Practical Quantum Computing

Lecture 09
Grover's Algorithm

with slides from Dave Bacon https://homes.cs.washington.edu/~dabacon/teaching/siena/

Week	Tuesday (3h)			Wednesday (3h)			Deadlines	
1. The Basics	Introduction	Gates	Circuit Identities	Qiskit	Cirq/Qualtran	Q&A		
	Programming Assignment 1: The basics of a quantum circuit simulator			**Programming Assignment 1:** The building blocks of a quantum circuit simulator				
2. Entanglement and its Applications	Teleportation	Superdense Coding	Quantum Key Distribution	Qualtran/ Assignment2	Terminology of Projects	Q&A		
	Programming Assignment 2: The basics of a quantum circuit optimizer			**Programming Assignment 2:** The building blocks of a quantum circuit optimizer				
3. Computing	Phase Kickback and Toffoli	Distinguishing quantum states and The First Algorithms	Grover's Algorithm	Invited TBA	PennyLane	Q&A		11 May 2024
4. Advanced Topics*	Arithmetic Circuits*	Fault-Tolerance*	QML*	Invited TBA	Crumble	Q&A	18 May 2024	

* not evaluated

Learning goals - 09 Grover's Algorithm (Computing)

1. What you have learned by now
   a. Quantum circuits: mathematics, diagrams and circuit identities
   b. Entanglement: teleportation, quantum games, QKD
   c. Superpositions, Phase Kickback and finding hidden strings
2. **Grover's Algorithm - Searching unstructured data**
   a. Problem Statement: Imagine a list of elements and you have to find a particular one
   b. Why is it faster than classical search – sources of speedup
   c. The sequential application of two operations
      i. Marking found elements using phase kickback
      ii. Diffusion operation
   d. **Intuitive step by step illustration of functionality**

- Deadline for programming Assignment 1
- 11 May 2024

Applications of Grover's Algorithm

Grover's algorithm is a framework

- It does not offer the exponential speedup like Shor's alg.
- Can be extended for different problems
    - cryptanalysis AES
    - combinatorial optimisation - e.g. travelling salesman

Applying Grover's algorithm to AES: quantum resource estimates

Markus Grassl[1], Brandon Langenberg[2], Martin Roetteler[3], and Rainer Steinwandt[2]

[1] Universität Erlangen-Nürnberg & Max Planck Institute for the Science of Light, Günther-Scharowsky-Straße 1, Bau 24, 91058 Erlangen, Germany, Markus.Grassl@fau.de
[2] Florida Atlantic University, 777 Glades Road, Boca Raton, FL 33431, U.S.A., {blangenb, rsteinwa}@fau.edu
[3] Microsoft Research, One Microsoft Way, Redmond, WA 98052, U.S.A., martinro@microsoft.com

Abstract. We present quantum circuits to implement an exhaustive key search for the Advanced Encryption Standard (AES) and analyze the quantum resources required to carry out such an attack. We consider the overall circuit size, the number of qubits, and the circuit depth as measures for the cost of the presented quantum algorithms. Throughout, we focus on Clifford+T gates as the underlying fault-tolerant logical quantum gate set. In particular, for all three variants of AES (key size 128, 192, and 256 bit) that are standardized in FIPS-PUB 197, we establish precise bounds for the number of qubits and the number of elementary logical quantum gates that are needed to implement Grover's quantum algorithm to extract the key from a small number of AES plaintext-ciphertext pairs.

Keywords: quantum cryptanalysis, quantum circuits, Grover's algorithm, Advanced Encryption Standard

Implementing **Grover** oracles for quantum key search on **AES** and LowMC
S Jaques, M Naehrig, M Roetteler, F Virdia - ... International Conference on ..., 2020 - Springer
... Keywords. Quantum cryptanalysis **Grover's** algorithm **AES** LowMC Post-quantum cryptography Q# implementation ... Since the publication of [21], other works have studied quantum circuits for **AES**, the **AES Grover** oracle and its use in **Grover's** algorithm. Almazrooie et al ...
Cited by 31 Related articles All 9 versions

[HTML] **Grover** on $SIMON$ SIMON
R Anand, A Maitra, S Mukhopadhyay - Quantum Information Processing, 2020 - Springer
... However, this does not rule out the need of analyzing the cost of **Grover's** algorithm on symmetric ciphers. In this direction, subsequent efforts have been made to derive cost estimation for applying **Grover's** search algorithm on all variants of **AES** [7, 11, 17, 28] ...
Cited by 5 Related articles All 6 versions

[PDF] **Grover** on SPECK: quantum resource estimates
K Jang, S Choi, H Kwon, H Seo - eprint.iacr.org
... computing, pp. 212–219, 1996. 6. M. Grassl, B. Langenberg, M. Roetteler, and R. **Steinwandt**, "Applying **Grover's** algorithm to **AES**: quantum resource estimates," in Post-Quantum Cryptography, pp. 29–43, Springer, 2016. 7. B ...
Cited by 4 Related articles

[PDF] Observations on the Quantum Circuit of the SBox of **AES**.
J Zou, Y Liu, C Dong, W Wu, L Dong - IACR Cryptol. ePrint Arch., 2019 - eprint.iacr.org
... [3] Markus Grassl, Brandon Langenberg, Martin Roetteler, and Rainer **Stein- wandt** ... TimeCspace complexity of quantum search algorithms in symmetric cryptanalysis: applying to **AES** and SHA-2. Quantum Information ... 8] Brandon Langenberg, Hai Pham, and Rainer **Steinwandt** ...
Cited by 2 Related articles

Quantum Resource Estimates of **Grover's** Key Search on ARIA
AK Chauhan, SK Sanadhya - International Conference on Security, Privacy ..., 2020 - Springer
... [10] studied the quantum circuits of **AES** and estimated the cost of quantum resources needed to apply **Grover's** algorithm to the **AES** oracle for key search. Almazrooie et al ... As a working example, they implemented the **AES Grover** oracle in Q# quantum programming language ...
Related articles

Solving Binary $\mathcal{MQ}$ with **Grover's** Algorithm
P Schwabe, B Westerbaan - ... Conference on Security, Privacy, and Applied ..., 2016 - Springer
... primitives. For example, in [GLRS16], Grassl, Langenberg, Roetteler, and **Steinwandt** describe how to attack **AES**-128 with **Grover's** algorithm using a quantum computer with 2953 logical qubits in time about \(2^{87}\). We note ...
Cited by 25 Related articles All 12 versions

Quantum **Grover** Attack on the Simplified-**AES**
M Almazrooie, R Abdullah, A Samsudin... - Proceedings of the 2018 ..., 2018 - dl.acm.org
... This paper is organized as follows: Sections 2 and 3 review the Simplified-**AES** (S-**AES**) cryptosystem and the quantum **Grover's** algorithm, respectively ... Figure 8. Applying **Grover** attack on S-**AES**. Figure 8 illustrates the complete model of the **Grover** attack against S-**AES** ...
Related articles

Borbely E. Grover search algorithm. arXiv preprint arXiv:0705.4171. 2007 May 29. - step by step derivation of Grover iterations

Quantum computers can search faster than a classical ones

- Assume the entries are indexed 0, 1, 2, 3, …., N

- Use binary vectors
  - Of the form 0 = 10….000, 1 = 01….000, … , N = 00...001
  - The length of the vectors is N bits
  - A bit signals if an entry is found in the database
  - Practically, multiple entries can be sought and then multiple bits will be on

- E.g. the vector |3> will have a 1 at the fourth index (zero-indexed)

$$\begin{array}{c} |0> \\ |1> \\ |2> \\ |3> \end{array} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

- Search: “Is the entry with index F in the list 0,1,…..,N?”

- Simplify and assume that the search is always for F=N (relabel the database entries)

Building block - Inner product

The why: We will use this notation to determine the relative rotation (angle) between two vectors

Example: a = (0, 0, 0, 1) b = (1, 1, 1, 1) -> ab = 0*1 + 0*1 + 0*1 + 1*1 = 1

Can be written as the multiplication of a row vector with a column vector

$$(0, 0, 0, 1) \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = 0*1 + 0*1 + 0*1 + 1*1 = 1$$

Depending if the vector is row or column we can use special notation

<a| for row vector

|a> for column vector

such that <a||b> is the notation for the inner product

Shorthand notation <a|b> = 1

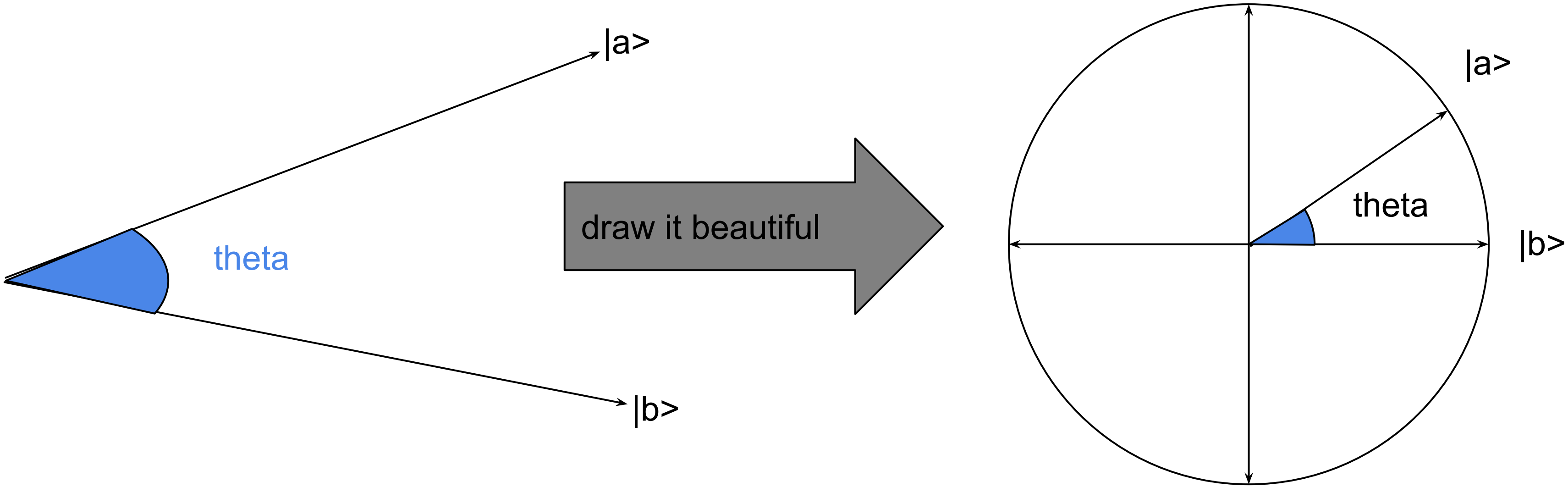
Building block - Angle between vectors

The why: Useful for building a method to rotate a third vector by knowing the angle between two other vectors

In general, <a|b> = |a||b|cos(theta)

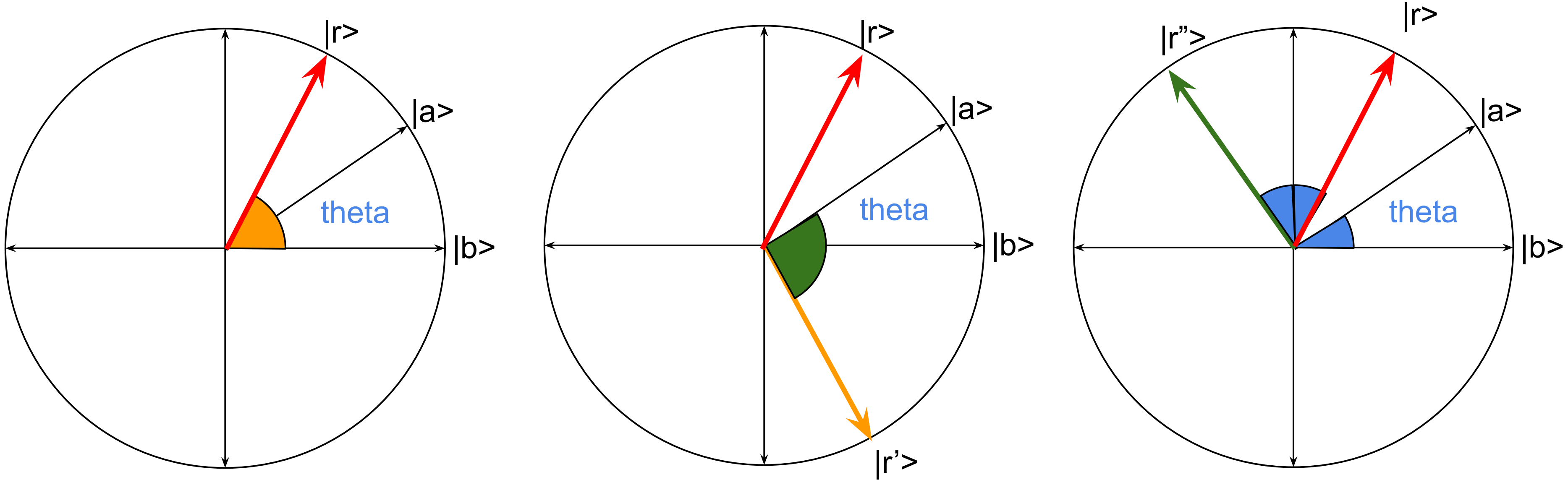
where |a| and |b| are the length of the vectors

Simplify and assume that all vectors have unit length, such that <a|b> = cos(theta)



Building block - rotate with twice the angle of theta

The why: Build a method to move |r> such that it is orthogonal to |b>

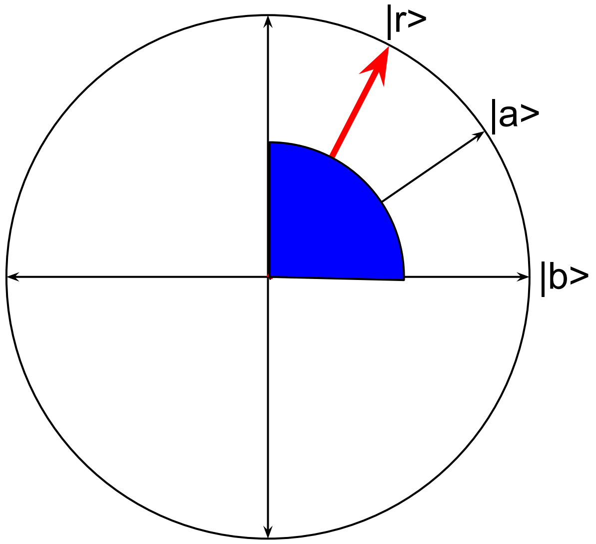


after mirror against |b>

after mirror against |a>

Building block - Number of mirror seq. to rotate pi/2

The why: It indicates where the quantum speed-up is coming from!



How many rotations (k=?) are necessary to get to pi/2?

theta + **k***2*theta = pi/2

2**k** = pi/(2 * theta) - 1

k = round(pi/(4*theta) - ½)

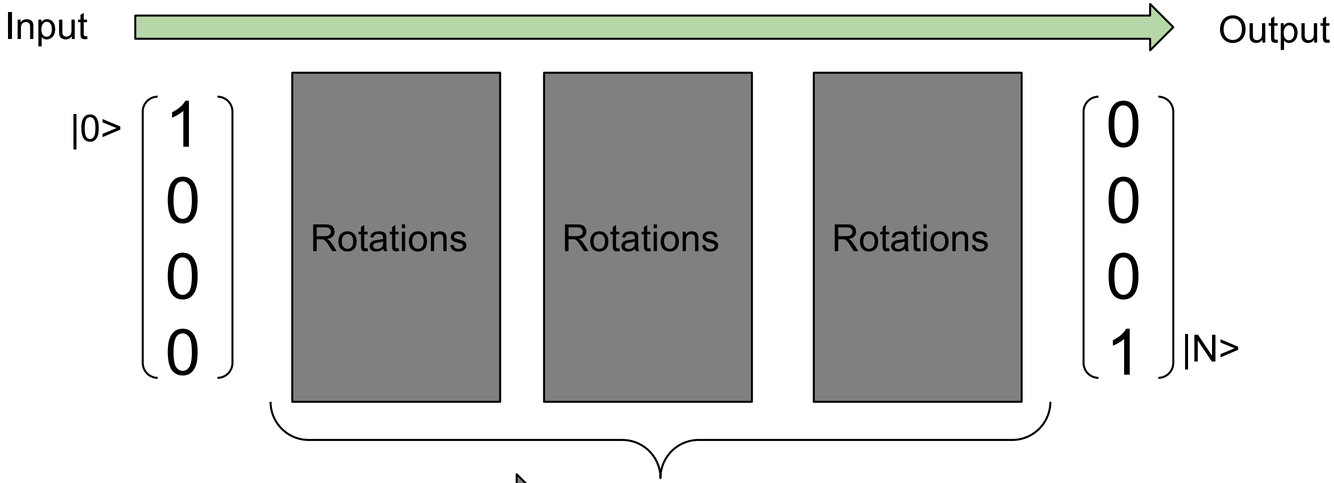
Use large values of M to create very small angles **theta = 1/M**
Example: sin(1/256) = 1/256, cos(1/256) = 1

k = approx. M

The difference between classical and quantum is the value of M!

Input to Output

The why: This is a sketch of a quantum circuit looks like



M times

blue is for the Grover speedup

Classical computer:

- exhaustive **$M=N=2^n$**
- random **$M=N/2=2^{n-1}$**

red is for classical runtime

Building rotations - Outer product - Rotations

The why: Mirroring against the two vectors has to be implemented mathematically

1) Transform **|0> to |1>** and **|1> to |0>** where $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

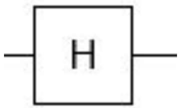
The **bit flip matrix X** = $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ = **|0X1| + |1X0|**

2) Define a matrix that takes **|0> to |+> = |0>+|1> and |1> to |-> = |0>-|1>**

$|0\rangle(\langle 0| + \langle 1|) = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$

$|1\rangle(\langle 1| - \langle 1|) = \begin{pmatrix} 0 & 0 \\ 1 & -1 \end{pmatrix}$

$\rightarrow \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ (almost) **Hadamard matrix**

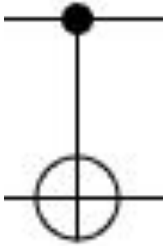


3) Define a matrix that **applies the X matrix only if the state of another vector is |1>**

|00X00| + |01X01| + |10X11| + |11X10|

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

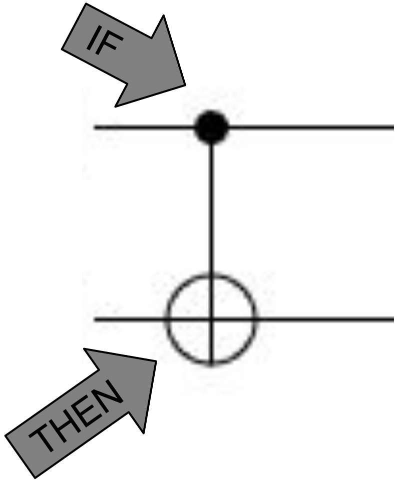
CNOT matrix

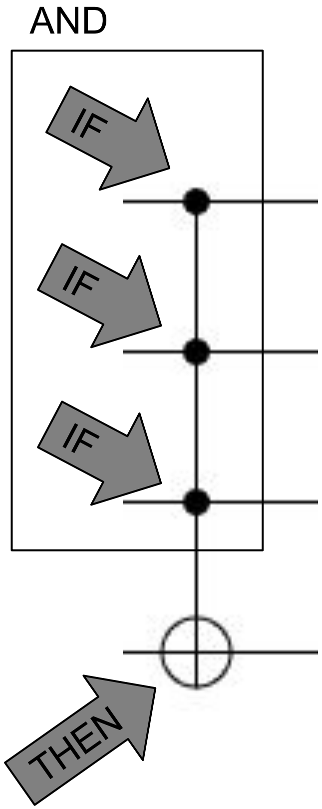


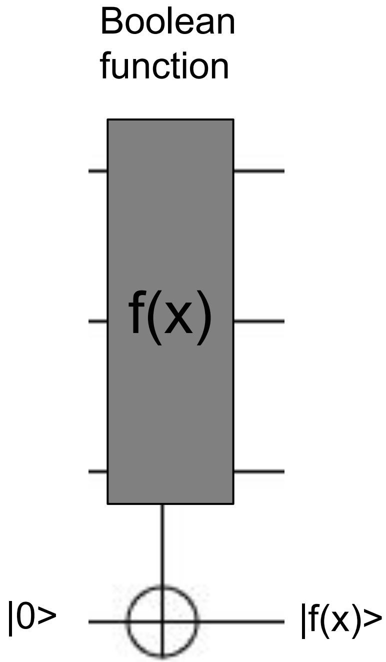
Building rotations - Encoding conditions for rotations

The why: Recipe for building rotations depending on configurable criteria

Classical problems can be imported into a quantum algorithm







The quantum state

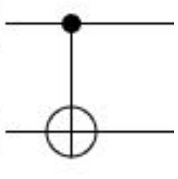
The why: There is an exponential representational explosion that is often mentioned when quantum computations are discussed

Previous statement: *All vectors have unit length*

A quantum state is a complex vector whose **L2 norm** is 1

- A qubit is a 2-dimensional complex vector. Examples |0>, |1>, |+>, |->
- The state of a n-qubit circuit is a 2^n-dimensional complex vector

  Example n=2, the state has four entries and the matrix has size 4 x 4

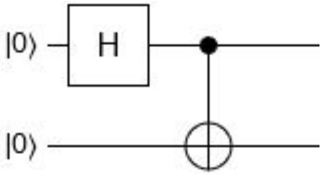


$$\underbrace{\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}}_{2^n} \left.\vphantom{\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}}\right\} 2^n$$

A quantum circuit is a 2^n x 2^n matrix

Entries in a state vector can be different from zero

Bell state $2^{-1/2}$(|00> + |11>)

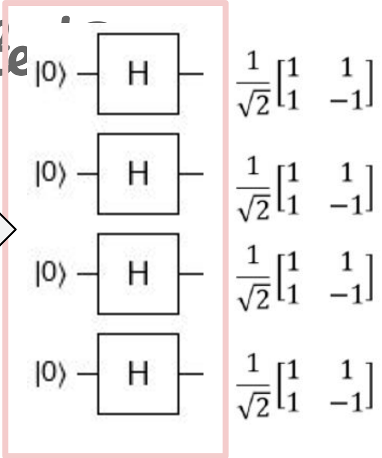


The superposition state

An n-qubit state has length 2^n

Define the n-qubit equal superposition |S> with H gates

$|S> = 2^{-n/2} (|00....00> + |00....01> + ... + |11....11>)$



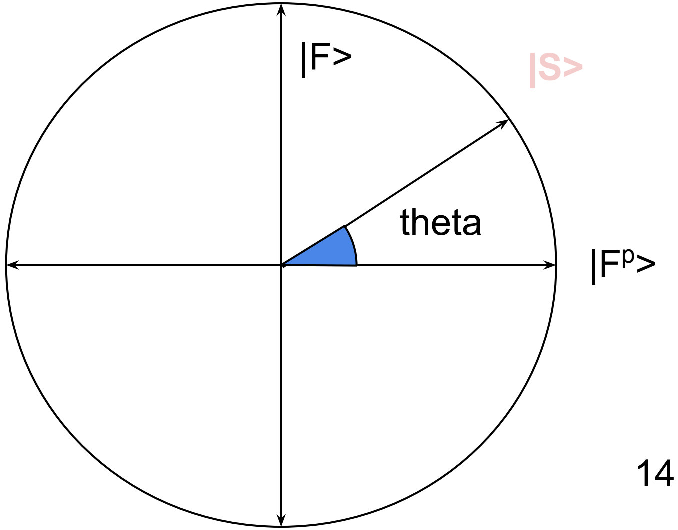
Assume that the sought element is $|N>=|11....11>$

$$<F|S> = 2^{-n/2} = 1/M$$

As a result, $M = sqrt(2^n)$ **rotations are needed**

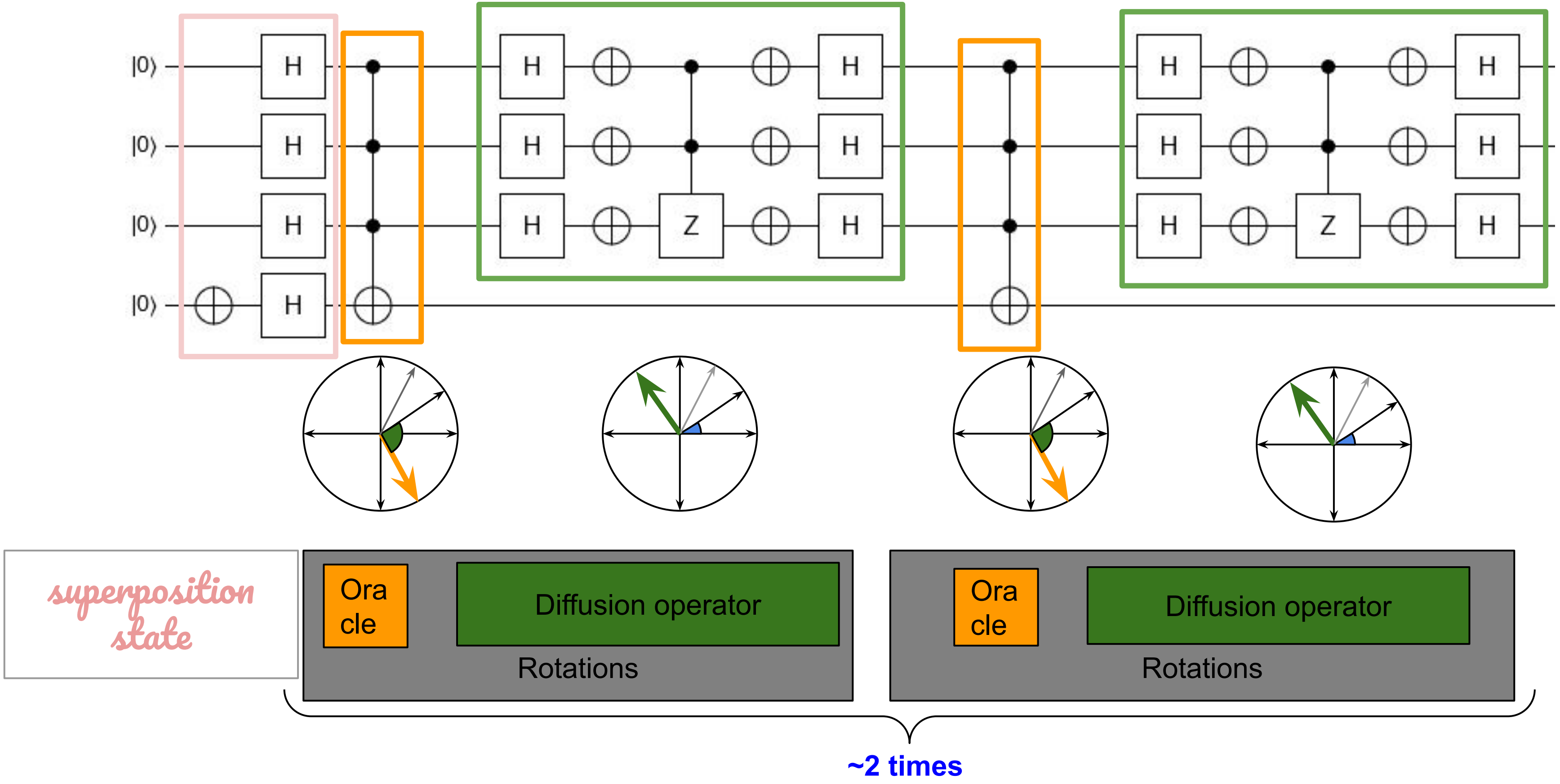
Each rotation (called Grover iteration) consists of

1) **mirror around $|F^p>$**
2) **mirror around |S>**



The why: We create a small enough angle necessary to implement the sequence of rotations with the necessary speedup

The Grover search circuit for n=3 qubits



Grover's Algorithm Summary

For N = 1000 entries

- classical exhaustive search method needs 1000 steps
- Grover's algorithm needs approx. 32 steps

The key concepts presented:

- quantum qubit, gate, circuit
- how to import classical problems (Boolean logic) into quantum circuits

The key elements of the algorithm are:

- Mirroring operations
    - a known vector - the equal superposition state
    - a configurable vector - the search criteria
    - mirror operations are implemented with quantum gates
- The speed-up is from the L2 norm to calculate the distance between two qubit states