Classical Reversible Circuits:

Can construct any bijection $f : \{0,1\}^n \to \{0,1\}^n$ as a reversible circuit s.t.

$$\underbrace{x}_{n\text{ bit}}\ \underbrace{0}_{n+k\text{ bits}} \longmapsto \underbrace{x}_{n\text{ bit}}\ \underbrace{f(x)}_{n\text{ bits}}\ \underbrace{0}_{k\text{ bits}}$$

Classical Reversible Circuits on a Quantum Computer:

Fact: Any reversible classical circuit f is a unitary transformation: U_f

So we can perform it on a quantum computer:

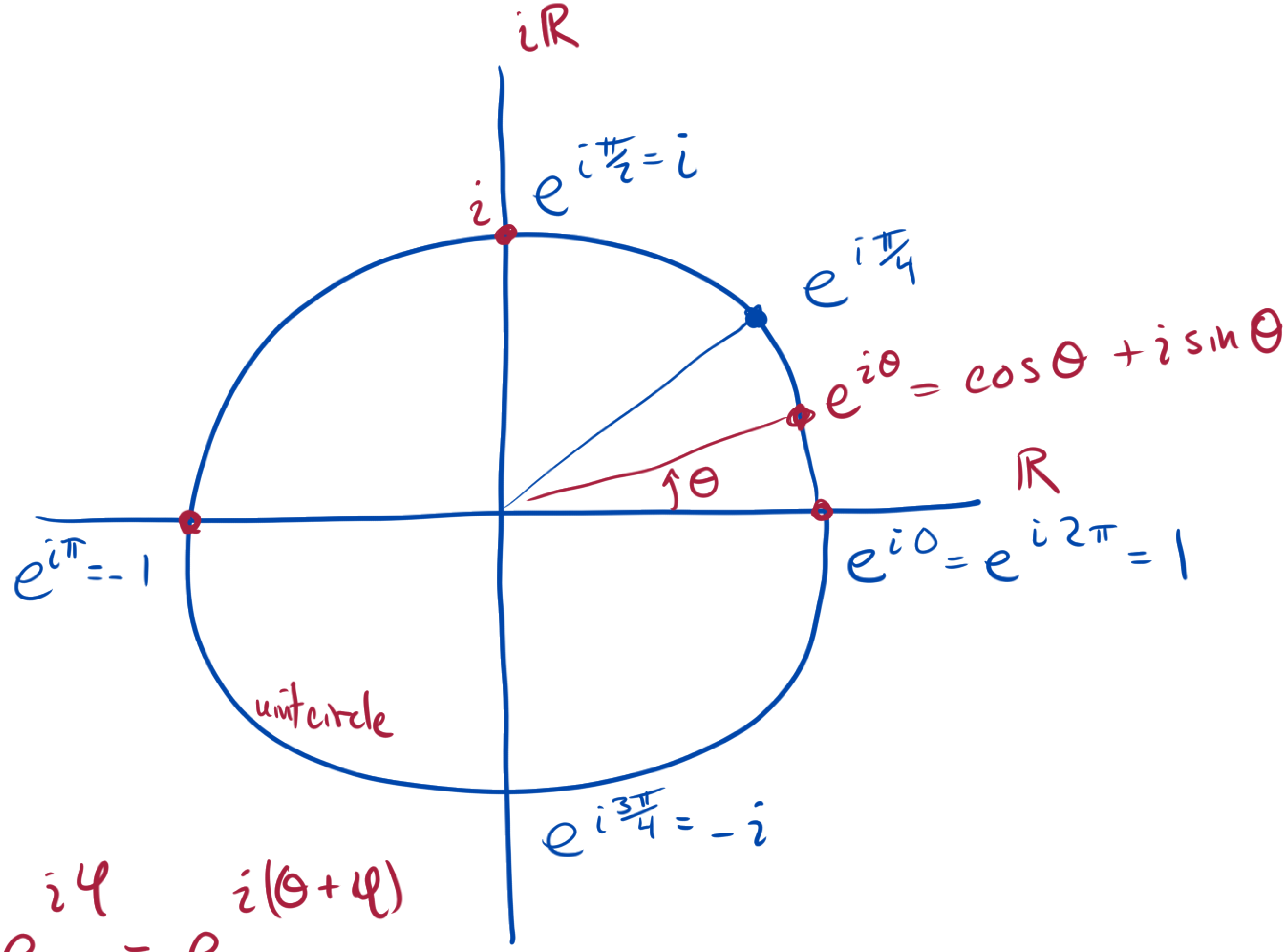
$$\underbrace{|x\rangle}_{\substack{n\text{ qubits}\\ \text{"register"}}}\underbrace{|0\rangle}_{n}\underbrace{|0\rangle}_{k} \longmapsto \underbrace{|x\rangle}_{n\text{ qubits}}\underbrace{|f(x)\rangle}_{n}\underbrace{|0\rangle}_{k}$$

"massive parallelism"

$$U_f \left(\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle |0\rangle \right) = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle |f(x)\rangle$$

"computes" $f(x)$ for all 2^n classical inputs simultaneously.

Roots of Unity in $\mathbb{C}$



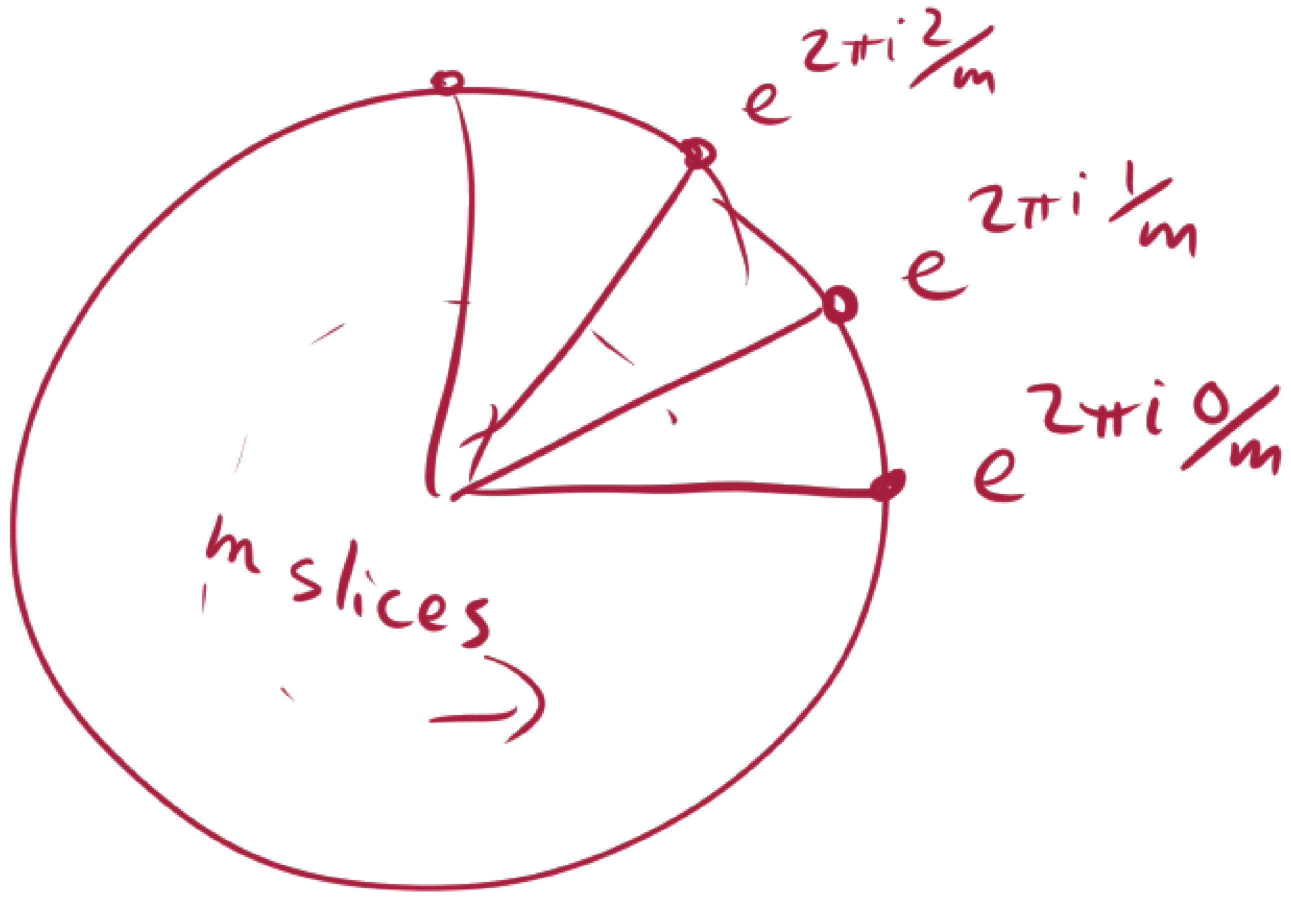
$$e^{i\theta} e^{i\varphi} = e^{i(\theta+\varphi)}$$

The m^{th} roots of unity are

$$\omega_m = e^{2\pi i/m}$$

$$\omega_m^k = e^{2\pi i k/m}$$

$k = 0, 1, \ldots, m-1$



$$\boxed{\omega_m^m = 1}$$

The Space of Functions $\{ f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{C} \}$ is a vector space.

Eg. $f : \mathbb{Z}/3\mathbb{Z} \to \mathbb{C}$ given by

$$f(0) = 1$$
$$f(1) = \pi$$
$$f(2) = i$$

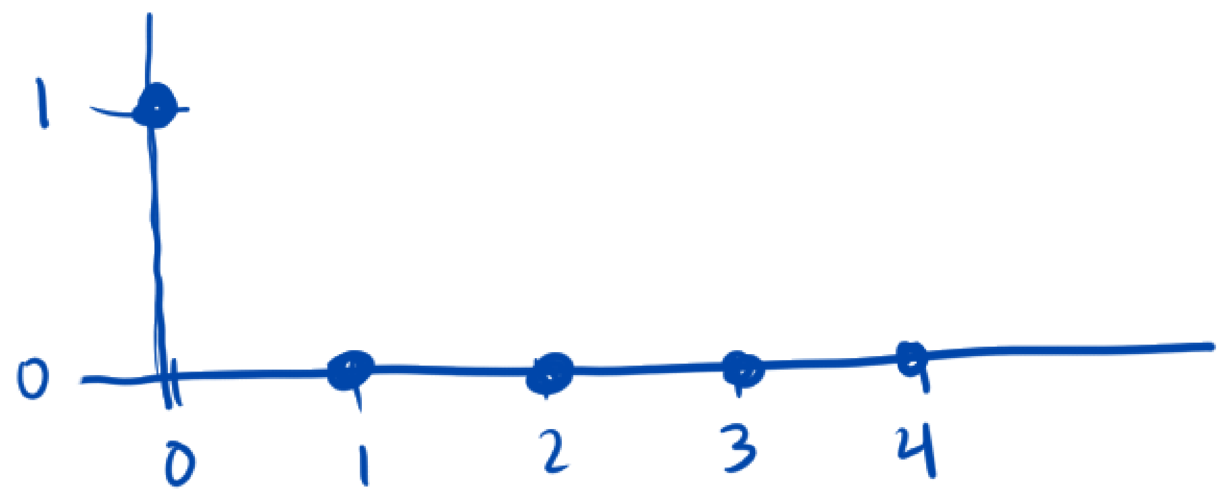
"is" the vector $\begin{pmatrix} 1 \\ \pi \\ i \end{pmatrix}$

in "standard" basis

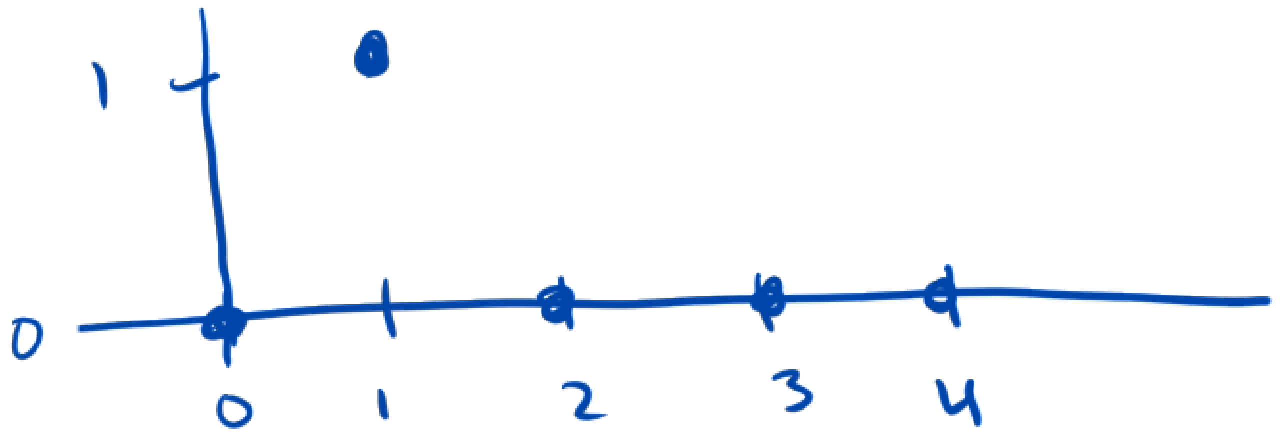
$$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

Standard Basis

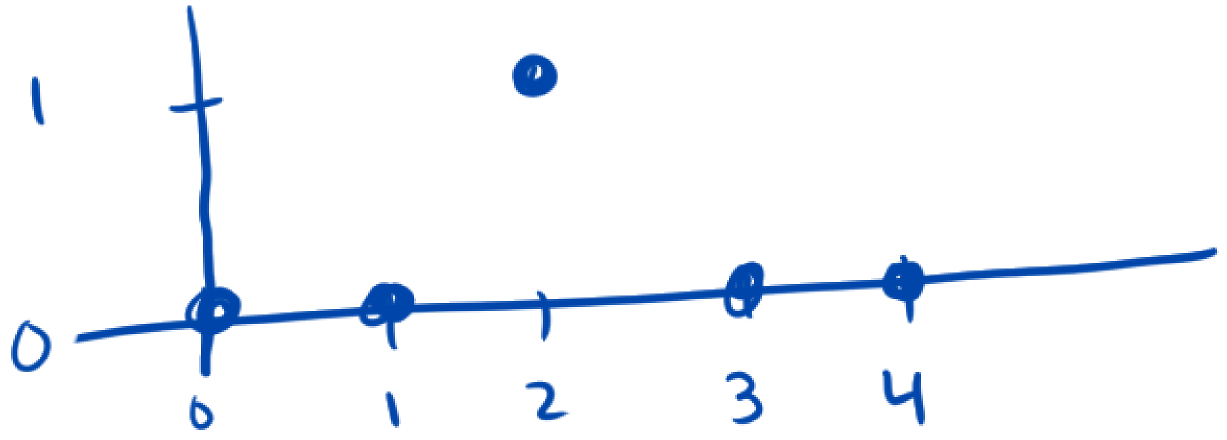
$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ \vdots \end{pmatrix}$$



$$\begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \end{pmatrix}$$

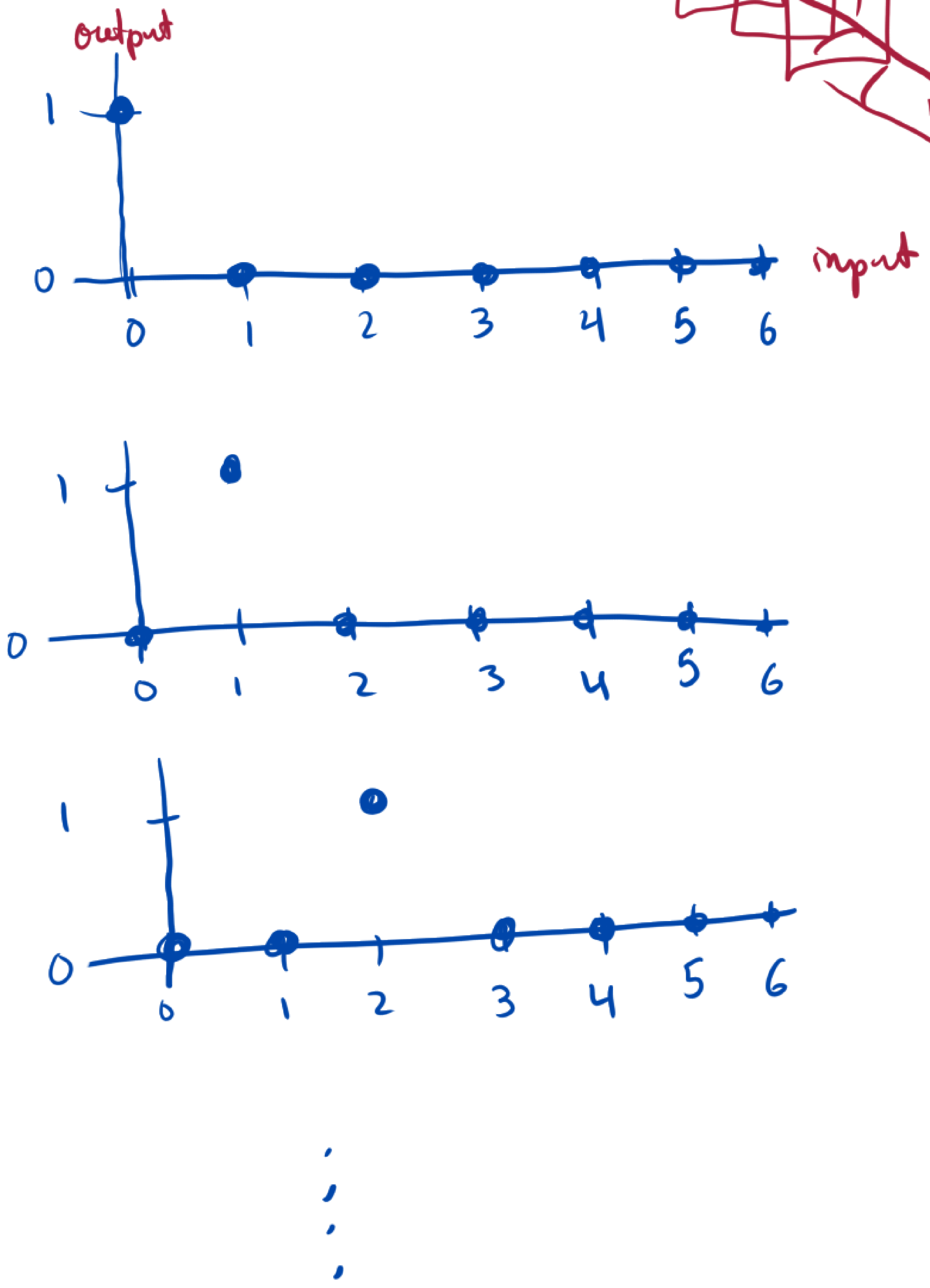


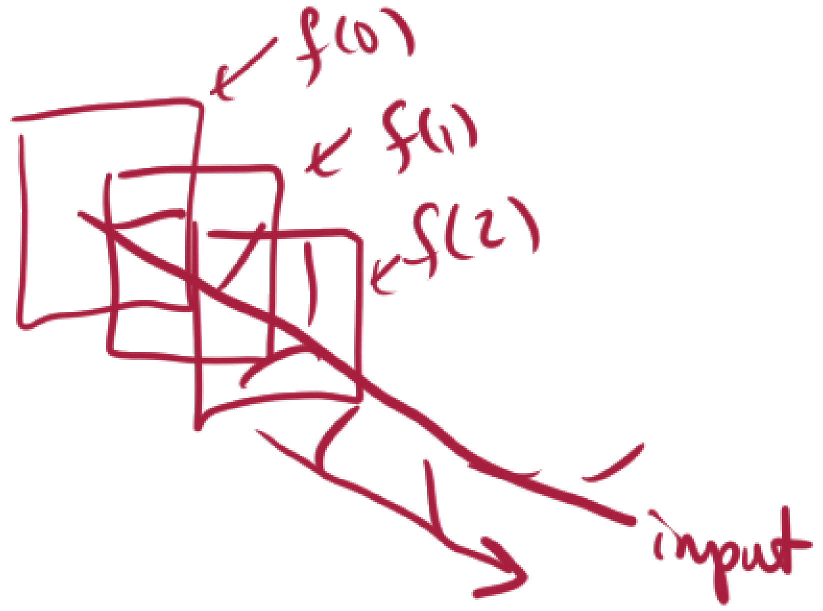
$$\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ \vdots \end{pmatrix}$$



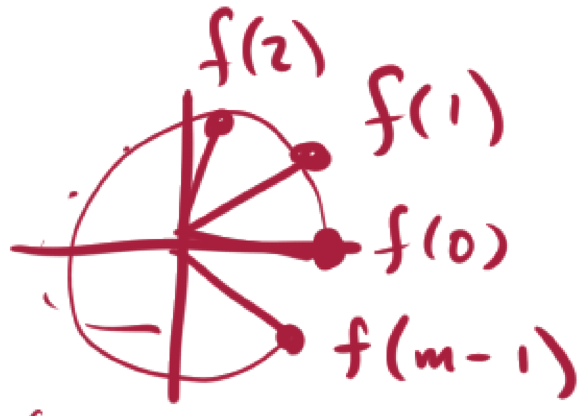
$\vdots$

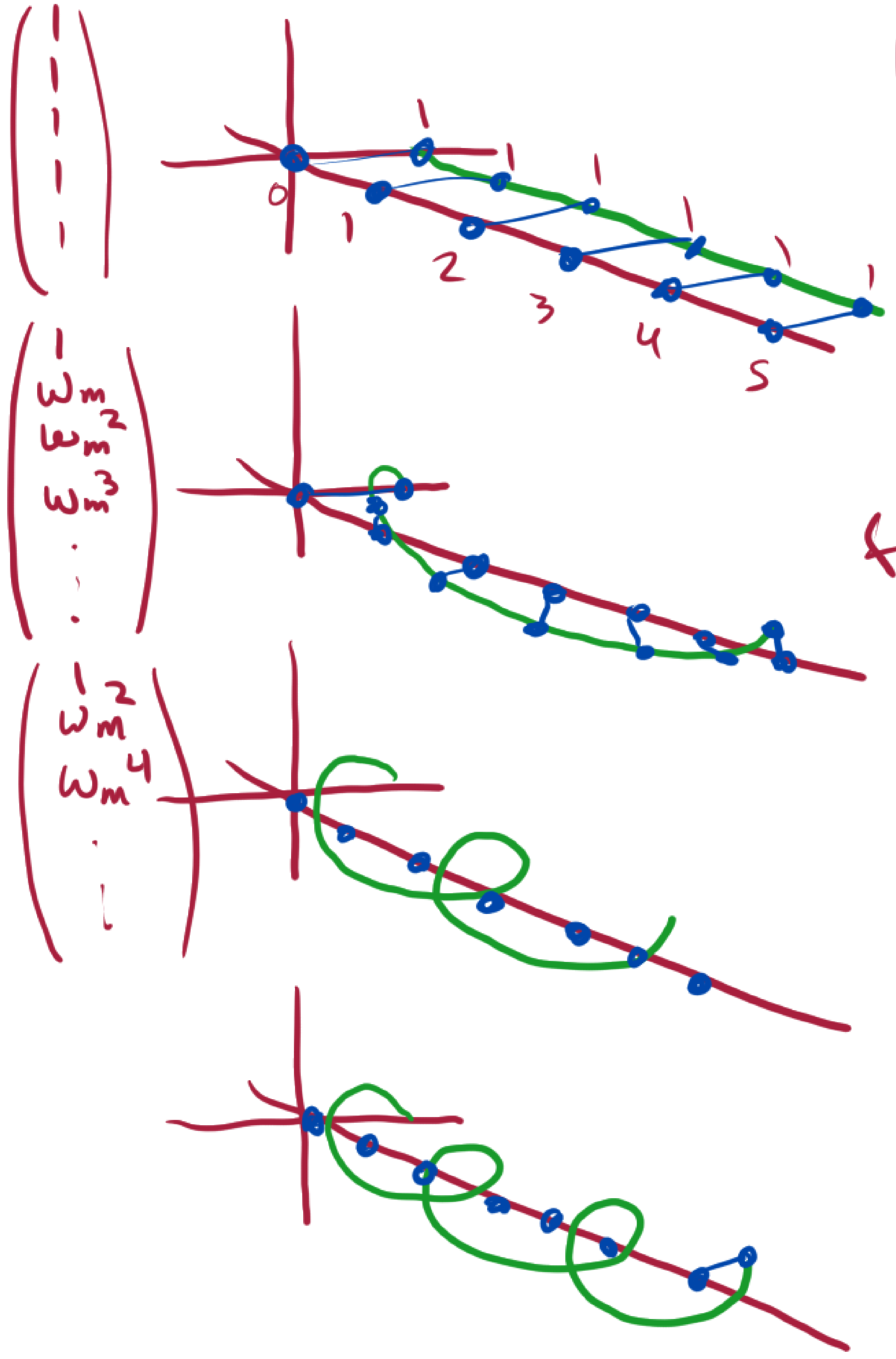
Standard Basis

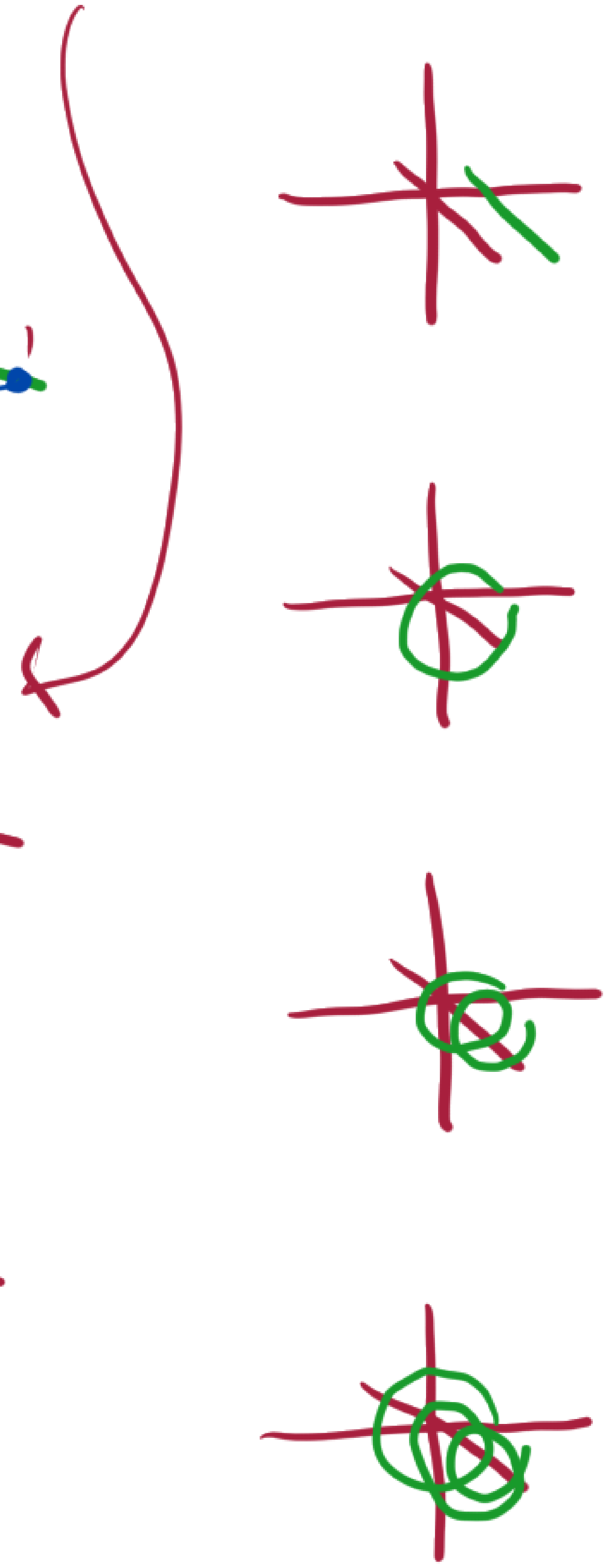


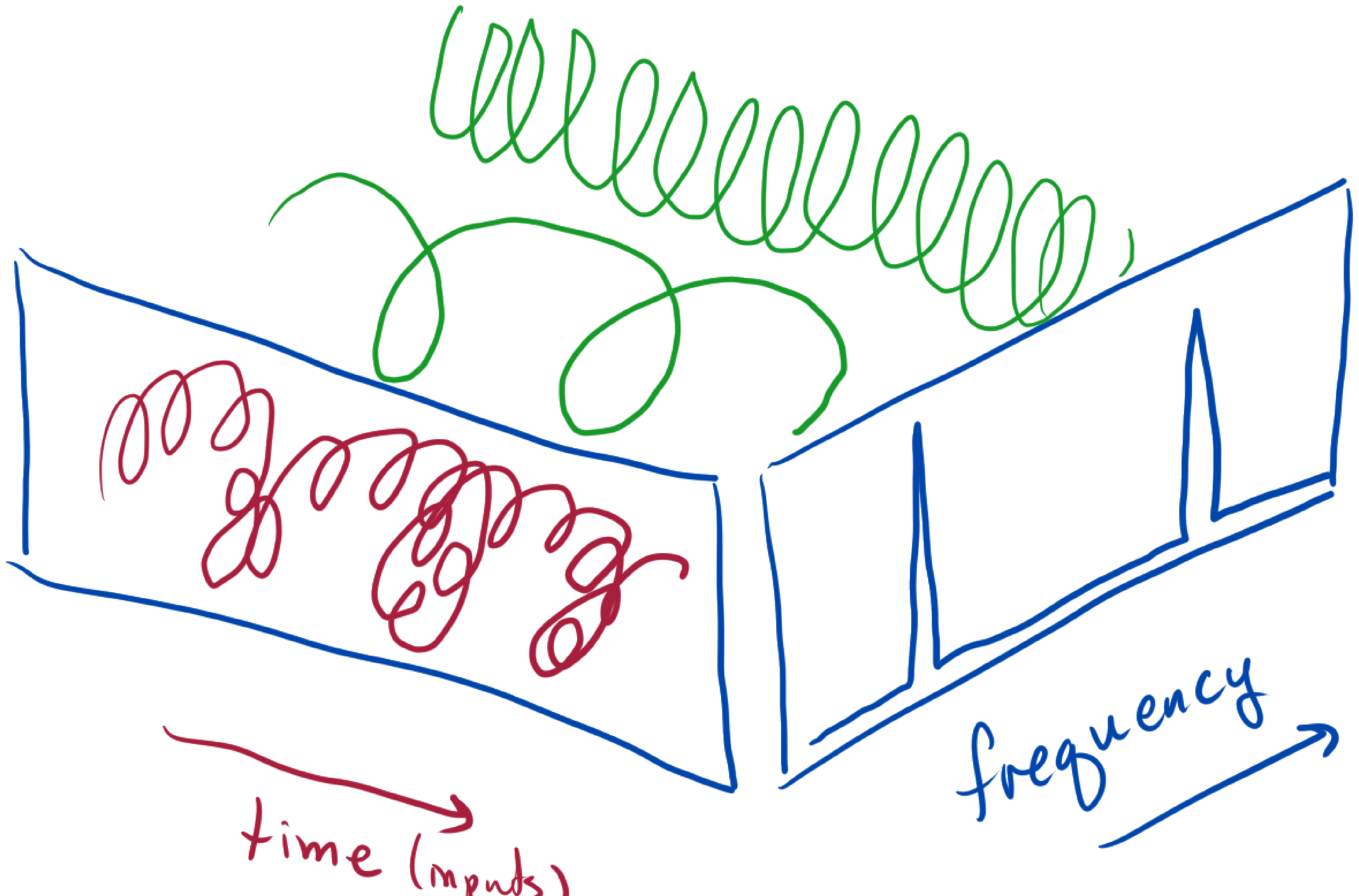


Fourier Basis









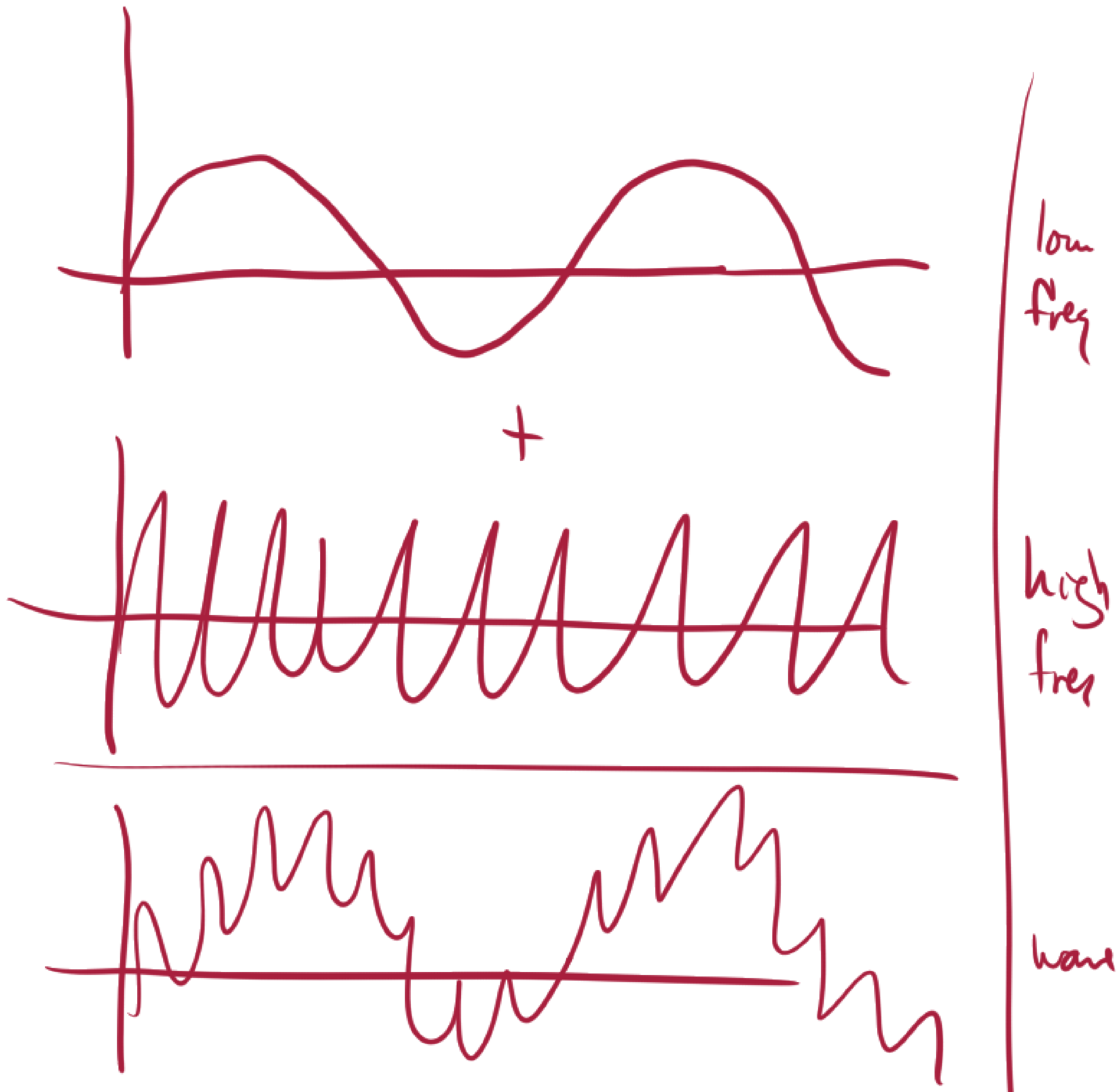
(the waveform)

(which waves to add)

Standard Basis

Fourier Basis

$$(f_1+f_2)(x)$$
$$= f_1(x) + f_2(x)$$



The Quantum Fourier Transform

$m \times m$, $\omega = \omega_m = e^{2\pi i/m}$

$$F_m = \frac{1}{\sqrt{m}} \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{m-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2m-2} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \cdots & \omega^{3m-3} \\ 1 & \omega^4 & \omega^8 & \omega^{12} & \cdots & \omega^{4m-4} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 1 & \omega^{m-1} & \omega^{2m-2} & \omega^{3m-3} & \cdots & \omega^{(m-1)m-1} \end{pmatrix}$$

$(ij)^{th}$ entry $= \omega_m^{ij}$

Examples.

$$\begin{pmatrix} 1 & 1 \\ 1 & \omega \end{pmatrix}$$

$m = 2$

$$\omega_2 = -1 \qquad F_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Hadamard

$(-1)^2 = 1$

$m = 4$

$$\omega_4 = i \qquad F_4 = \frac{1}{\sqrt{4}} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$$

$i^2 = -1$

$i^3 = -i$

$(-i)^2 = -1$

$(-i)^3 = i$

Input: vector $\vec{v}$ or function $f : \mathbb{Z}/_m\mathbb{Z} \to \mathbb{C}$

Output: $F_m \vec{v}$ or $\hat{f} : \mathbb{Z}/_m\mathbb{Z} \to \mathbb{C}$

Formula for new coefficients:

$$(F_m V)_n = \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} V_k \, \omega_m^{nk}$$

or

$$\hat{f}(n) = \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} f(k) \, \omega_m^{nk}$$

Computer

Demo

Runtime?

Classical: discrete fourier transform via matrix multiplication

$$O(m^2)$$

Fast Fourier Transform: $O(m \log(m))$

Quantum Fourier Transform: F_m is a unitary matrix

$$\sum_{x=0}^{m-1} f(x)|x\rangle \longmapsto \sum_{x=0}^{m-1} \hat{f}(x)|x\rangle$$

$$= \frac{1}{\sqrt{m}} \sum_{x=0}^{m-1} \sum_{k=0}^{m-1} \omega_m^{xk} f(k)\,|x\rangle$$

Quantum Fourier Transform: F_m is a unitary matrix

$$\sum_{x=0}^{m-1} f(x)|x\rangle \longmapsto \sum_{x=0}^{m-1} \hat{f}(x)|x\rangle$$

$$= \frac{1}{\sqrt{m}} \sum_{x=0}^{m-1} \sum_{k=0}^{m-1} \omega_m^{xk} f(k)\,|x\rangle$$

Can be implemented with $O(\log_2^2(m))$ gates

($\boxed{H}$ and a controlled phase gates)