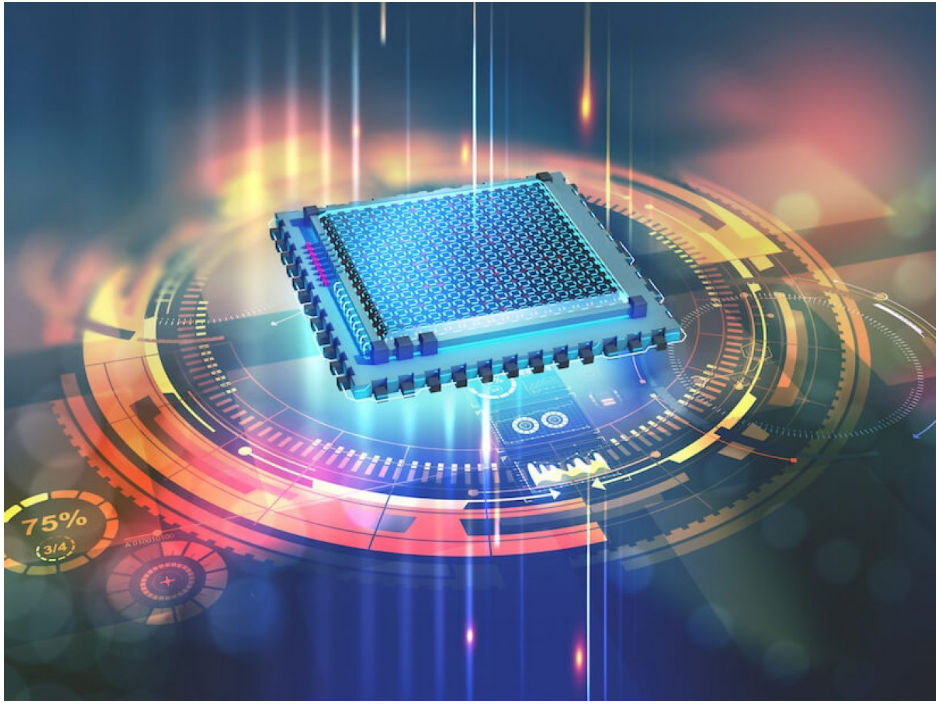
Bernstein-Vazirani Problem



Last class

- Deutsch’s problem
- Simplest example of quantum tradeoff that sacrifices particular information to get relational information.
- First “Quantum supremacy” result

Today

- Bernstein-Vazirani
- Another “Quantum supremacy” result

Bitwise Inner Product

- Let $x=(x_0,\ldots,x_n)$ and $a=(a_0,\ldots,a_n)$ be two integers, represented as n-bit strings.
- The bitwise inner product of x and a, denoted $x \cdot a$ modulo 2 is:

$$x_0a_0 \oplus x_1a_1 \oplus \ldots \oplus x_na_n$$

Binary arithmetic test

- Let $a=a_n\ldots a_0$ be an n-bit binary string (encoded as unsigned integer). What is the number a expressed in the decimal system?
- What is the value of the m-th bit of a?

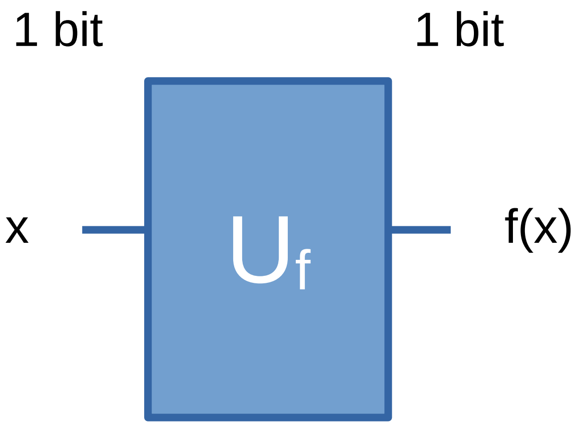
Bernstein-Vazirani

- Let a be an unknown non-negative integer less than 2^n
- Represent it as an n-bit string
- Let $f(x) = a \cdot x = x_0 a_0 \oplus x_1 a_1 \oplus \ldots \oplus x_n a_n$
- Suppose we have an oracle (subroutine) that given x, it gives you f(x)
- How many times do we need to call the oracle to determine a?

Bernstein-Vazirani

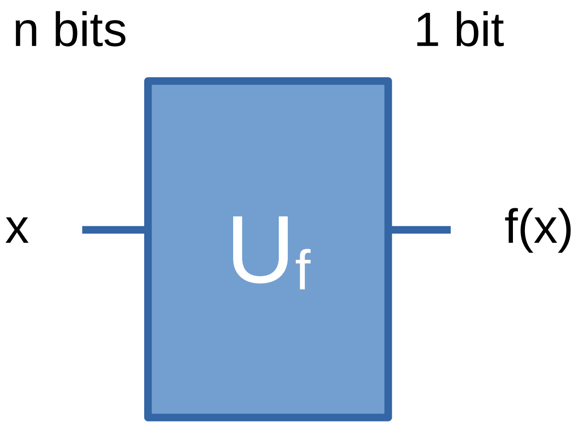
- Classically?
- We could learn the n bits of a by applying f to the n values $x = 2^m$, $0 \leq m < n$
- Each invocation tells me a bit of a
- Totally, n invocations of the subroutine
- With quantum we can ask once!
  - With some tricks…

The setup last time

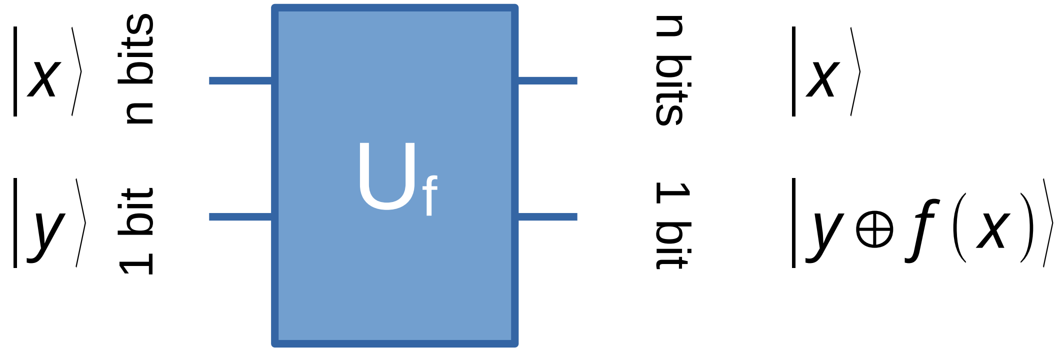


- Both input and output registers contain one bit
- Functions f that take one bit to one bit
- Two different ways to think about such f

The setup now

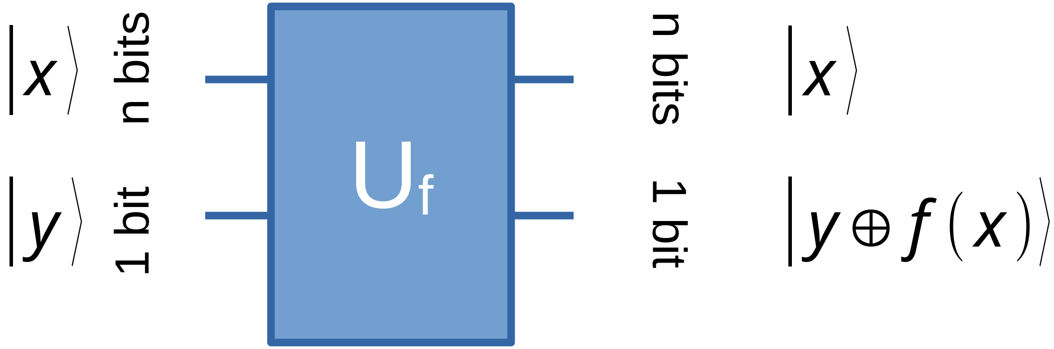


The setup, in quantum



- U_f applied to the computational basis state $|x\rangle_n |y\rangle_1$ flips the value y of the output register iff f(x)=1

The trick



- $U_f |x\rangle_n |0\rangle = |x\rangle_n |0 \oplus f(x)\rangle =$
  - $|x\rangle_n |0\rangle, \text{ if } f(x) = 0$
  - $|x\rangle_n |1\rangle, \text{ if } f(x) = 1$

$U_f |x\rangle_n |1\rangle = |x\rangle_n |1 \oplus f(x)\rangle =$
  - $|x\rangle_n |1\rangle, \text{ if } f(x) = 0$
  - $|x\rangle_n |0\rangle, \text{ if } f(x) = 1$

The trick

- It is useful here as well to set the output register to $HX|0\rangle = H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

$$U_f|x\rangle_n \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) =$$

  - $\frac{1}{\sqrt{2}}(|x\rangle_n \otimes |0\rangle - |x\rangle_n \otimes |1\rangle) \text{ if } f(x) = 0$
  - $\frac{1}{\sqrt{2}}(|x\rangle_n \otimes |1\rangle - |x\rangle_n \otimes |0\rangle) \text{ if } f(x) = 1$

$$= \frac{1}{\sqrt{2}}(-1)^{f(x)}(|x\rangle_n \otimes |0\rangle - |x\rangle_n \otimes |1\rangle)$$

This allows to change a bit flip to a sign change

Hadamard test

- Which is the formula for $H|x\rangle_1$?

$(A)\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$

$(B)\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$

$(C)\frac{1}{\sqrt{2}}(|0\rangle+(-1)^x|1\rangle)$

$(D)|x\rangle$

The second trick

- Recall: $H^{\otimes n}|0\rangle_n = \frac{1}{2^{n/2}} \sum_{0 \le x < 2^n} |x\rangle_n$
- From the previous slide:
  $H|x\rangle = \frac{1}{\sqrt{2}} \sum_{y=0,1} (-1)^{xy} |y\rangle$
- We need to generalize it to n qubits

Hadamard test, level up

- Which is the formula for $H^{\otimes n}|x\rangle_n$?

$$(A)\ \frac{1}{2^{n/2}}\sum_{0\le y<2^n}|x\rangle_n \qquad (B)\ -\frac{1}{2^{n/2}}\sum_{0\le y<2^n}|x\rangle_n$$

$$(C)\ \frac{1}{2^{n/2}}\sum_{0\le y<2^n}(-1)^{x\cdot y}|y\rangle_n \qquad (D)\ |x\rangle_n$$

Hadamard, level up solution

- Which is the formula for $H^{\otimes n}|x\rangle_n$?

$$H^{\otimes n}|x\rangle_n = \frac{1}{\sqrt{2}}\sum_{y=0,1}(-1)^{x_0 y}|y\rangle \otimes \ldots \otimes \frac{1}{\sqrt{2}}\sum_{y=0,1}(-1)^{x_{n-1} y}|y\rangle =$$

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

- Since x·y is used as exponent of -1, only its value mod 2 matters

The algorithm

- Prepare the input and output register

$$\left(H^{\otimes n}\otimes H\right)|0\rangle_n|1\rangle_1=\left(\frac{1}{2^{n/2}}\sum_{0\le x<2^n}|x\rangle_n\right)\frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right)$$

- Apply the function oracle

$$U_f\left(H^{\otimes n}\otimes H\right)|0\rangle_n|1\rangle_1=U_f\left(\frac{1}{2^{n/2}}\sum_{0\le x<2^n}|x\rangle_n\right)\frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right)=$$

$$=\left(\frac{1}{2^{n/2}}\sum_{0\le x<2^n}(-1)^{f(x)}|x\rangle_n\right)\frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right)$$

The algorithm (2)

- Prepare the input and output register
- Apply the function oracle

$$U_f(H^{\otimes n} \otimes H)|0\rangle_n|1\rangle_1 = \left(\frac{1}{2^{n/2}}\sum_{0\le x<2^n}(-1)^{f(x)}|x\rangle_n\right)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

- Apply Hadamard to the input register

$$(H^{\otimes n} \otimes 1)U_f(H^{\otimes n} \otimes H)|0\rangle_n|1\rangle_1 = \left(\frac{1}{2^{n/2}}H^{\otimes n}\sum_{0\le x<2^n}(-1)^{f(x)}|x\rangle_n\right)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) =$$

$$= \left(\frac{1}{2^n}\sum_{0\le x<2^n}\sum_{0\le y<2^n}(-1)^{f(x)+x\cdot y}|y\rangle_n\right)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

The algorithm (3)

- Prepare the input and output register
- Apply the function oracle
- Apply Hadamard to the input register

$$\left(H^{\otimes n} \otimes 1\right) U_f \left(H^{\otimes n} \otimes H\right) |0\rangle_n |1\rangle_1 =$$

$$= \left(\frac{1}{2^n} \sum_{0 \le x < 2^n} \sum_{0 \le y < 2^n} (-1)^{f(x) + x \cdot y} |y\rangle_n\right) \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) =$$

$$= \left(\frac{1}{2^n} \sum_{0 \le x < 2^n} \sum_{0 \le y < 2^n} (-1)^{a \cdot x + x \cdot y} |y\rangle_n\right) \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) =$$

$$= \left(\frac{1}{2^n} \sum_{0 \le x < 2^n} \sum_{0 \le y < 2^n} (-1)^{x \cdot (y + a)} |y\rangle_n\right) \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) =$$

Math test

- Let a =(a_1,a_2), y= (y_1,y_2) be arbitrary 2-bit strings such that y is not the same as a. What is $\sum_{x\in\{0,3\}}(-1)^{x\cdot(y+a)}$?

$(A)0$

$(B)4$

$(C)-4$

$(D)a\cdot y$

Math test solution

- Let a =(a1,a2), y= (y1,y2) be arbitrary 2-bit strings such that y is not the same as a. What is $\sum_{x \in \{0,3\}} (-1)^{x \cdot (y+a)}$?

$$\sum_{x \in \{0,3\}} (-1)^{x \cdot (y+a)} = \sum_{x \in \{0,3\}} (-1)^{\sum_{i=0}^{n-1} x_i (y_i + a_i)} = \sum_{x \in \{0,3\}} \prod_{i=0}^{n-1} (-1)^{x_i (y_i + a_i)} =$$

$$= \prod_{i=0}^{n-1} \sum_{x \in \{0,3\}} (-1)^{x_i (y_i + a_i)}$$

Math test solution

$$\sum_{x \in \{0,3\}} (-1)^{x \cdot (y+a)} = \prod_{i=0}^{n-1} \sum_{x \in \{0,3\}} (-1)^{x_i (y_i + a_i)}$$

- Since this is the exponent of -1, only its parity counts
- For $x_i = 0$, the term is 1, for $x_i = 1$ it is 1 if $y_i = a_i$, -1 otherwise
- We sum on all the possibilities, hence we alternate $x_i = 0$ and $x_i = 1$
- If $y_i \neq a_i$ they simplify, if $y_i = a_i$ they add up

Back to our problem

$$(H^{\otimes n} \otimes 1) U_f (H^{\otimes n} \otimes H) |0\rangle_n |1\rangle_1 =$$

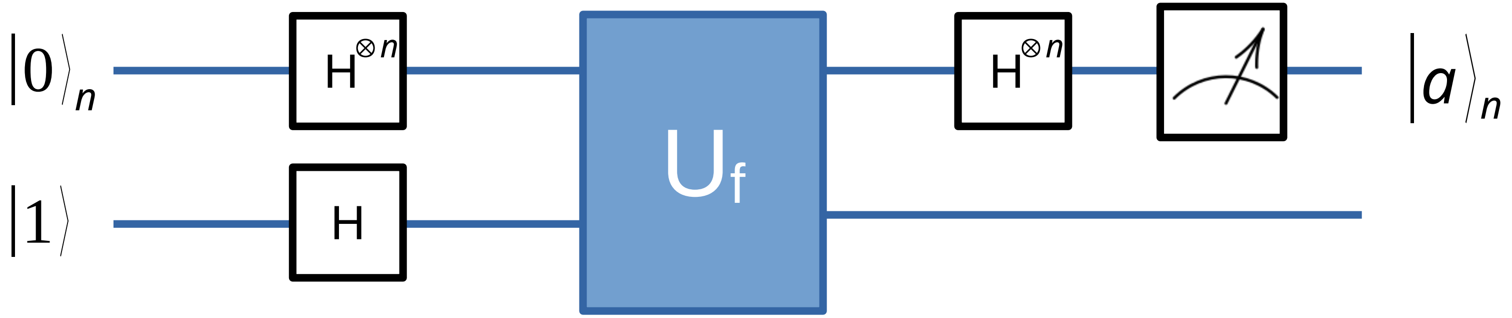
$$= \left(\frac{1}{2^n} \sum_{0 \le x < 2^n} \sum_{0 \le y < 2^n} (-1)^{x \cdot (y+a)} |y\rangle_n\right) \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) =$$

$$= \left(\frac{1}{2^n} 2^n |a\rangle_n\right) \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) = |a\rangle_n \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

- If we measure the input register we deterministically get a

The final circuit

$$\left(H^{\otimes n} \otimes 1\right) U_f \left(H^{\otimes n} \otimes H\right) |0\rangle_n |1\rangle_1$$



- We can restore the output register to $|1\rangle$ with an additional Hadamard