- The quantum state of a qubit can be thought of as a probability where: $|\alpha|^2$ and $|\beta|^2$ are the probabilities of being a 0 or 1, respectively

We can visualize this using the *Bloch sphere*:

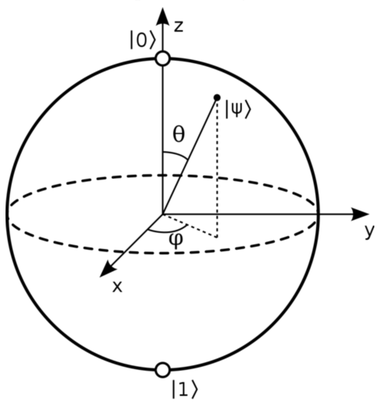

Figure 1: Qubit visualization with Bloch sphere

Any point that can be shown on the Bloch sphere represents a qubit's probability of being 0 or 1; with the positive Z-axis being the classical value of 0 and the negative Z-axis being the classical value 1.

1.2 Combinatorial search

- Combinatorial search explores hard problems that usually have a large solution space
- A D-optimal design can be thought out as a pair of sequences of length n (where n is odd), A and B, such that $\forall\, i \in \{-1, 1\}$, can be used to construct a $2N \times 2N$ matrix that has the maximum possible determinant [1]:

$$H = \begin{pmatrix} A & B \\ -B^T & -A^T \end{pmatrix}$$

- Search for D-optimal sequences of length N scales exponentially and results in heavy computational load
- Each sequence candidate is verified individually using a sum of *periodic correlation functions* (PAFs)
- The PAF for a given sequence, A, is: $P_A(s) = \sum_{k=1}^{N} a_k a_{k+s}$, where the lag $s = 1, ..., \frac{N-1}{2}$

$$P_A(s) + P_B(s) = 2, \qquad \forall\, i = 1, ..., \frac{N-1}{2} \tag{1}$$

PAF constraint for D-optimal sequence classification

2 Quantum search and Grover

Let's start with a system of n qubits, which yield 2^n possible sequences.

1. Setup the search with n qubits in starting state: $|\psi\rangle = |00...0\rangle$.
2. Put all the qubits in a state of superposition, which for a time, gives an equal probability to each solution. To do this, use a Hadamard gate on all qubits. On one qubit, it does the following: $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. When applying Hadamard gates to all qubits, use the following format:

$$H_N ... H_1 |x_n ... x_1\rangle = \frac{1}{2^{n/2}} \sum_{i=0}^{N-1} (-1)^{-i \cdot x} |x\rangle \tag{2}$$

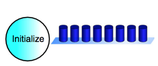

Figure 2: The state after Hadamard gates are applied [3]

The next steps are considered part of the "Grover iteration", which gets applied $(\frac{pi}{4})\sqrt{N}$ times.

3. Apply a unitary operator, known as an *oracle*, to the the state that flips each state based on function present in the oracle, in the case the PAF constraint.

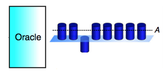

Figure 3: Applying the oracle to flip prababilities [3]

4. Next, we apply the diffusion operator. This step is the clever trick for Grover's operation. This will invert these flipped solutions over the mean and show the answers that are more than likely correct.

Figure 4: Inversion about the mean [3]

5. The final step is a set operations aimed at "amplifying" the solutions that get inverted about the mean. In combination with multiple iterations, we'd be able to measure the qubits at the end and be fairly certain we have the correct candidates from the search.

3 Bridging the gap

3.1 Quantum combinatorial search

- Quantum computing lends itself nicely to various disciplines including cryptography and search
- Performance increases yield more than polynomial speedup

Due to the underlying properties that are standard with working in a quantum environment, the barriers for solving combinatorial problems of a large N are lessened. Within the system, we are able to operate on all the possible solutions at once and avoid any lengthy brute-force iterations.

3.2 Quantum algorithm implementation

The ideas for the algorithm we've built up so far get implemented by way of a *quantum circuit*.

Let's visualize a Grover search circuit for finding D-optimal sequences of length $n = 3$, totalling 7 qubits: 6 for input, 1 for output.

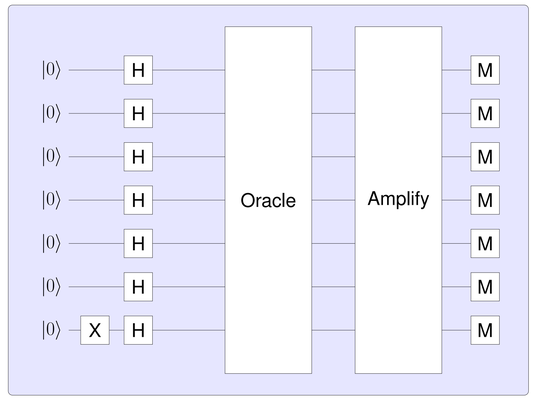

Figure 5: High level implementation of the quantum circuit for $n = 3$. *Note*: The oracle and amplification phases will be performed multiple times.

Conclusion

Lastly, detailed gates that represent the PAF oracle for finding D-optimal matrices have been developed for the case of $n = 3$, as a proof of concept and will be optimized for values of $n > 3$.

One of the unsolved combinatorial search problems right now, is finding D-optimal sequences for $n = 99$, where the search space is 2^{198}. Pending that status of a computer that has support for 198 qubits, this circuit could be used to find such sequences.

Acknowledgements

I'd like to thank Dr. Ghose and Dr. Kotsireas for giving me the privilege of working with them and advising me over the months. I'd like to thank George Liftchits for whom this research extends.

References

[1] G. Lifchits. D-optimal grover search. December 2015.

[2] Lov K. Grover. A fast quantum mechanical algorithm for database search. December 1996.

[3] K. A. Landsman N. M. Linke S. Debnath C. Figgatt, D. Maslov and C. Monroe. Complete 3-qubit grover search on a programmable quantum computer. December 2017.