Oracle Comparisons & Simulation

Thursday, February 25, 2021 9:51 PM

Part 1:

Motivating problem: people use different oracle models to hide a permutation $\pi \in S_n$

$$O_\pi^{sym} : |i\rangle \mapsto |\pi(i)\rangle \quad \text{acts on } \mathbb{C}^n \qquad \text{(our group)}$$

$$O_\pi^{std} : |i, j\rangle \mapsto |i, \pi(i) + j \bmod n\rangle \quad \text{acts on } \mathbb{C}^n \otimes \mathbb{C}^n \qquad \text{(everyone else)}$$

Q. Do these oracles give the same query complexity wrt any given learning problem?

Ex What is sign(π)? w/ O_π^{sym} Jamie & Daniel: $\lceil \frac{n}{2} \rceil$ queries needed & sufficient

classically $n-1$ queries required.

$$Q_{exact}(\text{sign}) = Q_{bdd}(\text{sign}) = \lceil \tfrac{n}{2} \rceil$$

w/ O_π^{std}: Dafni, Filmus, Lifshitz, Lindzey, Vinyals ITCS 2021 to appear

→ study complexity of Boolean functions on S_n.

$$\frac{n}{2} = \frac{\deg(\text{sign})}{2} \lesssim Q_{bdd}(\text{sign})$$

For learning the sign, the answer is yes, at least asymptotically. (but can we translate our $\lceil \frac{n}{2} \rceil$ algorithm to O_π^{std}?)

Ex What is $\pi^{-1}(1)$? w/ O_π^{sym}: special case of "right coset ID", in progress w/ Jamie

"permutation inversion" w/ O_π^{std}: Ambainis (2000) proves $\sqrt{n}$ queries needed

(apparently) achieved by implementing Grover search. (are adaptive queries needed?)

Remark David & Jamie provide numerical evidence that oracle implementations do matter in a different setting

(Single-query learning from Hamming distance oracles, 2010)

- questions remain: do these numerical results hold up if we let the oracles have ancillae?
  if we use non-equal superposition queries?

Related question: Can we simulate O_π^{sym} by O_π^{std}? Or vice versa?

$$O_\pi^{sym} |i\rangle = |\pi(i)\rangle$$

$$O_\pi^{std} |i, j\rangle = |i, \pi(i) + j \bmod n\rangle.$$

Part 2: Remarks on oracle simulations

I. Toy problem: Suppose we have two oracles in front of us, Bythia and Trythia.

They each hide (the same) bit $a \in \{0,1\}$. But they operate differently:

To Bythia we can input $x \in \{1,2\}$ and Bythia outputs $\pi_a(x)$ where

$$\pi_a = \begin{cases} e & \text{if } a=0 \\ (1,2) & \text{if } a=1 \end{cases}$$

To Trythia we can input $x \in \{1,2,3\}$ and Trythia outputs $\sigma_a(x)$ where

$$\sigma_a = \begin{cases} e & \text{if } a=0 \\ (1,2,3) & \text{if } a=1 \end{cases}$$

Who should we ask to learn the bit?

(It doesn't matter. We can learn the bit in one query from either oracle.)

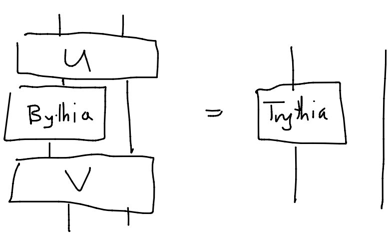
From the learning perspective, the oracles are equivalent.

Q. Can we simulate Bythia using a query to Trythia, and vice versa?

A. Classically, yes. But along the way we do some non-reversible computations (using non-injective functions).

Quantumly, there is no circuit to turn one into the other,

(reading circuit diagrams bottom to top)



$a=0$: both oracles are I, so $UV = I$, ie $U = V^{-1}$!

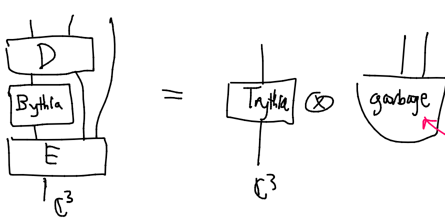
$a=1$: $\underbrace{V^{-1}(\text{Bythia} \otimes I)V}_{\text{order } 2} \neq \underbrace{\text{Trythia} \otimes I}_{\text{order } 3}$.

Beyond the circuit model?

Can we find quantum channels $\mathcal{E}, \mathcal{D}$ s.t. $\text{Trythia} = \mathcal{D} \circ \text{Bythia} \circ \mathcal{E}$?

$\Longleftrightarrow$ $\exists$ isometries E, D s.t.

(I think)



the garbage is allowed to depend on a!

Unknown to me.

II. A well-known "equivalence" of oracles.

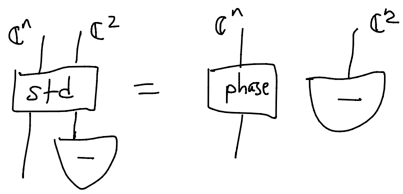
Suppose we want to learn something about $f : \{1, \dots, n\} \to \{0,1\}$.

$$O_f^{std} |i, b\rangle = |i, b \oplus f(x)\rangle \qquad \text{acting on } \mathbb{C}^n \otimes \mathbb{C}^2$$

$$O_f^{phase} |i\rangle = (-1)^{f(x)} |i\rangle \qquad \text{acting on } \mathbb{C}^n$$

Phase kickback:

$\boxed{-} = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

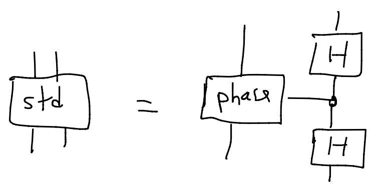


So the std oracle can simulate the phase oracle w/ one query

Contrary to popular belief the phase oracle CANNOT simulate standard oracle w/ any number of queries,

Why? The phase oracle can't tell apart f and $1-f$.

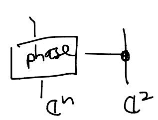
However:



so std is equivalent to controlled-phase.

(In the circuit model we cannot "add control" willy-nilly, but there are implementation specific proposals for how to do so.)

Note:



$$= \left[\begin{array}{c|c} \text{phase} & 0 \\ \hline 0 & I \end{array}\right]$$

($2n \times 2n$ matrix)

so "adding control" amounts to direct summing phase w/ a "trivial" subspace.

III. Adding control to unknown unitaries.

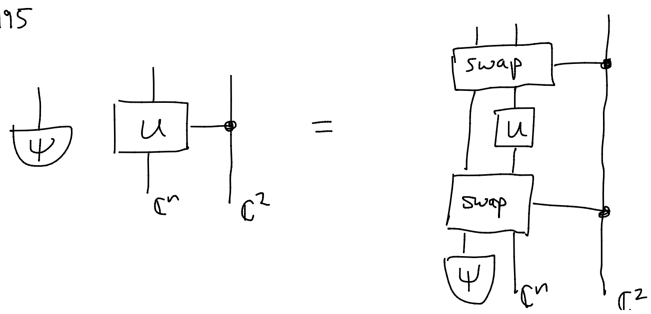
Problem Given $U \in \Omega$ = some fixed set of unitaries on $\mathbb{C}^n$

can we find a circuit that implements Controlled-U (acting on $\mathbb{C}^n \otimes \mathbb{C}^2$)?

How many queries do we need?

the circuit can depend on Ω but not U.

Kitaev: 1995 If the unitaries U have a shared fixed vector $|\psi\rangle \in \mathbb{C}^n$, then it's no problem with one query:



Gavarová, Seidel, Touati:
2020

If $\Omega = U(d)$ ($\underline{\text{all}}$ unitaries) then it is impossible even to implement

$$\text{Controlled-}_{\varphi}\, U = \left[\begin{array}{c|c} e^{i\varphi(U)}\, U & \\ \hline & I \end{array}\right]$$

w/any # of queries.

(Proof uses $\pi_1(U(d)) \cong \mathbb{Z}$. So what about $SU(d)$ which has trivial fund. group?)

Using Kitaev: If Ω is a group of unitaries acting on V and $V^{\otimes t}$ contains a copy of $\mathbb{1}$ and V, then Controlled-U can be implemented in t-queries.

$\underline{\text{Ex}}$ If Ω any collection of perm. matrices, then V contains a copy of trivial (equal superposition)

$\Rightarrow$ can always implement the controlled-U in this case.

$\underline{\text{Ex}}$ $\Omega =$ $SU(2)$ ($\dim_{\mathbb{R}} = 3$) acting faithfully on $\mathbb{C}^3 = V$. Then $V \otimes V$ contains $\mathbb{1}$ and V, so we can do it w/ 2-queries.

($V = \mathrm{Sym}^3(\mathbb{C}^2)$ as $SU(2)$ rep'n)

$\underline{\text{Ex}}$ $\Omega =$ compact real form of G_2 ($\dim_{\mathbb{R}} = 14$) acting on $\mathbb{C}^7$. Then again $V \otimes V$ contains $\mathbb{1}$ and V.