Problem set 6 — Solutions

CSE 534 Autumn 2026

Problem 1 (Understanding Grover's).

1. Notice that in this setting $\gamma = \frac{\pi}{6}$, and after a single iteration the angle of our state is $3\gamma = \pi/2$, so we find x with probability 1. The circuit is to prepare $|+\rangle^{\otimes 2}$, apply the phase oracle for f, apply the diffusion reflection, and measure.

2. The intermediate measurement forces a collapse of the state to either angle 0 or angle $\pi/2$ in the two-dimensional space that Grover's algorithm operates in. Let $\gamma = \arcsin\left(1/\sqrt{2^n}\right)$. The first measurement finds the solution with probability $\sin^2(3\gamma)$. If it fails, the state collapses to angle 0, and each subsequent Grover iteration finds the solution with probability $\sin^2(2\gamma)$. Therefore, the expected number of Grover iterations is

$$1 + \frac{\cos^2(3\gamma)}{\sin^2(2\gamma)}.$$

   This is $\Theta(2^n)$, so measuring after every iteration does not give Grover's quadratic speedup.

3. Grover's algorithm consists of two reflections; therefore, the application of the Grover operator stays in the two-dimensional space spanned by $|+\rangle^{\otimes n}$ and $\Pi|+\rangle^{\otimes n}$, where $\Pi = \sum_{f(x)=1} |x\rangle\langle x|$. Note that $\Pi|+\rangle^{\otimes n}$, when normalized, equals $\frac{1}{\sqrt{K}} \sum_{f(x)=1} |x\rangle$. Let

$$\theta = \arcsin\left(\sqrt{K/N}\right), \qquad N = 2^n.$$

   The initial state has angle θ from the subspace of unmarked inputs, and after t iterations its angle is $(2t+1)\theta$. Choosing t to be an integer nearest to $\frac{\pi}{4\theta} - \frac{1}{2}$ gives success probability at least $1/2$ when $K \le N/2$. Since $\arcsin(u) \ge u$, this takes $O(\sqrt{N/K})$ iterations. If $K > N/2$, measuring the initial state already finds a solution with probability greater than $1/2$.

4. If we believe there are K solutions, we will apply the Grover operator $\lfloor T \rceil$ (nearest integer) times where T is the solution to $(2T+1)\arcsin\left(\sqrt{K/N}\right) = \pi/2$. However, since there are K' solutions, the angle after T iterators of the Grover operator will be

$$(2T+1)\arcsin\left(\sqrt{K'/N}\right) = \frac{\pi}{2} \cdot \frac{\arcsin\left(\sqrt{K'/N}\right)}{\arcsin\left(\sqrt{K/N}\right)} \approx \frac{\pi}{2} \cdot \sqrt{\frac{K'}{K}}. \tag{1}$$

   Therefore, the success probability of finding a solution will be $\sin^2\left(\frac{\pi}{2} \cdot \sqrt{\frac{K'}{K}}\right)$.

5. Pick a sufficiently small fixed $\epsilon > 0$. Consider running Grover's for $K = (1+\epsilon)^J, (1+\epsilon)^{J-1}, \ldots, (1+\epsilon), 1$, where J is the minimum integer such that $(1+\epsilon)^{J+1} \ge N/4$. If the true number of solutions

K' is at most $N/4$, one of these guesses has K'/K within a factor $1+\epsilon$. By the exact formula in the previous part, the success probability on this run is bounded below by a positive constant of $\geq 1/4$ for some constant $\epsilon > 0$. If $K' > N/4$, a uniformly random input is a solution with probability greater than $1/4$.

Thus one pass through these guesses, including a uniformly random trial, succeeds with probability at least some constant $c > 0$. Repeating the entire pass $O(\log(1/\delta))$ times makes the probability of not finding a solution at most δ. The total number of Grover iterations in one pass is

$$\begin{aligned} O\left(\sum_{j=0}^{J}\sqrt{\frac{N}{(1+\epsilon)^j}}\right) &\leq O\left(\sqrt{N}\sum_{j=0}^{J}(1+\epsilon)^{-j/2}\right) \\ &= O\left(\frac{\sqrt{N}}{\epsilon}\right). \end{aligned}$$

Since ϵ is fixed, the total query complexity is upper bounded by $O\big(\sqrt{N}\log(1/\delta)\big)$.

To improve the expected runtime, for each $K = (1+\epsilon)^J, \ldots, 1$, run Grover's with that value K for $O(\log(1/\delta))$ times before moving on to the next value of K. For the true number of solutions K', with all but probability δ, we will halt when we reach the best multiplicative approximation of K'. Therefore, the expected number of queries will be

$$O(\log(1/\delta)) \cdot O\left(\frac{\sqrt{N/K'}}{\sqrt{1+\epsilon}-1}\right) = O\left(\sqrt{\frac{N}{K'}}\log(1/\delta)\right).$$

Problem 2 (Quantum query lower bounds).

1. (a) Notice that for the state of the algorithm after U_0, every coefficient is a constant independent of $\mathbf{z}$. Precisely, $\alpha_s^{(}(0) = \langle s|U_0|0^m\rangle$. Proceeding inductively, assume that $|\psi_t\rangle$ is the state immediately after U_t with coefficients $\alpha_s^{(t)}$ which are degree t polynomials in $\mathbf{z}$. Then, observe that

$$\begin{aligned} \alpha_s^{(t+1)} &= \langle s|U_{t+1}(\mathcal{O}_{\mathbf{z}}\otimes\mathbb{I})|\psi_t\rangle \\ &= \sum_{s'}\langle s|U_{t+1}(\mathcal{O}_{\mathbf{z}}\otimes\mathbb{I})|s'\rangle\cdot\alpha_{s'}^{(t)} \\ &= \sum_{s'=(x,b,y)}\langle s|U_{t+1}|s'\rangle\cdot\langle x,b,y|\mathcal{O}_{\mathbf{z}}\otimes\mathbb{I}|x,b,y\rangle\cdot\alpha_{s'}^{(t)} \\ &= \sum_{s'=(x,b,y)}\langle s|U_{t+1}|s'\rangle\cdot(1-2b\cdot z_x)\cdot\alpha_{s'}^{(t)}. \end{aligned}$$

Here we used the fact that $\mathcal{O}_Z\otimes\mathbb{I}$ is diagonal to extract the middle term. Now notice that each element in the sum is the product of a constant, a linear function, and a degree-t polynomial.

Therefore, $\alpha_s^{(t+1)}$ is a degree-t polynomial. Lastly, since the entries of the polynomial are 0 or 1, $z_x^2 = z_x$, so the polynomial is necessarily multilinear, as higher individual degrees can be simplified.

(b) The probability of outputting 1 is precisely

$$\|\langle 1| \otimes \mathbb{I} \, |\psi_t\rangle\|^2 = \sum_{s=(1,\cdot)} \left|\alpha_s^{(t)}\right|^2 = \sum_{s=(1,\cdot)} {\alpha_s^{(t)}}^\dagger \alpha_s^{(t)}.$$

Each term in the sum is a degree $2t$ multilinear polynomial and is real, so the whole sum is a degree $2t$ real multilinear polynomial. To see that it is real, write

$$\alpha_s^{(t)} = \operatorname{Re} \alpha_s^{(t)} + i \operatorname{Im} \alpha_s^{(t)}.$$

Then, it's easy to verify that

$${\alpha_s^{(t)}}^\dagger \alpha_s^{(t)} = \left(\operatorname{Re} \alpha_s^{(t)}\right)^2 + \left(\operatorname{Im} \alpha_s^{(t)}\right)^2.$$

2. (a) For any $j_1, \ldots, j_k$, $z_{j_1} \ldots z_{j_k} = 1$ iff each term is a 1. For a uniformly random choice of $\mathbf{z} \in S_i$, this occurs with probability $\binom{i}{k} / \binom{N}{i}$. Expanding this combinatorial identity gives the statement.

(b) The polynomial p is of degree at most $2t$ so it can be expressed as

$$p(\mathbf{z}) = \sum_{L \subset \binom{[N]}{\leq 2t}} \beta_L z_L \text{ where } z_L \stackrel{\text{def}}{=} \prod_{x \in L} z_x.$$

Then,

$$q(i) = \frac{1}{|S_i|} \sum_{\mathbf{z} \in S_i} p(\mathbf{z}) = \sum_{L \subset \binom{[N]}{\leq 2t}} \frac{\beta_L (N-k)!}{N!} \cdot i(i-1)\ldots(i-k+1)$$

which is indeed a degree $2t$ polynomial, as each term in the sum is a degree $\leq 2t$ polynomial.

3. (a) At every even integer i, $q(i) \in [0, 1/3]$ as it is the average of the success probabilities of quantum algorithms (and thus ≥ 0 and $\leq 1/3$ as the output is reject). Likewise, for every odd integer i, $q(i) \in [2/3, 1]$. Any cartoon that matches this is acceptable.

(b) Since the function is continuous, it crosses the line at $1/2$ at least N times (once per oscillation). Thus $q - 1/2$ has at least N zeroes and therefore q is degree $\geq N$.

(c) The degree of q satisifes both $\geq N$ and $\leq 2t$. Therefore, $t \geq N/2$.