Basic Python for Quantum Communications

Muhammad Imansyah Basudewa, S.T.

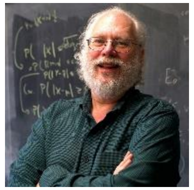
The University Center of Excellence for Advanced Intelligent Communications (AICOMS)
HUAWEI Beyond 5.5G Laboratory (HUAWEI B5.5G Lab),
School of Electrical Engineering, Telkom University, Bandung, INDONESIA
National Research and Innovation Agency,
Email: {imansyah@student., anwarkhoirul@,} telkomuniversity.ac.id

Presented at
The 2023 AICOMS WRITEX
Hybrid, June 3, 2023

Outline

Quantum Revolution

One of the main questions quantum mechanics addressed was the nature of light.
Eighteenth-century physicists believed light was a particle.
Nineteenth-century physicists proved it had to be a wave.
Twentieth-century physicists resolved the problem
by redefining particles using the principles of quantum mechanics.



Artur ekert, Oxford. Entanglement-based secure communication [1991]

Deutsch-Jozsa Algorithm **[1992]**

Simon's Problem, invents Oracle problem **[1994]**

Shor Algorithm **[1994]**

Scientists used laser cooling to observe a long-predicted state of matter: the Bose-Einstein condensate. **[1995]**

Dowling and Milburn coined the term "quantum revolution **[2002]**

the number of transistors in an integrated circuit (IC) doubles about every two years**[1965]**

Transistor used in Apollo Project **[1961]**

Theodore Maiman shining a high-power flash lamp on a ruby rod with silver-coated surfaces **[1960]**

Physicists at Bell Labs find a replacement for Vacuum tubes **[1947]**

©Imansyah 2023

Mach–Zehnder interferometer **[1891]**

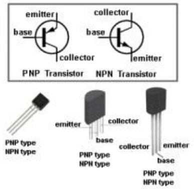
vacuum tubes were used in radios, televisions and long-distance telephone networks [Early 20th]

Schrödinger equation **[1926]**

uncertainty principle **[1927]**

A Mathematical Theory of Communication, Claude Shannon **[1948]**

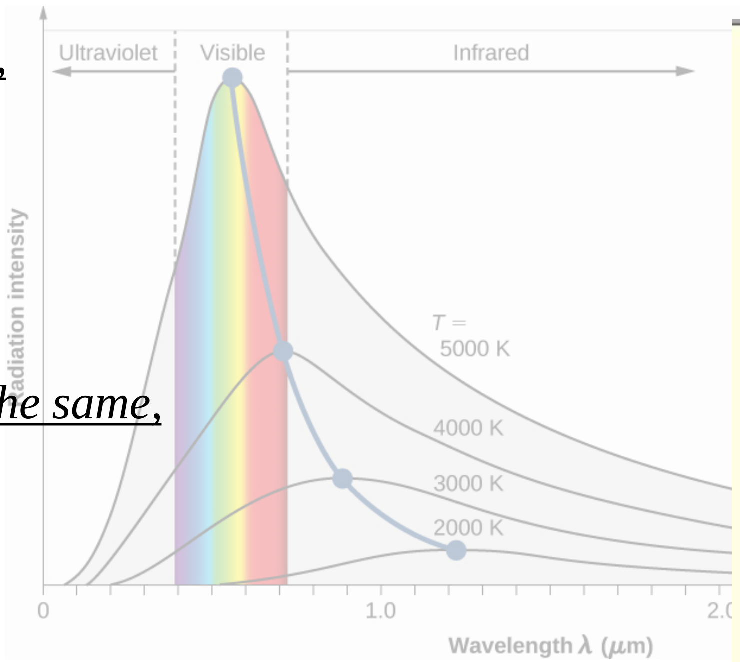
These quantum-inspired devices are central to every single modern electronic application that uses some computing power, such as cars, cellphones and digital cameras.
Transistors, which are an important part of what is now called **the first quantum revolution**

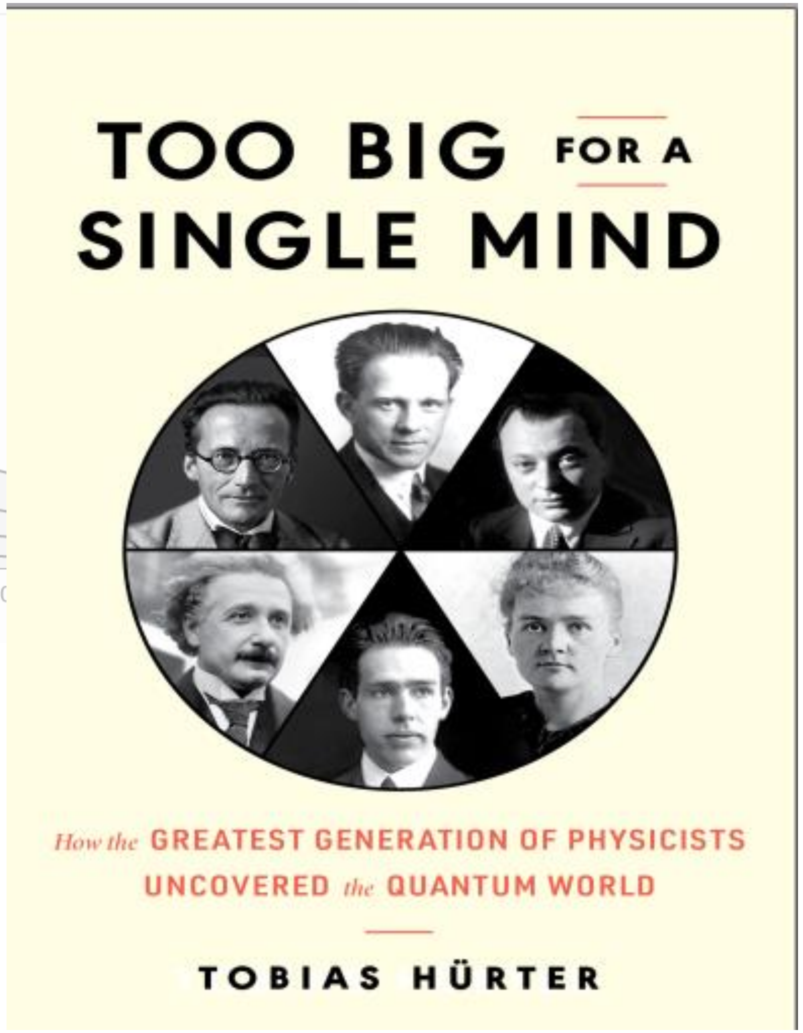


This second quantum revolution is defined by developments in technologies like quantum computing and quantum sensing, brought on by a deeper understanding of the quantum world and precision control down to the level of individual particles.

Blackbody problem

from the red of a glimmering ember in the hearth,
via the yellow of the Sun,
to the bluey whiteness of molten steel.
The higher its temperature rises,
the brighter and whiter the poker will glow,
until it gradually begins to take on a bluish hue.
This characteristic sequence of colors is always the same,
no matter where or what;





What was needed was a formula to describe accurately the correlation between the temperature and the frequency (that is, the color) of the light emitted. This was the **blackbody problem**, so named because it is based on a theoretical, idealized physical body that absorbs any and all electromagnetic radiation incident upon it. The blackbody problem had been formulated scientifically in 1859 by Gustav Kirchhoff, CHAPTER

1 Into Quantumland

In quantum theory the concept of a particle is not so sharp as in classical physics. Particles carry and deliver energy in a quantized form, in discrete packets. In many cases they have definite masses which clearly distinguish them from other particles and can carry specific amounts of other quantities, such as electric charge. Photons have zero rest mass (which also is a definite value). Real particles, those with a long-term existence, have strict relations between the values of mass, energy, and momentum. Where particles may be created and destroyed and have but a fleeting existence, then they do not obey such strict rules and the quantum fluctuations in their energy may be large. This is particularly true for those particles which are exchanged to provide an interaction between other particles. The entire energy of such particles is a quantum fluctuation. They are created literally from nothing. The vacuum is not completely empty, but is a seething mass of these short-lived particles.

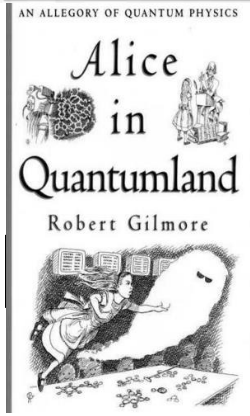
Quantum theory describes the behavior of particles in terms of *probability distributions*, and the actual observation of individual particles will occur at random within these. The probabilities may include classically forbidden processes, such as the penetration of particles through a thin energy barrier.

la

CONDITIONS OF LOAN

$\Delta E\, \Delta t = \hbar/2$

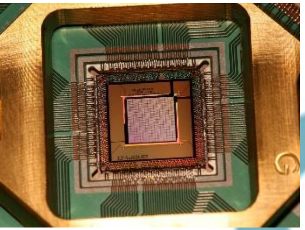
Prompt repayment would be appreciated.

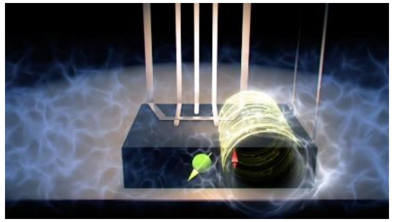


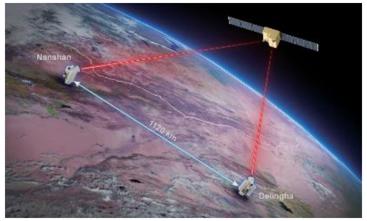
A *state* describes the condition of a physical system. It is the basic concept in quantum theory—the best description of the real world which can be given. In general the amplitude for a state gives the probability for various possible results of any observation. For some states there may be only one possible outcome to a particular measurement. When a system is in one of these so-called stationary states any measurement of that quantity will give one and only one possible result. Repeated measurements will give the same result every time. Hence the name *stationary state*, or the frequently used German equivalent *eigenstate*.

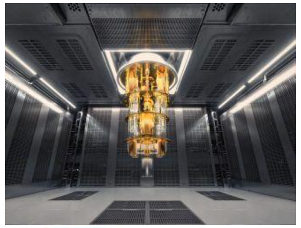
Particles in quantum theory are found to show properties which classically are associated with continuous waves. In a corresponding way, classical force fields are found to be composed of particles. The electrical interaction between any two charged particles is caused by the exchange of photons between them. These photons have a brief existence, which means they are well localized in time and so are uncertain in energy. They are *virtual particles*, whose energy and momentum may fluctuate well away from the values which would be normal for a long-lived particle.

Quantum Computing & Communication









First Teleportation using a satellite **[2017]**

Ritajit Majumdar Qutrit Codes [2019]

IBM Q System One **[2019]**

noise cancelling for qubits **[2020]**

China Build Quantum Communication Network **[2021]**

IBM presents its 433-qubit 'Osprey' quantum processor, the successor to its Eagle **system [2022]**

Alpine Quantum Technologies (AQT) has demonstrated a quantum volume of 128 on its 19-inch rack-compatible quantum computer **[2023]**

Shor's algorithm in an ion-trap-based quantum computer **[2016]**

EA Polar Codes **[2010]**

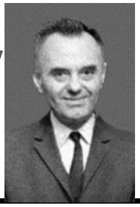
EA-QECC **[2000]**

Shor Codes **[1995]**
Steane Codes **[1995]**

quantum mechanical Turing machine **[1982]**

Holevo Theorem [1973]

Quantum Cryptography Charles H. Bennet **[1973]**



Quantum Information Theory **[1976]**

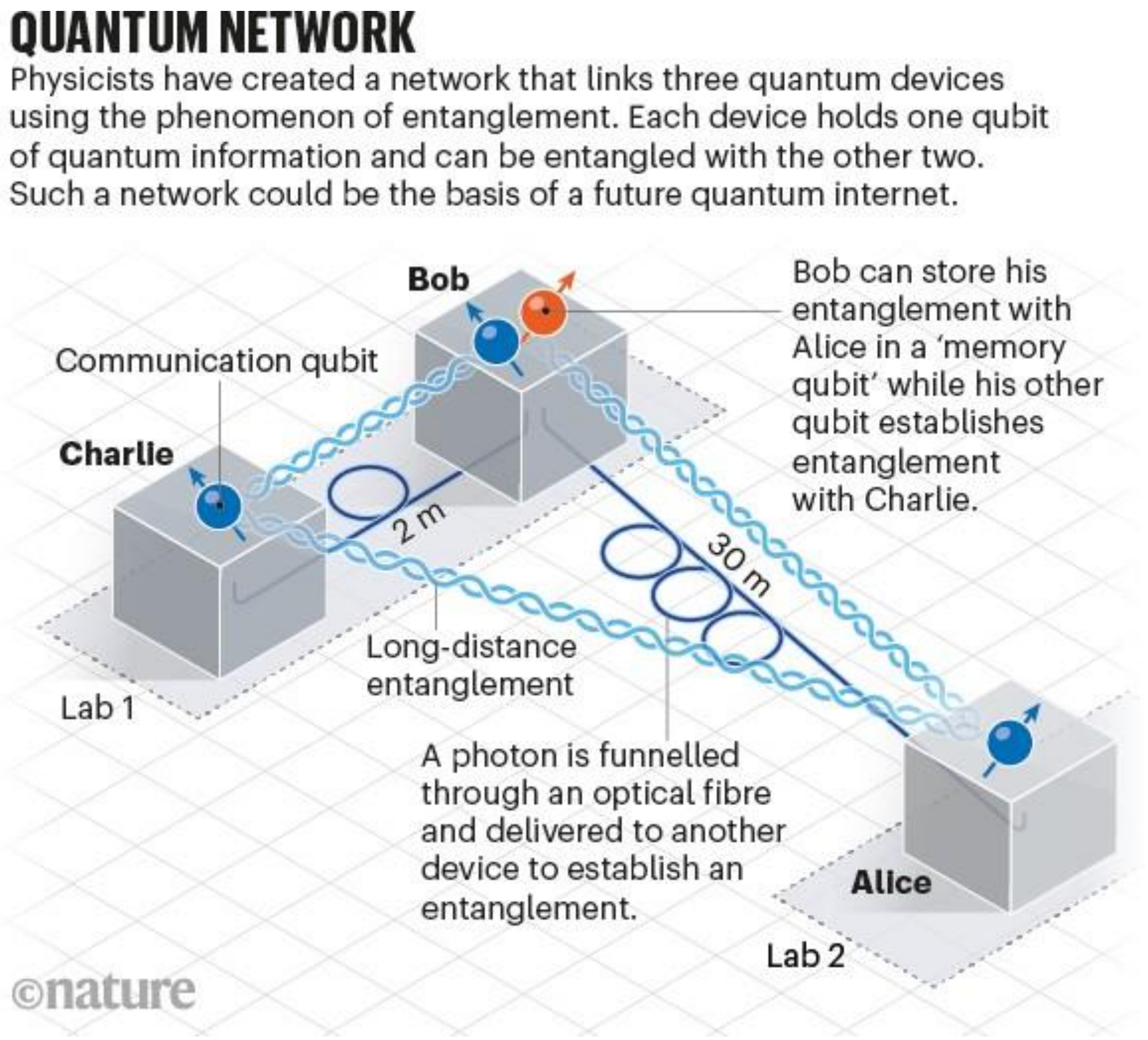
Toffoli Gate**[1980]**

Basic Model for quantum computer **[1981]**

Chinese researchers combining over 700 optical fibers with two QKD-ground-to-satellite links for a total distance between nodes of the network of networks of up to ~4,600

Griffith University, UNSW and UTS, in partnership with seven universities in the United States, develop noise cancelling for quantum bits via machine learning, taking quantum noise in a quantum chip down to 0%

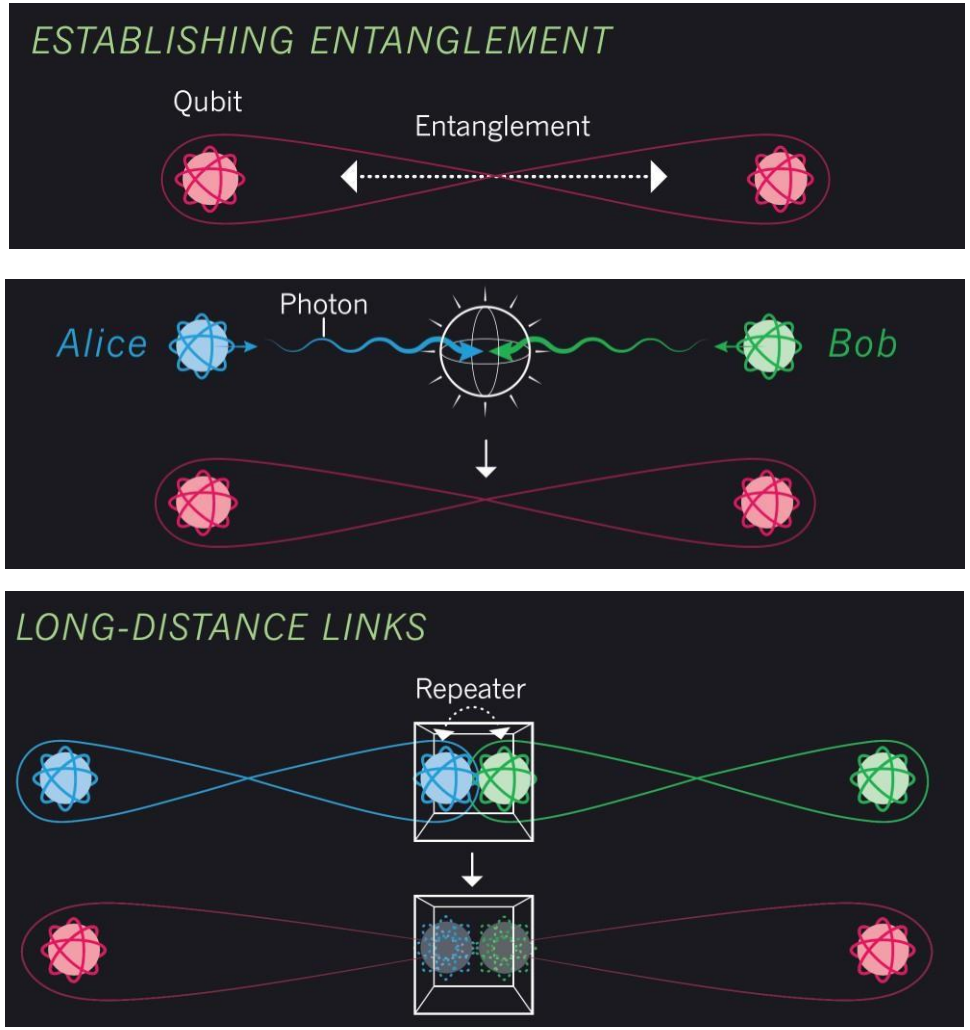
Quantum Internet



- Quantum network
  - Quantum communications
    - Quantum link
    - Quantum entanglement
    - Quantum repeater
- Quantum channel coding
  - Quantum repeater code
  - Quantum low density parity code (LDPC) code
  - Quantum polar code
  - Quantum raptor code
- Many quantum articles are published in *Nature*
  - Quantum internet is still a baby and hot topic
- Leader in Keio Univ and TU-Delft
  - Internet Engineering Task Force (IETF)
    - Quantum Internet Research Group (QIRG)

Image: D. Castelvecchi, “Quantum Network is Step Towards Ultrasecure Internet,“ *Nature,* vol. 590, pp. 540-541, 2021.

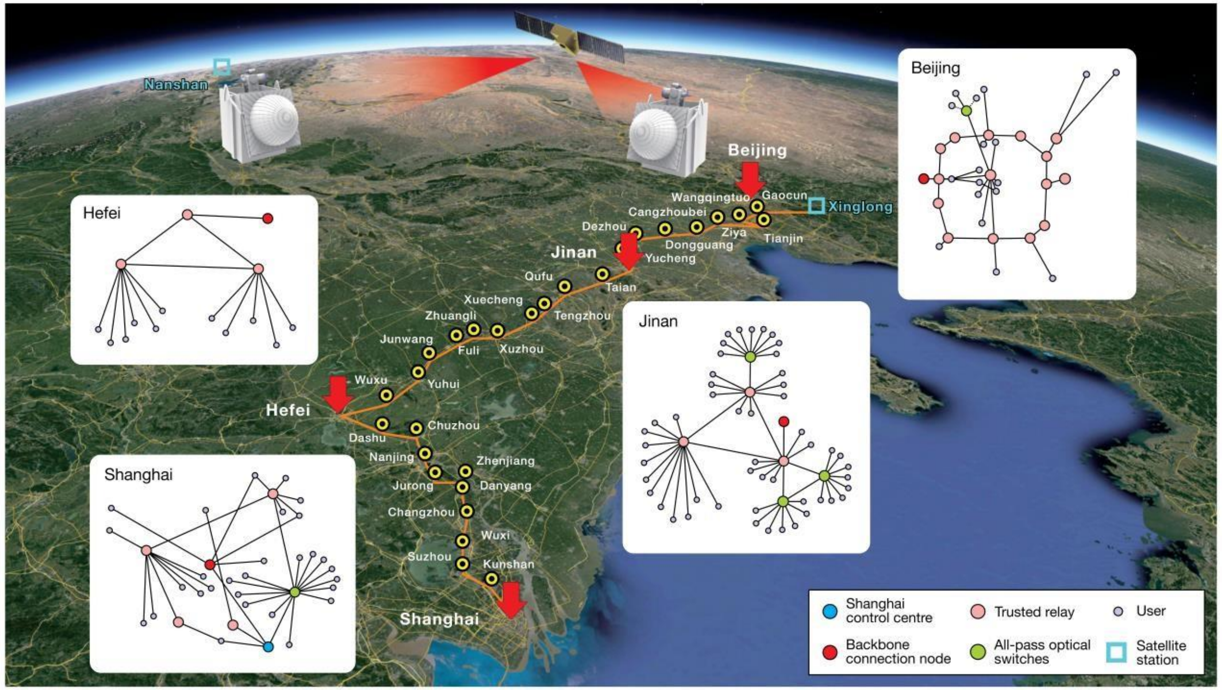
Quantum Communications

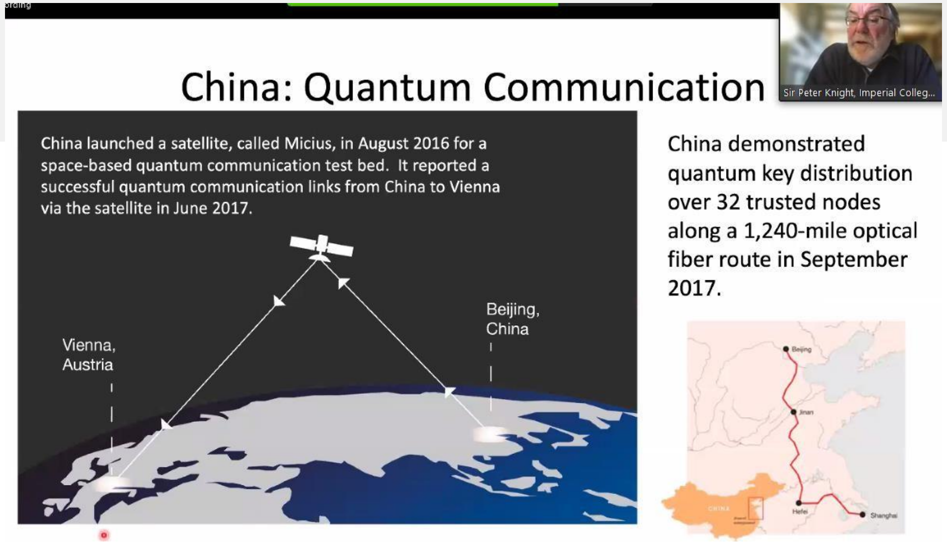


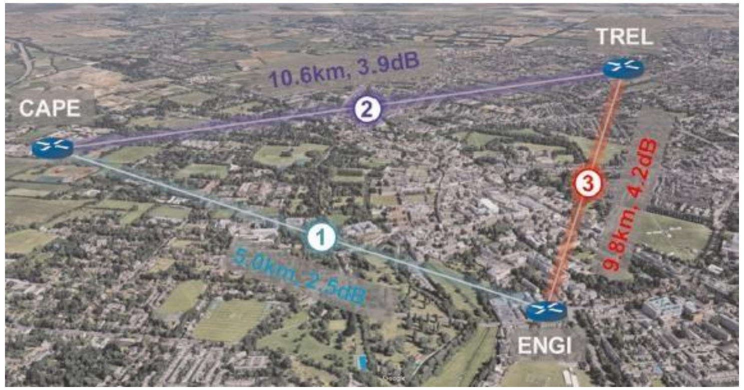
- Quantum Entanglement
  - One qubit changes the state, so does the other
  - Quantum communications channel that spans any distance
  - Each Alice and Bob emits a photon
  - Their photons meet in the middle
  - Each photon is entangled to its qubit
  - Hence, both qubits of Alice and Bob are entangled
- Quantum Repeater
  - Alice and Bob are far away from one another or not directly connected
  - One or more quantum repeaters will be needed to establish entanglement
  - One qubit in the repeater is entangled with Alice's qubit, and the other with Bob's
  - By performing an operation on the two qubits it holds
  - The repeater creates entanglement between Alice's and Bob's qubits

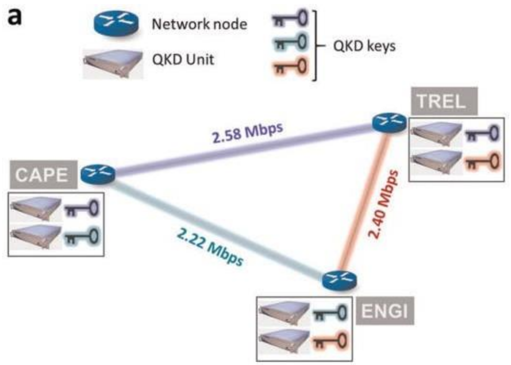
Image: D. Castelvechhi, "The Entangled Web," Nature, vol. 554, pp. 289-292, 15 February 2018.

Quantum Communications







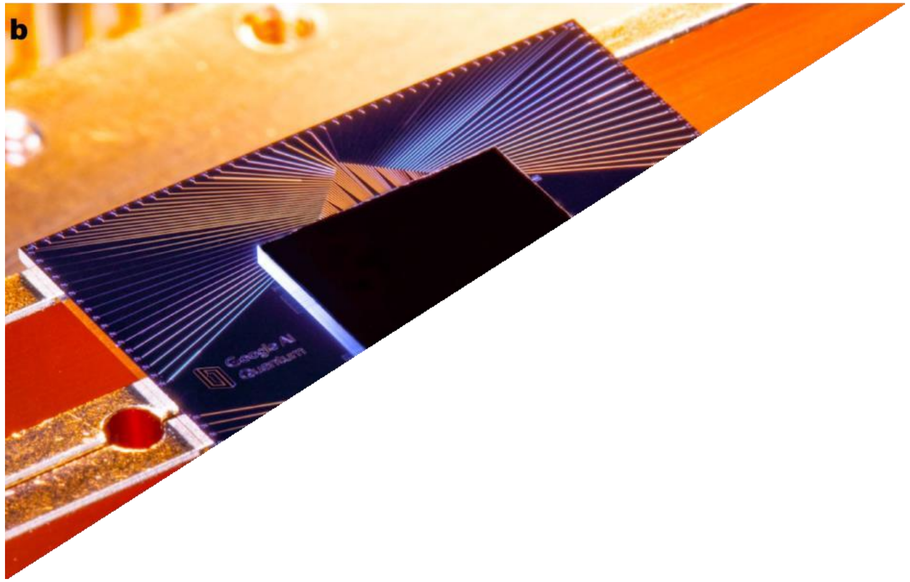


- Satellite Quantum was launched, 2016
  - Vienna – Beijing, 2017
- 1,240 mile of optical fiber, 2017
  - Beijing – Shanghai
- 4,600 km of satellite and optical fiber, 2021
  - Nanshan – Xinglong – Beijing - Shanghai

- A three nodes ring network in the Cambridge metropolitan area
- Three nodes denoted CAPE, TREL, and ENGI are connected in a triangular using underground single mode optical fibers
- High-speed GHz clocked QKD systems where each link produces a set of QKD keys identified by the link color

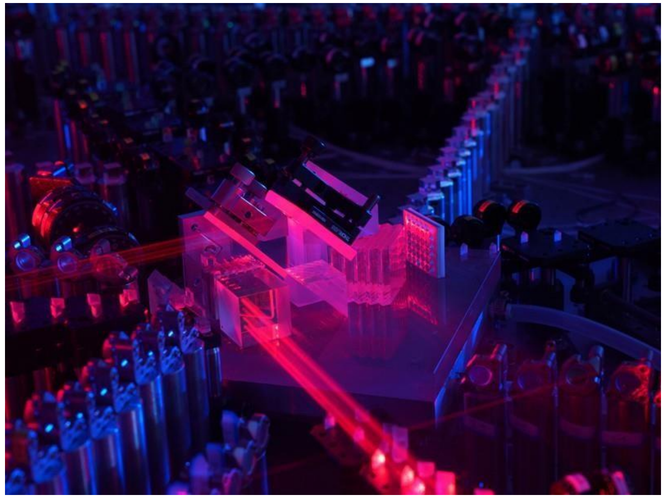
Y. A. Chen, Q. Zhang, T. Y. Chen, *et al*., "An Integrated Space-to-Ground Quantum Communication Network Over 4,600 Kilometres," *Nature,* vol. 589, pp. 214–219, 2021);
S. P. L. Knight, Imperial College, London, ITU Webinar, March 2021; J. F. Dynes *et al.,* "Cambridge Quantum Network," npj Quantum Information, vol. 5, no. 101, 2019.

Quantum Supremacy



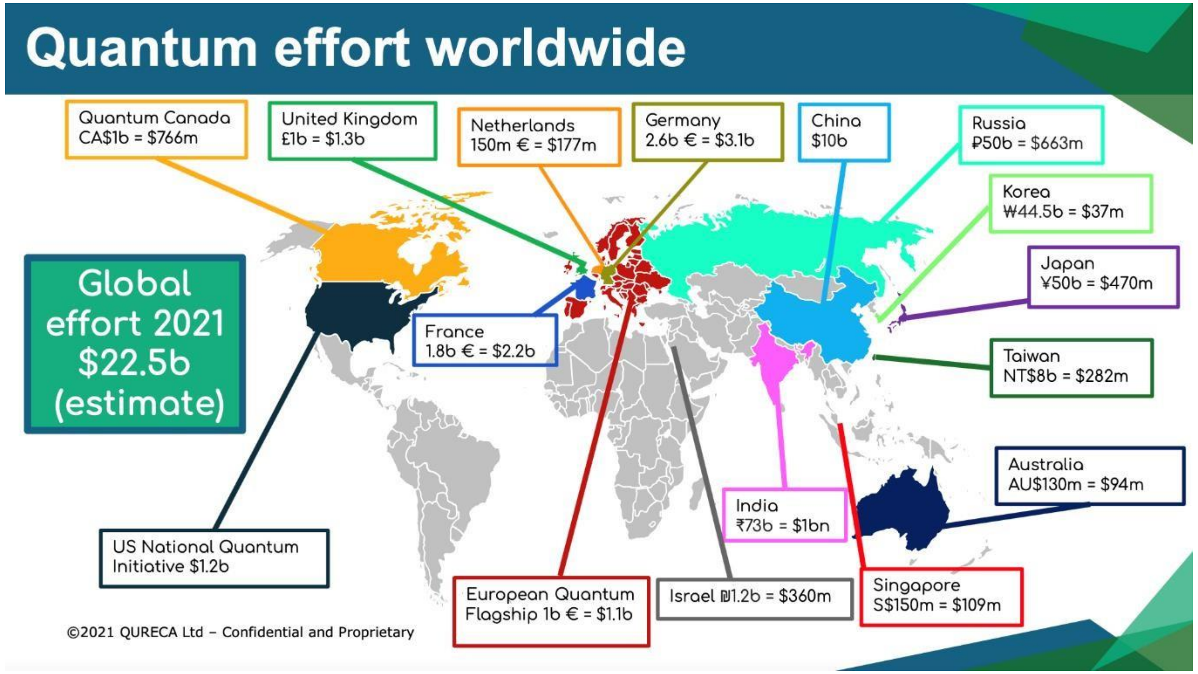
- Quantum supremacy
  - Google 2019
    - 10,000 years in classic computer
    - 200 seconds in quantum computer
    - The Sycamore processor
      - 54 qubits
      - Made from superconducting circuits that are kept at ultracold temperatures
  - The Hefei team 2020
    - This photonic computer
    - 200 seconds a calculation
    - 2.5 billion years an ordinary supercomputer
    - Boson-sampling problem
    - Not programmable
      - Cannot be used for solving practical problems

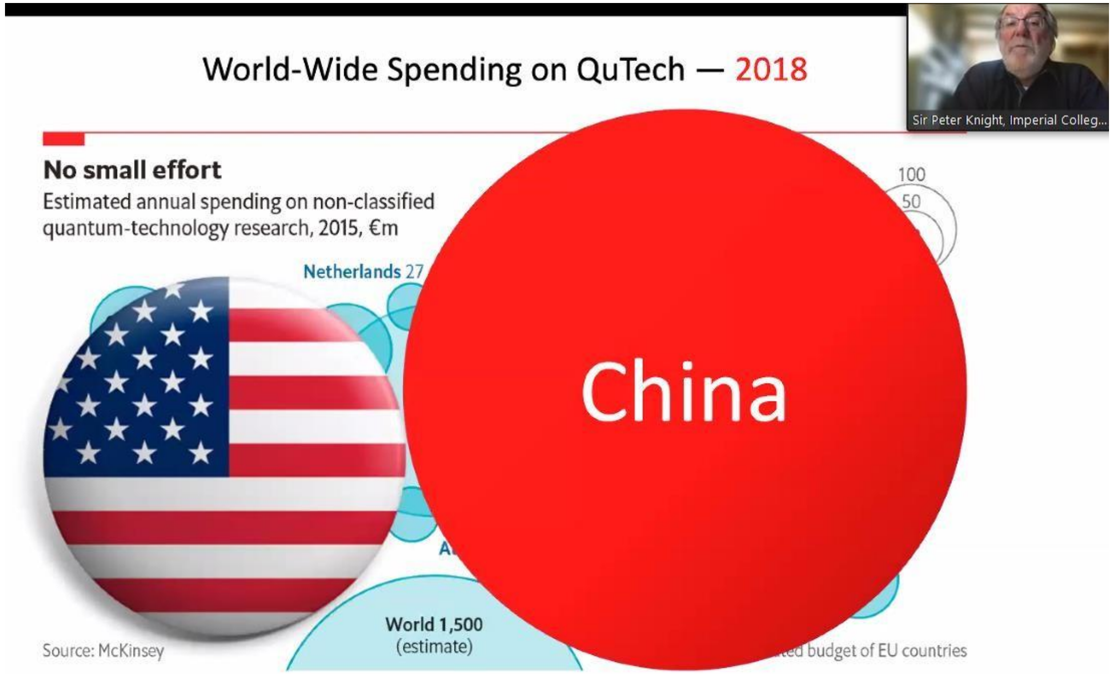
- Sep 2021, Zuchongzhi would have used 56 of its 66 qubits to solve in 72 minutes an operation that is 100 to 1000 times more complex than the one carried out by Sycamore



Arute, F., Arya, K., Babbush, R. et al. “Quantum supremacy using a programmable superconducting processor,” *Nature*, vol. 574, pp. 505–510, 2019; P. Ball, “Physicists in China Challenge Google’s ‘Quantum Advantage’,” *Nature*, vol. 588, no. 380, 2020; https://www.breakinglatest.news/health/china-is-winning-the-quantum-computer-race/

Quantum Research Effort in Global and Nationalism



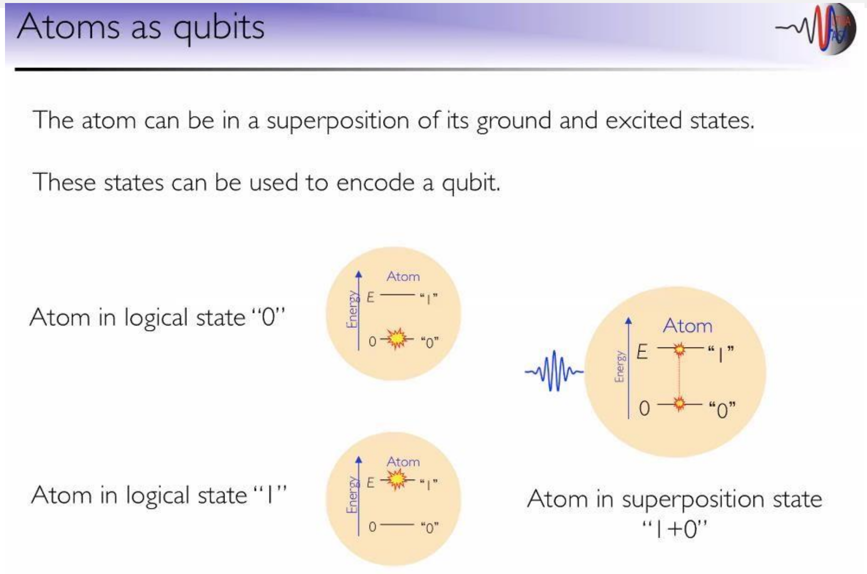


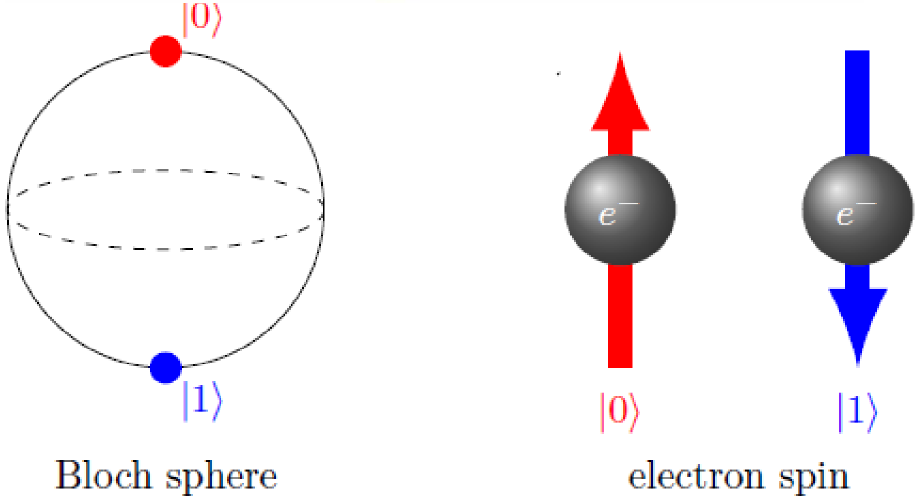
- China is leading with 10 BUSD
- India just started with 1 BUSD
- German 3.1 BUSD, UK 1.3 BUSD, USA 1.2 BUSD
- Indonesia is necessary to start immediately
- Quantum Nationalism
    - Study and Research in Quantum Technology is Part of National Defense

Image: S. P. L. Knight, Imperial College, London, ITU Webinar, March 2021.

Two-Level Quantum Systems

- The spin of the electron
  - A magnetic field to an electron can change its spin
- The polarization of a photon
  - Single photon is elementary particle of light
  - The fundamental unit of light
  - Used for quantum communication by sending the photon
- An atom with a ground state and an excited state
  - Pulsing an atom with a laser can excite one of its electrons from a ground state to an excited state

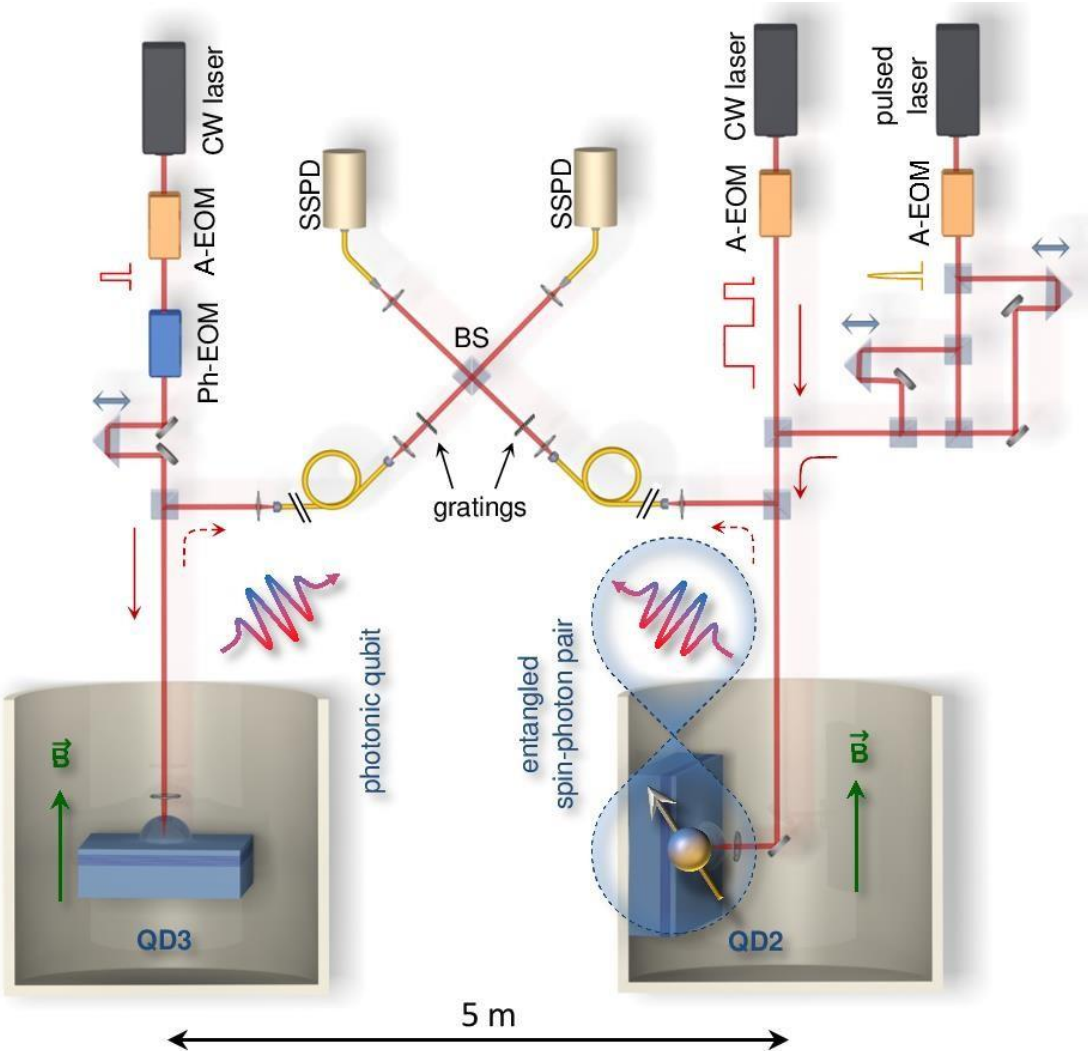




M. Wilde, *From Classical to Quantum Shannon Theory,* Cambridge University Press, 2019; A. B. D. Shaik and P. Palla, "Optical Quantum Technologies with Hexagonal Boron Nitride Single Photon Sources," *Scientific Reports,* vol. 11, no. 12285, 2021; I Walmsley, Imperial College, London, ITU Webinar, March 2021; https://medium.com/@lindat/how-quantum-computers-and-machine-learning-will-revolutionize-big-data-571d5594e9b8;

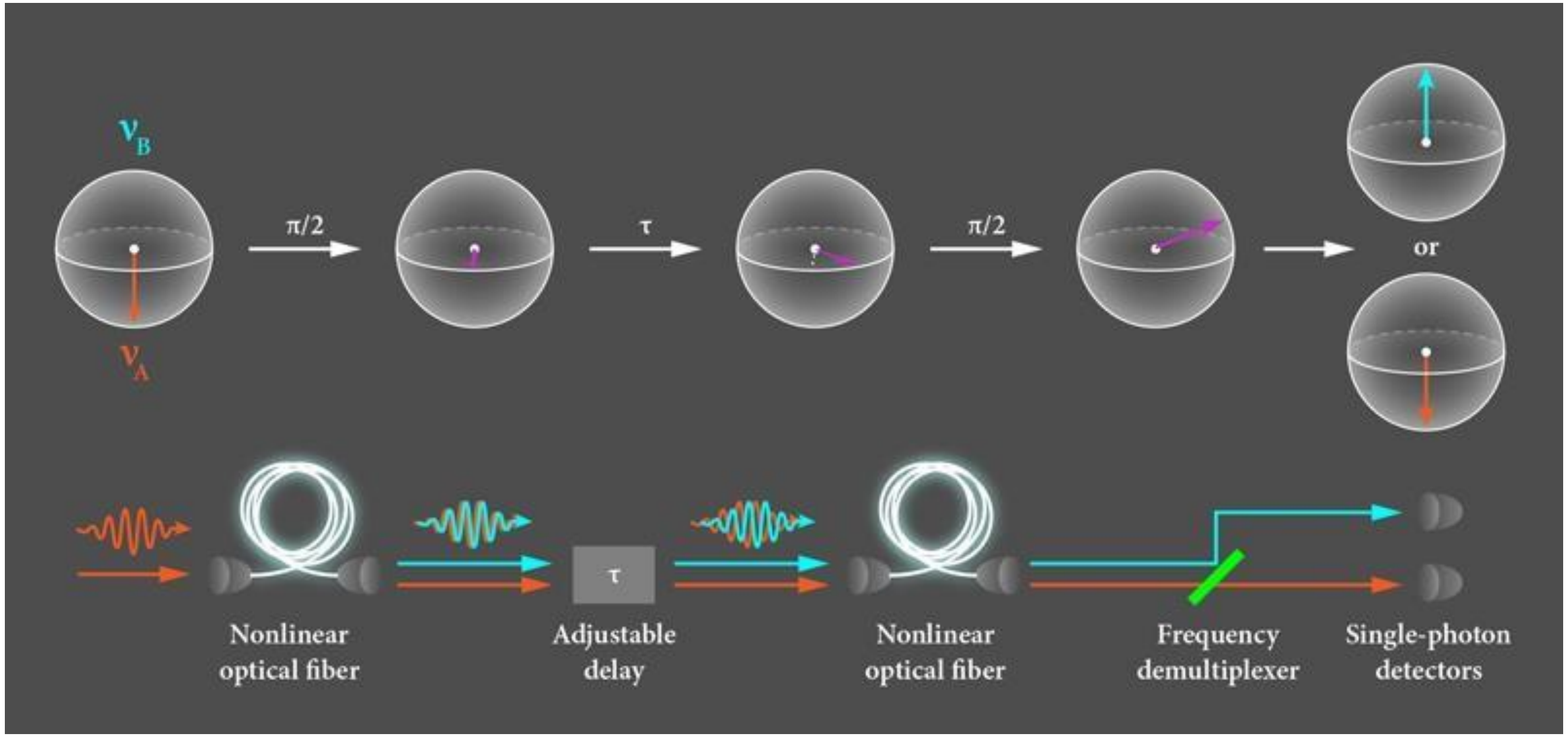
Photonic Qubit

- Quantum teleportation with the use of photon propagation
- Continuous wave (CW) laser
- Electro-optic modulator (EOM)
  - Amplitude EOM (A-EOM)
    - 800 and 400 picosecond (ps) pulses
  - Phase EOM (Ph-EOM)
    - Generate laser sidebands
- Quantum dot (QD)
  - High-efficiency sources for single photons



W. Gao, P. Fallahi, E. Togan *et al.,* "Quantum Teleportation from a Propagating Photon to a Solid-State Spin Qubit. Nature Communications, vol. 4, no. 2744, 2013.

Photon, The Quantum Particle of Light



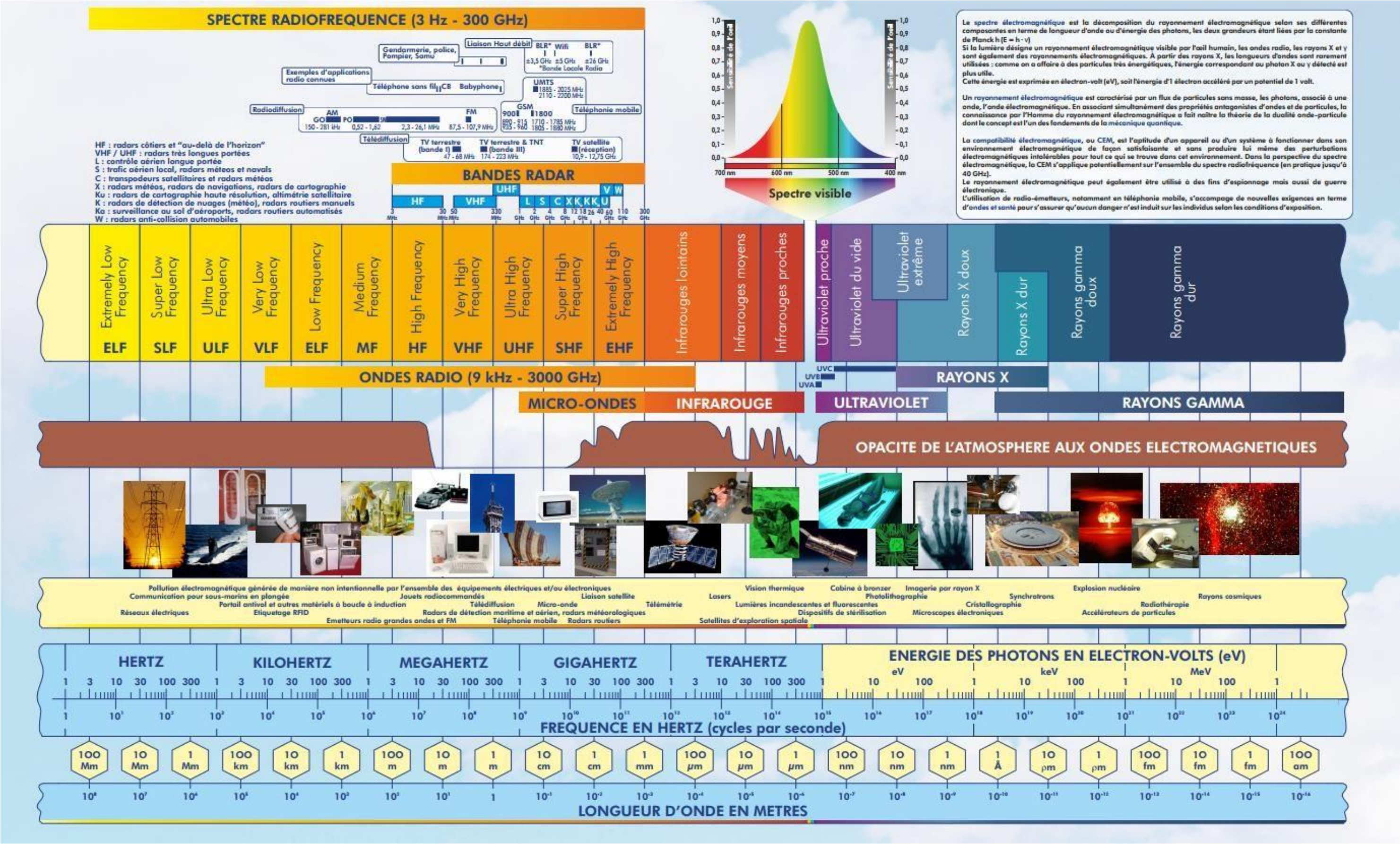
- Conversion
  - A photon of one frequency or color into
  - A photon of superposition of two colors
- A single photon of frequency
  - Sent through a nonlinear optical fiber
  - Converting it to a superposition with another frequency (blue)
- An adjustable delay
  - Changes the relative phase of the two frequency components in the superposition before they are mixed again

- The resulting state is analyzed by
  - Separating the two frequency components in a demultiplexer
  - Detecting the single photon, thereby projecting it onto one of its two colors

- A vector on the Bloch sphere with polar angle θ and azimuthal angle φ represents the state of the photon through the various steps of the conversion.

P. Treutlein, “Photon Qubit is Made of Two Colors,” https://physics.aps.org/articles/v9/135.

Photon is Particle of Light



- Light is electromagnetic wave
  - $400 - 790 \sim 800$ THz of frequency
  - $380 - 750$ nm of wavelength
  - $3 \cdot 10^8$ m/s of speed of light
- Can we receive signal in vacuum?
  - Yes, we can
  - Voice wave can not go through vacuum
  - The light from the sun arriving the earth
- Communications with the light
  - Visible light communication (VLC)
  - Light Fidelity (Li-Fi)
  - Free space optical (FSO): Laser
  - Visible light positioning (VLP)

Image: https://www.emitech.fr/sites/groupe-emitech.fr/files/spectre-radiofrequence.jpg

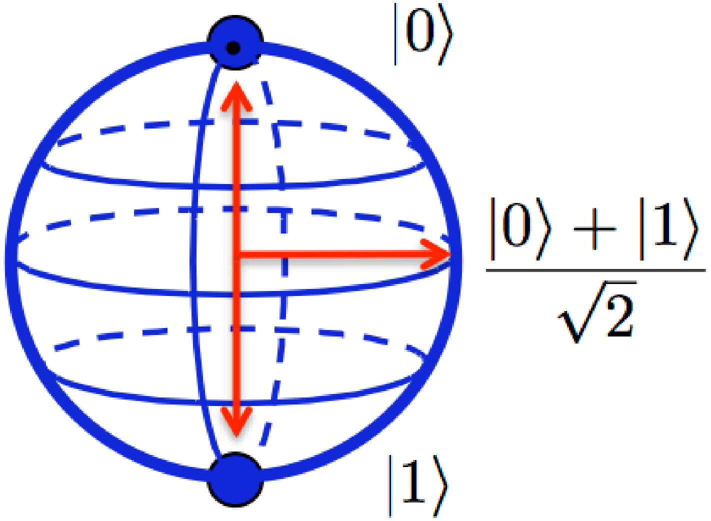
Behind the Quantum Circuit

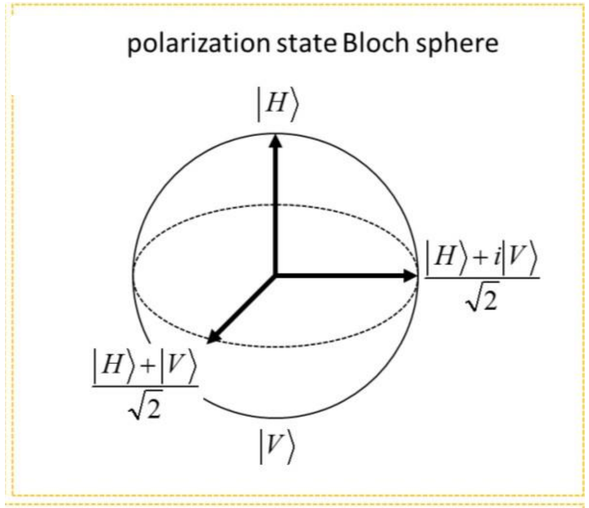
Basic of Quantum Computing and Quantum Information

Basics of quantum computing and quantum Information

- To help in reading article in journal, proceeding, and books of Quantum
- To help reading and calculating the Quantum Circuit
- To help in programming Python, Matlab, and Octave
- What we learn
  - Quantum bit
  - Quantum state
  - Amplitude probability
  - Computational basis
  - $+/-$ basis
  - Eigenstate, Eigenvalue, Eigenbasis
  - NOT gate, Bit flip, and phase flip
  - Pauli matrices
    - X, Z, I, Y operator
  - Hadamard gate or H operator
  - CNOT gate
  - Quantum circuit

Classical Bit (Cbit) and Quantum Bit (Qubit)





Classical Bit **Qubit**

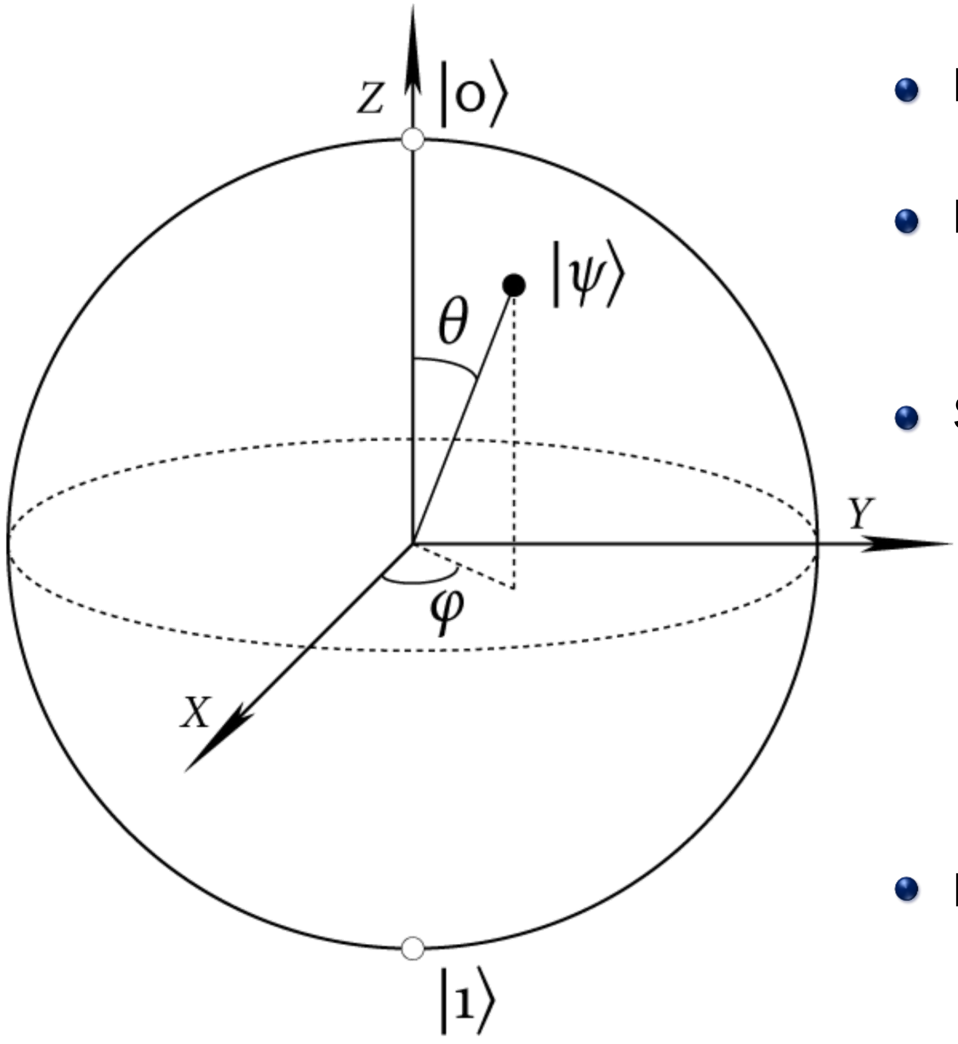
- Cbit to qubit mapping
  - $0 \rightarrow |0\rangle$
  - $1 \rightarrow |1\rangle$
- Superposition

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

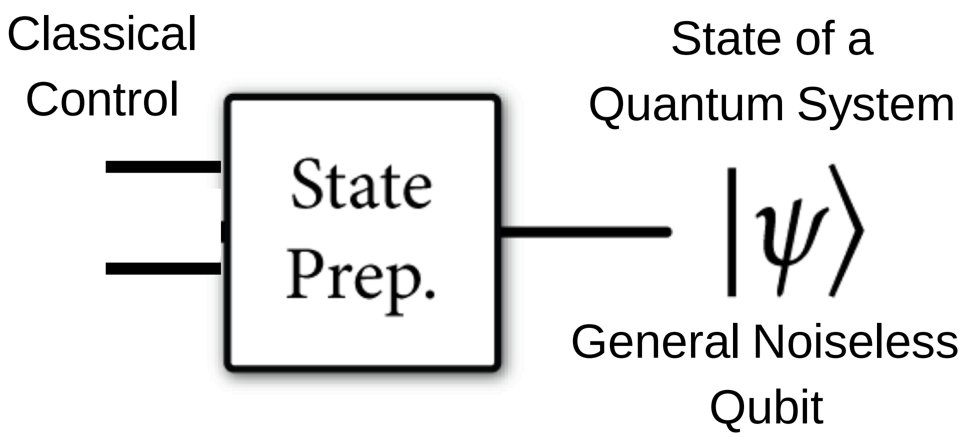
- Diract notation
  - bra $\langle 0|$
  - ket $|0\rangle$
- $(\cdot)^*$ is conjugate transpose
  - $\langle 0| = |0\rangle^*$
  - $\langle 1| = |1\rangle^*$
- Bloch sphere is to visualize a qubit
- Vector representation
  - $|0\rangle \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix}$
  - $|1\rangle \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix}$
  - $\langle 0| \equiv [1\ 0]$
  - $\langle 1| \equiv [0\ 1]$

M. Wilde, *From Classical to Quantum Shannon Theory,* Cambridge University Press, 2019; https://www.autodesk.com/products/eagle/blog/future-computing-quantum-qubits; C. A. Foell III, *Luminescent píopeíties of Pb-based (PbX) colloidal quantum dots (CQDs) in vacuum, on silicon and integíated with a silicon-on-insulatoí (SOI) photonic integíated cicuit (PIC)*, PhD Disseítation, ľhe Univeísity Of Bíitish Columbia (Vancouveí), May 2016.

General Noiseless Qubit



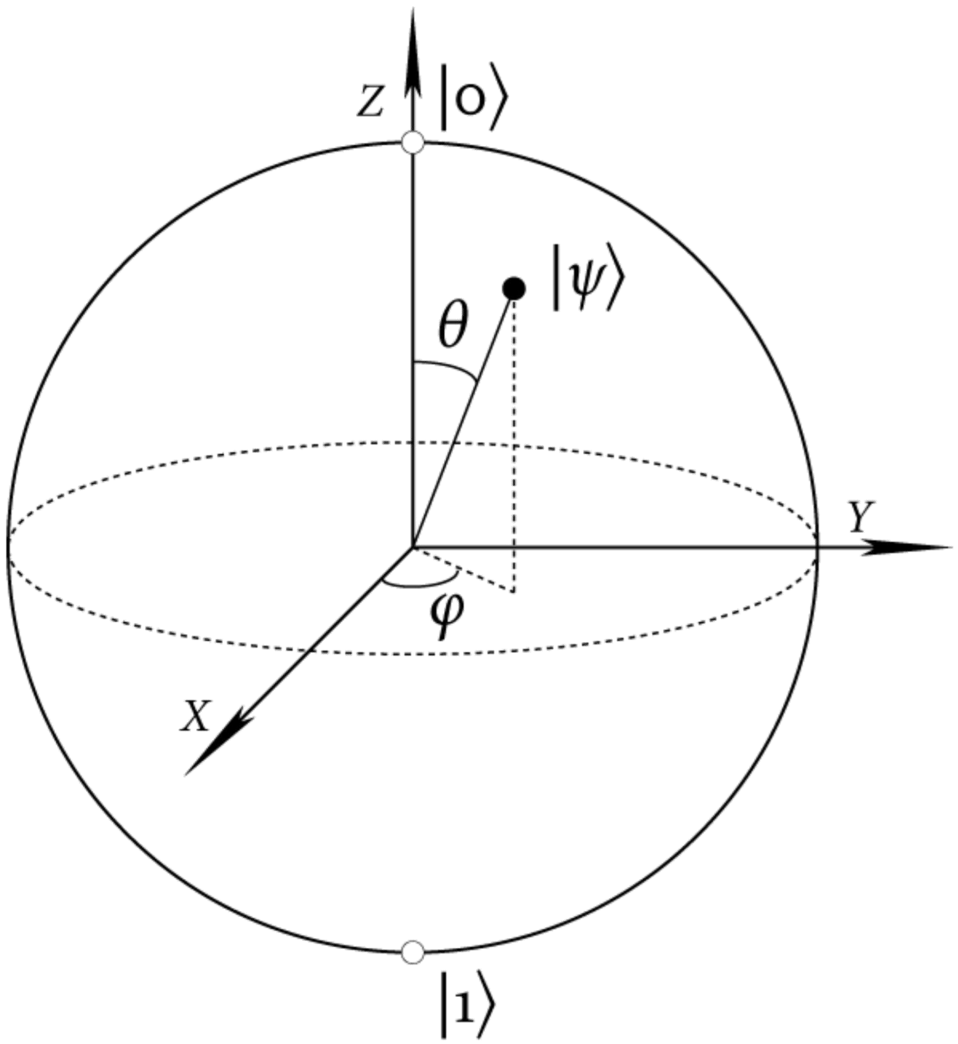
- Classical control
  - To initialize the state of a quantum system
- Noiseless
  - Do not interact with their surroundings
- Noiseless qubit channel
  - Free space, ideally photon does not interact with other particles
- Superposition state
  - $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
  - $|\psi\rangle = \alpha\begin{bmatrix}1\\0\end{bmatrix} + \beta\begin{bmatrix}0\\1\end{bmatrix}$
  - $|\psi\rangle = \begin{bmatrix}\alpha\\0\end{bmatrix} + \begin{bmatrix}0\\\beta\end{bmatrix}$
  - $|\psi\rangle = \begin{bmatrix}\alpha\\\beta\end{bmatrix}$
- Probability amplitude
  - $|\alpha|^2 + |\beta|^2 = 1$
  - Arbitrary complex numbers



- 1 line for Quantum
- 2 lines for Classic

M. Wilde, *From Classical to Quantum Shannon Theory,* Cambridge University Press, 2019.

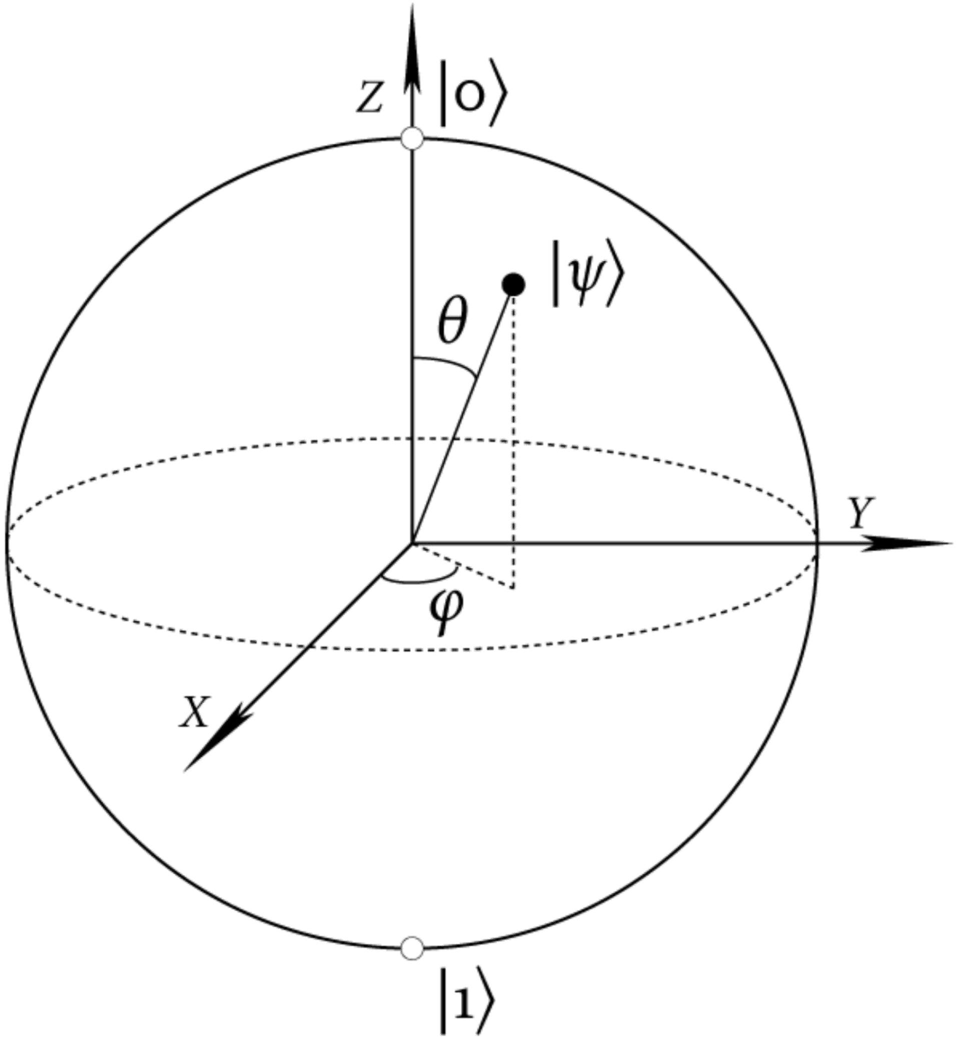
Qubit in Terms of The Angles



- Consider any two qubits
  - Equivalent up to a differing global phase
    - $|\psi_0\rangle \equiv |\psi\rangle$
    - $|\psi_1\rangle \equiv e^{i\chi}|\psi\rangle$
      - $0 \leq \chi \leq 2\pi$
    - Physically
      - The same results are obtained from measurement
- Probability amplitude as complex numbers
  - $\alpha = r_0 e^{i\varphi_0}$
  - $\beta = r_1 e^{i\varphi_1}$
- Factor out $e^{i\varphi_0}$
  - $\alpha = r_0 e^{i(\varphi_0 - \varphi_0)} = r_0 e^0 = r_0$
  - $\beta = r_1 e^{i(\varphi_1 - \varphi_0)}$
- Physically equivalent state
  - $|\psi\rangle \equiv |0\rangle + \beta|1\rangle$
  - $|\psi\rangle \equiv r_0|0\rangle + r_1 e^{i(\varphi_1 - \varphi_0)}|1\rangle$

M. Wilde, *From Classical to Quantum Shannon Theory,* Cambridge University Press, 2019.

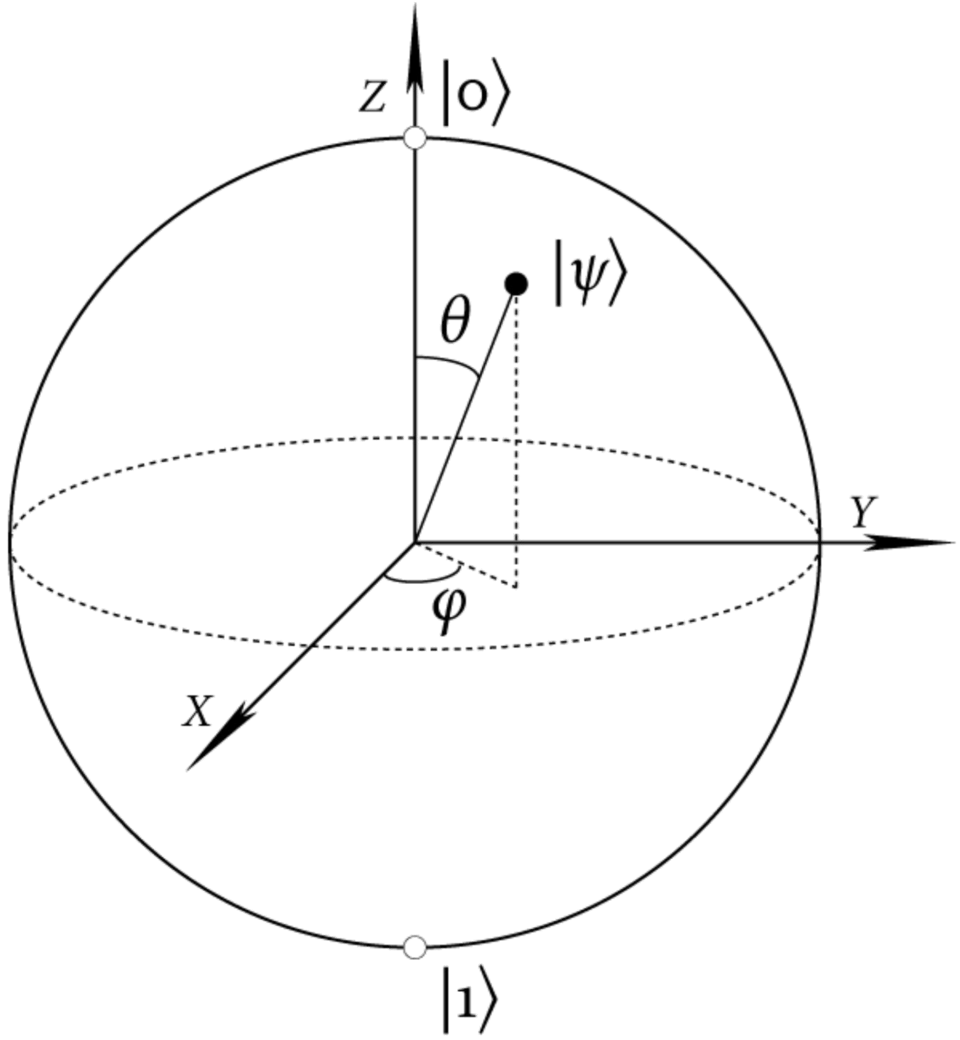
Qubit in Terms of The Angles



- Physically equivalent state
  - $|\psi\rangle \equiv |0\rangle + \beta|1\rangle$
  - $|\psi\rangle \equiv r_0|0\rangle + r_1 e^{i(\varphi_1 - \varphi_0)}|1\rangle$
- Redefine $|\psi\rangle$ to represent the state
  - Let $\varphi = \varphi_1 - \varphi_2$
  - $0 \leq \varphi \leq 2\pi$
- Recall the unit-norm constraint
  - $|r_0|^2 + |r_1|^2 = 1$
- Parametrize into term θ
  - $r_0 = \cos(\theta/2)$
  - $r_1 = \sin(\theta/2)$
  - $0 \leq \theta \leq \pi$
- Bloch sphere representation of the qubit
  - $|\psi\rangle = \cos(\theta/2)\,|0\rangle + e^{i\varphi}\sin(\theta/2)\,|1\rangle$
    - $0 \leq \theta \leq \pi$
    - $0 \leq \varphi \leq 2\pi$

M. Wilde, *From Classical to Quantum Shannon Theory,* Cambridge University Press, 2019.

Probability Amplitude



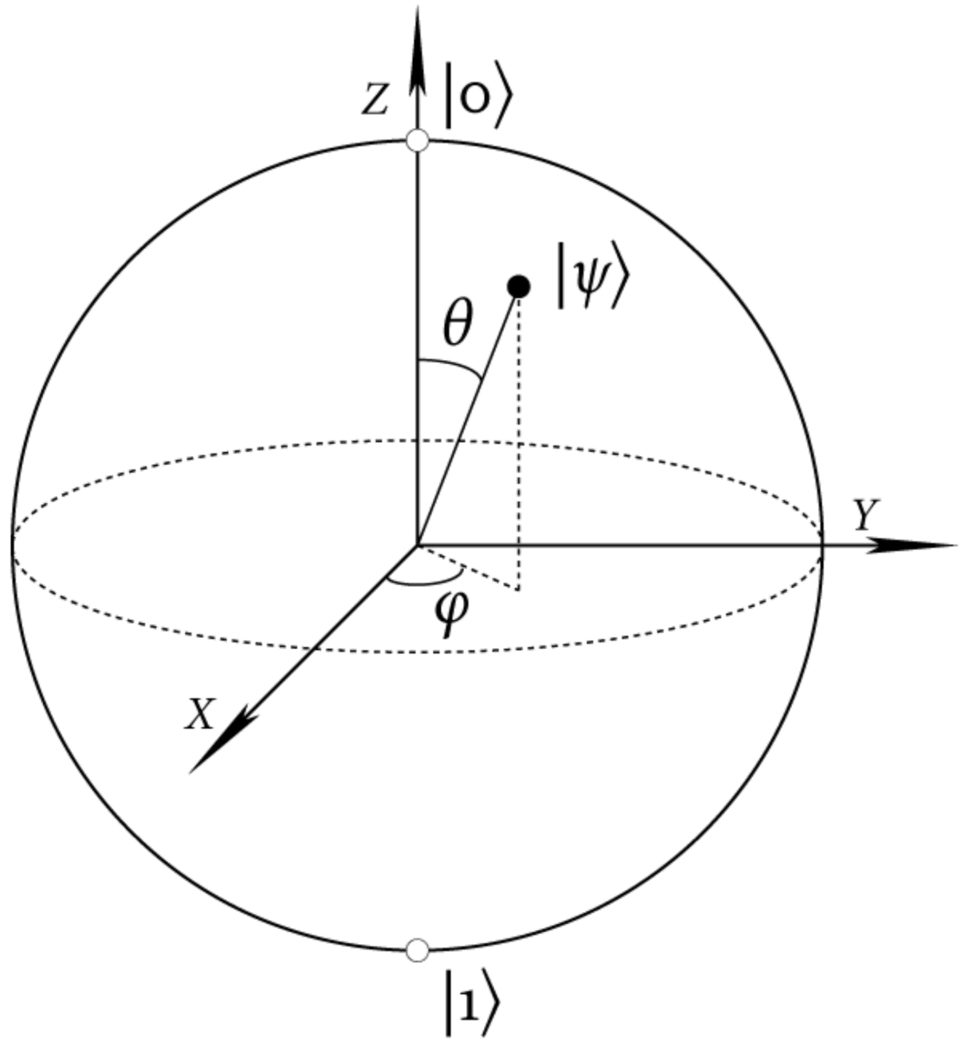
- $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

- $|\psi\rangle$ being in the state $|0\rangle$
  - $\langle 0|\psi\rangle = \langle 0|(\alpha|0\rangle + \beta|1\rangle)$
  - $\langle 0||\psi\rangle = \alpha\langle 0||0\rangle + \beta\langle 0||1\rangle$
  - $\langle 0||\psi\rangle = \alpha[1\ 0]\begin{bmatrix}1\\0\end{bmatrix} + \alpha[1\ 0]\begin{bmatrix}0\\1\end{bmatrix}$
  - $\langle 0||\psi\rangle = \alpha \cdot 1 + \beta \cdot 0$
  - $\langle 0||\psi\rangle = \alpha$

- $|\psi\rangle$ being in the state $|1\rangle$
  - $\langle 1|\psi\rangle = \langle 1|(\alpha|0\rangle + \beta|1\rangle)$
  - $\langle 1||\psi\rangle = \alpha\langle 1||0\rangle + \beta\langle 1||1\rangle$
  - $\langle 1||\psi\rangle = \alpha[0\ 1]\begin{bmatrix}1\\0\end{bmatrix} + \alpha[0\ 1]\begin{bmatrix}0\\1\end{bmatrix}$
  - $\langle 1||\psi\rangle = \alpha \cdot 0 + \beta \cdot 1$
  - $\langle 1||\psi\rangle = \beta$

M. Wilde, *From Classical to Quantum Shannon Theory,* Cambridge University Press, 2019.

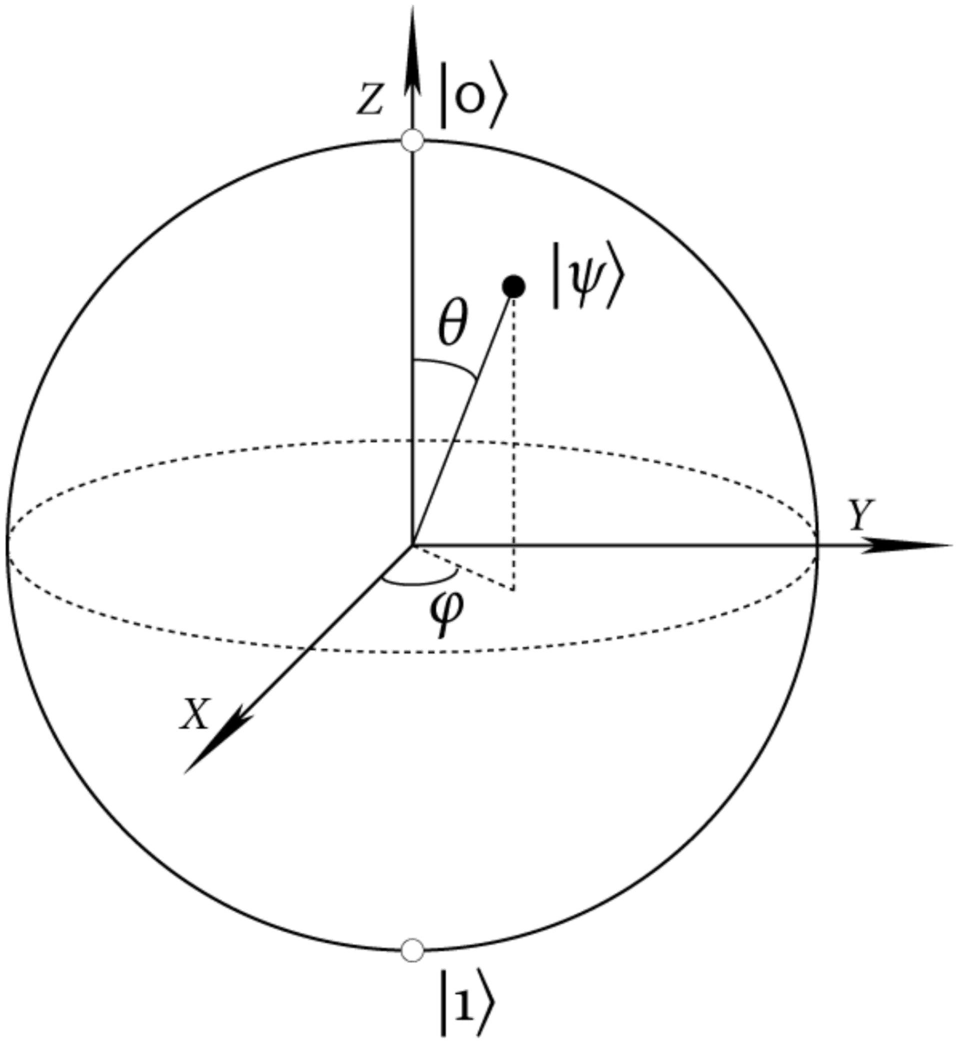
Probability Amplitudes



- Abbreviation
  - $\langle 0|\psi\rangle \equiv \langle 0||\psi\rangle$
  - "Braket"
- Orthogonal states
  - $\langle 1|0\rangle = [0\ 1]\begin{bmatrix}1\\0\end{bmatrix} = 0 + 0 = 0$
    - The state $|0\rangle$ to be in the state $|1\rangle$
  - $\langle 0|1\rangle = [1\ 0]\begin{bmatrix}0\\0\end{bmatrix} = 0 + 0 = 0$
    - The state $|1\rangle$ to be in the state $|0\rangle$
- The same states
  - $\langle 0|0\rangle = [1\ 0]\begin{bmatrix}1\\0\end{bmatrix} = 1 + 0 = 1$
    - The state $|0\rangle$ to be in the state $|0\rangle$
  - $\langle 1|1\rangle = [1\ 0]\begin{bmatrix}1\\0\end{bmatrix} = 1 + 0 = 1$
    - The state $|1\rangle$ to be in the state $|1\rangle$

M. Wilde, *From Classical to Quantum Shannon Theory,* Cambridge University Press, 2019.

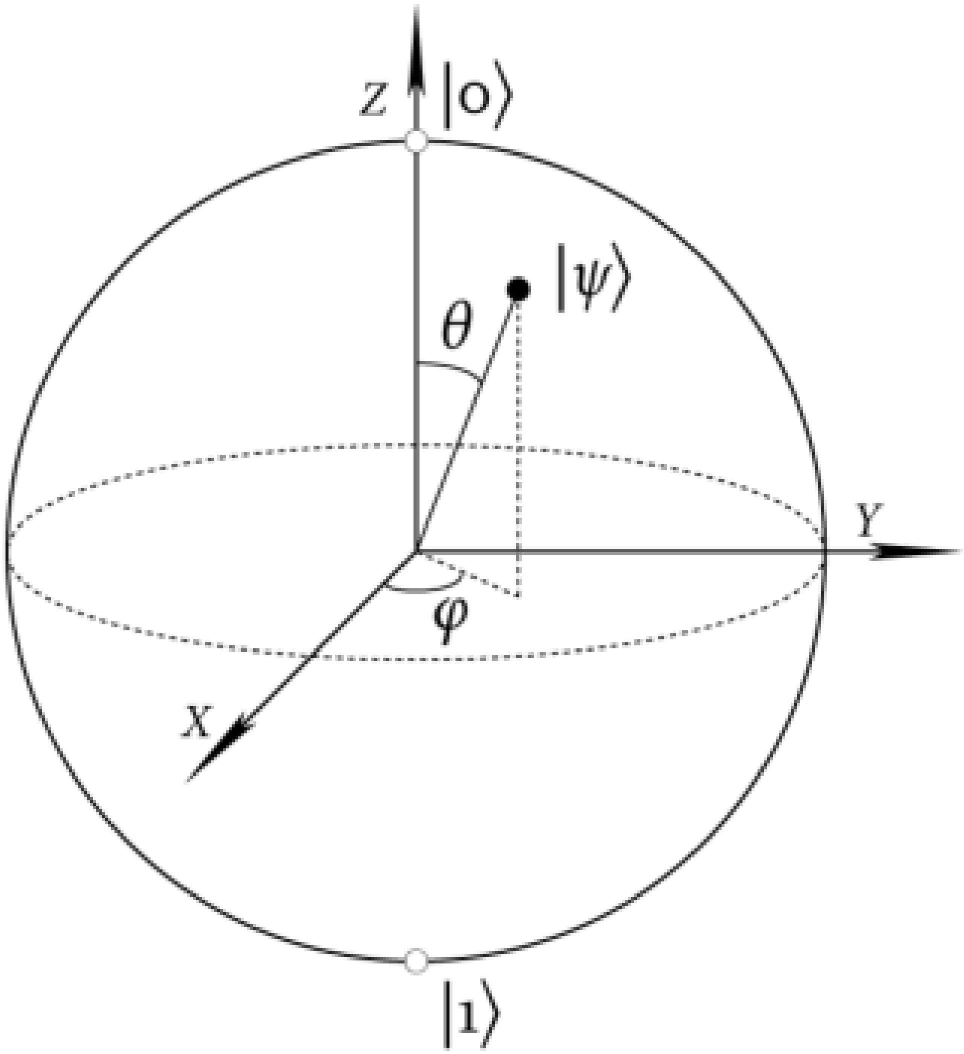
Probability Amplitudes



- Probability amplitude of any states
  - $\langle\psi|\psi\rangle = (\langle 0|\alpha^* + \langle 1|\beta^*)(\alpha|0\rangle + \beta|1\rangle)$
  - $\langle\psi|\psi\rangle = \alpha^*\alpha\langle 0|0\rangle + \beta^*\alpha\langle 1|0\rangle + \alpha^*\beta\langle 0|1\rangle + \beta^*\beta\langle 1|1\rangle$
  - $\langle\psi|\psi\rangle = |\alpha|^2 + 0 + 0 + |\beta|^2$
  - $\langle\psi|\psi\rangle = |\alpha|^2 + |\beta|^2$
  - $\langle\psi|\psi\rangle = 1$
    - The unit-norm constraint
- Euclidean norm of $|\psi\rangle$
  - $\||\psi\rangle\|_2 = \sqrt{\langle\psi|\psi}$
  - $\||\psi\rangle\|_2 = \sqrt{1}$
  - $\||\psi\rangle\|_2 = 1$
- Any quantum state has a unit amplitude for being itself

M. Wilde, *From Classical to Quantum Shannon Theory,* Cambridge University Press, 2019.

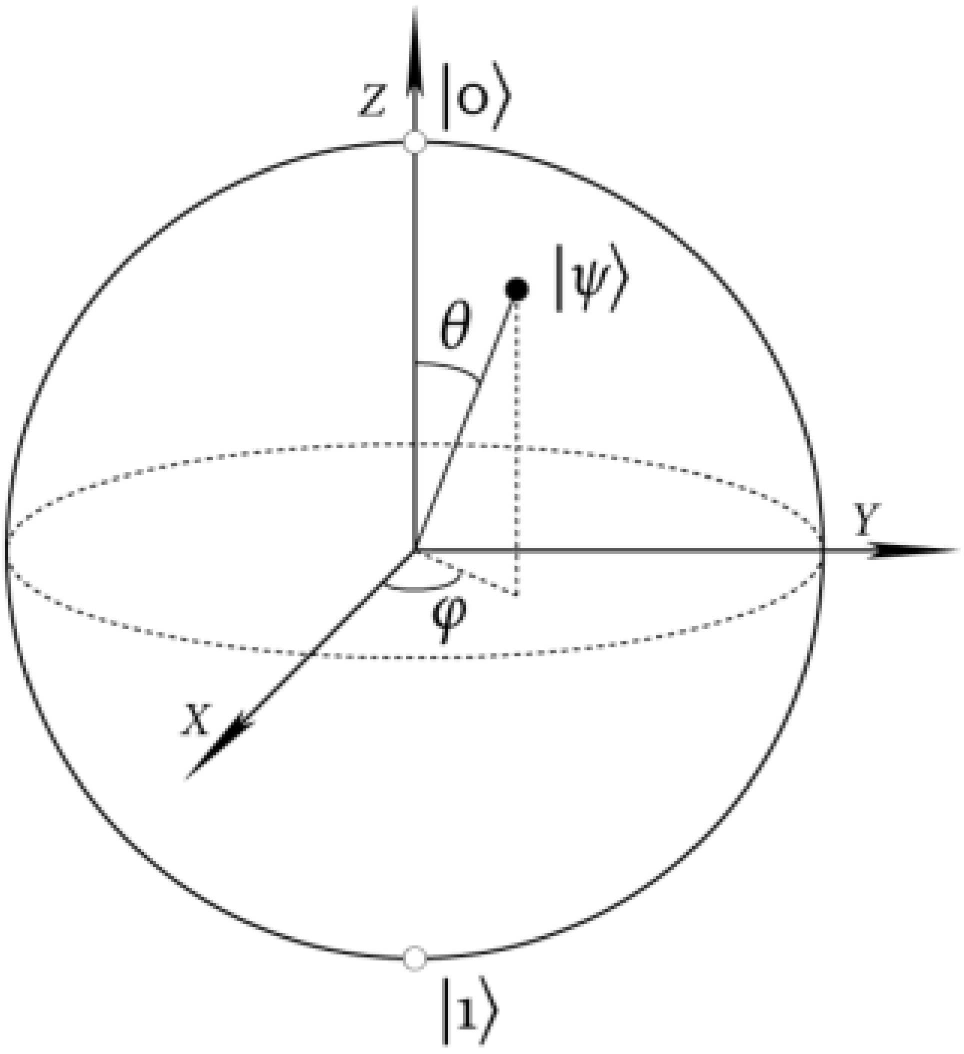
Bases



- Computational basis is a particular basis for qubit as standard basis employed in quantum computation and communication
  - $|0\rangle$
  - $|1\rangle$
- Other bases are important as well, i.e., orthonormal basis
  - $\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} = \frac{1}{\sqrt{2}}\left(\begin{bmatrix}1\\0\end{bmatrix} + \begin{bmatrix}0\\1\end{bmatrix}\right)$
  - $\frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix} = \frac{1}{\sqrt{2}}\left(\begin{bmatrix}1\\0\end{bmatrix} - \begin{bmatrix}0\\1\end{bmatrix}\right)$
- Diract notation in terms of the computational basis
  - $|+\rangle \equiv \frac{1}{\sqrt{2}}\left(\begin{bmatrix}1\\0\end{bmatrix} + \begin{bmatrix}0\\1\end{bmatrix}\right) = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$
  - $|-\rangle \equiv \frac{1}{\sqrt{2}}\left(\begin{bmatrix}1\\0\end{bmatrix} - \begin{bmatrix}0\\1\end{bmatrix}\right) = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$
- The common names for this alternate basis
  - "+/−" basis
  - Hadamard basis
  - Diagonal basis

M. Wilde, *From Classical to Quantum Shannon Theory*, Cambridge University Press, 2019.

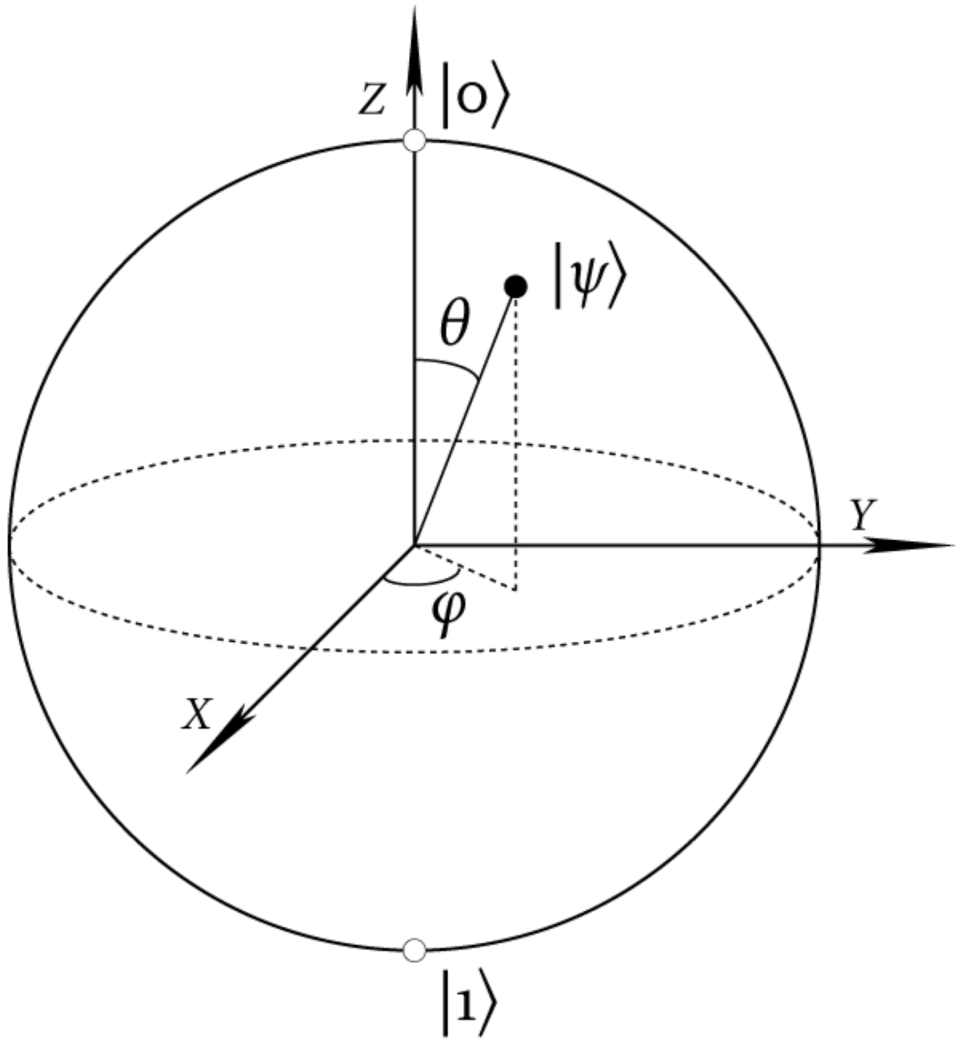
Amplitude in The “+/−“ Basis



- The amplitude that the state $|\psi\rangle$ is in the state $|+\rangle$
  - $\langle +|\psi\rangle = \langle +|(\alpha|0\rangle + \beta|1\rangle)$
  - $\langle +|\psi\rangle = \alpha\langle +|0\rangle + \beta\langle +|1\rangle$
  - $\langle +|\psi\rangle = \alpha\left(\frac{1}{\sqrt{2}}[1\ 1]\begin{bmatrix}1\\0\end{bmatrix}\right)+\beta\left(\frac{1}{\sqrt{2}}[1\ 1]\begin{bmatrix}0\\1\end{bmatrix}\right)$
  - $\langle +|\psi\rangle=\alpha\left(\frac{1}{\sqrt{2}}\right)+\beta\left(\frac{1}{\sqrt{2}}\right)$
  - $\langle +|\psi\rangle = \frac{\alpha+\beta}{\sqrt{2}}$
- The amplitude that the state $|\psi\rangle$ is in the state $|-\rangle$
  - $\langle -|\psi\rangle = \langle -|(\alpha|0\rangle + \beta|1\rangle)$
  - $\langle -|\psi\rangle = \alpha\langle -|0\rangle + \beta\langle -|1\rangle$
  - $\langle -|\psi\rangle = \alpha\left(\frac{1}{\sqrt{2}}[1\ -1]\begin{bmatrix}1\\0\end{bmatrix}\right)+\beta\left(\frac{1}{\sqrt{2}}[1\ -1]\begin{bmatrix}0\\1\end{bmatrix}\right)$
  - $\langle -|\psi\rangle=\alpha\left(\frac{1}{\sqrt{2}}\right)+\beta\left(\frac{-1}{\sqrt{2}}\right)$
  - $\langle -|\psi\rangle = \frac{\alpha-\beta}{\sqrt{2}}$

M. Wilde, *From Classical to Quantum Shannon Theory*, Cambridge University Press, 2019.

Superposition States and Identity Operator



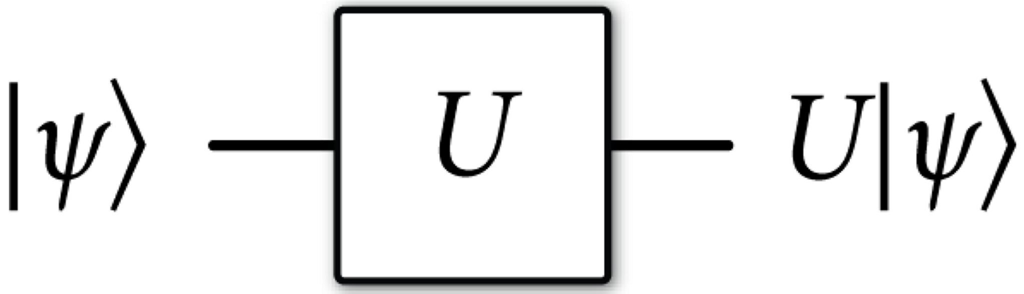
- $+/-$ basis is a *complete* orthonormal basis
  - Any qubit can be represented by two basis states
    - $|+\rangle$
    - $|-\rangle$
- To see qubit state representation in the “$+/-$” basis
  - Superposition states
    - $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
    - $|\psi\rangle = \langle+|\psi\rangle|+\rangle + \langle-|\psi\rangle|-\rangle$
    - $|\psi\rangle = \left(\frac{\alpha+\beta}{\sqrt{2}}\right)|+\rangle + \left(\frac{\alpha-\beta}{\sqrt{2}}\right)|-\rangle$
  - The amplitude $\langle+|\psi\rangle$ and $\langle-|\psi\rangle$ are scalar
    - $|\psi\rangle = \langle+|\psi\rangle|+\rangle + \langle-|\psi\rangle|-\rangle$
    - $|\psi\rangle = |+\rangle\langle+|\psi\rangle + |-\rangle\langle-|\psi\rangle$
    - $|\psi\rangle = (|+\rangle\langle+|+|-\rangle\langle-|)\,|\psi\rangle$
    - $|\psi\rangle = I|\psi\rangle$
  - Identity operator
    - $I = |+\rangle\langle+| + |-\rangle\langle-|$
    - $I = |0\rangle\langle 0| + |1\rangle\langle 1|$

- The completeness relation or the resolution of the identity.

M. Wilde, *From Classical to Quantum Shannon Theory,* Cambridge University Press, Fig. 2019.

Unitary Operation

Unitary Operation



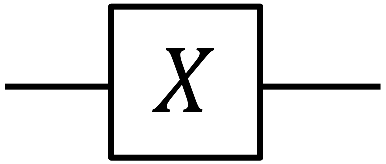
- Quantum circuit diagram for unitary evolution
- Unitary operation evolves the quantum system
- Unitary evolution implies reversibility
  - A unitary operator
    - U
  - Always possesses an inverse
    - U^*, conjugate transpose
- $U^*U = UU^* = I$

- The unitary property also ensures that evolution preserves the unit-norm constraint
  - An important requirement for a physical state
- Applying the unitary operator U to the example qubit state
  - $U|\psi\rangle$
- Every quantum state should have a unit amplitude for being itself
  - $\langle\psi|U^*U|\psi\rangle = \langle\psi|I|\psi\rangle = \langle\psi|\psi\rangle = 1$

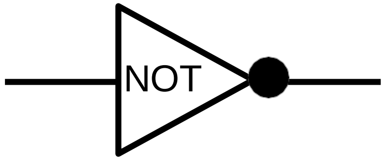
M. Wilde, *From Classical to Quantum Shannon Theory,* Cambridge University Press, 2019.

NOT Gate is Reversible

- An example of a single-qubit reversible operation is a NOT gate or X operator in quantum world
  - Flip the computational basis state
  - $|0\rangle \rightarrow |1\rangle$
    - $\begin{bmatrix}1\\0\end{bmatrix} \rightarrow \begin{bmatrix}0\\1\end{bmatrix}$
  - $|1\rangle \rightarrow |0\rangle$
    - $\begin{bmatrix}0\\1\end{bmatrix} \rightarrow \begin{bmatrix}1\\0\end{bmatrix}$



- NOT gate in the classical world
  - Flip the classical bit
    - $0 \rightarrow 1$
    - $1 \rightarrow 0$



- The NOT gate is reversible hence we can simply apply the NOT gate again to recover the original input state, where NOT gate is its own inverse

- Action of X on the computational basis states
  - $X|0\rangle = |0 \oplus 1\rangle = |1\rangle$
  - $X|1\rangle = |1 \oplus 1\rangle = |0\rangle$
  - $\oplus$ is binary addition

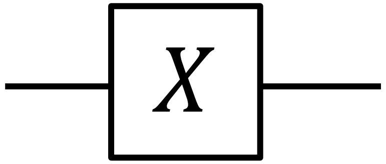
- NOT gate acts on a superposition state
  - $X|\psi\rangle = X(\alpha|0\rangle + |\beta\rangle)$

- Linearity of the quantum theory, distribution
  - $X|\psi\rangle = \alpha X|0\rangle + \beta X|1\rangle$
  - $X|\psi\rangle = \alpha|1\rangle + \beta|0\rangle$

- NOT gate or X operator merely flips the basis states of any quantum state when represented in the computational basis

M. Wilde, *From Classical to Quantum Shannon Theory,* Cambridge University Press, Fig. 3.1., 2019.

Matrix Representation of X Operator



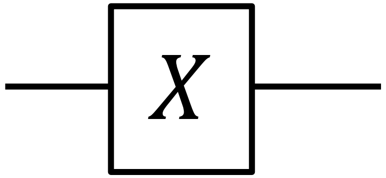
- With the use of bras $\langle 0|$ and $\langle 1|$
  - $\langle 0|X|0\rangle = \langle 0|1\rangle = 0$
  - $\langle 0|X|1\rangle = \langle 0|0\rangle = 1$
  - $\langle 1|X|0\rangle = \langle 1|1\rangle = 1$
  - $\langle 1|X|1\rangle = \langle 1|0\rangle = 0$
- X operator where rows with bras and columns with kets
  - $X = \begin{bmatrix} \langle 0|X|0\rangle & \langle 0|X|1\rangle \\ \langle 1|X|0\rangle & \langle 1|X|1\rangle \end{bmatrix}$
  - $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

- X operator on the $+/-$ basis
- $|+\rangle$ is eigenstate of X with eigenvalue 1
  - $X|+\rangle = X\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)$
  - $X|+\rangle = \frac{X|0\rangle+X|1\rangle}{\sqrt{2}}$
  - $X|+\rangle = \frac{X|1\rangle+X|0\rangle}{\sqrt{2}}$
  - $X|+\rangle = |+\rangle$
- $|-\rangle$ is eigenstate of X with eigenvalue -1
  - $X|-\rangle = X\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$
  - $X|-\rangle = \frac{X|0\rangle-X|1\rangle}{\sqrt{2}}$
  - $X|-\rangle = \frac{X|1\rangle-X|0\rangle}{\sqrt{2}}$
  - $X|-\rangle = |-\rangle$

M. Wilde, *From Classical to Quantum Shannon Theory,* Cambridge University Press, 2019.

Eigenbasis of X Operator

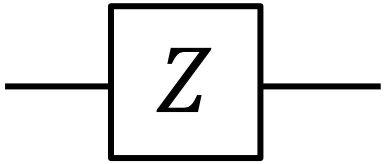
- X operator in $+/-$ basis
  - $\begin{bmatrix} \langle +|X|+\rangle & \langle +|X|-\rangle \\ \langle -|X|+\rangle & \langle -|X|-\rangle \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
  - Diagonal with respect to the $+/-$ basis
  - $+/-$ basis in an eigenbasis for X operator
  - Eigenbasis gives the states that are invariant under an evolution according to U



- How do we determine a function of an operator?
  - The standard way is to represent the operator in its diagonal basis and apply the function to the non-zero eigenvalues of the operator
  - For example, the diagonal representation of the X operator is
    - $X = |+\rangle\langle +| - |-\rangle\langle -|$
      - Proof left for quiz/homework

M. Wilde, *From Classical to Quantum Shannon Theory,* Cambridge University Press, 2019.

Z Operator



- Flips the states in $+/-$ basis

- $Z|+\rangle \to |-\rangle$
- $Z|-\rangle \to |+\rangle$

- $\begin{bmatrix} \langle +|Z|+\rangle & \langle +|Z|-\rangle \\ \langle -|Z|+\rangle & \langle -|Z|-\rangle \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

- Z operator in $+/-$ basis is the same X operator in computational basis

- Z operator is *phase flip* operator

- Z operator in computational basis

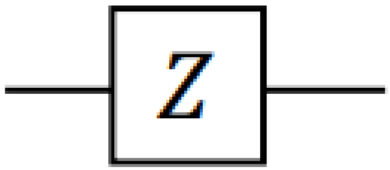
  - $\begin{bmatrix} \langle 0|Z|0\rangle & \langle 0|Z|1\rangle \\ \langle 1|Z|0\rangle & \langle 1|Z|1\rangle \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

  - Diagonalization of the Z operator

  - The behavior of the Z operator in the computational basis is the same as the behavior of the X operator in the $+/-$ basis

M. Wilde, *From Classical to Quantum Shannon Theory,* Cambridge University Press, 2019.

Z Operator on The $+/-$ Basis



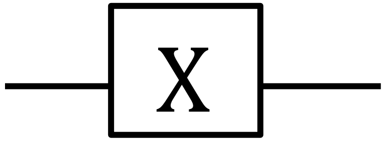
- $\frac{|+\rangle+|-\rangle}{\sqrt{2}}$ is eigenstate of Z with eigenvalue 1
  - $Z\left(\frac{|+\rangle+|-\rangle}{\sqrt{2}}\right)=\frac{Z|+\rangle+Z|-\rangle}{\sqrt{2}}$
  - $Z\left(\frac{|+\rangle+|-\rangle}{\sqrt{2}}\right)=\frac{|-\rangle+|+\rangle}{\sqrt{2}}$
  - $Z\left(\frac{|+\rangle+|-\rangle}{\sqrt{2}}\right)=\frac{|+\rangle+|-\rangle}{\sqrt{2}}$
- $\frac{|+\rangle-|-\rangle}{\sqrt{2}}$ is eigenstate of Z with eigenvalue -1
  - $Z\left(\frac{|+\rangle-|-\rangle}{\sqrt{2}}\right)=\frac{Z|+\rangle-Z|-\rangle}{\sqrt{2}}$
  - $Z\left(\frac{|+\rangle-|-\rangle}{\sqrt{2}}\right)=\frac{|-\rangle-|+\rangle}{\sqrt{2}}$
  - $Z\left(\frac{|+\rangle-|-\rangle}{\sqrt{2}}\right)=-\frac{|+\rangle-|-\rangle}{\sqrt{2}}$

M. Wilde, *From Classical to Quantum Shannon Theory*, Cambridge University Press, 2019.

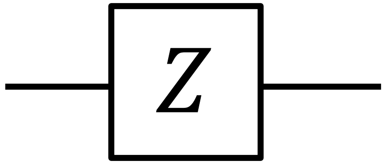
The Pauli Matrices and Hadamard Gate or Operator

- Computational basis is the standard basis for representing physical qubits

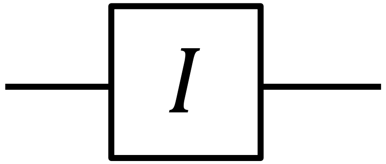
- X operator, bit flip
  - $X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$



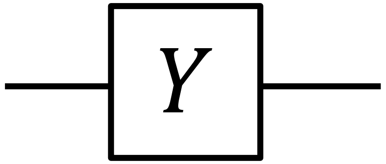
- Z operator, phase flip
  - $Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$



- I operator, identity
  - $I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

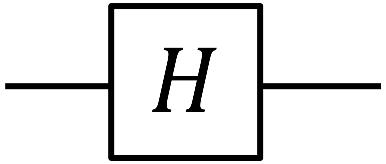


- Y operator
  - $Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
  - $Y = iXZ \rightarrow$ quiz/homework



- Hadamard gate

- Unitary operator to the transform computational basis to the $+/-$ basis
  - $|0\rangle \rightarrow |+\rangle$
  - $|1\rangle \rightarrow |-\rangle$



- Hadamard transformation
  - $H \equiv |+\rangle\langle 0| + |-\rangle\langle 1|$
  - $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$

M. Wilde, *From Classical to Quantum Shannon Theory,* Cambridge University Press, 2019.

Two Qubits

- The state of two cbits with particular states of qubits
  - $00 \ \rightarrow |0\rangle|0\rangle$
- Abbreviation
  - $|00\rangle \equiv |0\rangle|0\rangle$
- Tensor or Kroneker Product $\otimes$
  - $|00\rangle = |0\rangle \otimes |0\rangle$
  - $\begin{bmatrix} a_1 \\ b_1 \end{bmatrix} \otimes \begin{bmatrix} a_2 \\ b_2 \end{bmatrix} = \begin{bmatrix} a_1 \begin{bmatrix} a_2 \\ b_2 \end{bmatrix} \\ b_1 \begin{bmatrix} a_2 \\ b_2 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} a_1 a_2 \\ a_1 b_2 \\ b_1 a_2 \\ b_1 b_2 \end{bmatrix}$
- Simple way to remember these representations
  - The bits inside the ket index the element equal to one in the vector
  - The vector representation of $|01\rangle$ has a one as its second element because 01 is the second index for the two-bit strings

- $|00\rangle \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \begin{bmatrix} 1 \\ 0 \end{bmatrix} \\ 0 \begin{bmatrix} 1 \\ 0 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$
- $|01\rangle \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \begin{bmatrix} 0 \\ 1 \end{bmatrix} \\ 0 \begin{bmatrix} 0 \\ 1 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$
- $|10\rangle \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \begin{bmatrix} 1 \\ 0 \end{bmatrix} \\ 1 \begin{bmatrix} 1 \\ 0 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$
- $|11\rangle \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \begin{bmatrix} 0 \\ 1 \end{bmatrix} \\ 1 \begin{bmatrix} 0 \\ 1 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$

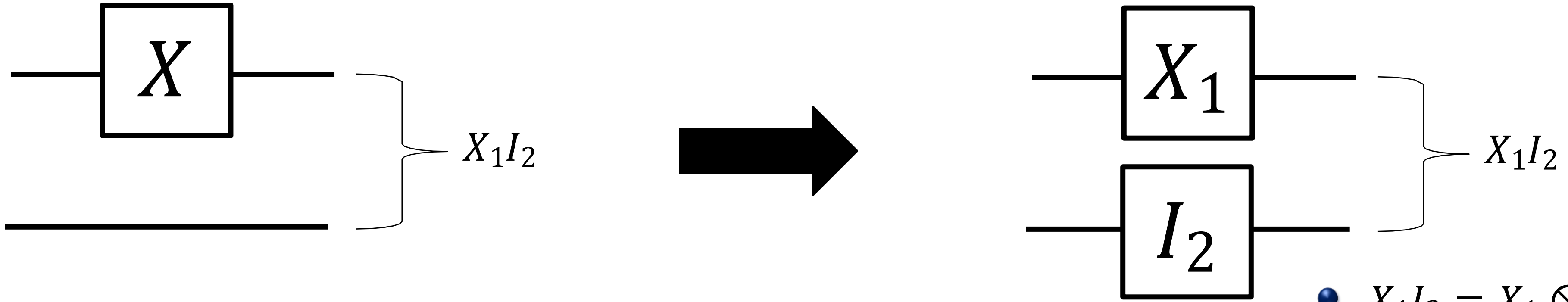
M. Wilde, *From Classical to Quantum Shannon Theory,* Cambridge University Press, 2019.

Two Qubits and Three Qubits

- Superposition of two-qubits states
  - $|\xi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle = \begin{bmatrix}\alpha\\ \beta\\ \gamma\\ \delta\end{bmatrix}$
  - $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$
- Common to use
  - $|\psi\rangle_L = \alpha|00\rangle + \beta|11\rangle$
  - $\alpha|00\rangle + \beta|11\rangle = \alpha\begin{bmatrix}1\\0\\0\\0\end{bmatrix} + \beta\begin{bmatrix}0\\0\\0\\1\end{bmatrix}$
  - $\alpha|00\rangle + \beta|11\rangle = \begin{bmatrix}\alpha\\0\\0\\0\end{bmatrix} + \begin{bmatrix}0\\0\\0\\\beta\end{bmatrix} = \begin{bmatrix}\alpha\\0\\0\\\beta\end{bmatrix}$
- Three qubits
  - $|000\rangle \equiv \begin{bmatrix}1\\0\end{bmatrix} \otimes \left[\begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix}\right]$
  - $|000\rangle \equiv \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}1\begin{bmatrix}1\\0\end{bmatrix}\\ 0\begin{bmatrix}1\\0\end{bmatrix}\end{bmatrix} = \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}1\\0\\0\\0\end{bmatrix}$
  - $|000\rangle \equiv \begin{bmatrix}1\begin{bmatrix}1\\0\\0\\0\end{bmatrix}\\ 0\begin{bmatrix}1\\0\\0\\0\end{bmatrix}\end{bmatrix} = \begin{bmatrix}1\\0\\0\\0\\0\\0\\0\\0\end{bmatrix}$
  - Three qubits and above are left for programming of Python (or MATLAB and Octave) due to huge matrix dimension

M. Wilde, *From Classical to Quantum Shannon Theory,* Cambridge University Press, 2019.

$X_1 I_2$ Operation

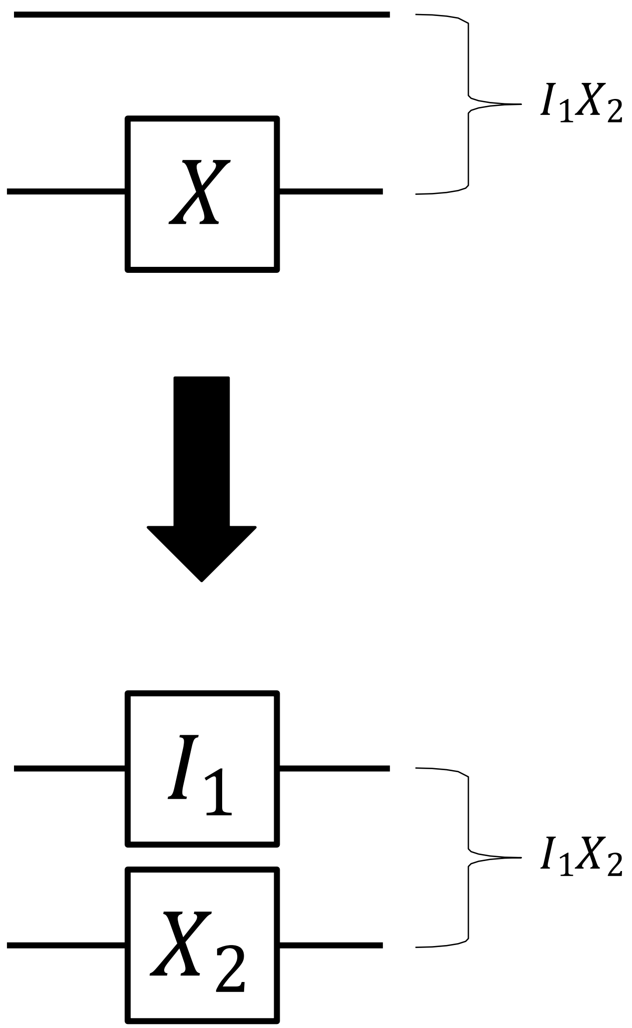


- $X_1 I_2 = X_1 \otimes I_1$
- $X_1 I_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$
- $X_1 I_2 = \begin{bmatrix} 0 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & 1 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\ 1 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & 0 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \end{bmatrix}$
- $X_1 I_2 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$

- Apply tensor or Kronecker product
- Obtain 4×4 dimension matrix
- X operator at the above line is placed at the left side of $\otimes$
- The line below is equivalent to Identity operator or I operator
- Place the I operator at the right side of $\otimes$
- Indexes $(\cdot)_1$ and $(\cdot)_2$ are for the first and second line or first and second qubits, respectively
- NOT gate or X operator flips the first qubit and does nothing (applies the identity or I operator) to the second qubit

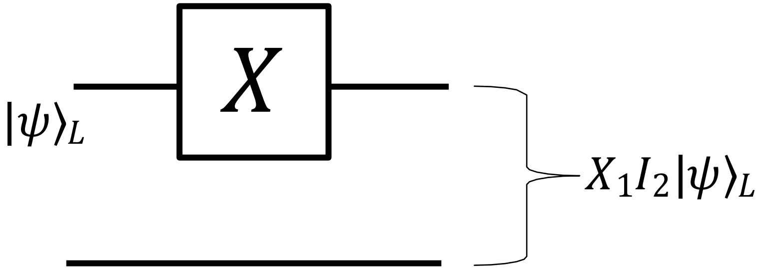
M. Wilde, *From Classical to Quantum Shannon Theory,* Cambridge University Press, 2019.

$I_1 X_2$ Operation

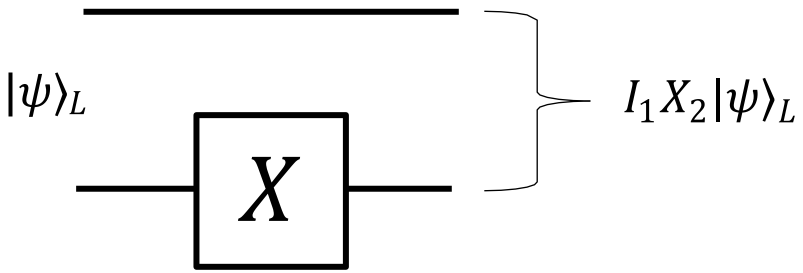


- $I_1X_2 = I_1 \otimes X_2$
- $I_1X_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
- $I_1X_2 = \begin{bmatrix} 1\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} & 0\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \\ 0\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} & 1\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \end{bmatrix}$
- $I_1X_2 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$

$X_1 I_2|\psi\rangle_L$ and $I_1 X_2|\psi\rangle_L$ Operations

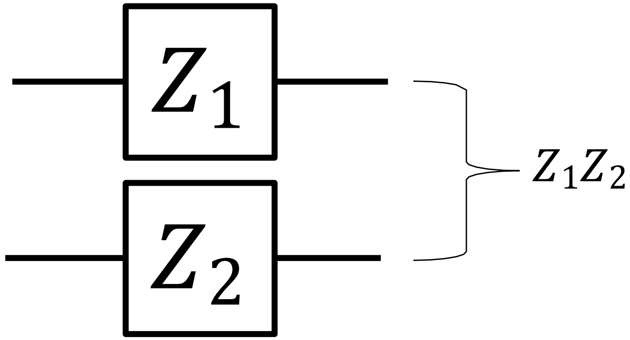


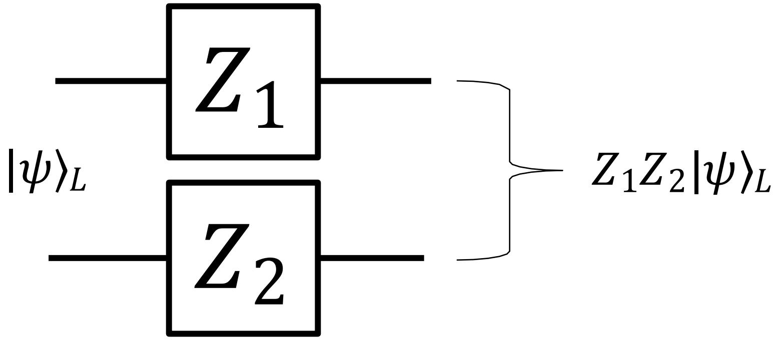
- $|\psi\rangle_L = \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix} \alpha \\ 0 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 0 \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ 0 \\ 0 \\ \beta \end{bmatrix}$
- $X_1 I_2|\psi\rangle_L = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ 0 \\ 0 \\ \beta \end{bmatrix}$
- $X_1 I_2\,|\psi\rangle_L = \begin{bmatrix} 0 \\ \beta \\ \alpha \\ 0 \end{bmatrix} = \alpha \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$
- $X_1|I_2\psi\rangle_L \ = \alpha|10\rangle + \beta|01\rangle$



- $I_1 X_2|\psi\rangle_L = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ 0 \\ 0 \\ \beta \end{bmatrix}$
- $I_i X_2|\psi\rangle_L = \begin{bmatrix} 0 \\ \alpha \\ \beta \\ 0 \end{bmatrix} = \alpha \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$
- $I_1 X_2|\psi\rangle_L = \alpha|01\rangle + \beta|10\rangle$

Z_1Z_2 and $Z_1Z_2|\psi\rangle$ Operations

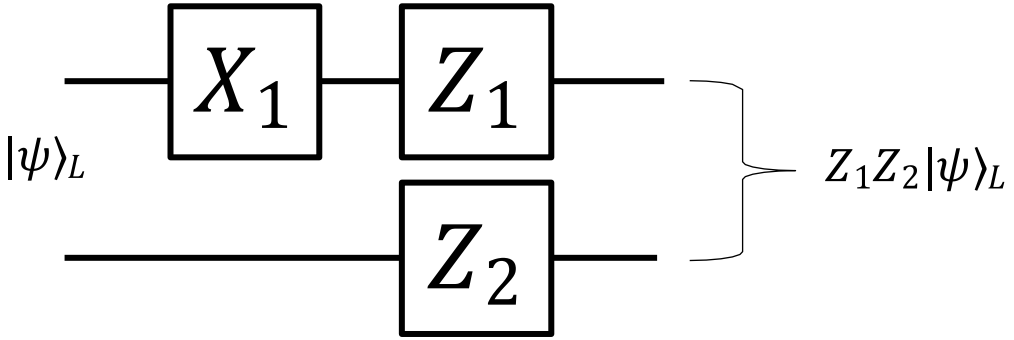


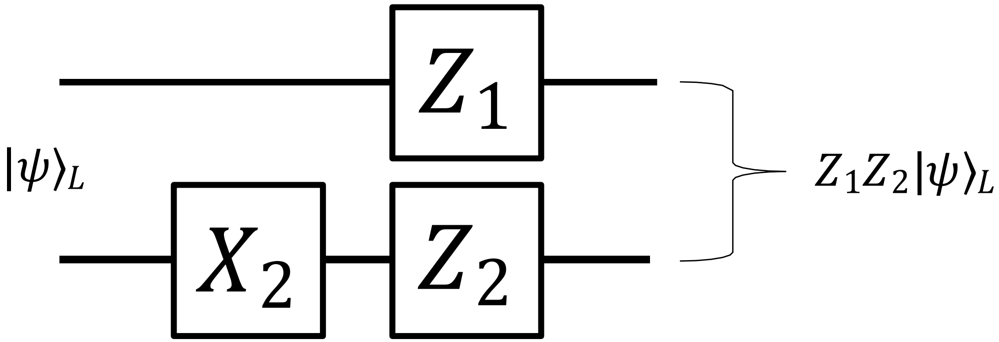


- $Z_1Z_2 = Z_1 \otimes Z_2$
- $Z_1Z_2 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
- $Z_1Z_2 = \begin{bmatrix} 1\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} & 0\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \\ 0\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} & -1\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \end{bmatrix}$
- $Z_1Z_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

- $Z_1Z_2|\psi\rangle_L = Z_1Z_2(\alpha|00\rangle + \beta|11\rangle)$
- $Z_1Z_2|\psi\rangle_L = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} \alpha \\ 0 \\ 0 \\ \beta \end{bmatrix}$
- $Z_1Z_2|\psi\rangle_L = (+1)\begin{bmatrix} \alpha \\ 0 \\ 0 \\ \beta \end{bmatrix} = (+1)\,|\psi\rangle_L$

$[Z_1Z_2][X_1I_2]|\psi\rangle$ and $[Z_1Z_2][I_1X_2]|\psi\rangle$ Operations





- $Z_1Z_2X_1I_2|\psi\rangle_L = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ \beta \\ \alpha \\ 0 \end{bmatrix}$
- $Z_1Z_2X_1I_2|\psi\rangle_L = (-1) \begin{bmatrix} 0 \\ \beta \\ \alpha \\ 0 \end{bmatrix}$
- $Z_1Z_2X_1I_2|\psi\rangle_L = -1\,(\alpha|10\rangle + \beta|01\rangle)$
- Note that the operation of the circuit
  - From the right side to the left
  - From the above line to the bottom line

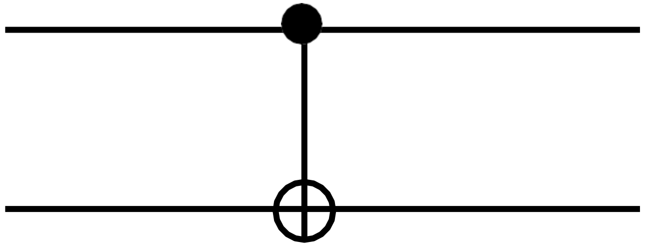
- $Z_1Z_2I_1X_2|\psi\rangle_L = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ \alpha \\ \beta \\ 0 \end{bmatrix}$
- $Z_1Z_2I_2X_2|\psi\rangle_L = (-1) \begin{bmatrix} 0 \\ \alpha \\ \beta \\ 0 \end{bmatrix}$
- $Z_1Z_2I_2X_2|\psi\rangle_L = -1(\alpha|01\rangle + \beta|10\rangle)$

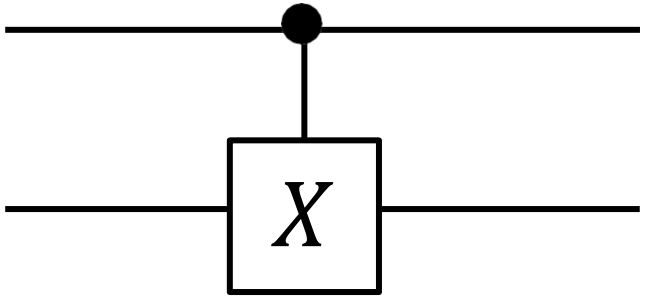
Controlled NOT (CNOT) Gate

- CNOT in two cbits
  - First bit zero → do nothing
  - First bit one → flip second bit
    - $00 \to 00$
    - $01 \to 01$
    - $10 \to 11$
    - $11 \to 10$
- CNOT in two qubits
  - $|00\rangle \to |00\rangle$
  - $|01\rangle \to |01\rangle$
  - $|10\rangle \to |11\rangle$
  - $|11\rangle \to |10\rangle$
- CNOT in superposition states
  - $\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$

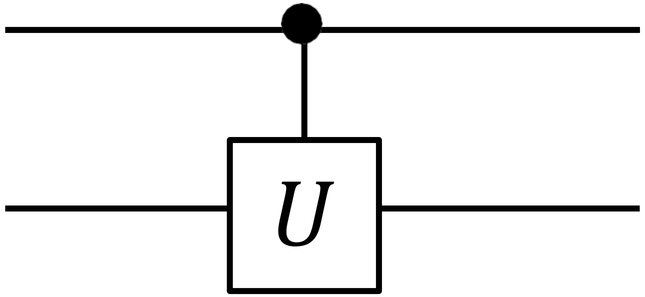
    $\big\downarrow$ CNOT
  - $\alpha|00\rangle + \beta|01\rangle + \gamma|11\rangle + \delta|10\rangle$

- $CNOT$ (CX) gate
  - Matrix with 4×4 dimension
  - $CNOT \equiv |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$
  - $CNOT \equiv \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$





- Controlled-U (CU) gate
  - $CU \equiv |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$
  - $U = \{X, Z, Y, I\}$
  - U is unitary operator

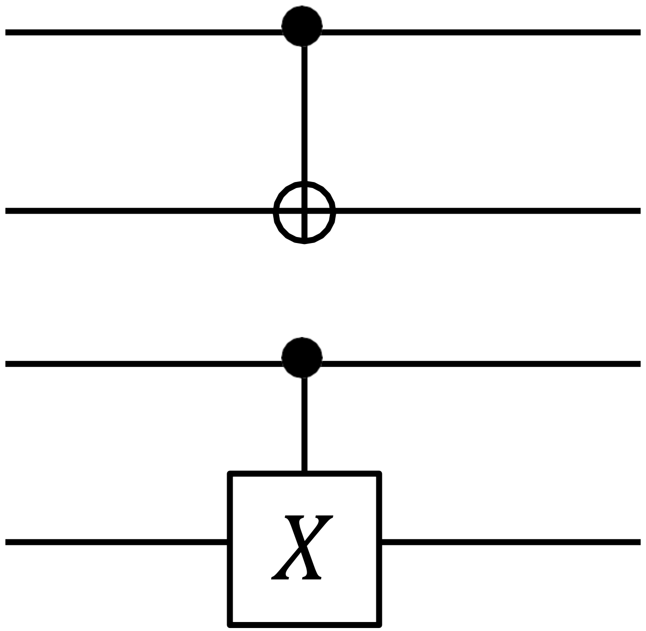


M. Wilde, *From Classical to Quantum Shannon Theory,* Cambridge University Press, 2019.

Controlled NOT (CNOT) Gate

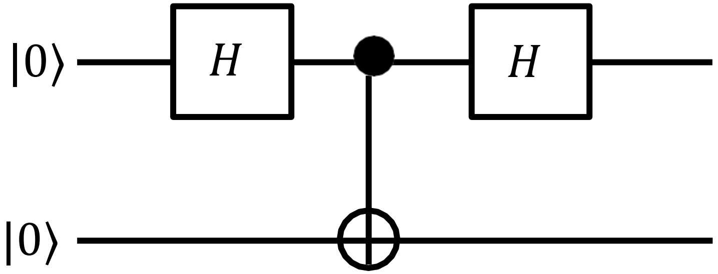
- $CNOT$ (CX) gate

  - $CNOT \equiv |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$
  - $CNOT \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
  - $CNOT \equiv \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
  - $CNOT \equiv \begin{bmatrix} 1\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & 0\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\ 0\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & 0\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \end{bmatrix} + \begin{bmatrix} 0\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} & 0\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \\ 0\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} & 1\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \end{bmatrix}$
  - $CNOT \equiv \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
  - $CNOT \equiv \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$



M. Wilde, *From Classical to Quantum Shannon Theory,* Cambridge University Press, 2019.

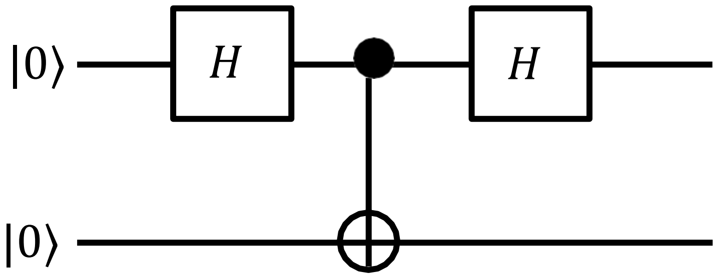
Hadamard and CNOT Circuit $[H \otimes I][CNOT][H \otimes I]|00\rangle$



- $[H \otimes I][CNOT][H \otimes I]|00\rangle = \left[\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right] \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \left[\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right] \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$

- $[H \otimes I][CNOT][H \otimes I]|00\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & 1\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\ 1\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & -1\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & 1\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\ 1\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & -1\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$

Hadamard and CNOT Circuit $[H \otimes I][CNOT][H \otimes I]|00\rangle$

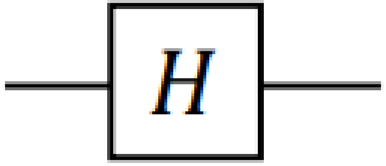


- $[H \otimes I][CNOT][H \otimes I]|00\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$
- $[H \otimes I][CNOT][H \otimes I]|00\rangle = \frac{1}{2}\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix}\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$
- $[H \otimes I][CNOT][H \otimes I]|00\rangle = \frac{1}{2}\begin{bmatrix} 1 \\ 1 \\ 1 \\ -1 \end{bmatrix} = \frac{1}{2}\left[\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 0 \\ -1 \end{bmatrix}\right] = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)$

Exercise #1

- Show Hadamard operator following matrix derivation!
  - $H \equiv |+\rangle\langle 0| + |-\rangle\langle 1| \rightarrow H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$

- Answer:
  - $H \equiv |+\rangle\langle 0| + |-\rangle\langle 1|$
  - $H = \frac{|0\rangle+|1\rangle}{\sqrt{2}}\langle 0| + \frac{|0\rangle-|1\rangle}{\sqrt{2}}\langle 1|$
  - $H = \frac{|0\rangle\langle 0|+|1\rangle\langle 0|}{\sqrt{2}} + \frac{|0\rangle\langle 1|-|1\rangle\langle 1|}{\sqrt{2}}$
  - $H = \frac{1}{\sqrt{2}}(|0\rangle\langle 0|+|1\rangle\langle 0| + |0\rangle\langle 1|-|1\rangle\langle 1|)$
  - $H = \frac{1}{\sqrt{2}}\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \end{bmatrix} - \begin{bmatrix} 0 \\ 1 \end{bmatrix}\begin{bmatrix} 0 & 1 \end{bmatrix}\right)$
  - $H = \frac{1}{\sqrt{2}}\left(\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}\right)$
  - $H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$



M. Wilde, *From Classical to Quantum Shannon Theory*, Cambridge University Press, 2019.

Exercise #2

- Show that $|0\rangle\langle +| + |1\rangle\langle -| = |+\rangle\langle 0| + |-\rangle\langle 1|$!

- Answer
- $|0\rangle\langle +| + |1\rangle\langle -| = \begin{bmatrix}1\\0\end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\end{bmatrix} + \begin{bmatrix}0\\1\end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix}1 & -1\end{bmatrix}$
- $|0\rangle\langle +| + |1\rangle\langle -| = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\0 & 0\end{bmatrix} + \frac{1}{\sqrt{2}}\begin{bmatrix}0 & 0\\1 & -1\end{bmatrix}$
- $|0\rangle\langle +| + |1\rangle\langle -| = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}$

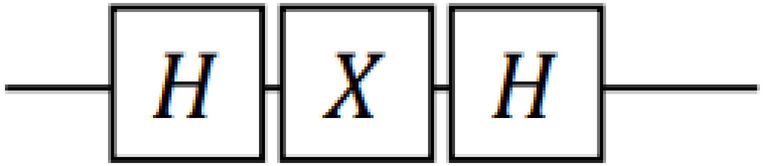
- $|+\rangle\langle 0| + |-\rangle\langle 1| = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}\begin{bmatrix}1 & 0\end{bmatrix} + \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}\begin{bmatrix}0 & 1\end{bmatrix}$
- $|+\rangle\langle 0| + |-\rangle\langle 1| = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 0\\1 & 0\end{bmatrix} + \frac{1}{\sqrt{2}}\begin{bmatrix}0 & 1\\0 & -1\end{bmatrix}$
- $|+\rangle\langle 0| + |-\rangle\langle 1| = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}$

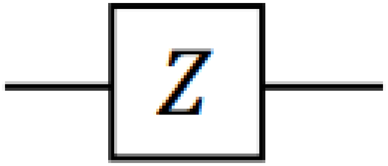
M. Wilde, *From Classical to Quantum Shannon Theory*, Cambridge University Press, 2019.

Exercise #3

- Show that $HXH = Z$!

- Answer:
  - $HXH = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}$
  - $HXH = \frac{1}{2}\begin{bmatrix}1 & 1\\-1 & 1\end{bmatrix}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}$
  - $HXH = \frac{1}{2}\begin{bmatrix}2 & 0\\0 & -2\end{bmatrix}$
  - $HXH = \begin{bmatrix}1 & 0\\0 & -1\end{bmatrix} = Z$



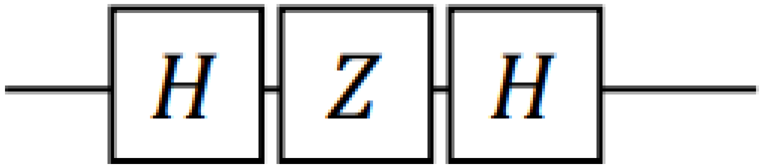


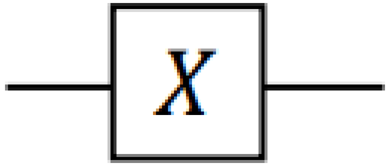
M. Wilde, *From Classical to Quantum Shannon Theory*, Cambridge University Press, 2019.

Exercise #4

- Show that $HZH = X$!

- Answer:
  - $HZH = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
  - $HZH = \frac{1}{2}\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
  - $HZH = \frac{1}{2}\begin{bmatrix} 0 & 2 \\ 2 & 0 \end{bmatrix}$
  - $HZH = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = X$



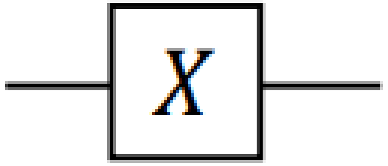


M. Wilde, *From Classical to Quantum Shannon Theory*, Cambridge University Press, 2019.

Exercise #5

- Show that $X = |+\rangle\langle+| - |-\rangle\langle-|$!

- Answer:
  - $X = |+\rangle\langle+| - |-\rangle\langle-|$
  - $X = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\end{bmatrix} - \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix}1 & -1\end{bmatrix}$
  - $X = \frac{1}{2}\begin{bmatrix}1 & 1\\1 & 1\end{bmatrix} - \frac{1}{2}\begin{bmatrix}1 & -1\\-1 & 1\end{bmatrix}$
  - $X = \frac{1}{2}\left(\begin{bmatrix}1 & 1\\1 & 1\end{bmatrix} - \begin{bmatrix}1 & -1\\-1 & 1\end{bmatrix}\right)$
  - $X = \frac{1}{2}\begin{bmatrix}0 & 2\\2 & 0\end{bmatrix}$
  - $X = \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$



M. Wilde, *From Classical to Quantum Shannon Theory*, Cambridge University Press, 2019.

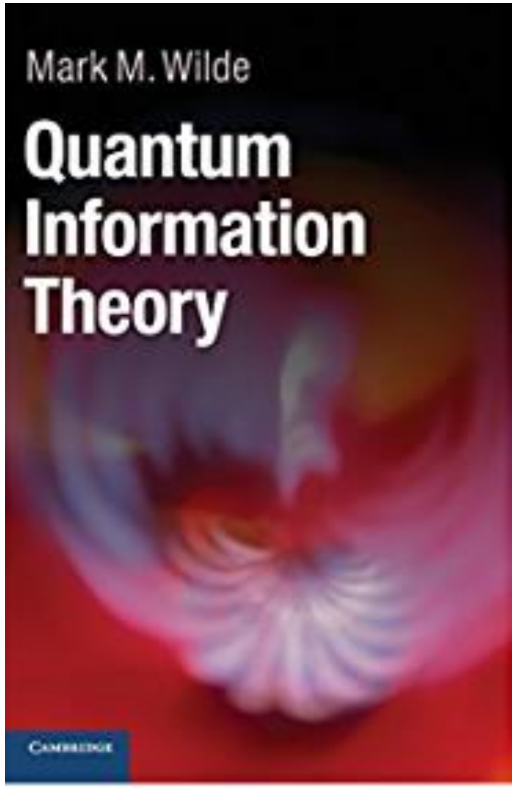
Exercise #6

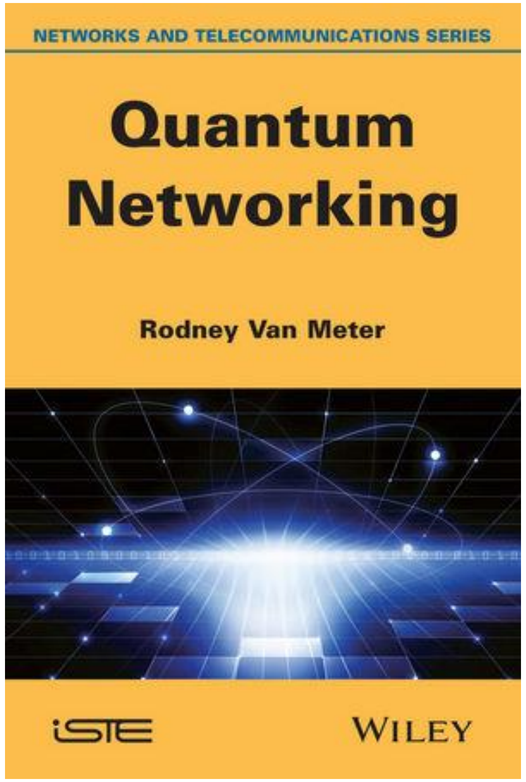
- Show that $Y = iXZ$!

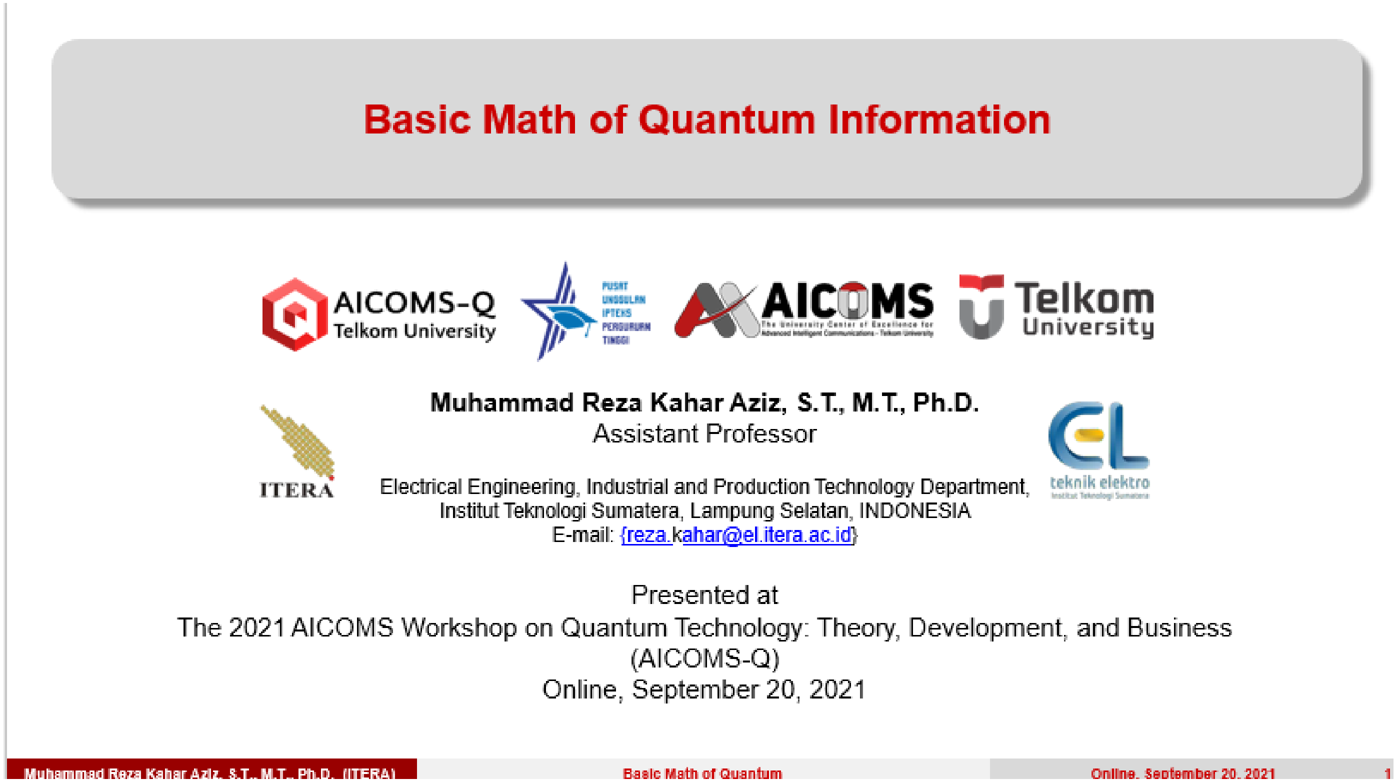
- Answer:
  - $Y = iXZ$
  - $Y = i\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
  - $Y = i\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$
  - $Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$

M. Wilde, *From Classical to Quantum Shannon Theory,* Cambridge University Press, 2019.

References







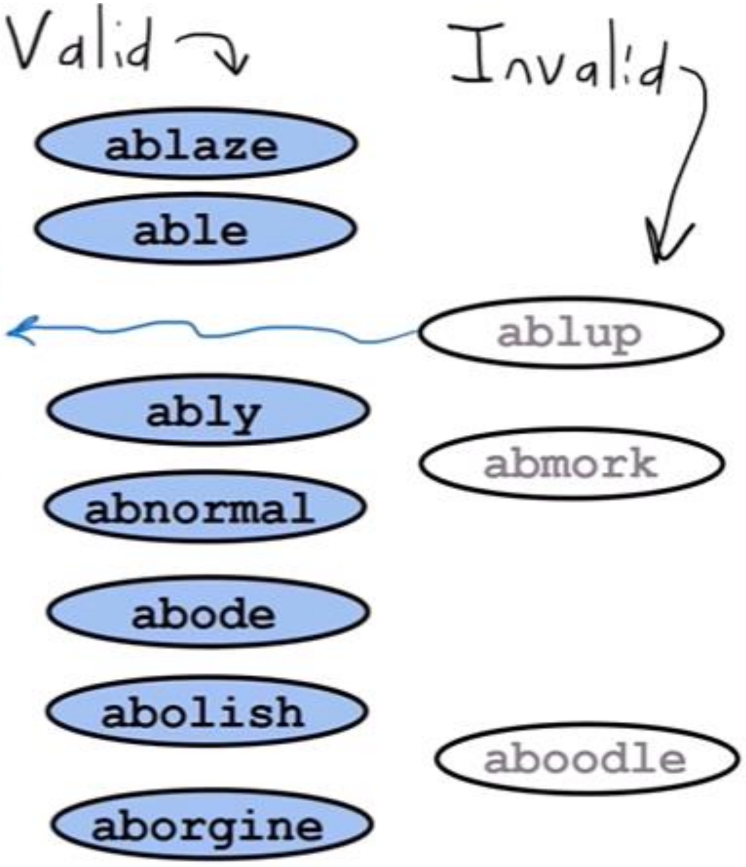
M. Wilde, *From Classical to Quantum Shannon Theory,* Cambridge University Press, 2019.
R. V. Meter, *Quantum Networking,* Wiley, 2014
The 2021 AICOMS-Q Workshop, *Basic Math of Quantum Information.* M. Reza Kahar Aziz.

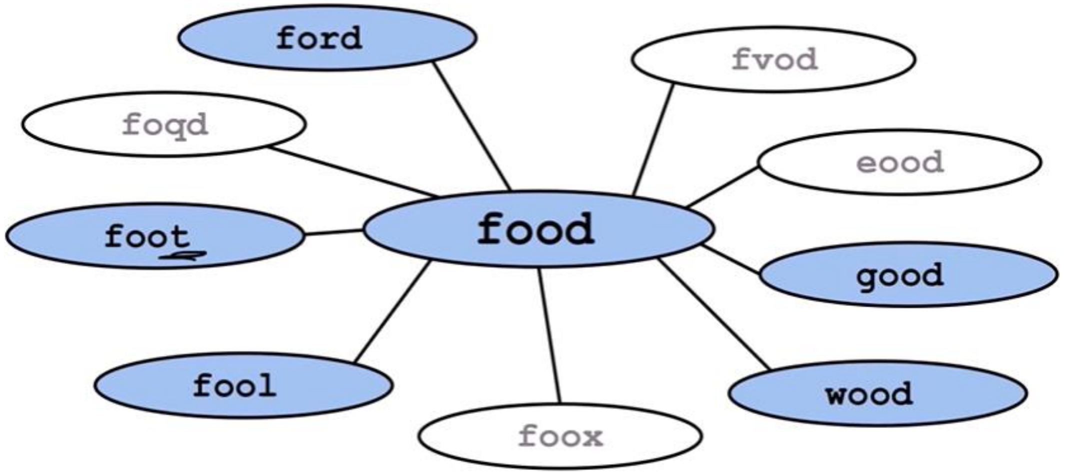
Error Correction Codes

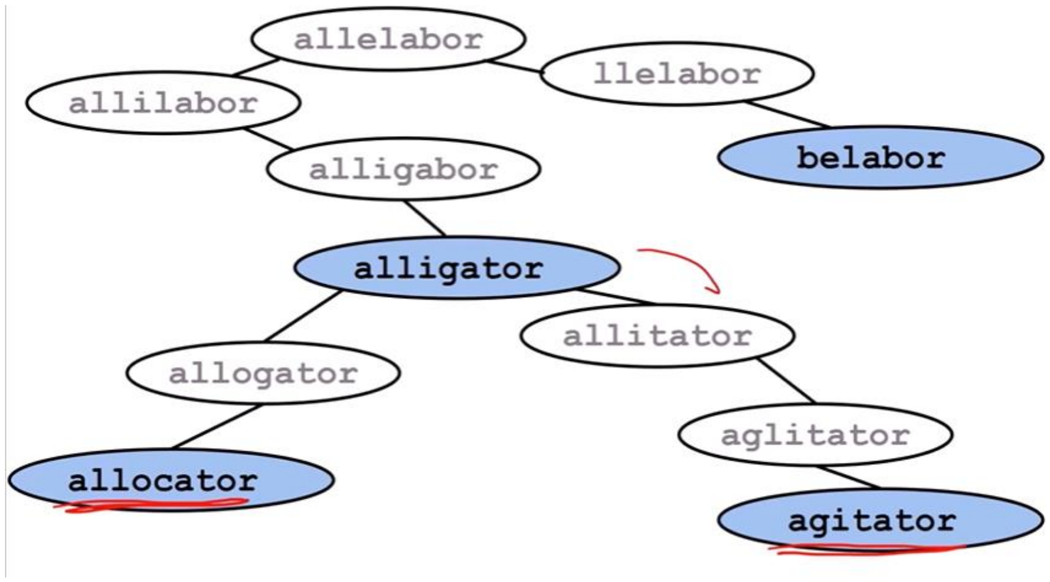
From Classic to Quantum

Valid and Invalid Codewords


ablaze [ə'bleɪz] adj [on fire] en llamas.
able ['eɪbl] adj **1.** [capable] ▸ **to be able to do sthg** poder hacer algo ▸ **to feel able to do sthg** sentirse capaz de hacer algo **2.** [skilful] capaz, competente.
ably ['eɪblɪ] adv competentemente.
abnormal [æb'nɔːml] adj anormal.
aboard [ə'bɔːd] ◆ adv a bordo. ◆ prep [ship, plane] a bordo de ; [bus, train] en.
abode [ə'bəʊd] n *fml* ▸ **of no fixed abode** sin domicilio fijo.
abolish [ə'bɒlɪʃ] vt abolir.
abolition [,æbə'lɪʃn] n abolición *f*.
abominable [ə'bɒmɪnəbl] adj abominable, deplorable.
aborigine [,æbə'rɪdʒənɪ] n aborigen *mf* de Australia.







“Best 2 out of 3” Repetition Code

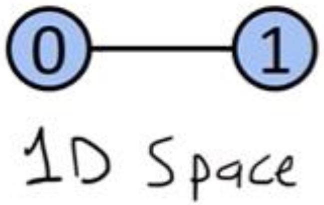
Original Message:

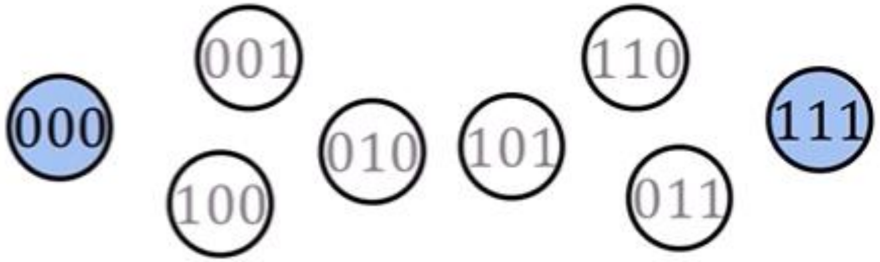
00101

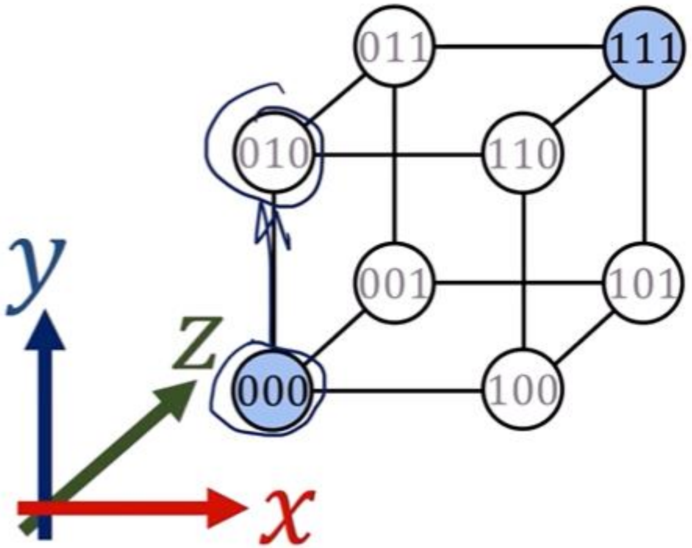
$0 \rightarrow 000$
$1 \rightarrow 111$

Repetition Code:

000 000 111 000 111







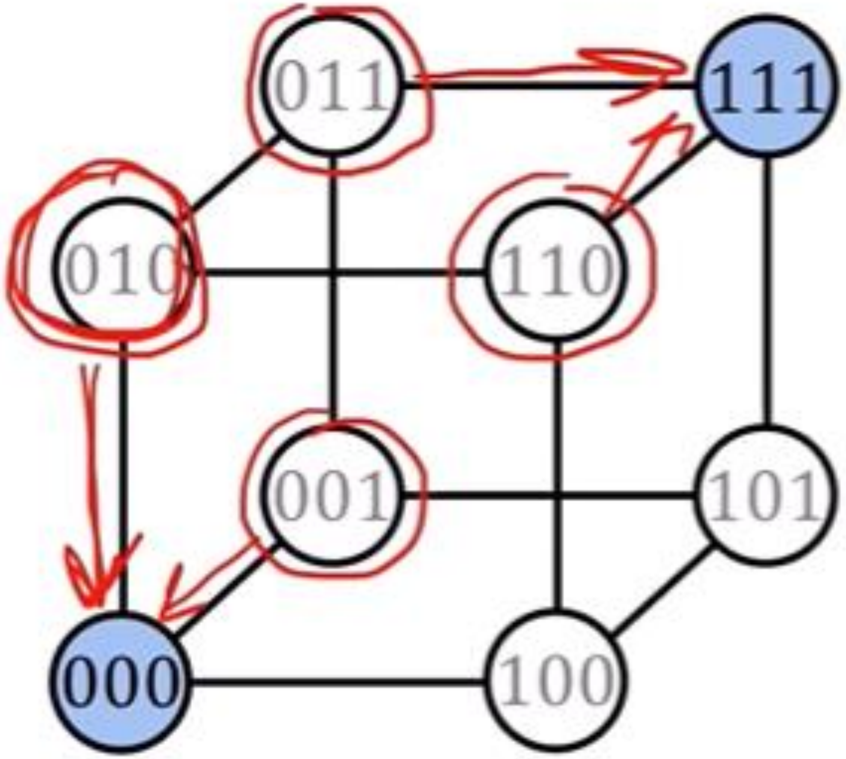
xyz

"Best 2 out of 3" Repetition Code

00101

$0 \rightarrow 000$
$1 \rightarrow 111$

000 000 111 000 111



010 001 110 010 011

000 000 111 000 111

00101

“Best 2 out of 3” Repetition Code

Original Message:

00101

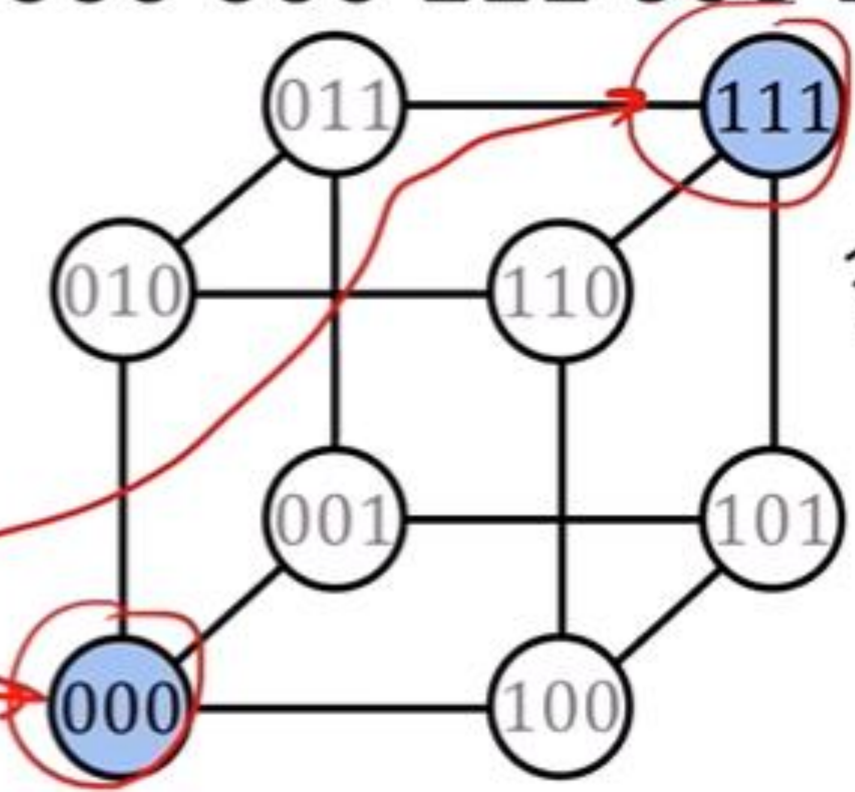
1D

Generator Matrix

$$[1\ 1\ 1]$$

Repetition Code:

000 000 111 000 111



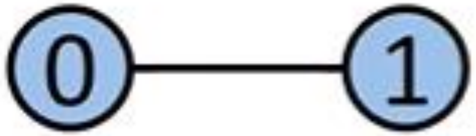
3D

“Best 2 out of 3” Repetition Code

Original Message:

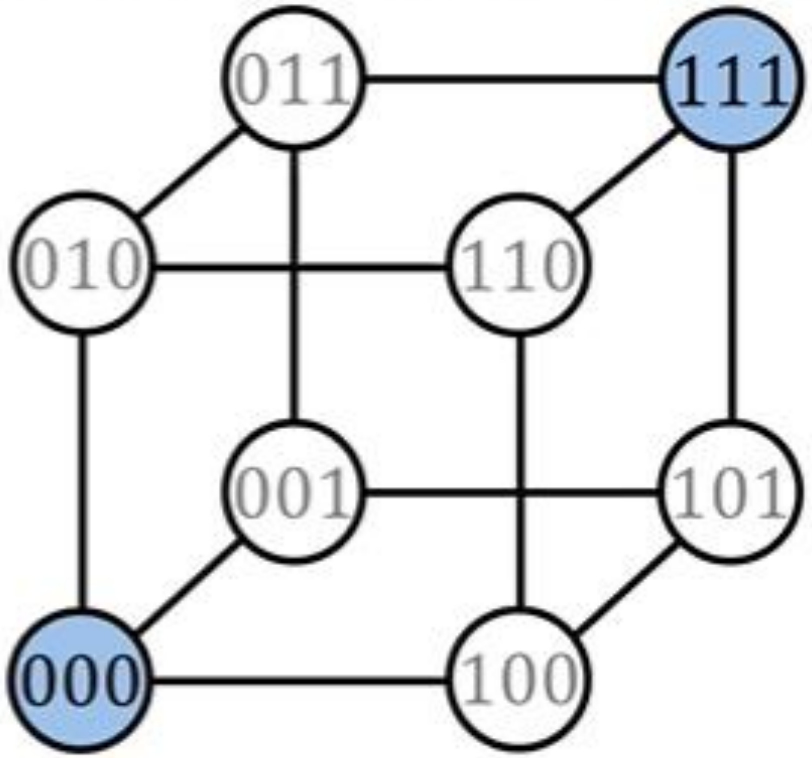
00101

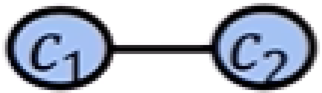
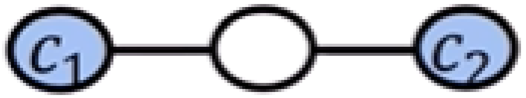
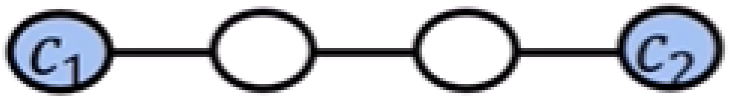
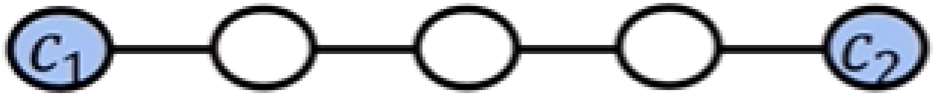
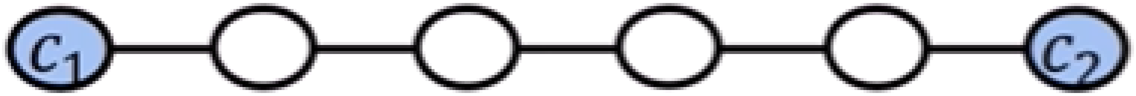
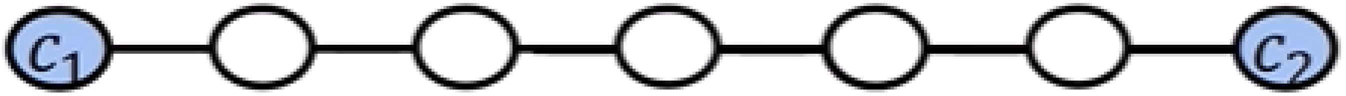
$$\underline{0}[111] \to [000]$$
$$\underline{1}[111] \to [111]$$



Repetition Code:

000 000 111 000 111



Distance $\boldsymbol{d}$	Visualization	# errors detected	# errors corrected
1		0	0
2		1	0
3		2	1
4		3	1
5		4	2
6		5	2
$\boldsymbol{d}$		$d-1$	$\left\lfloor \frac{d-1}{2} \right\rfloor$

Minimum Distance d

- Smallest distance between any two valid codewords

Recall for Linear Codes:

- Sum of any two valid codewords is another valid codeword

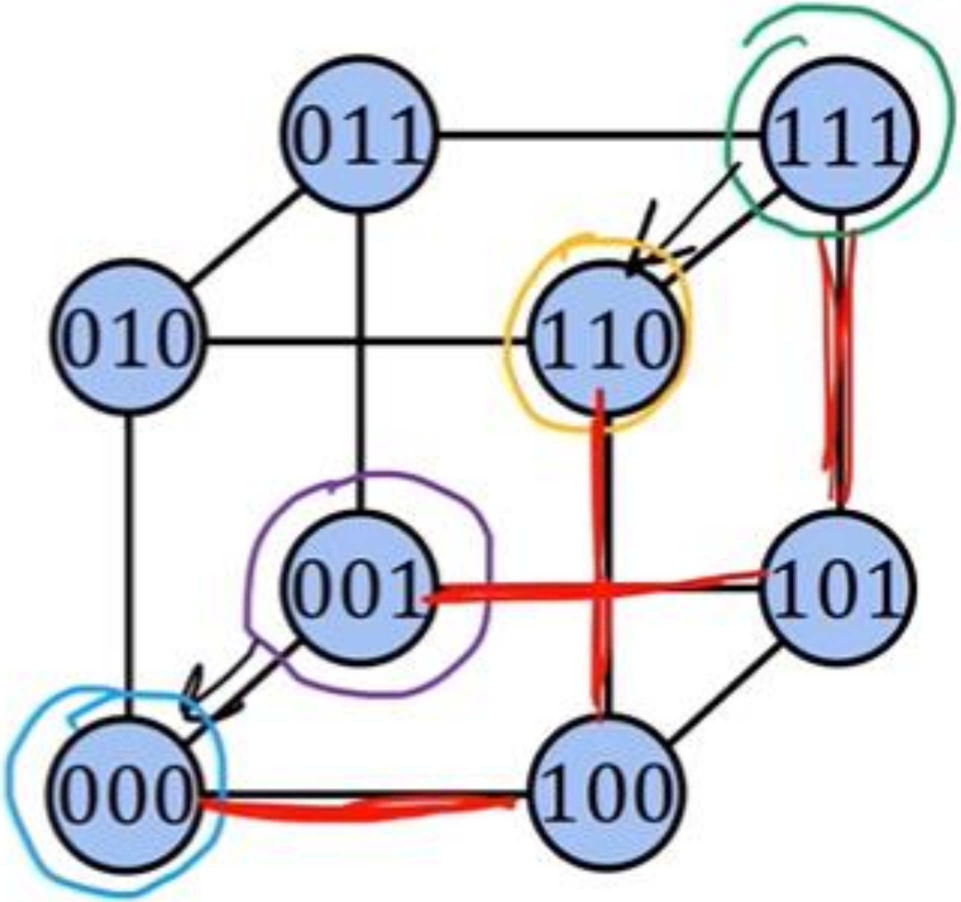
$$\min_{\overrightarrow{c_1},\overrightarrow{c_2}} D(\overrightarrow{c_1},\overrightarrow{c_2})$$

$$= \min_{\overrightarrow{c_1},\overrightarrow{c_2}} D(\overrightarrow{c_1} - \overrightarrow{c_1}, \overrightarrow{c_2} - \overrightarrow{c_1})$$

$$D(001,111) = 2$$

$$= D(001-001,111-001)$$

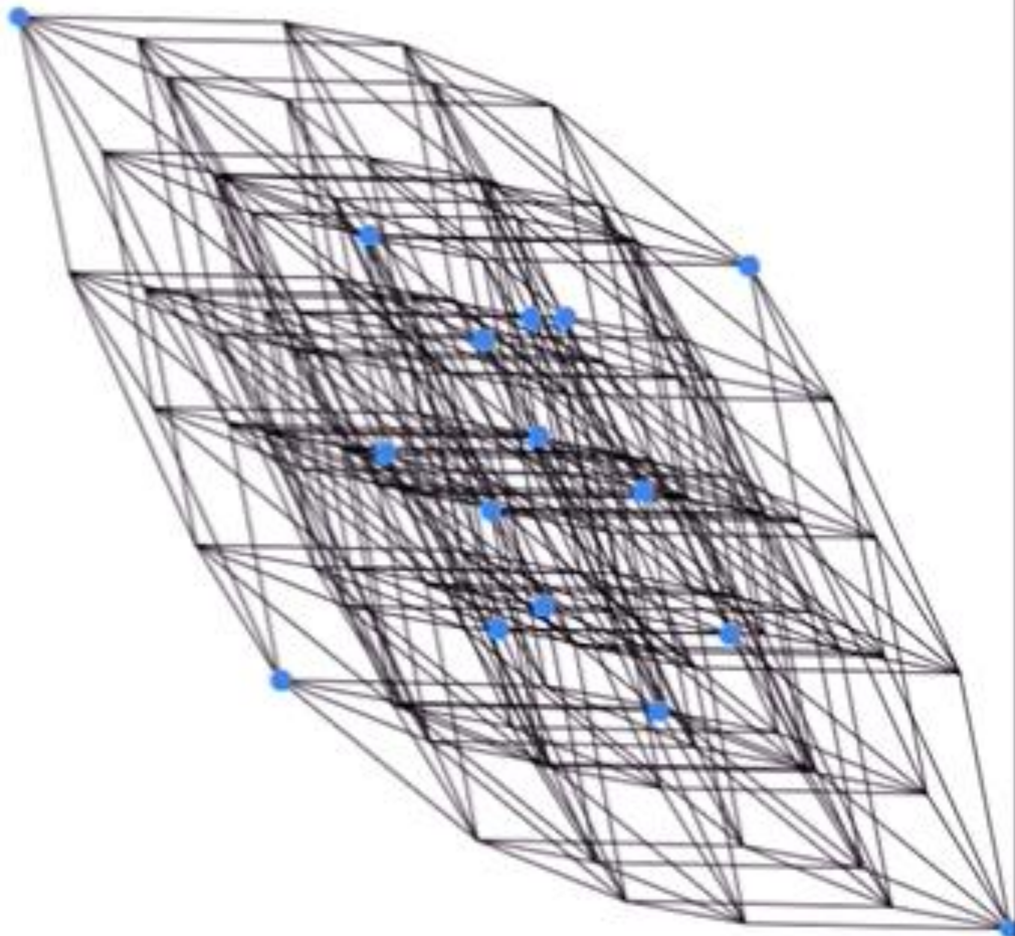
$$= D(000,110) = 2$$



Hamming (7,4) Code

Message	Codeword
0000	**0000 000**
0001	**0001 111**
0010	**0010 011**
0011	**0011 100**
0100	**0100 101**
0101	**0101 010**
0110	**0110 110**
0111	**0111 001**
1000	**1000 110**
1001	**1001 001**
1010	**1010 101**
1011	**1011 010**
1100	**1100 011**
1101	**1101 100**
1110	**1110 000**
1111	**1111 111**

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



Hamming (7,4) Code

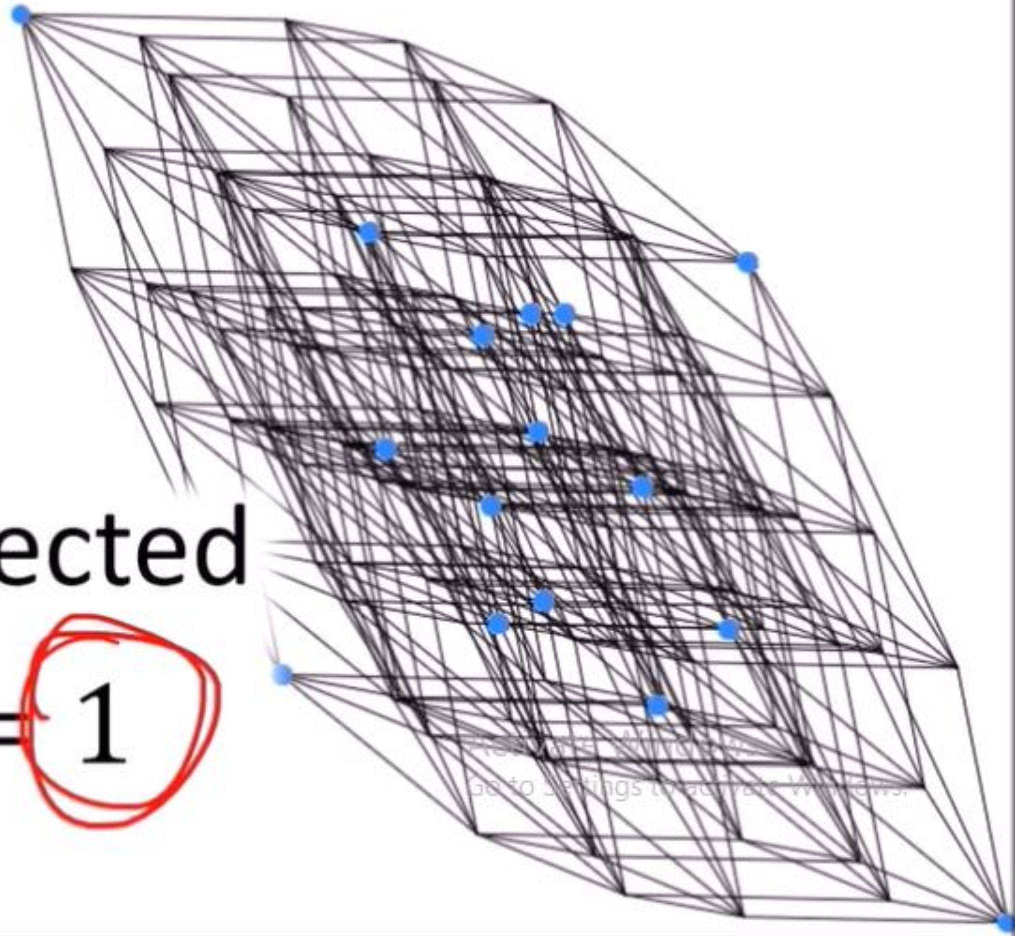
Message	Codeword
0000	**0000 000**
0001	**0001 111**
0010	**0010 011**
0011	**0011 100**
0100	**0100 101**
0101	**0101 010**
0110	**0110 110**
0111	**0111 001**
1000	**1000 110**
1001	**1001 001**
1010	**1010 101**
1011	**1011 010**
1100	**1100 011**
1101	**1101 100**
1110	**1110 000**
1111	**1111 111**

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

$$\boxed{d = 3}$$

errors corrected

$$= \left\lfloor \frac{d-1}{2} \right\rfloor = 1$$



Hamming Codes

$$Rate = \frac{k}{n}$$

$$n = 2^r - 1$$

$$k = 2^r - 1 - r$$

$$d = 3$$

1 error correction per codeword

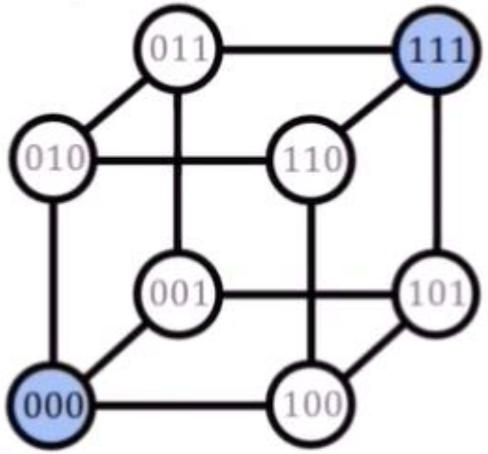
Hamming (7,4)	$Rate = \frac{4}{7} = 57.1\%$
Hamming (15,11)	$Rate = \frac{11}{15} = 73.3\%$
Hamming (31,26)	$Rate = \frac{26}{31} = 83.9\%$

Linear Codes

1. Generator Matrix $\boldsymbol{G}$
2. Minimum Distance $\boldsymbol{d}$
3. Parity-Check Matrix $\boldsymbol{H}$

$Hc^T = \vec{0}$ Valid codeword only

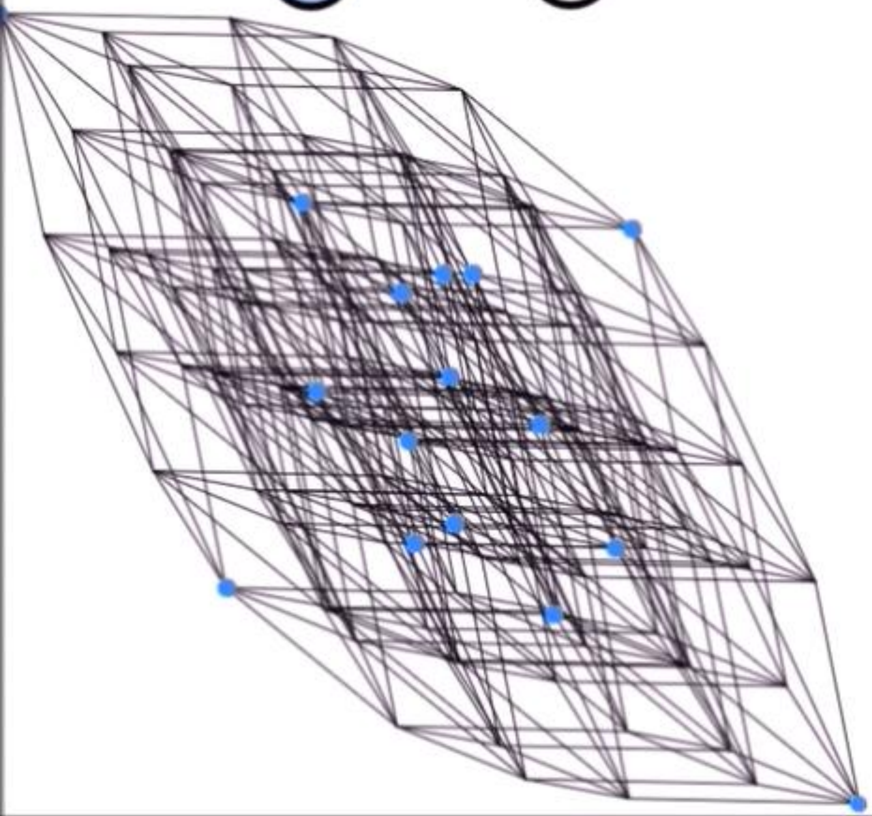
Parity-Check Matrix



$xyz \leftarrow$ 2 of 3

$x = y$

$x = z$



H(7,4)

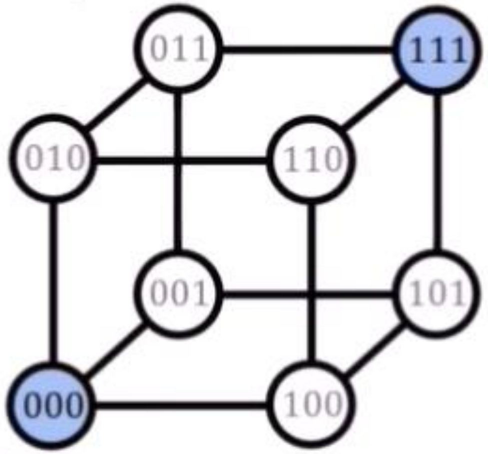
$abcd\ xyz$

$a \oplus b \oplus d = x$

$a \oplus c \oplus d = y$

$b \oplus c \oplus d = z$

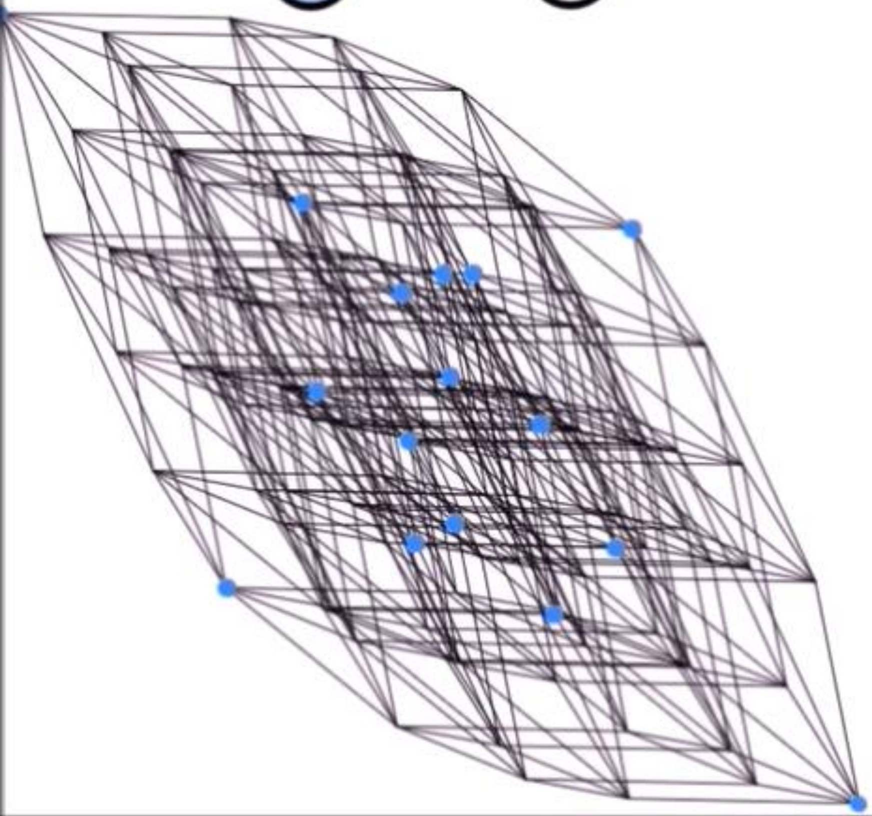
Parity-Check Matrix



$$xyz$$

$$x - y = 0$$

$$x - z = 0$$



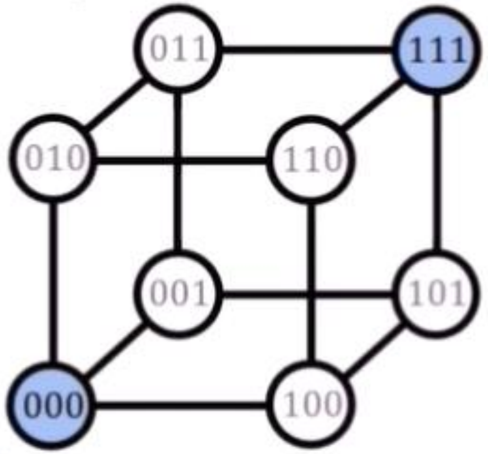
$$abcd \quad xyz$$

$$a \oplus b \oplus d - x = 0$$

$$a \oplus c \oplus d - y = 0$$

$$b \oplus c \oplus d - z = 0$$

Parity-Check Matrix

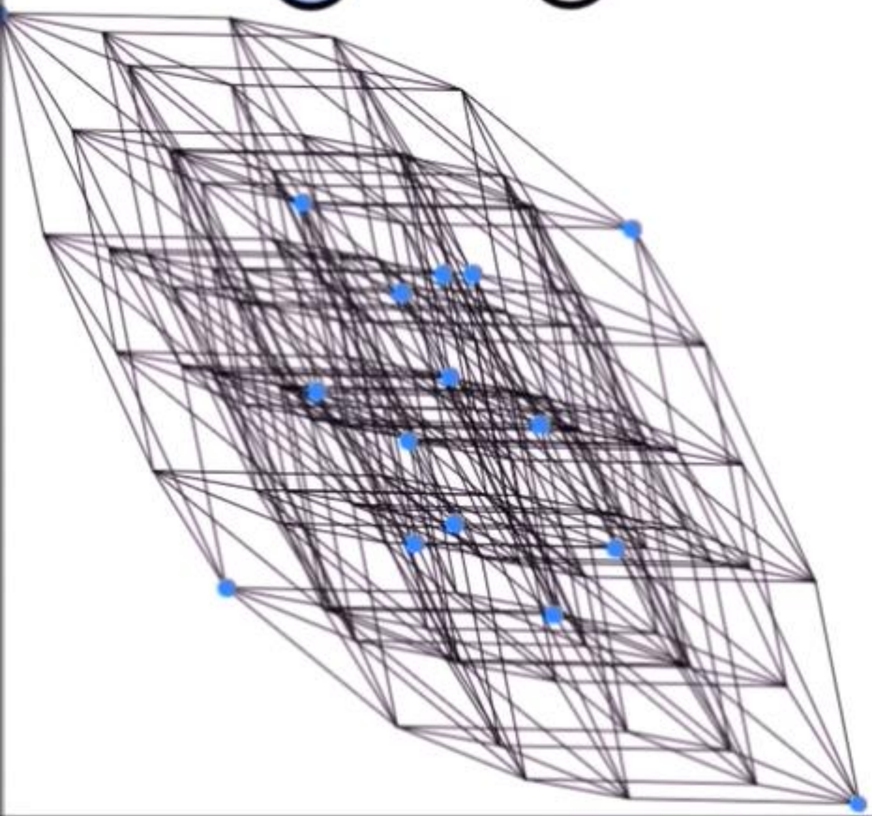


xyz

$x \oplus y = 0$

$x \oplus z = 0$

Linear Equations



$abcd \quad xyz$

$a \oplus b \oplus d \oplus x = 0$

$a \oplus c \oplus d \oplus y = 0$

$b \oplus c \oplus d \oplus z = 0$

$$x \oplus y \qquad\quad = 0$$

$$x \qquad\quad \oplus z = 0$$

$$\begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

Codeword: 1101100

$$H \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \overset{c^T}{\begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$$H\vec{c}^{\,T} = \vec{0}$$

$$H(\vec{c} + \vec{e})^T = \overset{0}{\cancel{H\vec{c}^{\,T}}} + H\vec{e}^{\,T} = \underline{\underline{H\vec{e}^{\,T}}}$$

Syndrome

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \left(\begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \right) = \left(\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} + \boxed{\begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}} \right)$$

$$H\vec{q}^T = \vec{0}$$

$$H(\vec{q}+\vec{e})^T = H\vec{q}^T + H\vec{e}^T = \underline{H\vec{e}^T}$$

Same syndrome

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \left(\begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \right) = \left(\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} + \boxed{\begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}} \right)$$

$$H\vec{q}^T = \vec{0}$$

$$H(\vec{q}+\vec{e})^T = H\vec{q}^T + H\vec{e}^T = \underline{H\vec{e}^T}$$

Same syndrome

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \left(\begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \right) = \left(\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} + \boxed{\begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}} \right)$$

2nd column

2nd bit

$$H\vec{c}^T = \vec{0}$$

$$H(\vec{c} + \overrightarrow{e_1} + \overrightarrow{e_2})^T = \underbrace{H\overrightarrow{e_1}^T} + \underbrace{H\overrightarrow{e_2}^T}$$

$$\begin{bmatrix} \boxed{\begin{matrix}1\\1\\0\end{matrix}} & \begin{matrix}1\\0\\1\end{matrix} & \begin{matrix}0\\1\\1\end{matrix} & \begin{matrix}1\\1\\1\end{matrix} & \boxed{\begin{matrix}1 & 0\\0 & 1\\0 & 0\end{matrix}} & \begin{matrix}0\\0\\1\end{matrix} \end{bmatrix} \left(\begin{bmatrix}1\\1\\0\\1\\1\\0\\0\end{bmatrix} + \begin{bmatrix}0\\0\\0\\0\\1\\0\\0\end{bmatrix} + \begin{bmatrix}0\\0\\0\\0\\0\\1\\0\end{bmatrix} \right) = \boxed{\begin{bmatrix}1\\1\\0\end{bmatrix}}$$

1st bit?

General Hamming Codes

- A code whose Parity-Check matrix H has columns with every possible combination of 0s and 1s (except all 0s)
- The parity-check matrix will have $2^r - 1$ columns
- r of these columns are for parity bits

(31, 26) code

$\leftarrow$ parity

$$\begin{array}{c}
\begin{matrix} x & y & & z & & & & w & & & & & & & & u & & & & & & & & & & & & & & & \end{matrix} \\
\begin{bmatrix}
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{bmatrix}
\end{array}$$

$$\begin{array}{ccccccccccccccc} & & a & & b & c & d & & e & f & g & h & i & j & k \end{array}$$

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

$$\begin{array}{ccccccccccccccc} x & y & & z & & & & w & & & & & & & \end{array}$$

$$a \oplus b \oplus d \oplus e \oplus g \oplus i \oplus k = x$$

$$a \oplus c \oplus d \oplus f \oplus g \oplus j \oplus k = y$$

$$b \oplus c \oplus d \oplus h \oplus i \oplus j \oplus k = z$$

$$e \oplus f \oplus g \oplus h \oplus i \oplus j \oplus k = w$$

$$
\begin{array}{c}
\begin{array}{ccccccccccccccc} & & a & & b & c & d & & e & f & g & h & i & j & k \end{array} \\
\begin{bmatrix}
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{bmatrix} \\
\begin{array}{ccccccccccccccc} x & y & & z & & & & w & & & & & & & \end{array}
\end{array}
$$

Syndrome for error in "c" bit

$$\left.\begin{array}{l} n = \text{codeword length} \\ k = \text{message length} \\ d = \text{minimum distance} \end{array}\right\} (n, k, d) \text{ code}$$

Hamming Codes

(r parity bits)

$$n = 2^r - 1$$

$$k = 2^r - 1 - r$$

$$d = 3$$

n = codeword length
k = message length
d = minimum distance

$\left.\begin{matrix} \\ \\ \\ \end{matrix}\right\}$ (n, k, d) code

$(\underbrace{n = 2^r - 1}, \underbrace{k = 2^r - 1 - r}, \underbrace{d = 3})$ code

Hamming Codes

$$Rate = \frac{k}{n}$$

$$n = 2^r - 1$$

$$k = 2^r - 1 - r$$

$$d = 3$$

1 error correction per codeword

Hamming (7,4)	$Rate = \frac{4}{7} = 57.1\%$
Hamming (15,11)	$Rate = \frac{11}{15} = 73.3\%$
Hamming (31,26)	$Rate = \frac{26}{31} = 83.9\%$

Aturan Penamaan Quantum Error Codes

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

Total qubit/blocklength

Quantum information

Distance
$d = 2t + 1$

- Quantum error correction digunakan di qauntum untuk untuk melindungi quantum informasi dari error yang diakibatkan karena dekoherensi dan quantum noise.
- Pada Quantum error correction terdapat **Stabilizer** yang merupakan qubit ancilla tambahan pada qubit informasi yang ingin diproteksi. Stabilizer dapat di definisikan $S = 2^{(n-k)}$.
- Quantum error correction memiliki **syndrome** yang digunakan untuk mendiagnosa qubit pada quantum yang terkena error pada encoded state.

General Quantum Error Corrections Step

1. Quantum Hamming Bound :

$$2^{n-k} \sum_{j=0}^{t} \binom{n}{j} 3^{j}$$

2. Quantum Singleton Bound :

$$n \geq 4t + k$$

3. Parity Check Matrix :

$$\boldsymbol{H} = [\boldsymbol{H}_X \mid \boldsymbol{H}_Z]$$

4. Simplectic Inner Product (SIP) :

$$\boldsymbol{H}_X \boldsymbol{H}_Z^T + \boldsymbol{H}_Z \boldsymbol{H}_X^T \ mod\ 2 = \ \boldsymbol{0_5}$$

5. Reduce-row Echelon Form (RREF) :

$$\mathbf{H}' = [\mathbf{H}'_X | \mathbf{H}'_Z]$$

6. Identifikasi Xbar dan Zbar :

$$\bar{X} = [0\ E^T I\ |(C^T C_1 + C_Z^T)0\ 0]$$

$$\bar{Z} = [0\ 0\ 0\ |A_2^T\ 0\ I]$$

7. Syndrome Extraction :

$$\mathbf{S_n} = \langle \psi_\mathbf{r} | \mathbf{g_n} | \psi_\mathbf{r} \rangle$$

- Untuk bisa mendeteksi dan mengkoreksi quantum error correction harus memenuhi quantum Hamming bound dan quantum Singleton bound.
- Syarat selanjutnya adalah SIP mod 2 harus bernilai 0.
- Dan proses RREF harus bernilai integer.

[[3,1,1]] Quantum Repetition Codes (1/5)

$g_1 = ZZI$

$g_2 = ZIZ$

$H = [H_x | H_z]$

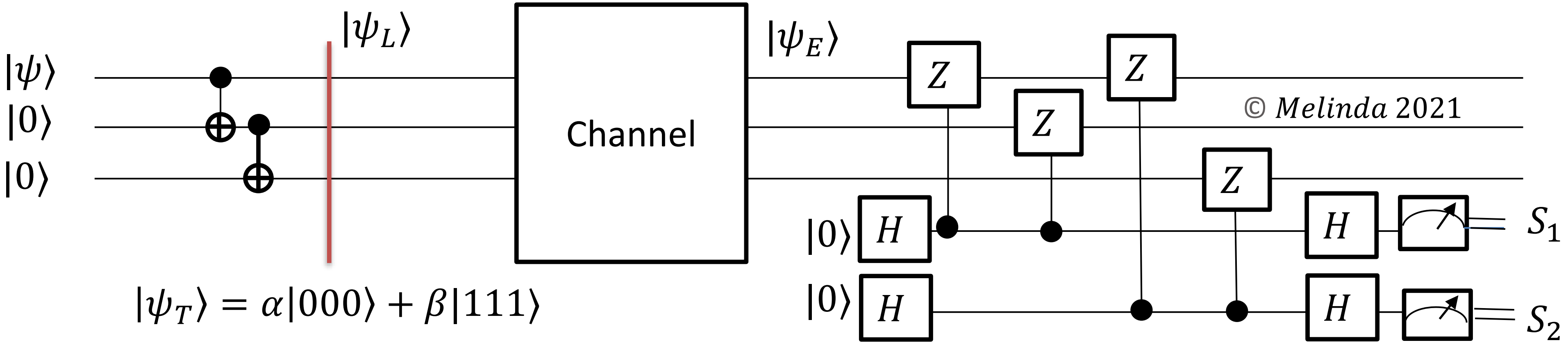
$H_x H_{z^T} + H_z H_{x^T} = 0_4 \; mod \; 2 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

$|0\rangle_L = |000\rangle$ $\qquad$ $|1\rangle_L = |111\rangle$

$$H = \left[\begin{array}{ccc|ccc} 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{array}\right]$$

$$H = \left[\begin{array}{cc|c|cc|c} 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{array}\right]$$

A_2 $\quad B \quad$ C_2

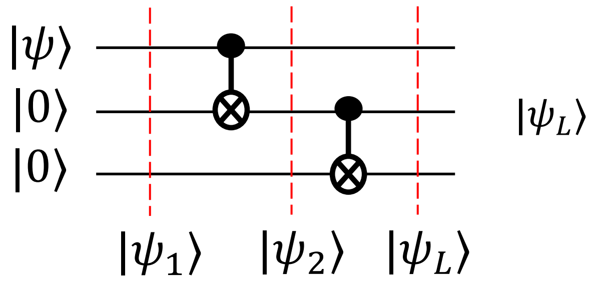


$|\psi_T\rangle = \alpha|000\rangle + \beta|111\rangle$

Tx $\qquad\qquad$ Rx

[[3,1,1]] Quantum Repetition Codes (2/5)

Transmitter



$$|0\rangle = \begin{bmatrix}1\\0\end{bmatrix} \qquad |1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$$

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}1\\0\\0\\0\end{bmatrix}$$

$$|\psi\rangle = |0\rangle + |1\rangle = \begin{bmatrix}1\\1\end{bmatrix}$$

$$|\psi_1\rangle = |\psi\rangle \otimes |00\rangle = \begin{bmatrix}1\\1\end{bmatrix} \otimes \begin{bmatrix}1\\0\\0\\0\end{bmatrix} = \begin{bmatrix}1\\0\\0\\0\\1\\0\\0\\0\end{bmatrix}$$

$$CNOTI = CNOT \otimes I = \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix} \otimes \begin{bmatrix}1&0\\0&1\end{bmatrix} = \begin{bmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&1\\0&0&0&0&1&0&0&0\\0&0&0&0&0&1&0&0\end{bmatrix}$$

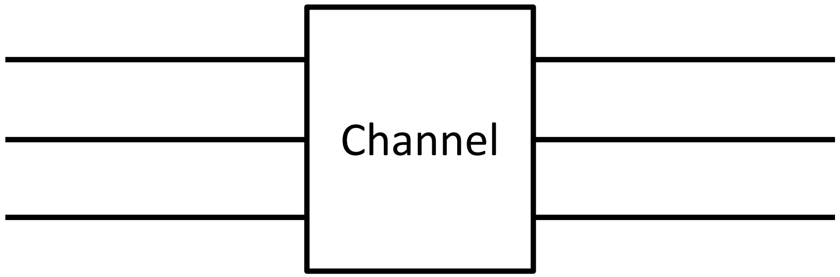
$$ICNOT = I \otimes CNOT = \begin{bmatrix}1&0\\0&1\end{bmatrix} \otimes \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix} = \begin{bmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&1&0&0\\0&0&0&0&0&0&0&1\\0&0&0&0&0&0&1&0\end{bmatrix}$$

$$|\psi_2\rangle = CNOTI * |\psi_1\rangle = \begin{bmatrix}1\\0\\0\\0\\0\\0\\1\\0\end{bmatrix}$$

$$|\psi_L\rangle = ICNOT * |\psi_2\rangle = \begin{bmatrix}1\\0\\0\\0\\0\\0\\0\\1\end{bmatrix}$$

[[3,1,1]] Quantum Repetition Codes (3/5)

Pada channel terjadi bit flip error $(Pauli - X)$ yang terjadi pada qubit pertama.



$|\psi_E\rangle$

$$II = I \otimes I$$

$$II = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$II = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$XI = \mathrm{X} \otimes I$$

$$XI = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$XI = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

*Error terjadi pada qubit pertama

$$XII = \mathrm{XI} \otimes I$$

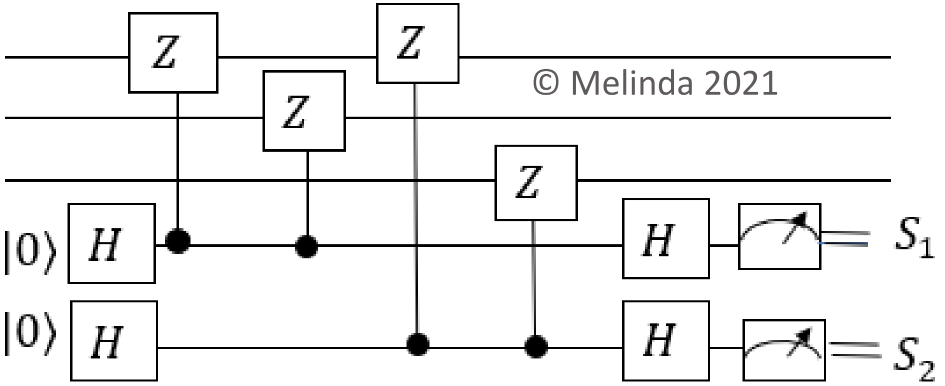
$$XII = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$XII = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

[[3,1,1]] Quantum Repetition Codes (4/5)

$|\psi_E\rangle = \mathrm{XII} \times |\psi_L\rangle$

$$|\psi_E\rangle = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix} \times \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$



Stabilizer :

$g_1 = ZZI$

$g_2 = ZIZ$

$$ZZ = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$|\psi_E\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Syndrome :

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

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$ZI = \mathrm{Z} \otimes \mathrm{I}$

$$ZI = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$ZI = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

$$ZZ = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$ZZI = ZZ \otimes I$

$$ZZI = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

[[3,1,1]] Quantum Repetition Codes (5/5)

$$ZZI = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$ZI = Z \otimes I$$

$$ZI = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$ZI = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

$$ZIZ = ZI \otimes I \qquad ZIZ = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$ZIZ = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Stabilizer menghasilkan Syndrome $S_1(ZZI)\ dan\ S_2(ZIZ)$

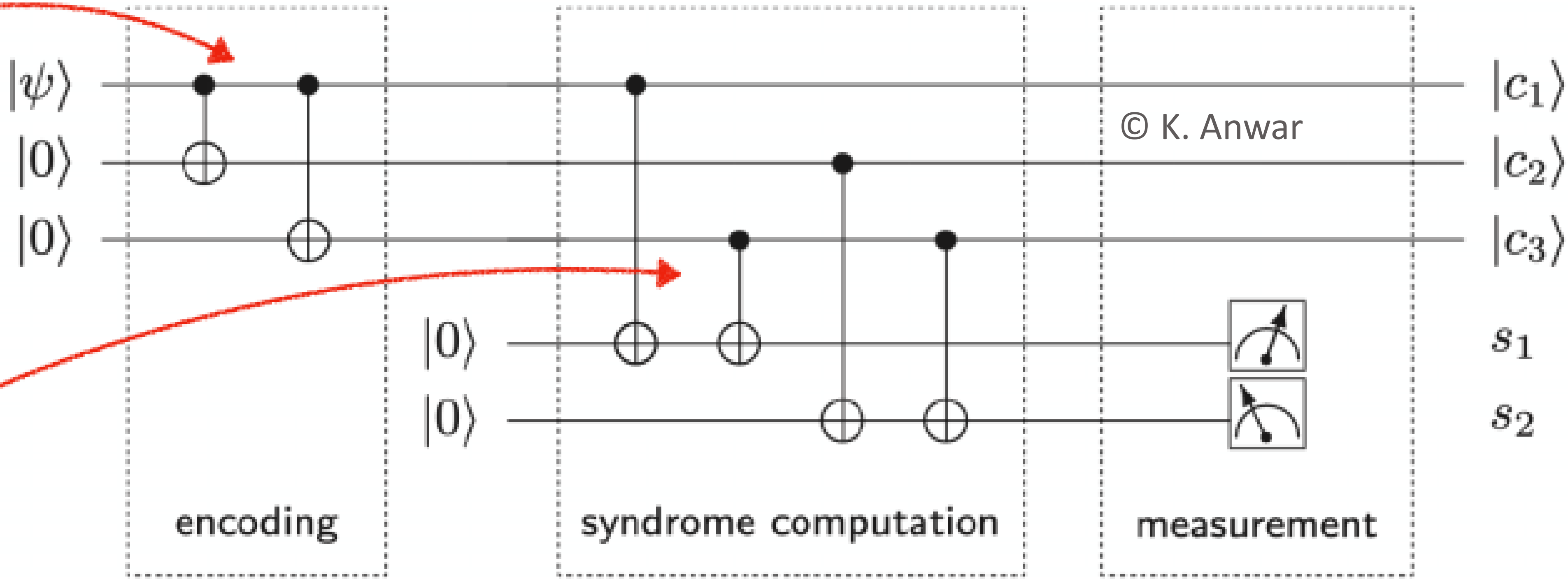
$$S_1 = \langle \psi_E | ZZI | \psi_E \rangle$$

$$S_2 = \langle \psi_E | ZIZ | \psi_E \rangle$$

Error	Syndrome [S1 S2]
XII	[1 1]
IXI	[1 0]
IIX	[0 1]

Simple Quantum Error Correction Coding

$$\mathbf{G} = [1 \quad 1 \quad 1]$$



$$\mathbf{H} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

Error $X \otimes I \otimes I$ gives syndrome $s_1 s_2 = 10$

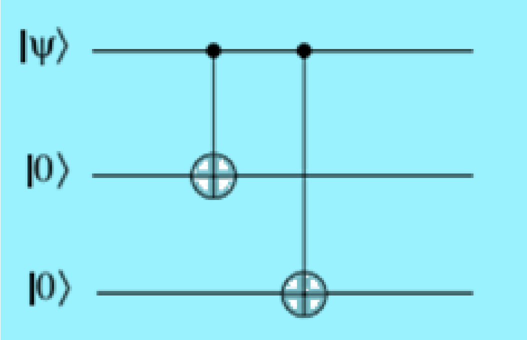
Error $I \otimes X \otimes I$ gives syndrome $s_1 s_2 = 01$

Error $I \otimes I \otimes X$ gives syndrome $s_1 s_2 = 11$

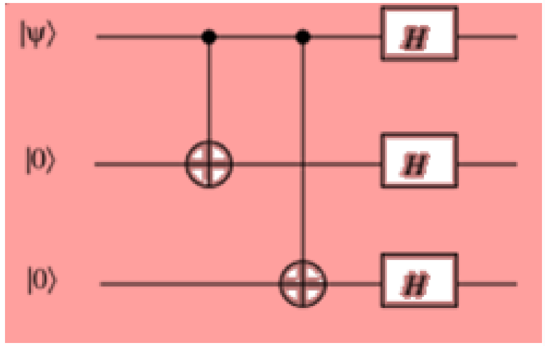
Philosophy of Stabilizer

- The state $|\psi\rangle$ is said to be stabilized by operator X_1X_2 if $X_1X_2|\psi\rangle = |\psi\rangle$.
- The state $|\psi\rangle$ is said to be stabilized by operator Z_1Z_2 if $Z_1Z_2|\psi\rangle = |\psi\rangle$.
- Many quantum codes (including CSS codes and the Shor code) can be much more compactly described using stabilizers than in the state vector description.
- For $n = 3$, we have stabilizer $S = \{III, Z_1Z_2, Z_2Z_3, Z_1Z_3\}$.
- Operator Z_1Z_2 stabilizes states $|000\rangle, |001\rangle, |110\rangle, |111\rangle$.
- Operator Z_2Z_3 stabilizes states $|000\rangle, |100\rangle, |011\rangle, |111\rangle$.
- Logical operator are the common states $|000\rangle$ and $|111\rangle$.

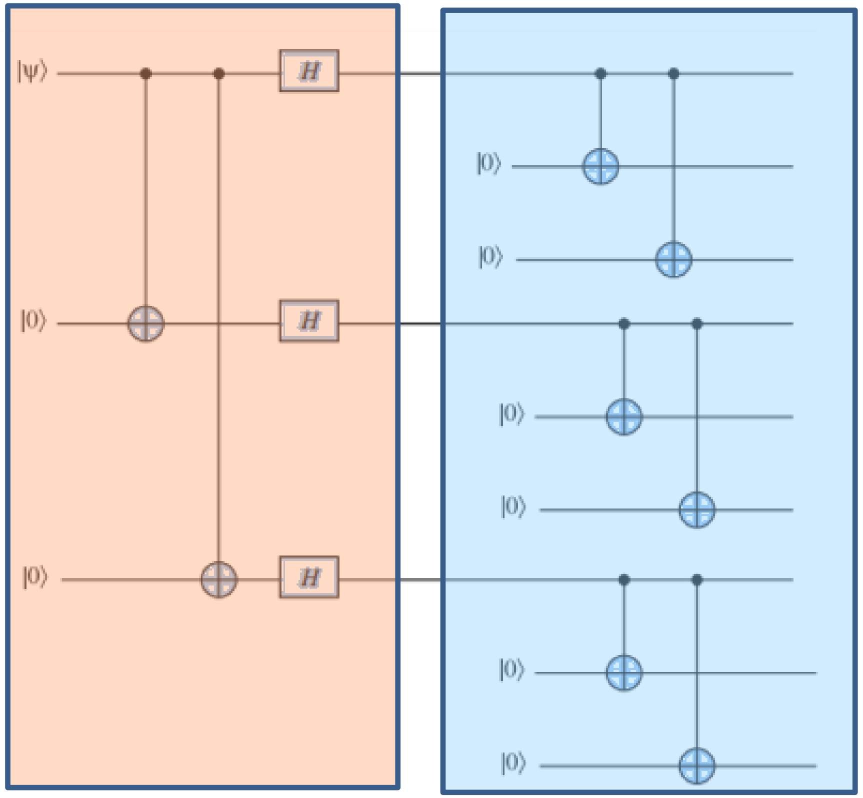
Qubit Shor Codes: Circuit



Three bit flip Codes



Three phase flip Codes



Nine Shor Codes

- The code is a combination of the three qubit phase flip and bit flip codes. We first encode the qubit using the phase flip code
  $|0\rangle \longrightarrow |+++\rangle$
  $|1\rangle \longrightarrow |---\rangle$
- Next, encode each of these qubits using the three qubit bit flip code
  $|+\rangle$ becomes $\frac{|000+111\rangle}{\sqrt{2}}$
  $|-\rangle$ becomes $\frac{|000-111\rangle}{\sqrt{2}}$

Qubit Shor Codes: Stabilizer and Syndrome

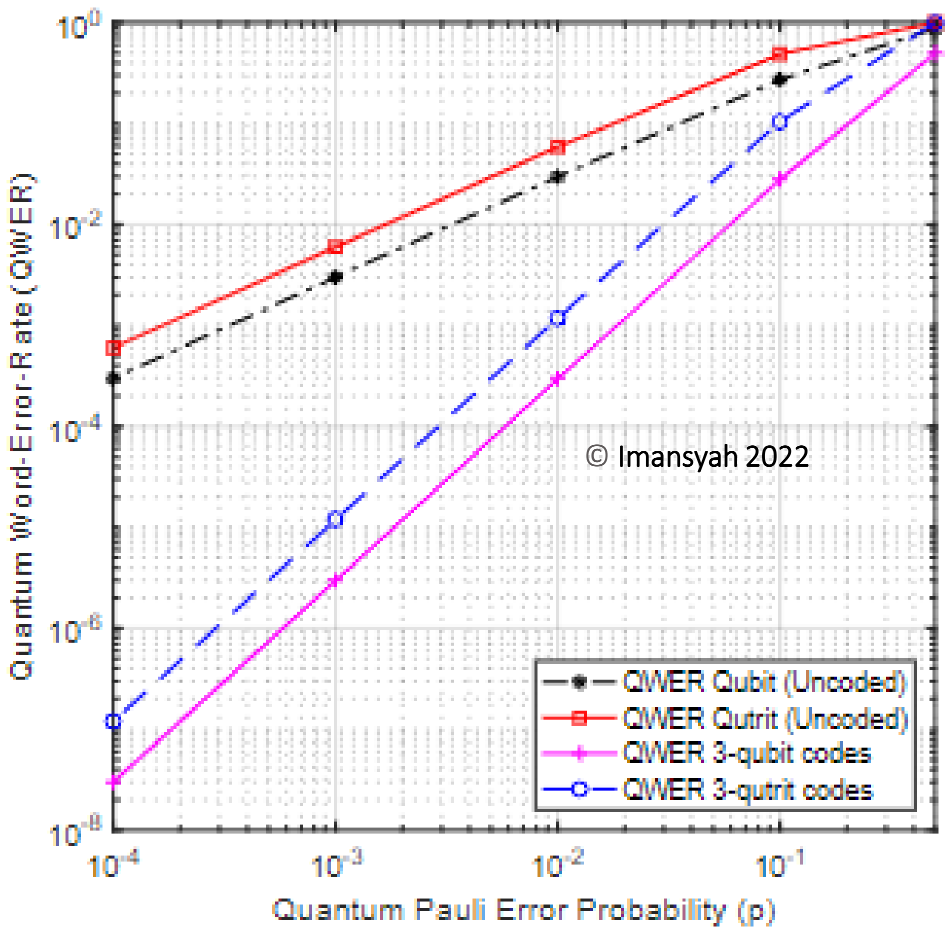
Z_1Z_2	Z_2Z_3	Error type	Action
+1	+1	no error	no action
+1	−1	bit 3 flipped	flip bit 3
−1	+1	bit 1 flipped	flip bit 1
−1	−1	bit 2 flipped	flip bit 2

Name	Operator
g_1	$Z\,Z\,I\,I\,I\,I\,I\,I\,I$
g_2	$I\,Z\,Z\,I\,I\,I\,I\,I\,I$
g_3	$I\,I\,I\,Z\,Z\,I\,I\,I\,I$
g_4	$I\,I\,I\,I\,Z\,Z\,I\,I\,I$
g_5	$I\,I\,I\,I\,I\,I\,Z\,Z\,I$
g_6	$I\,I\,I\,I\,I\,I\,I\,Z\,Z$
g_7	$X\,X\,X\,X\,X\,X\,I\,I\,I$
g_8	$I\,I\,I\,X\,X\,X\,X\,X\,X$
$\bar{Z}$	$X\,X\,X\,X\,X\,X\,X\,X\,X$
$\bar{X}$	$Z\,Z\,Z\,Z\,Z\,Z\,Z\,Z\,Z$

The stabilizer for the Shor code has eight generators

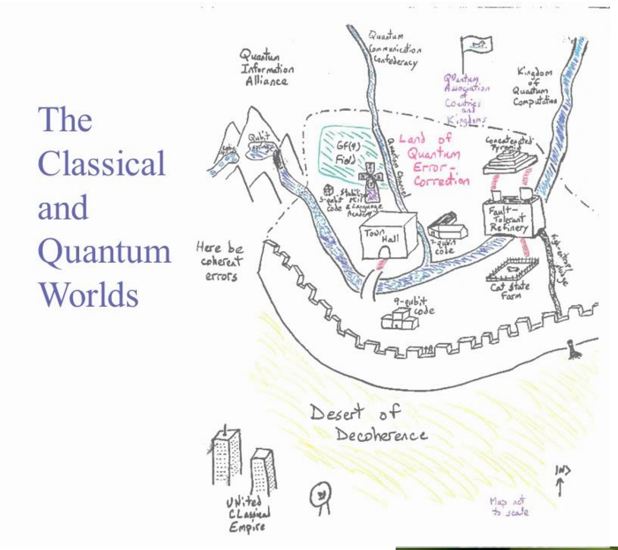
all other products of two errors from this error set are either in S or else anti-commute with at least one element of S and thus are not in $N(S)$, implying that the Shor code can be used to correct an arbitrary single qubit error.

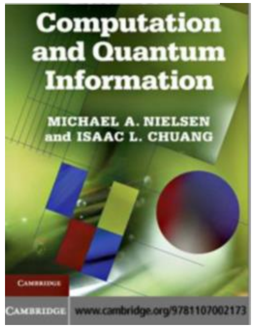
Theoretical QWER for Qubit and Qutrit



- Both the 3-qubit codes and the 3-qutrit codes can only correct single bit-flip-error.
- The stabilizer for qutrit in this paper is powerful enough to correct a bit-flip-error.
- Error correction is a must in qutrit because the performances of qutrit codes will be worse if the error correction is not applied.

Stabilizer Codes





10.5 Stabilizer codes

We cannot clone, perforce; instead, we split
Coherence to protect it from that wrong
That would destroy our valued quantum bit
And make our computation take too long.

Correct a flip and phase – that will suffice.
If in our code another error's bred,
We simply measure it, then God plays dice,
Collapsing it to X or Y or zed.

We start with noisy seven, nine, or five
And end with perfect one. To better spot
Those flaws we must avoid, we first must strive
To find which ones commute and which do not.

With group and eigenstate, we've learned to fix
Your quantum errors with our quantum tricks.
– 'Quantum Error Correction Sonnet', by Daniel Gottesman