Quantum Circuit Based on Grover's Algorithm to Solve Exact Cover Problem

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

研究生： 王昱傑

指導教授: 江振瑞 博士

ACAN Laboratory

Outline

- Introduction
- Background and related work
- Proposed Method
- Experiment and Result
- Conclusion

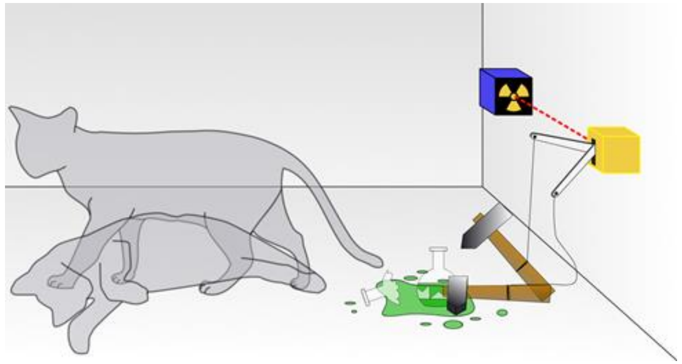
ACAN Laboratory

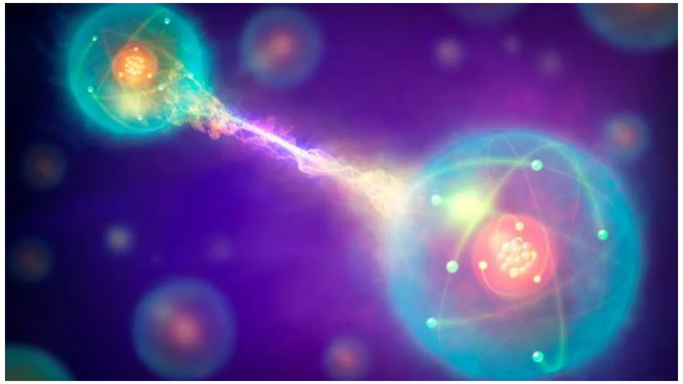
Outline

- **Introduction**
- Background and related work
- Proposed Method
- Experiment and Result
- Conclusion

Quantum Computing

- Quantum computing utilizes the principles of quantum mechanics to perform computations.
- Key principles of quantum mechanics include:
  - Superposition
  - Entanglement
- Quantum computing has the potential to revolutionize fields such as cryptography, drug discovery, optimization, and finance.





Quantum Computer

- Quantum computer is a type of computing device that leverages the principles of quantum mechanics to perform computations.
- Quantum computers can be broadly classified into two main types : universal quantum computer and quantum annealer.

IBM’s 20-qubit Q System One in 2019

Source:https://www.somagnews.com/ibm-said-the-quantum-chip-will-surpass-its-competitors-in-2-years/

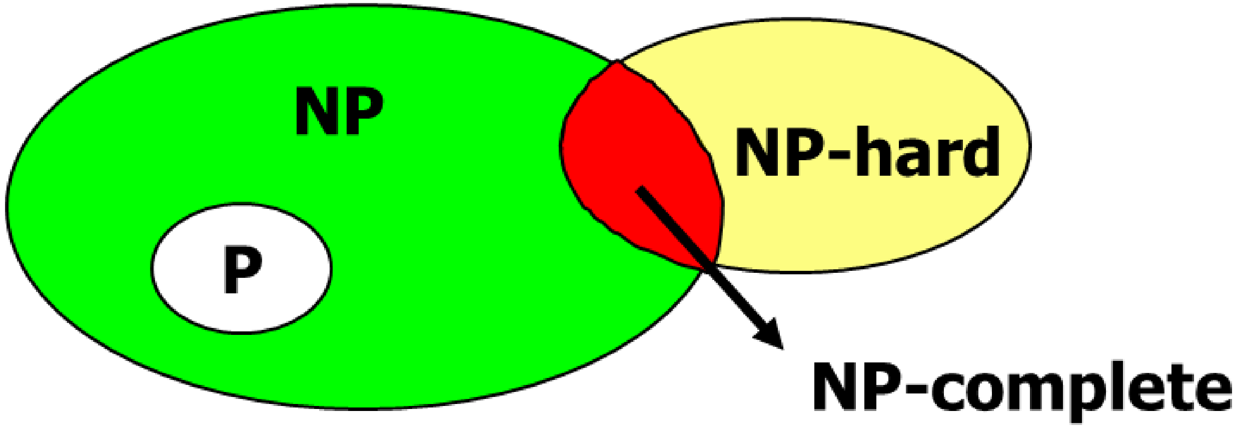
D-Wave Advantage in 2020

Source: https://tweakers.net/nieuws/187892/d-wave-gaat-net-als-ibm-en-google-universele-quantumcomputer-bouwen.html

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 reduces.
- **NP-complete (NPC)**: the class of problems which are NP-hard and belong to NP.



Outline

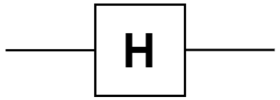
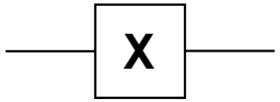
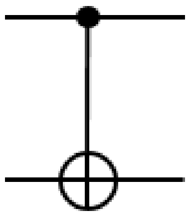
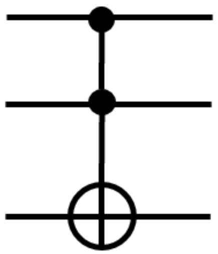
- Introduction
- Background knowledge and related work
- Proposed Method
- Experiment and Result
- Conclusion

ACAN Laboratory

Quantum Circuit

- In quantum computing, quantum circuits consist of qubits and quantum gates.
- A qubit is a superposition of zero and one.
- A quantum gate is used to manipulate the state of qubits.
- Quantum gates can be categorized into two types based on the number of qubits : single-qubit gates and multi-qubit gates.

Table : Quantum gates

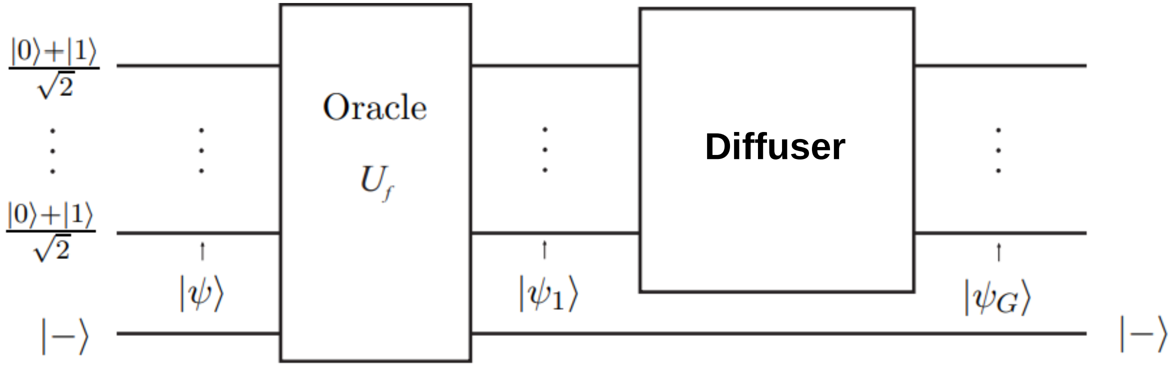
Operator	Quantum Gate	Matrix Form
Hadamard		$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
Pauli X		$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
CNOT		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$
Toffoli		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$

Grover’s algorithm - Oracle

- Grover's algorithm [1] is a quantum algorithm proposed by Grover in 1996 to solve the unstructured data search problem with high probability.
- Let U_f be the oracle for Grover’s algorithm, the oracle is defined as follows:

$$U_f\,|x\rangle = \begin{cases} |x\rangle & \text{if } x \neq x^* \\ -|x\rangle & \text{if } x = x^* \end{cases}$$

- Below shows the quantum circuit[2] of the Grover’s algorithm.



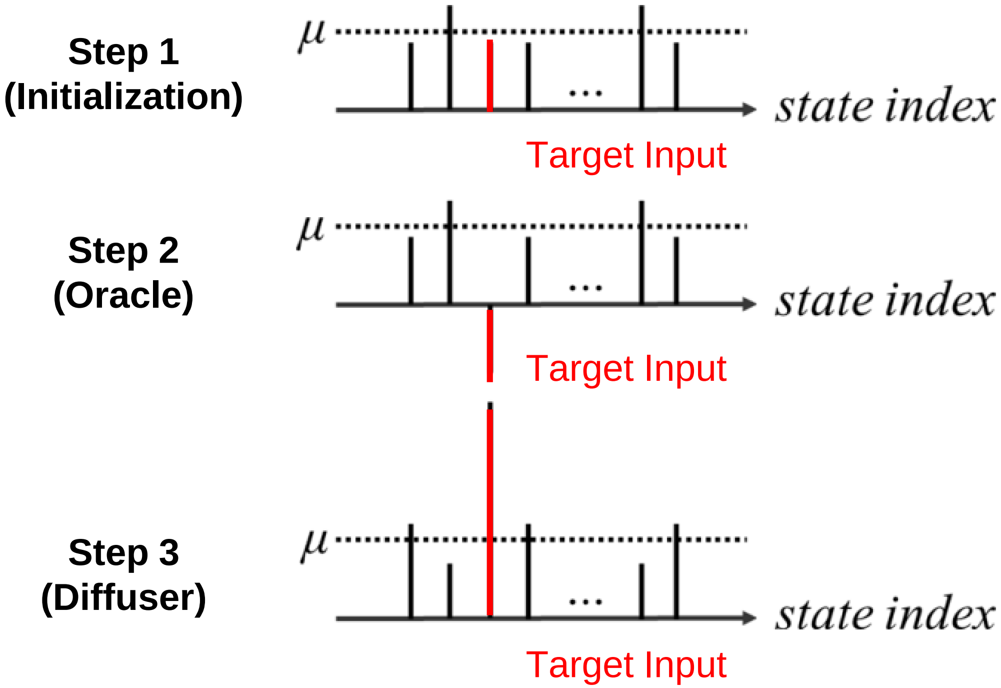
[1] Grover, L. K. (1996, July). A fast quantum mechanical algorithm for database search. In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing (pp. 212-219).

[2] Lavor, C., Manssur, L. R. U., & Portugal, R. (2003). Grover's algorithm: Quantum database search. arXiv preprint quant-ph/0301079.

ACAN Laboratory

Grover’s algorithm -Diffuser

- The diffuser causes the probability amplitudes of all qubits to invert around the mean μ of all amplitudes.
- The positive amplitude only decreases a little bit. However, the negative amplitude becomes a very large positive amplitude.



Grover's algorithm - Iterations

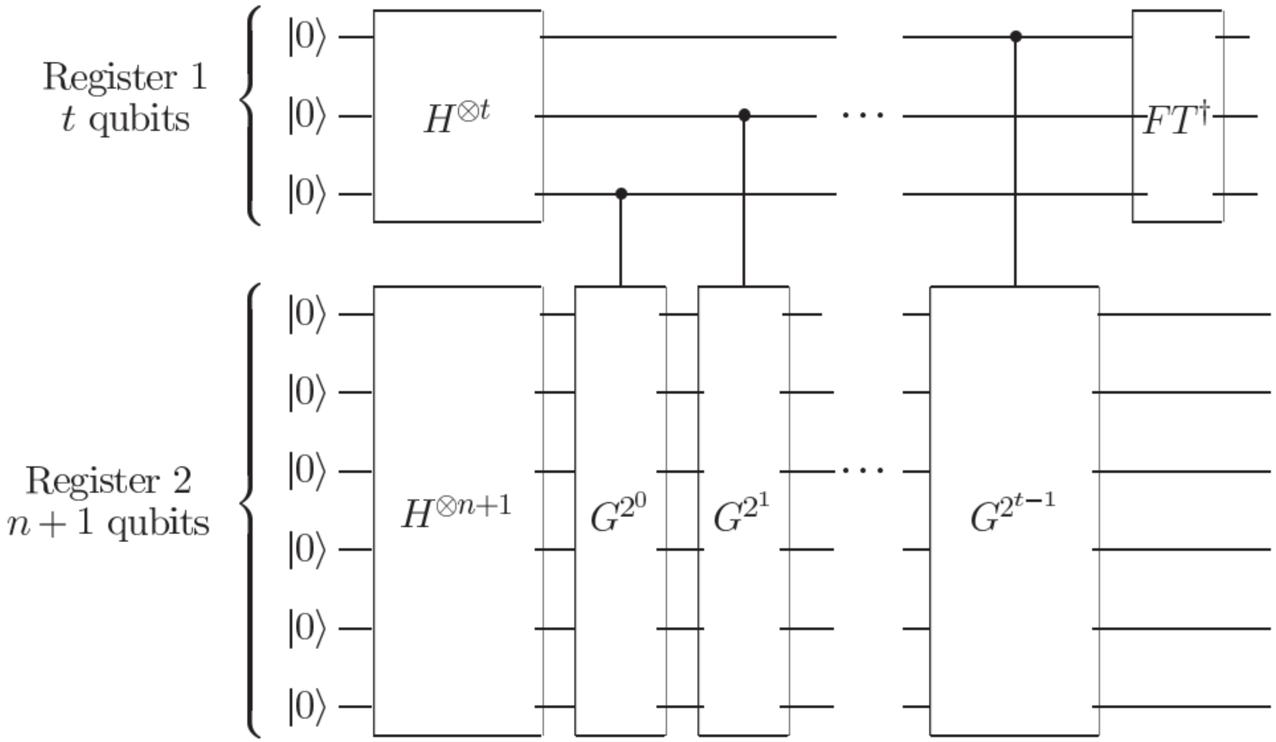
- Note that Chen et al. [4] showed that when the number of solution input instances is M, then diffusion operator should be repeated for $\left\lfloor \frac{\pi}{4}\sqrt{\frac{N}{M}} \right\rfloor$ times to find all the M solution input instances with high probability.

Reference :

[4]Chen, G., Fulling, S. A., Lee, H., & Scully, M. O. (2001). Grover's algorithm for multiobject search in quantum computing. In Directions in Quantum Optics: A Collection of Papers Dedicated to the Memory of Dan Walls Including Papers Presented at the TAMU-ONR Workshop Held at Jackson, Wyoming, USA, 26–30 July 1999 (pp. 165-175). Springer Berlin Heidelberg.

Quantum Counting - Searching M

- The quantum counting [5] algorithm can be used to evaluate the number of solutions.
- The algorithm is based on inverse Fourier transform algorithm and Grover's algorithm.



Reference :

[5] Brassard, G., Høyer, P., & Tapp, A. (1998, July). Quantum counting. In International Colloquium on Automata, Languages, and Programming (pp. 820-831). Springer, Berlin, Heidelberg.

[6] Michael A. Nielsen and Isaac L. Chuang. 2011. Quantum Computation and Quantum Information: 10th Anniversary Edition (10th ed.). Cambridge University Press, New York, NY, USA.

Exact Cover - Definition

- The exact cover problem (ECP) is defined as follows :
  - Given a universal set $U = \{u_1, u_2, ..., u_m\}$ with m elements, and a collection $S = \{S_1, S_2, ..., S_n\}$ of n subsets of U
  - The ECP is to determine whether or not there exist a sub-collection $S' \subseteq S$ such that S' is the exact cover of U.
  - That is, every element in U belongs to exactly one subset in S'.
- ECP has been shown to be both NP-hard and NP-complete.
- Note that the exact cover problem can also be represented as a bipartite graph.

ACAN Laboratory

Related Work

- [8] : Design a quantum circuit with explicit oracle to solve Hamiltonian Cycle problem.
- [9-10] : Design an invalid color detector and binary comparator for oracle to solve the K-coloring problem.
- [11] : Design oracle circuits using three different types of quantum registers: vertex registers, edge registers, and ancillary qubit registers,to solve List-Coloring problem
- [12] : Implementing an oracle for identifying clique and clique size comparison to solve the Maximum Clique problem.
- [13] : Design an oracle in which clauses are encoded into the circuit to construct the oracle, aiming to solve the Maximum Satisfiability Problem.
- [14] : To find Nash equilibria in graphical games by converting the graphical game into a Boolean satisfiability problem for solving.
- [15] Encodes two compounds as binary strings and compares their overlapping structures in a quantum circuit, which is used for drug patent analysis.

Reference :

[8] Jehn-Ruey Jiang, "Quantum Circuit Based on Grover Algorithm to Solve Hamiltonian Cycle Problem," accepted to present at IEEE Eurasia Confere
nce on IOT, Communication and Engineering (IEEE ECICE 2022), 2022.

[9] 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.

[10] Lutze, D. (2021). Solving Chromatic Number with Quantum Search and Quantum Counting.

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

[12] 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.

[13] 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

[14] 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.

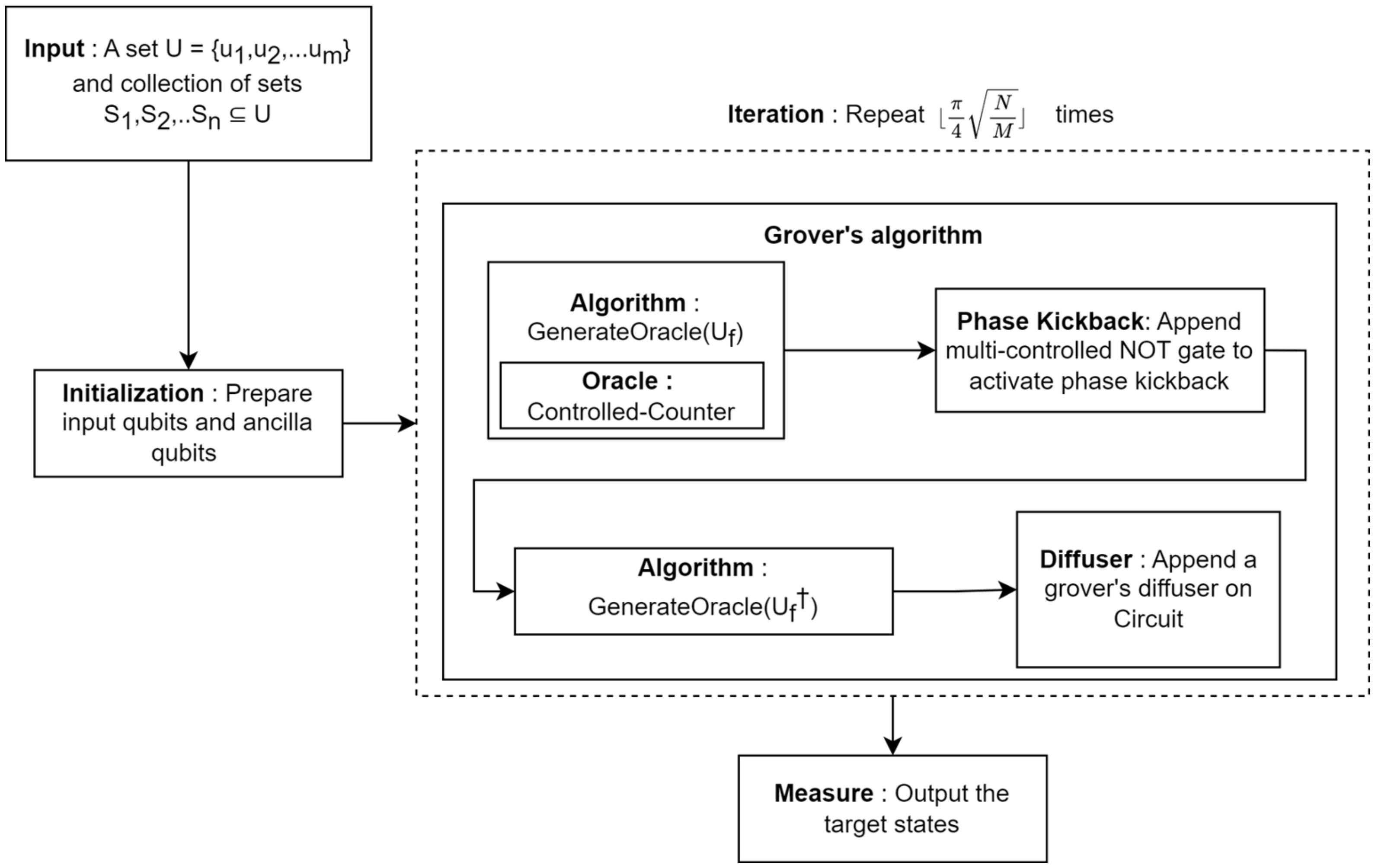
[15]Wang, P. H., Chen, J. H., & Tseng, Y. J. (2022). Intelligent pharmaceutical patent search on a near-term gate-based quantum computer. Scientific Reports, 12(1), 175.

Outline

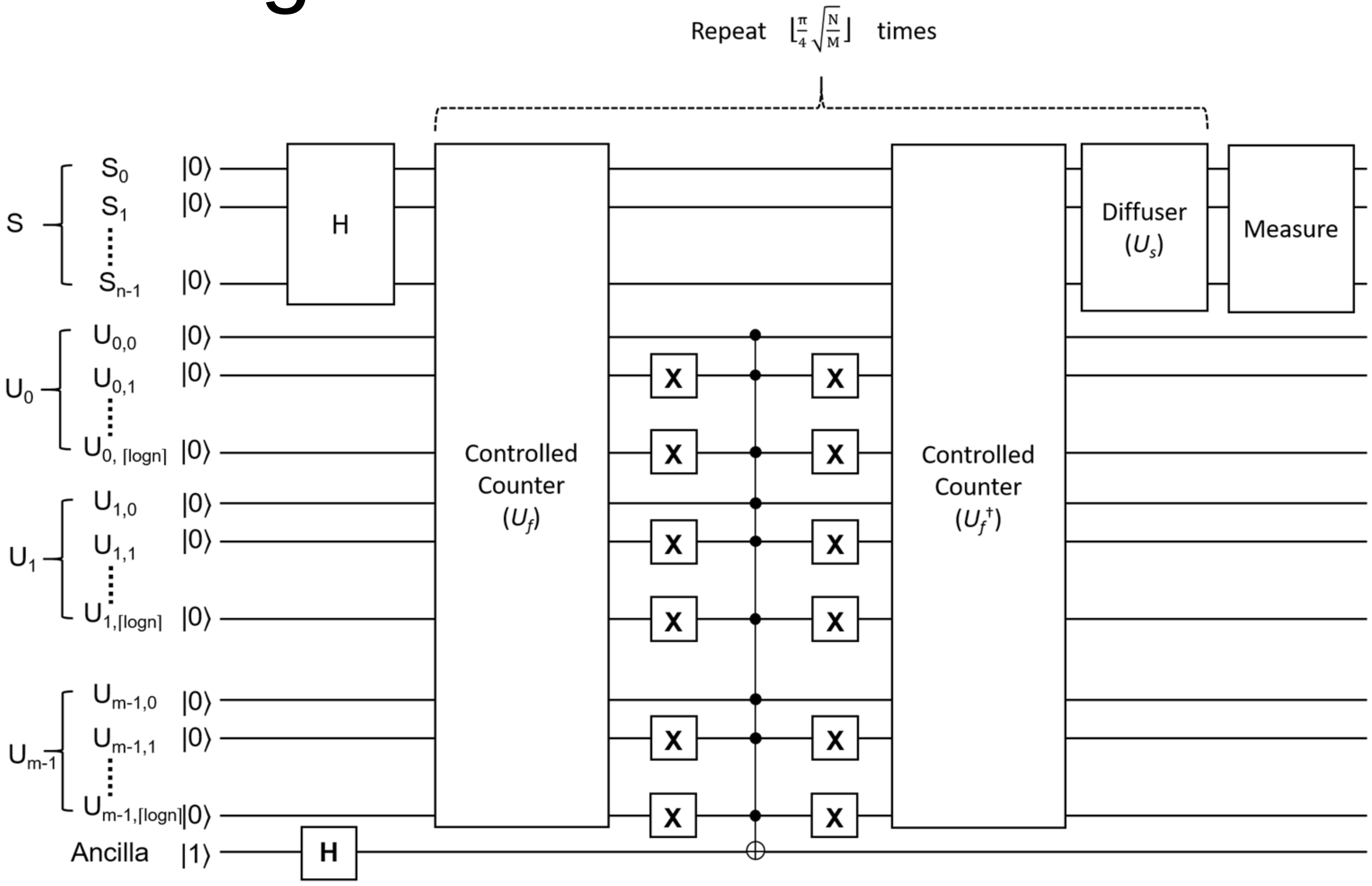
- Introduction
- Background and related work
- Proposed Method
- Experiment and Result
- Conclusion

ACAN Laboratory

Proposed Method

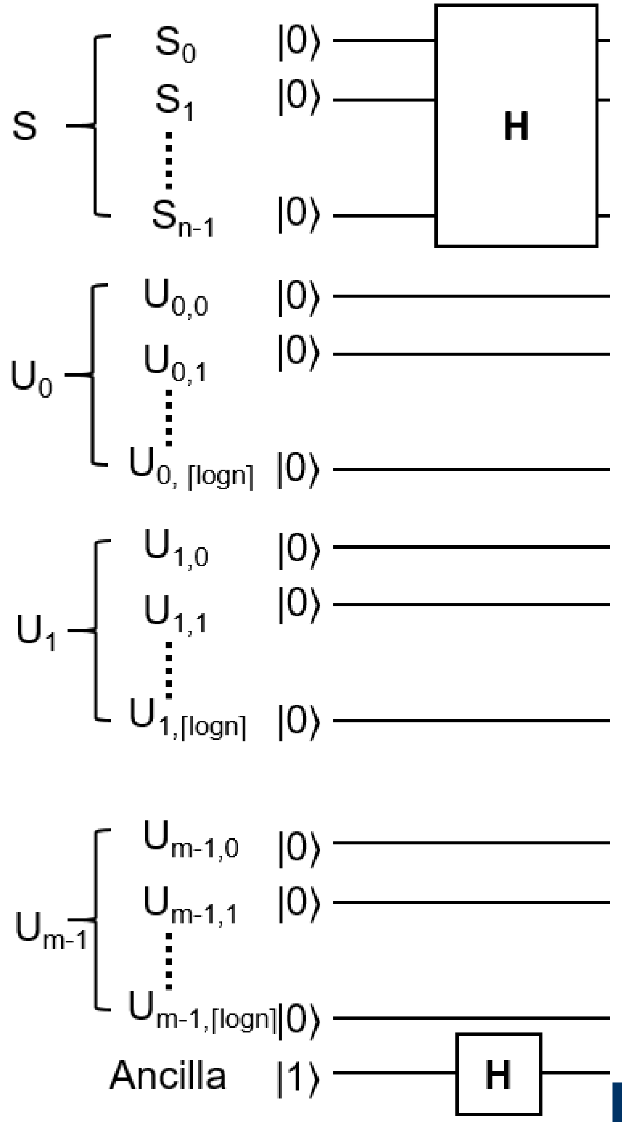


Circuit Diagram



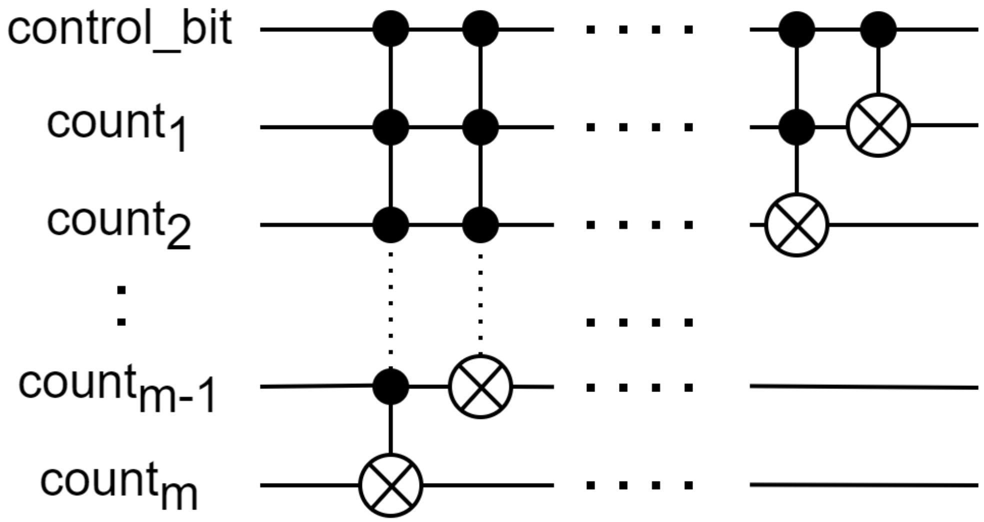
Initialization

- The initialization process can be divided into three steps:
  - Step 1 : Reading the input of the Exact Cover Problem.
  - Step 2 : Determining the number of qubits used based on the input.
  - Step 3 : Setting the initial states of the qubits.



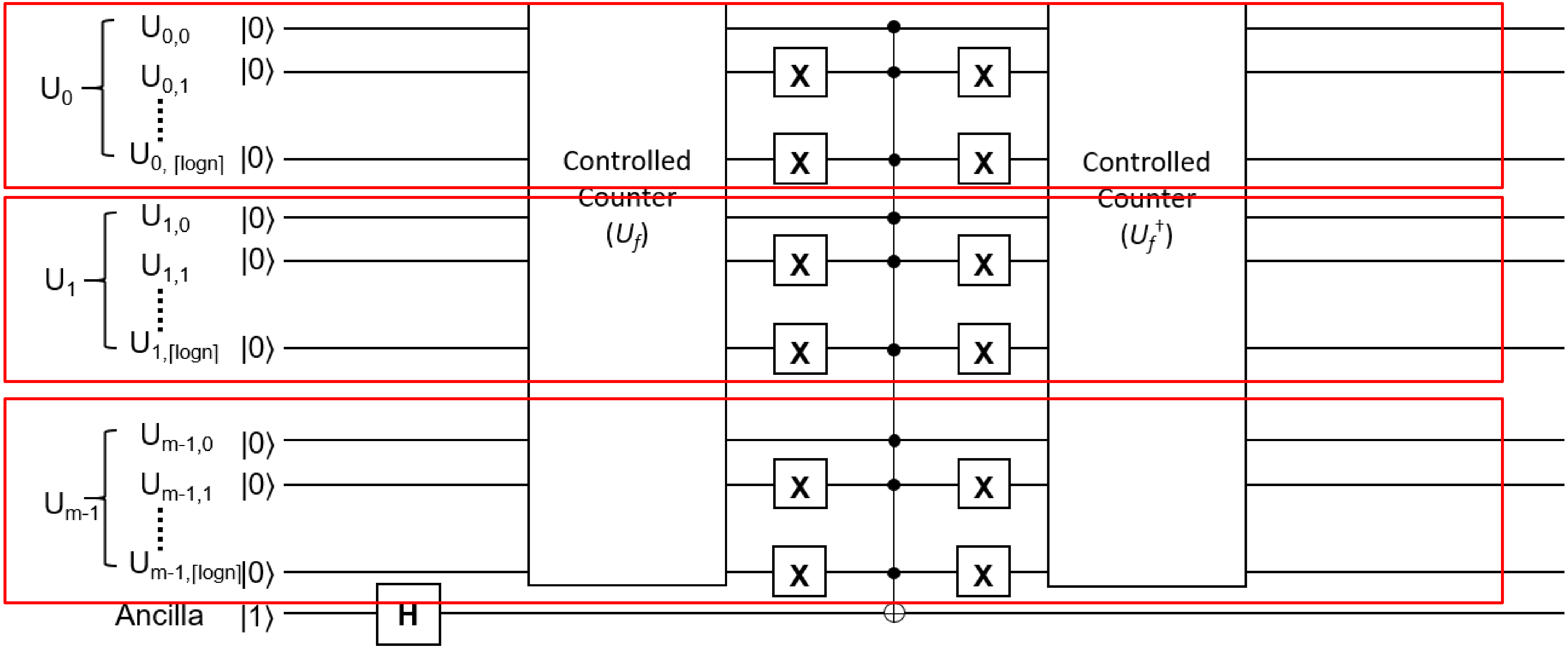
Oracle - Controlled-Counter

- The exact cover S' of U in the ECP satisfies the following two conditions :
  (i) Subsets in S' are mutually disjoint, as every element in U belongs to exactly one subset in S'.
  (ii) The union of all subsets in S’ is U.
- To achieve the above two conditions, a controlled counter is used.



ACAN Laboratory

Oracle - Controlled-Counter



The number of qubits

- Universal set U : m elements
- Collection of sets S: n qubits.
- Controlled counter : ceil($\log_2 n$) qubits.
  - Hence, the universal set U requires a total of m*(ceil($\log_2 n$)) qubits for representation.
- Ancillary qubit : 1
- Total qubits : n+ m*(ceil($\log_2 n$)) + 1

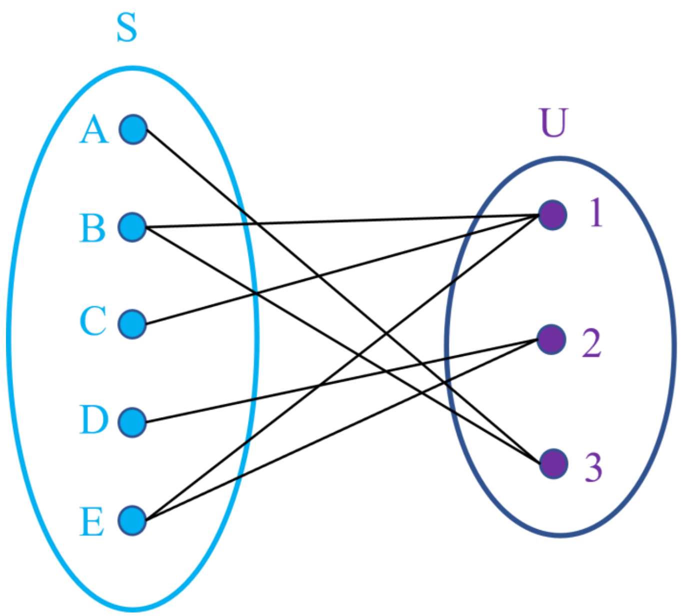
Outline

- Introduction
- Background and related work
- Proposed Method
- Experiment and Result
- Conclusion

ACAN Laboratory

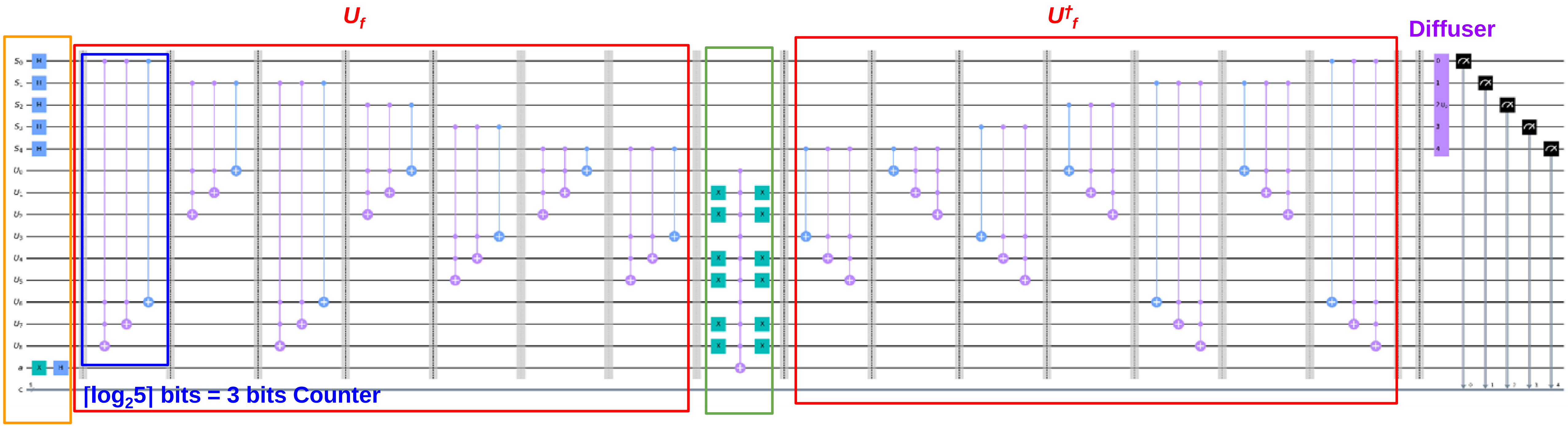
Experiment - Problem

- Collections of set U = {1, 2, 3}, A = {3}，B = {1, 3}，C = {1}，D = {2}，E = {1, 2}



Experiment - Oracle

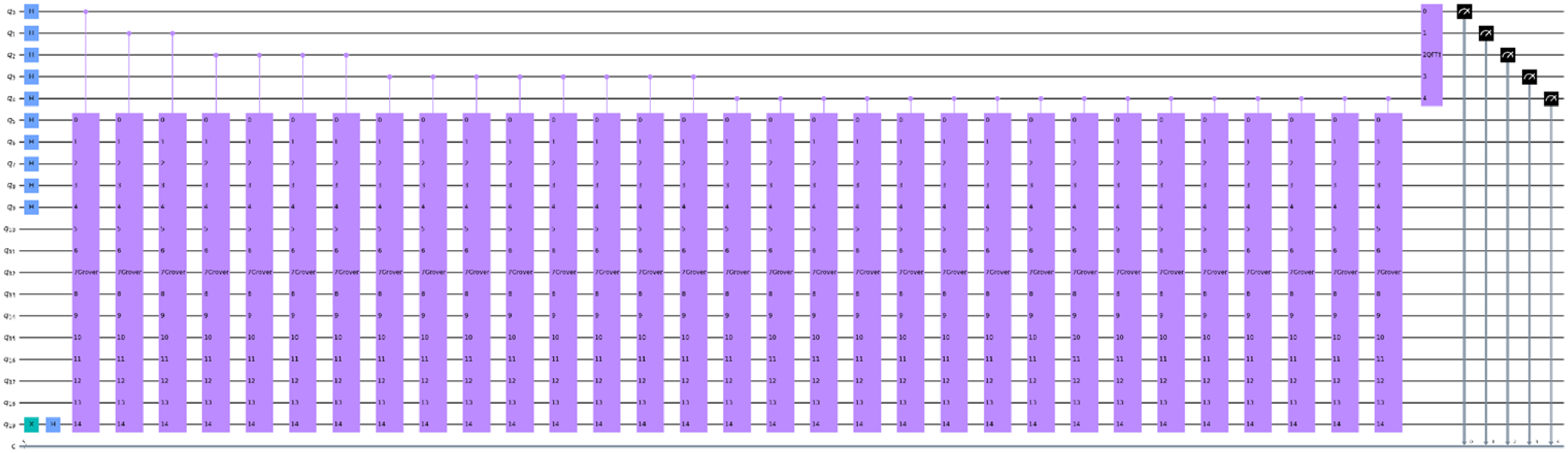
- Collections of set U = {1, 2, 3}, A = {3}，B = {1, 3}，C = {1}，D = {2}，E = {1, 2}



Initialization

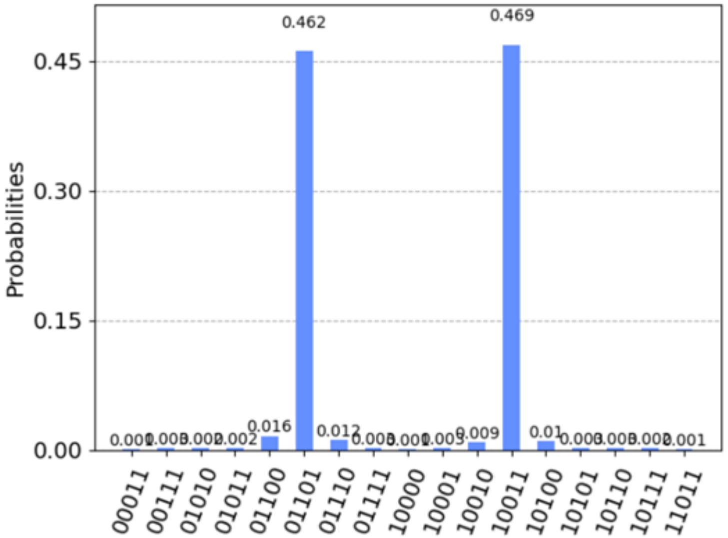
Phase Kickback

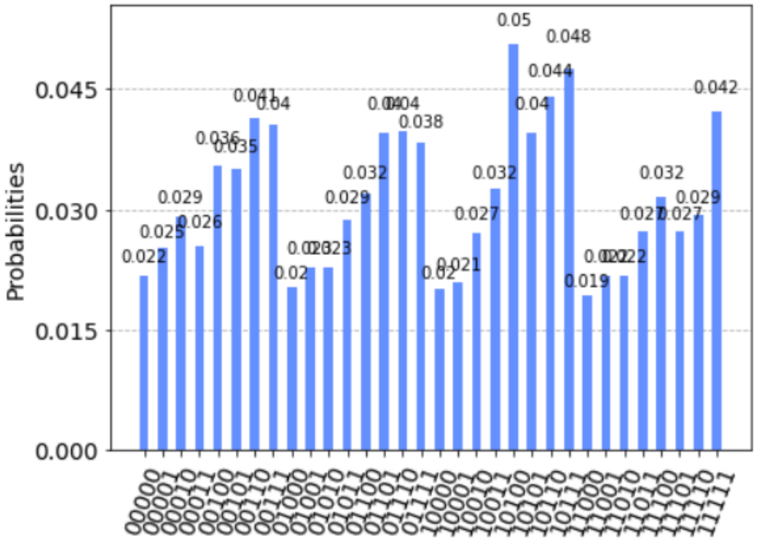
Experiment - Quantum Counting



ACAN Laboratory

Measurement - Quantum Counting





$$\theta = \left(\frac{\text{measurement int}}{2^t} - \frac{1}{2}\right)2\pi$$

$$M = N \times \sin^2 \frac{\theta}{2}$$

$$\theta = \left(\frac{19}{2^5} - \frac{1}{2}\right)2\pi \approx 0.59$$

$$M = 2^5 \times \sin^2 \frac{0.59}{2} \approx 2.7$$

ibmq_qasm_simulator

$$\theta = \left(\frac{20}{2^5} - \frac{1}{2}\right)2\pi \approx 0.785$$

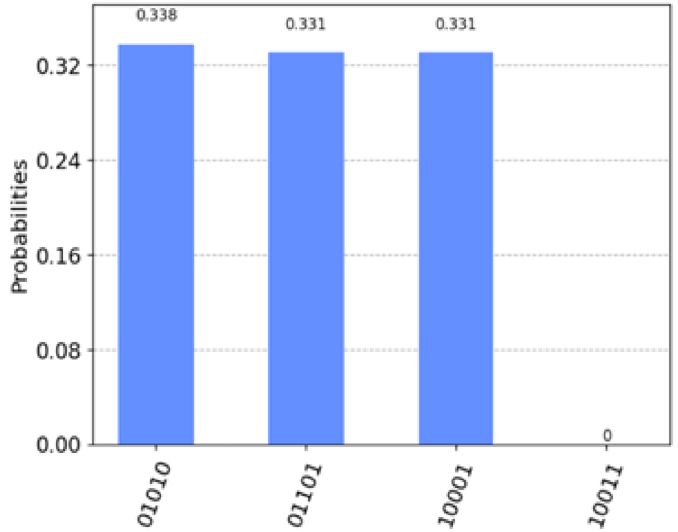
$$M = 2^5 \times \sin^2 \frac{0.785}{2} \approx 4.7$$

ibmq_kolkata

ACAN Laboratory

Measurement - Grover's algorithm

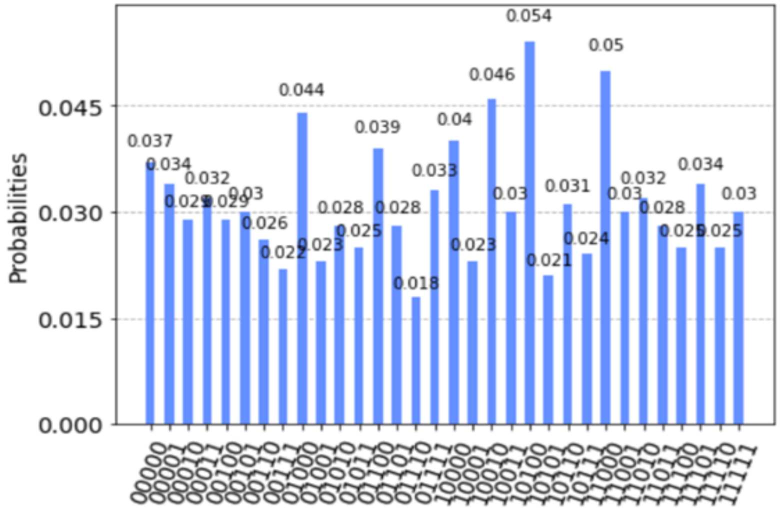
- Collections of set U = {1, 2, 3}, A = {3}, B = {1, 3}, C = {1}, D = {2}, E = {1, 2}



ibmq_qasm_simulator

$\lfloor \frac{\pi}{4}\sqrt{\frac{N}{M}} \rfloor = \lfloor \frac{\pi}{4}\sqrt{\frac{2^5}{2.7}} \rfloor = \lfloor 2.56 \rfloor = 2$

01010 ==> Choose B,D V
01101 ==> Choose A,C,D V
10001 ==> Choose A,E V



ibmq_kolkata

$\lfloor \frac{\pi}{4}\sqrt{\frac{N}{M}} \rfloor = \lfloor \frac{\pi}{4}\sqrt{\frac{2^5}{4.7}} \rfloor = \lfloor 2.04 \rfloor = 2$

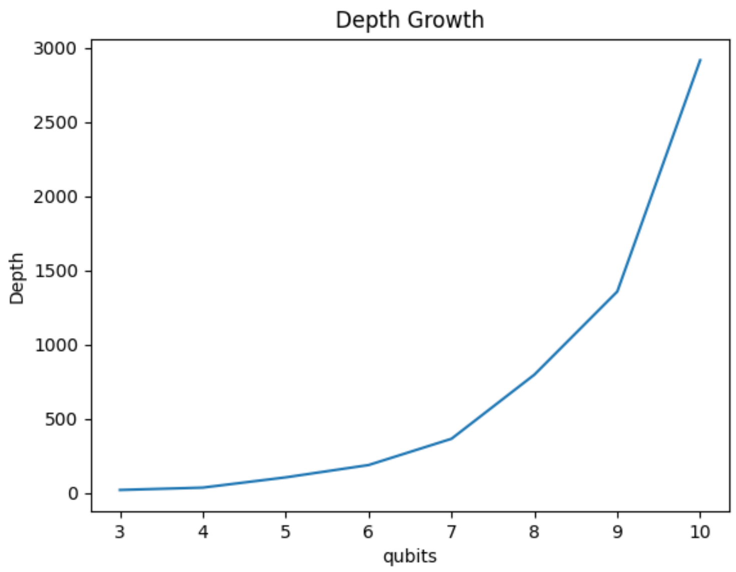
10110==> Choose B,C,E X
10111==> Choose A,B,C,E X
00111==> Choose A,B,C X

Analysis

Case	Qubits	Number of Quantum gates				Depth
		CX	RZ	SX	X	
P1	7	130	103	23	2	201
P2	8	222	157	36	3	326
P3	15	11199	5965	228	36	11613

Analysis - MCT gate

Qubits	Number of Quantum gates			Depth
	CX	RZ	SX	
3	9	10	2	19
4	20	18	2	35
5	69	51	10	104
6	164	96	2	187
7	311	192	2	364
8	632	384	2	796
9	1427	768	2	1356
10	2828	1536	2	2915



Comparison

Method	Type	Time Complexity
Exhaustive Search	-	$O(2^{\|S\|})$
Algorithm X[14]	Tree Search	$O(1.6181^{\|S\|})$
Branch and Reduce[15]	Tree Search	$O(1.4656^{\|S\|})$
Measure and Conquer[16]	Tree Search	$O(1.3842^{\|S\|})$
Proposed Method	Quantum Algorithm	$O(\sqrt{2^{\|S\|}}) \simeq O(1.414^{\|S\|})$

Reference :
[14] Knuth, D. E. (2000). Dancing links. arXiv preprint cs/0011047.
[15] Fomin, F. V., Grandoni, F., & Kratsch, D. (2005, July). Measure and conquer: Domination–a case study. In International Colloquium on Automata, Languages, and Programming (pp. 191-203). Springer, Berlin, Heidelberg.
[16] HU Qin, NING Ai-bing, GOU Hai-wen, ZHANG Hui-zhen. Measure and Conquer Algorithm for Exact Cover Problem. Operations Research and Management Science, 2020, 29(4): 179-186.

Outline

- Introduction
- Background and related work
- Proposed Method
- Experiment and Result
- Conclusion

ACAN Laboratory

Conclusion

- This paper proposes a quantum circuit based on the Grover's algorithm to solve the exact cover problem, and the oracle is constructed using controlled counters.
- Compared to the exhaustive algorithm used in classical computers, the proposed method provides a quadratic speedup

Conclusion

- In the experiments, the circuit is measured using IBM's quantum simulator "ibmq_qasm_simulator" and the quantum computer "ibmq_kolkata".
- The results show that the quantum simulator can find feasible solutions with high probability.
- However, on the quantum computer, due to noise effects, the circuit cannot distinguish the probability amplitudes of feasible and infeasible solutions in the measurement results.

ACAN Laboratory

Future Work

- Introducing the concept of quantum error correction to detect and correct errors in qubits.
- Improving the design of controlled counter to increase the success rate of finding feasible solutions on quantum computer.

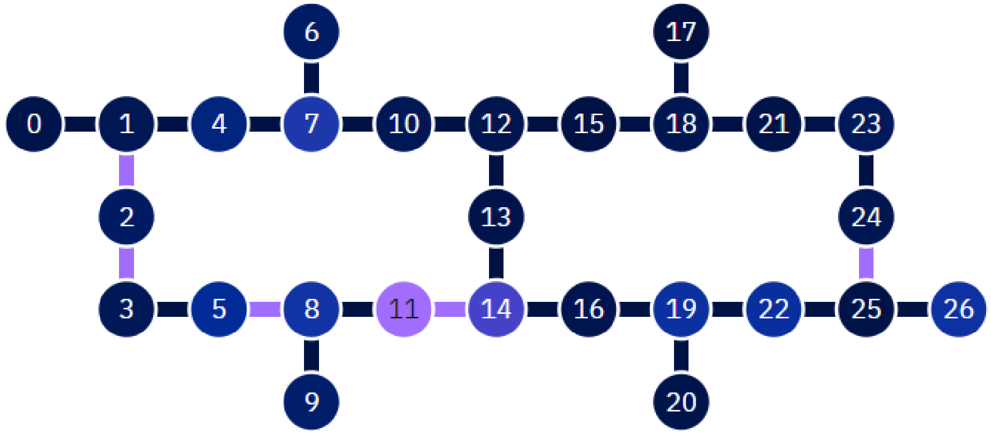
ACAN Laboratory

Q & A
THANK YOU FOR LISTENING !

ACAN Laboratory

Appendix

ibmq_kolkata



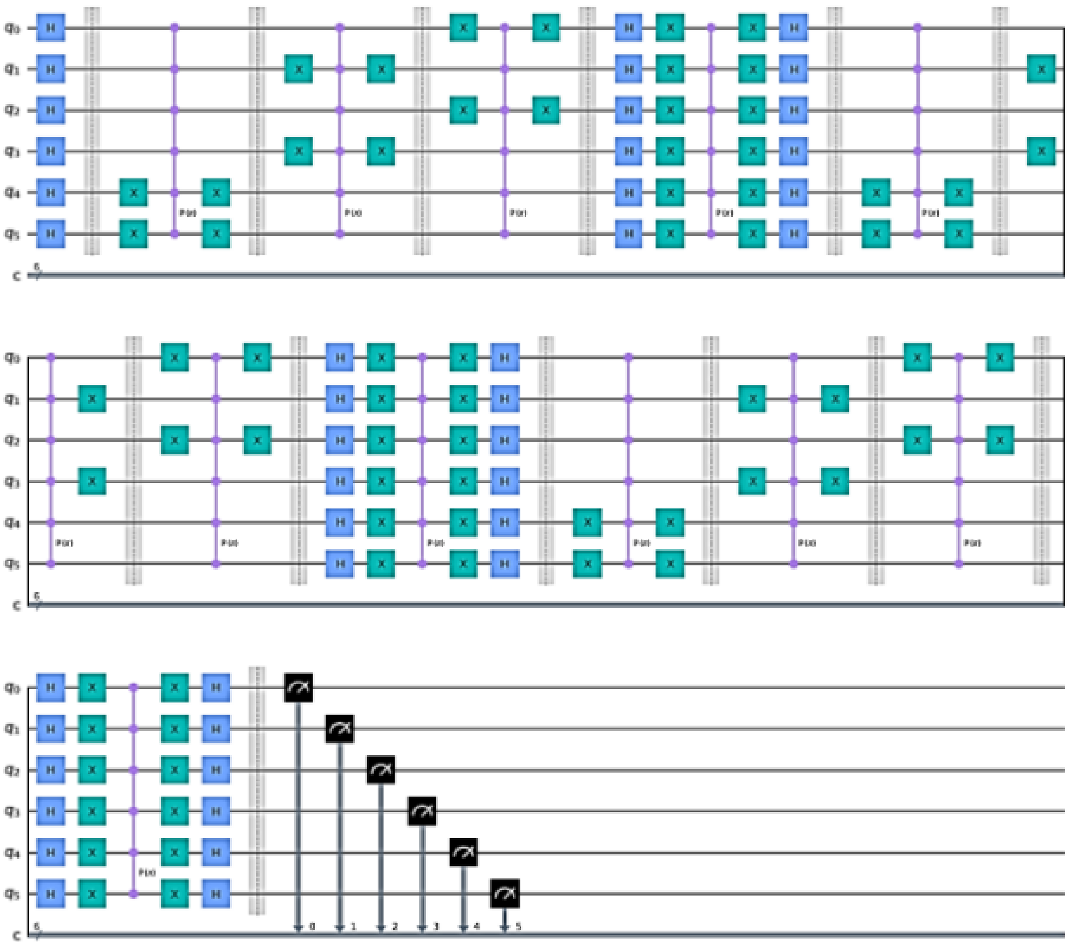
Name	ibmq_kolkata
Version	1.13.1
Qubits	27
Quantum Volume(QV)	128
Basic gates	CX, ID, RZ, SX, X

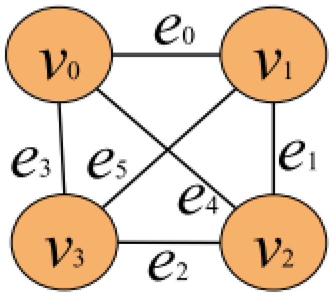
ibmq_qasm_simulator

Name	ibmq_qasm_simulator
Version	0.1.547
Qubits	32
Basic gates	U1, U2, U3, U, P, R, RX, RY, RZ, ID, X, Y, Z, H, S, SDG, SX, T, TDG, SWAP, CX, CY, CZ, CSX, CP, CU1, CU2, CU3, RXX, RYY, RZZ, RZX, CCX, CSWAP, MCX, MCY, MCZ, MCSX, MCP, MCU1, MCU2, MCU3, MCRX, MCRY, MCRZ, MCR, MCSWAP, UNITARY, DIAGONAL, MULTIPLEXER, INITIALIZE, KRAUS, ROERROR, DELAY

ACAN Laboratory

Hamiltonian Cycle

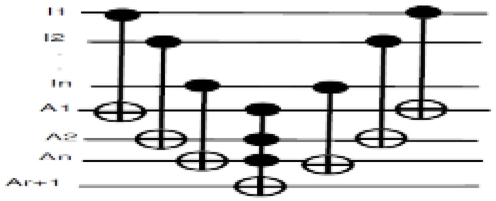




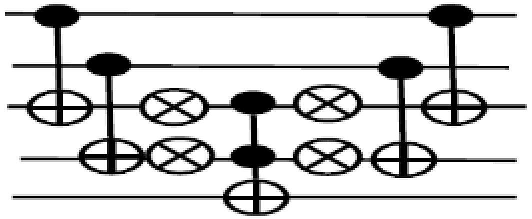
4-clique complete graph

Reference :Jehn-Ruey Jiang, "Quantum Circuit Based on Grover Algorithm to Solve Hamiltonian Cycle Problem," accepted to present at IEEE Eurasia Confere

K - Coloring problem

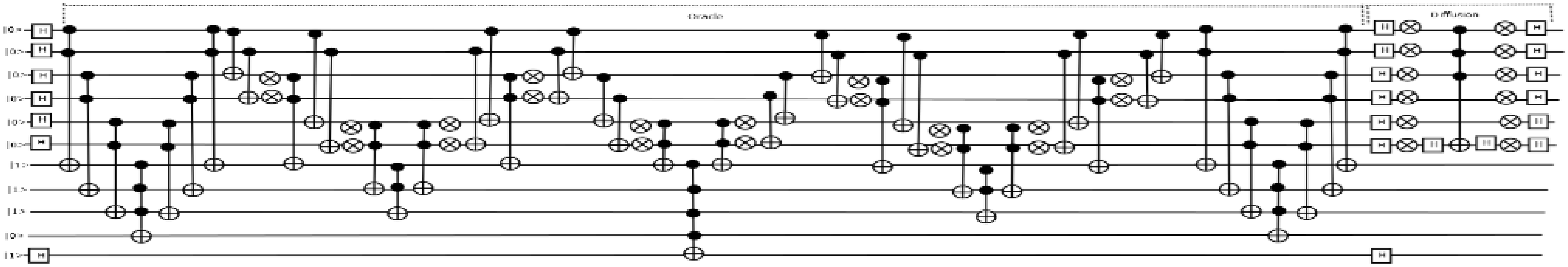


Invalid Color Detector



(b)

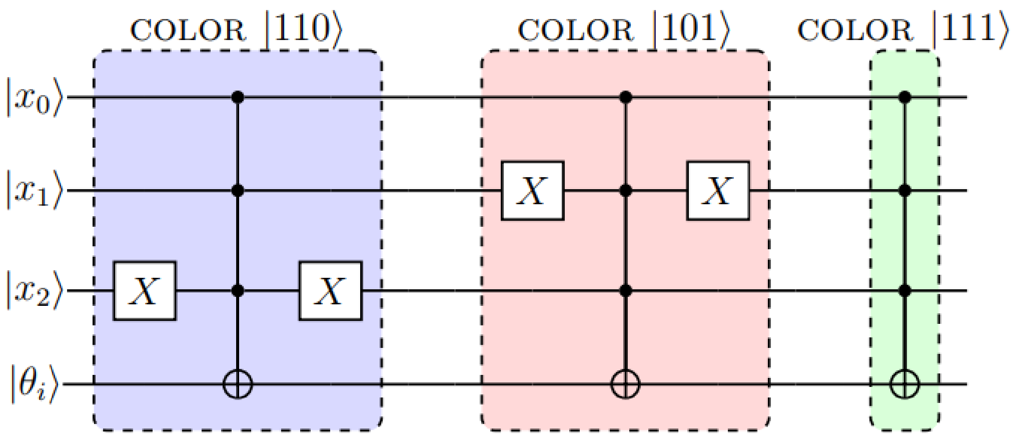
Comparator



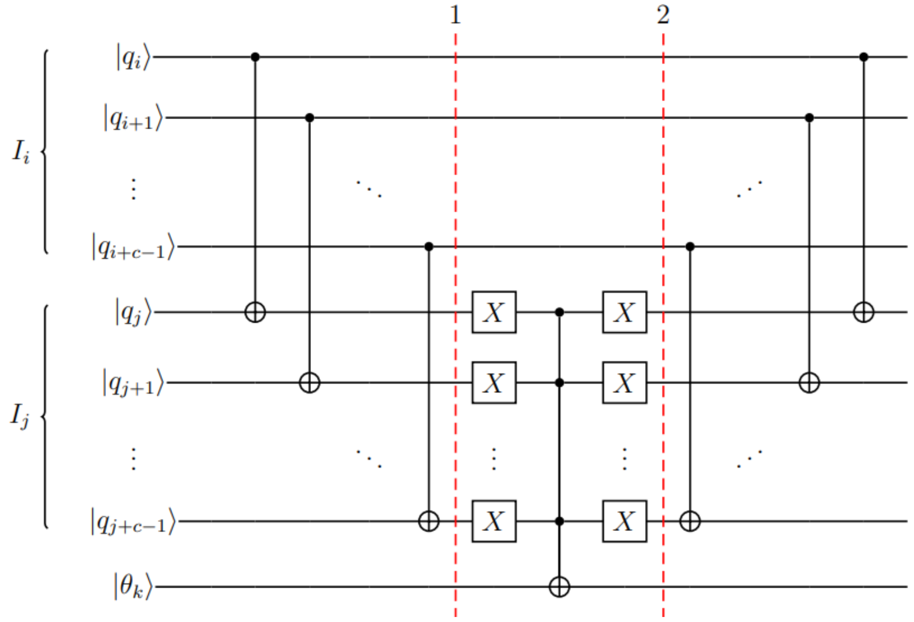
Circuit Diagram

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



Invalid Color Detector



Comparator

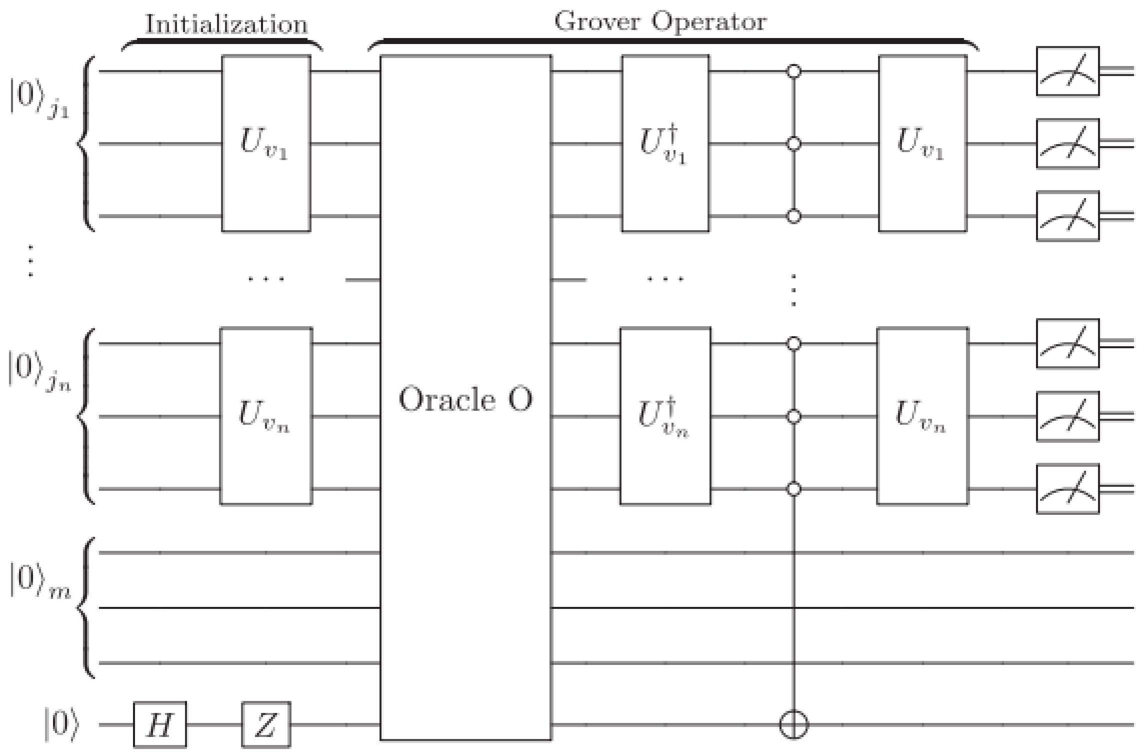
Reference : Lutze, D. (2021). Solving Chromatic Number with Quantum Search and Quantum Counting

List Coloring problem

Vertex Register

Edge Register

Ancilla Qubit Register

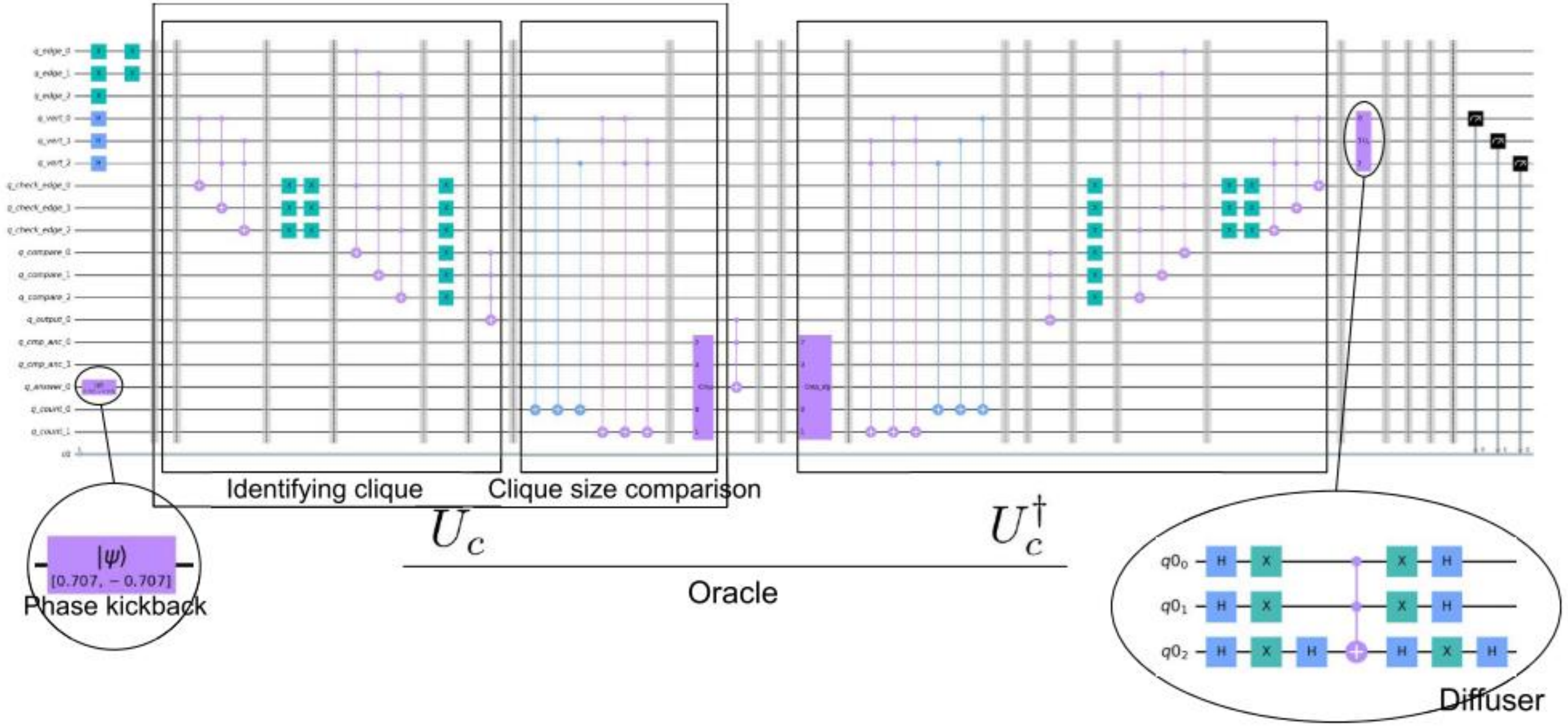


List Coloring Circuit

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

ACAN Laboratory

Maximum Clique



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.

Nash Equilibria

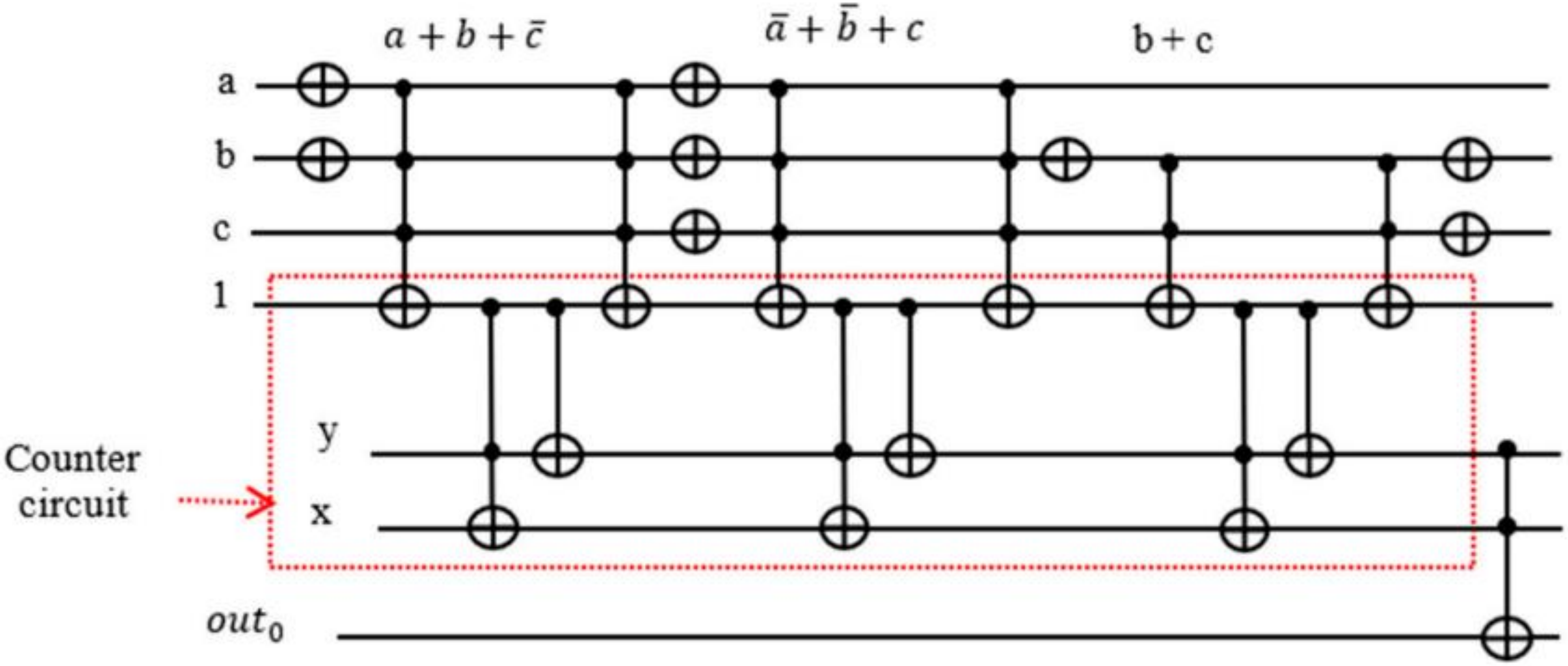
$$\mathcal{O}_{intra} = \mathcal{O}^{A}_{intra} \wedge \mathcal{O}^{B}_{intra} \wedge \cdots \wedge \mathcal{O}^{N}_{intra}$$

$$\mathcal{O}_{oracle} = \mathcal{O}_{intra} \wedge \mathcal{O}_{inter}$$

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.

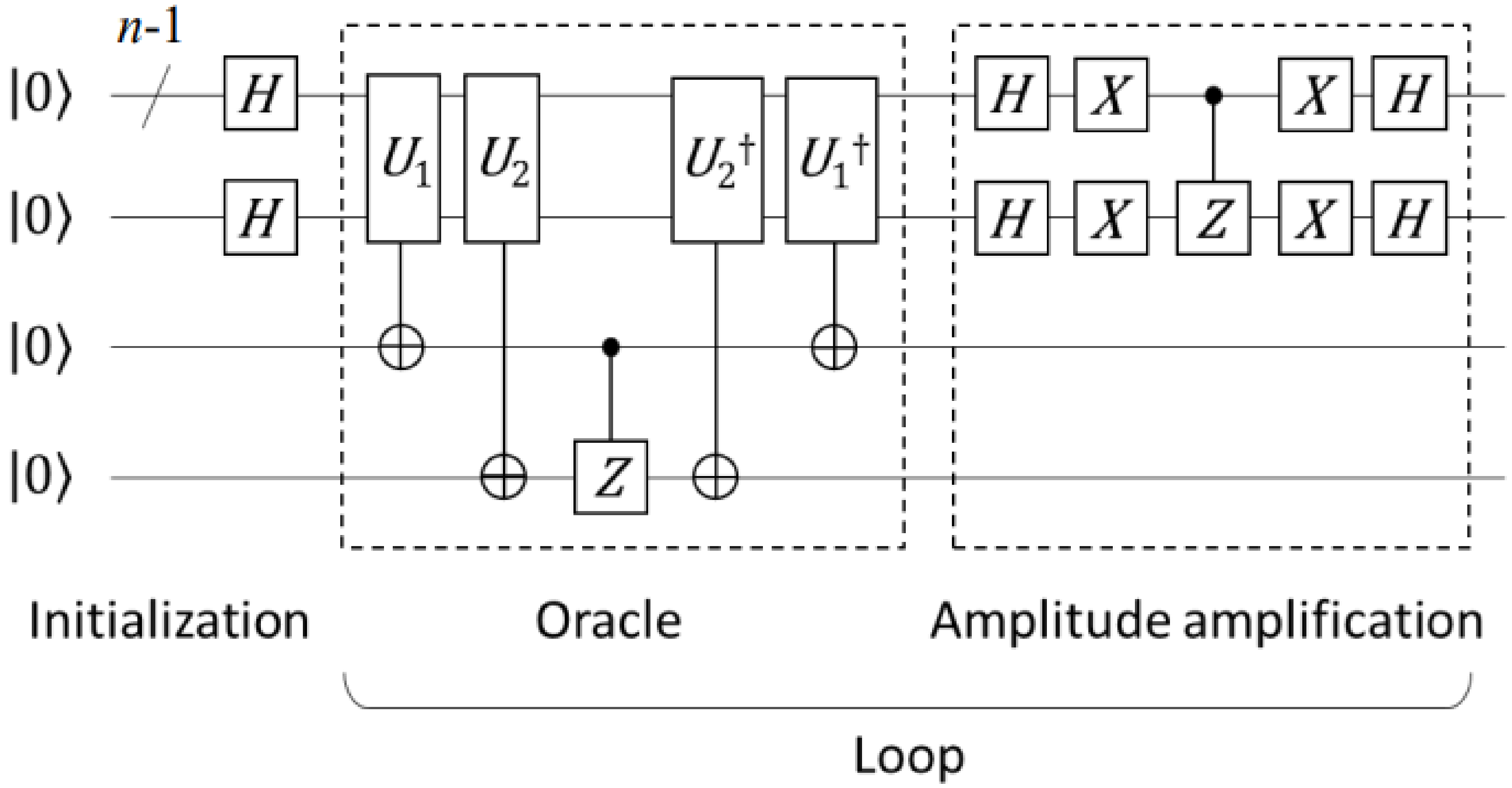
ACAN Laboratory

Maximum Satisfiability



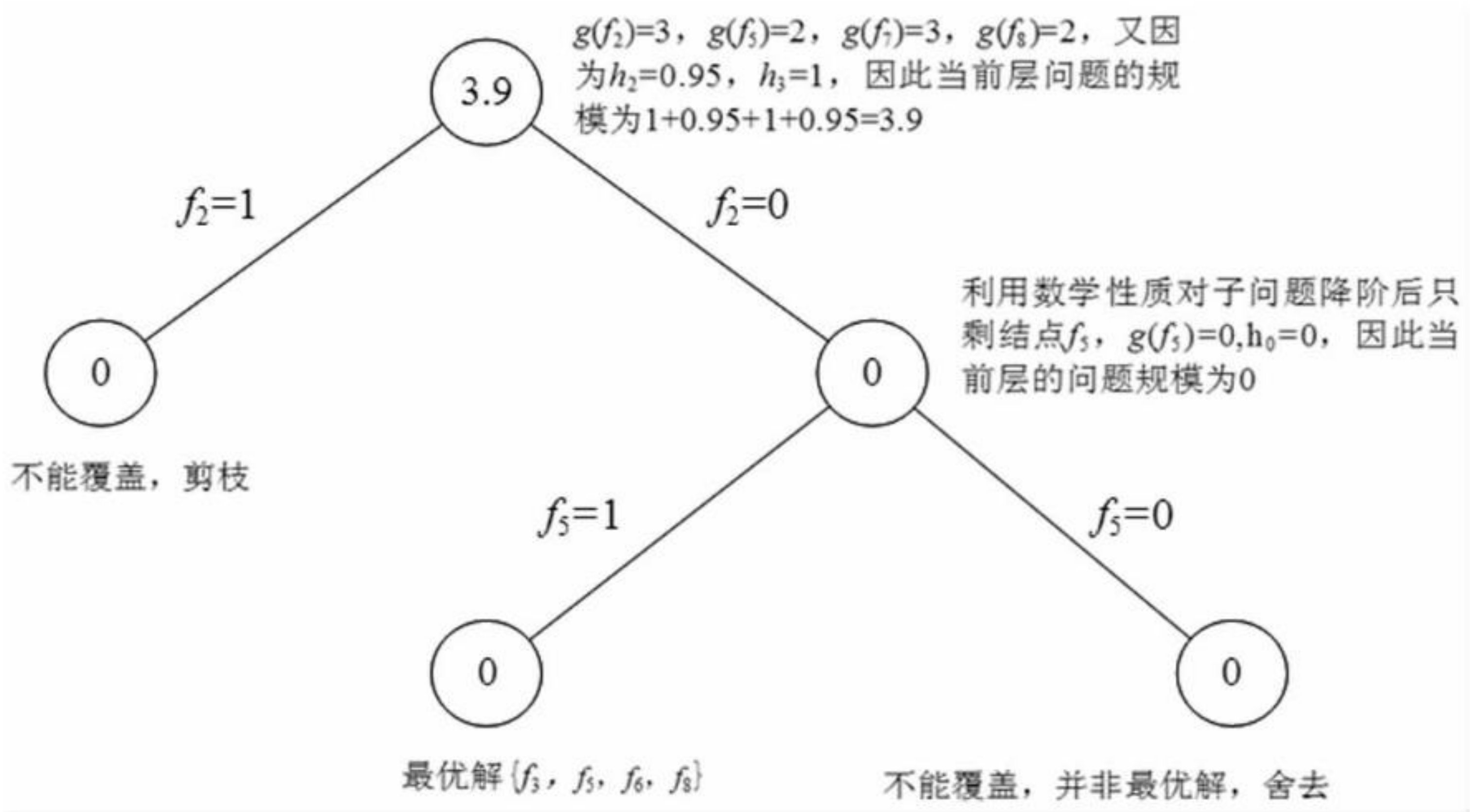
Reference : Alasow, A., & Perkowski, M. (2022, May). Quantum Algorithm for Maximum Satisfiability. In 2022 IEEE 52nd International Symposium on Multiple-Valued Logic (ISMVL) (pp. 27-34). IEEE

Drug Patent Analysis



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.

Measure and Conquer



Reference : HU Qin, NING Ai-bing, GOU Hai-wen, ZHANG Hui-zhen. Measure and Conquer Algorithm for Exact Cover Problem. Operations Research and Management Science, 2020, 29(4): 179-186.

X Algorithm

	1	2	3	4
A	0	1	1	0
B	1	0	1	1
C	0	1	0	0

(A)

	2
C	1

(B)

Reference : Knuth, D. E. (2000). Dancing links. arXiv preprint cs/0011047.

ACAN Laboratory