(ADAPTIVE) GROVER FIXED-POINT SEARCH FOR BINARY OPTIMIZATION PROBLEMS

ATITHI ACHARYA, ÁKOS NAGY, JAIME PARK, AND CINDY ZHANG

ABSTRACT. *to be completed later...*

1. INTRODUCTION

to be completed later...

Organization of the paper:

to be completed later...

2. (POLYNOMIAL UNCONSTRAINED) BINARY OPTIMIZATION

For the rest of the paper, $\mathbb{Z}_2^n$ denotes the space of length-n bitstrings. Given a function $f : \mathbb{Z}_2^n \to \mathbb{R}$, the associated (Unconstrained) Binary Optimization problem is the task of finding an element $x \in \mathbb{Z}_2^n$ such that $f(x)$ is maximal. Note that every binary function is polynomial, which can be seen by simple dimension count.

Many interesting Binary Optimization problems, such as finding maximal graph cuts or the Max 2-SAT problems are quadratic, and most of the contemporary research centers around Quadratic Unconstrained Binary Optimization (QUBO) problems. Hence, while our results and circuit designs apply to any binary functions, we use QUBO problems as examples. Furthermore, dealing with higher degree problems require more complicated circuits which makes them more prone to noise (and thus are less NISQ-y).

2.1. **Quantum Dictionaries.**

The first main contribution of the paper is an oracle design for encoding operators of (arbitrary) *quantum dictionaries*, as introduced in [1]. While such designs have already existed, cf. [2], ours has improved circuit depth, gate count, and CNOT count. Such oracles have applications, for example, in Grover type algorithms and threshold-QAOA [3].

Briefly, the quantum dictionary, corresponding to a function (thought of as a classical dictionary), $F : \mathrm{dom}(F) \to \mathbb{Z}_2^d$, where $\mathrm{dom}(F) \subseteq \mathbb{Z}_2^n$, is the following quantum state on $n+d$ qubits:

$$|\mathrm{QDICT}(F)\rangle := \frac{1}{\sqrt{|\mathrm{dom}(F)|}} \sum_{x \in \mathrm{dom}(F)} |x\rangle_n |F(x)\rangle_d.$$

Date: August 30, 2023.
Key words and phrases. Grover Fixed-point Search, Binary Optimization.

Note that an integer-valued function $f : \mathbb{Z}_n^2 \to \mathbb{Z}$ canonically determines a quantum dictionary via first defining $F(x)$ to be the digits of $f(x)$, then setting, by a slight abuse of notation, $\left|\textsc{qdict}\left(f\right)\right\rangle = |\textsc{qdict}(F)\rangle$. We handle signs via the "Two's complement" convention, in particular, a binary number $y_0 y_1 \dots y_{d-1}$ is negative exactly when $y_0 = 1$. In fact, every quantum dictionary can be realized in such a way. Since rational-valued functions can be handled similarly and real-valued functions can be approximated to arbitrary precision by rational ones, this construction can be used to encode (approximate) values of of arbitrary binary functions which, in Section 3, we use to give a concrete implementation of the Grover Fixed-point search for QUBO problems.

We construct these operators in three steps. First, we outline a modified version of the encoding operator given in [2] that is convenient to encode monomials, $x_{i_1} x_{i_2} \cdots x_{i_j}$. Then we show that every binary function can be rewritten in a basis of functions that can be more efficiently encoded then monomials. Finally, we modify the encoding operators of [2] to apply for our new basis.

2.2. **Polynomial encoder.** Let $I \subseteq \{1, 2, \dots, n-1\}$ and $x_I := x_{i_1} x_{i_2} \cdots x_{i_j}$ be an arbitrary monomial and consider a quantum circuit with $n+d$ registers. Following [2], we construct an oracle that sends $|x\rangle_n |0\rangle_d$ to $|x\rangle_n |x_I\rangle_d$, for any $x \in \mathbb{Z}_2^n$.

Let us make two definitions: Let QFT_d be the Quantum Fourier Transform on m qubits, that is for any $-2^{d-1} \leqslant y < 2^{d-1}$, we have

$$\mathrm{QFT}_d \left|y\right\rangle_d = 2^{-\frac{m}{2}} \sum_{z=-2^{d-1}}^{2^{d-1}-1} e^{\frac{2\pi y z}{2^d} i} |z\rangle_d.$$

Then

$$\mathrm{QFT}_d^\dagger |z\rangle_d = 2^{-\frac{d}{2}} \sum_{y'=-2^{d-1}}^{2^{d-1}-1} e^{-\frac{2\pi y' z}{2^d} i} \left|y'\right\rangle_d.$$

Now let $\mathscr{P}_d(k)$ be the following m-qubit gate

$$\begin{aligned}
|z_0\rangle &\text{ —— } \boxed{\textsc{phase}(\pi k)} \text{ —— } e^{\frac{2\pi k z_0 2^{d-1}}{2^d} i} |z_1\rangle \\
&\vdots \\
\left|z_j\right\rangle &\text{ —— } \boxed{\textsc{phase}\left(\frac{2\pi k}{2^{j+1}}\right)} \text{ —— } e^{\frac{2\pi z_j 2^{m-j-1}}{2^d}} \left|z_j\right\rangle \\
&\vdots \\
|z_{m-1}\rangle &\text{ —— } \boxed{\textsc{phase}\left(\frac{2\pi k}{2^d}\right)} \text{ —— } e^{\frac{2\pi k z_{m-1}}{2^d} i} |z_d\rangle
\end{aligned}$$

Thus $\mathscr{P}_d(k)|z\rangle_d = e^{\frac{2\pi kz}{2^d}i}|z\rangle_d$.

Now we can prove a well-known lemma. citation needed

Lemma 2.1. *For any $-2^{d-1} \leqslant y < 2^{d-1}$ and $k \in \mathbb{Z}$ we have*

$$\mathrm{QFT}_d^\dagger \circ \mathscr{P}_d(k) \circ \mathrm{QFT}_d \big|y\big\rangle_d = \Big|y + k \mod 2^{d-1}\Big\rangle.$$

Proof. First we compute

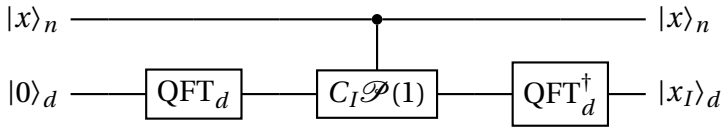
$$\begin{aligned}
\mathscr{P}_d(k) \circ \mathrm{QFT}_d \big|y\big\rangle_d &= \mathscr{P}(k)\left(2^{-\frac{m}{2}} \sum_{z=-2^{d-1}}^{2^{d-1}-1} e^{\frac{2\pi yz}{2^d}i}|z\rangle_d\right) \\
&= 2^{-\frac{d}{2}} \sum_{z=-2^{d-1}}^{2^{d-1}-1} e^{\frac{2\pi yz}{2^d}i}\mathscr{P}(k)|z\rangle_d \\
&= 2^{-\frac{d}{2}} \sum_{z=-2^{d-1}}^{2^{d-1}-1} e^{\frac{2\pi (y+k)z}{2^d}i}|z\rangle_d \\
&= \mathrm{QFT}_d \Big|y + k \mod 2^{d-1}\Big\rangle,
\end{aligned}$$

hence

$$\mathrm{QFT}_d^\dagger \circ \mathscr{P}(k) \circ \mathrm{QFT}_d \big|y\big\rangle_d = \Big|y + k \mod 2^{d-1}\Big\rangle.$$

□

By Lemma 2.1 it is immediate that



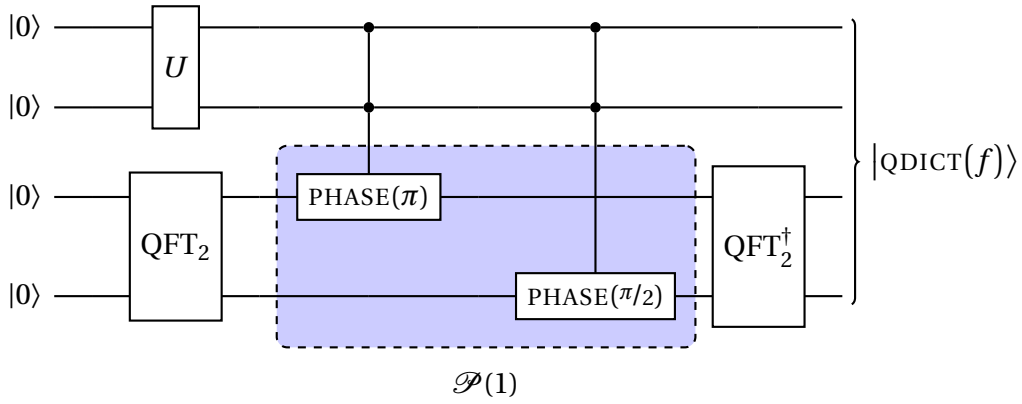
is the desired oracle, where C_I means control by the quantum registers $i_1, i_2, \ldots i_j$.

Finally, to create the full quantum dictionary, $\big|\mathrm{QDICT}(f)\big\rangle$, we need to pre-compose an oracle, call U, for which we have

$$U|0\rangle_n = \frac{1}{\sqrt{|\mathrm{dom}(f)|}} \sum_{x \in \mathrm{dom}(f)} |x\rangle_n.$$

If $\mathrm{dom}(f) = \mathbb{Z}_2^n$, then $U = H^{\otimes n}$.

Example 2.2. *Let $n = d = 2$ and $f(x) = x_0 x_1$. Now the encoder oracle takes the form*

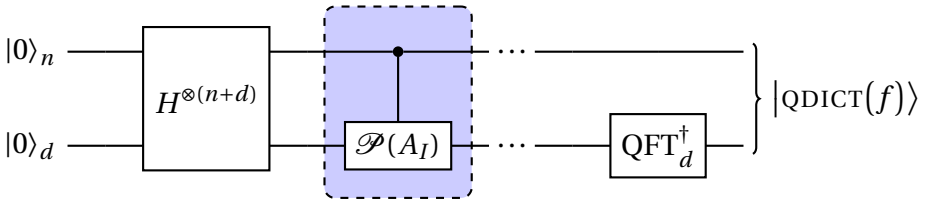


For the rest of the paper we assume that $\mathrm{dom}(f) = \mathbb{Z}_2^n$ and thus $U = H^{\otimes n}$. Furthermore, we note that $\mathrm{QFT}_d|0\rangle_d = H^{\otimes m}|0\rangle_d$ and thus we replace QFT_d with $H^{\otimes d}$ in the oracle, as the latter has depth 1 and uses only single-qubit gates.

Let $\mathbb{P}_n$ be the power set of $\{0, 1, \ldots, n-1\}$. Now, for an arbitrary polynomial,

$$f(x) = \sum_{I \in \mathbb{P}_n} A_I x^I,$$

and $d \in \mathbb{N}_+$ large enough so that all values of f can be digitized on m bits, we have that



one for each $I = \{i_1, i_2, \ldots, i_{|I|}\} \in \mathbb{P}_n$ with control registers being $x_{i_1}, x_{i_2}, \ldots, x_{i_{|I|}}$

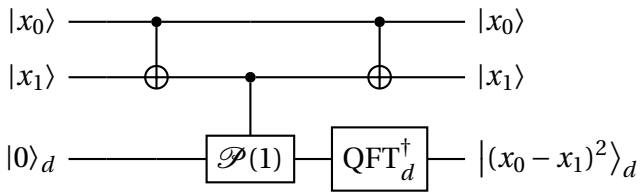
2.3. **New basis for polynomials.** We motivate the idea of the new basis by outlining it in the $n = 2$ case.

Note first that, since $x_i^2 = x_i$ for binary variables, we have that $x_0 x_1 = \frac{1}{2}\big(x_0 + x_1 - (x_0 - x_1)^2\big)$. Now $(x_0 - x_1)^2$ is also a binary variable, in fact, $(x_0 - x_1)^2 = x_0$ XOR x_1. Now let f be a generic polynomial, $f(x_0, x_1) = A_\emptyset + A_0 x_0 + A_1 x_1 + A_{01} x_0 x_1$. Since we are interested in finding the maximum of f, we can assume, without any loss of generality, that $f(0,0) = A_\emptyset = 0$. By generic we mean that $0 \notin \{A_0, A_1, A_{01}\}$. Using d digits, we need $2d$ CNOT gates for each linear terms and $6d$ CNOT gates for the quadratic term, thus a total of $10d$ CNOT gates (not counting the

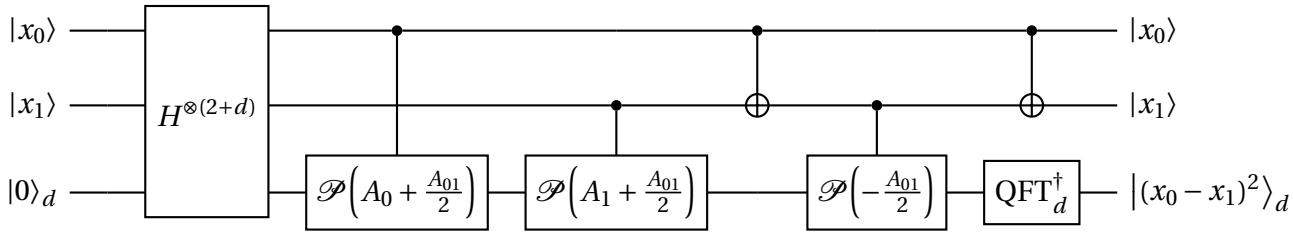
CNOT gates in $\mathrm{QFT}_d^\dagger$). However, we can rewrite f as

$$\begin{aligned} f(x_0,x_1) &= A_0x_0 + A_1x_1 + A_{01}x_0x_1 \\ &= \left(A_0 + \tfrac{1}{2}A_{01}\right)x_0 + \left(A_1 + \tfrac{1}{2}A_{01}\right)x_1 - \tfrac{1}{2}A_{01}(x_0 - x_1)^2, \end{aligned}$$

and note that the last term can be implemented as



which now has CNOT count only $2+2d$. Thus the whole oracle (for arbitrary f) can be realized as



making the new CNOT count for the whole oracle to be (at most) $2+6d$, again, not counting the CNOT gates in $\mathrm{QFT}_d^\dagger$. In fact, the only time the two counts equal is when $A_0 = A_1 = 0$, $A_{01} \neq 0$, and $d = 1$, that is, when middle of the oracle is a single doubly-controlled phase gate, in which case this construction recovers the well-known one; cf [4, Figure 4.8.].

3. Grover Fixed-point search for QUBO

Everything below is old stuff that I might or might not want to include.

Input: A symmetric, integer-valued, n-by-n matrix, Q and a constant $c \in \mathbb{Z}$, or, equivalently, a quadratic function on $x \in \{0,1\}^n$ given by

$$f(x) := x^T Q x + c. \tag{3.1}$$

(Note that since $x_i^2 = x_i$, we can move linear terms into the diagonal of Q.)

Output: An estimate for the value

$$M := \max\left(\{\ f(x) \ \middle|\ x \in \{0,1\}^n\ \}\right).$$

Example 3.1 (Maximal Graph Cuts)**.** *Given a simple, undirected graph, $G = (V,E)$, let Q be its graph Laplacian, defined as*

$$Q_{i,j} = \begin{cases} \deg(v_i), & \text{if } i = j, \\ -1, & \text{if } \{v_i, v_j\} \in E, \\ 0, & \text{otherwise,} \end{cases}$$

$b = 0$ and $c = 0$. Then $V = V^+ \coprod V^-$ is a maximal exactly when $\mathrm{MaxCut}(G) = f(x) = M$, where $x \in \{0,1\}^n$ is defined as $x_i = 1$ if $v_i \in V^+$ and zero otherwise.

The Edwards–Erdős bound yields

$$\mathrm{MaxCut}(G) \geqslant B_G := \begin{cases} \frac{2|V|+|E|-1}{4}, & \text{if (we know that) } G \text{ is connected,} \\ \frac{|V|}{2} + \sqrt{\frac{|V|}{8} + \frac{1}{64}} - \frac{1}{8}, & \text{otherwise.} \end{cases}$$

4. The oracles:

An element $x = (x_1, x_2, \ldots, x_n) \in \{0,1\}^n$ is also regarded as a binary number via $x \sim \overline{x_1 x_2 \ldots x_n} := \sum_i x_i 2^{n-i}$ and as an element of the computational basis via

$$|x\rangle_n := |x_1\rangle \ldots |x_{n-1}\rangle |x_n\rangle,$$

Given a function as in equation (3.1), let us pick $m \gg \log_2(M)$ (in fact, $m = \lceil \log_2(\mathrm{tr}(Q)) \rceil + 1$ works for our purposes). We use the binary 2s complement convention when digitizing integers and we with that in mind, we construct a oracle on $(n+m)$-qubits, U_f, so that

$$U_f |x\rangle_n \big|y\big\rangle_d = |x\rangle_n \big|y - f(x)\big\rangle_d.$$

Note that the $(n+1)^{\text{th}}$ register of $U_f |x\rangle_n \big|y\big\rangle_d$ is $|1\rangle$ exactly when $y < f(x)$.

5. Application to Grover fixed point search and state preparation

Fix $\delta \in (0,1)$ and y. Let $\lambda := \frac{|C_y|}{2^n}$, where $C_y := \{x \in \{0,1\}^n \,|\, f(x) \geqslant y\}$. Finally let $l := \left\lceil \frac{\log_2\left(\frac{2}{\delta}\right)}{2\sqrt{\lambda}} - \frac{1}{2} \right\rceil$. Then, following [5], we can construct a Quantum circuit (using U_f from the previous section), that results in a state $S_l|0\rangle_n|y\rangle_d$ with the following significance: When the first n qubits are measured in the computational basis, then

$$P\big(x \in C_y\big) = \sum_{x \in C_y} |\langle x|S_l|0\rangle|^2 \geqslant 1 - \delta^2.$$

Let us make the following definitions:

$$\begin{aligned} U_S &:= H^{\otimes n} \otimes \mathbb{1}^{\otimes m}, \\ R_0(\alpha) &:= \mathbb{1}^{\otimes(n+m)} + \left(1 - e^{i\alpha}\right)|0\rangle_n\langle 0|_n \otimes \mathbb{1}^{\otimes(1+m)}, \\ R_T\big(\beta\big) &:= U_f^\dagger P_{n+1}\big(\beta\big) U_f, \\ G\big(\alpha,\beta\big) &:= -U_S R_0(\alpha) U_S^\dagger R_T\big(\beta\big). \end{aligned}$$

Let $\big(\boldsymbol{\alpha},\boldsymbol{\beta}\big) = \big(\alpha_1,\beta_1,\cdots,\alpha_l,\beta_l\big)$ be given by

$$\forall\, j \in \{1,\ldots,l\}: \quad \alpha_j := -\beta_{l-j+1} = 2\cot^{-1}\left(\tan\left(\tfrac{2\pi j}{2l+1}\right)\sqrt{1-\gamma^2}\right),$$

where $\gamma := \big(T_{1/(2l+1)}\big(\delta^{-1}\big)\big)^{-1}$ and let

$$S_l\big(\boldsymbol{\alpha},\boldsymbol{\beta}\big) = G\big(\alpha_l,\beta_l\big)G\big(\alpha_{l-1},\beta_{l-1}\big)\cdots G\big(\alpha_1,\beta_1\big)U_S.$$

References

[1] Austin Gilliam, Charlene Venci, Sreraman Muralidharan, Vitaliy Dorum, Eric May, Rajesh Narasimhan, and Constantin Gonciulea, *Foundational patterns for efficient quantum computing* (2021). ↑1

[2] Austin Gilliam, Stefan Woerner, and Constantin Gonciulea, *Grover Adaptive Search for Constrained Polynomial Binary Optimization*, Quantum **5** (2021apr), 428. ↑1, 2

[3] John Golden, Andreas Bärtschi, Daniel O'Malley, and Stephan Eidenbenz, *Threshold-Based Quantum Optimization*, 2021 ieee international conference on quantum computing and engineering (qce), 2021, pp. 137–147. ↑1

[4] Nielsen, Michael A. and Chuang, Isaac L., *Quantum Computation and Quantum Information: 10th Anniversary Edition*, Cambridge University Press, 2010. ↑5

[5] Theodore J. Yoder, Guang Hao Low, and Isaac L. Chuang, *Fixed-point quantum search with an optimal number of queries*, Phys. Rev. Lett. **113** (2014Nov), 210501. ↑7

(Atithi Acharya)

(Ákos Nagy) Department of Mathematics, University of California, Santa Barbara
URL: akosnagy.com
Email address: contact@akosnagy.com

(Jaime Park)

(Cindy Zhang)