

Chapter 1

Introduction and overview

1.1 Global perspectives

1.2 Quantum bits

1.3 Quantum computation

1.4 Quantum algorithm

Exercise 1.1. Suppose that the problem is not to distinguish between the constant and balanced functions *with certainty*, but rather, with some probability of error $\epsilon < 1/2$. What is the performance of the best classical algorithm for this problem?

Solution: Suppose Alice queries Bob j times, where $j \leq 2^{n-1}$. If she receives both 0(s) and 1(s), then she can determine $f(x)$ as balanced with certainty. If she receives all 0(s) (or all 1(s)), then according to Bayes' theorem and Law of total probability, the probability that $f(x)$ is constant is

$$\begin{aligned} & P(f(x) \text{ is constant} | f(x) = 0 \forall x = 0, 1, \dots, j) = P(f(x) \text{ is constant} | f(x) = 1 \forall x = 0, 1, \dots, j) \\ &= \frac{P(f(x) \text{ is constant})P(f(x) = 0 \forall j = 0, 1, \dots, j | f(x) \text{ is constant})}{P(f(x) = 0 \forall j = 0, 1, \dots, j)} \\ &= \frac{P(f(x) \text{ is constant})P(f(x) = 0 \forall j = 0, 1, \dots, j | f(x) \text{ is constant})}{P(f(x) \text{ is constant})P(f(x) = 0 \forall j = 0, 1, \dots, j | f(x) \text{ is constant})} \\ &\quad + \frac{P(f(x) \text{ is balanced})P(f(x) = 0 \forall j = 0, 1, \dots, j | f(x) \text{ is balanced})}{P(f(x) \text{ is balanced})P(f(x) = 0 \forall j = 0, 1, \dots, j | f(x) \text{ is balanced})} \\ &= \frac{\frac{1}{2} \times \frac{1}{2}}{\frac{1}{2} \times \frac{1}{2} + \frac{1}{2} \times \frac{C_{2^{n-1}}^{2^n-k}}{C_{2^{n-1}}^{2^n}}} = \frac{1}{1 + 2 \frac{(2^n-j)!(2^{n-1}-j)!}{(2^n)!(2^{n-1}-j)!}} = \frac{(2^n-1)(2^n-2) \dots (2^n-j+1)}{(2^n-1)(2^n-2) \dots (2^n-j+1) + (2^{n-1}-1)(2^{n-1}-2) \dots (2^{n-1}-j+1)}. \end{aligned} \tag{1.1}$$

and the probability that $f(x)$ is balanced is

$$\begin{aligned} & P(f(x) \text{ is balanced} | f(x) = 0 \forall x = 0, 1, \dots, j) = P(f(x) \text{ is balanced} | f(x) = 1 \forall x = 0, 1, \dots, j) \\ &= \frac{P(f(x) \text{ is balanced})P(f(x) = 0 \forall j = 0, 1, \dots, j | f(x) \text{ is balanced})}{P(f(x) = 0 \forall j = 0, 1, \dots, j)} \\ &= \frac{P(f(x) \text{ is balanced})P(f(x) = 0 \forall j = 0, 1, \dots, j | f(x) \text{ is balanced})}{P(f(x) \text{ is constant})P(f(x) = 0 \forall x = 0, 1, \dots, j | f(x) \text{ is constant})} \\ &\quad + \frac{P(f(x) \text{ is balanced})P(f(x) = 0 \forall x = 0, 1, \dots, j | f(x) \text{ is balanced})}{P(f(x) \text{ is balanced})P(f(x) = 0 \forall x = 0, 1, \dots, j | f(x) \text{ is balanced})} \\ &= \frac{\frac{1}{2} \times \frac{C_{2^{n-1}}^{2^n-j}}{C_{2^{n-1}}^{2^n}}}{\frac{1}{2} \times \frac{1}{2} + \frac{1}{2} \times \frac{C_{2^{n-1}}^{2^n-k}}{C_{2^{n-1}}^{2^n}}} = \frac{2 \frac{(2^n-k)!(2^{n-1}-j)!}{(2^n)!(2^{n-1}-j)!}}{1 + 2 \frac{(2^n-k)!(2^{n-1}-j)!}{(2^n)!(2^{n-1}-j)!}} = \frac{(2^{n-1}-1)(2^{n-1}-2) \dots (2^{n-1}-j+1)}{(2^n-1)(2^n-2) \dots (2^n-j+1) + (2^{n-1}-1)(2^{n-1}-2) \dots (2^{n-1}-j+1)}. \end{aligned} \tag{1.2}$$

Note that

$$P(f(x) \text{ is constant} | f(x) = 0 \forall x = 0, 1, \dots, j) \geq P(f(x) \text{ is balanced} | f(x) = 0 \forall x = 0, 1, \dots, j) \tag{1.3}$$

with equality if and only if $j = 1$. Therefore, the best classical algorithm is:

1. Alice selects number $x = 0$ and queries Bob;
2.
 - i. If Alice have received both 0(s) and 1(s), then she determines $f(x)$ as balanced;
 - ii. If Alice have received either all 0(s) or 1(s), and $P(f(x) \text{ is constant} | f(x) = 0 \forall x = 0, 1, \dots, j) > \frac{1}{2}$ or $P(f(x) \text{ is constant} | f(x) = 1 \forall x = 0, 1, \dots, j) > \frac{1}{2}$, then she classifies $f(x)$ as constant;
 - iii. Otherwise, let $x = x + 1$ and return to step 1.

In the worst case, Alice queries Bob (say) k times and receives k 0s. She classifies $f(x)$ as constant since the error probability of her judgement is just below $1/2$:

$$\begin{aligned} P(\text{error} | f(x) = 0 \forall x = 0, 1, \dots, k-1) &= P(f(x) \text{ is balanced} | f(x) = 0 \forall x = 0, 1, \dots, k-1) \\ &= \frac{(2^{n-1} - 1)(2^{n-1} - 2) \dots (2^{n-1} - k + 1)}{(2^n - 1)(2^n - 2) \dots (2^n - k + 1) + (2^{n-1} - 1)(2^{n-1} - 2) \dots (2^{n-1} - k + 1)} < \frac{1}{2}. \end{aligned} \quad (1.4)$$

If Alice only queries Bob $(k-1)$ times and receives $(k-1)$ 0s, she can not make judgement with error probability less than $1/2$:

$$\begin{aligned} P(\text{error} | f(x) = 0 \forall x = 0, 1, \dots, k-2) &= P(f(x) \text{ is balanced} | f(x) = 0 \forall x = 0, 1, \dots, k-2) \\ &\geq \frac{(2^{n-1} - 1)(2^{n-1} - 2) \dots (2^{n-1} - k + 2)}{(2^n - 1)(2^n - 2) \dots (2^n - k + 2) + (2^{n-1} - 1)(2^{n-1} - 2) \dots (2^{n-1} - k + 2)} \geq \frac{1}{2}, \end{aligned} \quad (1.5)$$

so we have

$$k = 2. \quad (1.6)$$

i.e., the computation complexity of the best classical algorithm for this problem is $O(1)$. \square

1.5 Experimental quantum information processing

Exercise 1.2. Explain how a device which, upon input of one of two non-orthogonal quantum states $|\psi\rangle$ or $|\varphi\rangle$ correctly identified the state, could be used to build a theorem which cloned the states $|\psi\rangle$ and $|\varphi\rangle$, in violation of the no-cloning theorem. Conversely, explain how device for cloning could be used to distinguish non-orthogonal quantum states.

Proof: The no-cloning theorem says that it is impossible for a cloning device to clone states that are not orthogonal to one another. If we have a device that can distinguish two non-orthogonal quantum states $|\psi\rangle$ and $|\varphi\rangle$, given a state either $|\phi\rangle$ or $|\varphi\rangle$, we can use this device to know whether the state is $|\phi\rangle$ and $|\varphi\rangle$, then find a another system and initialize it to the same state with not too much difficulty. In this way, we can clone states that are non-orthogonal, which violate the no-cloning theorem.

Conversely, if we have a device for cloning quantum states, given an unknown state, we can use this device to generate copies of the state and measure it as many times as we want, so that we will obtain enough information to determine the state. In this way, we can distinguish non-orthogonal quantum states. \square

1.6 Quantum information