Quantum Computing & Cryptography

Week 16:

Classical bits & vectors
- Classical bits — as vectors
- Operations as matrices
- Reversible operations

States of Cbits
The state of a Cbit represents a bit 0 or 1
Write \( |0\rangle \), \( |1\rangle \) for the states.
- \( |1\rangle \) is like a box to put the value in
- Notation invented by Paul Dirac for QM
- He called \( |1\rangle \) a ket
  (The opposite, \( <1| \), also has a use, it is a bra.)

States of groups of Cbits
e.g. 5 Cbits representing 11001 (binary 25)
State written as
- \( |1\rangle |1\rangle |0\rangle |0\rangle |1\rangle \)
- \( |11001\rangle \)
- \( |125\rangle \)
- \( |125\rangle \)

2 usual meanings
for "bit"
abstract value,
0 or 1
place where 0 or 1 can be stored
Mermin distinguishes bit
between them

e.g. a 64-bit register in a computer is 64 Cbits
Indexing the Qubits

We index the Qubits
- starting on the right
- with index 0

\[ \text{index} = 4 \quad \text{index} = 3 \quad \text{index} = 2 \quad \text{index} = 1 \quad \text{index} = 0 \]

\[ |1\rangle |1\rangle |0\rangle |0\rangle |1\rangle \]

Least significant bit

Think Java: array of booleans

The world's worst notation for $125>$

Vector with 32 components for numbers 0..31.
$25$ indicated by 0 everywhere except 1 in component $25$.

Why is this so bad?
We know a 5-bit vector $11001$ is enough to describe $25$.
BUT - world's worst notation is just what we need for quantum computation.

Qubit states as vectors

For $n$ Qubits
- $2^n$ possible states

Represent as vector $2^n$ components
One component is $1$
Rest are all $0$

$2^n$: world's worst notation is exponentially bad
Makes it infeasible to simulate quantum algorithms on classical computers

Operations as matrices

Suppose $\alpha$ an operator on $n$-Qubit systems
Idea: Represent $\alpha$ as a matrix, acting by multiplication of column vectors

\[
\begin{pmatrix}
\alpha_1 & \alpha_2 & \cdots & \alpha_n
\end{pmatrix}
\begin{pmatrix}
\beta_1 \\
\beta_2 \\
\vdots \\
\beta_n
\end{pmatrix}
= 
\begin{pmatrix}
\alpha_1 \beta_1 + \cdots + \alpha_n \beta_n
\end{pmatrix}
\]
Composing operations is matrix multiplication

\[ \text{operator } a, \ x \mapsto a \cdot x \] as numbers

\[ \text{matrix } a, \ |x\rangle \mapsto a|x\rangle \] as vectors

& matrices

Thus \( a|x\rangle = |a \cdot x\rangle \)

Similarly for \( b \)

Then \( (a \cdot b)|x\rangle = a(b|x\rangle) = a(0|x\rangle) = |a \cdot b \cdot x\rangle \)

\[ \therefore \text{matrix } a \cdot b \text{ represents } a \cdot b \]

\[ \text{function composition} \]

\[ \text{associativity of matrix multiplication} \]

\[ \text{identity matrix} \]

\[ \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \]

1 on diagonal
0 everywhere else

\[ \text{eg. NOT operator } X \ (1 \text{ qubit}) \]

\[ X|0\rangle = |1\rangle \]

\[ X|1\rangle = |0\rangle \]

\[ X|0\rangle = X|1\rangle \]

\[ X^2|0\rangle = X|1\rangle = |0\rangle \]

\[ X^2|1\rangle = X|0\rangle = |1\rangle \]

\[ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \]

\[ \begin{pmatrix} 0 \ 1 \\ 1 \ 0 \end{pmatrix} \]

\[ \begin{pmatrix} 0 \ 1 \\ 1 \ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |1\rangle \]

\[ \begin{pmatrix} 0 \ 1 \\ 1 \ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle \]

\[ X^2|0\rangle = |1\rangle \]

\[ X|1\rangle = |0\rangle \]

\[ \text{eg. SWAP operator } S \ (2 \text{ qubits}) \]

\[ S \ |x\ y\rangle = |y\ x\rangle \]

\[ S \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \]

\[ S^2 = 1 \]
Reversible operations

Reversibility doesn't matter in classical computation, but very important in quantum computation.

\[ a \] is reversible if it has an inverse \( a^{-1} \) with \( a^{-1}a = 1\).

For example, \(1 \times S\) are reversible (each is its own inverse).

Copy operation \( |xy\rangle \mapsto |xx\rangle \)

A non-reversible operation for 2 qubits:

\[
\begin{align*}
|0\rangle_1 &= |0\rangle_2 \\
|1\rangle_1 &= |1\rangle_2
\end{align*}
\]

Original value of \(y\) is lost.

\[
\begin{pmatrix}
1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0
\end{pmatrix}
\]

Assignment \(y = x\), non-reversible.

No assignment in quantum comp.

Controlled-\( NOT \) gate \(CNOT\)

\(C\) uses \(C\) bit with index 1 (the control) to control \( NOT \) on \( C\) bit index 0 (target).

\[
\begin{align*}
C |xy\rangle &= \begin{cases} 
|xy\rangle & \text{if } x = 0 \\
|x\rangle |x\oplus y\rangle & \text{if } x = 1
\end{cases}
\end{align*}
\]

Reversible because \(C^2 |xy\rangle = |xy\rangle\) is exclusive or (\(\oplus\)) or addition modulo 2.

\[
\begin{pmatrix}
0 & 1 & 2 & 3 \\
1 & 0 & 0 & 0 \\
2 & 0 & 0 & 0 \\
3 & 0 & 0 & 1
\end{pmatrix}
\]

\(C|1y\rangle = |1\bar{y}\rangle\)

\(C\) fixes \(10\rangle = 10\rangle_2\) and \(11\rangle = 11\rangle_2\)

Exchanges \(10\rangle = 12\rangle_2\) and \(11\rangle = 13\rangle_2\)

\(\cdot\cdot\cdot\) matrix is
Indicating which qubits to operate on

Use qubit indexes as subscripts of operators

\[ X_{i} \text{ applies } X \text{ to qubit with index } i \]

\[ \langle x | y \rangle = | x \rangle | y \rangle \]

exchanges \[ \langle 10 \rangle = | 1 \rangle | 0 \rangle \]

exchanges \[ \langle 10 \rangle = | 1 \rangle | 0 \rangle \]

matrix
\[
\begin{pmatrix}
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0
\end{pmatrix}
\]

More examples

SWAP \( S_{ij} \) swaps states of qubits with indexes \( i \) and \( j \)

Note: \( S_{ij} = S_{ji} \) - swap is symmetric

\[ C = C_{0} \oplus C_{1} \]

CNOT \( C_{ij} \)

control \( \rightarrow \)

target \( \rightarrow \)

\[ C_{ij} \neq C_{ji} \]

Constructing \( S \) out of \( C \)

\[ S_{ij} = C_{ij} C_{ji} C_{ij} \]

E.g. for 2 qubits,

\[ C_{0} \oplus C_{0} \langle x | y \rangle = C_{0} \oplus C_{0} \langle x \rangle | x \rangle | y \rangle \]

\[ = C_{0} \langle x \rangle | x \rangle | y \rangle \]

\[ = C_{0} \langle x \rangle | y \rangle \]

\[ = | y \rangle | x \rangle \]

\[ = S_{0} \langle x | y \rangle \]

Circuit diagrams

Wire = 1 qubit = 2-dim vectors

\( n \) wires = \( n \) qubits = \( 2^{n} \)-dim vectors

E.g.: NOT: \[ \begin{array}{c}
\text{control} \\
\text{target}
\end{array} \]

SWAP: \[ \begin{array}{c}
\text{index qubits}
\end{array} \]

Gates applied left to right - opposite way round to operations

index qubits starting from 0 at bottom
Summary of reversible operations - on qubits

- On 1 qubit: 1, X
- On 2 qubits: 24 permutations of 4 states
  - Can construct them all using X, CNOT and \( \otimes \)

- On more qubits: Can construct them all if you also have Toffoli
  - For quantum bits, Toffoli can already be constructed from operations on 1 or 2 bits

Key concepts

- Several notations for register states, including "world's worst"
- Operations as matrices
- Reversibility is important
- Circuit diagrams to show combinations of operations