Implementation of the Quantum Hashing Algorithm for Real Devices

Kamil Khadiev
joint with
Aliya Khadieva, Ilnar Gazizov, and Eseniia Shcherbakova

Mathematical Modeling and Computational Physics - MMCP'2026,
Dubna, June 23, 2026





The Kazan E. K. Zavoisky
Physical-Technical Institute

Quantum Hashing Technique

- For $x \in \mathbb{Z}_p$ n-qubit hash is

$$|\psi(x)\rangle = \frac{1}{\sqrt{d}} \sum_{j=1}^{d} |j\rangle \left(R_a \left(\frac{4\pi k_j x}{p} \right) |q_n\rangle \right),$$

where $K = \{k_1, \ldots, k_d\}$ is the set of parameters such that

$$\frac{1}{d} \left| \sum_{j=1}^{d} e^{i \frac{2\pi k_j x}{p}} \right| \leq \varepsilon.$$

Note that $n = \log d + 1$ и $d = O(\log q/\varepsilon^2)$.

- For amplitude form of the quantum hashing $a = y$ and $|q_n\rangle = |0\rangle$.
- For phase form of the quantum hashing $a = z$ and $|q_n\rangle = |1\rangle$.

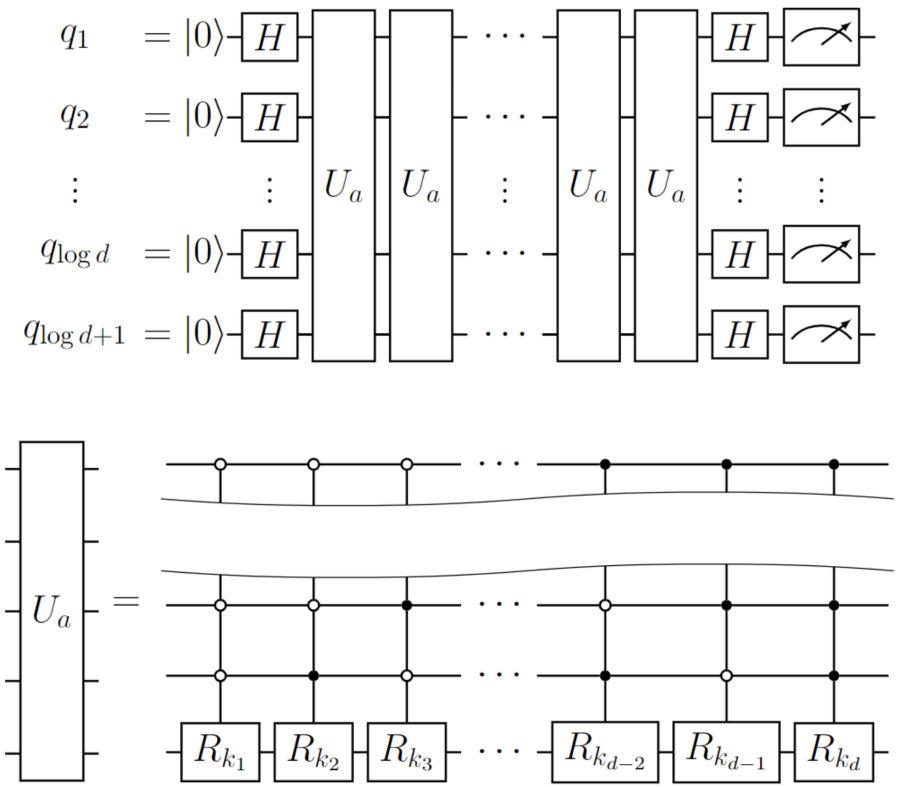
Quantum Hashing Technique

The technique has wide applications in

- communication complexity;
- streaming algorithms;
- automata
- quantum hashing;
- branching programs (OBDD);
- machine learning;
- query model algorithms
- ...

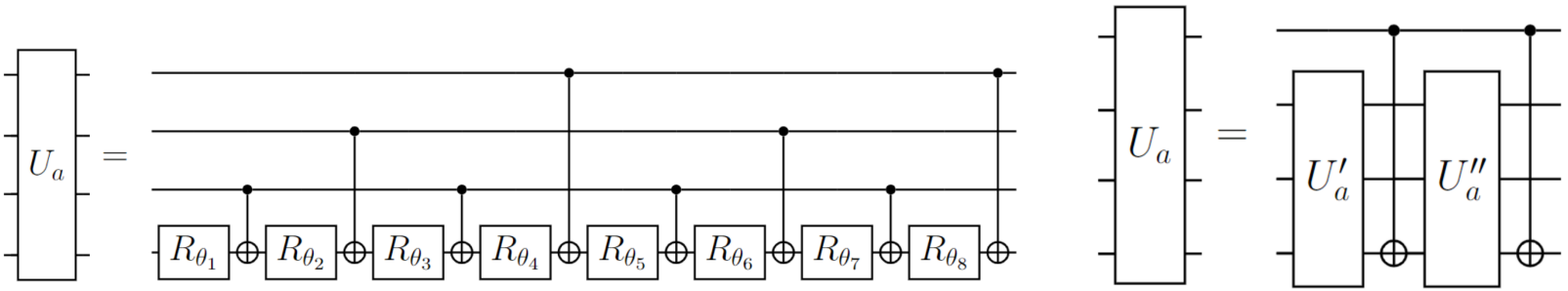
QFA for MOD_p Implementation. UCR-gate

A basic step of the quantum hashing algorithm is



Efficient Decomposition of UCRY-gate

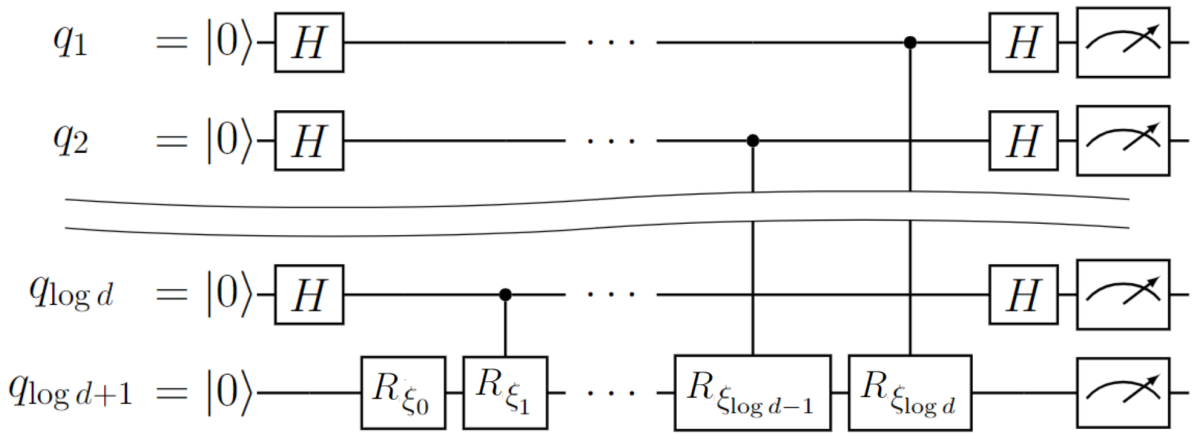
Möttönen et al.,2006:



- $\alpha_i = 2\pi k_i/p$ are the original angles, for $i \in \{1, \ldots, d\}$.
- $\begin{pmatrix}\theta_1 & \theta_2 & \cdots & \theta_d\end{pmatrix}^T = B \begin{pmatrix}\alpha_1 & \alpha_2 & \cdots & \alpha_d\end{pmatrix}^T$, where $B_{ij} = \frac{1}{d}(-1)^{(b_j - 1)\cdot(g_i - 1)}$ and b_m and g_m are binary code and binary reflected Gray code representations of the integer m, respectively.
- The CNOT cost of U_a is d.

Shallow Circuit for One Step of Quantum Hashing

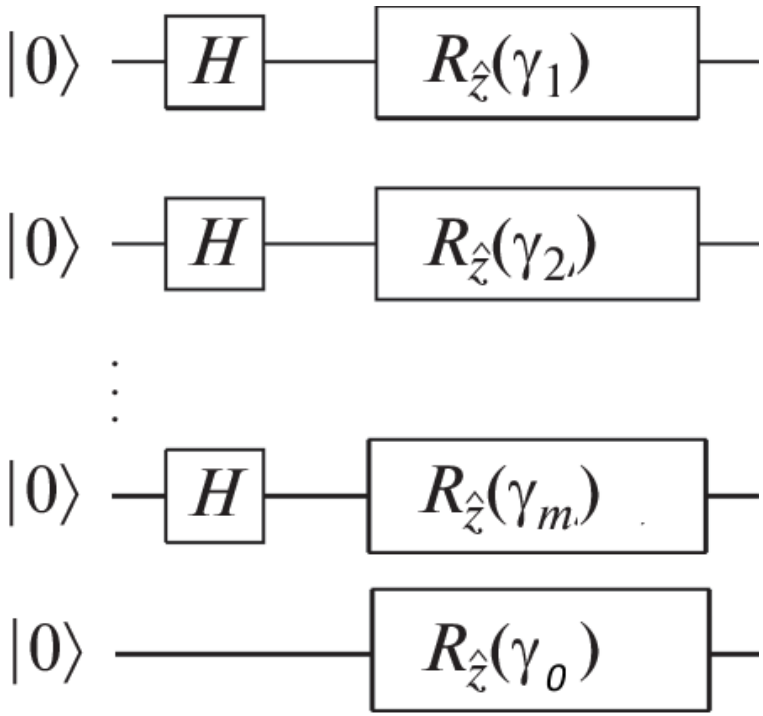
For 3 qubits: Kalis, 2018
The general technique: Ziiatdinov, A.K., Yakaryılmaz, 2023;
Ziiatdinov, A.K., K.K., 2025



CNOT cost is $O(\log d)$;

Phase Form of Quantum Hashing

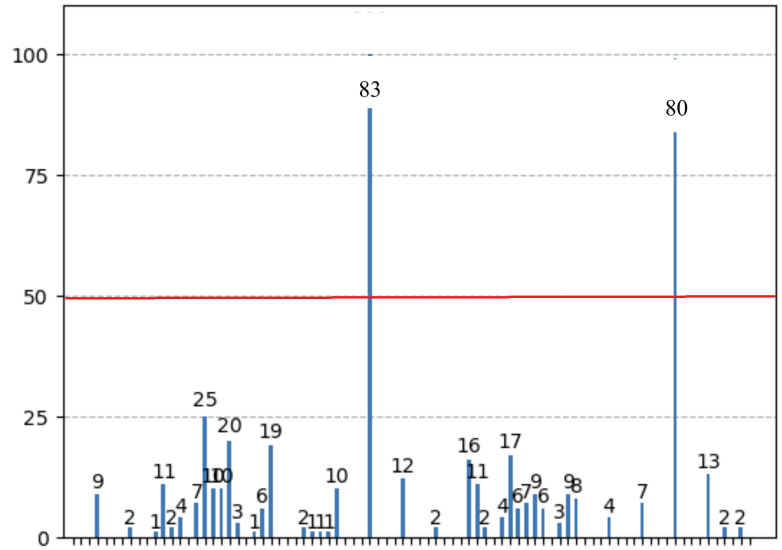
Vasiliev, 2023:



Phase Form of Quantum Hashing. Equality problem

- Let p be a prime
- $MOD_p(x) = 1$ if $\#_1(x)$ is divisible by p
- Hash is $|\psi(x)\rangle = \frac{1}{\sqrt{d}} \sum_{j=1}^{d} |j\rangle \left(R_a \left(\frac{4\pi k_j x}{p} \right) |q_n\rangle \right)$.

$p = 17,\ n = 4,\ K = (11, 8, 13, 16)$

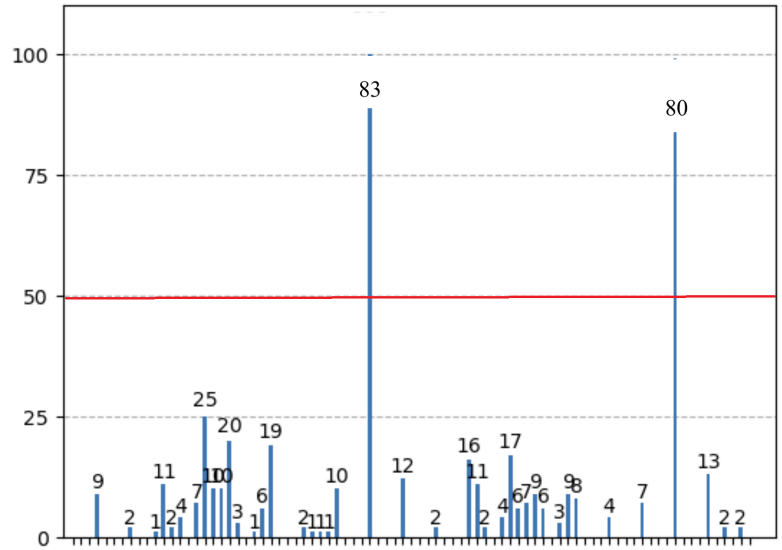


We implement it on 4 qubit quantum device
Bauman Octillion
SnowDrop 4Q

Phase Form of Quantum Hashing. Equality problem

- Let p be a prime
- $MOD_p(x) = 1$ if $\#_1(x)$ is divisible by p
- Hash is $|\psi(x)\rangle = \frac{1}{\sqrt{d}} \sum_{j=1}^{d} |j\rangle \left(R_a \left(\frac{4\pi k_j x}{p} \right) |q_n\rangle \right)$.

$p = 17,\ n = 4,\ K = (11, 8, 13, 16)$



We implement it on 4 qubit quantum device
Bauman Octillion
SnowDrop 4Q

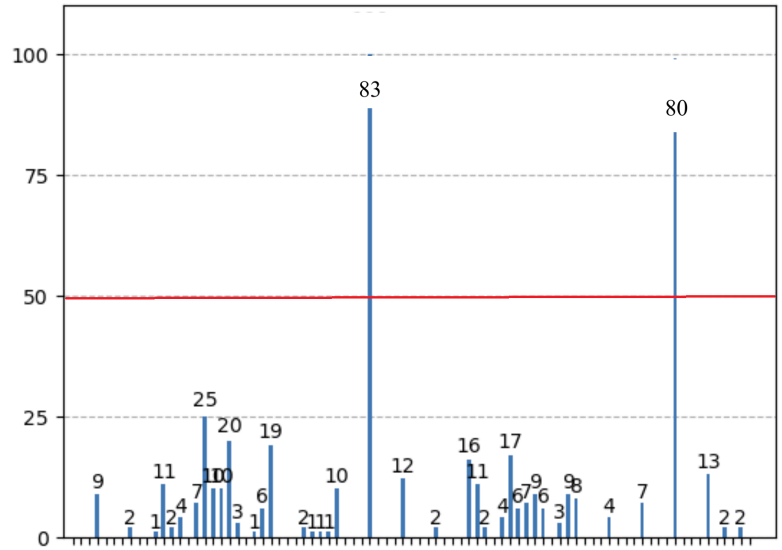
Ambainis, Freivalds, 98

Any classical algorithm requires at least $\lceil \log_2(p) \rceil = 5$ bits.

Phase Form of Quantum Hashing. Equality problem

- Let p be a prime
- $MOD_p(x) = 1$ if $\#_1(x)$ is divisible by p
- Hash is $|\psi(x)\rangle = \frac{1}{\sqrt{d}} \sum_{j=1}^{d} |j\rangle \left(R_a \left(\frac{4\pi k_j x}{p} \right) |q_n\rangle \right)$.

$p = 17,\ n = 4,\ K = (11, 8, 13, 16)$



- Equality of x and y

We implement it on 4 qubit quantum device
Bauman Octillion
SnowDrop 4Q

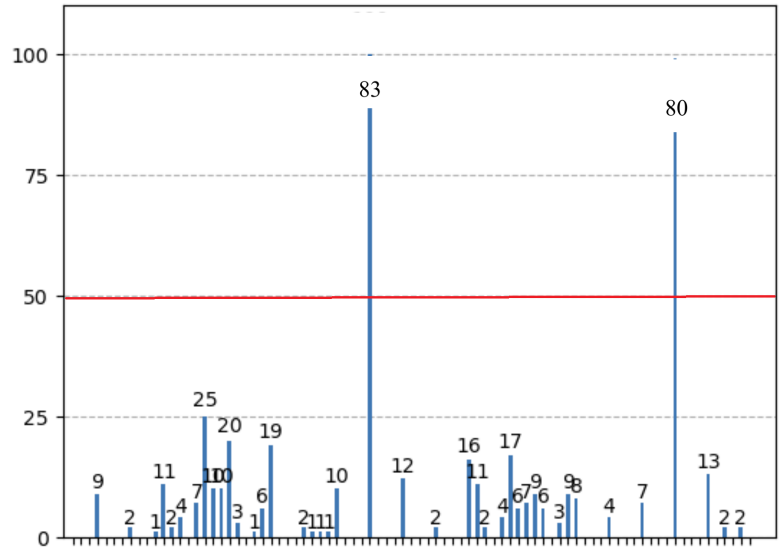
Ambainis, Freivalds, 98

Any classical algorithm requires at least $\lceil \log_2(p) \rceil = 5$ bits.

Phase Form of Quantum Hashing. Equality problem

- Let p be a prime
- $MOD_p(x) = 1$ if $\#_1(x)$ is divisible by p
- Hash is $|\psi(x)\rangle = \frac{1}{\sqrt{d}} \sum_{j=1}^{d} |j\rangle \left(R_a \left(\frac{4\pi k_j x}{p} \right) |q_n\rangle \right)$.

$p = 17,\ n = 4,\ K = (11, 8, 13, 16)$



- Equality of x and y
- $|\psi(x)\rangle = |\psi(y)\rangle$ means $x = y$.

We implement it on 4 qubit quantum device
Bauman Octillion
SnowDrop 4Q

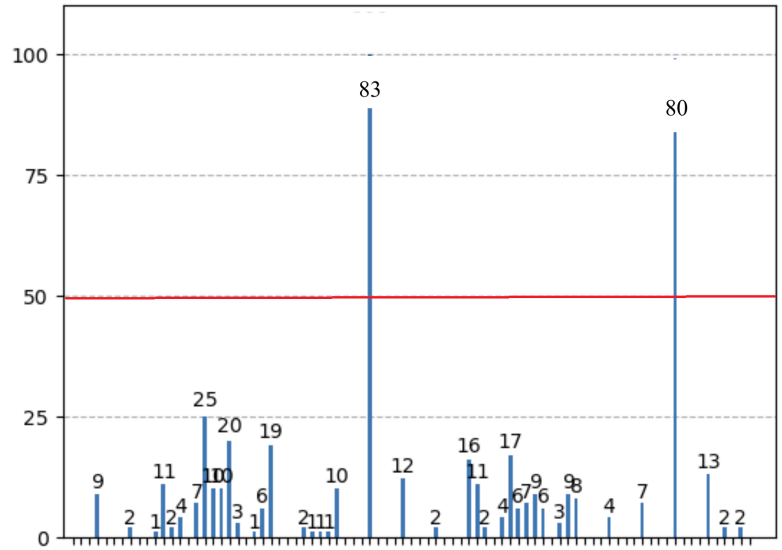
Ambainis, Freivalds, 98

Any classical algorithm requires at least $\lceil \log_2(p) \rceil = 5$ bits.

Phase Form of Quantum Hashing. Equality problem

- Let p be a prime
- $MOD_p(x) = 1$ if $\#_1(x)$ is divisible by p
- Hash is $|\psi(x)\rangle = \frac{1}{\sqrt{d}} \sum_{j=1}^{d} |j\rangle \left(R_a \left(\frac{4\pi k_j x}{p} \right) |q_n\rangle \right)$.

$p = 17$, $n = 4$, $K = (11, 8, 13, 16)$



- Equality of x and y
- $|\psi(x)\rangle = |\psi(y)\rangle$ means $x = y$.
- if $x = y$, then $x - y = 0$

We implement it on 4 qubit quantum device
Bauman Octillion
SnowDrop 4Q

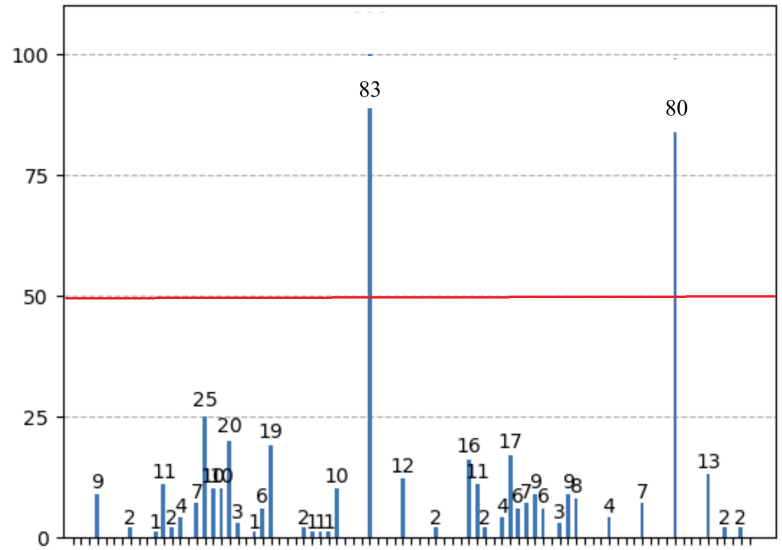
Ambainis, Freivalds, 98

Any classical algorithm requires at least $\lceil \log_2(p) \rceil = 5$ bits.

Phase Form of Quantum Hashing. Equality problem

- Let p be a prime
- $MOD_p(x) = 1$ if $\#_1(x)$ is divisible by p
- Hash is $|\psi(x)\rangle = \frac{1}{\sqrt{d}} \sum_{j=1}^{d} |j\rangle \left(R_a \left(\frac{4\pi k_j x}{p} \right) |q_n\rangle \right)$.

$p = 17,\ n = 4,\ K = (11, 8, 13, 16)$



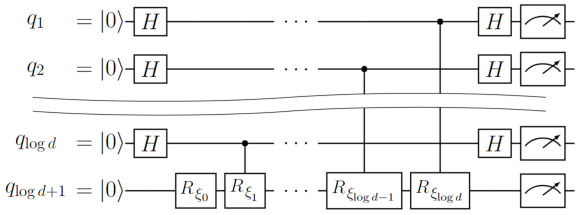
- Equality of x and y
- $|\psi(x)\rangle = |\psi(y)\rangle$ means $x = y$.
- if $x = y$, then $x - y = 0$
- $|\psi(x - y)\rangle$ is such that $x - y = 0$

We implement it on 4 qubit quantum device
Bauman Octillion
SnowDrop 4Q

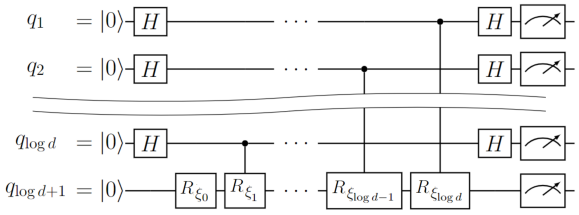
Ambainis, Freivalds, 98

Any classical algorithm requires at least $\lceil \log_2(p) \rceil = 5$ bits.

The Circuit for Amplitude Form of Quantum Hashing.

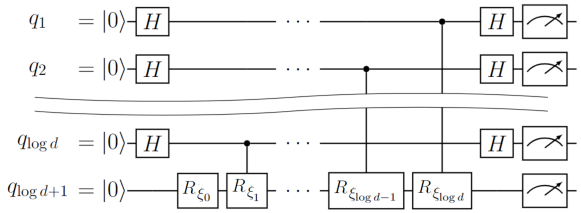


The Circuit for Amplitude Form of Quantum Hashing.



Issues:

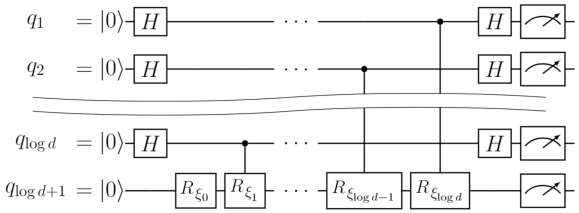
The Circuit for Amplitude Form of Quantum Hashing.

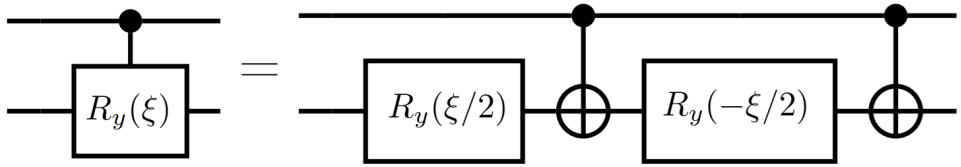


Issues:

- The gate set is $CNOT, X, H, R_y$.

The Circuit for Amplitude Form of Quantum Hashing.

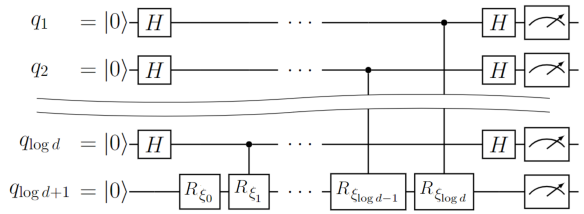




Issues:

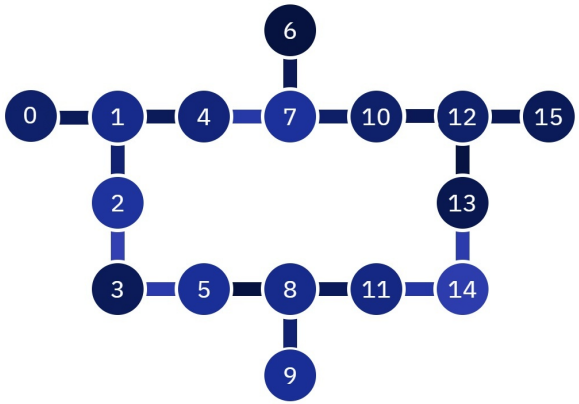
- The gate set is $CNOT, X, H, R_y$.

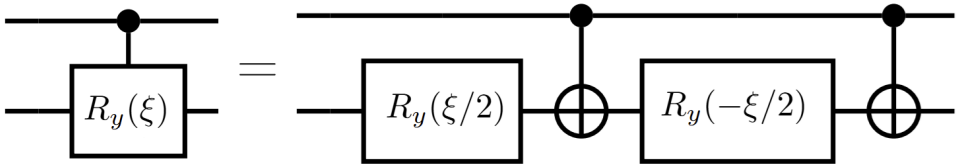
The Circuit for Amplitude Form of Quantum Hashing.



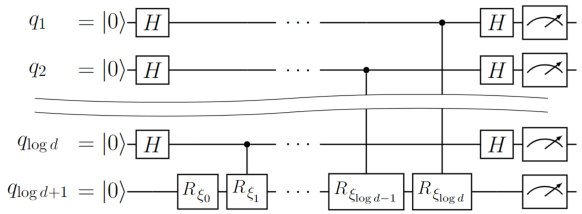
Issues:

- The gate set is $CNOT, X, H, R_y$.
- The qubit connectivity graph.



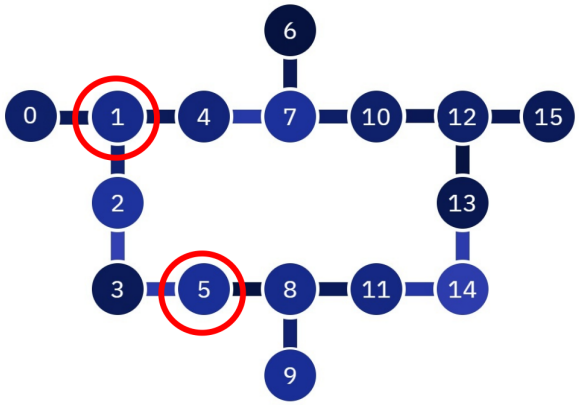


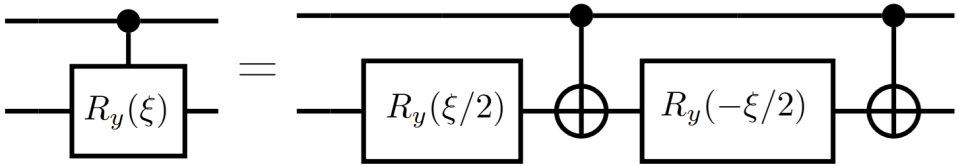
The Circuit for Amplitude Form of Quantum Hashing.



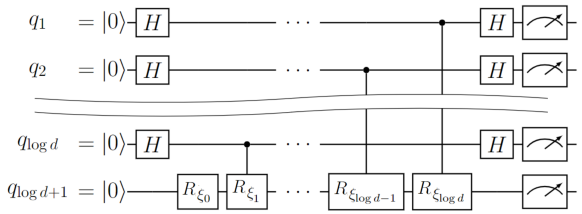
Issues:

- The gate set is $CNOT, X, H, R_y$.
- The qubit connectivity graph.



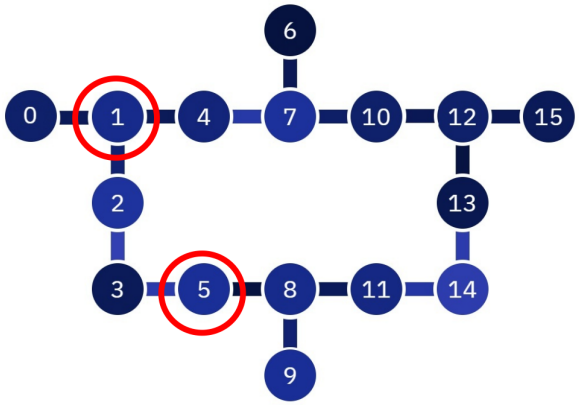


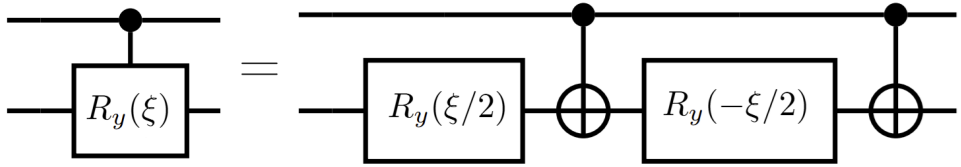
The Circuit for Amplitude Form of Quantum Hashing.



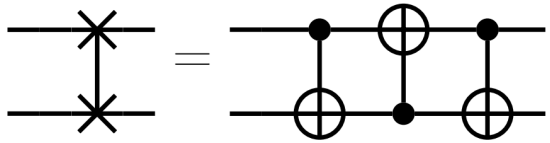
Issues:

- The gate set is $CNOT, X, H, R_y$.
- The qubit connectivity graph.

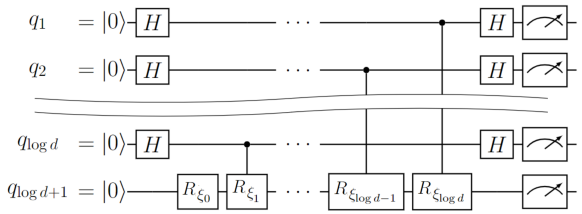




The SWAP-gate swaps values of two qubits

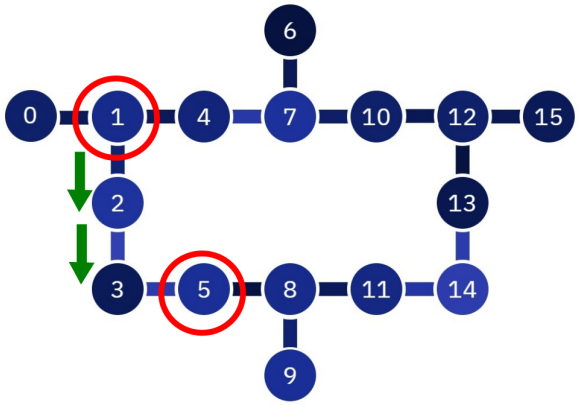


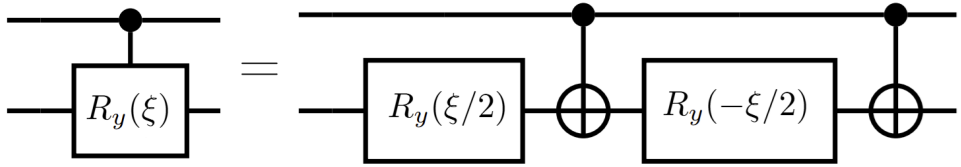
The Circuit for Amplitude Form of Quantum Hashing.



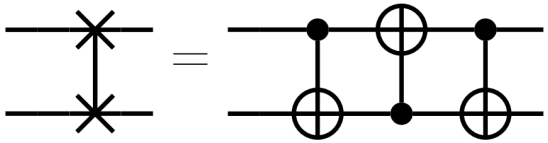
Issues:

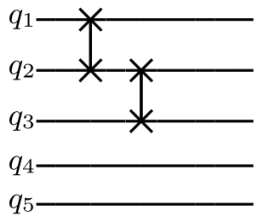
- The gate set is $CNOT, X, H, R_y$.
- The qubit connectivity graph.



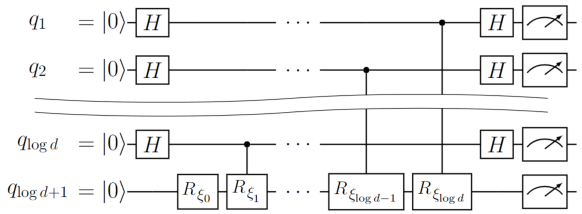


The SWAP-gate swaps values of two qubits



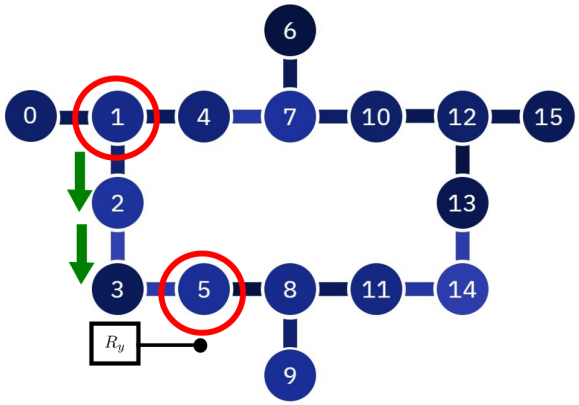


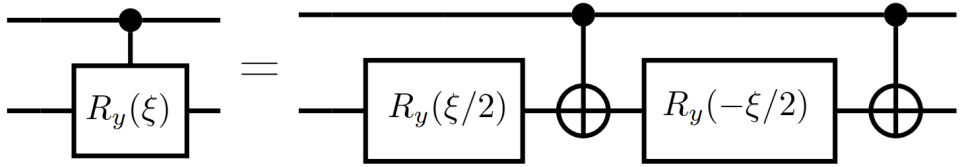
The Circuit for Amplitude Form of Quantum Hashing.



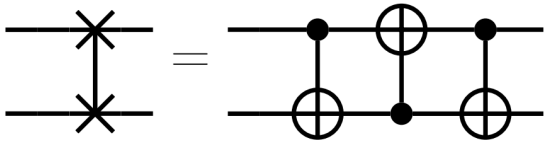
Issues:

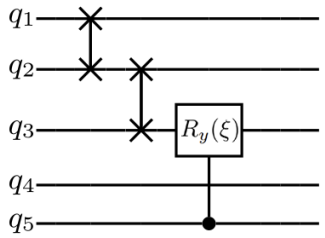
- The gate set is $CNOT, X, H, R_y$.
- The qubit connectivity graph.



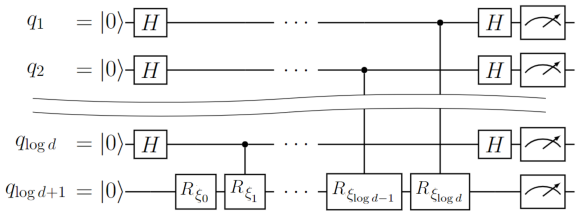


The SWAP-gate swaps values of two qubits



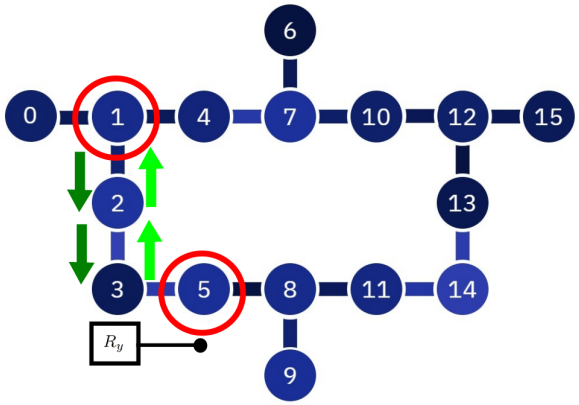


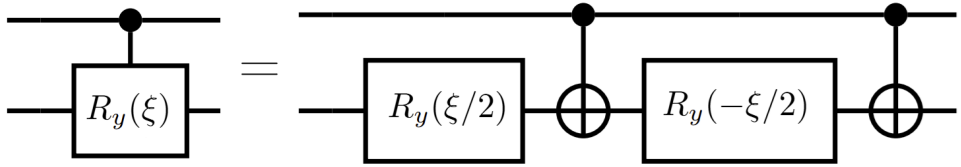
The Circuit for Amplitude Form of Quantum Hashing.



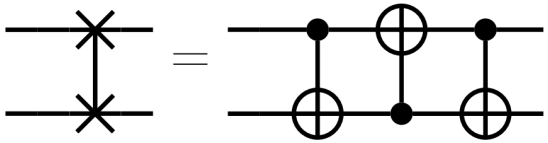
Issues:

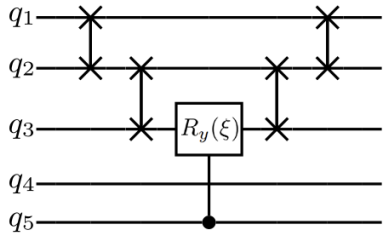
- The gate set is $CNOT, X, H, R_y$.
- The qubit connectivity graph.



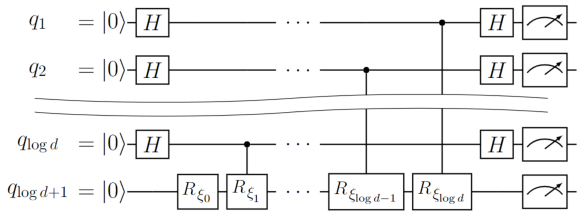


The SWAP-gate swaps values of two qubits



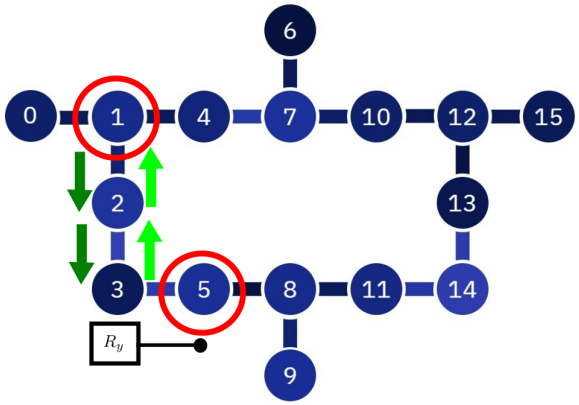


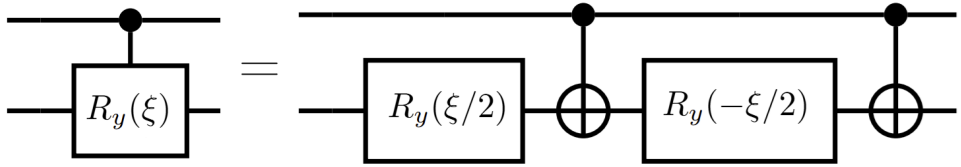
The Circuit for Amplitude Form of Quantum Hashing.



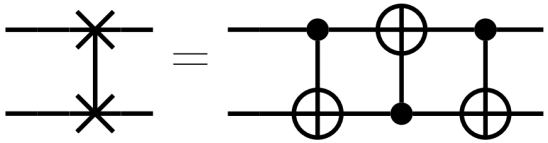
Issues:

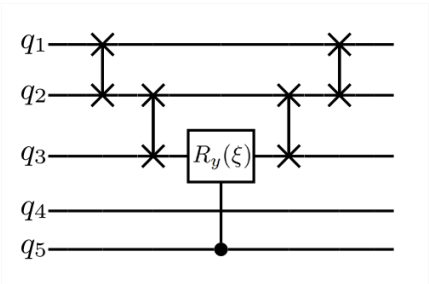
- The gate set is $CNOT, X, H, R_y$.
- The qubit connectivity graph.





The SWAP-gate swaps values of two qubits

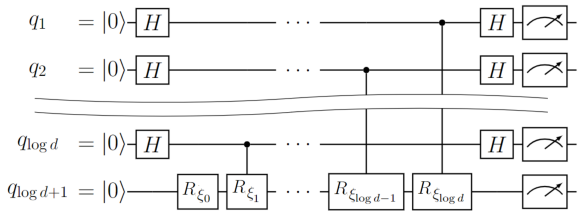




Originally, we need 2 CNOT-gates.

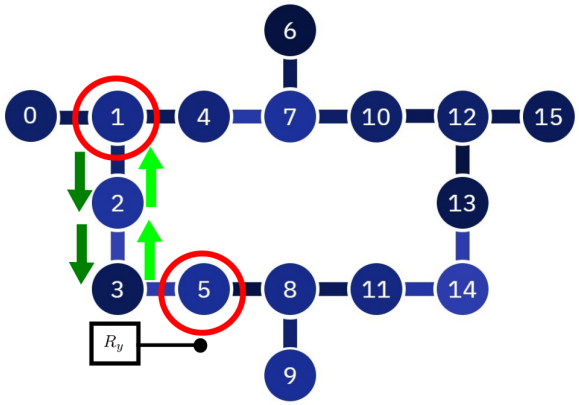
But now, we need $14 = 6 \cdot dist + 2$ CNOT-gates.

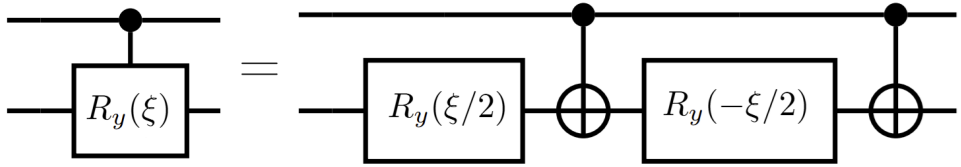
The Circuit for Amplitude Form of Quantum Hashing.



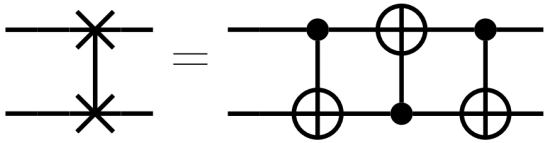
Issues:

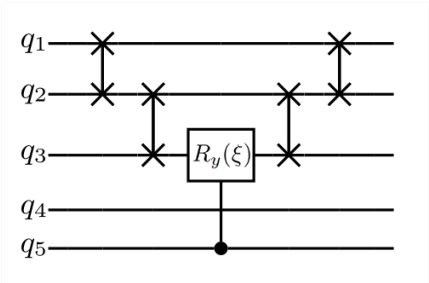
- The gate set is $CNOT, X, H, R_y$.
- The qubit connectivity graph.





The SWAP-gate swaps values of two qubits





Originally, we need 2 CNOT-gates.

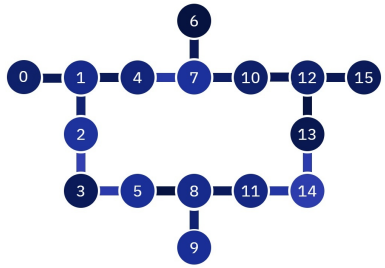
But now, we need $14 = 6 \cdot dist + 2$ CNOT-gates.

Our main goal is

to minimize the CNOT-cost (the number of CNOT-gates).

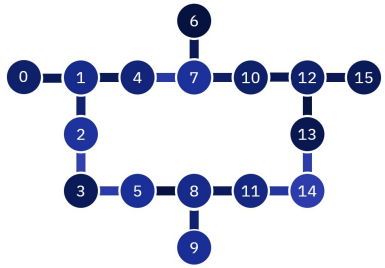
The (3,2,1)-Covering Path Problem

Let us have a graph $G = (V, E)$.
The vertices number is $n = |V|$.
The edges number is $m = |E|$.



The (3,2,1)-Covering Path Problem

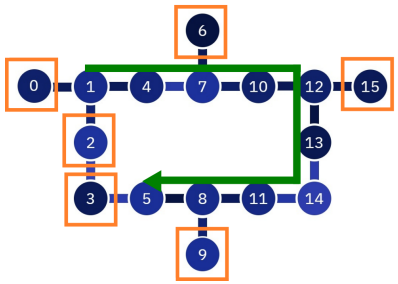
Let us have a graph $G = (V, E)$.
The vertices number is $n = |V|$.
The edges number is $m = |E|$.



A path P covering a set $\mathrm{Cvr}(P)$

The (3,2,1)-Covering Path Problem

Let us have a graph $G = (V, E)$.
The vertices number is $n = |V|$.
The edges number is $m = |E|$.

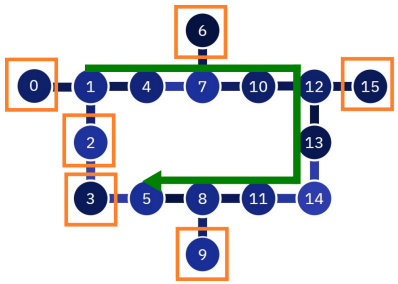


A path P covering a set $\mathrm{Cvr}(P)$

- A non-simple path $P = (v_{i_1}, \ldots, v_{i_k})$ covers a set of vertices $\mathrm{Cvr}(P)$ if each vertex $v \in \mathrm{Cvr}(P)$ is such that
  - v is from P (we call them "visited") or
  - v is connected with some v_{i_j} from the path (we call them "touched").

The (3,2,1)-Covering Path Problem

Let us have a graph $G = (V, E)$.
The vertices number is $n = |V|$.
The edges number is $m = |E|$.

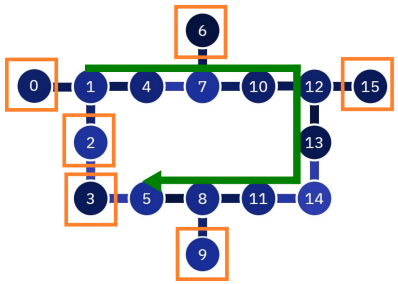


A path P covering a set $\mathrm{Cvr}(P)$

- A non-simple path $P = (v_{i_1}, \ldots, v_{i_k})$ covers a set of vertices $\mathrm{Cvr}(P)$ if each vertex $v \in \mathrm{Cvr}(P)$ is such that
  - v is from P (we call them "visited") or
  - v is connected with some v_{i_j} from the path (we call them "touched").
- Let $\mathrm{Tch}(P) = \mathrm{Cvr}(P) \backslash \{v_{i_1}, \ldots, v_{i_k}\}$ be the touched vertices.

The (3,2,1)-Covering Path Problem

Let us have a graph $G = (V, E)$.
The vertices number is $n = |V|$.
The edges number is $m = |E|$.

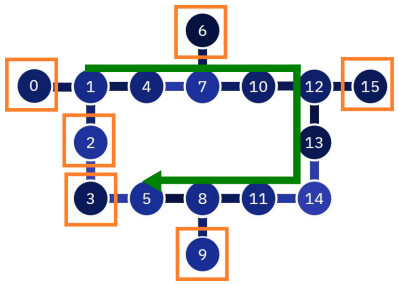


A path P covering a set $\mathrm{Cvr}(P)$

- A non-simple path $P = (v_{i_1}, \ldots, v_{i_k})$ covers a set of vertices $\mathrm{Cvr}(P)$ if each vertex $v \in \mathrm{Cvr}(P)$ is such that
  - v is from P (we call them "visited") or
  - v is connected with some v_{i_j} from the path (we call them "touched").
- Let $\mathrm{Tch}(P) = \mathrm{Cvr}(P) \backslash \{v_{i_1}, \ldots, v_{i_k}\}$ be the touched vertices.
- The cost of the path is $cost(P) = 2 \cdot |\mathrm{Tch}(P)| + 3|P|$.

The (3,2,1)-Covering Path Problem

Let us have a graph $G = (V, E)$.
The vertices number is $n = |V|$.
The edges number is $m = |E|$.



A path P covering a set $\mathrm{Cvr}(P)$

- A non-simple path $P = (v_{i_1}, \ldots, v_{i_k})$ covers a set of vertices $\mathrm{Cvr}(P)$ if each vertex $v \in \mathrm{Cvr}(P)$ is such that
  - v is from P (we call them "visited") or
  - v is connected with some v_{i_j} from the path (we call them "touched").
- Let $\mathrm{Tch}(P) = \mathrm{Cvr}(P) \backslash \{v_{i_1}, \ldots, v_{i_k}\}$ be the touched vertices.
- The cost of the path is $cost(P) = 2 \cdot |\mathrm{Tch}(P)| + 3|P|$.

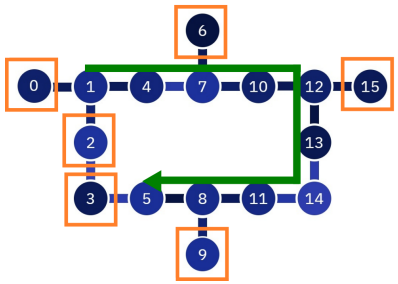
The (3,2,1)-Covering Path Problem

We want to find a path P such that

- $\mathrm{Cvr}(P) = V$,
- $cost(P)$ is minimum.

The (3,2,1)-Covering Path Problem

Let us have a graph $G = (V, E)$.
The vertices number is $n = |V|$.
The edges number is $m = |E|$.



A path P covering a set $\mathrm{Cvr}(P)$

- A non-simple path $P = (v_{i_1}, \ldots, v_{i_k})$ covers a set of vertices $\mathrm{Cvr}(P)$ if each vertex $v \in \mathrm{Cvr}(P)$ is such that
  - v is from P (we call them "visited") or
  - v is connected with some v_{i_j} from the path (we call them "touched").
- Let $\mathrm{Tch}(P) = \mathrm{Cvr}(P) \backslash \{v_{i_1}, \ldots, v_{i_k}\}$ be the touched vertices.
- The cost of the path is $cost(P) = 2 \cdot |\mathrm{Tch}(P)| + 3|P|$.

The (3,2,1)-Covering Path Problem

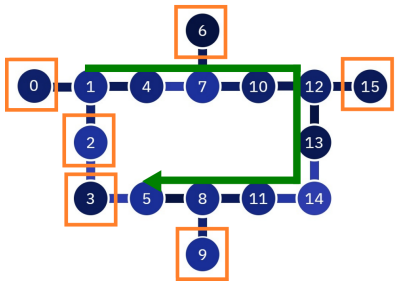
We want to find a path P such that

- $\mathrm{Cvr}(P) = V$,
- $cost(P)$ is minimum.

It is kind of a modification of The Shortest Covering Path (SCP) Problem

The (3,2,1)-Covering Path Problem

Let us have a graph $G = (V, E)$.
The vertices number is $n = |V|$.
The edges number is $m = |E|$.



A path P covering a set $\mathrm{Cvr}(P)$

- A non-simple path $P = (v_{i_1}, \ldots, v_{i_k})$ covers a set of vertices $\mathrm{Cvr}(P)$ if each vertex $v \in \mathrm{Cvr}(P)$ is such that
  - v is from P (we call them "visited") or
  - v is connected with some v_{i_j} from the path (we call them "touched").
- Let $\mathrm{Tch}(P) = \mathrm{Cvr}(P) \backslash \{v_{i_1}, \ldots, v_{i_k}\}$ be the touched vertices.
- The cost of the path is $cost(P) = 2 \cdot |\mathrm{Tch}(P)| + 3|P|$.

The (3,2,1)-Covering Path Problem

We want to find a path P such that

- $\mathrm{Cvr}(P) = V$,
- $cost(P)$ is minimum.

It is kind of a modification of The Shortest Covering Path (SCP) Problem

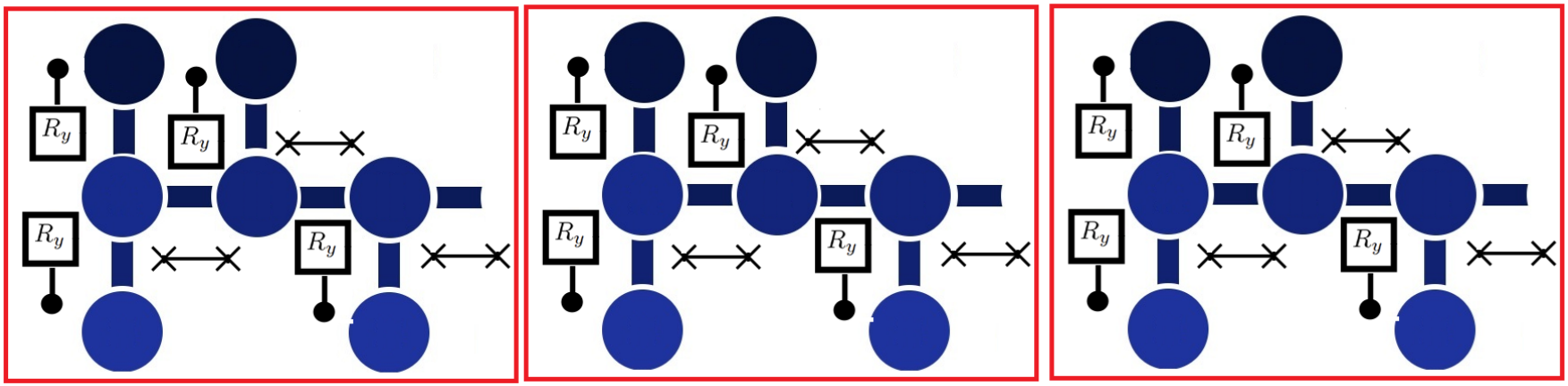
[Current, Pirkul and Rolland, 94] SCP Problem is NP-hard.

Greedy algorithm for large quantum processors

- We implement the algorithm for k qubits.

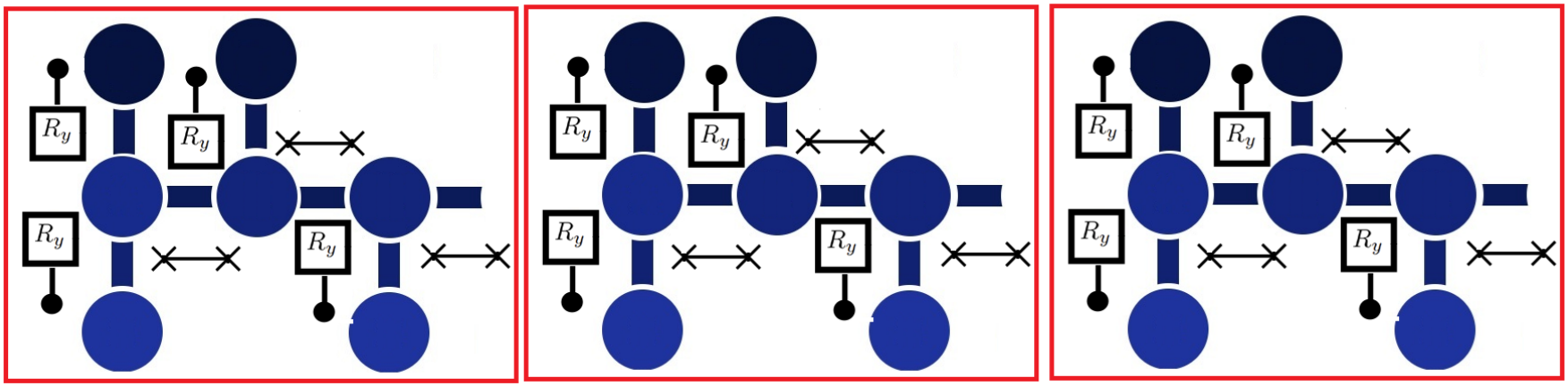
Greedy algorithm for large quantum processors

- We implement the algorithm for k qubits.
- Iterating a patterns and duplicate it enough times for covering k qubits

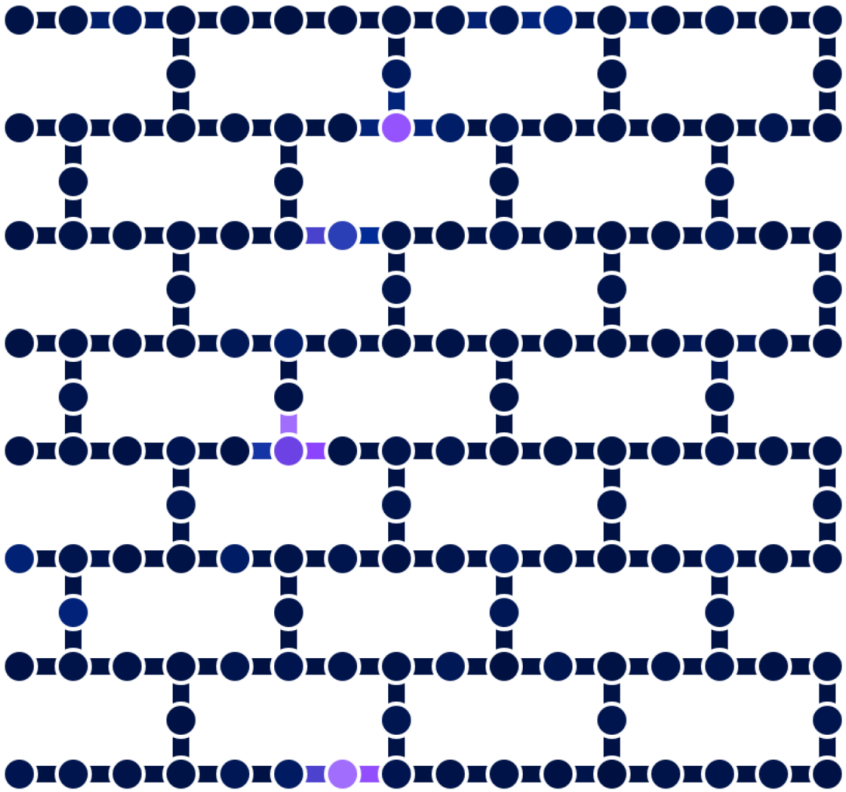


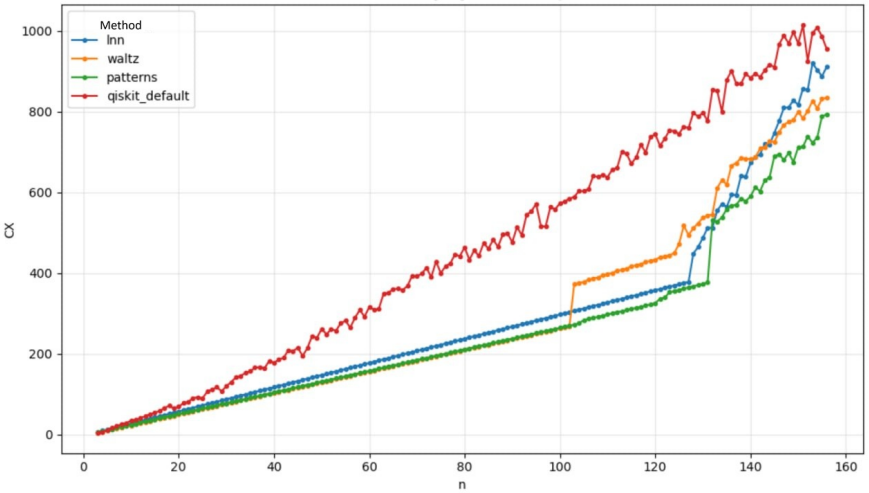
Greedy algorithm for large quantum processors

- We implement the algorithm for k qubits.
- Iterating a patterns and duplicate it enough times for covering k qubits
- apply qiskit transpiler.

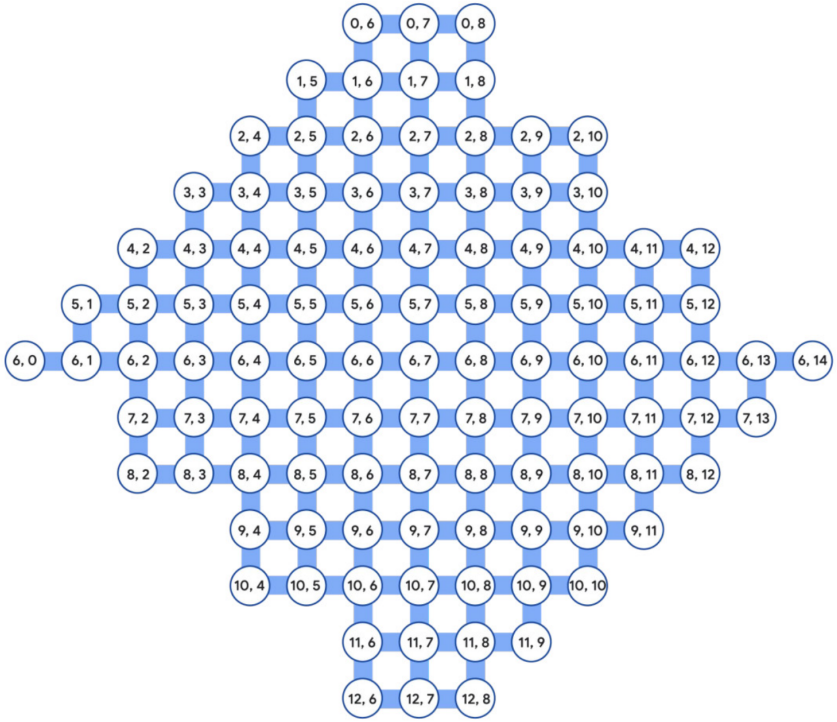


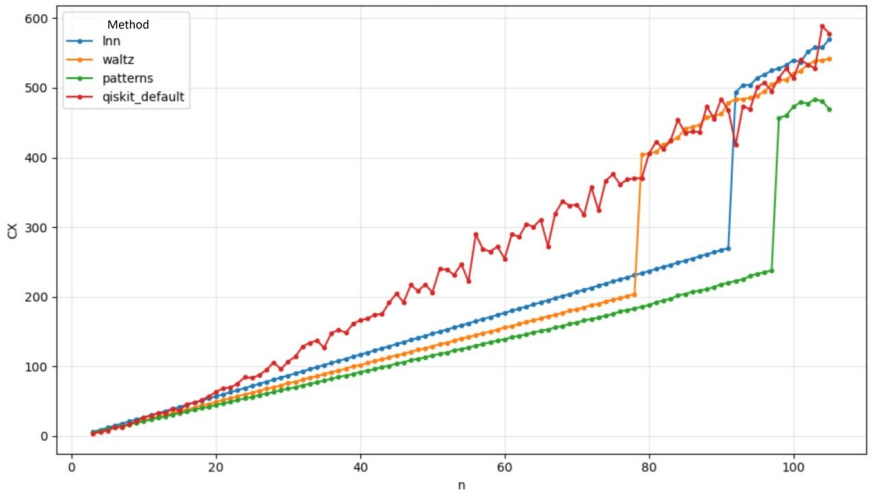
IBMQ Fez




Method
lnn
waltz
patterns
qiskit_default
CX
n
0
200
400
600
800
1000
0
20
40
60
80
100
120
140
160

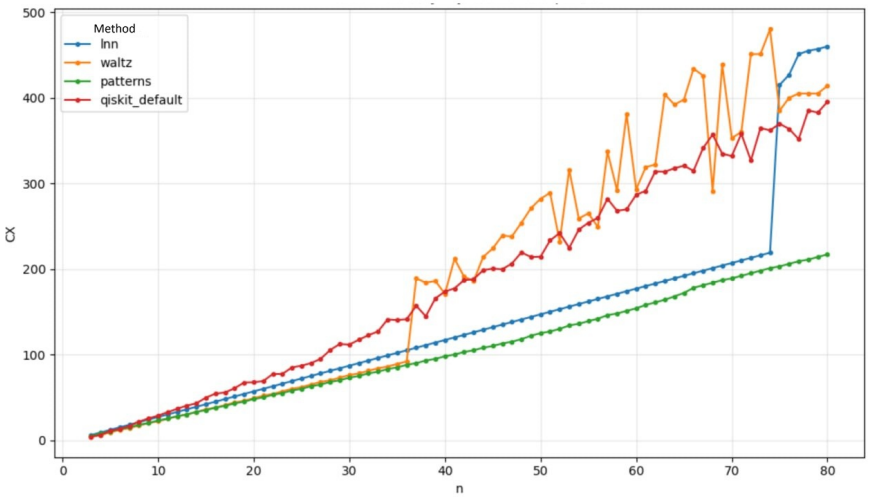
Google Willow



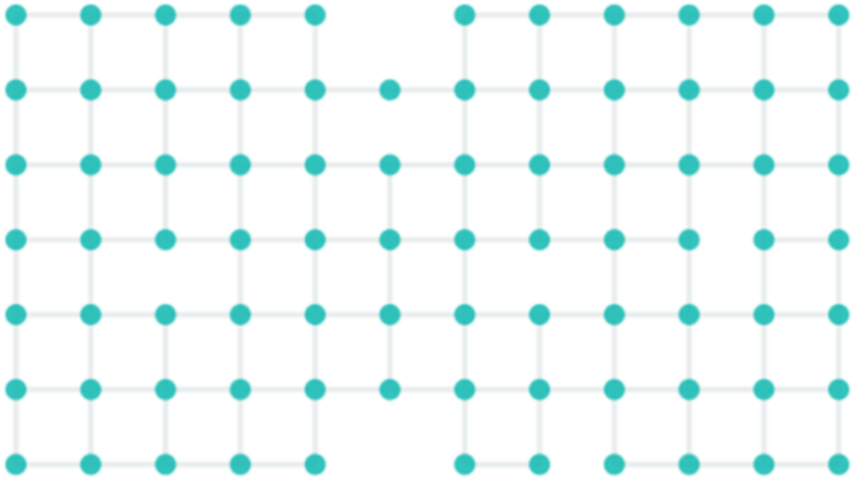


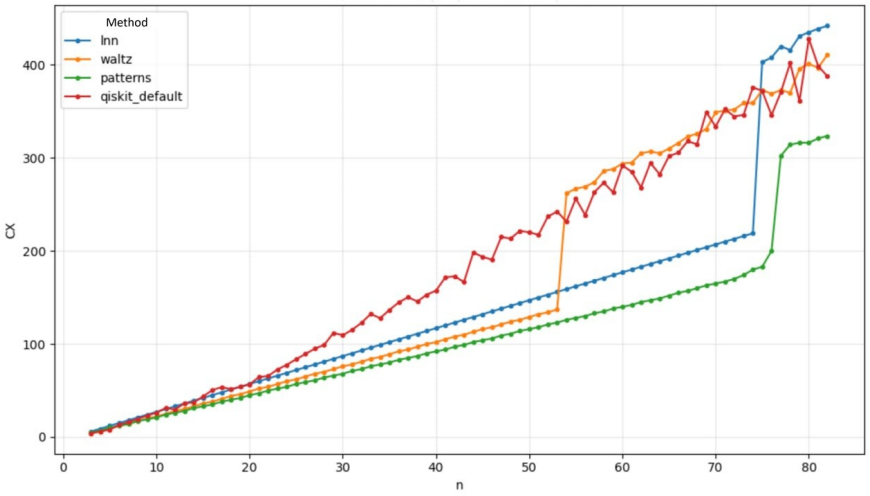
Rigetti Aspen



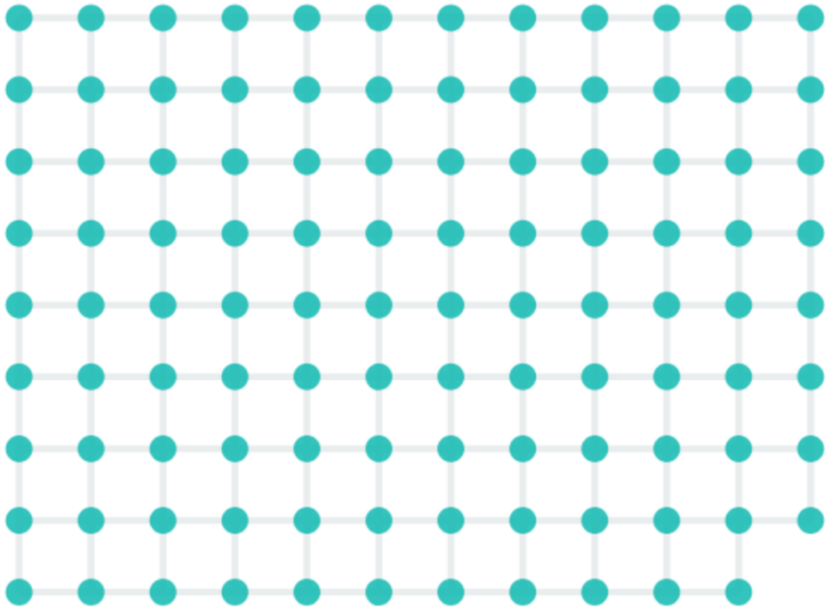


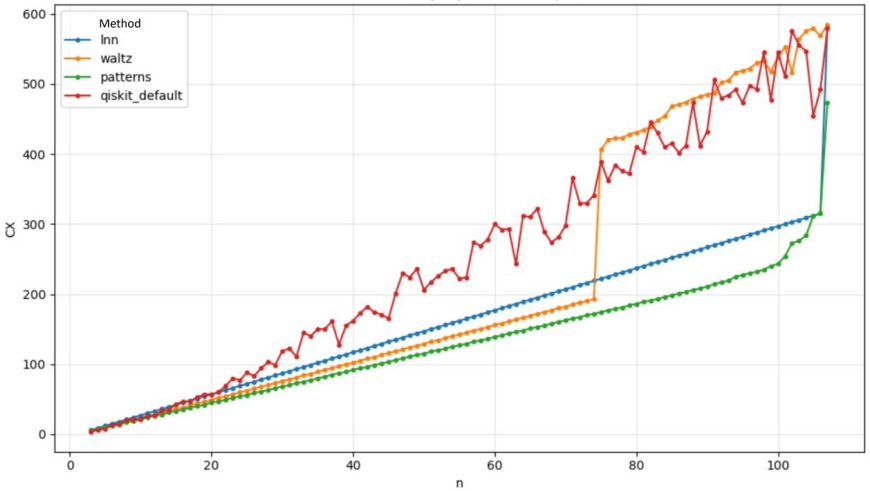
Rigetti Ankaa





Rigetti Cepheus





Thank you for your attention!

e-mail of the corresponding author: kamilhadi@gmail.com