④ If $f(0) = f(1)$: we measure 0 with proba 1.

else: we measure 1 with probability 1.

- Deutsch - Josza algorithm:

Problem 2: Given a function $f : \{0,1\}^n \longrightarrow \{0,1\}$ with a promise that f is

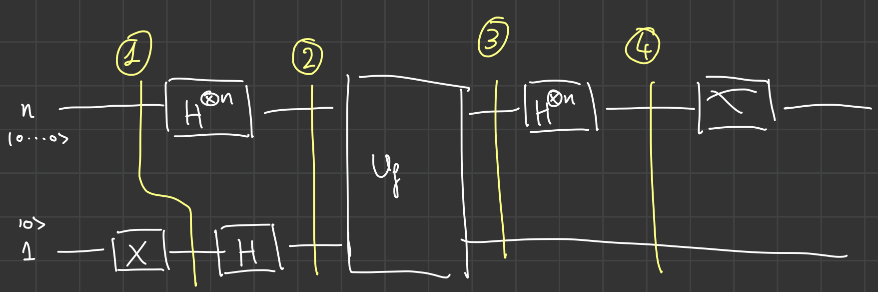
either - constant

or

- balanced $\left(\# f^{-1}(\{0\}) = \# f^{-1}(\{1\}) \right)$

We want to decide if f is balanced or constant.

(It is really specific, in maths we have the following example represented by this problem: if $f : (\mathbb{Z}/2\mathbb{Z})^n \longrightarrow \mathbb{Z}/2\mathbb{Z}$ is a group homomorphism.)



outcome is $(0, \ldots, 0)$: "constant"

outcome is not $(0, \ldots, 0)$: "balanced"

(Challenge: Write a function that creates the qubit $\frac{3}{5}|0\rangle + \frac{4}{5}|1\rangle$
↳ use phaseshifts)

Remark: • Notice that there is only one call to the function f.

Classically, a deterministic algorithm answering the Deutsch-Jozsa's problem needs to call f at least $2^{n-1}+1$ times.

⚠ If f is a group morphism (which is the most important case), only n calls to f are required.

Proof: ① $|0^n\rangle|1\rangle$

② We use the following proposition:

Proposition: let $x = (x_1, \dots, x_m) \in (\mathbb{Z}/2\mathbb{Z})^m$, then $H^{\otimes m}(|x\rangle) = \frac{1}{2^{m/2}} \sum_{y \in (\mathbb{Z}/2\mathbb{Z})^m} (-1)^{x \cdot y} |y\rangle$

where $x \cdot y = x_1 y_1 + \dots + x_m y_m$ is the scalar product.

Remark: When $x = 0$, we get $H^{\otimes m}(|0^n\rangle) = \frac{1}{2^{m/2}} \sum_{y \in (\mathbb{Z}/2\mathbb{Z})^m} |y\rangle$ → uniform superposition

Proof of the proposition.

• Note for $z \in \mathbb{Z}/2\mathbb{Z}$, we have $H(|z\rangle) = \frac{|0\rangle + (-1)^z |1\rangle}{\sqrt{2}}$

• $H^{\otimes m}(|x_1 \cdots x_m\rangle) = H(|x_1\rangle) \cdots H(|x_n\rangle)$

$$= \frac{1}{2^{m/2}} \left(|0\rangle + (-1)^{x_1}|1\rangle\right)\left(|0\rangle + (-1)^{x_2}|1\rangle\right) \cdots \left(|0\rangle + (-1)^{x_m}|1\rangle\right)$$

$$= \frac{1}{2^{m/2}} \sum_{y_1, \dots, y_m \in \mathbb{Z}/2\mathbb{Z}} (-1)^{x_1 y_1}|y_1\rangle \cdots (-1)^{x_m y_m}|y_m\rangle$$

- Internal state at ② is:

$$\frac{1}{2^{n/2}\sqrt{2}} \sum_{\substack{y\in(\mathbb{Z}/2\mathbb{Z})^n \\ z\in(\mathbb{Z}/2\mathbb{Z})}} (-1)^z |yz\rangle$$

③ : $\frac{1}{2^{n/2}\sqrt{2}} \sum_{y\in(\mathbb{Z}/2\mathbb{Z})^n} |y\rangle \left(|f(y)\rangle - |\overline{f(y)}\rangle \right)$

④ : $\frac{1}{2^n\sqrt{2}} \sum_{y\in(\mathbb{Z}/2\mathbb{Z})^n} \sum_{z\in(\mathbb{Z}/2\mathbb{Z})^n} (-1)^{y.z} |z\rangle \left(|f(y)\rangle - |\overline{f(y)}\rangle \right)$

$$= \sum_{z\in(\mathbb{Z}/2\mathbb{Z})^n} |z\rangle \otimes q_z$$

with $q_z = \frac{1}{2^n\sqrt{2}} \sum_{y\in(\mathbb{Z}/2\mathbb{Z})^n} (-1)^{y.z} \left(|f(y)\rangle - |\overline{f(y)}\rangle \right)$

<u>Measure:</u> We have to compute $\|q_z\|^2$ (this is the probability to get z as outcome).

In fact, we just need to do it when $z=0$

$$q_0 = \frac{1}{2^n\sqrt{2}} \sum_{y\in(\mathbb{Z}/2\mathbb{Z})^n} \left(|f(y)\rangle - |\overline{f(y)}\rangle \right)$$

<u>first case:</u> f is constant i.e $f(y)=a\ \forall y$

Then $q_0 = \frac{1}{2^n\sqrt{2}} \sum_{y\in(\mathbb{Z}/2\mathbb{Z})^n} \left(|a\rangle - |\bar{a}\rangle \right)$

$$= \frac{|a\rangle - |\bar{a}\rangle}{\sqrt{2}}$$

and $\|q_0\|^2 = 1$, hence the outcome is always 0.

Second case: f is balanced, i.e $\# \underbrace{f^{-1}(\{0\})}_{=A_0} = \# \underbrace{f^{-1}(\{1\})}_{=A_1} = 2^{n-1}$

$$q_0 = \frac{1}{2^n\sqrt{2}} \left(\sum_{y \in A_0} (|0\rangle - |1\rangle) + \sum_{y \in A_1} (|1\rangle - |0\rangle) \right)$$

$$= \frac{1}{2^n\sqrt{2}} \left(2^{n-1} (|0\rangle - |1\rangle) + 2^{n-1} (|1\rangle - |0\rangle) \right)$$

$$= 0$$

Conclusion: the outcome is never 0 $\blacksquare$

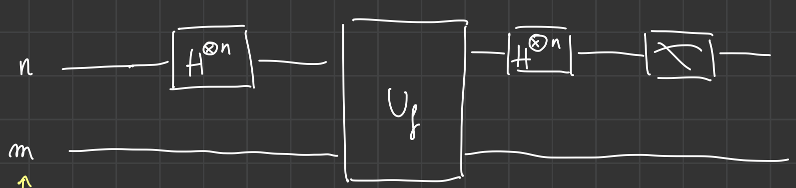
II. Simon's algorithm

Input: $f : (\mathbb{Z}/2\mathbb{Z})^n \longrightarrow X$ (a finite set) such that there exists $a \in (\mathbb{Z}/2\mathbb{Z})^n$, $(a \neq 0)$ such that $f(x) = f(y)$ iff $x = y$ or $x = y + a$

Question: find a

Example: If f is a group morphism (X is a group) and $\# \ker(f) = 2$, question is: compute $\ker(f)$.

Simon's circuit:



enough qubits to represent elements of X

Proposition: The outcome of Simon's circuit is a uniformly distributed random vector in

$$H_a = \langle a \rangle^{\perp} = \{ b \in (\mathbb{Z}/2\mathbb{Z})^n \text{ st } a.b = 0 \}$$

We postpone the proof of the proposition and now explain how to find a:

Method: (I assume $a \neq 0$)

Run Simon's algo several times until we get $(n-1)$ lineary independant vectors $b_1, \dots, b_{n-1}$.

* build $H_a = \mathrm{Span}(b_1, \dots, b_{n-1})$
* Compute $H_a^{\perp}$ and find a

Problem.

Let V be a $\mathbb{F}_q$ - vector space of dimension d. Let $v_1, \dots, v_m$ random vectors in V.

what is the probability that $v_1, \dots, v_m$ span V ?

We can pick a basis of V and work with coordinates.

The problem becomes:

What is the probability that a matrix

$$\begin{array}{c} v_1 \\ v_2 \\ \vdots \\ v_m \end{array} \left(\begin{array}{cccc} - & - & \cdots & - \\ - & - & \cdots & - \\ & & \vdots & \\ - & - & \cdots & - \end{array} \right) \updownarrow m \text{ lines}$$

$\longleftarrow d$ columns $\longrightarrow$

has rank d?

Assume $m \geq d$ (Otherwise the proba is 0)

Observation:

The matrix has rank d (i.e. full rank) if and only if its columns are linearly independent.

So the question becomes:

What is the proba that d random vectors in $\mathbb{F}_q^m$ are linearly independent?

It is: $$P_q^m = \frac{(q^m - 1)(q^m - q) \cdots (q^m - q^{d-1})}{q^{md}} = \left(1 - \frac{1}{q^m}\right)\left(1 - \frac{1}{q^{m-1}}\right) \cdots \left(1 - \frac{1}{q^{m-d+1}}\right)$$

Note that for $x, y \in [0,1]$,

$$(1-x)(1-y) = 1 - (x+y) + xy \geq 1 - (x+y)$$

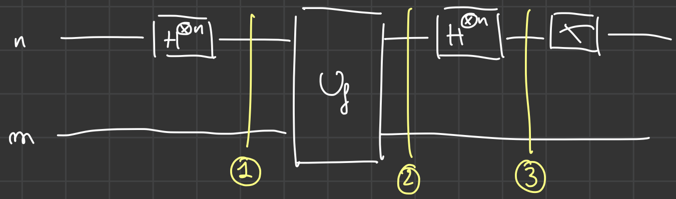
Here $$P_q^m \geq 1 - \left(\frac{1}{q^m} + \frac{1}{q^{m-1}} + \cdots + \frac{1}{q^{m-d+1}}\right)$$
$$\geq 1 - \frac{1}{q^{m-d+1}}\left(1 + \frac{1}{q} + \frac{1}{q^2} + \cdots\right)$$
$$\geq 1 - \frac{1}{q^{m-d}(q-1)}$$

When $m = d$: $P_q^d \geq 1 - \frac{1}{q-1}$ ($= 0$ for $q = 2$)

When $m = d+1$: $P_q^{d+1} \geq 1 - \frac{1}{q(q-1)}$ ($= \frac{1}{2}$ for $q = 2$)

When $m = d+k$ $P_q^{d+k} \geq 1 - \frac{1}{q^k(q-1)}$ ($= 1 - \frac{1}{2^k}$ for $q = 2$)

Come back to the Simon's circuit :



Analyzing Simon's circuit :

① $\frac{1}{2^{n/2}} \sum_{x \in (\mathbb{Z}/2\mathbb{Z})^n} |x\rangle |0^m\rangle$

② $\frac{1}{2^{n/2}} \sum_{x \in (\mathbb{Z}/2\mathbb{Z})^n} |x\rangle |f(x)\rangle$

③ $\frac{1}{2^n} \sum_{x \in (\mathbb{Z}/2\mathbb{Z})^n} \sum_{y \in (\mathbb{Z}/2\mathbb{Z})^n} (-1)^{x.y} |y\rangle |f(x)\rangle = \sum_{y \in (\mathbb{Z}/2\mathbb{Z})^n} |y\rangle \otimes q_y$

where $q_y = \frac{1}{2^n} \sum_{x \in (\mathbb{Z}/2\mathbb{Z})^n} (-1)^{x.y} |f(x)\rangle$

Measure : Assume again $a \neq 0$

$$G = (\mathbb{Z}/2\mathbb{Z})^n / \langle a \rangle$$

$$q_y = \frac{1}{2^n} \sum_{\{x, x+a\} \in G} \left((-1)^{x.y} |f(x)\rangle + (-1)^{(x+a).y} |f(x+a)\rangle \right)$$

$$= \frac{1}{2^n} \sum_{\{x, x+a\} \in G} \left(1 + (-1)^{a.y}\right) \left((-1)^{x.y} |f(x)\rangle \right)$$

$$= \frac{1}{2^n} \left(1 + (-1)^{a.y}\right) \sum_{\{x, x+a\} \in G} (-1)^{x.y} |f(x)\rangle$$

If $a.y = 1 \pmod 2$: $\quad q_y = 0$

If $a.y = 0 \pmod 2$: $\quad q_y = \frac{1}{2^{n-1}} \sum_{\{x, x+a\} \in G} (-1)^{x.y} |f(x)\rangle$

The $f(x)$ are pairwise distinct

So the $|f(x)\rangle$ are pairwise orthogonal

So $\|q_y\|^2 = \frac{1}{2^{2(n-1)}} \sum_{\{x, x+a\} \in G} 1 = \frac{1}{2^{n-1}}$

Conclusion : the proposition is proved!