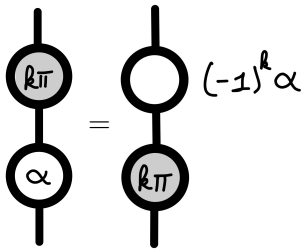
Quantum Processes and Computation

Candidate number: 1083152

Question 1

Before solving any questions, we will state two preliminary lemmas (and two corollaries) that will make our life easier later on.

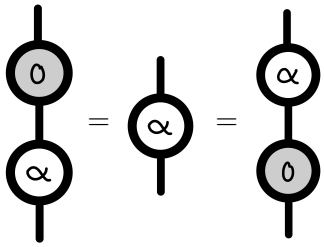
Lemma 1.1. *For all $k \in \{0, 1\}$ and all phases $\alpha \in [0, 2\pi)$:*



(1)

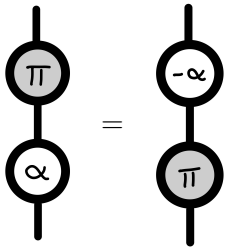
And the same equality holds when the colours are reversed and/or the diagram is reflected vertically.

Proof. We will prove this through a case analysis. If $k = 0$ then the $k\pi$-phase spider is just the identity, so



(2)

If $k = 1$ then it follows from equation (10.83) in Picturing Quantum Processes, a.k.a. the π-commute rule that

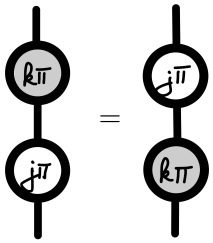


(3)

The same equality holds when taking transposes and/or when reversing the colours. The latter follows from the colour-symmetry of the ZX-calculus. □

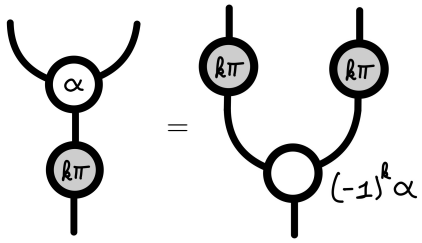
Considering the fact that $(-1)^k \cdot j\pi \equiv j\pi \pmod{2\pi}$ for all $j, k \in \{0, 1\}$, a simple corollary follows:

Corollary 1.1.1. *For all $j, k \in \{0, 1\}$:*



(4)

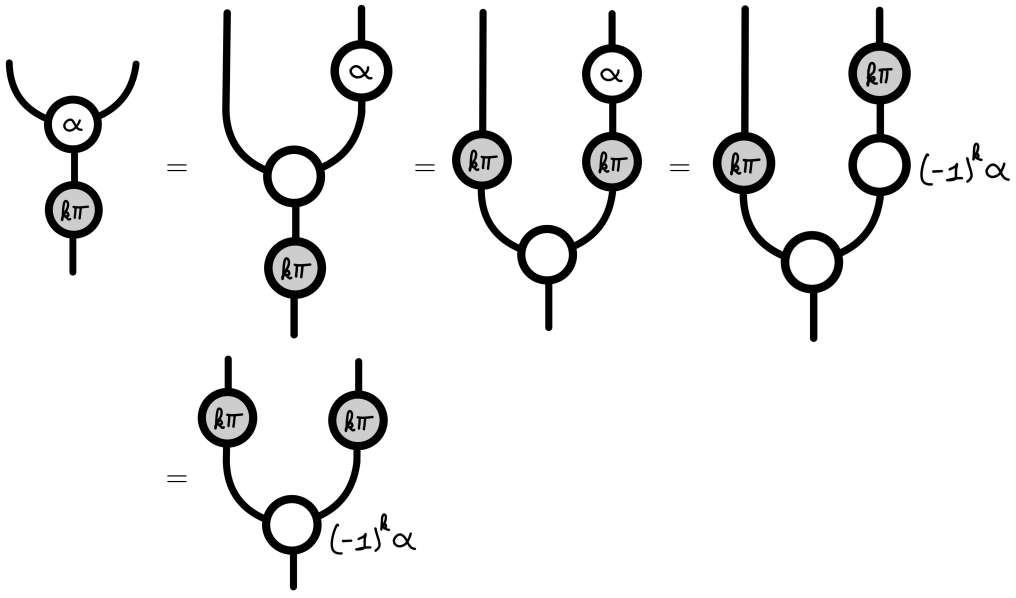
Lemma 1.2. *For all $k \in \{0, 1\}$ and all phases $\alpha \in [0, 2\pi)$:*



(5)

And the same equality holds when the colours are reversed.

Proof.



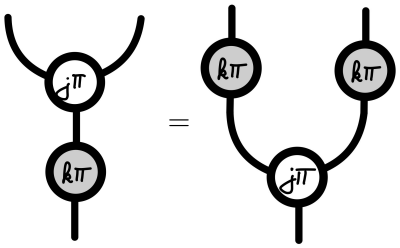
(6)

Here, the first equality follows from phase spider fusion, the second from the phase gate copy rule (equation (10.63) in Picturing Quantum Processes), the third from Lemma 1.1 and the fourth again from phase spider fusion.

The equality with reversed colours follows from the colour-symmetry of the ZX-calculus. □

Again a simple corollary follows from the fact that $(-1)^k \cdot j\pi \equiv j\pi \pmod{2\pi}$ for all $j, k \in \{0, 1\}$:

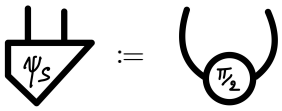
Corollary 1.2.1. *For all $j, k \in \{0, 1\}$:*



(7)

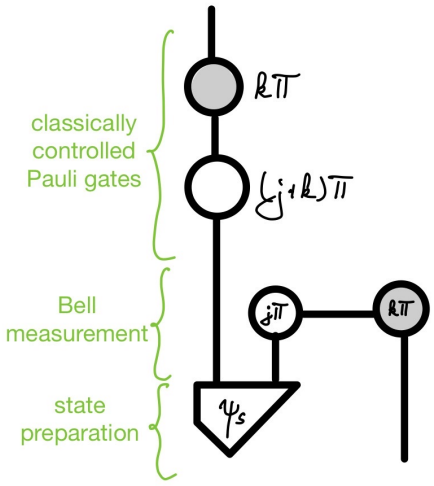
Question 1a

If we define ψ_S as follows, then we can use it to deterministically implement an S gate, as proven in Theorem 1.3.



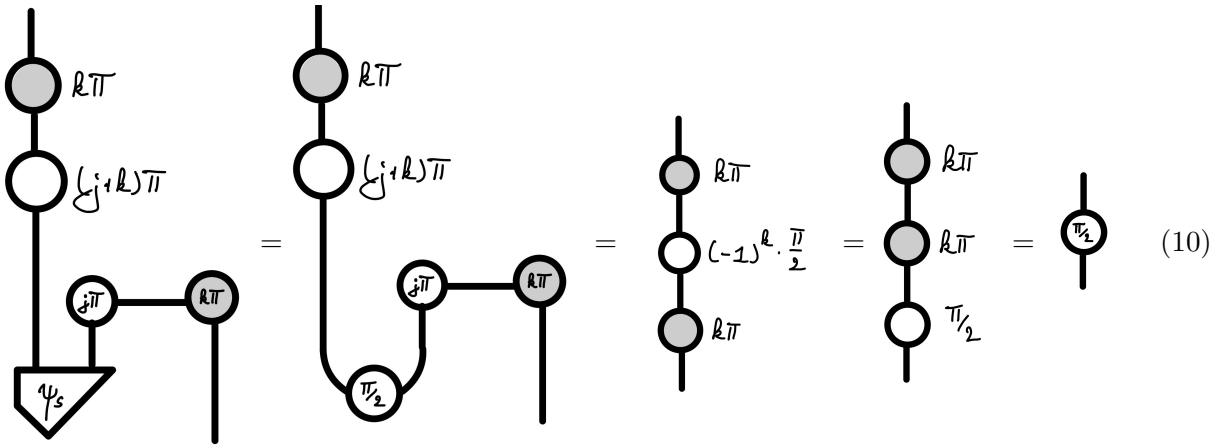
(8)

Theorem 1.3. *The following operation deterministically implements an S gate:*



(9)

Proof.

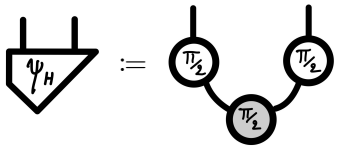


(10)

The first equality holds by the definition of ψ_S. The second holds by phase spider fusion and the fact that $(2j+k)\pi + \frac{\pi}{2} \equiv (-1)^k \frac{\pi}{2} \pmod{2\pi}$ for all $j, k \in \{0, 1\}$. The third follows from Lemma 1.1 and the fourth follows again from phase spider fusion and the fact that $2k\pi \equiv 0 \pmod{2\pi}$. □

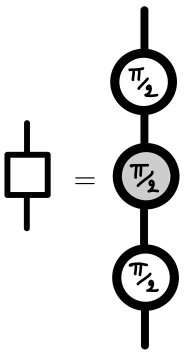
Question 1b

If we define ψ_H as follows, then we can use it to deterministically implement an H gate, as proven in Theorem 1.4.



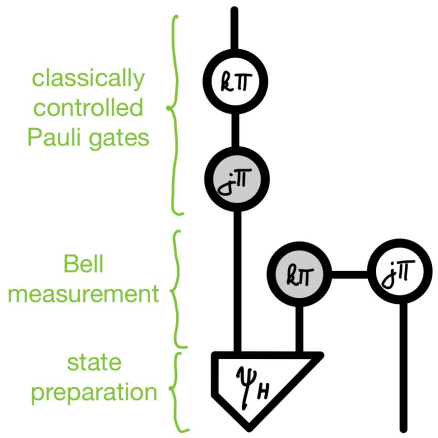
(11)

Recall the definition of the H gate. This is the doubled version of equation (9.120) in Picturing Quantum Processes.



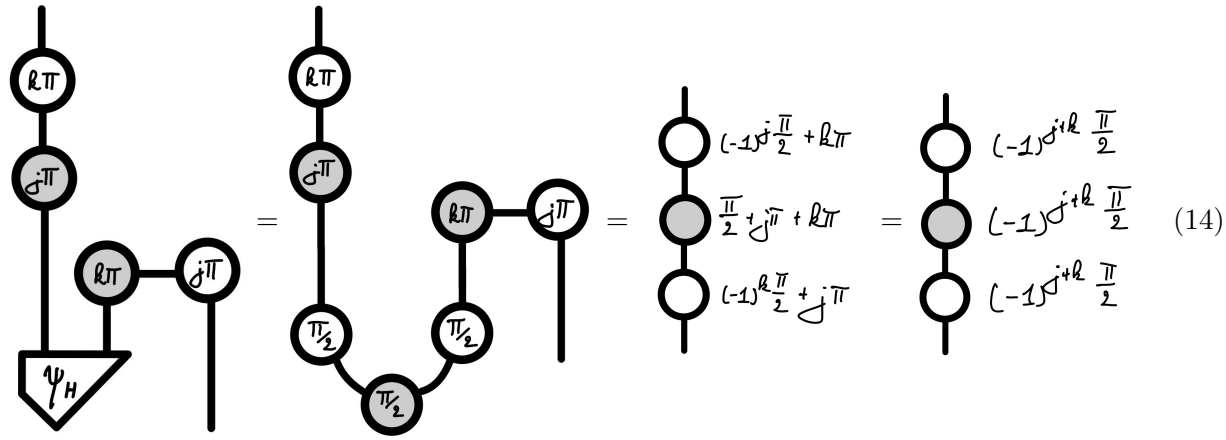
(12)

Theorem 1.4. *The following operation deterministically implements an H gate:*



(13)

Proof.



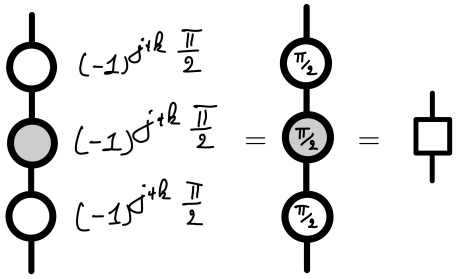
(14)

The first equality holds by the definition of ψ_H. The second can be proven by first using Lemma 1.1 to move all grey spiders to the middle and then applying phase spider fusion. The third is true because the phase on each spider remains unchanged mod 2π, as can be proven by doing a simple case analysis for all $j, k \in \{0, 1\}$.

Now there are two possible cases. In each case, we will prove that the implemented operation equals the H gate.

Case 1. $j + k \in \{0, 2\}$

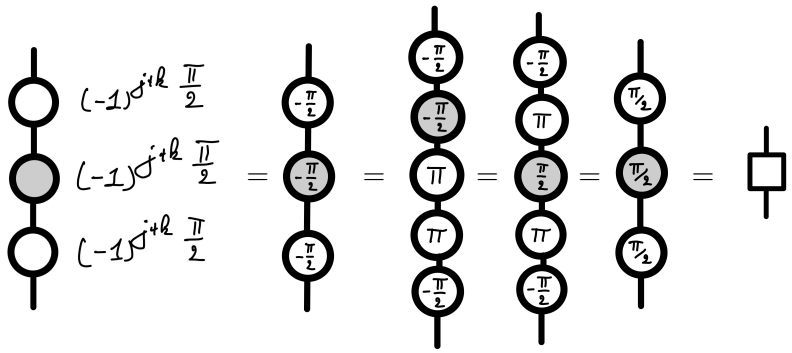
In this case, we are done, as



(15)

Case 2. $j + k = 1$

In this case, the right hand side of (14) has $-\frac{\pi}{2}$ in each spider. However, we can prove that this diagram is also equal to the H gate:

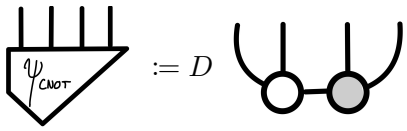


(16)

Where the second equality follows from phase spider fusion, the third from Lemma 1.1 and the fourth again from phase spider fusion. □

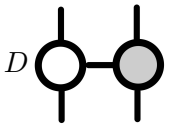
Question 1c

If we define ψ_{CNOT} as follows, then we can use it to deterministically implement a CNOT gate, as proven in Theorem 1.5.



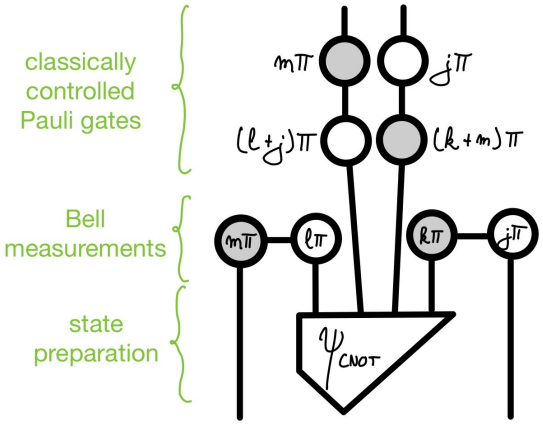
(17)

Recall the definition of a CNOT gate. This is equation (9.52) from Picturing Quantum Processes.



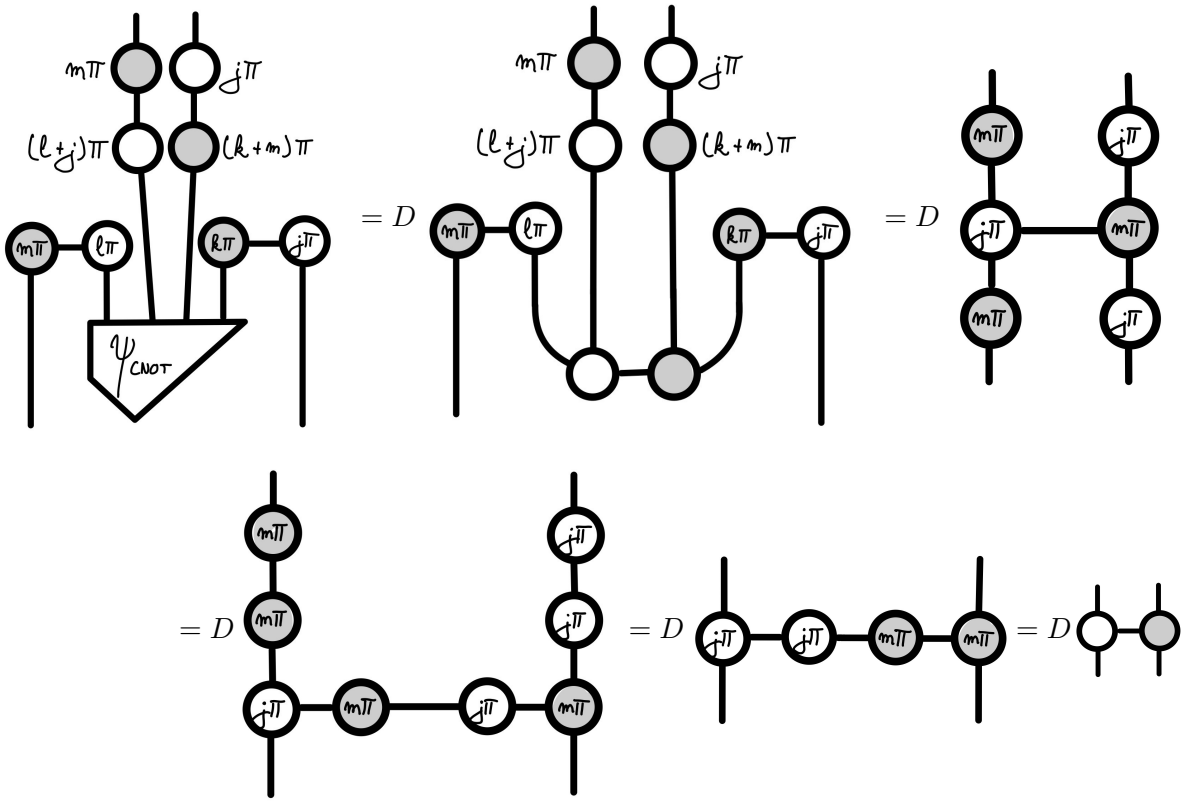
(18)

Lemma 1.5. *The following operation deterministically implements a CNOT gate:*



(19)

Proof.



(20)

The first equality holds by the definition of ψ_{CNOT} and the second by phase spider fusion. The third follows from Corollary 1.2.1. The fourth follows by fusing the upper phase spiders and applying Corollary 1.1.1 to the middle two phase spiders. The last equality holds again by phase spider fusion. □

Question 1d

In this question, we prove that the Bell model with the resource states defined so far is not approximately universal for quantum computation (Theorem 1.9). Afterwards, we add an extra resource state (26) to obtain the "Bell+" model and show that this extended model is approximately universal for quantum computation (Theorem 1.11).

Remark that the term "approximately universal for quantum computation" has never been defined rigorously, nor in Picturing Quantum Processes, nor in the project assignment. In this solution, we will take it to mean the following:

Definition 1.6. *A quantum computation model is approximately universal for quantum computation if it can approximate every causal quantum map to arbitrary precision.*

This definition is based on the definition of approximate universality for linear maps (in the Lecture Notes of Lecture 19). It makes sense, because causal quantum maps are the only ones that can be deterministically realised. Note that this definition encompasses the definition used in e.g. [Nielsen and Chuang, 2001] that only considers unitaries, because all unitary quantum maps are causal per Theorem 6.56 in Picturing Quantum Processes.

Lemma 1.7. *Every diagram that can be constructed with the Bell model with the resource states defined so far, is an (undoubled) Clifford diagram.*

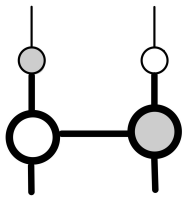
Proof. Every diagram that can be constructed with the Bell model can be constructed by composing the following components: preparing Z-basis states, preparing resource states defined in questions 1a-1c, performing 2-qubit Bell measurements, performing Z-basis measurements, performing Pauli Z and X gates.

Clearly the empty diagram is a Clifford diagram. Further, composing two Clifford diagrams yields a new Clifford diagram, because all phases stay integer multiples of $\frac{\pi}{2}$. Therefore, it is enough to prove that every allowed component is a Clifford diagram. Note that every doubled Clifford diagram is automatically also an undoubled Clifford diagram.

- Both Z-basis states are clearly Clifford diagrams, as they are equal to the following phase spiders:

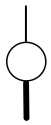
(21)

- All resource states are Clifford diagrams, because all of their phases are integer multiples of $\frac{\pi}{2}$. The same holds for Pauli Z and X gates.
- 2-qubit Bell measurements are Clifford diagrams. This can be easily seen when writing them down as a cq-map:



(22)

- In the same way, Z-basis measurements are Clifford diagrams:



(23)

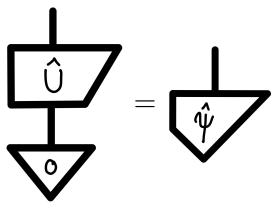
□

Lemma 1.8. *For all normalised n-qubit states ψ and ϕ, there exists a unitary U that maps ψ to ϕ.*

Proof. By Proposition 5.79 in Picturing Quantum Processes, we can extend the set $\{\psi\}$ to an ONB Ψ containing ψ, and analogously extend $\{\phi\}$ to an ONB Φ containing ϕ. We can choose the order of both ONBs so that the index of ψ in Ψ is the same as the index for ϕ in Φ. By Corollary 5.39 in Picturing Quantum Processes, there exists a unitary U that sends the i'th state of Ψ to the i'th state of Φ, thus sending ψ to ϕ. □

Theorem 1.9. *The Bell model with the resource states defined so far is not approximately universal for quantum computation.*

Proof. For any causal pure quantum state $\hat{\psi} = \text{double}(\psi)$, ψ is normalised and hence Lemma 1.8 guarantees the existence of a unitary U that maps $|0\rangle$ to ψ. This means that $\hat{U}$ is also unitary (by Proposition 6.20 in Picturing Quantum Processes) and



(24)

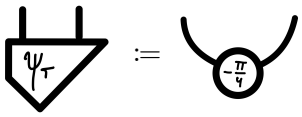
Suppose now that the Bell model with the resource states defined so far was approximately universal. Then we could approximate $\hat{\psi}$ to arbitrary precision using only operations allowed in the Bell model, by first approximating $\hat{U}$ to arbitrary precision and then plugging in the doubled Z-basis $|0\rangle$ state. This holds for any causal pure quantum state $\hat{\psi}$, in particular the ones in the following set:

$$\left\{ \frac{1}{D} \; \alpha \;\middle|\; \alpha \in [0, 2\pi) \right\} = \left\{ \frac{1}{D} \; -\alpha \;\; \alpha \;\middle|\; \alpha \in [0, 2\pi) \right\} \tag{25}$$

However, Lemma 1.7 shows that all diagrams that can be realised with the Bell model are Clifford diagrams. By considering that every Clifford state is equal to a graph state followed by Clifford unitaries (Proposition 9.122 in Picturing Quantum Processes), it follows that there are only a finite number of causal 2-qubit Clifford states. Hence it is impossible that the Bell model could approximate every quantum state in the uncountable set (25) to arbitrary precision. This is a contradiction, so the assumption that the Bell model was approximately universal must have been false.

□

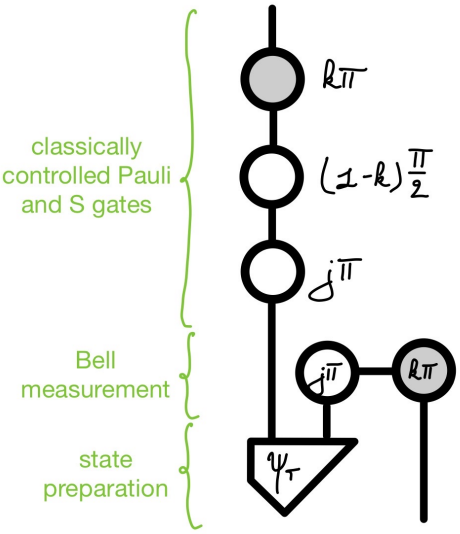
Now define an additional resource state ψ_T as follows:



(26)

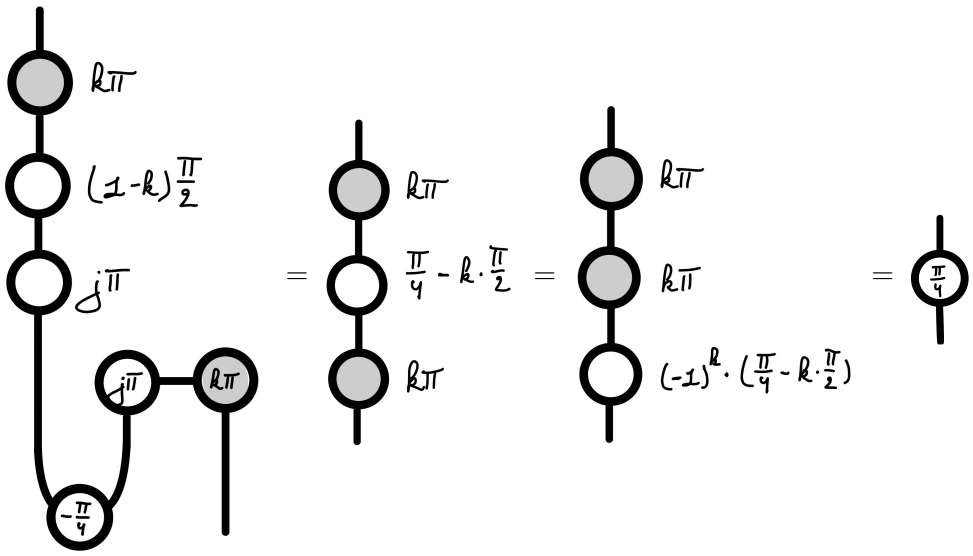
We can use ψ_T it to deterministically implement a T gate, as proven in Lemma 1.10.

Lemma 1.10. *The following operation deterministically implements a T gate:*



(27)

Proof.



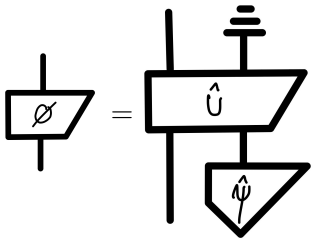
(28)

The first equality holds due to phase spider fusion, the second by Lemma 1.1 and the third by phase spider fusion and the fact that $(-1)^k \cdot \left(\frac{\pi}{4} - k\frac{\pi}{2}\right) \equiv \frac{\pi}{4} \pmod{2\pi}$ for all $k \in \{0, 1\}$. □

Call the Bell model enriched with this additional resource state ψ_T the "Bell+" model. We will now prove that the Bell+ model is approximately universal for quantum computation.

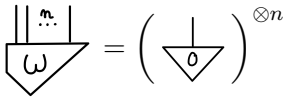
Theorem 1.11. *The Bell+ model is approximately universal for quantum computation.*

Proof. Consider an arbitrary causal quantum map ϕ. By Stinespring dilation (Corollary 6.63 in Picturing Quantum Processes), there exists a unitary $\hat{U}$ and a pure causal quantum state $\hat{\psi}$ such that



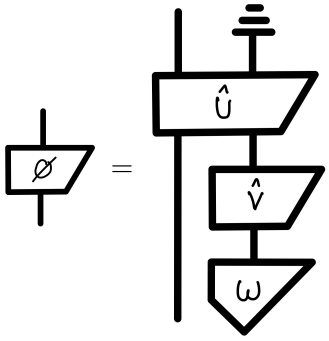
(29)

Moreover, by Lemma 1.8 there is a unitary V that maps ω to ψ where (supposing ψ is an n-qubit state) we define ω as



(30)

Note that it is possible to prepare $\hat{\omega} = \text{double}(\omega)$ in the Bell+ model. Substitution in (29) gives



(31)

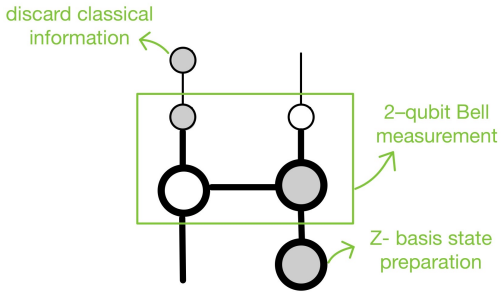
We have devised constructions in the Bell+ model to deterministically realise Hadamard gates (Theorem 1.4), CNOT gates (Theorem 1.5) and T gates (Lemma 1.10). [Nielsen and Chuang, 2001] prove that the combination of these three gates suffices to approximate any unitary on n qubits to arbitrary precision.

Therefore, the Bell+ model can approximate both $\hat{U}$ and $\hat{V}$ to arbitrary precision. Hence, by (31) it can also approximate ϕ to arbitrary precision. Thus the Bell+ model is approximately universal for quantum computation. □

Question 1e

Theorem 1.12. *The Bell- model, where we don't allow Z-basis measurements as basic operations, is just as powerful as before.*

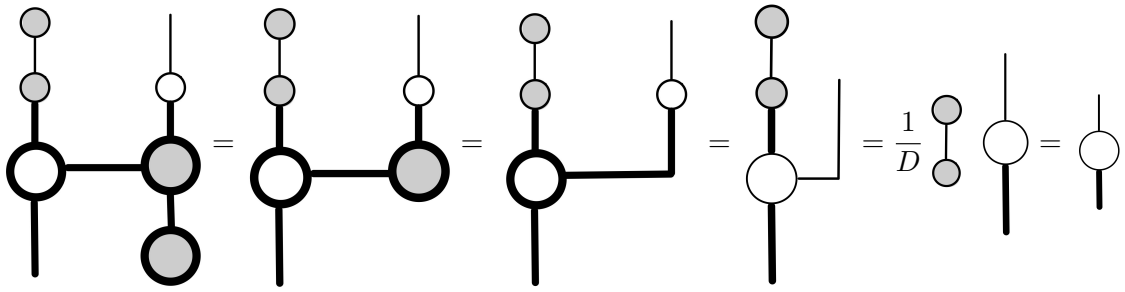
Proof. We can still perform a Z-basis measurements in the Bell- model as follows:



(32)

Here, we wrote the 2-qubit Bell measurement as a cq-map. Discarding classical information is possible by just ignoring the outcome of the left part of the measurement.

It is shown by the following series of equalities that (32) is indeed equal to a Z-basis measurement:



(33)

The first equality is a consequence of spider fusion. The second follows from noting that the two-legged (doubled) spider is just the (doubled) identity. The third follows from bastard spider fusion. The fourth is a consequence of complementarity between the X- and the Z-spiders. The last equality follows from applying spider fusion to the number on the left and noting that a zero-legged spider equals the number D.

We can still construct any diagram that we could construct before by replacing all Z-basis measurements by the construction given in (32). Therefore, the Bell- model is exactly as powerful as before. □

Question 2

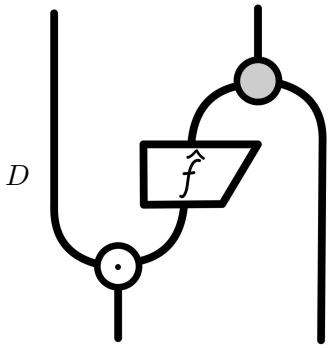
2.1 The problem

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 $f : \{0, 1, \ldots, 2^n\} \to \{0, 1\}$ evaluates to 1. The presented quantum algorithm allows to approximate the solution to this problem

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

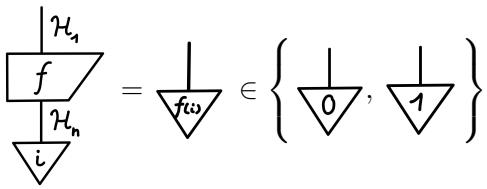
$$\{i \in \{0, 1, \ldots, 2^n\} \mid f(i) = 1\} \tag{34}$$

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



(35)

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



(36)

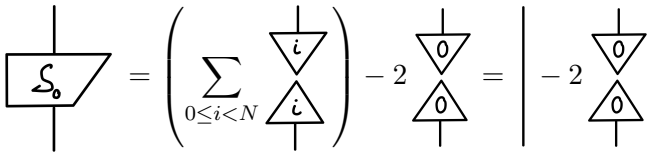
Note that this quantum oracle is unitary by Proposition 12.15 in Picturing Quantum Processes.

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 the number of qubits in the input register of the algorithm. For convencience, let $N \coloneqq 2^n$. Next, p is the number of qubits in an auxiliary register that will be used in the algorithm. For convenience, let $P \coloneqq 2^p$. 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.

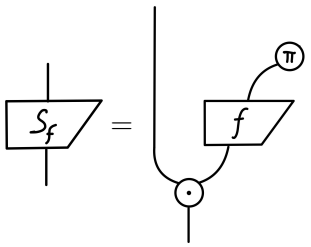
Component 2.2. Let $S_0 : \mathcal{H}_n \to \mathcal{H}_n$ be the unitary that negates the zero (standard) basis state, and maps every other basis state of $\mathcal{H}_n$ to itself.



(37)

Component 2.3. Let $S_f : \mathcal{H}_n \to \mathcal{H}_n$ 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.

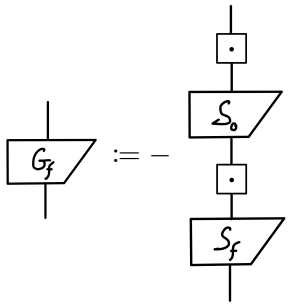
This component can be represented as follows, as proven in the discussion after equation (12.18) in Picturing Quantum Processes.



(38)

Its doubled version can be realised by plugging the doubled white π-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 $G_f : \mathcal{H} \to \mathcal{H}$ be the component defined by the following equation.

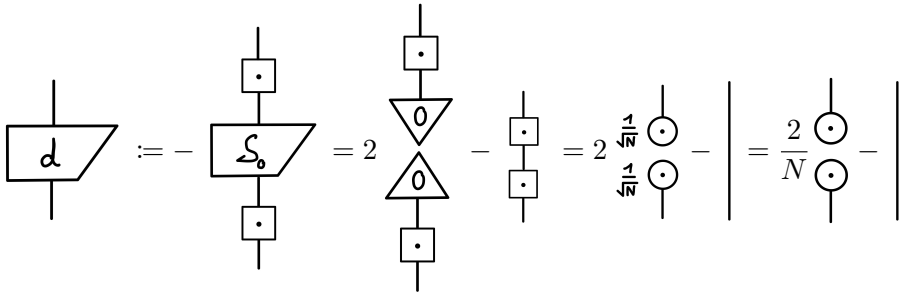


(39)

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

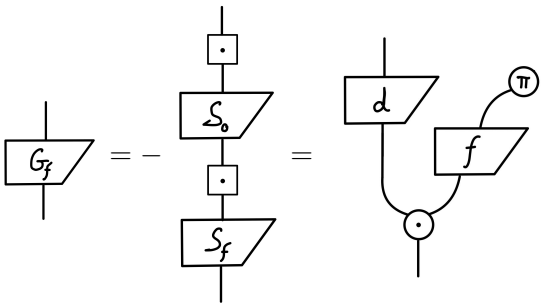
Lemma 2.5. *G_f is the Grover iteration from Picturing Quantum Processes, where the right input is fixed to be a white π-phase spider and the right output is deleted.*

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



(40)

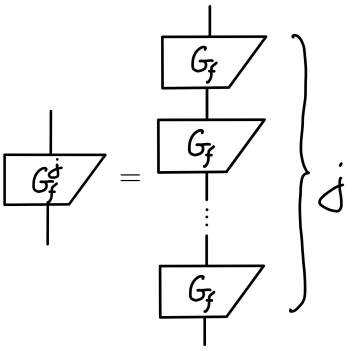
This is the same definition for d as the one used in section 12.2.3 of Picturing Quantum Processes. Putting (38-40) together yields



(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 π-phase spider and the right output is deleted (follows from Lemma 1.2). □

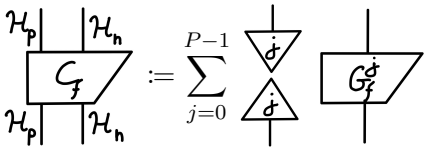
Component 2.6. Let $G_f^j : \mathcal{H}_n \to \mathcal{H}_n$ be the sequential composition of j times G_f, for every $j \in \mathbb{Z}^+$. For $j = 0$, define G_f^j to be the identity.



(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.

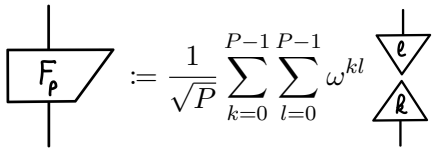
Component 2.7. Define $C_f : \mathcal{H}_p \otimes \mathcal{H}_n \to \mathcal{H}_p \otimes \mathcal{H}_n$ as follows:



(43)

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

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



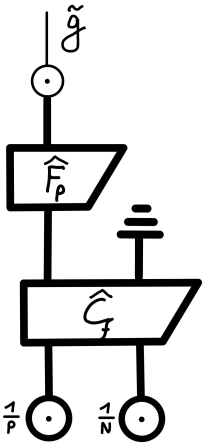
$$:= \frac{1}{\sqrt{P}} \sum_{k=0}^{P-1} \sum_{l=0}^{P-1} \omega^{kl} \tag{44}$$

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 $N \sin^2\left(\frac{\tilde{g}\pi}{P}\right)$.*



(45)

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*

$$|\tilde{N} - N_A| < \frac{2\pi}{P}\sqrt{N N_A} + \frac{\pi^2}{P^2} N \tag{46}$$

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

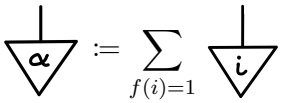
From this theorem follows that we can approximate N_A to arbitrary precision (by choosing P large enough) and with an arbitrarily large probability (by repeating the algorithm multiple times). For any constant c, [Brassard et al., 2002] exhibit a strategy to obtain an estimate $\tilde{N}$ such that

$$|\tilde{N} - N_A| < \frac{N_A}{c} \tag{47}$$

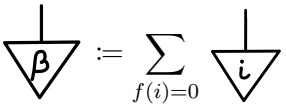
with probability at least $\frac{3}{4}$. They achieve this by running the algorithm multiple times, with an expected number of $\Theta\left((c + \log\log N)\sqrt{\frac{N}{N_A}}\right)$ function evaluations.

2.4 Correctness

Define the following two unnormalized n-qubit states:

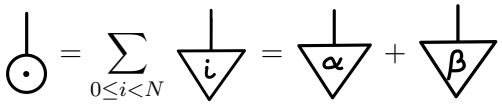


(48)



(49)

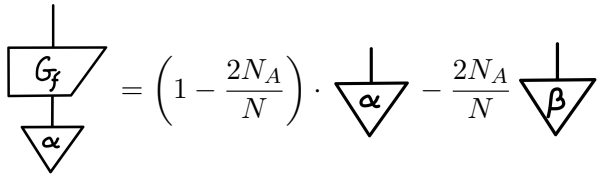
And note that



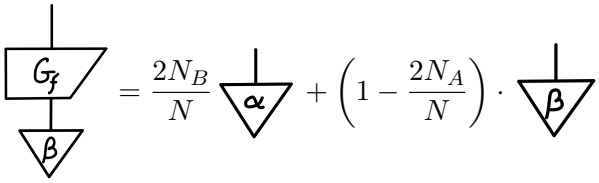
(50)

We will first investigate how G_f acts on α and β.

Lemma 2.11.

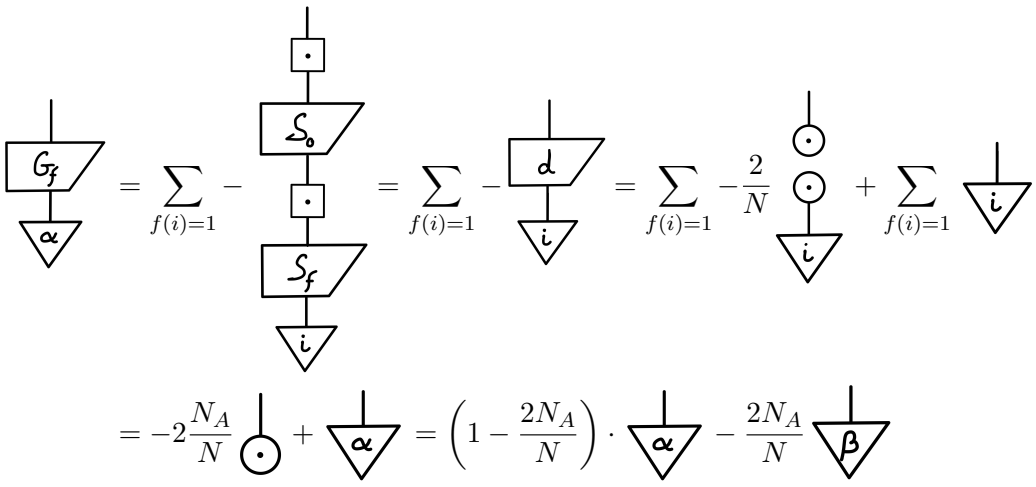


(51)



(52)

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

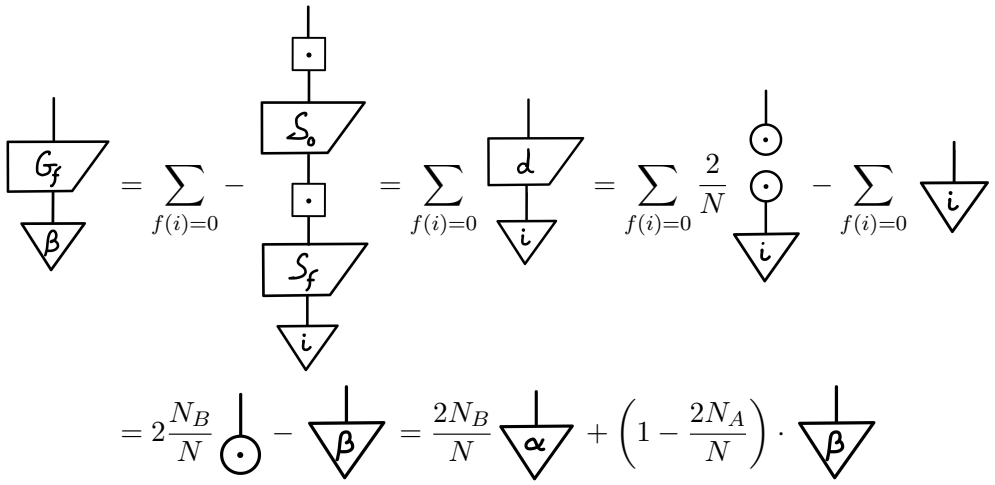


(53)

The first equality follows from expanding the definitions of G_f and α. 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:



(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 $f(i) = 0$. □

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 α and β, e.g. the dotted spider (50), the result will always be a new linear combination of α and β. At this stage, Grover's search algorithm would choose $j \in \mathbb{Z}$ to maximize the coefficient of α (relative to the coefficient of β) 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.

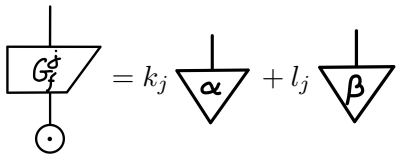
Define θ as the unique angle in $[0, \frac{\pi}{2}]$ such that

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

and (by consequence)

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

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



(57)

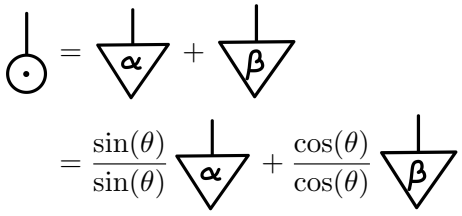
where

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

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

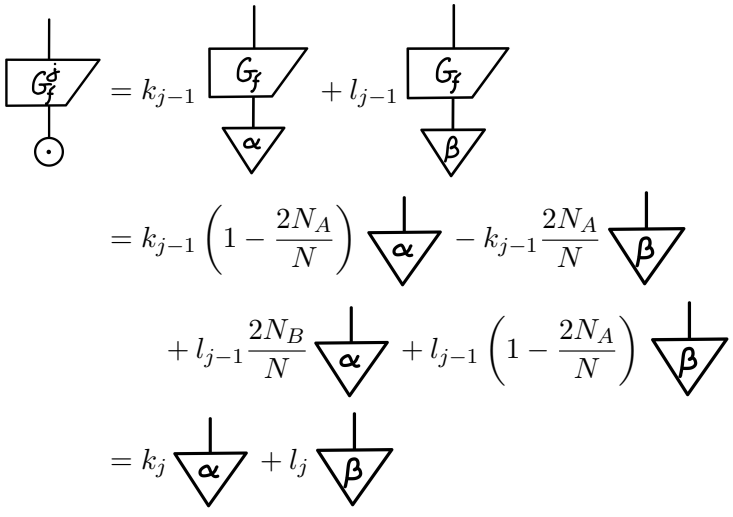
Proof. We will prove this by induction on j.

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



$$= \frac{\sin(\theta)}{\sin(\theta)} \quad + \quad \frac{\cos(\theta)}{\cos(\theta)} \tag{60}$$

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



$$= k_{j-1}\left(1 - \frac{2N_A}{N}\right) - k_{j-1}\frac{2N_A}{N} \tag{61}$$

$$+ l_{j-1}\frac{2N_B}{N} + l_{j-1}\left(1 - \frac{2N_A}{N}\right)$$

$$= k_j \quad + l_j$$

Where

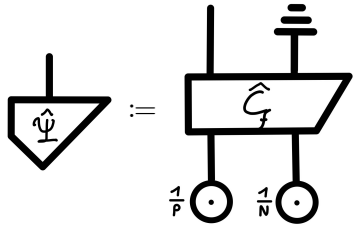
$$\begin{aligned} k_j &= k_{j-1}\left(1 - \frac{2N_A}{N}\right) + l_{j-1}\frac{2N_B}{N} \\ &= \frac{1}{\sin(\theta)}\sin\left((2j-1)\theta\right)\cdot(1-2\sin^2(\theta)) + \cos((2j-1)\theta)\cdot\frac{2\cos^2(\theta)}{\cos(\theta)} \\ &= \frac{1}{\sin(\theta)}\left(\sin\left((2j-1)\theta\right)\cos(2\theta)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

And

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

□

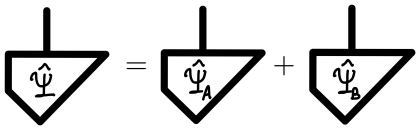
The algorithm applies $\hat{F_P}$ on the following quantum state $\hat{\Psi}$:



(64)

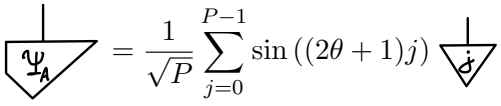
The expansion of $\hat{\Psi}$ contains a double sum. Luckily, we can decompose $\hat{\Psi}$ as a mixture of two pure quantum states $\hat{\Psi}_A$ and $\hat{\Psi}_B$. Afterwards, we continue our analysis by considering the action of F_P on both undoubled states.

Lemma 2.13.



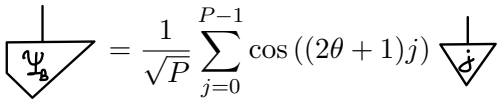
(65)

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



$$= \frac{1}{\sqrt{P}} \sum_{j=0}^{P-1} \sin\left((2\theta+1)j\right)$$

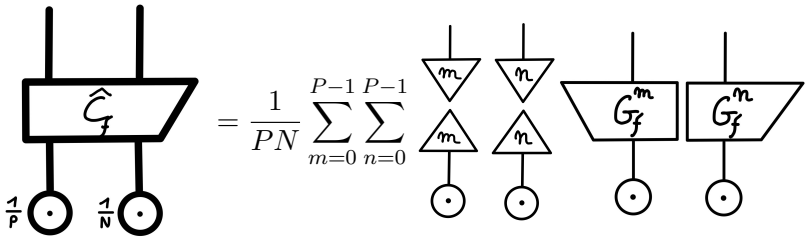
(66)



$$= \frac{1}{\sqrt{P}} \sum_{j=0}^{P-1} \cos\left((2\theta+1)j\right)$$

(67)

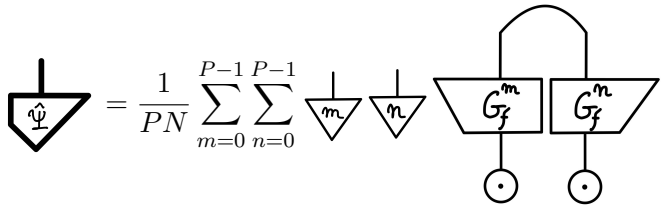
Proof. By expanding the definition of C_f (43) and doubling, we obtain



$$= \frac{1}{PN} \sum_{m=0}^{P-1} \sum_{n=0}^{P-1}$$

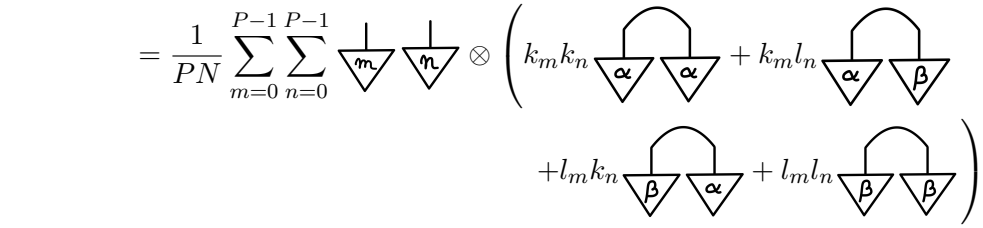
(68)

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

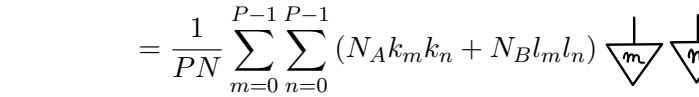


$$= \frac{1}{PN} \sum_{m=0}^{P-1} \sum_{n=0}^{P-1}$$

$$= \frac{1}{PN} \sum_{m=0}^{P-1} \sum_{n=0}^{P-1}$$

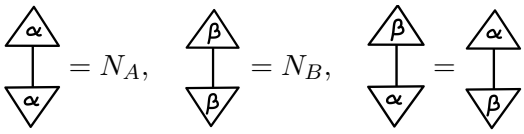


$$= \frac{1}{PN} \sum_{m=0}^{P-1} \sum_{n=0}^{P-1} (N_A k_m k_n + N_B l_m l_n)$$



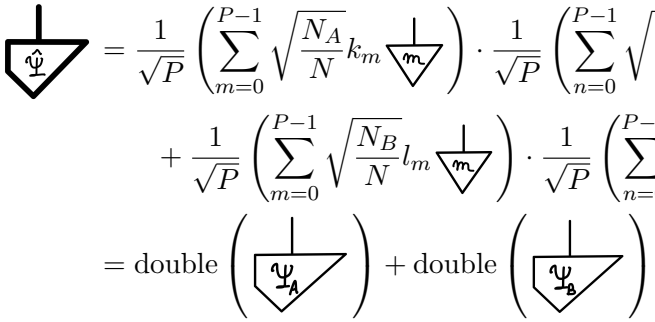
(69)

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



$$= N_A, \quad = N_B, \quad = = 0 \tag{70}$$

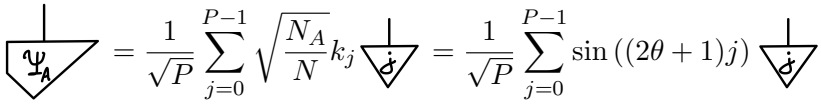
Now, we can split $\hat{\Psi}$ into two pure states by further manipulation of (69).



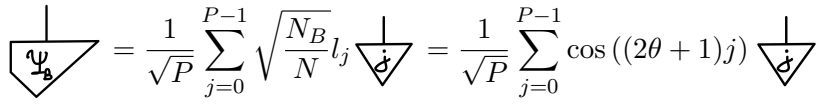
$$= \text{double}\left(\right) + \text{double}\left(\right)$$

(71)

Where Ψ_A and Ψ_B are defined as follows:



$$= \frac{1}{\sqrt{P}} \sum_{j=0}^{P-1} \sqrt{\frac{N_A}{N}} k_j = \frac{1}{\sqrt{P}} \sum_{j=0}^{P-1} \sin\left((2\theta+1)j\right) \tag{72}$$

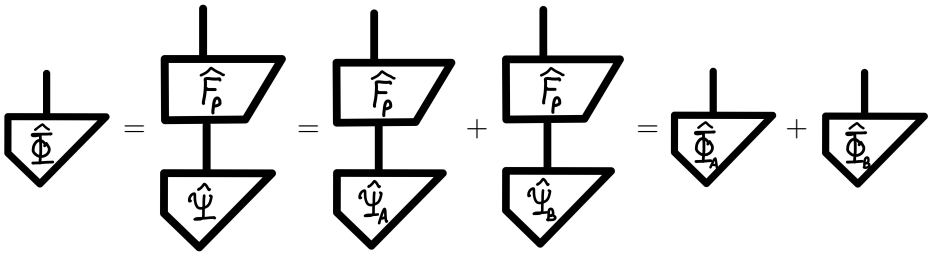


$$= \frac{1}{\sqrt{P}} \sum_{j=0}^{P-1} \sqrt{\frac{N_B}{N}} l_j = \frac{1}{\sqrt{P}} \sum_{j=0}^{P-1} \cos\left((2\theta+1)j\right) \tag{73}$$

□

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 Ψ_A by Φ_A and analogously for Φ_B. Note that $\hat{\Phi}_A$ and $\hat{\Phi}_B$

are pure quantum states such that



(74)

Define

$$g \coloneqq P\frac{\theta}{\pi} \tag{75}$$

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 Ψ_A or Ψ_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*

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

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

$$|\Phi_A\rangle = a|g^-\rangle + b|g^+\rangle + c|P - g^-\rangle + d|P - f^+\rangle + |R_A\rangle \tag{77}$$

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

$$|\Phi_A\rangle = a|0\rangle + b|1\rangle + c|P-1\rangle + |R_A\rangle \tag{78}$$

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

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

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

$$\langle R_A \,|\, R_A\rangle < \frac{2}{5}\langle \Phi_A \,|\, \Phi_A\rangle \tag{80}$$

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.

$$\langle R_B \,|\, R_B\rangle < \frac{2}{5}\langle \Phi_B \,|\, \Phi_B\rangle \tag{81}$$

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

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*

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

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

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

We can also upper bound the sum of both sines:

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

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

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

□

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.