Dipartimento di Fisica
Corso di laurea magistrale in Scienze fisiche

Algoritmi di ricerca quantistica assistiti da entanglement

Tesi per la laurea di:
Davide Falco
Mat. 536063

Relatore:
Prof. Paolo Perinotti

Anno accademico 2024 – 2025

Contents

This page was intentionally left blank

Introduction

Quantum computation has radically changed our understanding of what is computationally achievable within the laws of physics. However, to make this statement precise, one must first distinguish between different notions of algorithmic complexity, most notably *time* complexity and *query* complexity.

- *Time* complexity refers to the total number of elementary operations required for an algorithm to complete a task, from state preparation to the final measurement.

- *Query* complexity refers to the number of calls to an *oracle*, namely a black-box encoding information about the solution of the problem.

In oracle-based models, query complexity captures only one part of the overall computational cost, and is therefore typically no greater than the total time complexity.

Among the earliest and most striking examples of quantum advantage stands Grover's search algorithm, which demonstrated that an unstructured search problem, classically requiring $O(N)$ oracle queries, can be solved quantum mechanically in only $O(\sqrt{N})$ queries[11]. This quadratic speed-up represents one of the most fundamental separations between classical and quantum computation.
However, there are two points about the standard formulation of Grover's algorithm that deserve closer examination:

- It assumes a fully connected, abstract search space in which all computational basis states are equally and instantaneously accessible.

- The optimality proof[5] is built on the idea of studying a single register with an encoded generic state $|\psi\rangle$ where we apply the necessary operators.

Regarding the first point, in realistic physical scenarios, information is often encoded in different spatially distributed points in constrained structures, where locality and geometry impose limitations on propagation velocity and interference. This observation motivated the development of spatial search algorithms based on quantum walks, where the topology of an underlying graph directly affects algorithmic performance. As we will see in the dedicated section, this will impose some limitation on our quantum walk operator U.

In general, quantum walks have since emerged as a powerful framework for quantum algorithms[21], in both their discrete and continuous versions[10]. They generalize classical random walks, enabling search processes that outperform their classical counterparts even under locality constraints. Notably, quantum walk–based search algorithms on structured graphs, such as two-dimensional lattices, retain a quantum advantage, though typically at a slightly higher asymptotic complexity[3] than combinatorial Grover search due to limited propagation speed.

Furthermore, regarding the optimality proof, it has been proven that the structure of Grover's operator is optimal, but even though the proof was written considering a black-box scenario with a generic initial state $|\psi\rangle$, the evolution operators were still applied on a single register, with no bound on the possible results on entangled registers.
In general, entanglement remains the most distinctive trait of quantum theory[4] with many applications also in quantum computation theory, and despite that, the role of entanglement in search algorithms is not so straightforward and explored. This raises a natural and fundamental question:

> Can entanglement between multiple quantum systems be exploited to enhance the success probability of quantum search algorithms beyond known bounds?

This thesis investigates precisely this question. In order to do this, we explore two different search protocols, one spatially-constrained and one based on combinatorial Grover search, in which two quantum "walkers" (or equivalently, two registers) are prepared in entangled states and evolved in parallel. By analyzing symmetric and anti-symmetric configurations, along with more generic non-maximally entangled states, we study how interference terms contribute to the overall success probability and whether entanglement can effectively amplify search performance.

Structure of the thesis

This thesis is organized into six main chapters:

- **Chapter 1**: A review of Grover's algorithm and its geometric interpretation in Hilbert space.
- **Chapter 2**: An introduction to Quantum Amplitude Amplification (QAA), random walks, and quantum walks, with particular emphasis on spatial search on structured graphs.
- **Chapter 3**: An analysis of symmetric and antisymmetric entangled states and their effect on the success probability in quantum search scenarios.
- **Chapter 4**: A mathematical investigation culminating in a no-go theorem showing that the interference term in the success probability of maximally

entangled states decays asymptotically as $N \to \infty$ under tensor-product unitary evolution.

- **Chapter 5**: A numerical study of entanglement-assisted search strategies in systems with single and multiple solutions in space-constrained scenarios on a $2D$ lattice.
- **Chapter 6**: An analytical comparison of the different entanglement-assisted search protocols, including the role of two different auxiliary states and the scaling of the interference contribution across different solution-space regimes.

Our results sheds more light on the role of entanglement in quantum search. While anti-symmetric states can enhance success probability in finite-size systems, we demonstrate that for large databases the interference term responsible for the improvement vanishes asymptotically. This establishes fundamental limitations on entanglement-assisted speed-ups in standard amplitude amplification settings.

Chapter 1: Grover algorithm

1.1 Combinatorial Grover search

Grover's quantum search algorithm has been since its invention one of the most important result in quantum computation, showing the theoretical power of quantum computers, and their advantage over the classical counterpart.

The search problem goes as follows: given an unstructured array of $N = 2^k$ elements, where k is the number of qubits (or bits) used, the algorithm, classical or quantum, is given the task of finding a specific entry of the register, marked with a specific sequence of qubits (or bits). Classically, an algorithm needs at most N steps to discover with certainty the marked entry, so the number of queries needed is $O(N)$. Grover showed in his seminal paper[11], that a specifically designed quantum algorithm requires at most only $O(\sqrt{N})$ queries to reach certainty for an unstructured database, showing a quadratic speed up over the classical case.
The core idea of the quantum algorithm is to use a function f known as the "oracle" or black-box, that has knowledge of the solution in the system and can "mark" it. Classically, it acts as follows:

$$f(x) = \begin{cases} 1 & \text{if } x = x_0 \\ 0 & \text{if } x \neq x_0 \end{cases} \tag{1.1}$$

where x_0 is some specific value of the variable.
Quantumly, the same action can be performed by a unitary transformation acting on two registers, the first one with the information about the input string, and the second with the a single qubit where the output of the function will be registered:

$$R_f |x\rangle |b\rangle = \begin{cases} |x_0\rangle |b \oplus 1\rangle & \text{if } x = x_0 \\ |x\rangle |b\rangle & \text{if } x \neq x_0 \end{cases} \tag{1.2}$$

Given that the initial state of the algorithm is $|\psi_0\rangle = (H^{\otimes k} |0\rangle^{\otimes k}) \otimes (H |1\rangle) = |H\rangle |-\rangle$, it can be thought as distributing the information about the correct state on the input states that will be later measured. The quantum oracle can also be rewritten as follow:

$$R_f = I - 2|x\rangle\langle x| \rightarrow R_f |y\rangle = |y\rangle - 2\delta_{x,y} |x\rangle \tag{1.3}$$

This is due to the action of the oracle:

$$R_f\,|x_0\rangle\,|-\rangle = \frac{R_f\,|x_0\rangle\,|0\rangle - R_f\,|x_0\rangle\,|1\rangle}{\sqrt{2}} = \frac{R_f\,|x_0\rangle\,|1\rangle - R_f\,|x_0\rangle\,|0\rangle}{\sqrt{2}} = -R_f\,|x_0\rangle\,|-\rangle \tag{1.4}$$

After the oracle, a "diffusion operator" R_D is applied, defined as follows:

$$R_H = H^{\otimes k}(I - 2\,|0\rangle\langle 0|)H^{\otimes k} = I - 2\,|D\rangle\langle D| \tag{1.5}$$

where $H\,|0\rangle = |D\rangle = \frac{1}{\sqrt{2^k}}\sum_{y\in\{0,1\}^k}|y\rangle$, a uniform superposition with real coefficients of all the computational basis states.
Geometrically, the oracle act as a reflection around the plane orthogonal to the solution state $|x_0\rangle$, while the diffusion operator act as a reflection around the initialized state $H^{\otimes k}\,|0\rangle^{\otimes k} = |D\rangle$. A visual representation of the whole operation is the following:

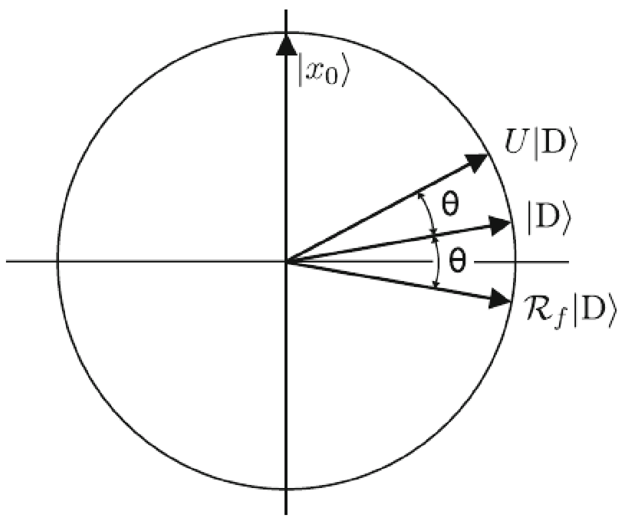


Figure 1.1: Grover's algorithm action

where $U = R_H R_f$. The whole algorithm aims to move with every iteration the vector state closer to the axis defined by $|x_0\rangle$. It can be easily proved[18] that after a number t_f of iterations of our unitary operator U, where $t_f = \lfloor \frac{\pi}{4\sqrt{p}} \rfloor$ and p is the initial success probability before the algorithm's applications (in our case $p = \frac{1}{\sqrt{2^k}}$), the final success probability is:

$$p_{x_0} = |\,\langle x_0|\,U^{t_f}\,|D\rangle\,|^2 \geq 1 - \frac{1}{2^k} \tag{1.6}$$

If the initial angle between the vector $\left|x_0^{\perp}\right\rangle = \frac{1}{\sqrt{2^k-1}}\sum_{y\in\{0,1\}^k, y\neq x_0}|y\rangle$ and $|D\rangle$ is $\theta_0 = \frac{\theta}{2}$, after a single iteration of the algorithm we have that the vector $U\,|D\rangle$ forms an angle $\theta_1 = \frac{\theta}{2} + \theta = \frac{3}{2}\theta$ with $\left|x_0^{\perp}\right\rangle$, so $U\,|D\rangle = \sin(\theta_1)\,|x_0\rangle + \cos(\theta_1)\left|x_o^{\perp}\right\rangle$. After n iterations, $U^n\,|D\rangle = \sin(\theta_n)\,|x_0\rangle + \cos(\theta_n)\left|x_0^{\perp}\right\rangle = \sin\!\big((n+\frac{1}{2})\theta\big)\,|x_0\rangle + \cos\big((n+\frac{1}{2})\theta\big)\left|x_0^{\perp}\right\rangle$.

The success probability will be the amplitude $\sin^2((n+\frac{1}{2})\theta)$, hence to have this quantity as close as possible to 1, we need to have that:

$$\Big(n+\frac{1}{2}\Big)\theta = \frac{\pi}{2} \rightarrow t_f = C.I.\Big[\Big(\frac{\pi}{\theta}-1\Big)\frac{1}{2}\Big] \tag{1.7}$$

Due to $\sin\big(\frac{\theta}{2}\big) = \frac{1}{\sqrt{2^k}}$, we have that $\theta = 2\arcsin\Big(\frac{1}{\sqrt{2^k}}\Big)$. For $k \gg 1$, $\theta \approx 2\frac{1}{\sqrt{2^k}}$, hence $t_f = \frac{\pi}{4}\sqrt{2^k} - \frac{1}{2} = \lfloor \frac{\pi}{4}\sqrt{N} \rfloor$, where $N = 2^k$.

In a more general framework, if there are multiple solutions[6] $m \geq 2$, where we require $m \ll N$, instead of a single $|x_0\rangle$ state, we will have the superposition:

$$|x_0\rangle = \frac{1}{\sqrt{m}} \sum_{|y\rangle \in M} |y\rangle\,, \quad \big|x_0^{\perp}\big\rangle = \frac{1}{\sqrt{N-m}} \sum_{|z\rangle, |z\rangle \notin M} |z\rangle \tag{1.8}$$

It is clear that for $m = 1$ we obtain again the previous case.

Optimality of Grover algorithm

As we said in the previous section, Grover algorithm can find a marked element in $O(\sqrt{N})$ queries. In their seminal paper, E.Bernstein, G.Brassard, U. Vazirani[5] proved that Grover algorithm is "optimal", meaning that no quantum algorithm can find a marked element in less than $\Omega(\sqrt{N})$ queries of the oracle function with a success probability greater that $\frac{1}{2}$ (the coin-tossed guess). We are going to retrace their seminal proof in the following section.

The algorithm used in the proof is built as a sequence of unitary operators, applied in series over a generic state $|\psi_0\rangle$, with a single measurement at the end. The state of the system at time t is the following:

$$|\psi_t\rangle = U_t R_f \ldots U_1 R_f U_0 |0\rangle \tag{1.9}$$

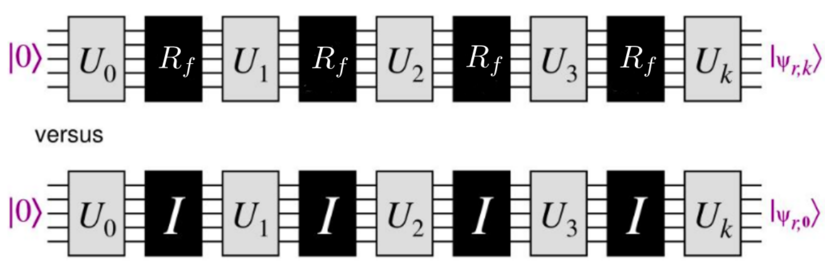


Figure 1.2: Black-box scheme in the optimality proof

The oracle R_f is in the form $R_f = 1 - 2|x_0\rangle\langle x_0|$, with (possibly) different unitary operators between each iterations. We will need also an auxiliary state:

$$|\phi_t\rangle = U_t \ldots U_0 |0\rangle \tag{1.10}$$

This state can be considered a "benchmark state", that we will use to see if the action of our oracles can improve the success probability. The quantity that we will study will be:

$$D_t = \frac{1}{N} \sum_{x_0=0}^{N-1} || \, |\psi_t\rangle - |\phi_t\rangle \, ||^2 \tag{1.11}$$

The sum runs over all the possible solution state. If, after t steps the distance D_t is too small, it will mean that we cannot distinguish effectively a marked element, implying that the action of the oracles is not able to improve our success probability. The following inequality can be proven:

$$c \leq D_t \leq \frac{4t^2}{N} \tag{1.12}$$

with $c > 0$. This also means that:

$$\sqrt{\frac{cN}{4}} \leq t \tag{1.13}$$

Meaning that any search algorithm able to improve the success probability of the initial state trough a certain number of queries to the oracle, must obey the lower bound for $t = \Omega(\sqrt{N})$. Therefore, a number of iterations smaller than that, like $t = N^{\frac{1}{4}}$, would violate this bound. This information, combined with Grover upper bound $O(\sqrt{N})$, implies that Grover algorithm, with its own unitary operator applied between different queries of the oracle, is optimally built, with $t = \theta(\sqrt{N})$ required iterations.

The main question we are going to tackle is the following: the unitary operators are applied in series on a single state, therefore a possible different and unexplored approach is to use instead two entangled "computers", and apply our operators in parallel on both of them, to see if there is room for improvement in the success probability. Moreover, we note that our scheme will retain the same structured operator, that will be in the form $U \otimes U$, applied on both registers. Therefore, the asymptotic complexity will remain the same.

Chapter 2: Preliminary tools

2.1 Quantum Amplitude amplification

G. Brasssard and P. Høyer in their seminal paper[7] have developed the notion of "Amplitude Amplification", which we will describe briefly, and show how Grover search can be seen as a special case of their algorithm.
Given a Hilbert space $\mathscr{H}$ containing all the possible states of a system, we denote as χ a boolean function that divides $\mathscr{H}$ into the direct sum of two subspaces: a "good" one and a "bad" one. In general, every pure state in $|\Gamma\rangle$ can be decomposed uniquely in these two subspaces as:

$$|\Gamma\rangle = a_0 |\Gamma_0\rangle + a_1 |\Gamma_1\rangle \tag{2.1}$$

The initial amplitudes are then a_0 and a_1, and because the two subspaces are orthogonal, it follows that: $|a_0|^2 + |a_1|^2 = 1$.
The aim of a QAA process is engineered to boost the coefficient a_0, which represents the fraction of the initial state in the "good" subspace. In order to do this, a specific operator Q is used, which is written as follows:

$$Q = -\mathscr{A}^{-1}\mathscr{S}_0\mathscr{A}\mathscr{S}_x \tag{2.2}$$

Where $\mathscr{A}$ is a generic unitary operator, used to initialize our system $|\psi\rangle = \mathscr{A}|0\rangle$. In Grover's case, this operator would be the Hadamard gate H.
The two operators $\mathscr{S}_0$ and $\mathscr{S}_x$ are reflections around respectively the initial state and the marked state. They are written as:

$$\mathscr{S}_x = 1 - 2|x\rangle\langle x|, \mathscr{S}_0 = 1 - 2|0\rangle\langle 0| \tag{2.3}$$

It can be shown that operator Q only acts non-trivially on the $2D$ plane $\mathscr{H}_\psi$ defined by $|\psi_1\rangle, |\psi_0\rangle$ (respectively, $|\psi\rangle$ components on the "good" subspace and the "bad" subspace), making the study of its effect much easier:

Consider the orthogonal complement $\mathscr{H}_\psi^\perp$ of $\mathscr{H}_\psi$. Since the operator $\mathscr{A}^{-1}\mathscr{S}_0\mathscr{A}$ acts as an identity on $\mathscr{H}_\psi^\perp$, the action of Q here is just $-\mathscr{S}_x$. But then, Q^2 is just the identity, so its eigenvalues outside $\mathscr{H}_\psi$, are ± 1. Therefore, in order to study Q, we just need to know what are its effects on the projection of any vector $|\psi\rangle$ on the subspace $\mathscr{H}_\psi$, where Q acts non-trivially[7].

Moreover, being Q a unitary operator, it has a set of orthonormal eigenvectors on such plane, which can be used to decompose $|\psi\rangle$ on the subspace. Then, it can be easily shown that:

$$Q^m |\psi\rangle = \sin((2m+1)\theta_a)|\psi_1\rangle + \cos((2m+1)\theta_a)|\psi_0\rangle \tag{2.4}$$

where $\sin(\theta_a) = \sqrt{p}$, with p the initial success probability of our state (in Grover's case it is $p = \frac{1}{2^k} = \frac{1}{N}$).
We can then boost the fraction of our initial state in the "good" subspace to 1 by applying our QAA operator Q an $m = \lfloor \frac{\pi}{4\theta_a} - \frac{1}{2} \rfloor$ times.

It is pretty straightforward at this point to view Grover Algorithm as a specific instance of the QAA protocol. In fact, we simply have to choose as the unitary operator $\mathscr{A} = H$, and we will obtain exactly Grover's results in the success probability after a t_f number of steps.

2.2 Random Walk

A random walk is a stochastic process of fundamental importance to analyse many different types of physical phenomena. In the following paragraph we will review some of its important aspects, which will then be naturally expanded to the quantum case.

A random walk process can be viewed as a Markov Chain (MC) on a graph $G(V,E)$ (where V is the set of nodes, with $|V| = n$, and E is the set of edges, with $|E| = m$). A discrete-time MC can be described as the repeated application of a stochastic $N \times N$ matrix P (i.e. $\sum_{j=1}^{N} P_{jk} = 1, \forall j, \forall k \; 0 \leq P_{jk} \leq 1$) on an initial probability distribution state. The P_{jk} element represents the transition probability from vertex j to vertex k. We are assuming for simplicity that the graph is finite.
A simple example is the random walk on a line, where a fair coin is tossed at each step to decide if the particle (or, "walker") will jump left or right its current position (we forbid the possibility of the walker remaining on the same spot). The matrix P that describes this process, in the case of a 4 dot line where the first and last dot are connected, is the following:

$$P = \begin{pmatrix} 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ \frac{1}{2} & 0 & \frac{1}{2} & 0 \end{pmatrix} \tag{2.5}$$

A common case is when $P_{u,v} = \frac{1}{d(u)}, \forall u, v \in V$, where $d(u)$ is the degree of u, i.e. the number of nodes linked to it. In other words, the latter model describes the situation where the transition probability from node u to all its neighbours is the same and it is uniform in the number of linked nodes. Given a probability distribution D_0 on the graph's nodes, which can be thought of as a uniform probability distribution over all the nodes of the graph, at time t we'll have the following:

$$D_t = P^t D_0 \tag{2.6}$$

We can then define a **stationary distribution** as:

$$\pi = D^t \pi, \forall t \tag{2.7}$$

If G is connected (i.e. it's always possible to find a path from a node to another), non-directed (i.e. every edge can be crossed in both directions), and finite, it can be shown that this type of distribution exist and is unique:[15]

$$\forall v \in V, \pi_v = d(v)/2m \tag{2.8}$$

The convergence rate to this distribution π can be evaluated in many different ways, for example:

- **Mixing time**[1]:

$$M_\epsilon := min\{T|\forall t \geq T, D_0 : ||D_t - \pi|| \leq \epsilon\} \tag{2.9}$$

- **Filling time**: the first time T such that the probability distribution on a subset of vertexes is more probable than the stationary distribution, minus ϵ

$$\tau_\epsilon := min\{T|\forall t \geq T, D_0, X \subseteq V : D_t(X) \geq (1-\epsilon)\pi(X)\}, D_t(X) = \sum_{x\in X} D_t(x) \tag{2.10}$$

- **Dispersion time**: the first time T such that the probability distribution on a subset of vertexes is less probable than the stationary distribution, plus ϵ: we are drifting away from the subset.

$$\xi_\epsilon := T|\forall t \geq T, D_0, X \subseteq V, D_t(X) \leq (1+\epsilon)\pi(X)\} \tag{2.11}$$

An instructive example is the random walk on a n-cycle graph, where it can be shown[14] that the random walk converges in $M_\epsilon = \theta(n^2 \log(1/\epsilon))$.

[1] The notion of distance that is usually used is the total variation distance between two distributions, defined as $||d_1 - d_2|| = \sum_i |d_1(i) - d_2(i)|$

2.3 Quantum Walk

First quantization approach

The generalization of the random walk to the quantum case is described in the present section.

We define a Cayley graph[17] $\Gamma(V,E)$ as the graph that encodes the structure of a group G, where each element of the group G is a node in the graph. Nodes can be reached from the identity node e by applying repeatedly the generators $h_i \in S, i = 1, ..., n$ on it. More formally, given a group G finitely generated, the sets of generators $S_0 := \{h_1, ..., h_n\}$ and $S_0^{-1} := \{h_1^{-1}, ..., h_n^{-1}\}$, and the free group F_n with $n = |S_0|$ (generated by $X = X_0 \cup X_0^{-1}$, with $X_0 = \{f_1, ..., f_n\}$), we can build the homomorphism $\phi : F_n \to G$, such that $\phi(F_n) \simeq G$.
It can be shown that every group G is isomorphic to the quotient set of a free group. In our case, $G \simeq F_n/Ker(\phi)$, where $Ker(\phi) := \{f \in F|\phi(f) = e_G\}$.

We can then introduce the idea of presentation of a group G as $G = \langle S_0|R\rangle$, where S_0 is the set of generators that can generate, through a finite combination, every element of G. On the other hand, R is defined as the relator set, the set of strings that belongs to $Ker(\phi)$. They represent closed loops, that link a node to itself.
Through the presentation of a group we can compactly characterize it, and graphically it can be viewed as a Cayley graph.

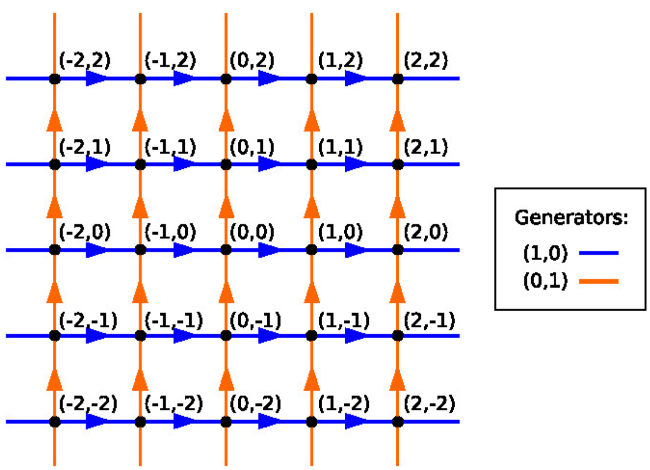


Figure 2.1: Cayley graph for $Z_2 = \langle a, b|aba^{-1}b^{-1}\rangle$, with a = (0,1), b=(1,0)

We can at this point define the Hilbert space $\mathscr{H}_V$ spanned by the $|v\rangle$ states, where $v \in V$. A Cayley graph is always regular, so each vertex of Γ is linked exactly to d others. Another space is also introduced, the "coin" space $\mathscr{H}_A$, of dimension

d. The unitary transformation applied in $\mathscr{H}_A$ on the initial state of the coin will be called **C**, and for every node the possible directions will be identified with the set of d-generators on Γ. A very common type of coin is the so-called Hadamard coin:

$$\mathbf{C} = \frac{1}{\sqrt{2}}(|0\rangle_c \langle 0| + |0\rangle_c \langle 1| + |1\rangle_c \langle 0| - |1\rangle_c \langle 1|) \tag{2.12}$$

We finally introduce the Quantum Walk operator as:

$$U = S(C \otimes \mathbb{I}) \tag{2.13}$$

where **S** is a shift operator, that is applied on $\mathscr{H}_A \otimes \mathscr{H}_C$ as $S|a,v\rangle = |a,u\rangle$, where u is the a-th neighbour of v. Remembering the Hadamard coin, a possible choice for the shift operator is:

$$\hat{S} = |0\rangle_c \langle 0| \otimes \sum_i |i+1\rangle_p \langle i| + |1\rangle_c \langle 1| \otimes \sum_i |i-1\rangle_p \langle i| \tag{2.14}$$

S, just like C, is unitary, being an operator that works by applying a permutation on the edge's labels. Hence, U is unitary too.
In general, unlike the classical case, if we start from an initial state on the graph $|\alpha_0\rangle$, the limit $\lim_{t\to\infty} U^t |\alpha_0\rangle$, where U is the unitary transformation acting on the graph as it is defined in Eq. (2.13).
To prove this point we will use an elegant result from number theory known as "Dirichlet's approximation theorem"[12], which states that:

> Given a string of number $(\alpha_1, ..., \alpha_n) \in \mathbb{R}$, $\forall N \in \mathbb{N}$, $\exists t \in \mathbb{Z}, (p_1, ..., p_n) \in \mathbb{N}$, with $1 \le t \le N$, s.t. $|t\alpha_j - p_j| < \frac{1}{N^{1/n}}$

In our case, we need to prove that:

$$\exists t : |e^{it\theta_j} - 1| < \epsilon, \forall \theta_j \tag{2.15}$$

In order to show it, we will use the following substitution:

$$\alpha_j := \frac{\theta_j}{2\pi} \tag{2.16}$$

with α_j a real number. In doing so, we are switching from the problem "what t we need to choose in order to have $t\theta_j$ as close as possible to 2π" (to obtain $e^{it\theta_j} = 1$), to the simpler problem "what t we need to choose in order to have $t\alpha_j$ close to an integer". This latter will be what in Dirichlet's theorem is called p_j. We can then choose t and p_j s.t. the previous theorem is satisfied, and choose our α_j.
We observe that:

$$e^{it\theta_j} = e^{i2t\pi\alpha_j} = e^{i2\pi p_j} e^{i2\pi(t\alpha_j - p_j)} \tag{2.17}$$

Hence:

$$
\begin{aligned}
|e^{i\theta_j t} - 1| = |e^{i2\pi(t\alpha_j - p_j)} - 1| = 2\left|\frac{sin(2\pi(t\alpha_j - p_j))}{2}\right| < \\
< 2\left|\frac{2\pi(t\alpha_j - p_j)}{2}\right| = 2\pi|(t\alpha_j - p_j)| < \frac{2\pi}{N^{\frac{1}{d}}}
\end{aligned}
\tag{2.18}
$$

d is the number of eigenvalues θ_j.
We can then choose an arbitrary N s.t. $N > (\frac{2\pi}{\epsilon})^d$, in order to have $\frac{2\pi}{N^{\frac{1}{d}}} < \epsilon$, proving our initial statement: there exist a time t s.t. $e^{it\theta_j}, \forall j$ are arbitrarily close to 1.

P_t is defined in terms of the application of the unitary matrix U^t on an initial distribution, but this matrix has eigenvalues $e^{it\theta}$. These eigenvalues represent unit vectors in the complex plane, rotating with different speeds based on the values of θ, but for an infinitely many values of t these vectors are all aligned near the real value 1, making the matrix U^t close to the identity on the state $|\alpha_0\rangle$. Hence, if the distribution P_0 associated to the state $|\alpha_0\rangle$, and the distribution P_1 associated to the state $|\alpha_1\rangle = U|\alpha_0\rangle$ are different, this difference will be preserved in the evolution after arbitrarily many steps.[2]

Given we can not study such a limit distribution, we will introduce an average distribution:

$$
\bar{P}_T(v|\alpha_0) := \frac{1}{T}\sum_{t=0}^{T-1} P_t(v|\alpha_0), \quad P_t(v|\alpha_0) = \sum_{a\in A} |\langle a, v|\alpha_t\rangle|^2 \tag{2.19}
$$

This distribution $\bar{P}_T$, unlike P_t, has a limit[2]. We define $\left|\phi_j\right\rangle$ and λ_j the eigenvectors and corresponding eigenvalues of U. It can be proven that:

$$
\lim_{T\to\infty} \bar{P_T}(v|\alpha_0) = \sum_{i,j,a} a_i a_j^* \langle a, v|\phi_i\rangle\langle\phi_j|a, v\rangle \tag{2.20}
$$

where the sum is done only on pairs i, j s.t. $\lambda_i = \lambda_j$.
If U is a QW operator on a Cayley graph of an Abelian group, then the limit distribution π defined in Eq. (2.20) is uniform on the graph's nodes and it is independent of the initial state.
Defining an initial state as $|a, v\rangle$, where a is the initial state of the "coin" and v is the starting node, we can now introduce the quantum version of the mixing time M_ϵ.

$$
M_\epsilon = \min\{T|\forall t \geq T, |a, v\rangle : ||\pi(\cdot|a, v) - \bar{P}_t(\cdot|a, v)|| \leq \epsilon\} \tag{2.21}
$$

where $P(\cdot|a, v)$ indicates the probability distribution conditioned by the initial state $|a, v\rangle$. M_ϵ measures the number of time steps required for the average distribution to be ϵ-close to the limiting distribution (which, in general, could depend from the initial state).
It is interesting to observe that in the classical case on the n-cycle graph (with odd

n) the $M_\epsilon^{(c)} = \theta(n^2 \log(1/\epsilon))$, while in the quantum case with the Hadamard coin it can be shown that $M_\epsilon^{(q)} \leq O(n \log(n)/\epsilon^3)$, showing a notable speed-up.

2.3.1 Hitting times in search algorithms: Classic vs Quantum search

We will now describe a general result in quantum search based algorithms, and how they outperform classic ones. We will follow the proof wrote by A.Childs in his lectures[8]:

Suppose we have a graph $G = (V, E)$ with a subset of marked vertices $M \subset V$. Classically, a natural way of creating a search algorithm is to design the stochastic matrix P' in such way that it stops if we encounter a marked vertex. In other words, P' is a matrix defined as the follows:

$$P'_{jk} = \begin{cases} 1 & k \in M \text{ and } j = k \\ 0 & k \in M \text{ and } j \neq k \\ P_{jk} & k \notin M \end{cases} \tag{2.22}$$

A needed assumption is that matrix P is symmetric ($P_{jk} = P_{kj}, \forall j, k$), even though matrix P' is not, due to the presence of the marked subset. We can now re-order the marked entries of our matrix through a number of permutation in order to obtain the following expression for P':

$$P' = \begin{pmatrix} P_M & 0 \\ Q & I \end{pmatrix} \tag{2.23}$$

where matrix P_M is obtained by deleting the rows and columns of P corresponding to vertices in M. Q represents the matrix that describe the transitions between "un-marked" vertexes and "marked" vertexes, but it will not be useful for our analysis. We now take t iterations of our matrix P'. It can be easily proven that:

$$(P')^t = \begin{pmatrix} P_M^t & 0 \\ Q(I + P_M + ... + P_M^{t-1}) & I \end{pmatrix} = \begin{pmatrix} P_M^t & 0 \\ Q\frac{P_M^t - I}{P_M - I} & I \end{pmatrix} \tag{2.24}$$

Starting from the uniform distribution over all the "un-marked" nodes of the graph the probability of *not* reaching a marked node of the graph is[2]:

$$\frac{1}{N - |M|} \sum_{j,k \notin M} [P_M^t]_{jk} \leq ||P_M^t|| = ||P_M||^t \tag{2.26}$$

there is an inequality because the left term is the expected value of P' on the normalized state of only the "un-marked" part of the graph. Given that $||P_M|| = 1 - \Delta$, the probability of reaching a marked item after t steps is at least $1 - ||P_M||^t = 1 - (1 - \Delta)^t$. If $t = O(\frac{1}{\Delta}) = O(\frac{1}{1 - ||P_M||})$, the subtracting term is negligible and the lower bound for

[2]We are going to use the following property:

$$\frac{1}{N - |M|} \sum_{j,k \notin M} [P_M^t]_{j,k} = \left| \langle v | P_M^t | v \rangle \right| \leq ||P_M^t||_\infty = \sup_{||\psi|| = 1} ||P_M^t \psi||, \quad |v\rangle = \frac{1}{\sqrt{N - |M|}} \sum_{j \notin M} |j\rangle \tag{2.25}$$

the success probability is $\Omega(1)$. To calculate the upper bound we refer the following lemma proved by A.Child[8]:

> If the second largest eigenvalue of P (in absolute value) is at most 1-δ and $|M| \leq \epsilon N$, then $||P_M|| \leq 1 - \delta\epsilon/2$

Under this lemma, it is immediate to see that the classical hitting time is $t = O(\frac{1}{\delta\epsilon})$

We now want to calculate the quantum hitting time. Given an initial state $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{j \notin M} \left|\psi_j\right\rangle$ and $N \times N$ stochastic matrix P, we define matrix D:

$$D = \begin{pmatrix} P_M & 0 \\ 0 & I \end{pmatrix} \tag{2.27}$$

where $D_{jk} = \sqrt{P_{j,k} P_{k,j}}$, and P_M is the matrix obtained by deleting the rows and columns of P corresponding to vertices in M.
If the marked set is non-empty, the initial state $|\psi\rangle$ belongs entirely to the subspace span$\{\left|\psi_j\right\rangle\}$, since it is explicitly a linear combination of the states $\left|\psi_j\right\rangle$ with $j \notin M$. It can be proven[8] that the quantum walk operator U corresponding to P has eigenvalues ± 1 only in the orthogonal complement of span$\{\left|\psi_j\right\rangle\}$, so $|\psi\rangle$ has no overlap with those eigenspaces. Inside span$\{\left|\psi_j\right\rangle\}$, the spectrum of U is made up of eigenvalues $e^{\pm i \arccos\lambda}$, where $\lambda \in \mathrm{spec}(P_M)$. Moreover, since $|\psi\rangle$ has support only on unmarked vertices, it lies entirely in the sector associated with P_M.
Therefore, when $M \neq \varnothing$, the state $|\psi\rangle$ is a superposition only of eigenvectors with eigenvalues $e^{\pm i \arccos\lambda}$. Since $||P_M|| < 1$, no λ can be equal to 1, so all corresponding phases are strictly different from 0. This is why phase estimation on U can distinguish the case $M = \varnothing$ from the case $M \neq \varnothing$. If a phase-estimation is performed on U with precision $O(\min_\lambda \arccos\lambda)$, we will see a phase different from 0. Being $\lambda \geq \sqrt{1-\lambda}$, precision $O(\sqrt{1-||P_M||})$ is enough. Therefore, the quantum algorithm spot a marked vertex in time $O(\frac{1}{\sqrt{1-||P_M||}}) = O(\frac{1}{\sqrt{\delta\epsilon}})$, showing a quadratic speedup over the classical case.

This speed-up is one of the main reasons that motivated the first applications of quantum walks to search algorithms[19][9].

2.4 Searching with a quantum walk

As we have already remarked several times, it is well known that Grover's algorithm can speed up the search of a marked input given an unsorted database of size N from the classical $O(N)$ queries to $O(\sqrt{N})$. What Aaronson and Ambainis ask in their seminal paper[1] is if the algorithm can go one step further, and speed up the search on a physical region, where the topological properties of a graph are taken into account as a limiting factor to the diffusion speed of a wavefunction on the graph itself.

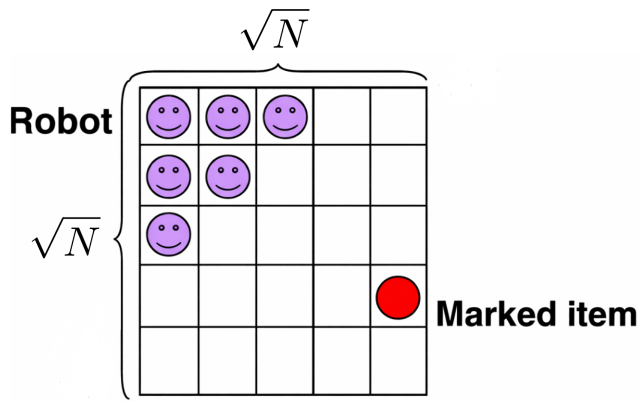


Figure 2.2: A quantum robot, in a superposition over m locations, searching for a marked item on a 2D grid of size $\sqrt{N} \times \sqrt{N}$

The reason why they wanted to explore this possibility is to give more physical robustness to the search problem, making information encoded in physically bounded region and not instantaneously accessible.

This problem had already been discussed by P.Benioff[16], who concluded that a quantum search operator built like the one designed by Grover, even if it could find a marked element $|m\rangle$ in $O(\sqrt{N})$ queries, it would have still required at each step between queries the application of a rotation on a superposition of all the lattice-sites. This requirement adds a layer of complexity to the operator, that needs to move $\sqrt{N}$ sites in each direction to perform the rotation. Therefore, the total complexity of the algorithm would become $O(N)$, resulting no better than a classical brute force search algorithm.
However, it was proven[1] by Aaronson and Ambainis that this problem could be overrun with a particular routine of the quantum robot.
To take into account this physical constraints, they had to require specific properties to their evolution operator U on the graph. In particular:

- **Z-locality**: Given any pair of non-neighboring vertices v_1, v_2 in G, U "sends no amplitude" from v_1 to v_2; that is, the corresponding entries in U are all 0.

More formally: "U is *Z-local* if $U_{(i,z)\to(i^*,z^*)} = 0$ whenever $i \neq i^*$ and (v_i, v_{i^*}) is not an edge in E"

- **C-Locality**: U must be written as product of unitaries that each sends amplitude through edges that connects neighboring vertices. More formally: "U is *C-local* if the basis states can be partitioned into subsets $P_1, ..., P_q$ s.t.:
  (i) $U_{(i,z)\to(i^*,z^*)} = 0$ whenever $|v_i, z\rangle$ and $|v_{i^*}, z^*\rangle$ belong to distinct P_j's
  (ii) For each j, all basis states in P_j are either from the same vertex or from two adjacent vertices."

- **H-locality**: U is *H-local* (for Hamiltonian) if it can be obtained by applying a locally-acting, low-energy Hamiltonian for some fixed amount of time. More formally: "U is *H-local* if $U = e^{iH}$ for some Hermitian H with eigenvalues of absolute value at most π, such that $H_{(i,z)\to(i^*,z^*)} = 0$ whenever $i \neq i^*$ and (v_i, v_{i^*}) is not an edge in E"

It is immediate that if a matrix U is *C-local*, it is also *Z-local* and *H-local*. Any unitary U can be written as e^{iH} for some H with eigenvalues of absolute value at most π. So, we can write the unitary U_j acting on each P_j as e^{iH_j} ; then since the U_j 's commute:

$$\prod U_j = e^{i\sum H_j} \tag{2.28}$$

They demonstrate that by modeling a quantum search operator like the one we discussed above, the speed up is provable[1] compared to the classical case, and they found that their quantum search operator can search for a single marked spot on a d-dimensional hypercube with N nodes in at most $O(\sqrt{N})$ for $d \geq 3$, and $O(\sqrt{N}\log^2(N))$ in $d = 2$. Moreover, they found that the probability of their quantum search operator to find the single marked spot (without any amplification algorithm) was:

$$P(n) \geq \Omega(N^{-1/11}) \tag{2.29}$$

The general structure of the algorithm goes as the following:

- Define a connected, undirected graph $G = (V, E)$, with $|V| = N$ nodes, and $X = x_1, ..., x_N \in \{0,1\}^N$ as an input to a boolean function $f : \{0,1\}^N \to \{0,1\}$

- Make each bit of the input string X be assigned to a different node, such that the Quantum walk operator can read the output x_i only when touching the i-th node

- Build a Quantum search operator as a sequence of repeated application of a unitary matrix U and an "oracle" matrix O: U works as a permutation matrix by distributing the probability distribution over the neighbor states of the current state with equal probability; O works by mapping the state of the walker $O|v_i, z\rangle = |v_i, z \oplus x_i\rangle$, where the z represent the internal state of the walker, encoding some bit string values. The direct sum is done on the first bit of the string z.

- Finally, the success probability of the algorithm in evaluating f(X) is larger than $1-\epsilon$ if:
$$\sum_{|v_i,z\rangle : z_{OUT}=f(x)} |\alpha_{i,z}^{(T)}(X)|^2 \geq 1-\epsilon \tag{2.30}$$

This results was later on improved by A.Ambainis, J.Kempe and A. Rivosh in their seminal paper "Coins makes Quantum Walk Faster", showing an improvement in the total time complexity to find a single marked item thanks to the usage of an auxiliary coin state, from $O(\sqrt{N}\log^2(N))$ to $O(\sqrt{N}\log(N))$. This result was obtained on a 2D lattice with periodic bounduary conditions (a lattice "torus shaped"): if the walker moves $\sqrt{N}$ steps toward the x-direction, it returns to original position. This bound was later on improved by A.Tulsi[20], using an additional ancilla qubit, to $O(\sqrt{N\log N})$.
Firstly they defined a quantum walk operator specifically for this graph, where as a Shift operator S they employed a "flip-flop" shift, built in a way such that:

$$\begin{aligned} S_{ff}: \quad & |\rightarrow\rangle \otimes |x,y\rangle \longrightarrow |\leftarrow\rangle \otimes |x+1,y\rangle \\ & |\leftarrow\rangle \otimes |x,y\rangle \longrightarrow |\rightarrow\rangle \otimes |x-1,y\rangle \\ & |\uparrow\rangle \otimes |x,y\rangle \longrightarrow |\downarrow\rangle \otimes |x,y+1\rangle \\ & |\downarrow\rangle \otimes |x,y\rangle \longrightarrow |\uparrow\rangle \otimes |x,y-1\rangle \end{aligned} \qquad \begin{aligned} S_{m}: \quad & |\rightarrow\rangle \otimes |x,y\rangle \longrightarrow |\rightarrow\rangle \otimes |x+1,y\rangle \\ & |\leftarrow\rangle \otimes |x,y\rangle \longrightarrow |\leftarrow\rangle \otimes |x-1,y\rangle \\ & |\uparrow\rangle \otimes |x,y\rangle \longrightarrow |\uparrow\rangle \otimes |x,y+1\rangle \\ & |\downarrow\rangle \otimes |x,y\rangle \longrightarrow |\downarrow\rangle \otimes |x,y-1\rangle \end{aligned}$$

Figure 2.3: A "flip-flop" vs "moving" shift: while in the moving shift the coin state is unaffected by the evolution operator, in the flip-flop case it is “flipped” at each iteration.

As a coin operator they employed a "Grover coin": $C = 2|D\rangle\langle D| - I$, where $|D\rangle$ is the uniform superposition of all the coin states (the four possible directions of movement on the 2D graph):

$$|D\rangle = \frac{1}{\sqrt{d}}\sum_{i=0}^{3}|i\rangle\langle i|, d=4 \tag{2.31}$$

This operator $U_{QW} = S(C\otimes I)$ is then paired with a reflection operator around the target state, the "oracle" $R = 1-2|D,v_0\rangle\langle D,v_0|$. The state $|D,v_0\rangle$ exist in the Hilbert space which is a tensor product between the coin space $\mathscr{H}_C$ of dimension $d=4$ and the node space $\mathscr{H}_V$ of dimension $d=N$, for a total dimension of $\mathscr{H}_T = \mathscr{H}_C \otimes \mathscr{H}_V, d=4N$. We take $N=2^k$, where k is the number of qubits used in the system.

Given an initial state $|\psi_0\rangle$ the quantum search operator $U' = UR$ goes through the following steps:

- Apply the operator $R = 1-2|D,v_0\rangle\langle D,v_0|$ to the initial state:

$$R|\psi\rangle|v\rangle = \begin{cases} -|D\rangle|v_0\rangle & \text{if } \psi = D \text{ and } v = v_0 \\ |\psi\rangle|v\rangle & \text{if } \psi \perp D \text{ or } v \perp v_0 \end{cases} \tag{2.32}$$

- apply $U = S(C \otimes I)$ to the output state to diffuse the wavefunction on the graph following its topological structure.
- Repeat T times the process
- Measure the position register and check if it is the target state

Although the "moving" shift S_m could seem a much more natural choice for our quantum walk operator (the coin state remain the same after the movement, and will only change with the next toss), it can be proven that it actually performs much worse than the "flip-flop" shift S_{ff}, taking at least $\Omega(N)$ steps to find a marked state, just like a brute-force classic algorithm (as it can be seen also numerically).
To explain this phenomenon, we will refer to the original article by A.Ambainis, J.Kempe and A.Rivosh[3].

The main idea is that by using the S_m, it can be proven that the initial uniform state $|D,D\rangle = |\phi_0\rangle$ has a large overlap at the start with the eigenvector $\left|\phi^\perp\right\rangle$ of U and $U' = U \cdot R$, with eigenvalue 1, and this overlap approaches 1 in the asymptotic regime.
This implies that, after any number of iterations of our quantum search operator U', the state will barely change at all from $\left|\phi^\perp\right\rangle$. Moreover, it can also be proven that $\left|\phi^\perp\right\rangle$ (which is obviously entirely contained in $\mathscr{H}_1$) is orthogonal to the projection of the marked state $|D, v_0\rangle$ on $\mathscr{H}_1$, making it orthogonal to $|D, v_0\rangle$ itself. Therefore, this implies that our state $|\phi_0\rangle$ has a large component orthogonal to the target state. Specifically:

$$|\left\langle\phi_0\middle|\phi^\perp\right\rangle|^2 = 1 - \frac{|\alpha_{00}|^2}{\sum_{i,j=1}^{\sqrt{N}} |\alpha_{ij}|} = 1 - \Omega(\frac{1}{N}) \tag{2.33}$$

where α_{ij} are the coefficients of the projection of the solution state $|D, v_0\rangle$ on eigenspace $\mathscr{H}_1$.
Therefore:

$$\begin{aligned} |\phi_0\rangle &= \beta_{00}\,|D, v_0\rangle + \sqrt{1-|\beta_{00}|^2}\left|\phi^\perp\right\rangle, |\beta_{00}|^2 \simeq 0 \\ \beta_{00} &= \frac{\alpha_{00}}{\sqrt{\sum_{i,j=1}^{\sqrt{N}} \alpha_{ij}}} \end{aligned} \tag{2.34}$$

This implies that after any number of iterations of U', almost all of our initial state will remain aligned with a vector orthogonal to the target state, making the success probability $p_D = ||\prod_{|D,v_0\rangle}(U')^{t_f}\,|\phi_0\rangle\,|| \simeq 0$.

2.4.1 Coined quantum walk on a 2D grid

In order to study how an initial state $|\psi_0\rangle$ evolves under the action of U', we will use the derivation originally written by A.Ambainis, J.Kempe and A.Rivosh[3] and later on elaborated by R. Portugual in his book "Quantum walks and search algorithms"[18]. We will follow the latter.

It is not necessary to study the whole spectral decomposition of U' as we will see, because it can be obtained from the eigenvectors and eigenvalues of the quantum walk operator U. The complete spectrum and decomposition of the latter on a 2D lattice is completely known.
This approach is, of course, an approximation only usable in the asymptotic regime for $N \to \infty$, and analytical results for finite values N will not be presented due to the difficulties introduced by the whole spectrum of U' (which can be proven to scale with the dimension of the lattice). This is due to the fact that in the asymptotic regime, it can be proven that the action of U' is limited to a 2D subspace spanned by two of its eigenvectors $|\alpha_\pm\rangle$ with eigenvalues $e^{\pm i\alpha}, \alpha = \min\{\theta_1, ..., \theta_j\}$, with $0 \leq \theta_i \leq \pi$.
These eigenvalues are the ones associated with a "slow-changing regime", while all the others are in the "fast changing regime", and eventually completely negligible in the asymptotic limit.
These two eigenvectors can be used to build the effective 2D plane where U' acts as a rotation:

$$|\beta_\pm\rangle = \frac{|\alpha_+\rangle \pm |\alpha_-\rangle}{\sqrt{2}} \tag{2.35}$$

The first step of our algorithm is initializing the Grover state $|\phi_0\rangle = |D, D\rangle$, which is the uniform superposition of all the coin and vertex states. At this point, there are two conditions that must hold in order to have an efficient algorithm:

- The initial overlap must be: $|\langle\phi_0|\beta_-\rangle|^2 \simeq 1$
- The final overlap must be: $|\langle D, v_0|\beta_+\rangle|^2 \simeq 1$

If these two conditions are true, the algorithm is perfectly efficient. However, the first conditions will only be true for our uniform initial state in the asymptotic regime (for reasons we have already partially explained above), while the second will be generally false. Therefore, in the end a QAA routine will be necessary to boost the overlap between the target state and $|\beta_+\rangle$.

Generally, the uniform state on the graph is an eigenvector with eigenvalue $+1$ of the quantum walk operator U_{QW}, i.e. $U^n |D, D\rangle = |D, D\rangle, \forall n$.
It can be proven that:

$$|\langle\phi_0|\beta_-\rangle| \simeq 1 - \alpha^4\Big(\frac{1}{4a_0^2}\sum_j \frac{a_j^2}{(1 - cos(\theta_j))^2} + \frac{1}{32a_0^2}\sum_k a_k^2\Big) \tag{2.36}$$

The coefficients in the sum a_0, a_j, a_k are all related to the spectral decomposition of U', but are not relevant, because the term α can be proven[18] to scale as

$\alpha = O(\frac{1}{\sqrt{N \log N}})$, justifying the fact that in the asymptotic regime for $N \to \infty$ it goes to 0, and the overlap becomes 1.
On the other hand, the overlap between the target state and $|\beta_+\rangle$ is a bit more tricky. In order to understand why, let's start by discussing the behaviour of $|\phi_0\rangle \simeq |\beta_-\rangle$ under the action of U'.

It follows that:

$$(U')^{t_f} |\phi_0\rangle \simeq (U')^{t_f} |\beta_-\rangle = (U')^{t_f} \frac{(|\alpha_+\rangle - |\alpha_-\rangle)}{\sqrt{2}} = \frac{(e^{i\alpha t_f} |\alpha_+\rangle - e^{-i\alpha t_f} |\alpha_-\rangle)}{\sqrt{2}} \tag{2.37}$$

If $t_f = \frac{\pi}{2\alpha}$, we obtain:

$$(U')^{t_f} |\beta_-\rangle = i \frac{(|\alpha_+\rangle + |\alpha_-\rangle)}{\sqrt{2}} = i |\beta_+\rangle \tag{2.38}$$

In other words, in the asymptotic regime with the correct amount of iteration of operator U', we are able to rotate $|\beta_-\rangle$ into $|\beta_+\rangle$.
It is now clear why it is important that the second condition is met: if the overlap between the target state and $|\beta_+\rangle$ is 1, we are certain that after t_f steps our algorithm give us as output the target state.
Unfortunately, the second condition is much less favorable than the first one, and it can be proven that:

$$|\langle D, v_0|\beta_+\rangle|^2 = O\Big(\frac{1}{\log(N)}\Big) \tag{2.39}$$

This results justifies the usage of a QAA routine after the Quantum search operator, in order to compensate this very unfavorable overlap. The total time complexity of such algorithm is the original time complexity t_f of the QS operator $O(\sqrt{N \log(N)})$, multiplied by the time complexity of the QAA routine. This latter, to make the overlap between $|\beta_+\rangle$ and the target state $O(1)$, needs a number of iterations[7] equal to $m = \lfloor \frac{\pi}{4\sqrt{p}} \rfloor$, where p is the original probability of the algorithm before the QAA routine. In our case $p = O(\frac{1}{\log(N)})$, bringing the whole time complexity to:

$$\boxed{O(\sqrt{N} \log(N))} \tag{2.40}$$

This results is better that the classic brute-force counterpart, which would require at most $O(N)$ iterations, but less favorable than the combinatorial Grover search, which has a time complexity equal to $O(\sqrt{N})$. Physically, this result is a consequence of the constraints emerging from the geometrical structure of the graph, where we cannot access (unlike the combinatorial Grover search) all the possible nodes from every other, and we have a limited propagation velocity on the graph itself.

Moreover, we can also show how the combinatorial version of Grover algorithm can be viewed in the framework of abstract search algorithm on graphs, specifically on a complete graph.
In a complete graph, all vertices are connected by undirected edges and each vertex

has a directed loop (an edge that connects to the same vertex at both ends)[22]. Then, each vertex has incident N edges with labels 1 to N. In this case, a natural choice for the basis states is the following: span$\{|a,v\rangle, 1 \leq a \leq N, 1 \leq v \leq N\}$, where $|a\rangle$ is the coin state and $|v\rangle$ is the position state. The shift operator, in order to generate the interference effect that amplifies the success probability on the marked vertex, acts as the following:

$$S|a,v\rangle = |v,a\rangle \tag{2.41}$$

It is interesting to note that the shift operator acts as a swap between the two register. Indeed, if the coin state was preserved, the final state would result "static": $S|a,v\rangle = |a,a\rangle$. The S shift action can be read as "from vertex v move to vertex a through the corresponding edge", but if we avoid the swap action, the final state would read "form vertex a move to vertex a through the corresponding edge", resulting in a contradictory effect.
The specific coin to use would be:

$$C'_G = -G \otimes |v_0\rangle\langle v_0| + G \otimes (I - |v_0\rangle\langle v_0|) \tag{2.42}$$

where on the marked node $|v_0\rangle$ the operator $-G$ is applied. The total evolution operator is given by:

$$U' = SC'_G = S(G \otimes R) \tag{2.43}$$

where $R = I - 2|v_0\rangle\langle v_0|$, the classic reflection around the hyperplane orthogonal to $|v_0\rangle$.
In Grover algorithm, the operator GR is used a $t_f = \lfloor \frac{\pi\sqrt{N}}{4} \rfloor$ number of times. In an abstract search algorithm on a graph, we know that U' must be applied a $t_f^{'} = \lfloor \frac{\pi\sqrt{N}}{2} \rfloor$ times to obtain the correct success probability. Therefore, given an initial state $|\phi_0\rangle = |D_c, D_v\rangle$ (the uniform superposition of both coin and vertex states), we obtain the following results:

$$\begin{aligned}
U'|\phi_0\rangle &= S(G|D\rangle \otimes R|D\rangle) \\
&= S((|D\rangle \otimes R|D\rangle) \\
&= R|D\rangle \otimes |D\rangle \\
(U')^2 &= S(G \otimes R)(R|D\rangle \otimes |D\rangle) = \\
&= S(GR|D\rangle \otimes R|D\rangle) \\
&= R|D\rangle \otimes GR|D\rangle
\end{aligned} \tag{2.44}$$

where the two registers are swapped under the action of S. If we now iterate this process $t_f^{'} = \lfloor \frac{\pi\sqrt{N}}{2} \rfloor$ times, we will obtain:

$$(U')^{\lfloor \frac{\pi\sqrt{N}}{2} \rfloor}|\phi_0\rangle = R(GR)^{\lfloor \frac{\pi\sqrt{N}}{4} \rfloor - 1}|D\rangle \otimes (GR)^{\lfloor \frac{\pi\sqrt{N}}{4} \rfloor}|D\rangle \tag{2.45}$$

Measuring the vertex state would give us exactly Grover algorithm result, completing the proof of the equivalence of the two approach.

Chapter 3: Entangled-state analysis for quantum search

3.1 Anti-symmetric case

We introduce the projector P onto the solution subspace and its complement $Q = \mathbb{I} - P$, so that $P^2 = P$, $Q^2 = Q$, and $PQ = QP = 0$. The success probability corresponds to projecting onto the subspace in which at least one register is in the marked subspace. Therefore, for the maximally entangled antisymmetric state

$$|F\rangle = \frac{1}{\sqrt{2}}(|\phi\rangle|\psi\rangle - |\psi\rangle|\phi\rangle), \tag{3.1}$$

the success probability is

$$p^F_{\text{succ}} = \left\| \left[(P \otimes Q) + (Q \otimes P) + (P \otimes P) \right] |F\rangle \right\|^2 \tag{3.2}$$

Using $Q = \mathbb{I} - P$, the projector onto the success subspace can be rewritten as

$$(P \otimes Q) + (Q \otimes P) + (P \otimes P) = P \otimes \mathbb{I} + \mathbb{I} \otimes P - P \otimes P \tag{3.3}$$

Hence, the entangled success probability will be:

$$p^F_{\text{succ}} = \|(P \otimes \mathbb{I} + \mathbb{I} \otimes P - P \otimes P)|F\rangle\|^2 \tag{3.4}$$

Let us define

$$a = (P \otimes \mathbb{I})|F\rangle, \qquad b = (\mathbb{I} \otimes P)|F\rangle, \qquad c = (P \otimes P)|F\rangle \tag{3.5}$$

Therefore,

$$p^F_{\text{succ}} = \|a + b - c\|^2 = \|a\|^2 + \|b\|^2 + \|c\|^2 + 2\,\text{Re}\,\langle a|b\rangle - 2\,\text{Re}\,\langle a|c\rangle - 2\,\text{Re}\,\langle b|c\rangle \tag{3.6}$$

We now compute the various contributions. First,

$$a = \frac{1}{\sqrt{2}}\big(P|\phi\rangle|\psi\rangle - P|\psi\rangle|\phi\rangle\big), \tag{3.7}$$

By studying $||a||^2$ we find:

$$||a||^2 = \frac{1}{2}\left(\langle\phi|\,P\,|\phi\rangle\,\langle\psi|\psi\rangle + \langle\psi|\,P\,|\psi\rangle\,\langle\phi|\phi\rangle - \langle\phi|\,P\,|\psi\rangle\,\langle\psi|\phi\rangle - \langle\psi|\,P\,|\phi\rangle\,\langle\phi|\psi\rangle\right) \tag{3.8}$$

Assuming $|\phi\rangle$ and $|\psi\rangle$ are normalized and orthogonal, this becomes

$$||a||^2 = \frac{p+q}{2}, \tag{3.9}$$

where

$$p = \langle\psi|\,P\,|\psi\rangle\,, \qquad q = \langle\phi|\,P\,|\phi\rangle$$

By symmetry, we can easily deduce what is the value of $||b||^2$:

$$||b||^2 = \frac{p+q}{2} \tag{3.10}$$

Lastly, we study c,:

$$c = \frac{1}{\sqrt{2}}\big(P\,|\phi\rangle\,P\,|\psi\rangle - P\,|\psi\rangle\,P\,|\phi\rangle\big), \tag{3.11}$$

and therefore

$$||c||^2 = pq - |\,\langle\psi|\,P\,|\phi\rangle\,|^2 \tag{3.12}$$

For the interference terms, one finds

$$\langle a|b\rangle = pq - |\,\langle\psi|\,P\,|\phi\rangle\,|^2, \tag{3.13}$$

while

$$\langle a|c\rangle = \langle b|c\rangle = pq - |\,\langle\psi|\,P\,|\phi\rangle\,|^2 \tag{3.14}$$

Substituting into the norm expansion gives

$$\begin{aligned} p^F_{\text{succ}} &= \frac{p+q}{2} + \frac{p+q}{2} + \big(pq - |\,\langle\psi|\,P\,|\phi\rangle\,|^2\big) + 2\big(pq - |\,\langle\psi|\,P\,|\phi\rangle\,|^2\big) \\ &\quad - 2\big(pq - |\,\langle\psi|\,P\,|\phi\rangle\,|^2\big) - 2\big(pq - |\,\langle\psi|\,P\,|\phi\rangle\,|^2\big) \\ &= p + q - pq + |\,\langle\psi|\,P\,|\phi\rangle\,|^2 \end{aligned} \tag{3.15}$$

Thus the success probability for the antisymmetric maximally entangled state is

$$p^F_{\text{succ}} = p + q - pq + |\,\langle\psi|\,P\,|\phi\rangle\,|^2 \tag{3.16}$$

3.2 Symmetric Case

As in the anti-symmetric case, for the symmetric maximally entangled state

$$|B\rangle = \frac{1}{\sqrt{2}}(|\phi\rangle\,|\psi\rangle + |\psi\rangle\,|\phi\rangle), \tag{3.17}$$

we compute the success probability as

$$\begin{aligned} p^b_{\text{succ}} &= \left\| \Big[(P \otimes \mathbb{I}) + (\mathbb{I} \otimes P) - (P \otimes P)\Big] \Big[\frac{1}{\sqrt{2}} (|\phi\rangle |\psi\rangle + |\psi\rangle |\phi\rangle) \Big] \right\|^2 \\ &= \left\| \Big[(P \otimes \mathbb{I}) + (\mathbb{I} \otimes P) - (P \otimes P)\Big] |B\rangle \right\|^2 \end{aligned} \tag{3.18}$$

As before, the mixed terms combine straightforwardly, giving

$$\|(P \otimes \mathbb{I} + \mathbb{I} \otimes P)\, |B\rangle\|^2 = p + q + 2pq + 2|\langle\psi|\, P\, |\phi\rangle|^2, \tag{3.19}$$

while

$$\|(P \otimes P)\, |B\rangle\, \|^2 = pq + |\langle\psi|\, P\, |\phi\rangle|^2 \tag{3.20}$$

Moreover,

$$2\,\mathrm{Re}[\langle B|\, (P \otimes \mathbb{I} + \mathbb{I} \otimes P)(P \otimes P)\, |B\rangle] = 2\big(pq + |\langle\psi|\, P\, |\phi\rangle|^2\big) \tag{3.21}$$

Therefore,

$$p^b_{\text{succ}} = p + q - pq - |\langle\psi|\, P\, |\phi\rangle|^2 \tag{3.22}$$

As it can be easily seen, the anti-symmetric case is much more favorable than the symmetric one, thanks to the minus sign present in the projection operator combined with the minus sign in the antisymmetric case.

Furthermore, to have a more general analysis, we will also study a more generic initial state $|\psi\rangle$ for our calculations:

$$|\psi\rangle = \frac{1}{\sqrt{2(1 + \cos(\theta)|\langle\phi|\chi\rangle|^2)}} \big(|\phi\rangle\, |\chi\rangle + e^{i\theta}\, |\chi\rangle\, |\phi\rangle \big) \tag{3.23}$$

with $|\phi\rangle\,, |\chi\rangle$ not necessarily orthogonal. In this case the success probability is:

$$\begin{aligned} p^{\psi}_{succ} &= \frac{1}{1 + \cos(\theta)|\langle\phi|\chi\rangle|^2} \Big(\langle\phi|\, P\, |\phi\rangle + \langle\chi|\, P\, |\chi\rangle - \langle\phi|\, P\, |\phi\rangle \langle\chi|\, P\, |\chi\rangle \\ &- \cos(\theta)(\langle\chi|\phi\rangle \langle\phi|\, P\, |\chi\rangle + \langle\phi|\chi\rangle \langle\chi|\, P\, |\phi\rangle - \langle\phi|\, P\, |\chi\rangle \langle\chi|\, P\, |\phi\rangle)\Big) \end{aligned} \tag{3.24}$$

Chapter 4: Mathematical analysis

4.1 No-go theorem: orthogonal states

We will now show how maximally entangled states have fast-decaying interference term, proving a fundamental bound in every possible system that suffices our hypothesis.

Given an initial state where a tensor product of the same unitary operators is applied:

$$(\mathcal{O}^n \otimes \mathcal{O}^n)\{\frac{1}{\sqrt{2}}(A|0\rangle A|n\rangle - A|n\rangle A|0\rangle)\} = \frac{1}{\sqrt{2}}(|\psi_0\rangle |\psi_1\rangle - |\psi_1\rangle |\psi_0\rangle) \tag{4.1}$$

Where the term $A|0\rangle = |\psi\rangle$ is the state obtained starting from the state $|0\rangle$ with a generic quantum algorithm that creates superpositions of all states in the computational basis (e.g. Hadamard). $A|n\rangle$ does the same but starting from the n^{th} state of the computational base.

Our assumptions are therefore:

- A unitary quantum algorithm
- $\mathcal{O}$ oracle able to apply the amplitude amplification routine devised by Brassard and Høyer[7] both on the state $A|0\rangle$ and on the state $A|n\rangle$

Since the states $|0\rangle, |n\rangle$ are orthogonal, this orthogonality is preserved after the action of both A and $\mathcal{O}^n$, which are unitary. Therefore, it holds that $\langle\psi_0|\psi_1\rangle = 0$. Furthermore, we can assume without a loss of generality that after the action of the unitary operator $\mathcal{O}$, $||P|\psi_0\rangle|| \geq 1-\delta(N), ||P|\psi_1\rangle|| \geq 1-\delta(N)$, with $\delta(N) = \frac{1}{N}$ (the initial success probability in Grover's algorithm).

One can then show that:

$$\lim_{N\to\infty} |\langle\psi_0| P |\psi_1\rangle| = 0 \tag{4.2}$$

Indeed:

$$|\psi_0\rangle = \bar{\alpha}_0 |\phi_0\rangle + \bar{\beta}_0 \left|\phi_0^\perp\right\rangle, |\psi_1\rangle = \bar{\alpha}_1 |\phi_1\rangle + \bar{\beta}_1 \left|\phi_1^\perp\right\rangle \tag{4.3}$$

But we know that:

$$A|0\rangle = \alpha_0 |\phi_0\rangle + \beta_0 \left|\phi_0^\perp\right\rangle, A|n\rangle = \alpha_1 |\phi_1\rangle + \beta_1 \left|\phi_1^\perp\right\rangle \tag{4.4}$$

Where $|\bar{\alpha}_0|, |\bar{\alpha}_1| > |\alpha_0|, |\alpha_1|$ (after the iteration of n routines of $\mathcal{O}$).

If we now take the projector onto the success states P, such that:

$$P|\psi_0\rangle = \bar{\alpha}_0 |\phi_0\rangle, \quad P|\psi_1\rangle = \bar{\alpha}_1 |\phi_1\rangle \tag{4.5}$$

Therefore:

$$\langle\psi_0| P |\psi_1\rangle = \langle\psi_0| P \cdot P |\psi_1\rangle = \bar{\alpha}_0^* \bar{\alpha}_1 \langle\phi_0|\phi_1\rangle \tag{4.6}$$

Given now $|\alpha_0|^2 = |\alpha_1|^2 = \frac{1}{N}$, and knowing that[7]$|\bar{\alpha}_0|^2 = |\bar{\alpha}_1|^2 \geq 1 - \frac{1}{N}, |\bar{\beta}_0| = |\bar{\beta}_1| \leq \sqrt{1/N}$.

Using this information, we obtain:

$$\begin{aligned}
&\langle\psi_0|\psi_1\rangle = 0 = \langle\psi_0| P |\psi_1\rangle + \langle\psi_0| (I - P) |\psi_1\rangle \\
&\langle\psi_0| P |\psi_1\rangle = -\langle\psi_0| (I - P) |\psi_1\rangle \\
&|\langle\psi_0| P |\psi_1\rangle| = |\langle\psi_0| (I - P) |\psi_1\rangle|
\end{aligned} \tag{4.7}$$

It is immediate then that:

$$\begin{aligned}
&\bar{\alpha}_1 \bar{\alpha}_0^* \langle\phi_0|\phi_1\rangle = -\bar{\beta}_0^* \bar{\beta}_1 \langle\phi_0^\perp|\phi_1^\perp\rangle \\
&|\bar{\beta}_0^* \bar{\beta}_1 \langle\phi_0^\perp|\phi_1^\perp\rangle| = |\bar{\alpha}_1 \bar{\alpha}_0^* \langle\phi_0|\phi_1\rangle| \geq \left(1 - \tfrac{1}{N}\right) |\langle\phi_0|\phi_1\rangle| \\
&|\bar{\beta}_0^* \bar{\beta}_1 \langle\phi_0^\perp|\phi_1^\perp\rangle| \leq |\bar{\beta}_0^*||\bar{\beta}_1| \leq \tfrac{1}{N}
\end{aligned} \tag{4.8}$$

Therefore:

$$\frac{1}{N} \geq |\bar{\alpha}_1 \bar{\alpha}_0^* \langle\phi_0|\phi_1\rangle| = |\langle\psi_0|P|\psi_1\rangle| \geq (1 - \tfrac{1}{N}) |\langle\phi_0|\phi_1\rangle| \geq 0 \tag{4.9}$$

But for $N \to \infty$, we obtain:

$$0 \geq |\langle\psi_0|P|\psi_1\rangle| \geq 0 \tag{4.10}$$

Therefore, the interference term that should have improved p_{succ} tends to 0 for large N (the number of elements in the register).

Chapter 5: Numerical results

Given the code described in 6.3.4, we simulated both the entangled success probability of the two particles in the combinatorial case after a QAA routine and the evolution the two walkers on the 2D lattice. The latter was studied both before and after the QAA routine.
Regarding the space-constrained quantum search, we used both a single and multiple solutions system.

5.1 $m = 1$ solutions

5.1.1 Biased target position

The first numerical analysis studies the single-solution system, chosen in different region of the graph in order to test how the success probability would change based on the distance between the target itself and the starting $(0, 0)$ node.
Firstly, we use a "Moving" shift instead of a "Flip-Flop" one, in order to study possible differences. The most interesting result is that, with this type of shift operator, the success probability of the two particles is very low, even lower than the starting one (in the uniform state case, the starting probability was $p = \frac{1}{N} = \frac{1}{\sqrt{2^k}}$, with k the number of qubits). The probability graphs for both states are reported below, for both the uniform and localized state:

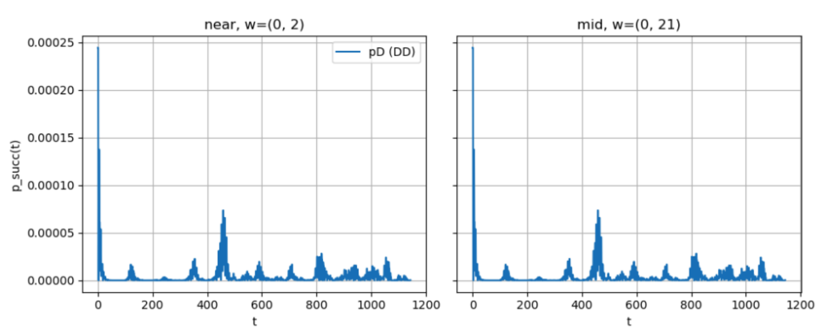


Figure 5.1: Success probability with S_m of $|D, D\rangle$

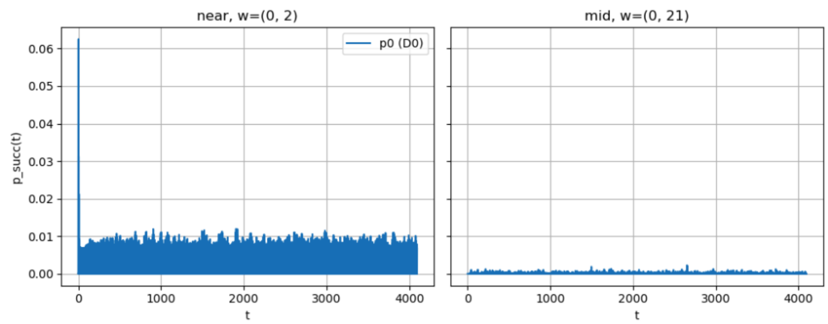


Figure 5.2: Success probability with S_m of $|D,0\rangle$

As it can be inferred from the graph, for $|D,0\rangle$ there is a clear difference between the success probability related to a "near" and a "mid" target state. The former is much more favorable than the latter, simply because our quantum walker can more easily access the targeted node, while it is much more difficult for it to reach the farthest one.

On the other hand, the success probability of the uniform state $|D,D\rangle$ drops to very low values after only the first iterations, going well below the starting one of $p = \frac{1}{2^k} = \frac{1}{N}$. It's also apparent that, given an initial uniform state on the graph, the success probability is the same for both a "near" and "mid" vertex.

On the other hand, if we now use the "Flip-Flop" Shift S_{ff}, the success probability behave quite differently

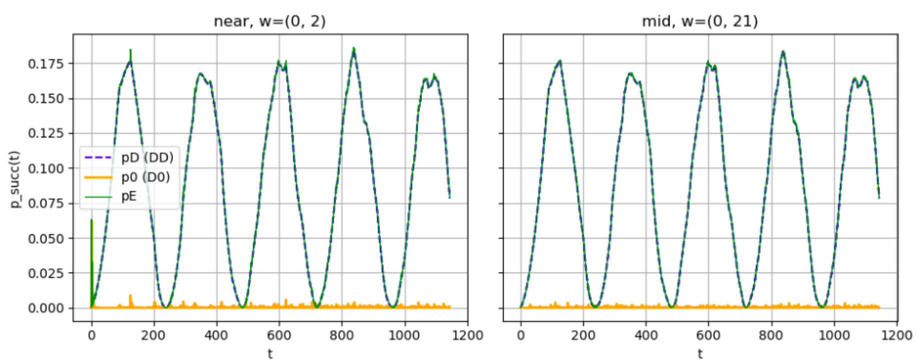


Figure 5.3: Success probability of the uniform, localized and entangled state in a $k = 12$ qubit system

The situation is now much different from before. We can derive two conclusions from this graph:

- The success probability of the entangled state and the uniform state are completely overlapped
- The localized state, despite the usage of the S_{ff} shift, is consistently very low: like the QAA case applied to the combinatorial entangled Grover search, our operators are perfectly tailored on the initial uniform state $|D, D\rangle$. This occurrence imply that our localized state $|D, 0\rangle$ will struggle much more to reach a significant success probability of finding the marked vertex.
- We can observe the oscillating pattern in the success probability P_t of the walkers, which is the numerical confirmation of our result on quantum walks in section 2.3.

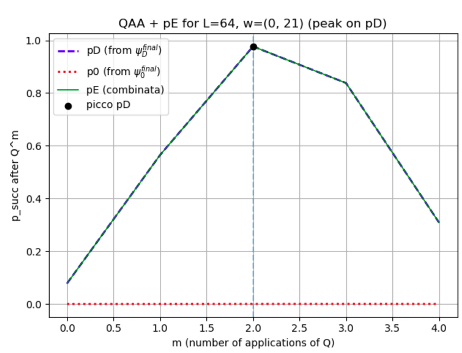
We can now move to the next numerical results, studying what happens after the QAA routine. It is known from literature that the optimal amount of iterations of a QAA routine is:

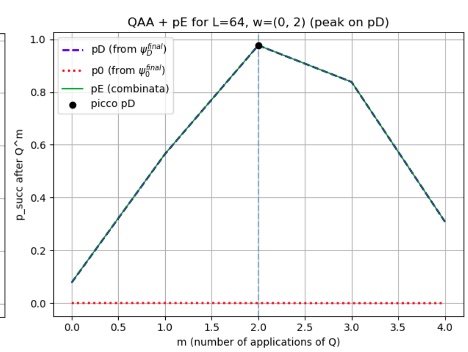
$$\boxed{m = \left\lfloor \frac{\pi}{4\theta_a} - \frac{1}{2} \right\rfloor}, \quad \theta_a = \arcsin(\sqrt{p}) \tag{5.1}$$

where p is the starting probability *before* the QAA routine. In our case, this value has been computed as:

$$\boxed{m = \frac{\pi}{4}\sqrt{\log(N)} - \frac{1}{2}} \tag{5.2}$$

Where $p = O(\frac{1}{\log(N)})$ is the success probability associated to the uniform state after $t_f = \frac{\pi}{2\alpha}$ iterations of the QW.
The graphs obtained were the following:





The evolved $|D, D\rangle$ state reach its peak success probability after just 2 steps, showing the efficiency of the QAA routine. It can also be observed that, while the p_D and p_E are practically overlapped, the p_0 curve had very little amplification from our operator Q.
Moreover, if we now analyze the fit function on a $\log-\log$ scale between the gained advantage $(p_E - p_D)$ and the number of computational basis states $N = 2^k$, we can observe the following result:

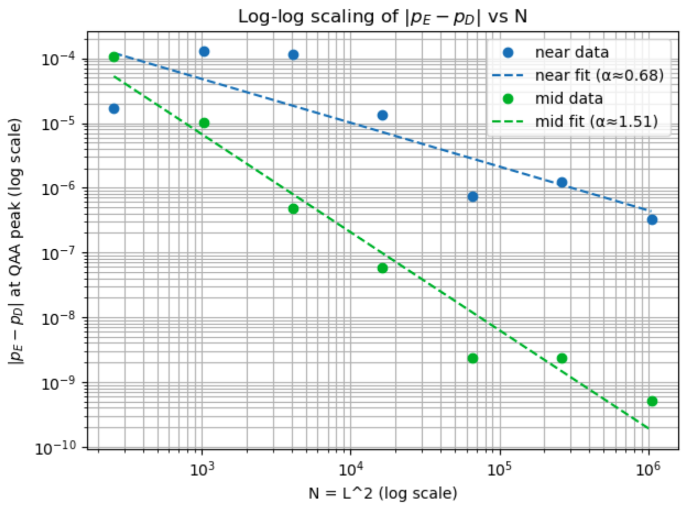


Figure 5.4: "Near" vs "Mid" targets for different values N

From the linear fit on the log−log scale we obtain the following results:

	Near	**Mid**
α	0.68 ± 0.19	1.51 ± 0.14

Table 5.1: α coefficients from the fit

It can be inferred that, while we we have a target "near" the $(0,0)$ starting node, the contribution of $|D,0\rangle$ to the overall success probability will be larger, and the overall advantage will decrease consistently as $1/\sqrt{N}$. On the other hand, as the distance between the target and the starting node increase, the advantage decreases much faster, as the constructive interference built by $|D,0\rangle$ will be much smaller, consistently with $1/N^{-\frac{3}{2}}$. We will see in the next part that without "choosing" explicitly the target position, we will obtain a results in between this two trends.

5.1.2 Randomly chosen target position

As we said before, the use of specific points in lattice in our simulations create a certain bias. In order to avoid it, the next section is devoted to the same simulations as above, but with the random sampling of a certain amounts of points each time for each $N = 2^k$. Our results are shown below:

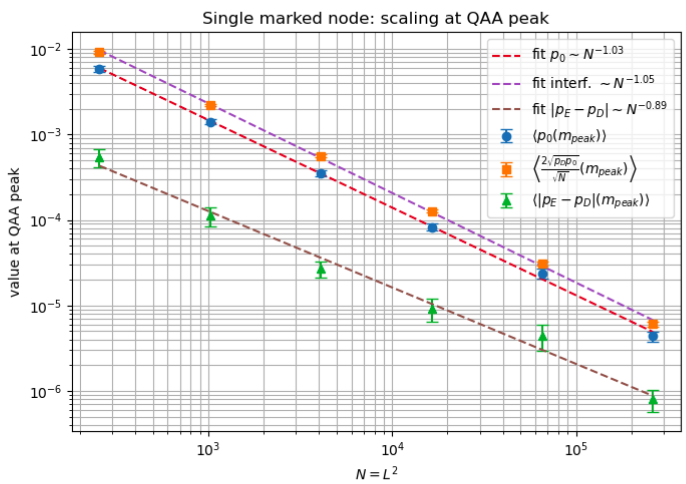


Figure 5.5: Comparison of the decrease of p_0, $\frac{\sqrt{p_D p_0}}{\sqrt{N}}$, $p_E - p_D$

obtaining the following results:

$$\alpha = -0.89 \pm 0.02, \beta = -2.9 \pm 0.2; \text{ where: } \quad \log(p_E - p_D) = \alpha \log N + \beta \qquad (5.3)$$

It is interesting to note that the asymptotic decrease of the difference between $p_E - p_D$ is not exactly $\frac{1}{N}$. Indeed, in the graph above we can observe how all the components of the numerator in the $p_E - p_D$ formula go to 0 as $\frac{1}{N}$, and yet the overall value of this difference does not.
This could be explained by small correction effect due to the finite size of our sample of points, where the overall value of the asymptotic decrease is damped by some cross-correction between the numerator terms. This effect will not be visible in the two solutions case, where instead a strong $\frac{1}{N}$ leading trend will be estimated.
Therefore, in the single-marked case, a pure power-law fit yields an effective exponent $\alpha \simeq 0.89$, that could be explained by the finite-size effect of a logarithmically corrected $1/N$ scaling rather than a genuinely distinct asymptotic exponent. Indeed, by adding another point to the graph, corresponding to $N = 2^{20}$, we obtained the following result:

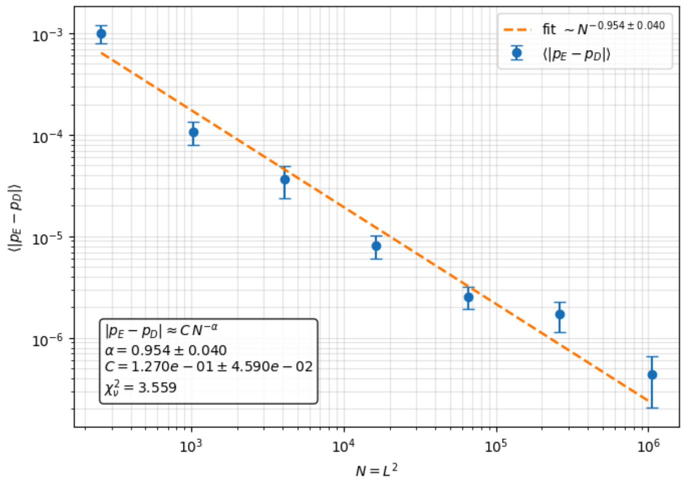


Figure 5.6: Adjusted scaling of $p_E - p_D$ with the added $N = 2^{20}$ point

As it can be clearly seen, the resulting α coefficients is consistent with 1 within 2σ:

$$\alpha = 0.95 \pm 0.04 \tag{5.4}$$

confirming our initial doubt on the finite-size effect. The last point has a much wider error bar due to the less amount of points used for its estimation.
Moreover, the error bars are asymmetrical due to the log scale translation used:

$$\sigma_{\log(y)} = \frac{\sigma_y}{y} \tag{5.5}$$

5.1.3 $m = 2$ solutions

The next section is devoted to the study of multiple solutions system.
Specifically, we used $m = 2$ solutions: firstly, with a single random chosen pair of targets, and then (as we did before) a sampling of $n = 50$ different pairs that we used to compute a mean value of $(p_E - p_D)$, in order to minimize possible biases in the target position's choice.
The first result we obtained is reported in the graph below:

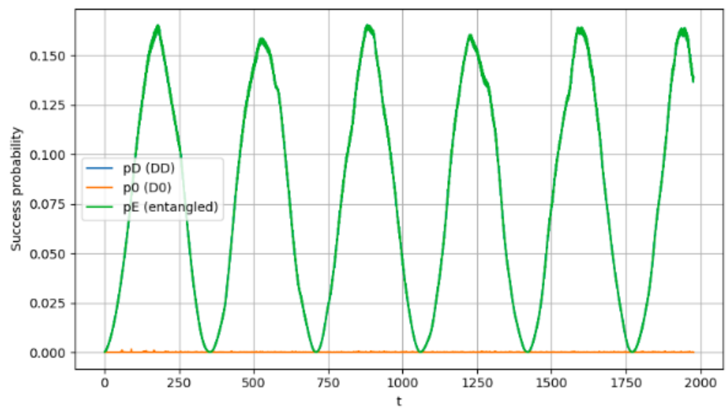


Figure 5.7: Success probability of search algorithms on a QW with random targets on the 2D lattice with $L = 128$

As it can be seen, just like the previous results with a one-solution system, $|D, D\rangle$ shows the typical oscillatory behavior of a Quantum Walk, with p_D practically overlapped with p_E, while $|D, 0\rangle$ is unable to build-up interference on the selected targets.
We also notice correctly that, without a QAA routine, the success probability is still very low, reaching slightly more than $p \simeq 0.15$. On the same-size 2D lattice with $L = 128$ we have also done the next analysis: $n = 50$ different samples of target pairs, studying the mean value of the maximum difference $(p_E - p_D)$, obtaining the following result:

$$\langle p_E - p_D \rangle = 0.0020 \pm 0.0003 \tag{5.6}$$

showing a marginal improvement.
With the implementation of a QAA routine the algorithm's performance slightly changed, and, just like before, the QAA immediately boost the success probability of $|D, D\rangle$ to $\simeq 1$.
However, as we expect, the probability associated to $|D, 0\rangle$ remains almost 0. The resulting mean value of $p_E - p_D$ is the following:

$$\langle p_E - p_D \rangle = 0.000129 \pm 0.000008 \tag{5.7}$$

Finally, we studied the dependence from N of this quantity, choosing for each graph $n = 50$ pairs of targets. The results obtained are shown below:

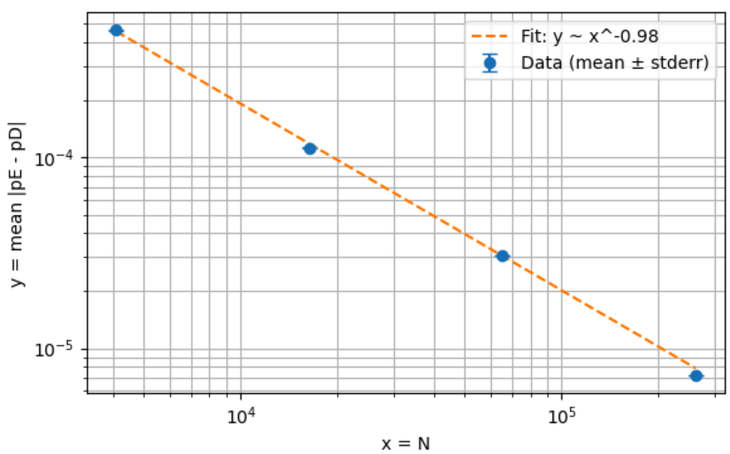


Figure 5.8: Simulations for $n = 50$ target in a $k = 12, 14, 16, 18$ system with two solutions

From the linear log−log fit we obtain the following value:

$$\alpha = -0.98 \pm 0.02, \quad b = 0.43 \pm 0.25 \tag{5.8}$$

showing a consistent $\frac{1}{N}$ trend, unlike the single-solution case. As we did before, we also tested the various asymptotic trends of the different term in the numerator, and we obtained the following values, all of them consistent with one another:

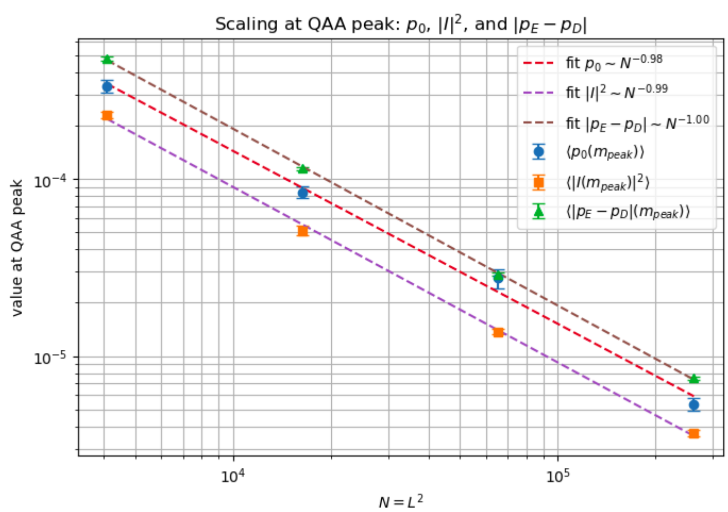


Figure 5.9: Comparison of the decrease of p_0, $|I|^2$, $p_E - p_D$

Chapter 6: Analytical results and comparison

As we have seen, on a 2D lattice the advantage in the success probability decreases as the graph becomes larger. We could only analyze it numerically, due to the difficulties presented by the mathematical structure of the quantum search operator U'. However, in the combinatorial case the calculations are much cleaner and we can obtain precise analytical results, as shown below. Being the combinatorial case a particular case of a quantum search where every node of the graph is linked to every other, we do not have the problem of having to deal with a quantum walk operator that diffuse our wave-function towards the target state, because it is already immediately accessible. This means that we will only need to boost the probability amplitude in the "good" subspace, and therefore we will start our analysis from a QAA operator.

6.1 $m = 1$ solutions

A general QAA operator has the follwoing structure:

$$\mathcal{O} = -A^{-1} S_0 A S_x \tag{6.1}$$

where we have chosen $A = H$, the Hadamard gate:

$$\mathcal{O} = -H S_0 H S_x \tag{6.2}$$

In order to study the action of t applications of this operator to the initial state, we first perform a few manipulations. Considering that:

$$\begin{aligned}
&\mathcal{O} H |0\rangle = -H S_0 H S_x H |0\rangle \\
&\mathcal{O}^t H |0\rangle = (-H S_0 H S_x) ... (-H S_0 H S_x) H |0\rangle = (-1)^t H (S_0 H S_x H) ... (S_0 H S_x H) |0\rangle \\
&= (-1)^t H O^t |0\rangle
\end{aligned} \tag{6.3}$$

where O:

$$O = S_0 H S_x H = (I - 2\,|0\rangle\langle 0|)H(I - 2\,|x\rangle\langle x|)H = I - 2\,|\bar{x}\rangle\langle\bar{x}| - 2\,|0\rangle\langle 0| + \frac{4}{\sqrt{N}}\,|0\rangle\langle\bar{x}| \tag{6.4}$$

where $|\bar{x}\rangle := H\,|x\rangle$. From the definition, it is clear that $\langle 0|\bar{x}\rangle = \frac{1}{\sqrt{N}}$. Given this rewriting of QAA operator $\mathscr{O}$, we will now focus on studying O.
Firstly, we will decompose $|\bar{x}\rangle$ on the span$\{|0\rangle, \left|0_x^\perp\right\rangle\}$:

$$|\bar{x}\rangle = \sqrt{\frac{1}{N}}\,|0\rangle + \sqrt{1 - \frac{1}{N}}\,\left|0_x^\perp\right\rangle \tag{6.5}$$

where $\left|0_x^\perp\right\rangle = \frac{1}{\sqrt{N-1}}\sum_{y\in\{0,1\}^k, y\neq 0} e^{i\pi x\cdot y}\,|y\rangle$.
In the base $\{|0\rangle, \left|0_x^\perp\}\right\rangle$, O becomes:

$$O = \begin{pmatrix} -1 + \frac{1}{2^{k-1}} & \frac{2}{\sqrt{N}}\sqrt{1-\frac{1}{N}} \\ -\frac{2}{\sqrt{N}}\sqrt{1-\frac{1}{N}} & -1 + \frac{1}{2^{k-1}} \end{pmatrix} \tag{6.6}$$

We can now easily diagonalize it, and obtain the following eigenvalues:

$$\lambda_\pm = -1 + \frac{2}{N} \pm \frac{2i}{\sqrt{N}}\sqrt{1 - \frac{1}{N}} \tag{6.7}$$

Given the eigenvalues, the eigenvectors are trivially estimated:

$$v_\pm = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ \pm i \end{pmatrix} \tag{6.8}$$

We can then calculate $O^t = S\Lambda^t S^{-1}$, substituting $\lambda_\pm = a \pm ib, a = -1 + \frac{2}{N}, b = \frac{2}{\sqrt{N}}\sqrt{1-\frac{1}{N}}$:

$$\begin{aligned} O^t &= \frac{1}{2}\begin{pmatrix} (a+ib)^t + (a-ib)^t & -i\big((a+ib)^t - (a-ib)^t\big) \\ i\big((a+ib)^t - (a-ib)^t\big) & (a+ib)^t + (a-ib)^t \end{pmatrix} \\ &= \begin{pmatrix} \mathrm{Re}\big((a+ib)^t\big) & -\mathrm{Im}\big((a+ib)^t\big) \\ \mathrm{Im}\big((a+ib)^t\big) & \mathrm{Re}\big((a+ib)^t\big) \end{pmatrix} \end{aligned} \tag{6.9}$$

A more compact form can be written as:

$$O^t = \begin{pmatrix} \mathrm{Re}(\lambda_+^t) & -\mathrm{Im}(\lambda_+^t) \\ \mathrm{Im}(\lambda_+^t) & \mathrm{Re}(\lambda_+^t) \end{pmatrix} \tag{6.10}$$

6.2 Algorithm exploiting entanglement

We now analyze the performance of a search algorithm that exploits two entangled registers, with the oracle acting on both:

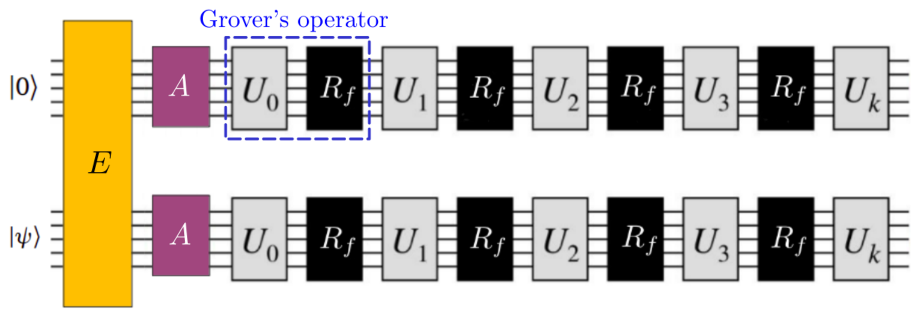


Figure 6.1: Entanglement-assisted quantum search scheme

The starting state can be freely chosen, and we are going to study two cases:

- $|\psi_1\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle\, |b\rangle + e^{i\theta}\, |b\rangle\, |0\rangle \Big)$
- $|\psi_2\rangle = \frac{1}{\sqrt{2(1+\cos(\theta)|\langle 0|H|0\rangle|^2)}}\Big(|0\rangle \otimes H\,|0\rangle + e^{i\theta} H\,|0\rangle \otimes |0\rangle \Big)$

On the $|0\rangle$ state, the action of the operator is trivial:

$$\begin{aligned}
&(-1)^t H O^t\,|0\rangle = (-1)^t H(Re(z^t)\,|0\rangle + Im(z^t)\,\big|0_x^{\perp}\big\rangle) = \\
&(-1)^t(rH\,|0\rangle + iH\,\big|0_x^{\perp}\big\rangle) \xrightarrow{\text{projecting on } \langle x|} \langle x|\,(-1)^t(rH\,|0\rangle + iH\,\big|0_x^{\perp}\big\rangle) = \\
&(-1)^t\Big(\frac{r}{\sqrt{N}} + \frac{i\sqrt{N-1}}{\sqrt{N}}\Big) = \mathscr{A}
\end{aligned} \tag{6.11}$$

where $r = \cos(t\theta_k)$ and $i = \sin(t\theta_k)$. From the seminal paper by Brassard and Høyer[7] we know that $\sin(\theta_a) = \sqrt{a} = \frac{1}{\sqrt{N}}$ (where a is the initial success probability of our algorithm before the N step amplitude amplification trough the oracle's action), so we can derive that $\cos(\theta_a) = \sqrt{1-\frac{1}{N}}$. Therefore, we can write a much more compact form for p_0:

$$\begin{aligned}
&p_D = \Big|\frac{\cos(t\theta_k)}{\sqrt{N}} + \frac{\sin(t\theta_k)\sqrt{N-1}}{\sqrt{N}}\Big|^2 = \\
&|\cos(t\theta_k)\sin(\theta_a) + \sin(t\theta_k)\cos(\theta_a)|^2 = |\sin(\theta_a + t\theta_k)|^2
\end{aligned} \tag{6.12}$$

Observe that $\theta_k = 2\theta_a$, so p_0 is exactly:

$$p_D = \sin^2(\theta_a + t\theta_k) = \sin^2((2t+1)\theta_a) \tag{6.13}$$

which is the correct success probability we expected to find after N steps of the QAA routine.

6.2.1 Auxiliary state: $|b\rangle$

On the state $|b\rangle$ we need to be a bit more careful. $|b\rangle$ is a generic state of the computational basis ($b \neq 0$), therefore is orthogonal to $|0\rangle$. Graphically, it can be viewed as the following:

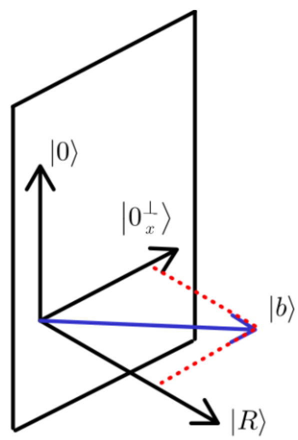


Figure 6.2: Graphical representation of our vectors

We can decompose it as:

$$|b\rangle = \frac{(-1)^{x\cdot b}}{\sqrt{N-1}} \left|0_x^\perp\right\rangle + \sqrt{\frac{N-2}{N-1}} |R\rangle \tag{6.14}$$

there is obviously no component of $|b\rangle$ on $|0\rangle$, due to orthogonality, while $|R\rangle$ is the representative state of the remainder Hilbert space, where O act as an identity.
If we then apply $(-1)^t HO^t$ on it, obtaining:

$$\begin{aligned}
(-1)^t HO^t |b\rangle &= (-1)^t H\Big(\frac{O^t(-1)^{x\cdot b}\left|0_x^\perp\right\rangle}{\sqrt{N-1}} + \sqrt{\frac{N-2}{N-1}} |R\rangle\Big) \\
&= (-1)^t H\Big(\frac{(-1)^{x\cdot b}}{\sqrt{N-1}}(-i|0\rangle + r\left|0_x^\perp\right\rangle) + \sqrt{\frac{N-2}{N-1}} |R\rangle\Big) \\
&\xrightarrow{\text{projecting on } \langle x|} = \frac{(-1)^t(-1)^{x\cdot b}}{\sqrt{N-1}}\Big(-\cos(t\theta_k)\sqrt{\frac{N-1}{N}} + \frac{\sin(t\theta_k)}{\sqrt{N}}\Big)
\end{aligned} \tag{6.15}$$

The resulting success probability is:

$$p_b = \frac{1}{N-1}\sin^2\Big(t\theta_k - \arctan\big(\sqrt{N-1}\big)\Big) \tag{6.16}$$

where we used the trigonometric substitution:

$$-a\cdot\cos(x) + \sin(x) = \sqrt{a^2+1}\,\sin(x - \arctan(a)) \tag{6.17}$$

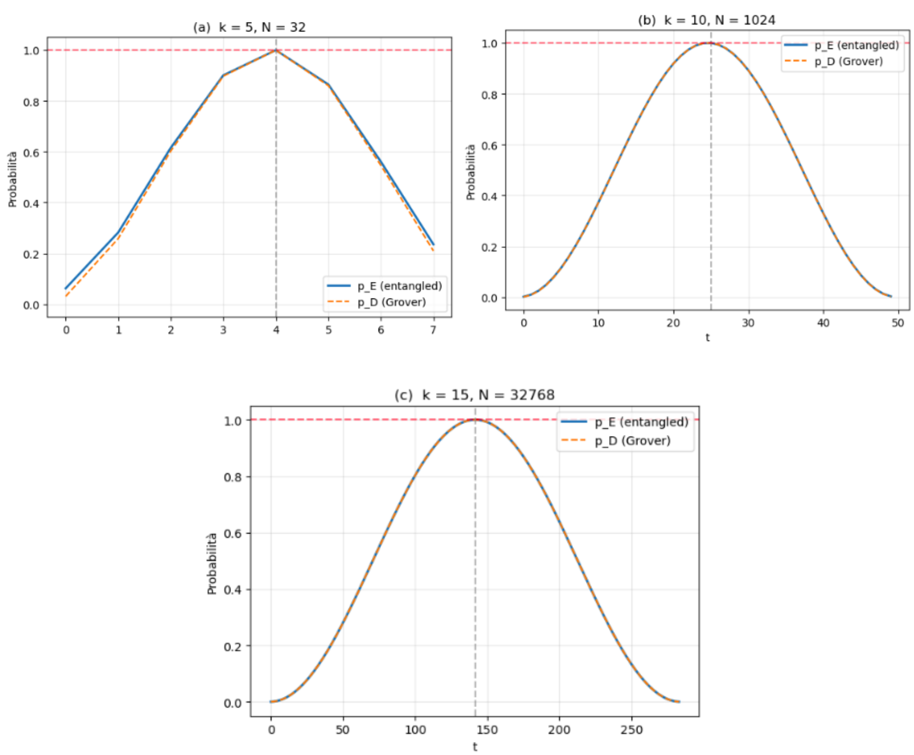
in our case $a = \sqrt{N-1}$.
This probability is correctly defined to be always upper bounded by 1, and it decays to 0 as $\simeq \frac{1}{N}$. We can then evaluate the p_E after N step of our algorithm as:

$$||(P\otimes(\mathbf{I}-P)+(\mathbf{I}-P)\otimes P+P\otimes P)(\mathcal{O}^t\otimes\mathcal{O}^t)\Big(\frac{1}{\sqrt{2}}\Big(|0\rangle\otimes|b\rangle+e^{i\theta}\,|b\rangle\otimes|0\rangle\Big)\Big)||^2 \tag{6.18}$$

The operator P is the projector $P = |x\rangle\langle x|$ on the 1-dimensional solution space.
It follows from Eq.3.24 that the success probability is:

$$p_E = p_D + p_b - p_D p_b - p_D p_b \cos(\theta) \tag{6.19}$$

where the inner products in Eq.3.24 $\langle 0|b\rangle = 0$, due to the orthogonality of the computational basis states.
In order to maximize the final expression, we use $\theta = \pi$. The resulting probability has a small improvement thanks to the interference term, and the success probability is slightly better than p_D, as it can be seen from the graphs below, showing a marginal increase:



k	**N=**N	p_E	p_D	$\Delta p = p_E - p_D$
5	32	0.99921	0.99918	$3 \cdot 10^{-5}$
10	1024	0.9994632	0.9994631	$1 \cdot 10^{-7}$
15	32768	0.9999868295	0.9999868293	$2 \cdot 10^{-10}$

Table 6.1: Success probability comparison with k=5,10,15

From this data it is clear that the advantage in using an entangled state disappears pretty quickly, resulting in an algorithm with the same asymptotic complexity $O(\sqrt{N})$ of the classic Grover algorithm, with a small advantage. However, in order to show how quickly this advantage disappears, we have programmed a linear fit of $\log(p_E - p_D) = \alpha \log(N) + \beta$, obtaining the following results:

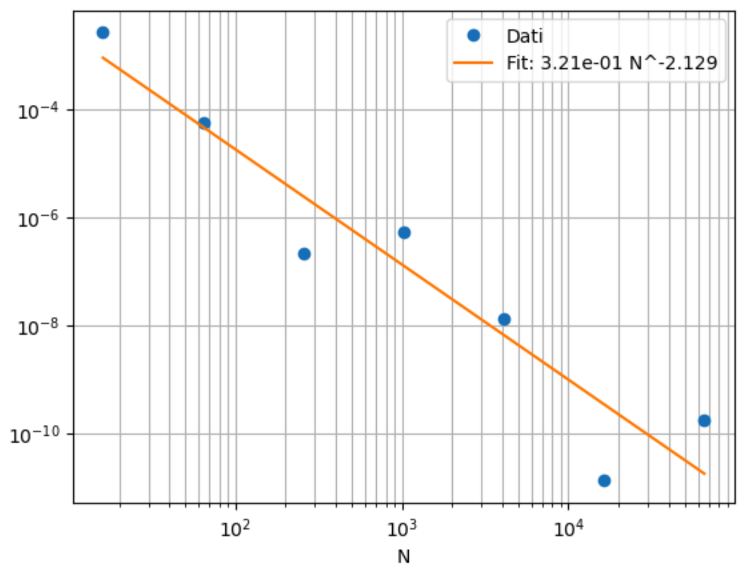


Figure 6.3: Numerical fit of the decrease trend of entanglement-based advantage

with the following parameter:

$$\alpha = -2.13 \pm 0.31, \quad \log(p_E - p_D) \propto \alpha \log(N) \tag{6.20}$$

Our results shows that, with an entangled-based state with a generic $|b\rangle$ state as an ancilla, the advantage over the classic case decays as $\simeq \frac{1}{N^2}$.

This result can be proved more formally, as it will be shown below. Indeed, consider:

$$\begin{aligned} p_E - p_D = p_b = \frac{1}{N-1}\sin^2\Big(t\theta_k - \arctan\big(\sqrt{N-1}\big)\Big) \\ \theta_k = 2\theta_a, \qquad \theta_a = \arcsin\frac{1}{\sqrt{N}} \end{aligned} \tag{6.21}$$

It is well known in the literature regarding Grover algorithm that the optimal time is defined as:

$$t := \frac{\pi}{4\theta_a} - \frac{1}{2}. \tag{6.22}$$

This time is, in general, a real number. However, being the number of application of our operator discrete, we necessarily need to approximate it to a discrete value. In order to do this, we can define $\tilde{t}_*$ through an auxiliary parameter ϵ that will round the value of t to the nearest integer. Analytically this means that:

$$\exists\varepsilon \in \left[-\tfrac{1}{2}, \tfrac{1}{2}\right] \quad \text{such that} \quad \tilde{t}_* = t + \varepsilon. \tag{6.23}$$

Using the exact identity

$$\arctan\big(\sqrt{N-1}\big) = \frac{\pi}{2} - \arctan\Big(\frac{1}{\sqrt{N-1}}\Big),$$

define

$$\phi := \arctan\Big(\frac{1}{\sqrt{N-1}}\Big).$$

Then

$$\tilde{t}_*\,\theta_k - \arctan\big(\sqrt{N-1}\big) = \tilde{t}_*(2\theta_a) - \Big(\frac{\pi}{2} - \phi\Big) \tag{6.24}$$

$$= \Big(2\tilde{t}_*\,\theta_a - \frac{\pi}{2}\Big) + \phi. \tag{6.25}$$

Now substitute $\tilde{t}_* = t + \varepsilon$:

$$2\tilde{t}_*\,\theta_a = 2(t+\varepsilon)\theta_a \tag{6.26}$$

$$= 2t\theta_a + 2\varepsilon\theta_a. \tag{6.27}$$

By definition of t,

$$2t\theta_a = 2\Big(\frac{\pi}{4\theta_a} - \frac{1}{2}\Big)\theta_a = \frac{\pi}{2} - \theta_a.$$

Hence

$$2\tilde{t}_*\,\theta_a - \frac{\pi}{2} = -\theta_a + 2\varepsilon\theta_a = (2\varepsilon - 1)\theta_a.$$

Therefore the sine argument becomes

$$\tilde{t}_*\,\theta_k - \arctan\big(\sqrt{N-1}\big) = \phi + (2\varepsilon - 1)\theta_a =: \delta. \tag{6.28}$$

For $N \to \infty$ we use the Taylor expansions

$$\arcsin x = x + O(x^3), \qquad \arctan x = x + O(x^3).$$

With $x = 1/\sqrt{N}$ and $x = 1/\sqrt{N-1}$ we obtain

$$\theta_a = \frac{1}{\sqrt{N}} + O(N^{-3/2}), \qquad \phi = \frac{1}{\sqrt{N-1}} + O(N^{-3/2}) = \frac{1}{\sqrt{N}} + O(N^{-3/2}).$$

Since ε is bounded,

$$(2\varepsilon - 1)\theta_a = O(N^{-1/2}).$$

Therefore

$$\delta = \phi + (2\varepsilon - 1)\theta_a = O(N^{-1/2}). \tag{6.29}$$

For $\delta \to 0$,

$$\sin\delta = \delta + O(\delta^3), \qquad \sin^2\delta = \delta^2 + O(\delta^4).$$

Since $\delta = O(N^{-1/2})$, we conclude

$$\sin^2(\delta) = O(N^{-1}).$$

Substituting into p_b,

$$p_b = \frac{1}{N-1}\sin^2(\delta) = \frac{1}{N-1}O(N^{-1}) = O(N^{-2}).$$

$$p_E - p_D = p_b = O(N^{-2}) \qquad \text{as } N \to \infty. \tag{6.30}$$

Obtaining analytically the exact scaling time showed in our graph.

6.2.2 Auxiliary state: $H|0\rangle$

We move now to evaluate the success probability on the state $H|0\rangle$. We start by decomposing it on the following orthogonal set: $\{|0\rangle, |0_x^\perp\rangle, |R\rangle\}$, where $|R\rangle$ is defined as an orthogonal vector to the plane spanned by $\{|0\rangle, |0_x^\perp\rangle\}$. Our operator O acts non-trivially only on that plane, while on $|R\rangle$ acts as the identity.
The decomposition can be written as follows:

$$H|0\rangle = \frac{|0\rangle}{\sqrt{N}} - \frac{|0^\perp\rangle}{\sqrt{N}\sqrt{N-1}} + \sqrt{\frac{N-2}{N-1}}|R\rangle \tag{6.31}$$

We now evaluate the action of the operator on such state:

$$(-1)^t HO^t(H|0\rangle) = (-1)^t H\Big(\frac{O^t|0\rangle}{\sqrt{N}} - \frac{O^t|0_x^\perp\rangle}{\sqrt{N}\sqrt{N-1}} + \sqrt{\frac{N-2}{N-1}}|R\rangle\Big) \tag{6.32}$$

In order to apply the operator O^t, we decompose the $\{|0\rangle, |0_x^\perp\rangle\}$ states onto the eigenvector basis $\{|v_+\rangle, |v_-\}\rangle$, and then return to the original base. We obtain the following result:

$$\begin{aligned}(-1)^t HO^t(H|0\rangle) = (-1)^t\Big(\frac{H|0\rangle}{\sqrt{N}}(r - \frac{i}{\sqrt{N-1}}) - \\ - \frac{H|0_x^\perp\rangle}{\sqrt{N}}(i + \frac{r}{\sqrt{N-1}}) + \sqrt{\frac{N-2}{N-1}}H|R\rangle\Big)\end{aligned} \tag{6.33}$$

If we want to evaluate the success probability, we need to project everything onto $\langle x|$. We observe that the last product, $\langle x|H|R\rangle$, is 0 because the state $H|x\rangle$ is by construction orthogonal to the state $|R\rangle$, due to $H|x\rangle$ being entirely contained in the plane spanned by $\{|0\rangle, |0_x^\perp\rangle\}$. It follows that:

$$p_{H|0\rangle} = \frac{\sin^2(t\theta_k)}{N-1} \tag{6.34}$$

The shape of this probability is physically predictable, due to the starting state being the superposition of all the computational basis states. Only a tiny fraction of the sum will be contained on the plane where our operator acts non-trivially as a rotation, so the final success probability will reflect exactly that, as it can be seen by the denominator that becomes exponentially bigger with k, the number of qubits.
Furthermore, we notice how for $t = 0$ the success probability is exactly 0. This result is also easily explainable: our states undergoes an initial unitary transform $\mathscr{A} = H$, therefore if we start from the $H|0\rangle$ state, after the first operator we will have $H(H|0\rangle) = |0\rangle$, due to the Hadamard being its own inverse. But then, with $t = 0$ steps of our QAA operator, the success probability starting from $|0\rangle$ is necessarily 0, due to the orthogonality between the solution state $|x\rangle$ and the $|0\rangle$ state.

We can then evaluate again the p_E after t step of our algorithm by following Eq.3.24, obtaining the following success probability:

$$p_E = \frac{p_0 + p_1 - p_0 p_1 + \cos(\theta)(2\sqrt{p_0}\sqrt{p_1}|\langle 0^F \left|\psi^F\right\rangle| - p_0 p_1)}{1+\cos(\theta)|\langle 0^F |\psi^F\rangle|^2} \tag{6.35}$$

whit $\langle \psi^F \left|0^F\right\rangle = \langle 0^F \left|\psi^F\right\rangle = \langle 0|O^{t\dagger}H^\dagger H O^t H|0\rangle = \langle 0|H|0\rangle = \frac{1}{\sqrt{N}}$.
By combing the two expressions we have found for the two success probabilities, we obtain the complete analytical expression for the p_{succ} (we set $\theta = \pi$ again as it is the optimum choice to maximize the whole expression):

$$\boxed{p_E = \frac{\sin^2((2t+1)\theta_a) + \frac{\sin^2(2t\theta_a)}{N-1} - 2\frac{\sin((2t+1)\theta_a)\sin(2t\theta_a)}{\sqrt{N}\sqrt{N-1}}}{1-\frac{1}{N}}} \tag{6.36}$$

This is the success probability after t steps of the operators $\mathscr{O}^t \otimes \mathscr{O}^t$ ($\mathscr{O}^t = (-1)^t H O^t$) given two computers entangled and initialized in two different states $|0\rangle, H|0\rangle$.
The optimal number of queries to maximize the success probability of a single computer initialized as $|0\rangle$ is:

$$t_{opt} = \frac{\pi}{4\theta_a} - \frac{1}{2}, \theta_a = \arcsin\Big(\frac{1}{\sqrt{N}}\Big) \tag{6.37}$$

while in order to maximize $p_{H|0\rangle}$, we need to maximize the numerator, so we obtain:

$$t_{opt} = \frac{\pi}{4\theta_a} \tag{6.38}$$

It is obvious that while evaluating the success probability of the entangled state, both the interference term and the $p_{H|0\rangle}$ term scale as $O(\frac{1}{\sqrt{N}})$, so for large numbers of entry in the register, they both become irrelevant, and all the weight is shifted towards p_D, justifying the choice of the fist t_{opt} for the number of application of O. As it can be seen from the table and graphs below, the two curves are practically the same, with just a minor increase in the success probability while using the entangled state.

k	**N**	p_E	p_D	$\Delta p = p_E - p_D$
5	32	0.99918316	0.99918231	$8.5 \cdot 10^{-7}$
10	1024	0.9994612454	0.9994612453	$1 \cdot 10^{-10}$
15	32768	0.999986829518989	0.999986829518976	$1.3 \cdot 10^{-14}$

Table 6.2: Success probability comparison for $k = 5, 10, 15$.

We can now study the difference $p_E - p_D$. Recalling the following definition:

$$\sin\theta_a = \gamma = \frac{1}{\sqrt{N}}. \tag{6.39}$$

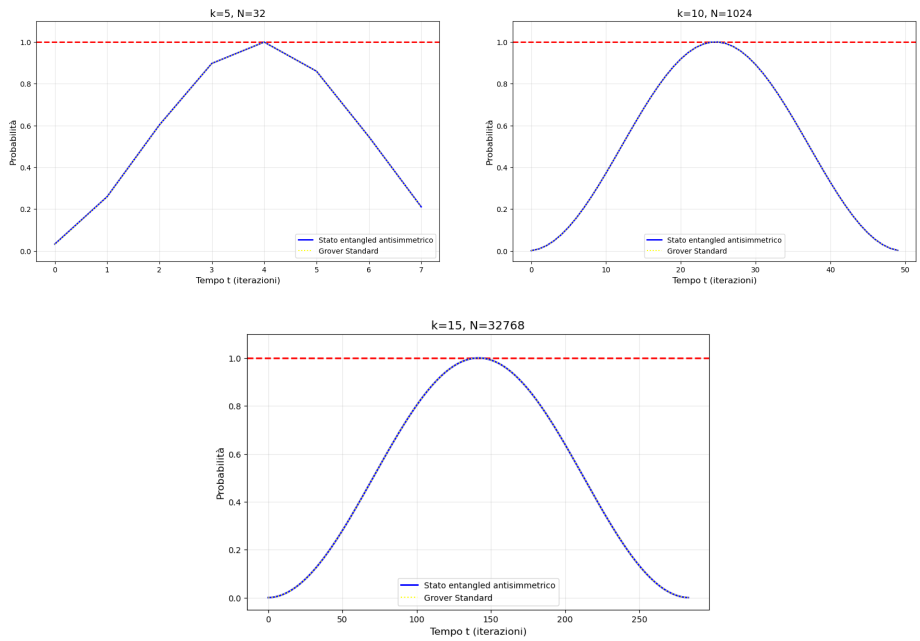


Figure 6.4: Comparison between p_E and p_D for different values of k.

It follows that:

$$N = \frac{1}{\sin^2\theta_a}, \qquad N-1 = \frac{1-\sin^2\theta_a}{\sin^2\theta_a} = \frac{\cos^2\theta_a}{\sin^2\theta_a} = \cot^2\theta_a \tag{6.40}$$

Hence:

$$\frac{1}{N-1} = \tan^2\theta_a, \qquad \frac{1}{\sqrt{N-1}} = \tan\theta_a \tag{6.41}$$

The two probabilities can be rewritten:

$$p_D = \sin^2\big((2t+1)\theta_a\big), \qquad p_{H|0\rangle} = p_0 = \sin^2(2t\theta_a)\tan^2\theta_a. \tag{6.42}$$

The numerator of p_E can be rewritten:

$$\begin{aligned}\text{num} = p_0 + p_D - 2\frac{\sqrt{p_0 p_D}}{\sqrt{N}} &= \sin^2(2t\theta_a)\tan^2\theta_a + \sin^2\big((2t+1)\theta_a\big) \\ &- 2\sin\theta_a\ \sin(2t\theta_a)\tan\theta_a\ \sin\big((2t+1)\theta_a\big)\end{aligned} \tag{6.43}$$

Obtaining:

$$p_E = \frac{\text{num}}{\cos^2\theta_a}. \tag{6.44}$$

$p_E - p_D$ can now be computed:

$$p_E - p_D = \frac{\text{num}}{\cos^2\theta_a} - p_D = \frac{\text{num} - p_D\cos^2\theta_a}{\cos^2\theta_a}. \tag{6.45}$$

Using the previous results, we can now prove that:

$$\begin{aligned}\mathrm{num} - p_D \cos^2\theta_a = \sin^2(2t\theta_a)\tan^2\theta_a - 2\sin\theta_a\sin(2t\theta_a)\tan\theta_a\sin\big((2t+1)\theta_a\big)\\ + \sin^2\theta_a\sin^2\big((2t+1)\theta_a\big).\end{aligned}$$

Substituting $\tan\theta_a = \dfrac{\sin\theta_a}{\cos\theta_a}$:

$$\sin^2(2t\theta_a)\tan^2\theta_a = \sin^2(2t\theta_a)\frac{\sin^2\theta_a}{\cos^2\theta_a},$$

$$2\sin\theta_a\tan\theta_a = 2\sin\theta_a\frac{\sin\theta_a}{\cos\theta_a} = 2\frac{\sin^2\theta_a}{\cos\theta_a}.$$

Hence:

$$\begin{aligned}\mathrm{num} - p_D\cos^2\theta_a = \frac{\sin^2\theta_a}{\cos^2\theta_a}\sin^2(2t\theta_a) - 2\frac{\sin^2\theta_a}{\cos\theta_a}\sin(2t\theta_a)\sin\big((2t+1)\theta_a\big)\\ + \sin^2\theta_a\sin^2\big((2t+1)\theta_a\big)\end{aligned}$$

It can be easily seen that this last result is a perfect square:

$$\left(\frac{\sin(2t\theta_a)}{\cos\theta_a} - \sin\big((2t+1)\theta_a\big)\right)^2 = \frac{\sin^2(2t\theta_a)}{\cos^2\theta_a} - 2\frac{\sin(2t\theta_a)}{\cos\theta_a}\sin\big((2t+1)\theta_a\big) + \sin^2\big((2t+1)\theta_a\big) \tag{6.46}$$

$$\mathrm{num} - p_D\cos^2\theta_a = \sin^2\theta_a\left(\frac{\sin(2t\theta_a)}{\cos\theta_a} - \sin\big((2t+1)\theta_a\big)\right)^2 \tag{6.47}$$

Dividing by $\cos^2\theta_a$ we obtain:

$$\begin{aligned}p_E - p_D &= \frac{\mathrm{num} - p_D\cos^2\theta_a}{\cos^2\theta_a}\\ &= \frac{\sin^2\theta_a}{\cos^2\theta_a}\left(\frac{\sin(2t\theta_a)}{\cos\theta_a} - \sin\big((2t+1)\theta_a\big)\right)^2\\ &= \tan^2\theta_a\left(\frac{\sin(2t\theta_a)}{\cos\theta_a} - \sin\big((2t+1)\theta_a\big)\right)^2\end{aligned}$$

All of this boils down to the much easier formula:

$$\boxed{p_E - p_D = \tan^2\theta_a\left(\frac{\sin(2t\theta_a)}{\cos\theta_a} - \sin\big((2t+1)\theta_a\big)\right)^2}. \tag{6.48}$$

In order to study how this formula behave in the asymptotic regime, let's remember that for $N \longrightarrow \infty$, $\theta_a = \arcsin(\frac{1}{\sqrt{N}}) \longrightarrow \frac{1}{\sqrt{N}} \longrightarrow 0$:

$$p_E - p_D \simeq \Big(\frac{1}{\sqrt{N}}\Big)^2\Big(\frac{2t}{\sqrt{N}} - \frac{(2t+1)}{\sqrt{N}}\Big)^2 \simeq \Big(\frac{1}{\sqrt{N}}\Big)^2\Big(\frac{1}{\sqrt{N}}\Big)^2 \simeq \frac{1}{N^2} \tag{6.49}$$

Both algorithm have the same asymptotic dependence from the number of queries of the oracle: $O(\sqrt{N})$, even though the difference in the success probability goes to 0 like $O(\frac{1}{N^2})$, making the use of entanglement in this scenario not very impactful. Moreover, as we did before, at $t^* = (\frac{\pi}{4\theta_a} - \frac{1}{2}) + \epsilon, \epsilon \in [-\frac{1}{2}, \frac{1}{2}]$, we can the asymptotic analysis:

$$E := \tan^2(\theta_a)\left(\frac{\sin(2t\theta_a)}{\cos(\theta_a)} - \sin\big((2t+1)\theta_a\big)\right)^2, \qquad \theta_a = \arcsin\frac{1}{\sqrt{N}}. \tag{6.50}$$

Let us denote $A := 2t\theta_a$. Then

$$(2t+1)\theta_a = A + \theta_a, \tag{6.51}$$

and by the addition formula,

$$\sin(A + \theta_a) = \sin A \cos\theta_a + \cos A \sin\theta_a. \tag{6.52}$$

Hence,

$$\frac{\sin A}{\cos\theta_a} - \sin(A+\theta_a) = \frac{\sin A}{\cos\theta_a} - (\sin A\cos\theta_a + \cos A\sin\theta_a) \tag{6.53}$$

$$= \sin A\left(\frac{1}{\cos\theta_a} - \cos\theta_a\right) - \cos A\sin\theta_a. \tag{6.54}$$

Since

$$\frac{1}{\cos\theta_a} - \cos\theta_a = \frac{1-\cos^2\theta_a}{\cos\theta_a} = \frac{\sin^2\theta_a}{\cos\theta_a}, \tag{6.55}$$

we obtain

$$\frac{\sin A}{\cos\theta_a} - \sin(A+\theta_a) = \sin A\frac{\sin^2\theta_a}{\cos\theta_a} - \cos A\sin\theta_a. \tag{6.56}$$

Factoring out $\sin\theta_a$,

$$= \sin\theta_a\,(\sin A\tan\theta_a - \cos A)\,. \tag{6.57}$$

Therefore,

$$E = \tan^2\theta_a\ \sin^2\theta_a\ (\sin A\tan\theta_a - \cos A)^2 = \frac{\sin^4\theta_a}{\cos^2\theta_a}(\sin A\tan\theta_a - \cos A)^2\,. \tag{6.58}$$

Now let t be the integer obtained by rounding the continuous optimum

$$t = \frac{\pi}{4\theta_a} - \frac{1}{2}. \tag{6.59}$$

Then there exists $\varepsilon \in [-\frac{1}{2}, \frac{1}{2}]$ such that

$$t^* = t + \varepsilon \in \mathrm{N} \tag{6.60}$$

Consequently,

$$A = 2t\theta_a = 2(t+\varepsilon)\theta_a \tag{6.61}$$

$$= \left(\frac{\pi}{2} - \theta_a\right) + 2\varepsilon\theta_a = \frac{\pi}{2} + \delta, \qquad \delta := (2\varepsilon - 1)\theta_a. \tag{6.62}$$

Using standard expansions for small θ_a,

$$\sin\left(\frac{\pi}{2} + \delta\right) = \cos\delta = 1 + O(\delta^2), \qquad \cos\left(\frac{\pi}{2} + \delta\right) = -\sin\delta = -\delta + O(\delta^3). \tag{6.63}$$

Since $\delta = O(\theta_a)$ and $\tan\theta_a = \theta_a + O(\theta_a^3)$, we get

$$\sin A \tan\theta_a - \cos A = (1 + O(\theta_a^2))(\theta_a + O(\theta_a^3)) - (-\delta + O(\theta_a^3)) \tag{6.64}$$

$$= \theta_a + \delta + O(\theta_a^3). \tag{6.65}$$

Because

$$\theta_a + \delta = \theta_a + (2\varepsilon - 1)\theta_a = 2\varepsilon\,\theta_a, \tag{6.66}$$

we obtain

$$\sin A \tan\theta_a - \cos A = 2\varepsilon\,\theta_a + O(\theta_a^3). \tag{6.67}$$

Hence,

$$\begin{aligned} (\sin A \tan\theta_a - \cos A)^2 &= 4\varepsilon^2\theta_a^2 + O(\theta_a^4) \\ \frac{\sin^4\theta_a}{\cos^2\theta_a} &= \theta_a^4(1 + O(\theta_a^2)) \end{aligned} \tag{6.68}$$

Therefore,

$$E = \theta_a^4\left(4\varepsilon^2\theta_a^2 + O(\theta_a^4)\right) = 4\varepsilon^2\theta_a^6 + O(\theta_a^8). \tag{6.69}$$

Finally, since

$$\sin\theta_a = \frac{1}{\sqrt{N}} \quad \rightarrow \quad \theta_a = O(N^{-1/2}), \tag{6.70}$$

we conclude

$$E = O(N^{-3}), \qquad N \rightarrow \infty. \tag{6.71}$$

This result was verified numerically in the graph below:

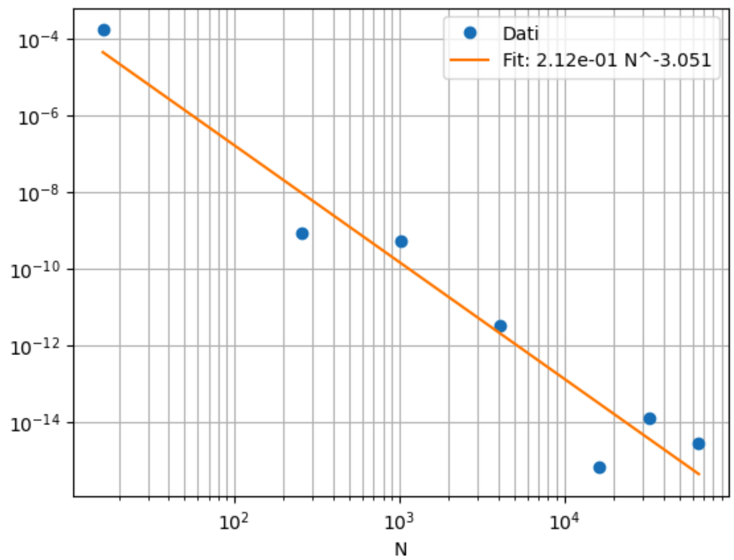


Figure 6.5: The direct numerical simulation of the $\frac{1}{N^3}$ trend

$$\alpha = -3.05 \pm 0.33, \quad \log(p_E - p_D) \propto \alpha \log(N) \tag{6.72}$$

This result tells us that with an ancilla state $H|0\rangle$, the entanglement-induced advantage is severely damped, showing a much faster decrease.

6.3 Multiple solution system

The natural follow-up question to our research on how to improve Grover algorithm through entanglement is to introduce more than one solution, to see if an entangled state could outperform a non-entangled one, while keeping the structure of the operator the same.

6.3.1 Two solution case

Given an unstructured and unsorted ensemble of $N = 2^k$ states, where k is the number of qubits, we suppose there are two marked elements. Given that they are both state of the computational basis, they will be orthogonal. Therefore, the projector P on the solution subspace will have the following structure:

$$P = |x_1\rangle\langle x_1| + |x_2\rangle\langle x_2| \tag{6.73}$$

We can then choose the structure of our initial entangled state as the ones we used for the single state solution case. Specifically:

- $|\psi_1\rangle = \frac{1}{\sqrt{2}}\big(\,|0\rangle\,|b\rangle + e^{i\theta}\,|b\rangle\,|0\rangle\,\big)$
- $|\psi_2\rangle = \frac{1}{\sqrt{2(1+\cos(\theta)|\langle 0|H|0\rangle|^2)}}\Big(\,|0\rangle \otimes H\,|0\rangle + e^{i\theta}H\,|0\rangle \otimes |0\rangle\,\Big)$

In general, we will still use the operator O defined in the previous section as $O = S_0 H S_x H$. We will study the following S_x:

$$S_x = 1 - 2\,|x_1\rangle\langle x_1| - 2\,|x_2\rangle\langle x_2| \tag{6.74}$$

This choice is optimal, as it can perfectly reproduce the action of the oracle on the target states.
Moreover, the expression of operator O will be the following:

$$\begin{aligned} O &= (1-2\,|0\rangle\langle 0|)H(1-2\,|x_1\rangle\langle x_1| - 2\,|x_2\rangle\langle x_2|)H \\ &= (1-2\,|0\rangle\langle 0|)(1-2\,|w_1\rangle\langle w_1| - 2\,|w_2\rangle\langle w_2|) \end{aligned} \tag{6.75}$$

where $|w_i\rangle := H\,|x_i\rangle\,, (i = 1, 2)$. In order to find an invariant subspace where O can act as a rotation, we need to rotate our states, defining:

$$|w_\pm\rangle := \frac{1}{\sqrt{2}}\big(\,|w_1\rangle \pm |w_2\rangle\,\big) \tag{6.76}$$

With this rotation in the computational basis, the structure of the operator remains the same, but we can observe something interesting:

$$\langle 0|w_i\rangle = \langle 0|\,H\,|x_i\rangle = \frac{1}{\sqrt{N}} \tag{6.77}$$

Hence:

$$\langle 0|w_\pm\rangle = \frac{\frac{1}{\sqrt{N}} \pm \frac{1}{\sqrt{N}}}{\sqrt{2}} \tag{6.78}$$

In the + case we obtain that $\langle 0|w_+\rangle = \sqrt{\frac{2}{N}}$, while $\langle 0|w_-\rangle = 0$.
The orthogonality between $|w_-\rangle$ and $|0\rangle$ is very useful, as it will be the necessary requirement in order to prove that $|w_-\rangle$ is an eigenvector of O with an eigenvalue of -1:

$$\begin{aligned} O\,|w_-\rangle &= (1-2\,|0\rangle\langle 0|)(1-2(|w_+\rangle\langle w_+| + |w_-\rangle\langle w_-|)\,|w_-\rangle \\ &= (1-2\,|0\rangle\langle 0|)(-|w_-\rangle) = -\,|w_-\rangle \end{aligned} \tag{6.79}$$

where we used that obviously $\langle w_-|w_+\rangle = 0$.
As we said before, the two vectors $|0\rangle\,, |w_+\rangle$ are not orthogonal, but they have an overlap of $\sqrt{\frac{2}{N}}$, living in a plane that is orthogonal to $|w_-\rangle$.
Thus, in order to study O as a rotation in the above-mentioned plane as we did in the previous section, we require a Gram–Schmidt process on span$\{|0\rangle\,, |w_+\rangle\}$:

$$\begin{aligned} |u_+\rangle &:= \frac{|w_+\rangle - \langle w_+|0\rangle\,|0\rangle}{\langle u_+|u_+\rangle} \\ \langle u_+|u_+\rangle &= \sqrt{1-\frac{2}{N}}, \langle w_+|0\rangle = \sqrt{\frac{2}{N}} \\ |u_+\rangle &= \frac{|w_+\rangle - \sqrt{\frac{2}{N}}\,|0\rangle}{\sqrt{1-\frac{2}{N}}} \end{aligned} \tag{6.80}$$

By construction, $|u_+\rangle$ is orthogonal to $|0\rangle$ and $|w_-\rangle$.
Being that we want to know the spectral decomposition of our operator O, we need to study it on the plane Γ spanned by $|0\rangle\,, |u_+\rangle$. We already know that $|w_-\rangle$ is an eigenvector.
Decomposing O on Γ:

$$\begin{aligned} O &= (I-2\,|0\rangle\langle 0|)(I-2(\sqrt{\frac{2}{N}}\,|0\rangle + \sqrt{1-\frac{2}{N}}\,|u_+\rangle)(\sqrt{\frac{2}{N}}\,\langle 0| + \sqrt{1-\frac{2}{N}}\,\langle u_+|)) \\ &= I - 2\Big(\frac{2}{N}\,|0\rangle\langle 0| + \sqrt{\frac{2}{N}}\sqrt{1-\frac{2}{N}}\,|0\rangle\langle u_+| + \sqrt{\frac{2}{N}}\sqrt{1-\frac{2}{N}}\,|u_+\rangle\langle 0| + (1-\frac{2}{N})\,|u_+\rangle\langle u_+|\Big) - \\ &- 2\,|0\rangle\langle 0| + \frac{4\sqrt{2}}{\sqrt{N}}\Big(\sqrt{\frac{2}{N}}\,|0\rangle\langle 0| + \sqrt{1-\frac{2}{N}}\,|0\rangle\langle u_+|\Big) \end{aligned} \tag{6.81}$$

In matrix form we obtain the following structure, which is reminiscent of the one obtained for the single state solution system. As we will see, this pattern will reoccur multiple times during our analysis.

$$\begin{aligned} O_{[0,u_+]} &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} -2+\frac{4}{N} & +2\sqrt{\frac{2}{N}}\sqrt{1-\frac{2}{N}} \\ -2\sqrt{\frac{2}{N}}\sqrt{1-\frac{2}{N}} & -2+\frac{4}{N} \end{pmatrix} \\ &= \begin{pmatrix} -1+\frac{4}{N} & +2\sqrt{\frac{2}{N}}\sqrt{1-\frac{2}{N}} \\ -2\sqrt{\frac{2}{N}}\sqrt{1-\frac{2}{N}} & -1+\frac{4}{N} \end{pmatrix} \end{aligned} \tag{6.82}$$

From the previous section we know that this matrix can be easily diagonalized, with eigenvalues:

$$\lambda_\pm = \Big(1-\frac{4}{N}\Big) \pm i\Big(2\sqrt{\frac{2}{N}}\sqrt{1-\frac{2}{N}}\Big) \tag{6.83}$$

and eigenvectors:

$$|v_\pm\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ \pm i \end{pmatrix} \tag{6.84}$$

At this point, we now know the complete spectral decomposition of O:

$$O = -|w_-\rangle\langle w_-| + \lambda_+ |v_+\rangle\langle v_+| + \lambda_- |v_-\rangle\langle v_-| + |R\rangle\langle R| \tag{6.85}$$

where $|R\rangle\langle R|$ is the projector on the remainder superposition of the Hilbert space orthogonal to the ensemble $(|0\rangle, |w_+\rangle, |w_-\rangle$, where O will act as an identity:

$$O|R\rangle = (I-2|0\rangle\langle 0|)(I-2|w_+\rangle\langle w_+|-2|w_-\rangle\langle w_-|)|R\rangle = (I-2|0\rangle\langle 0|)|R\rangle = |R\rangle \tag{6.86}$$

We can now easily apply O to a generic state of the computational basis $|b\rangle$.
Firstly, we can decompose $|b\rangle$ on the span$\{|0\rangle, |u_+\rangle, |w_-\rangle\}$. Due to the non completeness of this span, we will also need to add a $|R\rangle$ vector.
The general decomposition of $|b\rangle$ will be the following:

$$|b\rangle = \alpha|0\rangle + \beta|u_+\rangle + \gamma|w_-\rangle + \delta|R\rangle \tag{6.87}$$

We suppose that $b \neq 0$, so it is immediate that $\alpha = 0$.
β and γ can be derived explicitly:

$$\begin{aligned} \beta = \langle u_+|b\rangle = \frac{\langle w_+|b\rangle}{\Big(\sqrt{1-\frac{2}{N}}\Big)} &= \frac{\sqrt{N}}{\sqrt{N-2}}\frac{\langle x_1|H|b\rangle + \langle x_2|H|b\rangle}{\sqrt{2}} = \\ = \frac{\sqrt{N}}{\sqrt{N-2}}\frac{(-1)^{x_1\cdot b}+(-1)^{x_2\cdot b}}{\sqrt{2N}} \end{aligned} \tag{6.88}$$

We now define:

$$\sigma_i := (-1)^{x_i\cdot b}, \sigma_\pm = \frac{\sigma_1 \pm \sigma_2}{2} \tag{6.89}$$

We can then rewrite β as:

$$\beta = \frac{\sqrt{2}\sigma_+}{\sqrt{N-2}} \tag{6.90}$$

with a similar argument we can derive γ:

$$\gamma = \langle w_-|b\rangle = \frac{\langle x_1|H|b\rangle - \langle x_2|H|b\rangle}{\sqrt{2}} = \frac{\sqrt{2}\sigma_-}{\sqrt{N}} \tag{6.91}$$

If we now sum the square of γ and β, it is immediate that they do not sum to 1, justifying the necessity for vector $|R\rangle$. We can then derive δ:

$$\delta = \sqrt{1-|\gamma|^2-|\beta|^2} = \sqrt{1-\frac{2\sigma_+^2}{N-2}-\frac{2\sigma_+^2}{N-2}} \tag{6.92}$$

By definition, $|R\rangle$ will be the vector where O acts as an identity, or in other terms, the eigenvector of eigenvalue 1 of O.
Therefore, $|R\rangle \perp |\lambda_-\rangle, |\lambda_+\rangle, |w_-\rangle$.

6.3.2 Auxiliary state: $|b\rangle$

After t iterations of O, we can study its effect on the generic state $|b\rangle$. We will use the same scheme as the previous section, studying operator $(-1)^t HO^t$:

$$\begin{aligned}
&O^t = \begin{pmatrix} \mathrm{Re}(\lambda_+^t) & -\mathrm{Im}(\lambda_+^t) \\ \mathrm{Im}(\lambda_+^t) & \mathrm{Re}(\lambda_+^t) \end{pmatrix} = \begin{pmatrix} r & -i \\ i & r \end{pmatrix} \\
&\left|b^F\right\rangle := (-1)^t HO^t|b\rangle = (-1)^t H\Big(\beta O^t|u_+\rangle + \gamma O^t|w_-\rangle + \delta|R\rangle\Big) \\
&= (-1)^t H\Big(\beta(-i|0\rangle + r|u_+\rangle) + \gamma(-1)^t|w_-\rangle + \delta|R\rangle\Big) \\
&= (-1)^t\Big(\beta(-iH|0\rangle + r\sqrt{\frac{N}{N-2}}\Big(\frac{|x_1\rangle+|x_2\rangle}{\sqrt{2}} - \sqrt{\frac{2}{N}}H|0\rangle\Big)\Big) \\
&+ \gamma(-1)^t\Big(\frac{|x_1\rangle-|x_2\rangle}{\sqrt{2}}\Big) + \left|R'\right\rangle\Big)
\end{aligned} \tag{6.93}$$

Obtained this final state, we can project it onto the solution subspace.
Given that $P = |x_1\rangle\langle x_1| + |x_2\rangle\langle x_2|$, we can study separately the two projections on the two solutions:

$$\xrightarrow{|x_1\rangle\langle x_1|} (-1)^t\Big(\beta(-i\frac{1}{\sqrt{N}} + r\sqrt{\frac{N}{N-2}}\Big(\frac{1}{\sqrt{2}} - \sqrt{\frac{2}{N}}\frac{1}{\sqrt{N}}\Big) + \gamma\frac{(-1)^t}{\sqrt{2}}\Big)|x_1\rangle \tag{6.94}$$

$|R'\rangle$ vanished because $\delta\langle x_1|H|R\rangle = \delta\langle w_1|R\rangle = 0$. This can be explained with the following scheme:

$$\begin{cases} \langle w_-|R\rangle = \langle x_1|H|R\rangle - \langle x_2|H|R\rangle = 0 \\ \langle u_+|R\rangle = -\langle w_+|R\rangle = \langle x_1|H|R\rangle + \langle x_2|H|R\rangle = 0 \end{cases} \tag{6.95}$$

the only possible solution is therefore:

$$\langle x_1|H|R\rangle = \langle x_2|H|R\rangle = 0 \tag{6.96}$$

The projection of our final state on $|x_2\rangle\langle x_2|$ is almost the same as the previous one, with a minor change in the sign of the coefficient γ:

$$\xrightarrow{|x_2\rangle\langle x_2|} (-1)^t\Big(\beta(-i\frac{1}{\sqrt{N}}+r\sqrt{\frac{N}{N-2}}\Big(\frac{1}{\sqrt{2}}-\sqrt{\frac{2}{N}}\frac{1}{\sqrt{N}}\Big)-\gamma\frac{(-1)^t}{\sqrt{2}}\Big)|x_2\rangle \tag{6.97}$$

Due to the orthogonality of the two solution states $|x_1\rangle, |x_2\rangle$, we can easily compute the success probability:

$$\begin{aligned}
&A := \beta(-i\frac{1}{\sqrt{N}}+r\sqrt{\frac{N}{N-2}}\Big(\frac{1}{\sqrt{2}}-\sqrt{\frac{2}{N}}\frac{1}{\sqrt{N}}\Big)\Big) \quad B := \gamma\frac{(-1)^t}{\sqrt{2}} \quad c := \sqrt{1-\frac{2}{N}}\\
&||P\left|b^f\right\rangle||^2 = \left\langle b^f\right|P\left|b^f\right\rangle = |A+B|^2+|A-B|^2\\
&= 2|A|^2+2|B|^2 = 2|\beta|^2\Big(-\frac{\sin(N\theta_k)}{\sqrt{N}}+\cos(N\theta_k)\frac{c}{\sqrt{2}}\Big)^2+|\gamma|^2\\
&= \frac{4\sigma_+^2}{N-2}\Big(-\frac{\sin(N\theta_k)}{\sqrt{N}}+\cos(N\theta_k)\frac{c}{\sqrt{2}}\Big)^2+\frac{2\sigma_-^2}{N} = p_b
\end{aligned} \tag{6.98}$$

We now move to the analysis of state $|0\rangle$. The action of O^t on it is immediate:

$$\begin{aligned}
&(-1)^t HO^t|0\rangle = (-1)^t H(r|0\rangle + i|u_+\rangle)\\
&= (-1)^t\Big(rH|0\rangle + i\frac{1}{\sqrt{1-\frac{2}{N}}}\Big(\frac{|x_1\rangle+|x_2\rangle}{\sqrt{2}}-\sqrt{\frac{2}{N}}H|0\rangle\Big)\Big)\\
&= (-1)^t\Big(H|0\rangle(r-\frac{i\sqrt{2}}{\sqrt{N-2}})+\frac{i\sqrt{N}}{\sqrt{N-2}}\Big(\frac{|x_1\rangle+|x_2\rangle}{\sqrt{2}}\Big)\Big)
\end{aligned} \tag{6.99}$$

As we did before, we can project this final state on the solution subspace:

$$\xrightarrow{|x_1\rangle\langle x_1|} (-1)^t\Big(\frac{1}{\sqrt{N}}(r-\frac{i\sqrt{2}}{\sqrt{N-2}})+\frac{i\sqrt{N}}{\sqrt{N-2}}\frac{1}{\sqrt{2}}\Big)|x_1\rangle \tag{6.100}$$

The projection on $|x_2\rangle\langle x_2|$ is exactly the same, resulting in the following success probability:

$$\begin{aligned}
&p_0 = 2\Big(\frac{\cos(t\theta_k)}{\sqrt{N}}+\frac{1}{\sqrt{2}}\sqrt{1-\frac{2}{N}}\sin(t\theta_k)\Big)^2\\
&\text{using that } a\cdot\cos(x)-b\cdot\sin(x)=\sqrt{a^2+b^2}\cos(x+\delta), \quad \delta=\arctan\Big(\frac{b}{a}\Big)\\
&p_0 = \cos^2(t\theta_k-\delta_k), \quad \delta=\arctan\Big(\sqrt{\frac{N}{2}-1}\Big)
\end{aligned} \tag{6.101}$$

It is interesting to note that the success probability associated to $\left|b^F\right\rangle$ actually depends on the parity of the solutions $|x_1\rangle, |x_2\rangle$ compared to $|b\rangle$.
Indeed:

$$p_b = \begin{cases} \frac{2}{N} & \text{if } x_1\cdot b = x_2\cdot b\\ \frac{4}{N-2}\Big(-\frac{\sin(t\theta_k)}{\sqrt{N}}+\cos(t\theta_k)\frac{c}{\sqrt{2}}\Big)^2 & \text{if } x_1\cdot b \neq x_2\cdot b \end{cases} \tag{6.102}$$

For the entangled success probability we need to study the following function p_E (which again, can be derived from Eq.3.24, using that $P = \sum_j |x_j\rangle\langle x_j|$), in two different cases:

$$p_E = p_{1,0} + p_{2,0} + p_{1,b} + p_{2,b} - p_{1,0}p_{2,b} - p_{2,0}p_{1,b} + 2\sqrt{p_{1,b}p_{1,0}p_{2,0}p_{2,b}} \tag{6.103}$$

We have found that the success probability associated with $|0\rangle$ is independent of the chosen solution, therefore $p_{1,0} = p_{2,0} = \frac{p_D}{2}$. Moreover, after choosing the symmetry of the solutions, we also have that $p_{1,b} = p_{2,b} = \frac{p_b}{2}$.
However, it is important to note that the interference term $\sqrt{p_{1,b}p_{1,0}p_{2,0}p_{2,b}} = 0$ in the antisymmetric case $\sigma_1 \neq \sigma_2$, due a different sign in the expression of $\sigma_\pm$.
This result greatly simplifies our p_E:

$$p_E = \begin{cases} p_D + p_b - 2p_D p_b, & \text{if } \sigma_1 \neq \sigma_2 \\ p_D + p_b, & \text{if } \sigma_1 = \sigma_2 \end{cases} \tag{6.104}$$

The final success probability is then computed as:

$$p_E = \begin{cases} \cos^2(t\theta_k - \delta_k)\Big(1 - \dfrac{4}{N}\Big) + \dfrac{2}{N}, & \text{if } \sigma_1 \neq \sigma_2, \\ \dfrac{1}{2} + \dfrac{1}{2N(N-2)} - (N-4)^2 \cos\big(2t\theta_k\big) & \\ \quad + 2\sqrt{2}(N-4)\sqrt{N-2}\,\sin\big(2t\theta_k\big), & \text{if } \sigma_1 = \sigma_2. \end{cases} \tag{6.105}$$

To understand what is θ_k, we can follow the same reasoning of the previous section and find that $\theta_k = 2\theta_a$, the initial angle linked to the success probability before the oracle's action. Specifically, in the two solution case we will have that:

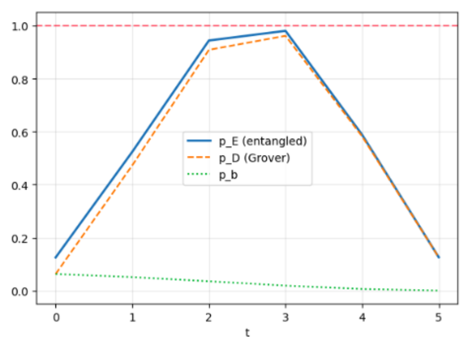
$$\begin{aligned}
&\sin^2(\theta_a) = \frac{2}{N} \longrightarrow \theta_a = \arcsin\left(\sqrt{\frac{2}{N}}\right) \\
&\cos(\theta_a) = \sqrt{1 - \frac{2}{N}} \\
&\tan(\theta_a) = \sqrt{\frac{2}{N-2}} \longrightarrow \theta_a = \arctan\left(\sqrt{\frac{2}{N-2}}\right) \\
&\arctan\left(\sqrt{\frac{N-2}{N}}\right) = \arctan\left(\frac{1}{\tan(\theta_a)}\right) = \arctan(\cot(\theta_a)) = \frac{\pi}{2} - \theta_a \\
&\cos^2(t\theta_k - \delta_k) = \cos^2(2t\theta_a - \frac{\pi}{2} + \theta_a) = \cos^2((2t+1)\theta_a - \frac{\pi}{2}) = \sin^2((2t+1)\theta_a)
\end{aligned} \tag{6.106}$$

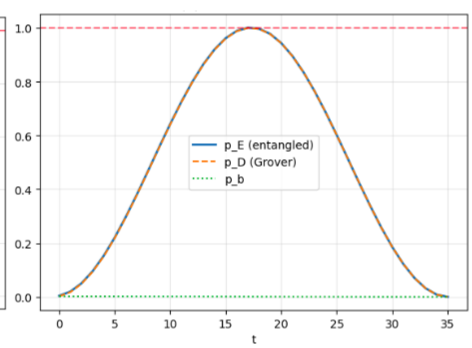
We have rightfully found that our success probability on $|0\rangle$ is exactly Grover's one with two solutions, showing that our method is correct.
This results tells us that if $\sigma_1 \neq \sigma_2$ there will be a reduction in the overall success probability, due to the lack of amplification in p_b, that remains equal to the starting one.

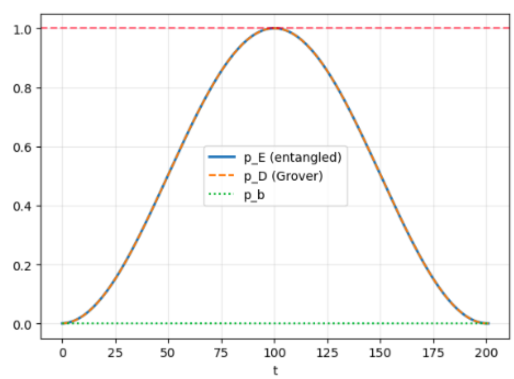
In the symmetric case we have a slightly more complex function. In order to study the asymptotic complexity in this case, we note that:

$$p_E - p_D = p_b = \frac{4}{N-2}\Big(-\frac{\sin(t\theta_k)}{\sqrt{N}} + \cos(t\theta_k)\frac{c}{\sqrt{2}}\Big)^2 \tag{6.107}$$

It is immediate to see that the dominant term, just like the previous case, has a complexity of $O(\frac{1}{N^2})$, showing no asymptotic improvement compared to the single-solution case. We can verify it numerically as well:







k	**N=**N	p_E	p_D	$\Delta p = p_E - p_D$
5	32	0.980	0.961	0.019
10	1024	0.9966	0.9957	0.0009
15	32768	0.9998	0.9997	0.0001

Table 6.3: Success probability comparison with k=5,10,15

By creating a plot of $\log(p_E - p_D)$ vs $\log(N)$, we observe an exact $O(\frac{1}{N^2})$ trend:

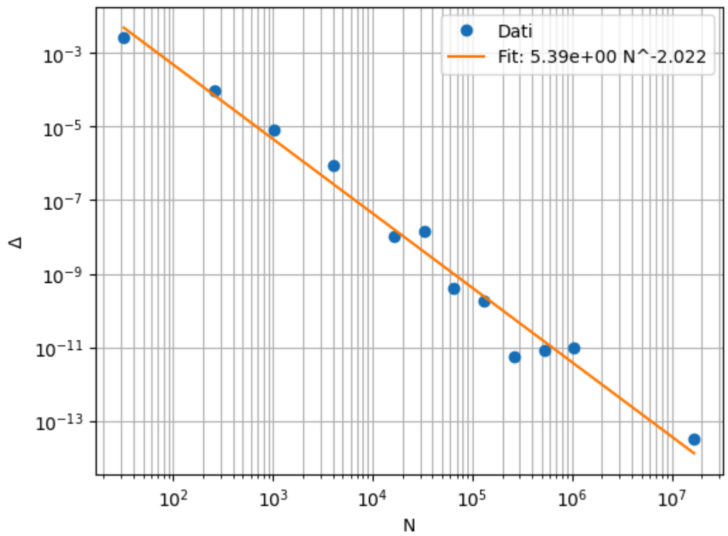


Figure 6.6: Caption

obtaining from the fit the following value:

$$\alpha = -2.02 \pm 0.09, \quad \log(p_E - p_D) \propto \alpha \log(N) \tag{6.108}$$

6.3.3 Auxiliary state: $H|0\rangle$

We can now move to the analysis of the second initial state in the multiple solutions system regime.
The first step is, as always, the decomposition of $H|0\rangle$ on span$\{|0\rangle, |u_+\rangle, |w_-\rangle, |R\rangle\}$:

$$H|0\rangle = \alpha|0\rangle + \beta|u_+\rangle + \gamma|w_-\rangle + \delta|R\rangle \tag{6.109}$$

It can be easily shown that $\gamma = 0$. In general:

$$\langle w_\pm|H|0\rangle = \frac{1}{\sqrt{2}}(\langle x_1|HH|0\rangle \pm \langle x_2|HH|0\rangle) = \frac{1}{\sqrt{2}}(\langle x_1|0\rangle \pm \langle x_2|0\rangle) = 0 \tag{6.110}$$

Regarding the other coefficients we obtain:

$$\begin{aligned}
\alpha &= \langle 0|H|0\rangle = \frac{1}{\sqrt{N}} \\
\beta &= \langle u_+|H|0\rangle = \sqrt{\frac{N}{N-2}}(\langle w_+| - \sqrt{\frac{2}{N}}\langle 0|)H|0\rangle = \\
&= \sqrt{\frac{N}{N-2}}(-\sqrt{\frac{2}{N}}\frac{1}{\sqrt{N}}) = \frac{-\sqrt{2}}{\sqrt{N(N-2)}} \\
\delta &= \sqrt{1-|\alpha|^2-|\beta|^2} = \sqrt{1-\frac{1}{N-2}}
\end{aligned} \tag{6.111}$$

We can now apply our operator $(-1)^t HO^t$ on $H|0\rangle$:

$$\begin{aligned}
(-1)^t HO^t H|0\rangle &= (-1)^t H\Big(\frac{O^t|0\rangle}{\sqrt{N}} - \frac{\sqrt{2}}{\sqrt{N(N-2)}}O^t|u_+\rangle\Big) + (-1)^t H|R\rangle \\
&= (-1)^t H\Big(\frac{\cos(t\theta_k)}{\sqrt{N}}|0\rangle + \frac{\sin(t\theta_k)}{\sqrt{N}}|u_+\rangle - \\
&\qquad \frac{\sqrt{2}}{\sqrt{N(N-2)}}\Big(-\sin(t\theta_k)|0\rangle + \cos(t\theta_k)|u_+\rangle\Big)\Big) + (-1)^t|R'\rangle \\
&= (-1)^t\Big(H|0\rangle\Big(\frac{\cos(t\theta_k)}{\sqrt{N}} + \frac{\sqrt{2}}{\sqrt{N(N-2)}}\sin(t\theta_k)\Big) \\
&\quad + H|u_+\rangle\Big(\frac{\sin(t\theta_k)}{\sqrt{N}} - \frac{\sqrt{2}}{\sqrt{N(N-2)}}\cos(t\theta_k)\Big)\Big) + (-1)^t|R'\rangle \\
&= (-1)^t\Big(H|0\rangle\Big(\frac{\cos(t\theta_k)}{\sqrt{N}} + \frac{\sqrt{2}}{\sqrt{N(N-2)}}\sin(t\theta_k) - \frac{\sqrt{2}}{\sqrt{N(N-2)}}\sin(t\theta_k) \\
&\quad + \frac{2}{\sqrt{N}(N-2)}\cos(t\theta_k)\Big) + \\
&\quad + \frac{\sqrt{N}}{\sqrt{N-2}}\Big(\frac{|x_1\rangle + |x_2\rangle}{\sqrt{2}}\Big)\Big(\frac{\sin(t\theta_k)}{\sqrt{N}} - \frac{\sqrt{2}}{\sqrt{N(N-2)}}\cos(t\theta_k)\Big)\Big) + (-1)^t|R'\rangle
\end{aligned}$$

$$= (-1)^t \Big(H\,|0\rangle \Big(\frac{\cos(t\theta_k)}{\sqrt{N}} \Big(1 + \frac{2}{N-2} \Big) \Big)$$
$$+ \frac{\sqrt{N}}{\sqrt{N-2}} \Big(\frac{|x_1\rangle + |x_2\rangle}{\sqrt{2}} \Big) \Big(\frac{\sin(t\theta_k)}{\sqrt{N}} - \frac{\sqrt{2}}{\sqrt{N(N-2)}} \cos(t\theta_k) \Big) \Big) + (-1)^t \left| R' \right\rangle \tag{6.112}$$

Projecting this final state onto the solution subspace yields the following results, symmetric for both solutions $|x_1\rangle, |x_2\rangle$:

$$p_{H|0\rangle,i} = \Big| \frac{1}{\sqrt{N}} (\cos(t\theta_k) \frac{\sqrt{N}}{\sqrt{N-2}}) + \frac{\sqrt{N}}{\sqrt{2(N-2)}} (\frac{\sin(t\theta_k)}{\sqrt{N}} - \frac{\sqrt{2}}{\sqrt{N(N-2)}} \cos(t\theta_k)) \Big|^2$$
$$= \Big| \frac{\cos(t\theta_k)}{N-2} + \frac{\sin(t\theta_k)}{\sqrt{2(N-2)}} - \frac{\cos(t\theta_k)}{N-2} \Big|^2 = \frac{\sin^2(t\theta_k)}{2(N-2)}, \quad i = \{1,2\} \tag{6.113}$$

From this result, it is clear that the complete success probability associated with the two-solution system is exactly the same of the previous section, with just a minor difference in the denominator, which follows a structure like $(N-m)$, where m is the number of solutions in the system.

In order to study the entangled scenario, we need to compute the following probability:

$$p_E = \frac{1}{1 + \cos(\theta) |\langle 0| H |0\rangle|^2} (\left\langle 0^F \right| P \left| 0^F \right\rangle + \left\langle \psi^F \right| P \left| \psi^F \right\rangle - \left\langle 0^F \right| P \left| 0^F \right\rangle \left\langle \psi^F \right| P \left| \psi^F \right\rangle$$
$$+ cos(\theta) (\left\langle 0^F \right| P \left| \psi^F \right\rangle \langle \psi | 0 \rangle + \left\langle \psi^F \right| P \left| 0^F \right\rangle \langle 0 | \psi \rangle - \left\langle 0^F \right| P \left| \psi^F \right\rangle \left\langle \psi^F \right| P \left| 0^F \right\rangle)$$
$$= \frac{1}{1 - \frac{1}{N}} (p_0 + p_{H|0\rangle} - p_0 p_{H|0\rangle} + \cos(\theta) (\frac{1}{\sqrt{N}} (\left\langle 0^F \right| (|x_1\rangle\langle x_1| + |x_2\rangle\langle x_2|) \left| \psi^F \right\rangle$$
$$+ \left\langle \psi^F \right| (|x_1\rangle\langle x_1| + |x_2\rangle\langle x_2|) \left| 0^F \right\rangle \frac{1}{\sqrt{N}} - |\left\langle 0^F \right| (|x_1\rangle\langle x_1| + |x_2\rangle\langle x_2|) \left| \psi^F \right\rangle|^2) \tag{6.114}$$

Using again that $p_D = 2p_{1,0} = 2p_{2,0}$, $p_b = 2p_{1,b} = 2p_{2,b}$ and $|\left\langle 0^F \right| (|x_1\rangle\langle x_1| + |x_2\rangle\langle x_2|) \left| \psi^F \right\rangle|^2 = p_{1,0}p_{1,H|0\rangle} + p_{2,0}p_{2,H|0\rangle} + 2\sqrt{p_{1,0}p_{1,H|0\rangle}p_{2,0}p_{2,H|0\rangle}} = p_{1,0}p_{1,H|0\rangle} + p_{2,0}p_{2,H|0\rangle} + 2p_{1,0}p_{1,H|0\rangle} = 4p_{1,0}p_{1,H|0\rangle} = p_D p_{H|0\rangle}$, we obtain:

$$p_E = \frac{\Big(\sin^2((2t+1)\theta_a) + \frac{\sin^2(2t\theta_a)}{N-2} - \frac{2}{\sqrt{N}} \frac{\sin((2t+1)\theta_a)}{\sqrt{2}} \frac{\sin(2t\theta_a)}{\sqrt{2(N-2)}} \Big)}{1 - \frac{1}{N}}$$
$$= \frac{\Big(\sin^2((2t+1)\theta_a) + \frac{\sin^2(2t\theta_a)}{N-2} - 2\sin((2t+1)\theta_a) \frac{\sin(2t\theta_a)}{\sqrt{N(N-2)}} \Big)}{1 - \frac{1}{N}} \tag{6.115}$$

6.3.4 $m \geq 3$ solutions case

The biggest problem for analyzing a generic multiple solutions scenario is finding a clever way to study the invariant plane where O act as a rotation. In the $m = 2$

system it was sufficient creating a diagonal superposition of the Hadamard transform of the two solutions, that created two different vectors $|w_{\pm}\rangle$, where one was orthogonal to $|0\rangle$. However, if the number of solutions is odd, this technique can not be used anymore.
For example, in the $m = 3$ scenario:

$$\begin{aligned} |w_-\rangle &= \frac{H|x_1\rangle - H|x_2\rangle + H|x_3\rangle}{\sqrt{3}} \\ \langle 0|w_-\rangle &= \frac{\frac{1}{\sqrt{N}} - \frac{1}{\sqrt{N}} + \frac{1}{\sqrt{N}}}{\sqrt{3}} = \frac{1}{\sqrt{3N}} \end{aligned} \tag{6.116}$$

this result is also valid in case we use any alternating signs sum of the three solutions. At this point, is clear that another strategy should be used to study this case, in order to build a more efficient superpositions of the solutions vectors.
One possible idea, is to build a superposition of antipodal points on the unitary circle in the C plane:

$$\begin{aligned} |w_m\rangle &:= \frac{1}{\sqrt{k}} \sum_{l=1}^{k} e^{i2\pi m \frac{l}{k}} |\bar{x}_l\rangle = \frac{1}{\sqrt{k}} \sum_{l=1}^{k} e^{i2\pi m \frac{l}{k}} H|x_l\rangle \\ |w_1\rangle &= \frac{1}{\sqrt{k}}(|\bar{x}_1\rangle + ... + |\bar{x}_k\rangle), \quad \text{(Uniform superposition)} \end{aligned} \tag{6.117}$$

The structure of this superpositions is such that, because $\langle 0|\bar{x}_i\rangle = 0, \forall i$, it is immediate that:

$$\begin{aligned} \langle 0|w_i\rangle &= 0 \quad \forall i, 2 \le i \le k \\ \langle 0|w_1\rangle &= \sqrt{\frac{k}{N}} \end{aligned} \tag{6.118}$$

where k is the number of solutions.
With this result, we can study operator O:

$$\begin{aligned} O &= (I - 2|0\rangle\langle 0|)H(I - 2\sum_l |x_l\rangle\langle x_l|)H \\ O &= (I - 2|0\rangle\langle 0|)(I - 2\sum_l |\bar{x}_l\rangle\langle \bar{x}_l|) \\ O &= (I - 2|0\rangle\langle 0|)(I - 2\sum_m |w_m\rangle\langle w_m|) \end{aligned} \tag{6.119}$$

The action of O on every $|w_i\rangle$ is immediate. Specifically:

$$\begin{aligned} O|w_i\rangle &= (I - 2|0\rangle\langle 0|)(I - 2\sum_m |w_m\rangle\langle w_m|)|w_i\rangle \\ &= (I - 2|0\rangle\langle 0|)(-|w_i\rangle) = -|w_i\rangle, \forall i, \quad 2 \le i \le k \\ O|w_1\rangle &= -|w_1\rangle + 2\sqrt{\frac{k}{N}}|0\rangle \end{aligned} \tag{6.120}$$

We have effectively found that all the $|w_i\rangle$, expect the uniform superposition, are eigenvectors of O with eigenvalues -1, while $|w_1\rangle$ lives in the same plane as $|0\rangle$. We can now move with the same type of analysis of the previous sections, applying a Gram-Schmidt process to $\{|0\rangle, |w_1\rangle\}$ in order to find two orthonormal vectors that define a base in the plane where O acts non-trivially:

$$|u_1\rangle = \frac{|w_1\rangle - \sqrt{\frac{k}{N}}\,|0\rangle}{\sqrt{1-\frac{k}{N}}} \tag{6.121}$$

We can now study $O_{[u_1,0]}$:

$$O = (I - 2\,|0\rangle\langle 0|)\Big[I - 2\Big(\sqrt{\frac{k}{N}}\,|0\rangle + \sqrt{1-\frac{k}{N}}\,|u_1\rangle\Big)\Big(\sqrt{\frac{k}{N}}\,\langle 0| + \sqrt{1-\frac{k}{N}}\,\langle u_1|\Big)\Big] \tag{6.122}$$

In matrix form:

$$\begin{aligned} O &= \begin{pmatrix} -1+\frac{2k}{N} & +2\sqrt{\frac{k}{N}}\sqrt{1-\frac{k}{N}} \\ -2\sqrt{\frac{k}{N}}\sqrt{1-\frac{k}{N}} & -1+\frac{2k}{N} \end{pmatrix} \\ \lambda_\pm &= -1 + \frac{2k}{N} \pm i2\sqrt{\frac{k}{N}\Big(1-\frac{k}{N}\Big)} \\ v_\pm &= \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ \pm i \end{pmatrix} \end{aligned} \tag{6.123}$$

The final spectral decomposition of O is then:

$$O = \lambda_+\,|v_+\rangle\langle v_+| + \lambda_-\,|v_-\rangle\langle v_-| + (-1)\sum_{i=2}^{k} |w_i\rangle\langle w_i| + |R\rangle\langle R| \tag{6.124}$$

where, as always, $|R\rangle$ represent the remainder of the Hilbert space where O acts as the identity.
We can now study the decomposition of a generic vector $|b\rangle$ on the eigenbase of O:

$$\begin{aligned} |b\rangle &= \beta\,|u_1\rangle + \sum_i \gamma_i\,|w_i\rangle + \delta\,|R\rangle \\ \langle u_i|b\rangle &= \frac{1}{\sqrt{1-\frac{k}{N}}}\,\langle w_1|b\rangle = \frac{\sqrt{N}}{\sqrt{N-k}}\frac{1}{\sqrt{k}}(\langle x_1|H\,|b\rangle + \ldots + \langle x_k|H\,|b\rangle) = \\ &= \frac{\sqrt{N}}{\sqrt{N-k}}\frac{1}{\sqrt{kN}}((-1)^{x_1\cdot b} + \ldots + (-1)^{x_k\cdot b}) \\ &= \frac{1}{\sqrt{k(N-k)}}\sum_i \sigma_i, \quad \sigma_i = (-1)^{x_i\cdot b} \\ \gamma_i &= \langle w_i|b\rangle = \frac{1}{\sqrt{k}}\sum_l e^{-i2\pi\frac{l}{k}i}\,\langle x_l|H\,|b\rangle = \frac{1}{\sqrt{Nk}}\sum_l e^{-i2\pi\frac{l}{k}i}e^{i\pi x_l b} \end{aligned} \tag{6.125}$$

We can now study the application of $(-1)^t HO^t$ on $|b\rangle$:

$$(-1)^t HO^t|b\rangle = (-1)^t H(\beta(-i|0\rangle + r|u_1\rangle) + (-1)^t \sum_i \gamma_i |w_i\rangle + \delta|R\rangle)$$

$$= (-1)^t(\beta(-iH|0\rangle + r\sqrt{\frac{N}{N-k}}\Big(\frac{\sum_i |x_i\rangle}{\sqrt{k}} - \sqrt{\frac{k}{N}}H|0\rangle\Big) + (-1)^t \sum_i H|w_i\rangle + \delta|R\rangle)$$

$$\xrightarrow{\text{project on } |x_m\rangle\langle x_m|} = (-1)^t\Big(\beta\Big(\frac{-i}{\sqrt{N}} + r\sqrt{\frac{N}{N-k}}\Big(\frac{1}{\sqrt{k}} - \frac{\sqrt{k}}{N}\Big)\Big) + (-1)^t \sum_i \gamma_i \langle x_m|H|x_i\rangle\Big) \tag{6.126}$$

The last term can be simplified:

$$\begin{aligned}\sum_{s=2}^{k} \gamma_s \langle x_m|H|w_s\rangle &= \sum_s \gamma_s \langle x_m|\sum_l e^{i2\pi\frac{l}{k}s}|x_s\rangle = \sum_s \gamma_s e^{i2\pi\frac{l}{k}m} \propto \\ \propto \sum_s \Big(\sum_{l=0}^{k-1} e^{-i2\pi\frac{l}{k}s}(-1)^{x_l\cdot b}\Big)e^{i2\pi\frac{l}{k}m} &= \sum_l (-1)^{x_l\cdot b} \sum_s e^{i2\pi\frac{l}{k}(m-s)}\end{aligned} \tag{6.127}$$

We can now study separately two cases:

$$\sum_s e^{i2\pi\frac{l}{k}(m-s)} = \begin{cases} 0 & m \neq l \\ k & m = l \end{cases} \tag{6.128}$$

This result brings us to the following conclusion:

$$\sum_l (-1)^{x_l\cdot b}(k\delta_{m,l} - 1) = k\sum_l (-1)^{x_l\cdot b}\delta_{m,l} - \sum_l (-1)^{x_l\cdot b} = k(-1)^{x_m\cdot b} - \sum_l \sigma_l \tag{6.129}$$

Finally we can compute the complete success amplitude $\mathscr{A}_{b,m}$:

$$\mathscr{A}_{b,m} = \frac{\sum_l \sigma_l}{\sqrt{k(N-k)}}\Big(\frac{\cos(t\theta_k)}{\sqrt{kN}}\sqrt{N-k} - \frac{\sin(t\theta_k)}{\sqrt{N}}\Big) + \frac{(-1)^t}{k\sqrt{N}}[k(-1)^{x_m\cdot b} - \sum_l \sigma_l] \tag{6.130}$$

In general, we could study three different scenarios:

- all the solutions x_j have the same parity compared to b: $\sum_l \sigma_l = k$
- half the solutions have a certain parity while the other half has the opposite: $\sum_l \sigma_l = \frac{k}{2} - \frac{k}{2} = 0$
- the solutions have mixed parity: $|\sum_l \sigma_l| \leq k$

In order to maximize the success probability, we will study the best case scenario, with all the solution having the same success probability:

$$\mathscr{A}_{b,m} = \frac{k}{\sqrt{k(N-k)}}\Big(\frac{\cos(t\theta_k)}{\sqrt{kN}}\sqrt{N-k} - \frac{\sin(t\theta_k)}{\sqrt{N}}\Big) \tag{6.131}$$

The success probability can be immediately computed:

$$\boxed{p_{b,m} = \frac{k}{(N-k)}\Big(\frac{\cos(t\theta_k)}{\sqrt{kN}}\sqrt{N-k} - \frac{\sin(t\theta_k)}{\sqrt{N}}\Big)^2} \tag{6.132}$$

It is obvious that the $p_{b,m}$ does not actually depends on the specific solution m we are studying, so we can infer that:

$$\left\langle b^f \middle| P \middle| b^f \right\rangle = \sum_m p_{b,m} = kp_{b,m'} = p_b = \frac{k^2}{N-k}\Big(\frac{\cos(t\theta_k)}{\sqrt{kN}}\sqrt{N-k} - \frac{\sin(t\theta_k)}{\sqrt{N}}\Big)^2 \tag{6.133}$$

With $m = 2$ we obtain the same result as the previous section, confirming the correctness of our calculations.

Then, noting that the success probability on $|0\rangle$ after t iterations of our operator is exactly the same as before, we can compute p_E:

$$p_E = p_0 + kp_{b,m'} - kp_0 p_{b,m'} + |\left\langle b^f \middle| P \middle| 0^f \right\rangle|^2 \tag{6.134}$$

where, just like the $m = 2$ solution case, we can easily compute $|\left\langle b^f \middle| P \middle| 0^f \right\rangle|^2 = kp_0 p_{b,m'}$.

Now that we have the general formula for the success probability p_b we can study different asymptotic regimes for $p_E - p_0$ as a function of N, the size of the system. Specifically, we obtain the following result from an analytical analysis at the optimal *discrete* time:

Starting from the explicit expression previously obtained for the total contribution p_b,

$$p_b = \frac{k^2}{N-k}\left(-\frac{\sin(t\theta_k)}{\sqrt{N}} + \frac{\cos(t\theta_k)}{\sqrt{k}}\sqrt{1-\frac{k}{N}}\right)^2, \tag{6.135}$$

we can rewrite the term in parentheses in a more compact way. Since

$$\sqrt{1-\frac{k}{N}} = \sqrt{\frac{N-k}{N}}, \tag{6.136}$$

we obtain:

$$p_b = \frac{k^2}{N-k}\left(-\frac{\sin(t\theta_k)}{\sqrt{N}} + \frac{\sqrt{N-k}}{\sqrt{Nk}}\cos(t\theta_k)\right)^2. \tag{6.137}$$

Factoring out $1/\sqrt{N}$, we get

$$p_b = \frac{k^2}{N(N-k)}\left(-\sin(t\theta_k) + \sqrt{\frac{N-k}{k}}\cos(t\theta_k)\right)^2. \tag{6.138}$$

Now define the angle θ_a through

$$\sin\theta_a = \sqrt{\frac{k}{N}}, \qquad \cos\theta_a = \sqrt{\frac{N-k}{N}}. \tag{6.139}$$

Then

$$\sqrt{\frac{N-k}{k}} = \frac{\cos\theta_a}{\sin\theta_a}, \tag{6.140}$$

and therefore

$$\begin{aligned}
&-\sin(t\theta_k) + \sqrt{\frac{N-k}{k}}\cos(t\theta_k) = -\sin(t\theta_k) + \frac{\cos\theta_a}{\sin\theta_a}\cos(t\theta_k)\\
&= \frac{1}{\sin\theta_a}\Big(\cos\theta_a\cos(t\theta_k) - \sin\theta_a\sin(t\theta_k)\Big)\\
&= \frac{\cos(\theta_a + t\theta_k)}{\sin\theta_a}.
\end{aligned} \tag{6.141}$$

Substituting this back, and using $\sin^2\theta_a = k/N$, we finally obtain

$$\boxed{p_b = \frac{k}{N-k}\cos^2\big(\theta_a + t\theta_k\big).} \tag{6.142}$$

This is the form most convenient for the asymptotic analysis.
The continuous optimal Grover time is

$$t_* = \frac{\pi}{4\theta_a} - \frac{1}{2}, \tag{6.143}$$

while the actual discrete time can be written as

$$t = t_* + \epsilon = \frac{\pi}{4\theta_a} - \frac{1}{2} + \epsilon, \qquad \epsilon \in \left[-\frac{1}{2}, \frac{1}{2}\right]. \tag{6.144}$$

At this stage we use the relation

$$\theta_k = 2\theta_a. \tag{6.145}$$

Hence,

$$\begin{aligned}
\theta_a + t\theta_k &= \theta_a + \left(\frac{\pi}{4\theta_a} - \frac{1}{2} + \epsilon\right)\theta_k\\
&= \theta_a + \left(\frac{\pi}{4\theta_a} - \frac{1}{2} + \epsilon\right)2\theta_a\\
&= \frac{\pi}{2} + 2\epsilon\theta_a.
\end{aligned} \tag{6.146}$$

Substituting into the previous formula, one gets

$$p_b = \frac{k}{N-k}\cos^2\!\Big(\frac{\pi}{2} + 2\epsilon\theta_a\Big) = \frac{k}{N-k}\sin^2(2\epsilon\theta_a). \tag{6.147}$$

This is the exact expression at the optimal discrete time.
For $m = o(N)$, one has $\theta_a \to 0$, since

$$\sin\theta_a = \sqrt{\frac{k}{N}} \quad\Longrightarrow\quad \theta_a = \sqrt{\frac{k}{N}} + O\!\left(\left(\frac{k}{N}\right)^{3/2}\right). \tag{6.148}$$

Hence,

$$\sin^2(2\epsilon\theta_a) = 4\epsilon^2\theta_a^2 + O(\theta_a^4) = 4\epsilon^2\frac{k}{N} + O\left(\frac{k^2}{N^2}\right). \tag{6.149}$$

It follows that

$$p_b = \frac{k}{N-k}\left(4\epsilon^2\frac{k}{N} + O\left(\frac{k^2}{N^2}\right)\right). \tag{6.150}$$

Therefore,

$$\boxed{p_E - p_D = p_b = 4\epsilon^2\frac{k^2}{N(N-k)} + O\left(\frac{k^3}{N^2(N-k)}\right).} \tag{6.151}$$

In the sparse regime $m \ll N$, this simplifies to

$$\boxed{p_E - p_D \sim 4\epsilon^2\frac{k^2}{N^2}.} \tag{6.152}$$

This immediately yields the following relevant cases:

- if m is fixed,

$$p_E - p_D = O\left(\frac{1}{N^2}\right); \tag{6.153}$$

- if $m = \sqrt{N}$,

$$p_E - p_D = O\left(\frac{1}{N}\right); \tag{6.154}$$

- more generally, if $m = N^\beta$ with $0 < \beta < 1$,

$$p_E - p_D = O\left(N^{2\beta-2}\right); \tag{6.155}$$

- if $m = \alpha N$, with $0 < \alpha < 1$ constant, then $\theta_a = \arcsin\left(\sqrt{\alpha}\right)$ is also constant, and Eq. (6.147) gives

$$\boxed{p_E - p_D = \frac{\alpha}{1-\alpha}\sin^2\left(2\epsilon\ \arcsin\sqrt{\alpha}\right),} \tag{6.156}$$

  which is of order $O(1)$.

Hence, at the optimal discrete time, the advantage $p_E - p_0$ is asymptotically governed by the scaling of m with N: it is negligible as $O(N^{-2})$ for fixed m, becomes $O(N^{-1})$ for $m \sim \sqrt{N}$, and remains constant when m is proportional to N. This results were also confirmed numerically, as it can seen from the following graphs:

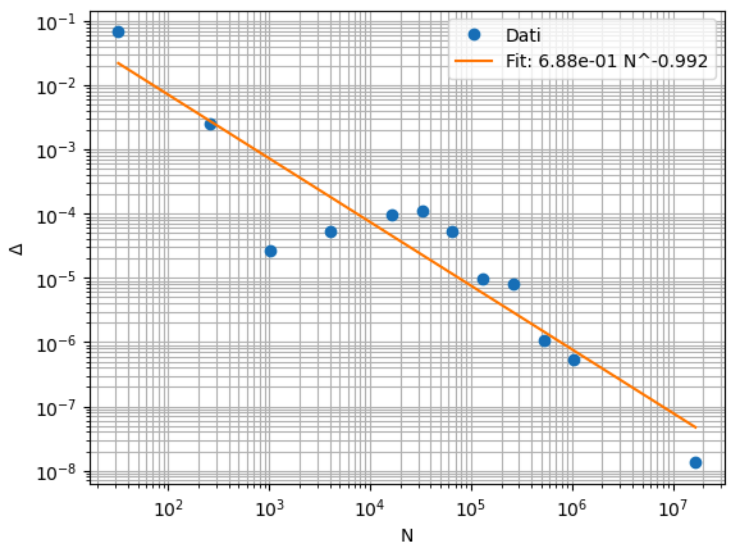


Figure 6.7: $\log(p_E - p_D) \propto \log(N)$ fit with $m \propto \sqrt{N}$ solutions

Another possible way of studying the advantage introduced by the initial entangled state is to compare the difference $p_E - p_D$ with the quantity $1 - p_D$. It is well known that Grover algorithm at the perfect continuous value of t_{opt} is such that $p_D = 1$, but with a discrete number of application of O, we will have a residual gap between p_D and 1. Therefore, we can ask ourselves if this gap can be adjusted by the usage of an initial entangled state:

$$R := \frac{p_E - p_D}{1 - p_D} = \frac{\frac{k}{N-k}\cos^2((2t+1)\theta_a)}{1 - \sin^2((2t+1)\theta_a)} = \frac{k}{N-k} \tag{6.157}$$

It is clear that the ratio R depends only by the number of solutions compared to N:

- if $m << N$, the ratio $R << 1$, so there is no advantage (this is the case where the scaling of $p_E - p_D$ goes to 0 as $O(\frac{1}{N^2})$)
- if $m \propto \sqrt{N}$, the ratio $R \propto \frac{1}{\sqrt{N}}$, so the advantage will still be small and negligible for $N \to \infty$
- in general, if $m \propto N^\gamma$, $\frac{1}{2} < \gamma < 1$, we will have $R = N^{\gamma - 1}$
- the last case is for $m \propto N$, where the ratio will actually remain constant, defining a regime where the entangled state introduces a stable compensation of the p_D gap

Lastly, it is interesting to analyze this problem from a different viewpoint. While both the entangled state and the uniform one reach their maximum success probability after the same number of steps, we need to actually address that the actual number of queries to the oracle in the entangled scenarios is *twice* that of the one in the single register case. The reason is that we are actually evolving two registers with two tensor product operators, that independently perform calls to the same oracle. Then, remembering that $p_E(t) = p_D(t) + \frac{k}{N-k}\Big(1 - p_D(t)\Big)$, one could argue that a complete analysis would require also the study of the following equation:

$$p_D(t_{opt}) - p_E\Big(\frac{t_{opt}}{2}\Big) = p_D(t_{opt}) - p_D\Big(\frac{t_{opt}}{2}\Big) - \frac{k}{N-k}\Big(1 - p_D\Big(\frac{t_{opt}}{2}\Big)\Big) \tag{6.158}$$

By calculating $p_E\Big(\frac{t_{opt}}{2}\Big)$, we are comparing two success probability obtained after the exact same number of queries. Recalling equation (6.158):

$$\Delta_{\text{cont}} := p_D(t_{opt}) - p_D\left(\frac{t_{opt}}{2}\right) - \frac{k}{N-k}\left(1 - p_D\left(\frac{t_{opt}}{2}\right)\right), \tag{6.159}$$

where t_{opt} is the continuous time maximizing $p_D(t)$. The maximum of $p_D(t)$ is obtained when:

$$(2t_{opt} + 1)\theta = \frac{\pi}{2}, \tag{6.160}$$

hence

$$t_{opt} = \frac{\pi}{4\theta} - \frac{1}{2}. \tag{6.161}$$

At this time,

$$p_D(t_{opt}) = \sin^2\left(\frac{\pi}{2}\right) = 1. \tag{6.162}$$

We now evaluate the function at half the optimal time:

$$p_D\left(\frac{t_{opt}}{2}\right) = \sin^2\left(\left(2\frac{t_{opt}}{2} + 1\right)\theta\right) = \sin^2\big((t_{opt} + 1)\theta\big). \tag{6.163}$$

Using the expression for t_{opt}, we obtain

$$(t_{opt} + 1)\theta = \left(\frac{\pi}{4\theta} - \frac{1}{2} + 1\right)\theta = \frac{\pi}{4} + \frac{\theta}{2}. \tag{6.164}$$

Therefore,

$$p_D\left(\frac{t_{opt}}{2}\right) = \sin^2\left(\frac{\pi}{4} + \frac{\theta}{2}\right). \tag{6.165}$$

Using the trigonometric identity

$$\sin^2\left(\frac{\pi}{4} + x\right) = \frac{1 + \sin(2x)}{2}, \tag{6.166}$$

with $x = \theta/2$, we get

$$p_D\left(\frac{t_{opt}}{2}\right) = \frac{1 + \sin\theta}{2}. \tag{6.167}$$

Since

$$\sin\theta = \sqrt{\frac{k}{N}}, \tag{6.168}$$

it follows that

$$p_D\left(\frac{t_{opt}}{2}\right) = \frac{1+\sqrt{k/N}}{2}. \tag{6.169}$$

Substituting into Δ_{cont}, we find

$$\Delta_{\text{cont}} = 1 - \frac{1+\sqrt{m/N}}{2} - \frac{k}{N-k}\left(1 - \frac{1+\sqrt{k/N}}{2}\right) \tag{6.170}$$

$$= \frac{1-\sqrt{k/N}}{2}\left(1 - \frac{k}{N-k}\right). \tag{6.171}$$

Now,

$$1 - \frac{k}{N-k} = \frac{N-2k}{N-k}, \tag{6.172}$$

so that

$$\boxed{\Delta_{\text{cont}} = \frac{1-\sqrt{k/N}}{2}\,\frac{N-2k}{N-k}}. \tag{6.173}$$

Equivalently, using

$$1 - \frac{k}{N} = \left(1 - \sqrt{\frac{k}{N}}\right)\left(1 + \sqrt{\frac{k}{N}}\right), \tag{6.174}$$

one obtain the following equation:

$$\boxed{\Delta_{\text{cont}} = \frac{1-2k/N}{2\left(1+\sqrt{k/N}\right)}} \tag{6.175}$$

It is interesting to analyze, as we did before, the different regimes of this result with different numbers of solutions:

- if $m << N$, $\Delta_{\text{cont}} \simeq \frac{1}{2}$
- if $m = N^{\gamma}, \quad 0 < \gamma < 1$, $\Delta_{\text{cont}} \to \frac{1}{2}, \quad N \to \infty$
- if $m \propto N$, and specifically $m = \frac{N}{2}$, $\Delta_{\text{cont}} = 0$

As it can be seen, in general, the success probability of the standard Grover algorithm will be asymptotically $\frac{1}{2}$ greater than the entangled one evaluated at half the oracle queries, with the only exception being when the number of solutions is half the number of total states in the system. But this result does not surprise us: from the graph we studied with $m = 5, 10, 15$ qubits, we saw that the p_E and p_D curves were nearly overlapped. Therefore, comparing essentially the same $\sin(\cdot)$ curve at the maximum height and at half the height immediately implies our result, showing that entangled registers can only retain a fair amount of advantage on single register if allowed to completely evolve with double the queries to an oracle.

Concluding Remarks

The central focus of this work was to explore whether entanglement between two quantum registers could provide an enhancement to quantum search success probability.
In the first chapter we illustrated the main features of Grover algorithm, explaining its mathematical structure and we showed how it can be seen as a specific instance of the more general QAA.
In the second chapter we introduced the concept of classical random walk, defining the main parameters used for its study (i.e. mixing time, filling time, dispersion time), moving then to its quantum counterpart, the quantum walk. Specifically, we studied its mathematical structure related to Cayley graph, explaining briefly their mathematical properties. We then described how a quantum walk can be effectively used to create a quantum search algorithm, and we provided some key examples of it, showing also a proof for the non-convergence of the probability distribution through Dirichlet's approximation theorem. Finally, we saw how hitting time in quantum walks is quadratically faster than in the classic version.

By preparing symmetric and anti-symmetric entangled states, we showed how interference can amplify the success probability of a search algorithm in the latter case, giving us the idea to study more closely this scenario. Moreover, we retraced the main ideas behind the general spatiallly-constraint quantum search algorithm developed by S.Aaronson and A.Ambainis, explaining its mathematical framework and notable assumptions, that we later on used for our own model.
In the last chapter we focused exclusively on our results, studying both analytical and numerical solutions. Initially we studied the single-state solution system, with both $|b\rangle$ and $H|0\rangle$ as an ancilla state. We found a way to diagonalize our oracle in an invariant $2D$ subspace, where our operator act as a rotation as it does in classic Grover algorithm. Moreover, we have found that in both cases, the advantage induced by entanglement vanishes for large-size systems, specifically as $O(N^{-2})$ for $|b\rangle$ and $O(N^{-3})$ for $H|0\rangle$. In the multiple solution systems we did the same routine, using as an ancilla state both $|b\rangle, H|0\rangle$, despite the more complex mathematical structure of the solution subpspace. Firstly, we tested the $m=2$ case, and using a symmetric and antisymmetric combinations of the solution states, we managed to diagonalize our operators in such a way that allowed us to easily study its effects. We identified in this case, as in the previous one, that the entangled-induced advan-

tage decays as $O(N^{-2})$ while using $|b\rangle$ as an auxiliary state and as $O(N^{-3})$ for $H|0\rangle$, with just a minor difference in the denominator for the latter success probability.
Differences with this cases started to emerge by changing the scaling of the number of solutions compared to N. With $m \propto \sqrt{N}$, and a clever way to create a superposition of all the solution states such that they would always have a zero overlap with $|0\rangle$, we found a quadratic improvement in the entangled induced advantage, that now decayed $O(N^{-1})$ while using $|b\rangle$ as an auxiliary state. This advantage could be further enhanced by using a more general $m \propto N^{\gamma}, \quad 1/2 \leq \gamma \leq 1$, obtaining a decay of the advantage of $O(N^{2(\gamma-1)})$. The only regime where the advantage remained constant was when $m \propto N$, in what could be called the "dense" solutions regime (compared to the previous ones that were "sparse"), in which the advantage was an $O(1)$.
Below, a complete table of our results is showed[1]:

m	Combinatorial case		Spatially constrained case
	$\|b\rangle$	$H\|0\rangle$	
1	$O(N^{-2})$	$O(N^{-3})$	$O(N^{-1})$
2	$O(N^{-2})$	$O(N^{-3})$	$O(N^{-1})$
$\sqrt{N}$	$O(N^{-1})$	$O(N^{-2})$	—
$\propto N^{\gamma}$	$O(N^{2(\gamma-1)})$	$O(N^{2(\gamma-3/2)})$	—
$\propto N$	$O(1)$	$O(N^{-1})$	—

Table 6.4: Scaling comparison between the combinatorial and spatially constrained cases.

Finally, under the assumption of maximally entangled initial states and unitary evolution, conditions naturally satisfied in Grover-like algorithms, we proved that the interference term $|\langle\psi| P |\phi\rangle|^2$ vanishes in the limit $N \to \infty$. Consequently, any entanglement-induced interference term becomes negligible for large databases. This result can be interpreted as a no-go theorem for entanglement-assisted speed-up within the standard amplitude amplification framework. While entanglement modifies finite-size behavior and may offer advantages in small systems or specific configurations, it does not alter drastically the performance in quantum search search. The numerical simulations further confirmed this picture.

In spatial search scenarios, the choice of the shift operator plays a decisive role: flip-flop shifts enable positive build-up of amplitude amplification on marked states, whereas moving shifts have the opposite effect, effectively killing any opportunity for amplification. This latter result was proved both analytically and numerically. We remark that entanglement, in this spatial-constraint context, does not overcome structural limits imposed by locality.

[1]For a complete analysis of the multiple solutions case with auxiliary state $H|0\rangle$, we refer to 6.3.4

Overall, this thesis highlights an important conceptual insight: quantum speed-up in search algorithms is fundamentally driven by controlled interference within a low-dimensional $2D$ invariant subspace, rather than by entanglement alone. Entanglement may enrich the structure of the initial state, but without a mechanism that preserves constructive interference at large scale, it cannot give a substantial help in the success probability.

Future research directions may include:

- Keeping the Grover oracle, one may ask the following question: given L available oracle uses, can we construct an algorithm capable of discriminating which one among the $\binom{2^k}{m}$ possible oracles (corresponding to m marked solutions) are the correct one in a specific search problem, and what is the most efficient architecture for distributing these oracle calls?
- Find an analytical solution to the entangled quantum spatial search on the $2D$ lattice

Understanding precisely when entanglement acts as a genuine computational resource, and when it remains a passive resource, remains a central question in quantum information theory[13], and we hope that this results contributes to the knowledge on this topic.

APPENDIX A: Multiple solutions case with auxiliary state $H|0\rangle$

Even though using as an auxiliary state $H|0\rangle$ makes the performance of the entangled quantum search algorithm worse than using a more general $|b\rangle$, it is still interesting to analyze how the difference $p_E - p_D$ changes with different numbers of solutions.
We can start by analyzing how our initial state $H|0\rangle$ is decomposed on the eigenbase of operator O:

$$\begin{aligned} & H|0\rangle = \alpha|0\rangle + \beta|u_+\rangle + \sum_{j=2}^{k}\gamma_j\left|w_j\right\rangle + \delta|R\rangle \\ & \alpha = \langle 0|H|0\rangle = \frac{1}{\sqrt{N}} \\ & \beta = \langle u_+|H|0\rangle = \frac{\sqrt{N}}{\sqrt{N-k}}\Big(\langle w_1| - \sqrt{\frac{k}{N}}\langle 0|\Big)H|0\rangle = -\sqrt{\frac{k}{N(N-k)}} \\ & \gamma_j = \left\langle w_j\middle|H|0\right\rangle = \frac{1}{\sqrt{k}}\Big(\langle x_0|H + \ldots + \langle x_k|H\Big)H|0\rangle = 0 \\ & \delta = \sqrt{1-|\alpha|^2-|\beta|^2} \end{aligned} \tag{6.176}$$

where we assumed, as we did in the $m=2$ section, that $\left|x_j\right\rangle \neq |0\rangle, \forall j$, simplifying greatly the decomposition coefficients.
We can now apply operator $(-1)^t HO^t$ on $H|0\rangle$, obtaining the following result:

$$(-1)^t HO^t H|0\rangle = (-1)^t \frac{\sin(t\theta_k)}{\sqrt{k(N-k)}} = \mathscr{A}_{m,H|0\rangle} \tag{6.177}$$

By noting that $p_{H|0\rangle} = \langle\psi|(\sum_m |x_m\rangle\langle x_m|)|\psi\rangle = \sum_m |\langle x_m|\psi\rangle|^2 = \sum_m \mathscr{A}^2_{m,H|0\rangle}$, we obtain:

$$p_{H|0\rangle} = \frac{\sin^2(2t\theta_a)}{N-k} \tag{6.178}$$

With this result, we can compute the value of p_E as we did in section 6.2.2, obtaining:

$$p_E = \frac{\sin^2((2t+1)\theta_a) + \frac{\sin^2(2t\theta_a)}{N-k} - 2\frac{\sin((2t+1)\theta_a)\sin(2t\theta_a)}{\sqrt{N}\sqrt{N-k}}}{1-\frac{1}{N}} \tag{6.179}$$

By computing $p_E - p_D$, we can study the asymptotic decrease of the entangled induced advantage for $N \to \infty$, and obtain with a bit of trigonometry the following quantity:

$$p_E - p_D = \frac{k}{N(N-1)}\left(\cos(2t\theta_a) - \sqrt{\frac{k}{N-k}}\sin(2t\theta_a)\right)^2, \qquad \sin\theta_a = \sqrt{\frac{k}{N}}. \tag{6.180}$$

Our goal is to study it at the rounded optimal time

$$t^* = \left(\frac{\pi}{4\theta_a} - \frac{1}{2}\right) + \varepsilon, \qquad \varepsilon \in \left[-\frac{1}{2}, \frac{1}{2}\right]. \tag{6.181}$$

Sparse-solutions regime

Assume first that

$$\frac{k}{N} \to 0 \qquad \text{as } N \to \infty. \tag{6.182}$$

Then

$$\theta_a = \arcsin\sqrt{\frac{k}{N}} \to 0, \qquad \tan\theta_a = \sqrt{\frac{k}{N-k}} = \theta_a + O(\theta_a^3). \tag{6.183}$$

Let

$$A := 2t^*\theta_a. \tag{6.184}$$

Using (6.181), we obtain

$$A = 2\left(\frac{\pi}{4\theta_a} - \frac{1}{2} + \varepsilon\right)\theta_a \tag{6.185}$$

$$= \frac{\pi}{2} - \theta_a + 2\varepsilon\theta_a \tag{6.186}$$

$$= \frac{\pi}{2} + \delta, \qquad \delta := (2\varepsilon - 1)\theta_a. \tag{6.187}$$

Since $\delta = O(\theta_a)$, we may use the standard small-angle expansions:

$$\sin A = \sin\left(\frac{\pi}{2} + \delta\right) = \cos\delta = 1 + O(\theta_a^2), \tag{6.188}$$

and

$$\cos A = \cos\left(\frac{\pi}{2} + \delta\right) = -\sin\delta = -\delta + O(\theta_a^3). \tag{6.189}$$

The term inside the square in (6.180) can therefore be written as

$$\cos A - \tan\theta_a \sin A = \big(-\delta + O(\theta_a^3)\big) - \big(\theta_a + O(\theta_a^3)\big)\big(1 + O(\theta_a^2)\big) \tag{6.190}$$

$$= -\delta - \theta_a + O(\theta_a^3). \tag{6.191}$$

Using the definition of δ,

$$\delta + \theta_a = (2\varepsilon - 1)\theta_a + \theta_a = 2\varepsilon\theta_a, \tag{6.192}$$

hence

$$\cos A - \tan\theta_a \sin A = -2\varepsilon\theta_a + O(\theta_a^3). \tag{6.193}$$

Squaring both sides gives

$$(\cos A - \tan\theta_a \sin A)^2 = 4\varepsilon^2\theta_a^2 + O(\theta_a^4). \tag{6.194}$$

Substituting (6.194) into (6.180), we find

$$p_E(t^*) - p_D(t^*) = \frac{k}{N(N-1)}\big(4\varepsilon^2\theta_a^2 + O(\theta_a^4)\big). \tag{6.195}$$

Since in the sparse regime

$$\theta_a^2 \sim \frac{k}{N}, \tag{6.196}$$

it follows that

$$p_E(t^*) - p_D(t^*) = O\left(\frac{k}{N^2}\cdot\frac{k}{N}\right) = O\left(\frac{k^2}{N^3}\right). \tag{6.197}$$

Therefore, in the sparse-solutions regime,

$$\boxed{p_E(t^*) - p_D(t^*) = O\left(\frac{k^2}{N^3}\right).} \tag{6.198}$$

Dense-solutions regime

Let us now consider the dense-solutions regime, namely

$$k = \rho N, \qquad 0 < \rho < 1, \tag{6.199}$$

with ρ fixed as $N \to \infty$. In this case,

$$\sin\theta_a = \sqrt{\rho}, \qquad \cos\theta_a = \sqrt{1-\rho}, \qquad \tan\theta_a = \sqrt{\frac{\rho}{1-\rho}}, \tag{6.200}$$

so θ_a is now a constant independent of N.

Substituting $k = \rho N$ into (6.180), we obtain

$$p_E - p_D = \frac{\rho}{N-1}\left(\cos(2t\theta_a) - \sqrt{\frac{\rho}{1-\rho}}\sin(2t\theta_a)\right)^2. \tag{6.201}$$

Since θ_a and ρ are constant, the quantity inside parentheses is generically $O(1)$. Therefore,

$$p_E - p_D = O\left(\frac{1}{N}\right). \tag{6.202}$$

In particular, at the rounded optimal time t^*, the same conclusion still holds:

$$p_E(t^*) - p_D(t^*) = \frac{\rho}{N-1}\left(\cos(2t^*\theta_a) - \sqrt{\frac{\rho}{1-\rho}}\sin(2t^*\theta_a)\right)^2. \tag{6.203}$$

Because θ_a is constant in this regime, the squared term remains bounded independently of N, and hence

$$\boxed{p_E(t^*) - p_D(t^*) = O\left(\frac{1}{N}\right).} \tag{6.204}$$

We have therefore shown once again that the asymptotic scaling of the quantum advantage depends on the density of marked states. In the sparse-solutions regime, the correction at the rounded optimal time is strongly suppressed:

$$p_E(t^*) - p_D(t^*) = O\left(\frac{k^2}{N^3}\right) \tag{6.205}$$

By contrast, in the dense-solutions regime $k = \rho N$, the angle θ_a no longer tends to zero, and the advantage decays only as

$$p_E(t^*) - p_D(t^*) = O\left(\frac{1}{N}\right). \tag{6.206}$$

Thus, in both cases the advantage vanishes asymptotically, but the suppression is much stronger in the sparse-solutions regime than in the dense one, and even more so compared to the initial state with auxiliary state $|b\rangle$, $b \neq 0$, for the same reasoning we already talked about in section 6.2.2

APPENDIX B: Numerical methods

As we said in 2.4, the quantum search algorithm is difficult to analyze at finite values of N, due to the lack of simplifications that the asymptotic regime brings.
Therefore, in order to study this case on the 2D lattice, we used a Python script to simulate it numerically.
The idea was to simulate the evolution of the walkers using functions defined similarly to the quantum case. In order to implement the idea of a "superposition" of quantum states, we defined a vector divided in four blocks, one for each possible state of the coin:

```
def state_uniform_DD(d, L):
    #Stato uniforme globale |D,D>
    psi = np.ones((d, L, L), dtype=np.complex64)
    psi /= np.sqrt(d * L * L)
    return psi


def state_local_D0(d, L, x0, y0):
    #Stato localizzato |D,(x0,y0)> con moneta uniforme
    psi = np.zeros((d, L, L), dtype=np.complex64)
    psi[:, x0 % L, y0 % L] = 1 / np.sqrt(d)
    return psi
```

Figure 6.8: Uniform and local states

With this implementation, we could essentially simulate the following quantum superposition:

$$|\psi\rangle = \frac{1}{\sqrt{4}}(|N\rangle \otimes |D\rangle + |S\rangle \otimes |D\rangle + |O\rangle \otimes |D\rangle + |E\rangle \otimes |D\rangle) \tag{6.207}$$

On this vector, we applied the operators that compose U': the reflection around the target state R, the coin operator C and the shift operator S. They were coded as the following:

```python
def apply_R_inplace(psi, w):
    #R = I - 2 |D,w><D,w|
    wx, wy = w
    local = psi[:, wx, wy]
    s = local.sum()
    psi[:, wx, wy] -= 2 * s / d


def apply_coin_inplace(psi):
    #Moneta di Grover applicata identicamente a ogni sito
    mean_coin = psi.mean(axis=0)
    psi[:] = 2 * mean_coin[None, :, :] - psi


def apply_shift_with_buffer(psi, buf):

    # Flip-flop shift con condizioni periodiche.
    # Convenzione: 0=up, 1=down, 2=right, 3=left

    # 0: up -> x-1, coin->1
    buf[1] = np.roll(psi[0], -1, axis=0)
    # 1: down -> x+1, coin->0
    buf[0] = np.roll(psi[1], +1, axis=0)
    # 2: right -> y+1, coin->3
    buf[3] = np.roll(psi[2], +1, axis=1)
    # 3: left -> y-1, coin->2
    buf[2] = np.roll(psi[3], -1, axis=1)
    return buf, psi
```

Figure 6.9: Implementation of R,C and S

It was intentionally left the possibility of changing the value of the target state, in order to test different scenarios in the success probability of the entangled state. This probability can change relative to the position of w.
To choose the position of the target, the following script was used:

```python
def torus_distance(x, y, L):
    dx = min(x, L - x)
    dy = min(y, L - y)
    return dx + dy


def pick_point_with_dist(L, target_dist):

    best = None
    best_diff = 1e9

    for x in range(L):
        for y in range(L):
            if x == 0 and y == 0:
                continue
            d = torus_distance(x, y, L)
            diff = abs(d - target_dist)
            if diff < best_diff:
                best_diff = diff
                best = (x, y, d)

    return best


def targets_for_L(L):
    """
    Definisce target near/mid in termini di distanza toroidale.
    """
    # distanza massima
    if L % 2 == 0:
        max_d = L
    else:
        max_d = L - 1

    near_target_dist = 2
    mid_target_dist = max_d / 3.0

    x_n, y_n, d_n = pick_point_with_dist(L, near_target_dist)
    x_m, y_m, d_m = pick_point_with_dist(L, mid_target_dist)

    print(f"L={L}: near=({x_n},{y_n}) d={d_n}, mid=({x_m},{y_m}) d={d_m}")

    return {
        "near": (x_n, y_n),
        "mid":  (x_m, y_m),
    }
```

Figure 6.10: Distance choosing script

The parts of the codes are defined as follows:

- **Torus distance**: The Manhattan distance, the natural choice on the 2D lattice; the $\min(x, L-x)$ is necessary due to the torus periodic conditions that could result in the shortest path between 0 and x as the one that "cross" the boundary

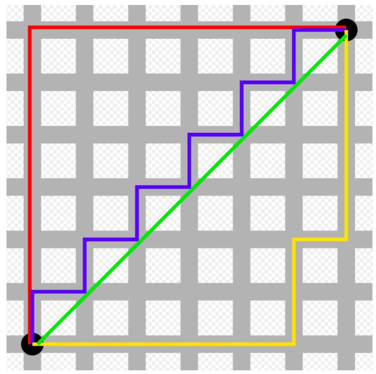


Figure 6.11: The blue, red, and yellow line have all the same length with the Manhattan distance; the green one is the euclidean one, for comparison

- **Picking point with a selected distance from the origin**: this is done by probing all the possible points on the grid and choosing what have the least amount of difference between their distance from the origin and a chosen "best distance" of our choice

- **Defining "near" and "mid" point**: the last script choose two points that have the correct distance from the origin; one "near", where we set the optimal distance heuristically to be 2, and a "mid" one that we set heuristically to $\frac{1}{3}$ of the total length of L

While the uniform superposition on the lattice $|D,D\rangle$ is spread all over the graph, *de facto* independent of the target position, the local state $|D,0\rangle$ is much more susceptible to its change. For this reason, to avoid any biases in the choice of the target state, we used a sample of n points chosen randomly on the graph to have more robust results.
The next part of the code was devoted to apply the QAA script, that was designed as the following:

```python
def qaa_diff_for_target(L, w, m_max, local_pos=(0,0), T_max=None):


    if T_max is None:
        T_max = estimate_T(L)

    _, _, psiD_final = quantum_walk_final_state('DD', L, w, T=T_max)

    _, _, psi0_final = quantum_walk_final_state('D0', L, w, local_pos=local_pos, T=T_max)

    vx, vy = w
    Dv0 = state_D_at_vertex(d, L, vx, vy)

    ms, probs_D = amplitude_amplification(psiD_final, psiD_final, Dv0, w, m_max)

    _, probs_0 = amplitude_amplification(psi0_final, psiD_final, Dv0, w, m_max)

    N = L * L
    pE_curve = compute_pE_curve(probs_D, probs_0, N)

    idx_peak = int(np.argmax(probs_D))

    pD_peak = probs_D[idx_peak]
    pE_peak = pE_curve[idx_peak]
    diff_peak = pE_peak - pD_peak

    return diff_peak
```

Figure 6.12: QAA script for a generic target state

After choosing the size L of the grid, the target position w and the starting node of the localized state (in our case $(0,0)$), the script applied m iterations of an amplitude amplification function, defined as the following:

```python
def apply_Q(psi, psiD_final, Dv0):

    #Q = (I - 2|psiD_final><psiD_final|) (I - 2|D,v0><D,v0|)

    psi = reflection_about(psi, Dv0)
    psi = reflection_about(psi, psiD_final)
    return psi

def amplitude_amplification(psi_init, psiD_final, Dv0, w, m_max):

    psiD_final = normalize_state(psiD_final.copy())
    Dv0 = normalize_state(Dv0.copy())

    psi = psi_init.copy()
    probs = []

    for m in range(m_max + 1):
        p = p_succ(psi, w)
        probs.append(p)
        psi = apply_Q(psi, psiD_final, Dv0)

    ms = np.arange(m_max + 1)
    return ms, np.array(probs)
```

Figure 6.13: QAA script

The first term applied the Q function defined as the unitary operator that applies two reflections, one around the starting state (in our case the evolved state after t iterations of the previous routine $(U')^{t_f}|\psi\rangle$) and one around the target state.
The QAA script for generic target state was used in combination with the random point selections, in order to ensure that as little bias as possible was included.

This page was intentionally left blank

Bibliography

[1] Scott Aaronson and Andris Ambainis. Quantum search of spatial regions. *Theory of Computing*, 1:47–79, 2005.

[2] Dorit Aharonov, Andris Ambainis, Julia Kempe, and Umesh Vazirani. Quantum walks on graphs. In *Proceedings of the 33rd Annual ACM Symposium on Theory of Computing (STOC)*, pages 50–59, 2001.

[3] Andris Ambainis, Julia Kempe, and Alexander Rivosh. Coins make quantum walks faster. *Proceedings of the 16th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 1099–1108, 2005.

[4] John S. Bell. On the einstein podolsky rosen paradox. *Physics*, 1(3):195–200, 1964.

[5] H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani. Strengths and weaknesses of quantum computing. *SIAM Journal on Computing*, 26(5):1510–1523, 1997.

[6] Michel Boyer, Gilles Brassard, Peter Høyer, and Alain Tapp. Tight bounds on quantum searching. *Fortsch.Phys.46:493-506*, 1998.

[7] Gilles Brassard, Peter Høyer, Michele Mosca, and Alain Tapp. Quantum amplitude amplification and estimation. In *Quantum Computation and Information*, pages 53–74. AMS, 2002.

[8] Andrew Childs. Lecture 14: Discrete quantum walk, 2004. Lecture notes.

[9] Andrew Childs, Richard Cleve, Enrico Deotto, Edward Farhi, Sam Gutmann, and Daniel Spielman. Exponential algorithmic speedup by quantum walk. *arXiv:quant-ph/0209131*, 2002.

[10] Andrew M. Childs and Jeffrey Goldstone. Spatial search by quantum walk. *Physical Review A*, 70:022314, 2004.

[11] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC)*, pages 212–219, 1996.

[12] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, 6 edition, 2008.

[13] Richard Jozsa and Noah Linden. On the role of entanglement in quantum computational speed-up. *Proceedings of the Royal Society A*, 459:2011–2032, 2003.

[14] David A. Levin, Yuval Peres, and Elizabeth L. Wilmer. *Markov Chains and Mixing Times*. American Mathematical Society, 2009.

[15] Rajeev Motwani and Prabhakar Raghavan. *Randomized Algorithms*. Cambridge University Press, 1995.

[16] P.Benioff. Space searches with a quantum robot. *AMS Contemporary Mathematics*, 305:1–12, 2002.

[17] Paolo Perinotti. Lecture 20: Cayley graphs and cellular automata, 2024. Lecture notes.

[18] Renato Portugal. *Quantum Walks and Search Algorithms*. Springer, 2013.

[19] Neil Shenvi, Julia Kempe, and K. Birgitta Whaley. A quantum random walk search algorithm. *Physical Review A*, 67:052307, 2003.

[20] Avatar Tulsi. Faster quantum-walk algorithm for the two-dimensional spatial search. *Physical Review A*, 78:012310, 2008. doi: 10.1103/PhysRevA.78.012310.

[21] Salvador Elías Venegas-Andraca. Quantum walks: A comprehensive review. *Quantum Information Processing*, 11:1015–1106, 2012.

[22] Wikipedia contributors. Wikipedia, the free encyclopedia. `https://en.wikipedia.org/wiki/Complete_graph`, 2026.