## Overview of Grover's search algorithm

(Adapted from Julian Brown, *The Quest for the Quantum Computer*, New York: Simon & Schuster, 2000.)

Suppose we've managed to discover the plaintext and corresponding ciphertext of a message encoded by an adversary using a known encryption algorithm with a secret 128-bit key. The message is "attackatdawn", and the ciphertext is "zvbegscixyfe". Since we know the encryption algorithm that was used, we can create a function $f$ that takes as input any 128-bit key $\mathbf{x}$, encrypts "attackatdawn" using that key, and then outputs 1 if the resulting ciphertext matches "zvbegscixyfe", or 0 if it doesn't. To discover our adversary's secret key, all we need to do is identify the input $\mathbf{x}$ such that $f(\mathbf{x}) = 1$. This is a job for Grover's algorithm!

Suppose a single evaluation of $f$ takes exactly *one picosecond* (one trillionth of a second).

How long would a classical computer using linear search take to find the key, on average?

picoseconds per century $= 10^{12} \times 60 \times 60 \times 24 \times 365 \times 100$

$$\text{time required} = \frac{\frac{1}{2} \times 2^{128} \text{ picoseconds}}{\text{picoseconds per century}} = 53{,}951{,}415{,}354{,}030{,}070 \text{ centuries}$$

More than 53 thousand trillion centuries!

How long would a quantum computer using Grover's algorithm take?

$$\text{time required} = \frac{\frac{\pi}{4} \times \sqrt{2^{128}} \text{ picoseconds}}{\text{picoseconds per century}} = 0.00459413 \text{ centuries}$$

About 5.5 months!

### Steps:

1. Initialize a 128-qubit register to a superposition of all keys from 0 to $2^{128} - 1$. This quantum state consists of $2^{128}$ amplitudes, exactly one of which corresponds to the key we are looking for. But the amplitudes are all equal and vanishingly small, and if we measured the register, the chances of obtaining the desired key would be practically zero.

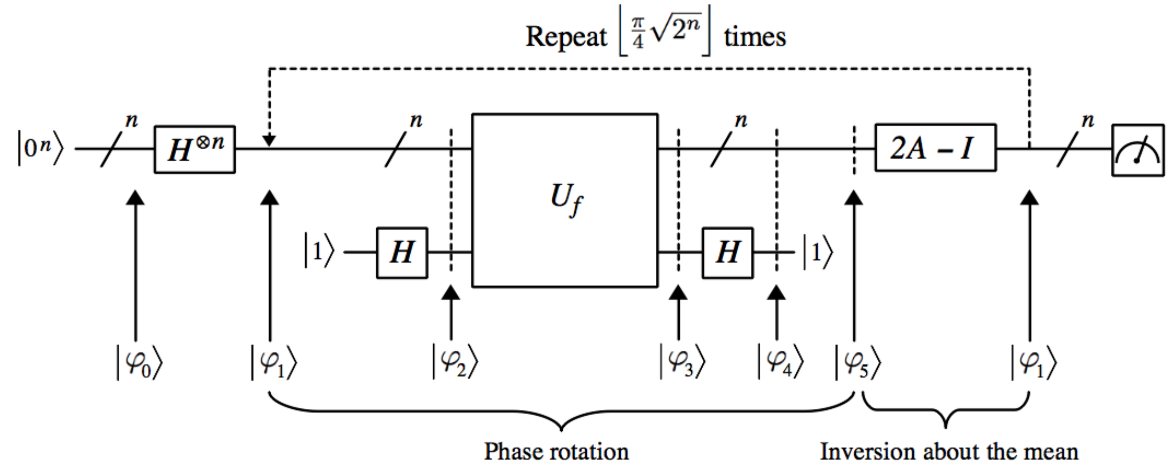
2. Apply $f$ to this superposition to calculate all possible ciphertexts of the plaintext message "attackatdawn" simultaneously, using quantum parallelism. The result is a superposition in which each key $\mathbf{x}$ is tied to its corresponding $f(\mathbf{x})$ value of 0 or 1, indicating whether that key's encoded ciphertext matches "zvbegscixyfe". This step is called *phase rotation*, and has the effect of negating the amplitude of the desired key, while leaving the others alone.

3. We find the mean of the amplitudes, and then subtract each amplitude from twice the mean. Together with step 2, this has the effect of slightly boosting the amplitude of the desired key, while making all of the others slightly shrink. This step is called *inversion about the mean.*

4. We "cook" the amplitudes by applying steps 2 and 3 over and over, a total of $\lfloor \frac{\pi}{4}\sqrt{2^{128}} \rfloor$ times.

5. We then measure the register. With very high probability, we will obtain the desired key.

## Grover's search algorithm



$|\varphi_0\rangle = |0^n\rangle$

So $|\varphi_1\rangle = H^{\otimes n}|\varphi_0\rangle = \dfrac{1}{\sqrt{2^n}} \displaystyle\sum_{\mathbf{x}\in\{0,1\}^n} |\mathbf{x}\rangle$

So $|\varphi_2\rangle = |\varphi_1\rangle \otimes H|1\rangle = \left(\dfrac{1}{\sqrt{2^n}} \displaystyle\sum_{\mathbf{x}\in\{0,1\}^n} |\mathbf{x}\rangle\right) \otimes H|1\rangle = \dfrac{1}{\sqrt{2^n}} \displaystyle\sum_{\mathbf{x}\in\{0,1\}^n} |\mathbf{x}\rangle \otimes H|1\rangle$

When $\mathbf{x}$ is a basis state (*i.e.*, a classical bit string), applying $U_f$ to $\mathbf{x}$ and $|0\rangle$ or $|1\rangle$ gives:

- $U_f\Big(|\mathbf{x}\rangle \otimes |0\rangle\Big) = |\mathbf{x}\rangle \otimes |0 \oplus f(\mathbf{x})\rangle = |\mathbf{x}\rangle \otimes |f(\mathbf{x})\rangle$
- $U_f\Big(|\mathbf{x}\rangle \otimes |1\rangle\Big) = |\mathbf{x}\rangle \otimes |1 \oplus f(\mathbf{x})\rangle = |\mathbf{x}\rangle \otimes |\overline{f(\mathbf{x})}\rangle$

When we apply $U_f$ to the superposition state $|\varphi_2\rangle$, we get:

$$U_f\left(\frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}} |\mathbf{x}\rangle \otimes H|1\rangle\right)$$

$$= \frac{1}{\sqrt{2^n}} U_f\left(\sum_{\mathbf{x}} |\mathbf{x}\rangle \otimes H|1\rangle\right) = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}} U_f\Big(|\mathbf{x}\rangle \otimes H|1\rangle\Big) \qquad \text{since } U_f \text{ is a linear operator}$$

$$= \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}} U_f\left(|\mathbf{x}\rangle \otimes \left(\tfrac{1}{\sqrt{2}}|0\rangle - \tfrac{1}{\sqrt{2}}|1\rangle\right)\right)$$

$$= \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}} U_f\left(\tfrac{1}{\sqrt{2}}\,|\mathbf{x}\rangle \otimes |0\rangle - \tfrac{1}{\sqrt{2}}\,|\mathbf{x}\rangle \otimes |1\rangle\right)$$

$$= \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}} \tfrac{1}{\sqrt{2}}\, U_f\Big(|\mathbf{x}\rangle \otimes |0\rangle\Big) - \tfrac{1}{\sqrt{2}}\, U_f\Big(|\mathbf{x}\rangle \otimes |1\rangle\Big) \qquad \text{since } U_f \text{ is a linear operator}$$

$$= \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}} \tfrac{1}{\sqrt{2}}\,|\mathbf{x}\rangle \otimes |f(\mathbf{x})\rangle - \tfrac{1}{\sqrt{2}}\,|\mathbf{x}\rangle \otimes |\overline{f(\mathbf{x})}\rangle$$

$$= \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}} |\mathbf{x}\rangle \otimes \left( \tfrac{1}{\sqrt{2}} |f(\mathbf{x})\rangle - \tfrac{1}{\sqrt{2}} |\overline{f(\mathbf{x})}\rangle \right)$$

$$= \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}} \begin{cases} |\mathbf{x}\rangle \otimes \left( \tfrac{1}{\sqrt{2}}|0\rangle - \tfrac{1}{\sqrt{2}}|1\rangle \right) & \text{if } \mathbf{x} \neq \mathbf{x_0} \qquad \text{that is, if } f(\mathbf{x}) = 0 \\ |\mathbf{x}\rangle \otimes \left( \tfrac{1}{\sqrt{2}}|1\rangle - \tfrac{1}{\sqrt{2}}|0\rangle \right) & \text{if } \mathbf{x} = \mathbf{x_0} \qquad \text{that is, if } f(\mathbf{x}) = 1 \end{cases}$$

$$= \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}} \begin{cases} +|\mathbf{x}\rangle \otimes H|1\rangle & \text{if } \mathbf{x} \neq \mathbf{x_0} \qquad \text{that is, if } f(\mathbf{x}) = 0 \\ -|\mathbf{x}\rangle \otimes H|1\rangle & \text{if } \mathbf{x} = \mathbf{x_0} \qquad \text{that is, if } f(\mathbf{x}) = 1 \end{cases}$$

$$= \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}} (-1)^{f(\mathbf{x})} |\mathbf{x}\rangle \otimes H|1\rangle$$

$$= \left( \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}} (-1)^{f(\mathbf{x})} |\mathbf{x}\rangle \right) \otimes H|1\rangle$$

So $|\varphi_3\rangle = \left( \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}} (-1)^{f(\mathbf{x})} |\mathbf{x}\rangle \right) \otimes H|1\rangle$

So $|\varphi_4\rangle = \left( \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}} (-1)^{f(\mathbf{x})} |\mathbf{x}\rangle \right) \otimes HH|1\rangle = \left( \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}} (-1)^{f(\mathbf{x})} |\mathbf{x}\rangle \right) \otimes |1\rangle$

So $|\varphi_5\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}} (-1)^{f(\mathbf{x})} |\mathbf{x}\rangle$

Thus the "phase rotation" sequence of gates transforms the first $n$ qubits as follows:

$$\frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}} |\mathbf{x}\rangle \quad \longrightarrow \quad \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}} (-1)^{f(\mathbf{x})} |\mathbf{x}\rangle$$

which means that the sign of the amplitude of the $|\mathbf{x}\rangle$ component representing the special input string $\mathbf{x_0}$ that we are searching for gets negated, while all the other amplitudes remain the same.

We then apply the "inversion about the mean" operator $2A - I$ to $|\varphi_5\rangle$

$|\varphi_1\rangle = (2A - I)|\varphi_5\rangle$

... and repeat

## Grover's search algorithm: an example

| $x$ | $f(x)$ |
|---|---|
| 00 | 0 |
| 01 | 0 |
| 10 | 1 |
| 11 | 0 |

When $\mathbf{x}$ is one of the basis states $|00\rangle$, $|01\rangle$, $|10\rangle$, or $|11\rangle$, applying $U_f$ to $\mathbf{x}$ and $|0\rangle$ or $|1\rangle$ gives:

- $U_f\Big(|\mathbf{x}\rangle \otimes |0\rangle\Big) = |\mathbf{x}\rangle \otimes |0 \oplus f(\mathbf{x})\rangle = |\mathbf{x}\rangle \otimes |f(\mathbf{x})\rangle$
- $U_f\Big(|\mathbf{x}\rangle \otimes |1\rangle\Big) = |\mathbf{x}\rangle \otimes |1 \oplus f(\mathbf{x})\rangle = |\mathbf{x}\rangle \otimes |\overline{f(\mathbf{x})}\rangle$

| $\mathbf{x}$ | $f(\mathbf{x})$ | $U_f\Big(\lvert\mathbf{x}\rangle \otimes \lvert 0\rangle\Big)$ | $U_f\Big(\lvert\mathbf{x}\rangle \otimes \lvert 1\rangle\Big)$ |
|---|---|---|---|
| 00 | 0 | $\lvert 00\rangle \otimes \lvert 0\rangle$ | $\lvert 00\rangle \otimes \lvert 1\rangle$ |
| 01 | 0 | $\lvert 01\rangle \otimes \lvert 0\rangle$ | $\lvert 01\rangle \otimes \lvert 1\rangle$ |
| 10 | 1 | $\lvert 10\rangle \otimes \lvert 1\rangle$ | $\lvert 10\rangle \otimes \lvert 0\rangle$ |
| 11 | 0 | $\lvert 11\rangle \otimes \lvert 0\rangle$ | $\lvert 11\rangle \otimes \lvert 1\rangle$ |

$$|\varphi_0\rangle = |00\rangle$$

$$|\varphi_1\rangle = (H \otimes H)|00\rangle = \tfrac{1}{2}|00\rangle + \tfrac{1}{2}|01\rangle + \tfrac{1}{2}|10\rangle + \tfrac{1}{2}|11\rangle$$

$$\begin{aligned}|\varphi_2\rangle = |\varphi_1\rangle \otimes H|1\rangle &= \Big(\tfrac{1}{2}|00\rangle + \tfrac{1}{2}|01\rangle + \tfrac{1}{2}|10\rangle + \tfrac{1}{2}|11\rangle\Big) \otimes H|1\rangle \\ &= \tfrac{1}{2}|00\rangle \otimes H|1\rangle + \tfrac{1}{2}|01\rangle \otimes H|1\rangle + \tfrac{1}{2}|10\rangle \otimes H|1\rangle + \tfrac{1}{2}|11\rangle \otimes H|1\rangle\end{aligned}$$

$$\begin{aligned}|\varphi_3\rangle &= U_f\Bigg(\tfrac{1}{2}|00\rangle \otimes H|1\rangle + \tfrac{1}{2}|01\rangle \otimes H|1\rangle + \tfrac{1}{2}|10\rangle \otimes H|1\rangle + \tfrac{1}{2}|11\rangle \otimes H|1\rangle\Bigg) \\ &= \tfrac{1}{2}\,U_f\Big(|00\rangle \otimes H|1\rangle\Big) + \tfrac{1}{2}\,U_f\Big(|01\rangle \otimes H|1\rangle\Big) + \tfrac{1}{2}\,U_f\Big(|10\rangle \otimes H|1\rangle\Big) + \tfrac{1}{2}\,U_f\Big(|11\rangle \otimes H|1\rangle\Big) \\ &= \tfrac{1}{2}\Bigg(U_f\Big(|00\rangle \otimes \Big(\tfrac{1}{\sqrt{2}}|0\rangle - \tfrac{1}{\sqrt{2}}|1\rangle\Big)\Big) + U_f\Big(|01\rangle \otimes \Big(\tfrac{1}{\sqrt{2}}|0\rangle - \tfrac{1}{\sqrt{2}}|1\rangle\Big)\Big) + \\ &\qquad U_f\Big(|10\rangle \otimes \Big(\tfrac{1}{\sqrt{2}}|0\rangle - \tfrac{1}{\sqrt{2}}|1\rangle\Big)\Big) + U_f\Big(|11\rangle \otimes \Big(\tfrac{1}{\sqrt{2}}|0\rangle - \tfrac{1}{\sqrt{2}}|1\rangle\Big)\Big)\Bigg) \\ &= \tfrac{1}{2}\Bigg(U_f\Big(\tfrac{1}{\sqrt{2}}|00\rangle \otimes |0\rangle - \tfrac{1}{\sqrt{2}}|00\rangle \otimes |1\rangle\Big) + U_f\Big(\tfrac{1}{\sqrt{2}}|01\rangle \otimes |0\rangle - \tfrac{1}{\sqrt{2}}|01\rangle \otimes |1\rangle\Big) + \\ &\qquad U_f\Big(\tfrac{1}{\sqrt{2}}|10\rangle \otimes |0\rangle - \tfrac{1}{\sqrt{2}}|10\rangle \otimes |1\rangle\Big) + U_f\Big(\tfrac{1}{\sqrt{2}}|11\rangle \otimes |0\rangle - \tfrac{1}{\sqrt{2}}|11\rangle \otimes |1\rangle\Big)\Bigg)\end{aligned}$$

$$= \frac{1}{2}\Bigg( \frac{1}{\sqrt{2}} U_f\Big(|00\rangle \otimes |0\rangle\Big) - \frac{1}{\sqrt{2}} U_f\Big(|00\rangle \otimes |1\rangle\Big) + \frac{1}{\sqrt{2}} U_f\Big(|01\rangle \otimes |0\rangle\Big) - \frac{1}{\sqrt{2}} U_f\Big(|01\rangle \otimes |1\rangle\Big) +$$

$$\frac{1}{\sqrt{2}} U_f\Big(|10\rangle \otimes |0\rangle\Big) - \frac{1}{\sqrt{2}} U_f\Big(|10\rangle \otimes |1\rangle\Big) + \frac{1}{\sqrt{2}} U_f\Big(|11\rangle \otimes |0\rangle\Big) - \frac{1}{\sqrt{2}} U_f\Big(|11\rangle \otimes |1\rangle\Big)\Bigg)$$

$$= \frac{1}{2}\Bigg( \frac{1}{\sqrt{2}}\Big(|00\rangle \otimes |0\rangle\Big) - \frac{1}{\sqrt{2}}\Big(|00\rangle \otimes |1\rangle\Big) + \frac{1}{\sqrt{2}}\Big(|01\rangle \otimes |0\rangle\Big) - \frac{1}{\sqrt{2}}\Big(|01\rangle \otimes |1\rangle\Big) +$$

$$\frac{1}{\sqrt{2}}\Big(|10\rangle \otimes |1\rangle\Big) - \frac{1}{\sqrt{2}}\Big(|10\rangle \otimes |0\rangle\Big) + \frac{1}{\sqrt{2}}\Big(|11\rangle \otimes |0\rangle\Big) - \frac{1}{\sqrt{2}}\Big(|11\rangle \otimes |1\rangle\Big)\Bigg)$$

$$= \frac{1}{2}\Bigg( |00\rangle \otimes \Big(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\Big) + |01\rangle \otimes \Big(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\Big) +$$

$$|10\rangle \otimes \Big(\frac{1}{\sqrt{2}}|1\rangle - \frac{1}{\sqrt{2}}|0\rangle\Big) + |11\rangle \otimes \Big(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\Big)\Bigg)$$

$$= \frac{1}{2}\Bigg( |00\rangle \otimes \Big(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\Big) + |01\rangle \otimes \Big(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\Big) +$$

$$- |10\rangle \otimes \Big(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\Big) + |11\rangle \otimes \Big(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\Big)\Bigg)$$

$$= \frac{1}{2}\Bigg( |00\rangle \otimes H|1\rangle + |01\rangle \otimes H|1\rangle - |10\rangle \otimes H|1\rangle + |11\rangle \otimes H|1\rangle \Bigg)$$

$$= \Bigg( \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle - \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle \Bigg) \otimes H|1\rangle$$

$$|\varphi_4\rangle = \Bigg( \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle - \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle \Bigg) \otimes HH|1\rangle = \Bigg( \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle - \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle \Bigg) \otimes |1\rangle$$

$$|\varphi_5\rangle = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle - \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$$

So phase rotation has transformed $|\varphi_1\rangle \rightarrow |\varphi_5\rangle$:

$$\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle \quad \rightarrow \quad \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle - \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$$

$$\begin{bmatrix} \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \end{bmatrix} \quad \rightarrow \quad \begin{bmatrix} \frac{1}{2} \\ \frac{1}{2} \\ -\frac{1}{2} \\ \frac{1}{2} \end{bmatrix}$$

Inversion about the mean:

$$A = \begin{bmatrix} \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \end{bmatrix} \qquad 2A - I = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{bmatrix} - \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \end{bmatrix}$$

$$|\varphi_6\rangle = (2A - I)|\varphi_5\rangle = \begin{bmatrix} -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \end{bmatrix} \begin{bmatrix} \frac{1}{2} \\ \frac{1}{2} \\ -\frac{1}{2} \\ \frac{1}{2} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

Measuring $|\varphi_6\rangle$ would give $\mathbf{x_0} = \mathbf{10}$ with 100% certainty.

```
# Grover's search algorithm

def grover(f_outputs):
    numOutputs = len(f_outputs)
    assert numOutputs > 1 and powerof2(numOutputs)

    # initialization
    n = log2(numOutputs)
    U = makeUf(f_outputs)
    H1 = H * q1
    A = Ones(2**n).scale(1.0/(2**n))
    InvertAboutMean = A.scale(2) - Iden(2**n)

    # create a superposition of all numbers from 0 to 2**n - 1
    phi0 = q0.tensorPower(n)
    phi1 = H.tensorPower(n) * phi0

    # repeat
    iterations = int((pi/4) * sqrt(2**n))
    for i in range(iterations):

        # phase rotation
        phi2 = phi1.tensor(H1)
        phi3 = U * phi2
        # drop last output qubit
        phi4 = IDEN.tensorPower(n).tensor(H) * phi3
        phi5 = factorX1(phi4)

        # inversion about the mean
        phi1 = InvertAboutMean * phi5

    print phi1
```