§4 Quantum Computers & Shor's Algorithm

§4.1 Classical Computers

$|01001011\rangle$

$\left[\begin{array}{l} |101\rangle \\ |1\rangle|0\rangle|1\rangle \\ |5\rangle \end{array}\right.$ the same

Q: is $|5\rangle$ $|101\rangle$ or $|00001011\rangle$?

If it matters $|5\rangle_3$

Classical computer

bitstrings → bitstrings

What can I do on one bit?

- ~~$f(|i\rangle) = |0\rangle$~~
- ~~$f(|i\rangle) = |1\rangle$~~
- identity 1
- the not operator

  $X(|0\rangle) = |1\rangle$

  $X(|1\rangle) = |0\rangle$

only four classical operations

Want reversible functions

$1|i\rangle = |i\rangle$

Weird idea:
make this into a vector space.

Formally: VS generated by

$|0\rangle_n, |1\rangle_n, \dots, |2^n-1\rangle_n$.

i.e. formal sums

$a_0|0\rangle_n + a_1|1\rangle_n + \dots + a_{2^n-1}|2^n-1\rangle_n$

$a_i \in \mathbb{C}$.

This is basically $\mathbb{C}^{2^n}$

$n=1$

$a|0\rangle + b|1\rangle$

$|0\rangle \leftrightarrow \begin{bmatrix}1\\0\end{bmatrix}$ $|1\rangle \leftrightarrow \begin{bmatrix}0\\1\end{bmatrix}$.

$1 \leftrightarrow \begin{bmatrix}1&0\\0&1\end{bmatrix}$ $\begin{bmatrix}1&1\\0&0\end{bmatrix}$

$X \leftrightarrow \begin{bmatrix}0&1\\1&0\end{bmatrix}$ $\begin{bmatrix}0&0\\1&1\end{bmatrix}$

define n by

$n(|x\rangle) = x|x\rangle$

$n(|0\rangle) = 0|0\rangle = \vec{0}$

$n(|1\rangle) = 1|1\rangle = |1\rangle$

$n \leftrightarrow \begin{bmatrix}0&0\\0&1\end{bmatrix}$

$\bar{n} = 1-n$

$\bar{n}(|0\rangle) = |0\rangle - \vec{0} = |0\rangle$

$\bar{n}(|1\rangle) = |1\rangle - |1\rangle = \vec{0}$.

$\bar{n} \leftrightarrow \begin{bmatrix}1&0\\0&0\end{bmatrix}$

2 bits $n=2$

$|00\rangle \leftrightarrow \begin{bmatrix}1\\0\\0\\0\end{bmatrix}$ $|01\rangle \leftrightarrow \begin{bmatrix}0\\1\\0\\0\end{bmatrix}$ $|10\rangle \leftrightarrow \begin{bmatrix}0\\0\\1\\0\end{bmatrix}$ $|11\rangle \leftrightarrow \begin{bmatrix}0\\0\\0\\1\end{bmatrix}$

formally: tensor product $\begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}1\\0\\0\\0\end{bmatrix}$

$|1\rangle \otimes |0\rangle = |10\rangle$

rule 13: $|K\rangle_n$ I have a 2^n-entry column vector w/ a 1 in the $k+1$st position

$|5\rangle_3 \leftrightarrow \begin{bmatrix}0\\0\\0\\0\\0\\1\\0\\0\end{bmatrix}$ $|3\rangle_3 \leftrightarrow \begin{bmatrix}0\\0\\0\\1\\0\\0\\0\\0\end{bmatrix}$

Swap operator: $S|xy\rangle = |yx\rangle$

Can build this out of pieces.

$$S = n\otimes n + \bar{n}\otimes\bar{n} + (X\otimes X)(n\otimes\bar{n}) + (X\otimes X)(\bar{n}\otimes n)$$

$$S(|01\rangle) = \cancel{\vec{0}\otimes|1\rangle} + \cancel{|0\rangle\otimes\vec{0}} + \cancel{\vec{0}\otimes\vec{0}} + |1\rangle\otimes|0\rangle = |10\rangle$$

Notation: super clunky

$$1\otimes 1\otimes X\otimes 1\otimes 1\otimes n\otimes 1\otimes 1 = X_5 n_2$$

$$S_{ij} = n_i n_j + \bar{n}_i \bar{n}_j + (X_i X_j)(n_i \bar{n}_j + \bar{n}_i n_j)$$

Controlled not C_{ij}

if i^{th} bit is 0, do nothing

if i^{th} bit is 1, flip j^{th} bit

$C_{10}|xy\rangle = |x\rangle|x \oplus y\rangle$

where $\oplus$ represents mod-2 addition

or exclusive-or

ex!

$C_{10}|11\rangle = |1\rangle|1\oplus 1\rangle$

$= |1\rangle|0\rangle = |10\rangle.$

$C_{10}|01\rangle = |0\rangle|0\oplus 1\rangle = |01\rangle$

Facts: $S_{ij} = C_{ij} C_{ji} C_{ij}$

$C_{ij} = \bar{n}_i + X_j n_i$

$Z = \bar{n} - n$

single-bit operator

$Z(|0\rangle) = |0\rangle$

$Z(|1\rangle) = -|1\rangle$

$\bar{n} \Leftrightarrow \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$

$n \Leftrightarrow \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$

$Z \Leftrightarrow \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

ZX

$|0\rangle \mapsto -|1\rangle \begin{bmatrix} 0 \\ -1 \end{bmatrix}$

$|1\rangle \mapsto |0\rangle \begin{bmatrix} 1 \\ 0 \end{bmatrix}$

XZ

$|0\rangle \mapsto |1\rangle \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

$|1\rangle \mapsto -|0\rangle \begin{bmatrix} -1 \\ 0 \end{bmatrix}$

$ZX = -XZ$

"anticommute"

$|0\rangle \neq \vec{0}$

$\begin{bmatrix} 1 \\ 0 \end{bmatrix} \neq \begin{bmatrix} 0 \\ 0 \end{bmatrix}$

Ket

$n = \frac{1}{2}(1 - Z)$

$\bar{n} = \frac{1}{2}(1 + Z)$

$$C_{ij} = \frac{1}{2}(1+Z_i) + \frac{1}{2} X_j (1-Z_i)$$

$$= \frac{1}{2}(1+X_j) + \frac{1}{2} Z_i (1-X_j)$$

Hadamard Transformation

$$H = \frac{1}{\sqrt{2}}(X+Z) \longleftrightarrow \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$X^2 = 1 = Z^2$$

we can check: $H^2 = 1$.

$$HXH = Z$$
$$HZH = X$$
$$\Rightarrow \quad C_{ji} = (H_i H_j) C_{ij} (H_i H_j)$$