AT24 Quantum Computing @ Imperial College London by ck21

Single qubit operations

$A_{xy} = \langle x|A|y\rangle \langle, x|A|\psi\rangle = \sum_y A_{xy}\psi_y . Z\,|0\rangle = |0\rangle\ ,\ Z\,|1\rangle = -\,|1\rangle\ .$

$|0\rangle\langle 1| = \begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}0 & 1\end{pmatrix} = \begin{pmatrix}0 & 1\\0 & 0\end{pmatrix}$ $|0\rangle\langle 1|\,|1\rangle = |0\rangle\,|0\rangle\,\langle 1|\,|0\rangle = 0$

Resolution of Unity: $\sum_n |n\rangle\langle n| = \mathbb{I}$

Orthonormal Basis ($o.n.$) Orthogonal (right angle) & Length 1: $\{|b_0\rangle \dots |b_{N-1}\rangle\}$

$\langle e_i|e_j\rangle = \delta_{ij} = \begin{cases}1 & \text{if } i = j\\ 0 & \text{if } i \neq j\end{cases}$

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

$$H\,|0\rangle = \frac{1}{\sqrt{2}}(X+Z)\,|0\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |0\rangle)$$

$$H^{-1} = H,\quad H\,|1\rangle = \frac{1}{\sqrt{2}}(X-Z)\,|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$C_{10} = \begin{bmatrix}1 & 0 & 0 & 0\\0 & 1 & 0 & 0\\0 & 0 & 0 & 1\\0 & 0 & 1 & 0\end{bmatrix}$$

Universality and the generalised born rule

Universality. Controlled-U Gates are operations that act as U only if the control qubit is in state 1. C^U for controlled U operation. So, X can be a controlled U operation, which corresponds to the CNOT case. $|x\rangle\, X^x\, |y\rangle = |x\rangle\,|y \oplus x\rangle$

QC can implement approximately any unitary on n qubits → Universal Quantum Computer. Every unitary can be written as a product of single qubit and CNOT gates e.g. Toffoli. Every single qubit gate can also be approximated using only H and T gates $\mathbb{G} = \{CNOT, H, T\}$

If $|\psi\rangle = \Sigma_{x=0}^{2^n-1}\gamma_x\,|x\rangle_n$, if we apply the gate to measure all qubit, the system is projected onto $|x\rangle_n$ then we readout x with probability $|\gamma_x|^2$.

Quantum State Representation.

$$|\psi\rangle = \sum_{x_{n-1},\dots,x_0} \alpha_{x_{n-1}\dots x_0}\,|x_{n-1}\cdots x_0\rangle\ ,\quad \text{with probability } |\alpha_{x_{n-1}\dots x_0}|^2.$$

If factorizable:

$$|x\rangle \otimes |\phi_x\rangle\ ,\quad x \in \{0,1\},$$

where $|x\rangle$ is a classical bit (encoded as a quantum state) and $|\phi_x\rangle$ is the conditional superposition state.

State Decomposition. For a 2-qubit system:

$$|\psi\rangle = \sum_{x_1=0}^{1}\sum_{x_0=0}^{1}\gamma_{x_1x_0}\,|x_1x_0\rangle = |0\rangle\sum_{x_0=0}^{1}\gamma_{0x_0}\,|x_0\rangle + |1\rangle\sum_{x_0=0}^{1}\gamma_{1x_0}\,|x_0\rangle\ .$$

Define $\alpha_0 = \sqrt{\sum_{x_0=0}^{1}|\gamma_{0x_0}|^2}$ and $\alpha_1 = \sqrt{\sum_{x_0=0}^{1}|\gamma_{1x_0}|^2}$:

$$|\psi\rangle = \alpha_0|0\rangle \otimes |\phi_0\rangle + \alpha_1|1\rangle \otimes |\phi_1\rangle\ ,$$

where $|\phi_0\rangle = \frac{1}{\alpha_0}\sum_{x_0=0}^{1}\gamma_{0x_0}\,|x_0\rangle$ and $|\phi_1\rangle = \frac{1}{\alpha_1}\sum_{x_0=0}^{1}\gamma_{1x_0}\,|x_0\rangle$.

Normalization Condition.

$$\langle\phi_0|\phi_0\rangle = \frac{1}{|\alpha_0|^2}\sum_{x_0=0}^{1}|\gamma_{0x_0}|^2 = 1 \implies \alpha_0 = \sqrt{\sum_{x_0=0}^{1}|\gamma_{0x_0}|^2}.$$

$$\langle\phi_1|\phi_1\rangle = \frac{1}{|\alpha_1|^2}\sum_{x_0=0}^{1}|\gamma_{1x_0}|^2 = 1 \implies \alpha_1 = \sqrt{\sum_{x_0=0}^{1}|\gamma_{1x_0}|^2}.$$

Marginal Probability. Probability of measuring $|x\rangle$:

$$c_x^2 = \sum_{x_0=0}^{1}|\alpha_{xx_0}|^2.$$

Why Normalize? 1. Ensures valid probabilities:
$\sum_{x_{n-1},\dots,x_0}|\alpha_{x_{n-1}\dots x_0}|^2 = 1$. 2. ϕ_x represents the superposition state, and $|x\rangle$ encodes the classical bit as a quantum state.

Bell-EPR State. $|0\rangle\,|0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|0\rangle \to \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

Entanglement and teleportation

Spooky Action. A and B share an EPR pair that's non-separable. We compute first the original marginal statistics of Bob.

$p(x_B) = \Sigma_{x_A=0}^{1}p(x_A, x_B) = \Sigma_{x_A=0}^{1}|\langle x_Ax_B|\psi_{00}\rangle|^2$. Using the GBR and expanding into the A and B components we get

$= \Sigma_{x_A=0}^{1}\langle\psi_{00}|x_Ax_B\rangle x_Ax_B|)\psi_{00}\rangle = \Sigma_{x_A=0}^{1}\langle\psi_{00}(|x_A\rangle\,\langle x_A|\otimes|x_B\rangle\,\langle x_B|)\psi_{00}\rangle$.

We use the Resolution of Unity to get $= \langle\psi_{00}|(\mathbb{1}_2 \otimes |x_B\rangle\,\langle x_B|\,|\psi_{00}\rangle) = \frac{1}{2}$. The only way A can contact B is by acting with U on her qubit. This does not change Bob's marginal statistics.

Teleportation. Achieves the transfer of an arbitrary quantum state from one location to another without the physical movement of the qubit. Leveraging entanglement and classical communication so A transfers state to B, but it is a must to retain classical communication for A to inform B when state has been measured (zx). This enables B to collapse his state back into A's original state.

Deutsch's problem

Quantum Parallelism. $H^{\otimes n}\,|0\rangle_n$. The general case $\implies \frac{1}{\sqrt{2^n}}\Sigma_{x=0}^{2^n-1}\,|x\rangle_n$.

Going to U_f we get $\frac{1}{\sqrt{2^n}}\Sigma_{x=0}^{2^n-1}\,|x\rangle_n\,|f(x)\rangle_m$. Seemingly computed 2^n values of $f(x)$ with one call to U_f. Cannot copy the state $\because$ the no-cloning theorem. But we can apply other gates on $|\psi\rangle$ to extract information we are interested in.

Proving No-Cloning. We cannot clone an arbitrary state, even approximately.
$U\,|\psi\rangle\,|0\rangle \approx |\psi\rangle\,|\psi\rangle\ U\,|\phi\rangle\,|0\rangle \approx |\phi\rangle\,|\phi\rangle$. We take the inner product.
$\langle\phi|\,\langle 0|\,U^\dagger U\,|\phi\rangle\,|0\rangle = \langle\phi|\psi\rangle \approx \langle\phi|\,\langle\phi|\,|\psi\rangle\,|\psi\rangle = \langle\phi|\psi\rangle^2$. Only possible if states are orthogonal or identical.

Deutsch's Problem.

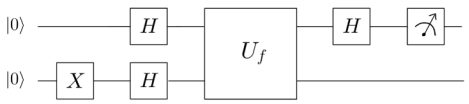


Figure 4.3:

Black box $f(x)$, where x is a single bit $x \in \{0,1\}$ and $f(x)$ returns 0 or 1. Determine if $f(x)$ is constant or balanced $\neq$. Classically - evaluate both $f(0)$ and $f(1)$. Quantum - one shot.

Initialise with $|\psi_0\rangle = |0\rangle\,|1\rangle$. We get
$|\psi_1\rangle = H\otimes H\,|\psi_0\rangle = \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) = \frac{1}{2}(|00\rangle + |10\rangle - |01\rangle - |11\rangle)$. Apply the oracle U_f. $U_f\,|x\rangle\,|y\rangle = |x\rangle\,|y \oplus f(x)\rangle$. $|\psi_2\rangle = U_f\,|\psi_1\rangle$. For $|0\rangle\,|0\rangle$:
$U_f(|0\rangle\,|0\rangle) = |0\rangle\,|0 \oplus f(0)\rangle = |0\rangle\,|f(0)\rangle$
$\implies |\psi_2\rangle = \frac{1}{2}(|0\rangle\,|f(0)\rangle - |0\rangle\,|f(0)\oplus 1\rangle + |1\rangle\,|f(1)\rangle - |1\rangle\,|f(1)\oplus 1\rangle)$. Apply the second H to understand f (relative, not exact value).

Ct Implementation. For $f = NOT$ we can check the circuit acting on $|0\rangle\,|1\rangle$ produces $C_{oi}Z_o\,|0\rangle\,|1\rangle = -C_{oi}\,|0\rangle\,|1\rangle = -\,|1\rangle\,|1\rangle$. And repeat for other combinations

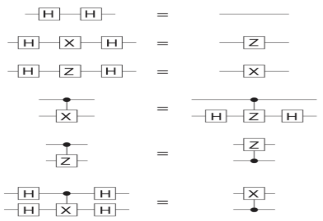
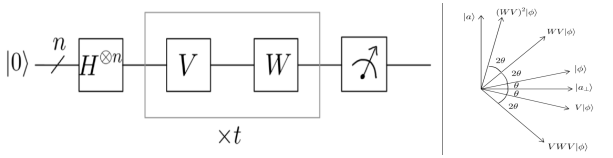


Figure 4.5:

Grover's algorithm for search



We are given a black box function $f(x), x \in \{0, 1, \dots, N-1\}$ and we know that $f(a) = 1$ and $f(x) = 0$ for $x \neq a$.

Initialisation. n qubits in $|0\rangle^{\otimes n}$ state. Apply Hadamard gate to each qubit to create an equal superposition of all 2^n possible states.

$$|\psi_0\rangle = H^{\otimes n}\,|0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}}\Sigma_{x=0}^{2^n-1}\,|x\rangle$$

Apply the Oracle. U_f to flip the phase of the state (or V in some texts) to distinguish $V = 1 - 2\,|a\rangle\,\langle a|\,.V\,|x\rangle = (-1)^{f(x)}\,|x\rangle\ V\,|x\rangle = -\,|a\rangle$ if $x = a$ and $|x\rangle$ if $x \neq a$.

Diffusion Operator for Amplitude Amplification (inversion by mean) W. Reflect the state about the average amplitude to amplify the probability of the marked state. $W = 2\,|\phi\rangle\,\langle\phi| - I\ |\phi\rangle = H^{\otimes n}\,|0\rangle_n = \frac{1}{\sqrt{2^n}}\,|x\rangle_n$

$W\,|v\rangle = \Sigma_x\gamma_x W\,|x\rangle = \Sigma_x\gamma_x(2\,|\phi\rangle\,\frac{1}{\sqrt{N}} - |x\rangle)) = \Sigma_x\,|x\rangle\,(2m - \gamma_x)$

$|v\rangle = (1, 2, -2, 3) \to W\,|v\rangle = (1, 0, 4, -1)$
Smaller than mean, pulled up. Larger than mean, pushed down. $2\cdot mean - \gamma_x$.
Repeat approximately $\sqrt{N}$ times to maximise amplitude of marked state and measure.

2D subspace geometric interpretation of Grover's. Evolves quantum state in 2D plane spanned by two orthonormal vectors $|\phi\rangle$ equal superposition state $|a\rangle$ marked state V reflects state about $|a\rangle$ axis: $-\,|a\rangle\ W$ reflects state about $|\phi\rangle$ axis: $\frac{2}{\sqrt{N}}\,|\phi\rangle - |a\rangle\ sin\theta = \langle a|\phi\rangle = \frac{1}{\sqrt{N}}\ (WV)^t\,|\phi\rangle$ forms angle $(2t+1)\theta$ with $|a_\perp\rangle$.

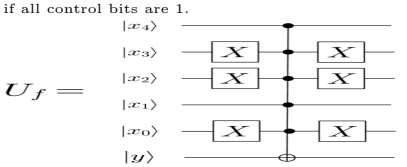
$$(WV)^t\,|\phi\rangle = cos((2t+1)\theta)\,|a_\perp\rangle + sin((2t+1)\theta)\,|a\rangle$$

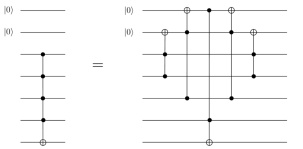
After t steps the probability of measuring a is $sin^2((2t+1)\theta)$ We need $(2t+1)\theta \approx \pi/2$. If N is large, then $\theta \approx \frac{1}{\sqrt{N}}$ $t \approx \frac{\pi}{4}\sqrt{N}$. Note $sin\theta = \sqrt{\frac{m}{N}}$ where m is the number of operations and $N = 2^n$ where n is the number of bits.

Prove Flipping and Fixing. Compute components of the vector $|a_\perp\rangle$. Show that V fixes $|a_\perp\rangle$. Then compute the components of the vector $|\phi_\perp\rangle$ and show that W flips $|\phi_\perp\rangle$
$|a_\perp\rangle = \alpha\,|\phi\rangle + \beta\,|a\rangle$ s.t. orthogonality condition $0 = \langle a|a_\perp\rangle = \alpha\langle a|\phi\rangle + \beta$. So
$|a_\perp\rangle = \underbrace{\alpha(|\phi\rangle - \langle a|\phi\rangle\,|a\rangle)}_{\beta = -\alpha\langle a|\phi\rangle}$

By normalisation.
$1 = \langle a_\perp|a_\perp\rangle = \alpha^2(\langle\psi| - \langle\phi|a\rangle\,\langle a|)(|\phi\rangle - \langle a|\phi\rangle\,|a\rangle) = \alpha^2(1 - \frac{1}{N})$
We need to show that $V\,|a_\perp\rangle = |a_\perp\rangle$. $V = 1 - 2\,|a\rangle\,\langle a|$
Do something similar for ϕ. $|\phi_\perp\rangle = \alpha\,|\phi\rangle + \beta\,|a\rangle$ s.t. $0 = \langle\phi|\phi_\perp\rangle = \alpha + \beta\langle\phi|a\rangle$

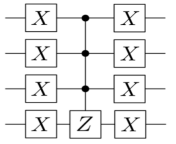
Oracle Implementation. Encode the marked state $|a\rangle$ Use a bitwise XOR operation to identify $|a\rangle$ $x \oplus a$. Use CNOT and Toffoli Gates. CNOT flips the target bit if the control bit is in the $|1\rangle$ state. Gates are used to encode the comparison between x and a. Toffoli Gates act as C^n, where n control qubits are required. Flip the output qubit only if all n control qubits are $|1\rangle$. After identifying the marked state, apply a Z gate / conditional phase flip to $|a\rangle$.
$U_f\,|a\rangle\,|y\rangle = |a\rangle\,|y \oplus 1\rangle$. $U_f\,|x\rangle\,|y\rangle = |x\rangle\,|y\rangle$ for $x \neq a$
$\implies U_f = X^{a\oplus 1^n}C^nX^{a\oplus 1^n}$.
C^n is the NOT gate on the output qubit with n control qubits. Flips the output bit only if all control bits are 1.





Inversion by the Mean W. Phase Flip, Multiply-Controlled Z gate, Followed-up by $X^{\otimes n}$ at start and end to make this usable for 0 and not just 1…1.
Ends up being $X^{\otimes n}(1 - 2\,|1\dots1\rangle\,\langle 1\dots1|)X^{\otimes n}$.

$\mathbf{1} - 2|0\rangle\langle 0| =$



Shor's algorithm for period finding

Efficient quantum algorithm to find period of modular exponentiation.
First introduce n_0 output qubits where n_0 is the number of bits of N and $n = 2n_0$ input qubits. Using $2n_0$ input qubits gives the ability to evaluate $f_{b,N}(x)$ for $x \in \{0, \dots, N^2 - 1\}$
We start with the superposition:
$U_fH^{\otimes n}\otimes\mathbf{1}\,|0\rangle_n\,|0\rangle_{n0} = \frac{1}{\sqrt{2^n}}\Sigma_{x=0}^{2^n-1}\,|x\rangle\,|f_{b,N}(x)\rangle$
Measuring the output register we obtain a y_0 s.t. if $0 \leq x_0 \leq r$ is the first x s.t. $f(x_0) = y_0$ the input qubits are in the state $\frac{1}{m}\Sigma_{k=0}^{m-1}\,|x_0 + kr\rangle$
We used that if $f_{b,N}(x_0) = y_0$ then $f_{b,N}(x_0 + kr) = b^{x_0+kr}\,mod N$
We know that $b^{kr}\,mod N$ is 1 if r is the period.
So adding a multiple of r does not change the output of the modular function $f_{b,N}(x_0 + kr) = y_0, \forall k$. All x values collapse to the same measured result y_0.
m is the smallest value s.t. $x_0 + mr \geq 2^n$

Extraction of r and elimination of x_0 with QFT. Identifies period r from the time domain into the frequency domain; r appears as a peak at a specific frequency proportional to $1/r$. It gives us y from the measurement, which we then use $\frac{y}{2^n} \approx \frac{j}{r}$ to deduce r.

QFT gives

$$QFT(\frac{1}{\sqrt{m}}\Sigma_{k=0}^{m-1}|x_0+kr\rangle) = \frac{1}{\sqrt{2^n m}}\Sigma_{y=0}^{2^n-1}\Sigma_{k=0}^{m-1} e^{2\pi i(x_0+kr)y/2^n}|y\rangle$$

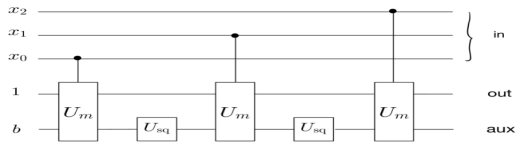
.
The phase term here encodes the information about r. We then get the probability of measuring the value y with $p(y) = \frac{1}{2^n m}|\Sigma_{k=0}^{m-1} e^{2\pi i k r y/2^n}|^2$.
Classical Postprocessing. There is a good chance to measure y close to a multiple of $2^n/r$. We eliminate $e^{\frac{2\pi i}{2^n}krj\frac{2^n}{r}}$ knowing that $e^{2\pi i k r} = 1$.
Utilising $\Sigma_{k=0}^{m-1}\omega^k = \frac{1-\omega^m}{1-\omega}$, setting $\omega = e^{\frac{2\pi i}{2^n}r\delta_j}$.
We obtain $p(y_j) = \frac{1}{2^n m}\frac{sin^2(\pi\frac{r}{2^n}\delta_j m)}{sin^2(\pi\frac{r}{2^n}\delta_j)}$.
$\rightarrow$ bearing in mind the identity $sin(\theta) = (e^{i\theta} - e^{-i\theta}))/(2i)$ and with two assumptions: N is large and $r/2^n$ is small so m can be replaced with $2^n/r$.
Combining this with $sin(x) \approx x$

$$p(y_j) \approx \frac{1}{r}\frac{sin^2(\pi\delta_j)}{(\pi\delta_j)^2}$$

.
Noting that $sin(x) \geq \frac{2}{\pi}x$ for $x \in [0, \pi/2]$ we replace $\pi\delta_j \in (-\pi/2, \pi/2)$ with $|\pi\delta_j| \in [0, \pi/2)$ obtaining $p(y_j) \geq \frac{1}{r}(\frac{2}{\pi})^2$.
So the probability of obtaining any y_j becomes $\Sigma_{j=1}^{r-1}p(y_j) \geq \frac{r-1}{r}\frac{r}{\pi^2} \approx 0.4$
Using the continued fraction method we can go and obtain r. $\frac{y}{2^n} = 0.5$ so candidate $r = 2$. We see that the candidate fails; $7^2 mod 15 = 49 mod 15 = 4 \neq 1$. Next candidate is $r = 4$. This works.
CF Method. invert: 87/19. $a_1 = \lfloor 87/19 \rfloor = 4$. $r_1 = 87/19 - 4 = 11/19$ and repeat. The expansion is $x = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \ldots}}$.
Proving Unitarity of QFT Operator. To prove unitarity, we need to show $U_{FT}^\dagger U_{FT} = I$, and that the rows and columns of the QFT matrix are orthonormal.
We do this by checking $\langle x'|U_{FT}^\dagger U_{FT}|x\rangle = \delta_{x,x'}$ 'Left' side $\rightarrow$

$$U_{FT}|x\rangle = \frac{1}{\sqrt{2^n}}\Sigma_{y=0}^{2^n-1}e^{2\pi i\frac{xy}{2^n}}|y\rangle \ \langle x'|U_{FT}^\dagger = \frac{1}{\sqrt{2^n}}\Sigma_{y=0}^{2^n-1}e^{-2\pi i\frac{x'y}{2^n}}\langle y| \ .$$

Now we compare the cases. If $x = x'$ then the exponential becomes 1. Thus the result is 1.
If not, the phases destructively interfere, giving 0 (Geometric Series expansion, denominator will be not equal to 0 and numerator cancels out due to cyclic summation of phases, like 1 + i - 1 - i = 0).
Thus this aligns with the Kronecker delta.
Modular Exponentiation. Operation of raising the number b to an exponent x and then taking the modulo N. The result is the remainder when b^x is divided by N. It's computationally expensive to directly compute b^x for large x and then taking the modulo. We use repeated squaring. e.g. 2^{13} mod 5: binary of exponent is 1101_2 compute powers: $2^1 mod 5 = 2, 2^2 mod 5 = 4, 2^4 mod 5 = (2^2)^2 = 16 mod 5 = 1$. We know that $2^{13} = 2^8 \cdot 2^4 \cdot 2^1$ and so the final results are $(1 \cdot 1 \cdot 2) mod 5 = 2$.
ModExp Oracle. We perform the binary decomposition of x to simplify $b^x mod N$ $x = x_{n-1}\cdot 2^{n-1} + x_{n-2}\cdot 2^{n-2} + \ldots + x - 1\cdot 2^1 + x_0\cdot 2^0$ This produces $b^{2^{n-1}x_{n-1}} \cdot b^{2^{n-2}x_{n-2}} \ldots$ Which we then put into modular arithmetic $b^{2^{n-1}x_{n-1} \bmod N} \cdot b^{2^{n-2}x_{n-2} \bmod N} \ldots$.
$\implies$ we can implement f as the composition of the n functions in parentheses where at the i-th step we multiply by $b^{2^i x_i} \bmod N$.
Operators. The following operators U_m and U_{sq} are introduced.
$U_m|a\rangle|b\rangle = |a\rangle|ab \bmod N\rangle$ $U_{sq}|b\rangle = |b^2 \bmod N\rangle$.



Step	out	aux
Multiply out with aux if $x_0 = 1$. Then square aux	b^{x_0}	b^2
Multiply out with aux if $x_1 = 1$. Then square aux	$b^{2x_1}b^{x_0}$	b^4
Multiply out with aux if $x_2 = 1$.	$b^{4x_2}b^{2x_1}b^{x_0}$	b^4

We see that indeed the output register has the state $f(x) = b^x$ as claimed.

QFT Summation Breakdown. $U_{FT}|x\rangle = \frac{1}{\sqrt{N}}\Sigma_{y=0}^{N-1}e^{2\pi i\frac{xy}{N}}|y\rangle$. We first break the summation, into components corresponding to each qubit.
$y = 2^3y_3 + 2^2y_2 + 2^1y_1 + y^0y_0$ We substitute this binary form into the phase $e^{2\pi i\frac{xy}{16}} = e^{2\pi i\frac{x}{16}(2^3y_3+\ldots+2^0y_0)}$.
We can expand and group the terms. Each term corresponds to a phase, depending on the binary components of y.
The QFT then transforms $|x\rangle$ into a superposition of states. $|y_3\rangle \otimes \ldots. \otimes |y_0\rangle$.
$U_{FT}|x\rangle = \frac{1}{\sqrt{16}}(|0\rangle + e^{2\pi i\frac{x}{16}}|1\rangle) \otimes \ldots.$
The transformation is distributed across individual qubits.
Hadamard—Controlled-V—Swap. Now we apply the Hadamard to the most significant qubit. Then, we apply controlled-phase gates V_k to introduce relative phases between qubits based on their significance. (Entanglement: x_0 with x_1, x_2, x_3, x_1 with x_2, x_3). $V_k = \begin{bmatrix}1 & 0\\ 0 & e^{i\pi/2^k}\end{bmatrix}$.
These gates are applied conditionally, depending on the state of other qubits. They encode periodicity into the system. The controlled phase gates apply the $e^{2\pi i\phi}$ terms to each qubit. Qubits with higher significance contribute larger phase shifts. After all operations, the qubits are in reverse order; we swap them to restore them to the original order.

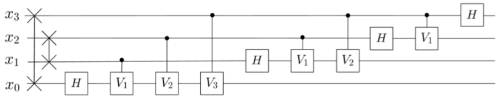
$$CV_{31}CV_{21}H_1|x_0x_1x_2x_3\rangle = CV_{31}CV_{21}|x_0x_1\rangle\frac{1}{\sqrt{2}}(|0\rangle + e^{i\pi x_2}|1\rangle)|x_3\rangle$$

$$= CV_{31}|x_0x_1\rangle\frac{1}{\sqrt{2}}(|0\rangle + e^{i\pi x_2}e^{i\pi\frac{1}{2}x_1}|1\rangle)|x_3\rangle$$

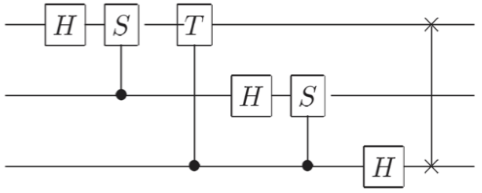
$$= |x_0x_1\rangle\frac{1}{\sqrt{2}}(|0\rangle + e^{i\pi(x_2+\frac{1}{2}x_1)}e^{i\pi\frac{1}{2}x_0}|1\rangle)|x_3\rangle$$

$$U_{FT}|x_3x_2x_1x_0\rangle = H_3(CV_{32}H_2)(V_{31}CV_{21}H_1)(CV_{30}CV_{20}CV_{10}H_0)P|x_3x_2x_1x_0\rangle$$

The quantum circuit is depicted in figure 6.3 where the gate with crosses at the end of a line corresponds to the swap operator of the two qubits that the line connects.



Quantum Ct and Matrix for Inverse QFT.Undoes the phase and entanglement operations by the forward QFT.
$U_{QFT}^\dagger|y\rangle = \frac{1}{\sqrt{N}}\Sigma_{x=0}^{N-1}e^{-2\pi i\frac{xy}{N}}|x\rangle$ with $N = 2^n$ for n qubits $V^\dagger = \begin{bmatrix}1 & 0\\ 0 & -i\end{bmatrix}$
The H acts as the inverse of the initial superposition steps in the forward QFT. The H on the first qubit removes the first level of interference (from $e^{\pm i\pi/2}$).
The controlled-phase gates applies the inverse phases. And the swap gates reverse the qubit order to undo the bit-level reversal.
QFT Matrices.$F = \frac{1}{\sqrt{4}}\begin{bmatrix}1 & 1 & 1 & 1\\ 1 & i & -1 & -i\\ 1 & -1 & 1 & -1\\ 1 & -i & -1 & i\end{bmatrix}$. Conjugate Transpose (swap rows and col and replace i with $-i$) for inverse. Compute the QFT of the two qubit state $(\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}, 0)^T \implies$ Just do the matrix multiplication with QFT matrix.



3 qubit QFT.Build the circuit with H, S, T gates. $S = \begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}$. Phase gate introduces relative phase $\pi/2$. T introduces smaller phase shift $e^{i\pi/4}$. For $n = 3$, the QFT transform includes phases of the form $e^{2\pi i\frac{xy}{2^n}}$. First qubit needs 2^{-1} and 2^{-2} phases. Relative phase of $\pi/4$. Second qubit just needs 2^{-1}.
N_{Ops}. Number of operations is the number of elementary gates. $2N_{FT} + n$ where N_{FT} is the number of operations for the QFT and n the number of gates for Ω. Ω is the product of single gate qubits. $\Omega = \Pi_{j=0}^{n-1}e^{\frac{2\pi i}{2^n}2^j B_j}$. With B_j being the projector on $|1\rangle$ for qubit j. N_{FT} is given by $\lfloor n/2 \rfloor$ swap gates plus n Hadamard plus $n(n-1)/2$ controlled V_k gates.
QCt for Addition Modulo. Consider the task of constructing a quantum circuit to perform addition modulo $2^n : |x\rangle \mapsto |x + 1 mod 2^n\rangle$, $x \in \{0, 1, \ldots, 2^n - 1\}$ Show that one efficient way to do this is to first apply a FT, then a phase shift $\Omega|y\rangle = e^{\frac{2\pi i}{2^n}y}|y\rangle$, then a IFT. $U_{FT}^\dagger\Omega U_{FT}|x\rangle = \frac{1}{2^{n/2}}\Sigma_{y=0}^{2^n-1}e^{\frac{2\pi i}{2^n}xy}U_{FT}^\dagger\Omega|y\rangle$.
We note that $U_{FT}^\dagger|y\rangle = \frac{1}{\sqrt{2^n}}\Sigma_{z=0}^{2^n-1}e^{-2\pi izy/2^n}|z\rangle$. So simplifying we get the Discrete Fourier Sum. $\Sigma_{y=0}^{2^n-1}e^{2\pi iy((x+1)-z)/2^n}$. Which evaluates to 2^n if $(x+1) \equiv z (mod 2^n)$ or 0 otherwise. $(x+1-z) mod 2^n = 0 \implies mod 2^n$ sticks to z? So only the term $z \equiv (x+1) mod 2^n$ survives, making the resulting state $|x + 1 mod 2^n\rangle$.

Quantum error correction

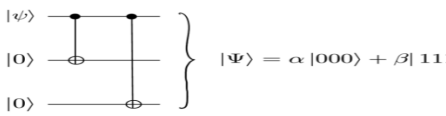
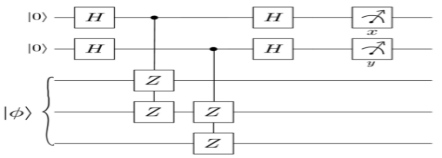
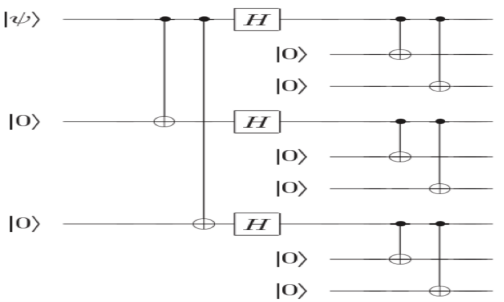


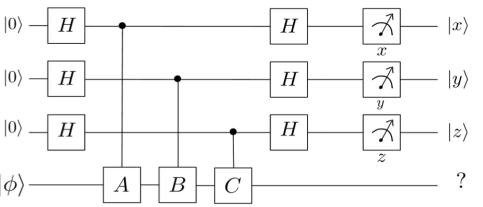
Figure 7.1:



Encoding Circuit. $|\psi\rangle$ with 2 CNOTS for $|0\rangle$ and $|0\rangle$.
$\alpha|0\rangle + \beta|1\rangle = \underbrace{\alpha|000\rangle}_{|\bar{0}\rangle} + \underbrace{\beta|111\rangle}_{|\bar{1}\rangle} = |\Psi\rangle$
Projector onto U eigenspace.
$|0\rangle|\psi\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|\psi\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle\not{|} + |1\rangle U)|\psi\rangle \mapsto$
$\frac{1}{2}(|0\rangle + |1\rangle)\not{|} + (|0\rangle - |1\rangle)U|\psi\rangle = (|0\rangle P_0^U + |1\rangle P_1^U)|\psi\rangle \mapsto |x\rangle P_x^U|\psi\rangle$
The code space is stabilised by Z_0Z_1, Z_1Z_2. From $\sum_{xy}|xy\rangle P_x^{Z_1Z_2}P_y^{Z_1Z_0}|\phi\rangle$,
$(0,0) \rightarrow |\Psi\rangle, (0,1) \rightarrow X_0|\Psi\rangle, (1,0) \rightarrow X_2|\Psi\rangle, (1,1) \rightarrow X_1|\Psi\rangle$).
9-Qubit Case. Drop assumption that only bit flips are allowed, consider a quantum ECC that corrects arbitrary single qubit errors.



Concatenated Design. Inner code protects against BF errors. uses states $|000\rangle$ and $|111\rangle$ as codewords. Outer code protects against phase-flip errors by encoding the logical states $|0\rangle \pm |1\rangle$ from inner code. Uses H transform to relate the errors.
Stabilisers $S_i^Z \rightarrow S_1^Z = Z_8Z_7$, $S_2^Z = Z_7Z_6$. Each stabiliser checks parity between two neighbouring qubits. Bit Flip Stabilisers S_j^X. Detect X type errors and are derived from outer phase flip code. $S_1^X = X_8X_7X_6X_5X_4X_3$, $S_2^X = X_5X_4X_3X_2X_1X_0$. Acts on 6 qubits each.
Commutation. Z error changes eigenvalue of stabiliser S_i^Z that acts on qubit i. Can be distinguished as they commute with all S_j^X but anti-commute with specific S_i^Z. X error anti-commutes with global stabilisers S_1^X or S_2^X - X errors commute with all S_i^Z. $Y = iXZ$ errors combine X and Z effects. Anti-commute with both S_i^Z and S_j^X. Y_3 anti-commutes with S_4^Z and S_1^X



Solution Since they square to 1 and are Hermitian, the eigenvalues are ± 1. We have

$$|0\rangle|0\rangle|0\rangle|\phi\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|\phi\rangle$$
$$\mapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)A\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)B\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)C|\phi\rangle$$
$$\mapsto \frac{1}{\sqrt{2}}(|0\rangle P_1^A + |1\rangle P_{-1}^A)\frac{1}{\sqrt{2}}(|0\rangle P_1^B + |1\rangle P_{-1}^B)\frac{1}{\sqrt{2}}(|0\rangle P_1^C + |1\rangle P_{-1}^C)|\phi\rangle$$
$$\mapsto P_{1-2x}^A P_{1-2y}^B P_{1-2z}^C|\phi\rangle.$$