INTRODUCTION

DATE : 03-09-20

CONTEXT & GLOBAL PERSPECTIVES → **QUANTUM COMPUTATION** & QUANTUM INFORMATION IS THE STUDY OF THE **INFORMATION PROCESSING** TASKS THAT CAN BE ACCOMPLISHED USING **QUANTUM MECHANICAL SYSTEMS.**

WE NEED TO CONSIDER 4 PERSPECTIVES:

1. PHYSICIST
2. COMP. SCIENTIST
3. INFO. THEORIST
4. CRYPTOGRAPHER

PHYSICIST PERSPECTIVE → QUANTUM INFORMATION AROSE FROM THE NEED TO UNDERSTAND **COMPLEX PARADOXES** IN **QUANTUM MECHANICS**.

- **NO-CLONING THEOREM** & LOCALITY.
- CONTROL OVER SINGLE QUANTUM SYSTEMS.

QUANTUM C&I PROVIDE PHYSICIST THE OPPORTUNITY TO PROBE NATURE'S HYPER-MICROSCOPIC REGIMES WITHIN A MORE INTUITIVE REALM OF QUANTUM MECHANICS.

THE NEED OF POWERFULL QUANTUM MECHANICAL SYSTEMS FOR INFORMATION PROCESSING IS A QUITE INTERESTING CHALLENGE FOR PHYSICISTS & ENGINEERS.

COMP. SCIENTIST PERSPECTIVE → LIMITATIONS OF THE **VON NEUMANN ARCHITECTURE** & THE **STRONG CHURCH TURING THESIS** ARE POSED BY Q. COMPUTING.

LIMITATIONS ON THE **SIZE OF TRANSISTORS** ARE A HUGE CHALLENGE TO THE TRADITIONAL IMPLEMENTATION OF TURING'S MODEL OF COMPUTATION.

QUANTUM COMPUTING MODEL FROM DEUTSCH MIGHT BE **MORE EFFICIENT** THAN ANY OTHER MODEL PROPOSED ACCORDING TO TURING'S ORIGINAL IDEA OR RANDOMIZED CLASSICAL ALGORITHMS.

THE NOTION THAT INFORMATION IS STORED IN ACTUAL PHISICAL SYSTEMS IS FUNDAMENTAL TO COMPUTER SCIENCE.

INFORMATION THEORIST PERSPECTIVE → A WELL STABLISHED THEORY OF **QUANTUM ERROR CORRECTION** IS WELL ESTABLISHED & **NETWORKED INFORMATION** THEORY IN QUANTUM INFO. IS PROMISING.

IT IS POSSIBLE FOR A QUANTUM COMMUNICATION CHANEL TO TRANSMIT 2 BITS OF INFORMATION BY TRANSMITTING JUST 1 QBIT (**SUPER DENSE CODING**)

QUANTUM COMPUTERS REQUIRE **EXPONENTIALLY LESS** COMMUNICATION TO SOLVE SOME PROBLEMS.

CRYPTOGRAPHER PERSPECTIVE → QUANTUM ENCRYPTION MIGHT ALLOW SECURE PRIVATE KEY COMMUNICATION. ALSO, PUBLIC KEY COMMUNICATION CAN BE IN JEOPARDY.

DUE TO **ENTANGLEMENT**, TWO PEOPLE COMMUNICATING OVER A QUANTUM CHANNEL CAN DETECT SPIES !!!

SHOR'S ALGORITHMS FOR FACTORING PRIMES & DISCRETE LOGARITHM PROBLEM PUT RSA AUTENTICATION IN JEOPARDY !!!

FUNDAMENTAL CONCEPTS

DATE: 04-09-20

QUANTUM BITS → THEY ARE QUANTUM SYSTEMS THAT MAY EXIST IN 2 POSSIBLE COMPUTATIONAL STATES (I.E. TWO-LEVEL SYSTEMS).

MATHEMATICALLY, A QBIT IS A VECTOR FROM A 2D COMPLEX VECTOR SPACE:

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

SUPERPOSITION STATES ALLOW TO PERFORM CALCULATIONS ON MANY "CLASSICAL" STATES AT THE SAME TIME.

A MEASUREMENT OF THE COMPUTATIONAL STATE OF A QBIT CANNOT YIELD FULL INFORMATION ABOUT ITS QUANTUM STATE. THIS IS DUE TO MEASUREMENT PROPERTIES IN Q.M.

ALTHOUGH QBITS STORE A LOT OF INFORMATION, THE AMOUNT ACCESSIBLE BY MEASUREMENTS IS QUITE LIMITED !!!

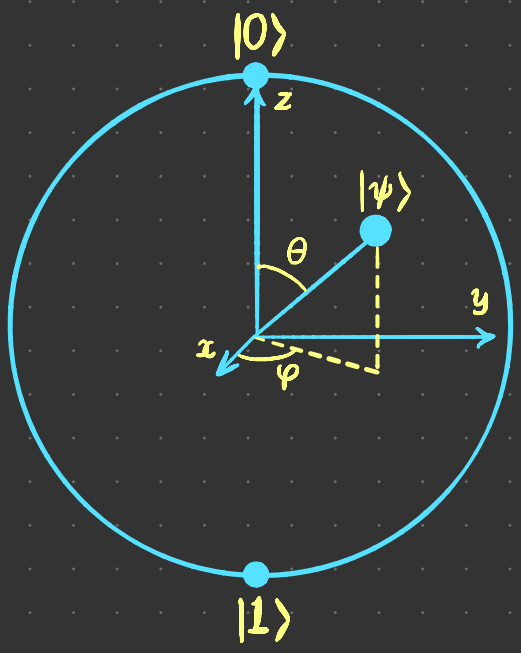
INTERFERENCE PROPERTIES OF QUANTUM STATES CAN BE USED TO DESIGN ALGORITHMS THAT REDUCE THE EFFECTS OF "DESTRUCTIVE" MEASUREMENTS.

DESIRED OUTPUTS INTERFERE CONSTRUCTIVELY. UNDESIRED OUTPUTS, DESTRUCTIVELY !!!

ALL QBIT STATES CAN BE DEFINED BY 2 PARAMETERS: θ, ϕ. THEY CAN BE WRITTEN AS:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$$

THIS LEADS TO THE NOTION OF THE **BLOCH SPHERE** REPRESENTATION OF SINGLE-QBIT STATES.



QBITS EVOLVE ACCORDING TO **UNITARY LINEAR OPERATORS** CALLED **GATES.** UNITARITY IMPLIES THAT EVOLUTION OF ISOLATED QBITS IS **REVERSIBLE.**

SYSTEMS OF N-QBITS → A SYSTEM OF INTERACTING QBITS IS REPRESENTED IN THE SPACE THAT IS A **"TENSOR" PRODUCT** OF THE INDIVIDUAL SPACES.

$$\begin{pmatrix}\text{SPACE OF}\\ N\text{-QBITS}\end{pmatrix} = \begin{pmatrix}\text{SPACE}\\ \text{QBIT 1}\end{pmatrix} \otimes \cdots \otimes \begin{pmatrix}\text{SPACE}\\ \text{QBIT } N\end{pmatrix}$$

THE STATE SPACE OF A N-QBIT SYSTEM HAS DIMENSION 2^N, SO THAT **EFFICIENCY INCREASES EXPONENTIALLY** !!!

MATHEMATICAL DESCRIPTION OF N-QBIT SYSTEMS LEADS NATURALLY TO THE NOTION OF **ENTANGLED STATES**:

$$\underbrace{|\psi^{(N)}\rangle}_{\text{ENTANGLED STATE}} \neq \underbrace{|\psi_1\rangle |\psi_2\rangle \cdots |\psi_N\rangle}_{\text{DIRECT (TENSOR) PROD. OF 1-QBIT STATES !!!}}$$

IS NOT

THE MOST ICONIC ENTANGLED STATE OF A 2-QBIT SYSTEM IS THE EPR PAIR:

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

THE SPACE OF QUANTUM GATES THAT ACT UPON A N-QBIT SYSTEM IS ALSO A **TENSOR PRODUCT OF OPERATORS** FROM 1-QBIT SYSTEMS.

SOME N-QBIT GATES CANNOT BE EXPRESSED AS A TENSOR PRODUCT OF 1-QBIT GATES. FOR EXAMPLE **CNOT.**

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

MEASUREMENT ⟶ THE TIME EVOLUTION THAT DESCRIBES THE INTERACTION BETWEEN A QUANTUM SYSTEM & A MEASURING APPARATUS IS NOT UNITARY.

THE STANDARD TYPE OF MEASUREMENTS IN QM. IS PROJECTIVE!!!

GIVEN A SET OF ORTHOGONAL VECTORS THAT PRODUCE A COMPLETE BASIS FOR THE SPACE OF A QUANTUM SYSTEM, IT IS POSSIBLE TO DEFINE A HERMITEAN OPERATOR THAT HAS THE SPECTRAL DECOMPOSITION:

$$\hat{O} = \sum_i o_i \hat{P}_i$$

WHERE $\hat{P}_i$ ARE PROJECTION OPERATORS: $\hat{P}_i^2 = \hat{P}_i$. AND:

$$\sum_{\hat{O}|\psi_i\rangle = o_i|\psi_i\rangle} |\psi_i\rangle\langle\psi_i| = \hat{P}_i$$

THIS THEOREM YIELDS THE STANDARD MEASURING POSTULATE IN QM:

PERFORMING A MEASUREMENT OF AN OBSERVABLE IN A SYSTEM IS EQUIVALENT TO APPLYING AN HERMITEAN OPERATOR TO THE STATE OF THE SYSTEM.

A PARTICULAR CASE OF HERMITEAN OPERATORS ARE $|\psi_i\rangle\langle\psi_i|$ FOR ALL VECTOR STATES IN A QBIT HILBERT SPACE. THOSE REPRESENT THE SO CALLED **VON NEUMANN MEASUREMENTS.**

EXAMPLE: PROVE THAT A PROJECTIVE MEASUREMENT WITH RESPECT TO PROJECTORS:

$$\hat{P}_0^{(N)} = \sum_{\substack{\text{EVEN \#} \\ \text{OF 1'S}}} |x_1 \cdots x_N\rangle\langle x_1 \cdots x_N|$$

$$\hat{P}_1^{(N)} = \sum_{\substack{\text{ODD \#} \\ \text{OF 1'S}}} |x_1 \cdots x_N\rangle\langle x_1 \cdots x_N|$$

IS EQUIVALENT TO A MEASUREMENT OF THE OBSERVABLE

$$Z^{\otimes N}$$

SOL: THE OPERATOR $Z^{\otimes N}$ HAS 2^N EIGENVECTORS. SINCE

$$Z|i\rangle = (1-2i)|i\rangle$$

ALL VECTORS OF THE FORM $|i_1 i_2 \cdots i_N\rangle$ ARE EIGENVECTORS OF $\underbrace{Z_1 \otimes Z_2 \otimes \cdots Z_N}_{N \text{ TIMES}}$. STATES WITH EVEN NUMBER OF 1's HAVE EIGENVALUE 1, WHILE STATES WITH ODD NUMBER OF 1's HAVE EIGENVALUE -1. DUE TO THE SPECTRAL DECOMPOSITION THEOREM:

$$Z^{\otimes N} = \hat{P}_0^{(N)} - \hat{P}_1^{(N)}$$

THIS STATES THE EQUIVALENCE OF THE OBSERVABLE MEASUREMENT & THE PROJECTIVE MEASUREMENT WITH RESPECT TO THE ABOVE MENTIONED OPERATORS.

MIXED STATES → THESE ARE STATES FOR WHICH THE **ACTUAL STATE VECTOR IS NOT** KNOWN EXACTLY, BUT THE **PROBABILITY DISTRIBUTION** OF BEING IN A PARTICULAR VECTOR STATE IS KNOWN.

MIXED STATES DESCRIBE ENSEMBLES OF PURE STATES:

$$\{ p_i , |\psi_i\rangle \}$$

p_i: PROBABILITY THAT SYSTEM IS ON STATE $|\psi_i\rangle$

$|\psi_i\rangle$: PURE STATE WITH DEFINED VECTOR IN HILBERT SPACE.

AN ENSEMBLE CAN BE DESCRIBED USING THE **DENSITY OPERATOR**, DEFINED AS:

$$\hat{\rho} = \sum_i p_i |\psi_i\rangle\langle\psi_i|$$

TIME EVOLUTION CORRESPONDS TO A UNITARY TRANSFORMATION:

$$\hat{\rho} \rightarrow \hat{u}\hat{\rho}\hat{u}^{+}$$

MEASUREMENT OPERATORS CORRESPOND TO TRANSFORMATIONS OF THE FORM:

$$\hat{\rho} \rightarrow \frac{\hat{M}\hat{\rho}\hat{M}^{+}}{tr(M^{+}M\hat{\rho})}$$

EXAMPLES ON LINEAR ALGEBRA

EXAMPLE 1: SHOW THAT A NORMAL MATRIX IS HERMITEAN IF AND ONLY IF IT HAS REAL EIGENVALUES.

SOL: CONSIDER A HERMITEAN OPERATOR:

$$\hat{B} = \sum_i \beta_i |i\rangle\langle i|$$

$$\hat{B}^+ = \sum_i \beta_i^* |i\rangle\langle i| \longrightarrow \beta_i^* = \beta_i .$$

IN GENERAL, FOR ALL OPERATORS:

$$\hat{B}^+\hat{B} = \left(\sum_j \beta_j^* |j\rangle\langle j|\right)\left(\sum_i \beta_i |i\rangle\langle i|\right)$$

$$= \sum_{ij} \beta_i \beta_j^* \left(\langle j|i\rangle\right) |j\rangle\langle i|$$

$$\hat{B}\hat{B}^+ = \sum_{ij} \beta_i^* \beta_j \left(\langle j|i\rangle\right) |j\rangle\langle i|$$

IF $\beta_i^* = \beta_i$, $\beta_i^*\beta_j = \beta_i\beta_j^*$, AND SO $\hat{B}\hat{B}^+ = \hat{B}^+\hat{B}$. CLEARLY, $\hat{B}^+ = \hat{B}$.

EXAMPLE 2: PROVE THAT FOR ANY NORMAL OPERATOR

$$\hat{B}|j\rangle = \beta_j|j\rangle , \hat{B}|i\rangle = \beta_i|i\rangle \rightarrow \langle i|j\rangle = 0$$

SOL: CONIDER DE EQUALITIES:

$$\langle i|\hat{B}\hat{B}^+|j\rangle = \langle i|\hat{B}^+\hat{B}|j\rangle$$

$$\beta_j^*\beta_i \langle i|j\rangle = \beta_i^*\beta_j \langle i|j\rangle$$

$$\rightarrow (\beta_i^*\beta_i - \beta_i^*\beta_j)\langle i|j\rangle = 0$$

$$\hat{B}\hat{B}^+|j\rangle = \hat{B}^+\hat{B}|j\rangle = \hat{B}^+(\beta_j|j\rangle) = \beta_j(\hat{B}^+|j\rangle), \quad |j_+\rangle = \hat{B}^+|j\rangle$$

$$\hat{B}|j_+\rangle = \beta_j|j\rangle \longrightarrow \hat{B}^+|j\rangle = \alpha|j\rangle \rightarrow \alpha = \beta_j^*$$

IF $\beta_i \neq \beta_j$, CLEARLY $\langle i|j\rangle = 0$. IF, $\beta_i = \beta_j$, USE GRAHM-SCHMIDT PROCESS TO ORTONORMALIZE.

EXAMPLE 3: SUPPOSE Δ' AND Δ'' ARE MATRIX REPRESENTATIONS OF AN OPERATOR Δ ON A VECTOR SPACE V WITH RESPECT TO TWO DIFFERENT ORTONORMAL BASES. RELATE THEIR MATRIX REPRESENTATION.

SOL: CONSIDER TWO BASES $\{|i\rangle, |\alpha\rangle\}$ SUCH THAT:

$$1 = \sum_i |i\rangle\langle i| \qquad \langle i|j\rangle = \delta_{ij}$$

$$1 = \sum_\alpha |\alpha\rangle\langle\alpha| \qquad \langle\alpha|\beta\rangle = \delta_{\alpha\beta}$$

THEN,

$$\begin{aligned}\langle i|\hat{\Delta}|j\rangle &= \langle i|\left(\sum_\alpha |\alpha\rangle\langle\alpha|\right)\hat{\Delta}\left(\sum_\beta |\beta\rangle\langle\beta|\right)|j\rangle \\ &= \sum_{\alpha\beta}\langle i|\alpha\rangle\left(\langle\alpha|\hat{\Delta}|\beta\rangle\right)\langle\beta|j\rangle \\ &= \sum_{\alpha\beta}\langle i|\alpha\rangle\langle\beta|j\rangle\left(\langle\alpha|\hat{\Delta}|\beta\rangle\right) \\ &= \langle i|\left(\sum_{\alpha\beta}|\alpha\rangle\langle\beta|\,\Delta_{\alpha\beta}\right)|j\rangle \\ &= \sum_{\alpha\beta}\langle i|\alpha\rangle\langle\beta|j\rangle\,\Delta_{\alpha\beta}\end{aligned}$$

$$\boxed{\Delta_{ij} = \sum_{\alpha\beta} C_{i\alpha}\,\Delta_{\alpha\beta}\,(C_{j\beta})^+}$$

IF $|\alpha\rangle = \sum_i C_{i\alpha}|i\rangle$, THEN,

$$\langle\alpha|\beta\rangle = \sum_{ij} C_{i\alpha}^*\langle i|\left(C_{j\beta}|j\rangle\right) = \sum_i C_{i\alpha}^* C_{i\beta} = \delta_{\alpha\beta}$$

THAT IS TO SAY,

$$\boxed{CC^+ = 1}$$

EXAMPLE 4: SHOW THAT FOR ANY OPERATOR $\hat{A}$, $\hat{A}^\dagger\hat{A}$ IS POSITIVE DEFINITE.

SOL: CONSIDER THE INNER PRODUCT $(|v\rangle, \hat{A}^\dagger\hat{A}|v\rangle)$:

$$\langle v|\hat{A}^\dagger\hat{A}|v\rangle = (\langle v|\hat{A}^\dagger)(\hat{A}|v\rangle)$$

IF $|\phi\rangle = \hat{A}|v\rangle \rightarrow \langle v|\hat{A}^\dagger\hat{A}|v\rangle = \langle\phi|\phi\rangle \geq 0$. THE EQUALITY HOLDS IF, AND ONLY IF, $|\phi\rangle = 0$.

EXAMPLE 5: PROVE THE SPECTRAL DECOMPOSITION THEOREM IN THE PARTICULAR CASE OF HERMITEAN OPS.

SOL: THE THEOREM STATES THAT ANY HERMITEAN (NORMAL) OPERATOR ON A VECTOR SPACE V IS DIAGONAL WITH RESPECT TO SOME ORTHONORMAL BASIS. AND CONVERSELY, ANY DIAGONALIZABLE OPERATOR IS NORMAL.

ON NIELSEN & CHUANG, THIS THEOREM IS PROVED BY INDUCTION. THE ESSENTIAL FEATURES ARE THAT ANY OPERATOR CAN BE EXPRESSED AS:

$$\hat{B} = (\hat{P}+\hat{Q})\hat{B}(\hat{P}+\hat{Q})$$

PROJECTOR ONTO SOME EIGENVALUE SUBSPACE

PROJECTOR ONTO ORTHOGONAL COMPLEMENT ($\hat{Q} = 1 - \hat{P}$)

SINCE $\hat{P}\hat{B}\hat{P} = \hat{P}(\beta\hat{P}) = \beta\hat{P}^2 = \beta\hat{P}$, $\hat{Q}\hat{B}\hat{P} = \ldots(\hat{P}-\hat{P}^2) = 0$ AND, FOR $\hat{B}^\dagger = \hat{B}$, $\hat{B}^\dagger\hat{P} = \hat{B}\hat{P} = \ldots \rightarrow (\hat{Q}\hat{B}^\dagger\hat{P})^\dagger = \hat{P}\hat{B}\hat{Q} = 0$ NOTING THAT

$$(\hat{Q}\hat{B}\hat{Q})^\dagger = \hat{Q}\hat{B}^\dagger\hat{Q} = \hat{Q}\hat{B}\hat{Q}$$ HERMITEAN

AND THUS DIAGONAL WITH RE... ONE ORTHONORMAL BASIS FOR THE ORTHOGON... -MENT (BY INDUCTION, $\hat{B} = \hat{P}\hat{B}\hat{P} + \hat{Q}\hat{B}\hat{Q}$ IS DIAG... WITH RESPECT TO AN ORTHONORMAL BASIS FOR V (IE THE BASIS FOR Q AND FOR P SUBSPACES COMBINED)

NOTE $\hat{P}$ CAN BE ANY ORTHOGONAL PROJECTOR GIVEN BY GRAHM-SCHMIT PROCCESS

EXAMPLE 6 SHOW THAT TRANSPOSE, COMPLEX CONJUGATION, AND ADJOINT OPERATORS DISTRIBUTE OVER TENSOR PRODUCT

SOL CONSIDER 2 VECTOR SPACES V & W, WITH ORTHONORMAL BASIS $\{|v\rangle\}$ & $\{|w\rangle\}$ CONSIDER OPERATORS $\hat{A}$ & $\hat{B}$ DEFINED ON V & W, RESPECTIVELY IN THE BASIS, THOSE OPERATORS HAVE MATRIX REPRESENTATIONS, AND TENSOR PRODUCT IS PERFORMED VIA KRONECKER PRODUCT

$$A \otimes B = \begin{bmatrix} A_{11}B & A_{12}B & \cdots & A_{1n}B \\ A_{21}B & A_{22}B & \cdots & A_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ A_{m1}B & A_{m2}B & \cdots & A_{mn}B \end{bmatrix}$$

IN TERMS OF THIS PRODUCT

$$(A \otimes B)^* = [A_{ij}^* B^*] = A \otimes B$$

$$(A \otimes B)^T = [A_{ji} B^T] = A^T \otimes B^T$$

SINCE $(A \otimes B)^\dagger = \{(A \otimes B)^*\}^T$, IT IS CLEAR THAT

$$(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$$

EXAMPLE 7 SHOW THAT THE TENSOR PRODUCT OF UNITARY OPERATORS IS A UNITARY OPERATOR

SOL CONSIDERING THAT $(A \otimes B)(C \otimes D)|\psi\rangle \otimes |\phi\rangle = (A \otimes B)\, C|\psi\rangle \otimes D|\phi\rangle = AC|\psi\rangle \otimes BD|\phi\rangle$, FOR ALL $|\psi\rangle \in V$, $|\phi\rangle \in W$, THEN IT IS CLEAR THAT

$$(\hat{u}^\dagger \otimes \hat{u}^\dagger)(\hat{u} \otimes \hat{u})|\psi\phi\rangle = |\psi\phi\rangle$$

SO IF $\hat{U} = \hat{u} \otimes \hat{u}$, THEN $\hat{U}\hat{U}^\dagger = 1_{V \otimes W}$

EXAMPLE 8 THE HADAMARD OPERATOR ON 1 QBIT MAY BE WRITTEN AS

$$\hat{H} = \frac{1}{\sqrt{2}} \left[(|0\rangle + |1\rangle)\langle 0| + (|0\rangle - |1\rangle)\langle 1| \right]$$

SHOW EXPLICITLY THAT THE HADAMARD TRANSFOR ON n QBITS, $H^{\otimes n}$, MAY BE WRITTEN AS

$$H^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x,y} (-1)^{xy} |x\rangle\langle y|$$

SOL THIS MAY BE PROVED BY INDUCTION THE FORMULA IS TRUE FOR $n=1$ CONSIDER THE TENSOR PRODUCT FOR $n=2$

$$H^{\otimes 2} = \frac{1}{\sqrt{2^2}} (|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| - |1\rangle\langle 1|)^{\otimes 2}$$

$$= \frac{1}{\sqrt{2^2}} \Big(|00\rangle\langle 00| + |01\rangle\langle 00| + |00\rangle\langle 01| - |01\rangle\langle 01| + |10\rangle\langle 00| + |11\rangle\langle 00| + |10\rangle\langle 01| - |11\rangle\langle 01| + |00\rangle\langle 10| + |01\rangle\langle 10| + |00\rangle\langle 11| - |01\rangle\langle 11| + - |10\rangle\langle 10| - |11\rangle\langle 10| - |10\rangle\langle 11| + |11\rangle\langle 11| \Big)$$

DEFINING THE BITWISE INNER PRODUCT MODULO 2

$$x \cdot y = \left(\sum_i x_i y \right) \bmod 2$$

IT IS CLEAR THAT THE FORMULA IS VALID IF

$$H^{\otimes n-1} = \frac{1}{\sqrt{2^{n-1}}} \sum_{xy} (-1)^{x \cdot y} |x\rangle\langle y|$$

WHERE x, y ARE STRINGS OF BITS WITH LENGTH $n-1$ LETS CONSIDER THE TENSOR PRODUCT

$$H \otimes H^{\otimes n-1} = H^{\otimes n}$$

$$H^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{xy} (-1)^{xy} \left[|0x\rangle\langle 0y| + |1x\rangle\langle 0y| + |0x\rangle\langle 1y| - |1x\rangle\langle 1y| \right]$$

GIVEN THAT $(\alpha x)(\beta y) = xy + \alpha\beta$, THEN FROM THE EXPANSION, IT IS CLEAR THAT

$$H^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{xy} (-1)^{xy} |x\rangle\langle y|$$

WHERE x, y NOW HAVE LENGTH n NOTICE THAT IN THE EXPANSION ALL POSSIBLE WAYS TO GENERALIZE EXTERNAL PRODUCTS OF $n-1$ QBIT STATES, TO n QBIT EXTERNAL PRODUCTS ARE INCLUDED

EXAMPLE 9 LET $\vec{v}$ BE ANY REAL, 3D UNIT VECTOR AND θ A REAL NUMBER PROVE THAT

$$\exp(i\theta \vec{v}\,\vec{\sigma}) = \cos\theta\, 1 + i\sin\theta\, \vec{v}\,\vec{\sigma}$$

SOL CONSIDER THE PRODUCT

$$\begin{aligned}(v_x\sigma_x + v_y\sigma_y + v_z\sigma_z)^2 = {} & v_x^2\sigma_x^2 + v_y^2\sigma_y^2 + v_z^2\sigma_z^2 \\ & + v_x v_y(\sigma_x\sigma_y + \sigma_y\sigma_x) \\ & + v_x v_z(\sigma_x\sigma_z + \sigma_z\sigma_x) \\ & + v_y v_z(\sigma_y\sigma_z + \sigma_z\sigma_y)\end{aligned}$$

BY DEFINITION OF PAULI MATRICES

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

IT IS CLEAR THAT $\sigma_i^2 = 1$, $\sigma_i\sigma_j + \sigma_j\sigma_i = 2\,1\,\delta_{ij}$ SO

$$(i\theta \vec{v}\,\vec{\sigma})^{2n} = (-1)^n \theta^{2n} 1$$

BY SERIES EXPANSION

$$\exp(i\theta\,\vec{v}\cdot\vec{\sigma}) = \left(\sum_{i=0}^{\infty}\frac{(-1)^n\theta^{2n}}{(2n)!}\right)\mathbb{1} + i\left(\sum_{i=0}^{\infty}\frac{(-1)^n\theta^{2n+1}}{(2n+1)!}\right)\vec{v}\cdot\vec{\sigma}$$

USING THE SERIES EXPANSION FOR $\sin\theta$ AND $\cos\theta$, THE DESIRED RESULT FOLLOWS

EXAMPLE 10 EXPRESS THE POLAR DECOMPOSITION OF A NORMAL MATRIX IN OUTER PRODUCT REPRESENTATION

SOL A NORMAL MATRIX IS DIAGONAL IN A CERTAIN ORTHONORMAL BASIS THAT IS TO SAY

$$\hat{\Delta} = \sum_{\alpha}\alpha\,|\alpha\rangle\langle\alpha|$$

HENCE $\hat{\Delta}^{+}\hat{\Delta} = \left(\sum_{\alpha'}\alpha'^{*}|\alpha'\rangle\langle\alpha'|\right)\left(\sum_{\alpha}\alpha|\alpha\rangle\langle\alpha|\right)$

$$= \sum_{\alpha\alpha'}\alpha'^{*}\alpha\,|\alpha'\rangle\underbrace{\langle\alpha'|\alpha\rangle}_{\delta_{\alpha\alpha'}}\langle\alpha|$$

$$= \sum_{\alpha}|\alpha|^2\,|\alpha\rangle\langle\alpha|$$

SO LET BE $\hat{J} = \sum_{\alpha}|\alpha|\,|\alpha\rangle\langle\alpha|$ LET $|\beta\rangle = \hat{\Delta}|\alpha\rangle$

CLEARLY $|\beta\rangle = \alpha|\alpha\rangle$, IF $\alpha = 0$, THEN $|\beta\rangle = 0$ IF $\alpha \neq 0$, $|\alpha|^{-1}|\beta\rangle = e^{i\theta_\alpha}|\alpha\rangle$ HENCE

$$\hat{J} = \sum_{\alpha}|\alpha|\,|\alpha\rangle\langle\alpha|$$

$$\hat{U} = \sum_{\alpha}e^{i\theta_\alpha}|\alpha\rangle\langle\alpha|$$

SINCE $\{|\alpha\rangle\}$ ARE A ORTHONORMAL BASIS, $\hat{U}$ IS CLEARLY UNITARY

EXAMPLE 11 USE SPECTRAL DECOMPOSITION TO SHOW THAT $\hat{\kappa} = -i\log(\hat{u})$ FOR ANY UNITARY $\hat{u}$ IS HERMITEAN

SOL SINCE $\hat{u}^+\hat{u} = \hat{u}\hat{u}^+ = 1$, IT HAS SPECTRAL DECOMPOSITION FURTHERMORE

$$\hat{u} = \sum_{\alpha} e^{i\alpha} |\alpha\rangle\langle\alpha| \quad \text{FOR } \alpha \in \mathbb{R}$$

THIS IS SO BECAUSE $\hat{u}|\alpha\rangle = \alpha'|\alpha\rangle \rightarrow |\alpha'|^2 = 1$ HENCE, IT IS THAT

$$\hat{\kappa} = \sum_{\alpha} \alpha |\alpha\rangle\langle\alpha|$$

WITHOUT LOSING GENERALITY, IT IS POSSIBLE TO RESTRICT TO THE BRANCH OF log THAT IS CONSISTENT WITH $0 < \alpha \leq 2\pi$ THEREFORE $\alpha > 0$, AND $\hat{\kappa}$ IS A HERMITEAN OPERATOR

ADVANCED TOPICS

DATE 19-09-20

QUANTUM MEASUREMENT $\longrightarrow$ FOLLOWING TOPICS ARE GOING TO BE DISCUSSED

1. DISTINGUISHING QUANTUM STATES
2. VON NEUMANN MEASUREMENTS
3. POVM MEASUREMENTS

EXAMPLE 12 SUPPOSE $\{\hat{L}_\ell\}$ AND $\{\hat{M}_m\}$ ARE TWO SETS OF MEASUREMENT OPERATORS SHOW THAT A CASCADED MEASUREMENT BY $\{\hat{L}_\ell\}$ & $\{\hat{M}_m\}$ IS EQUIVALENT TO A SINGLE MEASUREMENT DEFINED BY OPERATORS $\{\hat{N}_{\ell m}\}$, WITH $\hat{N}_{\ell m} = \hat{M}_m \hat{L}_\ell$

SOL SUPPOSE THE STATE OF THE SYSTEM BEFORE L-MEASUREMENT IS $|\psi\rangle$ THE PROBABILITY THAT A CASCADED MEASUREMENT PRODUCES (SEQUENTIAL) OUTCOMES (l,m) IS, BY THE MEASUREMENT POSTULATE

$$p(l,m|\psi) = p(m|l,\psi)\ p(l|\psi)$$

$$p(l,m|\psi) = \langle\psi_l|\hat{M}_m^\dagger \hat{M}_m|\psi_l\rangle\ \langle\psi|\hat{L}_l^\dagger \hat{L}_l|\psi\rangle$$

WHERE $|\psi_l\rangle = \dfrac{\hat{L}_l|\psi\rangle}{(\langle\psi|\hat{L}_l^\dagger \hat{L}_l|\psi\rangle)^{1/2}}$ THEREFORE, IT IS CLEAR

$$p(l,m|\psi) = \langle\psi|(\hat{M}_m\hat{L}_l)^\dagger(\hat{M}_m\hat{L}_l)|\psi\rangle$$

BY CONSIDERING $\sum_{lm} p(l,m|\psi) = 1$ FOR ALL $|\psi\rangle$, IT IS CLEAR THAT $\sum_{lm}(\hat{M}_m\hat{L}_l)^\dagger(\hat{M}_m\hat{L}_l) = \mathbb{1}$ CONSIDERING THE EVOLUTION OF THE SYSTEM'S STATE

$$|\psi_{final}\rangle = \frac{\hat{M}_m|\psi_l\rangle}{(\langle\psi_l|\hat{M}_m^\dagger\hat{M}_m|\psi_l\rangle)^{1/2}} = \frac{\hat{M}_m\hat{L}_l|\psi\rangle}{(\langle\psi|\hat{L}_l^\dagger\hat{M}_m^\dagger\hat{M}_m\hat{L}_l|\psi\rangle)^{1/2}}$$

$$|\psi_{final}\rangle = \frac{(\hat{M}_m\hat{L}_l)|\psi\rangle}{(\langle\psi|(\hat{M}_m\hat{L}_l)^\dagger(\hat{M}_m\hat{L}_l)|\psi\rangle)^{1/2}}$$

HENCE THE CASCADED MEASUREMENT IS EQUIVALENT TO A SINGLE MEASUREMENT USING OPERATORS $\{\hat{N}_{lm}\} = \{\hat{M}_m\hat{L}_l\}$

DISTINGUISHING QUANTUM STATES $\longrightarrow$ SUPPOSE A CERTAIN SET OF STATES $\{|\psi_j\rangle\}$ IS TO BE DISTINGUISHED

A CORRESPONDING SET OF MEASUREMENT OPERATORS $\{\hat{M}_j\}$ IS USED TO CHARACTERIZE THE T OF DETERMINING THE INDEX j OF A CERTAIN STATE

TWO STATES ARE DISTINGUISHABLE (RELIABLY !!!) IF $p(i|\psi_j) = \delta_{ij}$

ONLY ORTHOGONAL STATES CAN BE RELIABLY DISTINGUISHED

FROM EXAMPLE 12, AN IDENTIFICATION – CONFIRMATION MEASUREMENT CORRESPONDS TO OPERATORS $\{\hat{M}_i\}$ SUPPOSE A STATE $|\psi_i\rangle$ WERE RELIABLY DISTINGUISHED THAT WOULD MEAN $p(i|\psi_j) = 1$, $p(i|\psi_j) = 0$, AND THUS

$$\hat{M}_i |\psi_j\rangle = f(j)\delta_{ij}|\psi_j\rangle$$

BY THE SAME TOKEN, IF ANOTHER STATE $|\psi_{j'}\rangle$ IS DISTINGUISHABLE, THEN

$$\hat{M}_i |\psi_{j'}\rangle = f(j')\delta_{ij'}|\psi_{j'}\rangle$$

FOR TWO NON ORTHOGONAL STATES $|\psi\rangle$ & $|\phi\rangle$, IT IS THAT

$$|\psi\rangle = \alpha|\phi\rangle + |\psi\rangle_{\perp\phi}$$
$$|\phi\rangle = \beta|\psi\rangle + |\phi\rangle_{\perp\psi}$$

BY THE POSTULATE OF QUANTUM MEASUREMENTS, IF $|\psi_j\rangle \not\perp |\psi_{j'}\rangle$

$$\sum_i p(i|\psi_j) = \sum_i \langle\psi_j|\hat{M}_i^\dagger \hat{M}_i|\psi_j\rangle$$

$$= \langle\psi_j|\hat{M}_j^\dagger \hat{M}_j|\psi_j\rangle + \langle\psi_j|\hat{M}_{j'}^\dagger \hat{M}_{j'}|\psi_j\rangle + \sum_{i\neq j,j'} \langle\psi_j|\hat{M}_i^\dagger \hat{M}_i|\psi_j\rangle$$

$$= 1 + |\beta|^2 \quad \text{WHERE} \quad \langle\psi_j|\psi_{j'}\rangle = \beta \neq 0$$

SINCE $\sum_i p(i|\psi_j) = 1$, CONTRADICTION IMPLIES THAT NON-ORTHOGONAL STATES ARE NOT RELIABLY DISTINGUISHABLE

PROJECTIVE MEASUREMENTS $\longrightarrow$ THEY ARE COMMONLY REFERRED TO AS MEASUREMENTS IN A GIVEN BASIS

EXAMPLE 13 SHOW THAT $\vec{\sigma}\cdot\vec{\sigma}$ HAS EIGENVALUES ± 1, AND PROJECTORS ONTO THE CORRESPONDING EIG. SPACES ARE

$$\hat{P}_\pm = \frac{1}{2}(1 \pm \vec{\sigma}\cdot\vec{\sigma})$$

SOL CONSIDER THE EQUATION $\vec{\sigma}\cdot\vec{\sigma}|\psi\rangle = \lambda|\psi\rangle$

SINCE $(\sum_j v_j \hat{\sigma}_j)(\sum_i v_i \hat{\sigma}_i) = \sum_i v_i^2 \sigma_i^2 + \sum_{i \neq j} v_i v_j \{\sigma_i, \sigma_j\}$

$= (\sum_i v_i^2) 1 = 1$

IT IS FAIRLY EASY TO SHOW THAT $|\lambda|^2 = 1$ SINCE $(\vec{v}\cdot\vec{\sigma})^\dagger = \vec{v}\cdot\vec{\sigma}$, FOR $\vec{v}\cdot\vec{\sigma}|\psi\rangle = \lambda|\psi\rangle \rightarrow |\lambda|^2 = \langle\psi|(\vec{v}\cdot\vec{\sigma})^2|\psi\rangle = 1$ BECAUSE $\vec{v}\cdot\vec{\sigma}$ IS SELFADJOINT, $\lambda = \pm 1$ BY THE DEFINITION OF $\hat{P}_\pm$, IT IS QUITE CLEAR THAT

$$\vec{v}\cdot\vec{\sigma} = (+1)\hat{P}_+ + (-1)\hat{P}_-$$

AND $\hat{P}_+\hat{P}_- = 0$, $\hat{P}_+^2 = \hat{P}_-^2 = 1$ HENCE $\hat{P}_\pm$ ARE PROJECTORS ONTO CORRESPONDING EIGENSPACES

POVM MEASUREMENT → IT IS A FORMALISM IN WHICH THE OUTCOME OF THE MEASUREMENT RATHER THAN THE FINAL STATE IS HIGHLIGHTED

FOR A GIVEN MEASUREMENT OPERATORS SET $\{\hat{M}_m\}$, POSITIVE OPERATORS

$$\hat{E}_m = \hat{M}_m^\dagger \hat{M}_m$$

CAN BE DEFINED SUCH THAT $\begin{cases} p(m|\psi) = \langle\psi|\hat{E}_m|\psi\rangle \\ \sum_m \hat{E}_m = 1 \end{cases}$

CLEARLY, $\hat{E}_m$ ARE POSITIVE (HERMITEAN) OPERATORS THE SET $\{\hat{E}_m\}$ IS CALLED POV ELEMENTS ASSOCIATED TO THE MEASUREMENT

NOTE THE REFINEMENT IN MEASUREMENT REQUIRED IN QUANTUM COMPUTING AND QUANTUM INFORMATION SHOWS THAT NOT ALL MEASUREMENTS ARE PROJECTIVE IN NATURE IN PARTICULAR, REPEATABILITY IS NOT ALWAYS ENSURED

EXAMPLE 14 SHOW THAT ANY MEASUREMENT WHERE ALL MEASUREMENT OPERATORS & POVM ELEMENTS COINCIDE IS A PROJECTIVE MEASUREMENT

SOL FOR SUCH A MEASUREMENT, IT IS THAT

$$\hat{E}_m = \hat{M}_m^+ \hat{M}_m = \hat{M}_m$$

EQUALLY IMPORTANT, SINCE $\hat{E}_m^+ = \hat{E}_m$, $\hat{M}_m^+ = \hat{M}_m$ AS A RESULT

$$\hat{M}_m^2 = \hat{M}_m^+ \hat{M}_m = \hat{M}_m$$

AND THUS ALL OPERATORS ASSOCIATED TO THE MEASUREMENT ARE PROJECTORS SINCE THEY ARE HERMITEAN, FOR ALL m

$$\hat{M}_m = \sum_i \lambda_i^{(m)} |m_i\rangle\langle m_i|$$

WITH $\langle m_i | m_j \rangle = \delta_{ij}$ HENCE $p(m|m_i) = \langle m_i | \hat{M}_m^2 | m_i \rangle = |\lambda_i^{(m)}|^2$ SINCE FOR ALL PROJECTOR OPERATORS ITS EIGENVALUES ARE EITHER 0 OR 1, AND $|m_i\rangle \neq 0$, IT MUST BE THAT

$$p(m|m_i) = 1$$

THEREFORE, FOR ALL $m' \neq m$

$$0 = p(m'|m_i) = \langle m_i | \hat{M}_{m'} | m_i \rangle$$

THIS IMPLIES $\langle m_j' | m_i \rangle = \delta_{mm'} \delta_{ji}$ AS A RESULT

$$\hat{M}_{m'} \hat{M}_m = \sum_{ij} \lambda_j^{(m)} \lambda_i^{(m')} |m_j'\rangle\langle m_j'|m_i\rangle\langle m_i|$$

$$= \sum_{ij} \lambda_j^{(m)} \lambda_i^{(m')} \delta_{ij} \delta_{mm'} |m_j'\rangle\langle m_i| = \hat{M}_m^2 \delta_{mm'}$$

SINCE $\sum_m \hat{E}_m = \sum_m \hat{M}_m = \mathbb{1}$, IT IS CLEAR THAT THIS MEASUREMENT IS EQUIVALENT TO A PROJECTIVE MEASUREMENT, FOR $\{\hat{M}_m\}$ IS A SET OF ORTHOGONAL PROJECTORS

EXAMPLE 15 SUPPOSE BOB IS GIVEN A QUANTUM STATE CHOSEN FROM A SET $|\psi_1\rangle, \ldots, |\psi_m\rangle$ OF LINEARLY INDEPENDENT STATES CONSTRUCT A POVM $\{\hat{E}_1, \hat{E}_2, \ldots, \hat{E}_{m+1}\}$ SUCH THAT IF OUTCOME E_i OCCURS, $1 \leq i \leq m$, THEN HE KNOWS WITH CERTAINTY THAT HE WAS GIVEN THE STATE $|\psi_i\rangle$

SOL FOR EACH i, DEFINE $\mathcal{L}\{\psi_{i'\neq i}\}$, AND BUILD AN OPERATOR THAT PROJECTS A STATE ONTO $\mathcal{L}\{\psi_{i'\neq i}\}$'S ORTHOGONAL COMPLEMENT THIS WOULD BE PROPORTIONAL TO $\hat{E}_i$ THAT SUCH AN OPERATOR IS POSITIVE CAN BE SEEN FROM ITS BEING A PROJECTOR

$$\hat{Q}_{i'\neq i}^2 = (1 - \hat{P}_{i\neq i'})^2 = 1 - 2\hat{P}_{i'\neq i} + \hat{P}_{i'\neq i'} = \hat{Q}_{i'\neq i}$$

ON THE OTHER HAND, IT IS CLEAR THAT

$$\hat{Q}_{i'\neq i}|\psi_i\rangle \neq 0 \qquad \hat{Q}_{i\neq i}|\psi_{i'\neq i}\rangle = 0$$

NOW, SINCE $\langle\psi_i|\hat{Q}_{i'\neq i}|\psi_i\rangle > 0$, DEFINE

$$\hat{E}_i = \frac{1}{\sum_i \langle\psi_i|Q_{i'\neq i}|\psi_i\rangle}\hat{Q}_{i'\neq i}$$

FOR $1 \leq i \leq m$ THEN, DEFINE

$$\hat{E}_{m+1} = 1 - \sum_i \hat{E}_i$$

THEREFORE, IT IS CLEAR THAT

$$p(E_i|\psi_i) = \frac{\langle\psi_i|Q_{i'\neq i}|\psi_i\rangle\, \delta_{ii}}{\sum_i \langle\psi_i|\hat{Q}_{i'\neq i}|\psi_i\rangle} \qquad p(E_{m+1}|\psi_i) = 1 - p(E_i|\psi_i)$$

SO THAT $\sum_i p(E_i|\psi_i) = 1$ IT IS EASY TO SEE THAT THIS IS VALID FOR ALL $|\phi\rangle$, AND THUS $\sum_i \hat{E}_i = 1$

NOTE THIS IS A STRAIGHTFORWARD GENERALIZATION OF THE EXAMPLE INTRODUCED IN NIELSEN

SUPERDENSE CODING → 2 CLASSICAL BITS OF INFORMATION CAN BE SENT JUST TRANSMITTING 1 QBIT, USING BELL STATES

CONSIDER 4 BELL STATES FOR 2 ENTANGLED QBITS

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|\psi_3\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)$$

$$|\psi_4\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

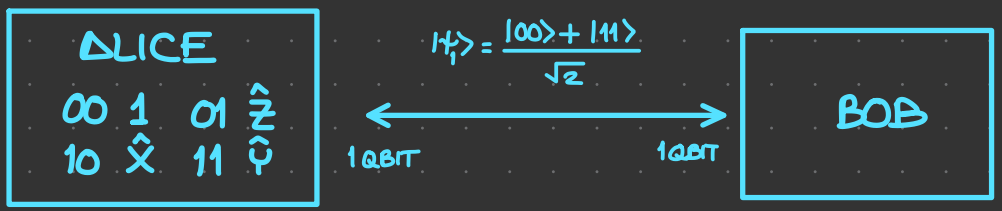
IT IS NOT DIFFICULT TO SEE THAT

$$\hat{X}_1 |\psi_1\rangle = \hat{\sigma}_{x1} |\psi_1\rangle = |\psi_3\rangle$$

$$\hat{Z}_1 |\psi_1\rangle = \hat{\sigma}_{z1} |\psi_1\rangle = |\psi_2\rangle$$

$$i\hat{Y}_1 |\psi_1\rangle = i\hat{\sigma}_{y1} |\psi_1\rangle = |\psi_4\rangle$$

WHERE THE GATES ARE ACTING ON THE FIRST QBIT ONLY
CONSIDER TWO PARTIES, EACH ONE WITH ONE OF A PAIR OF QBITS ON STATE $|\psi_1\rangle$



SINCE BELL STATES ARE ORTHOGONAL, THEY ARE COMPLETELY DISTINGUISHABLE HENCE, IF ONE OF THE PARTIES APPLIES ONE OF THE ABOVE GATES TO HIS/HER QBIT, ANY OF THE 2-BIT STRINGS CAN BE ENCODED

EXAMPLE 16 SUPPOSE $\hat{E}$ IS ANY POSITIE OPERATOR ACTING ON ALICE'S QBIT SHOW THAT $\langle\psi|\hat{E}\otimes 1_2|\psi\rangle$ TAKES THE SAME VALUE WHEN $|\psi\rangle$ IS ANY OF THE 4 BELL STATES

SOL CONSIDER $|\psi_1\rangle$ FOR THIS STATE

$$\langle\psi_1|\hat{E}\otimes 1_2|\psi_1\rangle = \frac{1}{2}\left(\langle 11|\langle 11| + \langle 01|\langle 01|\right)\hat{E}\otimes 1\left(|10\rangle|10\rangle + |11\rangle|11\rangle\right)$$

$$= \frac{1}{2}\left(\langle 01|\hat{E}|10\rangle + \langle 1|\hat{E}|1\rangle\right)$$

$$\langle\psi_2|\hat{E}\otimes 1_2|\psi_2\rangle = \frac{1}{2}\left(\langle 01|\langle 01| - \langle 11|\langle 11|\right)\hat{E}\otimes 1_2\left(|10\rangle|10\rangle - |11\rangle|11\rangle\right)$$

$$= \frac{1}{2}\left(\langle 01|\hat{E}|10\rangle + \langle 11|\hat{E}|11\rangle\right)$$

$$\langle\psi_3|\hat{E}\otimes 1_3|\psi_3\rangle = \frac{1}{2}\left(\langle 11|\langle 01| + \langle 01|\langle 11|\right)\hat{E}\otimes 1_2\left(|11\rangle|10\rangle + |10\rangle|11\rangle\right)$$

$$= \frac{1}{2}\left(\langle 11|\hat{E}|11\rangle + \langle 01|\hat{E}|10\rangle\right)$$

$$\langle\psi_4|\hat{E}\otimes 1_3|\psi_4\rangle = \frac{1}{2}\left(\langle 01|\langle 11| - \langle 11|\langle 01|\right)\hat{E}\otimes 1_2\left(|10\rangle|11\rangle - |11\rangle|10\rangle\right)$$

$$= \frac{1}{2}\left(\langle 01|\hat{E}|10\rangle + \langle 11|\hat{E}|11\rangle\right)$$

NOTICE THAT THIS IMPLIES THAT NO MEASUREMEN ON A SINGLE QBIT FROM THE ENTANGLED PAIR YIELDS ANY USEFUL INFORMATION HENCE, NOBODY CAN READ OFF ALICE'S MESSAGE BY INTERCEPTING THE CHANNEL

DENSITY OPERATOR FORMALISM → CONSIDER AN ENSEMBLE OF PURE STATES $\{p_i, |\psi_i\rangle\}$ THE STATE OF THIS SYSTEM WAS DESCRIBED BY THE OPERATOR

$$\hat{\rho} = \sum_i p_i |\psi_i\rangle\langle\psi_i|$$

CONSIDER THE TIME EVOLUTION & MEASUREMENT POSTULATES IN THIS FORMALISM

PURE STATES EVOLV ACCORDING TO A UNITARY LINEAR OPERATOR

$$|\psi'\rangle = \hat{U}|\psi\rangle \quad , \quad \hat{U}\hat{U}^\dagger = 1$$

THEREFORE, IT IS EXPECTED THAT DENSITY OPERATOR EVOLVES LIKE

$$\hat{\rho}' = \sum_i p_i |\psi_i'\rangle\langle\psi_i'| = \hat{U}\left(\sum_i p_i |\psi_i\rangle\langle\psi_i|\right)\hat{U}^\dagger = \hat{U}\hat{\rho}\hat{U}^\dagger$$

THE TIME EVOLUTION POSTULATE CAN BE REESTATED BY ASSERTING THAT DENSITY OPERATOR EVOLVES SUCH THAT

$$\hat{\rho} \longrightarrow \hat{\rho}' = \hat{U}\hat{\rho}\hat{U}^\dagger$$

CONSIDER NOW THE MEASUREMENT POSTULATE CONSIDER A MEASUREMENT DESCRIBED BY OPERATORS $\{\hat{M}_m\}$ BY PROBABILITY THEORY.

$$p(m|\hat{\rho}) = \sum_i p_i p(m|\psi_i)$$

$$= \sum_i p_i \langle\psi_i|\hat{M}_m^\dagger \hat{M}_m|\psi_i\rangle$$

$$= \sum_i p_i \, tr\left(\hat{M}_m^\dagger \hat{M}_m |\psi_i\rangle\langle\psi_i|\right)$$

$$= tr\left(\hat{M}_m^\dagger \hat{M}_m \sum_i p_i |\psi_i\rangle\langle\psi_i|\right)$$

$$= tr\left(\hat{M}_m^\dagger \hat{M}_m \hat{\rho}\right)$$

AFTER MEASUREMENT, THE ENSEMBLE CHANGES ACCORDING TO THE MEASUREMENT OUTCOME NOT ONLY THE STATES, BUT ALSO THE PROBABILITY DISTRIBUTION

THE PROBABILITY DISTRIBUTION CHANGES AS FOLLOWS

$$p_i' = p_i \frac{p(m|\psi_i)}{p(m)} = p_i \frac{\langle \psi_i | \hat{M}_m^\dagger \hat{M}_m | \psi_i \rangle}{\mathrm{tr}(\hat{M}_m^\dagger \hat{M}_m \hat{\rho})}$$

BY DEFINITION OF CONDITIONAL PROBABILITY ON THE OTHER HAND, STATES CHANGE AS FOLLOWS

$$|\psi_i'\rangle = \frac{\hat{M}_m |\psi_i\rangle}{\sqrt{\langle \psi_i | \hat{M}_m^\dagger \hat{M}_m | \psi_i \rangle}}$$

THEREFORE, THE FINAL ENSEMBLE $\{p_i', |\psi_i'\rangle\}$ IS

$$\hat{\rho}' = \sum_i p_i \frac{\hat{M}_m |\psi_i\rangle\langle\psi_i| \hat{M}_m^\dagger}{\mathrm{tr}(\hat{M}_m^\dagger \hat{M}_m \hat{\rho})}$$

$$\hat{\rho}' = \frac{\hat{M}_m \hat{\rho} \hat{M}_m^\dagger}{\mathrm{tr}(\hat{M}_m^\dagger \hat{M}_m \hat{\rho})}$$

MEASUREMT POSTULATE CAN BE RESTATED BY SETTING THAT OUTCOME m OF A MEASUREMENT $\{\hat{M}_m\}$ HAS PROBABILITY $\mathrm{tr}(\hat{M}_m^\dagger \hat{M}_m \hat{\rho})$ AND IF OBSERVED, THE SYSTEM EVOLVES

$$\hat{\rho} \longrightarrow \hat{\rho}' = \frac{\hat{M}_m \hat{\rho} \hat{M}_m^\dagger}{\mathrm{tr}(\hat{M}_m \hat{M}_m^\dagger \hat{\rho})}$$

NOT ONLY DOES THIS FORMALISM INCLUDE PURE STATES AS A PARTICULAR CASE, BUT ALSO CAN BE USED TO DESCRIBE MIXTURES OF ENSEMBLES $\{p_i, \hat{\rho}_i\}$

$$\hat{\rho} = \sum_i p_i \hat{\rho}_i$$

THIS COULD BE OF GREAT USE WHEN CONSIDERING THE STATE OF A MEASURED SYSTEM IN WHICH THE OUTCOME HAS BEEN LOST

$$\hat{\rho} \longrightarrow \sum_m p(m)\hat{\rho}_m = \sum_m \hat{M}_m \hat{\rho} \hat{M}_m^\dagger$$

WHEN DESCRIBING INTERACTING SYSTEMS, THE GLOBAL STATE IS GIVEN BY TENSOR PRODUCT OF INDIVIDUAL SYSTEMS

EXERCISE SHOW THAT A STATE IS PURE IIF ITS DENSITY OPERATOR SATISFIES $tr(\hat{\rho}^2) = 1$

SOL IT IS STRAIGHTFORWARD TO SEE THAT $\hat{\rho}$ IS A POSITIVE OPERATOR FOR ALL SYSTEMS BY THE SPECTRAL DECOMPOSITION THEOREM

$$\hat{\rho} = \sum_i \lambda_i |i\rangle\langle i| \quad \text{WITH} \quad \langle i|i'\rangle = \delta_{ii'} \;\&\; \sum_i \lambda_i = 1$$

SINCE $\hat{\rho}^2 = \sum_i \lambda_i^2 |i\rangle\langle i|$, AND

$$\left(\sum_i \lambda_i\right)^2 = \sum_i \lambda_i^2 + 2\sum_{j<i} \lambda_i \lambda_j = 1$$

IT IS CLEAR THAT $tr(\hat{\rho}^2) \leq 1$, FOR $\lambda_i \geq 0$ EQUALITY HOLDS IIF $\lambda_i \lambda_j = 0$ FOR $i \neq j$ THIS IS ONLY POSSIBLE IF $\lambda_i = 1$ FOR SOME i & $\lambda_j = 0$ FOR $j \neq i$ BUT THIS IS A PURE STATE'S DENSITY OPERATOR

EXAMPLE SHOW THAT AN ARBITRARY DENSITY MATRIX FOR A MIXED STATE QBIT MAY BE WRITTEN AS

$$\hat{\rho} = \frac{1 + \vec{r}\,\hat{\sigma}}{2}$$

SOL ALL DENSITY OPERATORS ARE POSITIVE DEFINITE, & HAVE TRACE ONE FOR A SINGLE QBIT, $\{\mathbb{I}, \hat{\sigma}_x, \hat{\sigma}_y, \hat{\sigma}_z\}$ ARE A BASE FOR THE SPACE OF OPERATORS SO, ALL QBIT OPERATORS CAN BE WRITTEN AS

$$\hat{\Delta} = \alpha 1 + \sum_i \tilde{r}_i \hat{\sigma}_i$$

SINCE A DENSITY OPERATOR IS HERMITEAN, α & $\tilde{r}_i$ ARE REAL THE TRACE CONSTRAINT IMPLIES $\alpha = 1/2$, FOR $\hat{\sigma}_i$ ARE TRACELESS THEREFORE, A DENSITY OPERATOR IS OF THE FORM

$$\hat{\rho} = \frac{1 + \sum_i \tilde{r}_i \hat{\sigma}_i}{2}$$

CONSIDERING THAT

$$\hat{\rho}^2 = \frac{1}{4}\left(1 + 2\sum_i \tilde{r}_i \hat{\sigma}_i + |\vec{r}|^2 1\right), \quad |\vec{r}|^2 = \sum_i \tilde{r}_i^2$$

IT MUST BE THAT

$$\frac{1}{4}\left(2 + 2|\vec{r}|^2\right) \leq 1$$

$$1 + |\vec{r}|^2 \leq 2$$

$$|\vec{r}|^2 \leq 1$$

IF A STATE IS PURE, $|\vec{r}|^2 = 1$, AND THUS

$$\tilde{r}_x = \sin\theta\cos\phi$$
$$\tilde{r}_y = \sin\theta\sin\phi$$
$$\tilde{r}_z = \cos\theta$$

THEREFORE $\vec{r}$ CORRESPONDS TO THE BLOCH VECTOR, WHICH REPRESENTS QBIT'S STATE ON BLOCH SPHERE THIS IS READILY SEEN BY COMPUTING $\hat{\rho}$ FOR A PURE STATE

$$\hat{\rho} = \left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right)\left(\cos\frac{\theta}{2}\langle 0| + e^{-i\phi}\sin\frac{\theta}{2}\langle 1|\right)$$

$$= \cos^2\frac{\theta}{2}|0\rangle\langle 0| + \sin^2\frac{\theta}{2}|1\rangle\langle 1| + e^{-i\phi}\sin\frac{\theta}{2}\cos\frac{\theta}{2}|0\rangle\langle 1| + e^{i\phi}\sin\frac{\theta}{2}\cos\frac{\theta}{2}|1\rangle\langle 0|$$

$$= \frac{1}{2} + \frac{1}{2}\left\{\cos\theta\,\tilde{\sigma}_z + \sin\theta\left(e^{-i\phi}|0\rangle\langle 1| + e^{i\phi}|1\rangle\langle 0|\right)\right\}$$

$$= \frac{1}{2} + \frac{1}{2}\left\{\cos\hat{\sigma}_z + \sin\theta\cos\phi\left(|0\rangle\langle 1| + |1\rangle\langle 0|\right) + \sin\theta\sin\phi\left(-i|0\rangle\langle 1| + i|1\rangle\langle 0|\right)\right\}$$

$$= \frac{1 + \vec{r}\,\hat{\sigma}}{2} \quad \text{WITH } \vec{r} \text{ AS MENTIONED BEFORE}$$

MATHEMATICAL TOOLS FOR COMPOSITE SYSTEMS → SOME OF THE MOST IMPORTANT TOOLS FOR TREATING COMPOSITE SYSTEMS ARE

1. PARTIAL TRACES
2. SCHMIDT DECOMPOSITIONS
3. PURIFICATIONS

PARTIAL TRACE → IT IS A LINEAR OPERATION THAT CONSISTS IN TRACING OUT A SYSTEM

$$tr_B(|a\rangle\langle a| \otimes |b\rangle\langle b|) = |a\rangle\langle a|\, tr(|b\rangle\langle b|)$$

$$tr_A(|a\rangle\langle a| \otimes |b\rangle\langle b|) = tr(|a\rangle\langle a|)\, |b\rangle\langle b|$$

FOR A COMPOSITE SYSTEM AB, FORMED BY SUBSYSTEMS A & B TRACING OUT SYSTEM A(B), LEADS TO A CORRECT DESCRIPTION OF OBSERVABLE QUANTITIES FOR SYSTEM B(A)

EXAMPLE FIND THE REDUCED DENSITY OPERATOR FOR BOTH QBITS ON A BELL PAIR

SOL CONSIDER A PAIR $|q_0 q_1\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

THE DENSITY OPERATOR ASSOCIATED TO THIS STATE IS

$$\hat{\rho} = \frac{1}{2}(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|)$$

IF THE SECOND QBIT IS TRACED OUT

$$\hat{\rho}_1 = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) = \frac{1}{2}$$

A MIXED STATE IN THE CENTER OF BLOCH SPHERE

EQUALY · $\hat{\rho}_2 = \frac{1}{2}$ THIS IS EASILY EXTENDED TO THE OTHER 3 STATES OF BELL'S BASIS FOR

$|q_0 q_1\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ IT IS CLEAR

$$\hat{\rho} = \frac{1}{2}(|01\rangle\langle 01| + |10\rangle\langle 01| + |01\rangle\langle 10| + |10\rangle\langle 10|)$$

SO THAT $\hat{\rho}_1 = \frac{1}{2}$ & $\hat{\rho}_2 = \frac{1}{2}$ THEREFORE, THE STATISTICS OF EACH OF THE QBITS ON AN ENTANGLED BELL PAIR IS IN A MIXED STATE WITH UNIFOR PROBABILITY OF BEING ON $|0\rangle$ OR $|1\rangle$! SUCH THE 2 QBIT STATE IS PURE, AND THUS WITH MAXIMAL KNOWLEDGE, SINGLE QBIT STATES HAVE MINIMAL KNOWLEDGE THIS IS A REMARKABLE FEATURE OF ENTANGLEMENT

SCHMIDT DECOMPS → IT IS A CONSEQUENCE OF A PROPERTY OF LINEAR SPACES CALLED SINGLE VALUE DECOMPOSITION

THIS PROPERTY STATES THAT ANY COMPLEX MATRIX CAN BE EXPRESSED AS THE PRODUCT OF UNITARY & DIAGONAL MATRICES AS A CONSECUENCE ANY COMPOSITE SYSTEM CAN BE EXPRESSED IN AN ORTHONORMAL BASIS WITH POSITIVE COEFFICIENTS

SUPPOSE AN m-DIMENSIONAL HILBERT SPACE $\mathcal{H}^m$, AND AN n-DIMENSIONAL HILBERT SPACE $\mathcal{H}^n$ CONSIDER AN ARBITRARY LINEAR OPERATOR $\hat{\Delta}\ \mathcal{H}^n \to \mathcal{H}^m$ LET $\{|i_m\rangle\}$ & $\{|i_n\rangle\}$, ORTHONORMAL BASIS ON $\mathcal{H}^n$ & $\mathcal{H}^m$ RESPECTIVELY THEN, IT IS CLEAR THAT

$$\hat{\Delta} = \sum_{ij} a_{ij} |i_m\rangle\langle j_n|$$

NOW, $\hat{\Delta}^+\hat{\Delta}$ & $\hat{\Delta}\hat{\Delta}^+$ ARE POSITIVE OPERATORS ON $\mathcal{H}^n$ & $\mathcal{H}^m$ RESPECTIVELY THEREFORE, THEIR EIGENBASIS ARE ORTHONORMAL THEN

$$\hat{\Delta}\hat{\Delta}^+ = \sum_i \lambda_{im}^2 |\lambda_{im}\rangle\langle\lambda_{im}| \quad , \quad \hat{\Delta}^+\hat{\Delta} = \sum_i \lambda'^2_{in} |\lambda'_{in}\rangle\langle\lambda'_{in}|$$

THEN $\hat{J} = \sqrt{\hat{\Delta}^+\hat{\Delta}} = \sum_i \lambda'_{in} |\lambda'_{in}\rangle\langle\lambda'_{in}|$ NOW CONSIDER THE ACTION OF $\hat{\Delta}$ ON THE BASIS $\{|\lambda'_{in}\rangle\}$

$$|i_m\rangle \in \mathcal{H}^m \ , \ |i_m\rangle = \hat{\Delta}|\lambda'_{in}\rangle$$

NOTICE $\langle i_m | j_m\rangle = (\langle\lambda'_{in}|\hat{\Delta}^+)(\hat{\Delta}|\lambda'_{jn}\rangle) = \lambda'^2_{in}\,\delta_{ij}$ HENCE $\{|\lambda_{in}\rangle\}$ IS MAPPED TO A SET OF ORTHOGONAL VECTORS ON $\mathcal{H}^m$ ALL $|\lambda'_{in}\rangle$ FOR WHICH $\lambda'^2_{in} = 0$ ARE MAPPED TO 0 DEFINE THE ORTHONORMAL SET $|\psi_{im}\rangle = (\lambda'_{in})^{-1}\hat{\Delta}|\lambda'_{in}\rangle$ FOR $\lambda'_{in} \neq 0$ AN ORTHONORMAL BASIS FOR $\mathcal{H}^m$ CONTAINING THIS SET COULD BE BUILT USING GRAM-SCHMIDT PROCEDURE WHEN EXPRESSED ON $\{|\psi_{im}\rangle\}$, $\{\lambda'_{in}\}$ $\hat{\Delta}$ IS REPRESENTED BY A DIAGONAL $m \times n$ MATRIX, PADDED WITH ZEROES FOR CONSISTENCY WHEN EXPRESSED ON AN ARBITRARY PAIR OF BASIS, THE OPERATOR $\hat{\Delta}$ CAN BE REPRESENTED BY THE MATRIX

$$\hat{\Delta} = \hat{U}_m^+ \; J_{m\times n} \; V$$

- $\hat{U}_m^+$: UNITARY CHANGE OF BASIS FROM $\{|\psi_{im}\rangle\}$
- $J_{m\times n}$: DIAGONAL REPRESENTATION IN $\{|\psi_{im}\rangle\}, \{|\lambda'_{in}\rangle\}$ OF $J = \sqrt{\hat{\Delta}\hat{\Delta}^+}$
- V: UNITARY CHANGE OF BASIS TO $\{|\lambda'_{in}\rangle\}$

THIS CORRESPONDS TO SINGULAR VALUE DECOMPOSITION OF AN OPERATOR NOW CONSIDER AN STATE OF A COMPOSITE SYSTEM

$$|\psi\rangle = \sum_{ij} a_{ij} |i\rangle|j\rangle$$

NOTICE THAT, BY SINGLE VALUE DE COMPOSITION

$$a_{ij} = \sum_{kl} u_{ik} d_{kl} v_{lj}$$

WITH u_{ik}, v_{lj} UNITARY MATRICES, s d_{kl} A mxn DIAGONAL MATRIX NOTICE THAT

$$\left\{ \sum_i u_{ik} |i\rangle = |k\rangle \right\}$$

$$\left\{ \sum_j v_{lj} |j\rangle = |l\rangle \right\}$$

ARE ORTHONORMAL BASIS FOR EACH COMPOUNDING SYSTEM ALSO, $d_{kl} \geq 0$ THEN

$$|\psi\rangle = \sum_{kl} d_{kl} |k\rangle|l\rangle$$

ALSO, SINCE $d_{kl} = d_k \delta_{kl}$

$$|\psi\rangle = \sum_k d_k |k\rangle|k\rangle$$

AND $\sum_k d_k^2 = 1$ d_k'S ARE NAMED SCHMIDT COEFFICIENTS THIS DECOMPOSITION IS OF CAPITAL IMPORTANCE SINCE IT SHOWS THAT PROPERTIES OF INTERACTING SYSTEMS THAT DEPEND ON THE EIGENVALUES OF THE REDUCED TRACE OPERATOR OF SINGLE SYSTEMS ARE THE SAME FOR ALL COMPOUNDING SYSTEMS IF THE COMPOSITE SYSTEM IS IN A PURE STATE

THE NUMBER OF NON-ZERO SCHMIDT VALUES IS CALLED **SCHMIDT NUMBER** THIS NUMBER A MEASURE OF THE "AMOUNT" OF ENTANGLEMENT

EXAMPLE FIND SCHMIDT DECOMPOSITIONS OF STATES

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} \;,\; \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}$$

SOL CONSIDER THE FIRST STATE SINCE

LET $|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$, $|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ THEN

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\left(|+_A\rangle|+_B\rangle + |-_A\rangle|-_B\rangle\right)$$

NOTICE IT IS ALREADY A SCHMIDT DECOMPOSITION

FOR THE SECOND STATE

$$\frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2} = |+_A\rangle|+_B\rangle$$

EXAMPLE SUPPOSE $|\psi\rangle$ & $|\phi\rangle$ ARE TWO PURE STATES OF A COMPOSITE QUANTUM SYSTEM WITH COMPONENTS A & B, WITH IDENTICAL SCHMIDT COEFFICIENTS SHOW THAT THERE ARE UNITARY TRANSFORMATIONS ON SYSTEM A & B SUCH THAT $|\psi\rangle = (U \otimes V)|\phi\rangle$

SOL SUPPOSE $|\psi\rangle = \sum_i \lambda_i |i_A\rangle|i_B\rangle$

$$|\phi\rangle = \sum_i \lambda_i |i'_A\rangle|i'_B\rangle$$

DEFINE $U = \sum_i |i_A\rangle\langle i'_A|$, $V = \sum_i |i_B\rangle\langle i'_B|$

THEN $(U \otimes V)|\phi\rangle = \sum_{ijk} \lambda_i |j_A\rangle|k_B\rangle\langle j'_A|i'_A\rangle\langle k'_B|i'_B\rangle$

$$= \sum_{ijk} \lambda_i \delta_{ji}\delta_{ki}|j_A\rangle|k_B\rangle = \sum_i \lambda_i |i_A\rangle|i_B\rangle$$

EXAMPLE PROVE THAT THE SCHMIDT NUMBER OF A COMPOUND STATE $|\psi\rangle$ IS EQUAL TO THE RANK OF THE REDUCED DENSITY MATRIX $\rho^A = tr_B(|\psi\rangle\langle\psi|)$

SOL FOR $|\psi\rangle$ A PURE STATE

$$|\psi\rangle\langle\psi| = \sum_{ij} \lambda_i \lambda_j (|i_A\rangle|i_B\rangle)(\langle j_A|\langle j_B|)$$

$$= \sum_{ij} \lambda_i \lambda_j (|i_A\rangle\langle j_A|)(|i_B\rangle\langle j_B|)$$

THEREFORE, $\rho^A = \sum_{ij} \lambda_i \lambda_j \delta_{ij} |i_A\rangle\langle j_A| = \sum_i \lambda_i^2 |i_A\rangle\langle i_A|$

HENCE, IT IS CLEAR THAT RANK OF ρ^A IS EQUAL TO THE SCHMIDT NUMBER OF $|\psi\rangle$

PURIFICATIONS ⟶ THEY ARE A TOOL THAT ALLOWS TRANSFORMING A SINGLE SYSTEM MIXED STATE INTO A COMPOUND SYSTEM PURE STATE

THE PRINCIPLE IS TO DIAGONALIZE THE DENSITY OPERATOR FOR SYSTEM A, AND TAKE ITS EIGENVECTORS AS ITS SCHMIDT BASIS IF

$$\rho^A = \sum_i p_i |i_A\rangle\langle i_A|$$

THEN A COMPOUNDING SYSTEM CAN BE APPENDED, WITH THE SAME STATE SPACE AS A THE SISTEM A & R CAN BE DESCRIBED BY THE STATE

$$|AR\rangle = \sum_i \sqrt{p_i} |i_A\rangle|i_R\rangle$$

NOTICE THAT TRACING OUT SYSTEM R, THE DENSITY OPERATOR FOR THE SYSTEM A IS RECOVERED

EXAMPLE SUPPOSE $\{p_i, |\psi_i\rangle\}$ IS AN ENSEMBLE OF STATES GENERATING DENSITY MATRIX $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ INTRODUCE A SYSTEM R WITH ORTHONORMAL BASIS $|i\rangle$ SHOW THAT $\sum_i \sqrt{p_i}|\psi_i\rangle|i\rangle$ IS A PURIFICATION OF ρ

SOL DEFINE $|AR\rangle = \sum_i \sqrt{p_i}|\psi_i\rangle|i\rangle$, THEN

$$\rho^{AR} = \sum_{ij} \sqrt{p_i p_j}\, |\psi_i\rangle\langle\psi_j| \otimes |i\rangle\langle j|$$

TRACING OUT SYSTEM R LEADS TO $\rho^A = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ AND THUS THIS IS A PURIFICATION

IF SYSTEM AR IS MEASURED ON $|i\rangle$ BASIS, THEN A SYSTEM IS LEFT ON STATE $|\psi_i\rangle$, WITH PROBABILITY p_i GIVEN THE FREEDOM ON PURIFICATIONS BY UNITARY TRANSFORMATIONS, IT IS ALWAYS POSSIBLE TO FIND ORTHONORMAL BASIS $|i\rangle$ FOR SYSTEM R SUCH THAT THE ABOVE STATEMENT IS TRUE

BELL INEQUALITIES $\longrightarrow$ CONSIDER OPERATORS DEFINED AS

$$\hat{Q} = \vec{q}\,\vec{\sigma}, \quad \hat{R} = \vec{r}\cdot\vec{\sigma}, \quad \hat{S} = \vec{s}\,\vec{\sigma}, \quad \hat{T} = \vec{t}\cdot\vec{\sigma}$$

CONSIDER A 2 QBIT SYSTEM, AND DEFINE OPERATOR

$$\hat{O} = \hat{Q}\otimes\hat{S} + \hat{R}\otimes\hat{S} + \hat{R}\otimes\hat{T} - \hat{Q}\otimes\hat{T}$$

GIVEN THAT

$$\begin{aligned}(\hat{Q}\otimes\hat{S} + \hat{R}\otimes\hat{S} + \hat{R}\otimes\hat{T} - \hat{Q}\otimes\hat{T})^2 = \\ 4\hat{1} + \hat{Q}\hat{R}\otimes\hat{1} + \hat{R}\hat{Q}\otimes\hat{1} + \hat{Q}\hat{R}\otimes\hat{S}\hat{T} \\ + \hat{R}\hat{Q}\otimes\hat{T}\hat{S} - \hat{1}\otimes\hat{S}\hat{T} - \hat{1}\otimes\hat{T}\hat{S} + \hat{1}\otimes\hat{S}\hat{T} \\ + \hat{1}\otimes\hat{T}\hat{S} - \hat{R}\hat{Q}\otimes\hat{S}\hat{T} - \hat{Q}\hat{R}\otimes\hat{T}\hat{S} - \hat{R}\hat{Q}\otimes\hat{1} \\ - \hat{Q}\hat{R}\otimes\hat{1} = 4\hat{1} + [\hat{Q},\hat{R}]\otimes[\hat{S},\hat{T}]\end{aligned}$$

AND $[\vec{\mu}\cdot\vec{\sigma}, \vec{\nu}\cdot\vec{\sigma}] = \left[\sum_i \mu_i \hat{\sigma}_i, \sum_j \nu \hat{\sigma}_j\right]$

$= \sum_{ij} \mu_i \nu_j [\hat{\sigma}_i, \hat{\sigma}_j] = 2i \sum_{ijk} \mu_i \nu_j \hat{\sigma}_k \epsilon_{ijk}$

$= 2i (\vec{\mu}\times\vec{\nu})\cdot\vec{\sigma}$

IT TURNS OUT THAT

$$\hat{O}^2 = 4\left(\hat{1}\otimes\hat{1} - (\vec{q}\times\vec{r})\vec{\sigma}\otimes(\vec{s}\times\vec{t})\vec{\sigma}\right)$$

NOTICE THAT $\hat{Q}^2$ IS MAXIMUM WHEN SPIN MEASUREMENTS ALONG AXES $\vec{q}\times\vec{r}$ AND $\vec{s}\times\vec{t}$ ARE ANTICORRELATED FOR A GIVEN STATE IN THAT CASE

$$\langle \hat{O}^2 \rangle_{MAX} = 8$$

IN GENERAL, $\langle \hat{Q} \rangle \leq \sqrt{\langle Q^2 \rangle}$ FROM PROBABILITY THEORY AND THUS

$$\langle \hat{Q}\otimes\hat{S} + \hat{R}\otimes\hat{S} + \hat{R}\otimes\hat{T} - \hat{Q}\otimes\hat{T} \rangle \leq 2\sqrt{2} = \sqrt{8}$$

SINCE ALL OPERATORS HAVING EIGENVALUES ± 1 ARE AKIN TO A π-RAD ROTATION AROUND SOME AXIS, IT IS STRAIGHT FORWARD TO SEE THAT THE ABOVE INEQUALITY HOLDS FOR ANY SET OF OPERATORS $\hat{Q}, \hat{R}, \hat{S}, \hat{T}$ THAT HAVE EIGENVALUES ± 1

IN GENERAL, FOR A SET OF MEASUREMENTS Q, R, S, T, WITH OUTCOMES ± 1 EACH, QUANTUM MECHANICS IMPOSES

$$\langle QS \rangle + \langle RS \rangle + \langle RT \rangle - \langle QT \rangle \leq 2\sqrt{2}$$

WHERE (FIRST) SECOND PROPERTY IS MEASURED ON THE (FIRST) SECOND QBIT

THAT MAXIMUM VALUE PREDICTED BY QUANTUM MECHANICS IS A CONSEQUENCE OF THE POSSIBILITY OF PERFECT ANTICORRELATION BETWEEN THE 2 QBITS THIS IS ACHIEVED, FOR EXAMPLE, BY THE PREPARATION OF A BELL STATE

CLASSICALY, ON THE OTHER HAND, THOSE ANTICORRELATIONS ARE LIMITED BY THE ASSUMPTION OF LOCAL REALISM THAT IS TO SAY, IF QBITS ARE FAR ENOUGH NO POSSIBLE CAUSAL RELATION CAN LEAD TO ANTICORRELATIONS LIKE THOSE PREDICTED BY Q M, AND BOTH HAVE DEFINED VALUES OF PROPERTIES Q, R, S, T

IF FOR EXAMPLE, A PAIR OF QBITS IS SENT TO 2 FAR AWAY LABS, ANY CLASSICAL THEORY WOULD PREDICT THAT

$$\langle QS \rangle + \langle RS \rangle + \langle RT \rangle - \langle QT \rangle \leq 2$$

GIVEN THAT, UNDER THE ASSUMPTION OF LOCAL REALISM, $QS + RS + RT - \langle QT \rangle \leq 2$ THIS BECAUSE ANTICORRELATIONS LIKE THOSE OF BELL STATES ARE FORBIDDEN BY THIS HYPOTHESIS

ALTHOUGH THE FULL PHISICAL UNDERSTANDING OF ENTANGLEMENT IS YET TO BE ACQUIRED IT IS AN IMMENSELY IMPORTANT RESOURCE FOR QUANTUM COMPUTATIONS AND INFORMATION.

FUNDAMENTALS OF COMPUTER SCIENCE

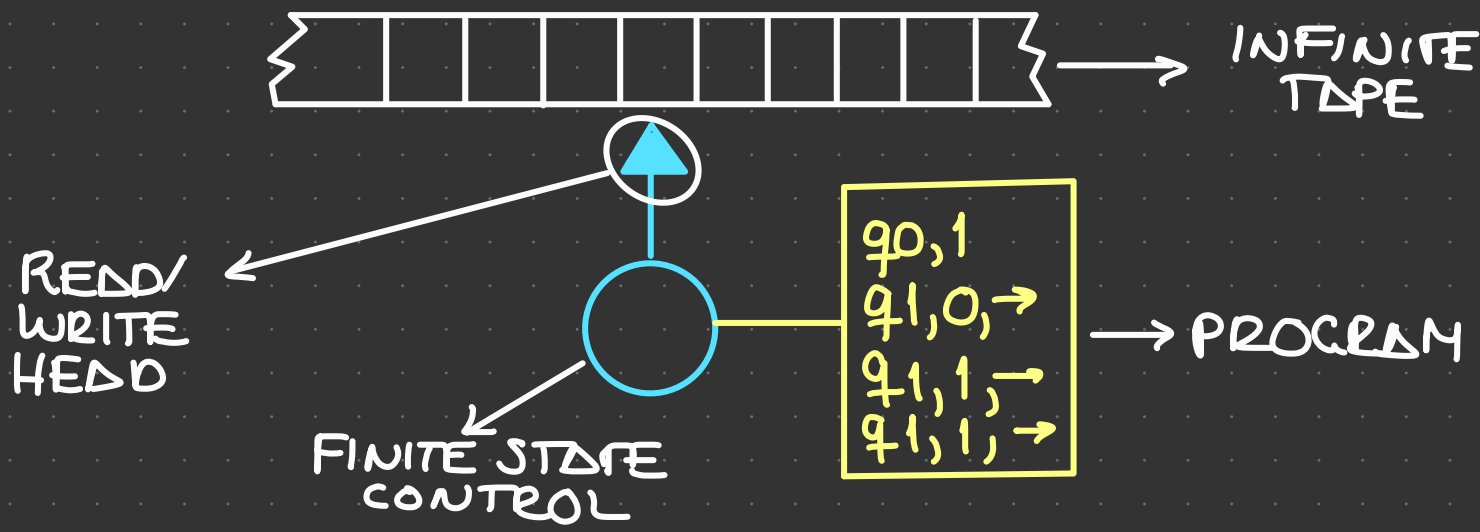
BEFORE ADDRESSING THE FUNDAMENTAL NOTIONS OF QUANTUM COMPUTING, THE FUNDAMENTAL IDEAS OF COMPUTER SCIENCE ARE REVISED

I SHALL FOCUS ON DISCUSSING TWO CLASSICAL MODELS OF COMPUTATION, AND THE BASIC NOTIONS OF COMPUTATIONAL COMPLEXITY FINALLY, I POINT OUT THE IMPORTANCE OF REVERSIBLE COMPUTATIONS BOTH FROM THE PERSPECTIVE OF CLASSICAL AND QUANTUM COMPUTING

MODELS OF COMPUTATION → THEY ARE PRECISE MATHEMATICAL FRAMEWORKS THAT CONDENSE THE NOTION OF ALGORITHM

I SHALL DISCUSS TWO MODELS TURING MACHINES AND LOGIC CIRCUITS

TURING MACHNS → THESE ARE SIMPLE MACHINES COMPOSED BY



THIS MACHINE LOOKS LIKE A PRIMITIVE COMPUTER

THE TAPE ACTS LIKE A MEMORY IN A COMMON COMPUTER

THE STATE CONTROL IS LIKE A PROCESSOR DEPENDING ON THE SYMBOL ON THE TAPE READ BY THE HEAD, AND ITS CURRENT STATE, IT CHANGES ITS STATE AND TELLS IT TO WRITE A SYMBOL ON THE TAPE FOLLOWING THE PROGRAM

THE PROGRAM OF A TURING MACHINE IS A SET OF INSTRUCTIONS OF THE FORM

$$(q, s) \longmapsto (q', s', M)$$

WHERE q, q' ARE STATES OF THE CONTROL s, s' ARE SYMBOLS ON THE TAPE, AND M IS A MOTION THAT CAN BE MOVE LEFT, RIGTH OR STAY THE INSTRUCTION TELLS THE STATE CONTROL TO

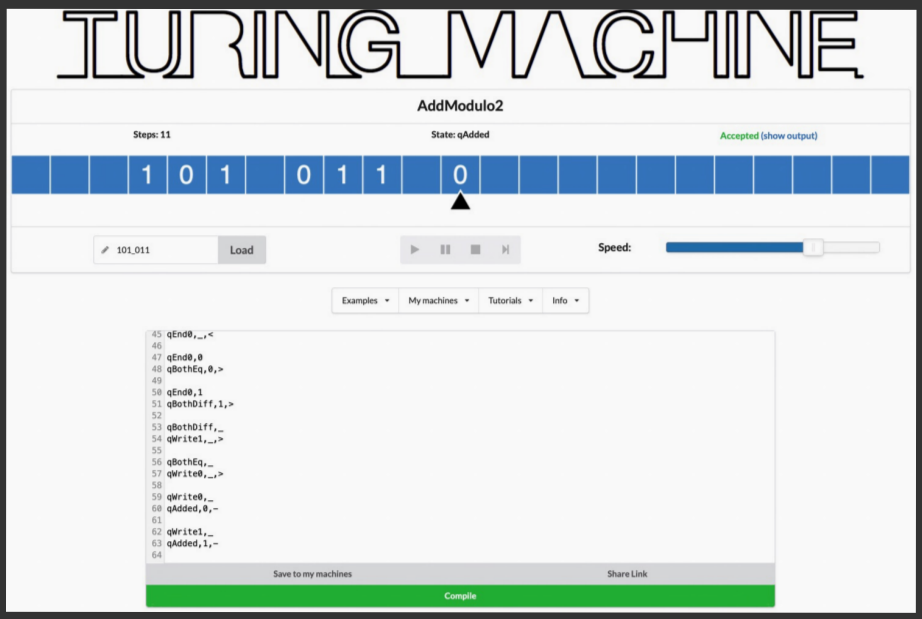
1. CHANGE ITS CURRENT STATE
2. TELL THE HEAD TO WRITE s' AT CURRENT POSITION
3. MOVE THE HEAD TO A NEW TAPE CELL

ALL THIS DEPENDING ON THE CURRENT STATE OF THE CONTROL AND THE SYMBOL READ AT THE CURRENT HEAD POSITION

ON TURINGMACHINESIMULATOR.COM EVERYONE CAN PLAY WITH TURING MACHINES THE PLATFORM ALLOWS SIMULATION OF MULTITAPE TURING MACHINES AS WELL

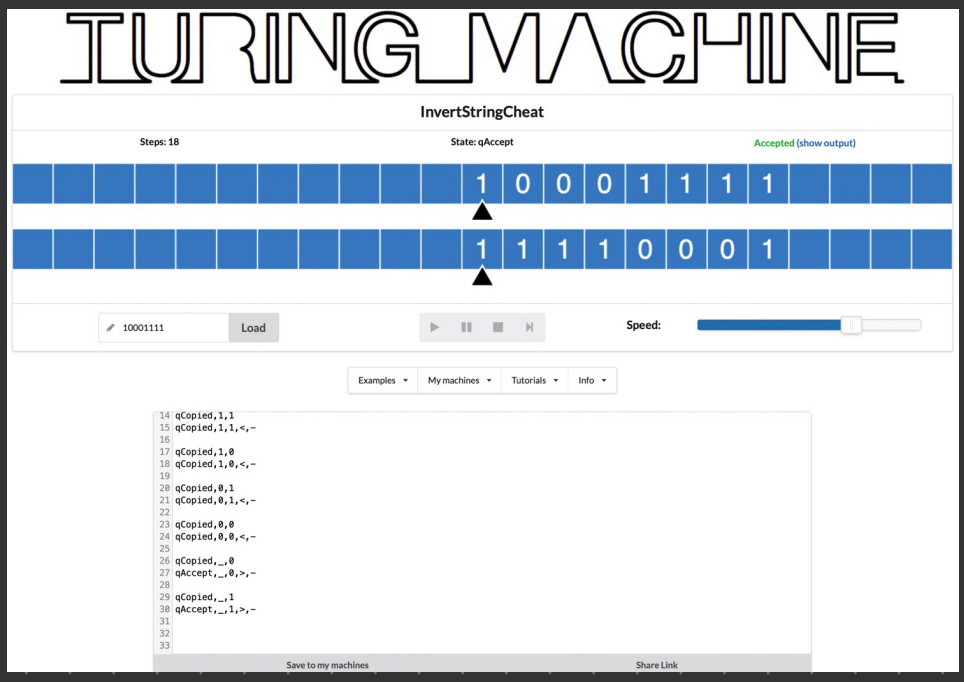
EXAMPLE BUILD A TURING MACHINE THAT IS CAPABLE OF ADDING 2 NUMBERS MODULO 2 YOU CAN USE A 2-TAPE MACHINE

SOL GO TO http://turingmachinesimulator.com/shared/vallmromip I INCLUDE A SCREENSHOT OF THE SIMULATOR



EXAMPLE BUILD A TURING MACHINE THAT REVERSES A BIT STRING

SOL FOR SIMPLICITY, I USE A 2-TAPE TURING MACHINE GO TO http://turingmachinesimulator.com/shared/pvzjkhhzyf TO SEE A POSSIBLE SOLUTION



A TURING MACHINE CAN BE USED TO COMPUTE ANY FUNCTION THAT WOULD BE REGARDED AS COMPUTABLE BY AN ALGORITHM THIS STATEMENT IS KNOWN AS THE CHURCH TURING THESIS THIS THESIS PUTS THE STUDY OF ALGORITHMS AND COMPUTATIONS IN THE REALM OF RIGUROUS MATHEMATICAL STUDY

QUANTUM MACHINES COMPUTE THE SAME CLASS OF FUNCTIONS AS TURING MACHINES THE DIFFERENCE IS EFFICIENCY

WITH THE AID OF CHURCH – TURING THESIS, IT IS POSSIBLE TO SPECIFY AN ALGORITHM USING PSEUDOCODE, TRUSTING IT CAN BE TRANSLATED INTO THE TURING MACHINE MODEL THIS ALLOS AVOIDING THE EXCRUCIATING PAIN OF HAVING TO BUILD A TURING MACHINE FOR EVERY ALGORITHM

AN INTEGER NUMBER, CALLED TURING NUMBER, MAY BE ASSOCIATED UNIQUELY TO A TURING MACHINE

A UNIVERSAL TURING MACHINE MAY BE BUILT SUCH THAT IT RECIVES AS INPUT ANOTHER MACHINES TURING NUMBER AND A STRING x ACCEPTABLE BY THE FORMER MACHINE THE UNIVERSAL TURING MACHINE WOULD OUTPUT THE SAME AS THAT OTHER MACHINE ON INPUT x

$$U(n_T, x) \longrightarrow T(x)$$

IT IS BELIEVED THAT THERE IS NO PHYSICAL WAY TO EXTEND THE CLASS OF FUNCTIONS COMPUTED IN THE TURING MACHINE MODEL NEITHER MULTITAPE TURING MACHINES NOR PROBABILISTIC TURING MACHINES DO THIS HOWEVER THEY MAY BE MORE EFFICIENT ON COMPUTING SOME FUNCTIONS

THE VERY IMPORTANT CONCEPT OF UNDECIDABILITY IS EMBODIED BY THE **HALTING PROBLEM** IT IS IMPOSSIBLE TO BUILD A TURING MACHINE THAT DETERMINES IF ANOTHER MACHINE WILL STOP A COMPUTATION ON A GIVEN INPUT, IN FINITE TIME

ALTHOUGH THE PRACTICAL IMPOSSIBILITY IS PROVING THAT A MACHINE LOOPS INDEFINITELY, THIS PROBLEM ILLUSTRATES THE EXISTANCE OF QUESTIONS SO DIFFICULT THAT ARE IMPOSSIBLE TO SOLVE BY TURING MACHINES

CIRCUIT MODEL ⟶ THIS MODEL OF COMPUTATION IS EQUIVALENT TO THE TURING MACHINE MODEL, BUT NEARER TO MODERN ELECTRONIC COMPUTING DEVICES

A CIRCUIT IS MADE OF **WIRES** AND **GATES** WIRES CAN BE IN EITHER OF 2 STATES, AND THUS ENCODES A **BIT** OF INFORMATION A SET OF WIRES ENCODES BINARY STRINGS

NUMBERS ARE STORED IN BINARY REPRESENTATION

$$N = \sum_i a_i 2^i \qquad a_i = 0,1$$

THE STATE OF A WIRE MIGHT HAVE DIRECT RELATION TO A PHYSICAL QUANTITY, LIKE VOLTAGE OR CURRENT

COMPUTATION OF LOGICAL FUNCTIONS OF THE FORM

$$f : \{0,1\}^n \longrightarrow \{0,1\}^l$$

IS PERFORMED BY A SEQUENCE OF ELEMENTARY LOGICAL OPERATIONS CALLED GATES

GATES OF THE FORM $f: \{0,1\} \to \{0,1\}$

NOT

a	$\bar{a}$
0	1
1	0

IDENTITY

a	a
0	0
1	1

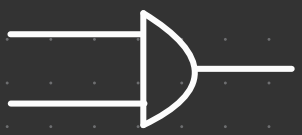
GATES OF THE FORM $f: \{0,1\}^2 \to \{0,1\}$

OR GATE

a	b	$a \vee b$
0	0	0
1	0	1
0	1	1
1	1	1

AND GATE

a	b	$a \wedge b$
0	0	0
1	0	0
0	1	0
1	1	1



XOR GATE

a	b	$a \oplus b$
0	0	0
1	0	1
0	1	1
1	1	0

NAND GATE

a	b	$a \uparrow b$
0	0	1
1	0	1
0	1	1
1	1	0

NOR GATE

a	b	$a \downarrow b$
0	0	1
1	0	0
0	1	0
1	1	0

OTHER IMPORTANT GATES

$f \quad a \longrightarrow (a,a)$

FANOUT

$f \quad (a,b) \longrightarrow (b,a)$

SWAP

THE AFORE MENTIONED GATES CAN BE USED TO COMPUTE ANY BOOLEAN FUNCTION

$$f \quad \{0,1\}^n \longrightarrow \{0,1\}$$
$$f(x_0, \ldots, x_n) \longrightarrow y$$

THIS IS EASILY SEEN BY INDUCTION

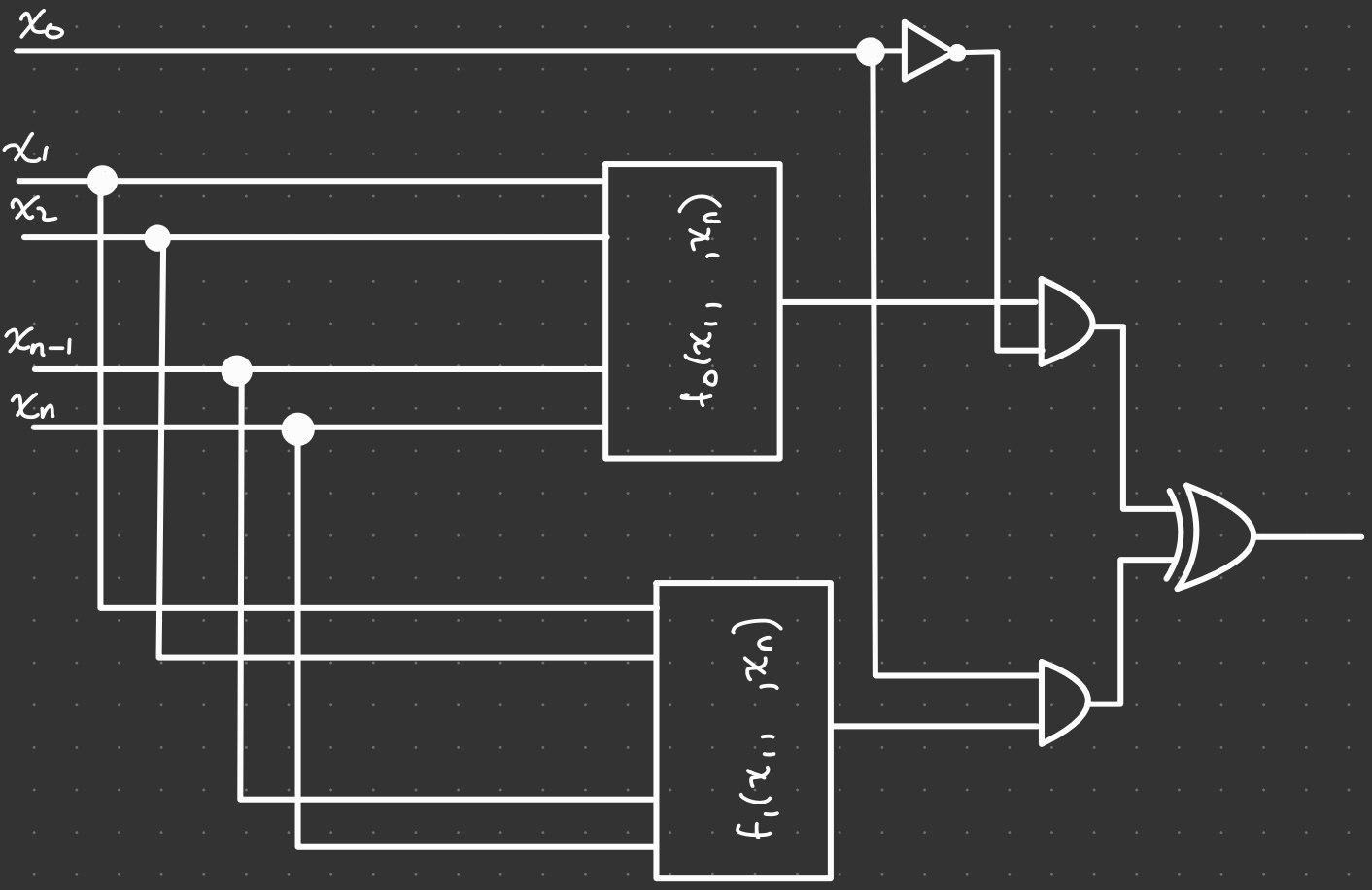
DEFINE $(n-1)$-BIT FUNCTIONS

$$f_0 \quad \{0,1\}^{n-1} \longrightarrow \{0,1\}$$
$$f(x_1, \ldots, x_n) \longrightarrow f(0, x_1, \ldots, x_n)$$

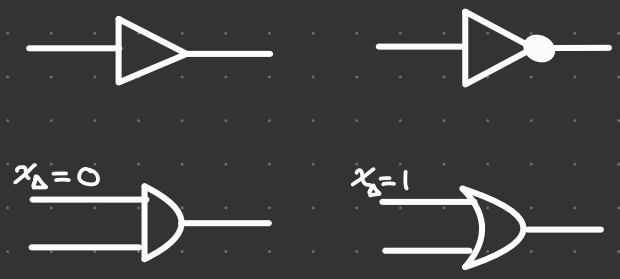
$$f_1 \quad \{0,1\}^{n-1} \longrightarrow \{0,1\}$$
$$f(x_1, \ldots, x_n) \longrightarrow f(1, x_1, \ldots, x_n)$$

FROM INDUCTION HYPOTHESIS, THERE ARE CIRCUITS THAT COMPUTE f_0 AND f_1

BY SCREENING WIRE WITH x_0 FOR CASES $x_0 = 1$ AND $x_0 = 0$, IT IS POSSIBLE TO BUILD AN n-WIRE (BIT) CIRCUIT THAT COMPUTES $f(x_0, \ldots, x_n)$ THIS IS ILLUSTRATED IN THE FOLLOWING CIRCUIT



FOR $n=1$, THE CONSTRUCTIONS ARE TRIVIAL SINCE THERE ARE ONLY 4 BOOLEAN FUNCTIONS, WHOSE CIRCUITS CAN BE BUILT EXPLICITLY

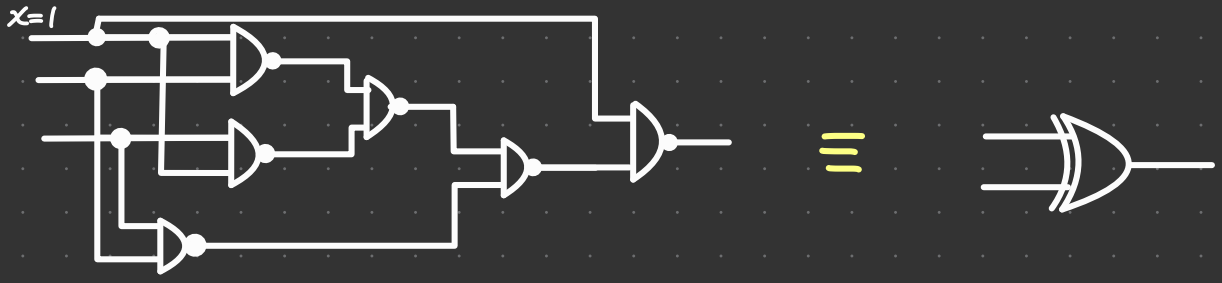


NOTICE THAT, APPART FROM THE GATES MENTIONED, ANCILLA BITS PREPARED ON STANDARD STATES ARE NEEDE FOR THIS UNIVERSAL CIRCUIT CONSTRUCTION

EXAMPLE SHOW THAT NAND AND FANOUT CAN BE USED TO SIMULATE AND, XOR, NOT GATES

SOL CONSIDER THE CASES

USING DE MORGAN'S LAWS



A **FAMILY OF CIRCUITS** IS A COLLECTION OF CIRCUITS $\{C_n\}$ THAT TAKE AS INPUT AN n-BIT STRING CIRCUIT FAMILIES ARE REQUIRED TO BE CONSISTENT A CIRCUIT C_m FROM THE FAMILY, ON INPUT x, A BT MOST m-BIT STRING, OUTPUTS THE SAME AS A CIRCUIT C_n FROM THE FAMILY IF $m < n$

A **UNIFORM CIRCUIT FAMILY** IS A FAMILY FOR WICH AN ALGORITHM RUNNING ON A TURING MACHINE EXISTS SUCH THAT IT GENERATES A DESCRIPTION OF A MEMBER CIRCUIT C_n ON INPUT C_n

THE CLASS OF FUNCTION COMPUTED BY UNIFORM CIRCUIT FAMILIES IS THE SAME AS THAT OF TURING MACHINES

COMPUTATIONAL COMPLEXITY → ANALYSIS OF COMPUTATIONAL PROBLEMS DEPENDS UPON 3 KEY QUESTIONS

1 WHAT IS A COMPUTATIONAL PROBLEM?

2 HOW MAY WE DESIGN ALGORITHMS TO SOLVE A GIVEN COMPUTATIONAL PROBLEM?

3 WHAT ARE THE MINIMAL RESOURSES REQUIRED TO SOLVE A GIVEN COMPUTATIONAL PROBLEM?

AS A FIRST APPROACH, COMPUTER SCIENTISTS FOCUS ON STUDYING THE SPECIAL CLASS OF DECIDABLE PROBLEMS THIS CLASS OF PROBLEMS ARE THOSE WHICH CAN BE RESTATED AS YES/NO QUESTIONS ON ITS INPUTS THE TECHNIQUES INVOLVED IN DESIGNING ALGORITHMS FOR SOLVING A GIVEN COMPUTATIONAL PROBLEM ARE THE FRUIT OF HARD WORK AND INGENUITY OF MANY RESEARCHERS THE AMOUNT OF RESOURCES EMPLOYED BY THE BEST OF THOSE ALGORITHMS IS QUANTIFIED IN TERMS OF SPACE, TIME AND ENERGY

QUANTIFICATION OF COMPUTATIONAL RESOURCES IS VITAL IN QUANTUM COMPUTING THIS PROCESS ASSUMES THAT THE NUMBER OF STEPS AND MEMORY UNITS TO SOLVE A PROBLEM ARE A FUNCTION OF THE INPUT SIZE THE MOST IMPORTANT ASPECT OF THIS FUNCTIONAL DEPENDENCE IS SUMMARISED BY ITS ASYMPTOTIC BEHAVIOR BIG O NOTATION IS USED TO SET UPPER BOUNDS TO THE AMOUNT OF RESOURCES NEEDED TO SOLVE A COMPUTATIONAL PROBLEM ON INPUT OF SIZE n

IN GENERAL, A COMPROMISE MUST BE MADE BETWEEN TIME, SPACE AND ENERGY

GIVEN 2 FUNCTIONS $f(n)$, $g(n)$, $f = O(g)$ IF THERE EXIST FINITE C_1, C_2 SUCH THAT, FOR $n \to \infty$, $C_1 \leq |f(n)/g(n)| \leq C_2$

TRACTABLE PROBLEMS ARE THOSE WHOSE REQUIRED RESOURCES SCALE AS A POLYNOMIAL FUNCTION OF THE INPUT SIZE THESE ARE EFFICIENTLY SOLVABLE

THE STRONG CHURCH-TURING THESIS STATES THAT ANY COMPUTATIONAL MODEL IS EFFICIENTLY SIMULATED BY A PROBABILISTIC TURING MACHINE THUS IF A PROBLEM IS NOT EFFICIENTLY SOLVABLE BY A PROBABILISTIC TURING MACHINE, IT IS NOT EFFICIENTLY SOLVABLE

QUANTUM MACHINES POSE A CHALLENGE TO THE STRONG CHURCH-TURING THESIS

PROBLEMS WHOSE RESOURCES SCALE FASTER THAN POLYNOMIAL ARE CONSIDERED DIFFICULT, INTRACTABLE OR INFEASABLE

REVERSIBLE COMPUTATION $\longrightarrow$ THE LEAST AMOUNT OF ENERGY CONSUMPTION IS REACHED BY REVERSIBLE COMPUTATIONS

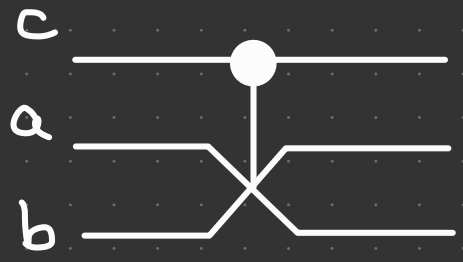
REVERSIBLE COMPUTATIONS ARE THOSE IN WHICH NO BIT OF INFORMATION IS ERASED ACCORDING TO LANDAUER'S PRINCIPLE ERASING A SINGLE BIT OF INFORMATION DISSIPATES AT LEAST $k_B T \ln 2$ UNITS OF ENERGY (T IS THE TEMPERATURE OF THE COMPUTER ENVIRONMENT)

THUS REVERSIBLE COMPUTATIONS ARE THE MOST EFFICIENT FROM A MATEMATICAL POINT OF VIEW, REVERSIBLE COMPUTATIONS ARE THOSE IN WHICH **INVERTIBLE FUNCTIONS** OF THE FORM

$$f\ \{0,1\}^m \longrightarrow \{0,1\}^m$$

ARE COMPUTED ANY FUNCTION CAN BE REVERSIBLY COMPUTED WITH THE AID OF **ANCILLA BITS** THE GATES NOT AND IDENTITY ARE REVERSIBLE HOWEVER, THE OTHER GATES ARE NOT REVERSIBLE

FREDKIN GATE (CSWAP) IS A 3-BIT GATE THAT IS CAPABLE OF SIMULATING ALL UNIVERSAL GATES, AND THUS IS THE ONLY MEMBER OF AN ALTERNATIVE UNIVERSAL SET

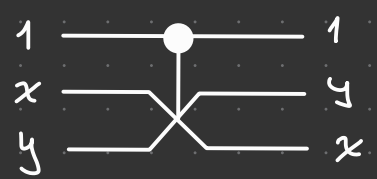


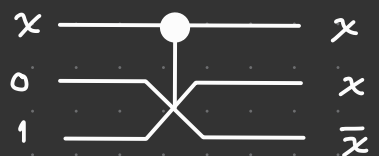
$$c' = c$$

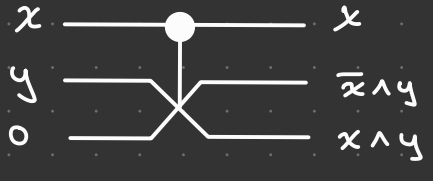
$$a' = \begin{cases} a, & c=0 \\ b, & c=1 \end{cases}$$

$$b' = \begin{cases} b, & c=0 \\ a, & c=1 \end{cases}$$

AS WAS PREVIOUSLY SHOWN, WITH NOT AND FANOUT, IT IS POSSIBLE TO SIMULATE ANY CIRCUIT GIVEN THAT

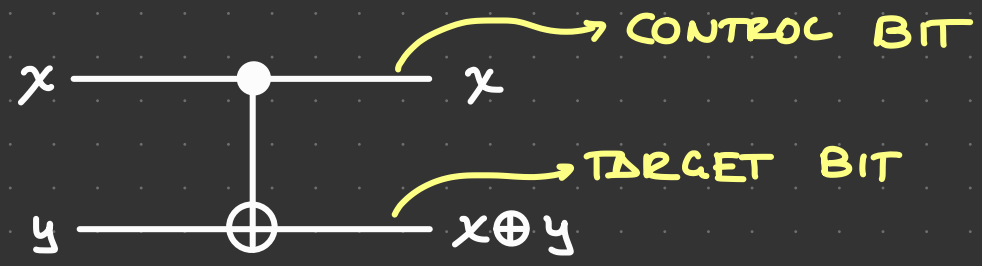




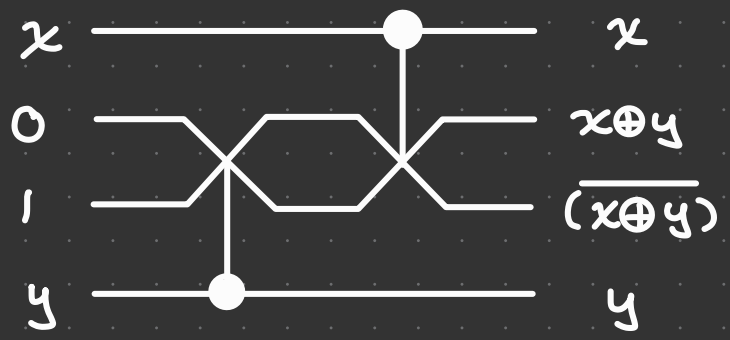


FREDKIN GATE PLUS ANCILLA BITS ARE ENOUGH TO SIMULATE ANY CIRCUIT IN A REVERSIBLE WAY HOWEVER, THE CIRCUIT ACCUMULATES A LOT OF **GARBAGE BITS** THAT MIGHT CAUSE TROUBLE WHEN MEASURING THE OUTPUT

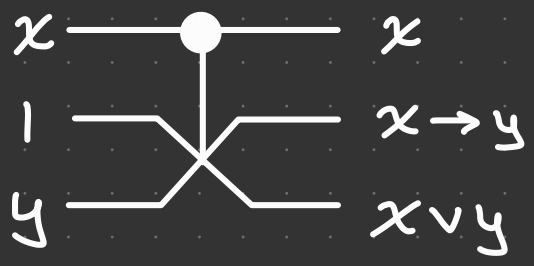
A VERY IMPORTANT REVERSIBLE GATE IS THE CNOT (OR REVERSIBLE XOR) THIS GATE IS REPRESENTED AS FOLLOWS



IT CAN BE SIMULATED BY FREDKIN GATES AS FOLLOWS



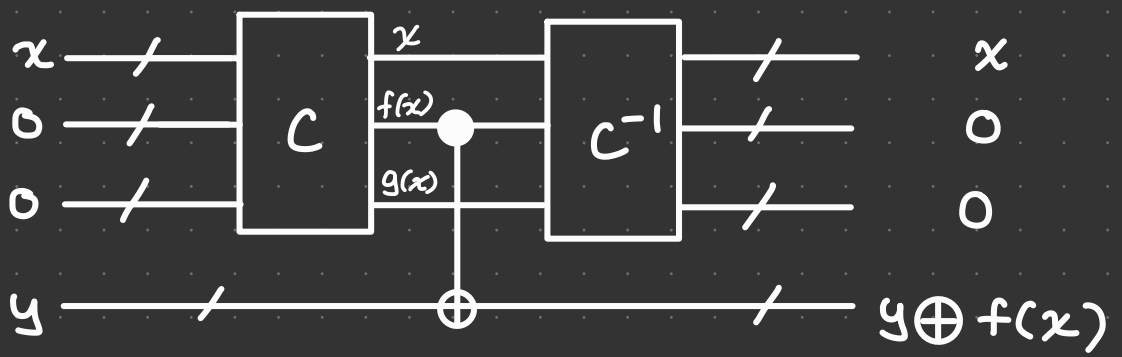
NOTE



WITH A CNOT GATE AVAILABLE, IT IS POSSIBLE TO UNCOMPUTE THE GARBAGE BITS THE PRINCIPLE IS TO USE 4 BIT REGISTERS

1 FOR THE INPUT STRING
2 FOR THE OUTPUT STRING
3 FOR THE GARBAGE BITS
4 FOR COPYING THE OUTPUT STRING

FIRST OF ALL, NOTICE THAT A CNOT WITH A TARGET BIT AT 0 IS A FANOUT (COPY) GATE THE IDEA IS TO APPLY THE CIRCUIT TO THE FIRST 3 REGISTERS, COPY THE OUTPUT TO THE COPY REGISTER AND UNDO THE CALCULATIONS ON THE FIRST 3 REGISTERS



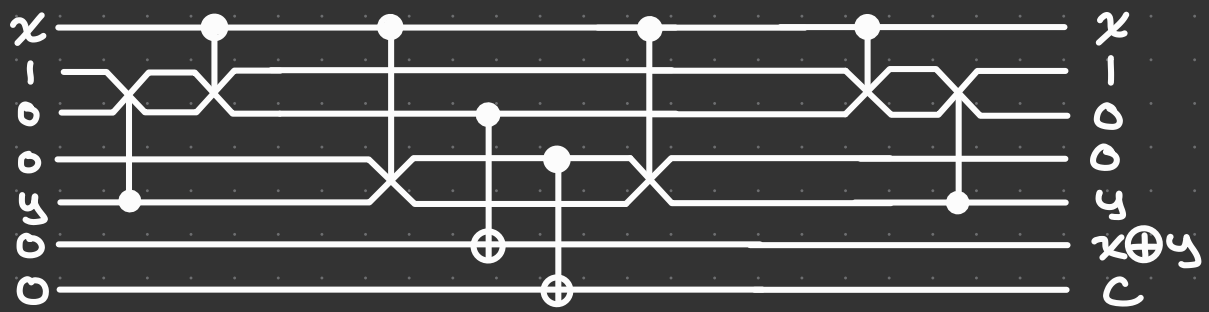
IN THE ABOVE (SOMEWHAT SIMPLIFIED) CIRCUIT, $g(x)$ DENOTES GARBAGE BITS, WHILE $f(x)$ IS THE FUNCTION TO BE COMPUTED

IMPORTANT XORING IS A COMMON TECHNIQUE USED IN COMPUTING FOR COPYING A REGISTER GIVEN THAT

$$(x \oplus y) \oplus y = x$$

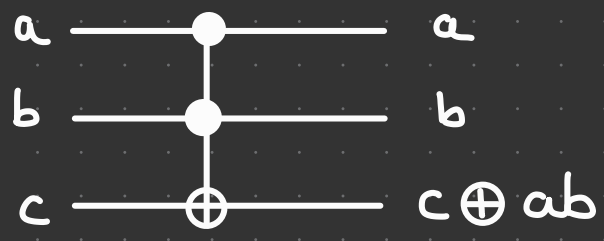
NOTE THAT, FOR THE SAKE OF COMPLEXITY ANALYSIS IF A COMPUTATION IS EFFICIENT WHEN PERFORMED IRREVERSIBLY, IT IS EFFICIENT WHEN COMPUTED REVERSIBLY THIS IS SO BECAUSE THE NUMBER OF REVERSIBLE GATES USED TO SIMULATE IRREVERSIBLE ONES IS PROPORTIONAL TO THE NUMBER OF IRREVERSIBLE GATES WITH A CONSTANT FACTOR AND THE NUBER OF ANCILLA BITS SCALE LINEARLY AT MOST WITH THE NUMBER OF IRREVERSIBLE GATES UNCOMPUTATION ADDS A FACTOR OF 2 (WICH IS IRRELEVANT) AND COPY OUTS ADD AT MOST A LINEAR CONTRIBUTION

EXAMPLE BUILD A REVERSIBLE HALF ADDER



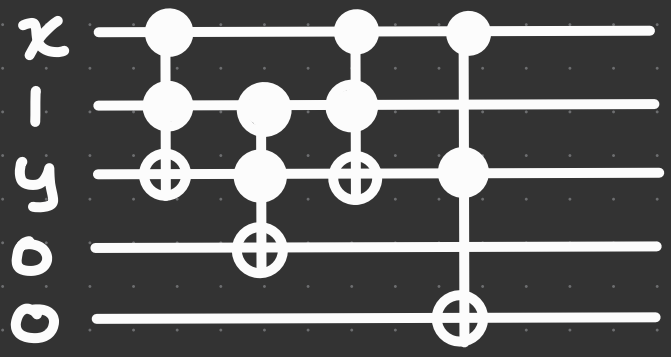
WHERE C IS THE CARRY BIT

ANOTHER IMPORTANT REVERSIBLE GATE IS THE TOFFOLI GATE (OR CCNOT GATE)



IT IS FAIRLY STRAIGHTFORWARD TO SEE THAT THIS GATE CAN BE USED TO SIMULATE NAND AND FANOUT THEREFORE, IT IS UNIVERSAL HENCE ANY CIRCUIT CAN BE SIMULATED EFFICIENTLY USING TOFFOLI GATES

EXAMPLE BUILD A HA USING TOFFOLI GATES



NOTICE THAT UNCOMPUTATION IS UNNECESSARY SOMETHING THAT CONTRASTS WITH FREDKIN-BASED IMPLEMENTATION

IMPORTANT GARBAGE BITS CAN BE RECYCLED FOR FURTHER USAGE THIS IS A QUITE RELEVANT ASPECT OF THE UNCOMPUTING TECHNIQUE DESCRIBED

TO HARNESS THE POWER OF QUANTUM COMPUTATION, CLASSICAL COMPUTATIONS MUST BE PERFORMED REVERSIBLY AND WITHOUT THE PRODUCTION OF GARBAGE BITS

QUANTUM CIRCUIT MODEL

LIKE CLASSICAL CIRCUITS, QUANTUM CIRCUITS ARE COMPOSED OF WIRES AND GATES HOWEVER, WIRES REPRESENT QBITS, AND GATES ARE UNITARY LINEAR OPERATORS ACTING ON A MULTI-QBIT SYSTEM

UNLIKE CLASSICAL GATES, SINGLE QBIT GATES ARE VERY DIVERSE NOT ONLY IS A NOT GATE AVAILABLE

$$\hat{X} = \hat{\sigma}_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

BUT ALSO A WHOLE RANGE OF UNITARY OPERATORS CAN BE GENERATED BY THE OTHER PAULI OPERATORS

$$\hat{Y} = \hat{\sigma}_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

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

PLUS THE IDENTITY OPERATOR TO PROVE THIS, NOTE THAT ANY OPERATOR CAN BE EXPANDED IN THE BASIS $\{1, \hat{\sigma}_i\}$

$$\hat{u} = \iota \hat{1} + \sum_i \alpha_i \hat{\sigma}_i$$

CONSIDER

$$\hat{u}^\dagger = \iota^* \hat{1} + \sum_i \alpha_i^* \hat{\sigma}_i$$

THEREFORE

$$\hat{u}+\hat{u} = (\lambda^* 1 + \Sigma_j \alpha_j^* \hat{\sigma}_j)(\lambda 1 + \Sigma_i \alpha_i \sigma_i)$$

$$= |\lambda|^2 1 + \sum_i (\lambda^* \alpha_i + \lambda \alpha_i^*) \sigma_i + \Sigma_{ij} \alpha_j^* \alpha_i \hat{\sigma}_j \hat{\sigma}_i$$

NOW, FROM THE IDENTITY

$$\hat{\sigma}_i \hat{\sigma}_j = \delta_{ij} 1 + i \Sigma_k \epsilon_{ijk} \sigma_k$$

$$\hat{u}+\hat{u} = (|\lambda|^2 + |\vec{\alpha}|^2)\, 1 + i \Sigma_{ijk} \alpha_j^* \alpha_i \hat{\sigma}_n \epsilon_{jik} + \Sigma_{ij} (\lambda^* \alpha_i + \lambda \alpha_i^*) \hat{\sigma}_i$$

$$= (|\lambda|^2 + |\vec{\alpha}|^2)\, 1 + \Sigma_i \left(\lambda^* \alpha_i + \lambda \alpha_i^* + i (\vec{\alpha}^* \times \vec{\alpha})_i \right) \hat{\sigma}_i$$

$$= (|\lambda|^2 + |\vec{\alpha}|^2)\, 1 + \left[2\,\mathrm{Re}(\lambda \vec{\alpha}) + i \vec{\alpha}^* \times \vec{\alpha} \right] \vec{\sigma}$$

UNITARITY IMPLIES

$$2\,\mathrm{Re}(\lambda^* \vec{\alpha}) = -i \vec{\alpha}^* \times \vec{\alpha}$$

$$|\lambda|^2 = 1 - |\vec{\alpha}|^2$$

DEFINE $|\lambda| = \cos\frac{\theta}{2}$

$$|\vec{\alpha}| = \sin\frac{\theta}{2}$$

THIS TRIVIALLY SATISFIES THE SECOND CONDITION AND THUS

$$\hat{U} = e^{i\delta}\cos\frac{\theta}{2}\,\mathbb{1} + \sin\frac{\theta}{2}\,\tilde{n}\cdot\hat{\sigma}$$

WHERE $\tilde{n}$ IS A COMPLEX (IN GENERAL) UNITARY VECTOR GIVEN THAT

$$\mathrm{Re}(\vec{\alpha}^* \times \vec{\alpha}) = [\mathrm{Re}(\vec{\alpha}) - i\,\mathrm{Im}(\vec{\alpha})] \times [\mathrm{Re}(\vec{\alpha}) + i\,\mathrm{Im}(\vec{\alpha})]$$

$$\mathrm{Re}(\vec{\alpha}^* \times \vec{\alpha}) = 2i\,\mathrm{Re}(\vec{\alpha}) \times \mathrm{Im}(\vec{\alpha})$$

$$\mathrm{Re}(\lambda^* \vec{\alpha}) = \mathrm{Re}(\lambda)\,\mathrm{Re}(\vec{\alpha}) + \mathrm{Im}(\lambda)\,\mathrm{Im}(\vec{\alpha})$$

THE FIRST CONDITION CAN ONLY BE SATISFIED IF $\lambda^* \vec{\alpha}$ IS PURELY IMAGINARY, AND

$$\mathrm{Re}(\vec{\alpha}) = C\,\mathrm{Im}(\vec{\alpha})$$

FOR SOME CONSTANT C THE LAST CONDITION IMPLIES

$$\tilde{n} = e^{i\gamma}\,\hat{n} \quad \text{WITH } \hat{n} \text{ REAL UNIT}$$

VECTOR THE FORMER CONDITION IMPLIES

$$e^{i(\gamma-\delta)} = -i$$

THEREFORE ANY UNITARY SINGLE QBIT OPERATOR (A SINGLE QBIT GATE) MAY BE REPRESENTED AS

$$\hat{U} = e^{i\delta}\left[\cos\frac{\theta}{2}\hat{1} - i\sin\frac{\theta}{2}\hat{n}\,\vec{\sigma}\right]$$

WITH $\hat{n}$ SOME REAL UNIT VECTOR NOTICE THAT

$$\exp\left(-i\frac{\theta}{2}\Delta\right) = \sum_n \frac{(-i)^{2n}}{(2n)!}(\Delta^2)^n + \sum_n \frac{(-i)(-i)^{2n}}{(2n+1)!}\Delta(\Delta^2)^n$$

IF $\Delta^2 = 1$, THEN

$$\exp\left(-i\frac{\theta}{2}\Delta\right) = \cos\frac{\theta}{2}1 - i\sin\frac{\theta}{2}\Delta$$

WITH $\Delta = \hat{n}\,\vec{\sigma}$, THIS LEMMA IMPLIES THAT ANY SINGLE QBIT GATE ON A CIRCUIT IS A COMBINATION OF A GLOBAL PHASE AND A ROTATION AROUND AN AXIS $\hat{n}$ OF AN ANGLE θ THE ROTATION REPRESENTED BY OPERATORS

$$R_{\hat{n}}(\theta) = \exp\left(-i\frac{\theta}{2}\hat{n}\,\vec{\sigma}\right)$$

IT IS VERY INTERESTING TO SEE WHAT A GENERAL GATE DOES TO A SINGLE QBIT ON A QUANTUM CIRCUIT TO DO THIS, REMEMBER THAT THE DENSITY OPERATOR OF ONE QBIT IS

$$\hat{\rho} = \frac{1 + \vec{r}\,\vec{\sigma}}{2}$$

WHERE $\vec{r}$ IS THE BLOCH VECTOR OF THE CURRENT QBIT STATE FROM TIME EVOLUTION POSTULATE, AFTER APPLYING A GATE, THE DENSITY OPERATOR EVOLVES AS

$$\hat{\rho}' = \hat{U}\hat{\rho}\hat{U}^{+}$$

$$= \frac{1 + R_{\hat{n}}(\theta)\left[\vec{r}\,\vec{\sigma}\right]R_{\hat{n}}(-\theta)}{2}$$

SINCE

$$\sum_{i,j} n_i r_j \sigma_i \sigma_j = \hat{n}\vec{r} + i(\hat{n}\times\vec{r})\,\vec{\sigma}$$

IT IS THAT

$$\hat{R}_{\hat{n}}(\theta)\left[\vec{r}\,\vec{\sigma}\right]R_{\hat{n}}(-\theta) =$$

$$\cos^2\frac{\theta}{2}\,\vec{r}\,\vec{\sigma} - i\sin\frac{\theta}{2}\cos\frac{\theta}{2}\left(\cancel{\hat{n}\vec{r}} + i\cancel{(\hat{n}\times\vec{r})}\,\vec{\sigma}\right)$$

$$+ i\sin\frac{\theta}{2}\cos\frac{\theta}{2}\left(\cancel{\hat{n}\vec{r}} - i\cancel{(\hat{n}\times\vec{r})}\,\vec{\sigma}\right)$$

$$+ \sin^2\frac{\theta}{2}\left((\hat{n}\vec{r})(\hat{n}\,\vec{\sigma}) - (\hat{n}\times\vec{r})\times\hat{n}\cdot\vec{\sigma}\right)$$

$$= \sin\theta\,(\hat{n}\times\vec{r})\,\vec{\sigma} + \cos^2\frac{\theta}{2}\left[\hat{n}(\vec{r}\,\hat{n})\,\vec{\sigma} + (\hat{n}\times\hat{r})\times\hat{n}\;\vec{\sigma}\right] + \sin^2\frac{\theta}{2}\left[\hat{n}(\vec{r}\,\hat{n})\,\vec{\sigma} - (\hat{n}\times\hat{r})\times\hat{n}\;\vec{\sigma}\right]$$

FROM DOUBLE ANGLE IDENTITIES.

$$= \left[\hat{n}(\hat{n}\cdot\vec{r}) + \sin\theta(\hat{n}\times\vec{r}) + \cos\theta(\hat{n}\times\vec{r}\times\hat{n})\right]\vec{\sigma}$$

THE QUANTITY ON BRACKETS CAN BE PROVEN TO BE A ROTATION OF BLOCH VECTOR $\vec{r}$ AN ANGLE θ (COUNTERCLOCKWISE) AROUND AXIS $\hat{n}$ THEREFORE

AN ARBITRARY SINGLE QBIT GATE CORRESPONDS TO A ROTATION AROUND AN AXIS IN BLOCH SPHERE

EXAMPLE PROVE THAT $\hat{X}\hat{Y}\hat{X} = -\hat{Y}$, AND THUS $\hat{X}R_{\hat{y}}(\theta)\hat{X} = R_{\hat{y}}(-\theta)$

SOL CONSIDERING

$$\hat{\sigma}_i\hat{\sigma}_j = \delta_{ij}\mathbb{1} + i\epsilon_{ijk}\hat{\sigma}_k$$

IT TURNS

$$\hat{\sigma}_x\hat{\sigma}_y = \epsilon_{xyk}\hat{\sigma}_k = i\hat{\sigma}_z$$
$$i\hat{\sigma}_z\hat{\sigma}_x = -\epsilon_{zxk}\hat{\sigma}_k = -\hat{\sigma}_y$$

THEREFORE $\hat{X}\hat{Y}\hat{X} = -\hat{Y}$ NOTICE

$$\hat{X}\hat{Y}^n\hat{X} = \underbrace{(\hat{X}\hat{Y}\hat{X})(\hat{X}\hat{Y}\hat{X})\quad(\hat{X}\hat{Y}\hat{X})}_{n\text{ TIMES}}$$

SINCE $\hat{X}^2 = \mathbb{1}$ THEFORE

$$\hat{X}\hat{Y}^n\hat{X} = (-\hat{Y})^n$$

AN IMMEDIATE COROLLARY IS $\hat{X}f(\hat{Y})\hat{X} = f(-\hat{Y})$ FROM WHICH IT FOLLOWS THE DESIRED RESULT

CONSIDER 2 GENERAL OPERATORS

$$R_{\hat{n}}(\theta) = \cos\frac{\theta}{2}\,1 - i\sin\frac{\theta}{2}\,\hat{n}\,\vec{\sigma}$$

$$R_{\hat{m}}(\tau) = \cos\frac{\tau}{2}\,1 - i\sin\frac{\tau}{2}\,\hat{m}\,\vec{\sigma}$$

THESE ARE ROTATIONS AROUND $\hat{n}$ AND $\hat{m}$ AXES, ANGLES θ AND τ, RESPECTIVELY. I WILL SHOW THAT ANY ROTATION OPERATOR $R_{\hat{\beta}}(\alpha)$ CAN BE COMPOSED AS A SEQUENCE OF ROTATIONS AROUND AXES $\hat{m}$ AND $\hat{n}$

$$R_{\hat{n}}(\theta)R_{\hat{m}}(\tau) = \cos\frac{\theta}{2}\cos\frac{\tau}{2}\,1 - i\sin\frac{\theta}{2}\cos\frac{\tau}{2}\,\hat{n}\,\vec{\sigma}$$
$$- i\sin\frac{\tau}{2}\cos\frac{\theta}{2}\,\hat{m}\,\vec{\sigma} - \sin\frac{\theta}{2}\sin\frac{\tau}{2}\,(\hat{n}\,\vec{\sigma})(\hat{m}\,\vec{\sigma})$$
$$= \left[\cos\frac{\theta}{2}\cos\frac{\tau}{2} - \sin\frac{\theta}{2}\sin\frac{\tau}{2}\,(\hat{n}\,\hat{m})\right]1$$
$$- i\left[\sin\frac{\theta}{2}\cos\frac{\tau}{2}\,\hat{n} + \sin\frac{\tau}{2}\cos\frac{\theta}{2}\,\hat{m} + \sin\frac{\theta}{2}\sin\frac{\tau}{2}\,(\hat{n}\times\hat{m})\right]\vec{\sigma}$$

NOTICE THAT $|\hat{n}\times\hat{m}|^2 = 1 - (\hat{n}\,\hat{m})^2$, AND THUS IT IS SO THAT

$$R_{\hat{n}}(\theta)R_{\hat{m}}(\tau) = R_{\hat{\ell}}(\beta)$$

WITH $\cos\frac{\beta}{2} = \cos\frac{\theta}{2}\cos\frac{\tau}{2} - \sin\frac{\theta}{2}\sin\frac{\tau}{2}(\hat{n}\,\hat{m})$

$$\sin\frac{\beta}{2}\,\hat{\ell} = \sin\frac{\theta}{2}\cos\frac{\tau}{2}\,\hat{n} + \sin\frac{\tau}{2}\cos\frac{\theta}{2}\,\hat{m} + \sin\frac{\theta}{2}\sin\frac{\tau}{2}\,(\hat{n}\times\hat{m})$$

THEREFORE, THE PRODUCT OF ROTATIONS IS ITSELF A ROTATION OPERATOR NOTICE THAT THE PRODUCT OF $R_{\hat{n}}(\theta) R_{\hat{m}}(\gamma)$ ONLY HAS 2 FREE PARAMETERS FOR FIXED AXES A GENERAL ROTATION HAS 3 PARAMETERS THEREFORE BY VARYING θ AND γ, ONLY A RESTRICTED SUBSET OF ALL ROTATION OPERATORS CAN BE GENERATED BY INTRODUCING ANOTHER ROTATION OPERATOR IN THE PRODUCT, $R_{\hat{m}}(\delta)$ OR $R_{\hat{n}}(\delta)$, AND VARYING THE ANGLES θ, γ, δ, IT IS POSSIBLE TO GENERATE ALL ROTATION OPERATORS

IT HAS BEEN SHOWN THAT

$$\hat{U} = R_{\hat{n}}(\theta) R_{\hat{m}}(\gamma)$$

IS A ROTATION OPERATOR WITH AXES

$$\hat{p} = \hat{p}(\theta, \gamma)$$

AND ANGLE OF ROTATION

$$\beta = \beta(\theta, \gamma)$$

THIS SET OF EQUATIONS CAN BE INVERTED ONLY FOR A RESTRICTED SET OF $\hat{p}$ AND β HOWEVER

$$\hat{U}' = R_{\hat{n}}(\theta) R_{\hat{m}}(\delta) R_{\hat{n}}(\gamma)$$

IS ALSO A ROTATION OPERATOR WITH AXIS AND ANGLE

$$\hat{p}(\theta, \delta, \gamma) \quad , \quad \beta = (\theta, \delta, \gamma)$$

THIS SET OF EQUATIONS IS INVERTIBLE FOR GIVEN $\hat{p}$ AND β AS A RESULT, ANY ROTATION OPERATOR CAN BE DECOMPOSED AS A PRODUCT

$$R_{\hat{p}}(\beta) = R_{\hat{n}}(\theta) R_{\hat{m}}(\delta) R_{\hat{n}}(\gamma)$$

FOR SOME VALUES OF θ, δ, γ AND FIXED AXIS $\hat{n}, \hat{m}$ THIS YIELDS A REMARKABLE COROLLARY

ANY SINGLE QBIT GATE CAN BE DECOMPOSED AS A SUCCESSIVE APPLICATION OF ROTATIONS AROUND 2 FIXED AXES, UP TO A GLOBAL PHASE FACTOR

A PARTICULAR IMPORTANT CASE IS THE X-Y DECOMPOSITION, WHICH STATES THAT A SINGLE QBIT GATE CAN BE DECOMPOSED AS A SEQUENCE OF ROTATIONS AROUND THE $\hat{x}$ AND $\hat{y}$ AXES ON BLOCH SPHERE

$$\hat{u} = e^{i\alpha} R_{\hat{x}}(\theta) R_{\hat{m}}(\delta) R_{\hat{n}}(\gamma)$$

A Z-Y DECOMPOSITION OF REMARKABLE IMPORTANCE STATES

$$\hat{u} = e^{i\alpha} R_{\hat{z}}(\theta) R_{\hat{y}}(\delta) R_{\hat{z}}(\gamma)$$

THIS SORT OF DECOMPOSITIONS ARE ONLY RESTRICTED BY THE REQUIREMENT THAT $\hat{n}$ AND $\hat{m}$ NOT BE PARALLEL

CIRCUIT MODEL $\longrightarrow$ IN THIS MODEL OF COMPUTATION, A WIRE REPRESENTS A QBIT AN ORTHONORMAL BASIS OF ITS SPACE CAN BE MAPPED TO BIT VALUES 0 OR 1 THIS MEANS THAT A MEASUREMENT IN THIS BASIS WOULD YIELD THE BIT VALUE, ANALOGOUS TO THE CLASSICAL MODEL

SUCH A BASIS WOULD BE CALLED **COMPUTATIONAL BASIS**, FOR OBVIOUS REASONS AS MENTIONED BEFORE, GATES CORRESPOND TO UNITARY OPERATORS FROM THE PRECEEDING DISCUSSION, QUANTUM GATES ARE FAR MORE DIVERSE THAN CLASSICAL GATES

SINGLE QBIT GATES EXTEND FAR BEYOND THE CLASSICAL NOT ALL POSSIBLE GATES CORRESPOND TO ROTATIONS IN BLOCH SPHERE, AND THUS ARE INFINITE IN # BEFORE DISCUSSING SOME IMPORTANT SINGLE QBIT GATES, I SHALL POINT OUT THAT THE FACT THAT QUANTUM GATES ARE UNITARY IMPLIES THAT **ALL QUANTUM COMPUTATIONS ARE REVERSIBLE** THIS IS A REMARKABLE FEATURE THAT MUST BE TAKEN INTO ACCOUNT WHEN DESIGNING QUANTUM ALGORITHMS

MULTIWIRE CIRCUITS CORRESPOND TO MULTI-QBIT SYSTEMS BY THE SAME TOKEN, MULTI-QBIT GATES ARE UNITARY OPERATORS ON A MULTIQBIT SPACE

SINGLE QBIT GATES ⟶ AS MENTIONED BEFORE, ALL UNITARY OPERATORS ARE ROTATIONS IN BLOCH SPHERE

THE SIMPLEST ARE THE OPERATORS

$$\hat{X} = R_{\hat{x}}(\pi) = \hat{\sigma}_x$$
$$\hat{Y} = R_{\hat{y}}(\pi) = \hat{\sigma}_y$$
$$\hat{Z} = R_{\hat{z}}(\pi) = \hat{\sigma}_z$$

NOTICE THAT BASES

$$\left\{\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\right\} \qquad \left\{\frac{1}{\sqrt{2}}(|0\rangle+i|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle-i|1\rangle)\right\} \qquad \{|0\rangle, |1\rangle\}$$

ARE EIGENBASIS OF GATES $\hat{X}, \hat{Y}, \hat{Z}$ RESPECTIVELY THIS IS EASILY SEEN BY CONSIDERING THE BLOCK VECTORS OF EACH STATEVECTOR IF

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

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$|+i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$$

$$|-i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$$

THEN, THE MENTIONED EIGENBASIS ARE

$$\{|+\rangle, |-\rangle\} \qquad \{|+i\rangle, |-i\rangle\} \qquad \{|0\rangle, |1\rangle\}$$

EACH OF THIS BASIS IS INVARIANT UNDER $\hat{X}$, $\hat{Y}$ AND $\hat{Z}$ GATES RESPECTIVELY

IMPORTANT I DELIBERATELY MISS THE GLOBAL PHASE FACTOR IN THE ROTATION REPRESENTATION OF $\hat{Z}, \hat{Y}, \hat{X}$ GIVEN THAT IT IS IRRELEVANT

NOTICE THAT $\hat{X}|0\rangle = |1\rangle$, $\hat{X}|1\rangle = |0\rangle$ AND THUS $\hat{X}$ IS THE QUANTUM EQUIVALENT OF A CLASSICAL NOT GATE

ALSO $\hat{Y}|0\rangle = i|1\rangle$ $\hat{Y}|1\rangle = -i|0\rangle$ THIS GATE ALSO ACTS LIKE A NOT, BUT ADDS AN EXTRA RELATIVE PHASE OF -1, WHICH CAN BE USEFUL IN SOME COMPUTATIONS

FINALY, $\hat{Z}|0\rangle = |0\rangle$, $\hat{Z}|1\rangle = -|1\rangle$, AND THUS IS NAMED 'PHASE GATE' IN SOME INSTANCES

THESE GATES ARE REPRESENTED AS

THE FOLLOWING GATES IN COMPLEXITY ARE THOSE THAT MAP BETWEEN THE BASIS

$$\{|0\rangle, |1\rangle\} \qquad \{|+\rangle, |-\rangle\} \qquad \{|+i\rangle, |-i\rangle\}$$

ALL THESE CORRESPOND TO A $\pi/2$ ROTATION IN BLOCK SPHERE AROUND AXES $\hat{x}, \hat{y}, \hat{z}$
A GATE THAT DOES THE MAPPING FROM COMPUTATIONAL BASIS TO $\{|+\rangle, |-\rangle\}$ BASIS IS THE SO CALLED HADAMARD GATE UNLIKE $R_{\hat{y}}(\pi/2)$, THIS GATE DOES NOT INTRODUCE RELATIVE PHASES π IS DESCRIBED BY

$$\hat{H} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$\hat{H}|0\rangle = |+\rangle$$
$$\hat{H}|1\rangle = |-\rangle$$

IT IS NOT DIFICULT TO SEE THAT THIS GATE IS A ROTATION IN BLOCH SPHERE AROUND AXIS $\frac{1}{\sqrt{2}}(\hat{x}+\hat{y})$, WITH ANGLE π HADAMARD GATE IS REPRESENTED AS

THIS GATE IS USEFUL FOR MEASURING ON $\{|+\rangle, |-\rangle\}$ BASIS, AND GENERATING SUPERPOSITION THIS IS VALUABLE FOR PROFITING QUANTUM PARLELISM AND PRODUCING ENTANGLEMENT

CHANGE OF BASIS PERFORMED BY A GATE $\hat{U}$ IS EQUIVALENT TO CHANGING OPERATORS AS

$$\hat{O}' = \hat{U}\hat{O}\hat{U}^{+}$$

THEREFORE, A SYSTEM CAN BE MEASURED ON ANOTHER BASIS DIFFERENT FROM COMPUTATIONAL BASIS BY JUST TRANSFORMING MEASUREMENT OPERATORS AS ABOVE

TO SIMPLIFY BY INSPECTION SOME CIRCUITS, IT IS USEFUL THE FOLLOWING IDENTITY

$$\frac{1}{\sqrt{2}}(\hat{\sigma}_x + \hat{\sigma}_z)\,\hat{\sigma}_i\,\frac{1}{\sqrt{2}}(\hat{\sigma}_x + \hat{\sigma}_z)$$

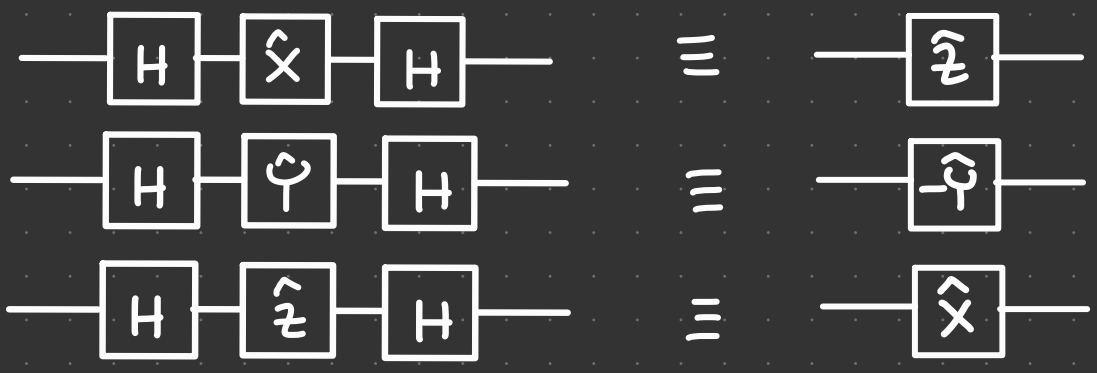
$$= \frac{1}{2}(\delta_{ix}\,\mathbb{1} + \delta_{iz}\,\mathbb{1} + i\epsilon_{xik}\hat{\sigma}_k + i\epsilon_{zil}\hat{\sigma}_l)(\hat{\sigma}_x + \hat{\sigma}_z)$$

$$= \frac{1}{2}\Big[(\delta_{ix} + \delta_{iz})(\hat{\sigma}_x + \hat{\sigma}_z) - \epsilon_{xik}\epsilon_{kxm}\hat{\sigma}_m - \epsilon_{xik}\epsilon_{kzm}\hat{\sigma}_m - \epsilon_{zil}\epsilon_{lxm}\hat{\sigma}_m - \epsilon_{zie}\epsilon_{izm}\hat{\sigma}_m\Big]$$

$$= \frac{1}{2}\Big[(\delta_{ix} + \delta_{iz})(\hat{\sigma}_x + \hat{\sigma}_z) - (1 - \delta_{ix})\,\delta_{im}\,\hat{\sigma}_m + \delta_{zi}\delta_{xm}\hat{\sigma}_m + \delta_{xi}\delta_{zm}\hat{\sigma}_m - (1 - \delta_{iz})\,\delta_{im}\,\hat{\sigma}_m\Big]$$

FOR $i = x, y, z$, THE FOLLOWING GATE IDENTITIES ARE OBTAINED

$$\hat{H}\hat{X}\hat{H} = \hat{Z}\,, \quad \hat{H}\hat{Y}\hat{H} = -\hat{Y}\,, \quad \hat{H}\hat{Z}\hat{H} = \hat{X}$$



THE BFORE MENTIONED IDENTITIES BRE OF GREAT IMPORTANCE, SINCE THEY IMPLY THAT

$$\hat{H} f(\hat{Z}) \hat{H} = f(\hat{X})$$

AND THUS ANY ROTATION AROUND $\hat{Z}$ AXIS IS TRANSFORMED TO A ROTATION AROND $\hat{X}$ AXIS BY A SANDWICH OF HADAMARD GATES

AS STATED BEFORE, GENERAL SINGLE QBIT GATES ARE ROTATIONS IN BLOCH SPHERE PLUS A GLOBAL PHASE COMMON GATES ARE ROTATIONS AROUND THE $\hat{Z}$ AXIS OF BLOCH SPHERE THE MOST USED ARE

$$\hat{S} = R_{\hat{Z}}(\pi/2) = e^{i\pi/4} \begin{bmatrix} e^{-i\pi/4} & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$$

$$\hat{T} = R_{\hat{Z}}(\pi/4) = e^{i\pi/8} \begin{bmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{i\pi/8} \end{bmatrix}$$

IMPORTANT EQUALITY SYMBOL $=$ MEANS EQUALITY UP TO A GLOBAL PHASE FACTOR

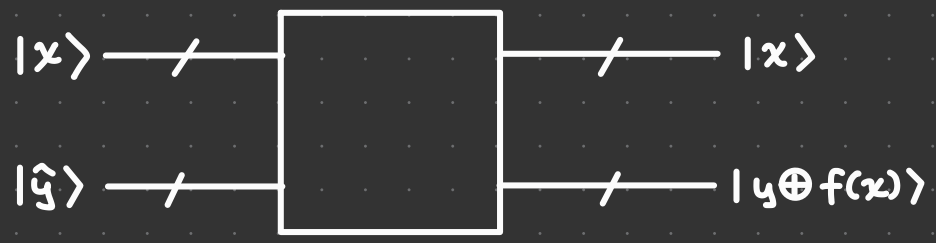
THE IMPORTANCE OF THE GATES S AND T IS THAT THEY COMPOSE THE Z GATE

$$\hat{S}^2 = \hat{T}^4 = \hat{Z}$$

THIS IS PARTICULARLY USEFUL FOR GENERATING MULTIQBIT CONTROLLED GATES ANALOGOUS TO CLASSICAL CONTROLLED GATES DISCUSSED BEFORE

MULTIQBIT GATES → UNLIKE CLASSICAL GATES, MULTIQBIT GATES DO NOT CORRESPOND DIRECTLY TO LOGICAL CONJUNCTIONS OR COMMON BOOLEAN OPERATORS ON 2 BITS

SINCE QUANTUM COMPUTING IS REVERSIBLE, MULTIQBIT GATES SHOULD BE OF THE FORM



IMPORTANT A CROSSED WIRE REPRESENTS MULTIPLE WIRES OR QBITS

THE SIMPLEST NON TRIVIAL MULTIQBIT GATE IS THE CNOT GATE IT HAS ALREADY BEEN DISCUSSED IN THE CONTEXT OF CLASSICAL COMPUTATIONS BEFORE INTRODUCING THIS GATE IT IS USEFUL TO DESCRIBE THE PHYSICAL INTUITION BEHIND A MULTIQBIT CIRCUIT

A MULTIQBIT CIRCUIT CORRESPOND TO A SYSTEM OF MULTIPLE QBITS THE STATE OF THE SET OF WIRES CORRESPONDS TO A STATE-VECTOR ON A MULTIDIMENSIONAL HILBERT SPACE IN FACT, THIS STATE IS

$$|a_0\rangle \otimes |a_1\rangle \otimes \quad \otimes |a_n\rangle = |a_0 a_1 \quad a_n\rangle$$

WITH $a_i = 0, 1$ MUCH LIKE CLASSICAL MULTIWIRE CIRCUITS, QUANTUM MULTIWIRE CIRCUITS ARE CAPABE OF COMPUTING FUNCTIONS

$$f \{0,1\}^n \longrightarrow \{0,1\}^m$$

ALL COMPUTATIONS SHOULD BE REVERSIBLE, WHICH IS NO RESTRICTION AT ALL HOWEVER DUE TO THE QUANTUM EVOLUTION OF A QUANTUM CIRCUIT SOME ADVANTAGES SHOULD BE RECOGNISED TO THIS MODEL

1 ALTHOUG THE COMPUTATIONAL BASIS OF AN n-WIRE QUANTUM CIRCUIT

$$|x\rangle \quad , \quad \text{WITH } x \text{ A } n\text{-BIT STRING}$$

HAS NO ADVANTAGE WITH RESPECT TO CLASSICAL n-BIT STATES, SUPERPOSITION OF QUANTUM STATES ALLOWS FOR NATIVE PARALLELISM OF QUANTUM COMPUTATIONS

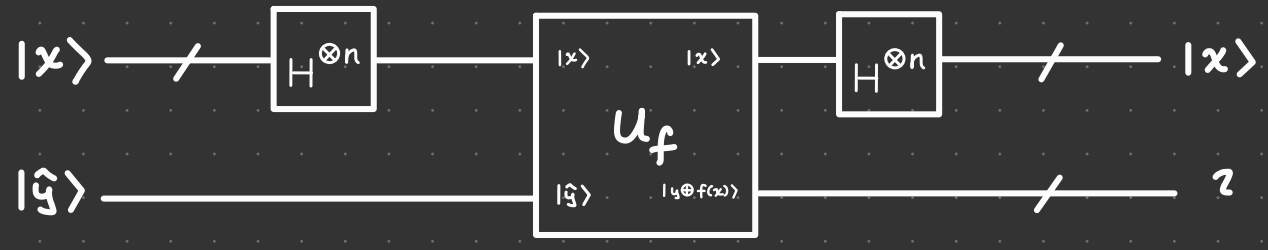
TO SEE THIS, RECALL THE DEFINITION OF HADAMARD TRANSFORM

$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_y (-1)^{x\,y} |y\rangle$$

WHERE $x\,y = x_1 y_1 \oplus x_2 y_2 \oplus \cdots \oplus x_n y_n$ NOTICE THAT

$$H^{\otimes n}|00\ldots0\rangle = \frac{1}{\sqrt{2^n}} \sum_y |y\rangle$$

SUPPOSE A CIRCUIT THAT REVERSIBLY COMPUTES A FUNCTION $f(x)$ IS GIVEN CONSIDER



THE ACTION OF THE CIRCUIT IS

$$|x\rangle|y\rangle \longrightarrow \sum_{zw} \frac{(-1)^{xz+zw}}{2^n}|w\rangle|y\oplus f(z)\rangle$$

DUE TO THE LINEARITY OF QUANTUM GATES ON ONE FUNCTION EVALUATION STAGE, IT IS POSSIBLE TO COMPUTE $f(z)$ FOR ALL VALUES OF z A CLASSICAL COMPUTATION WOULD REQUIRE AT LEAST $O(2^n)$ GATES TO PERFORM THIS TASK A QUANTUM COMPUTATION WOULD REQUIRE ONLY A IMPLEMENTATION OF THE HADAMARD TRANSFORM SINCE

$$H^{\otimes n} = \underbrace{H \otimes H \otimes H \otimes \quad \otimes H}_{n \text{ TIMES}}$$

IT IS POSSIBLE TO USE $O(n)$ GATES TO DO THE TRICK WITH A QUANTUM COMPUTATION THE CAVEAT IS THAT IT IS NOT POSSIBLE TO MEASURE ALL OUTCOMES AT THE SAME TIME THIS WOULD STILL REQUIRE AT LEAST $O(2^n)$ MEASUREMENTS IN THE COMPUTATIONAL BASIS OF THE INPUT WIRE STATE $|x\rangle$

HOWEVER GLOBAL PROPERTIES OF A BOOLEAN FUNCTION CAN BE DETERMINED WITH A SINGLE MEASUREMENT THIS IS ILLUSTRATED BY THE SOLUTION OF THE DEUTSCH-JOZA PROBLEM

CONSIDER A GATE THAT COMPUTES A FUNCTION

$$f \quad \{0,1\}^n \longrightarrow \{0,1\}$$

SUCH A FUNCTION IS SAID TO BE BALANCED IF THE OUTPUT IS 1 FOR 2^{n-1} n-BIT INPUT STRINGS AND 0 FOR THE REMAINING n-BIT STRS THE PROBLEM IS TO DETERMINE IF AN ARBITRARY FUNCTION IS EITHER BALANCED OR CONSTANT

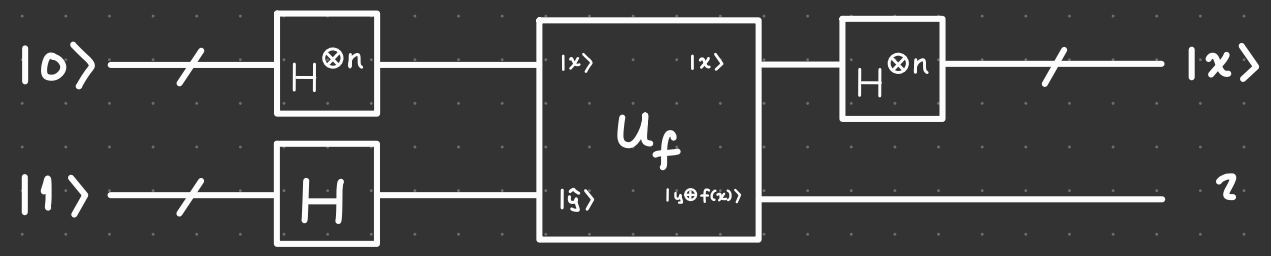
TO SOLVE THE PROBLEM, IT WOULD BE DESIRABLE TO PROFIT QUANTUM PARALLELISM ALSO, $|y\rangle$ REGISTER COULD BE USED TO "MEASURE" THE FUNCTION OUTCOME THIS CAN BE DONE BY NOTING THAT

$$0 \oplus f(x) = f(x) \qquad 1 \oplus f(x) = \overline{f(x)}$$

THE UPPER BAR INDICATES NEGATION SINCE $f(x)$ IS EITHER 0 OR 1, IT IS NOT HARD TO SEE THAT THE STATE

$$\frac{1}{\sqrt{2}}\left(|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle\right) = \frac{1}{\sqrt{2}}\left(|f(x)\rangle - |\overline{f(x)}\rangle\right) = (-1)^{f(x)}|-\rangle$$

GIVEN THAT A HADAMARD OPERATOR MAPS A QBIT IN $|1\rangle$ TO $|-\rangle$, IT IS CLEAR THAT BY INITALISING REGISTER $|y\rangle$ TO $|1\rangle$, IT IS POSSIBLE TO ENCODE $f(x)$ AS A PHASE DIFFERENCE ON THE OUTPUT STATE OF A FUNCTION EVALUATING CIRCUIT LIKE THE ONE SHOWN WHEN ILLUSTRATING QUANTUM PARALLELISM



THE OUTPUT OF THE ABOVE CIRCUIT IS

$$|0\rangle|1\rangle \longrightarrow \sum_{wz} \frac{(-1)^{f(z)+w\,z}}{2^n}|w\rangle|-\rangle$$

THIS IS READILY SEEN BY CONSIDERING THE STATE OF THE WIRES IMMEDIATELY AFTER THE APPLICATION OF U_f

$$|0\rangle|1\rangle \longrightarrow |\psi_i\rangle = \sum_z \frac{1}{\sqrt{2^n}} |z\rangle|-\oplus f(z)\rangle$$

WHERE $|-\oplus f(z)\rangle = \frac{1}{\sqrt{2}}(|0\oplus f(z)\rangle - |1\oplus f(z)\rangle)$

$$= (-1)^{f(x)}|-\rangle$$

THIS IS IMMEDIATE FROM SUPERPOSITION PRINCIPLE AT THIS STAGE THE FUNCTION EVALUATION RESULTS ARE STORED ON THE RELATIVE PHASES APPLYING HADAMARD TRANSFORM TO THE UPPER SET OF WIRES (REGISTER), THE CLAIMED RESULT IS OBTAINED

NOTE THAT THE FINAL STATE MIGHT BE REWRITTEN AS

$$|\psi_f\rangle = \left(\sum_w \mathcal{A}(w)|w\rangle\right) \otimes |-\rangle$$

WITH $$\mathcal{A}(w) = \sum_z \frac{(-1)^{f(z)+w\,z}}{2^n}$$

FOR $w = 00\ldots0$ $(|w\rangle = |0\rangle)$

$$\mathcal{A}(0) = \frac{1}{2^n}\sum_z (-1)^{f(z)}$$

IF $f(z)$ IS BALANCED, HALF $(-1)^{f(x)} = -1$ AND THE OTHER HALF $(-1)^{f(x)} = 0$ THUS $\mathcal{A}(0) = 0$
IF $f(x)$ IS CONSTANT $\mathcal{A}(0) = (-1)^{f(x)} = \pm 1$
FROM THE POSTULATES OF QUANTUM MECHANICS, IT IS IMPOSSIBLE TO MEASURE $|0\rangle$ ON THE INPUT REGISTER IF THE FUNCTION IS BALANCED IN THIS CASE, AT LEAST 1 QBIT MUST BE MEASURED WITH BIT VALUE 1 ON THE OTHER HAND, IF $f(x)$ IS CONSTANT $|0\rangle$ IS ALWAYS MEASURED, AND NO QBIT SHOULD BE SEEN WITH BIT VALUE 1

THUS MEASURING THE STATE OF $|x\rangle$ REGISTER ONCE ALLOWS FOR DETERMINATION OF A GLOBAL PROPERTY OF A FUNCTION IN THE CONTEXT OF THE DEUTSCH-JOZA PROBLEM THE PRESENTED SOLUTION IS KNOWN AS THE **DEUTSCH-JOZA ALGORITHM**

NOTICE THAT IF $f(x)$ IS UNKNOWN, I E U_f IS GIVEN BY SOME GOD IN A HIDDEN BOX, A CLASSICAL ALGORITHM WOULD NEED AT LEAST $2^{n-1}+1$ FUNCTION EVALUATIONS A QUANTUM ALGORITHM ONLY NEEDS 1 EVALUATION DUE TO QUANTUM PARALLELISM DERIVED FROM THE SUPERPOSITION PRINCIPLE

IMPORTANT SUCH U_f WHICH ARE GIVEN BY GODS ARE CALLED ORACLES, FOR IT IS NOT KNOWN HOW THEY WORK!!!

2 QUANTUM BITS CAN BE **ENTANGLED**, SOMETHING THAT CAN BE BOTH A BLESS AND A CURSE AS WAS SEEN BEFORE, ENTANGLEMENT ALLOS TRANSMISSION OF 2 BITS OF INFORMATION WITH THE TRANSMISSION OF 1 QBIT HOWEVER, ENTANGLEMENT IS AT THE HEART OF THE SO CALLED **NO CLONING THEOREM**, WHICH PREVENTS COPYING INFORMATION

CLASSICALY, COPYING IS PERFORMED BY A FANOUT GATE, WHICH MAY BE SIMULATED BY A CNOT GATE QUANTUM GATES, HOWEVER SHOULD CORRESPOND TO LINEAR OPERATORS SUPPOSE A QUANTUM FANOUT EXISTS AND NAME IT $\hat{U}$ THIS OPERATOR WOULD ACT THUSLY ON A PAIR OF QBITS

$$\hat{U}\,|0\rangle_1|\psi_0\rangle_2 = |0\rangle_1|0\rangle_2$$

$$\hat{U}\,|1\rangle|\psi_0\rangle_2 = |1\rangle_1|1\rangle_2$$

WHERE $|\psi_0\rangle$ IS JUST SOME INITIAL STATE OF THE COPY TARGET QBIT, SOMETHIN ANALOGOUS TO THE 0-INIT BIT IN A CLASSICAL CNOT

DUE TO LINEARITY, FOR ANY STATE OF THE FIRST QBIT

$$|\psi\rangle_1 = a|0\rangle + b|1\rangle$$

THE FINAL STATE OF THE SYSTEM ORIGINAL + COPY AFTER FANOUT IS

$$\hat{U}|\psi\rangle_1|\psi_0\rangle_2 = a|0\rangle_1|0\rangle_2 + b|1\rangle_1|1\rangle_2$$

THIS IS AN ENTANGLED STATE !!! THE ORIGINAL AND COPY QBIT ARE NOT INDEPENDENT, AND THUS THE QUANTUM FANOUT DOES NOT PRODUCE A COPY IN THE CLASSICAL SENSE FOR THIS TO HAPPEN THE FANOUT OUTCOME SHOULD BE

$$\hat{U}|\psi\rangle_1|\psi_0\rangle = |\psi\rangle_1|\psi_0\rangle$$

SOMETHING THAT IS AT ODDS WITH LINEARITY OF QUANTUM GATES LINEARITY IMPLIES THAT COPYING PRODUCES ENTANGLEMENT, IN GENERAL, AND THUS THE OUTCOMES ARE IRREMEDIABLY JOINED TOGETHER

"COPYING" A SUPERPOSITION STATE ALWAYS PRODUCES ENTANGLEMENT

ALTHOUGH THIS MAY APPEAR AS A PROBLEM AT FIRST, IT ALLOWS FOR TRANSPORTING QUANTUM STATES FROM 1 QBIT TO ANOTHER EVEN IN THE ABSENCE OF A QUANTUM COMMUNICATION CHANEL !!!

CONSIDER A PAIR OF ENTANGLED QBITS AND A THIRD QBIT, SO THAT THE SYSTEM STATE IS

$$|\psi\rangle = \frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle)(|00\rangle + |11\rangle)$$

SUPPOSE FURTHER THAT A THIRD PARTY GIVES ONE ENTANGLED QBIT TO EACH OF 2 SCIENTISTS AND THE OTHER QBIT TO ONE OF THEM THEY ARE NOT ABLE TO SEND QBITS, AND THE ONE WITH 2 QBITS HAS THE TASK TO SEND THE STATE OF THE NON ENTANGLED QBIT TO THE OTHER ONE

THE 2 QBIT SCIENTIST CAN ONLY OPERATE ON HIS QBITS AND ENTANGLEMENT IS THE KEY CONSIDER A SIMPLER SITUATION IN WHICH THE 2QBIT SCIENTIST WANTS TO COMMUNICATE THE STATE FROM 1 QBIT TO ANOTHER IT HAS BEEN SHOWN THAT SUCH A QUANTUM ALGORITHM SHOULD TRANSFORM THE STATE OF THE 2 QBITS THUSLY.

$$\hat{U}\,|\psi\rangle|\psi_0\rangle = \alpha|00\rangle + \beta|11\rangle$$

WITH $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ A MEASUREMENT OF THE FIRST QBIT ON THE COMPUTATIONAL BASIS WOULD DESTROY MOST OF THE INFORMATION ENCODED ON THE STATE FOR THE STATE TO BE COMMUNICATED, ENTANGLEMENT MUST BE BROKEN WITHOUT DESTROYING INFORMATION ON α OR β THIS CAN BE DONE BY MEASURING THE COPIED QBIT IN A BASIS DIFFERENT FROM COMPUTATIONAL

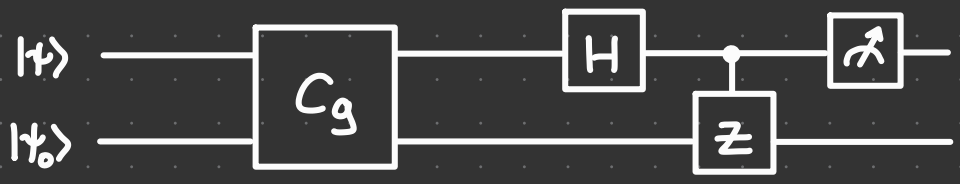
$$\alpha|00\rangle + \beta|11\rangle = \frac{\alpha}{\sqrt{2}}(|+\rangle + |-\rangle)|0\rangle + \frac{\beta}{\sqrt{2}}(|+\rangle - |-\rangle)|1\rangle$$

$$= \frac{1}{\sqrt{2}}|+\rangle\left(\alpha|0\rangle + \beta|1\rangle\right) + \frac{1}{\sqrt{2}}|-\rangle\left(\alpha|0\rangle - \beta|1\rangle\right)$$

IF THIS MEASUREMENT PRODUCES +, THEN THE STATE OF THE COPY IS PRECISELY THE PREVIOUS STATE OF THE COPIED QBIT IF THE OUTCOME IS −, THEN A PHASE SHIFT SHOULD BY APPLIED TO THE COPY TO FULLY RECOVER THE DESIRED STATE

THIS PROCEDURE SHOULD BE CALLED LOCAL TELEPORTATION IT IS A WAY TO BREAK THE ENTANGLEMENT GENERATED BY A QUANTUM COPYING PROCESS, AND COMMUNICATE A STATE WITHOUT DIRECT TRANSMISSION OF QUANTUM INFORMATION, BUT USING LOCAL INTERACTION

THIS OPERATION CAN BE SUMMARISED AS FOLLOWS



THE METER DENOTES MEASUREMENT ON COMPUTATIONAL BASIS THE GATE

DENOTES A CONTROLLED Z GATE THIS MEANS

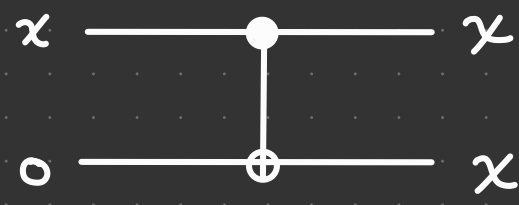
$$C(Z)\,|0\rangle|\psi\rangle = |0\rangle|\psi\rangle$$
$$C(Z)\,|1\rangle|\psi\rangle = |1\rangle(\hat{Z}|\psi\rangle)$$

FROM LINEARITY THE REST FOLLOWS ON THE SAME MANNER EXTEND CNOT GATE

$$C(\hat{X})\,|0\rangle|\psi\rangle = |0\rangle|\psi\rangle$$
$$C(\hat{X})\,|1\rangle|\psi\rangle = |1\rangle(\hat{X}|\psi\rangle)$$

IT IS NOT HARD TO SEE THAT THE LOCAL TELETRANSPORTATION PROCESS CAN BE REPRESENTED AS FOLLOWS

THIS FOLLOWS DIRECTLY FROM THE DISCUSSION OF THE SIMULATION OF FANOUT USING A CNOT GATE AND ITS QUANTUM EXTENSION

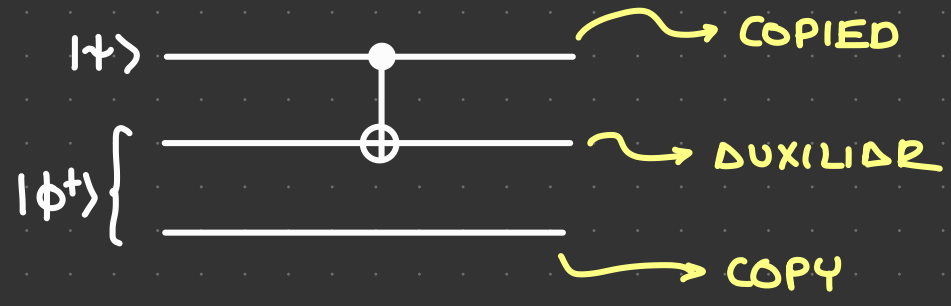


← CLASSICAL CNOT SIMULATING FANOUT

IMPORTANT MEASUREMENT CAN BE DELAYED !!!

CONSIDER NOW THE FULL SITUATION IN WHICH THE COPY QBIT IS FAR ENOUGH TO MAKE IMPOSSIBLE LOCAL INTERACTION THIS IS THE SITUATION OF THE 2 SCIENTISTS POSED BEFORE IF A THIRD QBIT ENTANGLED TO THE COPY QBIT IS GIVEN TO THE SENDER, IT COULD BE USED TO "MEDIATE" THE INTERACTION BETWEEN COPY QBIT AND COPIED QBIT

TO SEE THIS, CONSIDER THE OPERATION



THE AUXILIAR AND COPY ARE ON STATE

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

THE OPERATION THUS LEADS TO THE STATE

$$|\Psi\rangle = \alpha|0\rangle\left(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\right) + \beta|1\rangle\left(\frac{1}{\sqrt{2}}|10\rangle + \frac{1}{\sqrt{2}}|01\rangle\right)$$

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(\alpha|000\rangle + \beta|101\rangle\right) + \frac{1}{\sqrt{2}}\left(\alpha|011\rangle + \beta|110\rangle\right)$$

NOTICE THAT IF THE SECOND AUXILIARY QBIT IS MEASURED ON COMPUTATIONAL BASIS, THE TOTAL STATE VECTOR COLLAPSES TO

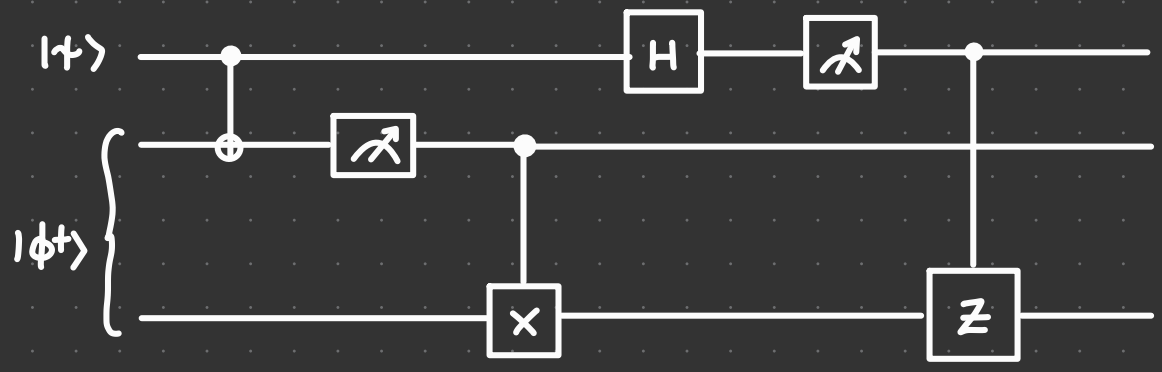
$\alpha|0\rangle_1|0\rangle_3 + \beta|1\rangle_1|1\rangle_3$ IF 2ND BIT = 0

$\alpha|0\rangle_1|1\rangle_3 + \beta|1\rangle_1|0\rangle_3$ IF 2ND BIT = 1

WITH A CONTROLLED BIT FLIP FROM THE 2ND BIT TO THE COPY QBIT, IT IS AS IF THE COPIED AND COPY QBIT WERE IN THE LOCAL TELETRANSPORTATION SITUATION

FOR THE FULL TELETRANSPORTATION ALGORITHM, GIVE THE SENDER OF THE STATE AND THE RECEIVER ONE OF AN ENTANGLED PAIR EACH THE SENDER APPLIES A CNOT TO HIS ENTANGLED QBIT, WITH THE COPIED STATE AS CONTROL THEN MEASURES THE ENTANGLED QBIT ON THE COMPUTATIONAL BASIS USING A CLASSIC CHANNEL, THE OUTCOME IS SEND TO THE RECEIVER IF 0, THE THE COPY QBIT IS LEFT INTACT, OTHERWISE, THE RECEIVER APPLIES A $\hat{X}$ GATE TO HIS/HER QBIT THIS ALLOWS USAGE OF THE LOCAL TELEPORTATION

THAT IS, THE COPIED QBIT IS MEASURED ON +,- BASIS, THE OUTCOME IS COMMUNICATED TO THE SENDER USING A CLASSICAL CHANNEL, AND A PHASE SHIFT WITH $\hat{Z}$ GATE IS PERFORMED DEPENDING ON THE OUTPUT THE WHOLE PROCESS IS DEPICTED BELOW.



IN SUMMARY, COPYING USING A QUANTUM ALGORITHM IS NOT COMPLETE EITHER ENTANGLEMENT IMPLIES THAT COPY AND COPIED QBITS ARE INSEPARABLY LINKED, OR, AS IN TELEPORTATION, THE ORIGINAL MUST BE DESTROYED HOWEVER, IN THE LAST CASE, THE REMARKABLE RESULT IS THAT A QUANTUM STATE CAN BE SENT USING A 2 BIT CLASSICAL CHANNEL, EVEN IN THE ABSENCE OF A QUANTUM CHANNEL

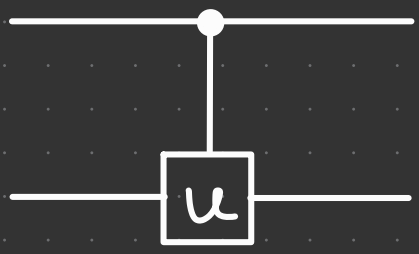
IMPORTANT NOTE THAT THE DIFFERENCE BETWEEN QUANTUM AND CLASSICAL COPYING IS MORE CLEAR ON THE DENSITY OPERATOR FORMALISM AFTER A COPY STAGE, THE STATE OF EACH QBIT IS A MIXED STATE THIS SHOWS THAT IT IS IMPOSSIBLE TO DESCRIBE THEM SEPARATELY

NOTE TO CREATE A BELL STATE USE

CONTROLLED OPERATIONS → THESE ARE THE MOST USEFUL OPERATIONS OF QUANTUM COMPUTING A CONTROLLED-U OPERATION IS A 2 QBIT OPERATION THAT HAS A CONTROL QBIT AND A TARGET QBIT THE ACTION IS AS FOLLOWS

$$C(u)\,|0\rangle|\psi\rangle = |0\rangle|\psi\rangle$$
$$C(u)\,|1\rangle|\psi\rangle = |1\rangle(u|\psi\rangle)$$

WHERE U IS A SINGLE QBIT GATE THE 1ST QBIT IS THE CONTROL, AND THE SECOND IS THE TARGET NOTE THAT THE ABOVE SET OF EQNS AND LINEARITY SPECIFY COMPLETELY THE ACTION OF 2 QBIT GATE C(U) IT IS REPRESENTED AS FOLLOWS



THE SIMPLEST ONE IS THE CNOT GATE, WICH IS SIMPLY C(X)

CONTROLLED GATES ARE THE EQUIVALENCE OF "IF-THEN" STATEMENTS IN MODERN PROGRAMMING LANGUAGES

EXAMPLE USE C(Z) AND H GATES TO SIMULATE A CNOT GATE

SOL USE IDENTITY $HZH = X$

THIS CAN BE SHOWN EASILY FOR THE STATES $|0\rangle|\psi\rangle$

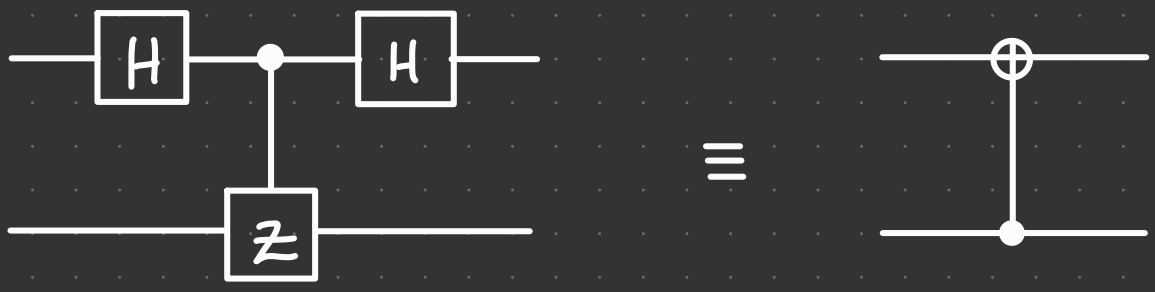
$$C(u)|0\rangle|\psi\rangle = |0\rangle(H^2|\psi\rangle) = |0\rangle|\psi\rangle$$
$$C(u)|1\rangle|\psi\rangle = |0\rangle(HZH|\psi\rangle) = |0\rangle(X|\psi\rangle)$$

EQUALLY IMPORTANT

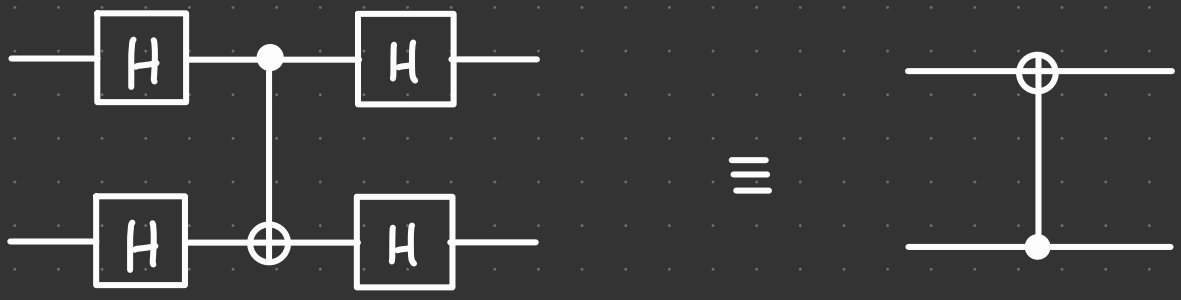
BY THE ACTION OF Z, IT IS CLEAR THAT

FOR THE RELATIVE PHASE IS ONLY ADDED TO STATE $|11\rangle$ AND ACTION ON AN ARBITRARY STATE FOLLOWS FROM LINEARITY

BY SANDWICHING THE PREVIOUS GATES USING HADAMARD GATES



FROM $H \times H = Z$, THEN



THIS IDENTITY IS VERY INTERESTING, FOR THE ACTION OF $H^{\otimes 2}$ ON STATES $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ IS TO CHANGE TO $\{|++\rangle, |+-\rangle, |-+\rangle, |--\rangle\}$ BOTH ARE ORTONORMAL BASIS THEREFORE, ABOVE CIRCUIT IDENTITY IS STATING THAT A CNOT IN COMPUTATIONAL BASIS IS A CNOT IN SIGN BASIS, BUT WITH TARGET AND CONTROL ROLES INVERTED !!!

THE ROLE OF CONTROL AND TARGET DEPENDS ON THE BASIS CONSIDERED

AN ARBITRARY CONTROLLED OPERATION MAY BE IMPLEMENTED USING ONLY SINGLE GATE OPERATIONS AND A CNOT

REMEMBER THAT ALL SINGLE QBIT GATES CAN BE EXPRESSED IN Z-Y DECOMPOSITION

$$\hat{U} = e^{i\alpha} R_{\hat{z}}(\beta) R_{\hat{y}}(\gamma) R_{\hat{z}}(\delta)$$

THE IDENTITY $XYX = -Y$ CAN BE PROFITED TO IMPLEMENT U, FOR A CNOT IS $C(X)$ IT IS DESIRABLE TO WRITE

$$U = e^{i\alpha} AXBXC$$

WITH $ABC = 1$ FOR THIS WOULD IMPLY THAT USING $C(X)$, $C(U)$ FOLLOWS DIRECTLY FROM THE DEFINITION OF ROTATIONS

$$A = R_{\hat{z}}(\beta) R_{\hat{y}}(\gamma/2)$$

$$B = R_{\hat{y}}\left(-\frac{\gamma}{2}\right) R_{\hat{z}}\left(-\frac{\beta+\delta}{2}\right)$$

$$C = R_{\hat{z}}\left(-\frac{\beta-\delta}{2}\right)$$

FOR THEN, $ABC = 1$, AND, SINCE

$$XBX = X R_{\hat{y}}(-\gamma/2) X X R_{\hat{z}}\left(-\frac{\beta+\delta}{2}\right) X$$

$$= R_{\hat{y}}(\gamma/2) \left[X R_{\hat{z}}\left(-\frac{\beta+\delta}{2}\right) X \right]$$

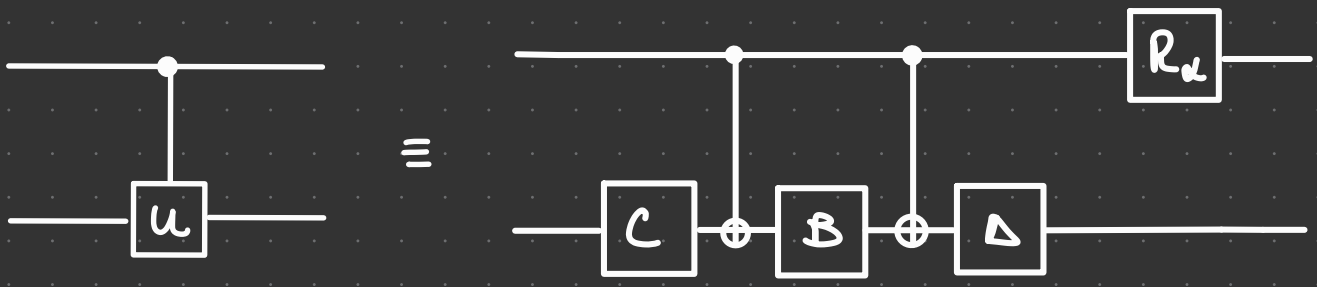
$$= R_{\hat{y}}(\gamma/2) R_{\hat{z}}\left(\frac{\beta+\delta}{2}\right) \quad XzX = -z$$

THEREFORE, IT IS STRAIGHTFORWARD TO SEE THAT ANY CONTROLLED OPERATION CAN BE IMPLEMENTED AS

IF $\alpha = 0$ SINCE CONTROLLED PHASE GATES CAN BE IMPLEMENTED BY ROTATIONS ON Z AXIS, DEFINED BY GATES

$$R_\phi = R_{\hat{z}}(\phi) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix}$$

IT IS EASY TO SEE THAT



EXAMPLE BUILD A C(H) GATE

SOL USE THE IDENTITY $H = e^{-i\pi/2} R_{\hat{y}}(\frac{\pi}{2}) R_{\hat{z}}(\pi)$ SO THAT

$$H = e^{-i\pi/2} R_{\hat{y}}(\pi/4) \times \left(R_{\hat{y}}(-\pi/4) R_{\hat{z}}(-\pi/2) \right) \times R_{\hat{z}}(\pi/2)$$

FROM DEFINITION OF S GATE

$$R_{\hat{z}}(-\pi/2) = e^{i\pi/4} S^\dagger$$

$$R_{\hat{z}}(\pi/2) = e^{-i\pi/4} S$$

AND THUS A POSSIBLE CIRCUIT THAT IMPLEMENTS C(H) IS

IS THIS THE BEST CIRCUIT? NOT NECESSARILY A BETTER ONE CAN BY FOUND BY FINDING V SUCH THAT $VXV^+ = H$ THIS IS EQUIVALENT TO $X = V^+HV$ IF $H = \cos\left(\frac{\theta}{2}\right)1 + i\sin\left(\frac{\theta}{2}\right)\vec{n}\,\vec{\sigma}$

AXIS $\hat{m}$ AND ANGLE ω SHOULD BE FOUND SUCH THAT:

$$\left(\cos\tfrac{\omega}{2}1 + i\sin\tfrac{\omega}{2}\hat{m}\,\vec{\sigma}\right) i\hat{x}\,\vec{\sigma}\left(\cos\tfrac{\omega}{2} - i\sin\tfrac{\omega}{2}\hat{m}\,\vec{\sigma}\right)$$

$$= \cos\tfrac{\theta}{2}1 + i\sin\tfrac{\theta}{2}\vec{n}\,\vec{\sigma}$$

CONSIDER

$$i\hat{x}\,\vec{\sigma}\left(\cos\tfrac{\omega}{2} - i\sin\tfrac{\omega}{2}\hat{m}\,\vec{\sigma}\right)$$

$$= i\cos\tfrac{\omega}{2}\hat{x}\,\vec{\sigma} + \sin\tfrac{\omega}{2}\left(\hat{m}\,\hat{x} + i(\hat{x}\times\hat{m})\,\vec{\sigma}\right)$$

$$= \hat{m}\,\hat{x}\sin\tfrac{\omega}{2} + i\left(\cos\tfrac{\omega}{2}\hat{x} + \sin\tfrac{\omega}{2}(\hat{x}\times\hat{m})\right)\vec{\sigma}$$

$$iVXV^+ = \tfrac{1}{2}\hat{m}\,\hat{x}\sin\omega - \tfrac{1}{2}\hat{m}\,\hat{x}\sin\omega$$

$$+ i\left(\cos^2\tfrac{\omega}{2}\hat{x} + \tfrac{1}{2}\sin\omega(\hat{x}\times\hat{m})\right)\vec{\sigma}$$

$$+ i\sin^2\tfrac{\omega}{2}\hat{m}\,\hat{x}\,(\vec{m}\,\vec{\sigma})$$

$$-i\sin\tfrac{\omega}{2}\left(\cos\tfrac{\omega}{2}\hat{m}\times\hat{x} + \sin\tfrac{\omega}{2}\hat{m}\times(\hat{x}\times\hat{m})\right)\vec{\sigma}$$

$$\imath V X V^{+} = \imath\left(\cos^2\frac{w}{2}\,\hat{x} + \sin w\ \hat{x}\times\hat{m} + \sin^2\frac{w}{2}(\hat{m}\ \hat{x})\,\hat{m} - \sin^2\frac{w}{2}\,\hat{m}\times(\hat{x}\times\hat{m})\right)\vec{\sigma}$$

$$V X V^{+} = (\cos w\ \hat{x} + \sin w\ \hat{x}\times\hat{m})\ \vec{\sigma}$$

BY CHOOSING $w = \pi/4$, $\hat{m} = \hat{y}$, HADAMARD GATE CAN BE BUILT AS

AS A MATTER OF FACT, IT HAS BEEN SHOWN THAT ANY π ROTATION GATE CAN BE CONTROLLED USING ONLY ONE CNOT GATE A $C(Y)$ MAY BE DEVISED SETTING $w = -\pi/2$, $\hat{m} = \hat{z}$

MORE GENERAL ROTATIONS NEED 2 CNOT GATES TO BE EFFECTIVELY IMPLEMENTED AS A CONTROLLED OPERATION

EXAMPLE SIMULATE A SWAP GATE USING CNOT

SOL A CLASSICAL ALGORITHM FOR SWAPPING BITS IS SIMPLY XORING IN SEQUENCE

$$x, y \xrightarrow[\text{CNOT}]{} x, y \oplus x \xrightarrow[\substack{\text{INV}\\ \text{CNOT}}]{} y, x \oplus y \xrightarrow[\text{CNOT}]{} y, x$$

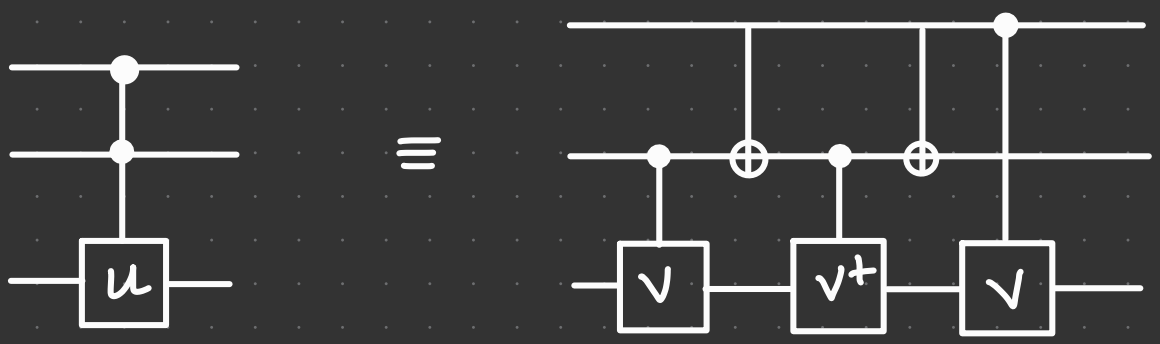
THIS ALGORITHM CAN BE GENERALISED IN A STRAIGHTFORWARD MANNER TO QUANTUM COMPUTING.

SUPPOSE A CIRCUIT WITH $n+k$ QBITS, AND U A k-QBIT GATE THE $C^n(U)$ OPERATION IS DEFINED BY

$$C^n(U)\,|x_1, x_2 \ldots x_n\rangle|\psi\rangle = |x_1 \ldots x_n\rangle\, U^{\pi_i x_i}\,|\psi\rangle$$

$x_1 \ldots x_n$ ARE CONTROL BITS IF ALL CONTROL BITS ARE 1, THEN U IS APPLIED TO THE OTHER k BITS

A $C^2(U)$ OPERATION CAN BE IMPLEMENTED EASILY IF THERE EXISTS V SUCH THAT $V^2 = U$ FOR THEN



THE GATE $C^2(X)$ CORRESPOND TO CLASSICAL TOFFOLI GATE GIVEN $R_{\hat{x}}(\pi) = R_{\hat{x}}(\pi/2)^2$, AND $R_{\hat{x}}(\pi) = iX$, BY CHOOSING

$$V = e^{-i\pi/4} R_{\hat{x}}(\pi/2)$$

IT IS POSSIBLE TO BUILD A QUANTUM TOFFOLY GATE USING THE CONSTRUCT INTRODUCED BEFORE SINCE CNOT AND SINGLE QBIT GATES CAN BE USED TO BUILD TOFFOLI GATE, THEY AND CNOT ARE UNIVERSAL FOR CLASSICAL COMPUTATIONS ALTHOUGH YET TO BE PROVEN IN THIS NOTES, THEY ARE UNIVERSAL FOR QUANTUM COMPUTATIONS AS WELL