

Quantum Computing & Cryptography

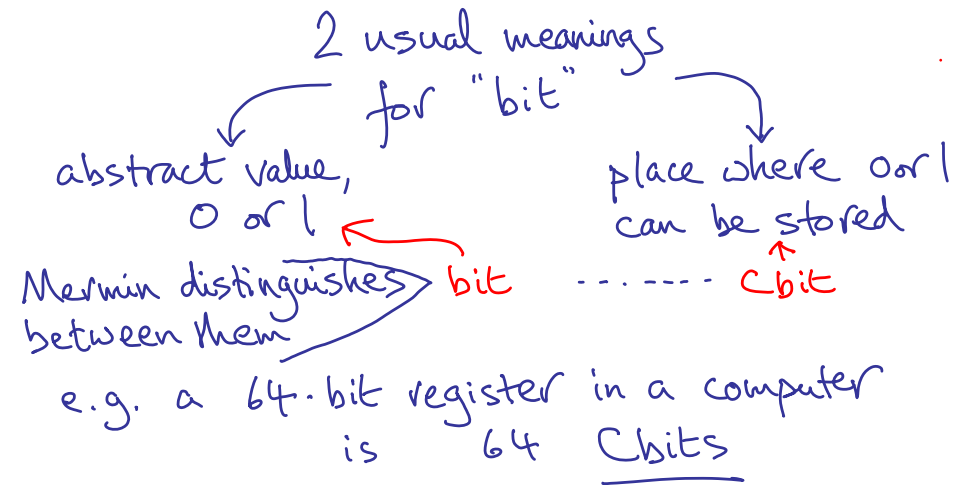
Week 1b :

Classical bits & vectors

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

Steve Vickers

bits and Cbits ^{.....} (for Classical = not quantum)



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 ^{quantum mechanics}
- Notation invented by Paul Dirac for QM
- He called $| \rangle$ a **ket**.
(The opposite, $\langle |$, also has a use.
It is a **bra**.)

States of groups of Cbits

e.g. 5 Cbits representing 11001 (binary 25)
state written as

$|1\rangle|1\rangle|0\rangle|0\rangle|1\rangle$

$|11001\rangle$

$|25\rangle$

$|25\rangle$

..... to make it clear there are 5 Cbits

$|1\rangle \otimes |1\rangle \otimes |0\rangle \otimes |0\rangle \otimes |1\rangle$
tensor product

but... sometimes use subscripts for other purposes

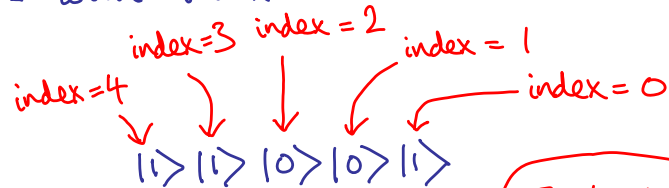
Indexing the Cbits

We index the Cbits

- starting on the right
- with index 0

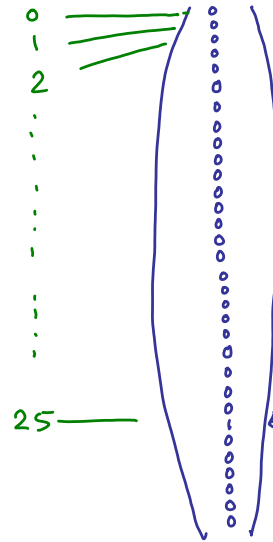
least significant bit

e.g.



Think Java:
array of booleans

The world's worst notation for $|25\rangle_5$



Vector with 32 components for numbers 0 .. 31.

25 indicated by 1 everywhere except 1 in component 25.

Why is this so bad?

We know a 5-bit vector $|11001\rangle$ is enough to describe 25.

BUT - world's worst notation is just what we need for quantum computation.

Cbit states as vectors

For n Cbits

- 2^n possible states

Represent as vector 2^n components

One component is 1
Rest are all 0

dimension = 2^n

Same idea as the world's worst notation!

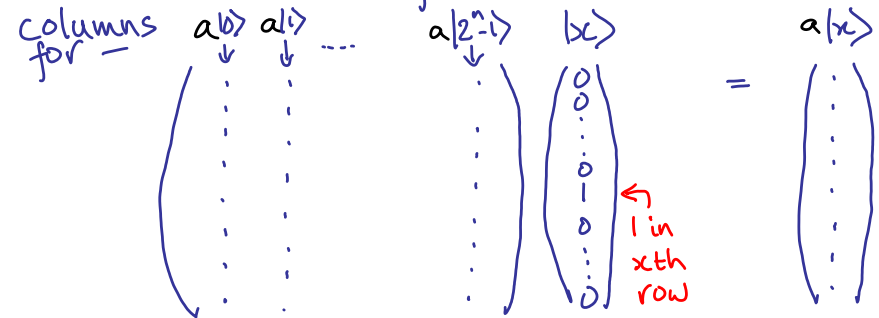
$n \mapsto 2^n$: world's worst notation is exponentially bad

makes it infeasible to simulate quantum algorithms on classical computers

Operations as matrices

Suppose a an operator on n -Cbit systems

Idea Represent a as a matrix, acting by multiplication of column vectors



Composing operations is matrix multiplication

operator $a, x \mapsto a(x)$ as numbers
 matrix $a, |x\rangle \mapsto a|x\rangle$ as vectors & matrices

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

Similarly for b

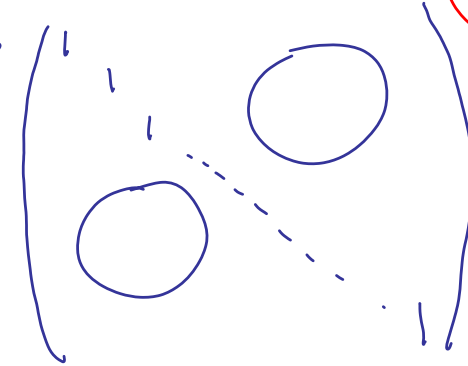
Then $(a \circ b)|x\rangle = a(b|x\rangle) = a|b(x)\rangle$
 $= |a(b(x))\rangle = |a \circ b(x)\rangle$
 \therefore matrix ab represents $a \circ b$

matrix \rightarrow *column vector*
function composition
associativity of matrix multiplication

e.g. Identity operation

$$\mathbb{1}|x\rangle = |x\rangle$$

Matrix is



identity matrix

1 on diagonal
0 everywhere else

e.g. NOT operator X (1 bit)

$$X|0\rangle = |1\rangle$$

$$X|1\rangle = |0\rangle$$

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

flips state of cbit
 $X|x\rangle = |\bar{x}\rangle$
 $\bar{0} = 1, \bar{1} = 0$

$$X^2 = \mathbb{1} \quad X^2|0\rangle = X|1\rangle = |0\rangle$$

$$X^2|1\rangle = X|0\rangle = |1\rangle$$

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

$X|0\rangle = |1\rangle$

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

$X|1\rangle = |0\rangle$

SWAP operator S (2 bits)

SWAP S swap states of 2 bits

$$S|x y\rangle = |y x\rangle$$

- $|0\rangle_2 = |00\rangle \mapsto |00\rangle = |0\rangle_2$
- $|1\rangle_2 = |01\rangle \mapsto |10\rangle = |2\rangle_2$
- $|2\rangle_2 = |10\rangle \mapsto |01\rangle = |1\rangle_2$
- $|3\rangle_2 = |11\rangle \mapsto |11\rangle = |3\rangle_2$

matrix $\begin{matrix} 0 & 1 & 2 & 3 \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \end{matrix}$

$$S^2 = \mathbb{1}$$

Reversible operations

Reversibility doesn't matter in classical computation

But ... very important in quantum computation

∴ explore reversible operations classically.
 a is reversible if it has an inverse a^{-1} with $aa^{-1} = a^{-1}a = \mathbb{1}$

e.g. $\mathbb{1}$ & S are reversible (each is its own inverse)
 Only two reversible classical 1-bit operators

though some interesting thermo-dynamic issues. See Feynman

Copy operation $|xy\rangle \mapsto |xx\rangle$

A **non-reversible** operation for 2 Cbits

$y := x$ Original value of y is lost

$ 0\rangle_2 = 00\rangle$	\mapsto	$ 00\rangle = 0\rangle_2$	} $\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$
$ 1\rangle_2 = 01\rangle$	\mapsto	$ 00\rangle = 0\rangle_2$	
$ 2\rangle_2 = 10\rangle$	\mapsto	$ 11\rangle = 3\rangle_2$	} $\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$
$ 3\rangle_2 = 11\rangle$	\mapsto	$ 11\rangle = 3\rangle_2$	

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

Assignment $y := x$ non-reversible. No assignment in quantum comp.

controlled-NOT gate cNOT

C uses Cbit with index 1 (the control) to control NOT on Cbit index 0 (target)

$$C |x\rangle_{\text{control}} |y\rangle_{\text{target}} = \begin{cases} |xy\rangle & \text{if } x=0 \\ |x\bar{y}\rangle & \text{if } x=1 \end{cases}$$

$$= |x\rangle |x \oplus y\rangle$$

\oplus is exclusive or (xor) i.e. addition modulo 2

Reversible: because

$$C^2 |xy\rangle = C |x\rangle |x \oplus y\rangle = |x\rangle |x \oplus x \oplus y\rangle = |x\rangle |y\rangle = |xy\rangle$$

$$1 \oplus y = \bar{y}$$

Matrix for C

$$C |0y\rangle = |0y\rangle$$

C fixes $|00\rangle = |0\rangle_2$ and $|01\rangle = |1\rangle_2$
 exchanges $|10\rangle = |2\rangle_2$ and $|11\rangle = |3\rangle_2$

$$C |1y\rangle = |1\bar{y}\rangle$$

∴ matrix is

$$\begin{matrix} & \begin{matrix} 0 & 1 & 2 & 3 \end{matrix} \\ \begin{matrix} 0 \\ 1 \\ 2 \\ 3 \end{matrix} & \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \end{matrix}$$

Indicating which Cbits to operate on

Use Cbit indexes as subscripts of operators

e.g. X_i applies X to Cbit with index i

$$X_i |xy\rangle = |x\bar{y}\rangle$$

exchanges $|00\rangle = |0\rangle_2$ with $|10\rangle = |2\rangle_2$

exchanges $|01\rangle = |1\rangle_2$ with $|11\rangle = |3\rangle_2$

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 Cbits with indexes i, j

Note: $S_{ij} = S_{ji}$ - swap is symmetric

$$S = S_{10}$$

CNOT C_{ij} uses i th Cbit as control, j th Cbit as target

control $\rightarrow i$
target $\rightarrow j$
 $C_{ij} \neq C_{ji}$

Constructing S out of C

$$S_{ij} = C_{ij} C_{ji} C_{ij}$$

e.g. for 2 Cbits

$$C_{10} C_{01} C_{10} |xy\rangle = C_{10} C_{01} |x\rangle |x \oplus y\rangle$$

$$= C_{10} |x \oplus y \oplus x\rangle |x \oplus y\rangle$$

$$= C_{10} |y\rangle |x \oplus y\rangle$$

$$= |y\rangle |y \oplus x \oplus y\rangle$$

$$= |y\rangle |x\rangle$$

$$= S_{10} |xy\rangle$$


easier than multiplying matrices

$y := x \oplus y$
 $x := y \oplus x$
 $y := x \oplus y$
swaps x, y

Circuit diagrams

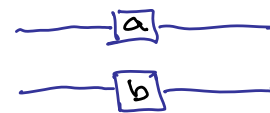
wire = 1 Cbit = 2-dim vectors

n wires = n Cbits = 2^n -dim vectors

e.g. NOT:  cNOT C_{10} : 

SWAP:  = 

operations applied independently:



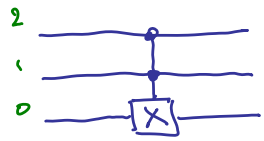
$A \otimes B$

Gates applied left to right - opposite way round to operations

sometimes bundle together in thicker wire

index Cbits starting from 0 at bottom

Toffoli gate ccNOT (controlled-controlled-NOT)



$$T|x_1y_1z\rangle = |x_1\rangle|y_1\rangle|z \oplus x_1y_1\rangle$$

Cbit 0 flipped if Cbits 1,2 are both 1.

reversible form of AND gate.

$T^2 = 1, \therefore T$ reversible



Summary of reversible operations - on Cbits

On 1 Cbit: $1, X$

On 2 Cbits: 24 permutations of 4 states

00
01
10
11

Can construct them all using $X, cNOT$ and \otimes

On more Cbits: 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