Lecture 12

ELEMENTARY QUANTUM CIRCUITS AND PROGRAMS. PART 2.

of the course "Fundamentals of Quantum Computing"

Stoyan Mishev

INSTITUTE *for* ADVANCED PHYSICAL STUDIES

NEW BULGARIAN UNIVERSITY

June 10, 2022

План

On constructing quantum circuits

Quantum Subtractor - $a - b$

Quantum Adder Modulo N - $(a + b) \bmod N$

Homework

On constructing quantum circuits

- Preparation of the input register

- Preparation of the input register
- Implementation of classical functions f by means of quantum circuits U_f on a suitable quantum register

Steps in QC

- Preparation of the input register
- Implementation of classical functions f by means of quantum circuits U_f on a suitable quantum register
- Transformation of the quantum register by means of suitable quantum gates or circuits

- Preparation of the input register
- Implementation of classical functions f by means of quantum circuits U_f on a suitable quantum register
- Transformation of the quantum register by means of suitable quantum gates or circuits
- Reading (observing) the result in the output register

Factor-wise binary addition $\boxplus^2$

$$\begin{aligned} \boxplus : \P\mathbb{H}^{\otimes m} \otimes \P\mathbb{H}^{\otimes m} &\longrightarrow \P\mathbb{H}^{\otimes m} \\ |a\rangle \otimes |b\rangle &\longmapsto |a\rangle \boxplus |b\rangle := \bigotimes_{j=m-1}^{0} |a_j \overset{2}{\oplus} b_j\rangle \end{aligned}$$

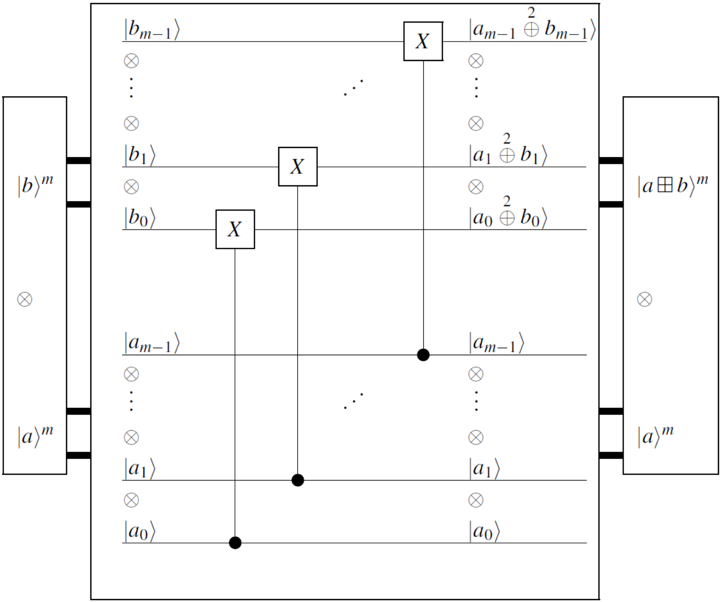
Factor-wise binary addition $\boxplus^2$

$$\begin{aligned} \boxplus : \P\mathbb{H}^{\otimes m} \otimes \P\mathbb{H}^{\otimes m} &\longrightarrow \P\mathbb{H}^{\otimes m} \\ |a\rangle \otimes |b\rangle &\longmapsto |a\rangle \boxplus |b\rangle := \bigotimes_{j=m-1}^{0} |a_j \overset{2}{\oplus} b_j\rangle \end{aligned}$$

A circuit described by the operator U_f implements the function f on $H^A \otimes H^B$ if

$$\begin{aligned} U_f : \mathbb{H}^A \otimes \mathbb{H}^B &\longrightarrow \mathbb{H}^A \otimes \mathbb{H}^B \\ |x\rangle \otimes |y\rangle &\longmapsto |x\rangle \otimes |y \boxplus f(x)\rangle \end{aligned}$$

Quantum circuit for $U_f \equiv U_{\boxplus}$



Hadamard gates to prepare input registers

$$|\Psi_0\rangle = \frac{1}{2^{\frac{n}{2}}} \sum_{x=0}^{2^n-1} |x\rangle^n \in \mathbb{H}^{I/O}$$

Hadamard gates to prepare input registers

$$|\Psi_0\rangle = \frac{1}{2^{\frac{n}{2}}} \sum_{x=0}^{2^n-1} |x\rangle^n \in \mathbb{H}^{I/O}$$

Hadamard gate : $H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$

Hadamard gates to prepare input registers

$$|\Psi_0\rangle = \frac{1}{2^{\frac{n}{2}}} \sum_{x=0}^{2^n-1} |x\rangle^n \;\in \mathbb{H}^{I/O}$$

$$\text{Hadamard gate}: \quad H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$H^{\otimes n}|0\rangle^n = H^{\otimes n}\Big(|0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle\Big) = \bigotimes_{j=n-1}^{0} H|0\rangle = \bigotimes_{j=n-1}^{0} \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$= \frac{1}{2^{\frac{n}{2}}} (|0\rangle + |1\rangle) \otimes \cdots \otimes (|0\rangle + |1\rangle)$$

$$= \frac{1}{2^{\frac{n}{2}}} \Big(\underbrace{|0\ldots 0\rangle}_{=|0\rangle^n} + \underbrace{|0\ldots 1\rangle}_{=|1\rangle^n} + \cdots + \underbrace{|1\ldots 1\rangle}_{=|2^n-1\rangle^n} \Big)$$

$$= \frac{1}{2^{\frac{n}{2}}} \sum_{x=0}^{2^n-1} |x\rangle^n ,$$

General U_f implementation

A circuit described by the operator U_f implements the function f on $H^A \otimes H^B$ if

$$\begin{aligned} U_f : \mathbb{H}^A \otimes \mathbb{H}^B &\longrightarrow \mathbb{H}^A \otimes \mathbb{H}^B \\ |x\rangle \otimes |y\rangle &\longmapsto |x\rangle \otimes |y \boxplus f(x)\rangle \end{aligned}$$

How can we do that?

General U_f implementation

A circuit described by the operator U_f implements the function f on $H^A \otimes H^B$ if

$$\begin{aligned} U_f : \mathbb{H}^A \otimes \mathbb{H}^B &\longrightarrow \mathbb{H}^A \otimes \mathbb{H}^B \\ |x\rangle \otimes |y\rangle &\longmapsto |x\rangle \otimes |y \boxplus f(x)\rangle \end{aligned}$$

How can we do that?

1. helper gates A and B which implement f in some way non-unitarily

General U_f implementation

A circuit described by the operator U_f implements the function f on $H^A \otimes H^B$ if

$$\begin{aligned} U_f : \mathbb{H}^A \otimes \mathbb{H}^B &\longrightarrow \mathbb{H}^A \otimes \mathbb{H}^B \\ |x\rangle \otimes |y\rangle &\longmapsto |x\rangle \otimes |y \boxplus f(x)\rangle \end{aligned}$$

How can we do that?

1. helper gates A and B which implement f in some way non-unitarily

$$\begin{aligned} A_f\left(|x\rangle \otimes |\omega_i\rangle\right) &= |\psi(x)\rangle \otimes |f(x)\rangle \\ B_f\left(|\psi(x)\rangle \otimes |f(x)\rangle\right) &= |x\rangle \otimes |\omega_f\rangle \end{aligned}$$

General U_f implementation

A circuit described by the operator U_f implements the function f on $H^A \otimes H^B$ if

$$\begin{aligned} U_f : \mathbb{H}^A \otimes \mathbb{H}^B &\longrightarrow \mathbb{H}^A \otimes \mathbb{H}^B \\ |x\rangle \otimes |y\rangle &\longmapsto |x\rangle \otimes |y \boxplus f(x)\rangle \end{aligned}$$

How can we do that?

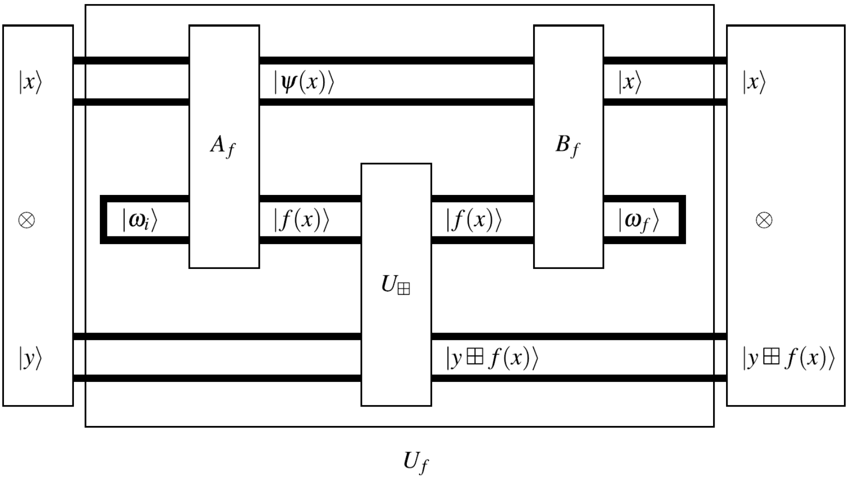
1. helper gates A and B which implement f in some way non-unitarily

$$\begin{aligned} A_f\left(|x\rangle \otimes |\omega_i\rangle\right) &= |\psi(x)\rangle \otimes |f(x)\rangle \\ B_f\left(|\psi(x)\rangle \otimes |f(x)\rangle\right) &= |x\rangle \otimes |\omega_f\rangle \end{aligned}$$

2. auxiliary qubits and circuit which uses A and B

$$\hat{U}_f := \left(\mathbf{1}^A \otimes S^{B,B}\right)\left(B_f \otimes \mathbf{1}^B\right)\left(\mathbf{1}^A \otimes U_{\boxplus}\right)\left(A_f \otimes \mathbf{1}^B\right)\left(\mathbf{1}^A \otimes S^{B,B}\right)$$

where $S^{B,B} : |b_1\rangle \otimes |b_2\rangle \to |b_2\rangle \otimes |b_1\rangle$ is a swap operator.


$|x\rangle$
$\otimes$
$|y\rangle$
A_f
$|\psi(x)\rangle$
$|\omega_i\rangle$
$|f(x)\rangle$
$U_\boxplus$
$|f(x)\rangle$
$|y \boxplus f(x)\rangle$
B_f
$|x\rangle$
$|\omega_f\rangle$
$|x\rangle$
$\otimes$
$|y \boxplus f(x)\rangle$
U_f

$$\hat{U}_f \left(|x\rangle \otimes |y\rangle \otimes |\omega_i\rangle \right)$$

$$\left(\mathbf{1}^A \otimes S^{B,B}\right)\left(B_f \otimes \mathbf{1}^B\right)\left(\mathbf{1}^A \otimes U_{\boxplus}\right)\left(A_f \otimes \mathbf{1}^B\right)\left(|x\rangle \otimes |\omega_i\rangle \otimes |y\rangle\right)$$

$$\left(\mathbf{1}^A \otimes S^{B,B}\right)\left(B_f \otimes \mathbf{1}^B\right)\left(\mathbf{1}^A \otimes U_{\boxplus}\right)\left(|\psi(x)\rangle \otimes |f(x)\rangle \otimes |y\rangle\right)$$

$$\left(\mathbf{1}^A \otimes S^{B,B}\right)\left(B_f \otimes \mathbf{1}^B\right)\left(|\psi(x)\rangle \otimes |f(x)\rangle \otimes |y \boxplus f(x)\rangle\right)$$

$$\left(\mathbf{1}^A \otimes S^{B,B}\right)\left(|x\rangle \otimes |\omega_f\rangle \otimes |y \boxplus f(x)\rangle\right)$$

$$|x\rangle \otimes |y \boxplus f(x)\rangle \otimes |\omega_f\rangle .$$

Let us apply a function to the state $H^n|0\rangle$, i.e. to act on a state $H^n|0\rangle$ with H_f:

$$U_f|\Psi_0\rangle = U_f\left((H^n|0\rangle^n)\otimes|0\rangle^m\right) = \frac{1}{2^{\frac{n}{2}}}\sum_{x=0}^{2^n-1} U_f\left(|x\rangle^n\otimes|0\rangle^m\right)$$

$$= \frac{1}{2^{\frac{n}{2}}}\sum_{x=0}^{2^n-1} \underbrace{|x\rangle\otimes|f(x)\rangle}_{\in\mathbb{H}^A\otimes\mathbb{H}^B}$$

Let us apply a function to the state $H^n|0\rangle$, i.e. to act on a state $H^n|0\rangle$ with H_f:

$$U_f|\Psi_0\rangle = U_f\left((H^n|0\rangle^n)\otimes|0\rangle^m\right) = \frac{1}{2^{\frac{n}{2}}}\sum_{x=0}^{2^n-1} U_f\left(|x\rangle^n\otimes|0\rangle^m\right)$$

$$= \frac{1}{2^{\frac{n}{2}}}\sum_{x=0}^{2^n-1} \underbrace{|x\rangle\otimes|f(x)\rangle}_{\in\mathbb{H}^A\otimes\mathbb{H}^B}$$

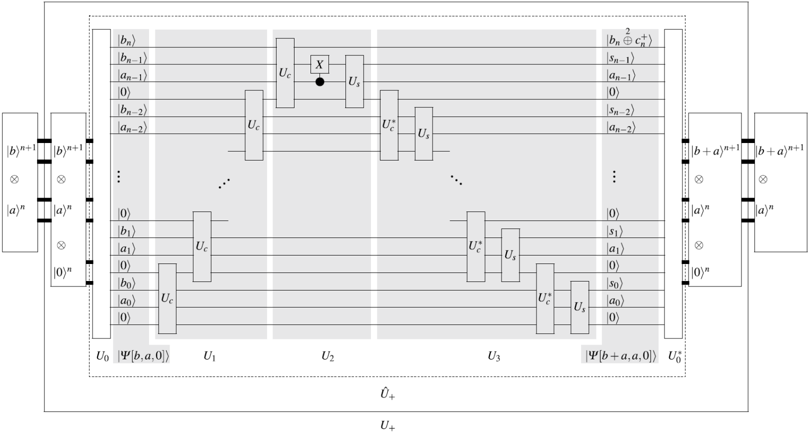
One may take the view on this result as applying a single gate produces $2^n - 1$ values of the function at once - parallelism.

The qubits in the register can be read *independently* using the operators $\Sigma_z^j = 1^{\otimes n-1-j} \otimes \sigma_z \otimes 1^{\otimes j}$ which commute : $[\Sigma_z^j, \Sigma_z^i] = 0$ if $i \neq j$.

The qubits in the register can be read *independently* using the operators $\Sigma_z^j = 1^{\otimes n-1-j} \otimes \sigma_z \otimes 1^{\otimes j}$ which commute :
$[\Sigma_z^j, \Sigma_z^i] = 0$ if $i \neq j$.
The obtained values $(s_{n-1}, \ldots, s_0) \in \{\pm 1\}^n$ are stored in classical (binary) registers.

Quantum Subtractor - $a - b$

if U_+ implements binary add then $U_+^{-1} \equiv U_-$ implements binary subtract !



Corollary 5.39 *There exists a circuit U_- on $\mathbb{H}^{I/O} = \mathbb{H}^B \otimes \mathbb{H}^A$, which is implemented with the help of the auxiliary register $\mathbb{H}^W$ by $\hat{U}_+^* = \hat{U}_+^{-1}$, that is, for arbitrary $|\Phi\rangle \in \mathbb{H}^{I/O}$ one has*

$$\hat{U}_+^*\big(|\Phi\rangle \otimes |0\rangle^n\big) = \big(U_-|\Phi\rangle\big) \otimes |0\rangle^n, \tag{5.107}$$

where also $U_- = U_+^* = U_+^{-1}$ holds. Furthermore, for $a,b \in \mathbb{N}_0$ with $a,b < 2^n$ we have that

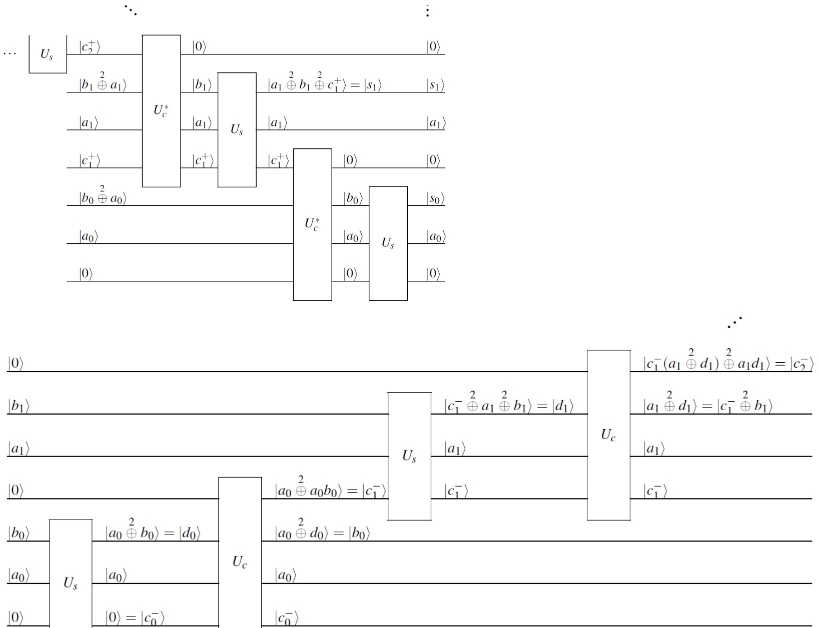
$$U_1^* U_2^* U_3^* |\Psi[b,a,0]\rangle = |\Psi[c_n^- 2^{n+1} + b - a, a, 0]\rangle \tag{5.108}$$

$$b - a = \sum_{j=0}^{n-1} \hat{d}_j 2^j + \hat{c}_n^- 2^n$$

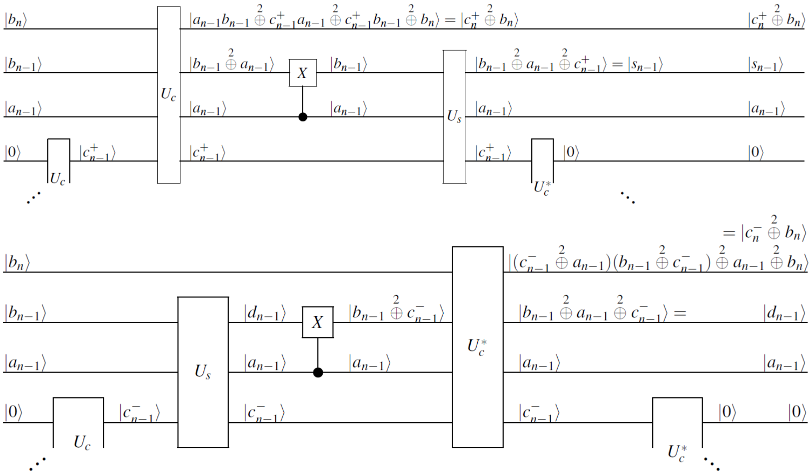
$$c_j^- := \big(1 \overset{2}{\oplus} b_{j-1}\big)\big(a_{j-1} \overset{2}{\oplus} c_{j-1}^-\big) \overset{2}{\oplus} a_{j-1} c_{j-1}^- \quad \textit{for } j \in \{1,\ldots,n\}$$

$$d_j := a_j \overset{2}{\oplus} b_j \overset{2}{\oplus} c_j^- \quad \textit{for } j \in \{0,\ldots,n-1\}.$$

U_3 and U_3^*

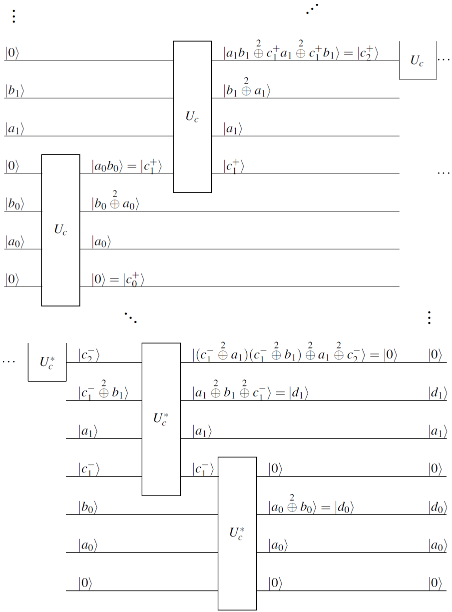

U_s
$|c_2^+\rangle$
$|0\rangle$
$|b_1 \overset{2}{\oplus} a_1\rangle$
$|b_1\rangle$
$|a_1 \overset{2}{\oplus} b_1 \overset{2}{\oplus} c_1^+\rangle = |s_1\rangle$
$|s_1\rangle$
U_c^*
$|a_1\rangle$
U_s
$|c_1^+\rangle$
$|b_0 \overset{2}{\oplus} a_0\rangle$
$|b_0\rangle$
$|s_0\rangle$
$|a_0\rangle$
$|0\rangle$
$|b_1\rangle$
$|c_1^-\rangle$
$|c_1^- \overset{2}{\oplus} a_1 \overset{2}{\oplus} b_1\rangle = |d_1\rangle$
$|c_1^-(a_1 \overset{2}{\oplus} d_1) \overset{2}{\oplus} a_1 d_1\rangle = |c_2^-\rangle$
$|a_1 \overset{2}{\oplus} d_1\rangle = |c_1^- \overset{2}{\oplus} b_1\rangle$
U_c
$|a_0 \overset{2}{\oplus} a_0 b_0\rangle = |c_1^-\rangle$
$|a_0 \overset{2}{\oplus} b_0\rangle = |d_0\rangle$
$|a_0 \overset{2}{\oplus} d_0\rangle = |b_0\rangle$
$|0\rangle = |c_0^-\rangle$
$|c_0^-\rangle$

U_2 and U_2^*



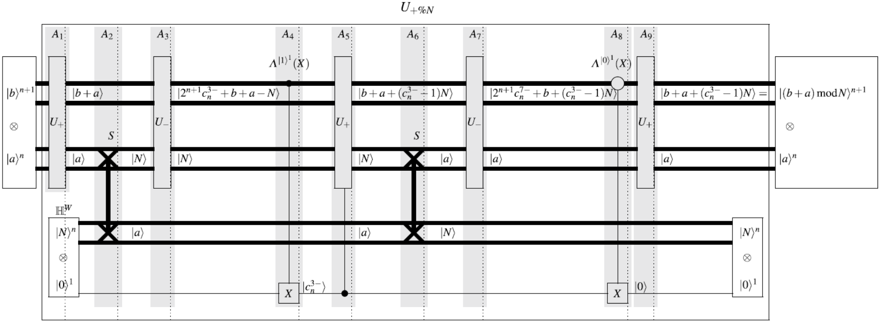
$|b_n\rangle$
$|b_{n-1}\rangle$
$|a_{n-1}\rangle$
$|0\rangle$
U_c
$|c_{n-1}^+\rangle$
$|a_{n-1}b_{n-1} \overset{2}{\oplus} c_{n-1}^+a_{n-1} \overset{2}{\oplus} c_{n-1}^+b_{n-1} \overset{2}{\oplus} b_n\rangle = |c_n^+ \overset{2}{\oplus} b_n\rangle$
$|b_{n-1} \overset{2}{\oplus} a_{n-1}\rangle$
X
$|b_{n-1}\rangle$
$|a_{n-1}\rangle$
U_s
$|b_{n-1} \overset{2}{\oplus} a_{n-1} \overset{2}{\oplus} c_{n-1}^+\rangle = |s_{n-1}\rangle$
U_c^*
$|0\rangle$
$|c_n^+ \overset{2}{\oplus} b_n\rangle$
$|s_{n-1}\rangle$
$|d_{n-1}\rangle$
$|c_{n-1}^-\rangle$
$|b_{n-1} \overset{2}{\oplus} c_{n-1}^-\rangle$
$|(c_{n-1}^- \overset{2}{\oplus} a_{n-1})(b_{n-1} \overset{2}{\oplus} c_{n-1}^-) \overset{2}{\oplus} a_{n-1} \overset{2}{\oplus} b_n\rangle$
$= |c_n^- \overset{2}{\oplus} b_n\rangle$
$|b_{n-1} \overset{2}{\oplus} a_{n-1} \overset{2}{\oplus} c_{n-1}^-\rangle =$

U_1 and U_1^*



$|0\rangle$
$|b_1\rangle$
$|a_1\rangle$
$|0\rangle$
$|b_0\rangle$
$|a_0\rangle$
$|0\rangle$
U_c
$|a_0 b_0\rangle = |c_1^+\rangle$
$|b_0 \overset{2}{\oplus} a_0\rangle$
$|a_0\rangle$
$|0\rangle = |c_0^+\rangle$
U_c
$|a_1 b_1 \overset{2}{\oplus} c_1^+ a_1 \overset{2}{\oplus} c_1^+ b_1\rangle = |c_2^+\rangle$
$|b_1 \overset{2}{\oplus} a_1\rangle$
$|a_1\rangle$
$|c_1^+\rangle$
U_c
U_c^*
$|c_2^-\rangle$
$|c_1^- \overset{2}{\oplus} b_1\rangle$
$|a_1\rangle$
$|c_1^-\rangle$
$|b_0\rangle$
$|a_0\rangle$
$|0\rangle$
U_c^*
$|(c_1^- \overset{2}{\oplus} a_1)(c_1^- \overset{2}{\oplus} b_1) \overset{2}{\oplus} a_1 \overset{2}{\oplus} c_2^-\rangle = |0\rangle$
$|a_1 \overset{2}{\oplus} b_1 \overset{2}{\oplus} c_1^-\rangle = |d_1\rangle$
$|a_1\rangle$
$|c_1^-\rangle$
U_c^*
$|0\rangle$
$|a_0 \overset{2}{\oplus} b_0\rangle = |d_0\rangle$
$|a_0\rangle$
$|0\rangle$
$|0\rangle$
$|d_1\rangle$
$|a_1\rangle$
$|0\rangle$
$|d_0\rangle$
$|a_0\rangle$
$|0\rangle$

Quantum Adder Modulo N - $(a + b) \bmod N$



$\mathbb{H}^W \ni \lvert 0\rangle^1$	$\lvert 0\rangle$	$\lvert 0\rangle$	$\lvert 0\rangle$ $\lvert 1\rangle$	$\lvert 0\rangle$ $\lvert 1\rangle$	$\lvert 0\rangle$ $\lvert 1\rangle$	$\lvert 0\rangle$ $\lvert 0\rangle$	$\lvert 0\rangle$ $\lvert 0\rangle$	Target-qubit for $\Lambda^{\lvert\cdot\rangle^1}(X)$ in A_4 and A_8
b_n	c_n^{1+}	$c_n^{3-} = \begin{cases} 0 \Leftrightarrow b+a \geq N \\ 1 \Leftrightarrow b+a < N \end{cases}$	0 1	0 0	$c_n^{7-} = 1$ $c_n^{7-} = 0$	1 0	0 0	Control-qubit for $\Lambda^{\lvert\cdot\rangle^1}(X)$ in A_4 and A_8
b_{n-1}	s_{n-1}^1	d_{n-1}^3	d_{n-1}^3	d_{n-1}^3 s_{n-1}^5	d_{n-1}^7 b_{n-1}	d_{n-1}^7 b_{n-1}	$(b+a-N)_{n-1}$ $(b+a)_{n-1}$	
$\vdots$							$\vdots$	
b_1	s_1^1	d_1^3	d_1^3	d_1^3 s_1^5	d_1^7 b_1	d_1^7 b_1	$(b+a-N)_1$ $(b+a)_1$	
b_0	s_0^1	d_0^3	d_0^3	d_0^3 s_0^5	d_0^7 b_0	d_0^7 b_0	$(b+a-N)_0$ $(b+a)_0$	

$$|b+a+(c_n^{3-}-1)N\rangle = \begin{cases} |b+a-N\rangle & \text{if } b+a \geq N \\ |b+a\rangle & \text{if } b+a < N \end{cases} = |(b+a) \mod N\rangle$$

Homework

Write qiskit code to subtract 5 - 4 and submit the code to
`quantumcomputing@quanterall.com`

THANK YOU FOR YOUR ATTENTION!

БЛАГОДАРЯ ЗА ВНИМАНИЕТО!