

Quantum Computing & Cryptography

Week 7a

More simple quantum algorithms

- Bernstein-Vazirani Mermin 2.4
- Simon Mermin 2.5

Steve Vickers

Mermin 2.4

The Bernstein-Vazirani problem

- Simple artificial problem
- Classical solution:
apply function n times
- Quantum:
apply function once
- to Hadamard state
- Diagrammatic explanation
easier than algebraic

The problem

a - unknown n -bit number
 $0 \leq a \leq 2^n - 1$

$f(x)$ defined as $a \cdot x$ - like a scalar product

$a_0 x_0 \oplus a_1 x_1 \oplus \dots \oplus a_{n-1} x_{n-1}$

\uparrow
addition mod 2

\leftarrow
n-bit argument

e.g. $n=3$: $5 \cdot 7 = 101 \cdot 111 = 1 \oplus 0 \oplus 1 = 0$

Given f , how do you find a ?

Given f , how do you find a ? - Classically

Try $x = 2^m = 0 \dots 0 1 0 \dots 0$

\uparrow
position m

$a = a_{n-1} \dots a_m a_{m-1} \dots a_0$

$f(x) = a \cdot x = 0 \oplus \dots \oplus 0 \oplus a_m \oplus 0 \oplus \dots \oplus 0$
 $= a_m$

\therefore find a in binary by evaluating $f(2^m)$
($0 \leq m \leq n-1$)

- n applications of f

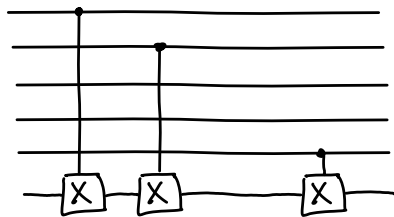
and can't do better

Given f , how do you find a ? - Quantum

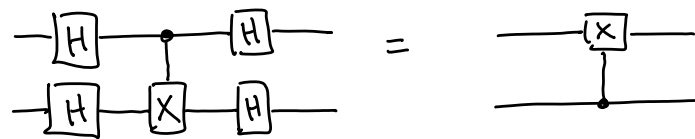
as usual $U_f |x\rangle_n |y\rangle_1 = |x\rangle_n |y \oplus f(x)\rangle_1 = |x\rangle_n |y \oplus a \cdot x\rangle_1$
 Each m with $a_m = x_m = 1$: flips output
 $a_m = 1 \Rightarrow x_m$ controls NOT on output

e.g.
 $a = 25$
 $= 11001$

$a_4 = 1$ $|x_4\rangle$
 $a_3 = 1$ $|x_3\rangle$
 $a_2 = 0$ $|x_2\rangle$
 $a_1 = 0$ $|x_1\rangle$
 $a_0 = 1$ $|x_0\rangle$
 $|y\rangle$

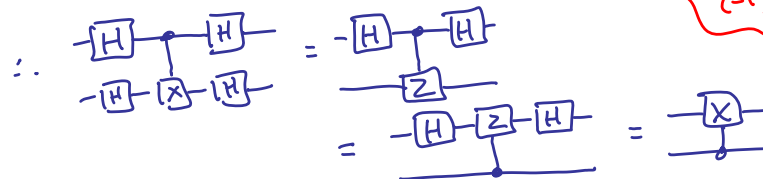


Remember Hadamards swap roles of CNOT

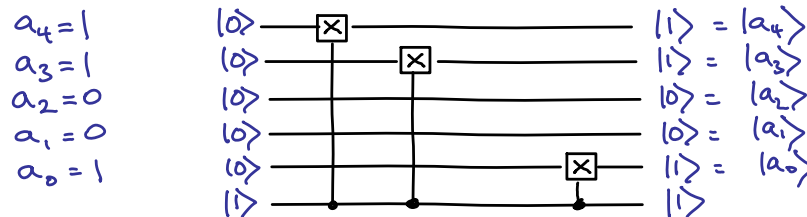
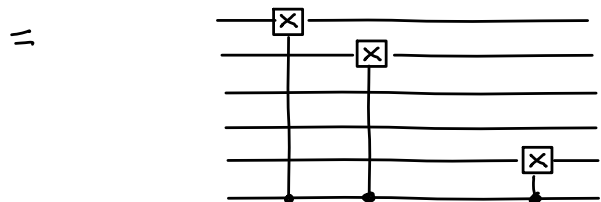
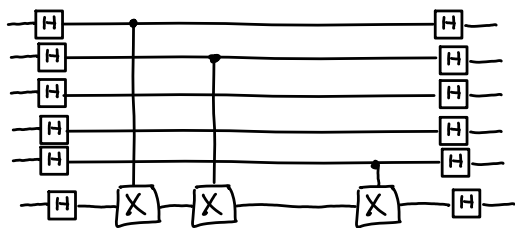


Key ingredients: $-H-X-H = Z$

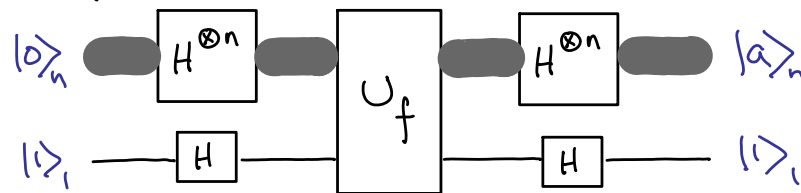
$Z = -Z$ transforms $|xy\rangle$ to $(-1)^{xy} |xy\rangle$



Hadamards everywhere



In general:



To find a :
 • prepare input as $|0\rangle$ output as $|1\rangle$
 • apply $(H^{\otimes n} \otimes H) U_f (H^{\otimes n} \otimes H)$
 • measure input

Something for nothing?

Classically: apply f once -
get one bit of information

Quantum: found a - n bits of information

Measuring $n+1$ qbits \Rightarrow $n+1$ Cbits

Some worthless $\begin{cases} \text{if random} \\ \text{if known already \& unchanged} \end{cases}$

With care - may get > 1 Cbit of value.

Algebraically - calculation much harder (see Mermin)
- one feature worth noting

U_f as defined: $U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle$
shows result 1 by flipping output

First prepare output as $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
 $\otimes H|1\rangle = \frac{1}{\sqrt{2}}(|1\rangle - |0\rangle) = -H|1\rangle$ $\circ\circ$ $\times H = HZ$

$\Rightarrow U_f$ shows result 1 by overall sign change
 $U_f(|x\rangle_n \otimes H|1\rangle) = (-1)^{f(x)} |x\rangle_n \otimes H|1\rangle$

Keeps input & output unentangled

Similarly to trick with Deutsch's problem

Worth remembering this trick!

For f with one result bit:

replace U_f

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

with $U_f (I \otimes H|1\rangle)$

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

& think of it as an operator on the input

- Deutsch
- Bernstein-Vazirani

- Grover

Something similar for Deutsch's problem?

Can we find f by applying U_f just once?

e.g. unitaries V, W with $W U_{uv} V |00\rangle = |uv\rangle$
say $U_{uv} = U_f$ where $f(0) = u$
 $f(1) = v$

measuring gives 2 Cbits - could be enough to distinguish 4 possibilities of f ?

Not possible! $U_{00} + U_{11} = U_{01} + U_{10}$

$$U_{00} |xy\rangle + U_{11} |xy\rangle = |x\rangle |y\rangle + |x\rangle |y \oplus 1\rangle$$

$$U_{01} |xy\rangle + U_{10} |xy\rangle = |x\rangle |y \oplus x\rangle + |x\rangle |y \oplus \bar{x}\rangle$$

one is $|y\rangle$, other is $|y \oplus 1\rangle$

$$\therefore W U_{ab} V |00\rangle = |ab\rangle \text{ would imply } |00\rangle + |11\rangle = |01\rangle + |10\rangle$$

Mermin 2.5

Simon's problem

- Simple example of period finding
- classically: time exponential with n
- quantum: time linear with n
- probabilistic

(cf. Shor's algorithm)

Problem

a - unknown non-zero n -bit number
 $1 \leq a \leq 2^n - 1$

f - function - n -bit argument
 $(n-1)$ -bit result

We are told:

$$f(x) = f(y) \text{ if and only if } x = y \text{ or } x = y \oplus a$$

$a = 0$ would not work.

$f(x \oplus a) = f(x)$: f periodic under \oplus (period = a)
 How do you find a ?

How do you find a ?

Classically

Have to find $x \neq y$ with $f(x) = f(y)$.

Then $a = x \oplus y$

Apply f to x_1, x_2, \dots looking for $f(x_i) = f(x_j)$

After m applications with no luck yet:

Have eliminated $\leq \frac{m(m-1)}{2}$ possibilities $x_i \oplus x_j$

For good chance of success need $\frac{m(m-1)}{2} \approx 2^n$

$m \approx$ order of $2^{n/2}$

exponential in n

After Hadamards

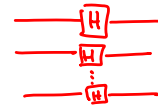
$$\begin{aligned} U_f (H^{\otimes n} |0\rangle_n |0\rangle_{n-1}) &= \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle_n |f(x)\rangle_{n-1} \\ &= \frac{1}{2^{n/2}} \sum_{y=0}^{2^{n-1}-1} (|x_0\rangle_n + |x_0 \oplus a\rangle_n) |y\rangle_{n-1} \\ &\quad \text{where } f(x_0) = y \\ &= \frac{1}{2^{n/2}} \sum_{y=0}^{2^{n-1}-1} \frac{1}{\sqrt{2}} (|x_0\rangle + |x_0 \oplus a\rangle) |y\rangle \end{aligned}$$

\therefore measuring output with result y
 leaves input state $\frac{1}{\sqrt{2}} (|x_0\rangle + |x_0 \oplus a\rangle)$

What we can't do

measuring output with result y
leaves input state $\frac{1}{\sqrt{2}}(|x_0\rangle + |x_0 \oplus a\rangle)$

- measure input: get random number x_0 or $x_0 \oplus a$
- clone input state, measure repeatedly to find x_0 and $x_0 \oplus a$ can't clone ☹️
- run repeatedly, measuring each time:
get different x_0 each time.

n-fold Hadamard $H^{\otimes n}$ 

$$H|x\rangle_1 = \frac{1}{\sqrt{2}} (|0\rangle + (-1)^x |1\rangle) = \frac{1}{\sqrt{2}} \sum_{y=0}^1 (-1)^{xy} |y\rangle$$

$$H^{\otimes n}|x\rangle_n = H|x_{n-1}\rangle_1 \otimes \dots \otimes H|x_0\rangle_1$$

$$= \frac{1}{2^{n/2}} \sum_{y_{n-1}=0}^1 \dots \sum_{y_0=0}^1 (-1)^{x_{n-1}y_{n-1} \oplus \dots \oplus x_0y_0} |y_{n-1}\rangle \dots |y_0\rangle$$

$$= \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle_n$$

x · y as defined for Bernstein-Vazirani

Note $H^{\otimes n}|0\rangle_n = \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} |y\rangle_n$

Another Hadamard

$$H^{\otimes n}|x\rangle_n = \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle_n$$

$$H^{\otimes n} \frac{1}{\sqrt{2}} (|x_0\rangle + |x_0 \oplus a\rangle)$$

$$= \frac{1}{2^{n/2}} \sum_{z=0}^{2^n-1} \left((-1)^{x_0 \cdot z} + (-1)^{(x_0 \oplus a) \cdot z} \right) |z\rangle_n$$

(|y>_{n-1} was output

$$= \frac{1}{2^{n/2}} \sum_{z=0}^{2^n-1} (-1)^{x_0 \cdot z} \left(1 + (-1)^{a \cdot z} \right) |z\rangle$$

$$= \frac{1}{2^{n/2}} \sum_{\substack{z=0 \\ a \cdot z = 0}}^{2^n-1} (-1)^{x_0 \cdot z} |z\rangle$$

2 if $a \cdot z = 0$
0 if $a \cdot z = 1$

In state - $\frac{1}{2^{n/2}} \sum_{\substack{z=0 \\ a \cdot z = 0}}^{2^n-1} (-1)^{x_0 \cdot z} |z\rangle$

Measure input: get result z
 z is random, except that -

We know $a \cdot z = 0$

If $z = 0$ - learn nothing about a

very improbable

Otherwise look at bits that are 1 in z
Corresponding bits in a sum to 0 (mod 2)

Repeat whole process

Search space is halved each time probably

Example

$n = 4$ $a \neq 0$ Search space for a

- $z = 0$ ☹️
- $z = 2$ 0010 😊
- $z = 6$ 0110 😊
- $z = 4$ 0100 ☹️
- $z = 11$ 1011 😊

0001	0010	0011	0100	0101	0110	0111
1000	1001	1010	1011	1100	1101	1110
0001	0010	0011	0100	0101	0110	0111
1000	1001	1010	1011	1100	1101	1110
0001	0010	0011	0100	0101	0110	0111
1000	1001	1010	1011	1100	1101	1110
0001	0010	0011	0100	0101	0110	0111
1000	1001	1010	1011	1100	1101	1110
0001	0010	0011	0100	0101	0110	0111
1000	1001	1010	1011	1100	1101	1110
0001	0010	0011	0100	0101	0110	0111
1000	1001	1010	1011	1100	1101	1110

$a = 9$

Example

$n = 4$ Symbolically

- $z = 0$ ☹️ $a \cdot 0 = 0$ $0 = 0$
 - $z = 2$ 0010 😊 $a \cdot 2 = 0$ $a_1 = 0$
 - $z = 6$ 0110 😊 $a \cdot 6 = 0$ $a_2 \oplus a_1 = 0, \therefore a_2 = 0$
 - $z = 4$ 0100 ☹️ $a \cdot 4 = 0$ $a_2 = 0$ we knew that
 - $z = 11$ 1011 😊 $a \cdot 11 = 0$ $a_3 \oplus a_1 \oplus a_0 = 0$
 $\therefore a_3 \oplus a_0 = 0$
- Two possibilities ~~0000~~ $a \neq 0$, 1001 $a = 9$

Summary of algorithm

- prepare state $H^{\otimes n} |0\rangle_n \otimes |0\rangle_{n-1}$
- apply U_f
- measure output actually, you don't need to do this
- apply $H^{\otimes n}$ to input
- measure input, result z
- record equation $a \cdot z = 0$
- repeat until equations determine a

Classical v. quantum

- One quantum measurement eliminates $2^{n/2}$ possibilities of a
 $\sim n$ measurements needed linear algorithm
- Two classical measurements - may find a exactly exceedingly unlikely
 - otherwise eliminate one possibility
 $\sim 2^{n/2}$ measurements needed exponential

Exact calculation

See Mermin

Some quantum measurements z useless
- tell you $a \cdot z = 0$ you knew already
 \therefore expect to need more than n .

With $n+k$ measurements:

probability of discovering a
 $= \left(1 - \frac{1}{2^{n+k}}\right) \left(1 - \frac{1}{2^{n+k-1}}\right) \dots \left(1 - \frac{1}{2^{k+2}}\right)$

e.g. $k=20$ prob $> 1 - \frac{1}{2^{21}} \approx 1 - \frac{1}{2 \times 10^6} > 1 - \frac{1}{2^{k+1}}$
better than a million to 1 !

Features of Simon's problem

- Much more efficient on quantum computer
exponential \rightarrow linear
 - Probabilities involved applications of f
Unlucky \Rightarrow iterations wasted
- But... with high probability get answer quickly
quantifiable