If f is balanced the amplitude of $|\underline{y}=0,0,\ldots 0)$ is zero since then

$$\sum_{\underline{x}=0}^{2^n-1}(-1)^{(\underline{x}\cdot\underline{y}+f(\underline{x}))}=\sum_{\underline{x}=0}^{2^n-1}(-1)^{f(\underline{x})}=0 \tag{104}$$

If f is constant $f(\underline{x})=f\in\{0,1\}$

$$\sum_{\underline{x}=0}^{2^n-1}(-1)^{(\underline{x}\cdot\underline{y}+f(\underline{x}))}=(-1)^f\sum_{\underline{x}=0}^{2^n-1}(-1)^{\underline{x}\cdot\underline{y}} \tag{105}$$

$$=0 \quad \text{for all } \underline{y} \text{ except } \underline{y}=(0,0,0,\ldots 0)$$

□

The Deutch-Josza problem is however a problem within BPP, i.e. it can be efficiently solved probabilistically with a classical computer.

3.4 BQP ≠ BPP : the Simon problem

We will now discuss a problem which is believed to be outside of BPP but can be solved with polynomial effort using a quantum algorithm:

Simon problem

given $f: \{0,1\}^n \to \{0,1\}^q$

with a binary period a, i.e.

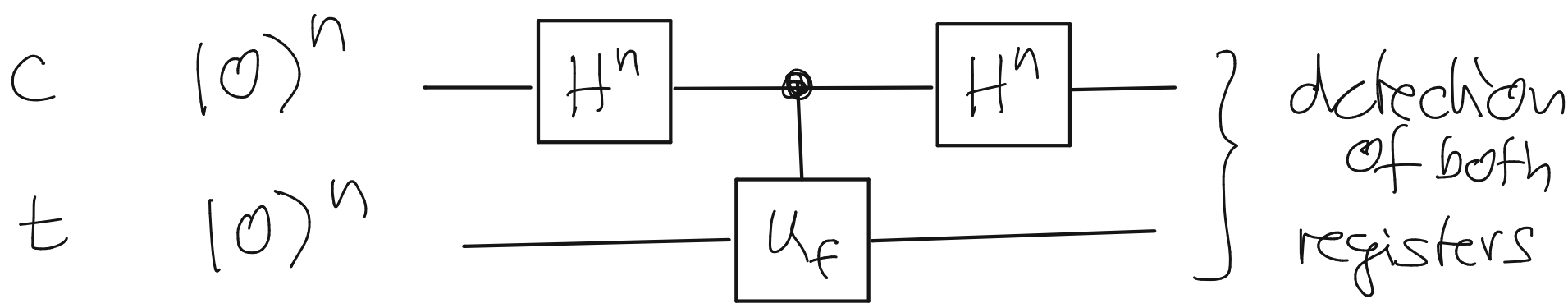
(106) $$f(\underline{x}) = f(\underline{y}) \quad \text{if} \quad \underline{y} = \underline{x} \oplus \underline{a}$$

Here $\oplus$ is bitwise addition modulo 2. The task is to find the period a (note $\underline{x} \oplus \underline{a} \oplus \underline{a} = \underline{x}$)

- classically this is a NP hard problem since we have to test pairs $\underline{x}, \underline{y}$ such that

(107) $$\underline{x} \oplus \underline{y} = \underline{a} \qquad (\text{note: } \underline{x} \oplus \underline{x} = \underline{0})$$

- quantum mechanically



where $f(\underline{x})$ is encoded in U_f

short notation $|\underline{0}) \equiv |0)^n = |0\rangle|0\rangle \cdots |0\rangle$

$|\underline{x}), |\underline{y}\rangle$ in n-dim. computational basis

e.g. $|\underline{x}\rangle = |10011010111\ldots\rangle$

(108) $$U_f |\underline{x})|\underline{y}) = |\underline{x}, \underline{y} \oplus f(\underline{x})\rangle$$

then

$$|\underline{0}\rangle|\underline{0}\rangle \xrightarrow{H^n} \frac{1}{2^{n/2}} \sum_{\underline{x}=0}^{2^n-1} |\underline{x}\rangle|\underline{0}\rangle$$

(109)
$$\xrightarrow{U_f} \frac{1}{2^{n/2}} \sum_{\underline{x}=0}^{2^n-1} |\underline{x}\rangle|f(\underline{x})\rangle$$

- measure 2nd register (target) $\Rightarrow$ this yields randomly one of the 2^n possible outputs of f:

1	$\|f(0,0,0\ldots)\rangle$		
n	$\|f(1,0,0\ldots)\rangle$	$\|f(0,1,0,\ldots)\rangle$	$\ldots \|f(0,0\ldots 01)\rangle$
$n(n-1)$	$\|f(1,1,0,\ldots)\rangle$	$\|f(1,01,\ldots)\rangle$	$\ldots \|f(0,0\ldots,1,1)\rangle$
	$\vdots$	$\vdots$	
1	$\|f(1,1,1,\ldots)\rangle$		

Suppose measurement yielded $|f(\underline{x}_0)\rangle$

e.g. $|f(0,1,0,1,0,\ldots 0)\rangle$

Since both $\underline{x} = \underline{x}_0$ and $\underline{x} = \underline{x}_0 + \underline{a}$ give the same result, the first register is after the measurement in the state

(110)
$$\frac{1}{\sqrt{2}}\left(|\underline{x}_0\rangle + |\underline{x}_0 \oplus \underline{a}\rangle\right)$$

Now how can we determine $\underline{a}$?

- bitwise Hadamard of 1st register

$$H^n \frac{1}{\sqrt{2}} \left(|\underline{x_0}\rangle + |\underline{x_0} \oplus \underline{a}\rangle \right) =$$

$$= \frac{1}{2^{(n+1)/2}} \sum_{\underline{y}=0}^{2^n-1} \left[(-1)^{\underline{x_0}\cdot\underline{y}} + (-1)^{(\underline{x_0}+\underline{a})\cdot\underline{y}} \right] |\underline{y}\rangle \quad (171)$$

$$= \frac{1}{2^{(n+1)/2}} \sum_{\underline{y}=0}^{2^n-1} (-1)^{\underline{x_0}\cdot\underline{y}} \left[1 + (-1)^{\underline{a}\cdot\underline{y}} \right] |\underline{y}\rangle$$

Now since

$$\underline{a}\cdot\underline{y} = a_1 y_1 + a_2 y_2 + \cdots \bmod 2 \in \{0,1\} \quad (172)$$

$$\Rightarrow$$

$$H^n \frac{1}{\sqrt{2}} \left(|\underline{x_0}\rangle + |\underline{x_0} \oplus \underline{a}\rangle \right)$$

$$= \frac{1}{2^{(n+1)/2}} \sum_{\underline{a}\cdot\underline{y}=0} (-1)^{\underline{x_0}\cdot\underline{y}} |\underline{y}\rangle \quad (173)$$

- measurement of $|y\rangle$ register projects to one of the 2^{n-1} states $|\underline{y}\rangle$ with $\underline{a}\cdot\underline{y}=0$

  this gives one value of $\underline{y}$, say $\underline{y}_0$

- repeat the protocol until we have n linear independent binary vectors $\underline{y}_j$

with

(114) $\underline{y_j} \circ \underline{a} = 0 \qquad j = 1, 2, \ldots, n$

This yields n linear equations for the n components of $\underline{a}$

(115) $y_{j1} a_1 + y_{j2} a_2 + \cdots + y_{jn} a_n \overset{\text{mod } 2}{=} 0 \qquad j = 1 \ldots n$

$\Rightarrow$ determine a

In order to find n linear independent vectors $\underline{y_j}$ the algorithm has to be performed on average $O(n)$ times i.e. with polynomial effort.

The Simon problem shows

$BQP > BPP$

(i.e. $BQP \neq BPP$)

3.5 Grover's search algorithm

Problem: given an unsorted list with N entries (reverse telephone book) How to find an entry (e.g. a given telephon number)?

- classically $N/2$ inquiries are needed!

remark: a search in an ordered list requires only $O(\log_2 N)$ inquiries. (successive bi-section)

$0 \leq x \leq N$

$0 \leq x < N/2$ | $N/2 \leq x \leq N$

$0 \leq x < N/4$ | $N/4 \leq x < N/2$ | $N/2 \leq x < \frac{3}{4}N$ | $\frac{3}{4}N \leq x \leq N$

⋮ etc

Lev Grover found an algorithm that finds an entry in

$$O(\sqrt{N})$$

steps quantum mechanically. This is practically very relevant but does not change the complexity class as

$$(116) \qquad N = 2^{\log_2 N} \qquad \sqrt{N} = 2^{\frac{1}{2}\log_2 N}$$

both scale exponentially with number of bits $(\log_2 N)$ needed to encode N

Lets assume that the unsorted list (inverse telephone book) is encoded in an oracle

For a given telephone number $\underline{w}$ corresponding to the persons name $\underline{x}_0$ we have

$$f_{\underline{w}}(\underline{x}) = 1 \quad \text{for } \underline{x} = \underline{x}_0 \tag{117}$$

$$f_{\underline{w}}(\underline{x}) = 0 \quad \text{else}$$

quantity we look for!

$f_{\underline{w}}$ is encoded in a unitary $U_{\underline{w}}$

$$U_{\underline{w}} |\underline{x}\rangle|\underline{y}\rangle = |\underline{x}\rangle|\underline{y} \oplus f_{\underline{w}}(\underline{x})\rangle \tag{118}$$

Note that for given $\underline{x}$ (name) it is easy to find $\underline{w}_0$ (telephone number) since in this direction the list is ordered, i.e. $\underline{x} \to f_{\underline{w}}(\underline{x})$ is easy: if $\underline{w} = \underline{w}_0$ than $f_{\underline{w}} = 1$ else $f_{\underline{w}} = 0$.

As seen before

$$U_{\underline{w}} |\underline{x}\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = (-1)^{f_{\underline{w}}(\underline{x})} |\underline{x}\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{119}$$

I.e. ignoring the second registe which stays unchanged, the action of $U_{\underline{w}}$ is

$$U_{\underline{w}} |\underline{x}\rangle \longrightarrow (-1)^{f_{\underline{w}}(\underline{x})} |\underline{x}\rangle \tag{120}$$

This means $U_{\underline{w}}$ changes the sign of all states orthogonal to the state $|\underline{x}_0\rangle$ corresponding to $\underline{w}$ (input telephone number).

(130) $$\boxed{U_w \hat{=} \underline{1} - 2|\underline{x}_0\rangle\langle\underline{x}_0|}$$

Now we use as input a superposition of computational basis states as input

(131) $$|\underline{s}\rangle = \frac{1}{\sqrt{N}} \sum_{\underline{x}=0}^{N-1} |\underline{x}\rangle$$

$|\underline{s}\rangle$ contains the state $|\underline{x}_0\rangle$ which we are looking for with probability $P_{x_0} = 1/N$.

Grovers Algorithm aims at an iterative amplification of this probability. To this end we apply

(132) $$R = \bar{U}_s U_w$$

where

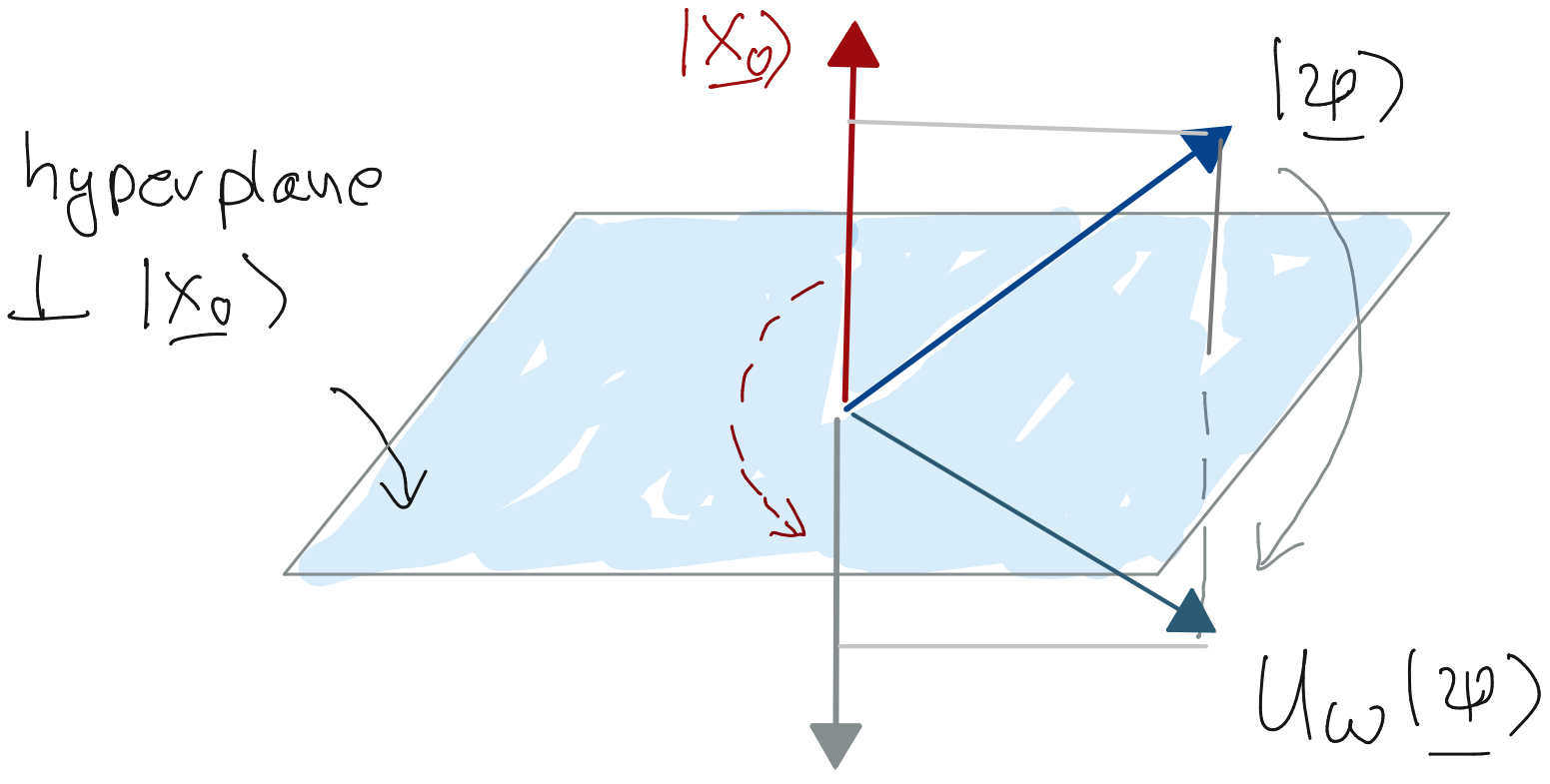
(133) $$\bar{U}_s = 2|s\rangle\langle s| - 1$$

R is called reflection about the mean

geometric illustration

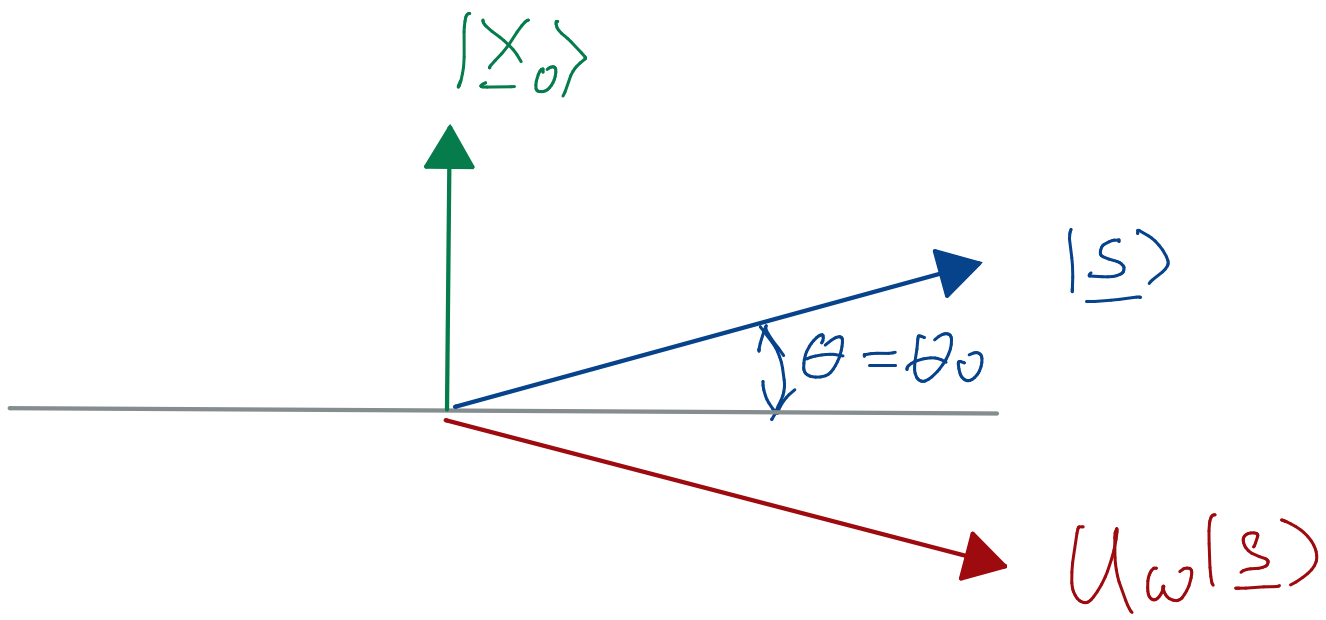
(134) $$|\langle \underline{s} | \underline{x}_0 \rangle| = \frac{1}{\sqrt{N}} \doteq \sin\theta \approx \theta$$

- action of U_w: The component of a general state $|\psi\rangle$ proportional to $|\underline{x}_0\rangle$ changes sign

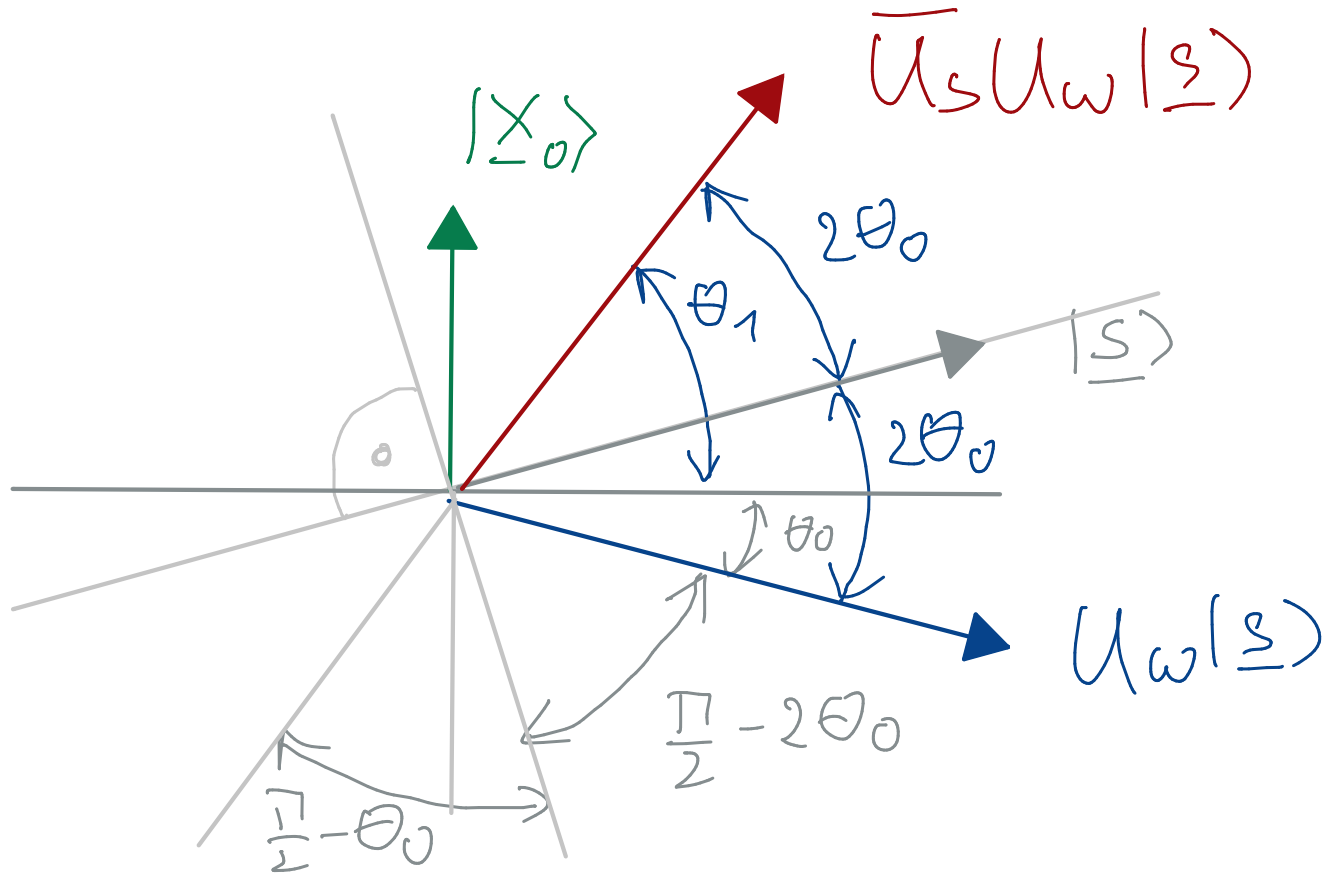


- action of $\overline{U}_s U_\omega$

(i)



(ii)



(135) $$\theta_1 = \pi - 2\left(\frac{\pi}{2} - 2\theta_0\right) - \theta_0 = 3\theta_0$$

i.e. in every iteration step the vector is shifted by $\Delta\theta = 2\theta_0$ in the direction of $|\underline{x}_0\rangle$

So

(136) $$|\psi_0\rangle = |\underline{s}\rangle \quad \text{and} \quad |\psi_{k+1}\rangle = R\,|\psi_k\rangle$$

Thus

(137) $$|\psi_k\rangle = \alpha_k \sum_{\underline{x} \neq \underline{x}_0} |\underline{x}\rangle + \beta_k\, |\underline{x}_0\rangle$$

we have

(138) $$\alpha_k = \frac{1}{\sqrt{N-1}} \cos\left((2k+1)\theta\right) \qquad \beta_k = \sin\left((2k+1)\theta\right)$$

The amplitude of the state $|\underline{x}_0\rangle$, which we are looking for keeps increasing as long as

$$(2k+1)\theta \leq \frac{\pi}{2}$$

Optimum number $k_{opt} = T$ of steps is $(2T+1)\theta = \frac{\pi}{2}$. Using that for large N $\sin\theta \simeq \theta = \frac{1}{\sqrt{N}} \Rightarrow$

(139) $$\boxed{T = \frac{\pi}{4}\sqrt{N} + \vartheta(1)}$$

number of steps in Grover algorithm

and $\sin\left((2T+1)\theta\right) \simeq 1$.

I.e. after $\mathcal{O}(\sqrt{N})$ steps $|\underline{x}_0\rangle$ is approximated with probability close to 1 !

Implementation of $\overline{U}_S$

$$(140)\qquad |\underline{s}\rangle = H^{(n)}|\underline{0}\rangle = \frac{1}{2^{n/2}} \sum_{\underline{x}=0}^{2^n-1} |\underline{x}\rangle$$

i.e.

$$(141)\qquad \overline{U}_S = 2|\underline{s}\rangle\langle\underline{s}| - \mathbb{1} = H^{(n)}\left(2|\underline{0}\rangle\langle\underline{0}| - \mathbb{1}\right)H^{(n)}$$

$H^{(n)}$ is easy, but how about $2|\underline{0}\rangle\langle\underline{0}| - 1$, or equivalently $1 - 2|\underline{0}\rangle\langle\underline{0}|$?

$$1 - 2|\underline{0}\rangle\langle\underline{0}| = \overline{X}^{(n)}\left(1 - 2|\underline{1}\rangle\langle\underline{1}|\right)\overline{X}^{(n)}$$

$\overline{X}$: bitwise Pauli X

$1 - 2|\underline{1}\rangle\langle\underline{1}|$: changes sign of $|1111\ldots1\rangle$ only

$1 - 2|\underline{1}\rangle\langle\underline{1}|$ is unitary as

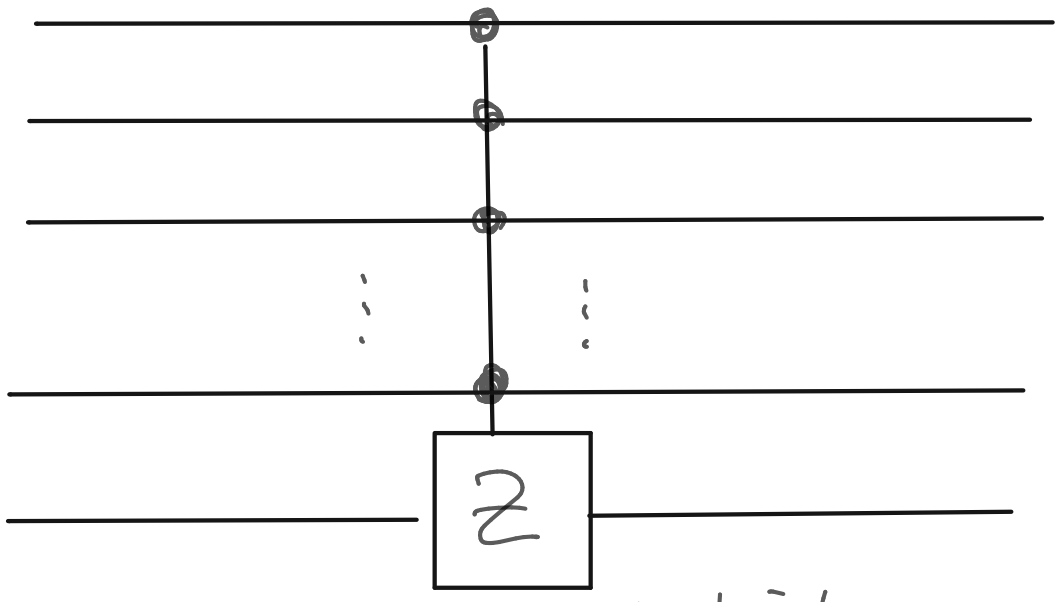
$$\left(1 - 2|\underline{1}\rangle\langle\underline{1}|\right)^+ = \left(1 - 2|\underline{1}\rangle\langle\underline{1}|\right)$$

and $\left(1 - 2|\underline{1}\rangle\langle\underline{1}|\right)\left(1 - 2|\underline{1}\rangle\langle\underline{1}|\right) =$

$$= 1 - 4|\underline{1}\rangle\langle\underline{1}| + 4|\underline{1}\rangle\langle\underline{1}| = 1 \quad \checkmark$$

and can be implemented by an N-fold controlled gate

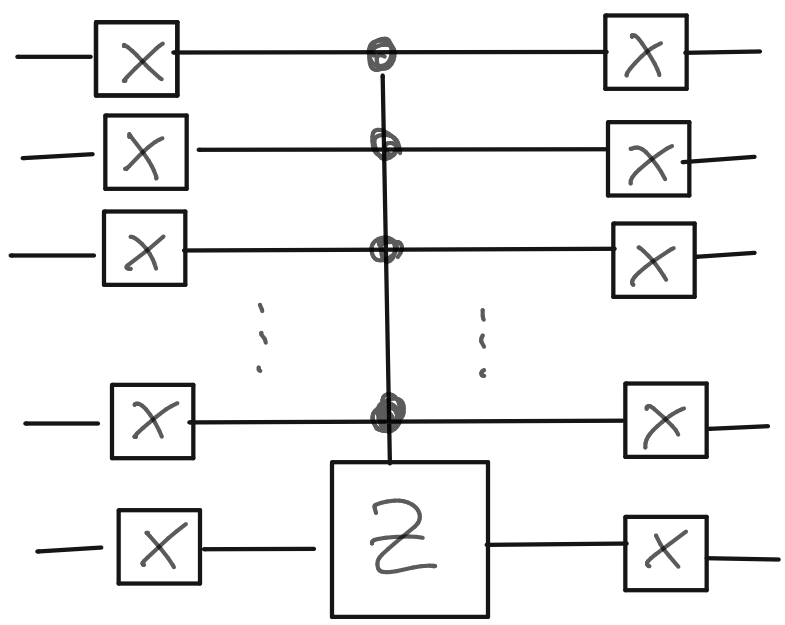
$1-2(|1\rangle\langle 1|)$



all of these bits need to be in $|1\rangle$ else gate does nothing

If all but the last qubit are in $|1\rangle$ and the last in $|0\rangle$ the state is unchanged. If the last qubit is in $|1\rangle$ the sign is flipped to, i.e.

So $\bar{U}_S$ is



This gate can be implemented with $\mathcal{O}(n = \log_2 N)$ elementary gates. I.e. Grovers search algorithm requires

(142) $\sim \sqrt{N}\ \text{poly}(\log N)$

gate operations.

One can show that Grovers algorithm is optimal for a search in an un-sorted list