(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), $F : \mathrm{dom}(F) \to \mathbb{Z}_2^m$, where $\mathrm{dom}(F) \subseteq \mathbb{Z}_2^n$, is the following quantum state on $n+m$ qubits:

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

Date: August 28, 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, $\left|f\right\rangle = |F\rangle$. We handle signs via the "Two's complement" convention, in particular, a number is negative exactly when its first digit is 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. **Monomial encoder.** Let $f(x) = x_{i_1}x_{i_2}\cdots x_{i_j}$ be an arbitrary monomial and consider a quantum circuit with $m+n$ registers. Following [2], we construct an oracle that sends $|x\rangle_n|0\rangle_m$ to $|x\rangle_n\left|f(x)\right\rangle_m$, for any $x \in \mathbb{Z}_2^n$.

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

$$\mathrm{QFT}_m\left|y\right\rangle_m = 2^{-\frac{m}{2}} \sum_{z=-2^{m-1}}^{2^{m-1}-1} e^{\frac{2\pi yz}{2^m}i}|z\rangle_m.$$

Then

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

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

$$\begin{array}{ccc}
|z_0\rangle & \text{---}\boxed{\mathrm{PHASE}(\pi k)}\text{---} & e^{\frac{2\pi k z_0 2^{m-1}}{2^m}i}|z_1\rangle \\
\vdots & & \\
\left|z_j\right\rangle & \text{---}\boxed{\mathrm{PHASE}\left(\frac{2\pi k}{2^{j+1}}\right)}\text{---} & e^{\frac{2\pi z_j 2^{m-j-1}}{2^m}}\left|z_j\right\rangle \\
\vdots & & \\
|z_{m-1}\rangle & \text{---}\boxed{\mathrm{PHASE}\left(\frac{2\pi k}{2^m}\right)}\text{---} & e^{\frac{2\pi k z_{m-1}}{2^m}i}|z_m\rangle
\end{array}$$

Thus $\mathscr{P}_m(k)|z\rangle_m = e^{\frac{2\pi kz}{2^m}i}|z\rangle_m$.

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

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

$$\mathrm{QFT}_m^\dagger \circ \mathscr{P}_m(k) \circ \mathrm{QFT}_m \big|y\big\rangle_m = \big|y + k \mod 2^{m-1}\big\rangle.$$

Proof. First we compute

$$\begin{aligned}
\mathscr{P}_m(k) \circ \mathrm{QFT}_m \big|y\big\rangle_m &= \mathscr{P}(k)\left(2^{-\frac{m}{2}} \sum_{z=-2^{m-1}}^{2^{m-1}-1} e^{\frac{2\pi yz}{2^m}i}|z\rangle_m\right)\\
&= 2^{-\frac{m}{2}} \sum_{z=-2^{m-1}}^{2^{m-1}-1} e^{\frac{2\pi yz}{2^m}i}\mathscr{P}(k)|z\rangle_m\\
&= 2^{-\frac{m}{2}} \sum_{z=-2^{m-1}}^{2^{m-1}-1} e^{\frac{2\pi (y+k)z}{2^m}i}|z\rangle_m
\end{aligned}$$

hence

$$\begin{aligned}
\mathrm{QFT}_m^\dagger \circ \mathscr{P}(k) \circ \mathrm{QFT}_m \big|y\big\rangle_m &= 2^{-\frac{m}{2}} \sum_{z=-2^{m-1}}^{2^{m-1}-1} e^{\frac{2\pi (y+k)z}{2^m}i}\mathrm{QFT}_m^\dagger|z\rangle_m\\
&= 2^{-\frac{m}{2}} \sum_{z=-2^{m-1}}^{2^{m-1}-1} e^{\frac{2\pi (y+k)z}{2^m}i} 2^{-\frac{m}{2}} \sum_{y'=-2^{m-1}}^{2^{m-1}-1} e^{-\frac{2\pi y' z}{2^m}i}\big|y'\big\rangle_m\\
&= 2^{-m} \sum_{y'=-2^{m-1}}^{2^{m-1}-1} \sum_{z=-2^{m-1}}^{2^{m-1}-1} e^{\frac{2\pi\left(y+k-y'\right)z}{2^m}i}\big|y'\big\rangle_m\\
&= 2^{-m} \sum_{y'=-2^{m-1}}^{2^{m-1}-1} 2^m \delta_{[y+k]_{2^{m-1}},[y']_{2^{m-1}}}\big|y'\big\rangle_m\\
&= \big|y + k \mod 2^{m-1}\big\rangle,
\end{aligned}$$

where $[\cdot]_{2^{m-1}}$ is a remainder class modulo 2^{m-1}. □

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

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

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

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

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

4.1. **Oracle design:** Let $\mathscr{P}(\theta)$ be the following m-qubit gate

$$
\begin{array}{ccc}
\left|y_1\right\rangle & \text{—}\boxed{P\left(2^{m-1}\theta\right)}\text{—} & e^{i\theta y_1 2^{m-1}}\left|y_1\right\rangle \\
\vdots & & \\
\left|y_j\right\rangle & \text{—}\boxed{P\left(2^{m-j}\theta\right)}\text{—} & e^{i\theta y_j 2^{m-j}}\left|y_j\right\rangle \\
\vdots & & \\
\left|y_m\right\rangle & \text{—}\boxed{P(\theta)}\text{—} & e^{i\theta y_m}\left|y_m\right\rangle
\end{array}
$$

Thus $\mathscr{P}(\theta)\left|y\right\rangle_m = e^{i\theta y}\left|y\right\rangle_m$. Note that

$$
\left|y\right\rangle_m \text{—}\boxed{\mathrm{QFT}}\text{—}\boxed{\mathscr{P}\left(k\tfrac{2\pi}{2^m}\right)}\text{—}\boxed{\mathrm{QFT}^\dagger}\text{—} \left|z+k\right\rangle_m
$$

Thus if $f(x) = \sum_{i,j} Q_{i,j} x_i x_j + c$, then we need to add:

(1) $-Q_{i,j}$, exactly when $x_i = x_j = 1$. This amounts to the addition of a $\mathrm{QFT}^\dagger \circ \mathscr{P}\left(-Q_{i,j}\frac{2\pi}{2^m}\right) \circ$ QFT gate, controlled by the i^{th} and j^{th} register of $|x\rangle_n$,
(2) $-c$, independent of $|x\rangle$. This amounts to the addition of a $\mathrm{QFT}^\dagger \circ \mathscr{P}\left(-c\frac{2\pi}{2^m}\right) \circ \mathrm{QFT}$ gate.

However, the following observation further simplifies the circuit. Let $q_i = \sum_{j=1}^n Q_{i,j}$ and for $i < j$ let $S^{(i,j)}$ be the n-by-n matrix defined via

$$
S^{(i,j)}_{k,l} = \begin{cases} 1, & \text{if } k = l \in \{i,j\}, \\ -1, & \text{if } k = i, l = j, \text{ or } k = j, l = j, \\ 0, & \text{otherwise.} \end{cases}
$$

Then Q can be written as

$$
Q = \mathrm{diag}\left(q_1, q_2, \ldots, q_n\right) + \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} Q_{i,j} S^{(i,j)}.
$$

Since QFT is unitary, only the first one is needed; similarly, only the last $\mathrm{QFT}^\dagger$ is need. Hence U_f is given by:

$$
\begin{array}{lcccccl}
|x\rangle_n & \text{————} & \bullet & \text{——} & \bullet & \text{————} & |x\rangle_n \\
\left|y\right\rangle_m & \text{—}\boxed{\mathrm{QFT}}\text{—} & \boxed{\mathscr{P}\left(-Q_{1,1}\frac{2\pi}{2^m}\right)} & \text{——} & \boxed{\cdots} & \text{—}\boxed{\mathrm{QFT}^\dagger}\text{—} & \left|y - f(x)\right\rangle_m
\end{array}
$$

Example 4.1. *Let* $n = 4$ *and* $f(x) = 3x_1^2 + x_2^2 + x_3^2 + x_4^2 - 2(x_1x_2 + x_1x_3 + x_1x_4)$*. This is equivalent to equation* (3.1)*, with*

$$Q_{1,2} = Q_{1,2} = Q_{1,4} = -1, \quad b_1 = 3, \quad b_2 = b_3 = b_4 = 1,$$

and all other coefficient zero. Furthermore, $m = 3$ *works.*

Remark 4.2. *When* f *has symmetries, the above picture can be simplified. For example, in the case of MaxCut, we can assume that, say the last vertex is always in the* 0*-components, thus that qubit register can be eliminated.*

Note that the adjusted cost, $y - f(x)$, is encoded, which can later be used to implements the unitary operators $\exp\left(i\gamma H_f\right)$ without Trotterization as follow: let $\gamma \in \mathbb{R}$ and let us omit the ancilla qubit. Then $\exp\left(i\gamma H_f\right)|x\rangle_n = e^{i\gamma(y-f(x))}|x\rangle$ can be prepared via a $\mathscr{P}\left(\gamma\frac{2\pi}{2^m}\right)$-gate.

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 $C_y := \left\{x \in \{0,1\}^n \middle| f(x) \geqslant y\right\}$. Finally let $l := \left\lceil \frac{\log_2\left(\frac{2}{\delta}\right)}{2\sqrt{\lambda}} - \frac{1}{2} \right\rceil$. Then, following [4], we can construct a Quantum circuit (using U_f from the previous section), that results in a state $S_l|0\rangle_n\left|y\right\rangle_m$ with the following significance: When the first n qubits are measured in the computational basis, then

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

Let us make the following definitions:

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

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

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

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

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

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] 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. ↑6

(Atithi Acharya)

(Ákos Nagy) DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, SANTA BARBARA
URL: akosnagy.com
Email address: contact@akosnagy.com

(Jaime Park)

(Cindy Zhang)