Contents

1 Postulates

1.1 Quantum states

1.1.1 kets

- For $i \in \left[d = 2^N\right]$, $|i\rangle$ = the column vector which is 0 everywhere except for the i^{th} entry where it is 1 — we will actually use the binary representation of i as we will be using it to describe the observed states of a collection of N qbits (each of which collapses into either a 0 or a 1 when measured)

- For $\psi \in \mathbb{C}^d$, $|\psi\rangle = \sum_{i \in [d]} \psi_i \, |i\rangle$ i.e. **the column vector $\boldsymbol{\psi}$ — k̲et for c̲olumn**

- **Postulate 1: A quantum state $|\boldsymbol{\psi}\rangle$ is a vector of complex probabilities: $|\boldsymbol{\psi}\rangle \in \mathbb{C}^{\boldsymbol{d}}$ and $\sum_{\boldsymbol{i} \in [\boldsymbol{d}]} |\boldsymbol{\psi_i}|^{\mathbf{2}} = \mathbf{1}$** (or equivalently, $|\psi| = 1$)

- Observer effect: **We cannot directly observe $|\psi\rangle$, as when measured it collapses into a classical state $|i\rangle$ for some $i \in [d]$. In particular, each classical state $i \in [d]$ has probability $|\psi_i|^2$ of being observed when the quantum state $|\psi\rangle$ is measured**

1.1.2 bras

- For $\psi \in \mathbb{C}^d$, $\langle i| = \left(|i\rangle^T\right)^*$ = **the row vector of the conjugate of ψ — bra for row with an asterisk (conjugated)**

- **Proposition: $\langle i|M|j\rangle = M_{ij}$**. Note that this denotes $(\langle i| M)\,|j\rangle$ (or equivalently $\langle i|\,(M\,|j\rangle)$ as matrix multiplication is associative)
  Proof: Exercise

1.1.3 bra-kets

- For $u, v \in \mathbb{R}^d$, inner-product of u and $v = u \cdot v = \sum_{i \in [d]} u_i v_i = \left(u^T v\right) \in \mathbb{R}$
- Moreover, $|u| = \sqrt{u \cdot u} \in \mathbb{R}_{\geq 0}$
- **For $\boldsymbol{\psi, \phi \in \mathbb{C}^d}$, inner-product of $\boldsymbol{\psi}$ and $\boldsymbol{\phi} = \boldsymbol{\langle \psi | \phi \rangle} = \boldsymbol{\sum_{i \in [d]} (u_i)^* v_i = (\langle \psi | \, | \phi \rangle) \in \mathbb{C}}$** — note that this is right-associative
- Moreover, $|\psi| = \sqrt{\langle \psi | \psi \rangle} \in \mathbb{R}_{\geq 0}$ — note that this inner-product of a vector with itself is still always real
- Note that: $u \cdot v = v \cdot u$, whereas $\langle \psi | \phi \rangle = \langle \phi | \psi \rangle^*$
- *Proposition: If $\psi, \phi \in \mathbb{R}^d$ then $\langle \psi | \phi \rangle = \psi \cdot \phi$*
  Proof: Obvious
- We can take the outer-product (ket-bra) $|\psi\rangle \langle \phi|$ to get a matrix from 2 vectors instead of a scalar (the inner product (braket) $\langle \psi | \phi \rangle$)

1.2 Quantum operators

1.2.1 Quantum operators

- A quantum operator linearly transforms the state vector of its input to produce the state vector of its output. Thus, a quantum operator corresponds to a matrix (and so a geometric transformation to the basis of the state vector). That is that, **every quantum operator is entirely defined by how it affects the basis of its state vectors** (for example $|0\rangle$ and $|1\rangle$ for an operator that acts on a single qbit)

- Recall that a matrix M over the reals is orthogonal iff $M^T M$ (or equivalently MM^T) $= I$. **A matrix $\boldsymbol{U}$ is unitary iff $\boldsymbol{U^\dagger U}$ (or equivalently $\boldsymbol{UU^\dagger}$) $= \boldsymbol{I}$ where † denotes the conjugate transpose**

- **Postulate 2: The evolution of $|\boldsymbol{\psi}\rangle$ obeys $|\boldsymbol{\psi_{\text{out}}}\rangle = \boldsymbol{U}\,|\boldsymbol{\psi_{\text{in}}}\rangle$ where $\boldsymbol{U}$ is a unitary matrix**

- Every unitary matrix is a quantum gate (quantum operator), and vice versa

- Proposition: Let U be a unitary matrix. Then, $\psi' = U\psi$ and $\phi' = U\phi$ are orthogonal $\Leftrightarrow$ ψ and ϕ are orthogonal
  Proof: ψ' and ϕ' are orthogonal $\Leftrightarrow \langle U\psi | U\phi \rangle = 0 \Leftrightarrow \psi^\dagger U^\dagger U\phi = 0 \Leftrightarrow$ $\psi^\dagger I\phi \Leftrightarrow \langle \psi | \phi \rangle = 0 \Leftrightarrow \psi$ and ϕ are orthogonal

- Proposition: Transforming a vector by a unitary matrix does not affect the magnitude of the vector
  Proof: Let $M \in \mathbb{C}^{d\times d}$ be an arbitrary unitary matrix and $\psi \in \mathbb{C}^d$ be an arbitrary vector. Recall that $\forall\phi \in \mathbb{C}^d; |\phi|^2 = \phi^\dagger\phi$. Thus, $|M\psi|^2 =$ $(M\psi)^\dagger M\psi = \psi^\dagger M^\dagger M\psi = \psi^\dagger I\psi = |\psi|^2$. Thus, $|M\psi| = |\psi|$ as required

- Taking the two propositions above together, it is apparent why unitary matrices are appropriate to describe quantum gates (they preserve the orthogonality of the basis directions, and the normalisation of the state vectors)

- *Proposition: Let U be a unitary matrix. Then, every eigenvalue (which may be complex-valued) of U has magnitude 1*
  Proof: Exercise

1.2.2 Hermitian quantum operators

- Exactly as we could when doing linear algebra over the reals, we can consider a change of basis from $\{|0\rangle, |1\rangle\}$ to any set of linearly-independent orthonormal (pairwise orthogonal, and all normalised) vectors that span $\mathbb{C}^d$. Some quantum operators are more intuitive when seen in a different basis
- It can easily be seen that $\left\{|+\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}\mathbf{1}\\ \mathbf{1}\end{bmatrix}, |-\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}\mathbf{1}\\ \mathbf{-1}\end{bmatrix}\right\}$ is an alternative basis to $\{|0\rangle, |1\rangle\}$
- Recall that $\boldsymbol{M} = \begin{bmatrix}\boldsymbol{a} & \boldsymbol{b}\\ \boldsymbol{c} & \boldsymbol{d}\end{bmatrix} \Rightarrow \boldsymbol{M^{-1}} = \frac{1}{\boldsymbol{ad-bc}}\begin{bmatrix}\boldsymbol{d} & \boldsymbol{-b}\\ \boldsymbol{-c} & \boldsymbol{a}\end{bmatrix}$

- We call a real matrix M symmetric iff $M^T = M$. **We call a (possibly complex) matrix M self-adjoint (or Hermitian) iff $M^\dagger = M$**

- *Theorem (Spectral theorem): Every Hermitian matrix has real eigenvalues. Moreover, every Hermitian matrix of dimension $n \times n$ has n distinct orthogonal eigenvectors.*
  Proof:
  Let $v_1, v_2, \lambda_1, \lambda_2$ be arbitrary eigenvectors of a self-adjoint matrix M and their corresponding eigenvalues respectively.
  Real eigenvalues: $M|v_1\rangle = \lambda_1|v_1\rangle$. Thus, $\langle v_1| M|v_1\rangle = \langle v_1|\lambda_1|v_1\rangle = \lambda_1\langle v_1|v_1\rangle$ and so $\lambda_1 = \frac{\langle v_1|M|v_1\rangle}{\langle v_1|v_1\rangle}$. $\langle v_1|v_1\rangle \in \mathbb{R}$ is well-known, but the realness of the numerator will require an argument.
  $\langle v_1| M|v_1\rangle = \left(\langle v_1| M^\dagger|v_1\rangle\right)^* = (\langle v_1| M|v_1\rangle)^*$ as M is self-adjoint. Thus, as $\langle v_1| M|v_1\rangle = (\langle v_1| M|v_1\rangle)^*$, $\langle v_1| M|v_1\rangle \in \mathbb{R}$. Thus, λ_1 (which was arbitrary and so the same argument applies to every eigenvalue) is a ratio of two reals and so is itself real.

Orthogonal eigenvectors: $\langle Mv_1|v_2\rangle = \langle \lambda_1 v_1|v_2\rangle$. *Thus,* $\langle v_1| M^\dagger |v_2\rangle = \langle v_1| \lambda_1^* |v_2\rangle = \lambda_1 \langle v_1|v_2\rangle$ *using the previous part. As* M *is self-adjoint (and* v_2 *is an eigenvector),* $\langle v_1| \lambda_2 |v_2\rangle = \langle v_1| M |v_2\rangle = \lambda_1 \langle v_1|v_2\rangle$. *Thus,* $(\lambda_2 - \lambda_1)\langle v_1|v_2\rangle = 0$. *If* $\lambda_1 \neq \lambda_2$, v_1 *and* v_2 *are evidently orthogonal. Suppose however that* $\lambda_1 = \lambda_2 = \lambda$. *Then, consider* $|v_2'\rangle = |v_2\rangle + \langle v_2|v_1\rangle |v_1\rangle$. *Then,* $M|v_2'\rangle = \lambda_2|v_2\rangle + \lambda_1\langle v_2|v_1\rangle|v_1\rangle = \lambda|v_2\rangle + \lambda\langle v_2|v_1\rangle|v_1\rangle = \lambda|v_2'\rangle$ *and so* $|v_2'\rangle$ *is also an eigenvector. Moreover,* $\langle v_1|v_2'\rangle = \langle v_1|v_2\rangle + \langle v_2|v_1\rangle\langle v_1|v_1\rangle = \langle v_1|v_2\rangle - \langle v_1|v_2\rangle\langle v_1|v_1\rangle =$ *[assume wlog that* $\langle v_1|v_1\rangle = 1 / 0$ *and so* v_1, v_2' *are orthogonal*
Exercise: Use induction to extend to to $n > 2$

- Lemma:
  i) If M is self-adjoint, then (M is unitary $\Leftrightarrow M^2 = I$)
  ii) If $M^2 = I$, then (M is unitary $\Leftrightarrow M$ is self-adjoint)
  Proof:
  i) $\Leftarrow$: $M^2 = MM^\dagger = I$
  $\Rightarrow$: $I = M^2 = MM^\dagger$
  ii) $\Leftarrow$: As $MM^\dagger = I$, $M^2M^\dagger = M$. As $M^2 = I$, $M^\dagger = M$ as required
  $\Rightarrow$: This follows from i)

- Proposition: The transition matrix to change basis from $\{|0\rangle, |1\rangle\}$ to $\{|+\rangle, |-\rangle\}$ is $\frac{\mathbf{1}}{\sqrt{\mathbf{2}}}\begin{bmatrix}\mathbf{1} & \mathbf{1}\\ \mathbf{1} & \mathbf{-1}\end{bmatrix}$. **This matrix is called the Hadamard gate, denoted $\boldsymbol{H}$**. Moreover, $H = H^{-1}$ (although it is the case that all quantum gates are invertible (in stark contrast to classical gates) as they are unitary matrices, it is not always the case that they are self-inverse)

Proof:

The matrices whose sets of column vectors are our basises are $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ respectively. Recall from linear algebra that, as our initial basis is the standard basis, the transition matrix will simply be the new basis.

$H^2 = \frac{1}{\sqrt{2}\sqrt{2}} \begin{bmatrix} 1+1 & 1-1 \\ 1-1 & 1--1 \end{bmatrix} = I$. Thus $H = H^{-1}$.

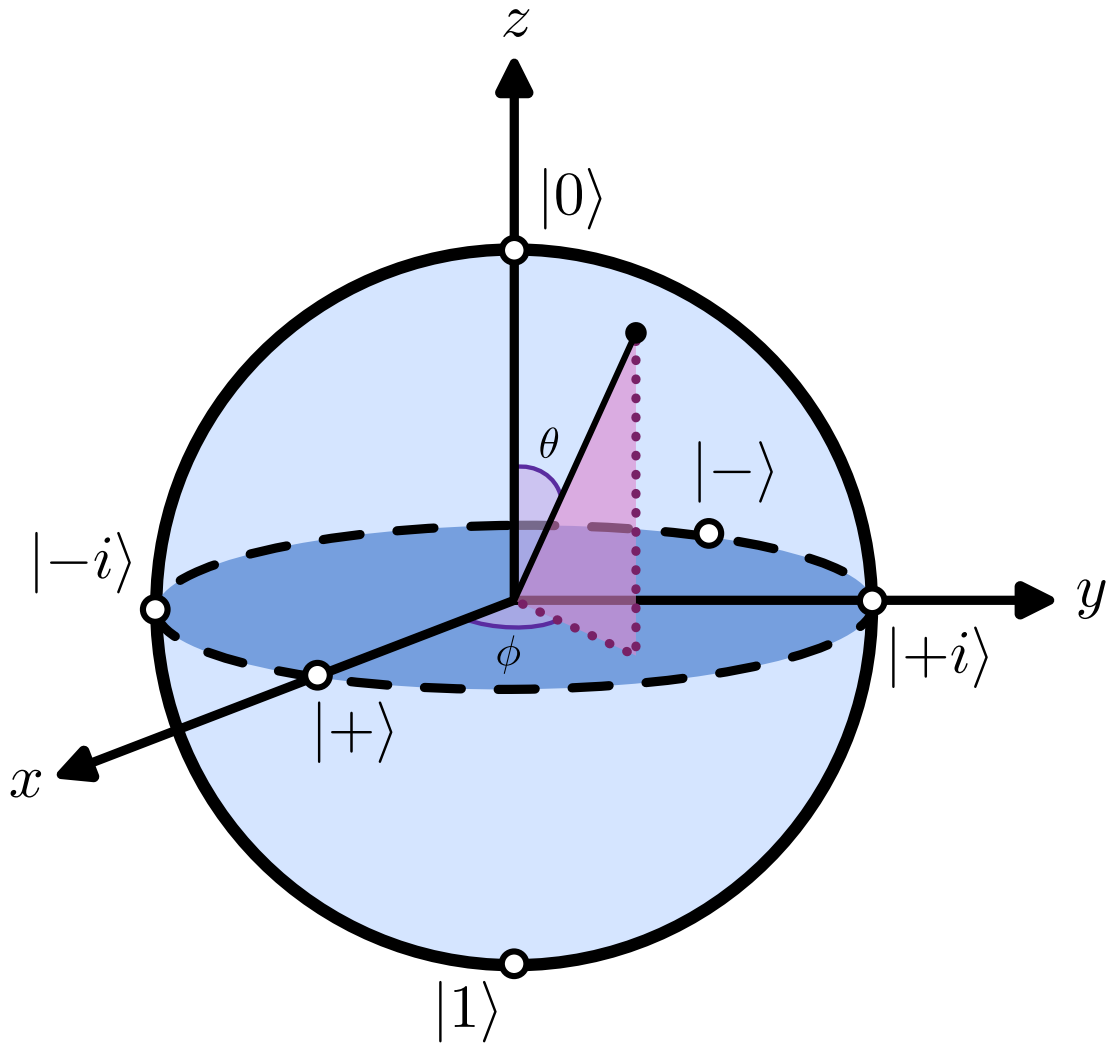
$H^\dagger = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}^T = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = H$.

By the earlier lemma, H is a unitary.

1.2.3 *The Bloch sphere*

- *Proposition: Although the state of a single qbit state* $\psi \in \mathbb{C}^2 \cong \mathbb{R}^4$ *and almost all humans cannot visualise in 4D, actually quantum states are constrained enough that they only contain 3 dimensions of independent information and so can be plotted on a unit sphere (the Bloch sphere). However, beyond single qbits we really do have to blindly follow the maths rather than trying to visualise*
  Proof:
  $\exists \alpha, \beta \in \mathbb{C} : |\psi\rangle = \alpha |0\rangle + \beta |1\rangle$. *We can write* α, β *in Euler form:*
  $\exists r_\alpha, r_\beta, \psi_\alpha, \psi_\beta \in \mathbb{R} : |\psi\rangle = r_\alpha \exp(i\phi_\alpha) |0\rangle + r_\beta \exp(i\phi_\beta) |1\rangle$. *Physics tells us that the "global phase" is an artefact of the mathematical model with no effect on reality, so we can remove any global phase we like:* $|\psi\rangle =$ *[technically this not mathematically equal to our original* $|\psi\rangle$ *but wlog to physical reality it is]* $r_\alpha |0\rangle + r_\beta \exp(i(\phi_\beta - \phi_\alpha)) |1\rangle$ *[*$\phi_\beta - \phi_\alpha$ *is called the relative phase and very much does have physical significance].*

As $|\psi\rangle$ *is a quantum state,* $\langle\psi|\psi\rangle = |r_\alpha|^2 + |r_\beta \exp(i(\phi_\beta - \phi_\alpha))|^2 = 1 \Rightarrow$
${r_\alpha}^2 + {r_\beta}^2 = 1 \Rightarrow \exists\theta \in \mathbb{R} : r_\alpha = \cos(\theta), r_\beta = \sin(\theta)$. *Thus,*
$|\psi\rangle = \cos(\theta)|0\rangle + \sin(\theta)\exp(i(\phi_\beta - \phi_\alpha))|1\rangle$.
It can be shown that this corresponds to $|\psi\rangle$ *being a point on the unit sphere where:* $|0\rangle$ *is at the North pole* ($x = y = 0, z = 1$), $|1\rangle$ *is at the South pole* ($x = y = 0, z = -1$), $\phi_\beta - \phi_\alpha$ *is the angle made between the* x*-axis and the projection of* $|\psi\rangle$ *onto the* xy*-plane, and* 2θ *is the angle made between the* z*-axis and* $|\psi\rangle$ *(no projection involved here).*
Thus, (as can actually be seen from our algebra), θ *controls the probability balance between* $|0\rangle$ *and* $|1\rangle$ *(ie is the sole influence on* z *in the sphere) and* ϕ *controls the balance between real and imaginary parts of the probabilities (which is relevant when the state is in superposition, and so is relevant for intermediate steps in the computation, but cannot be observed when the system is measured to be obtain the result)*


z
$|0\rangle$
θ
$|-\rangle$
$|-i\rangle$
y
ϕ
$|+i\rangle$
$|+\rangle$
x
$|1\rangle$

- *Lemma 1: If* $U = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ *is a unitary matrix and* $|U| = 1$*, then* $c = -b^*$ *and* $d = a^*$
  Proof: Exercise

- *Lemma 2: If* $U = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ *is a unitary matrix, then* $\exists \alpha, \beta, \gamma, \delta \in \mathbb{R}$ *such that* $U = e^{i\alpha} \begin{bmatrix} e^{i\beta}\cos\gamma & e^{i\delta}\sin\gamma \\ -e^{-i\delta}\sin\gamma & e^{-i\beta}\cos\gamma \end{bmatrix}$.

  Proof sketch: $e^{i\alpha}$ *can correspond to taking out a factor so that lemma 1 is applicable to the remaining matrix. It fairly easy to see that the first row can represent any numbers necessary, and then the second row simply follows from lemma 1*

- *Proposition: If U is a quantum gate that acts on a single qubit, then $\exists \alpha, \beta, \gamma, \delta \in \mathbb{R}$ such that $U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$ where*
  $R_z(\theta) = \begin{bmatrix} \exp(\frac{-i\theta}{2}) & 0 \\ 0 & \exp(\frac{i\theta}{2}) \end{bmatrix}$ *and* $R_y(\theta) = \begin{bmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{bmatrix}$.
  Moreover, R_z, R_y are rotation matrices (of the Bloch sphere about the z- or y- axis respectively) and so are unitarities.
  Proof: By lemma 2, $\exists \alpha', \beta', \gamma', \delta' \in \mathbb{R}$ such that
  $U = e^{i\alpha'} \begin{bmatrix} e^{i\beta'} \cos\gamma' & e^{i\delta'} \sin\gamma' \\ -e^{-i\delta'} \sin\gamma' & e^{-i\beta'} \cos\gamma' \end{bmatrix}$ *It remains to show that $\exists \beta, \gamma, \delta \in \mathbb{R}$*
  $R_z(\beta) R_y(\gamma) R_z(\delta) = \begin{bmatrix} e^{i\beta'} \cos\gamma' & e^{i\delta'} \sin\gamma' \\ -e^{-i\delta'} \sin\gamma' & e^{-i\beta'} \cos\gamma' \end{bmatrix}$. *Consider,*
  $\beta = -\beta' - \delta', \gamma = -2\gamma', \delta = \delta' - \beta'$. *With this substitution we have the required equivalence (proof by WolframAlpha)*
  Corollary: $\{R_y(\theta), R_z(\theta) : \theta \in [-\pi, \pi]\}$ is a set of universal gates

In case you do not believe that R_y, R_z are unitarities:

R_y *is unitary:* $R_y(\theta)^\dagger = \begin{bmatrix} \cos(\theta/2) & \sin(\theta/2) \\ -\sin(\theta/2) & \cos(\theta/2) \end{bmatrix}$ *and*

$R_y(\theta)^{-1} = \frac{1}{\cos^2(\theta/2)+\sin^2(\theta/2)} \begin{bmatrix} \cos(\theta/2) & \sin(\theta/2) \\ -\sin(\theta/2) & \cos(\theta/2) \end{bmatrix}$ *and* $\sin^2 + \cos^2 \equiv 1$

R_z *is unitary:* $R_z(\theta)^\dagger = \begin{bmatrix} \exp(\frac{i\theta}{2}) & 0 \\ 0 & \exp(\frac{-i\theta}{2}) \end{bmatrix}$ *and*

$R_z(\theta)^{-1} = \frac{1}{\exp(0)} \begin{bmatrix} \exp(\frac{i\theta}{2}) & 0 \\ 0 & \exp(\frac{-i\theta}{2}) \end{bmatrix}$ *and* $\exp(0) = 1$

1.3 Measurement

- When we measure a quantum state $|\psi\rangle$ we do so with respect to a particular basis $\{\phi_1, ..., \phi_{2^n}\}$
- For now we will assume for simplicity that we are measuring a single qbit — the generalisation to $n > 1$ is intuitive and is proved in subsubsection 1.4.1
- Recall that: When we take a measurement, the superposition collapses and the probability of collapsing into each ϕ_i is given by $|\langle\phi_i|\psi\rangle|^2$ — taking a measurement mid-computation alters the course of the rest of the computation

- **Proposition: It suffices to only measure in the computational basis ($\{|0\rangle, |1\rangle\}$). In particular, measuring ψ with respect to a basis B is equivalent to, given M the change of basis matrix from the computational basis to ϕ, applying the operator $M^\dagger$ to ψ then measuring with respect to the computational basis**

  Proof: Let $|\phi_i\rangle$ be an arbitrary outcome in a basis B we want to measure with respect to. Let M be the matrix to change basis from the computational basis to B *(deduce that M is the matrix with set of column vectors B)*. That is that, $|\phi_i\rangle = M|i\rangle$. Thus, $\langle\phi_i| = \langle i| M^\dagger$. And so, $\langle\phi_i|\psi\rangle = (\langle i| M^\dagger)|\psi\rangle = \langle i|(M^\dagger|\psi\rangle)$ which is the required result.

  We ought to verify that M will be a unitary matrix:

  $M = \begin{bmatrix} z_1 & z_2 \\ z_3 & z_4 \end{bmatrix}$ where $\phi_1 = \begin{bmatrix} z_1 & z_3 \end{bmatrix}$ and $\phi_2 = \begin{bmatrix} z_2 & z_4 \end{bmatrix}$.

  Because this comes from a legal basis, $\langle\phi_1|\phi_2\rangle = 0 = \langle\phi_2|\phi_1\rangle$ and so $z_1^* z_2 + z_3^* z_4 = 0 = z_1 z_2^* + z_3 z_4^*$. Moreover, $|\phi_1|^2 = 1 = |\phi_2|^2$ and so $|z_1|^2 + |z_3|^2 = 1 = |z_2|^2 + |z_4|^2$.

$M^\dagger M = \begin{bmatrix} z_1^* & z_3^* \\ z_2^* & z_4^* \end{bmatrix} \begin{bmatrix} z_1 & z_2 \\ z_3 & z_4 \end{bmatrix} = \begin{bmatrix} z_1^* z_1 + z_3^* z_3 & z_1^* z_2 + z_3^* z_4 \\ z_1 z_2^* + z_3 z_4^* & z_2^* z_2 + z_4^* z_4 \end{bmatrix} = I$ by the previously identified properties and $z_i z_i^* \equiv |z_i|^2$

- Proposition (Principle of deferred measurement): Measurements can always be moved to the end of the circuit
  Proof: Exercise (ensure to demonstrate how classical conditional logic (for classical post-processing that now no longer has the measurement prior to it) can be rewritten as a quantum circuit)

1.4 Composition

1.4.1 Tensor product

- **Let A, B be matrices (not necessarily with any shared size). Then,** outer-product of A and B = **tensor-product of $\boldsymbol{A}$ and $\boldsymbol{B}$ = $\boldsymbol{A \otimes B = [a_{ij}B]}$ as a block matrix. For example,**

$$\begin{bmatrix} \boldsymbol{a_{1,1}} & \boldsymbol{a_{1,2}} \\ \boldsymbol{a_{2,1}} & \boldsymbol{a_{2,2}} \end{bmatrix} \otimes \begin{bmatrix} \boldsymbol{b_{1,1}} & \boldsymbol{b_{1,2}} \\ \boldsymbol{b_{2,1}} & \boldsymbol{b_{2,2}} \end{bmatrix} = \begin{bmatrix} \boldsymbol{a_{1,1}b_{1,1}} & \boldsymbol{a_{1,1}b_{1,2}} & \boldsymbol{a_{1,2}b_{1,1}} & \boldsymbol{a_{1,2}b_{1,2}} \\ \boldsymbol{a_{1,1}b_{2,1}} & \boldsymbol{a_{1,1}b_{2,2}} & \boldsymbol{a_{1,2}b_{2,1}} & \boldsymbol{a_{1,2}b_{2,2}} \\ \boldsymbol{a_{2,1}b_{1,1}} & \boldsymbol{a_{2,1}b_{1,2}} & \boldsymbol{a_{2,2}b_{1,1}} & \boldsymbol{a_{2,2}b_{1,2}} \\ \boldsymbol{a_{2,1}b_{2,1}} & \boldsymbol{a_{2,1}b_{2,2}} & \boldsymbol{a_{2,2}b_{2,1}} & \boldsymbol{a_{2,2}b_{2,2}} \end{bmatrix}$$

- Note that the tensor-product is not commutative

- Proposition: The tensor-product is associative
  Proof: By induction it suffices to prove that $(A \otimes B) \otimes C = A \otimes (B \otimes C)$
  Exercise

1.4.2 Combining states

- **Let $\boldsymbol{u} = \begin{bmatrix} \boldsymbol{u_1} & \boldsymbol{...} & \boldsymbol{u_n} \end{bmatrix}$ and $\boldsymbol{v} = \begin{bmatrix} \boldsymbol{v_1} & \boldsymbol{...} & \boldsymbol{v_m} \end{bmatrix}$. Then, we know that $\boldsymbol{u \otimes v} = \begin{bmatrix} \boldsymbol{u_1 v_1} & \boldsymbol{...} & \boldsymbol{u_1 v_m} & \boldsymbol{...} & \boldsymbol{u_n v_1} & \boldsymbol{...} & \boldsymbol{u_n v_m} \end{bmatrix}$**

- Proposition: Let $H_{AB} = H_A \otimes H_B$ be the set of states the system composed of states from H_A and H_B can be in.
  Then, $\forall \left|\psi\right\rangle \in H_{AB} : \left|\psi\right\rangle = \sum_{i,j} \psi_{ij} \left|i\right\rangle \otimes \left|j\right\rangle$. That is that **every state of the system can be written as a linear combination of the tensor products of the basis vectors of the components of the system**, which as quantum mechanics is all about linear algebra is fortunate.
  Proof sketch: Deduce that each $\left|i\right\rangle \otimes \left|j\right\rangle$ is a basis vector of H_{AB} and we are summing over all of them. Then, the required result is trivial

- **Postulate 4: Let $\boldsymbol{\left|\psi\right\rangle}$ be the state of a system composed of $\boldsymbol{k}$ subsystems in states $\boldsymbol{\left|\psi_1\right\rangle, ... \left|\psi_k\right\rangle}$. Then, $\boldsymbol{\left|\psi\right\rangle = \left|\psi_1\right\rangle \otimes ... \otimes \left|\psi_k\right\rangle}$.**
  For brevity, we will often write states as bit-strings $\left|x_1 ... x_n\right\rangle$ when technically we mean $\left|x_1\right\rangle \otimes ... \otimes \left|x_n\right\rangle$

- Postulate 4 only tells us how to write the state of the system when it is in a state where the states of each qbit are independent (for example in a classical input). There also exist states (such as if the system evolves by the application of certain gates) that cannot be factored out into independent subsystems (entangled states)

- Proposition: $k(|u\rangle \otimes |v\rangle) = (k\,|u\rangle) \otimes |v\rangle = |u\rangle \otimes (k\,|v\rangle)$
  Proof: Exercise
  Corollary: $(a\,|u\rangle \otimes b\,|v\rangle) = ab(|u\rangle \otimes b\,|v\rangle)$ and so
  $(k\,|u\rangle \otimes k\,|v\rangle) = k^2(|u\rangle \otimes b\,|v\rangle)$ not $k(|u\rangle \otimes b\,|v\rangle)$

- Proposition: Tensor product distributes over addition:
  $|u\rangle \otimes (|v_1\rangle + |v_2\rangle) = |u\rangle \otimes |v_1\rangle + |u\rangle \otimes |v_2\rangle$
  Proof: Exercise

- Proposition: **Let $(\boldsymbol{a}, \boldsymbol{b})$ denote the inner product of $\boldsymbol{a}$ and $\boldsymbol{b}$.**
  $\left(\sum_i a_i\,|v_i\rangle \otimes |w_i\rangle\,, \sum_j b_j\,|v'_j\rangle \otimes |w'_j\rangle\right) = \sum_{i,j} {a_i}^* b_j\,\langle v_i|v'_j\rangle\,\langle w_j|w'_j\rangle$

Proof: Exercise
Corollary: $\boldsymbol{(|v\rangle \otimes |w\rangle \, , |v'\rangle \otimes |w'\rangle) = \langle v|v'\rangle \, \langle w|w'\rangle}$

- We will abbreviate $|\psi\rangle \otimes ...$ (k times) $\otimes |\psi\rangle$ to $|\psi\rangle^{\otimes k}$ or even further to $|\psi\rangle^k$

- Proposition: Measurement for multiple qbit systems extends single qbit measurement in the obvious way, that is that
  $\mathbf{Pr(|\overline{x}\rangle) = |\langle \overline{x}|\psi\rangle|^2 = |\psi_{\overline{x}}|^2}$ **if** $\boldsymbol{|\overline{x}\rangle}$ **is a component of** $\boldsymbol{\psi}$ (for example $|\psi\rangle$ is written in terms of the computational basis and $|\overline{x}\rangle$ is an element of the computational basis). Here $\overline{x}$ denotes a vector of bits rather than a complementation operator.
  Proof: $\Pr(|\overline{x}\rangle) = |\langle \overline{x}|\psi\rangle|^2$ is how we define qbit measurement in general. Then, $|\langle \overline{x}|\psi\rangle|^2 = |\langle \overline{x}| \sum_{\overline{y}\in\{0,1\}^n} \psi_{\overline{y}} |\overline{y}\rangle|^2 = |\psi_{\overline{x}}|^2$ as $\langle \overline{x}|\psi_{\overline{y}}\rangle = 0$ if $\overline{x} \neq \overline{y}$ (as then x and y are distinct basis vectors and so are orthogonal) and $\psi_{\overline{x}}$ if $\overline{x} = \overline{y}$

1.4.3 Combining operators

- **The matrix of the operator that applies operator $\boldsymbol{A}$ to the first qbit and operator $\boldsymbol{B}$ to the second qbit is $\boldsymbol{A \otimes B}$** (by induction this extends to systems with $n > 2$ qbits). Recall that A, B are matrices and we already know how to compute the tensor product of matrices

- *Simulating the quantum computer $A_1 \otimes ... \otimes A_n$ (for single-qbit matrices $A_1, ..., A_n$) on a classical computer requires a matrix with 4^n entries and so is computationally infeasible, and yet the universe is able to do it for us tractably! Albeit, using quantum phenomena is why we have to design quantum algorithms to work around the measurement collapse limitation, whereas the classical simulation does not suffer from this*

- Proposition: $(A \otimes B)(a\,|v_i\rangle \otimes |w_i\rangle) = a_i A\,|v_i\rangle \otimes B\,|w_i\rangle$
  Proof: Exercise
  Corollary: $(A \otimes B)(|v\rangle \otimes |w\rangle) = A\,|v\rangle \otimes B\,|w\rangle$. This is essentially a formalisation of the first bullet

1.4.4 Entanglement

- Proposition: **There exist states which n-qbit systems can be in, but which cannot be written as a pure tensor product of n single-qbit states** (however they can, by a previous proposition, be written as a linear combination of (2^n (or fewer)) tensor products of single-qbit states), **we call these states entangled states**.
  Measurements of the different qbits are not independent iff the state is entangled.
  Proof sketch: We will witness the existential claim of the first sentence in the next proposition. It remains to prove the second sentence.
  A state is not entangled iff it can be written as a direct tensor product iff the joint probabilities are the product of the elementary probabilities iff they are independent events

- Proposition: $\{|\phi^+\rangle = ..., |\phi^-\rangle = ..., |\psi^+\rangle = ..., |\psi^-\rangle = ...\}$ **is a basis for a 2-qbit system. Moreover, these are all maximally entangled states (that is that, although measuring one qbit causes that qbit to collapse into a random state, what the other qbit will collapse into if subsequently measured is then certain based on that (the same state for ϕ, the opposite state for ψ)). These are called the Bell states, and the symbol given to each of them here is standard**

  Proof: Witness a circuit/unitary that shows a system can be in these states: Exercise

  For them to be a basis, it only remains to check that they are pairwise orthogonal. Exercise

  The most interesting property to verify is the entanglement. Exercise

  We can also demonstrate the maximal entanglement. Exercise

1.4.5 Projective measurement (partial measurement)

- In linear algebra **a matrix P is a projector iff** $P^2 = P$. In quantum computing, we are only interested in self-adjoint projectors:
  $\boldsymbol{P^2 = P = P^\dagger}$ — note that projectors are typically not unitary

- Proposition: For every (self-adjoint (this is the last time we will specify this, but it will always hold)) projector P, there exists an orthonormal basis $\{|u_i\rangle\}$ such that $\boldsymbol{P = \sum_i |u_i\rangle \langle u_i|}$
  Proof: Out of scope

- **Postulate 3: A quantum measurement is defined by a collection $\{M_m\}$ of measurement operators where each m corresponds to a possible measurement outcome. $\Pr(m) = |M_m |\psi\rangle|^2 = \langle\psi| M_m{}^\dagger M_m |\psi\rangle$. The state of the system after a measurement outcome m is $\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m{}^\dagger M_m|\psi\rangle}} = \frac{M_m|\psi\rangle}{\sqrt{\Pr(m)}}$**

- **Quantum measurement operators must obey the completeness equation $\sum_{\boldsymbol{m}} \boldsymbol{M_m}^\dagger \boldsymbol{M_m} = \boldsymbol{I}$ as this is necessary and sufficient for $\sum_{\boldsymbol{m}} \mathbf{Pr}(\boldsymbol{m}) = \mathbf{1}$**
- **In IQC we only need projective measurement: Each $\boldsymbol{M_m}$ is a projector**, or equivalently $\sum_m mM_m$ is a Hermitian matrix for which each m is an eigenvalue
- *Projective measurement corresponds to the very reasonable constraint that measurement is idempotent (repeating a measurement does not change the outcome, as we have already collapsed the state)*
- As projectors in QC are self-adjoint, we can replace the $M_m^\dagger$s with M_m. In particular, **the completeness equation "simplifies" to $\sum_{\boldsymbol{m}} \boldsymbol{P_m} = \boldsymbol{I}$ and $\langle \boldsymbol{P_m} | \boldsymbol{P_{m'}} \rangle = \mathbb{1}[\boldsymbol{m} = \boldsymbol{m'}]$**
- Let $M = \{P_m\}$ be a projective measurement. Then, expected outcome of $M = \langle M \rangle = \sum_m m \Pr(m) = \sum_m m \langle \psi | P_m | \psi \rangle = \langle \psi | \left(\sum_m mP_m \right) | \psi \rangle$

2 Quantum algorithms

2.1 Quantum gates

- NOT gate = $\boldsymbol{X} = \begin{bmatrix} \mathbf{0} & \mathbf{1} \\ \mathbf{1} & \mathbf{0} \end{bmatrix}$
- $\boldsymbol{Y} = \begin{bmatrix} \mathbf{0} & -\boldsymbol{i} \\ \boldsymbol{i} & \mathbf{0} \end{bmatrix}$
- $\boldsymbol{Z} = \begin{bmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{-1} \end{bmatrix}$
- Hadamard gate = $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
- Z-rotation gate = $\boldsymbol{R_\theta} = \begin{bmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \boldsymbol{e^{i\theta}} \end{bmatrix}$

- Phase gate $= S = R_{\frac{\pi}{2}}$
- $T = R_{\frac{\pi}{4}}$
- For any unitary U, Controlled-U gate $= |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$
  - CNOT $= |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$
  - $\bigwedge U_{i,j} = U$ on j^{th} qbit controlled by i^{th} qbit — qbits are typically considered to be 1-indexed
- SWAP gate $= \Pi = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

- Theorem: {X, Z, H, S, T} is a set of universal gates. Moreover, the construction is only exponential in the number of T gates required (it is easy to see that it is unavoidable to, when creating arbitrary gates from a finite set of gates, use less than exponential number of overall gates in some cases, so being able to pin all the exponential behaviour to one type of gate is an achievement)
  Proof: Out of scope

- A and B commute iff $AB = BA$. We define $\boldsymbol{[A, B] = AB - BA}$. Then, A and B commute iff $[A, B] = 0$

- A and B anti-commute iff $AB = BA$. We define $\boldsymbol{\{A, B\} = AB + BA}$. Then, A and B anti-commute iff $\{A, B\} = 0$ A, B = AB + BA. Thus, A and B anti-commute iff A, B = 0

- Proposition: **The set of Pauli matrices** $= \boldsymbol{\{I, X, Y, Z\}}$. Each Pauli matrix σ is Hermitian. Moreover, **pairs of Pauli matrices anti-commute**

Proof:
$XX = I, \quad XY = iZ, \quad XZ = -iY$
$YX = -iZ, YY = I, \quad YZ = iZ$
$ZX = iY, \quad ZY = -iZ, ZZ = I$
Symmetry $\times -1$ when reflected in diagonal demonstrates anti-commutation

As σ is unitary and $\boldsymbol{\sigma^2 = I}$, σ is Hermitian.

2.2 Phase-kickback

- Proposition: Every classical oracle has a corresponding quantum oracle (possibly with additional inputs and outputs in order to make it reversible)
  Proof sketch: Consider the Toffoli gate
  $|a\rangle \otimes |b\rangle \otimes |c\rangle \mapsto |a\rangle \otimes |b\rangle \otimes |c \oplus ab\rangle$. The $\oplus ab$ (this type of thing will come up a lot) only has the classically intuitive meaning (XOR (a AND b)) on the $|0\rangle$, $|1\rangle$ states; for general quantum states we will have to break the state down into a sum of computational basis states first to be able to apply this definition.
  It is easy to see that this is a (self-inverse) quantum unitary. Moreover, it is also easy to see that this can simulate a NAND gate (which is a universal classical gate). Note that Toffoli is not universal for quantum computation, only for (reversible) classical computation.

- Proposition: **Let O_f be a quantum oracle $O_f |xy\rangle = |x\rangle \otimes |y \oplus f(x)\rangle$. Then there exists a so called phase-kickback circuit U_f such that $U_f |x\rangle = (-1)^{f(x)} |x\rangle$** $(\otimes |z\rangle)$ (we don't actually care about $|z\rangle$)
  Proof: Consider $U_f |x\rangle = O_f(I \otimes H)(|x\rangle \otimes |1\rangle)$.
  Then, $U_f |x\rangle = O_f(|x\rangle \otimes |-\rangle)$
  Case $f(x) = 0$: $O_f |xy\rangle = |x\rangle \otimes |y\rangle$. Thus, $U_f |x\rangle = |x\rangle \otimes |-\rangle = (-1)^0 |x\rangle \otimes |-\rangle$
  Case $f(x) = 1$: $O_f |xy\rangle = |x\rangle \otimes X |y\rangle$. Thus, $U_f |x\rangle = |x\rangle \otimes -1 |-\rangle = -1 |x\rangle \otimes |-\rangle = (-1)^1 |x\rangle \otimes |-\rangle$

2.3 Deutsch–Jozsa algorithm

- Proposition **(Walsh-Hadamard Transform):**
  $H^{\otimes n} |x\rangle = \frac{1}{(\sqrt{2})^n} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle$ where $x = x_1 ... x_n$ and $x_1, ..., x_n \in \{0, 1\}$

Proof:
$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
Thus, $H|x_i\rangle = \frac{1}{\sqrt{2}}\sum_{y_i\in\{0,1\}}(-1)^{x_i\cdot y_i}|y_i\rangle$.
Thus, $H^{\otimes n}|x\rangle = \bigotimes_{i\in[n]}\frac{1}{\sqrt{2}}\sum_{y_i\in\{0,1\}}(-1)^{x_i\cdot y_i}|y_i\rangle =$
$\frac{1}{(\sqrt{2})^n}\sum_{y\in\{0,1\}^n}(-1)^{\sum_j x_j\cdot y_j}|y\rangle = \frac{1}{(\sqrt{2})^n}\sum_{y\in\{0,1\}^n}(-1)^{x\cdot y}|y\rangle$
Corollary: $\boldsymbol{|+\rangle^{\otimes n} = \frac{1}{(\sqrt{2})^n}\sum_{x\in\{0,1\}^n}|x\rangle}$

- **Deutsch-Jozsa problem:** Given an oracle for a boolean function f, and a promise that f is either constant ($\exists c \in \{0,1\} : \forall x; f(x) = c$) or balanced (for exactly half of the possible inputs $f(x) = 1$ (and for exactly half of the possible inputs $f(x) = 0$)), **decide whether f is constant or balanced**

- A classical computer requires $O(\frac{2^n}{2} + 1) = O(2^n)$ oracle calls as we need to put in half + 1 of the inputs to be sure to never make a mistake

- Proposition: A quantum computer can solve Deutsch-Jozsa using a single oracle call!
  Proof: The quantum circuit is $\boldsymbol{\psi_{\text{out}} = H^{\otimes n}\left(U_f\left(H^{\otimes n}\left|0\right\rangle^{\otimes n}\right)\right)}$ where U_f is the phase kickback unitary for the oracle.
  $\psi_{\text{out}} = H^{\otimes n}\left(U_f\left|+\right\rangle^{\otimes n}\right) = H^{\otimes n}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}\left|x\right\rangle$
  Using the lemma,
  $\psi_{\text{out}} = \frac{1}{(\sqrt{2})^n}\sum_{x\in\{0,1\}^n}\left((-1)^{f(x)}\frac{1}{(\sqrt{2})^n}\sum_{y\in\{0,1\}^n}(-1)^{x\cdot y}\left|y\right\rangle\right) =$
  $\sum_{y\in\{0,1\}^n}\left(\frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{f(x)+x\cdot y}\right)\left|y\right\rangle.$
  Thus, $\mathbf{Pr(0^{\otimes n}) = \left|\frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{f(x)+x\cdot 0^{\otimes n}}\right|^2 =}$
  $\boldsymbol{\left|\frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}\right|^2}$.
  Case $f(x) = c$ for all x: $\Pr(0^{\otimes n}) = \left|\frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{c}\right|^2 =$
  $\left|\frac{1}{2^n}\left((-1)^c 2^n\right)\right|^2 = 1$

Case f is balanced: $\Pr(0^{\otimes n}) = \left|\frac{1}{2^n}0\right|^2 = 0$

2.4 Bernstein-Vazirani algorithm

- **Bernstein-Vazirani problem: Given an oracle for an $f(x) = a \cdot x$, find the value of $a \in \{0,1\}^n$**
- A classical computer requires at least $\Omega(n)$ oracle queries (proof out of scope, but uses communication complexity) to solve Bernstein-Vazirani
- Proposition: A quantum computer can solve Bernstein-Vazirani in a single oracle call! Moreover, **the same circuit as Deutsch–Jozsa suffices**.
  Proof: Recall that each output state $|y\rangle$ of the Deutsch-Jozsa circuit has probability $\left|\frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{f(x)+x\cdot y}\right|^2$. Using our definition of f(x),
  $\Pr(y) = \left|\frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{a\cdot x+x\cdot y}\right|^2 = \left|\frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{a\cdot x}(-1)^{x\cdot y}\right|^2$

Suppose $y = a$, then $\Pr(y) = \left|\frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{ax}(-1)^{ax}\right|^2 =$
$\left|\frac{1}{2^n}\sum_{x\in\{0,1\}^n}((-1)^{ax})^2\right|^2 = \left|\frac{1}{2^n}\sum_{x\in\{0,1\}^n}1\right|^2 = 1.$
Suppose $y \neq a$, then by elementary laws of probability
$\Pr(y) \leq 1 - Pr(a) = 1 - 1 = 0.$

2.5 Grover's algorithm

- **Grover's problem: Given an oracle for a boolean function $\boldsymbol{f}$**, and a promise that there is exactly one satisfying input (this is only for simplicity, it can be relaxed fairly easily), **find the $\boldsymbol{s \in \{0,1\}^n}$ such that $\boldsymbol{f(s) = 1}$**

- *Note this is a "harder" problem than SAT (although actually it is not even known whether quantum algorithms can solve NP-Complete problems deterministically in polynomial time) as the boolean function is an oracle rather than a formula we can inspect*

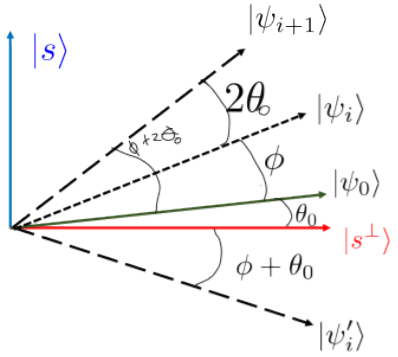
- Lemma: $R = 2\left|\phi\right\rangle\left\langle\phi\right| - I$ is the unitary that reflects in the line $\left|\phi\right\rangle$
  Proof:
  $R\left(a\left|\phi\right\rangle + b\left|\phi^{\perp}\right\rangle\right) = 2a\left|\phi\right\rangle + 0b\left|\phi^{\perp}\right\rangle - a\left|\phi\right\rangle - b\left|\phi^{\perp}\right\rangle = a\left|\phi\right\rangle - b\left|\phi^{\perp}\right\rangle$

- Proposition: **A quantum algorithm can solve Grover's problem with high probability in $O(\sqrt{2^n})$ oracle calls, whereas corresponding classical algorithms would require $O(2^n)$ oracle calls** (there can be no classical shortcuts for an arbitrary boolean function oracle, so asymptotically all of the elements have to be looked at to even attain high probability)
  Algorithm: Start with the $\left|0\right\rangle^{\otimes n}$ state (as many quantum algorithms do). Repeatedly apply identical units called Grover iterations. Each Grover iteration is $\left|\psi_{i+1}\right\rangle = H^{\otimes n}U_0H^{\otimes n}U_f\left|\psi_i\right\rangle$ where $U_0 =$ the phase-kickback unitary for $g(x) = \mathbb{1}[x \neq 0^{\otimes n}]$

Proof: Break-up $H^{\otimes n}\left|0\right\rangle^n = \frac{1}{\sqrt{2^n}}\left|s\right\rangle + \frac{\sqrt{2^n-1}}{\sqrt{2^n}}\left|s^\perp\right\rangle$ where $\left|s^\perp\right\rangle = \left[\sum_{x\in\{0,1\}^n:x\neq s}\left|x\right\rangle\right]$. Notice that $\left(\frac{1}{\sqrt{2^n}}\right)^2 + \left(\frac{\sqrt{2^n-1}}{\sqrt{2^n}}\right)^2 = 1$ and thus deduce that $\exists\theta : \left(\sin(\theta) = \frac{1}{\sqrt{2^n}} \text{ and } \cos(\theta) = \frac{\sqrt{2^n-1}}{\sqrt{2^n}}\right)$.
Thus, $\psi_0 = \sin(\theta_0)\left|s\right\rangle + \cos(\theta_0)\left|s^\perp\right\rangle$. Let G be the grover iteration unitary. We will demonstrate later that $\boldsymbol{G^t\left|\psi_0\right\rangle = \sin((2t+1)\theta_0)\left|s\right\rangle + \cos((2t+1)\theta_0)\left|s^\perp\right\rangle}$.
Thus, by running $\boldsymbol{T = \frac{\pi}{4}\sqrt{2^n}}$ Grover iterations we obtain an output state
$G^T\left|\psi_0\right\rangle \approx$ [as $2T+1 \approx T$ for large T (i.e. large n)]
$\sin(\frac{\pi}{2}\sqrt{2^n}\theta_0)\left|s\right\rangle + \cos(\frac{\pi}{2}\sqrt{2^n}\theta_0)\left|s^\perp\right\rangle = \sin(\frac{\pi}{2}\frac{1}{\sin(\theta_0)}\theta_0)\left|s\right\rangle + \cos(\frac{\pi}{2}\frac{1}{\sin(\theta_0)}\theta_0)\left|s^\perp\right\rangle$
$\approx$ [as $\sin(\theta_0) \approx \theta_0$ for small θ_0]
$\sin(\frac{\pi}{2})\left|s\right\rangle + \cos(\frac{\pi}{2})\left|s^\perp\right\rangle = \left|s\right\rangle$. Thus, the state is $\left|s\right\rangle$ with high probability (and we can use probability amplification to get it even higher if we necessary, as we get the same quantum state every time and it collapses independently every time) and we used $T \in O(\sqrt{2^n})$ oracle calls.

Now we need to actually prove that each Grover iteration does the rotation we claimed.
As U_f = the matrix which is 0 everywhere expect for the diagonal where it is $+1$ expect for the s position on the diagonal where it is -1,
$U_f = I - 2\left|s\right\rangle\left\langle s\right|$. Thus, by the lemma, (up to an irrelevant global phase) $\boldsymbol{U_f}$ **is reflection in the line** $\boldsymbol{\left|s\right\rangle}$.
As U_0 = the matrix which is 0 everywhere expect for the diagonal where it is -1 expect for the $0^{\otimes n}$ position on the diagonal where it is $+1$,
$U_f = 2\left|0^{\otimes n}\right\rangle\left\langle 0^{\otimes n}\right| - I$. Thus, U_0 is reflection in the line $\left|0\right\rangle^{\otimes n}$. Thus, as $\left|\psi_0\right\rangle = H^{\otimes n}\left|0\right\rangle^{\otimes n}$, $\boldsymbol{H^{\otimes n}U_0H^{\otimes n}}$ **is reflection in the line** $\boldsymbol{\left|\psi_0\right\rangle}$.
We have shown that a Grover iteration corresponds to reflection in the line $\left|s\right\rangle$ followed by reflection in the line $\left|\psi_0\right\rangle$. It remains to demonstrate what rotation this composition corresponds to.

The definition of θ_0 was that it is the angle made between $|\psi_0\rangle$ and $|s^\perp\rangle$. Let ϕ_t be the angle made between $|\psi_t\rangle$ and $|\psi_0\rangle$. Then, the state after $|\psi_t\rangle$ is reflected in $|s^\perp\rangle$ by U_f makes an angle of $\theta_0 + \phi_t$ with $|s^\perp\rangle$. It is this state which is reflected in $|\psi_0\rangle$ by $H^{\otimes n}U_0H^{\otimes n}$ to obtain ϕ_{t+1}. Thus, ϕ_{t+1} makes an angle of $2\theta_0 + \phi_t$ with $|\psi_0\rangle$ and so makes an angle of $2\theta_0$ with $|\psi_t\rangle$.



Thus, as $|\psi_0\rangle$ makes an angle of θ_0 with $|s^\perp\rangle$ and each $|\psi_{t+1}\rangle$ makes an angle of $2\theta_0$ with $|\psi_t\rangle$, by induction each $|\psi_t\rangle$ makes an angle of $(2t+1)\theta_0$ with $|\psi_0\rangle$

2.6 Simon's algorithm

- **Simon's problem: Given an oracle for a function $f : \{0,1\}^n \mapsto \{0,1\}^n$, and a promise that $\exists a \in \{0,1\}^n$: $\forall x; \forall x' \neq x; f(x') = f(x)$ if and only if $x' = x \oplus a$, find the value of a**

- **To solve Simon's problem it suffices to find any pair x, x' such that $x' \neq x$ but $f(x) = f(x')$ as then $a = x' \oplus x$.** However, a classical algorithm would need $\Omega(\sqrt{2^n})$ to find such a pair with high probability

- Proposition: A quantum algorithm can solve Simon's problem with high probability exponentially faster than a classical algorithm could
  Algorithm:
  $|\psi_y\rangle \otimes |z\rangle = H^{\otimes n} \otimes I^{\otimes n} \left(O_f \left(H^{\otimes n} \otimes I^{\otimes n} \left(|0\rangle^{\otimes n} \otimes |0\rangle^{\otimes n} \right) \right) \right)$
  Proof:
  Let $|\phi\rangle$ = the state immediately after the O_f.

Then, $|\phi\rangle = O_f\left(|+\rangle^{\otimes n} \otimes |0^{\otimes n}\rangle\right) = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \otimes |f(x)\rangle =$
$\frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} \left(\sum_{x\in f^{-1}(y)} |x\rangle\right) \otimes |y\rangle$.
We will suppose of the sake of simplifying the proof that $|z\rangle$ is measured at this point. It is important to understand that this has no impact on correctness.
Let y now refer to the particular (arbitrary) measurement outcome of the lower register. The corresponding projector is $P_y = I^{\otimes n} \otimes |y\rangle\langle y|$.
$P_y |\phi\rangle = \frac{1}{\sqrt{2^n}} \left(\sum_{x\in f^{-1}(y)} |x\rangle\right) \otimes |y\rangle$. $\Pr(y) = \frac{\left|f^{-1}(y)\right|}{2^n}$
$|\psi_y\rangle = H^{\otimes n} \frac{1}{\sqrt{\Pr(y)}} P_y |\phi\rangle = H^{\otimes n} \frac{1}{\sqrt{\left|f^{-1}(y)\right|}} \sum_{x\in f^{-1}(y)|x\rangle}$
By the promise, f is either one-to-one or two-to-one. Assume (HOW?) that it is two-to-one for the output y. Then,
$|\psi_y\rangle = H^{\otimes n} \frac{1}{\sqrt{2}} (|x_y\rangle + (x_y \oplus a))$

By the Walsh-Hadamard transform,
$|\psi_y\rangle = \frac{1}{\sqrt{2}}\frac{1}{\left(\sqrt{2}\right)^n}\sum_{z\in\{0,1\}^n}\left((-1)^{x_y\cdot z}+(-1)^{\left(x_y\oplus a\right)\cdot z}\right)|z\rangle =$
$\frac{1}{\sqrt{2}}\frac{1}{\left(\sqrt{2}\right)^n}\sum_{z\in\{0,1\}^n}\left((-1)^{x_y\cdot z}+(-1)^{x_y\cdot z}(-1)^{a\cdot z}\right)|z\rangle =$
$\frac{1}{\sqrt{2}}\frac{1}{\left(\sqrt{2}\right)^n}\left(\sum_{z\in\{0,1\}^n:a\cdot z=0}\left((-1)^{x_y\cdot z}+(-1)^{x_y\cdot z}\right)|z\rangle\right)+$
$\frac{1}{\sqrt{2}}\frac{1}{\left(\sqrt{2}\right)^n}\left(\sum_{z\in\{0,1\}^n:a\cdot z=1}(-1)^{x_y\cdot z}-(-1)^{x_y\cdot z}|z\rangle\right)) =$
$\frac{1}{\sqrt{2}}\frac{1}{\left(\sqrt{2}\right)^n}\left(2\sum_{z\in\{0,1\}^n:a\cdot z=0}(-1)^{x_y\cdot z}|z\rangle\right) =$
$\frac{1}{\left(\sqrt{2}\right)^{n-1}}\sum_{z\in\{0,1\}^n:a\cdot z=0}(-1)^{x_y\cdot z}|z\rangle.$
Thus, **measuring the upper register gives us some z such that $a\cdot z=0$**. Note we no longer care about y, it just made the algebra a bit easier (yes really!) to have y be deterministic.
By repeating this process until we obtain linearly independent $z^{(1)},...,z^{(n-1)}$, we can use classical post-processing to build and solve a

system of simultaneous equations to find a: $\forall i \in [n]; a_i \in \{0,1\}$ and $a_1 + ... + a_n \neq 0$ and $\forall j \in \{1, ..., n-1\}; a_1 z_1^{(k)} \oplus ... \oplus a_n z_n^{(k)} = 0$. The luckiest our algorithm can be is to only make $n - 1 \in O(n)$ runs and immediately get a set of $n - 1$ linearly independent zs, it is possible to show that this happens with probability at least $\frac{1}{4}$. Suppose we make $O(n)$ runs of our algorithm (where our algorithm includes internally running the circuit $O(n)$ times (and each run of the circuit only makes a single oracle call)), then the probability we don't get a linearly independent set is at most $O\left(\left(\frac{3}{4}\right)^n\right)$ which means we succeed with high probability and we only used $O(n) \times O(n) = O(n^2)$ oracle calls

3 Quantum subroutines

3.1 Hadamard test

- **Hadamard test circuit: Let Π_0, Π_1 be projectors that partition the Hilbert space into subspaces (ie $\Pi_0 + \Pi_1 = I$). The Hadamard test induced by Π_0, Π_1 is $\boldsymbol{U_m} |\mathbf{0}\rangle \otimes |\boldsymbol{\psi}\rangle$ where $\boldsymbol{U_m} = (\boldsymbol{H} \otimes \boldsymbol{I}) \bigwedge \boldsymbol{A_{1,...}} (\boldsymbol{H} \otimes \boldsymbol{I})$ where $\boldsymbol{A} = \boldsymbol{\Pi_0} - \boldsymbol{\Pi_1}$**

- Proposition: A is unitary, and so this is a valid circuit
  Proof: $AA^\dagger = (\Pi_0 - \Pi_1)^2 = \Pi_0^2 - \Pi_0\Pi_1 - \Pi_1\Pi_0 + \Pi_1^2 = \Pi_0 + \Pi_1 = I$

- Proposition: Π_0, Π_1 are eigenspaces of A with eigenvalues $+1, -1$ respectively
  Proof:
  $A\Pi_0 = \Pi_0^2 - \Pi_1\Pi_0 = \Pi_0$ by properties of projectors
  $A\Pi_1 = \Pi_0\Pi_1 - \Pi_1^2 = -\Pi_1$ by properties of projectors

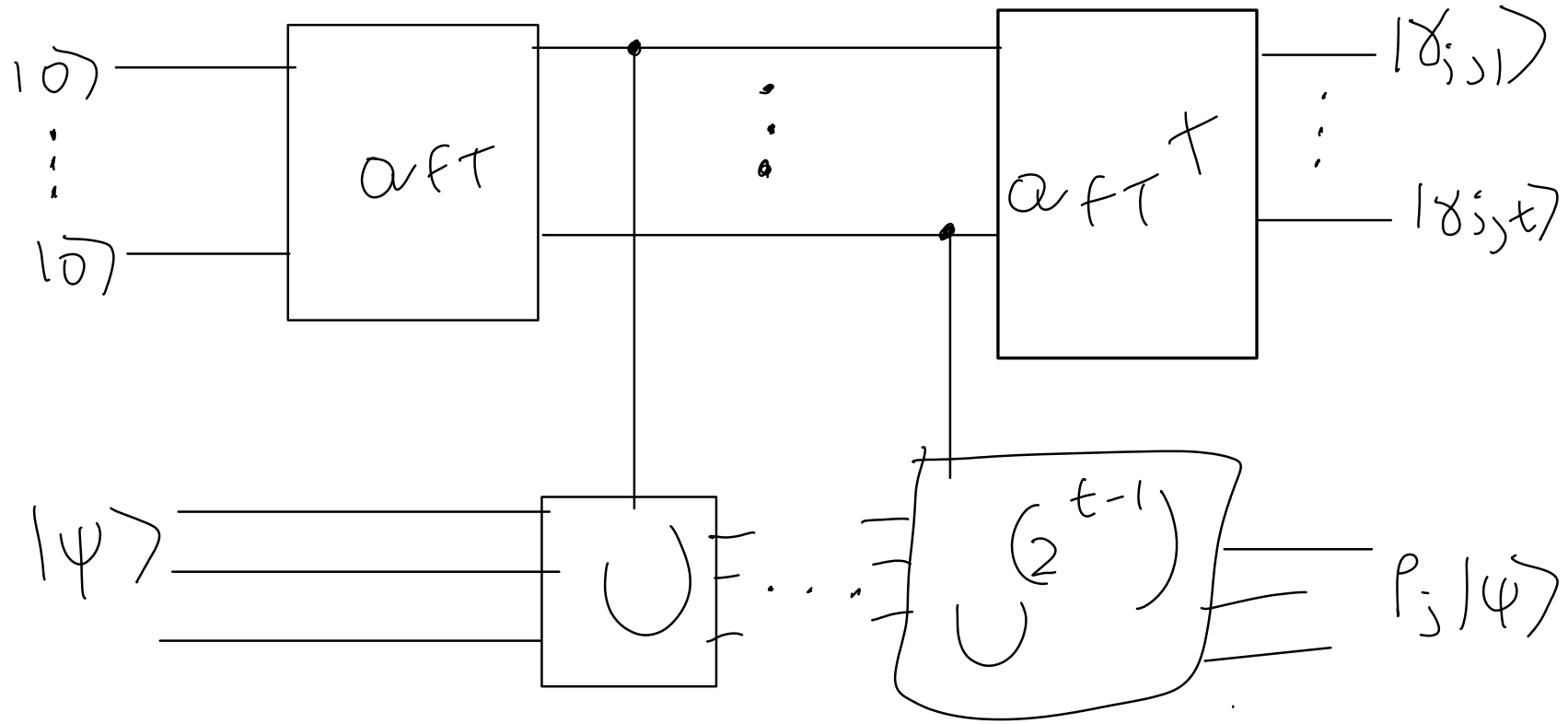
- Proposition: **Measuring the top qbit gives measurement outcome i with probability $\mathbf{Pr}(i) = |\mathbf{\Pi}_i |\boldsymbol{\psi}\rangle|^2$ and sends the lower register $|\boldsymbol{\psi}\rangle$ to $\mathbf{\Pi}_i |\boldsymbol{\psi}\rangle$**
  Proof: Exercise
  Corollary: If $|\psi\rangle$ lies entirely inside one of Π_0, Π_1, then the measurement of the upper qbit tells us deterministically which one it is in and the projection of the lower register does not affect the state (by the definition of projection). This is useful as it means we can measure certain properties of a quantum state for quantum error correction purposes without collapsing the state

- Proposition: **For any Hadamard test, bias of outcomes = $\mathbf{Pr(0) - Pr(1)} = |\Pi_0 |\psi\rangle|^2 - |\Pi_1 |\psi\rangle|^2 = \langle A \rangle = \langle \boldsymbol{\psi}| \boldsymbol{A} |\boldsymbol{\psi}\rangle$**
  Proof: Exercise
  Corollary: Hadamard test with A as the SWAP gate and input state $|\psi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle$ gives probability bias $|\langle \phi_1 | \phi_2 \rangle|^2$

3.2 Quantum Fourier transform

- $\mathbf{QFT_q} = \frac{1}{\sqrt{q}} \sum_{y \in \{0,\ldots,Q-1\}} \mathbf{exp}(i\frac{2\pi}{q})^{xy} |y\rangle$. Thus, $H = \mathrm{QFT}_2$
- We will only consider q where $\exists n : q = 2^n$
- Proposition: $\mathbf{QFT_{2^n}} |x_1 \ldots x_n\rangle =$
  $\frac{1}{\sqrt{2^n}} \bigotimes_{j \in \{0,\ldots,n-1\}} (|0\rangle + \mathbf{exp}(2\pi i\, (0.x_{n-i} \ldots x_n)) |1\rangle$ **where**
  $0.x_{n-i} \ldots x_n$ **is a fixed point binary fraction**
  Proof: Omitted due to time

3.3 Quantum phase estimation



- **Quantum phase estimation uses QFT to generalise the Hadamard test. The state is projected onto some P_j subspace (with probability $|P_j|\,|\psi\rangle\,|^2$), and we obtain the t most significant bits of the fixed point binary representation of γ_j where the eigenvalue of P_j is $\exp(2\pi i\gamma_j)$**

- Intuition: Each $U^{(2^j)}$ doubles the phase of U causing a bit shift in γ_j. The $QFT^\dagger$ then extracts the most-significant fractional bit from the amplitude of $|1\rangle$ on each wire.

4 Quantum Algorithms For Optimization

4.1 Variational Quantum Algorithms (VQA)

4.1.1 Motivation

- Because we are currently in the NISQ (Noisy Intermediate-scale Quantum) era of quantum computing hardware, we have enough qbits for quantum advantage in principle but not enough qbits to be able to do error correction (to account for the noisiness) on large enough inputs for the algorithms we have seen so far to have demonstrable quantum advantage
- VQA solves problems of the form: Given a Hermitian matrix H compute the smallest eigenvalue. In physics terms: Given a Hamiltonian H compute the ground state energy
- It is unfortunate that we have a notation clash with the Hadamard gate, but this is the standard notation!

- BQP is the quantum equivalent of P
- QMA is the quantum equivalent of NP
- $P \subseteq BQP \subseteq QMA$
- $NP \subseteq QMA$
- $\exists X : X \in NP$ but $X \notin BQP$
- $\exists X : X \in BQP$ but $X \notin NP$
- k-local-Hamiltonian = Given a Hermitian matrix $H = \sum_i H_i$, where each H_i acts on at most k qbits, compute the smallest eigenvalue. This sounds similar to k-SAT because it is:
  $k - local - Hamiltonian \in QMA - Complete$. Thus, as VQA can solve k-local-Hamiltonian, VQA can solve any $X \in QMA$ and so certainly any $X \in NP \cup BQP$. However, VQA takes exponential time unless approximations are acceptable (in which case heuristics can be used)

4.1.2 VQA framework

VQA framework for solving some problem X:

1. Determine how to express X as finding the ground state energy of a Hamiltonian H

2. Identify a quantum algorithm to estimate the energy $\langle\psi| H |\psi\rangle$ of a given state $|\psi\rangle$

3. Select a family of states $\psi(\overrightarrow{\theta})$ to consider. Restricting our attention in this way means we may only approximate the ground state energy

4. Use a classical optimization algorithm (eg gradient decent) to solve $\min_{\overrightarrow{\theta}} C(\overrightarrow{\theta}) = \langle\psi(\overrightarrow{\theta})| H |\psi(\overrightarrow{\theta})\rangle$ with the aid of the quantum oracle from step 2

4.1.3 VQA framework: Step 1

- **Many NP-Complete problems correspond to finding the ground state energy of some Ising Spin Glass Hamiltonian:** $\boldsymbol{H = -1\left(\sum_{i,j}\left(J_{ij}Z_i \otimes Z_j\right) + \mu\left(h_i z_i\right)\right)}$ where Zs are the Pauli gate, and μ, J_{ij}, h_i are constants encoding the problem.

- MAX-CUT corresponds to $H(\overrightarrow{x}) = \sum_{i,j \in E(G)} 1 - 2\sum_{i,j \in E'(G)}$ where $E'(G)$ denotes the edges that cross the cut induced by $\overrightarrow{x}$. This in turn corresponds to (PROVE IT!) $H = \sum_i, j \in E(G) Z_i \otimes Z_j$ where $Z_i, Z - j$ denotes Z gates on the ith and jth qbits (and I gates everywhere else). This is an Ising Spin Glass Hamiltonian with $\mu = 0$ and $J_{ij} = -1\ \forall i, j$.

4.1.4 VQA framework: Step 2

- We will decompose H into Pauli's as these are best for NISQ measurements
- Ising Spin Glass Hamiltonians are already written as a sum of Paulis
- It is known that for any n-bit Hamiltonian H, $\exists \boldsymbol{P_1, ..., P_n} \in \boldsymbol{\{I, X, Y, Z\}} : \boldsymbol{H = \sum_i c_i P_i}$ for a sequence of Paulis P_is of the appropriate length and vector c_i
- **Pauli decomposition: Define $< \boldsymbol{A, B} >= \frac{\mathbf{Trace}(\boldsymbol{A^\dagger B})}{\boldsymbol{2^n}}$ (recall that the trace is the sum along the leading diagonal) where $\boldsymbol{n}$ is the number of qbits $\boldsymbol{H}$ (or equiv $\boldsymbol{P_j}$) operates on. Then, each $\boldsymbol{c_i} =< \boldsymbol{P_i, H} >$**
- N copies of $|\psi\rangle$ will be prepared for us by the VQA process. For each j, we will compute $\langle\psi| P_j |\psi\rangle$ on the j^{th} copy of $|\psi\rangle$

- Using a Hadamard test we can measure the ± 1 eigenvalue of P_j (probabilistically collapsing into one or the other in the likely event that $|\psi\rangle$ is not an eigenstate of P_j). Call the measurement outcome $O_i \in \{-1, +1\}$. By making K runs for each P_j, we can classically compute an estimate $O = \frac{\sum_i O_i}{K}$ of $\langle\psi| P_j |\psi\rangle$. Using our decomposition, we can classically compute an estimate of $\langle\psi| H |\psi\rangle$

4.1.5 VQA framework: Step 4

- Gradient decent is the most straightforward choice, but there are the risks of local minima and flat regions

- Proposition: If E is a sum of Pauli's, then $\frac{\partial}{\partial\theta}(E(\theta)) = E\left(\theta + \frac{\pi}{4}\right) - E\left(\theta - \frac{\pi}{4}\right)$
  Proof: Out of scope
  Corollary: We don't have to use the limit definition to approximate the gradient

- We could use **Monte-Carlo optimization** instead of gradient decent: **At each step $t+1$ randomly vary a parameter in θ_t to obtain a candidate θ'_t. Let $\delta = E(\theta'_t) - E(\theta_t)$. If $\delta \leq 0$, certainly set $\theta_{t+1} = \theta'_t$. If $\delta > 0$, set $\theta_{t+1} = \theta'_t$ with probability $\exp(-\beta\delta)$ and set $\theta_{t+1} = \theta_t$ otherwise**. temperature $= \frac{1}{\beta}$ — β is often set to increase alongside round number t

4.2 Quantum Machine Learning

4.2.1 Quantum neural network

- Quantum neural network inference: Encode input x into a quantum state $|\phi(x)\rangle$. Use a variational circuit $U(\theta)$ with trainable parameters θ to obtain an output z. Apply an activation function f to z
- **Quantum neural network training: In the style of VQA, search for a $\boldsymbol{\theta}$ that minimizes $\langle \boldsymbol{\phi(x)}| \boldsymbol{U^\dagger(\theta) f(z) U(\theta)} |\boldsymbol{\phi(x)}\rangle$**
- **Basis encoding: $\boldsymbol{\phi_B(x) = |x_{n-1} ... x_0\rangle}$**
- **Amplitude encoding: $\boldsymbol{\phi_A(x) = \frac{1}{n} \sum_{i \in \{0,...,n-1\}} x_i |i\rangle}$**
- Amplitude encoding only requires $\log_2 n$ qbits whereas basis encoding requires n qbits
- **Unitary encoding: $\boldsymbol{\phi(x) = V(x) |0\rangle}$** where V is a given unitary

4.2.2 Quantum kernels

- Recall the SVM kernel trick, and that is corresponds to altering the definition of the inner product
- **The inner product is easy to product in a quantum circuit. To compute $|\langle \phi(y)|\phi(x)\rangle|^2$ we simply use the circuit $U_\phi^\dagger(y)U_\phi(x)\,|0\rangle^{\otimes n}$**

5 Measurement-Based Quantum Computing (MBQC)

5.1 Foundations

- Our entanglement resources is defined as a graph state: Each vertex corresponds to a qbit initialized to $|+\rangle$. For each edge apply $\bigwedge Z$ (for control Z it does not matter which qbit is the control), thus entangling the endpoints. That is that $|\boldsymbol{G}\rangle = \left(\prod_{\boldsymbol{a},\boldsymbol{b}\in\boldsymbol{E}} \wedge \boldsymbol{Z}_{(}\boldsymbol{a},\boldsymbol{b})\right)|+\rangle^{\otimes|\boldsymbol{V}|}$
- $\boldsymbol{\bigwedge Z}$ **commutes with other** $\boldsymbol{\bigwedge Z}$**s**
- $\boldsymbol{M_j^B}$ **= measurement of** $\boldsymbol{j^{\text{th}}}$ **qbit in basis** $\boldsymbol{B}$
- $\boldsymbol{Z}$**-basis** $= \{|0\rangle, |1\rangle\}$
- $\boldsymbol{\theta}$**-basis** $= \{|+_\theta\rangle, |-_\theta\rangle\}$ **where** $|\pm_\theta\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm \exp(i\theta)|1\rangle)$

- **By convention inputs are on the far LHS of G and outputs are on the far RHS of G. Non-output nodes are labelled with their measurement (typically a measurment angle θ with which to measure in the θ-basis) and the outcome of their measurement**

5.2 Correcting measurement angles

- If the measurement outcome is 0, then the measured qbit collapsed into the $+_\theta$ state and the state teleported to the neighbour as wanted. If a measurement outcome is 1, then the state teleported to the neighbour with an unwated X applied

- Proposition: **For each $i \in V$, $K_i = X_i \left(\prod_{j \in N_G(i)} Z_j\right)$ is a stabilizer of $|G\rangle$** ($|G\rangle$ is an eigenstate with eigenvalue $+1$)
  Proof: Omitted due to time

- **A qbit i needs an X correction from the qbit $f^{-1}(i)$ and Z corrections from each qbit in $\{j : i \in N_G(f(j))$ and $j \neq i\}$**
- **An X correction corresponds to correcting a ϕ to $-\phi$ and a Z correction corresponds to correcting a ϕ to $\phi + \pi$**
- We can only rewrite the correction of intermediate qbits in this way as changes to the measurement angles in this way, the output qbits must actually have gates applied

5.3 Blind MBQC

- Alice will prepare single qbits. Bob: store qbits, entangle qbits, make measurements, apply gates. Can Alice use Bob as a quantum computing cloud while keeping her data private?

- Alice can use MBQC and hide both her true resource state $|G\rangle$ and her true measurement angles from Bob

- Measurement angles can be hidden because rotations and the same axis are additive (and so commute). Alice sends Bob an angle $\phi + \theta$ to measure in and keeps θ secret, she pre-rotates her states by θ and so Bob is really measuring in ϕ without knowing ϕ

- Hiding the measurement angles means the measurement outcome is also hidden as which corrections to apply are only known to Alice

- Each step in the computation requires Bob to communicate with Alice to correct the output of that step then apply a new secret rotation to obtain the state for Bob to use in the next step

6 Quantum Error Correcting Codes (QECC)

6.1 Quantum error correction

- When error correcting quantum computers we need to deal with phase flips as well as bit flips
- We cannot make independent replicas of quantum states (due to the no-cloning theorem), we can only create redundancy through entanglement: Let $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$. Then, $CNOT(|\psi\rangle \otimes |0\rangle) = a\,|00\rangle + b\,|11\rangle$
- Principle of digitization of error: Every error (other than those that cause the state to actually collapse, which we can't do anything about because of no cloning) can be expressed as a unitary that rotates the Bloch sphere and so can be rewritten using X and Z gates only. Thus, the ability to detect and correct X-errors (bit-flips) and Z-errors (phase flips) is sufficient despite the continuous nature of quantum computation

- **Proposition: A pair of Pauli operators (tensor products of single-qbit Paulis) which have an odd number of overlaps (on the same qbit there is a different Pauli to itself that is also not I) anti-commute. A pair of Pauli operators which have an even number of overlaps commute**
  Proof sketch: Single-qbit Paulis anti-commute. Thus, each overlap multiplies on a (-1) phase, creating the described effect

6.2 Stabilizers and logical operators

- The Pauli group $P = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}$. A stabiliser group S_G is an $S_G \subseteq P^{\otimes n}$ such that $\forall G_i \in S_G; G_i |\psi\rangle_L = |\psi\rangle_L$ or equivalently logical basis states are eigenstates of G_i with eigenvalue +1

- Recall from group theory that $\langle S \rangle = \{U^k : U \in S, k \in \mathbb{Z}\}$. **We detect errors by running Hadamard tests with each element in turn of a generating set of stabalizers** $S \subseteq S_G$ such $\langle S \rangle = S_G$.

Outcome of 0 means the error operator (if there is one at all eg may be I) commutes with S, outcome of 1 means the error operator anti-commutes with S. **We call the concatenation of Hadamard test outcomes the error syndrome**

- By using a Hadamard test to measure the error without measuring the underlying state, we can carry on applying quantum operations to our state (having applied any necessary quantum error correcting operation if an error was detected) as we have not collapsed the actual information in it
- **A generating set $\boldsymbol{S}$ is minimal iff** $\boldsymbol{\forall U \in S; \forall T \subseteq S; U \neq \prod_{U' \in T} U'}$
- **number of logical qbits $\boldsymbol{k}$ encoded by $\boldsymbol{n}$ physical qbits:** $\boldsymbol{k = n - \text{rank}(S_G) = n - |S|}$ **where $\boldsymbol{|S|}$ is the size of a minimal generating set**

- **An $[n, k, d]$ code is an encoding of k logical bits into n physical bits such that the minimum distance between codewords is d error operations**
- Proposition: **Let t = maximum number of error operations that can occur for a state to always be able to be corrected. Then $t = \lfloor \frac{d-1}{2} \rfloor$**
- Unique syndromes are sufficient but not necessary to be able to correct all errors, as we can get d high enough by other means as we only need their to be able to correct every error operator into a stabilizer not necessarily I specifically
- **L_G = group of logical operators = set of Pauli operators that act non-trivially on basis states and commute with all the operators in S_G**
- Proposition: $\forall L_i \in L_G; \forall S_i \in S_G; S_i L_i \in L$

Proof: Exercise (hint: $G_i L_i = L_i G_i$ by definition of logical operator)

- For a stabilizer code we must chose a logical operator X_L such that $X_L \left|0\right\rangle_L = \left|1\right\rangle_L$ and $X_L \left|1\right\rangle_L = \left|0\right\rangle_L$ and a logical operator Z_L such that $Z_L \left|0\right\rangle_L = \left|0\right\rangle_L$ and $Z_L \left|1\right\rangle_L = -1 \left|1\right\rangle_L$

- Proposition: **$\boldsymbol{d}$ = number of non-$\boldsymbol{I}$ gates in a logical operator for which this counter is minimal (which may not be $\boldsymbol{X_L}$ nor $\boldsymbol{Z_L}$ but rather their product with a stabilizer)**
  Proof: Out of scope

6.3 Code concatenation

- Designate one code as outer and the other as inner
- $|\psi\rangle_{\boldsymbol{L}} = \otimes_{\phi \in |\psi\rangle_{\boldsymbol{L}}^{\text{outer}}} |\phi\rangle_{\boldsymbol{L}}^{\text{inner}}$
- **Stabilizer set = inner stabilizer with a (suitably re-indexed) copy for each qbit in the outer code unioned with outer stabilizers with their Pauli's replaced by the corresponding logical Pauli in the inner code**
- **Each logical operator = logical operator in outer code with its Pauli's replaced by the corresponding logical Pauli in the inner code**
- **A CSS-code is a code for which the stabilizers can be partitioned into ones that only contain Is and Xs (detect phase flips only) and ones that only detect Is and Zs (detect bit flips only). For a concatenated CSS-code, $\boldsymbol{d = \min\left(d_X^{\text{outer}} d_X^{\text{inner}}, d_Z^{\text{outer}} d_Z^{\text{inner}}\right)}$**

6.4 Surface codes

- In a Tanner graph: circles denote data qbits, and squares denote syndrome measurements (where the type of lines coming out of to the data qbits determines the type of stabalizer it measures according to a key provided with the graph)
- **Xs on the physical qbits of any left-to-right path across the surface code is an X_L — if this occurs as an error, then there is zero syndrome but the data has been changed!**
- **Zs** on the physical qbits of any **top-to-bottom** path across the surface code is a $\boldsymbol{Z_L}$ — if this occurs as an error, then there is zero syndrome but the logical data has been changed!
- **Zero syndrome errors that neither an $\boldsymbol{X_L}$ nor a $\boldsymbol{Z_L}$ are stabilisers — if these occur as an error, then there is no problem as the logical data is unaffected**

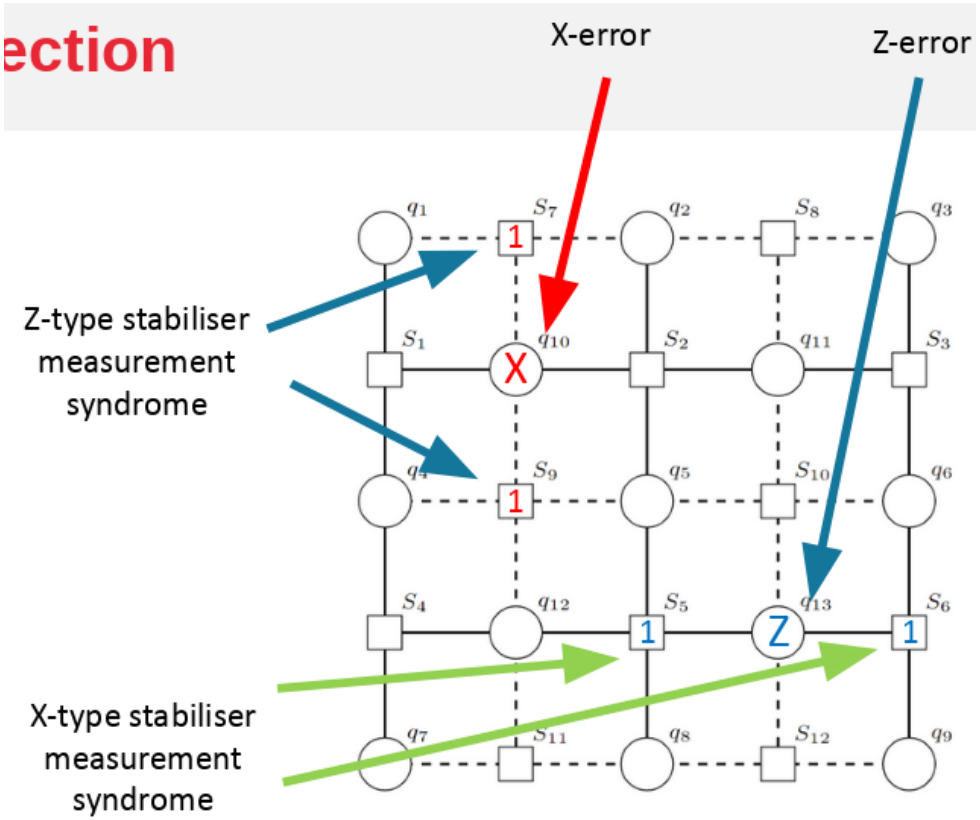


Figure 1: A surface code for a single logical qbit. Can be tiled for more logical qbits

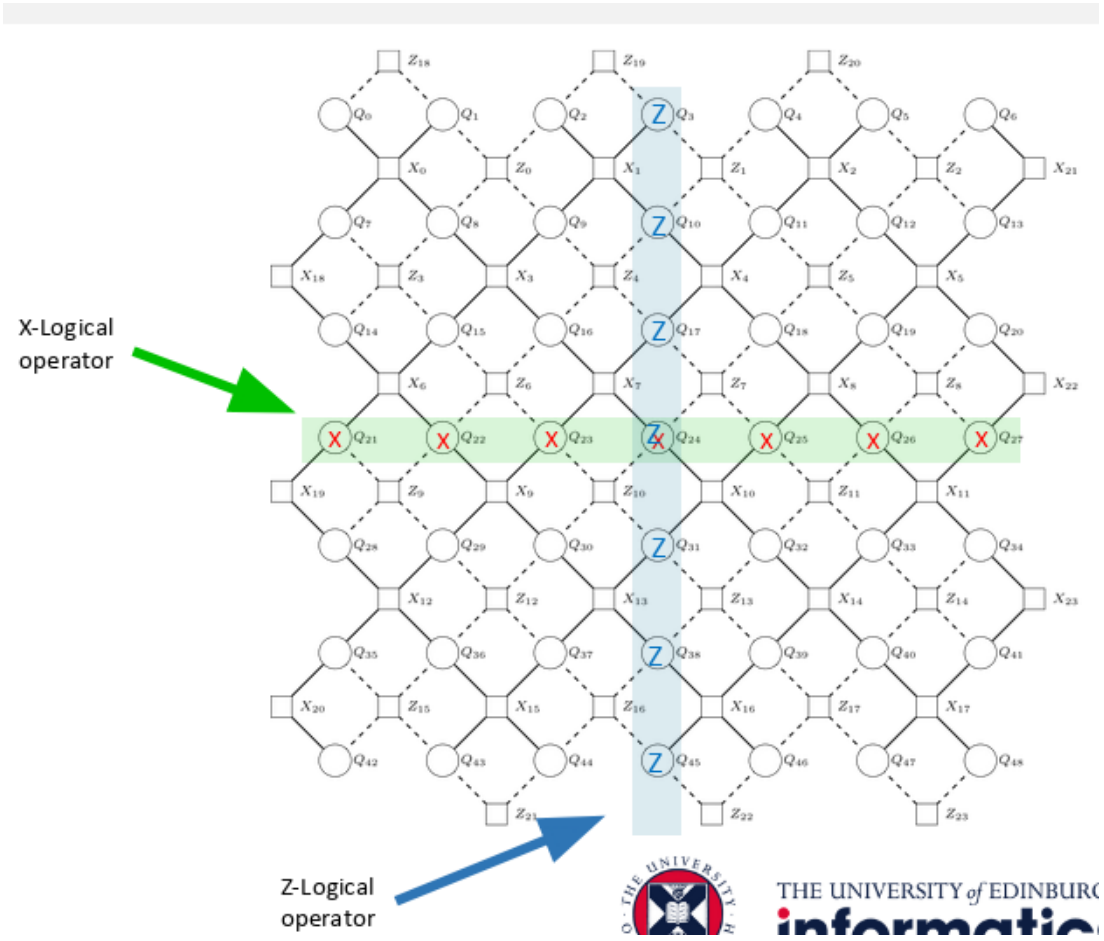


Figure 2: A rotated surface code. The same rules apply