Contents

1. Hidden subgroup problem

1.1. Review of Shor's algorithm

Definition 1.1 The **factoring problem** is: given a positive integer N, find a non-trivial factor ($\neq 1, N$) in time polynomial in n (i.e. $O(\text{poly}(n))$), where $n = O(\log N)$ is the length of the description of the problem input (memory/space used to store it).

Definition 1.2 An **efficient problem** is one that can be solved in polynomial time.

Remark 1.3 Clasically, the best known factoring algorithm runs in $e^{O\left(n^{1/3}(\log n)^{2/3}\right)}$. Shor's algorithm (quantum) runs in $O(n^3)$ by converting factoring into period finding:

- Given input N, choose $a < N$ which is coprime to N.
- Define $f : \mathbb{Z} \to \mathbb{Z}/N$, $f(x) = a^x \bmod N$. f is periodic with period r (the order of $a \bmod N$), i.e. $f(x+r) = f(x)$ for all $x \in \mathbb{Z}$. Finding r allows us to factor N.

1.2. Period finding

Problem 1.4 (Periodicity Determination) Given an oracle for $f : \mathbb{Z}/M \to \mathbb{Z}/N$ with promises:

- f is periodic with period $r < M$ (i.e. $\forall x \in \mathbb{Z}/M$, $f(x+r) = f(x)$),
- f is one-to-one in each period (i.e. $\forall 0 \leq x < y < r$, $f(x) \neq f(y)$),

find r in time $O(\text{poly}(m))$, where $m = O(\log M)$.

Clasically, this requires takes time $O(\sqrt{M})$.

Definition 1.5 Let $f : \mathbb{Z}/M \to \mathbb{Z}/N$. Let H_M and H_N be quantum state spaces with orthonormal state bases $\{|i\rangle : i \in \mathbb{Z}/N\}$ and $\{|j\rangle : j \in \mathbb{Z}/M\}$. Define the unitary **quantum oracle** for f by U_f by

$$U_f |x\rangle|z\rangle = |x\rangle|z + f(x)\rangle.$$

The first register $|x\rangle$ is the **input register**, the last register $|z\rangle$ is the **output register**.

Definition 1.6 The **quantum query complexity** of an algorithm is the number of times it queries f (i.e. uses U_f).

Definition 1.7 The **quantum Fourier transform** over $\mathbb{Z}/M$ is the unitary defined by its action on the computational basis:

$$U_{\text{QFT}}|x\rangle = \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} \omega^{xy} |y\rangle,$$

where $\omega = e^{2\pi i/M}$. Note that U_{QFT} requires only $O((\log M)^2)$ gates to implement, whereas a general unitary requires $O(4^n/n)$ elementary gates.

Lemma 1.8 Let $\alpha = e^{2\pi i y/M}$. Then

$$\sum_{j=0}^{k-1} \alpha^j = \begin{cases} \frac{1-\alpha^k}{1-\alpha} = 0 \text{ if } \alpha \neq 1 \text{ i.e. } M \nmid y \\ k \qquad\qquad \text{if } \alpha = 1 \text{ i.e. } M \mid y \end{cases}.$$

Lemma 1.9 (Boosting success probability) If a process succeeds with probability p on one trial, then

$$\Pr(\text{at least one success in } t \text{ trials}) = 1 - (1-p)^t > 1 - \delta$$

for $t = \frac{\log(1/d)}{p}$.

Theorem 1.10 (Co-primality Theorem) The number of integers less than r that are coprime to r is $O(r/\log\log r)$ for large r.

Algorithm 1.11 (Quantum Period Finding) Let $f : \mathbb{Z}/M \to \mathbb{Z}/N$ be periodic with period $r < M$ and one-to-one in each period. Let $A = \frac{M}{r}$ be the number of periods. We work over the state space $H_M \otimes H_N$.

1. Construct the state $\frac{1}{\sqrt{M}} \sum_{i=0}^{M-1} |i\rangle|0\rangle$.
2. Query U_f on the state, giving $\frac{1}{\sqrt{M}} \sum_{i=0}^{M-1} |i\rangle|f(i)\rangle$.
3. Measure second register in computational basis, giving outcome $y \in \mathbb{Z}/N$, and input state collapses to $|\text{per}\rangle = \frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} |x_0 + jr\rangle$, where $f(x_0) = y$ and $0 \leq x_0 < r$. TODO: add diagram showing amplitudes for this state.
4. Apply the Quantum Fourier Transform to $|\text{per}\rangle$:

$$\begin{aligned} \text{QFT}|\text{per}\rangle &= \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} \frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} \omega^{(x_0+jr)y} |y\rangle \\ &= \frac{1}{\sqrt{MA}} \sum_{y=0}^{M-1} \omega^{x_0 y} \sum_{j=0}^{A-1} \omega^{jry} |y\rangle \\ &= \sqrt{\frac{A}{M}} \sum_{k=0}^{r-1} \omega^{x_0 kM/r} |kM/r\rangle \end{aligned}$$

   Note now the outcomes and probabilities are independent of x_0, so carry useful information about r. TODO add diagram showing amplitudes for this state.
5. Measure $\text{QFT}|\text{per}\rangle$, yielding outcome $c = k_0 M/r$ for some $0 \leq k_0 < r$. So $\frac{c}{M} = \frac{k_0}{r}$. If k_0 is corpime to r, then the denominator r_0 of the simplified fraction $\frac{c}{M}$ is equal to r.
6. By the coprimality theorem, the probability that k_0 is coprime to r is $O(1/\log\log r)$.
7. To check if the computed value r_0 of r is correct, compute/query U_f to check if $f(0) = f(r_0)$ (this works since f is periodic and one-to-one in each period, and $r_0 \leq r$).
8. Repeat the previous steps $O(\log\log r) = O(\log\log M) = O(\log m)$ times. This obtains the correct value of r with high probability.

1.3. Analysis of QFT part of period finding algorithm

Notation 1.12 For $R = \{0, r, ..., (A-1)r\} \subseteq \mathbb{Z}/M$ $(Ar = M)$, write $|R\rangle$ for the uniform superposition of all computational basis states in R:

$$|R\rangle = \frac{1}{\sqrt{A}} \sum_{k=0}^{A-1} |kr\rangle.$$

Definition 1.13 For each $x_0 \in \mathbb{Z}/M$, define the lienar map by its action on the computational basis states:

$$\begin{aligned} U(x_0) : H_M &\to H_M, \\ |k\rangle &\mapsto |x_0 + k\rangle. \end{aligned}$$

Definition 1.14 Note that since $(\mathbb{Z}/M, +)$ is abelian, all $U(x_i)$ commute: $U(x_1)U(x_2) = U(x_1 + x_2) = U(x_2)U(x_1)$. Hence, they have a simultaneous basis of eigenvectors $\{|\chi_k\rangle : k \in \mathbb{Z}/M\}$, i.e. for all $k, x_0 \in \mathbb{Z}/M$, $U(x_0)|\chi_k\rangle = w(x_0, k)|\chi_k\rangle$, where $|w(x_0, k)| = 1$. The $|\chi_k\rangle$ are called **shift-invariant states** and form an orthonormal basis for H_M. The $|\chi_k\rangle$ are given explicitly by

$$|\chi_k\rangle = \frac{1}{\sqrt{M}} \sum_{\ell=0}^{M-1} e^{-2\pi i k\ell/M} |\ell\rangle.$$

Proposition 1.15 The explicit definition of the $|\chi_k\rangle$ indeed satisfies the property $\forall k, x_0 \in \mathbb{Z}/M$, $U(x_0)|\chi_k\rangle = w(x_0, k)|\chi_k\rangle$, and we have $w(x_0, k) = \omega^{kx_0}$, where $\omega = e^{2\pi i/M}$.

Proof (Hints). Straightforward. □

Proof. We have that

$$\begin{aligned} U(x_0)|\chi_k\rangle &= \frac{1}{\sqrt{M}} \sum_{\ell=0}^{M-1} e^{-2\pi i k\ell/M} |x_0 + \ell\rangle \\ &= \frac{1}{\sqrt{M}} \sum_{\tilde{l}=0}^{M-1} e^{-2\pi i \left(\tilde{l} - x_0\right)k/M} |\tilde{l}\rangle \\ &= e^{2\pi i k x_0/M} |\chi_k\rangle \\ &=: w(x_0, k)|\chi_k\rangle \end{aligned}$$

□

Remark 1.16 Let $U : H_M \to H_M$ be the unitary mapping the shift-invariant basis to the computational basis: $U : |\chi_k\rangle \mapsto |k\rangle$. The matrix representation of U^{-1} with respect to the computational basis has entries

$$\left(U^{-1}\right)_{jk} = \langle j|U^{-1}|k\rangle = \langle j|\chi_k\rangle = \frac{1}{\sqrt{M}} e^{-2\pi i jk/M}$$

So the matrix representation of U with respect to the same basis has entries $U_{kj} = \overline{\left(U^{-1}\right)_{jk}} = \frac{1}{\sqrt{M}} e^{2\pi i jk/M}$. Hence, we have

$$U|k\rangle = \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} e^{2\pi ijk/M} |j\rangle,$$

and so U is precisely the QFT $\bmod M$.

1.4. The hidden subgroup problem (HSP)

Problem 1.17 (Discrete Logarithm Problem (DLP) on $\mathbb{Z}/p^\times$) Let p be prime.

- **Input** $g, x \in \mathbb{Z}/p^\times$.
- **Promise** g is a generator of $\mathbb{Z}/p^\times$.
- **Task** Find $\log_g x$, i.e. find $L \in \mathbb{Z}/(p-1)$ such that $x = g^L$.

Notation 1.18 Write $[n]$ for $\{1, ..., n\}$. Write e.g. ij for the set $\{i, j\}$.

Definition 1.19 Let $\Gamma_1 = ([n], E_1)$ and $\Gamma_2 = ([n], E_2)$ be (undirected) graphs. Γ_1 and Γ_2 are **isomorphic** if there exists a permutation $\pi \in S_n$ such that for all $1 \leq i, j < n$, $ij \in E$ iff $\pi(i)\pi(j) \in E$.

Definition 1.20 Let $\Gamma = ([n], E)$ be a graph. The **automorphism group** of Γ is

$$\mathrm{Aut}(\Gamma) = \{\pi \in S_n : ij \in E \text{ iff } \pi(i)\pi(j) \in E \quad \forall i, j \in [n]\}.$$

$\mathrm{Aut}(\Gamma)$ is a subgroup of S_n, and $\pi \in \mathrm{Aut}(\Gamma)$ iff π leaves Γ invariant as a labelled graph.

Definition 1.21 The **adjacency matrix** of a graph $\Gamma = (V, E)$ is the $n \times n$ matrix M_A defined by its entries:

$$(M_A)_{ij} := \begin{cases} 1 & \text{if } ij \in E \\ 0 & \text{otherwise} \end{cases}.$$

Problem 1.22 (Graph Isomorphism Problem)

- **Input** Adjacency matrices M_1 and M_2 of graphs $\Gamma_1 = ([n], E_1)$ and $\Gamma_2 = ([n], E_2)$.
- **Task** Determine whether Γ_1 and Γ_2 are isomorphic.

Remark 1.23 The best known classical algorithm for solving the graph isomorphism problem has quasi-polynomial time complexity $n^{O((\log n)^2)}$.

Problem 1.24 (Hidden Subgroup Problem (HSP)) Let G be a finite group.

- **Input** An oracle for a function $f : G \to X$.
- **Promise** There is a subgroup $K < G$ such that:
  1. f is constant on the (left) cosets of K in G.
  2. f takes a different value on each coset.
- **Task** Determine K.

Remark 1.25

- To find K, we either find a generating set for K, or sample a uniformly random element from K.

- We want to determine K with high probability in $O(\text{poly} \log|G|)$ queries. Using $O(|G|)$ queries is easy, as we just query all values $f(g)$ and find the "level sets" (sets where f is constant).

Example 1.26 The following problems are special cases of HSP:

- The period finding problem: $G = \mathbb{Z}/M$, $K = \langle r \rangle = \{0, r, ..., (A-1)r\}$. The cosets are $x_0 + K = \{x_0, x_0 + r, ..., x_0 + (A-1)r\}$ for each $0 \leq x_0 < r$.
- The DLP on $(\mathbb{Z}/p)^\times$: let $f : \mathbb{Z}/(p-1) \times \mathbb{Z}/(p-1) \to (\mathbb{Z}/p)^\times$ be defined by $f(a, b) = g^a x^{-b} = g^{a-Lb}$. $G = \mathbb{Z}/(p-1) \times \mathbb{Z}/(p-1)$, the hidden subgroup is $K = \{\lambda(L, 1) : \lambda \in \mathbb{Z}/(p-1)\}$. (Note that if we know K, we can pick any $(c, d) = (\lambda L, \lambda) \in G$ and compute $L = \frac{c}{d}$ to find L.)
- The graph isomorphism problem: $G = S_n$, hidden subgroup is $K = \text{Aut}(G)$. Let $f_\Gamma : S_n \to X$ where X is set of adjacency matrices of labelled graphs on $[n]$, defined by $f_\Gamma(\pi) = \pi(A)$. Note $|S_n| = |G| = n!$, so $\log|G| \approx n \log n$, so $O(\text{poly} \log|G|) = O(\text{poly}\, n)$.

Definition 1.27 An **irreducible representation (irrep)** of a finite abelian group G is a homomorphism $\chi : G \to \mathbb{C}^\times$.

Theorem 1.28

- Let $\chi : G \to \mathbb{C}^\times$ be an irrep. For all $g \in G$, $\chi(g)$ is a $|G|$-th root of unity.
- There are always exactly $|G|$ distinct irreps. In particular, we can label each irrep uniquely by some $g \in G$.

Theorem 1.29 (Schur's Lemma) Let χ_i and χ_j be irreps of G. Then

$$\frac{1}{|G|} \sum_{g \in G} \chi_i(g) \overline{\chi_j}(g) = \delta_{ij}.$$

Example 1.30 $\chi_0 : G \to \mathbb{C}^\times$, $\chi_0(g) = 1$ is the **trivial irrep**. Note that for any $\chi_i \neq \chi_0$, $\sum_{g \in G} \chi_i(g) = 0$ by Schur's lemma.

Definition 1.31 For finite abelian G, we define the **shift operators** on $H_{|G|}$ for each $k \in G$ by

$$\begin{aligned} U(k) : H_{|G|} &\to H_{|G|}, \\ |g\rangle &\mapsto |k + g\rangle. \end{aligned}$$

Note that since G is abelian, the $U(k)$ commute: $U(k)U(l) = U(l)U(k)$ for all $k, l \in G$. Hence, they have simultaneous eigenstates, which gives an orthonormal basis for $H_{|G|}$.

Proposition 1.32 For each $k \in G$, consider the state

$$|\chi_k\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} \overline{\chi_k(g)} |g\rangle.$$

The $|\chi_k\rangle$ are shift-invariant (invariant up to a phase under the action of all $U(g)$, $g \in G$).

Proof (Hints). Straightforward. □

Proof.

- Note that $\overline{\chi_k(g)} = \chi_k(-g)$.
- We have

$$\begin{aligned}
U(g_0)|\chi_k\rangle &= \frac{1}{\sqrt{|G|}} \sum_{g \in G} \overline{\chi_k(g)} |g_0 + g\rangle \\
&= \frac{1}{\sqrt{|G|}} \sum_{g' \in G} \overline{\chi_k(g' - g_0)} |g'\rangle \\
&= \frac{1}{\sqrt{|G|}} \sum_{g' \in G} \overline{\chi_k(g')} \chi_k(g_0) |g'\rangle \\
&= \chi_k(g_0)|\chi_k\rangle.
\end{aligned}$$

□

Definition 1.33 The **quantum Fourier transform (QFT)** on $H_{|G|}$ is the unitary implementing the change of basis from the shift-invariant states $\{|\chi_g\rangle : g \in G\}$ to the computational basis $\{|g\rangle : g \in G\}$.

Note that $\mathrm{QFT}^{-1}|g\rangle = |\chi_g\rangle$. So $\left(\mathrm{QFT}^{-1}\right)_{kg} = \langle k|\chi_g\rangle = \frac{1}{\sqrt{|G|}}\overline{\chi_g(k)}$, so $\mathrm{QFT}_{kg} = \frac{1}{\sqrt{|G|}}\chi_k(g)$. So the explicit form is

$$\mathrm{QFT}|g\rangle = \frac{1}{\sqrt{|G|}} \sum_{k \in G} \chi_k(g)|k\rangle.$$

Example 1.34

- For $G = \mathbb{Z}/M$, we can check that $\chi_a(b) = e^{2\pi i ab/M}$ are irreps. So the irreps of $\mathbb{Z}/M$ are naturally labelled by $a \in \mathbb{Z}/M$ and this gives the usual $\mathrm{QFT} \bmod M$ as defined earlier.
- Similarly, for $G = \mathbb{Z}/(M_1) \times \cdots \times \mathbb{Z}/(M_r)$, $\chi_g(h) = e^{2\pi i (g_1 h_1/M_1 + \cdots + g_r h_r/M_r)}$ are the irreps.

Algorithm 1.35 (Quantum HSP solver for finite abelian G)

- We work in the state space $H_{|G|} \otimes H_{|X|}$.
- Prepare the state

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle|0\rangle$$

- Query f on the state, giving

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle|f(g)\rangle$$

- Measure the output register, yielding a uniformly random value $f(g_0)$ from $f(G)$. The state collapses to a **coset state**

$$|g_0 + K\rangle = \frac{1}{\sqrt{|K|}} \sum_{k \in K} |g_0 + k\rangle.$$

- Apply QFT mod $|G|$, and measure the input register, yielding some $g \in G$. We have $|K\rangle = \sum_{g \in G} a_g |\chi_g\rangle$, so $|g_0 + K\rangle = U(g_0)|K\rangle = \sum_{g \in G} a_g \chi_g(g_0)|\chi_g\rangle$. So applying QFT gives $\sum_{g \in G} a_g \chi_g(g_0)|g\rangle$, so probability of measuring outcome k is $|a_k \chi_k(g_0)|^2 = |a_k|^2$. Now

$$\begin{aligned}\mathrm{QFT}|K\rangle &= \frac{1}{\sqrt{|K|}} \sum_{k \in K} \mathrm{QFT}|k\rangle \\ &= \frac{1}{\sqrt{|G||K|}} \sum_{g \in G} \left(\sum_{k \in K} \chi_g(k) \right) |g\rangle\end{aligned}$$

Note that irreps of G restricted to K are irreps of K. The trivial irrep $\chi_0 : G \to \mathbb{C}$ remains the trivial irrep χ_0 for K. But there may be other irreps that become the trivial irrep on restriction to K. Hence

$$\sum_{k \in K} \chi_g(k) = \begin{cases} |K| & \text{if } \chi_g|_K = \chi_0|_K \\ 0 & \text{otherwise} \end{cases}$$

Hence

$$\mathrm{QFT}|K\rangle = \sqrt{\frac{|K|}{|G|}} \sum_{\substack{g \in G \\ \chi_g|_K = \chi_0|_K}} |g\rangle$$

and measuring in the computational basis on this state yields random $g \in G$ such that $\forall k \in K$, $\chi_g(k) = 1$.

If K has generators $k_1, ..., k_m$ (note that for an arbitrary group, we have $m = O(\log|G|)$), then we have a set of equations $\chi_g(k_i) = 1$ for all $i \in [m]$. We can show that $O(\log|G|)$ such g are drawn uniformly at random, then with probability at least $2/3$, we have enough equations to determine $k_1, ..., k_m$.

Example 1.36 Let $G = \mathbb{Z}/M_1 \times \cdots \times \mathbb{Z}/M_r$. The irreps are $\chi_g(h) = e^{2\pi i (g_1 h_1/M_1 + \cdots + g_r h_r/M_r)}$. For $k \in K$, $\chi_g(k) = 1$ iff $\frac{g_1 k_1}{M_1} + \cdots + \frac{g_r k_r}{M_r} = 0 \bmod 1$. This is a homogenous linear equation in k, and $O(\log|G|)$ independent such equations determine K as the nullspace.

Remark 1.37 We can implement QFT over abelian groups (and some non-abelian groups, including S_n) using circuits with $O((\log|G|)^2)$ elementary gates.

In the non-abelian case, we can still easily prepare coset states with one query to f. But the shift operators $U(g_0)$ no longer commute, so we don't have a (canonical) shift-invariant basis.

Definition 1.38 A ***d*-dimensional unitary representation** of a finite group G is a homomorphism

$$\chi : G \to U(d)$$

where $U(d)$ is the group of $d \times d$ unitary matrices.

Definition 1.39 A d-dimensional unitary representation χ of G is **irreducible** if no non-trivial subspace of $\mathbb{C}^d$ is invariant under the action of $\{\chi(g_1), ..., \chi(g_{|G|})\}$ (i.e. we cannot simultaneously block diagonalise all the $\chi(g)$ matrices by a basis change).

Definition 1.40 A set of irreps $\{\chi_1, ..., \chi_m\}$ is a **complete set of irreps** for every irrep χ of G, there exists $1 \leq i \leq m$ such that χ is unitarily equivalent to χ_i, i.e. for some $V \in U(d)$, $\forall g \in G, \chi(g) = V\chi_i(g)V^\dagger$.

Theorem 1.41 Let the dimensions of a complete set of irreps $\chi_1, ..., \chi_m$ be $d_1, ..., d_m$. Then $d_1^2 + \cdots + d_m^2 = |G|$.

Theorem 1.42 (Schur Orthogonality) Let $\chi_1, ..., \chi_m$ be a complete set of irreps for G, and $i, j, k \in [m]$. Then

$$\sum_{g \in G} \chi_{i,j,k}\chi_{i,j,k}(g)\overline{\chi_{i',j',k'}(g)} = |G|\delta_{ii'}\delta_{jj'}\delta_{kk'}.$$

Definition 1.43 The **Fourier basis** for a group G consists of

$$|\chi_{i,jk}\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} \overline{\chi_{i,jk}(g)}|g\rangle$$

for each $i \in [n]$ and $j, k \in [d_i]$. Note that by Schur orthogonality, this is an orthonormal basis.

Remark 1.44

- Note that these states are not shift invariant for every $U(g_0) : |g\rangle \mapsto |g_0 g\rangle$.
- The coset state is

$$|g_0 K\rangle = \frac{1}{\sqrt{|K|}} \sum_{k \in K} |g_0 k\rangle$$

Definition 1.45 The **Quantum Fourier transform** over $H_{|G|}$ is the unitary mapping the Fourier basis to the computational basis:

$$\mathrm{QFT}|\chi_{i,jk}\rangle = |i, jk\rangle.$$

($|i, jk\rangle$ is a relabelling of the states $|g\rangle$ for $g \in G$.)

Remark 1.46

- Measuring $\mathrm{QFT}|g_0 K\rangle$ does **not** give g_0-independent outcomes. A complete measurement in the computational basis gives an outcome i, j, k.
- However, there is an incomplete measurement which projects into the d_i^2-dimensional subspaces

$$S_i = \mathrm{span}\{|\chi_{i,jk}\rangle : j, k \in [d_i]\}.$$

  for each $i \in [n]$. Call this measurement operator M_{rep}.

- Measuring only the representation labels of $\mathrm{QFT}|g_0K\rangle$ gives outcomes that are independent of the random shift g_0, since the χ_i are homomorphisms.
- Note this only gives partial information about K. If K is a normal subgroup, then in fact we can then determine K with $O(\log|G|)$ queries.

2. Quantum phase estimation (QPE)

Quantum phase estimation is a unifying algorithmic primitive, e.g. there is an alternative factoring algorithm based on QPE, and has many important applications in physics.

Problem 2.1 (Quantum Phase Estimation)

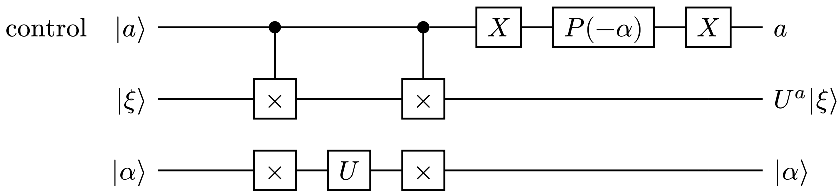
Input A unitary $U \in U(d)$ acting on $\mathbb{C}^d$, a state $|v_\varphi\rangle \in \mathbb{C}^d$ and a level of precision $n \in \mathbb{N}$.

Promise $|v_\varphi\rangle$ is an eigenstate of U with **phase** (eigenvalue) $e^{2\pi i\varphi}$, $\varphi \in [0,1)$ (i.e. $U|v_\varphi\rangle = e^{2\pi i\varphi}|v_\varphi\rangle$).

Task Output an estimate $\tilde{\varphi}$ of φ, accurate to n binary bits of precision.

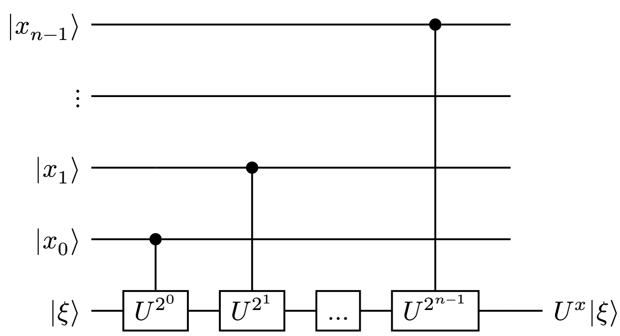
Remark 2.2 Note if U is given as a cirucit, we can implement the controlled-U operation, C-U, by controlling each elementary gate in the circuit of U.

If U is given as a black box, we need more information. Note that U is equivalent to $U' = e^{i\theta}U$ and $|\psi\rangle$ is equivalen to $e^{i\theta}|\psi\rangle$, but C-U is not equivalent to C-U'. Given an eigenstate $|\alpha\rangle$ with known phase $e(i\alpha)$ (so $U|\alpha\rangle = e^{i\alpha}|\alpha\rangle$). Then $U'|\alpha\rangle = e^{i(\theta+\alpha)}|\alpha\rangle$. so U and U' can be distinguished using this additional information.

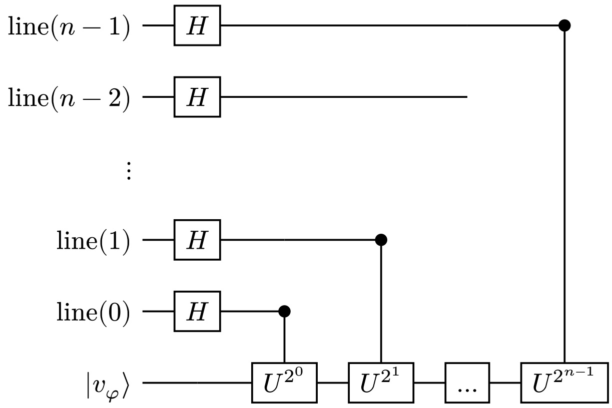


where $P(-\alpha) = \begin{bmatrix} 1 & 0 \\ 0 & e^{-i\alpha} \end{bmatrix}$. $\times$ shows controlled SWAP operation.

Definition 2.3 Generalised control: C-U$|x\rangle|\xi\rangle = |x\rangle U^x|\xi\rangle$, $x \in \{0,1\}^n$ (e.g. C-U$|11\rangle|\xi\rangle = |11\rangle U^3|\xi\rangle$). Note that C-$U^k$ = (C-U)^k. The following circuit implements generalised control:



Algorithm 2.4 (Quantum Phase Estimation) Work over the space $(\mathbb{C}^2)^{\otimes n} \otimes \mathbb{C}^d$, where $(\mathbb{C}^2)^{\otimes n}$ is the n-qubit register, $\mathbb{C}^d$ is the "qudit" register.



TODO finish diagram After C-U^{2^n-1}, the state is $\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} e^{2\pi i \varphi x} |x\rangle |v_\varphi\rangle$. After this, applying QFT^{-1} on the state $\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} e^{2\pi i \varphi x} |x\rangle = \mathrm{QFT}_{2^n} |\varphi\rangle$.

If φ had an exact n-bit expansion $0.i_1 i_2 ... i_n = \frac{i_1 ... i_n}{2^n}$,