9. Qubitization: Block encodings

Isaac H. Kim (UC Davis)

Recap: Qubitization

$$e^{i\phi_0 Z}e^{i\theta X}e^{i\phi_1 Z}\cdots e^{i\theta X}e^{i\phi_d Z} = \begin{bmatrix} P(a) & iQ(a)\sqrt{1-a^2} \\ iQ^*(a)\sqrt{1-a^2} & P^*(a) \end{bmatrix},$$

where $\theta = \cos^{-1}(a)$. Using qubitization, we can implement (upon measuring $|0\rangle$)

$$\underbrace{|\psi\rangle_s \rightarrow P(H)|\psi\rangle_s,}$$

(for a polynomial that satisfies the conditions in QSP.)

Qubitization: The gate sequence

$e^{i\phi'_0\tilde{Z}}U(H)e^{i\phi'_1\tilde{Z}}\cdots U(H)e^{i\phi'_d\tilde{Z}}$,

where $\tilde{Z} = Z_a \otimes I_s$ and $U(H) = Z_a \otimes H + X_a \otimes \sqrt{1 - H^2}$.

Cost $\approx$ Cost of $U(H) \times$ Degree of the polynomial

Unitary Encoding

$\|H\| \leq 1$

$U(H) = Z_a \otimes H + X_a \otimes \sqrt{1 - H^2}$ is called as a *unitary encoding* of H .

1. $U(H)$ is a unitary.
2. Alternatively, we can view it as a block-diagonal matrix:

$$U(H) = \begin{pmatrix} H & \cdot \\ \cdot & \cdot \end{pmatrix}.$$

Unitary Encoding Revisited

$U(H)|0\rangle_a|\lambda\rangle_s = \lambda|0\rangle_a|\lambda\rangle_s + \sqrt{1-\lambda^2}\,|\phi\rangle$

orthogonal to $|0\rangle_a|\lambda\rangle_s$

So far, we *defined* the unitary encoding of H to be $U(H) = Z_a \otimes H + X_a \otimes \sqrt{1-H^2}$. However, this definition is somewhat restrictive. For instance, this construction demands $U(H)$ to be exactly

$$U(H) = \begin{pmatrix} \boxed{H} & \sqrt{I-H^2} \\ \sqrt{I-H^2} & -H \end{pmatrix}.$$

However, in actual application, **we only use the top left corner of the matrix!**

This motivates a more relaxed definition of unitary encoding, defined as

$$U(H)|G\rangle_a|\lambda\rangle_s = \lambda|G\rangle_a|\lambda\rangle_s + \sqrt{1-\lambda^2}\,|G_\lambda^\perp\rangle_{as},$$

where $\left(\langle G|_a \otimes I_s\right)|G_\lambda\rangle_{as}^\perp = 0$.

Fixed state

Previous: $|G\rangle_a = |0\rangle_a$

Today: $|G\rangle_a$: some fixed state on $k \geq 1$ qubits

1. The ancilla no longer has to be a single qubit.
2. We can simply avoid defining some of the matrix elements.

λ-subspace

This motivates a more relaxed definition of unitary encoding, defined as

$$U(H)\,|G\rangle_a|\lambda\rangle_s = \lambda\,|G\rangle_a|\lambda\rangle_s + \sqrt{1-\lambda^2}\,|G_\lambda^\perp\rangle_{as},$$

where $\left(\langle G|_a \otimes I_s\right)|G_\lambda\rangle_{as}^\perp = 0.$

Unfortunately, this definition seems to have a problem. Upon applying $U(H)$ twice, we may leave the subspace spanned by $|G_\lambda\rangle = |G\rangle|\lambda\rangle$ and $|G_\lambda^\perp\rangle$. You apply it three times, and potentially more trouble will be waiting us…

$$U(H)\,|G\rangle_a|\lambda\rangle_s = \lambda\underbrace{|G\rangle_a|\lambda\rangle_s}_{|G_\lambda\rangle} + \sqrt{1-\lambda^2}\,|G_\lambda^\perp\rangle_{as}$$

$$U(H)^2|G_\lambda\rangle = \underbrace{\lambda\,U(H)|G_\lambda\rangle}_{\text{Okay}} + \sqrt{1-\lambda^2}\,U(H)|G_\lambda^\perp\rangle$$

*Remark: Our definition is slightly different from Low & Chuang

$W(H)_{\text{our}} = \underset{\substack{\uparrow \\ \text{unitary}}}{V}\, W(H)_{\text{Low \& Chuang}}$

λ-subspace

Low & Chuang (2016)

Iterate of H

To avoid this problem, we need a unitary $W(H)$ such that

$$W(H)\,|G\rangle_a|\lambda\rangle_s = \lambda\,|G\rangle_a|\lambda\rangle_s + \sqrt{1-\lambda^2}\,|G_\lambda^\perp\rangle_{as},$$

where $\left(\langle G|_a \otimes I_s\right)|G_\psi\rangle_{as}^\perp = 0$. Moreover, we need $W(H)$ to preserve the subspace spanned by $|G_\lambda\rangle = |G\rangle|\lambda\rangle$ and $|G_\lambda^\perp\rangle$.

key

By unitarity, it suffices to show that $W(H)$ reduces to a 2×2 $\boxed{\text{unitary}}$ on that subspace (for each λ). Moreover, while not too important, it will be convenient to make this unitary similar to the $R(\lambda)$ discussed last time.

$$W(H)\,|G_\lambda\rangle = \lambda\,|G_\lambda\rangle + \sqrt{1-\lambda^2}\,|G_\lambda^\perp\rangle$$

$$W(H)\,|G_\lambda^\perp\rangle = \alpha\,|G_\lambda\rangle + \beta\,|G_\lambda^\perp\rangle + \gamma\,|\tilde{G}_\lambda\rangle$$

$$W(H) = \begin{array}{cc|c} |G_\lambda\rangle & |G_\lambda^\perp\rangle & \\ \hline \lambda & \sqrt{1-\lambda^2} & |G_\lambda\rangle \\ \alpha & \beta & |G_\lambda^\perp\rangle \end{array}$$

If $W(H)$ is unitary $\downarrow$ $\alpha\lambda + \beta\sqrt{1-\lambda^2} = 0$ $\rightarrow$

$$\boxed{\begin{aligned} \alpha &= \sqrt{1-\lambda^2}\, e^{i\phi} \\ \beta &= -\lambda\, e^{i\phi} \end{aligned}}$$

$$\underbrace{W(H)|G_\lambda^\perp\rangle}_{\text{norm}=1} = \underbrace{\sqrt{1-\lambda^2}\, e^{i\phi}|G_\lambda\rangle - \lambda e^{i\phi}|G_\lambda^\perp\rangle}_{\text{norm}=1} + \underbrace{\gamma|G_\lambda\rangle}_{\text{norm}=0}$$

$\downarrow$

$\gamma = 0$

Matrix elements

Let's recall our toy version of qubitization: $e^{i\phi_0'\tilde{Z}}U(H)e^{i\phi_1'\tilde{Z}}\cdots U(H)e^{i\phi_d'\tilde{Z}}$,

where $\tilde{Z} = Z_a \otimes I_s$ and $U(H) = Z_a \otimes H + X_a \otimes \sqrt{1-H^2}$.

In the λ-subspace, we get a 2×2 matrix $R(\lambda) = \begin{pmatrix} \lambda & \sqrt{1-\lambda^2} \\ \sqrt{1-\lambda^2} & -\lambda \end{pmatrix}$.

$$\boxed{W_\lambda(H) = \begin{pmatrix} \lambda & \sqrt{1-\lambda^2} \\ \sqrt{1-\lambda^2}\, e^{i\phi} & -\lambda e^{i\phi} \end{pmatrix}}$$

$\phi = 0 \rightarrow W_\lambda(H) = R(\lambda)$

$$W(H)|G_\lambda\rangle = \lambda|G_\lambda\rangle + \sqrt{1-\lambda^2}\,|G_\lambda^\perp\rangle$$

$$W_\lambda(H) = \begin{array}{cc} \begin{array}{cc} |G_\lambda\rangle & |G_\lambda^\perp\rangle \end{array} & \\ \begin{pmatrix} \lambda & \sqrt{1-\lambda^2} \\ \sqrt{1-\lambda^2}\,e^{i\phi} & -\lambda e^{i\phi} \end{pmatrix} & \begin{array}{c} |G_\lambda\rangle \\ |G_\lambda^\perp\rangle \end{array} \end{array}$$

Matrix elements

$$|G_\lambda^\perp\rangle = \frac{(W(H)-\lambda I)|G_\lambda\rangle}{\sqrt{1-\lambda^2}}$$

$$\langle G_\lambda|W(H)|G_\lambda\rangle = \lambda$$

$$\langle G_\lambda^\perp|W(H)|G_\lambda\rangle = \sqrt{1-\lambda^2}$$

$$\langle G_\lambda|W(H)|G_\lambda^\perp\rangle = ?$$

$$\langle G_\lambda^\perp|W(H)|G_\lambda^\perp\rangle = ?$$

$$\langle G_\lambda|W(H)|G_\lambda^\perp\rangle = \frac{1}{\sqrt{1-\lambda^2}}\left(\langle G_\lambda|W(H)^2|G_\lambda\rangle - \lambda\langle G_\lambda|W(H)|G_\lambda\rangle\right)$$

$$= \frac{1}{\sqrt{1-\lambda^2}}\left(\langle G_\lambda|W(H)^2|G_\lambda\rangle - \lambda^2\right)$$

$$= \sqrt{1-\lambda^2}\,e^{i\phi}$$

$$\langle G_\lambda^\perp|W(H)|G_\lambda^\perp\rangle = \frac{1}{1-\lambda^2}\langle G_\lambda|(W(H)^\dagger-\lambda I)\,W(H)\,(W(H)-\lambda I)|G_\lambda\rangle$$

$$= \frac{1}{1-\lambda^2}\Big(\langle G_\lambda|W(H)|G_\lambda\rangle + \lambda^2\langle G_\lambda|W(H)|G_\lambda\rangle - \langle G_\lambda|G_\lambda\rangle\lambda - \lambda\langle G_\lambda|W(H)^2|G_\lambda\rangle\Big)$$

$$= \frac{1}{1-\lambda^2}\left(\lambda+\lambda^3-\lambda-\lambda\langle G_\lambda|W(H)^2|G_\lambda\rangle\right)$$

$$= \frac{\lambda}{1-\lambda^2}\left(\lambda^2-\langle G_\lambda|W(H)^2|G_\lambda\rangle\right)$$

$$= -\lambda e^{i\phi}$$

Unique solution!

$\phi = 0$, $\langle G_\lambda|W(H)^2|G_\lambda\rangle = 1$

Key conditions

$W(H)|G_\lambda\rangle = \lambda|G_\lambda\rangle + \sqrt{1-\lambda^2}\,|G_\lambda^\perp\rangle$

$$\langle G_\lambda | W(H) | G_\lambda \rangle = \lambda$$

$$\langle G_\lambda | W(H)^2 | G_\lambda \rangle = 1$$

Let's recall what we did last time…

$$U(H) = Z_a \otimes H + X_a \otimes \sqrt{1 - H^2}.$$

This is just one viable example of $W(H)$. But now we can play with other possibilities!

$U(H)|0\rangle|\lambda\rangle = \lambda|0\rangle|\lambda\rangle + \sqrt{1-\lambda^2}\,|\phi\rangle$ $\qquad U(H)^2 = I \qquad \langle G_\lambda|\, U(H)^2 \,|G_\lambda\rangle = 1$

$|G\rangle_a = |0\rangle \qquad |G_\lambda^\perp\rangle = |\phi\rangle$

But we are still not done yet, because we need to figure out how to ensure
$\langle G_\lambda | W(H)^2 | G_\lambda \rangle = 1.$

A Trick

We can simply add one more qubit and replace the $U(H)$ by controlled-$U(H)$ and its inverse, to implement $W(H)$.

(Usually) Easy to come up with $U(H)$ s.t.

Condition 1) $U(H)\,|G\rangle_a|\lambda\rangle_s = \lambda\,|G\rangle_a|\lambda\rangle_s + |G_\lambda^\perp\rangle_{as}$

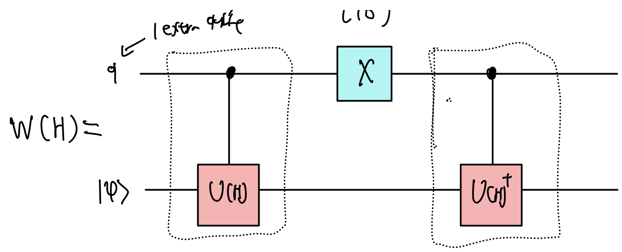
Not straightforward to come up with $U(H)$ s.t. Condition 1 is satisfied and $\langle G_\lambda|U(H)^2|G_\lambda\rangle = 1$

Goal: Given $U(H)$, construct $W(H)$ (and $|G'\rangle_a$) s.t.

$W(H)\,|G'\rangle_a|\lambda\rangle_s = \lambda\,|G'\rangle_a|\lambda\rangle_s + |G_\lambda^{\perp\prime}\rangle_{as}$

and $\langle G_\lambda'|W(H)^2|G_\lambda'\rangle = 1$

$(|G_\lambda'\rangle = |G'\rangle_a|\lambda\rangle_s)$

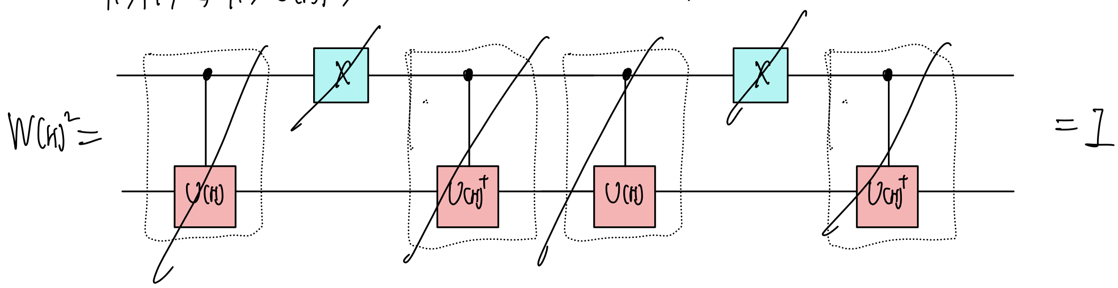


$|0\rangle|\varphi\rangle \to |0\rangle|\varphi\rangle$

$|1\rangle|\varphi\rangle \to |1\rangle U(H)|\varphi\rangle$

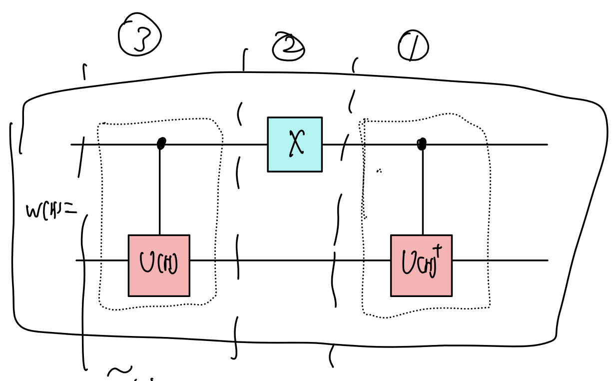
$|0\rangle|\psi\rangle \to |0\rangle|\psi\rangle$

$|1\rangle|\psi\rangle \to |0\rangle U(H)^\dagger|\psi\rangle$



$W(H)|G'\rangle_a|\lambda\rangle_s = \lambda|G'\rangle_a|\lambda\rangle_s + |G_\lambda^{\perp'}\rangle_{as}$

$|G'\rangle_a = \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)_q|G_a\rangle$ associated $U(H)$



$W(H)\frac{1}{\sqrt{2}}\left(|0\rangle_q|G\rangle_a|\lambda\rangle_s + |1\rangle_q|G\rangle_a|\lambda\rangle_s\right)$

① $\Rightarrow \frac{1}{\sqrt{2}}\left(|0\rangle_q|G\rangle_a|\lambda\rangle_s + |1\rangle_q U(H)^\dagger|G\rangle_a|\lambda\rangle_s\right)$

$= \frac{1}{\sqrt{2}}\left(|0\rangle_q|G\rangle_a|\lambda\rangle_s + \lambda|1\rangle_q|G\rangle_a|\lambda\rangle_s + |1\rangle_q\sqrt{1-\lambda^2}|\tilde{G}_\lambda^\perp\rangle_{as}\right)$

② $\Rightarrow \frac{1}{\sqrt{2}}\left(|1\rangle_q|G\rangle_a|\lambda\rangle_s + \lambda|0\rangle_q|G\rangle_a|\lambda\rangle_s + |0\rangle_q\sqrt{1-\lambda^2}|\tilde{G}_\lambda^\perp\rangle_{as}\right)$

③ $\Rightarrow \frac{1}{\sqrt{2}}\left(\lambda|1\rangle_q|G\rangle_a|\lambda\rangle_s + \sqrt{1-\lambda^2}|1\rangle_q\sqrt{1-\lambda^2}|G_\lambda^\perp\rangle_{as} + \lambda|0\rangle_q|G\rangle_a|\lambda\rangle_s + |0\rangle_q\sqrt{1-\lambda^2}|\tilde{G}_\lambda^\perp\rangle_{as}\right.$

$= \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)_q|G\rangle_a\lambda|\lambda\rangle_s + \sqrt{1-\lambda^2}|G_\lambda^{\perp''}\rangle_{as}$

Last time: $U(H) = Z_a \otimes H + X_a \otimes \sqrt{I - H^2}$

Qubitization: Block-encoding framework

Flexible $U(H)$

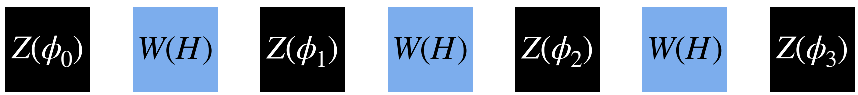
$$Z(\phi_0) \quad W(H) \quad Z(\phi_1) \quad W(H) \quad Z(\phi_2) \quad W(H) \quad Z(\phi_3)$$

No longer a single-qubit operator. Problem?

No! We are always living in the λ-subspace, in which $|G_\lambda\rangle = |G\rangle_a |\lambda\rangle$ and $|G_\lambda^\perp\rangle$ forms a "qubit." By applying $Z_a(\phi)$ such that $Z_a(\phi)|G\rangle_a = e^{i\phi}|G\rangle_a$ and $Z_a(\phi)|G^\perp\rangle_a = |G^\perp\rangle_a$

(for a fixed λ), we can implement the desired operation.

Side remark



Let's talk about the implementation of $Z_a(\phi)$ such that $Z_a(\phi)\,|\,G\rangle_a = e^{i\phi}\,|\,G\rangle_a$ and $Z_a(\phi)\,|\,G^\perp\rangle_a = |\,G^\perp\rangle_a$.

$V\,|1\cdots 1\rangle_a = |G\rangle_a \quad \longleftrightarrow \quad |1\cdots 1\rangle_a = V^\dagger\,|G\rangle_a$

1) $V^\dagger$

2) Toffoli gate: $|1\cdots 1\rangle_a\,|0\rangle_{q'} \xrightarrow{\text{Toffoli}} |1\cdots 1\rangle_a\,|1\rangle_{q'}$

$|x\rangle_a\,|0\rangle_{q'} \xrightarrow{\text{Toffoli}} |x\rangle_a\,|0\rangle_{q'}$ if $x \neq 1\cdots 1$

3) Phase on q' 4) Toffoli^{-1} 5) V

Qubitization: Block-encoding framework

$$Z(\phi_0) \quad W(H) \quad Z(\phi_1) \quad W(H) \quad Z(\phi_2) \quad W(H) \quad Z(\phi_3)$$

Cost $\approx$ Cost of $W(H) \times$ Degree of the polynomial

Cost of $W(H) \approx 2 \times$ Cost of controlled-$U(H)$