

## Question 2

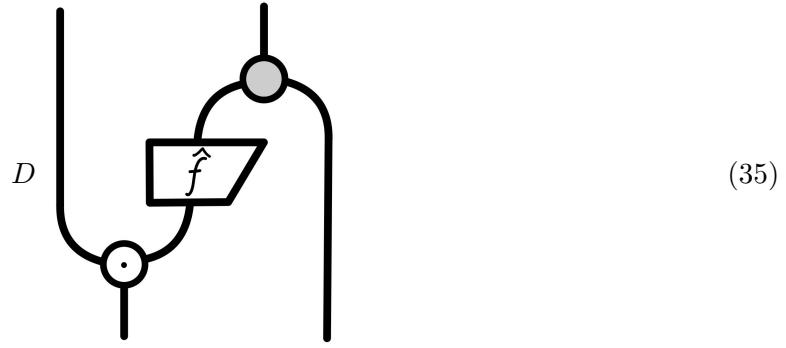
### 2.1 The problem

For this open-ended question, we will present a diagrammatic quantum algorithm for the Quantum Counting Problem, based on [Brassard et al., 2002]. This problem consists of counting the number of input values  $i$  for which a boolean function  $f : \{0, 1, \dots, 2^n\} \rightarrow \{0, 1\}$  evaluates to 1. The presented quantum algorithm allows to approximate the solution to this problem

**Problem 2.1.** Given the function  $f : \{0, 1, \dots, 2^n\} \rightarrow \{0, 1\}$ , count the size of the following set:

$$\{i \in \{0, 1, \dots, 2^n\} \mid f(i) = 1\} \quad (34)$$

We assume that we are given access to the following quantum oracle:



Where we encoded the function  $f$  as a linear map from  $\mathcal{H}_n$  to  $\mathcal{H}_1$ .

$$\begin{array}{c} \boxed{\mathcal{H}_1} \\ f \\ \boxed{\mathcal{H}_n} \\ \downarrow i \end{array} = \downarrow_{f\omega} \in \left\{ \downarrow_0, \downarrow_1 \right\} \quad (36)$$

Note that this quantum oracle is unitary by Proposition 12.15 in Picturing Quantum Processes.

Here, we denoted the Hilbert space of a  $k$ -qubit system by  $\mathcal{H}_k$ , i.e.  $\mathcal{H}_k = (\mathbb{C}^2)^k$ , which we will continue to do for the rest of this question. Additionally, here follow some constants that will be useful throughout this presentation. First,  $n$  is an integer such that the input domain of  $f$  has size  $2^n$ . It will also be the number of qubits in the input register of the algorithm. For convenience, let  $N := 2^n$ . Next,  $p$  is the number of qubits in an auxiliary register that will be used in the algorithm. For convenience, let  $P := 2^p$ . Finally, denote the size of the set (34) by  $N_A$  (this is the number we are approximating) and let  $N_B = N - N_A$ .

### 2.2 Components

In this subsection, we will build up some components that will be used in the final algorithm.

**Component 2.2.** Let  $S_0 : \mathcal{H}_n \rightarrow \mathcal{H}_n$  be the unitary that negates the zero (standard) basis state, and maps every other basis state of  $\mathcal{H}_n$  to itself.

$$\begin{array}{c} \text{Schematic of } S_0 \end{array} = \left( \sum_{0 \leq i < N} \begin{array}{c} \text{Schematic of } S_0 \\ \text{with index } i \end{array} \right) - 2 \begin{array}{c} \text{Schematic of } S_0 \\ \text{with index } 0 \end{array} = \begin{array}{c} \text{Schematic of } S_0 \end{array} - 2 \begin{array}{c} \text{Schematic of } S_0 \\ \text{with index } 0 \end{array} \quad (37)$$

**Component 2.3.** Let  $S_f : \mathcal{H}_n \rightarrow \mathcal{H}_n$  be the unitary that negates all (standard) basis states  $|i\rangle$  of  $\mathcal{H}_n$  for which  $f(i) = 1$ , and maps the other basis states to themselves.

This component can be represented as follows, as proven in the discussion after equation (12.18) in Picturing Quantum Processes.

$$\begin{array}{c} \text{Schematic of } S_f \end{array} = \begin{array}{c} \text{Schematic of } S_f \end{array} \circ \begin{array}{c} \text{Schematic of } f \\ \text{with } \pi \text{-phase spider} \end{array} \quad (38)$$

Its doubled version can be realised by plugging the doubled white  $\pi$ -phase spider into the right input of the quantum oracle (35) and discarding the oracle's right output. This follows immediately from Lemma 1.2.

**Component 2.4.** Let  $G_f : \mathcal{H} \rightarrow \mathcal{H}$  be the component defined by the following equation.

$$\begin{array}{c} \text{Schematic of } G_f \end{array} := - \begin{array}{c} \text{Schematic of } G_f \\ \text{with } S_0 \text{ and } S_f \end{array} \quad (39)$$

We will prove in the following lemma that  $G_f$  is a slightly modified version of the Grover iteration used in Picturing Quantum Processes.

**Lemma 2.5.**  $G_f$  is the Grover iteration from Picturing Quantum Processes, where the right input is fixed to be a white  $\pi$ -phase spider and the right output is deleted.

*Proof.* First, note that we can rewrite the upper part of  $G_f$  as follows:

This is the same definition for  $d$  as the one used in section 12.2.3 of Picturing Quantum Processes. Putting (38-40) together yields

$$\begin{array}{c} \text{Diagram showing the decomposition of } G_f \\ \text{into } S_0 \text{ and } S_f \text{ components,} \\ \text{and its equivalence to a } d \text{-} f \text{ circuit with } \pi \text{ and a dot.} \end{array} \quad (41)$$

Which is the Grover iteration from section 12.2.3 in Picturing Quantum Processes, where the right input is fixed to be a white  $\pi$ -phase spider and the right output is deleted (follows from Lemma 1.2).  $\square$

**Component 2.6.** Let  $G_f^j : \mathcal{H}_n \rightarrow \mathcal{H}_n$  be the sequential composition of  $j$  times  $G_f$ , for every  $j \in \mathbb{Z}^+$ . For  $j = 0$ , define  $G_f^j$  to be the identity.

$$G_f^j = \left\{ G_f^j, \dots, G_f^j \right\} \quad (42)$$

For the next component, we will introduce an auxiliary register with  $p$  qubits. Let  $P = 2^p$ . The precision of the algorithm's approximation will scale exponentially with  $p$ .

**Component 2.7.** Define  $C_f : \mathcal{H}_p \otimes \mathcal{H}_n \rightarrow \mathcal{H}_p \otimes \mathcal{H}_n$  as follows:

$$\begin{array}{c} \mathcal{H}_p | \quad | \mathcal{H}_n \\ \text{---} \quad \text{---} \\ \mathcal{H}_p \quad | \quad \mathcal{H}_n \end{array} := \sum_{j=0}^{P-1} \begin{array}{c} \text{---} \\ \triangle \dot{\downarrow} \\ \triangle \dot{\uparrow} \\ \text{---} \end{array} \quad \begin{array}{c} \text{---} \\ G_f^j \\ \text{---} \end{array} \quad (43)$$

$C_f$  can be implemented using  $P$  evaluations of the quantum oracle [Brassard et al., 2002].

**Component 2.8.** Let  $F_P : \mathcal{H}_p \rightarrow \mathcal{H}_p$  be the process that applies a quantum Fourier transform with phase factor  $\omega = e^{\frac{2\pi i}{P}}$ .

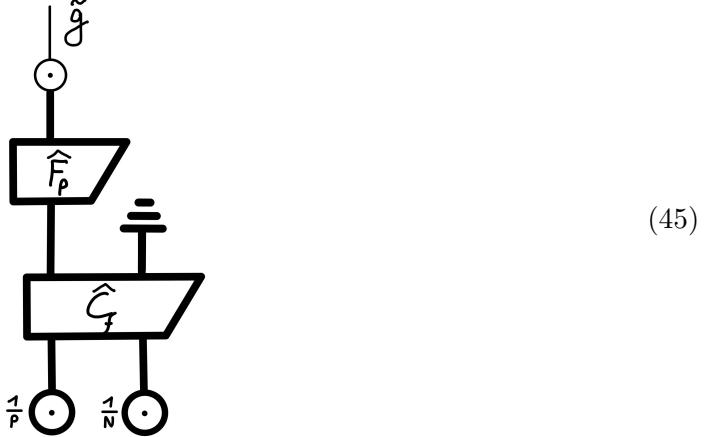
$$\boxed{F_p} := \frac{1}{\sqrt{P}} \sum_{k=0}^{P-1} \sum_{l=0}^{P-1} \omega^{kl} \begin{array}{c} \text{e} \\ \text{r} \end{array} \quad (44)$$

$F_P$  can be implemented efficiently, as shown in [Shor, 1999].

## 2.3 Algorithm

Now that all necessary components have been defined, we can state the algorithm.

**Algorithm 2.9.** Realise the following quantum circuit and call the measurement outcome  $\tilde{g}$ . Then output  $N \sin^2 \left( \frac{\tilde{g}\pi}{P} \right)$ .



Here, the left dotted spider is a doubled  $\mathcal{H}_p$ -spider and the right one is a doubled  $\mathcal{H}_n$ -spider.

We claim the following and will prove it over the course of the following section.

**Theorem 2.10** (Correctness of Algorithm 2.9). If  $\tilde{N} = N \sin^2 \left( \frac{\tilde{g}\pi}{P} \right)$  is the output of Algorithm 2.9, then

$$|\tilde{N} - N_A| < \frac{2\pi}{P} \sqrt{NN_A} + \frac{\pi^2}{P^2} N \quad (46)$$

with probability at least  $\frac{3}{5}$ .

From this theorem follows that we can approximate  $N_A$  to arbitrary precision (by choosing  $P$  large enough) and with an arbitrarily large probability (by repeating the algorithm multiple times). For any constant  $c$ , [Brassard et al., 2002] exhibit a strategy to obtain an estimate  $\tilde{N}$  such that

$$|\tilde{N} - N_A| < \frac{N_A}{c} \quad (47)$$

with probability at least  $\frac{3}{4}$ . They achieve this by running the algorithm multiple times, with an expected number of  $\Theta \left( (c + \log \log N) \sqrt{\frac{N}{N_A}} \right)$  function evaluations.

## 2.4 Correctness

Define the following two unnormalized  $n$ -qubit states:

$$\begin{array}{c} \text{---} \\ \alpha \end{array} := \sum_{f(i)=1} \begin{array}{c} \text{---} \\ i \end{array} \quad (48)$$

$$\begin{array}{c} \text{---} \\ \beta \end{array} := \sum_{f(i)=0} \begin{array}{c} \text{---} \\ i \end{array} \quad (49)$$

And note that

$$\begin{array}{c} \text{---} \\ \bullet \end{array} = \sum_{0 \leq i < N} \begin{array}{c} \text{---} \\ i \end{array} = \begin{array}{c} \text{---} \\ \alpha \end{array} + \begin{array}{c} \text{---} \\ \beta \end{array} \quad (50)$$

We will first investigate how  $G_f$  acts on  $\alpha$  and  $\beta$ .

**Lemma 2.11.**

$$\begin{array}{c} \text{---} \\ G_f \end{array} \begin{array}{c} \text{---} \\ \alpha \end{array} = \left(1 - \frac{2N_A}{N}\right) \cdot \begin{array}{c} \text{---} \\ \alpha \end{array} - \frac{2N_A}{N} \begin{array}{c} \text{---} \\ \beta \end{array} \quad (51)$$

$$\begin{array}{c} \text{---} \\ G_f \end{array} \begin{array}{c} \text{---} \\ \beta \end{array} = \frac{2N_B}{N} \begin{array}{c} \text{---} \\ \alpha \end{array} + \left(1 - \frac{2N_A}{N}\right) \cdot \begin{array}{c} \text{---} \\ \beta \end{array} \quad (52)$$

*Proof.* By doing some manipulations, we can prove (51):

$$\begin{aligned} \begin{array}{c} \text{---} \\ G_f \end{array} \begin{array}{c} \text{---} \\ \alpha \end{array} &= \sum_{f(i)=1} - \begin{array}{c} \text{---} \\ S_0 \end{array} \begin{array}{c} \text{---} \\ \alpha \end{array} = \sum_{f(i)=1} - \begin{array}{c} \text{---} \\ d \end{array} \begin{array}{c} \text{---} \\ i \end{array} = \sum_{f(i)=1} - \frac{2}{N} \begin{array}{c} \text{---} \\ \bullet \end{array} + \sum_{f(i)=1} \begin{array}{c} \text{---} \\ i \end{array} \\ &= -2 \frac{N_A}{N} \begin{array}{c} \text{---} \\ \bullet \end{array} + \begin{array}{c} \text{---} \\ \alpha \end{array} = \left(1 - \frac{2N_A}{N}\right) \cdot \begin{array}{c} \text{---} \\ \alpha \end{array} - \frac{2N_A}{N} \begin{array}{c} \text{---} \\ \beta \end{array} \end{aligned} \quad (53)$$

The first equality follows from expanding the definitions of  $G_f$  and  $\alpha$ . The second can be obtained by rewriting the upper part of  $G_f$  as in (40) and realizing that, by definition,  $S_f$  maps every basis

state  $|i\rangle$  for which  $f(i) = 1$  to  $-|i\rangle$ . The third follows from the definition of  $d$  and the fourth from the fact that, by the definition of the dotted spider, the number at the bottom of the first summation is the empty diagram. Finally, the last equality follows from (50).

The proof of (52) proceeds analogously:

$$\begin{aligned}
 \text{Diagram } G_f^j &= \sum_{f(i)=0} - \text{Diagram } S_0 \text{ (dotted spider)} = \sum_{f(i)=0} \text{Diagram } d = \sum_{f(i)=0} \frac{2}{N} \text{Diagram } i - \sum_{f(i)=0} \text{Diagram } i \\
 &= 2 \frac{N_B}{N} \text{Diagram } i - \text{Diagram } \beta = \frac{2N_B}{N} \text{Diagram } \alpha + \left(1 - \frac{2N_A}{N}\right) \cdot \text{Diagram } \beta
 \end{aligned} \tag{54}$$

Note that there is no minus sign in the third expression, because  $S_f$  does not negate the basis states  $|i\rangle$  for which  $f(i) = 0$ .  $\square$

Lemma 2.11 is quite surprising, as it means that the subspace spanned by the set  $\{\alpha, \beta\}$  is invariant under the action of  $G_f$  and hence also of  $G_f^j$ . I.e., if we apply  $G_f^j$  to a linear combination of  $\alpha$  and  $\beta$ , e.g. the dotted spider (50), the result will always be a new linear combination of  $\alpha$  and  $\beta$ . At this stage, Grover's search algorithm would choose  $j \in \mathbb{Z}$  to maximize the coefficient of  $\alpha$  (relative to the coefficient of  $\beta$ ) and perform an  $n$ -qubit ONB measurement, which would yield a basis state  $|i\rangle$  with  $f(i) = 1$  with high probability. However, we are interested in *counting* the number of states with  $f(i) = 1$  rather than finding them. For this purpose, we will show in Lemma 2.12 that applying  $G_f^j$  to the dotted spider, for  $j \in \{0, 1, 2, \dots\}$  yields a function that is sinusoidal in  $j$  and whose period depends on  $\frac{N_A}{N}$ . The algorithm recovers this period with high accuracy by applying a quantum Fourier transform on the auxiliary  $p$ -qubit register.

Define  $\theta$  as the unique angle in  $[0, \frac{\pi}{2}]$  such that

$$\sin^2(\theta) = \frac{N_A}{N} \tag{55}$$

and (by consequence)

$$\cos^2(\theta) = \frac{N_B}{N} \tag{56}$$

**Lemma 2.12.** *For every  $j \in \{0, 1, \dots\}$ :*

$$\text{Diagram } G_f^j = k_j \text{Diagram } \alpha + l_j \text{Diagram } \beta \tag{57}$$

where

$$k_j = \frac{\sin((2j+1)\theta)}{\sin(\theta)} \quad (58)$$

$$l_j = \frac{\cos((2j+1)\theta)}{\cos(\theta)} \quad (59)$$

*Proof.* We will prove this by induction on  $j$ .

For the base case  $j = 0$ , it follows from (50) that

$$\begin{aligned} \bullet &= \underset{\alpha}{\text{---}} + \underset{\beta}{\text{---}} \\ &= \frac{\sin(\theta)}{\sin(\theta)} \underset{\alpha}{\text{---}} + \frac{\cos(\theta)}{\cos(\theta)} \underset{\beta}{\text{---}} \end{aligned} \quad (60)$$

Now assume that the induction hypothesis (57-59) holds for  $j - 1$ . Then

$$\begin{aligned} \underset{\bullet}{\text{---}} \underset{G_j^j}{\boxed{\text{---}}} &= k_{j-1} \underset{\alpha}{\text{---}} \underset{G_j^j}{\boxed{\text{---}}} + l_{j-1} \underset{\beta}{\text{---}} \underset{G_j^j}{\boxed{\text{---}}} \\ &= k_{j-1} \left(1 - \frac{2N_A}{N}\right) \underset{\alpha}{\text{---}} - k_{j-1} \frac{2N_A}{N} \underset{\beta}{\text{---}} \\ &\quad + l_{j-1} \frac{2N_B}{N} \underset{\alpha}{\text{---}} + l_{j-1} \left(1 - \frac{2N_A}{N}\right) \underset{\beta}{\text{---}} \\ &= k_j \underset{\alpha}{\text{---}} + l_j \underset{\beta}{\text{---}} \end{aligned} \quad (61)$$

Where

$$\begin{aligned} k_j &= k_{j-1} \left(1 - \frac{2N_A}{N}\right) + l_{j-1} \frac{2N_B}{N} \\ &= \frac{1}{\sin(\theta)} \sin((2j-1)\theta) \cdot (1 - 2\sin^2(\theta)) + \cos((2j-1)\theta) \cdot \frac{2\cos^2(\theta)}{\cos(\theta)} \\ &= \frac{1}{\sin(\theta)} \left( \sin((2j-1)\theta) \cos(2\theta) + \cos((2j-1)\theta) \sin(2\theta) \right) \\ &= \frac{\sin((2j+1)\theta)}{\sin(\theta)} \end{aligned} \quad (62)$$

And

$$\begin{aligned}
l_j &= k_{j-1} \frac{-2N_A}{N} + l_{j-1} \left( 1 - \frac{2N_A}{N} \right) \\
&= \sin((2j-1)\theta) \cdot \frac{-2\sin^2(\theta)}{\sin(\theta)} + \frac{1}{\cos(\theta)} \cos((2j-1)\theta) \cdot (1 - 2\sin^2(\theta)) \\
&= \frac{1}{\cos(\theta)} \left( -\sin((2j-1)\theta) \sin(2\theta) + \cos((2j-1)\theta) \cos(2\theta) \right) \\
&= \frac{\cos((2j+1)\theta)}{\cos(\theta)}
\end{aligned} \tag{63}$$

□

The algorithm applies  $\hat{F}_P$  on the following quantum state  $\hat{\Psi}$ :



The expansion of  $\hat{\Psi}$  contains a double sum. Luckily, we can decompose  $\hat{\Psi}$  as a mixture of two pure quantum states  $\hat{\Psi}_A$  and  $\hat{\Psi}_B$ . Afterwards, we continue our analysis by considering the action of  $F_P$  on both undoubled states.

**Lemma 2.13.**

$$|\hat{\Psi}\rangle = |\hat{\Psi}_A\rangle + |\hat{\Psi}_B\rangle \tag{65}$$

where  $\hat{\Psi}_A$  and  $\hat{\Psi}_B$  are the doubled versions of the following states:

$$|\Psi_A\rangle = \frac{1}{\sqrt{P}} \sum_{j=0}^{P-1} \sin((2\theta+1)j) |\downarrow_j\rangle \tag{66}$$

$$|\Psi_B\rangle = \frac{1}{\sqrt{P}} \sum_{j=0}^{P-1} \cos((2\theta+1)j) |\downarrow_j\rangle \tag{67}$$

*Proof.* By expanding the definition of  $C_f$  (43) and doubling, we obtain

$$\begin{aligned}
\text{Circuit } (64) &= \frac{1}{PN} \sum_{m=0}^{P-1} \sum_{n=0}^{P-1} |\downarrow_m\rangle \langle \downarrow_n| \otimes G_f^m \otimes G_f^n
\end{aligned} \tag{68}$$

After discarding the right output in the previous expression, we obtain  $\hat{\Psi}$ :

$$\begin{aligned}
\hat{\Psi} &= \frac{1}{PN} \sum_{m=0}^{P-1} \sum_{n=0}^{P-1} \downarrow_m \downarrow_n \quad G_f^m \quad G_f^n \\
&= \frac{1}{PN} \sum_{m=0}^{P-1} \sum_{n=0}^{P-1} \downarrow_m \downarrow_n \otimes \left( k_m k_n \downarrow_\alpha \downarrow_\alpha + k_m l_n \downarrow_\alpha \downarrow_\beta \right. \\
&\quad \left. + l_m k_n \downarrow_\beta \downarrow_\alpha + l_m l_n \downarrow_\beta \downarrow_\beta \right) \\
&= \frac{1}{PN} \sum_{m=0}^{P-1} \sum_{n=0}^{P-1} (N_A k_m k_n + N_B l_m l_n) \downarrow_m \downarrow_n
\end{aligned} \tag{69}$$

Here, we first used the expansion derived in Lemma 2.12 to further expand the second factor and then noted the following:

$$\begin{array}{c} \alpha \\ \downarrow \\ \alpha \end{array} = N_A, \quad \begin{array}{c} \beta \\ \downarrow \\ \beta \end{array} = N_B, \quad \begin{array}{c} \beta \\ \downarrow \\ \alpha \end{array} = \begin{array}{c} \alpha \\ \downarrow \\ \beta \end{array} = 0
\tag{70}$$

Now, we can split  $\hat{\Psi}$  into two pure states by further manipulation of (69).

$$\begin{aligned}
\hat{\Psi} &= \frac{1}{\sqrt{P}} \left( \sum_{m=0}^{P-1} \sqrt{\frac{N_A}{N}} k_m \downarrow_m \right) \cdot \frac{1}{\sqrt{P}} \left( \sum_{n=0}^{P-1} \sqrt{\frac{N_A}{N}} k_n \downarrow_n \right) \\
&\quad + \frac{1}{\sqrt{P}} \left( \sum_{m=0}^{P-1} \sqrt{\frac{N_B}{N}} l_m \downarrow_m \right) \cdot \frac{1}{\sqrt{P}} \left( \sum_{n=0}^{P-1} \sqrt{\frac{N_B}{N}} l_n \downarrow_n \right) \\
&= \text{double} \left( \begin{array}{c} \downarrow \\ \boxed{\Psi_A} \end{array} \right) + \text{double} \left( \begin{array}{c} \downarrow \\ \boxed{\Psi_B} \end{array} \right)
\end{aligned} \tag{71}$$

Where  $\Psi_A$  and  $\Psi_B$  are defined as follows:

$$\begin{array}{c} \downarrow \\ \boxed{\Psi_A} \end{array} = \frac{1}{\sqrt{P}} \sum_{j=0}^{P-1} \sqrt{\frac{N_A}{N}} k_j \downarrow_j = \frac{1}{\sqrt{P}} \sum_{j=0}^{P-1} \sin((2\theta+1)j) \downarrow_j
\tag{72}$$

$$\begin{array}{c} \downarrow \\ \boxed{\Psi_B} \end{array} = \frac{1}{\sqrt{P}} \sum_{j=0}^{P-1} \sqrt{\frac{N_B}{N}} l_j \downarrow_j = \frac{1}{\sqrt{P}} \sum_{j=0}^{P-1} \cos((2\theta+1)j) \downarrow_j
\tag{73}$$

□

Now we are ready to consider the state just before the measurement of  $\tilde{g}$ . Denote this state by  $\hat{\Phi}$ . Also denote the result of applying  $F_P$  to  $\Psi_A$  by  $\Phi_A$  and analogously for  $\Phi_B$ . Note that  $\hat{\Phi}_A$  and  $\hat{\Phi}_B$

are pure quantum states such that

$$\hat{\Phi} = \hat{F}_P \hat{\Psi} + \hat{F}_P \hat{\Psi}_A = \hat{\Phi}_A + \hat{\Phi}_B \quad (74)$$

Define

$$g := P \frac{\theta}{\pi} \quad (75)$$

From  $\theta \in [0, \frac{\pi}{2}]$  follows that  $g \in [0, \frac{P}{2}]$ . When we apply the quantum Fourier transform  $F_P$  to either  $\Psi_A$  or  $\Psi_B$ , the output state will be a linear combination of basis states with high coefficients for the basis states  $|l\rangle$  for which  $l \approx g$  or  $l \approx P - g$ . When  $g$  is an integer,  $|g\rangle$  and  $|P - g\rangle$  are even the only basis states with a nonzero coefficient. This all follows from the frequency filtering property of the discrete Fourier transform [Sundararajan, 2001], of which the quantum Fourier transform is a variation. We will now prove (without diving too much into out-of-scope algebraic details) that the result  $\tilde{g}$  of the standard ONB measurement of  $\hat{\Phi}$  satisfies  $|\tilde{g} - g| < 1$  or  $|\tilde{g} - (P - g)|$  with a probability of at least  $\frac{3}{5}$ .

**Lemma 2.14.** Denote the result of an ONB measurement on  $\hat{\Phi}$  by  $\tilde{g}$ . Then

$$|\tilde{g} - g| < 1 \quad \text{or} \quad |\tilde{g} - (P - g)| < 1 \quad (76)$$

with probability of at least  $\frac{3}{5}$ .

*Proof.* If  $g$  is an integer, then both  $|\Phi_A\rangle$  and  $|\Phi_B\rangle$  have only non-zero coefficients for basis states  $|g\rangle$  and  $|P - g\rangle$  by the frequency filtering property of the Fourier transform. Hence, the result of a measurement of  $\hat{\Phi}$  is either  $\tilde{g} = g$  or  $\tilde{g} = P - g$ , which always satisfies (76).

If  $g$  is not an integer, we define  $g^- = \lfloor g \rfloor$  and  $g^+ = \lceil g \rceil$ . We analyse  $|\Phi_A\rangle$  for the three cases  $0 < g < 1$ ,  $1 < g < \frac{P}{2} - 1$  and  $\frac{P}{2} - 1 < g < \frac{P}{2}$ .

If  $1 < g < \frac{P}{2} - 1$ , then

$$|\Phi_A\rangle = a|g^-\rangle + b|g^+\rangle + c|P - g^-\rangle + d|P - g^+\rangle + |R_A\rangle \quad (77)$$

For some  $a, b, c, d \in \mathbb{C}$  and some unnormalized error term  $|R_A\rangle$ . If  $0 < g < 1$  then

$$|\Phi_A\rangle = a|0\rangle + b|1\rangle + c|P - 1\rangle + |R_A\rangle \quad (78)$$

and if  $\frac{P}{2} - 1 < g < \frac{P}{2}$  then

$$|\Phi_A\rangle = a|\frac{P}{2} - 1\rangle + b|\frac{P}{2}\rangle + c|\frac{P}{2} + 1\rangle + |R_A\rangle \quad (79)$$

In all of these three cases, extensive algebraic manipulation [Brassard et al., 2002] shows that the norm of the error term can be upper bounded by

$$\langle R_A | R_A \rangle < \frac{2}{5} \langle \Phi_A | \Phi_A \rangle \quad (80)$$

Totally analogously, for all three cases there is decomposition of  $|\Phi_B\rangle$  into basis states  $|l\rangle$  for which  $|l - g| < 1$  or  $|l - (P - g)| < 1$  and an unnormalized error term  $|R_B\rangle$ . The norm of this error term can again be bounded.

$$\langle R_B | R_B \rangle < \frac{2}{5} \langle \Phi_B | \Phi_B \rangle \quad (81)$$

By (80) and (81) the probability that the result of measuring  $\hat{\Phi}$  comes from one of the error terms is upper bounded by  $\frac{2}{5}$ .  $\square$

We can now prove the crux of this presentation: Theorem 2.10 about the correctness of Algorithm 2.9 (repeated here for clarity).

**Theorem 2.10** (Correctness of Algorithm 2.9 [repeated]). *If  $\tilde{N} = N \sin^2\left(\frac{\tilde{g}\pi}{P}\right)$  is the output of Algorithm 2.9, then*

$$|\tilde{N} - N_A| < \frac{2\pi}{P} \sqrt{NN_A} + \frac{\pi^2}{P^2} N \quad (46)$$

*with probability at least  $\frac{3}{5}$ .*

*Proof.* We showed in Lemma 2.14 that  $|\tilde{g} - g| < 1$  or  $|\tilde{g} - (P - g)| < 1$  with probability at least  $\frac{3}{5}$ . Now, we will show that either of these two cases entails (46). Assume that  $|\tilde{g} - g| < 1$ , the other case is equivalent because  $\sin\left(\frac{(P-g)\pi}{P}\right) = \sin\left(\frac{g\pi}{P}\right) = \sin(\theta)$ .

From  $|\tilde{g} - g| < 1$  follows  $|\tilde{g}\frac{\pi}{P} - \theta| < \frac{\pi}{P}$ . Because the derivative of  $\sin(x)$  is always in  $[-1, 1]$ :

$$\left| \sin\left(\tilde{g}\frac{\pi}{P}\right) - \sin(\theta) \right| \leq \left| \tilde{g}\frac{\pi}{P} - \theta \right| < \frac{\pi}{P} \quad (82)$$

We can also upper bound the sum of both sines:

$$\left| \sin\left(\tilde{g}\frac{\pi}{P}\right) + \sin(\theta) \right| \leq \left| \sin\left(\tilde{g}\frac{\pi}{P}\right) \right| + |\sin(\theta)| < \frac{\pi}{P} + 2|\sin(\theta)| = \frac{\pi}{P} + 2\sqrt{\frac{N_A}{N}} \quad (83)$$

Combining (82) and (83) yields an upper bound on  $|\tilde{N} - N_A|$ :

$$\begin{aligned} |\tilde{N} - N_A| &= N \cdot \left| \sin\left(\tilde{g}\frac{\pi}{P}\right) + \sin(\theta) \right| \cdot \left| \sin\left(\tilde{g}\frac{\pi}{P}\right) - \sin(\theta) \right| \\ &< N \cdot \left( \frac{\pi}{P} + 2\sqrt{\frac{N_A}{N}} \right) \cdot \frac{\pi}{P} \\ &= \frac{2\pi}{P} \sqrt{NN_A} + \frac{\pi^2}{P^2} N \end{aligned} \quad (84)$$

$\square$

## References

- [Brassard et al., 2002] Brassard, G., Hoyer, P., Mosca, M., and Tapp, A. (2002). Quantum amplitude amplification and estimation. *Contemporary Mathematics*, 305:53–74.
- [Coecke and Kissinger, 2018] Coecke, B. and Kissinger, A. (2018). Picturing quantum processes: A first course on quantum theory and diagrammatic reasoning. In *Diagrammatic Representation and Inference: 10th International Conference, Diagrams 2018, Edinburgh, UK, June 18-22, 2018, Proceedings* 10, pages 28–31. Springer.
- [Nielsen and Chuang, 2001] Nielsen, M. A. and Chuang, I. L. (2001). Quantum computation and quantum information. *Phys. Today*, 54(2):60.
- [Shor, 1999] Shor, P. W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332.
- [Sundararajan, 2001] Sundararajan, D. (2001). *The discrete Fourier transform: theory, algorithms and applications*. World Scientific.