Quantum Algorithm for Roots of Multivariate Functions Over Finite Fields

Project Statement

Alexander J. Heilman & Andy Phillips

October 8, 2021

Overview

- We can encode multivariate finite functions over finite fields in multi-qudit quantum states [3]

Overview

- We can encode multivariate finite functions over finite fields in multi-qudit quantum states [3]
- Relatively new generalizations of Grover's search algorithm apply to multi-valued functions [2][1]

Overview

- We can encode multivariate finite functions over finite fields in multi-qudit quantum states [3]
- Relatively new generalizations of Grover's search algorithm apply to multi-valued functions [2][1]
- Application of multi-valued search algorithms to the known encoding should facilitate the evaluation of roots

Overview

- We can encode multivariate finite functions over finite fields in multi-qudit quantum states [3]
- Relatively new generalizations of Grover's search algorithm apply to multi-valued functions [2][1]
- Application of multi-valued search algorithms to the known encoding should facilitate the evaluation of roots
- Google's Cirq SDK allows simulation of qudit circuits

Finite Function Encoding States

Given an n-qu$d$it system, where d is prime, we can encode an n-variable finite function over the field $\mathbb{F}_d$ in the amplitude of the basis states.

$$|f(x_n)\rangle \rightarrow \frac{1}{\sqrt{d^n}} \sum_{k=0}^{d^n-1} \omega_d^{f(k)} |k\rangle$$

Finite Function Encoding States Ex.

Let's look at a very simple case of two qutrits (i.e. $d = 3$). We can encode the polynomial function $xy^2 + x$ over the field $\mathbb{F}_d$ (i.e. the field with three elements, $0, 1, 2$) as follows:

$$\frac{1}{\sqrt{9}} \sum_{k=0}^{9} \omega^{xy^2+x} |k\rangle$$

$$= \frac{1}{3}(\omega^{0 \cdot 0^2+0} |00\rangle$$

Finite Function Encoding States Ex.

Let's look at a very simple case of two qutrits (i.e. $d = 3$). We can encode the polynomial function $xy^2 + x$ over the field $\mathbb{F}_d$ (i.e. the field with three elements, $0, 1, 2$) as follows:

$$\frac{1}{\sqrt{9}} \sum_{k=0}^{9} \omega^{xy^2+x} |k\rangle$$

$$= \frac{1}{3}(\omega^{0 \cdot 0^2+0}|00\rangle + \omega^{0 \cdot 1^2+0}|01\rangle$$

Finite Function Encoding States Ex.

Let's look at a very simple case of two qutrits (i.e. $d = 3$). We can encode the polynomial function $xy^2 + x$ over the field $\mathbb{F}_d$ (i.e. the field with three elements, $0, 1, 2$) as follows:

$$\frac{1}{\sqrt{9}} \sum_{k=0}^{9} \omega^{xy^2+x} |k\rangle$$

$$= \frac{1}{3}(\omega^{0\cdot 0^2+0}|00\rangle + \omega^{0\cdot 1^2+0}|01\rangle + \omega^{0\cdot 2^2+0}|02\rangle + \omega^{1\cdot 0^2+1}|10\rangle + \omega^{1\cdot 1^2+1}|11\rangle + \omega^{1\cdot 2^2+1}|12\rangle + \omega^{2\cdot 0^2+2}|20\rangle + \omega^{2\cdot 1^2+2}|21\rangle + \omega^{2\cdot 2^2+2}|22\rangle)$$

$$= \frac{1}{3}(|00\rangle + |01\rangle + |02\rangle + \omega|10\rangle + \omega^2|11\rangle + \omega^2|12\rangle + \omega^2|20\rangle + \omega|21\rangle + \omega|22\rangle)$$

$xy^2 + x$ Example cont.

$$|xy^2 + x\rangle = \begin{array}{cc} xy & \omega^{xy^2+x} \\ |00\rangle & \left[\begin{array}{c} 1 \\ 1 \\ 1 \\ \omega \\ \omega^2 \\ \omega^2 \\ \omega^2 \\ \omega \\ \omega \end{array}\right] \\ |01\rangle & \\ |02\rangle & \\ |10\rangle & \\ |11\rangle & \\ |12\rangle & \\ |20\rangle & \\ |21\rangle & \\ |22\rangle & \end{array}$$

Multi-Valued Grover Search

The typical Grover search algorithm is effectively used to find a set of basis states marked in a complete superposition of basis states by a relative amplitude of -1.

Multi-Valued Grover Search

The typical Grover search algorithm is effectively used to find a set of basis states marked in a complete superposition of basis states by a relative amplitude of -1.

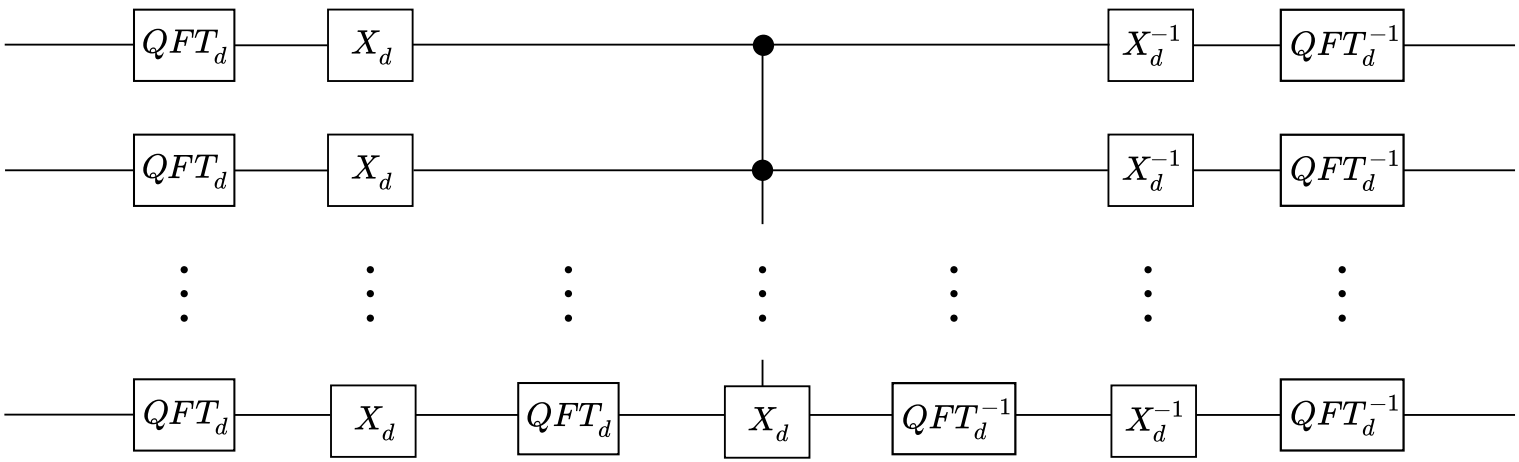
A generalization of this is to find basis states marked with one of many relative amplitudes, which if equally spaced are the roots of unity $\omega_d = e^{2\pi i/d}$

Multi-Valued Grover Search

Maximilian Hunt and Samuel Hunt have recently published *Grovers Algorithm and Many-Valued Quantum Logic* (December 2020, [2]).

Multi-Valued Grover Search

Maximilian Hunt and Samuel Hunt have recently published *Grovers Algorithm and Many-Valued Quantum Logic* (December 2020, [2]).They generalize the Grover diffusion operator to qudits and multi-valued functions using the circuit below:



For gates see `https://alexheilman.com/qis/qudits.html`

Goals/Expected Problems

- Grover's search generally only works for sparse databases

Goals/Expected Problems

- Grover's search generally only works for sparse databases, those are collections where the solutions are a minority of the population

Goals/Expected Problems

- Grover's search generally only works for sparse databases, those are collections where the solutions are a minority of the population
- We should be able to at least count the number of roots using a generalized counting/amplitude estimation scheme

Next Steps

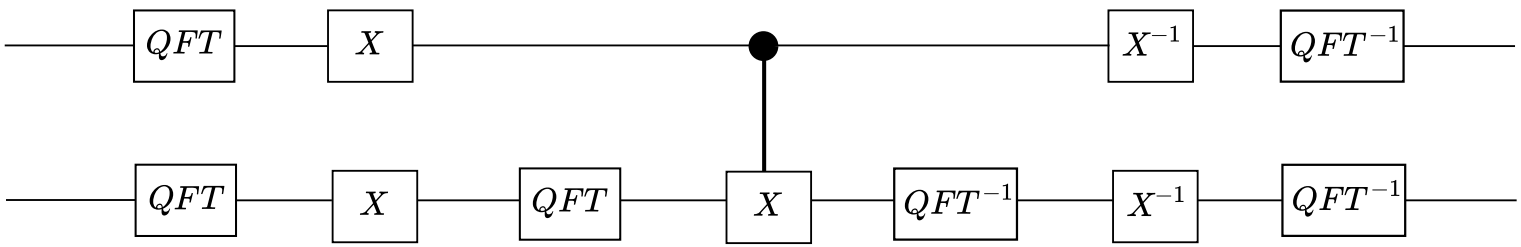
- Better understand multi-valued Grover search

Next Steps

- Better understand multi-valued Grover search
- Implement examples in Cirq simulations and get hands on

Next Steps

- Better understand multi-valued Grover search
- Implement examples in Cirq simulations and get hands on, specifically for the state from above and the 2-qutrit GGDO:



References I

[1] Yale Fan. "Applications of multi-valued quantum algorithms". In: *arXiv preprint arXiv:0809.0932* (2008).

[2] Samuel Hunt and Maximilien Gadouleau. "Grover's Algorithm and Many-Valued Quantum Logic". In: *arXiv preprint arXiv:2001.06316* (2020).

[3] Paul Appel, Alexander J Heilman, Ezekiel W Wertz, et al. "Finite-Function-Encoding Quantum States". In: *arXiv preprint arXiv:2012.00490* (2020).