CS621/CSL611
Quantum Computing For Computer Scientists

Quantum Search

Dhiman Saha

Winter 2024

IIT Bhilai

Quantum Search

Index View of Amplitude Vectors

Adapted from Bernstein's Invited Talk at Indocrypt 2021

- Do **not** worry about **normalization**!

State Representation

Non-Quantum Computer

- Data stored in 3 bits
- List of 3 elements $\in \{0, 1\}$
- e.g (0,0,0)
- e.g (0,1,1)
- Data stored in 64 bits
- List of 64 elements $\in \{0, 1\}$
- e.g.: (1; 1; 1; 1; 1; 0; 0; 0; 1; 0; 0; 0; 0; 0; 0; 1; 1; 0; 0; 0; 0; 1; 0; 0; 1; 0; 0; 0; 0; 0; 1; 1; 0; 1; 0; 0; 0; 1; 0; 0; 0; 1; 0; 0; 1; 1; 1; 0; 0; 1; 0; 0; 0; 1; 1; 0; 1; 1; 0; 0; 1; 0; 0; 1):

Quantum Computer

- Data stored in 3 qubits
- List of 8 numbers,
- **Not** all zero
- e.g.: [3; 1; 4; 1; 5; 9; 2; 6].
- e.g.: [-2; 7; -1; 8; 1; -8; -2; 8].
- e.g.: [0; 0; 0; 0; 0; 1; 0; 0].
- Data stored in 64 qubits:
- List of 2^{64} numbers
- Not all zero.

Adapted from Bernstein's Invited Talk at Indocrypt 2021

Interpreting The Quantum State Vector

- If n qubits have state $[a_0; a_1; \ldots; a_q; \ldots; a_{2^n-1}]$ then measurement produces q with probability

$$\frac{|a_q|^2}{\sum_r |a_r|^2}$$

- Recall measuring n qubits
  - produces n bits and
  - collapses the state.
- Collapse $\implies$ New state is all zeros except 1 at position q.

$$[a_0; a_1; \ldots; a_q; \ldots; a_{2^n-1}] \xrightarrow{Measure} [0; 0; \ldots; \underbrace{1}_{Position-q}; \ldots; 0]$$

Adapted from Bernstein's Invited Talk at Indocrypt 2021

Example

- e.g.: Say 3 qubits have state

$$[1;1;1;1;1;1;1;1] \to \sum_r |a_r|^2 = 8$$

- Measurement produces q with probability $\frac{|a_q|^2}{\sum_r |a_r|^2}$
  - $000 = 0$ with probability $\frac{1}{8}$
  - $001 = 1$ with probability $\frac{1}{8}$
  - $010 = 2$ with probability $\frac{1}{8}$
  - $011 = 3$ with probability $\frac{1}{8}$
  - $100 = 4$ with probability $\frac{1}{8}$
  - $101 = 5$ with probability $\frac{1}{8}$
  - $110 = 6$ with probability $\frac{1}{8}$
  - $111 = 7$ with probability $\frac{1}{8}$

Adapted from Bernstein's Invited Talk at Indocrypt 2021

- e.g.: Say 3 qubits have state

$$[3; 1; 4; 1; 5; 9; 2; 6] \to \sum_r |a_r|^2 = 173$$

- Measurement produces q with probability $\frac{|a_q|^2}{\sum_r |a_r|^2}$
  - $000 = 0$ with probability $\frac{9}{173}$
  - $001 = 1$ with probability $\frac{1}{173}$
  - $010 = 2$ with probability $\frac{4}{173}$
  - $011 = 3$ with probability $\frac{1}{173}$
  - $100 = 4$ with probability $\frac{25}{173}$
  - $101 = 5$ with probability $\frac{81}{173}$
  - $110 = 6$ with probability $\frac{4}{173}$
  - $111 = 7$ with probability $\frac{36}{173}$

Adapted from Bernstein's Invited Talk at Indocrypt 2021

Example

- e.g.: Say 3 qubits have state

$$[0; 0; 0; 0; 0; 1; 0; 0] \rightarrow \sum_r |a_r|^2 = 1$$

- Measurement produces q with probability $\frac{|a_q|^2}{\sum_r |a_r|^2}$
  - $000 = 0$ with probability 0
  - $001 = 1$ with probability 0
  - $010 = 2$ with probability 0
  - $011 = 3$ with probability 0
  - $100 = 4$ with probability 0
  - $101 = 5$ with probability $1 \rightarrow$ guaranteed outcome
  - $110 = 6$ with probability 0
  - $111 = 7$ with probability 0

Adapted from Bernstein's Invited Talk at Indocrypt 2021

Revisiting the NOT gate

- NOT_0 gate on 3 qubits:

$$\left[\underbrace{3}_{000};\underbrace{1}_{001};\underbrace{4}_{010};\underbrace{1}_{011};\underbrace{5}_{100};\underbrace{9}_{101};\underbrace{2}_{110};\underbrace{6}_{111}\right]$$

$$\downarrow \text{ Flipping qubit 0}$$

$$\left[\underbrace{3}_{001};\underbrace{1}_{000};\underbrace{4}_{011};\underbrace{1}_{010};\underbrace{5}_{101};\underbrace{9}_{100};\underbrace{2}_{111};\underbrace{6}_{110}\right]$$

$$\downarrow \text{ Rearranging Indices}$$

$$\left[\underbrace{1}_{000};\underbrace{3}_{001};\underbrace{1}_{010};\underbrace{4}_{011};\underbrace{9}_{100};\underbrace{5}_{101};\underbrace{6}_{110};\underbrace{2}_{111}\right]$$

Adapted from Bernstein's Invited Talk at Indocrypt 2021

- NOT_0 gate on 3 qubits:

$$\left[\underbrace{3}_{000};\underbrace{1}_{001};\underbrace{4}_{010};\underbrace{1}_{011};\underbrace{5}_{100};\underbrace{9}_{101};\underbrace{2}_{110};\underbrace{6}_{111}\right]$$

$$\left[\underbrace{1}_{000};\underbrace{3}_{001};\underbrace{1}_{010};\underbrace{4}_{011};\underbrace{9}_{100};\underbrace{5}_{101};\underbrace{6}_{110};\underbrace{2}_{111}\right]$$

- **Note:** Adjacent values in state vector have been swapped

Adapted from Bernstein's Invited Talk at Indocrypt 2021

- NOT_0 gate on 4 qubits:

$$[3; 1; 4; 1; 5; 9; 2; 6; 5; 3; 5; 8; 9; 7; 9; 3] \to$$
$$[1; 3; 1; 4; 9; 5; 6; 2; 3; 5; 8; 5; 7; 9; 3; 9]$$

- NOT_1 gate on 3 qubits:

$$[3; 1; 4; 1; 5; 9; 2; 6] \to$$
$$[4; 1; 3; 1; 2; 6; 5; 9]$$

- NOT_2 gate on 3 qubits:

$$[3; 1; 4; 1; 5; 9; 2; 6] \to$$
$$[5; 9; 2; 6; 3; 1; 4; 1].$$

Adapted from Bernstein's Invited Talk at Indocrypt 2021

Interpreting NOT_0 w.r.t Measurement

state	measurement
$[1, 0, 0, 0, 0, 0, 0, 0]$	000
$[0, 1, 0, 0, 0, 0, 0, 0]$	001
$[0, 0, 1, 0, 0, 0, 0, 0]$	010
$[0, 0, 0, 1, 0, 0, 0, 0]$	011
$[0, 0, 0, 0, 1, 0, 0, 0]$	100
$[0, 0, 0, 0, 0, 1, 0, 0]$	101
$[0, 0, 0, 0, 0, 0, 1, 0]$	110
$[0, 0, 0, 0, 0, 0, 0, 1]$	111

- Operation on quantum state: NOT_0, swapping pairs.
- Operation after measurement: flipping bit 0 of result.

Adapted from Bernstein's Invited Talk at Indocrypt 2021

Revisiting Controlled-NOT (CNOT) Gates

- e.g. C_1NOT_0 :

$$\left[\underbrace{3}_{000};\underbrace{1}_{001};\underbrace{4}_{010};\underbrace{1}_{011};\underbrace{5}_{100};\underbrace{9}_{101};\underbrace{2}_{110};\underbrace{6}_{111}\right]$$

$\downarrow$ Flipping qubit 0 based on qubit 1

$$\left[\underbrace{3}_{000};\underbrace{1}_{001};\underbrace{4}_{011};\underbrace{1}_{010};\underbrace{5}_{100};\underbrace{9}_{101};\underbrace{2}_{111};\underbrace{6}_{110}\right]$$

$\downarrow$ Rearranging Indices

$$\left[\underbrace{3}_{000};\underbrace{1}_{001};\underbrace{1}_{010};\underbrace{4}_{011};\underbrace{5}_{100};\underbrace{9}_{101};\underbrace{6}_{110};\underbrace{2}_{111}\right]$$

Adapted from Bernstein's Invited Talk at Indocrypt 2021

Revisiting Controlled-NOT (CNOT) Gates

- e.g. C_2NOT_0 :

$$\left[\underbrace{3}_{000};\underbrace{1}_{001};\underbrace{4}_{010};\underbrace{1}_{011};\underbrace{5}_{100};\underbrace{9}_{101};\underbrace{2}_{110};\underbrace{6}_{111}\right]$$

$$\downarrow \text{ Flipping qubit 0 based on qubit 2}$$

$$\left[\underbrace{3}_{000};\underbrace{1}_{001};\underbrace{4}_{010};\underbrace{1}_{011};\underbrace{5}_{101};\underbrace{9}_{100};\underbrace{2}_{111};\underbrace{6}_{110}\right]$$

$$\downarrow \text{ Rearranging Indices}$$

$$\left[\underbrace{3}_{000};\underbrace{1}_{001};\underbrace{4}_{010};\underbrace{1}_{011};\underbrace{9}_{100};\underbrace{5}_{101};\underbrace{6}_{110};\underbrace{2}_{111}\right]$$

Adapted from Bernstein's Invited Talk at Indocrypt 2021

- Compute C_0NOT_2 :

$$\left[\underbrace{3}_{000};\underbrace{1}_{001};\underbrace{4}_{010};\underbrace{1}_{011};\underbrace{5}_{100};\underbrace{9}_{101};\underbrace{2}_{110};\underbrace{6}_{111}\right]$$

$\downarrow$ Flipping qubit 2 based on qubit 0

$$\left[\underbrace{3};\underbrace{1};\underbrace{4};\underbrace{1};\underbrace{5};\underbrace{9};\underbrace{2};\underbrace{6}\right]$$

$\downarrow$ Rearranging Indices

$$\left[\underbrace{\quad}_{000};\underbrace{\quad}_{001};\underbrace{\quad}_{010};\underbrace{\quad}_{011};\underbrace{\quad}_{100};\underbrace{\quad}_{101};\underbrace{\quad}_{110};\underbrace{\quad}_{111}\right]$$

Adapted from Bernstein's Invited Talk at Indocrypt 2021

- e.g. $\mathrm{C}_2\mathrm{C}_1\mathrm{NOT}_0$:

$$\Big[\underbrace{3}_{000};\underbrace{1}_{001};\underbrace{4}_{010};\underbrace{1}_{011};\underbrace{5}_{100};\underbrace{9}_{101};\underbrace{2}_{110};\underbrace{6}_{111}\Big] \rightarrow$$

$$\Big[\underbrace{3}_{000};\underbrace{1}_{001};\underbrace{4}_{010};\underbrace{1}_{011};\underbrace{5}_{100};\underbrace{9}_{101};\underbrace{6}_{110};\underbrace{2}_{111}\Big]$$

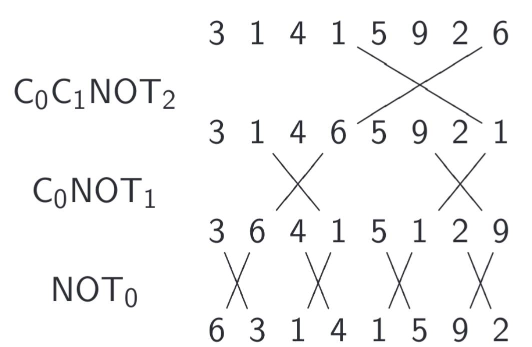
- e.g. $\mathrm{C}_0\mathrm{C}_1\mathrm{NOT}_2$:

$$\Big[\underbrace{3}_{000};\underbrace{1}_{001};\underbrace{4}_{010};\underbrace{1}_{011};\underbrace{5}_{100};\underbrace{9}_{101};\underbrace{2}_{110};\underbrace{6}_{111}\Big] \rightarrow$$

$$\Big[\underbrace{3}_{000};\underbrace{1}_{001};\underbrace{4}_{010};\underbrace{6}_{011};\underbrace{5}_{100};\underbrace{9}_{101};\underbrace{2}_{110};\underbrace{1}_{111}\Big]$$

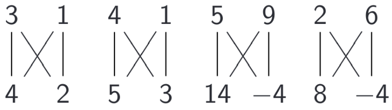
Adapted from Bernstein's Invited Talk at Indocrypt 2021

- Combine NOT, CNOT, Toffoli to build other permutations.
- e.g. series of gates to rotate 8 positions by distance 1:



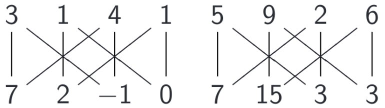
Adapted from Bernstein's Invited Talk at Indocrypt 2021

$[a, b] \mapsto [a + b, a - b]$.



Hadamard$_1$:

$[a, b, c, d] \mapsto$
$[a + c, b + d, a - c, b - d]$.



Adapted from Bernstein's Invited Talk at Indocrypt 2021

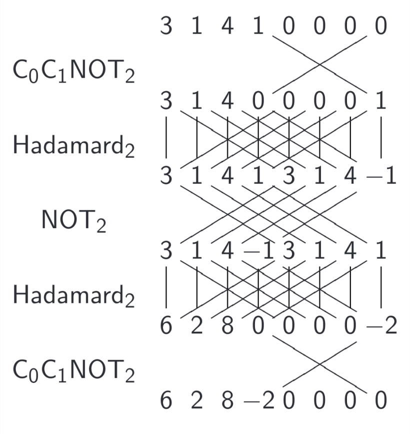
Hadamard$_0$, NOT$_0$, Hadamard$_0$:

3	1	4	1	5	9	2	6
4	2	5	3	14	−4	8	−4
2	4	3	5	−4	14	−4	8
6	−2	8	−2	10	−18	4	−12

- "Multiplied each amplitude by 2."
- This is not physically observable.
- What other change has happened?
- "Negated amplitude if q_0 is set." No effect on measuring now.

Advanced Example

- "Negate amplitude if $q_0 q_1$ is set."
- Assumes $q_2 = 0$: "ancilla" qubit.

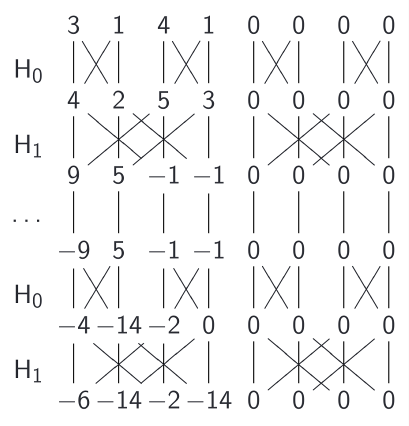


Adapted from Bernstein's Invited Talk at Indocrypt 2021

Affects measurements

- "Negate amplitude around its average."

$$[3, 1, 4, 1] \to [1.5, 3.5, 0.5, 3.5]$$



Adapted from Bernstein's Invited Talk at Indocrypt 2021