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)

Input An oracle for a function $f : \mathbb{Z}/M \to \mathbb{Z}/N$.

Promise

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

Task Determine the period r.

Remark 1.5 Solving the periodicity determination problem classically requires takes time $O(\sqrt{M})$.

Definition 1.6 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 1.7 The **quantum query complexity** of an algorithm is the number of times it queries f (i.e. uses U_f).

Definition 1.8 The **quantum Fourier transform** over $\mathbb{Z}/M$ is the unitary QFT defined by its action on the computational basis:

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

where $\omega = e^{2\pi i/M}$ is an M-th root of unity. Note that QFT requires only $O((\log M)^2)$ gates to implement, whereas a general $M \times M$ unitary requires $O(4^M/M)$ elementary gates.

Lemma 1.9 Let $\alpha = e^{2\pi i y/M}$. Then

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

Proof (Hints). Trivial. □

Proof. The sum is a geometric series with common ratio α. □

Lemma 1.10 (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 $t = \frac{\log(1/d)}{p}$.

Proof (Hints). Trivial. □

Proof. Trivial. □

Theorem 1.11 (Co-primality Theorem) The number of integers less than r that are coprime to r is $O(r/\log\log r)$.

Algorithm 1.12 (Quantum Period Finding) The algorithm solves the periodicity determination problem: 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 $\frac{1}{\sqrt{M}} \sum_{i=0}^{M-1} |i\rangle|0\rangle$ and query U_f on it.
2. Measure second register in computational basis and discard the second register.
3. Apply the quantum Fourier transform to the input state.
4. Measure the input state, yielding outcome c.
5. Compute the denominator r_0 of the simplified fraction $\frac{c}{M}$.
6. Repeat the previous steps $O(\log\log r) = O(\log\log M) = O(\log m)$ times, halting if at any iteration, $f(0) = f(r_0)$.

Theorem 1.13 (Correctness of Quantum Period Finding Algorithm) When repeated, $O(\log\log r) = O(\log\log M)$ times, the quantum period finding algorithm obtains the correct value of r with high probability.

Proof. After querying U_f, we have the state $\frac{1}{\sqrt{M}} \sum_{i=0}^{M-1} |i\rangle|f(i)\rangle$. Upon measuring the second register in the computational basis, the 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 $0 \leq x_0 < r$. Applying the quantum Fourier transform to $|\text{per}\rangle$ then gives Quantum Fourier Transform to $|\text{per}\rangle$:

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

Importantly, now the outcomes and probabilities are independent of x_0, so carry useful information about r. TODO add diagram showing amplitudes for this state. The outcome after the measuring the input state is $c = k_0 M/r$ for some $0 \leq k_0 < r$ (so $c/M = k_0/r$). If k_0 is coprime to r, then the denominator r_0 of the simplified fraction $\frac{c}{M}$ is equal to r. By the coprimality theorem, the probability that k_0 is coprime to r is $O(1/\log\log r)$. Checking if $f(0) = f(r_0)$ tells us if $r_0 = r$, since f is periodic and one-to-one in each period, and $r_0 \leq r$. □

1.3. Analysis of QFT part of period finding algorithm

Notation 1.14 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 1.15 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 1.16 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 1.17 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 1.18 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

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

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

1.4. The hidden subgroup problem (HSP)

Problem 1.19 (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 1.20 Write $[n]$ for $\{1, ..., n\}$. Write e.g. ij for the set $\{i, j\}$.

Definition 1.21 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 1.22 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 1.23 The **adjacency matrix** of a graph $\Gamma = (V, E)$ is the $n \times n$ matrix M_A defined by its entries:

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

Problem 1.24 (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 1.25 The best known classical algorithm for solving the graph isomorphism problem has quasi-polynomial time complexity $n^{O((\log n)^2)}$.

Problem 1.26 (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 1.27

- To find K, we either find a generating set for K, or sample uniformly random elements from K.
- We want to determine K with high probability in $O(\operatorname{poly}\log|G|)$ 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 1.28 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 $0 \le x_0 < r$.
- 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 $K = \operatorname{Aut}(G)$. 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 $O(\operatorname{poly}\log|G|) = O(\operatorname{poly} n)$.

Definition 1.29 An **irreducible representation (irrep)** of a finite abelian group G is a homomorphism $\chi : G \to \mathbb{C}^\times$.

Theorem 1.30

- 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 1.31 (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 1.32 $\chi_0 : G \to \mathbb{C}^\times$, $\chi_0(g) = 1$ 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 1.33 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 1.34 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. Since χ_k is a homomorphism, we have $\overline{\chi_k(g)} = \chi_k(-g)$. Now

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

□

Definition 1.35 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 $(\mathrm{QFT}^{-1})_{kg} = \langle k|\chi_g\rangle = \frac{1}{\sqrt{|G|}}\overline{\chi_g(k)}$, 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 1.36

- 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 1.37 (Quantum HSP solver for finite abelian G) The algorithm solves the hidden subgroup problem for finite abelian G. We work in the state space $H_{|G|} \otimes H_{|X|}$.

1. Prepare the uniform superposition state
$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle|0\rangle$$
and query U_f on it.
2. Measure the output register, then discard this register.
3. Apply QFT mod $|G|$ to the input register, then measure this register.
4. Repeat the above steps $O(\log|G|)$ times.

Theorem 1.38 (Correctness of Quantum HSP Solver) The quantum HSP solver algorithm solves the hidden subgroup problem for finite abelian groups with high probability.

Proof. Query U_f on the state gives
$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle|f(g)\rangle$$

Upon measurement of the output register, we obtain a uniformly random value $f(g_0)$ from $f(G)$, and the state collapses to a **coset state**
$$|g_0 + K\rangle = \frac{1}{\sqrt{|K|}} \sum_{k \in K} |g_0 + k\rangle.$$

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 to the input state gives $\sum_{g \in G} a_g \chi_g(g_0)|g\rangle$, so the 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 if $O(\log|G|)$ such g are drawn uniformly at random, then with probability at least $2/3$, we have enough equations to determine $k_1, ..., k_m$. $\square$

Example 1.39 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 1.40 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 1.41 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 1.42 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 1.43 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 1.44 Let the dimensions of a complete set of irreps $\chi_1, ..., \chi_m$ be $d_1, ..., d_m$. Then $d_1^2 + \cdots + d_m^2 = |G|$.

Notation 1.45 Write $\chi_{i,jk}(g)$ for the (j, k)-th entry of the matrix $\chi_i(g)$.

Theorem 1.46 (Schur Orthogonality) Let $\chi_1, ..., \chi_m$ be a complete set of irreps for G with respective dimensions $d_1, ..., d_m$, and let $i \in [m]$, $j, k \in [d_i]$. Then

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

Definition 1.47 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 1.48 Note that these states are not shift invariant for every $U(g_0) : |g\rangle \mapsto |g_0 g\rangle$. So measurement of the coset state $|g_0 K\rangle$ yields an output distribution that is not independent of g_0.

Definition 1.49 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 $g \in G$ (note this is valid by Theorem 1.44).

Remark 1.50

- 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}. Note that this distinguishes only between the irreps.
- Measuring only the representation labels of $\mathrm{QFT}|g_0 K\rangle$ gives an outcome distribution of the i values that i 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)

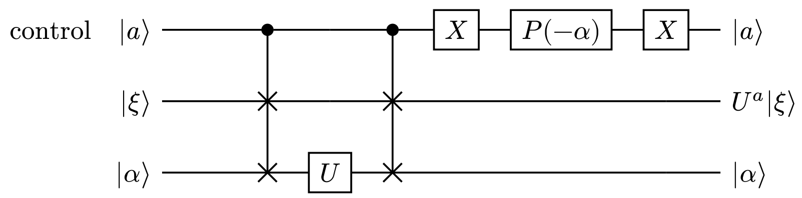
Input Unitary $U \in U(d)$ acting on $\mathbb{C}^d$; state $|v_\varphi\rangle \in \mathbb{C}^d$; level of precision $n \in \mathbb{N}$.

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 If U is given as a cirucit, we can implement the controlled-U operation, $C\text{–}U$, 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 equivalent to $e^{i\theta}|\psi\rangle$, but $C\text{–}U$ is not equivalent to $C\text{–}U'$. Given an eigenstate $|\alpha\rangle$ with known phase $e^{i\alpha}$ (so $U|\alpha\rangle = e^{i\alpha}|\alpha\rangle$), we have $U'|\alpha\rangle = e^{i(\theta+\alpha)}|\alpha\rangle$. so U and U' can be distinguished using this additional information.

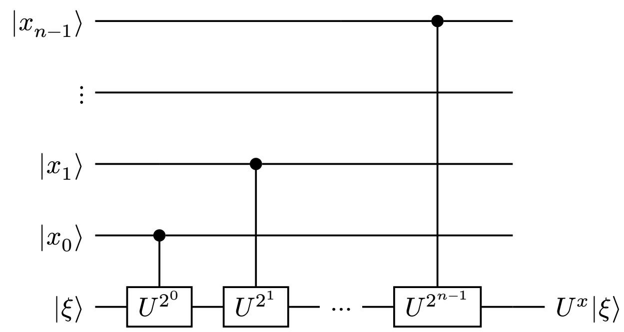


where $P(-\alpha) = \begin{bmatrix} 1 & 0 \\ 0 & e^{-i\alpha} \end{bmatrix}$. $\bullet{-}\times{-}\times$ denotes the controlled SWAP operation.

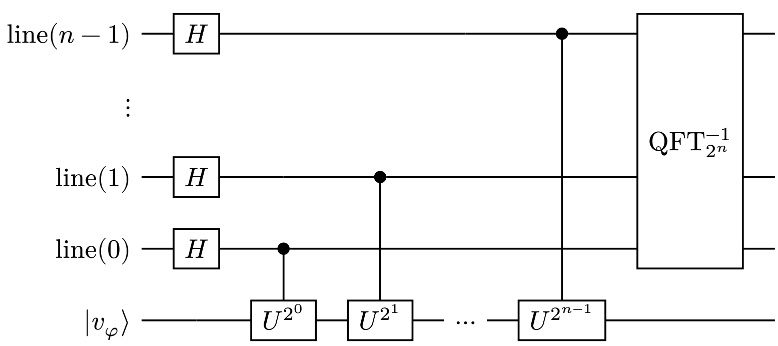
Definition 2.3 For a unitary U, the **generalised control** unitary $C{-}U$ is defined linearly by

$$\forall x \in \{0,1\}^n, \quad C{-}U|x\rangle|\xi\rangle = |x\rangle U^x|\xi\rangle,$$

where U^x denotes U applied x times (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 $C{-}U$:



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.



After $C{-}U^{2^{n-1}}$, the state is $\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} e^{2\pi i\varphi x}|x\rangle|v_\varphi\rangle$. We now discard the qudit register holding $|v_\varphi\rangle$. If φ had an exact n-bit expansion $0.i_1 i_2 \ldots i_n = \frac{i_1\ldots i_n}{2^n} =: \frac{\varphi_n}{2^n}$, then this is precisely $\mathrm{QFT}_{2^n}|\varphi_n\rangle$. After this, applying QFT^{-1} on the state $\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} e^{2\pi i\varphi x}|x\rangle$. We then measure the state, yielding outcome $y = y_{n-1}\cdots y_0$. Our estimate of φ is $\tilde{\varphi} = \frac{y}{2^n} = \frac{y_{n-1}}{2} + \cdots + \frac{y_0}{2^n}$.

Lemma 2.5 For all $\alpha \in \mathbb{R}$,

1. If $|\alpha| \leq \pi$, then $\left|1 - e^{i\alpha}\right| = 2|\sin(\alpha/2)| \geq \frac{2}{\pi}|\alpha|$ (graphically, this says the line $y = \frac{2}{\pi}\alpha$ lies below $2\sin(\alpha/2)$ for $0 \leq \alpha \leq \pi$).
2. If $\alpha \geq 0$, then $\left|1 - e^{i\alpha}\right| \leq \alpha$ (graphically, this says that on the complex unit circle, the arc length α from 1 to $e^{i\alpha}$ is at least the chord length from 1 to $e^{i\alpha}$).

Theorem 2.6 (Phase Estimation Theorem) Let $\tilde{\varphi}$ be the estimate of φ from the quantum phase estimation algorithm. Then

1. $\Pr(\tilde{\varphi}$ is closest n-bit approximation of $\varphi) \geq \frac{4}{\pi^2} \approx 0.4$.
2. For all $\varepsilon > 0$, $\Pr(|\tilde{\varphi} - \varphi| > \varepsilon) = O\left(\frac{1}{2^n\varepsilon}\right)$. So for any desired accuracy ε, the probability of failure decays exponentially with the number of bits of precision (lines in the circuit).

Proof. Let $|A\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} e^{2\pi i\varphi x}|x\rangle$. Let $\delta(y) = \varphi - y/2^n = \varphi - \tilde{\varphi}$. Since $\mathrm{QFT}^{-1}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} e^{-2\pi ixy/2^n}|y\rangle$, we have

$$\mathrm{QFT}^{-1}|A\rangle = \frac{1}{2^n} \sum_{y\in\{0,1\}^n} \sum_{x\in\{0,1\}^n} e^{2\pi ix\delta(y)}|y\rangle$$

so the probability of measuring outcome y is

$$p_y = \frac{1}{2^{2n}} \left| \frac{1 - e^{2^n 2\pi i\delta(y)}}{1 - e^{2\pi i\delta(y)}} \right|^2.$$

1. Let $\alpha = 2^n 2\pi\delta(a)$, where a is the closest n-bit approximation of φ. Note we can imagine the possible values of $\tilde{\varphi}$ as lying on the unit circle, spaced by angle $\frac{2\pi}{2^n}$. This gives a visual intuition to the fact that $|\delta(a)| \leq \frac{1}{2^{n+1}}$. Hence $|\alpha| \leq \pi$, and so by the above lemma,

$$\Pr(\tilde{\varphi} = a) \geq \frac{1}{2^{2n}} \left(\frac{2^{n+2}\delta(a)}{2\pi\delta(a)} \right)^2 = \frac{4}{\pi^2}.$$

2. Note that $\left|1 - e^{2^n 2\pi i\delta(y)}\right| \leq 2$ by the triangle inequality. Let $B = \{y \in \{0,1\}^n : |\delta(y)| > \varepsilon\}$ denote the set of "bad" values of y. For all $y \in \{0,1\}^n$, we have $\delta(y) \in [-1, 1]$. If $|\delta(y)| \leq 1/2$, then, by the above lemma, we have $\left|1 - e^{2\pi i\delta(y)}\right| \geq 4|\delta(y)|$. If $\delta(y) > 1/2$, then $\delta(y) - 1 \in [-1/2, 1/2]$, so by the above lemma, $\left|1 - e^{2\pi i\delta(y)}\right| \geq 4|\delta(y) - 1|$ hence

$$p_y \leq \frac{1}{2^{2n}} \left(\frac{2}{4\delta(y)} \right)^2 = \frac{1}{2^{2n+2}\delta(y)^2}.$$

Let $\delta^+ = \min\{\delta(y) : y \in B, \delta(y) > 0\}$ be the smallest $\delta(y)$ such that $\delta(y) > \varepsilon$, and $\delta^- = \max\{\delta(y) : y \in B : \delta(y) < 0\}$ be the largest $\delta(y)$ such that $\delta(y) < -\varepsilon$. For all $y \in B$, we have $\delta(y) = \delta^+ + k_y/2^n$ or $\delta(y) = \delta^- - k_y/2^n$ for some $k_y \in \mathbb{N}$, so $|\delta(y)| > \varepsilon + k_y/2^n$. Note that each $k \in \mathbb{N}$, $k = k_y$ for at most 2 values of $y \in B$. Hence,

$$
\begin{aligned}
\Pr(|\delta(y)| > \varepsilon) = \Pr(y \in B) &= \sum_{y \in B} p_y \\
&\leq \sum_{y \in B} \frac{1}{2^{2n+2}\left(\varepsilon + k_y/2^n\right)^2} \\
&< 2 \sum_{k=0}^{\infty} \frac{1}{2^{2n+2}} \frac{1}{\left(\varepsilon + k/2^n\right)^2} \\
&\leq \frac{1}{2^{2n+1}\varepsilon^2} + \sum_{k=1}^{\infty} \frac{1}{2^{2n+1}} \frac{1}{\left(\varepsilon + k/2^n\right)^2} \\
&= \frac{1}{2^{2n+1}\varepsilon^2} + \int_0^{\infty} \frac{1}{2^{2n+1}} \frac{1}{\left(\varepsilon + x/2^n\right)^2} \,\mathrm{d}x \\
&= \frac{1}{2^{2n+1}\varepsilon^2} + \int_{2^n\varepsilon}^{\infty} \frac{1}{2u^2} \,\mathrm{d}u = \frac{1}{2^{2n+1}\varepsilon^2} + \frac{1}{2^{n+1}\varepsilon}.
\end{aligned}
$$

□

Remark 2.7 The QPE algorithm excluding the measurement is a unitary - call this unitary U_{PE}. If we apply U_{PE} to an arbitrary state $|\psi\rangle = \sum_j c_j |v_j\rangle$ where $|v_j\rangle$ are the eigenstates of U with eigenvalue $e^{2\pi i \varphi_j}$, then we have

$$
U_{\mathrm{PE}}|\psi\rangle = \sum_j c_j |\tilde{\varphi}_j\rangle |v_j\rangle
$$

If every φ_j has an exact n-bit representation, then this is exact. Otherwise, we have $|\tilde{\varphi}_j\rangle = \sqrt{1-\eta}|\tilde{\varphi}_1\rangle + \sqrt{\eta}|\tilde{\varphi}_0\rangle$, where $|\tilde{\varphi}_1\rangle$ is a superposition of all n-bit strings that are correct to the first n-bits of φ, and $|\tilde{\varphi}_0\rangle$ is a superposition of strings with the first n bits not all correct.

Remark 2.8 Complexity of QPE: we use $C\text{–}U, ..., C\text{–}U^{2^{n-1}}$, so the number of uses of $C\text{–}U$ is $\approx 2^n$. So this initially looks like exponential time, but there are special cases of U where by repeated squaring, this can be implemented with $\mathsf{poly}(n)$ gates.

If we want to estimate φ accurate to m bits of precision with probability $1-\eta$, then by the phase estimation theorem with $\varepsilon = \frac{1}{2^m}$, we need $n = O(m + \log(1/\eta))$ lines. Note this is a modest, polynomial increase in the number of lines of the circuit for an exponential reduction in η.

3. Amplitude amplification

Amplitude amplification is an extension of the key insights in Grover's algorithm (TODO: read part II notes for Grover's).

Notation 3.1 Given $|\alpha\rangle \in H_d$, write $L_{|\alpha\rangle} = \mathrm{span}\{|\alpha\rangle\}$ for the one-dimensional subspace generated by $|\alpha\rangle$, and $L_a^{\perp}$ for its $(d-1)$-dimensional orthogonal complement.

Notation 3.2 Given a k-dimensional subspace $A \leq H_d$ with orthonormal basis $\{|a_1\rangle, ..., |a_k\rangle\}$, denote the projector onto the subspace A by $P_A = \sum_{i=1}^{k} |a_i\rangle\langle a_i|$. Note that P_A is independent of the orthonormal basis.

Notation 3.3 Given a subspace $A \leq H_d$, define the unitary $I_A = I - 2P_A$, which is the reflection in the "mirror" $A^{\perp}$: indeed, not that for all $|\varphi\rangle \in A$, $I_A = -|\varphi\rangle$, and for all $|\psi\rangle \in A^{\perp}$, $I_A|\psi\rangle = |\psi\rangle$, since $P_A|\psi\rangle = 0$.

In the case that A is one-dimensional and spanned by $|\alpha\rangle$, we have $P_A = |\alpha\rangle\langle\alpha|$, and write $I_{|\alpha\rangle} = I - 2|\alpha\rangle\langle\alpha|$.

Proposition 3.4 Let $|\alpha\rangle \in H_d$. For any unitary $U \in U(d)$, we have

$$UI_{|\alpha\rangle}U^{\dagger} = I_{U|\alpha\rangle}.$$

Proof (Hints). Trivial. □

Proof. $UI_{|\alpha\rangle}U^{\dagger} = UU^{\dagger} - 2U|\alpha\rangle\langle\alpha|U^{\dagger} = I_{U|\alpha\rangle}$. □

Problem 3.5 (Unstructured Search)
  Input An oracle for a function $f : \{0,1\}^n \to \{0,1\}$.
  Promise There is a unique $x_0 \in \{0,1\}^n$ such that $f(x_0) = 1$.
  Task Find x_0.

Remark 3.6 The unstructured search problem is closely related to the complexity class NP and to Boolean satisfiability.

Definition 3.7 For fixed $|x_0\rangle \in H_2^{\otimes n}$, the **Grover iteration operator** Q is defined as

$$Q := -H^{\otimes n} I_{|0\rangle} H^{\otimes n} I_{|x_0\rangle} = -I_{H^{\otimes n}|0\rangle} I_{|x_0\rangle}.$$

Remark 3.8 Note that for a function $f : \{0,1\}^n \to \{0,1\}$ fulfilling the promise of the unstructured search problem, we can implement $I_{|x_0\rangle}$ without knowing x_0: we have $U_f|x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = (-1)^{f(x)}|x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Hence, implementing Q requires only one query to f.

Theorem 3.9 (Grover) In the 2-dimensional subspace spanned by $|\psi\rangle = H^{\otimes n}|0\rangle$ and $|x_0\rangle$, the action of Q is a rotation by angle 2α, where $\sin(\alpha) = \frac{1}{\sqrt{2^n}} = \langle x_0|\psi\rangle$.

Algorithm 3.10 (Grover's Algorithm) Work in the state space $H_2^{\otimes n}$.
1. Prepare $|\psi\rangle = H^{\otimes n}|0\rangle$.
2. Apply Q^m to $|\psi\rangle$, where m is closest integer to $\frac{\arccos(1/\sqrt{N})}{2\arcsin(1/\sqrt{N})} = \frac{\theta}{2\alpha}$ and $\cos(\theta) = \sin(\alpha) = \langle x_0|\psi\rangle = 1/\sqrt{2^n}$. This rotates $|\psi\rangle$ to be close to $|x_0\rangle$ (within angle $\pm\alpha$ of $|x_0\rangle$).
3. Measure to get x_0 with probability $p = |\langle x_0|Q^m|\psi\rangle|^2 = 1 - \frac{1}{N}$. For large N, $\arccos(1/\sqrt{N}) \approx \frac{\pi}{2}$, and $\arcsin(1/\sqrt{N}) \approx 1/\sqrt{N}$. The number of iterations is $m = \frac{\pi}{4}\sqrt{N} = O(\sqrt{N})$. So we need $O(\sqrt{N})$ queries to U_f. In contrast, clasically we need $\Omega(N)$ queries to f to find x_0 with any desired constant probability. Note that $\Omega(N)$ queries are both necessary and sufficient.

Notation 3.11 Write G for the subspace of the state space H whose associated amplitudes in a given state we wish to amplify. G is called the "good" subspace. We call the subspace $G^{\perp}$ the "bad" subspace. Note that $H = G \oplus G^{\perp}$, and for any state $|\varphi\rangle \in H$, there is a unique decomposition with real, positive coefficients $|\varphi\rangle = \sin(\theta)|g\rangle + \cos(\theta)|b\rangle$, where $|g\rangle = P_G|\varphi\rangle$ and $|b\rangle = P_{G^{\perp}}|\varphi\rangle$.

Theorem 3.12 (Amplitude Amplification Theorem/2D-subspace Lemma) Let $|\psi\rangle = H^{\otimes n}|0\rangle$. Let $G \leq H_2^{\otimes n}$ be a subspace and $|g\rangle = P_G|\psi\rangle$, $|b\rangle = P_{G^{\perp}}|\psi\rangle$. In the 2-dimensional subspace $\text{span}\{|g\rangle,|\psi\rangle\} = \text{span}\{|g\rangle,|b\rangle\}$, the unitary $Q = -I_{|\psi\rangle}I_G$ is a rotation by angle 2θ, where $\sin(\theta) = \|P_G|\psi\rangle\|^2$, the length of the "good" projection of $|\psi\rangle$.

Remark 3.13 In the amplitude amplification process, the relative amplitudes of basis states inside $|g\rangle$ and $|b\rangle$ won't change. So amplitude amplification boosts the overall amplitude of $|g\rangle$ at the expense of the amplitude of $|b\rangle$.