Basic Quantum Algorithms

- An **oracle** O_f is a black-box circuit which computes function f
  - **Phase oracle**: $O_f|x\rangle \mapsto (-1)^{f(x)}|x\rangle$
  - **Bit oracle**: $O_f|x, y\rangle = |x, y \oplus f(x)\rangle$
- Theorem: bit and phase oracles are equivalent
  - Bit → phase: Given bit oracle O_f, phase oracle equivalent to $O_f(I^{\otimes |x|} \otimes Z)O_f$
    - $O_f(I^{\otimes |x|} \otimes Z)O_f|x,0\rangle \mapsto O_f(I^{\otimes |x|} \otimes Z)|x, f(x)\rangle \mapsto (-1)^{f(x)}O_f|x, f(x)\rangle \mapsto (-1)^{f(x)}|x,0\rangle$
    - Idea: convert basis-value to relative phase via Z gates
  - Phase → bit: given bit oracle O_f, bit oracle equivalent to $(I^{\otimes |x|} \otimes H)O_f(I^{\otimes X} \otimes H)$
    - Key identity: bit oracle like C^X and phase oracle like C^Z, and $X = HZH$
- Hadamard **transform** $H^{\otimes n}$ applies H to every incoming qubit
  - $\forall x \in \{0,1\}^n$, $H^{\otimes n}|x\rangle = \dfrac{1}{\sqrt{2^n}} \displaystyle\sum_{j \in \{0,1\}^n} (-1)^{x \cdot j}|j\rangle$: we pick up $-1 \iff |x_i\rangle = |j_i\rangle = 1$
- **Deutsch-Josza Algorithm**
  - Given phase oracle O_f, determine in one oracle pass whether f is balanced or constant
  - $H^{\otimes n}O_f H^{\otimes n}|0\rangle^{\otimes n} = H^{\otimes n}\left(\dfrac{1}{\sqrt{2^n}}\sum_x (-1)^{f(x)}|x\rangle\right) = \dfrac{1}{2^n}\sum_x \sum_z (-1)^{z \cdot x + f(x)}|z\rangle$
  - Amplitude for $|0\rangle^{\otimes n} = \dfrac{1}{2^n}\sum_x (-1)^{f(x)} = 0 \iff f$ balanced else $\pm 1 \implies f$ constant,
  - Then whether measurement outcome is $|0\rangle^{\otimes n}$ tells whether f constant or balanced
  - Remark: we need the strong assumption on f to guarantee $||0\rangle^{\otimes n}|$ is either 0 or 1
- **Simon's Algorithm**
  - Given oracle for $f : \{0,1\}^n \to \{0,1\}^n$ which $\exists c \in \{0,1\}^n : f(x) = f(x \oplus c)$, find c
  - Classical solution is slow
    - Given query $x, y \in \{0,1\}^n$ and $f(x) \neq f(y)$, we conclude $c \neq x \oplus y$
    - Classically, takes at most $2^{n-1} + 1$ queries at worst and $O(2^n)$ queries on average
  - $(H^{\otimes n} \otimes I^{\otimes n})O_f(H^{\otimes n} \otimes I^{\otimes n})|0\rangle^{\otimes 2n} = (H^{\otimes n} \otimes I^{\otimes n})O_f\left(\frac{1}{\sqrt{2^n}}\sum|x\rangle|0\rangle^{\otimes n}\right) = (H^{\otimes n} \otimes I^{\otimes n})\left(\frac{1}{\sqrt{2^n}}\sum|x\rangle|f(x)\rangle\right) = \frac{1}{2^n}\sum_x\sum_j(-1)^{x \cdot j}|j\rangle|f(x)\rangle$
  - $|j\rangle|f(x)\rangle = |j\rangle|f(x \oplus c)\rangle$ amplitude $\dfrac{(-1)^{x \cdot j} + (-1)^{(x \oplus c)\cdot j}}{2^n} \neq 0 \iff c \cdot j \equiv 0 \mod 2$
  - Find c from $n - 1$ independent j satisfying $j \cdot c = 0$—solve linear system of equations
- **Backaction principle**: System A has effect on system $B \iff B$ has effect on system A

Quantum Fourier Transform

- **Discrete Fourier Transform**: $\{x_k\}_N \mapsto \{y_k \equiv \frac{1}{\sqrt{N}} \sum x_j e^{2\pi ijk/N}\}$
  - Compare with $f(x) \mapsto F(k) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} f(x) e^{-ikx}\, dx$
  - It is convenient to write in terms of $\omega \equiv e^{2\pi i/N}$, then $x_k \mapsto \frac{1}{\sqrt{N}} \sum x_j \omega^{jk}$
- **Quantum Fourier transform** $F : F\,|\,j\rangle = \frac{1}{\sqrt{N}} \sum e^{\omega jk}\,|\,k\rangle$
  - $F\left(\sum x_j |\,j\rangle\right) = \frac{1}{\sqrt{N}} \sum_j x_j \sum_k e^{\omega jk}\,|\,k\rangle = \frac{1}{\sqrt{N}} \sum_k \left(\sum_j x_j e^{\omega jk}\right) |\,k\rangle = \sum_k y_k\,|\,k\rangle$
  - Lemma: $\forall N \in \mathbb{N} - \{0\}, \omega \equiv e^{2\pi i/N} : \sum_{j=0}^{N-1} e^{\omega jk} = \delta_{k0}$
  - Assume $a = \gcd(N, k) = 1$, else reducible to proof for $N/a, k/a$
  - Then $\operatorname{lcm}(N, k) = Nk \implies \{jk \mod N\}_{j=0}^{N-1} = \{j\}_{j=0}^{N-1} \implies \sum_{j=0}^{N-1} e^{\omega jk} = \sum_{j=0}^{N-1} e^{\omega j} = 0$
  - F is unitary: $\langle j\,|\,F^\dagger F\,|\,k\rangle = \frac{1}{N}\left(\sum_a e^{-aj\omega}\langle a\,|\right)\left(\sum_b e^{bk\omega}\,|\,b\rangle\right) = \frac{1}{N}\sum_b e^{b(k-j)\omega} = \delta_{jk}$
- Corollary: Inverse Quantum Fourier Transform: $F^\dagger\,|\,m\rangle = \frac{1}{\sqrt{N}} \sum e^{-\omega nm}\,|\,n\rangle$
  - $F\left(\frac{1}{\sqrt{N}} \sum e^{-\omega nm}\,|\,n\rangle\right) = \frac{1}{N} \sum \sum e^{-\omega nm} e^{\omega nk}\,|\,k\rangle = \frac{1}{N} \sum \sum \delta_{mk}\,|\,k\rangle = |\,m\rangle$
- Interchange $j \in [2^n] \leftrightarrow j_1 \ldots j_n$ its binary expansion: $F\,|\,j\rangle = \frac{1}{\sqrt{2^n}} \bigotimes_{l=1}^{n} \left(|\,0\rangle + e^{2\pi ij2^{-l}}\,|\,1\rangle\right)$

- $\sqrt{2^n} F \,|\, j\rangle = \sum_{k=0}^{2^n-1} e^{2\pi ijk2^{-n}} \,|\, k\rangle = \sum_{k=0}^{2^n-1} e^{2\pi ij2^{-n}\sum k_l 2^l} \,|\, k\rangle = \sum_{k=0}^{2^n-1} e^{2\pi ij \sum k_l 2^{-l}} \,|\, k_1 \ldots k_n\rangle$

$$= \sum_{k_0=0}^{1} \cdots \sum_{k_{n-1}=0}^{1} \bigotimes_{l=1}^{n} e^{2\pi ijk_l 2^{-l}} \,|\, k_l\rangle = \bigotimes_{l=1}^{n} \sum_{k_l=0}^{1} e^{2\pi ijk_l 2^{-l}} \,|\, k_l\rangle = \bigotimes_{l=1}^{n} \left(\,|\, 0\rangle + e^{2\pi ij2^{-l}} \,|\, 1\rangle \right)$$

- Define decimal $0.b_1 \ldots b_n = \sum \frac{b_k}{2^k}$, then $F \,|\, j\rangle = \frac{1}{\sqrt{2^n}} \bigotimes_{l=1}^{n} \left(\,|\, 0\rangle + e^{2\pi i 0.j_{n-l+1}\cdots j_n} \,|\, 1\rangle \right)$
  - Though $j2^{-l} \neq 0.j_{n-l+1} \ldots j_n$, $x \mapsto e^{2\pi ix}$ allows us to disregard integer parts of x
- Corollary: Applying $F \in \mathscr{H}(2^n)$ needs $O(n^2)$ H and $R_k \equiv \begin{bmatrix} 1 & \\ & e^{2\pi i/2^k} \end{bmatrix}$ gates

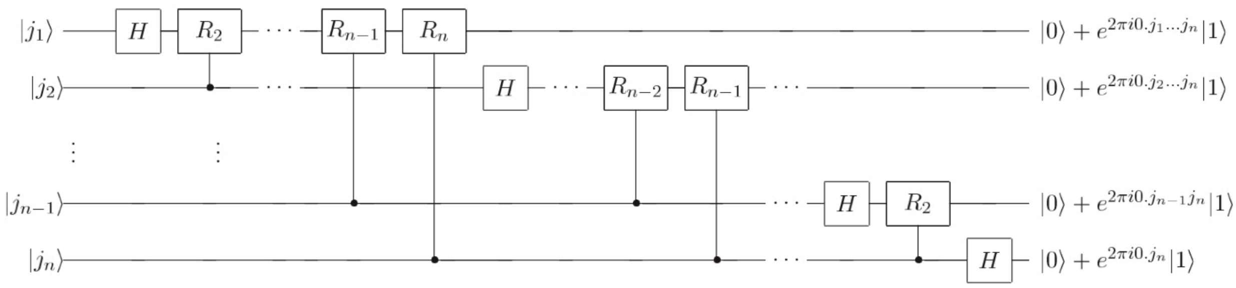
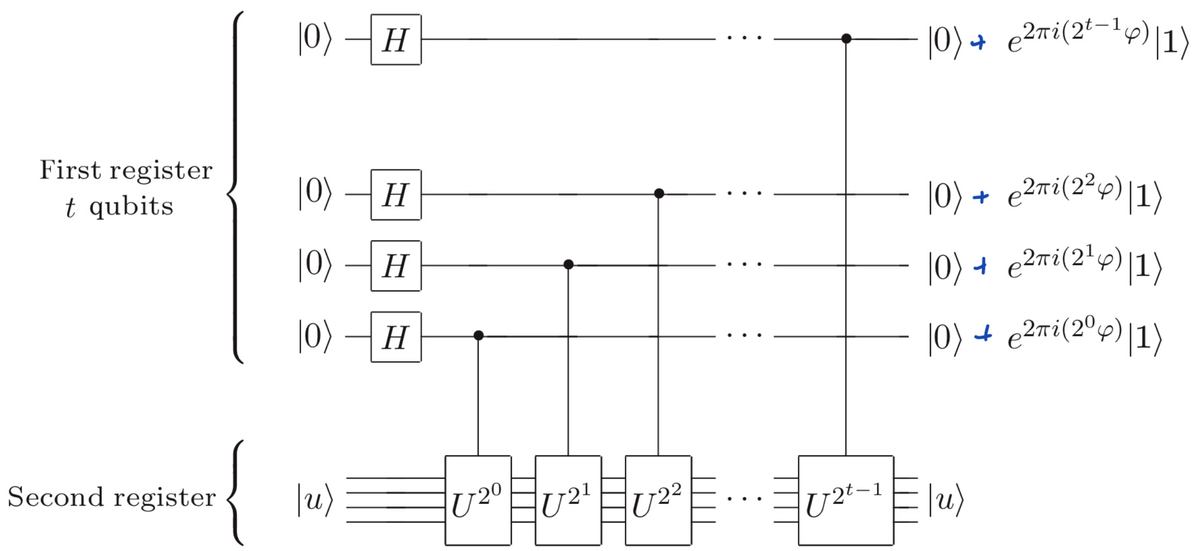


Figure 5.1. Efficient circuit for the quantum Fourier transform. This circuit is easily derived from the product representation (5.4) for the quantum Fourier transform. Not shown are swap gates at the end of the circuit which reverse the order of the qubits, or normalization factors of $1/\sqrt{2}$ in the output.

- $\frac{1}{\sqrt{N}} \sum e^{2\pi ijk2^{-n}} \,|\, k\rangle = \frac{1}{\sqrt{2^n}} \bigotimes_{l=1}^{n} \left(\,|\, 0\rangle + e^{2\pi ij2^{-l}} \,|\, 1\rangle \right) = \frac{1}{\sqrt{2^n}} \bigotimes_{l=1}^{n} \left(\,|\, 0\rangle + e^{2\pi i 0.j_{n-l+1}\cdots j_n} \,|\, 1\rangle \right)$

Phase Estimation

- Problem: given U and eigenvector $|u\rangle$, find $\phi : U|u\rangle = e^{2\pi i\phi}|u\rangle$
  - $|u\rangle$ may be multiple qubits. Note that U unitary $\implies \phi \in [0,1]$
- Assume access to $|u\rangle$ and efficient $\forall k \in \mathbb{N}, C(U^{2^k})$
  - $|0\rangle^{\otimes n} \otimes |u\rangle \mapsto \left(\bigotimes_{j=0}^{t-1} |0\rangle + e^{2\pi i\phi 2^j}|1\rangle\right) \otimes |u\rangle = \left(\sum_{k=0}^{2^t-1} e^{2\pi i k\phi}|k\rangle\right) \otimes |u\rangle \approx F|\phi\rangle \otimes U$
    - Note introduction of relative phase: $|j\rangle C(U^k)|u\rangle = e^{2\pi i k\phi j}|j\rangle|u\rangle$ for $j \in \{0,1\}$
    - If $\phi = 0.\phi_1 \ldots \phi_t$, let $\hat{\phi} = \phi_1 \ldots \phi_t \in [0,2^n - 1]$ and recall equation in QFT



- If $\phi = 0.\phi_1 \ldots \phi_t\phi_{t+1} \ldots$ (more digits) — we still get an approximation
  - Let $b \in [0,2^t - 1]$ be such that $b \cdot 2^{-t} \le \phi, \delta \equiv \phi - b2^{-t} \le 2^{-t}$
  - $F^\dagger\left(\frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^t-1} e^{2\pi i k\phi}|k\rangle\right) = \frac{1}{2^n}\sum_{k=0}^{2^t-1}\sum_{j=0}^{2^t-1} e^{\omega k(\phi 2^t - j)}|j\rangle = \frac{1}{2^t}\sum_{j=0}^{2^t-1}\left(\sum_{k=0}^{2^t-1} e^{\omega k(\phi 2^t - j)}\right)|j\rangle \equiv \frac{1}{2^t}\sum_{j=0}^{2^t-1}\alpha_j|j\rangle$
  - $\alpha_j \equiv \sum_{k=0}^{2^t-1} e^{\omega k(\phi 2^t - j)} = \frac{1 - e^{\omega 2^t(\phi 2^t - j)}}{1 - e^{\omega(\phi 2^t - j)}}$ and let $\beta_j \equiv \alpha_{(j-b) \mod 2^t}$
  - $|\beta_j| = \left|\frac{1 - e^{\omega 2^t(\phi 2^t - (j+b))}}{1 - e^{\omega(\phi 2^t - (j+b))}}\right| \le \frac{2}{|1 - e^{2\pi i(\delta - j2^{-t})}|} \le \frac{1}{4|\delta - j2^{-t}|}$
    - Note that $-1 \le \theta \le 1 \implies |1 - e^{i\pi\theta}| \ge 2|\theta|$

- $$P(|j-b|>E)=\frac{1}{2^n}\left(\sum_{-2^{t-1}}^{-E-1}|\beta_j|^2+\sum_{E+1}^{2^{t-1}}|\beta_j|^2\right)<\ldots<\frac{1}{2(e-1)}$$
  - Takeaways: center around element of least error, and complex angular identities
  - To successfully obtain ϕ accurate to n bits with probability of success at least $1-\epsilon$ it suffices to use $t=n+\log\left(2+\frac{1}{2\epsilon}\right)$

Period Finding, Order Finding, and Factoring

- Period Finding problem: for some periodic f, find its period. Assumptions:
  - Period $0\le r<2^t$ for known t, and $\{f_i\}_{0\le i<r}$ are distinct
  - We can efficiently implement U^{2^j} and some $|f(k)\rangle, 0\le k<r$
- Define unitary U s.t. $U|y\rangle=U|f(f^{-1}(y)+1)\rangle$
  - In other words, for $0\le i<r, y_i\equiv f(i)$, we have $U|y_i\rangle=|y_{i+1 \mod r}\rangle$
  - Remark: unitary ill-defined if 2nd distinct assumption fails
  - Consider the eigenvalues of $U: U^r=I \iff f$ has period r
    - Eigenvectors must be $|u\rangle=\frac{1}{\sqrt{r}}\sum_{c=0}^{r-1}c_n|y_n\rangle$ where $U|u\rangle=\frac{1}{\sqrt{r}}\sum c_{(n-1) \mod r}|u_n\rangle$
    - $c_{n+1 \mod r}=\lambda c_n \implies c_n=e^{-2\pi ins/r}, \lambda=e^{2\pi is/r}$
    - Eigenvectors $|u_s\rangle=\frac{1}{\sqrt{r}}\sum_{n=0}^{r-1}e^{-2\pi ins/r}|y_n\rangle$ with eigenvalues $\lambda_s=e^{2\pi is/r}$
    - Moreover $\frac{1}{\sqrt{r}}\sum e^{2\pi iks/r}|u_s\rangle=\frac{1}{r}\sum_{s=0}^{r-1}\sum_{n=0}^{r-1}e^{2\pi i(k-n)s/r}|y_n\rangle=|y_k\rangle$
- $|y_k\rangle=\frac{1}{\sqrt{r}}\sum e^{2\pi iks/r}|u_s\rangle\mapsto\frac{1}{\sqrt{r}}\sum e^{2\pi iks/r}|\lambda_k=e^{2\pi is/r}\rangle|u_s\rangle\mapsto\frac{1}{\sqrt{r}}\sum e^{2\pi iks/r}|s/r\rangle|u_s\rangle$
  - Measure first register and use continued fraction to obtain s/r
  - Remark: we can use phase estimation on superposition of eigenstates so long as we can accept randomness in obtaining eigenvalues
- Obtaining r from s/r for some random $0\le s<r$:
  - **Continued fractions algorithm**: Define $[a_0,\ldots,a_M]\equiv a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{\ldots+\frac{1}{a_M}}}}$.

    - For $0 \leq m \leq M$, let m^{th} convergent to this continued fraction be $[a_0, \ldots, a_m]$
  - Theorem: Suppose s/r is a rational number such that $\left| s/r - \phi \right| \leq 1/(2r^2)$, then s/r is a convergent of the continued fraction for ϕ and can be computed in $O(L^3)$ operations using continued fractions algorithm
  - Accounting for $\gcd(s, r) > 1$:
    - Repeat phase-estimation-continued-fractions procedure twice to obtain $(r_1', s_1'), (r_2', s_2')$. Note that $\gcd(s_1', s_2') = 1 \implies r = \operatorname{lcm}(r_1, r_2)$ where the former happens with $P \geq 1/4$
- **Order-finding**:
  - If $\gcd(x, N) = 1$, the **order** of x modulo N is $\min_{r \in \mathbb{N}} : x^r \equiv 1 \mod N$.
  - Given N and some co-prime $g < N$, define $f_{N,g} : f_{N,g}(x) = g^x \mod N$
  - $f_{N,g}$ satisfies assumptions above: $f_{N,g}(0) = f_{N,g}(r) = 1$, and distinct since g, N co-prime
  - Define $U : U|y\rangle = U|xy \mod N\rangle$, then U^{2^j} via modular exponentiation
  - Corollary: exists poly quantum algorithm for order finding
- Factoring $\leq_p$ Order finding
  - A nontrivial solution to $x^2 \equiv 1 \mod N$ (i.e. $x \neq \pm 1 \mod N$) yields factor
    - $x^2 - 1 = 0 \mod N \implies (x+1)(x-1) = 0 \mod N$, then $\gcd(x-1, N)$ or $\gcd(x+1, N)$ yields a nontrivial factor for N
  - Choose an x: co-prime to N, even order, and $x^{r/2} \neq -1 \mod N$
  - For odd N with m factors, uniformly chosen co-prime x has even order with $P \geq 1 - 2^{-m}$
    - Chinese Remainder Theorem: x has odd order $\iff$ remainder on each prime factor is odd
- Failure cases for factoring:
  - x has even order, $x^{r/2} \neq -1 \mod N$, or s/r has $\gcd(x, r) > 1$

Grover's Search Algorithm

- Assume: **Grover's algorithm**: assume phase oracle $U_f|x\rangle = (-1)^{f(x)}|x\rangle$
    - Prepare $|\psi\rangle \equiv \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}|j\rangle = H^{\otimes n}|0\rangle^{\otimes n}$
    - Define **Grover iteration**: $G \equiv H^{\otimes n}(2|0^n\rangle\langle 0^n| - I)H^{\otimes n}O_p$
        - Claim: $G \equiv (2|\psi\rangle\langle\psi| - I)U_f \iff H^{\otimes n}(2|0^n\rangle\langle 0^n| - I)H^{\otimes n} = 2|\psi\rangle\langle\psi| - I$
        - $H^{\otimes n}|\psi\rangle = |0\rangle^{\otimes n}$, and $2|0^n\rangle\langle 0^n| - I$ negates all other components
        - Algebra: $H^{\otimes n}(2|0^n\rangle\langle 0^n| - I)H^{\otimes n} = 2(H^{\otimes n}|0^n\rangle)(\langle 0^n|H^{\otimes n}) - I = 2|\psi\rangle\langle\psi| - I$
    - Repeatedly apply G and measure
- Analysis: suppose M solutions, let $|\alpha\rangle \equiv \frac{1}{\sqrt{N-M}}\sum_{f(x)=0}|x\rangle, |\beta\rangle \equiv \frac{1}{\sqrt{M}}\sum_{f(x)=1}|x\rangle$
    - $|\psi\rangle \equiv H^{\otimes n}|0\rangle^{\otimes n} = \sqrt{\frac{N-M}{N}}|\alpha\rangle + \sqrt{\frac{M}{N}}|\beta\rangle = \cos\theta|\alpha\rangle + \sin\theta|\beta\rangle, \theta \equiv \arctan\left(\sqrt{\frac{M}{N-M}}\right)$
    - $O_f : |\beta\rangle \to -|\beta\rangle$ is reflection about $|\alpha\rangle$; $H^{\otimes n}(2|0^n\rangle\langle 0^n| - I)H^{\otimes n}$ reflection about $|\psi\rangle$
- If we overdo the number of grover iterations, we may get non-solutions again!
    - Assume no knowledge of M/N, repeat long enough to end up in "random" state projecting onto $|\beta\rangle, |\alpha\rangle$ with equal probability
- Optimality of Grover's algorithm
    - Assume 1 solution with phase oracle $O_x = I - 2|x\rangle\langle x|$
    - Consider $|\psi_k^x\rangle \equiv U_kO_xU_{k-1}O_x\ldots U_1O_x|\psi\rangle$ and $|\psi_k\rangle = U_kU_{k-1}\ldots U_1|\psi\rangle$
    - Consider quantity $D_k \equiv \sum_x \|\psi_k^x - \psi_k\|^2$, we show by induction that $D_k \leq 4k^2$
        - $D_{k+1} = \sum_x \|U_kO_x\psi_k^x - U_k\psi_k\|^2 = \sum_x \|O_x\psi_k^x - U_k\psi_k\|^2 = \sum_x \|O_x(\psi_k^x - \psi_k) + (O_x - I)\psi_k\|^2$
            - Note that $(O_x - I)\psi_k = -2|x\rangle\langle x|\psi_k\rangle$
        - Note that $\|a+b\|^2 = \langle a+b, a+b\rangle = \|a\|^2 + \|b\|^2 + 2\|a\|\|b\|$, then $D_{k+1} \leq \sum \|\psi_k^x - \psi_k\|^2 + 4\|\psi_k^x - \psi_k\||\langle x|\psi_k\rangle| + 4|\langle\psi_k|x\rangle|^2 \leq D_k + 4\sqrt{D_k} + 4$
    - Reliable search implies $\forall x, |\langle\psi_k^x|x\rangle|^2 \geq 1/2 \implies |\langle\psi_k^x|x\rangle| \geq 1/\sqrt{2}$
        - Then $E_k \equiv \sum \|\psi_k^x - x\|^2 \leq 2N - 2\sum|\langle\psi_k^x|x\rangle| \leq (2-\sqrt{2})N$
        - Let $F_k \equiv \sum \|x - \psi_k\|^2 \geq 2N - 2\sqrt{N}$
    - $D_k = \sum \|(\psi_k^x - x) + (x - \psi_k)\|^2 \geq E_k + F_k - 2\sum \|\psi_k^x - x\| \cdot \|x - \psi_k\| \geq E_k + F_k - 2\sqrt{E_kF_k} = (\sqrt{E_k} - \sqrt{F_k})^2$

- Then $4k^2 \geq \left(\sqrt{2-\sqrt{2}} \cdot \sqrt{N} - \sqrt{2} \cdot \sqrt{N-\sqrt{N}}\right)^2 = O(N)$, then $k \geq O(\sqrt{N})$

- Proof idea: ψ_k^x is the result of "looking for x after k steps," ψ_k is the "anchor" of executing k steps: $\sum_x \psi_k^x = \sum_x U_k O_x \psi_{k-1}^x = -U_k \psi_{k-1}^x, \psi_k = (-1)^k \sum_{x_1,\ldots,x_k} U_k O_{x_k} \ldots U_1 O_{x_1} \psi$.

  The limited action of O_x upper-bounds D_k, successful search criterion upper-bounds D_k, algebra upper-bounds F_k, and Cauchy-Schwarz relates D_k, E_k, F_k

- Remark: $U_1, \ldots, U_k$ are independent of ψ : No-cloning, and $U_1(|\psi\rangle)$ implies U_1's result dependent on measurement of $|\psi\rangle$ and can be deferred

- **Black box model**: given an oracle for $f: \{0,1\}^n \to \{0,1\}$ and $F: \{0,1\}^{2^n} \to \{0,1\}$, how many calls to f do we need to obtain $F(X_0, \ldots, X_{N-1})$ where $X_j \equiv f(j)$?
  - **Deterministic query complexity** $D(F)$ minimum #queries classical computer needs to compute F with certainty
    - $Q_E(F)$ number of queries quantum computers need to compute F exactly.
  - **Bounded error complexity** $Q_2(F)$ minimum #Q-queries to compute with $P \geq 2/3$
  - **Zero-error complexity** $Q_0(F)$, minimum #queries required to compute F with certainty *or admits inconclusive result with* $P < 1/2$
  - $\forall F, Q_2(F) \leq Q_0(F) \leq Q_E(F) \leq D(F) \leq N$
- **Method of Polynomials**: minimum-degree *multilinear* polynomial represent boolean functions
  - $p: \mathbb{R}^n \to \mathbb{R}$ represents $F \iff \forall X \in \{0,1\}^n, F(X) = p(X)$
  - $\deg F \equiv \min_p : \forall X \in \{0,1\}^N, p(X) = F(X)$
    - Idea: $\deg F$ is like "what is the maximum number of conjunctive variables"
    - Polynomial is multilinear i.e. $x_i^2, x_i^3, \ldots$ do not appear since $\forall x_i \in \{0,1\}, x_i^{n>1} = x_i$
    - e.g. $\mathrm{OR}(X) = 1 - (1-X_0)(1-X_1)\ldots(1-X_{N-1})$, and $\deg \mathrm{OR} = N$
    - Similarly, $\mathrm{AND}(X) = X_0 \ldots X_{N-1}$, $\deg \mathrm{AND} = N$
  - Minimum-degree polynomial always exist: $p_F(X) \equiv \sum_{Y \in \{0,1\}^N} F(Y) \prod_{k=0}^{N-1} \left[1 - (Y_k - X_k)^2\right]$
    - $Z \neq X \implies \exists k : 1 - (Z_k - X_k)^2 = 0 \implies \prod \left[1 - (Z_k - Y_k)^2\right] = 0$
  - Theorem: Minimum-degree polynomial representing boolean function $F(X)$ is unique
  - p **approximates** $F \iff \forall X \in \{0,1\}^N, |p(X) - F(X)| \leq 1/3$
    - $\widetilde{\deg}(F)$ is minimum degree of approximating polynomial

- Facts: $D(F) \leq 2(\deg F)^4$, $D(F) \leq 216 \cdot \tilde{\deg}(F)^6$, $\tilde{\deg}(\mathrm{OR}), \tilde{\deg}(\mathrm{AND}) \in \Theta(\sqrt{N})$
- Let output of quantum algorithm $\mathcal{Q}$ performing T queries to oracle O be $\sum_{k=0}^{2^n-1} c_k |k\rangle$
- Theorem: c_k are polynomials of degrees at most T in $X = X_0, \ldots, X_{N-1}$

Simulating Quantum Systems

- Governing equation: $i\hbar \frac{d|\psi\rangle}{dt} = H|\psi\rangle$
    - Absorb $\hbar$ into $H \mapsto i\frac{d|\psi\rangle}{dt} = H|\psi\rangle$
    - Solution $|\psi\rangle = e^{iHt/\hbar}$
- Example: **Heisenberg interaction** between qubits: $H \equiv \sum \sigma_a \otimes \sigma_a = \begin{bmatrix} 1 & & & \\ & -1 & 2 & \\ & 2 & -1 & \\ & & & 1 \end{bmatrix}$
- Eigenvectors $(|00\rangle, 1)$; $(|11\rangle, 1)$; $(|01\rangle + |10\rangle, 1)$; $(|01\rangle - |10\rangle, -3)$
- SWAP has eigenstuff $(|00\rangle, 1)$; $(|11\rangle, 1)$; $(|01\rangle + |10\rangle, 1)$; $(|01\rangle - |10\rangle, -1)$, so $e^{i\pi H/4} = \mathrm{SWAP}$
- Given a composite system H over n subsystems, assume H is **local**
    - $H = \sum_{n=1}^{m} H_m$ where H_m acts nontrivially on a constant number of systems
    - If $\forall j, k : [H_j, H_k] = 0$, then $e^{-iHt} = \prod e^{-iH_jt}$ by simultaneous diagonalization theorem
    - $\exists [H_j, H_k] \neq 0 \implies e^{-iHt} \neq \prod e^{-iH_jt}$: $e^{-iH_jt} = I - itH_j - \frac{t^2}{2}H_j^2 + \frac{it^3}{6}H_j^3 + O(t^4)$,

      then $e^{-iH_jt}e^{-iH_kt} = I - it(H_j + H_k) - \frac{t^2}{2}\left(H_j^2 + H_k^2 + 2H_jH_k\right) + O(t^3)$ while

      $e^{-i(H_j+H_k)t} = I - it(H_j + H_k) - \frac{t^2}{2}\left(H_j^2 + H_k^2 + \{H_j, H_k\}\right) + O(t^3)$
- **Trotter formula**: for Hermitian A, B, $\lim_{n\to\infty}\left(e^{iAt/n}e^{iBt/n}\right)^n = e^{i(A+B)t}$
    - $e^{iAt/n}e^{iBt/n} = I + i(A+B)t/n + O(1/n^2)$.

- $(e^{iAt/n}e^{iBt/n})^n = I + \sum_{k=1}^{n} \binom{n}{k} \frac{1}{n^k} \left[i(A+B)t\right]^k + O(1/n) = \sum_{k=0}^{n} \frac{(i(A+B)t)^k}{k!} \left(1 + O(1/n)\right) + O(1/n)$
  - Take the limit $n \to \infty$ equates $e^{i(A+B)t}$ (P

Error-correction

- Consider a **binary symmetric channel**: a bit is flipped with $p \in [0,1)$
  - What do we mean by asymptotically good
- 3-bit bit-flip code: use fanout gate $|0\rangle \mapsto |000\rangle, |1\rangle \mapsto |111\rangle$ and check parity
  - Protects against one bit-flip error out of three
  - Example: $\alpha|0\rangle + \beta|1\rangle \mapsto \alpha|000\rangle + \beta|111\rangle$, with $\sigma_x(2)$ error we receive $\alpha|010\rangle + \beta|101\rangle$. Project, measure, and correct correspondingly: $\langle 000\rangle + \langle 111\rangle, \langle 100\rangle + \langle 011\rangle, \langle 010\rangle + \langle 101\rangle, \langle 001\rangle + \langle 110\rangle$
  - Probability of bit-flip error diminishes $p \mapsto 3p^2$: to cause an error on represented qubit we need to have error on two of three qubits $p \mapsto p^2$, and there are 3 ways this can happen
  - Remark: we cannot distinguish phase-flip errors using this encoding: total phase flip error on 1 or 3 qubits so $p \mapsto p^3 + 3p(1-p)^2 = 3p$. This is an encoding problem
    - Consider $\sigma_z(2)$ error, then representation coincides
- By conjugating by H we can diminish phase errors at the risk of amplifying bit errors
  - How do we get the best of both worlds? Concatenate the codes?
- Apply phase-flip code to 3 qubits and bit-flip code to each of the resulting codes to get 9-bit
  - Protects against 1 bit-flip and 1 phase-flip
  - $|0\rangle_L \equiv \frac{1}{\sqrt{8}}(|000\rangle + |111\rangle)^{\otimes 3}, |1\rangle_L \equiv \frac{1}{\sqrt{8}}(|000\rangle - |111\rangle)^{\otimes 3}$
- Theorem: correcting X, Z errors suffices to correct any 1-qubit error
  - Key idea: when projected and measured, error is discretized and can be simply corrected
  - The key component here is that measurement alters the state
  - $E = \langle E|I\rangle I + \langle E|X\rangle X + \langle E|Y\rangle Y + \langle E|Z\rangle Z$, and measuring error syndrome collapses superposition to $|\psi\rangle, X_i|\psi\rangle, Z_i|\psi\rangle, X_iZ_i|\psi\rangle$