A Primer on

Classical and Quantum

Error-Correction

Miami 2017

P. Ramond
University of Florida

Classical Information

Classical Error-Correction

Quantum Information

Quantum Error-Correction

Examples

Classical Information

- *"seminar in five minutes"*, information.
- *"asnxwzzyq!4htic"*, no information, but could be a coded message!

Receiver rates information in terms of its value.

Transfer of information is the focus at the Bell Telephone Company.

Shannon (1948): defines Information

- Independently of sender or receiver.
- Probabilistically

$$H(A = \{p_1, p_2, \ldots, p_n\}) = -\sum_i^n p_i \log_2 p_i \qquad \textit{Shannon Entropy}$$

Tukey: bit as the unit of information:

$$n_{\text{bits}} \equiv \log_2(2^n) = n.$$

Shannon's Noiseless Coding Theorem:

- If the number of available bits per message is greater than $H(A)$, N-dimensional sequences of messages from A can be coded with probability of error less than ϵ.

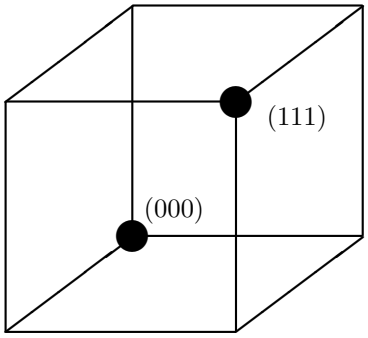
- If the number of available bits is less that $H(A)$, the probability of error is greater than $1 - \epsilon$.

Transmission Fidelity F: probability that the decoded message is the same as the original message.

Classical Error-Correction

Three bits $(x_1, x_2, x_3),\ x_i = 0, 1$

Hamming put the eight words at the vertices of a cube



Codewords at the vertices (000), (111).

Single flip errors are unambiguously identified.

Double flip errors are ambiguous.

Hamming weight: the number of "ones" in a word.

Hamming distance: the number of flips between two words.

Hamming sphere: the "sphere" centered at the codeword with radius equal to the number flips.

Perfect code: Codewords and their Hamming spheres saturate all words.

Classical codes $[\,n,\,k,\,d\,]$

n codewords length in bits

$k < n$ length of the messages

d *minimum* distance between codewords

$[\,7,\,4,\,3\,]$ Hamming code

- (4×7) generator matrix

$$G = (I_4|A) = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix},$$

- (3×7) parity check matrix

$$H = (-A^T|I_3) = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

$$GH^T = 0, \pmod 2$$

Generator inserts $2^{k=4}$ bits messages into $n = 7$ bits codewords,

G rows define four independent codewords.

Error Detection

$$w \longrightarrow w'$$

Recipient computes the Error Syndrome:

- $Hw' = 0$: no error, w' is a codeword

- $Hw' \neq 0$: error(s)

H chosen such that such that the seven locations of a *single* flip correspond to a unique error syndrome:

$$Hw' = \begin{pmatrix}1\\0\\0\end{pmatrix} \quad \begin{pmatrix}0\\1\\0\end{pmatrix} \quad \begin{pmatrix}0\\0\\1\end{pmatrix} \quad \begin{pmatrix}1\\1\\0\end{pmatrix} \quad \begin{pmatrix}1\\0\\1\end{pmatrix} \quad \begin{pmatrix}0\\1\\1\end{pmatrix} \quad \begin{pmatrix}1\\1\\1\end{pmatrix}$$

for one flip in the first, second, ..., seventh positions

Only Classical errors are flips, $X = \sigma_1$

Number of points in a Hamming sphere of radius h for $[\,n,\,k,\,d\,]$ Code:

$$M(n,h) = 1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{h}$$

h: largest integer in $d/2 - 1$

As many (2^k) codewords as Hamming spheres

Total number of points $= 2^k M(n,h)$

$$2^k M(n,h) = 2^n \qquad \longrightarrow \quad \text{Perfect code}$$

Golay (co-inventor of Hamming's code) discovered several perfect codes:

$$\sum_{i=0}^{2} \binom{90}{i} = 2^{12} \qquad \longrightarrow \quad \text{alas not a code}$$

$$\sum_{i=0}^{3} (2-1)^i \binom{23}{i} = 2^{11} \qquad \longrightarrow \quad \text{single error} - \text{correcting binary code}$$

extend to Galois Fields: e.g. ternary qubits (qutrits)

$$\sum_{i=0}^{2} (3-1)^i \binom{11}{i} = 3^5 \qquad \longrightarrow \quad \text{ternary (p = 3) perfect two} - \text{error correcting code}$$

Path to the Leech Lattice & Sporadic Groups

Many more error-correcting classical codes ...

Quantum Information

Use quantum mechanics to read, store, manipulate and transfer information.

• Allowed operations on quantum states are linear reversible unitary transformations, $\mathcal{U}^\dagger\mathcal{U} = \mathcal{U}\mathcal{U}^\dagger = 1$,

$$\mathcal{U}\big[|\,\psi\,\rangle + \mathcal{U}|\,\phi\,\rangle\big] = \mathcal{U}|\,\psi\,\rangle + \mathcal{U}|\,\phi\,\rangle.$$

• In the classical world, I can copy my passport for safety. Define a *duplicator* $\mathcal{D}$, whose action on any states $|\,\psi\,\rangle$ and $|\,\phi\,\rangle$ is given by

$$\mathcal{D}|\,\psi\,\rangle \otimes |\,\cdot\,\rangle = |\,\psi\,\rangle \otimes |\,\psi\,\rangle \otimes |\,\cdot\,\rangle, \qquad \mathcal{D}|\,\phi\,\rangle \otimes |\,\cdot\,\rangle = |\,\phi\,\rangle \otimes |\,\phi\,\rangle \otimes |\,\cdot\,\rangle$$

where $|\,\cdot\,\rangle$ denotes the extra room need for unitary duplication. BUT

$$\begin{aligned}
\mathcal{D}\big[|\,\psi\,\rangle + |\,\phi\,\rangle\big] \otimes |\,\cdot\,\rangle &= (|\,\psi\,\rangle + |\,\phi\,\rangle) \otimes (|\,\psi\,\rangle + |\,\phi\,\rangle) \otimes |\,\cdot\,\rangle, \\
&= |\,\psi\,\rangle \otimes |\,\psi\,\rangle \otimes |\,\cdot\,\rangle + |\,\phi\,\rangle \otimes |\,\phi\,\rangle \otimes |\,\cdot\,\rangle + \Big[|\,\psi\,\rangle \otimes |\,\phi\,\rangle + |\,\phi\,\rangle \otimes |\,\psi\,\rangle\Big] \otimes |\,\cdot\,\rangle \\
&\neq \mathcal{D}|\,\psi\,\rangle \otimes |\,\cdot\,\rangle + \mathcal{D}|\,\phi\,\rangle \otimes |\,\cdot\,\rangle,
\end{aligned}$$

$\mathcal{D}$ is not a linear operator : no − cloning theorem

• Classical computers proceed by logical operations e.g. the non-reversible **NAND** gate maps two pieces of information into one

Why Bother?

Quantum Parallelism

$$x \quad \longrightarrow \quad f(x),\ x = 0, 1$$

$f(0) = 0, 1$ and $f(1) = 0, 1$. $f(x)$ requires four pieces of information.

How many pieces of information required in the quantum case?

"Bit" $\longrightarrow$ "Qubit" = two-dimensional Hilbert space. Important operations:

$$\mathrm{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{Flip}, \quad \mathrm{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{Phase}, \quad \mathrm{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \text{Hadamard}$$

David Deutsch (1985):

$$\mathcal{U}_f : \quad |\, x \,\rangle \otimes |\, y \,\rangle \quad \longrightarrow \quad |\, x \,\rangle \otimes |\, y + f(x) \,\rangle$$

$$|\, \Psi_D \,\rangle = \Big[\mathrm{H} \otimes \mathrm{H}\Big]\Big[X \otimes X\Big]|\, 0 \,\rangle \otimes |\, 0 \,\rangle$$

"Constant Case": $f(0) = f(1)$

$$|\, \Psi_{const} \,\rangle = \mathcal{U}_f |\, \Psi_D \,\rangle = \frac{1}{2}\big[|\, 0 \,\rangle - |\, 1 \,\rangle\big] \otimes \big[|\, f(0) \,\rangle - |\, 1 + f(0) \,\rangle\big]$$

"Balanced Case": $f(0) \neq f(1) \rightarrow f(1) = 1 + f(0)$

$$|\, \Psi_{bal} \,\rangle = \mathcal{U}_f |\, \Psi_D \,\rangle = \frac{1}{2}\big[|\, 0 \,\rangle + |\, 1 \,\rangle\big] \otimes \big[|\, f(0) \,\rangle - |\, 1 + f(0) \,\rangle\big].$$

$$\frac{1}{\sqrt{2}}\big[\langle\, 0 \,| - \langle\, 1 \,|\big] \begin{cases} |\, \Psi_{const} \,\rangle \neq 0 & \text{constant} \\ |\, \Psi_{bal} \,\rangle = 0 & \text{balanced} \end{cases} .$$

One "measurement" determines half possible outcomes

without destroying the state!

Three Qubits

Hamming cube in a three qubits Hilbert space

$$|\,\psi_{Ham}\,\rangle = \alpha|\,000\,\rangle + \beta|\,111\,\rangle$$

Defined by two commuting idempotents stabilizers

$$S_1 = (Z \otimes I \otimes Z) \equiv (Z, I, Z) \equiv Z_{13}, \qquad S_2 = Z_{23}$$

$$S_a|\,\psi_{Ham}\,\rangle = +|\,\psi_{Ham}\,\rangle, \qquad a = 1, 2.$$

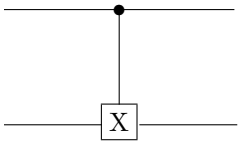
Append to $|\,\psi_{in}\,\rangle = \alpha|\,0\,\rangle + \beta|\,1\,\rangle$ a two-qubit ancillary Hilbert space

$$|\,\Psi_{in}\,\rangle \equiv \big[\alpha|\,0\,\rangle + \beta|\,1\,\rangle\big] \otimes |\,00\,\rangle = \alpha|\,000\,\rangle + \beta|\,100\,\rangle.$$

Generate the Hamming ket by unitary transformation

$$|\,\psi_{Ham}\,\rangle = \mathcal{U}_{Ham}|\,\psi_{in}\,\rangle$$

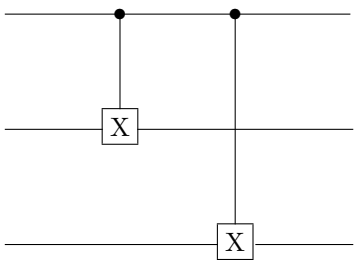
Introduce the CNOT $2-2$ gate:



If the top input line is $|\,0\,\rangle$ the lower line goes through unaffected,

If the top input line is $|\,1\,\rangle$ the lower line is acted on by X

$\mathcal{U}_{Ham}$ is graphically represented by the action of two CNOT gates,



Suppose a single flip has occurred and the Hamming ket is in fact

$$|\,\psi_{Ham}\,\rangle \quad \longrightarrow \quad |\,\psi_{flip\ error}\,\rangle = \alpha|\,010\,\rangle + \beta|\,101\,\rangle$$

Inverse unitary transformation

$$\mathcal{U}^{\dagger}_{Ham}\big[\alpha|\,010\,\rangle + \beta|\,101\,\rangle\big] = \big[\alpha|\,0\,\rangle + \beta|\,1\,\rangle\big] \otimes |\,01\,\rangle$$

Ancilla state no longer in the ground state!

To each single flip error corresponds a different ancilla state.

Measure the ancilla, without affecting the original qubit.

Very similar to Hamming's classical code

BUT! No protection from *phase errors*

$$|\,\psi_{Ham}\,\rangle \quad \longrightarrow \quad |\,\psi_{phase\ error}\,\rangle = \alpha|\,000\,\rangle - \beta|\,111\,\rangle = Z_{123}|\,\psi_{Ham}\,\rangle$$

Insufficient as a quantum code

Going further requires Peter Shor's brain

Enlarge the Hilbert space to nine qubits, and consider two linear combinations

$$
\begin{aligned}
|\,\bar{0}\,\rangle &\equiv \frac{1}{2\sqrt{2}}\big[|\,000\,\rangle + |\,111\,\rangle\big] \otimes \big[|\,000\,\rangle + |\,111\,\rangle\big] \otimes \big[|\,000\,\rangle + |\,111\,\rangle\big] \\
|\,\bar{1}\,\rangle &\equiv \frac{1}{2\sqrt{2}}\big[|\,000\,\rangle - |\,111\,\rangle\big] \otimes \big[|\,000\,\rangle - |\,111\,\rangle\big] \otimes \big[|\,000\,\rangle - |\,111\,\rangle\big]
\end{aligned}
$$

BOTH single flips and single phase errors in these states can be diagnosed

• Single flips are easily taken into account by using six stabilizers,

$$Z_{13},\ Z_{23},\ Z_{46},\ Z_{56},\ Z_{79},\ Z_{89}$$

• Add two new stabilizers for phase errors

$$X_{123456},\ X_{123789}$$

Assume a phase error in the seventh qubit,

$$
\begin{aligned}
|\,\bar{0}_{phase\ error}\,\rangle &= \frac{1}{2\sqrt{2}}\big[|\,000\,\rangle + |\,111\,\rangle\big] \otimes \big[|\,000\,\rangle + |\,111\,\rangle\big] \otimes \big[|\,000\,\rangle - |\,111\,\rangle\big] \\
|\,\bar{1}_{phase\ error}\,\rangle &= \frac{1}{2\sqrt{2}}\big[|\,000\,\rangle - |\,111\,\rangle\big] \otimes \big[|\,000\,\rangle - |\,111\,\rangle\big] \otimes \big[|\,000\,\rangle + |\,111\,\rangle\big].
\end{aligned}
$$

Diagnose with the new counters

$$
\begin{aligned}
X_{123789}|\,\bar{0}_{phase\ error}\,\rangle &= -|\,\bar{0}_{phase\ error}\,\rangle, \qquad X_{456789}|\,\bar{0}_{phase\ error}\,\rangle = -|\,\bar{0}_{phase\ error}\,\rangle \\
\mathcal{X}_{123789}|\,\bar{1}_{phase\ error}\,\rangle &= -|\,\bar{1}_{phase\ error}\,\rangle, \qquad X_{456789}|\,\bar{1}_{phase\ error}\,\rangle = -|\,\bar{1}_{phase\ error}\,\rangle
\end{aligned}
$$

$\longrightarrow$ Phase error in the 789 cluster

Floodgates open for quantum error-correcting codes

Quantum Error-Correcting Codes

Hilbert space $\mathcal{H}_n$ of size 2^n with n qubits

Pauli group $\mathcal{P}_n$ with elements of the form $X^{\mathbf{a}}Z^{\mathbf{b}}$ acts on $\mathcal{H}_n$

$\mathcal{P}_n$ automorphism group: Clifford Group generated by

$$\mathrm{H} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}, \quad K = \begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}, \quad \mathrm{CNOT}: \ |\,x, y\,\rangle \longrightarrow |\,x, x+y\,\rangle$$

Three sources of error: flip, phase, and flip-phase: X, Y , Z

$k < n$ protected qubits against single errors

Example: Perfect binary single error-correcting quantum code

$$2^k(1+3n) = 2^n$$

lowest solution $n = 5$ $k = 1$:

one protected qubit living in a five qubit Hilbert space

Constructed by Bennett et al and Laflamme et al. (1996)

Five-Qubits Code $[[5, 1, 3]]$

Represented on five qubits Hilbert space with $2^5 = 32$ states. 2048-dimensional Pauli group $\mathcal{P}_5$, with 1054 elements of order two and 992 of order four.

Stabilizers in $\mathcal{S}$, 32-element Abelian $\mathcal{P}_5$ subgroup generated by idempotents

$$\begin{aligned} S_1 &= (X, Z, Z, X, I) \equiv X_{14} Z_{23}, \quad S_2 = (I, X, Z, Z, X) \equiv X_{25} Z_{34}, \\ S_3 &= (X, I, X, Z, Z) \equiv X_{13} Z_{45}, \quad S_4 = (Z, X, I, X, Z) \equiv X_{24} Z_{15} \end{aligned}$$

$\mathcal{S}$ generators label 2^4 states with eigenvalues $\pm 1, \pm 1, \pm 1, \pm 1$ in the 2^5 dimensional Hilbert space, with doubly degenerate multiplicities

Span the $\mathcal{D}_4$ (generated by Y_{12345} and X_{12345}) doublet representation

Two orthogonal states with $++++$ eigenvalues

$$\begin{aligned} |\,\bar{0}\,\rangle &= \Big[1 + \sum_{i=1}^{4} S_i + \sum_{i>j}^{4} S_i S_j + \sum_{i>j>k}^{4} S_i S_j S_k + S_1 S_2 S_3 S_4\Big] |\,00000\,\rangle \\ |\,\bar{1}\,\rangle &= X_{12345} |\,00000\,\rangle \end{aligned}$$

$$\text{Codewords}: \qquad |\,\psi\,\rangle = \alpha|\,\bar{0}\,\rangle + \beta|\,\bar{1}\,\rangle,$$

$$\begin{aligned} |\,\bar{0}\,\rangle \;=\; & |\,00000\,\rangle + |\,10010\,\rangle + |\,01001\,\rangle + |\,10100\,\rangle \\ & + |\,01010\,\rangle - |\,11011\,\rangle - |\,00110\,\rangle - |\,11000\,\rangle \\ & - |\,11101\,\rangle - |\,00011\,\rangle - |\,11110\,\rangle - |\,01111\,\rangle \\ & - |\,10001\,\rangle - |\,01100\,\rangle - |\,10111\,\rangle + |\,00101\,\rangle, \end{aligned}$$

$$\begin{aligned} |\,\bar{1}\,\rangle \;=\; & |\,11111\,\rangle + |\,01101\,\rangle + |\,10110\,\rangle + |\,01011\,\rangle \\ & + |\,10101\,\rangle - |\,00100\,\rangle - |\,11001\,\rangle - |\,00111\,\rangle \\ & - |\,00010\,\rangle - |\,11100\,\rangle - |\,00001\,\rangle - |\,10000\,\rangle \\ & - |\,01110\,\rangle - |\,10011\,\rangle - |\,01000\,\rangle + |\,11010\,\rangle. \end{aligned}$$

Coefficients as traces of matrices A and B corresponding to 0 and 1 in ket space

$$\mathrm{Tr}(AAAAA) = \mathrm{Tr}(BBBBB) = \mathrm{Tr}(BABAA) = \mathrm{Tr}(ABABB) = +1,$$

$$\mathrm{Tr}(BAAAA) = \mathrm{Tr}(ABBBB) = \mathrm{Tr}(BBAAA) = \mathrm{Tr}(AABBB) = -1,$$

Single Error States

Other $(2 \cdot 15)$ states generated by X_k, Y_k, Z_k on the kth entry of $|\,\psi\,\rangle$

	S_1	S_2	S_3	S_4
$X_1\|\,\psi\,\rangle$	$+$	$+$	$+$	$-$
$X_2\|\,\psi\,\rangle$	$-$	$+$	$+$	$+$
$X_3\|\,\psi\,\rangle$	$-$	$-$	$+$	$+$
$X_4\|\,\psi\,\rangle$	$+$	$-$	$-$	$+$
$X_5\|\,\psi\,\rangle$	$+$	$+$	$-$	$-$

	S_1	S_2	S_3	S_4
$Z_1\|\,\psi\,\rangle$	$-$	$+$	$-$	$+$
$Z_2\|\,\psi\,\rangle$	$+$	$-$	$+$	$-$
$Z_3\|\,\psi\,\rangle$	$+$	$+$	$-$	$+$
$Z_4\|\,\psi\,\rangle$	$-$	$+$	$+$	$-$
$Z_5\|\,\psi\,\rangle$	$+$	$-$	$+$	$+$

	S_1	S_2	S_3	S_4
$Y_1\|\,\psi\,\rangle$	$-$	$+$	$-$	$-$
$Y_2\|\,\psi\,\rangle$	$-$	$-$	$+$	$-$
$Y_3\|\,\psi\,\rangle$	$-$	$-$	$-$	$+$
$Y_4\|\,\psi\,\rangle$	$-$	$-$	$-$	$-$
$Y_5\|\,\psi\,\rangle$	$+$	$-$	$-$	$-$

- X_k flips the kth entry ($0 \to 1$ and $1 \to 0$)

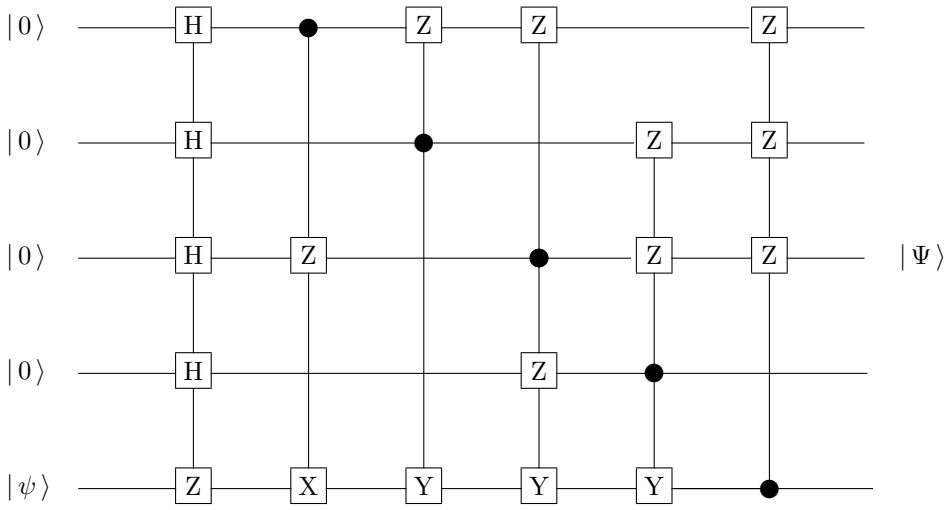
- Z_k maps the kth entry as $0 \to 0$ and $1 \to -1$, generates the phase error

- $Y_k = X_k Z_k$ generates the "flip & phase" error

Any single transmission error puts codeword into one of these states

All are orthogonal to one another and can be identified without ambiguities

Five Qubit Entangling Quantum Circuit: $\mathcal{U}$



Encoding $\mathcal{U}$: $|\psi\rangle \otimes |0000\rangle \longrightarrow |\Psi\rangle$

Decoding $\mathcal{U}^{\dagger}$: $|\Psi\rangle \longrightarrow |\psi\rangle \otimes |????\rangle$

Measure Ancilla $|????\rangle \rightarrow$ Error Syndrome

"Dynamical" System

Consider the "Hamiltonian"

$$h = -\frac{1}{4}\Big[S_1 + S_2 + S_3 + S_4\Big]$$

Ground state, (all $S_i = +1$): doubly degenerate qubit

Excited states split into different levels

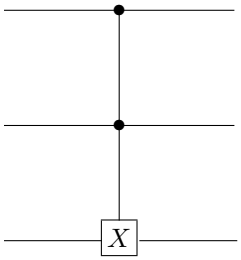
h	1	$\frac{1}{2}$	0	$-\frac{1}{2}$	-1
	1	4	6	4	1

$++++$	1
$+++-$	4
$++--$	6
$+---$	4
$----$	1

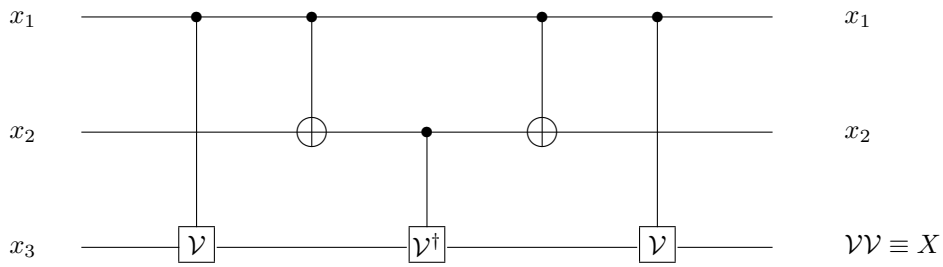
h identified with helicity, it might look familiar to certain physicists!

Universal Quantum Gates

Toffoli Gate



All n-qubit gates can be written in terms of two-qubit gates



The third qubit has three inputs

- $\mathcal{V}_1$ applied if $x_2 = 1$

- $\mathcal{V}_2^\dagger$ applied if $x_1 + x_2 = 1$

- $\mathcal{V}_3$ applied if $x_1 = 1$

- $x_1 = 0$, $x_2 = 0$ $\mathcal{V}_1$, $\mathcal{V}^\dagger$, $\mathcal{V}_3$ not applied, $x_3 = 1$
- $x_1 = 0$, $x_2 = 1$ $\mathcal{V}_3$ not applied, $x_3 = \mathcal{V}_1\mathcal{V}^\dagger = 1$
- $x_1 = 0$, $x_2 = 1$ $\mathcal{V}_1$ not applied, $x_3 = \mathcal{V}^\dagger\mathcal{V}_3 = 1$
- $x_1 = 0$, $x_2 = 1$ $\mathcal{V}_2^\dagger$ not applied, $x_3 = \mathcal{V}_1\mathcal{V}_2$

$$\mathcal{V} = \sqrt{\mathrm{X}} = \frac{1}{\sqrt{2}} \begin{pmatrix} e^{i\pi/4} & e^{-i\pi/4} \\ e^{-i\pi/4} & e^{i\pi/4} \end{pmatrix}$$

General Unitary Transformations not realizable by classical computers

Small Sliver of Quantum Codes and Information

Maybe More Next Year?

END