

Quantum Computation

Amplitude amplification

Luís Soares Barbosa & Renato Neves



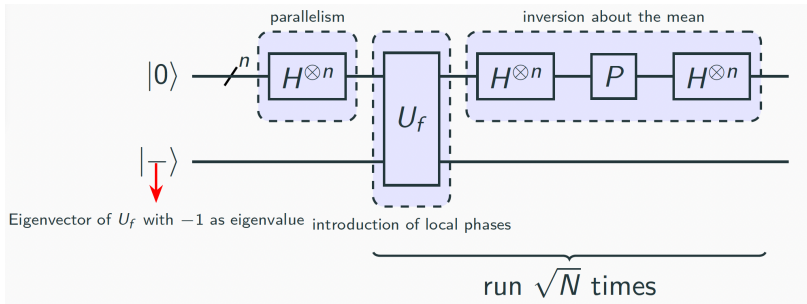
Universidade do Minho



MSc Physics Engineering

Universidade do Minho, 2024-25

Recall Grover's iterator $G = WU_f$



Question

Can Grover's algorithm be generalised to search in contexts with multiple solutions?

Multiple solutions

Assume there are M (out of $2^n = N$) input strings evaluating to 0 by f

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle = \underbrace{\sqrt{\frac{M}{N}}|s\rangle}_{\text{solution}} + \underbrace{\sqrt{\frac{N-M}{N}}|r\rangle}_{\text{the rest}}$$

where

$$|s\rangle = \frac{1}{\sqrt{M}} \sum_{x \text{ solution}} |x\rangle \quad \text{and} \quad |r\rangle = \frac{1}{\sqrt{N-M}} \sum_{x \text{ no solution}} |x\rangle$$

Multiple solutions

$$t = \left\lceil \frac{\frac{\pi}{2} - \arcsin \sqrt{\frac{M}{N}}}{2\theta} \right\rceil$$

which, for N large, $M \ll N$ (thus $\theta \approx \sin \theta$), yields

$$t \approx \frac{\pi}{4} \sqrt{\frac{N}{M}}$$

The probability to retrieve a correct solution is

$$|\langle s | G^t | \psi \rangle|^2 \geq \cos^2 \theta = 1 - \sin^2 \theta = \frac{N - M}{N}$$

which, for $M = \frac{N}{2}$ yields $\frac{1}{2}$, but for $M \ll N$, is again close to 1.

Multiple solutions

Computing the effect of G : 2θ

$$2\theta = \arcsin\left(2\frac{\sqrt{M(N-M)}}{N}\right)$$

WHY?

M (out of 100)	$\sin 2\theta$	2θ
0		
1		
20		
30		
40		
50		
60		
70		
80		
99		
M		

Multiple solutions

Computing the effect of G : 2θ

$$2\theta = \arcsin\left(2\frac{\sqrt{M(N-M)}}{N}\right)$$

M (out of 100)	$\sin 2\theta$	2θ
0	0	0
1	0.198	0.199
20	0.8	0.927
30	0.916	1.158
40	0.979	1.365
50	1	1.571
60	0.979	1.365
70	0.916	1.158
80	0.8	0.927
99	0.198	0.199
M	0	0

Multiple solutions

Surprisingly, the rotation in each iteration decreases from $M = \frac{N}{2}$ to N , and the number of iterations consequently increases, although one would expect to be easier to find a correct solution if their number increases!

Solution: resort to draft paper!

To double the number of elements in the search space, by adding N extra elements, none of which being a solution.

The technique: Amplitude amplification

Grover's algorithm made use of

$$H^{\otimes n}|0\rangle$$

to prepare a **uniform** superposition of potential solutions.

In general, one may resort to any program K to map the solution space to any **superposition of guesses**, plus some extra qubits to be used as **draft paper**:

$$K|0\rangle = \sum_x \alpha_x |x\rangle |\text{draft}(x)\rangle$$

The technique: Amplitude amplification

$$|\psi\rangle = \sum_{x \text{ solution}} \alpha_x |x\rangle |\text{draft}(x)\rangle + \sum_{x \text{ no solution}} \alpha_x |x\rangle |\text{draft}(x)\rangle$$

yielding the following **probabilities**:

$$p_s = \sum_{x \text{ solution}} |\alpha_x|^2 \quad \text{and} \quad p_{ns} = \sum_{x \text{ no solution}} |\alpha_x|^2 = 1 - p_s$$

Of course, amplification has no use if $p_s \in \{0, 1\}$.

The technique: Amplitude amplification

Otherwise ($0 < p_s < 1$), the amplitudes of **solution** inputs should be amplified.

First, express

$$|\psi\rangle = \sqrt{p_s}|\psi_s\rangle + \sqrt{p_{ns}}|\psi_{ns}\rangle$$

for the **normalised** components

$$|\psi_s\rangle = \sum_{x \text{ solution}} \frac{\alpha_x}{\sqrt{p_s}} |x\rangle |\text{draft}(x)\rangle$$

$$|\psi_{ns}\rangle = \sum_{x \text{ solution}} \frac{\alpha_x}{\sqrt{p_{ns}}} |x\rangle |\text{draft}(x)\rangle$$

which rewrites to

$$|\psi\rangle = \sin \theta |\psi_s\rangle + \cos \theta |\psi_{ns}\rangle$$

for $\theta \in [0, \frac{\pi}{2}]$ such that $\sin^2 \theta = p_s$.

The technique: Amplitude amplification

A generic search iterator is built as

$$S = KPK^{-1}V = W_KV$$

where

$$W_K|\psi\rangle = |\psi\rangle$$

$$W_K|\phi\rangle = -|\phi\rangle \quad \text{for all states orthogonal to } |\psi\rangle$$

The sets $\{|\psi_s\rangle, |\psi_{ns}\rangle\}$ and $\{|\psi\rangle, |\bar{\psi}\rangle\}$ are bases for the relevant 2-dimensional subspace.

The technique: Amplitude amplification

As expected, starting in $|\psi\rangle$, the oracle produces

$$-\sin\theta|\psi_s\rangle + \cos\theta|\psi_{ns}\rangle = \cos(2\theta)|\psi\rangle - \sin(2\theta)|\bar{\psi}\rangle$$

which, followed by the amplifier, yields

$$\cos(2\theta)|\psi\rangle + \sin(2\theta)|\bar{\psi}\rangle$$

i.e. the effect of iterator S is

$$S|\psi\rangle = \cos(2\theta)|\psi\rangle + \sin(2\theta)|\bar{\psi}\rangle$$

The technique: Amplitude amplification

Exercise

Show that

$$S|\psi\rangle = \cos(2\theta)|\psi\rangle + \sin(2\theta)|\bar{\psi}\rangle$$

can be expressed in the basis $\{|\psi_s\rangle, |\psi_{ns}\rangle\}$ as

$$S|\psi\rangle = \sin(3\theta)|\psi_s\rangle + \cos(3\theta)|\psi_{ns}\rangle$$

The technique: Amplitude amplification

$$\begin{aligned}
 S|\psi\rangle &= \cos(2\theta)|\psi\rangle + \sin(2\theta)|\bar{\psi}\rangle \\
 &= \cos(2\theta)(\sin\theta|\psi_s\rangle + \cos\theta|\psi_{ns}\rangle) + \sin(2\theta)(\cos\theta|\psi_s\rangle - \sin\theta|\psi_{ns}\rangle) \\
 &= \cos(2\theta)\sin\theta|\psi_s\rangle + \cos(2\theta)\cos\theta|\psi_{ns}\rangle + \sin(2\theta)\cos\theta|\psi_s\rangle - \sin(2\theta)\sin\theta|\psi_{ns}\rangle \\
 &= (\cos(2\theta)\sin\theta + \sin(2\theta)\cos\theta)|\psi_s\rangle + (\cos(2\theta)\cos\theta - \sin(2\theta)\sin\theta)|\psi_{ns}\rangle \\
 &= ((\cos^2\theta - \sin^2\theta)\sin\theta + \sin(2\theta)\cos\theta)|\psi_s\rangle + ((\cos^2\theta - \sin^2\theta)\cos\theta - \sin(2\theta)\sin\theta)|\psi_{ns}\rangle \\
 &= (\cos^2\theta\sin\theta - \sin^2\theta\sin\theta + \sin(2\theta)\cos\theta)|\psi_s\rangle + (\cos^2\theta\cos\theta - \sin^2\theta\cos\theta - \sin(2\theta)\sin\theta)|\psi_{ns}\rangle \\
 &= (\cos^2\theta\sin\theta - \sin^3\theta + 2\sin\theta\cos^2\theta)|\psi_s\rangle + (\cos^3\theta - \sin^2\theta\cos\theta - 2\sin^2\theta\cos\theta)|\psi_{ns}\rangle \\
 &= (\cos^2\theta\sin\theta - \sin^3\theta + 2\sin\theta\cos^2\theta)|\psi_s\rangle + (\cos^3\theta - \sin^2\theta\cos\theta - 2\sin^2\theta\cos\theta)|\psi_{ns}\rangle \\
 &= (3\cos^2\theta\sin\theta - \sin^3\theta)|\psi_s\rangle + (\cos^3\theta - 3\sin^2\theta\cos\theta)|\psi_{ns}\rangle \\
 &= (3(1 - \sin^2\theta)\sin\theta - \sin^3\theta)|\psi_s\rangle + (\cos^3\theta - 3(1 - \cos^2\theta)\cos\theta)|\psi_{ns}\rangle \\
 &= (3\sin\theta - 3\sin^3\theta - \sin^3\theta)|\psi_s\rangle + (\cos^3\theta - 3\cos\theta + 3\cos^2\theta)|\psi_{ns}\rangle \\
 &= (3\sin\theta - 4\sin^3\theta)|\psi_s\rangle + (4\cos^3\theta - 3\cos\theta)|\psi_{ns}\rangle \\
 &= \sin(3\theta)|\psi_s\rangle + \cos(3\theta)|\psi_{ns}\rangle
 \end{aligned}$$

The technique: Amplitude amplification

By an inductive argument, the repeated application of S a total of k times rotates the initial state $|\psi\rangle$ to

$$S^k|\psi\rangle = \sin((2k+1)\theta)|\psi_s\rangle + \cos((2k+1)\theta)|\psi_{ns}\rangle$$

For the correct number of iterations, this procedure reaches a state such that a measurement will return an element of the **subspace spanned by $|\psi_s\rangle$** with a probability close to 1.

The technique: Amplitude amplification

As before, to get that high probability, the smallest value for k one can choose is such that

$$(2k + 1)\theta \approx \frac{\pi}{2}$$

For a **small** θ , as

$$\sin \theta = \sqrt{p_s} \approx \theta$$

the magnitude of the right number of iterations is

$$\mathcal{O}\left(\sqrt{\frac{1}{\theta}}\right)$$

because

$$(2k + 1)\sqrt{p_s} = \theta \Leftrightarrow k = \frac{\pi}{4\sqrt{p_s}} - \frac{1}{2}$$

To follow

The algorithm requires that one knows **in advance** how many times iterator S is to be applied:

- For $K = H$ (uniform sampling the input) this boils down to know the number of solutions of the search problem.
- For a generic K this amounts to know the probability with which K guesses a solution to the problem, i.e. $\sin(\theta)$.

To see ...

- **blind** search
- **estimate the amplitude** with which K maps $|0\rangle$ to the subspace of solutions

