University of Jyväskylä - Course TIEJ6003

Introduction to Quantum Computing

Precept-04

Prof. Ofer Shir
oshir@alumni.Princeton.EDU

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

Summer 2024
Jyväskylä, Finland

ex3

...processing solutions to ex3...

...in-class practice...

computing the order

Show that the order of $x = 5$ modulo $N = 21$ is 6.

computing the order

Show that the order of $x = 5$ modulo $N = 21$ is 6.

Solution:

$$\begin{aligned} 5^2 &= 4 \mod 21 \\ 5^3 &= 20 \mod 21 \\ 5^4 &= 16 \mod 21 \\ 5^5 &= 19 \mod 21 \\ &\boxed{5^6 = \mathbf{1} \mod 21} \end{aligned}$$

QFT is unitary

The QFT on a state $|x\rangle$ for $x \in \{0, 1, \ldots, N-1\}$ is defined as:

$$\text{QFT}\,|x\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i \frac{xk}{N}}\,|k\rangle$$

Show that it is a unitary operator.

QFT is unitary

The QFT on a state $|x\rangle$ for $x \in \{0, 1, \ldots, N-1\}$ is defined as:

$$\mathrm{QFT}\,|x\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i \frac{xk}{N}}\,|k\rangle$$

Show that it is a unitary operator.
Proof: The matrix form of QFT is given by:

$$F_{jk} = \frac{1}{\sqrt{N}} e^{2\pi i \frac{jk}{N}}$$

The conjugate transpose $F^\dagger$ of F is:

$$(F^\dagger)_{kj} = \overline{F_{jk}} = \frac{1}{\sqrt{N}} e^{-2\pi i \frac{jk}{N}}$$

We need to verify that $F^\dagger F = I$.

QFT is unitary: proof (i)

Let's compute the element in the (j, m)-th position of the product $F^\dagger F$:

$$(F^\dagger F)_{jm} = \sum_{k=0}^{N-1} (F^\dagger)_{jk} F_{km}$$

Substituting the elements:

$$\begin{aligned}
(F^\dagger F)_{jm} &= \sum_{k=0}^{N-1} \left(\frac{1}{\sqrt{N}} e^{-2\pi i \frac{jk}{N}} \right) \left(\frac{1}{\sqrt{N}} e^{2\pi i \frac{km}{N}} \right) \\
&= \frac{1}{N} \sum_{k=0}^{N-1} e^{-2\pi i \frac{jk}{N}} e^{2\pi i \frac{km}{N}} \\
&= \frac{1}{N} \sum_{k=0}^{N-1} e^{2\pi i \frac{k(m-j)}{N}}
\end{aligned}$$

QFT is unitary: proof (ii)

When $m = j$:

$$(F^\dagger F)_{jm} = \frac{1}{N} \sum_{k=0}^{N-1} e^{2\pi i \frac{k(m-j)}{N}} = \frac{1}{N} \sum_{k=0}^{N-1} e^{2\pi i \cdot 0} = \frac{1}{N} \cdot N = 1$$

When $m \neq j$, the geometric series sums to zero:

$$\sum_{k=0}^{N-1} e^{2\pi i \frac{k(m-j)}{N}} = \frac{1 - e^{2\pi i (m-j)}}{1 - e^{2\pi i \frac{(m-j)}{N}}} = 0$$

Altogether, this completes our proof, since

$$(F^\dagger F)_{jm} = \delta_{jm}$$

and therefore $F^\dagger F = I$, as claimed.

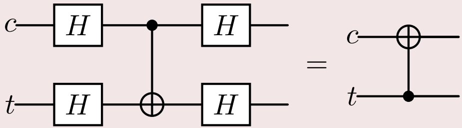
reviewing the take-out exercises

take-out problem-set

We now review the exercises that appear in the fourth problem-set ("take-out"). We shall go over the solution in tomorrow's Precept.

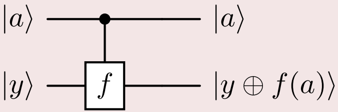
Exercise 4.1: circuits equivalence

Show this equivalence:

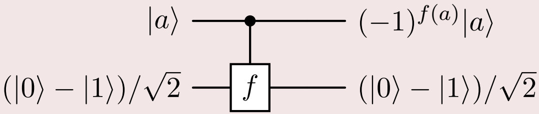


Exercise 4.2: controlled-f gate

Verify that given the following controlled-f gate,



the following “trick” is valid:



Exercise 4.3: identity

Let $H^{\otimes n}$ denote Hadamard gates applied individually to n qubits. Let $P := 2\left|0^{\otimes n}\right\rangle\left\langle 0^{\otimes n}\right| - I^{\otimes n}$, where $|0^{\otimes n}\rangle\langle 0^{\otimes n}|$ is the projector onto the n-qubit zero state.

Prove that

$$H^{\otimes n} P H^{\otimes n} = 2\left|\psi_u\right\rangle\left\langle\psi_u\right| - I$$

where $|\psi_u\rangle$ is the uniform superposition over the computational basis states,

$$|\psi_u\rangle := \frac{1}{2^{n/2}} \sum_{j}^{2^n-1} |j\rangle$$