Create a unitary single qubit gate taking $|0\rangle \longmapsto \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$.

$$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad \begin{array}{c} |0\rangle \\ \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & \\ i & \end{pmatrix} \end{array}$$

$$= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}$$

$$\begin{pmatrix} 1 & b \\ i & -ib \end{pmatrix} \begin{pmatrix} 1 & -i \\ \bar{b} & i\bar{b} \end{pmatrix} = \begin{pmatrix} 1+b\bar{b} & -i+ib\bar{b} \\ i-ib\bar{b} & 1+b\bar{b} \end{pmatrix} \stackrel{?}{=} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

---

n-qubit gate $= 2^n \times 2^n$ unitary matrix

$n=1$	2×2	$|0\rangle$ $|1\rangle$
$n=2$	4×4	$|00\rangle$ $|01\rangle$ $|10\rangle$ $|11\rangle$

infinitely many n-qubit gates (continuous space)

We approximate any desired gate using a universal finite gate set.

Bottom line: can compute any n-qubit gate & chain them together. (matrix multiplication)

Exercise: ① a unitary × unitary = unitary.

② inverse is also unitary.

Every quantum gate is reversible. $\mathcal{U}^{-1}$ "undoes" $\mathcal{U}$.

AND

in		out
0	0	0
0	1	0
1	0	0
1	1	1

Challenge: How to create a reversible quantum "AND" gate?

in			out		
in		out	in		out
0	0	0	0	0	0
0	1	0	0	1	0
1	0	0	1	0	0
1	1	0	1	1	1
0	0	1	0	0	1
0	1	1	0	1	1
1	0	1	1	0	1
1	1	1	1	1	0

becomes bijective.

eg. $|000\rangle \longmapsto |000\rangle$

idea:

$(x, y) \longmapsto (x, y \text{ XOR } f(x))$

make a unitary:

$$\begin{array}{c|cccccccc} & |000\rangle & |001\rangle & |010\rangle & |011\rangle & |100\rangle & |101\rangle & |110\rangle & |111\rangle \\ \hline |000\rangle & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ |001\rangle & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ |010\rangle & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ |011\rangle & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ |100\rangle & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ |101\rangle & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ |110\rangle & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ |111\rangle & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{array}$$

General principle: Let $f : \{0,1\}^n \longrightarrow \{0,1\}^k$ be classical f^n.

Then we can make a reversible quantum gate:

$$|\vec{x}\rangle\,|\vec{0}\rangle\,\big(|\vec{0}\rangle\big) \longmapsto |\vec{x}\rangle\,|f(\vec{x})\rangle\,\big(|\vec{0}\rangle\big)$$

input register n qubit

output register k qubits

extra

ignore

ignore

Call this gate $\mathcal{U}_f$.

notation $\vec{x}$ = vector ie. string of bits 00010011 0 ... length n

"Massive parallelism" in one gate, can "compute" f on all inputs.

$$\mathcal{U}_f\Big(\sum_{\vec{x}\in\{0,1\}^n} \alpha_{\vec{x}}\,|\vec{x}\rangle\,|\vec{0}\rangle\Big) = \sum_{\vec{x}\in\{0,1\}^n} \alpha_{\vec{x}}\,|\vec{x}\rangle\,|f(\vec{x})\rangle$$

$$\mathcal{U}_f\Big(\tfrac{1}{2}|00\rangle|0\rangle + \tfrac{1}{2}|01\rangle|0\rangle + \tfrac{1}{2}|10\rangle|0\rangle + \tfrac{1}{2}|11\rangle|0\rangle\Big)$$

$$= \tfrac{1}{2}|00\rangle|f(00)\rangle + \tfrac{1}{2}|01\rangle|f(01)\rangle + \tfrac{1}{2}|10\rangle|f(10)\rangle + \tfrac{1}{2}|11\rangle|f(11)\rangle$$

$\boxed{\text{BUT}}$ we can't see the state, we can only measure it!

If we measure (in computational basis) we get

$|00\rangle, |01\rangle, \ldots$

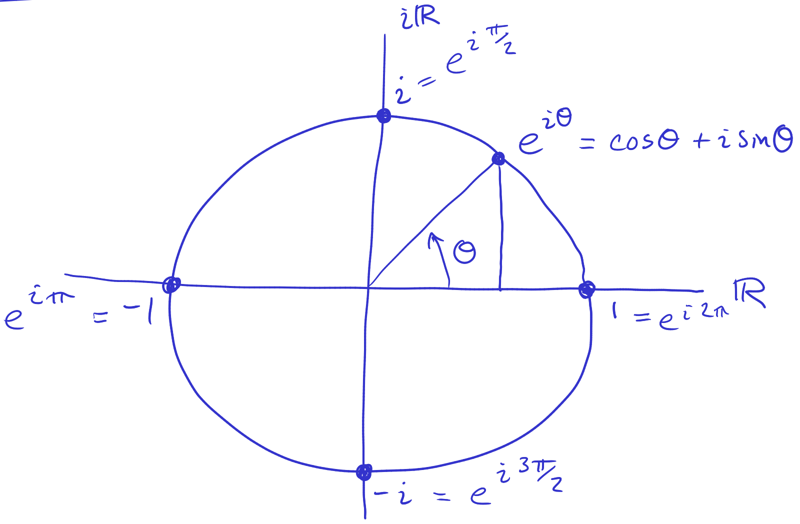
$|\vec{x}\rangle\,|f(\vec{x})\rangle$ for some random $\vec{x}$.

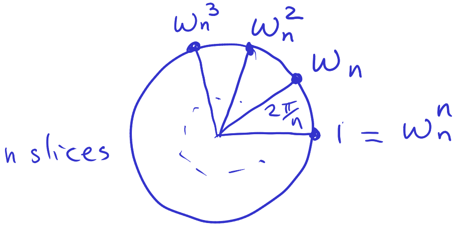
And we can't measure again.

Roots of unity in $\mathbb{C}$

$$re^{i\theta} = \begin{cases}\text{angle } \theta \\ \text{length } r\end{cases}$$

$$e^{i\theta} = \cos\theta + i\sin\theta$$



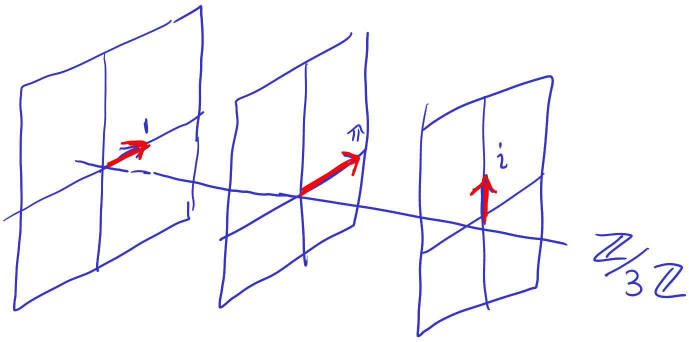


$$w_n = e^{i\frac{2\pi}{n}} = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right).$$

$$w_n^k = e^{ik\frac{2\pi}{n}} = \cos\left(\frac{2\pi k}{n}\right) + i\sin\left(\frac{2\pi k}{n}\right).$$

<u>The vector space of functions</u> $\{ f : \mathbb{Z}/_m\mathbb{Z} \longrightarrow \mathbb{C} \}$ is a vector space.

<u>eg.</u> $f : \mathbb{Z}/_3\mathbb{Z} \to \mathbb{C}$ given by $\begin{cases} f(0) = 1 \\ f(1) = \pi \\ f(2) = i \end{cases}$ "is" the vector $\begin{pmatrix} 1 \\ \pi \\ i \end{pmatrix}$



eg. $\begin{pmatrix} 1 \\ \omega_3 \\ \omega_3^2 \end{pmatrix}$