Quantum Circuit Design for Vertex Cover Problem Based on Grover's Algorithm

Advanced Computing and Networking Laboratory
National Central University
Department of Computer Science & Information Engineering

研究生: 顏暐翰　　　　指導教授: 江振瑞 博士

ACAN Laboratory

Outline

- Introduction
- Background knowledge
- Related Works
- Proposed Method
- Experiment and Result
- Conclusion

ACAN Laboratory

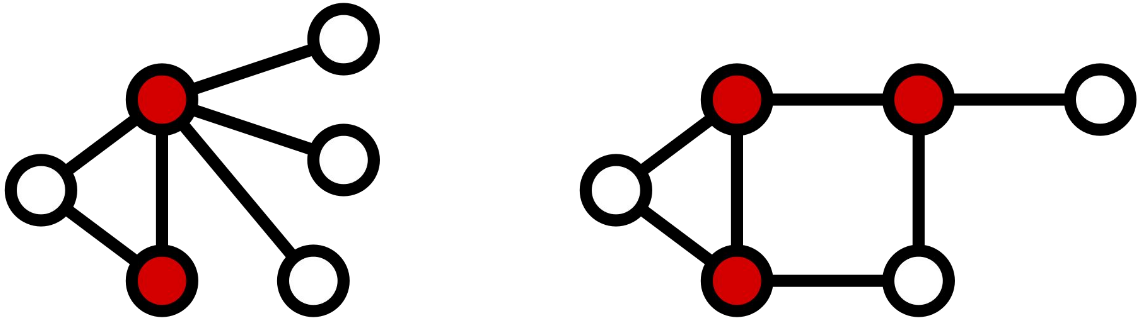
Outline

- Introduction
- Background knowledge
- Related Works
- Proposed Method
- Experiment and Result
- Conclusion

ACAN Laboratory

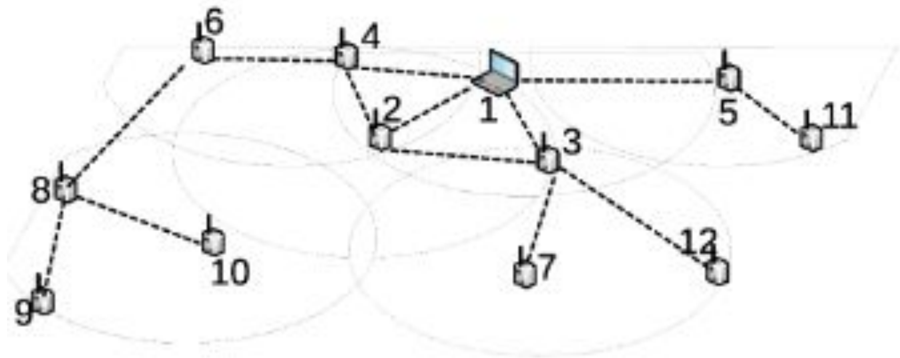
Vertex cover

- Formally, a vertex cover *V'* of a undirected graph G=(V,E) is a subset of *V* such that u,v ∈ E $\Rightarrow$ u ∈ *V'* or v ∈ *V'*.
- In graph theory, a vertex cover of a graph is a set of vertices that includes at least one endpoint of every edge of the graph.



Vertex cover problem (VCP)

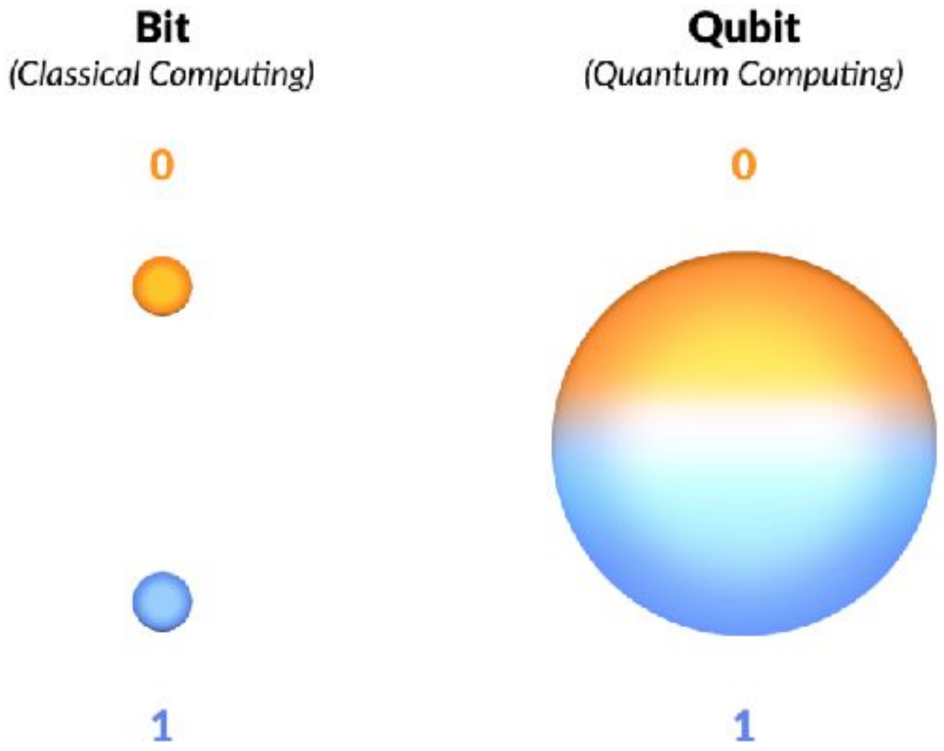
- Given an undirected graph G(V,E) and a positive integer k, does G have a vertex cover of size at most k?
- Vertex cover problem serves as a model for many real-world and theoretical problems.



Reference : Gusev, V. V. (2020). The vertex cover game: Application to transport networks. Omega, 97, 102102.

Quantum Computing

- Quantum computing is a field that utilize quantum mechanics to solve complex problems faster than on classical computers.
- The property of quantum superposition gives quantum computation the potentia to surpass classical computation, especially in complex problems like combinatorial optimization.



ACAN Laboratory

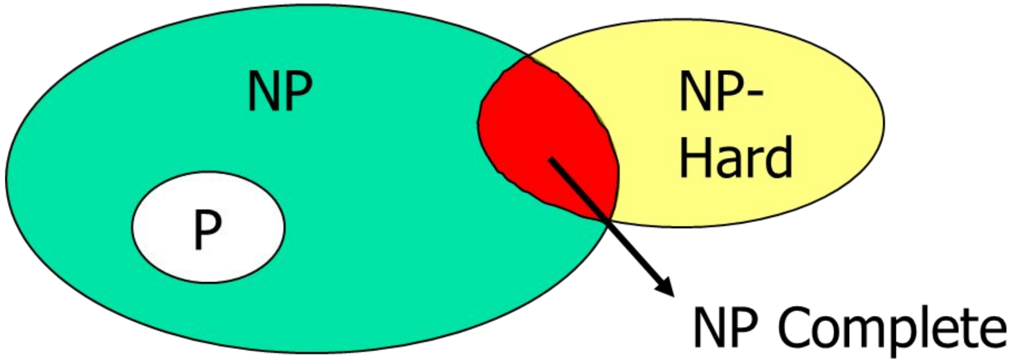
Outline

- Introduction
- Background knowledge
- Related Works
- Proposed Method
- Experiment and Result
- Conclusion

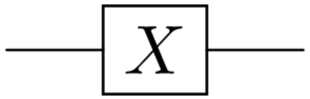
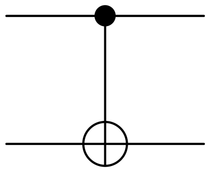
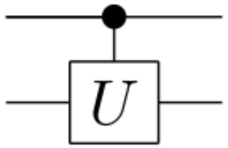
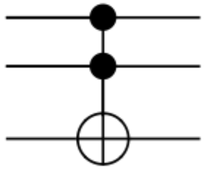
ACAN Laboratory

Problem Classification

- P : the class of problems which can be solved by a deterministic polynomial time complexity algorithm.
- NP : the class of problems which can be solved by a non-deterministic polynomial time complexity algorithm.
- NP-hard : the class of problems to which every NP problem polynomial reduces to.
- NP-complete(NPC) : the class of problems which are NP-hard and belong to NP.

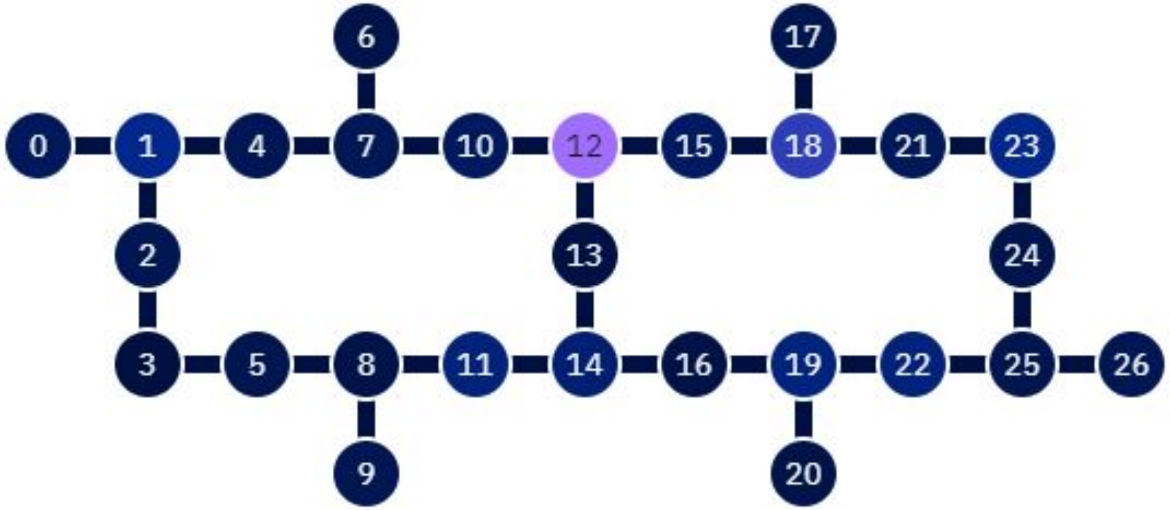


Quantum Gates

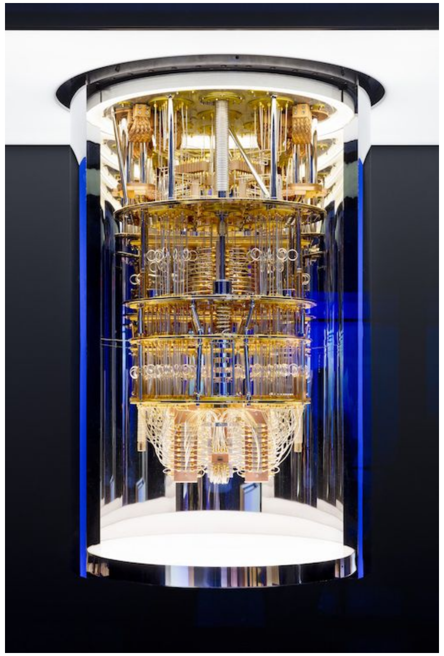
Gate name	Notation	Unitary Matrix
Hadamard gate		$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$
Pauli-X gate		$\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$
Controlled Not gate		$\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}$
Controlled Unitary gate		$\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & u_{00} & u_{01}\\ 0 & 0 & u_{10} & u_{11}\end{bmatrix}$
Toffoli gate		$\begin{bmatrix}1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1\\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0\end{bmatrix}$

Quantum Computer

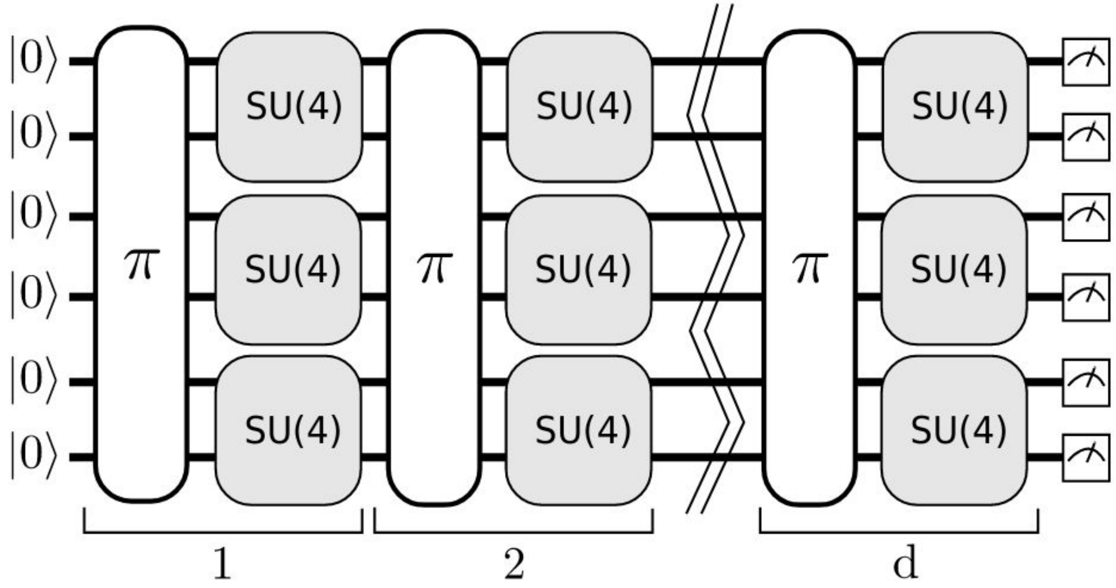
- Transpilation is the process of rewriting a given input circuit to match the topology of a specific quantum device, and to optimize the circuit for execution on present day noisy quantum systems.
- Most circuits must undergo a series of transformations that make them compatible with a given target device.

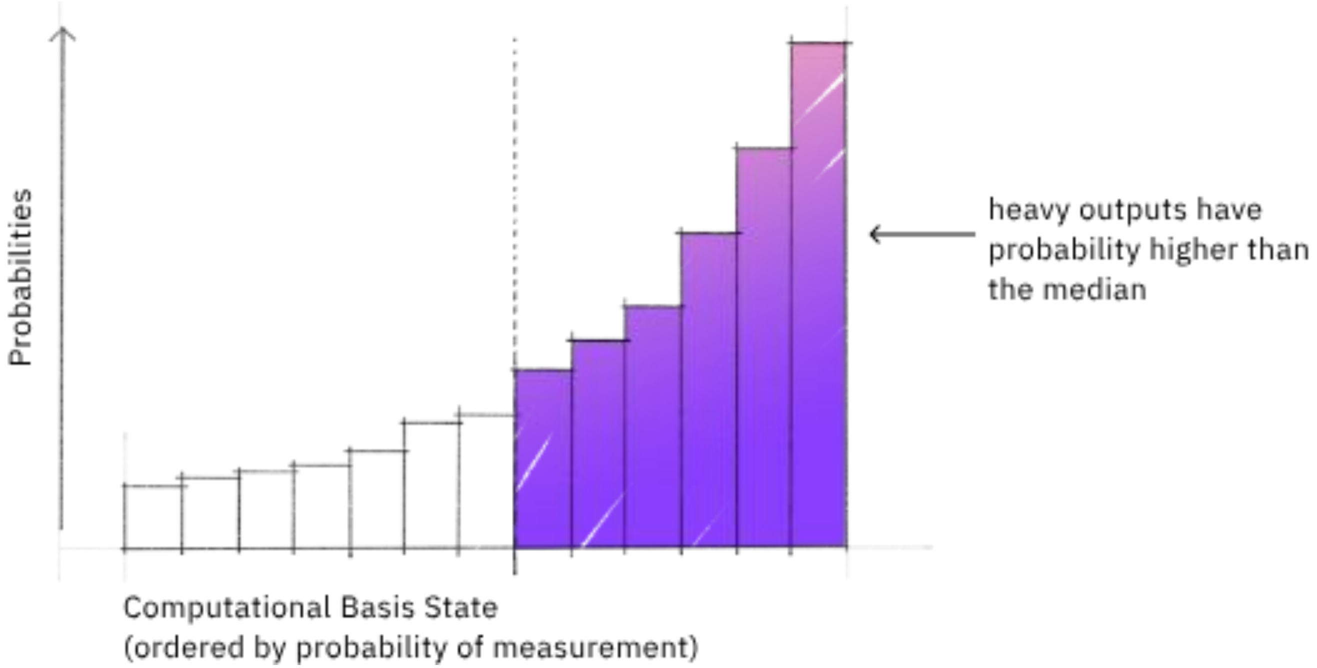


Topology : IBMQ mumbai



Quantum Volume

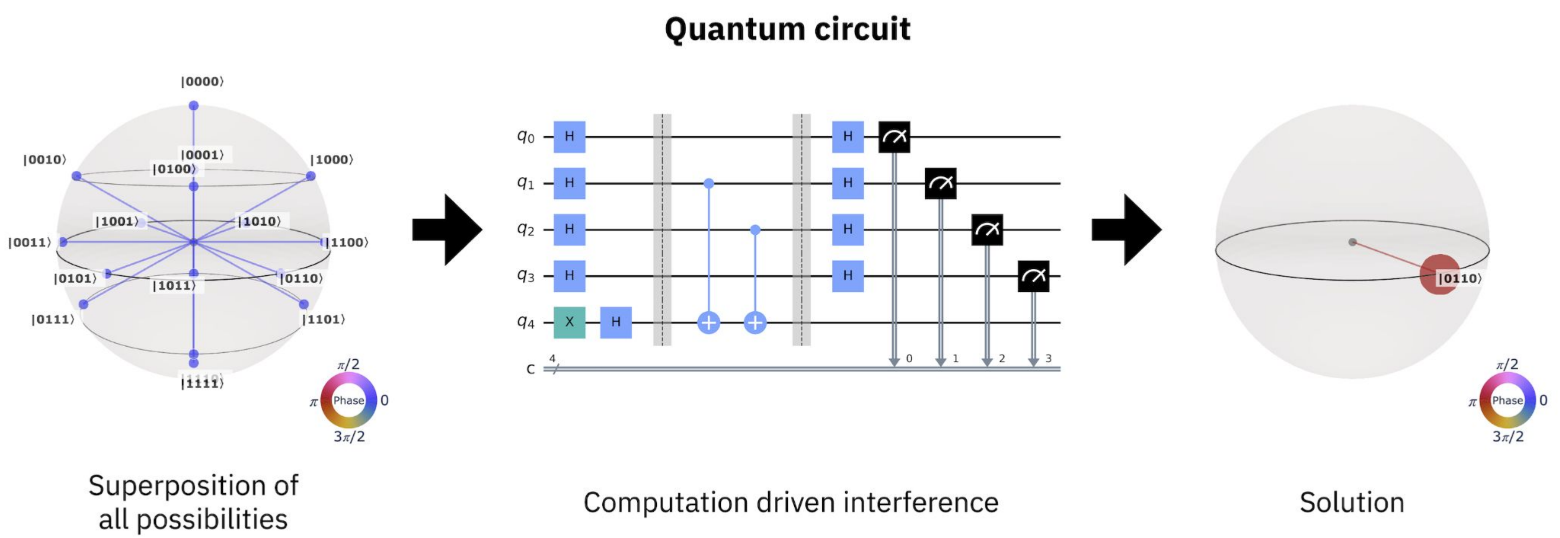




Reference : Cross, A. W., Bishop, L. S., Sheldon, S., Nation, P. D., & Gambetta, J. M. (2019). Validating quantum computers using randomized model circuits. Physical Review A, 100(3), 032328.

Quantum Computer Simulator

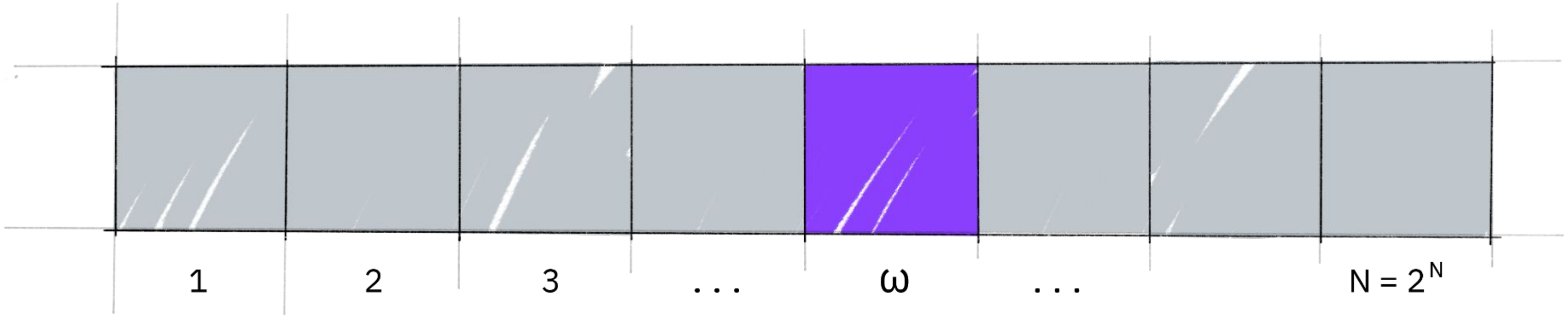
- In the design stage of the quantum algorithm, it is necessary to use a quantum computer simulator to test or debug the quantum algorithm.
- The quantum computer simulator is to simulate the behavior of the quantum computer in the way of mathematical calculation on the classical computer, so the error rate of the quantum computer simulator is extremely low.



ACAN Laboratory

Grover’s Algorithm

- Grover's algorithm, also known as quantum search algorithm was proposed by Indian-American computing scientist Grover in 1996.
- Grover's algorithm can find specific element in unstructured list, speeding up an unstructured search problem quadratically.

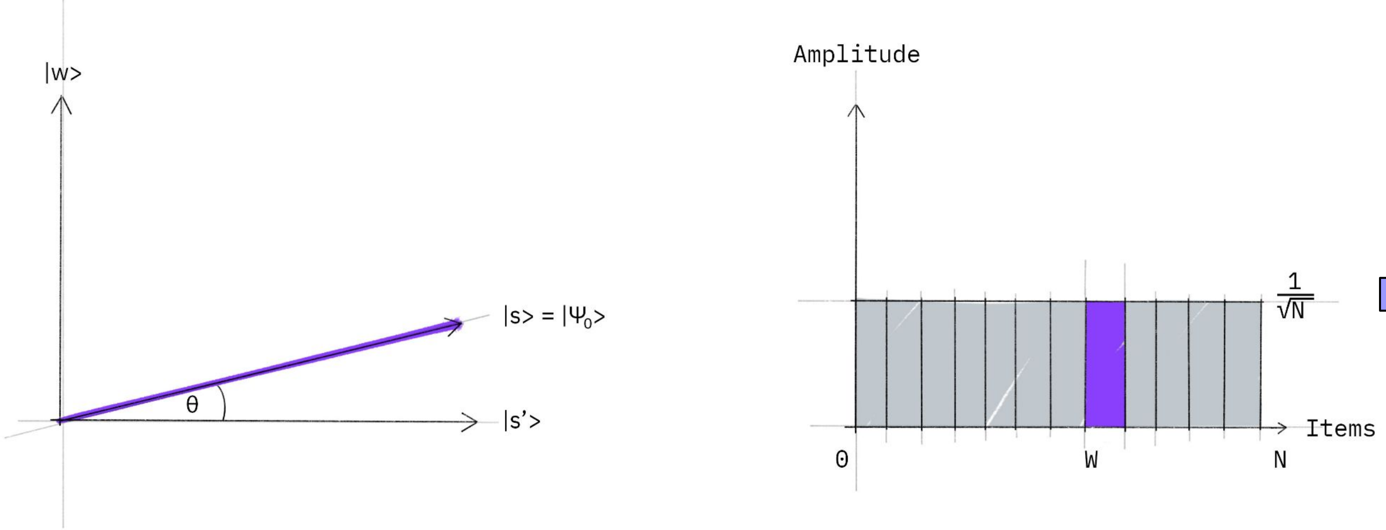


$$U_\omega|x\rangle = \begin{cases} |x\rangle & \text{if } x \neq \omega \\ -|x\rangle & \text{if } x = \omega \end{cases}$$

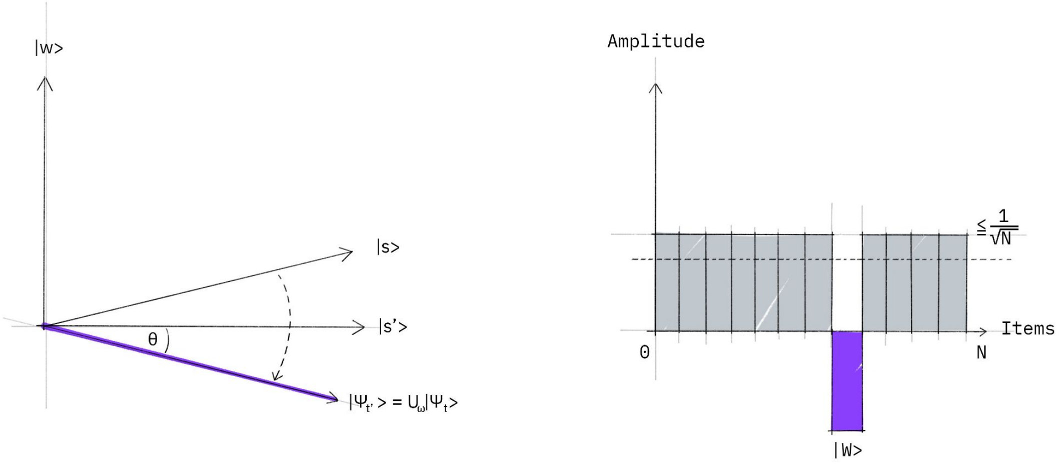
Reference : Grover, L. K. (1996, July). A fast quantum mechanical algorithm for database search. In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing (pp. 212-219).

Amplitude Amplification

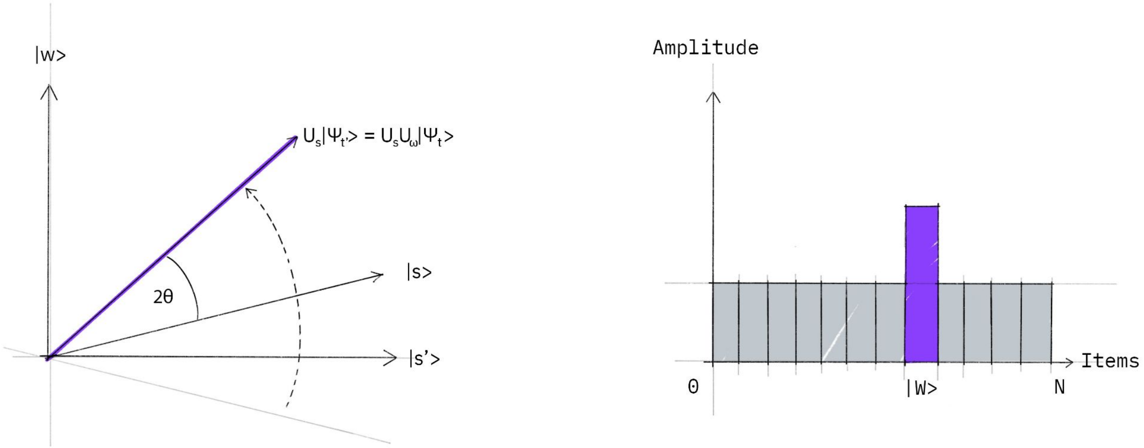
1.



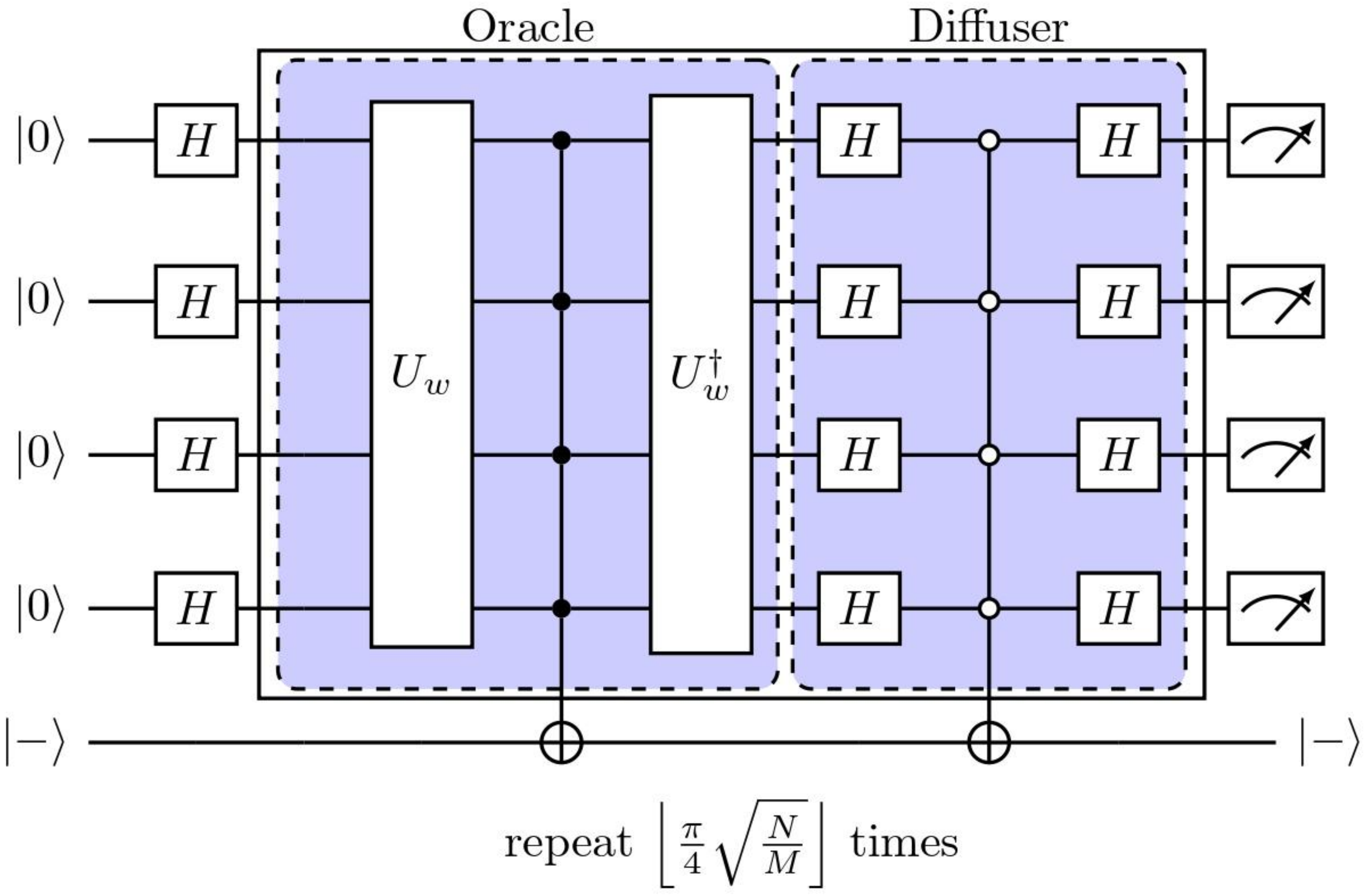
2.



3.



Grover's Algorithm Overview



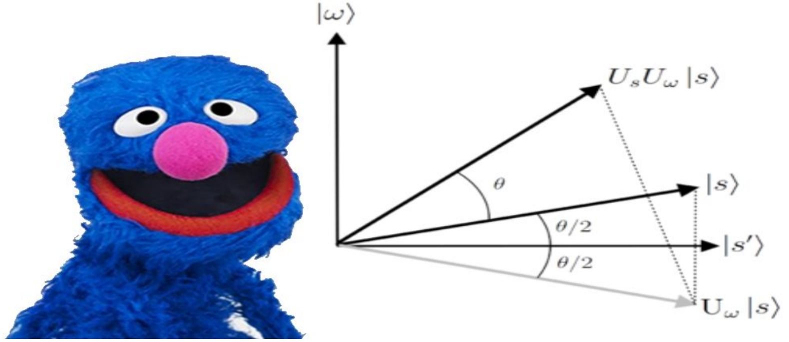
N : possible computational states
M : solution numbers

Quantum Counting Algorithm

- Whereas Grover's algorithm attempts to find a solution to the Oracle, the quantum counting algorithm tells us how many of these solutions there are.
- In quantum counting, we simply use the quantum phase estimation algorithm to find an eigenvalue of a Grover search iteration.

$$\text{repeat } \left\lfloor \frac{\pi}{4}\sqrt{\frac{N}{M}} \right\rfloor \text{ times}$$

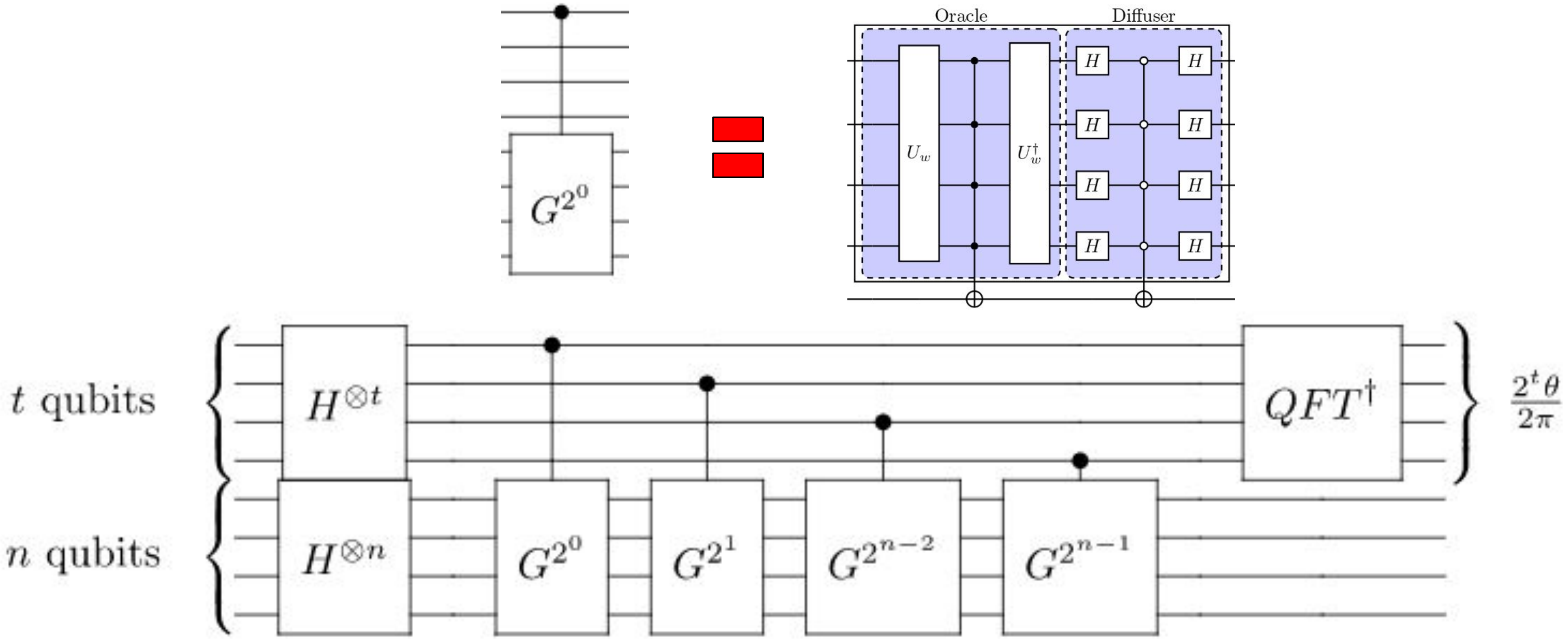
Grover can't find the state in the database,
can you help him??



Reference : Brassard, G., Høyer, P., & Tapp, A. (1998). Quantum counting. In Automata, Languages and Programming: 25th International Colloquium, ICALP'98 Aalborg, Denmark, July 13–17, 1998 Proceedings 25 (pp. 820-831). Springer Berlin Heidelberg.

Quantum Counting Algorithm

- Moreover, this algorithm solves the quantum existence problem (namely, deciding whether any solution exists) as a special case.



Outline

- Introduction
- Background knowledge
- Related Works
- Proposed Method
- Experiment and Result
- Conclusion

Grover’s Algorithm on NP-hard problems

- K - coloring problem[1] : design quantum comparator to detect valid colors between vertices.
- Chromatic number problem[2] : use quantum counting algorithm to find K efficiently.
- List coloring problem[3] : proposed restricted Grover’s search to reduce solution space from 2^n to coloring lists.
- Finding Nash Equilibria problem[4] : transform Nash Equilibria problem to SAT problem and solved by IBM Qiskit SDK.
- Maximum satisfiability problem[5] : check whether every clauses is TRUE and calculate the TRUE clauses' total number.
- Maximum clique problem[6] : design quantum OR gate to check whether there is a clique in the graph.
- Explicit Hamiltonian cycle problem[7] : proposed the concept of explicit oracle and validate on quantum simulator.
- Intelligent Pharmaceutical Patent Search problem[8] : design constraint satisfaction oracle to compare two non-enumerated Markush structures.

ACAN Laboratory

Related Works

[1] Saha, A., Saha, D., & Chakrabarti, A. (2020, December). Circuit design for k-coloring problem and its implementation on near-term quantum devices. In 2020 IEEE International Symposium on Smart Electronic Systems (iSES)(Formerly iNiS) (pp. 17-22). IEEE.
[2] Lutze, D. (2021). Solving Chromatic Number with Quantum Search and Quantum Counting.
[3] Mukherjee, S. (2022). A grover search-based algorithm for the list coloring problem. IEEE Transactions on Quantum Engineering, 3, 1-8.
[4] Roch, C., Castillo, S. L., & Linnhoff-Popien, C. (2022, March). A Grover based Quantum Algorithm for Finding Pure Nash Equilibria in Graphical Games. In 2022 IEEE 19th International Conference on Software Architecture Companion (ICSA-C) (pp. 147-151). IEEE.
[5] Alasow, A., & Perkowski, M. (2022, May). Quantum Algorithm for Maximum Satisfiability. In 2022 IEEE 52nd International Symposium on Multiple-Valued Logic (ISMVL) (pp. 27-34). IEEE.
[6] Haverly, A., & López, S. (2021, July). Implementation of Grover's Algorithm to Solve the Maximum Clique Problem. In 2021 IEEE Computer Society Annual Symposium on VLSI (ISVLSI) (pp. 441-446). IEEE.
[7] Jehn-Ruey Jiang, "Quantum Circuit Based on Grover Algorithm to Solve Hamiltonian Cycle Problem," accepted to present at IEEE Eurasia Conference on IOT, Communication and Engineering (IEEE ECICE 2022), 2022.
[8] Wang, P. H., Chen, J. H., & Tseng, Y. J. (2022). Intelligent pharmaceutical patent search on a near-term gate-based quantum computer. Scientific Reports, 12(1), 175.

ACAN Laboratory

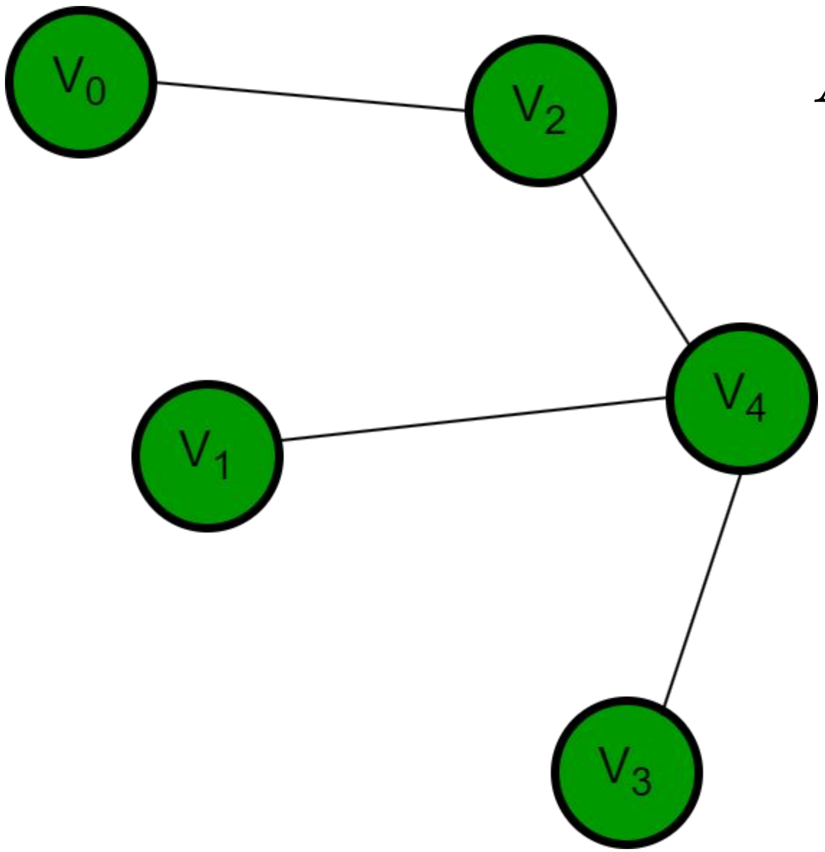
Outline

- Introduction
- Background knowledge
- Related Works
- Proposed Method
- Experiment and Result
- Conclusion

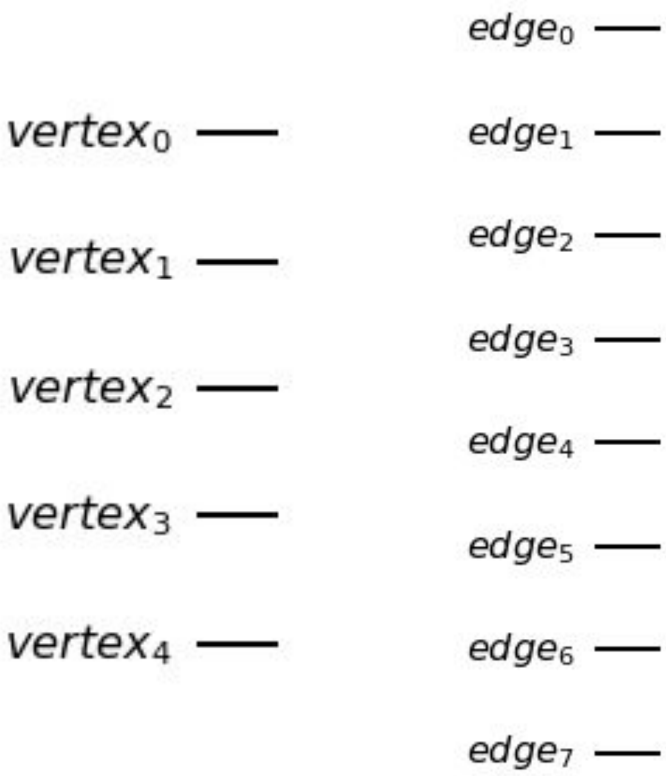
ACAN Laboratory

Input - Undirected Graph

Example G(V,E)



$$A = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$



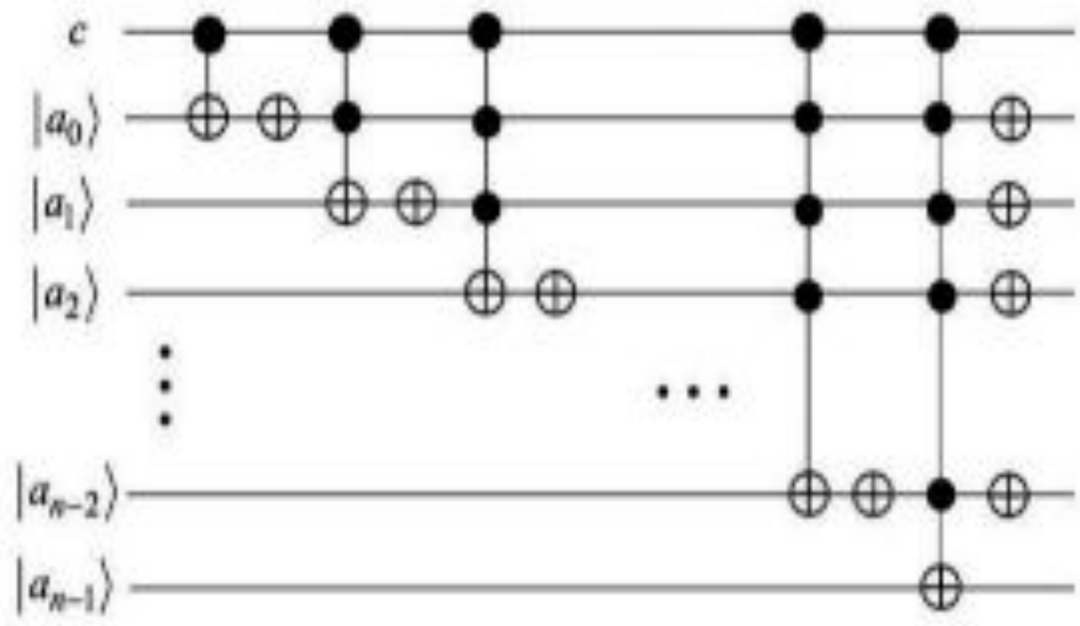
ACAN Laboratory

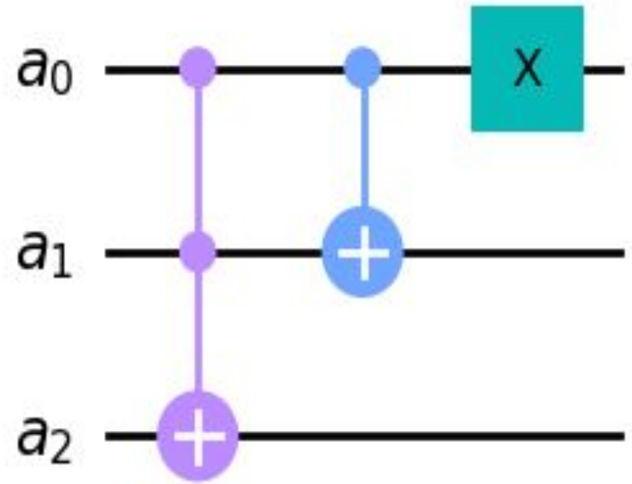
VCP Oracle Construction

Condition :

1. Is the size of the selected vertex set equal to k ?
   - Solution : Quantum Counter
2. Are all the edge marked ?
   - Solution : Quantum Semaphore

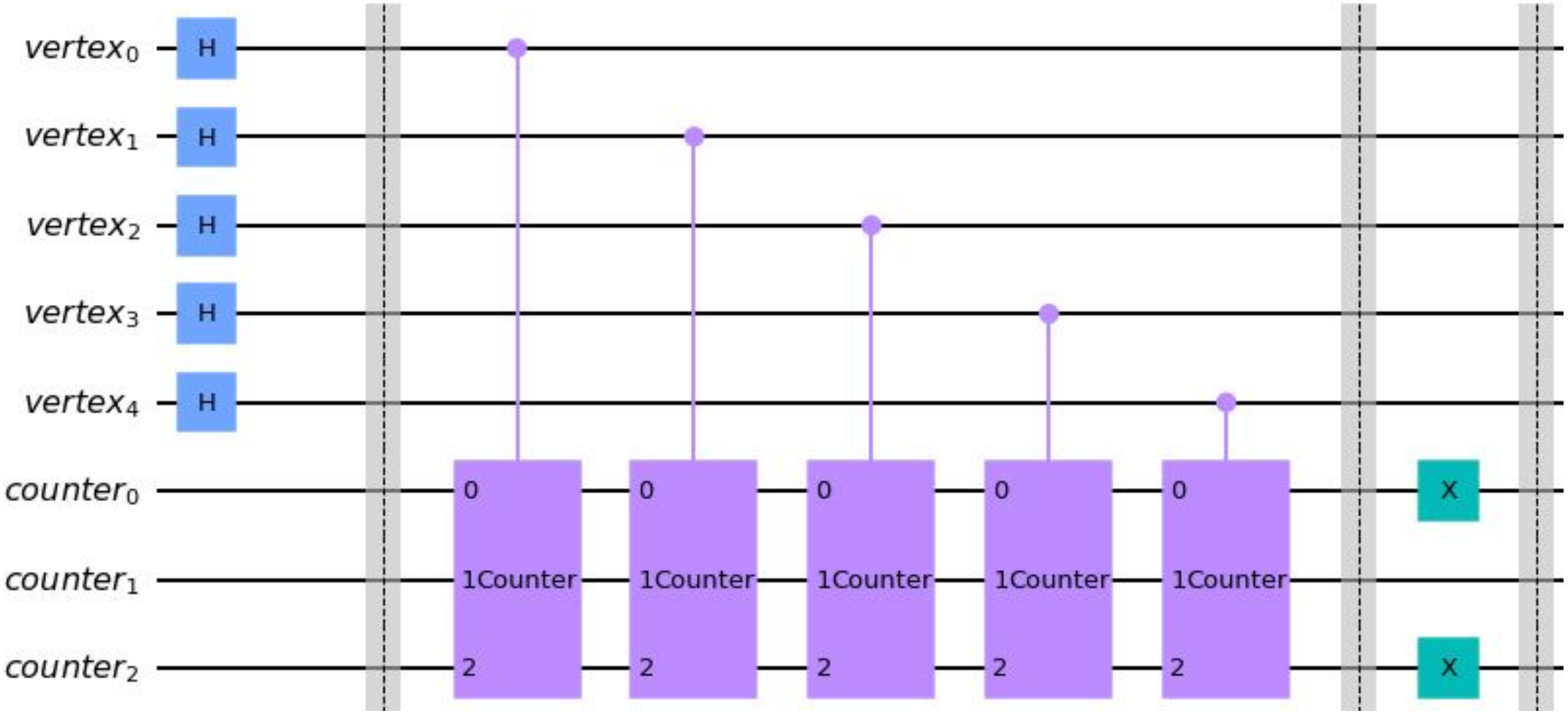
Quantum Counter : Select k vertices





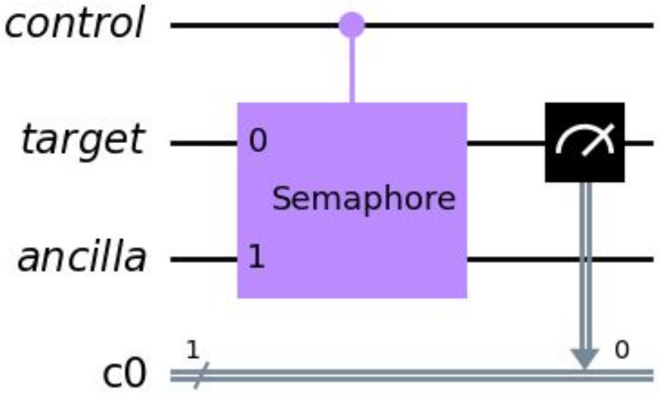
Reference : Heidari, S., & Farzadnia, E. (2017). A novel quantum LSB-based steganography method using the Gray code for colored quantum images. Quantum Information Processing, 16(10), 1-28.

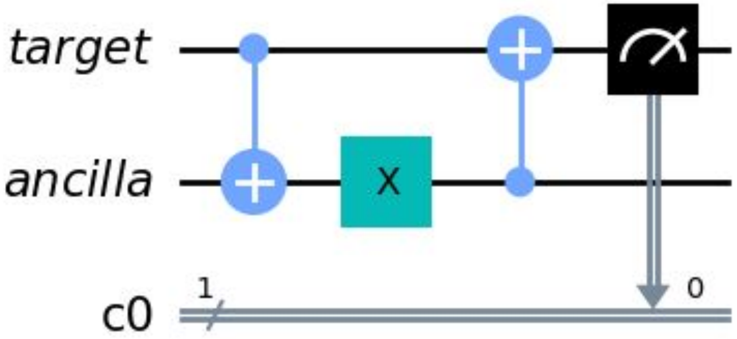
Quantum Counter : Select k vertices



case : k=2

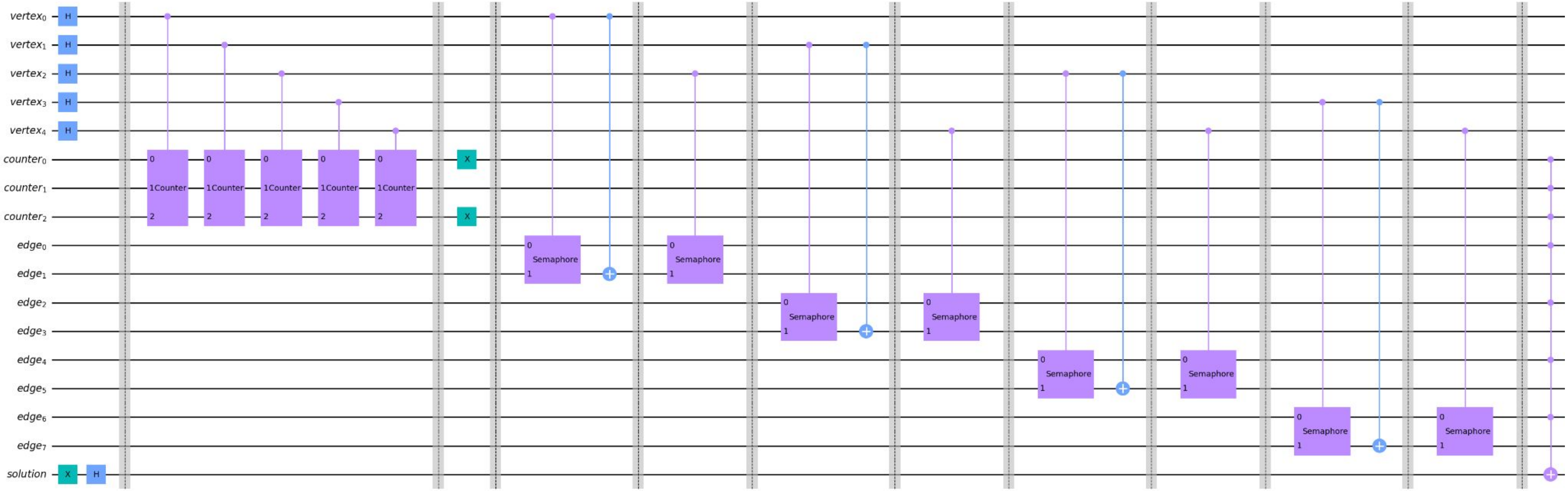
Quantum Semaphore : Mark Edges



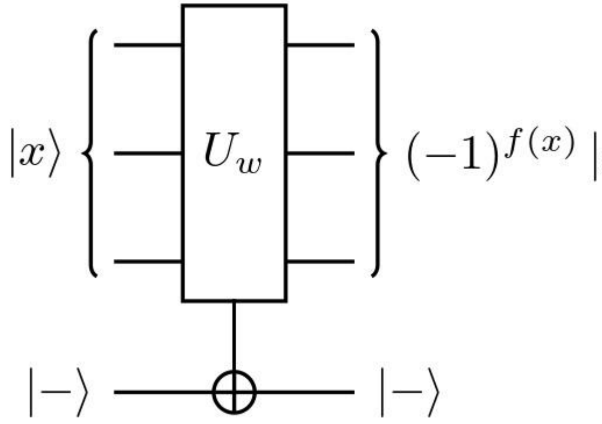


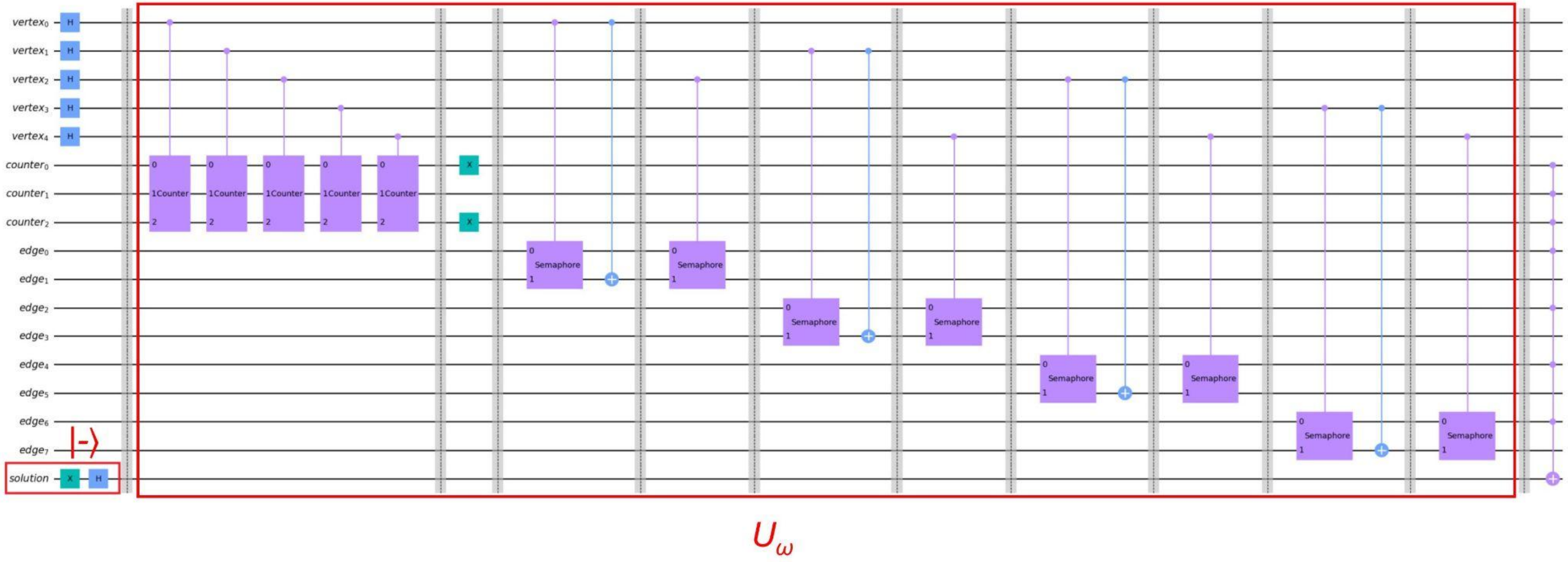
Control bits	Target bits(before)	Target bits(after)
$\|0\rangle$	$\|0\rangle$ or $\|1\rangle$	Do Nothing
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|1\rangle$	$\|1\rangle$

Quantum Semaphore : Mark Edges

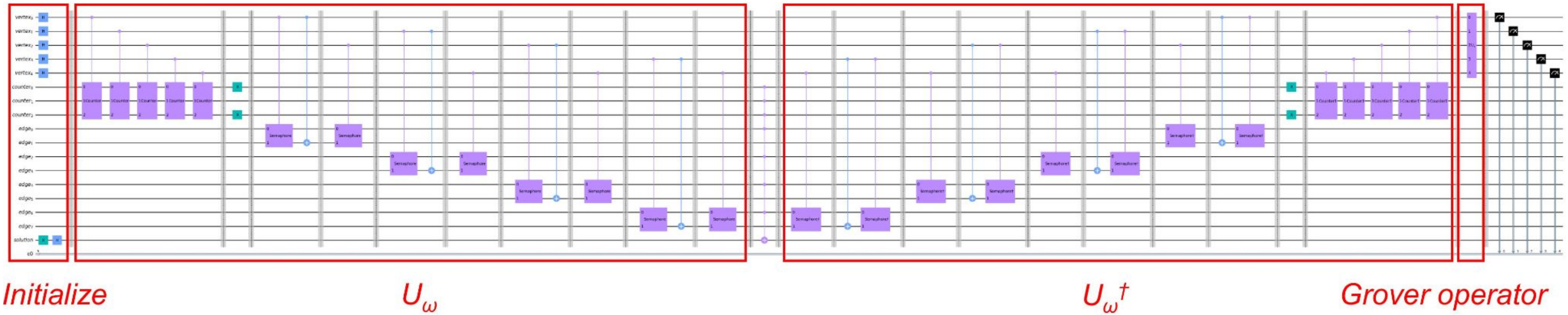


Phase Kickback

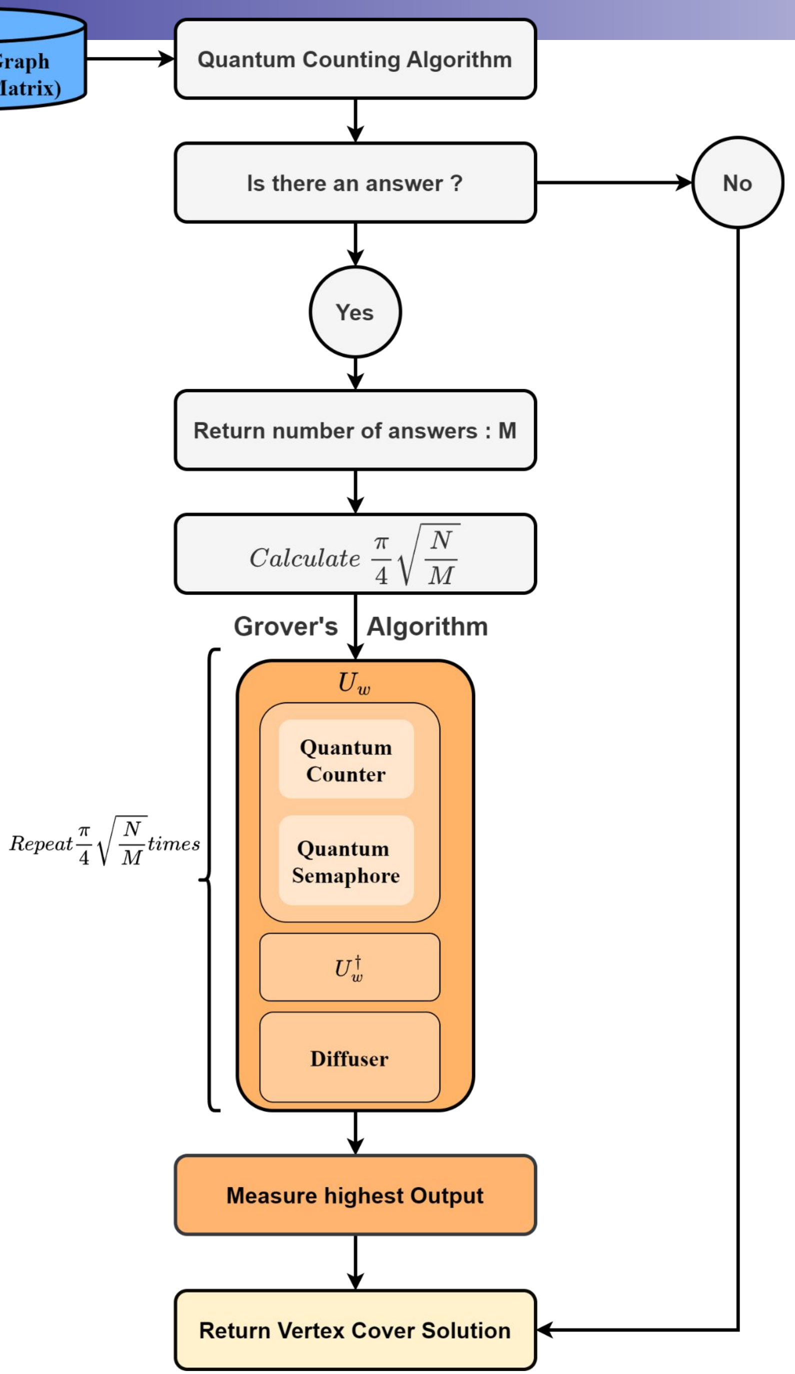




Grover Iteration



Flowchart


Undirected Graph (Adjacency Matrix)
Quantum Counting Algorithm
Is there an answer ?
No
Yes
Return number of answers : M
$Calculate \frac{\pi}{4}\sqrt{\frac{N}{M}}$
Grover's Algorithm
U_w
Quantum Counter
Quantum Semaphore
$U_w^\dagger$
Diffuser
$Repeat \frac{\pi}{4}\sqrt{\frac{N}{M}} times$
Measure highest Output
Return Vertex Cover Solution

ACAN Laboratory

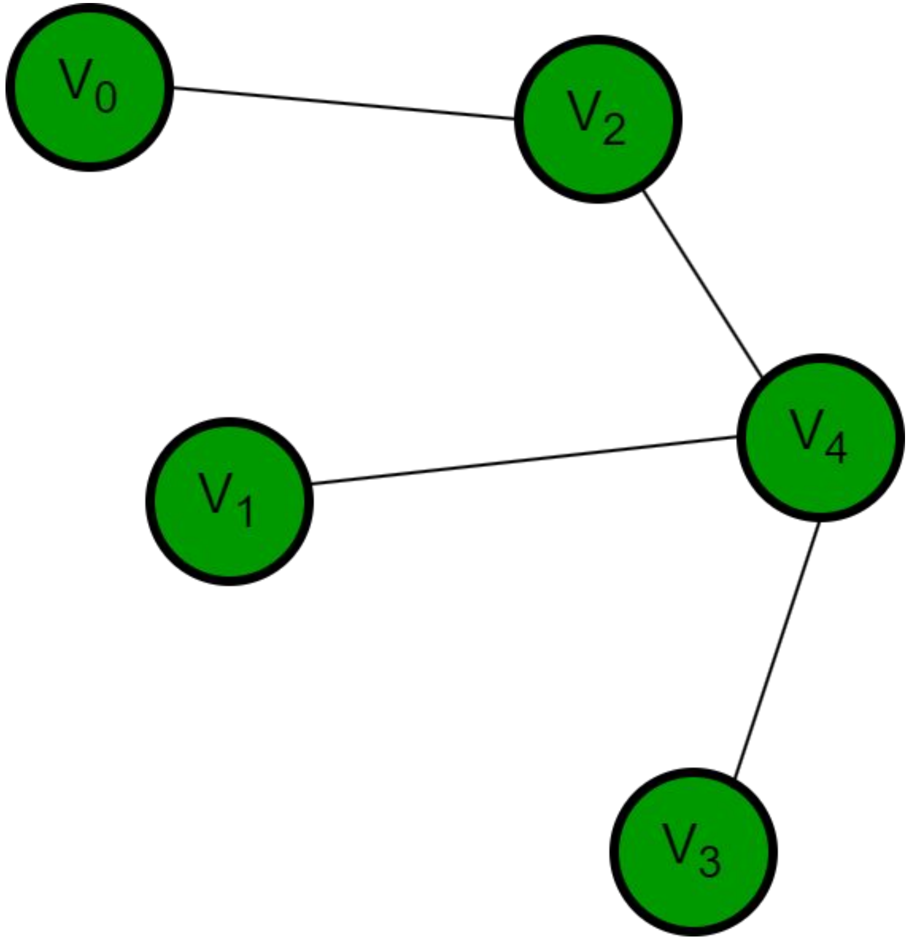
Outline

- Introduction
- Background knowledge
- Related Works
- Proposed Method
- Experiment and Result
- Conclusion

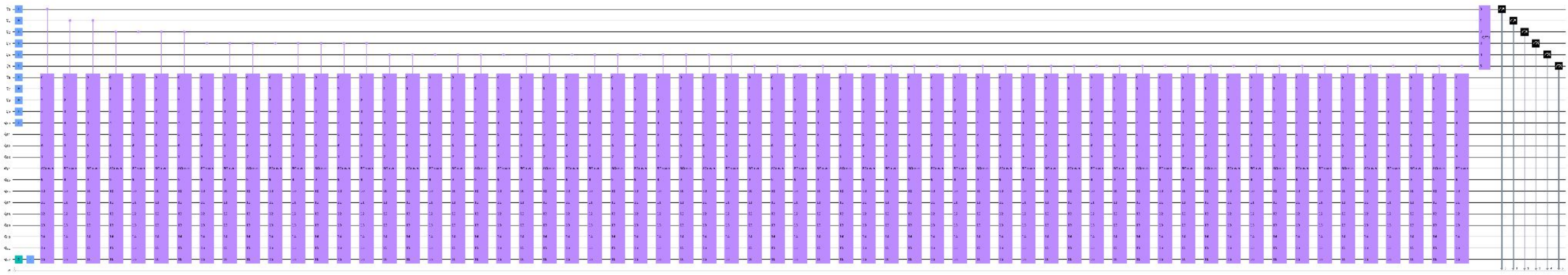
ACAN Laboratory

Device :Quantum Computer Simulator

case : k=2

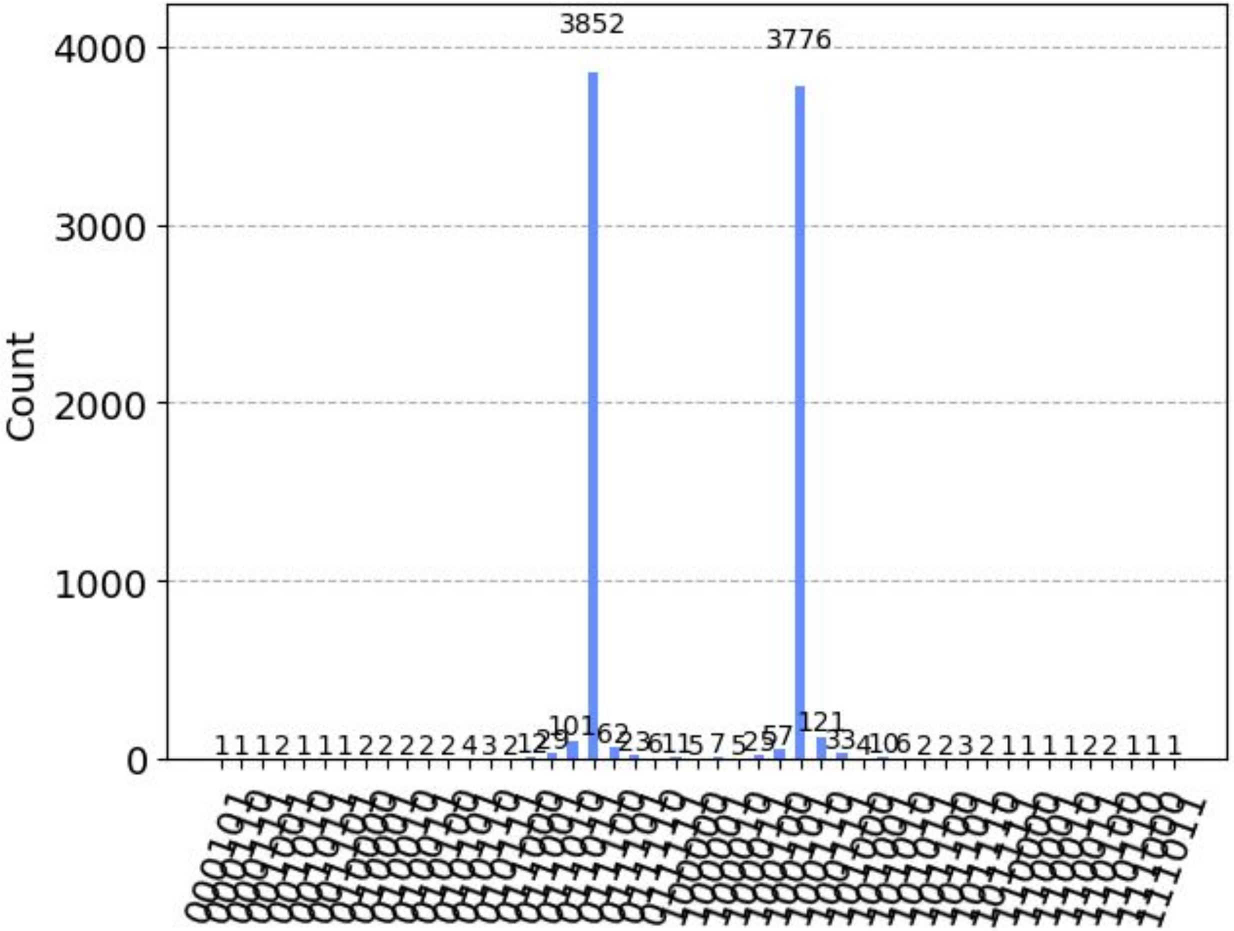


Quantum Counting Circuit



Counting bits : 6

Quantum Counting Result



Proposed Method

$N = 2^5 = 32$

$$e^{\pm i\theta}$$

Register Output = 27

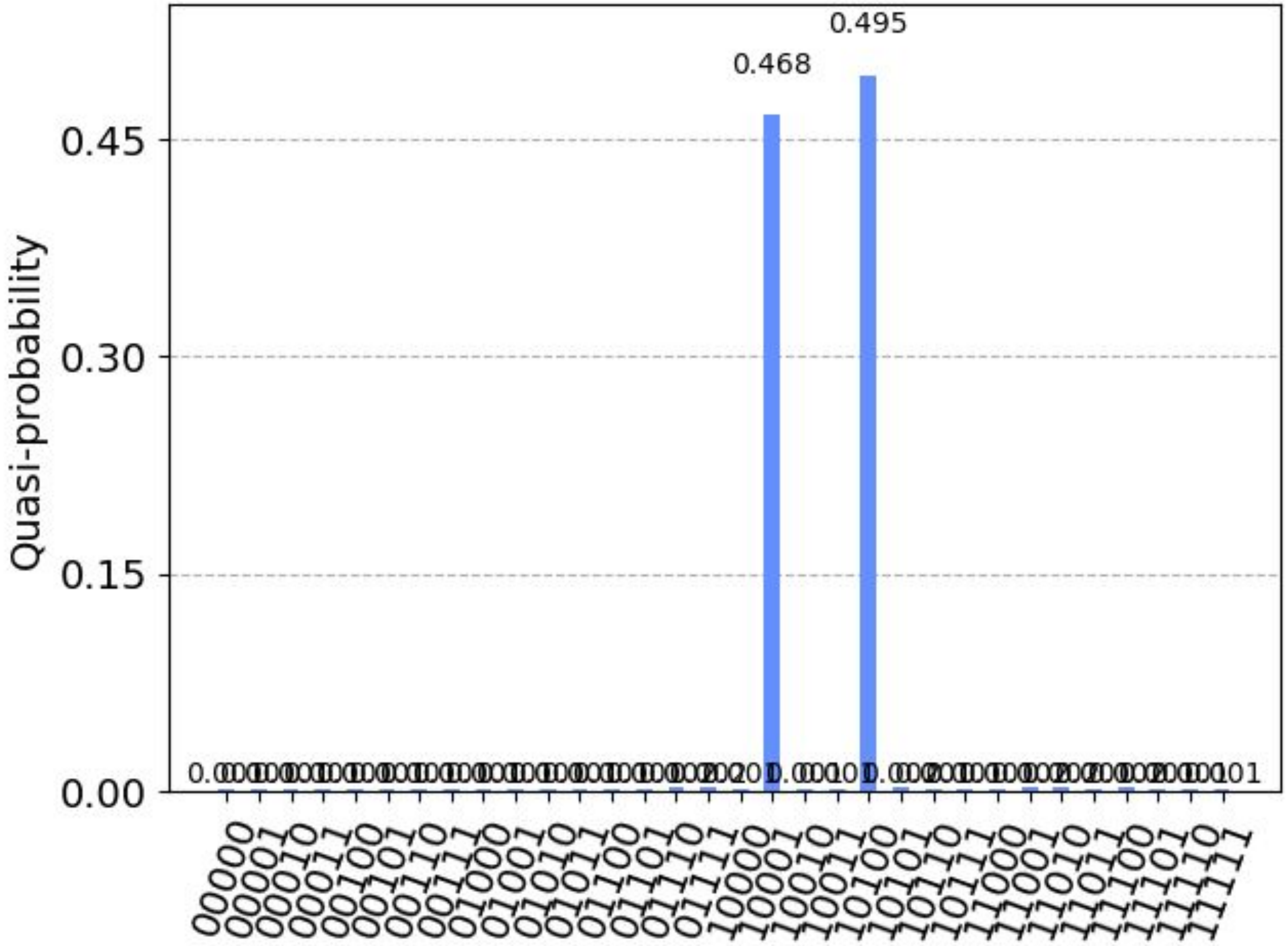
Theta ≈ 2.65072

$$\Rightarrow \quad N\cos^2\frac{\theta}{2} = M \quad = 1.9$$

$$\Rightarrow \quad \left\lfloor \frac{\pi}{4}\sqrt{\frac{N}{M}} \right\rfloor \quad = 3$$

ACAN Laboratory

Grover's Algorithm Result

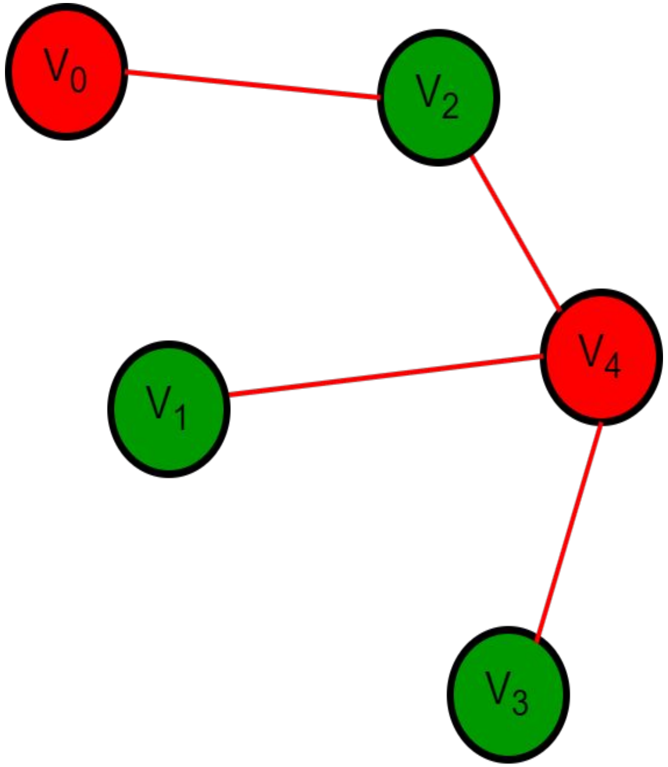


$|V_4V_3V_2V_1V_0\rangle$

Register Output = '10001','10100'

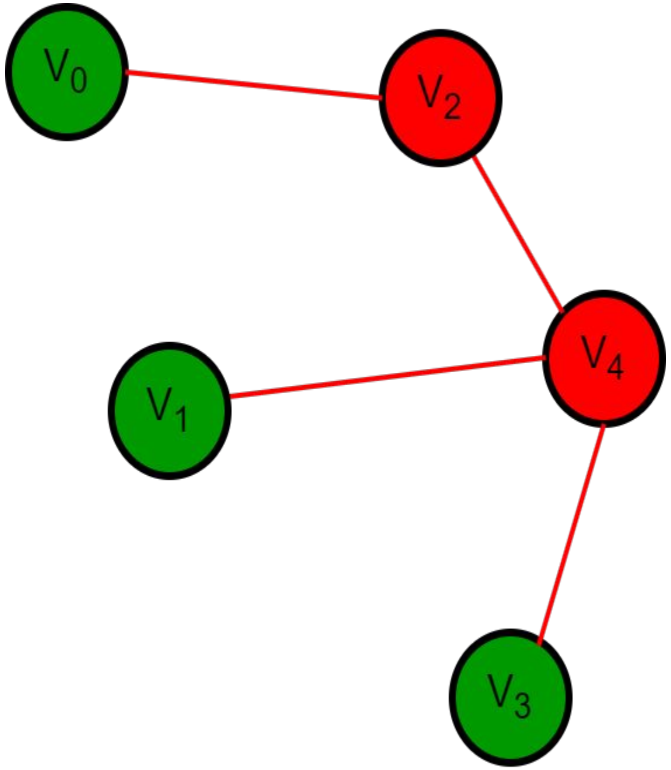
Matching : 'V_4V_0', 'V_4V_2'

Validation Result



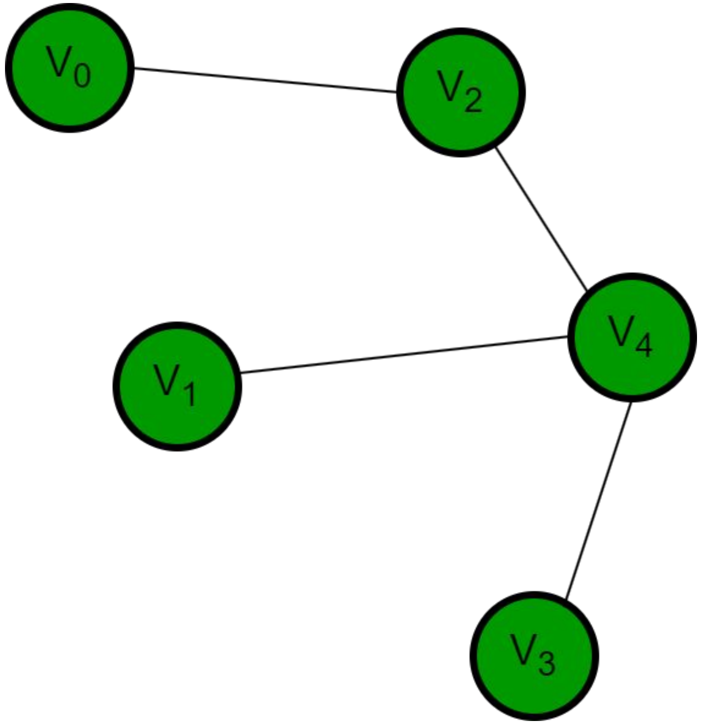
(a)

choose : V_4V_0



(b)

choose : V_4V_2



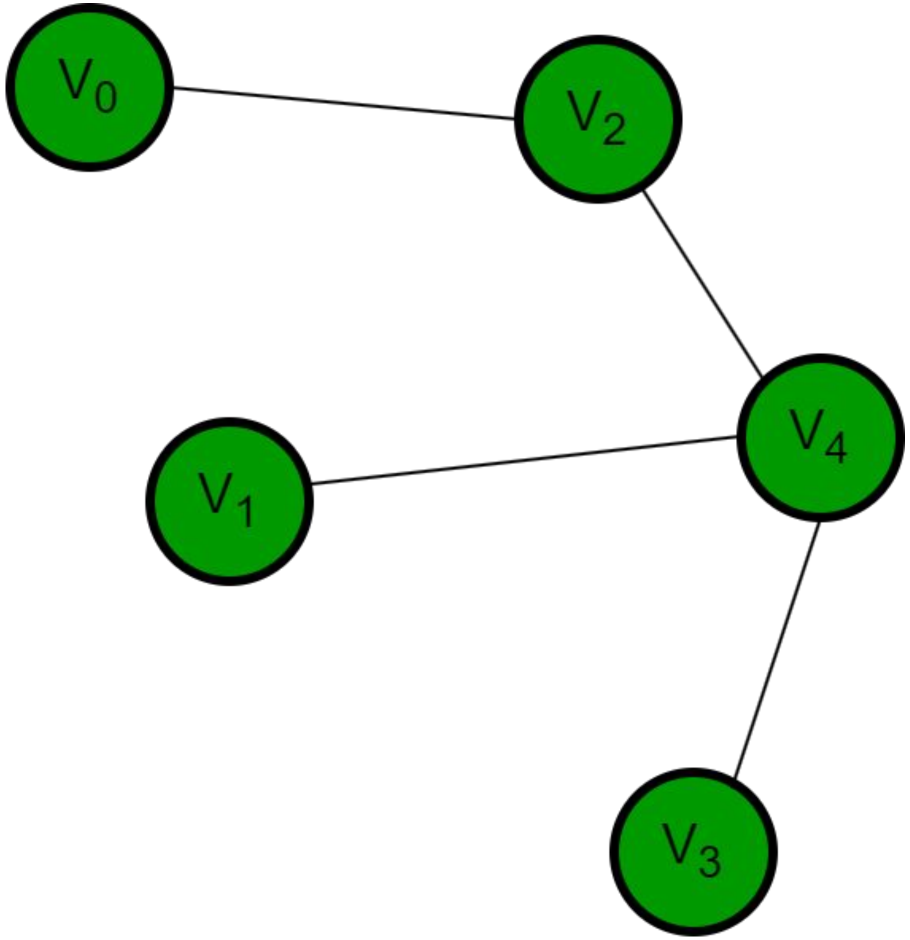
G(V,E)

Correct !

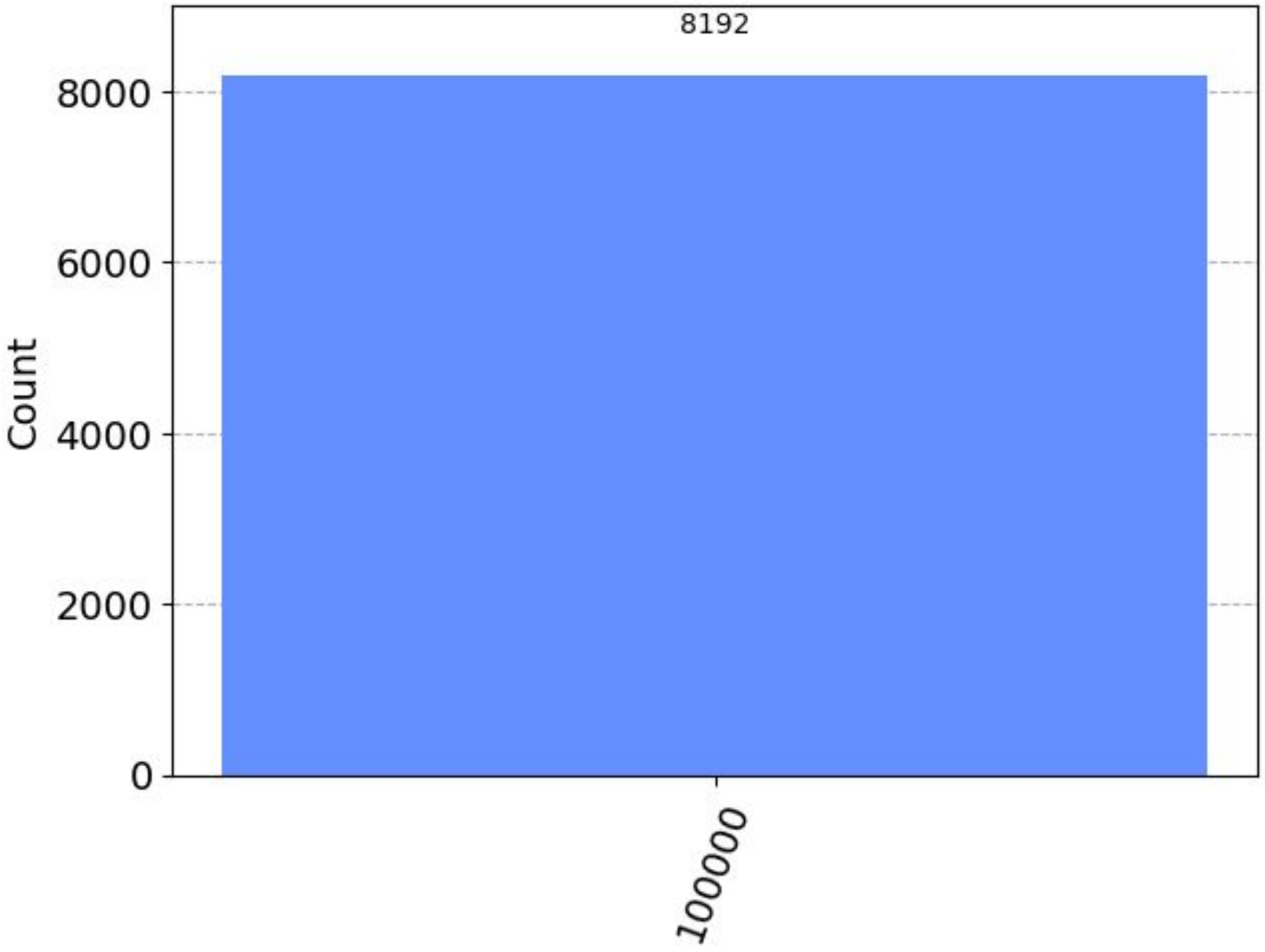
Device :Quantum Computer Simulator

What if ?

case : k=1



Quantum Counting Result



Proposed Method

$N = 2^5 = 32$

Register Output = 32

Theta ≈ 3.14159….

$\Rightarrow \quad N\cos^2\frac{\theta}{2} = M = 0$

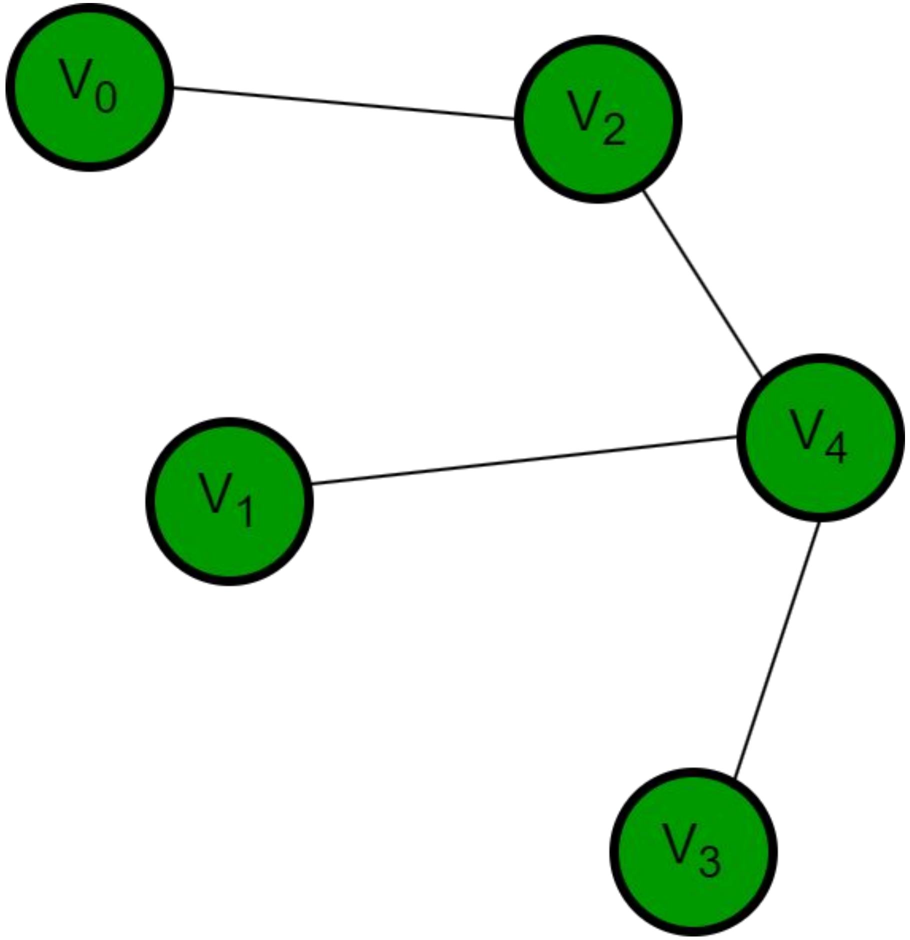
No Answer !

Device : Quantum Computer

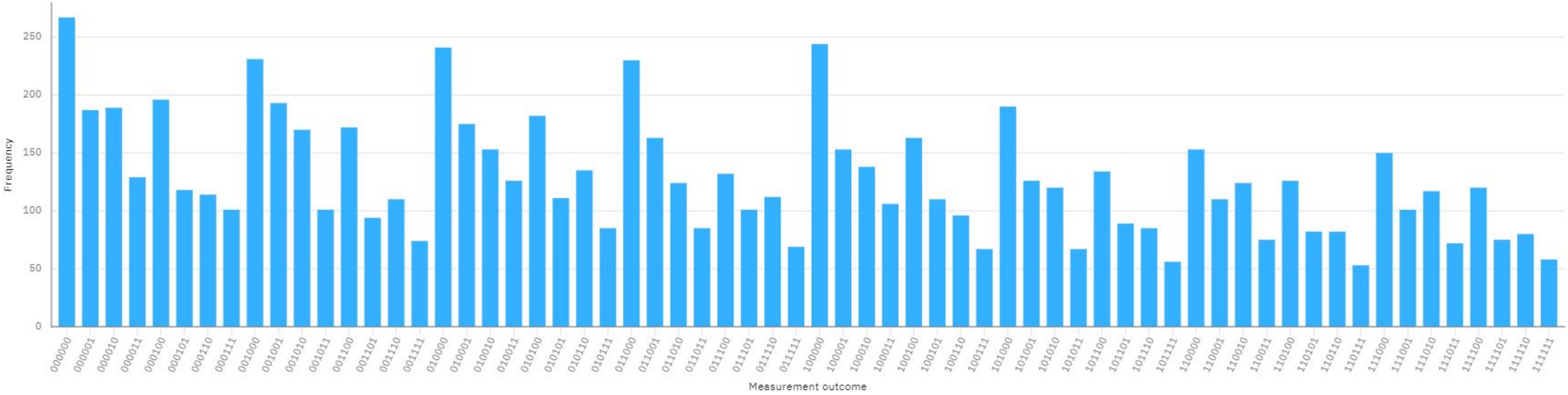
Device Name :“ibmq_mumbai"

Qubits : 27

Quantum Volume : 128

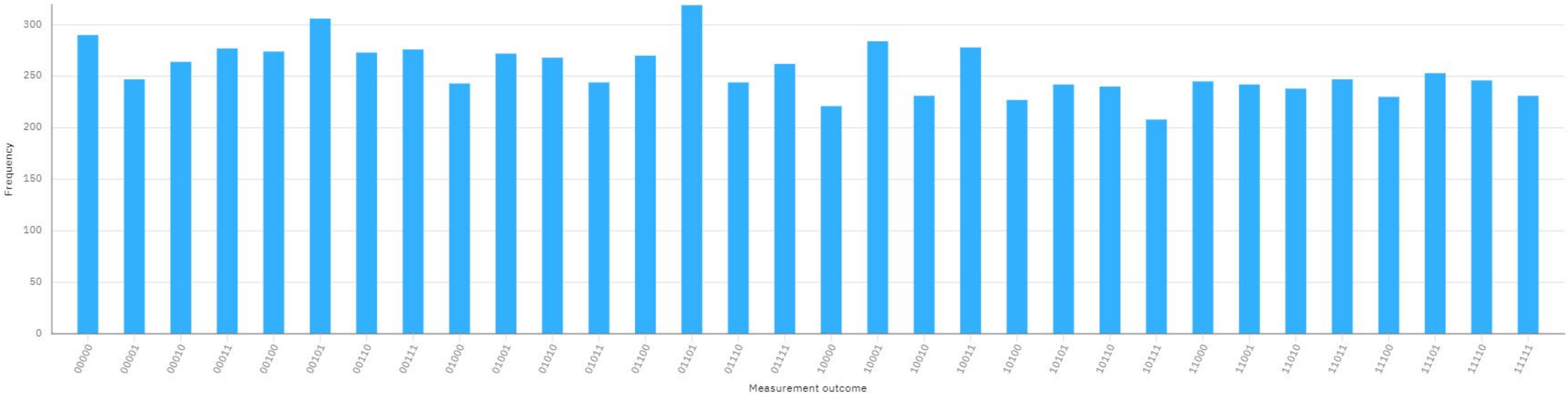


Quantum Counting Result (k=2)



No Heavy Outputs !

Grover's Algorithm Result (k=2)



No Heavy Outputs !

Scalability

Vertex	Edge	k	Qubits	Quantum Gate Counts				Depth
				CX	RZ	SX	X	
5	4	2	17	8309	5003	828	12	10834
5	4	3	17	2586	1678	280	2	3532
6	6	2	22	23514	12831	1367	16	27514
6	6	3	22	11074	6419	687	4	13801
6	7	3	24	32975	19285	1431	8	37917
6	7	4	24	18407	9651	719	8	19639

Related Works

- Fixed Parameter Algorithm
- Exhausted Search Algorithm

Reference :Chen, J., Kanj, I. A., & Xia, G. (2010). Improved upper bounds for vertex cover. Theoretical Computer Science, 411(40-42), 3736-3756.

Circuit Cost

Item	Qubits Cost
Vertex	$\|V\|$
Quantum Counter	$\lfloor \log_2\|V\| \rfloor +1$
Quantum Semaphore	$2\|E\|$
Solution Qubit	1
Total	$\|V\|+\lfloor \log_2\|V\| \rfloor + 2\|E\| + 2$

ACAN Laboratory

Time Complexity

Algorithm	Big O notation	Computing
Exhausted Search Algorithm	$O(2^{\|V\|})$	Classical
Fixed Parameter Algorithm	$O(1.2738^k+kn)$	Classical
Proposed Method	$O(\sqrt{2^{\|V\|}})$	Quantum

Reference :Chen, J., Kanj, I. A., & Xia, G. (2010). Improved upper bounds for vertex cover. Theoretical Computer Science, 411(40-42), 3736-3756.

ACAN Laboratory

Outline

- Introduction
- Background knowledge
- Related Works
- Proposed Method
- Experiment and Result
- Conclusion

Conclusion

- We design the oracle for the Grover's algorithm to solve the vertex cover problem, improving the existing quantum counter and design the quantum semaphore.
- The results are verified on both the IBM quantum simulator and IBM quantum computer.

Future Work

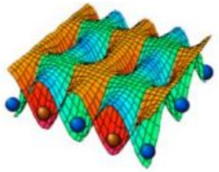
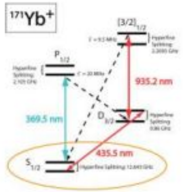
- When robust quantum hardware with more qubits appears, the method proposed in this paper can be practically applied to solve vertex cover application problems in the real world.
- Try to apply different quantum circuit optimization to find the best balance between usage of qubits and quantum circuit depth.

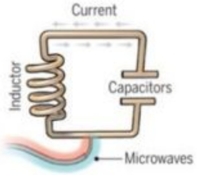
THANK YOU FOR LISTENING !

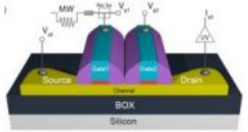
Q & A

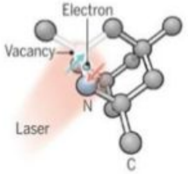
Appendix

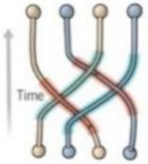
Qubits

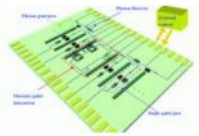













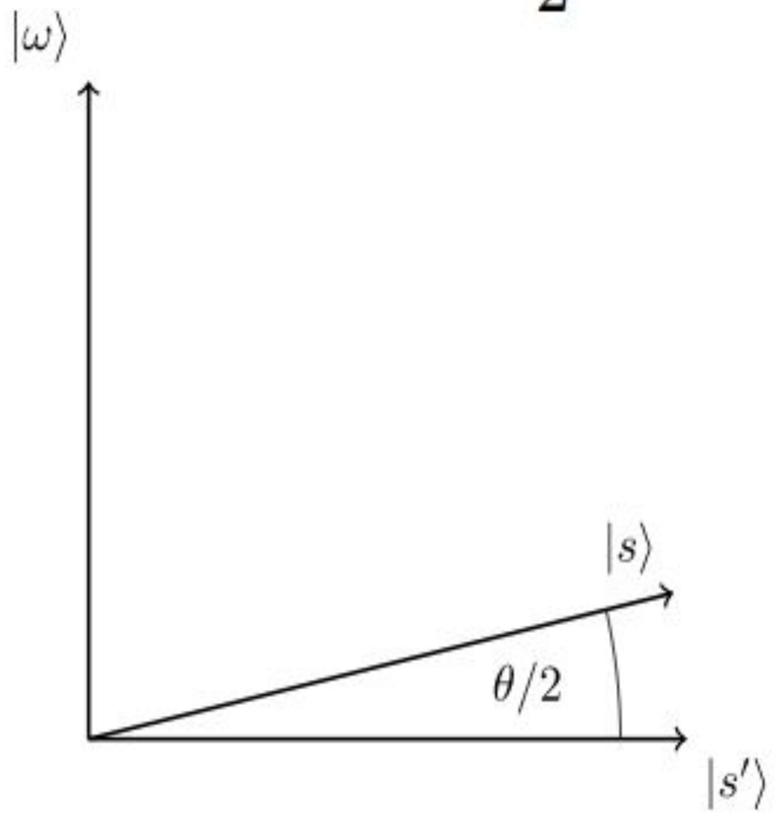
	atoms		electrons superconducting & spins				photons
	cold atoms	trapped ions	superconducting	silicon	NV centers	Majorana fermions	photons
qubit size	about 1 µm space between atoms	about 1 µm space between atoms	$(100\mu)^2$	$(100nm)^2$	$<(100nm)^2$	$(100\mu)^2$	$(100\mu)^2$
two gates fidelities	98%	99,9%	99,4%	>98%	99,2%	N/A	98%
readout fidelity	99%	99,9%	99,4%	98%	98%	N/A	50%
gate time	1 µs	100 µs	20 ns - 300 ns	≈5 µs	10-700 ns	N/A	1 ms
coherence		0,2s-10mn	100-400µs	20-120µs	2.4 ms	N/A	
qubits temperature	< 5mK	<1mK to 10K	15mK	100mK-1K	4K-ambiant	15mK	ambiant & 4K/10K photons generators & detectors
operational qubits	100-196 (simulator)	32 (IonQ)	65 (IBM) 56-66 (China)	4 (Delft)	5 (Quantum Brilliance)-10	N/A	70 (China)
scalability	1000	<50	100s	millions	100s	?	100s-1M

Source: Ezratty, O. (2021). Understanding Quantum Technologies. le lab quantique.

ACAN Laboratory

Finding the Number of Solutions - M

$$\theta = \text{value} \times \frac{2\pi}{2^t}$$



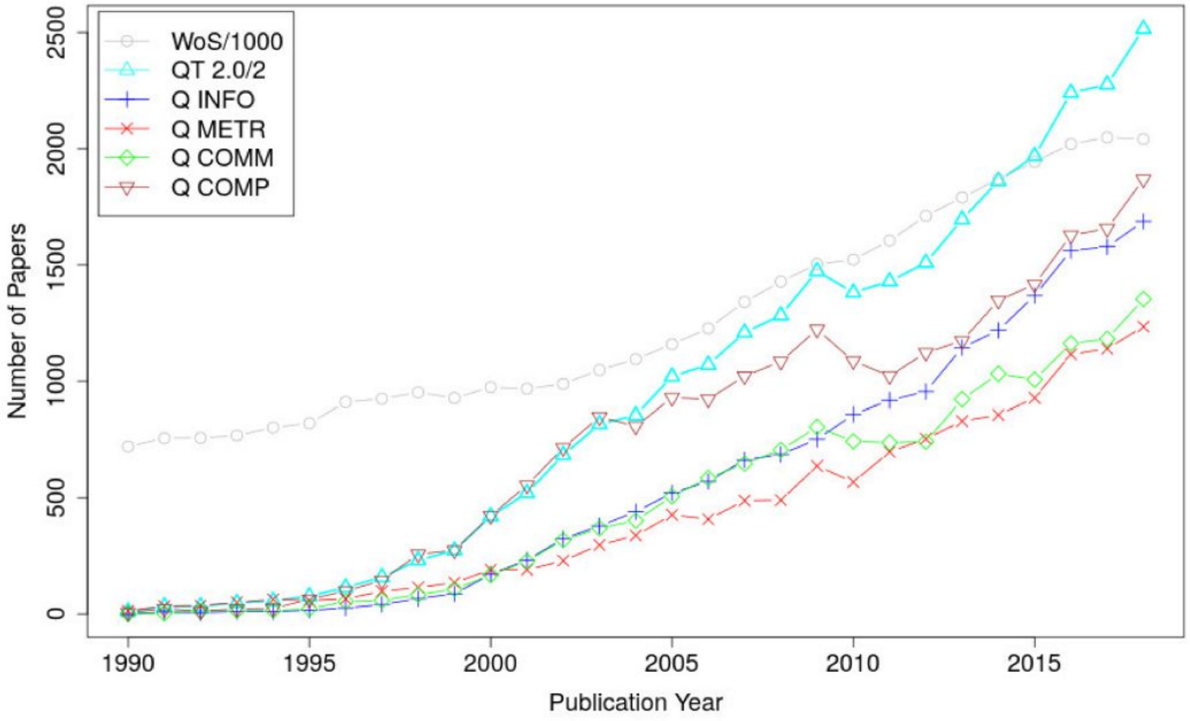
$$|s\rangle = \sqrt{\tfrac{M}{N}}|\omega\rangle + \sqrt{\tfrac{N-M}{N}}|s'\rangle$$

$$\Rightarrow \quad \langle s'|s\rangle = \sqrt{\frac{N-M}{N}} = \cos\frac{\theta}{2}$$

$$\Rightarrow \quad N\cos^2\frac{\theta}{2} = M$$

Quantum Computing Trend

- According to the database of Web of Science (WoS), whether it is in quantum information science, quantum metrology, quantum communication or the main axis of this paper -quantum computing.
- The number of publications is showing a growing trend.

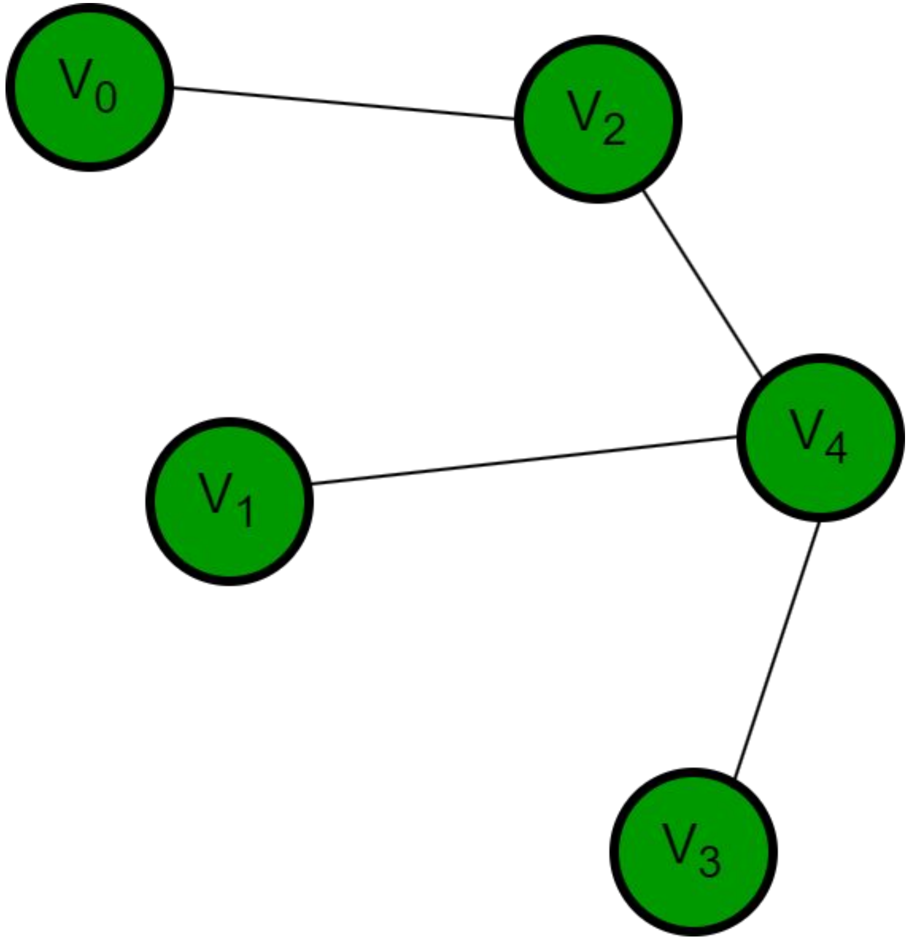


Reference : Scheidsteger, T., Haunschild, R., Bornmann, L., & Ettl, C. (2021). Bibliometric analysis in the field of quantum technology. Quantum Reports, 3(3), 549-575.

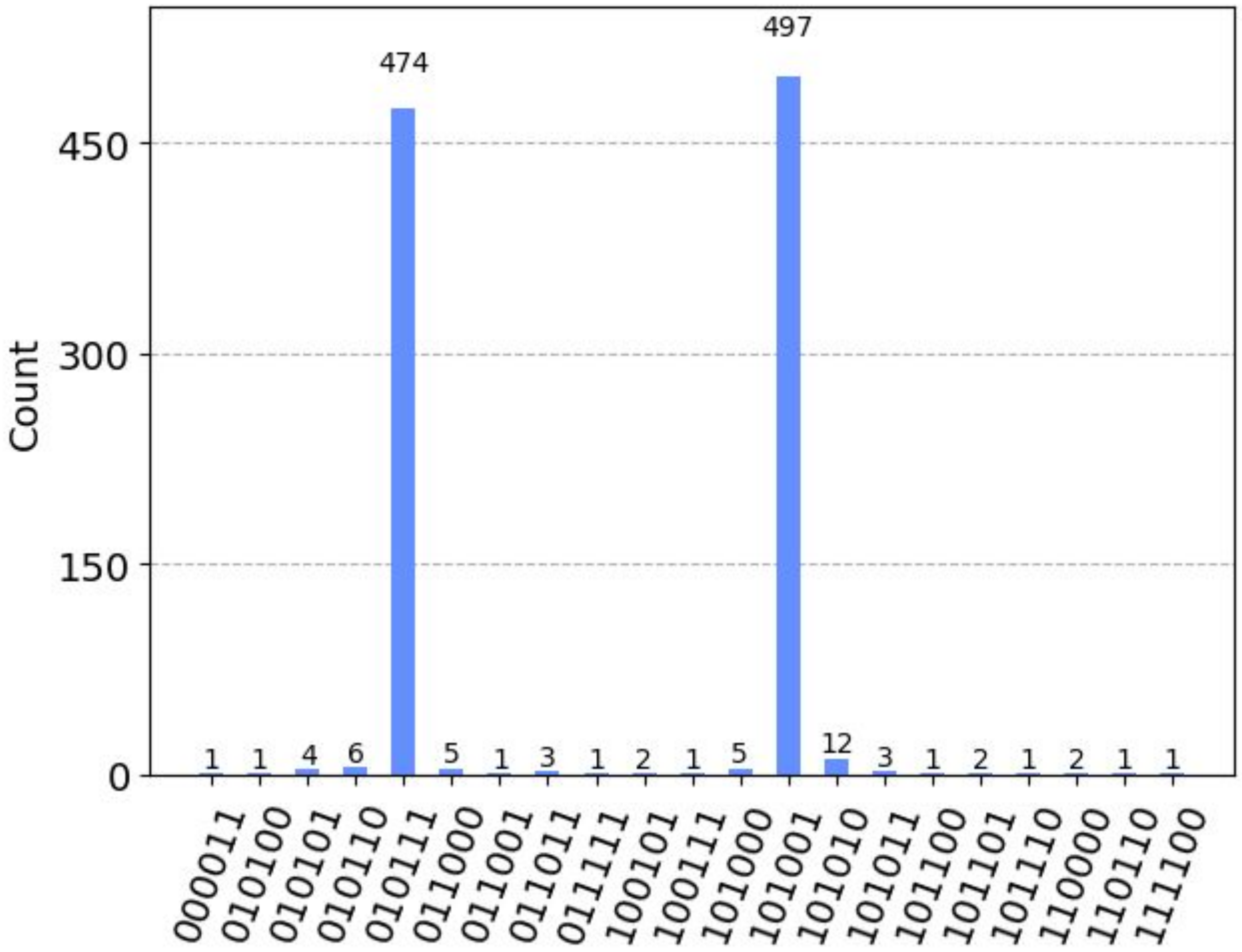
ACAN Laboratory

Device :Quantum Computer Simulator

case : k=3



Quantum Counting Result



Proposed Method

$N = 2^5 = 32$

$e^{\pm i\theta}$

Register Output = 41

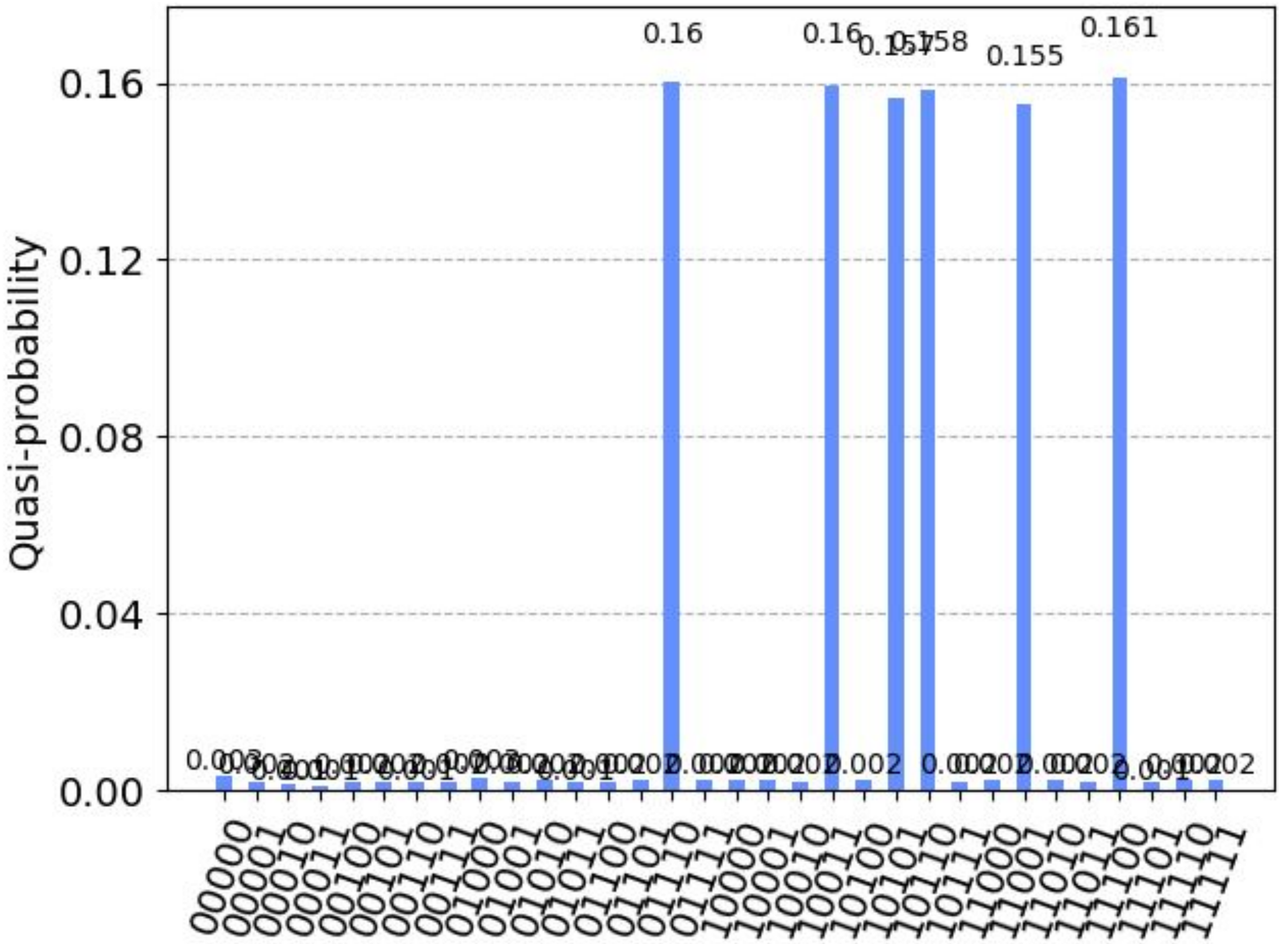
Theta ≈ 4.02517

$\Rightarrow \quad N \cos^2 \frac{\theta}{2} = M$ = 5.8

$\Rightarrow \quad \left\lfloor \frac{\pi}{4} \sqrt{\frac{N}{M}} \right\rfloor$ = 1

ACAN Laboratory

Grover's Algorithm Result



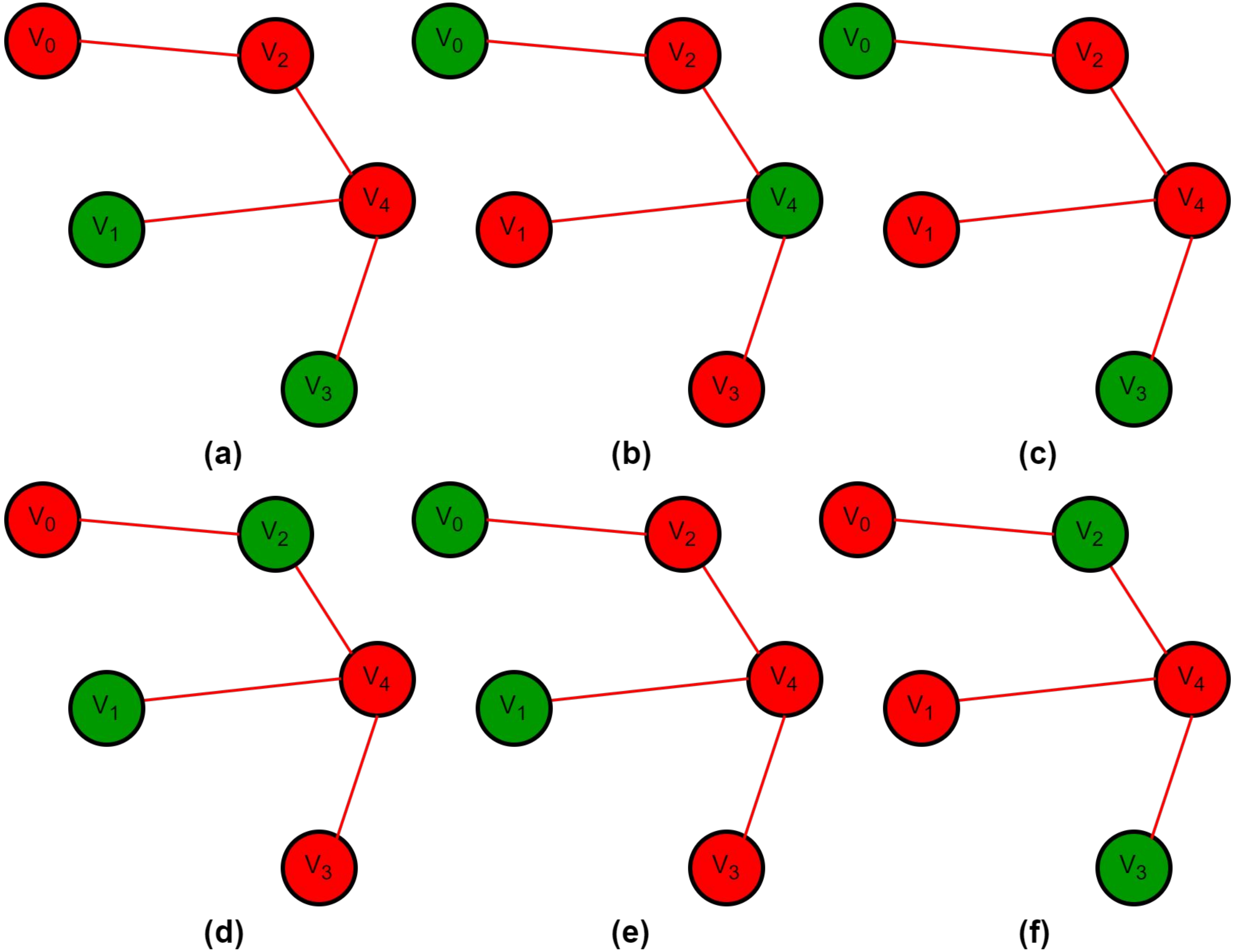
$$\left\lfloor \frac{\pi}{4}\sqrt{\frac{N}{M}} \right\rfloor = 1$$

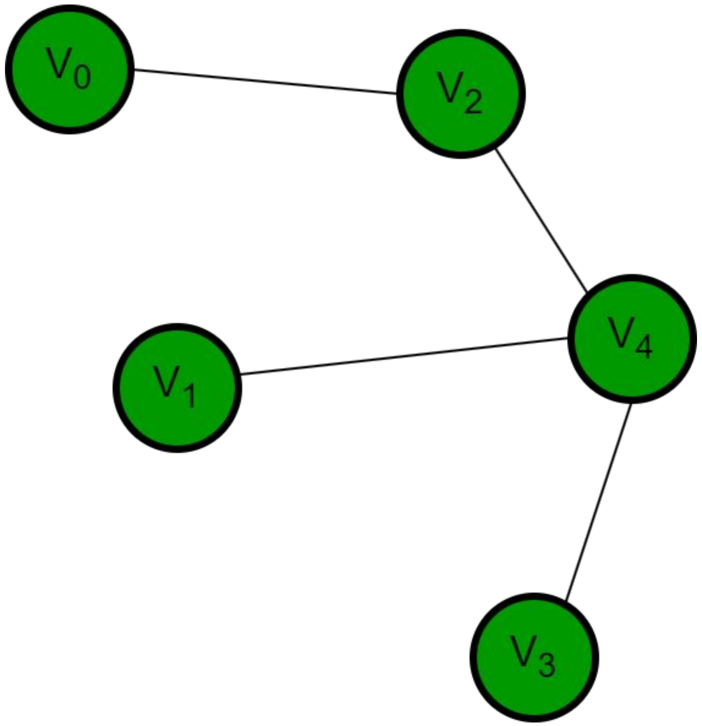
Register Output = '10101','01110', '10110','11001','11100','10011'

Matching : '$V_4V_2V_0$','$V_3V_2V_1$', '$V_4V_2V_1$','$V_4V_3V_0$','$V_4V_3V_2$','$V_4V_1V_0$'

ACAN Laboratory

Validation Result

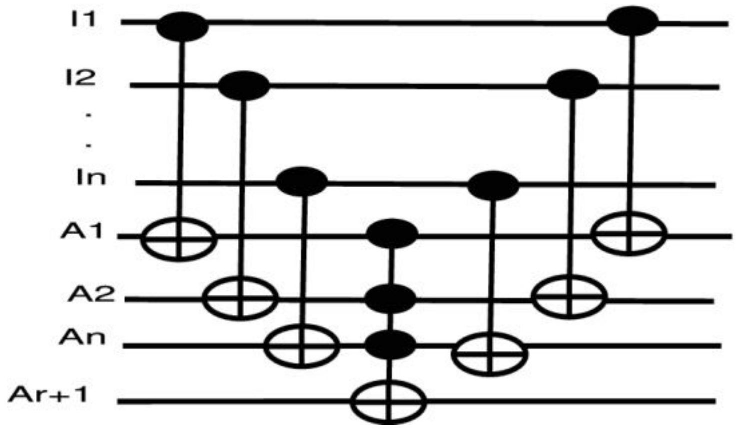




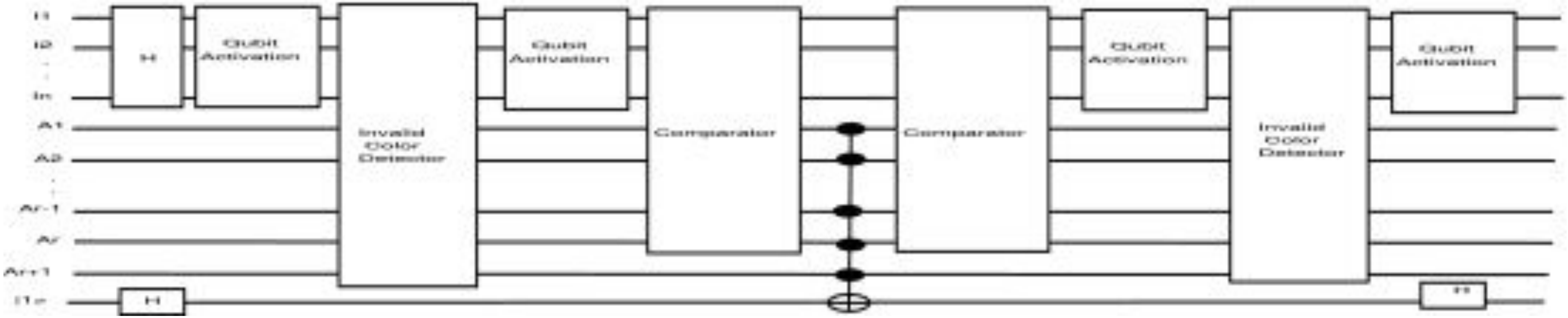
G(V,E)

Correct !

K - coloring problems

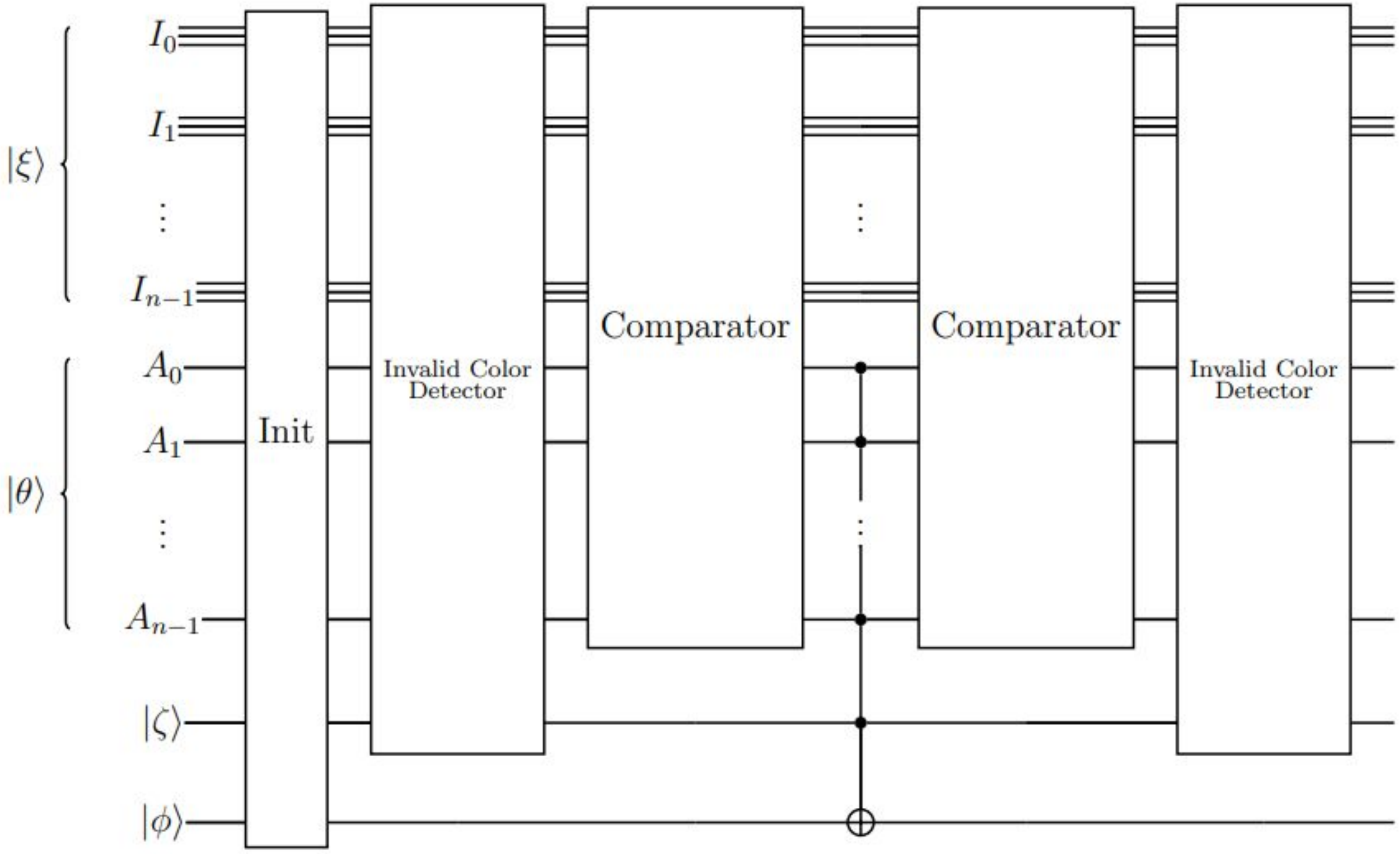


Invalid Color Detector



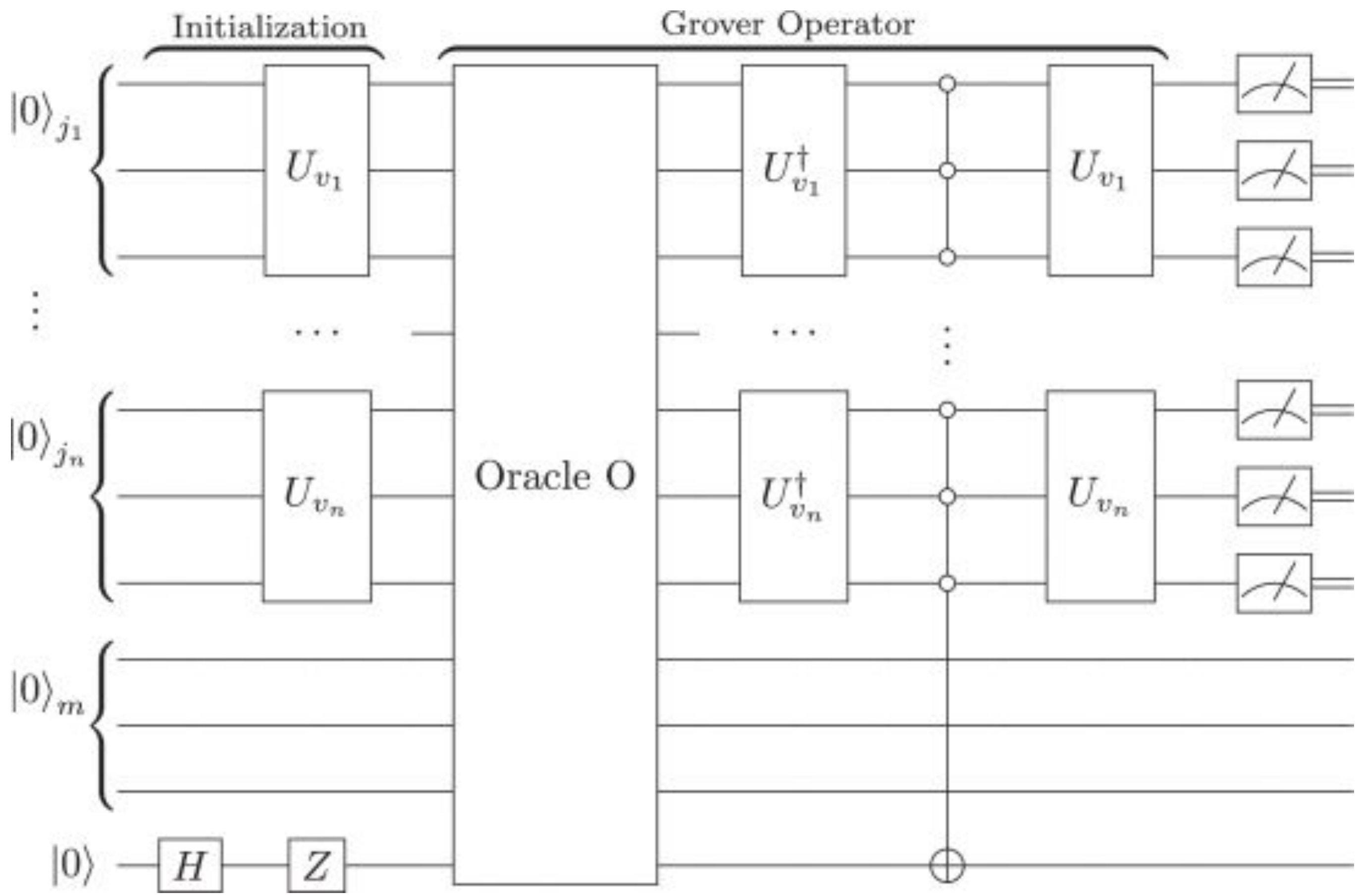
Reference : Saha, A., Saha, D., & Chakrabarti, A. (2020, December). Circuit design for k-coloring problem and its implementation on near-term quantum devices. In 2020 IEEE International Symposium on Smart Electronic Systems (iSES)(Formerly iNiS) (pp. 17-22). IEEE.

Chromatic number problem



Reference : Lutze, D. (2021). Solving Chromatic Number with Quantum Search and Quantum Counting.

List coloring problem



Restricted Grover's Search

Reference : Mukherjee, S. (2022). A grover search-based algorithm for the list coloring problem. IEEE Transactions on Quantum Engineering, 3, 1-8.

Nash Equilibria problem

囚犯的賽局矩陣		囚犯乙	
		招供	不招供
囚犯甲	招供	各判刑2年	甲立即釋放，乙判刑10年
	不招供	甲判刑10年，乙立即釋放	各判刑半年

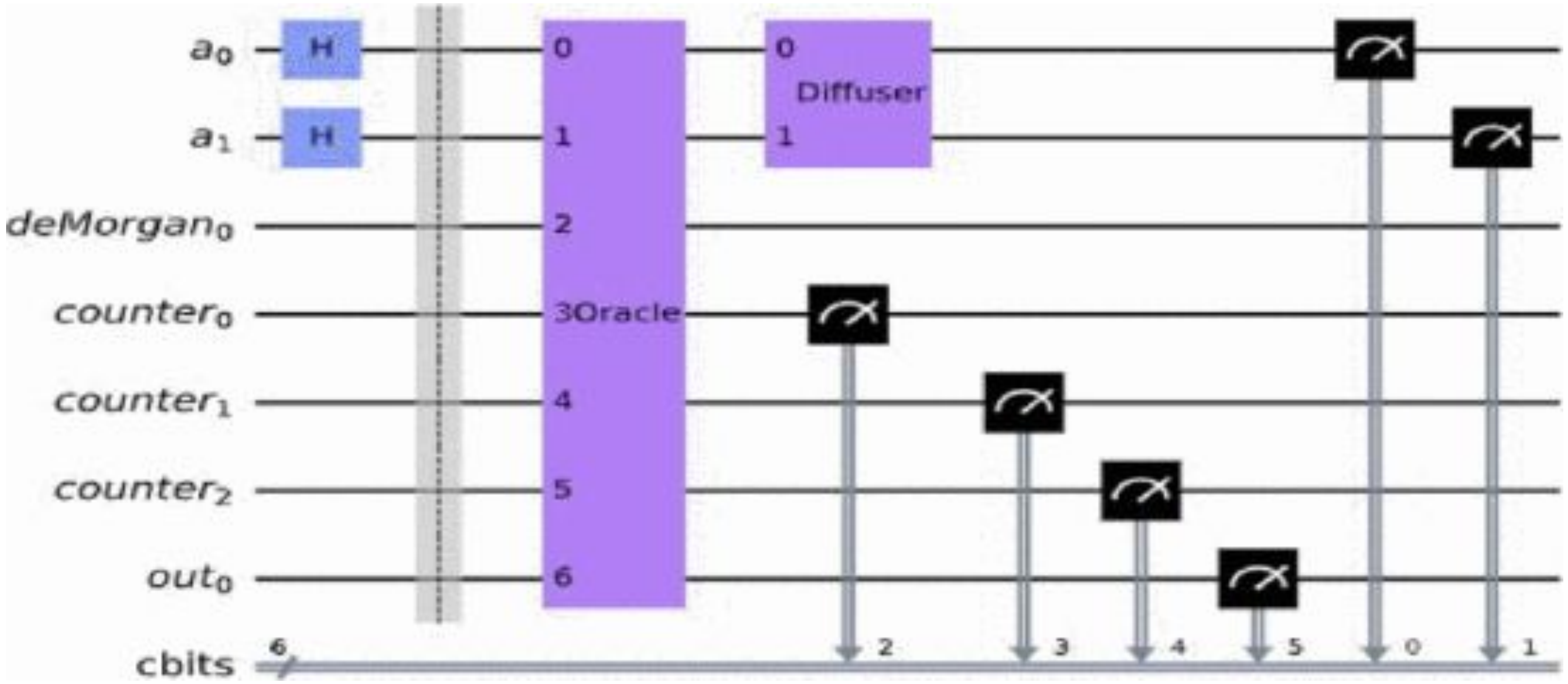
$$O_{oracle} = O_{intra} \land O_{inter}$$

$$O_{intra} = O^{A}{}_{intra} \land O^{B}{}_{intra} \land \ldots O^{N}{}_{intra}$$

Reference : Roch, C., Castillo, S. L., & Linnhoff-Popien, C. (2022, March). A Grover based Quantum Algorithm for Finding Pure Nash Equilibria in Graphical Games. In 2022 IEEE 19th International Conference on Software Architecture Companion (ICSA-C) (pp. 147-151). IEEE.

Maximum satisfiability problem

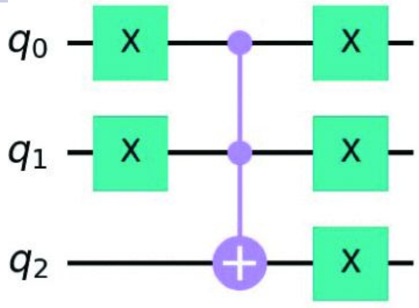
$$f(a,b,c) = (a+b+\bar{c})\,(\bar{a}+\bar{b}+c)\,(b+c)$$



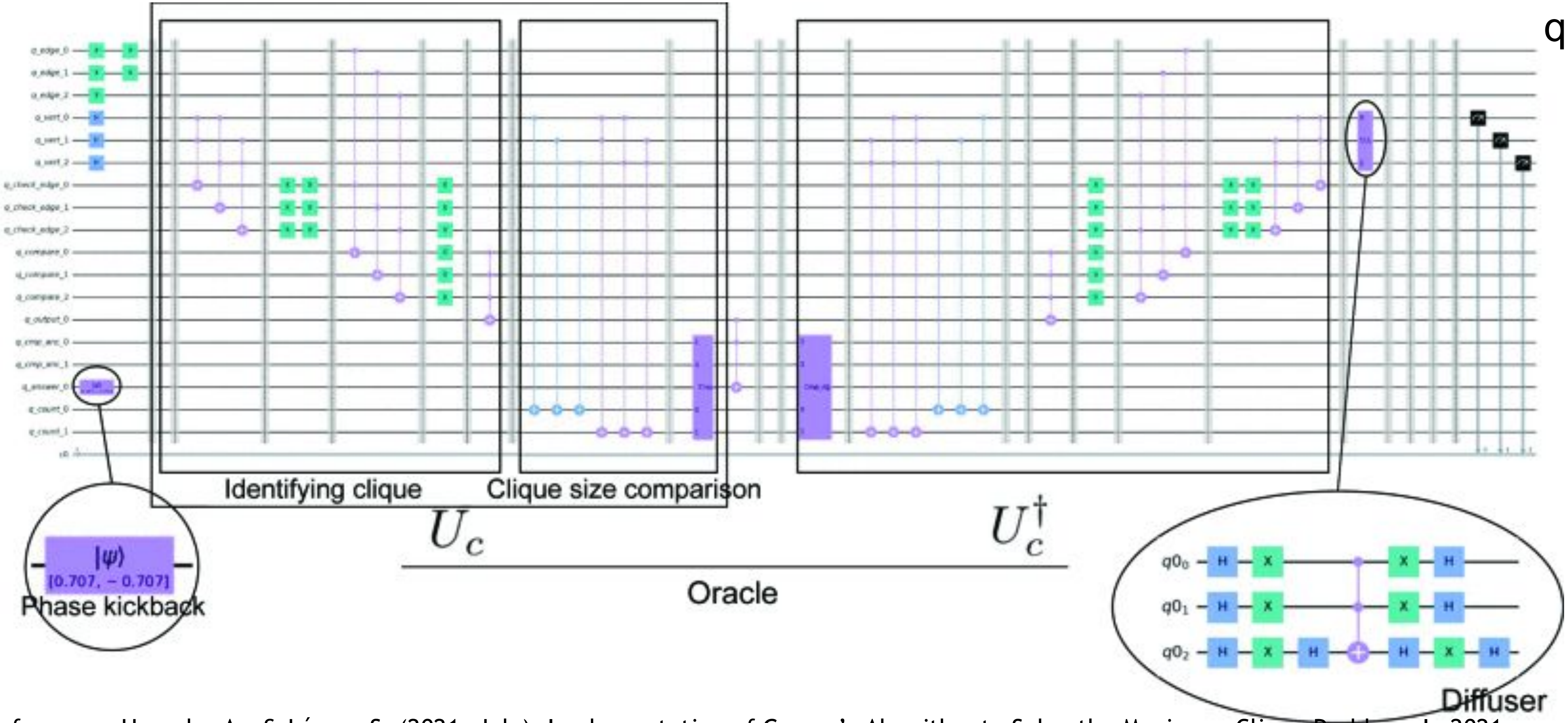
Reference : Alasow, A., & Perkowski, M. (2022, May). Quantum Algorithm for Maximum Satisfiability. In 2022 IEEE 52nd International Symposium on Multiple-Valued Logic (ISMVL) (pp. 27-34). IEEE.

ACAN Laboratory

Maximum clique problem

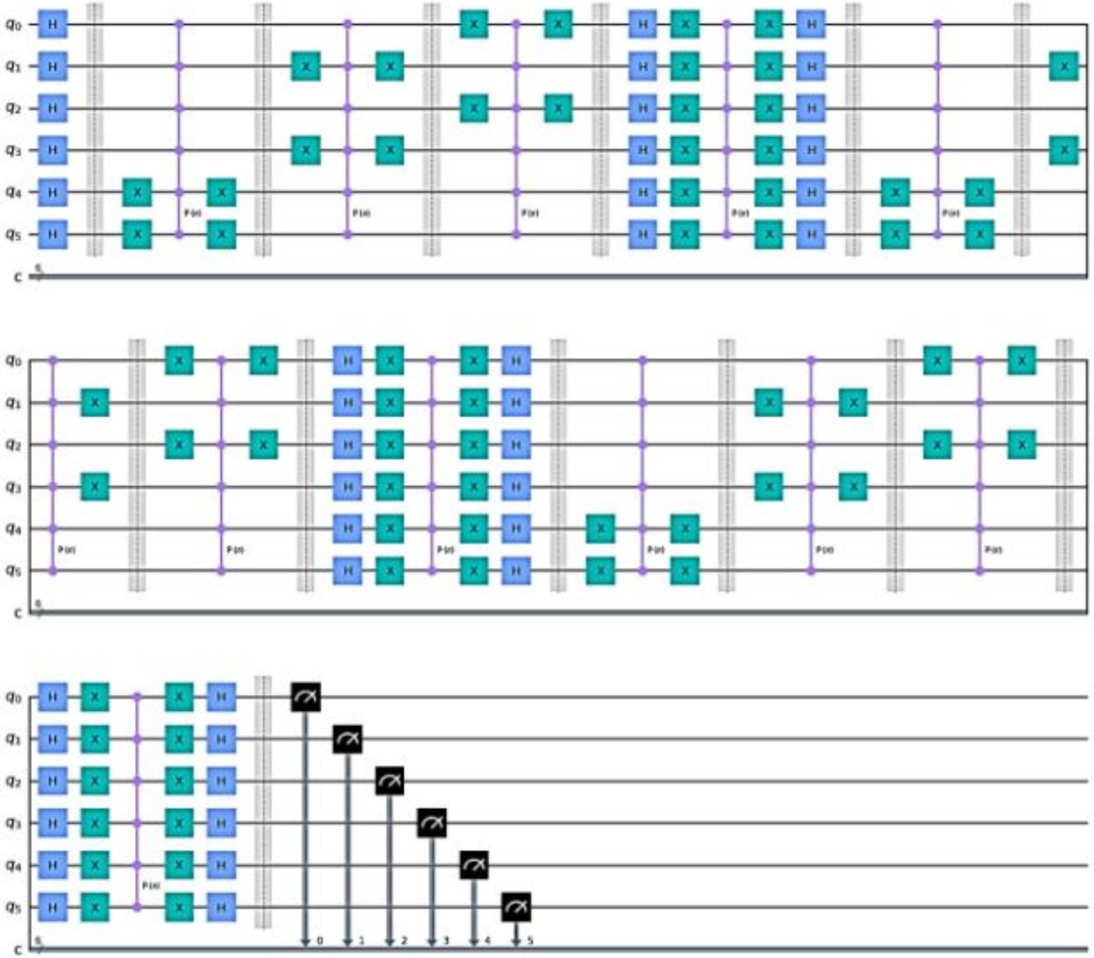


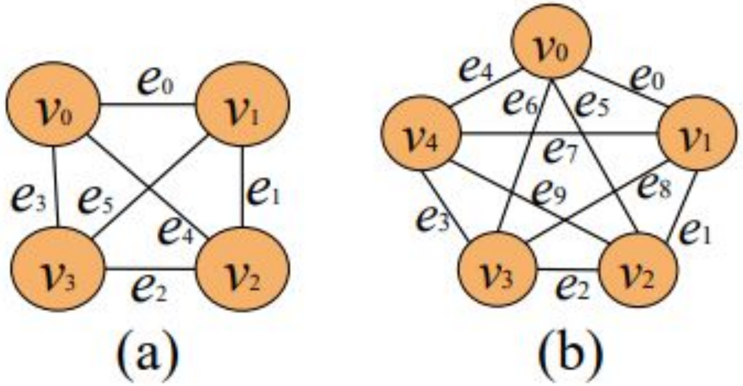
quantum OR gate



Reference : Haverly, A., & López, S. (2021, July). Implementation of Grover's Algorithm to Solve the Maximum Clique Problem. In 2021 IEEE Computer Society Annual Symposium on VLSI (ISVLSI) (pp. 441-446). IEEE.

Hamiltonian cycle problem

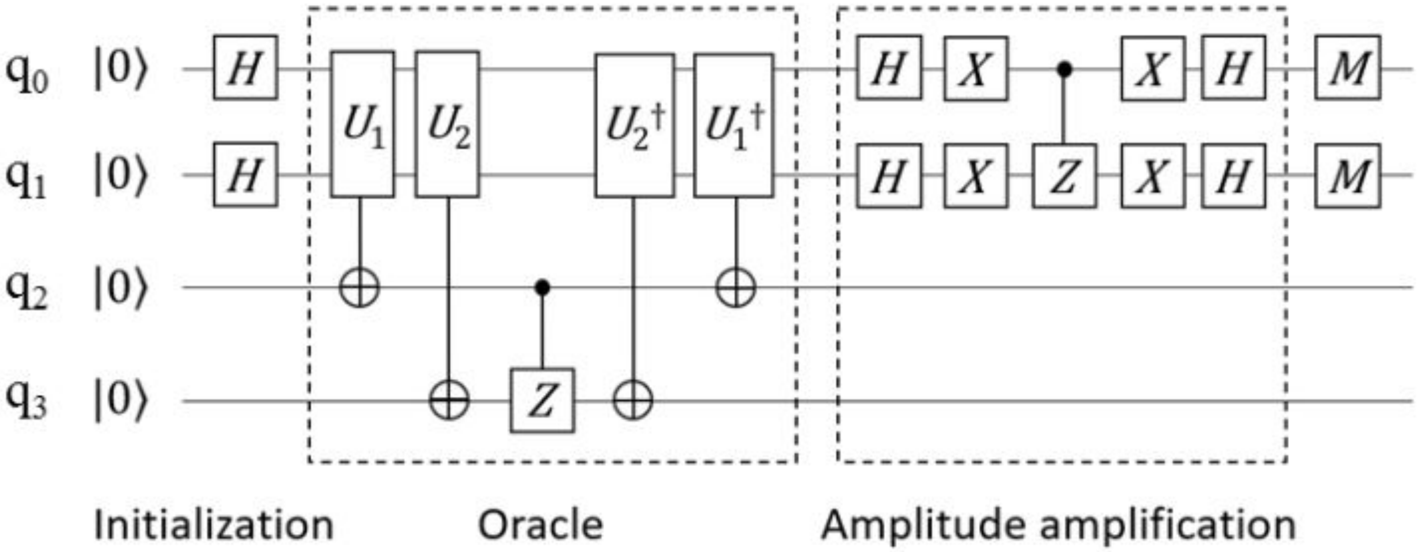


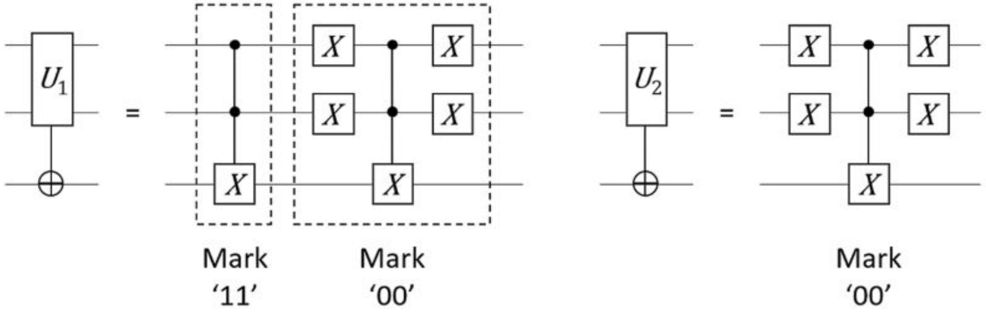


Explicit Oracle

Reference : Jehn-Ruey Jiang, "Quantum Circuit Based on Grover Algorithm to Solve Hamiltonian Cycle Problem," accepted to present at IEEE Eurasia Conference on IOT, Communication and Engineering (IEEE ECICE 2022), 2022.

Intelligent patent search problem





SMILES	Code
C	00
[H] or empty	11

Reference : Wang, P. H., Chen, J. H., & Tseng, Y. J. (2022). Intelligent pharmaceutical patent search on a near-term gate-based quantum computer. Scientific Reports, 12(1), 175.

Fixed Parameter Algorithms

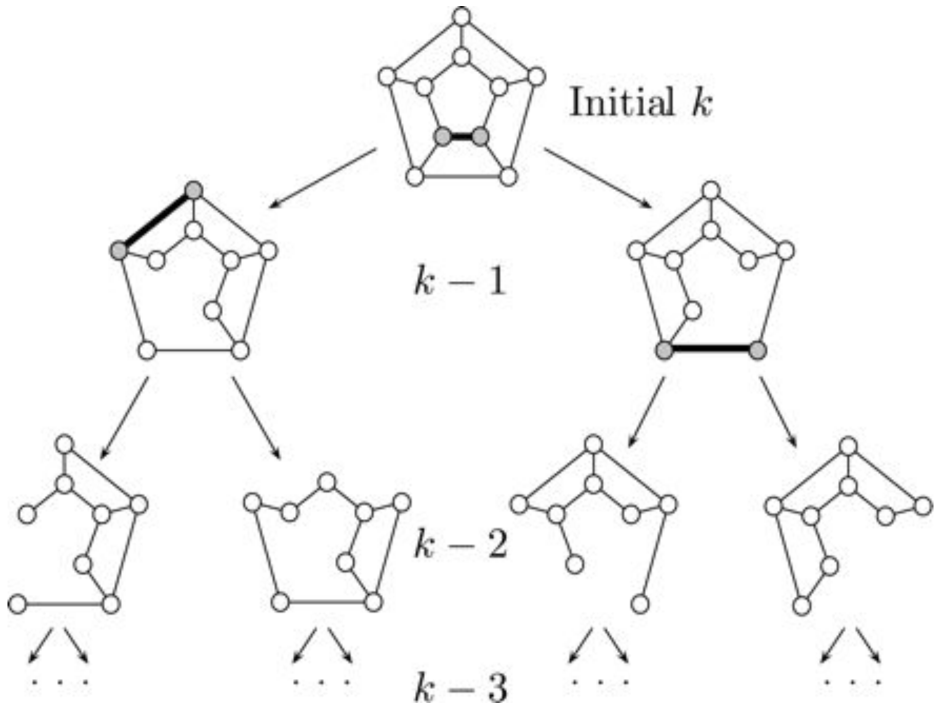
- Many problems were found to be fixed parameter tractable, because of small parameters in practice.
- VCP Kernelization :
  - Remove all isolated vertices
  - For all vertices with a branching degree of 1, first put their adjacent nodes into the candidate vertex cover set, and remove the edge connected to the point from the input.
  - If there is a vertex with branching degree k+1, put this vertex into the vertex cover set.

Reference : Hüffner, F., Niedermeier, R., & Wernicke, S. (2008). Techniques for practical fixed-parameter algorithms. The Computer Journal, 51(1), 7-25.

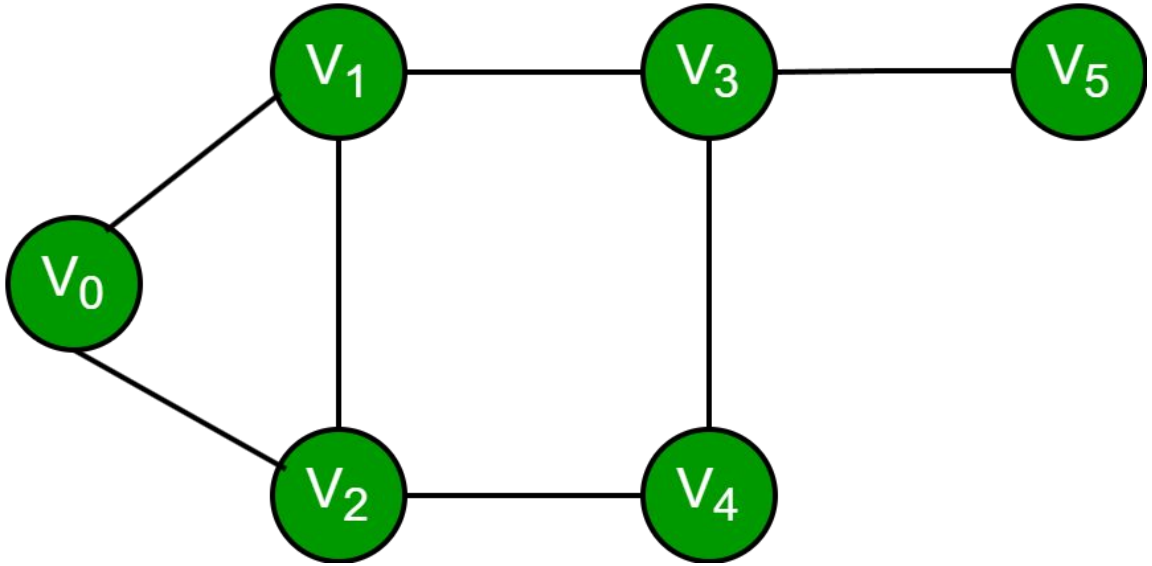
ACAN Laboratory

Bounded Search Tree

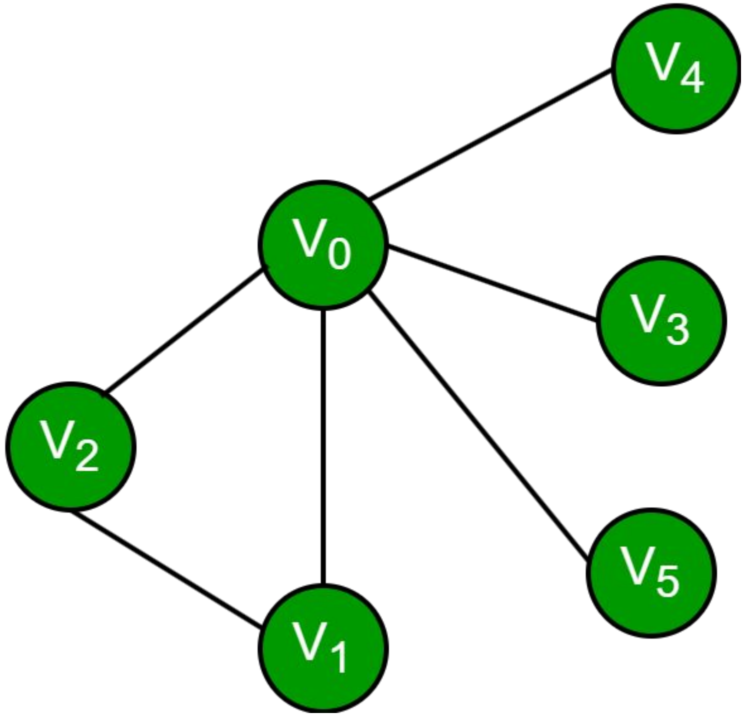
- The core concept of the fixed parameter algorithm is to reduce the combinatorial explosion space as much as possible. The time complexity of the algorithm is $O(1.2738^k+kn)$, which is known as the best classical algorithm for vertex cover problem when k is small.



Input



Graph 2



Graph 3