

# Saturs

1. Bra-Ket Notation .....	1	4.2.2. Entangled States .....	4
1.1. Ket $ \psi\rangle$ .....	1	4.3. Multi-Qubit Measurement & Normalization .....	4
1.1.1. Basis states .....	2	5. Quantum Logic Gates & Circuits .....	4
1.2. Bra $\langle\psi $ .....	2	5.1. Common Multi-Qubit Gates .....	4
1.3. Scalar Product $\langle\varphi \psi\rangle$ .....	2	5.1.1. <i>CNOT</i> (Controlled-NOT) .....	4
1.3.1. Orthogonal states .....	2	5.1.2. <i>SWAP</i> Gate .....	4
1.4. Projection $\langle i \psi\rangle$ .....	2	5.1.3. Toffoli Gate ( <i>CCNOT</i> ) .....	4
2. Fundamentals .....	2	5.1.4. Universality (Universalitāte) .....	4
2.1. Qubit (Kvantu bits) .....	2	6. Key Quantum Protocols & Concepts .....	4
2.1.1. Basis states .....	2	6.1. No-Cloning Theorem .....	4
2.1.2. Superposition .....	2	6.2. Quantum Teleportation .....	5
2.1.3. Normalization .....	2	6.3. Dense Coding (Bļīvā kodēšana) .....	5
2.1.4. Bloch Sphere .....	2	6.3.1. Steps .....	5
2.2. Measurement (Mērījumi) .....	2	7. Quantum Algorithms .....	5
2.2.1. Measurement operators .....	2	7.1. Oracle ( $U_f$ ) .....	5
2.2.2. Measuring in $ +\rangle,  -\rangle$ basis .....	2	7.1.1. Phase kickback .....	5
3. Single Qubit Unitary Transformations .....	2	7.2. Deutsch's Algorithm .....	5
3.0.1. Properties .....	2	7.3. Grover's Search Algorithm .....	5
3.0.2. Matix form .....	2	7.4. Quantum Fourier Transform (QFT) .....	6
3.1. Pauli Gates .....	3	7.5. Period Finding (Kvantu algoritms perioda atrašanai) .....	6
3.1.1. I (Identity) .....	3	7.6. Shor's Algorithm (Skaitļa sadalīšanai reizinātājos) .....	6
3.1.2. X (NOT) .....	3	7.7. Simon's Algorithm .....	6
3.1.3. Y Gate .....	3	8. Advanced Topics .....	7
3.1.4. Z Gate .....	3	8.1. Density Matrices (Blīvuma matricas $\rho$ ) .	7
3.2. Hadamard Gate ( $H$ ) .....	3	8.2. Quantum Cryptography .....	7
3.3. Phase Gates .....	3	8.2.1. BB84 Protocol .....	7
3.3.1. $S$ Gate ( $\sqrt{Z}$ ) .....	3	8.2.2. Security .....	7
3.3.2. $T$ Gate ( $\frac{\pi}{8}$ ) .....	3	8.3. Quantum Error Correction .....	7
3.4. Rotation Gates ( $R_n(\theta)$ ) .....	3	8.3.1. 3-Qubit Bit Flip Code .....	7
3.5. Game Compositions .....	3	8.3.2. 3-Qubit Phase Flip Code .....	7
3.6. Inverse Transformation .....	3	8.3.3. Shor's 9-Qubit Code .....	7
3.7. Non-Unitary Operations .....	3		
3.7.1. Qubit Deletion .....	3		
4. Multi-Qubit Systems .....	3		
4.1. Tensor product .....	3		
4.1.1. Operators .....	3		
4.2. Product States vs. Entangled States .....	3		
4.2.1. Product state .....	3		

## 1. Bra-Ket Notation

### 1.1. Ket $|\psi\rangle$

Represents a column vector for a quantum state.

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \iff \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

### 1.1.1. Basis states

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

### 1.2. Bra $\langle\psi|$

Represents a **conjugate transpose vector (kompleksi saistīts)** (row vector) of  $|\psi\rangle$ .

$$\text{If } |\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \text{ then } \langle\psi| = (a^* \quad b^*)$$

### 1.3. Scalar Product $\langle\varphi|\psi\rangle$

Inner product of two states.

$$\text{If } |\varphi\rangle = \gamma|0\rangle + \delta|1\rangle, \text{ then } \langle\varphi|\psi\rangle = \gamma^*\alpha + \delta^*\beta$$

### 1.3.1. Orthogonal states

$$\langle\varphi|\psi\rangle = 0$$

### 1.4. Projection $\langle i|\psi\rangle$

Amplitude of the basis state  $|i\rangle$  in  $|\psi\rangle$ .

$$\text{For } |\psi\rangle = \alpha|0\rangle + \beta|1\rangle : \langle 0|\psi\rangle = \alpha, \langle 1|\psi\rangle = \beta.$$

$$\text{Probability of measuring state } |i\rangle : P(i) = |\langle i|\psi\rangle|^2$$

## 2. Fundamentals

### 2.1. Qubit (Kvantu bits)

#### 2.1.1. Basis states

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

#### 2.1.2. Superposition

A qubit can be in a linear combination of basis states:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \text{ where } \alpha, \beta \in \mathbb{C}$$

are probability amplitudes.

#### 2.1.3. Normalization

$$|\alpha|^2 + |\beta|^2 = 1$$

$|\alpha|^2$  is the probability of measuring  $|0\rangle$ ,  $|\beta|^2$  is the probability of measuring  $|1\rangle$ .

#### 2.1.4. Bloch Sphere

Geometric representation of a single qubit state:

$$|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle$$

## 2.2. Measurement (Mērījumi)

• Projective measurement in the basis (e.g. computational  $\{|0\rangle, |1\rangle\}$  or Hadamard  $\{|+\rangle, |-\rangle\}$ ).

• If state is  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ :

– Outcome 0: probability  $P(0) = |\langle 0|\psi\rangle|^2 = |\alpha|^2$ .

Post-measurement state:  $|0\rangle$ .

– Outcome 1: probability  $P(1) = |\langle 1|\psi\rangle|^2 = |\beta|^2$ .

Post-measurement state:  $|1\rangle$ .

• Measurement collapses the superposition (mērījums maina kvantu bitu (observer effect)).

### 2.2.1. Measurement operators

$$M_0 = |0\rangle\langle 0|, M_1 = |1\rangle\langle 1|$$

$$\sum_m M_m^\dagger M_m = I$$

### 2.2.2. Measuring in $|+\rangle, |-\rangle$ basis

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

To measure  $|0\rangle$  in this basis:  $|0\rangle = \frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle$ .

$$P(+)=|\langle +|0\rangle|^2 = \frac{1}{2}, P(-)=|\langle -|0\rangle|^2 = \frac{1}{2}$$

#### 2.2.2.1. Example: $|\psi\rangle = \frac{1+2i}{\sqrt{7}}|0\rangle + \frac{1-i}{\sqrt{7}}|1\rangle$

$$P(0) = \left| \frac{1+2i}{\sqrt{7}} \right|^2 = \frac{1^2 + 2^2}{7} = \frac{5}{7}$$

$$P(1) = \left| \frac{1-i}{\sqrt{7}} \right|^2 = \frac{1^2 + (-1)^2}{7} = \frac{2}{7}$$



#### Tip

Sum must be 1.

## 3. Single Qubit Unitary Transformations

Quantum gates are unitary matrices  $U$ .

• Unitary condition:  $UU^\dagger = U^\dagger U = I$ , where  $U^\dagger$  is the conjugate transpose.

• Action on state  $|\psi'\rangle = U|\psi\rangle$

### 3.0.1. Properties

Linearity ( $U(\alpha|\psi_1\rangle + \beta|\psi_2\rangle) = \alpha U|\psi_1\rangle + \beta U|\psi_2\rangle$ ) and preserves vector length.

### 3.0.2. Matix form

If  $U|0\rangle = a|0\rangle + b|1\rangle$  and  $U|1\rangle = c|0\rangle + d|1\rangle$ , then

$$U = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

Columns (and rows) must be orthonormal vectors:

$$\vec{v}_1^* \cdot \vec{v}_2 = 0 \text{ and } |\vec{v}_1|^2 = 1.$$

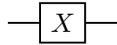
### 3.1. Pauli Gates

#### 3.1.1. I (Identity)

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \begin{cases} I|0\rangle = |0\rangle \\ I|1\rangle = |1\rangle \end{cases}$$

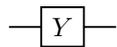
#### 3.1.2. X (NOT)

Bit flip



$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \begin{cases} X|0\rangle = |1\rangle \\ X|1\rangle = |0\rangle \end{cases}$$

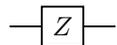
#### 3.1.3. Y Gate



$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \begin{cases} Y|0\rangle = -i|1\rangle \\ Y|1\rangle = i|0\rangle \end{cases}$$

#### 3.1.4. Z Gate

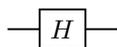
Phase flip



$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \begin{cases} Z|0\rangle = |0\rangle \\ Z|1\rangle = -|1\rangle \end{cases}$$

### 3.2. Hadamard Gate (H)

Creates superpositions



$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \begin{cases} H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \\ H|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \end{cases}$$

$$\begin{cases} H|0\rangle = |+\rangle \\ H|1\rangle = |-\rangle \end{cases} \quad HH = H^2 = I$$

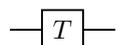
### 3.3. Phase Gates

#### 3.3.1. S Gate ( $\sqrt{Z}$ )



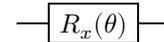
$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad S^2 = Z$$

#### 3.3.2. T Gate ( $\frac{\pi}{8}$ )

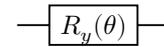


$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix} \quad T^2 = S$$

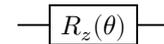
### 3.4. Rotation Gates ( $R_n(\theta)$ )



$$R_x(\theta) = e^{-\frac{i\theta X}{2}} = \begin{pmatrix} \cos \frac{\theta}{2} & -i \sin \frac{\theta}{2} \\ -i \sin \frac{\theta}{2} & \cos \frac{\theta}{2} \end{pmatrix}$$



$$R_y(\theta) = e^{-\frac{i\theta Y}{2}} = \begin{pmatrix} \cos \frac{\theta}{2} & -\sin \frac{\theta}{2} \\ \sin \frac{\theta}{2} & \cos \frac{\theta}{2} \end{pmatrix}$$



$$R_z(\theta) = e^{-\frac{i\theta Z}{2}} = \begin{pmatrix} e^{-\frac{i\theta}{2}} & 0 \\ 0 & e^{\frac{i\theta}{2}} \end{pmatrix}$$



**Tip**

$$R_\alpha : \begin{cases} R_\alpha|0\rangle: \cos \alpha|0\rangle + \sin \alpha|1\rangle \\ R_\alpha|1\rangle: -\sin \alpha|0\rangle + \cos \alpha|1\rangle \end{cases}. \text{ This is } R_{y(-2\alpha)}.$$

### 3.5. Gate Compositions

Applied right to left.  $UV|\psi\rangle = U(V|\psi\rangle)$ .

- $HZH = X$
- $HXH = Z$

### 3.6. Inverse Transformation

$$U^{-1} = U^\dagger$$

### 3.7. Non-Unitary Operations

(Not physically realizable as closed system evolution)

#### 3.7.1. Qubit Deletion

$$\begin{cases} U|0\rangle = |0\rangle \\ U|1\rangle = |0\rangle \end{cases}$$

### 4. Multi-Qubit Systems

#### 4.1. Tensor product

Combines state space.

$$\begin{aligned} (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) &= \\ = ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle \end{aligned}$$

For  $k$  qubits,  $2^k$  basis states.

#### 4.1.1. Operators

$$(A \otimes B)(|\psi_A\rangle \otimes |\psi_B\rangle) = (A|\psi_A\rangle) \otimes (B|\psi_B\rangle)$$

#### 4.2. Product States vs. Entangled States

##### 4.2.1. Product state

Can be written as  $|\psi_A\rangle \otimes |\psi_B\rangle$ .

### 4.2.1.1. Example

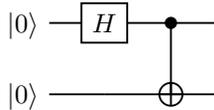
$$\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) = \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) \otimes \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right)$$

### 4.2.2. Entangled States

Cannot be factored

#### 4.2.2.1. Example

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \text{ (Bell state } |\Phi^+\rangle)$$



### 4.3. Multi-Qubit Measurement & Normalization

Measure one qubit from a multi-qubit system.

#### 4.3.0.1. Example

##### 4.3.0.1.1. State

$$a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$$

##### 4.3.0.1.2. Measure 1st qubit

###### 4.3.0.1.2.1. Prob of 0

$$P(q_1 = 0) = |a|^2 + |b|^2$$

Post-measurement state:

$$\frac{a|00\rangle + b|01\rangle}{\sqrt{|a|^2 + |b|^2}} = |0\rangle \otimes \frac{a|0\rangle + b|1\rangle}{\sqrt{|a|^2 + |b|^2}}$$

###### 4.3.0.1.2.2. Prob of 1

$$P(q_1 = 1) = |c|^2 + |d|^2$$

Post-measurement state:

$$\frac{c|10\rangle + d|11\rangle}{\sqrt{|c|^2 + |d|^2}} = |1\rangle \otimes \frac{c|0\rangle + d|1\rangle}{\sqrt{|c|^2 + |d|^2}}$$

#### 4.3.0.2. Example

##### 4.3.0.2.1. State

$$\frac{2}{3}|00\rangle + \frac{1}{3}|01\rangle + \frac{2}{3}|10\rangle$$

##### 4.3.0.2.2. Measure 1st qubit

###### 4.3.0.2.2.1. Prob of 0

$$P(0) = \left(\frac{2}{3}\right)^2 + \left(\frac{1}{3}\right)^2 = \frac{5}{9}$$

State of 2nd qubit:

$$\frac{\frac{2}{3}|0\rangle + \frac{1}{3}|1\rangle}{\sqrt{\frac{5}{9}}} = \frac{1}{\sqrt{5}}(2|0\rangle + |1\rangle)$$

#### 4.3.0.2.2.2. Prob of 1

$$P(1) = \left(\frac{2}{3}\right)^2 = \frac{4}{9}$$

State of 2nd qubit:

$$\frac{\frac{2}{3}|0\rangle}{\sqrt{\frac{4}{9}}} = |0\rangle$$

## 5. Quantum Logic Gates & Circuits

### 5.1. Common Multi-Qubit Gates

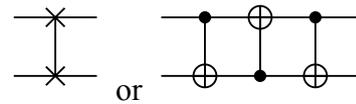
#### 5.1.1. CNOT (Controlled-NOT)

$$CNOT|c\rangle|t\rangle = |c\rangle|t \oplus c\rangle$$



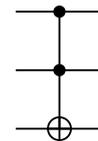
#### 5.1.2. SWAP Gate

Swaps two qubits.



#### 5.1.3. Toffoli Gate (CCNOT)

$$CCNOT|c_1 c_2 t\rangle = |c_1 c_2 t \oplus (c_1 \cdot c_2)\rangle$$



#### 5.1.4. Universality (Universalitāte)

Jebkurai unitārai  $U$ :  $U = U_m U_{m-1} \dots U_1$ , katra  $U_i$  maina tikai 2 bāzes stāvokļus

$$U_i|x_1 \dots x_n\rangle = a|x_1 \dots x_n\rangle + b|y_1 \dots y_n\rangle$$

$$U_i|y_1 \dots y_n\rangle = c|x_1 \dots x_n\rangle + d|y_1 \dots y_n\rangle$$

$$U_i|z_1 \dots z_n\rangle = |z_1 \dots z_n\rangle$$

ja  $z_1 \dots z_n \neq x_1 \dots x_n, z_1 \dots z_n \neq y_1 \dots y_n$ .

## 6. Key Quantum Protocols & Concepts

### 6.1. No-Cloning Theorem

Impossible to create an identical copy of an arbitrary unknown quantum state.

## 6.2. Quantum Teleportation

Transmits  $|\psi\rangle = a|0\rangle + b|1\rangle$  using an entangled pair  $|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$  and 2 classical bits.

Initial state (Alice has  $|\psi\rangle_C$  and qubit  $A$ , Bob has  $B$ ):

$$\begin{aligned} |\psi\rangle_C \otimes |\Phi^+\rangle_{AB} &= \\ &= (a|0\rangle_C + b|1\rangle_C) \frac{1}{\sqrt{2}}(|0_A0_B\rangle + |1_A1_B\rangle) = \\ &= \frac{a}{\sqrt{2}}|000\rangle + \frac{a}{\sqrt{2}}|011\rangle + \frac{b}{\sqrt{2}}|100\rangle + \frac{b}{\sqrt{2}} \end{aligned}$$

(qubits  $C, A, B$ )

Alice applied  $CNOT$  ( $C$  is control,  $A$  is target):

$$\frac{a}{\sqrt{2}}|000\rangle + \frac{a}{\sqrt{2}}|011\rangle + \frac{b}{\sqrt{2}}|110\rangle + \frac{b}{\sqrt{2}}|101\rangle$$

Alice applies  $H$  to qubit  $C$ :

$$\begin{aligned} \frac{1}{2}[a(|0\rangle + |1\rangle)|11\rangle + a(|0\rangle + |1\rangle)|11\rangle + \\ + b(|0\rangle - |1\rangle)|10\rangle + b(|0\rangle - |1\rangle)|01\rangle] \end{aligned}$$

Regroup by Alice's qubits  $CA$ :

$$\begin{aligned} \frac{1}{2}[|00\rangle_{CA}(a|0\rangle + b|1\rangle) + |01\rangle_{CA}(a|1\rangle + b|0\rangle) + \\ + |10\rangle_{CA}(a|0\rangle - b|1\rangle) + |11\rangle_{CA}(a|1\rangle - b|0\rangle)] \end{aligned}$$

Alice measures  $CA$ , sends 2 classical bits to Bob. Bob applies correction to his qubit  $B$ :

- Alice gets 00  $\implies$  Bob has  $a|0\rangle + b|1\rangle$  (Needs  $I$ ).
- Alice gets 01  $\implies$  Bob has  $a|1\rangle + b|0\rangle$  (Needs  $X$ ).
- Alice gets 10  $\implies$  Bob has  $a|0\rangle - b|1\rangle$  (Needs  $Z$ ).
- Alice gets 11  $\implies$  Bob has  $a|1\rangle - b|0\rangle$  (Needs  $ZX$ ).

## 6.3. Dense Coding (Bĭivā koděšana)

Sends 2 classical bits of information From Alice to Bob by sending only 1 qubit, using pre-shared entangled pair.

### 6.3.1. Steps

- 1) Alice and Bob share  $|\Phi^+\rangle_{AB}$
- 2) To send classical bits  $xy$ :
  - 00: Alice does nothing (applies  $I$ ) to her qubit.
  - 01: Alice applies  $X$  to her qubit.
  - 10: Alice applies  $Z$  to her qubit.
  - 11: Alice applies  $X$  then  $Z$  (or  $iY$ ) to her qubit.

3) Alice sends her modified qubit to Bob.

4) Bob performs a Bell measurement on the two qubits he now possesses to recover  $xy$ .

## 7. Quantum Algorithms

### 7.1. Oracle ( $U_f$ )

Black box for  $f(x)$ .

$$U_f|x\rangle|y\rangle = |x\rangle|y \otimes f(x)\rangle$$

#### 7.1.1. Phase kickback

If  $|y\rangle = |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ , then

$$U_f|x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle$$

### 7.2. Deutsch's Algorithm

- Problem:  $f : \{0, 1\} \rightarrow \{0, 1\}$  Constant or balanced? One query.
- Task: Calculate  $(f(0) + f(1)) \pmod 2$ .
- Circuit:

$$|0\rangle|1\rangle \xrightarrow{H \otimes H} \frac{1}{2} \sum_x |x\rangle(|0\rangle - |1\rangle) \xrightarrow{U_f}$$

$$\xrightarrow{U_f} \frac{1}{2} \sum_x (-1)^{f(x)} |x\rangle(|0\rangle - |1\rangle) \xrightarrow{H \otimes I}$$

$$\xrightarrow[\text{Result on 1st qubit:}]{H \otimes I} \frac{1}{2} ((-1)^{f(0)} + (-1)^{f(1)})|0\rangle +$$

$$+ \frac{1}{2} ((-1)^{f(0)} - (-1)^{f(1)})|1\rangle$$

- Measure 1st qubit:
  - If  $f(0) = f(1)$  (constant), state is  $\pm|0\rangle$ . Measure 0.  $(f(0) + f(1)) \pmod 2 = 0$ .
  - If  $f(0) \neq f(1)$  (balanced), state is  $\pm|1\rangle$ . Measure 1.  $(f(0) + f(1)) \pmod 2 = 1$ .

### 7.3. Grover's Search Algorithm

- Problem: Find  $x_w$  s.t.  $f(x_w) = 1$  (marked item) in  $N = 2^n$  items.
- Oracle  $O$ :  $O|x\rangle = (-1)^{f(x)}|x\rangle$ .
- Grover Diffusion Operator  $D$  (Inversion about the mean):  $D = 2|s\rangle\langle s| - I$ , where  $|s\rangle = H^{\otimes n}|0\rangle^{\otimes n}$ .
- Grover Iteration:  $G = DO$ .
- Algorithm:
  - 1) Start  $|s\rangle$ .
  - 2) Repeat  $G$  for  $k$  iterations.

- 1 marked item ( $L = 1$ ):  $k \approx \frac{\pi}{4}\sqrt{N}$
- $L$  marked items:  $k \approx \frac{\pi}{4}\sqrt{\frac{N}{L}}$

3) Measure. High probability of marked item.

- Geometric Interpretation: Rotation in 2D plane spanned by  $|s\rangle$  and  $|w\rangle$  (superposition of marked items).

More precisely, plane spanned by  $|\Psi_1\rangle = \frac{1}{\sqrt{L}} \sum_{x:f(x)=1} |x\rangle$  and  $|\Psi_0\rangle = \frac{1}{\sqrt{N-L}} \sum_{x:f(x)=0} |x\rangle$ . Initial state  $|s\rangle = \sin \alpha |\Psi_1\rangle + \cos \alpha |\Psi_0\rangle$ , where  $\sin \alpha = \sqrt{\frac{L}{N}}$ .

Oracle  $O$  reflects about  $|\Psi_0\rangle$ . Diffusion  $D$  reflects about  $|s\rangle$ . Each Iteration  $G = DO$  rotates by  $2\alpha$ .

After  $k$  iterations, angle with  $|\Psi_0\rangle$  is  $(2k + 1)\alpha$ .

Prob. of measuring a marked item:  $\sin^2((2k + 1)\alpha)$ .

- Unknown  $L$ : Iterative deepening: try iterations  $t = 1, 3, 3^2, \dots$ , up to  $\approx \sqrt{N}$

## 7.4. Quantum Fourier Transform (QFT)

- Definition:

$$QFT_N |j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{2\pi i j k}{N}} |k\rangle$$

Let  $\omega_N = e^{\frac{2\pi i}{N}}$ .

- Circuit: Uses  $H$  and controlled- $R_m$  gates (

$$R_m = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^m}} \end{pmatrix}$$

), then  $SWAPs$ .

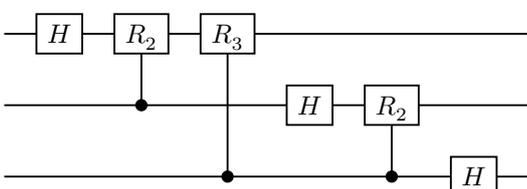
- Property (Periodicity): If input is periodic sum

$$|\psi\rangle = \frac{1}{\sqrt{q}} \sum_{l=0}^{q-1} |a + lp\rangle$$

(where  $N = pq$ , period  $p$ ), then

$$QFT_N |\psi\rangle = \frac{1}{\sqrt{p}} \sum_{k=0}^{p-1} c_k \left| k \cdot \frac{N}{p} \right\rangle$$

(Output is superposition of multiples of  $\frac{N}{p}$ ).



## 7.5. Period Finding (Kvantu algoritms perioda atrašānai)

- Problem: Given  $f(x) = f(x + r)$ , find period  $r$ .  $N$  is size of domain.

- Algorithm:

$$1) \quad \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle |0\rangle \xrightarrow{U_f} \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle |f(x)\rangle$$

- 2) Measure 2nd register (gets some  $y_0$ ). 1st register becomes

$$\frac{1}{\sqrt{M}} \sum_{k:f(k)=y_0} |k\rangle \approx \frac{1}{\sqrt{\frac{N}{r}}} \sum_{j=0}^{\frac{N}{r}-1} |x_0 + jr\rangle$$

- 3) Apply  $QFT_N$  to 1st register. Result is superposition of states  $k \cdot \frac{N}{r}$ .

- 4) Measure 1st register. Get some value  $m_j \approx j \cdot \frac{N}{r}$ .

- Classical Post-processing: If  $N$  is a multiple of  $r$ :  $m_j = j \cdot \frac{N}{r}$ . Find  $r$  using  $\gcd(m_j, N)$  and continued fractions / Euclidean algorithm to find  $\frac{j}{r}$  from  $\frac{m_j}{N}$ .

## 7.6. Shor's Algorithm (Skaitļa sadalīšanas algoritms)

- Reduces factoring  $N$  to finding order  $r$  of  $a^x \pmod{N}$ . Uses Period Finding for  $f(x) = a^x \pmod{N}$ .
- Order  $r$  of  $a^x \pmod{N}$ : Smallest  $r > 0$  s.t.  $a^r \equiv 1 \pmod{N}$ .

## 7.7. Simon's Algorithm

- Problem: Given  $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$  such that  $f(x) = f(y)$  if  $x \oplus y = s$  for some secret string  $s \in \{0, 1\}^n$  (or  $x = y$ , i.e.,  $s = 0^n$ ). Find  $s$ .

- Algorithm:

1) Prepare  $H^{\otimes n} |0\rangle^{\otimes n} |0\rangle^{\otimes n}$ .

2) Apply:  $U_f : \frac{1}{\sqrt{2^n}} \sum_x |x\rangle |f(x)\rangle$ .

3) Measure second register. First register collapses to  $\frac{1}{\sqrt{2}}(|x_0\rangle + |x_0 \oplus s\rangle)$  for some  $x_0$ .

4) Apply  $H^{\otimes n}$  to the first register.

5) Measure first register to get string  $y$  such that  $y \cdot s = 0 \pmod{2}$ .

- 6) Repeat  $n - 1$  times to get  $n - 1$  linearly independent equations for  $s$ . Solve the system to find  $s$ .

## 8. Advanced Topics

### 8.1. Density Matrices (Blivuma matrices $\rho$ )

- Describes quantum states, including mixed states (statistical ensemble of pure states).
- Pure state  $|\psi\rangle : \rho = |\psi\rangle\langle\psi|$ .
- Mixed state:  $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ , where  $p_i$  are probabilities,  $\sum p_i = 1$ .
- Properties:
  - $Tr(\rho) = 1$ .
  - $\rho^\dagger = \rho$  (Hermitian).
  - $\rho$  is positive semi-definite (eigenvalues  $\geq 0$ ).
- Evolution:  $\rho' = U\rho U^\dagger$ .
- Measurement: Probability of outcome  $m$  :  $P(m) = Tr(M_m^\dagger M_m \rho)$ . Post-measurement state:  $\frac{M_m \rho M_m^\dagger}{Tr(M_m \rho M_m^\dagger)}$
- Purity:  $Tr(\rho)^2 \leq 1$ .  $Tr(\rho)^2 = 1$  if  $\rho$  is a pure state.
- Partial Trace ( $Tr_B$ ): If  $\rho_{AB}$  describes system  $AB$ ,  $\rho_A = Tr_B(\rho_{AB})$  describes system  $A$ .

## 8.2. Quantum Cryptography

### 8.2.1. BB84 Protocol

- 1) Alice chooses random bits and random bases (rectilinear  $+$  or diagonal  $\times$ ) for each bit.
  - $0 \xrightarrow{+} |0\rangle, 1 \xrightarrow{+} |1\rangle$
  - $0 \xrightarrow{\times} |+\rangle, 1 \xrightarrow{\times} |-\rangle$
- 2) Alice sends qubits to Bob.
- 3) Bob chooses random bases to measure each qubit.
- 4) Alice and Bob publicly announce their basis choices. They keep bits where bases matched (sifted key).
- 5) They sacrifice a portion of the sifted key to estimate error rate (detect eavesdropping). If error rate is low, remaining bits form the secret key.

### 8.2.2. Security

Eavesdropping (Eve) introduces errors because she doesn't know Alice's bases and her measurements disturb the states.

## 8.3. Quantum Error Correction

Protects quantum states from decoherence and errors.

### 8.3.1. 3-Qubit Bit Flip Code

- Encoding:  $|0\rangle \rightarrow |0_L\rangle = |000\rangle, |1\rangle \rightarrow |1_L\rangle = |111\rangle$ .
- Error detection: Measure stabilizers  $Z_1 Z_2, Z_2 Z_3$ .
- Correction: If  $Z_1 Z_2$  flips, error on  $Q1$  or  $Q2$ . If  $Z_2 Z_3$  flips, error on  $Q2$  or  $Q3$ . (e.g., if  $Z_1 Z_2 = -1, Z_2 Z_3 = +1 \implies$  error on  $Q1$ , apply  $X_1$ ).

### 8.3.2. 3-Qubit Phase Flip Code

- Encoding:  $|0\rangle \rightarrow |+_L\rangle = |+++ \rangle, |1\rangle \rightarrow |-_L\rangle = |-- \rangle$ . (Hadamard basis of bit flip code).
- Error detection: Measure stabilizers  $X_1 X_2, X_2 X_3$ .

### 8.3.3. Shor's 9-Qubit Code

Corrects arbitrary single-qubit errors (bit flips, phase flips, or both). Concatenates bit-flip and phase-flip codes.

$$|0\rangle \rightarrow \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$$

$$|1\rangle \rightarrow \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)$$

- Stabilizer Codes: A general framework for QEC. Code space is the simultaneous  $+1$  eigenspace of a set of commuting Pauli operators (stabilizers).