Quantum walk search algorithm on hypercube : eigenanalysis and calculation of the probability of success in polynomial time

Hugo Pillin

COLLEGE MATHSTIC
DOCTORAL BRETAGNE
BRETAGNE OCEANE

Université de Bretagne Occidentale

CyberIoT
CHAIRE D'EXCELLENCE

THÈSE DE DOCTORAT DE

L'UNIVERSITÉ
DE BRETAGNE OCCIDENTALE

ÉCOLE DOCTORALE N° 644
Mathématiques et Sciences et Technologies
de l'Information et de la Communication en Bretagne Océane
Spécialité : *Télécommunications*

Par
Hugo PILLIN

Quantum walk search algorithm on hypercube

Eigenanalysis and calculation of the probability of success in polynomial time

Thèse présentée et soutenue à Brest, le 5 avril 2024
Unité de recherche : CNRS UMR 6285 Lab-STICC et CNRS UMR 6205 LMBA

Rapporteuses avant soutenance :

Claire GOURSAUD	Maître de Conférences HDR, INSA Lyon
Jingbo WANG	Professor, University of Western Australia

Composition du Jury :

Président :	Yannick DEVILLE	Professeur, Université Toulouse III Paul-Sabatier
Examinateurs :	El-Houssaïn BAGHIOUS	Maître de Conférences, Université de Bretagne Occidentale
	Olivier BERDER	Professeur, IUT Lannion
	Claire GOURSAUD	Maître de Conférences HDR, INSA Lyon
Dir. de thèse :	Gilles BUREL	Professeur, Université de Bretagne Occidentale
Co-dir. de thèse :	Paul BAIRD	Professeur, Université de Bretagne Occidentale

Invités

Roland GAUTIER	Professeur, Université de Bretagne Occidentale
Jean-Marie NICOLAS	Professeur, Université de Bretagne Occidentale
Yannick SAOUTER	Chargé de recherche CNRS, IMT Atlantique
Jingbo WANG	Professor, University of Western Australia

Acknowledgments

And here is the traditional thank-you page. The first page for you and the last for me. The end of the last four years of my life. Four paradoxical years, simultaneously very long and too short, surrounded by colleagues, yet a bit lonely in front of my screen. Four years from which I emerge both proud and tired. Four years to finally arrive at this point, my tiny contribution to science, my thesis. But my thesis is not just mine, because at every stage, from my first steps in the bibliography to the writing of this manuscript, there have been people to guide me, to teach me, to support me, to listen to me. And to all these people, all essential in their own way to the existence of this thesis, and although I am not very good at expressing it, I would simply like to say thank you.

Of course, there can be no thesis without thesis directors, so it is only logical to start with the two initiators of this adventure, Professors Gilles Burel and Paul Baird. To both of you, a huge thank you, for proposing this project, for trusting me more than I trust myself, for proofreading all my mistakes, for redirecting me when I was at a dead end, and above all for inspiring me throughout this thesis. And if the thesis has not been easy for me, it probably has not been for you either. Thank you for your patience in the face of my absolute inability to meet a deadline, and thank you for refocusing me every time I wandered off (that is, very often). Of course, thanks also to my two other supervisors, Roland Gautier and El-Houssain Baghious, for all your help and ideas over the last four years. This thesis is as much yours as it is mine.

Although we do not know each other, I would like to thank the members of the jury, and in particular the reviewers, for agreeing to travel to the depths of Brittany to assess the results of this work, and to examine this manuscript (sorry in advance for the headaches).

I would also like to thank my roommates in office C113, Clément, Cristina, Jean-Baptiste and Zaynab, for the cakes, for the overlong coffee breaks, for the debates that the whole floor could hear and for the moral support when faced with piles of exam papers to correct or when the printer went on strike. Many thanks also to the colleagues in the Informatics department, Alan, Aymeric, Manele, Morgane and Yoann, for this oasis of relaxation every lunchtime. I will miss our Thursday blind tests and our (often fruitless) expeditions in search of a working coffee machine. We will see each other again to celebrate the end of our respective theses.

Next, I would like to thank Dakodoc, the Brest PhD students' association, for getting me out of my home after the difficult period of confinement, for all the people I would never have met, for organizing all these events, from the exceptional popular science event "Science en theizh" to the simplest of gatherings over a drink. There are too many

of you to mention here, but I know you will recognize each other.

More generally, thanks to all my long-time friends, former classmates and role-playing partners, and even those from before, who have seen a lot less of me lately. Hopefully, I will have more time to see you now.

Many thanks to (almost) all the students I have had the pleasure of teaching over the past four years. Over that time, I probably learned as much as you did, and even if I did not always give the easiest or most interesting lessons, I hope that, despite my slight sadism, you will remember our lectures as fondly as I do. In the end, you were my favorite part of the job.

Finally, a huge thank you to my mother (who has put up with me since I was born, which is no mean feat) and my little sister for everything the three of us have been through. Even though we see each other all too rarely, I certainly would not be who I am today without your support. I send you my love. And finally, a word to Lotus, who cannot read these rows (because she is a cat), but whose presence has been vital to me and who quickly realized that her daddy could not work if she was lying on the keyboard.

Contents

Notations **13**

Introduction **17**

1. Notions of quantum information **19**
1.1. Fundamentals of quantum physics 19
1.2. Quantum bits 21
1.2.1. Qubit definition 21
1.2.2. Qubit representation 21
1.2.3. Qubit association 23
1.2.4. Quantum entanglement 23
1.3. Quantum operations 24
1.3.1. Quantum gates and circuits 24
1.3.2. Usual quantum gates 25
1.4. Quantum state measurement 29
1.4.1. Measurement principles 29
1.4.2. Examples of measurements 31
1.4.3. Measurement of entangled states 34
1.5. No-cloning theorem 36

2. Quantum walks **37**
2.1. Formalism and walk on an axis 38
2.2. Walk on hypercube 45

3. Quantum search algorithm **53**
3.1. Quantum Oracle and Grover iteration 53
3.2. Grover's algorithm execution 58
3.3. Hypercube search algorithm 63

4. Eigenanalysis of the hypercube search algorithm **69**
4.1. Search operator eigenspaces 70
4.1.1. Shift operator 70
4.1.2. Coin operator 70
4.1.3. Oracle 72

4.2. Generator matrices . . . 73
4.2.1. Generators G_1, G_2, G_3 . . . 73
4.2.2. Generator G'_3 and its submatrices . . . 75
4.3. Joint eigenspaces . . . 76
4.3.1. Joint eigenspaces of operators C and O . . . 76
4.3.2. Joint eigenspaces of operators S and C . . . 78
4.3.3. Joint eigenspaces of operators S, C and O . . . 79
4.4. Eigenanalysis of the uniform walk . . . 81
4.4.1. Overview of the uniform walk eigenanalysis . . . 81
4.4.2. Detail of the eigenanalysis of the uniform walk . . . 83
4.5. Dimension of the space of interest . . . 88
4.5.1. Overview of the computation of the dimension of the space of interest . . . 88
4.5.2. Detail of the computation of the dimension of the space of interest 89
4.6. Summary of the eigenanalysis . . . 93

5. Search algorithm probability of success calculation 95
5.1. Space of interest eigenanalysis . . . 96
5.1.1. Overview of the space of interest eigenanalysis . . . 96
5.1.2. Detail of the space of interest eigenanalysis . . . 97
5.2. Eigenvalue search in polynomial time . . . 101
5.3. Vector components in the space of interest . . . 103
5.3.1. Overview of the vector component calculation . . . 103
5.3.2. Detail of the vector component calculation . . . 104
5.4. Summary of the probability of success calculation . . . 112

6. Results and perspectives 115
6.1. Probability of success computation procedure . . . 115
6.2. Improvements and applications . . . 118

Conclusion 123

A. Dirac notation 125
A.1. Definition . . . 125
A.2. Properties . . . 126

B. Kronecker tensor product 127

C. Permutation matrices 129

D. SAT problem 131

E. Singular value decomposition 133

List of Figures

1.1. Bloch sphere representation of the qubit $0.8|0\rangle + 0.6e^{i\pi/4}|1\rangle$ 22
1.2. Succession of quantum gates 25
1.3. Association of quantum gates 26
1.4. Symbol and effect of Hadamard gate 26
1.5. Symbol and effect of the Pauli gate 27
1.6. Symbol and effect of the CNOT gate 28
1.7. Symbol and effect of the SWAP gate 29
1.8. Bell circuit 34

2.1. Position probability on the axis after 100 iterations of the walk initialized with $|0\rangle|\downarrow\rangle$ 41
2.2. Comparison of the exact and asymptotic position probabilities of the equation on the axis after 100 iterations 43
2.3. Comparison of the slow position probability P_{slow} and asymptotic position probability on the axis after 100 iterations 44
2.4. Position probability on axis after 100 iterations of the symmetrical walk 45
2.5. 4-dimensional hypercube with numbered vertices and directions 47
2.6. Shift operator S^{CS} for $n = 4$ 48
2.7. Diagonalized shift operator $\widetilde{S}^{\text{CS}}$ for $n = 4$ 49
2.8. Shift operator S for $n = 4$ 50
2.9. Diagonalized shift operator $\widetilde{S}$ for $n = 4$ 51

3.1. Oracle of a $N = 16$ element problem whose solutions are 0, 3 and 6 . . 55
3.2. Grover iteration circuit 56
3.3. Effect of the Grover iteration GO on an arbitrary state $|s\rangle$ in the plane directed by $|s\rangle$ and $|\bar{s}\rangle$ 57
3.4. Circuit for Grover's algorithm 58
3.5. Probability of success $\mathbf{P}(s)$ of Grover's algorithm as a function of M/N 61
3.6. Evolution of the system during Grover's algorithm with $N = 1\,024$ and $M = 25$, in the plane directed by $|s\rangle$ and $|\bar{s}\rangle$ 62
3.7. Evolution over 50 iterations of the probability of success of the hypercube search algorithm for $n = 6$ with a single solution 65
3.8. Evolution over 50 iterations of the probability of success of the hypercube search algorithm for $n = 6$ with a solution 66

3.9. Oracle of a search problem on a hypercube of dimension $n = 4$ with solutions 0, 3 and 6 67

4.1. Operator of the spatial Fourier transform F in $\mathcal{H}$ for $n = 4$ 71
4.2. Generator matrix $G_{1,2,3}$ of a hypercube search problem of dimension $n = 4$ with solutions 0, 3, and 6 74
4.3. Generator matrix G'_3 for $n = 4$ 75
4.4. Operator of the uniform walk U for $n = 4$ 84
4.5. Diagonalized uniform walk operator $\widetilde{U}$ for $n = 4$ 85

6.1. Search for the eigenvalues of U' associated with eigenspaces in $\mathcal{E}$ . . . 116
6.2. Evolution of the probability of success in function of the number of iterations 118
6.3. Comparison of the original and modified hypercube search algorithms for $n = 8$ and $M = 3$ 120
6.4. Comparison of the original and modified hypercube search algorithms for $n = 8$ and $M = 12$ 121

List of Tables

4.1. Generator matrices 77
4.2. Eigenspaces of walk operators 81
4.3. Eigenspaces of the uniform walk operator 87
4.4. Eigenspaces of the search algorithm operator 92

6.1. Non-zero components of vectors $|s\rangle$ and $|u\rangle$ in $\mathcal{E}$ 117

Notations

Symbol	Introduction	Definition
$\mathbb{R}$		Set of real numbers
$\mathbb{C}$		Set of complex numbers
$\mathbb{Z}$		Set of relative integers
$\mathbb{Z}_N$		Set of relative integers in $[0, N-1]$
$\dim(E)$		Dimension of vector space E
$\text{span}(V)$	Sect. 2.1	Space generated by the vectors or columns of the matrices of the set V
$\mathcal{H}$		Hilbert space
$\mathcal{H}^{\text{S}}$		Shift space
$\mathcal{H}^{\text{C}}$		Coin space
$\text{wt}(p)$	Sect. 4.2	Hamming weight of the binary word corresponding to position p
$\oplus$	Sect. 3.1	Modulo 2 addition, exclusive OR
$\mathbin{+\!\!+}$	Sect. 4.2	Horizontal matrix concatenation
z^*		Complex conjugate of z
$A^\intercal$		Transpose matrix of A
$A^\dagger$		Adjoint matrix of A, i.e. transpose and conjugate
$\otimes$	Ann. B	Kronecker tensor product
$A^{\otimes n}$	Eq. (B.3)	Tensor power of A, equivalent to $A \otimes A \otimes \cdots \otimes A$, n times

Symbol	Introduction	Definition
n	Sect. 2.2	Hypercube dimension for a given problem, length of binary words
N	Sect. 2.2	Number of positions on the n-dimensional hypercube, dimension of the $\mathcal{H}^{\mathrm{S}}$ shift space
M	Sect. 3.1	Number of solutions to a given problem
G	Eq. (2.64)	Grover diffusion operator
S	Sect. 2.2	Shift operator
C	Eq. (2.66)	Coin operator
O	Eq. (3.50)	Oracle of a given problem
U	Sect. 2.2	Operator of an oracle-less quantum walk iteration
U'	Eq. (3.55)	Operator of an iteration of the hypercube quantum walk search algorithm
I		Identity matrix of size 2×2
I_N		Identity matrix of size $N \times N$
H	Eq. (1.13)	Hadamard matrix of size 2×2
H_N	Sect. 2.2	Tensor power of the Hadamard matrix, equivalent to $H^{\otimes n}$ with $N = 2^n$
$I_N^{(s)}$	Tab. 4.1	Submatrix of I_N obtained by keeping only the M columns associated with solutions
$H_N^{(s)}$	Tab. 4.1	Submatrix of H_N obtained by keeping only the M columns associated with solutions
$H_N^{(s,w)}$	Tab. 4.1	Submatrix of $H_N^{(s)}$ obtained by keeping only the $\binom{n}{w}$ rows associated with positions of Hamming weight w
$\bar{H}_N$	Sect. 5.2	Unnormalized Hadamard matrix, containing only $+1$ and -1, equivalent to $\sqrt{N}\,H_N$
X	Eq. (1.17)	Pauli X matrix, quantum equivalent of the logical NO
F	Eq. (2.59)	Spatial Fourier transform operator
F_+	Sect. 4.1.1	Submatrix of F constructed by keeping only the columns with signature $\varsigma_i = 1$
F_-	Sect. 4.1.1	Submatrix of F constructed by keeping only the columns with signature $\varsigma_i = -1$

Symbol	Introduction	Definition
Λ	Eq. (4.16)	Matrix defined by $\langle u_n \vert \Lambda = 0$ and $\Lambda^\intercal \Lambda = I_{n-1}$
$\vert u_n \rangle$	Eq. (2.65)	Uniform superposition of n basis states of a n-dimensional Hilbert space
$\vert s \rangle$	Eq. (3.7)	Uniform superposition of a problem solution elements
$\vert \bar{s} \rangle$	Eq. (3.8)	Uniform superposition of a problem non-solution elements
$\mathbf{P}(s)$	Eq. (3.23)	Probability of success, i.e. of measuring an element of the superposition $\vert s \rangle$
E_α^A	Eq. (4.5)	Eigenspace of operator A associated with eigenvalue α
$E_{\alpha,\beta}^{A,B}$	Eq. (4.6)	Joint eigenspace of operators A and B associated with eigenvalues α and β
ς_i	Eq. (4.7)	Signature associated with the i-th dimension of $\mathcal{H}$

Introduction

Since the work of Turing [Tur37] and Von Neumann on the first electronic calculators in the first half of the 20th century, the concept at the core of computers has been the same: the manipulation of units of information, *bits*, materialized by voltages, currents, light intensity or even magnetization in two distinct states. With the invention of the transistor, followed by the integrated circuit, the use of semiconductors, mainly silicon, became the standard for almost all components.

During the same period, the field of quantum mechanics developed, but it was not until 1980 that Benioff proposed the first quantum Turing machine [Ben80]. Shortly afterwards, faced with the difficulty of simulating quantum phenomena on a computer, physicists like Feynman proposed the use of calculators exploiting the properties of quantum mechanics [Fey82]. This was the birth of quantum computing.

Today, quantum computing is still at an early stage. Computers are very limited and expensive, and algorithms are mostly very specific. There are, however, some concrete applications of quantum computing, such as Bennett and Brassard's BB84 quantum cryptography protocol [BB14], which is used in several secure networks and has inspired other quantum cryptography protocols. Another example is Shor's famous algorithm [Sho94], capable of breaking RSA encryption, the most widely used on the Internet. This algorithm opens up new possibilities for cryptological attack, leading to the emergence of the field of "post-quantum" cryptography.

Quantum physics marks a major rupture with previous theories, and implies a complete re-imagining of the computer, from components to algorithms. As the medium of quantum information is subject to different physical laws from classical information, we redefine the bit and the operations that can be performed on it in chapter 1. Readers familiar with quantum information can start directly with chapter 2.

The main subject of study in this work is the hypercube quantum search algorithm, a quantum walk adaptation of Grover's algorithm, one of the most impactful quantum algorithms. The quantum walk concept is presented in chapter 2, Grover's algorithm in chapter 3. These two chapters also introduce many of the notations that will be used later.

As we will see in chapters 1 and 3, a quantum operation is represented by a unitary operator, and the algorithm consists of the repetition of the same operator. An eigenanalysis of the algorithm, presented in chapter 4, is therefore suited to understanding its behavior over the course of iterations. We will see in chapter 5 that this analysis allows us to evaluate the evolution of the probability of success of the algorithm, an essential characteristic

of any quantum algorithm, effectively with a classical computer. This procedure for computing the probability of success was presented in [PBB+23]. The eigenanalysis and computation of the success probability of the hypercube quantum search algorithm form the core of this thesis. As is often the case in quantum algebra, these two chapters are relatively heavy on linear algebra and are summarized in sections 4.6 and 5.4. Readers wishing to avoid mathematical developments can limit themselves to these summaries

One might wonder why such a theoretical study was undertaken. As is often the case, it was originally a detour. One of the ideas we have been working on is the improvement of the hypercube quantum search algorithm, a subject quickly touched on at the end of the chapter 6. With this in mind, we felt the need for an analysis tool to compare the original version of the algorithm with our variation. Despite the existence of simulation options like Qiskit [Cro18] or more specialized Python libraries like QuOp_MPI [MW22], being able to compute the algorithm's probability of success in polynomial time is necessary for the study of high-dimensional problems.

1. Notions of quantum information

1.1. Fundamentals of quantum physics

In this work, we will quickly move away from the physical aspects of quantum phenomena. However, it is essential to talk about the main principles of quantum physics to explain where the mathematical formalism comes from and the often counter-intuitive rules that govern the field of quantum information.

In a few words, quantum physics is a set of theories born in the 20th century that radically changes our description of natural properties and behaviors at the particle scale. Physics prior to this break with the past is often described as classical. By abuse of language, we use the term "classical" to designate everything that is not "quantum".

A number of experiments, such as Young's slit, Stern-Gerlach [GS22] and later Aspect [Asp76], highlighted the limits of so-called classical physics at the microscopic scale, and the need for a new model of particle behavior. Among the observed phenomena incompatible with classical physics is the principle of quantum superposition. Described by Dirac in *The Principles of Quantum Mechanics* [Dir35], this principle can be summarized as the possibility of a quantum system being in several classically incompatible states. Here are two examples:

- at any given moment, an electron may be in a superposition of several positions around the nucleus of its atom. This is not a consequence of the experimenter's lack of information about the electron's state, but rather of "existence", that is, the possibility of measuring the electron's position in an entire region of space around the nucleus.

- in the Young's slit experiment, the particle studied passes through both slits at the same time, in proportions that depend on the nature of the slits. Furthermore, it is the component passing through one slit that interferes with that of the other slit, leading to the formation of interference patterns even when the slits are crossed by only one particle at a time.

When we measure superimposed states, we only have access to one of these states, and we return to a classical case. For example, if we measure the position of a particle in a superposition of two positions A and B, the measurement will be randomly either A or B, and not an average of the two. We will see that the behavior of the measurement

of a quantum state is random but predictable. Surprisingly, if the particle's position is measured again, all the measurements will give the same result as the first. The conclusion is that the initial measurement conditions all subsequent measurements. This result, known as wave-packet reduction, implies that the observation modifies the state of the system in such a way as to conform to the measurement. In Young's slit experiment, if we observe which slit the particle passes through, we lose the interference patterns, as it ceases to pass through both slits at the same time.

The main principles of quantum physics are usually summarized in six postulates:

- principle de superposition : superposition principle: the state of a quantum system is fully described by a state vector in a Hilbert space $\mathcal{H}$, often denoted $|\psi(t)\rangle$, itself a complex linear combination of orthogonal basis states representing classically exclusive states.

- correspondence principle: observables (we do not use the term quantities in quantum physics) are represented by Hermitian operators.

- quantization principle: the possible results of measuring an observable are the eigenvectors of the operator associated with the measured observable.

- Born rule: the outcome of a measurement is probabilistic, and the associated probabilities can be calculated from the state vector and operator of the measured observable.

- wave-packet reduction principle: the measurement retains only the state that has occurred, and causes the others to disappear. The measured state is changed to conform to the measurement result.

- Schrödinger equation: the evolution of a system over time is determined by the following differential equation :

$$\mathrm{i}\hbar\frac{\mathrm{d}}{\mathrm{d}t}|\psi(t)\rangle = \widehat{H}|\psi(t)\rangle, \tag{1.1}$$

  where $\hbar$ is the reduced Planck constant and $\widehat{H}$ is the Hamiltonian of the system, an operator corresponding to the total energy of that system.

In this work, we restrict ourselves to the study of discrete-time quantum information systems. These postulates will reappear in forms adapted to this particular framework of quantum physics. We will see in section 1.2 how we exploit the superposition principle to define a quantum bit, in section 1.4 how the principles of correspondence, quantization and wave packet reduction, as well as Born's rule, condition measurement, and in section 1.3 the implications of Schrödinger's equation on the modeling of quantum operations.

1.2. Quantum bits

1.2.1. Qubit definition

In classical computing, the properties of electronics are exploited to form bits, mathematical objects that can take on two values, noted 0 and 1. Similarly, the quantum bit, or "qubit", is defined as the superposition of two orthogonal states denoted $|0\rangle$ and $|1\rangle$. The notion and term qubit were formalized by Schumacher [Sch95]. Although the qubit was first thought of for electron spins, the physical nature of these orthogonal states is of no importance in the theoretical study of quantum information. The $|0\rangle$ and $|1\rangle$ states can refer to spins, polarizations, energy levels and so on. If the reader is unfamiliar with $|0\rangle$ and $|1\rangle$ notation, he can refer to appendix A. Alternatively, they can simply consider that $|x\rangle$ is a column vector and $\langle x|$ is the vector obtained by the Hermitian transpose of $|x\rangle$ (i.e. a row vector).

Any qubit can be expressed as

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{1.2}$$

with $(\alpha, \beta) \in \mathbb{C}^2$ and $|\alpha|^2 + |\beta|^2 = 1$. The coefficients α and β are complex to reflect a possible phase shift between the $|0\rangle$ and $|1\rangle$ states, and must be normalized so that $|\psi\rangle$ has a norm equal to 1. We will see that the unit norm condition ensures that the sum of all probabilities at measurement is equal to 1.

The only condition on $|0\rangle$ and $|1\rangle$ is that they form an orthonormal basis of $\mathbb{C}^2$. We can then set

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \ |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{1.3}$$

The choice of basis is not unique. Any pair of orthogonal unit vectors may be suitable, and changing the basis is even a frequent tool in quantum physics. For example, we often use the $|+\rangle$ and $|-\rangle$ states, defined as

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix}, \ |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix}. \tag{1.4}$$

1.2.2. Qubit representation

The qubit is made up of two complex values, which may suggest that it is a 4-dimensional object, but it is subject to two constraints:

- the qubit must have a unit norm, that is $\||\psi\rangle\| = 1$.
- the qubit is equivalent to itself up to a phase factor, that is $|\psi\rangle \equiv \lambda|\psi\rangle$, with $|\lambda| = 1$.

The qubit is therefore an object of dimension 2, and we show that the set of all possible qubits is isomorphic to a sphere. We can rewrite any qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ as

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{1.5a}$$
$$= e^{i\varphi_a}|\alpha||0\rangle + e^{i\varphi_b}|\beta||1\rangle, \tag{1.5b}$$
$$= |\alpha||0\rangle + e^{i(\varphi_b-\varphi_a)}|\beta||1\rangle, \tag{1.5c}$$
$$= \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle, \tag{1.5d}$$

with $0 \leqslant \theta \leqslant \pi$, $\cos(\theta/2) = |\alpha|$, $\sin(\theta/2) = |\beta|$, $0 \leqslant \varphi < 2\pi$ and $\varphi = \varphi_b - \varphi_a + 2k\pi, k \in \mathbb{Z}$. Any qubit is therefore a function of two angles θ and φ, and can therefore be placed on the surface of a sphere of radius 1 with spherical coordinates $(1, \theta, \varphi)$. We call this sphere the Bloch sphere. It provides a unique visual representation of a qubit. Figure 1.1 shows the example of the qubit $|\psi\rangle = 0.8|0\rangle + e^{i\pi/4}\,0.6|1\rangle$ placed on the Bloch sphere.

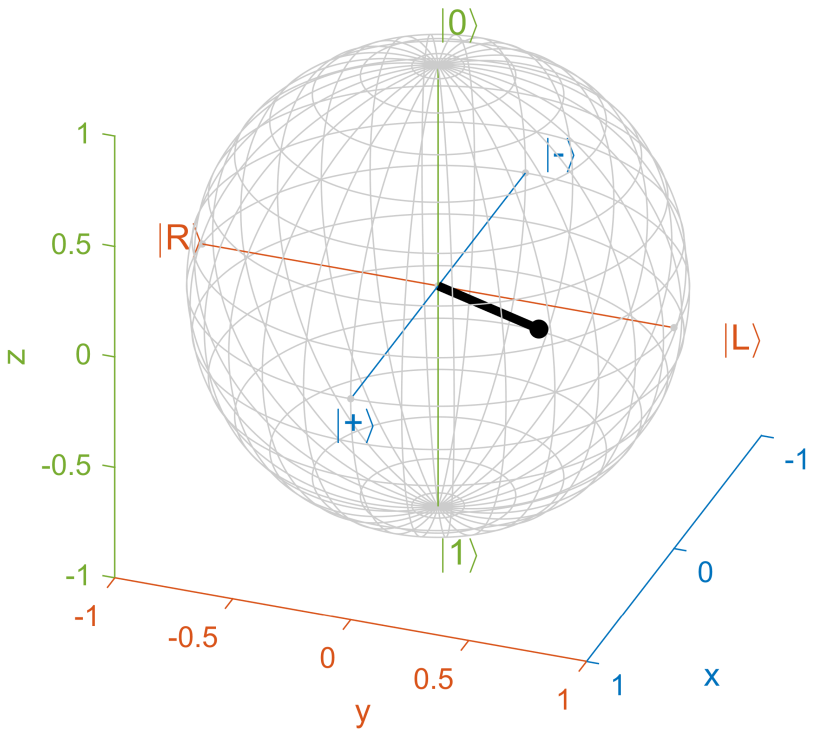

Figure 1.1 Bloch sphere representation of the qubit $0.8|0\rangle + 0.6e^{i\pi/4}|1\rangle$

1.2.3. Qubit association

A quantum information system is obviously made up of several qubits. The system is also fully represented by a state vector, defined by the qubits that compose it.

If we use two qubits, there are four exclusive states: the two qubits are at $|0\rangle$, the first is at $|0\rangle$ and the second at $|1\rangle$, the first is at $|1\rangle$ and the second at $|0\rangle$, and finally the two qubits are at $|1\rangle$. These four states are denoted $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$ respectively. They form an orthonormal basis of $\mathbb{C}^4$, and are therefore called basis states. The state of any two-qubit quantum system can be expressed as

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle, \tag{1.6}$$

still with the norm condition $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$.

To calculate the state vector $|\psi\rangle$ of a two-qubit system with state qubits $|\psi_A\rangle$ and $|\psi_B\rangle$, we use the Kronecker tensor product, that is

$$|\psi\rangle = |\psi_A\rangle \otimes |\psi_B\rangle. \tag{1.7}$$

If required, a summary of the properties of the Kronecker tensor product is available in appendix B. In this work, the Kronecker tensor product will be referred to simply as "tensor product". Note that the tensor product ensures that the global state has a unitary norm: as shown by the equation (B.9), the norm of the tensor product of two vectors is equal to the product of their norms. Equivalently, we use the notations $|\psi_A\rangle \otimes |\psi_B\rangle$, $|\psi_A\rangle|\psi_B\rangle$ and $|\psi_A\psi_B\rangle$ to designate the tensor product of two state vectors.

The basis vectors of the two-qubit system can be calculated as tensor products of $|0\rangle$ and $|1\rangle$. We then obtain

$$|00\rangle = \begin{bmatrix}1\\0\\0\\0\end{bmatrix},\ |01\rangle = \begin{bmatrix}0\\1\\0\\0\end{bmatrix},\ |10\rangle = \begin{bmatrix}0\\0\\1\\0\end{bmatrix},\ |11\rangle = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}, \tag{1.8}$$

and we can see that these vectors have unit norms and form a basis of $\mathbb{C}^4$.

Generally speaking, a system of n qubits is represented by a complex vector of size 2^n, itself a linear combination of 2^n basis states. This exponential growth in the size of the system, and therefore in the quantity of information, partly explains the potential processing power of quantum computers.

1.2.4. Quantum entanglement

The state vector of a system on n qubits cannot always be decomposed into tensor products of n distinct qubits. This means that the qubits of the system are entangled.

Entanglement is a quantum phenomenon that links the states of separate particles, unconstrained by distance or time. Mathematically, this means that there is a fundamental correlation between the states of the entangled particles, and the existence of such a phenomenon has strong implications for our interpretation of the laws of nature. Moreover, the qubits of such a system cannot be described by state vectors. We speak of mixed states, but this notion will not be explored in this work.

Entanglement is proving to be a very powerful tool, providing the basis for such things as quantum teleportation and superdense coding.

The states that best illustrate the phenomenon of entanglement are Bell states, also known as EPR pairs (for Einstein, Podolsky, and Rosen) or maximally entangled pairs. These states are

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),\ \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle),\ \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle),\ \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \tag{1.9}$$

If we take as an example the state $|\psi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, we can see that there is no combination of two qubits $|\psi_A\rangle$ and $|\psi_B\rangle$ such that $|\psi\rangle = |\psi_A\rangle|\psi_B\rangle$. In section 1.4.3, we will see how to create such a state. In $|\psi\rangle$, we find a superposition of the $|00\rangle$ and $|11\rangle$ states, but no $|01\rangle$ or $|10\rangle$. This implies that the two qubits can be observed at $|0\rangle$ or $|1\rangle$ in an equiprobable way, but that both are necessarily observed at the same value, and that there is therefore a correlation between the states of the two qubits: the measurement of one conditions that of the other.

1.3. Quantum operations

1.3.1. Quantum gates and circuits

Schrödinger's famous equation (1.1) is a differential equation whose solutions depend on the Hamiltonian $\widehat{H}$ of the system under study. According to this equation, the evolution of the system between two times t_1 and t_2 is

$$|\psi(t_2)\rangle = \exp\Big(-\frac{\mathrm{i}}{\hbar}\widehat{H}(t_2 - t_1)\Big)|\psi(t_1)\rangle, \tag{1.10}$$

and the operator of this evolution is

$$U(t_1, t_2) = \exp\Big(-\frac{\mathrm{i}}{\hbar}\widehat{H}(t_2 - t_1)\Big). \tag{1.11}$$

Since the Hamiltonian is an observable, $\widehat{H}$ is a Hermitian operator. For any Hermitian operator X, $\exp(\mathrm{i}X)$ is a unitary operator. We therefore conclude that $U(t_1, t_2)$ is unitary and that any evolution of a quantum system is modeled by a unitary operator. This

result is consistent with the unit norm criterion for state vectors: an operator that always preserves the norm of a vector is necessarily unitary.

In the context of quantum information, we restrict ourselves to finite-dimensional cases. We can then represent a unitary operator by a square matrix U such that $UU^\dagger = U^\dagger U = I$, where $U^\dagger$ denotes the adjoint matrix of U and I is the identity matrix. In other words, $U^\dagger = U^{-1}$.

When we apply an operator U to a state $|\psi\rangle$, we obtain the state $U|\psi\rangle$. Note that the matrix multiplies the state vector on the left, as it is in column form. Consequently, if we apply U and then V successively, we obtain $VU|\psi\rangle$. Figure 1.2 shows a basic circuit illustrating the sequence of two gates. A quantum circuit is read from left to right.

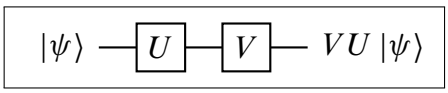

Figure 1.2 Succession of quantum gates

When working on an n qubit system, an operator U must be of size $2^n \times 2^n$. In practice, it is unrealistic to design a different component for each U operation you wish to perform. As in electronics, we use elementary components called quantum gates, by analogy with logic gates. These gates act on a limited number of qubits, usually one or two, and are associated with unitary matrices. To perform operations on large-scale systems, quantum circuits are designed from these gates.

Quantum gates are applied locally to one or more qubits, and the global operator can be calculated from the matrices of each gate. When no gate is applied to a qubit, we note that it undergoes an operation I whose matrix is the identity. This does not mean that the qubit will be unchanged by the operation, as applying an operation to a qubit can affect all the other qubits with which it is entangled. In general, the state of a single qubit cannot be defined independently of the rest of the system. For this reason, we need to be able to calculate the global operator from the individual gates. Like state vectors, gate matrices are associated by tensor product. For example, let us assume a 5-qubit system. We apply a gate A to qubit 2 and a gate B to qubits 4 and 5. Such gates are sometimes referred to as A_2 and $B_{4,5}$ to specify the qubits affected. This example is illustrated in figure 1.3. The global operation matrix will be

$$U = I_1 \otimes A_2 \otimes I_3 \otimes B_{4,5}. \tag{1.12}$$

1.3.2. Usual quantum gates

There are a number of regularly encountered quantum gates, with which most operators are composed. In this work, we will study just a few of them.

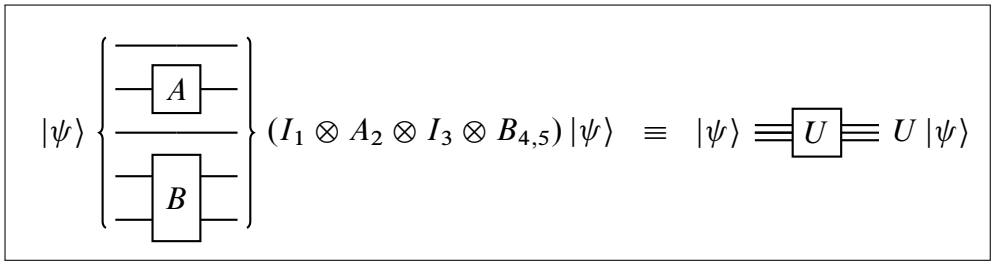

Figure 1.3 Association of quantum gates

Hadamard gate

The Hadamard gate is one of the most common gates in quantum circuits, as it transforms a basis state into a superposition. Its matrix is

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{1.13}$$

Its effect on the $|0\rangle$ and $|1\rangle$ states is as follows:

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle, \tag{1.14}$$

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle. \tag{1.15}$$

We find the $|+\rangle$ and $|-\rangle$ states defined by equation (1.4).

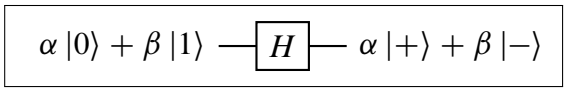

Figure 1.4 Symbol and effect of Hadamard gate

It is common to see Hadamard gates on each qubit at the input and output of a quantum circuit. When the Hadamard gate is repeated n times, the global operator is $H^{\otimes n}$ (see (B.3) for notation). Applying $H^{\otimes n}$ to the system creates a uniform superposition of all states on n qubits. Indeed, we have

$$H^{\otimes n}|0\rangle^{\otimes n} = H^{\otimes n}\begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2^n}}\begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \\ 1 \end{bmatrix} \tag{1.16}$$

Pauli gates

Pauli gates are represented by the Pauli matrices X, Y and Z, which are used, for example, in spintronics or in modeling errors in quantum transmissions. Their matrices are

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \tag{1.17}$$

$$Y = \begin{bmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{bmatrix}, \tag{1.18}$$

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{1.19}$$

The X gate causes a bit-flip, inverting $|0\rangle$ and $|1\rangle$, that is

$$X(\alpha|0\rangle + \beta|1\rangle) = \alpha|1\rangle + \beta|0\rangle. \tag{1.20}$$

The Z gate causes a phase-flip. It transforms $|0\rangle$ into $|0\rangle$ and $|1\rangle$ into $-|1\rangle$, meaning it reverses the phase between the superimposed states, that is

$$Z(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle - \beta|1\rangle. \tag{1.21}$$

This means that the Z gate has no effect on the basis states $|0\rangle$ and $|1\rangle$:

$$Z|0\rangle = |0\rangle, \tag{1.22}$$

$$Z|1\rangle = -|1\rangle \equiv |1\rangle. \tag{1.23}$$

The Y gate combines the effects of the other two gates. It is equivalent (up to a phase factor) to the sequence of the other two Pauli gates. Indeed, we have

$$Y(\alpha|0\rangle + \beta|1\rangle) = \mathrm{i}(\alpha|1\rangle - \beta|0\rangle) \equiv \alpha|1\rangle - \beta|0\rangle. \tag{1.24}$$

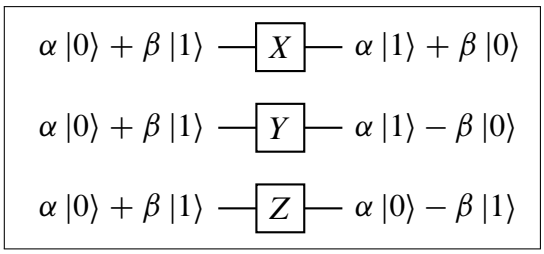

Figure 1.5 Symbol and effect of the Pauli gate

A property of Pauli matrices that will be used later is

$$X = HZH, \tag{1.25}$$

$$Z = HXH. \tag{1.26}$$

CNOT gate

The Controlled-NOT gate, or CNOT, is by far the most widespread gate capable of causing two qubits to interact. It is found in almost all quantum circuits, as it enables conditional relationships to be established in a system. In a way, it is the analog of the "if" in classical programming.

The CNOT gate affects two qubits. It inverts the second if the first is $|1\rangle$, that is, it applies X to it, and does nothing otherwise. Note that the first qubit may be in a superposition of $|0\rangle$ and $|1\rangle$, so the second qubit may be partially inverted. Its matrix is

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \tag{1.27}$$

Its effect on the basis states is as follows:

$$\text{CNOT}|00\rangle = |00\rangle, \tag{1.28a}$$
$$\text{CNOT}|01\rangle = |01\rangle, \tag{1.28b}$$
$$\text{CNOT}|10\rangle = |11\rangle, \tag{1.28c}$$
$$\text{CNOT}|11\rangle = |10\rangle. \tag{1.28d}$$

These relationships can be summarized as

$$\text{CNOT}(|x\rangle|y\rangle) = |x\rangle|x \oplus y\rangle, \tag{1.29}$$

where $\oplus$ denotes Boolean exclusive OR. On any state, we have

$$\text{CNOT}(\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle) = \alpha|00\rangle + \beta|01\rangle + \gamma|11\rangle + \delta|10\rangle. \tag{1.30}$$

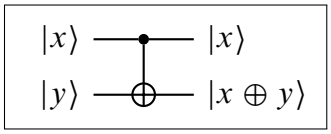

Figure 1.6 Symbol and effect of the CNOT gate

We will see in section 1.4.3 that applying the CNOT gate to superimposed states creates entanglement between the two qubits concerned.

SWAP gate

The SWAP gate simply inverts the position of two qubits in a system. Its existence is important, as it demonstrates that it is possible to make two non-adjacent qubits interact. Its matrix is

$$\text{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \tag{1.31}$$

Its effect on the basis states is as follows:

$$\text{SWAP}|00\rangle = |00\rangle, \tag{1.32a}$$
$$\text{SWAP}|01\rangle = |10\rangle, \tag{1.32b}$$
$$\text{SWAP}|10\rangle = |01\rangle, \tag{1.32c}$$
$$\text{SWAP}|11\rangle = |11\rangle. \tag{1.32d}$$

These relationships can be summarized as

$$\text{SWAP}(|x\rangle|y\rangle) = |y\rangle|x\rangle, \tag{1.33}$$

which corresponds to the exchange of qubit positions.

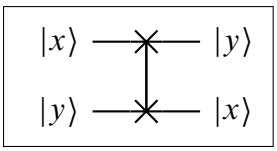

Figure 1.7 Symbol and effect of the SWAP gate

1.4. Quantum state measurement

1.4.1. Measurement principles

Measuring a quantum state is a delicate operation, as it can modify or destroy the measured state. It is therefore irreversible, unlike all other quantum operations. The behavior of quantum measurement is unique, and has its own mathematical formalism.

First, we need to define what we are measuring. In quantum physics, we don't talk about quantities, but about "observables". An observable is not a scalar, as a quantity is in classical physics, but a Hermitian operator. From this observable, we can predict all possible results of a measurement on a given state, as well as their probabilities of occurrence.

An observable $\widehat{M}$, like any Hermitian operator, can be decomposed into

$$\widehat{M} = \sum_m m|\psi_m\rangle\langle\psi_m|, \tag{1.34}$$

where m represents the eigenvalues of $\widehat{M}$ and $|\psi_m\rangle$ the associated eigenvectors. This matrix representation is called the "spectral decomposition", and exists for all normal matrices, including Hermitian and unitary matrices.

When $\widehat{M}$ is measured on a state $|\psi\rangle$, the possible results of the measurement are the values of m, that is, the eigenvalues of the observable. We define $P_m = |\psi_m\rangle\langle\psi_m|$ as the projector on the $|\psi_m\rangle$ state. Indeed, we have

$$P_m|\psi\rangle = |\psi_m\rangle\langle\psi_m||\psi\rangle = |\psi_m\rangle\langle\psi_m|\psi\rangle = \langle\psi_m|\psi\rangle|\psi_m\rangle, \tag{1.35}$$

which corresponds to the orthogonal projection of $|\psi\rangle$ onto $|\psi_m\rangle$. The probability of measuring m is the square of the norm of this orthogonal projection, that is

$$\mathbf{P}(m) = |\langle\psi_m|\psi\rangle|^2 = \langle\psi|P_m|\psi\rangle. \tag{1.36}$$

After measurement, the state is modified to conform to the realization, that is

$$|\psi\rangle \xrightarrow{\widehat{M}} |\psi_m\rangle = \frac{P_m|\psi\rangle}{\sqrt{\mathbf{P}(m)}}. \tag{1.37}$$

If $\widehat{M}$ is normal, then its eigenvectors $|\psi_m\rangle$ form an orthonormal basis of $\mathbb{C}^n$, and hence

$$\sum_m P_m = I_n, \tag{1.38}$$

where I_n is the identity of size $n \times n$. This explains the unit norm condition for state vectors: since the sum of probabilities must be 1, we have

$$\begin{aligned}
\sum_m \mathbf{P}(m) &= \sum_m \langle\psi|P_m|\psi\rangle, && (1.39)\\
&= \langle\psi|\sum_m P_m|\psi\rangle, && (1.40)\\
&= \langle\psi|I_n|\psi\rangle, && (1.41)\\
&= \langle\psi|\psi\rangle, && (1.42)\\
&= \||\psi\rangle\|^2 && (1.43)
\end{aligned}$$

and since $\sum_m \mathbf{P}(m) = 1$, we must have $\||\psi\rangle\| = 1$.

It is possible to study the statistical behavior of projective measurements. Knowing that a measurement returns a value m with probability $\mathbf{P}(m)$, the mean value of a measurement of the observable $\widehat{M}$ is

$$\begin{aligned}\mathbf{E}(\widehat{M}) &= \sum_m m\mathbf{P}(m), &(1.44)\\ &= \sum_m m\langle\psi|P_m|\psi\rangle, &(1.45)\\ &= \langle\psi|\sum_m mP_m|\psi\rangle, &(1.46)\\ &= \langle\psi|\widehat{M}|\psi\rangle. &(1.47)\end{aligned}$$

We often note $\langle\psi|\widehat{M}|\psi\rangle = \langle\widehat{M}\rangle$. In the same way, we can calculate the variance and standard deviation, or any other statistical property. For example, the variance of $\widehat{M}$ will be

$$\text{var}(\widehat{M}) = \langle\widehat{M}^2\rangle - \langle\widehat{M}\rangle^2. \tag{1.48}$$

When we apply the same measurement several times, we will always obtain the same thing as the first time. If one measurement gives us m, then the output state is $|\psi_m\rangle$, and the next measurement will give m with a probability of

$$\begin{aligned}\mathbf{P}(m) &= \langle\psi_m|P_m|\psi_m\rangle, &(1.49)\\ &= \langle\psi_m||\psi_m\rangle\langle\psi_m||\psi_m\rangle, &(1.50)\\ &= |\langle\psi_m|\psi_m\rangle|^2, &(1.51)\\ &= 1. &(1.52)\end{aligned}$$

1.4.2. Examples of measurements

Example of measurement on a single qubit

Assume we receive a qubit $|\psi\rangle = 0.8|0\rangle - 0.6\text{i}|1\rangle$ and perform a measurement that can give $|0\rangle$ or $|1\rangle$. The projectors of the measure are $P_0 = |0\rangle\langle 0|$, and $P_1 = |1\rangle\langle 1|$. We can check that $P_0 + P_1 = I_2$:

$$P_0 + P_1 = \begin{bmatrix}1\\0\end{bmatrix}\begin{bmatrix}1 & 0\end{bmatrix} + \begin{bmatrix}0\\1\end{bmatrix}\begin{bmatrix}0 & 1\end{bmatrix} = \begin{bmatrix}1 & 0\\0 & 0\end{bmatrix} + \begin{bmatrix}0 & 0\\0 & 1\end{bmatrix} = \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}, \tag{1.53}$$

and therefore that our measurement is correctly defined.

In this case, as is often the case in quantum information, we are not concerned with the result m of the measurement, but only with the observed vector $|\psi_m\rangle$ and the probability

of its realization $\mathbf{P}(m)$. In this case, we do not use the observable $\widehat{M}$ but only the projectors P_m. The probability of measuring $|0\rangle$ is

$$\begin{aligned}
\mathbf{P}(0) &= \langle\psi|P_0|\psi\rangle, && (1.54)\\
&= (0.8\langle 0| + 0.6\mathrm{i}\langle 1|)(|0\rangle\langle 0|)(0.8|0\rangle - 0.6\mathrm{i}|1\rangle), && (1.55)\\
&= (0.8\langle 0|)(|0\rangle\langle 0|)(0.8|0\rangle), && (1.56)\\
&= 0.64\langle 0|0\rangle\langle 0|0\rangle, && (1.57)\\
&= 0.64. && (1.58)
\end{aligned}$$

Here, $|1\rangle$ disappears, as $|0\rangle$ and $|1\rangle$ are orthogonal, and so $\langle 0|1\rangle = \langle 1|0\rangle = 0$. Furthermore, as with any state vector, $\langle 0|0\rangle = \||0\rangle\|^2 = 1$. In the end, $\mathbf{P}(0) = 0.64$. The calculation of $\mathbf{P}(1)$ is similar, except that we use P_1 instead of P_0 :

$$\begin{aligned}
\mathbf{P}(1) &= \langle\psi|P_1|\psi\rangle, && (1.59)\\
&= (0.8\langle 0| + 0.6\mathrm{i}\langle 1|)(|1\rangle\langle 1|)(0.8|0\rangle - 0.6\mathrm{i}|1\rangle), && (1.60)\\
&= (0.6\mathrm{i}\langle 1|)(|1\rangle\langle 1|)(-0.6\mathrm{i}|1\rangle), && (1.61)\\
&= 0.36\langle 1|1\rangle\langle 1|1\rangle, && (1.62)\\
&= 0.36. && (1.63)
\end{aligned}$$

We verify that $\mathbf{P}(0) + \mathbf{P}(1) = 1$. After measurement, the state becomes, according to the realization

$$|\psi_0\rangle = \frac{P_0|\psi\rangle}{\sqrt{\mathbf{P}(0)}} = \frac{|0\rangle\langle 0|(0.8|0\rangle - 0.6\mathrm{i}|1\rangle)}{0.8} = |0\rangle, \quad (1.64)$$

$$|\psi_1\rangle = \frac{P_1|\psi\rangle}{\sqrt{\mathbf{P}(1)}} = \frac{|1\rangle\langle 1|(0.8|0\rangle - 0.6\mathrm{i}|1\rangle)}{0.6} = |1\rangle. \quad (1.65)$$

This means that when we measure $|0\rangle$, the state $|\psi\rangle$ becomes $|\psi_0\rangle = |0\rangle$. Similarly, when we measure $|1\rangle$, the state $|\psi\rangle$ becomes $|\psi_1\rangle = |1\rangle$.

In this measurement example, we can directly find the probabilities of each realization: the state vector being of the form $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, the probabilities of measuring $|0\rangle$ and $|1\rangle$ are respectively $\mathbf{P}(0) = |\alpha|^2 = 0.64$ and $\mathbf{P}(1) = |\beta|^2 = 0.36$. For this reason, if we wish to make a measurement that can give two results $|x\rangle$ and $|y\rangle$, we can choose to express $|\psi\rangle$ as a superposition of $|x\rangle$ and $|y\rangle$, that is, $|\psi\rangle = \alpha'|x\rangle + \beta'|y\rangle$ (provided that $|x\rangle$ and $|y\rangle$ are orthogonal).

For example, we perform a measurement which may result in $|+\rangle$ and $|-\rangle$. Since $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$, we can write

$$|\psi\rangle = 0.8|0\rangle + 0.6\mathrm{i}|1\rangle = \frac{0.8 + 0.6\mathrm{i}}{\sqrt{2}}|+\rangle + \frac{0.8 - 0.6\mathrm{i}}{\sqrt{2}}|-\rangle, \quad (1.66)$$

and therefore

$$\mathbf{P}(+) = \left|\frac{0.8 + 0.6\mathrm{i}}{\sqrt{2}}\right|^2 = \frac{1}{2}, \tag{1.67}$$

$$\mathbf{P}(-) = \left|\frac{0.8 - 0.6\mathrm{i}}{\sqrt{2}}\right|^2 = \frac{1}{2}. \tag{1.68}$$

A direct calculation with the projectors would, of course, produce the same result.

Example of measurement on two qubits

Assume we have two qubits $|\psi_\mathrm{A}\rangle = 0.6|0\rangle + 0.8|1\rangle$ and $|\psi_\mathrm{B}\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, and that in both cases we wish to make a measurement that can give $|0\rangle$ or $|1\rangle$. We can show that the probabilities of measuring $|0\rangle$ and $|1\rangle$ on the first qubit are respectively $\mathbf{P}^\mathrm{A}(0) = 0.36$ and $\mathbf{P}^\mathrm{A}(1) = 0.64$. Similarly, on the second qubit, they are $\mathbf{P}^\mathrm{B}(0) = \mathbf{P}^\mathrm{B}(1) = 0.5$.

Consider the system composed of these two qubits. Its state vector is $|\psi_\mathrm{AB}\rangle = |\psi_\mathrm{A}\rangle \otimes |\psi_\mathrm{B}\rangle = (0.6|00\rangle + 0.6|01\rangle + 0.8|10\rangle + 0.8|11\rangle)/\sqrt{2}$. If we perform a measurement with the states $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$ as possible outcomes, the projectors will be $P_{00} = |00\rangle\langle 00|$, $P_{01} = |01\rangle\langle 01|$, $P_{10} = |10\rangle\langle 10|$, and $P_{11} = |11\rangle\langle 11|$. Once again, we can check that $P_{00} + P_{01} + P_{10} + P_{11} = I_4$, which means that our measure is correctly defined. The probabilities of each possible outcome are

$$\mathbf{P}(00) = \langle\psi|P_{00}|\psi\rangle = 0.18, \tag{1.69}$$

$$\mathbf{P}(01) = \langle\psi|P_{01}|\psi\rangle = 0.18, \tag{1.70}$$

$$\mathbf{P}(10) = \langle\psi|P_{10}|\psi\rangle = 0.32, \tag{1.71}$$

$$\mathbf{P}(11) = \langle\psi|P_{11}|\psi\rangle = 0.32. \tag{1.72}$$

As in the one-qubit case, since the measured state is expressed as $\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$, we can directly deduce that $\mathbf{P}(00) = |\alpha|^2$, $\mathbf{P}(01) = |\beta|^2$, $\mathbf{P}(10) = |\gamma|^2$ and $\mathbf{P}(11) = |\delta|^2$. Moreover, as the two qubits in the system are not entangled, their measurements are independent of each other, and we observe that $\mathbf{P}(00) = \mathbf{P}^\mathrm{A}(0)\mathbf{P}^\mathrm{B}(0)$, $\mathbf{P}(01) = \mathbf{P}^\mathrm{A}(0)\mathbf{P}^\mathrm{B}(1)$, $\mathbf{P}(10) = \mathbf{P}^\mathrm{A}(1)\mathbf{P}^\mathrm{B}(0)$ and that $\mathbf{P}(11) = \mathbf{P}^\mathrm{A}(1)\mathbf{P}^\mathrm{B}(1)$.

It may happen that we wish to measure only part of a system. Assume we keep the same state $|\psi_\mathrm{AB}\rangle$ as in the previous example, and perform a measurement that may give $|0\rangle$ or $|1\rangle$ on the first qubit, leaving the second intact. We will note the two projectors of this measure $P_{0\times}$ and $P_{1\times}$, the "$\times$" in second position indicating that we ignore the state of the second qubit. These projectors are

$$P_{0\times} = |00\rangle\langle 00| + |01\rangle\langle 01| = |0\rangle\langle 0| \otimes I_2, \tag{1.73}$$

$$P_{1\times} = |10\rangle\langle 10| + |11\rangle\langle 11| = |1\rangle\langle 1| \otimes I_2. \tag{1.74}$$

In matrix form, we have

$$P_{0\times} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \; P_{1\times} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \tag{1.75}$$

and we verify that $P_{0\times} + P_{1\times} = I_4$.

In the end, the probabilities of each possible outcome are

$$\mathbf{P}(0\times) = \langle\psi|P_{0\times}|\psi\rangle = 0.36, \tag{1.76}$$
$$\mathbf{P}(1\times) = \langle\psi|P_{1\times}|\psi\rangle = 0.64, \tag{1.77}$$

and we find the probabilities $\mathbf{P}^{\mathrm{A}}(0)$ and $\mathbf{P}^{\mathrm{A}}(1)$. This is a logical but reassuring result: measuring a qubit in a system is equivalent to measuring it in isolation.

It is possible to design measurements that are not concerned with the states of each qubit independently, but only in some of their properties. For example, the projectors $P_{=} = |00\rangle\langle 00| + |11\rangle\langle 11|$ and $P_{\neq} = |01\rangle\langle 01| + |10\rangle\langle 10|$ correspond to a measure whose results are "the two qubits are identical" or "the two qubits are different", without knowing the state of these qubits.

1.4.3. Measurement of entangled states

Introduced in equation (1.9), Bell states are the most strongly entangled two-qubit systems, resulting in total correlation between the measurements of the two qubits.

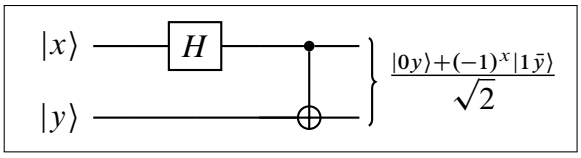

Figure 1.8 Bell circuit

These states can be obtained from the Bell circuit shown in figure 1.8. Each of the two input qubits, $|x\rangle$ and $|y\rangle$, can be initialized to $|0\rangle$ or $|1\rangle$. For the four possible inputs, the successive transformations are :

$$|00\rangle \xrightarrow{H\otimes I} (|0\rangle + |1\rangle)|0\rangle/\sqrt{2} \xrightarrow{\text{CNOT}} (|00\rangle + |11\rangle)/\sqrt{2}, \tag{1.78a}$$
$$|01\rangle \xrightarrow{H\otimes I} (|0\rangle + |1\rangle)|1\rangle/\sqrt{2} \xrightarrow{\text{CNOT}} (|01\rangle + |10\rangle)/\sqrt{2}, \tag{1.78b}$$
$$|10\rangle \xrightarrow{H\otimes I} (|0\rangle - |1\rangle)|0\rangle/\sqrt{2} \xrightarrow{\text{CNOT}} (|00\rangle - |11\rangle)/\sqrt{2}, \tag{1.78c}$$
$$|11\rangle \xrightarrow{H\otimes I} (|0\rangle - |1\rangle)|1\rangle/\sqrt{2} \xrightarrow{\text{CNOT}} (|01\rangle - |10\rangle)/\sqrt{2}. \tag{1.78d}$$

These four states are then denoted $|\beta_{xy}\rangle$, with the general equation

$$|\beta_{xy}\rangle = \frac{|0y\rangle + (-1)^x|1\bar{y}\rangle}{\sqrt{2}}. \tag{1.79}$$

Assume that we have the state $|\beta_{00}\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ and that we perform a measurement on each of its qubits that can give the result $|0\rangle$ or $|1\rangle$. If we start by measuring the first qubit, we use the projectors $P_{0\times} = |0\rangle\langle 0| \otimes I_2$ and $P_{1\times} = |1\rangle\langle 1| \otimes I_2$, and we have the measurement probabilities

$$\begin{aligned}
\mathbf{P}^{\mathrm{A}}(0) &= \frac{1}{\sqrt{2}}(\langle 00| + \langle 11|)(|0\rangle\langle 0| \otimes I_2)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)), && (1.80)\\
&= \frac{1}{2}(\langle 0| + \langle 1|)|0\rangle\langle 0|(|0\rangle + |1\rangle), && (1.81)\\
&= \frac{1}{2}\langle 0|0\rangle\langle 0|0\rangle = \frac{1}{2}, && (1.82)\\
\mathbf{P}^{\mathrm{A}}(1) &= \frac{1}{\sqrt{2}}(\langle 00| + \langle 11|)(|1\rangle\langle 1| \otimes I_2)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)), && (1.83)\\
&= \frac{1}{2}(\langle 0| + \langle 1|)|1\rangle\langle 1|(|0\rangle + |1\rangle), && (1.84)\\
&= \frac{1}{2}\langle 1|1\rangle\langle 1|1\rangle = \frac{1}{2}. && (1.85)
\end{aligned}$$

Here, we simplify the expressions using the mixed product (see equation (B.8)) and the fact that $\langle x|I_2|x\rangle = \||x\rangle\|^2 = 1$ for all $|x\rangle$. In the end, we obtain, quite logically, $\mathbf{P}^{\mathrm{A}}(0) = \mathbf{P}^{\mathrm{A}}(1) = 0.5$.

By symmetry, if we start with the measurement of the second qubit with projectors $P_{\times 0}$ and $P_{\times 1}$, we will find $\mathbf{P}^{\mathrm{B}}(0) = \mathbf{P}^{\mathrm{B}}(1) = 0.5$. However, if the two measurements are made one after the other, the behavior of the second is conditioned by the first. Assume that the first qubit has been measured first. We can have, equiprobably, one of the states

$$\begin{aligned}
|\psi_{0\times}\rangle &= \frac{P_{0\times}|\beta_{00}\rangle}{\sqrt{\mathbf{P}^{\mathrm{A}}(0)}}, && (1.86)\\
&= \sqrt{2}(|0\rangle\langle 0| \otimes I_2)(|00\rangle + |11\rangle)/\sqrt{2}, && (1.87)\\
&= |00\rangle, && (1.88)\\
|\psi_{1\times}\rangle &= \frac{P_{1\times}|\beta_{00}\rangle}{\sqrt{\mathbf{P}^{\mathrm{A}}(1)}}, && (1.89)\\
&= \sqrt{2}(|1\rangle\langle 1| \otimes I_2)(|00\rangle + |11\rangle)/\sqrt{2}, && (1.90)\\
&= |11\rangle. && (1.91)
\end{aligned}$$

This means that if the measurement of the first qubit gave $|0\rangle$, then the second will be on state $|00\rangle$, and if the measurement of the first qubit gave $|1\rangle$, then the second will be on state $|11\rangle$. If we measure the second qubit of $|00\rangle$, we will still get $|0\rangle$ and therefore $\mathbf{P}^{\mathrm{B}}(0) = 1$. Similarly, if we measure the second qubit of $|11\rangle$ we will always get $|1\rangle$ and therefore $\mathbf{P}^{\mathrm{B}}(1) = 1$. In the end, the second measurement will always give the same result as the first.

We can deduce from these results that the measurements of the two qubits are not independent. In this case, they are even totally correlated. This correlation is an expression of the entanglement phenomenon, and can be exploited, for example, in teleportation, since the two qubits of an entangled pair are not necessarily close to each other.

1.5. No-cloning theorem

In classical computing, one of the most common operations is copying information. Whether to save data or to add redundancy to a message, cloning bits is considered an elementary manipulation. In quantum computing, it turns out that it is impossible to clone any quantum state. More precisely, a given device can only clone orthogonal states.

Let a system be defined by a state vector $|s\rangle$, where $|s\rangle$ is the location reserved for copying $|s\rangle$. We are looking for a unitary operation U capable of making this copy. We must then have

$$U(|\psi\rangle|s\rangle) = |\psi\rangle|\psi\rangle. \tag{1.92}$$

Then, assume that this operation U can clone another state $|\varphi\rangle$. In the same way

$$U(|\varphi\rangle|s\rangle) = |\varphi\rangle|\varphi\rangle. \tag{1.93}$$

The inner product of these expressions is, on either side of the equalities

$$\big((\langle\psi|\langle s|)U^{\dagger}\big)\big(U(|\varphi\rangle|s\rangle)\big) = (\langle\psi|\langle\psi|)(|\varphi\rangle|\varphi\rangle), \tag{1.94}$$

$$\langle\psi|\varphi\rangle\langle s|s\rangle = \langle\psi|\varphi\rangle\langle\psi|\varphi\rangle, \tag{1.95}$$

$$\langle\psi|\varphi\rangle = \langle\psi|\varphi\rangle^2, \tag{1.96}$$

which implies that $\langle\psi|\varphi\rangle = 0$ or that $\langle\psi|\varphi\rangle = 1$. Consequently, the operator U that clones $|\psi\rangle$ and $|\varphi\rangle$ only exists if these two states are orthogonal, and U cannot, for example, clone a superposition $\alpha|\psi\rangle + \beta|\varphi\rangle$. This is known as the no-cloning theorem, and is a major constraint in quantum information.

2. Quantum walks

In classical computer science, random walk algorithms form a family of probabilistic algorithms that consist of a succession of random moves in a given space. Because of their "organic" nature, random walks are used in a wide variety of fields, including biology and economics. It turns out that they are also suitable for solving several important algorithmic problems, such as estimating the volume of a convex body [DFK91], or calculating the permanent of a matrix [JSV04]. In particular, random walks can be used to solve an important family of problems: Boolean satisfiability problems, or "SAT", in a relatively short time [Sch99], including 3-SAT with a complexity $\mathcal{O}(1.334^n)$. This is an important result, because according to Cook's theorem [Coo71], SAT is a NP-complete problem, and we can reduce any SAT problem to 3-SAT [Kar72]. This means that we can theoretically reduce any NP problem to 3-SAT, and thus solve it with a random walk algorithm. A quick overview of the SAT problem and its importance in algorithmics is available in appendix D.

The notion of quantum random walk originates from the work of physicists Aharonov, Davidovich and Zagury [ADZ93]. The concept of quantum walks is to move a particle according to a position-independent parameter, such as the spin. The difference between quantum walks and classical quantum walks lies in the possibility of superposition of positions and directions of motion, leading to the appearance of interference. In this work, we will only consider the case of discrete time quantum walks, which are analogous to classical random walks.

The question of how to implement quantum walks is still open. A quantum computer could simulate such walks, just as a classical computer simulates random walks on a graph. Pending the arrival of a universal quantum computer, various implementation solutions have been rapidly proposed, such as ion traps [TM02] or optical lattices [DRKB02]. There are also proposed implementations on modern quantum processors [AAMP20], [QWX+21].

As with classical walks, the potential applications of quantum walks are multiple. In addition to their interest in the study of search algorithms, which will be covered in section 3.3, they can be used, for example, to solve various combinatorial optimization problems [MW19], [MW20], such as portfolio optimization problems [SMMW21].

In this chapter, we first look at the case of walk on an axis in order to present the concepts common to every quantum walk and to illustrate their particular behaviors in section 2.1. Then, in section 2.2, we will focus on the hypercube walk, which will serve as the basis for the search algorithm studied in this work, presented in section 3.3.

2.1. Formalism and walk on an axis

In this section, we will introduce the formalism of quantum walks with the example of the simplest of them all, the walk on an axis. For illustrative purposes, we will limit ourselves to a superficial analysis of the behavior of this walk. A more complete analysis of this walk can be found in [NV00]. We assume that we have a particle placed on an infinite axis and that this particle is endowed with a property that can take two values (for example, its spin), which we will denote as $|\uparrow\rangle$ and $|\downarrow\rangle$. We write $|\psi\rangle = |4\rangle|\downarrow\rangle$ the state of a particle placed at position $x = 4$ with a spin $|\downarrow\rangle$.

In a quantum walk, the state of a particle is represented in a composite Hilbert space $\mathcal{H} = \mathcal{H}^S \otimes \mathcal{H}^C$, where $\mathcal{H}^S$ is the shift space, representing the positions, and $\mathcal{H}^C$ is the coin space, representing the directions of motion. The term "coin" refers to the random drawing of the direction at each stage of a classical random walk, such as a coin toss. A basic state in $\mathcal{H}$ can therefore be written as

$$|\psi\rangle = |p\rangle|d\rangle, \tag{2.1}$$

where $|p\rangle$ is a basis state in $\mathcal{H}^S$ designating a position on the graph and $|d\rangle$ is a base state in $\mathcal{H}^C$ designating a direction of motion. In the case of the walk on an infinite axis, the spaces $\mathcal{H}^S$ and $\mathcal{H}^C$ are defined as

$$\mathcal{H}^S = \text{span}(\{|p\rangle \mid p \in \mathbb{Z}\}), \tag{2.2}$$
$$\mathcal{H}^C = \text{span}(\{|\downarrow\rangle, |\uparrow\rangle\}), \tag{2.3}$$

where $\text{span}(V)$ denotes the vector space spanned by the set of vectors V. Often, a matrix M is used instead of the set V. In this case, $\text{span}(M)$ designates the vector space spanned by the columns of M. If required, all the notations used in this work can be found on page 13.

The displacement of the particle on the axis will depend on $|d\rangle$: if $|d\rangle = |\uparrow\rangle$, then the particle moves from position p to position $p + 1$, and if $|d\rangle = |\downarrow\rangle$, then the particle moves from position p to position $p - 1$. We define the shift operator S by

$$S|p\rangle|\downarrow\rangle = |p - 1\rangle|\downarrow\rangle. \tag{2.4}$$
$$S|p\rangle|\uparrow\rangle = |p + 1\rangle|\uparrow\rangle, \tag{2.5}$$

Before each move, we "mix" the directions in which the particle will move. This is equivalent to a random draw for the next move in the classical random walks. The operator responsible for this action is the coin operator C, and is defined in terms of the walk we wish to obtain. On the axis, to obtain a balanced walk, we use the Hadamard matrix H defined in equation (1.13), considering that $|\downarrow\rangle \equiv |0\rangle$ and $|\uparrow\rangle \equiv |1\rangle$. We then

have

$$C|p\rangle|\downarrow\rangle = |p\rangle(H|\downarrow\rangle) = |p\rangle\frac{|\downarrow\rangle + |\uparrow\rangle}{\sqrt{2}}, \tag{2.6}$$

$$C|p\rangle|\uparrow\rangle = |p\rangle(H|\uparrow\rangle) = |p\rangle\frac{|\downarrow\rangle - |\uparrow\rangle}{\sqrt{2}}. \tag{2.7}$$

We start the walk on the axis in the central position $|p_0\rangle = |0\rangle$, and in this first example with $|d_0\rangle = |\downarrow\rangle$. The initial state is therefore

$$|\psi_0\rangle = |0\rangle|\downarrow\rangle. \tag{2.8}$$

The walk consists of the repeated application of the operators C and S. The uniform walk operator is $U = SC$. The first iteration is therefore

$$|\psi_1\rangle = U|\psi_0\rangle, \tag{2.9}$$

$$= SC|0\rangle|\downarrow\rangle, \tag{2.10}$$

$$= S|0\rangle\frac{|\downarrow\rangle + |\uparrow\rangle}{\sqrt{2}}, \tag{2.11}$$

$$= S\frac{|0\rangle|\downarrow\rangle + |0\rangle|\uparrow\rangle}{\sqrt{2}}, \tag{2.12}$$

$$= \frac{|-1\rangle|\downarrow\rangle + |1\rangle|\uparrow\rangle}{\sqrt{2}}. \tag{2.13}$$

The result obtained after one iteration is identical to what a classic walk would produce, that is, a symmetrical distribution between the -1 and 1 positions. Similarly, the second iteration produces an intuitive result:

$$|\psi_2\rangle = U|\psi_1\rangle, \tag{2.14}$$

$$= SC\frac{|-1\rangle|\downarrow\rangle + |1\rangle|\uparrow\rangle}{\sqrt{2}}, \tag{2.15}$$

$$= S\frac{|-1\rangle(|\downarrow\rangle + |\uparrow\rangle) + |1\rangle(|\downarrow\rangle - |\uparrow\rangle)}{2}, \tag{2.16}$$

$$= \frac{|-2\rangle|\downarrow\rangle + |0\rangle|\downarrow\rangle + |0\rangle|\uparrow\rangle - |2\rangle|\uparrow\rangle}{2}. \tag{2.17}$$

We have a probability of 0.5 of measuring position $p = 0$, and a probability of 0.25 of measuring position $p = 2$ or $p = -2$. It is at the third iteration that the particular

behavior of the walk becomes apparent:

$$|\psi_3\rangle = U|\psi_2\rangle, \tag{2.18}$$

$$= SC\frac{|-2\rangle|\downarrow\rangle + |0\rangle|\downarrow\rangle + |0\rangle|\uparrow\rangle - |2\rangle|\uparrow\rangle}{2}, \tag{2.19}$$

$$= S\frac{|-2\rangle(|\downarrow\rangle + |\uparrow\rangle) + 2|0\rangle|\downarrow\rangle - |2\rangle(|\downarrow\rangle - |\uparrow\rangle)}{2\sqrt{2}}, \tag{2.20}$$

$$= \frac{|-3\rangle|\downarrow\rangle + |-1\rangle|\uparrow\rangle + 2|-1\rangle|\downarrow\rangle - |1\rangle|\downarrow\rangle + |3\rangle|\uparrow\rangle}{2\sqrt{2}}. \tag{2.21}$$

We observe that the probability of measuring position $p = -1$ is 0.625, that is 5 times more than positions $p = -3$, $p = 1$ and $p = 3$. An asymmetry therefore arises during the process. The probability of finding the particle in a particular location on the axis after 100 iterations is shown in figure 2.1. This figure shows that the distribution of the probability of finding the particle in a particular location is remarkably irregular.

Its shape is very different from the bell-shaped curve you would get with a conventional random walk (drawn in orange dotted lines), that is going right or left with a probability of 0.5 at each step. Note that on this curve, only even positions are plotted, since after an even number of iterations, only even positions can be obtained. To study the behavior of this walk, we can decompose the position probability function into two components with opposite directions. At position p and iteration t, if we denote these components $\psi_\downarrow(p,t)$ and $\psi_\uparrow(p,t)$, we can represent the system by the vector

$$\Psi(p,t) = \begin{bmatrix}\psi_\downarrow(p,t)\\ \psi_\uparrow(p,t)\end{bmatrix}. \tag{2.22}$$

The evolution of the system can then be expressed as

$$\Psi(p,t+1) = M_+\Psi(p-1,t) + M_-\Psi(p+1,t), \tag{2.23}$$

with

$$M_+ = \begin{bmatrix}0 & 0\\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}}\end{bmatrix}, M_- = \begin{bmatrix}\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\\ 0 & 0\end{bmatrix}.$$

In this representation, the initial state of the walk is

$$\Psi(0,0) = \begin{bmatrix}1\\0\end{bmatrix}, \tag{2.24}$$

$$\forall n \neq 0, \Psi(n,0) = \begin{bmatrix}0\\0\end{bmatrix}. \tag{2.25}$$

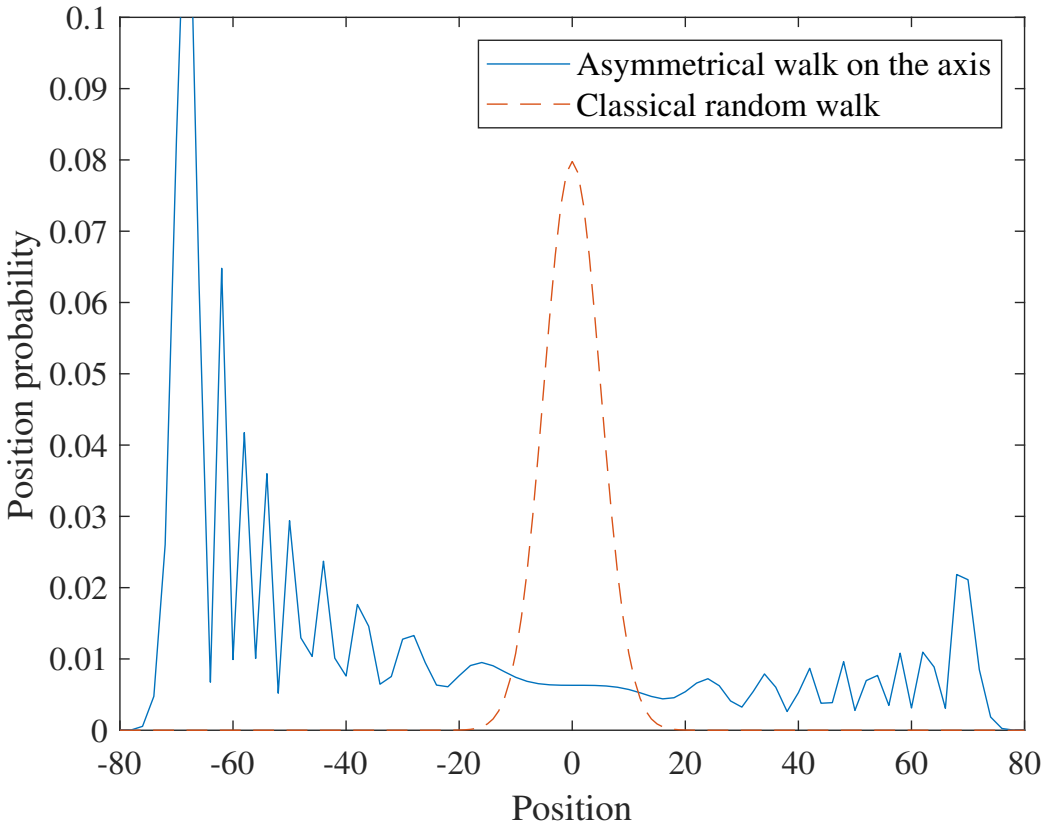

Figure 2.1 Position probability on the axis after 100 iterations of the walk initialized with $|0\rangle|\downarrow\rangle$. Only even-numbered positions are plotted

We can calculate the spatial Fourier transform $\tilde{\Psi}(k,t)$ of $\Psi(p,t)$, defined as

$$\tilde{\Psi}(k,t) = \sum_p \Psi(p,t)\mathrm{e}^{\mathrm{i}kp}, \tag{2.26}$$

with $k \in [-\pi, \pi]$. In the Fourier domain, the system evolves as follows:

$$\begin{aligned}\tilde{\Psi}(k,t+1) &= \sum_p (M_+\Psi(p-1,t) + M_-\Psi(p+1,t))\mathrm{e}^{\mathrm{i}kp}, &(2.27)\\ &= (\mathrm{e}^{\mathrm{i}k}M_+ + \mathrm{e}^{-\mathrm{i}k}M_-)\tilde{\Psi}(k,t), &(2.28)\\ &= M_k\tilde{\Psi}(k,t), &(2.29)\end{aligned}$$

with

$$M_k = \mathrm{e}^{\mathrm{i}k}M_+ + \mathrm{e}^{-\mathrm{i}k}M_- = \frac{1}{\sqrt{2}}\begin{bmatrix}\mathrm{e}^{-\mathrm{i}k} & \mathrm{e}^{-\mathrm{i}k}\\ \mathrm{e}^{\mathrm{i}k} & -\mathrm{e}^{\mathrm{i}k}\end{bmatrix}. \tag{2.30}$$

The state of the system at iteration t is thus

$$M_k^t \widetilde{\Psi}(k,0). \tag{2.31}$$

If $\mu_{k,1}|m_{k,1}\rangle\langle m_{k,1}| + \mu_{k,2}|m_{k,2}\rangle\langle m_{k,2}|$ is the spectral decomposition of M_k, where $\mu_{k,1}$ and $\mu_{k,2}$ are its eigenvalues and $|m_{k,1}\rangle$ and $|m_{k,2}\rangle$ its eigenvectors, then we can write

$$M_k^t = \mu_{k,1}^t |m_{k,1}\rangle\langle m_{k,1}| + \mu_{k,2}^t |m_{k,2}\rangle\langle m_{k,2}|. \tag{2.32}$$

According to Nayak and Vishwanath [NV00], we have $\mu_{k,1} = \mathrm{e}^{-\mathrm{i}\omega_k}$, $\mu_{k,2} = \mathrm{e}^{\mathrm{i}(\pi+\omega_k)}$ and

$$|m_{k,1}\rangle = \frac{1}{\sqrt{2}}\Big(1 + \cos^2 k - \cos k\sqrt{1+\cos^2 k}\Big)^{-\frac{1}{2}} \begin{bmatrix} \mathrm{e}^{-\mathrm{i}k} \\ \sqrt{2}\mathrm{e}^{-\mathrm{i}\omega_k} - \mathrm{e}^{-\mathrm{i}k} \end{bmatrix}, \tag{2.33}$$

$$|m_{k,2}\rangle = \frac{1}{\sqrt{2}}\Big(1 + \cos^2 k + \cos k\sqrt{1+\cos^2 k}\Big)^{-\frac{1}{2}} \begin{bmatrix} \mathrm{e}^{-\mathrm{i}k} \\ -\sqrt{2}\mathrm{e}^{\mathrm{i}\omega_k} - \mathrm{e}^{-\mathrm{i}k} \end{bmatrix}, \tag{2.34}$$

with $\omega_k \in [-\pi/2, \pi/2]$ such that

$$\sin\omega_k = \frac{\sin k}{\sqrt{2}}. \tag{2.35}$$

In the Fourier domain, the initial state is

$$\forall k, \widetilde{\Psi}(k,0) = \begin{bmatrix} 1 \\ 0 \end{bmatrix}. \tag{2.36}$$

We then have

$$\widetilde{\psi}_\uparrow(k,t) = \frac{1}{2}(1 + \frac{\cos k}{\sqrt{1+\cos^2 k}})\mathrm{e}^{-\mathrm{i}\omega_k t} + \frac{(-1)^t}{2}(1 - \frac{\cos k}{\sqrt{1+\cos^2 k}})\mathrm{e}^{\mathrm{i}\omega_k t}, \tag{2.37}$$

$$\widetilde{\psi}_\downarrow(k,t) = \frac{\mathrm{i}\mathrm{e}^{\mathrm{i}k}}{2\sqrt{1+\cos^2 k}}(\mathrm{e}^{-\mathrm{i}\omega_k t} - (-1)^t \mathrm{e}^{\mathrm{i}\omega_k t}). \tag{2.38}$$

Inverting the Fourier transform, we finally obtain

$$\psi_\uparrow(p,t) = \frac{1+(-1)^{p+t}}{4\pi}\int_{-\pi}^{\pi}\Big(1 + \frac{\cos k}{\sqrt{1+\cos^2 k}}\Big)\mathrm{e}^{-\mathrm{i}(\omega_k t + kp)}\,\mathrm{d}k, \tag{2.39}$$

$$\psi_\downarrow(p,t) = \frac{1+(-1)^{p+t}}{4\pi}\int_{-\pi}^{\pi}\frac{\mathrm{e}^{\mathrm{i}k}}{\sqrt{1+\cos^2 k}}\mathrm{e}^{-\mathrm{i}(\omega_k t + kp)}\,\mathrm{d}k. \tag{2.40}$$

The probability of finding the particle at position $p = \alpha t$ at iteration t is

$$P(\alpha, t) = |\psi_\downarrow(p,t)|^2 + |\psi_\uparrow(p,t)|^2. \tag{2.41}$$

These expressions show that the probability of finding the particle at position is zero when $p + t$ is odd, that is every other point. It is also possible to find an asymptotic expression that approximates the behavior of the walk when t becomes large. The asymptotic asymptotic position probability is expressed as

$$P(\alpha, t) \approx \frac{1 + (-1)^{(\alpha+1)t}}{\pi t |\omega''_{k_\alpha}|}\Big((1-\alpha)^2 \cos^2(\phi_\alpha t + \frac{\pi}{4}) + (1-\alpha^2)\cos^2(\phi_\alpha t + \frac{\pi}{4} + k_\alpha)\Big), \tag{2.42}$$

where ω'_k and ω''_k are the first and second derivatives of ω_k, k_α is the root of equation $\omega'_k + \alpha$ in $[0, \pi]$ and $\phi_\alpha = -\omega_{k_\alpha} - \alpha k_\alpha$. A comparison of the exact probability of presence and its asymptotic approximation is shown in figure 2.2.

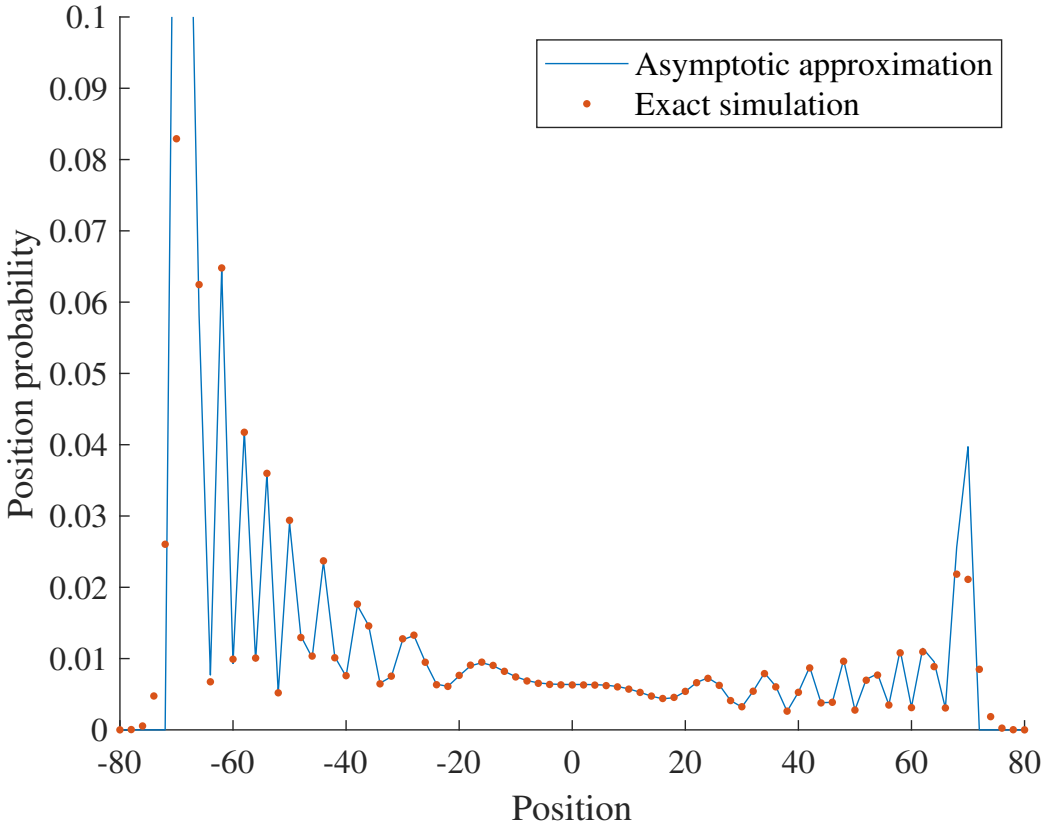

Figure 2.2 Comparison of the exact and asymptotic position probabilities of the equation (2.42) on the axis after 100 iterations. Only even positions are plotted

It is possible to extract from the asymptotic approximation the non-oscillating component, generally called P_{slow} :

$$P_{\text{slow}}(\alpha, t) = \frac{1-\alpha}{\pi t |\omega''_{k_\alpha}|}. \tag{2.43}$$

The P_{slow} approximation, shown in figure 2.3, is useful in the study of the walk on the axis, as it contributes more strongly than the oscillating component to the statistical properties of the distribution.

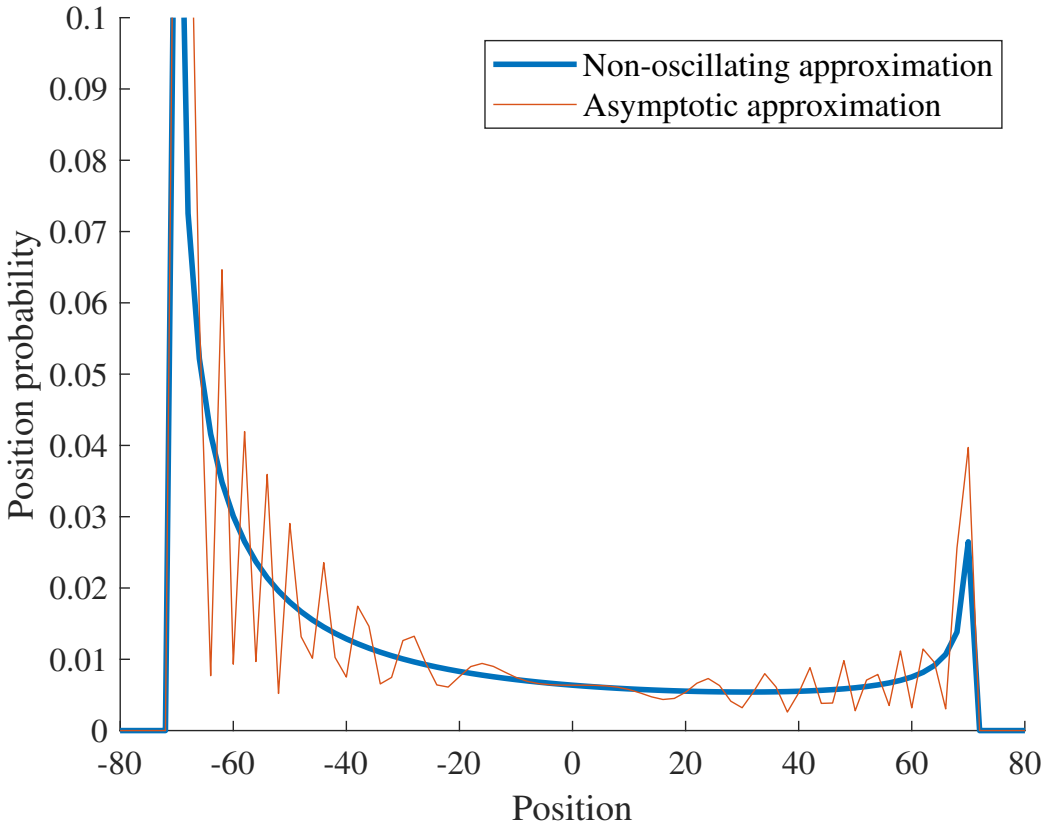

Figure 2.3 Comparison of the slow position probability P_{slow} and asymptotic position probability on the axis after 100 iterations. Only even-numbered positions are plotted. P_{slow} is multiplied by 2 as it also contains odd-numbered points.

Different presence probability distributions can be obtained by choosing different initial states $|\psi_0\rangle$. For example, a distribution symmetrical to the one studied above is obtained if we initialize with $|\psi_0\rangle = |0\rangle|\uparrow\rangle$. To obtain a symmetrical distribution with respect to the walking origin, initialize with

$$|\psi_0\rangle = |0\rangle \frac{|\downarrow\rangle + \mathrm{i}|\uparrow\rangle}{\sqrt{2}}. \tag{2.44}$$

The resulting probability distribution is symmetrical, but still very different from the classical case, as shown in figure 2.4.

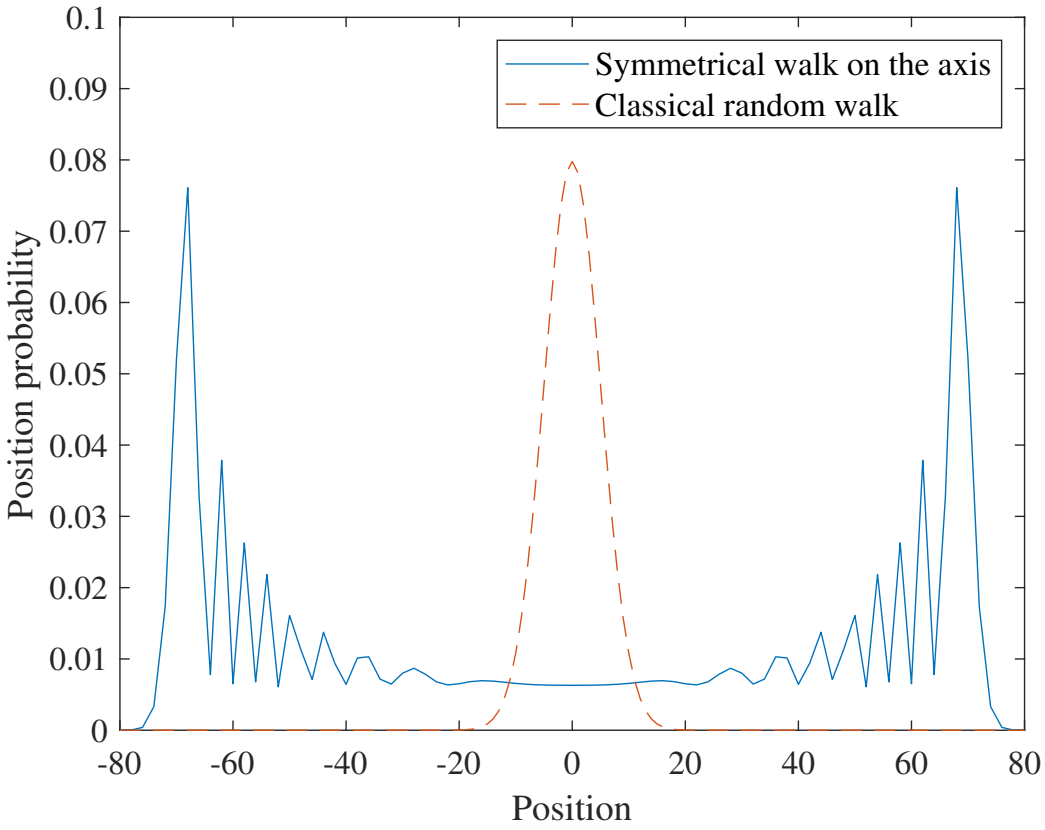

Figure 2.4 Position probability on axis after 100 iterations of the symmetrical walk. Only even positions are plotted

2.2. Walk on hypercube

Hypercube graphs are particularly suitable for representing binary words. On a hypercube of dimension n, the $N = 2^n$ vertices of all n-bit binary words can be assigned in such a way that each binary word is adjacent to n words located at a Hamming distance equal to 1, that is, differing by a single bit. They are therefore widely used in information theory.

As in the case of the walk on the axis, the state vector of the system lies in a composite Hilbert space $\mathcal{H} = \mathcal{H}^{\mathrm{S}} \otimes \mathcal{H}^{\mathrm{C}}$. In the case of the n-dimensional hypercube, these subspaces are

$$\mathcal{H}^{\mathrm{S}} = \mathrm{span}(\{|p\rangle \mid p \in \mathbb{Z}_2^n\}), \tag{2.45}$$

$$\mathcal{H}^{\mathrm{C}} = \mathrm{span}(\{|d\rangle \mid d \in \{1, 2, \ldots, n\}\}), \tag{2.46}$$

The dimensions of these spaces are

$$\dim(\mathcal{H}^{\mathrm{S}}) = N, \tag{2.47}$$

$$\dim(\mathcal{H}^{\mathrm{C}}) = n, \tag{2.48}$$

which implies that the dimension of the global space $\mathcal{H}$ is

$$\dim(\mathcal{H}) = nN. \tag{2.49}$$

As on the axis, the walk on the hypercube consists of the repeated application of a uniform walking operator $U = SC$, where S is the shift operator and C is the coin operator. These two operators are defined in a similar way to those used for walking on the axis.

In this work, the position p on the dimension n hypercube will be designated as needed by a binary word in $\mathbb{Z}_2^n$, or by its decimal representation in $\mathbb{Z}_N$. For example, the state corresponding to the vertex 0010 of the dimension 4 hypercube could be written as $|0010\rangle$ or $|4\rangle$. Note that the most significant bit is always located to the right of the binary word. The vertices of the hypercube are numbered so that a move along the d-th dimension of the hypercube corresponds to an inversion of the d-th bit from the right in the binary word of the position. For example, after moving in the second direction, the state $|0010\rangle|2\rangle$ will become $|0000\rangle|2\rangle$.

To construct the operator S capable of performing this shift, we build n operators S_d of size $N \times N$, each performing the shift in direction d. To invert a bit, we locally apply the operator X, defined by equation (1.17). As a reminder, $X|0\rangle = |1\rangle$ and $X|1\rangle = |0\rangle$. An operator S_d must therefore apply X to the d-th qubit from the right, and I to all the others. The result is

$$S_d = I^{\otimes(n-d)} \otimes X \otimes I^{\otimes(d-1)}. \tag{2.50}$$

From the operators S_d, it is simpler to construct the shift operator in $\mathcal{H}^{\mathrm{C}} \otimes \mathcal{H}^{\mathrm{S}}$ space. The shift operator in this space, which we will denote S^{CS}, can be expressed as

$$S^{\mathrm{CS}} = \sum_{d=1}^{n} |d\rangle\langle d| \otimes S_d. \tag{2.51}$$

This is a block-diagonal matrix where the blocks are the n matrices S_d arranged in ascending order of d. The S^{CS} matrix is shown in figure 2.6 for $n = 4$.

On the hypercube, the Fourier transform is equivalent to the application of Hadamard matrices. Indeed, the unit matrix performing the Fourier transform is

$$U_{\mathbf{F}} = \frac{1}{\sqrt{k}} \begin{bmatrix} \omega_k^{0\times0} & \omega_k^{0\times1} & \dots & \omega_k^{0\times(k-1)} \\ \omega_k^{1\times0} & \omega_k^{1\times1} & \dots & \omega_k^{1\times(k-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \omega_k^{(k-1)\times0} & \omega_k^{(k-1)\times1} & \dots & \omega_k^{(k-1)\times(k-1)} \end{bmatrix}, \tag{2.52}$$

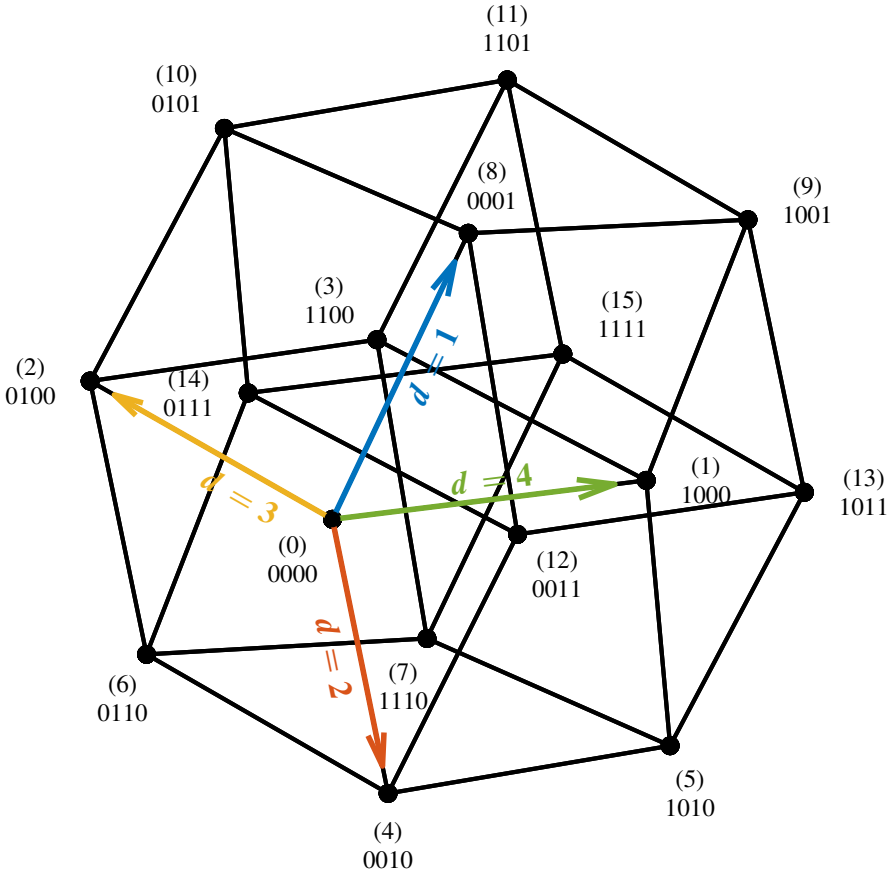

Figure 2.5 4-dimensional hypercube with numbered vertices and directions

with $\omega_k = \mathrm{e}^{-\mathrm{i}2\pi/k}$. Since there are only two elements per dimension, we have $k = 2$ and this implies $U_{\mathbf{F}} = H$, where H is the Hadamard matrix defined in equation (1.13). We define H_N the $N \times N$ Hadamard matrix that performs the N-dimensional Fourier transform, such that, for $N = 2^n$, we have $H_N = H^{\otimes n}$. It can be shown that the S_d blocks are diagonalizable by Fourier transform. Let $\widetilde{S}_d$ be the Fourier transform of S_d. We have

$$\begin{aligned}
\widetilde{S}_d &= H_N S_d H_N, && (2.53)\\
&= H^{\otimes n}\left(I^{\otimes(n-d)} X I^{\otimes(d-1)}\right) H^{\otimes n}, && (2.54)\\
&= (HIH)^{\otimes(n-d)} \otimes (HXH) \otimes (HIH)^{\otimes(d-1)}, && (2.55)\\
&= I^{\otimes(n-d)} \otimes Z \otimes I^{\otimes(d-1)}, && (2.56)
\end{aligned}$$

because $H^2 = I$, and where Z is the Pauli matrix defined in equation (1.19). Since I and Z are diagonal, then the $\widetilde{S}_d$ matrices are also diagonal. Each of them has, on its

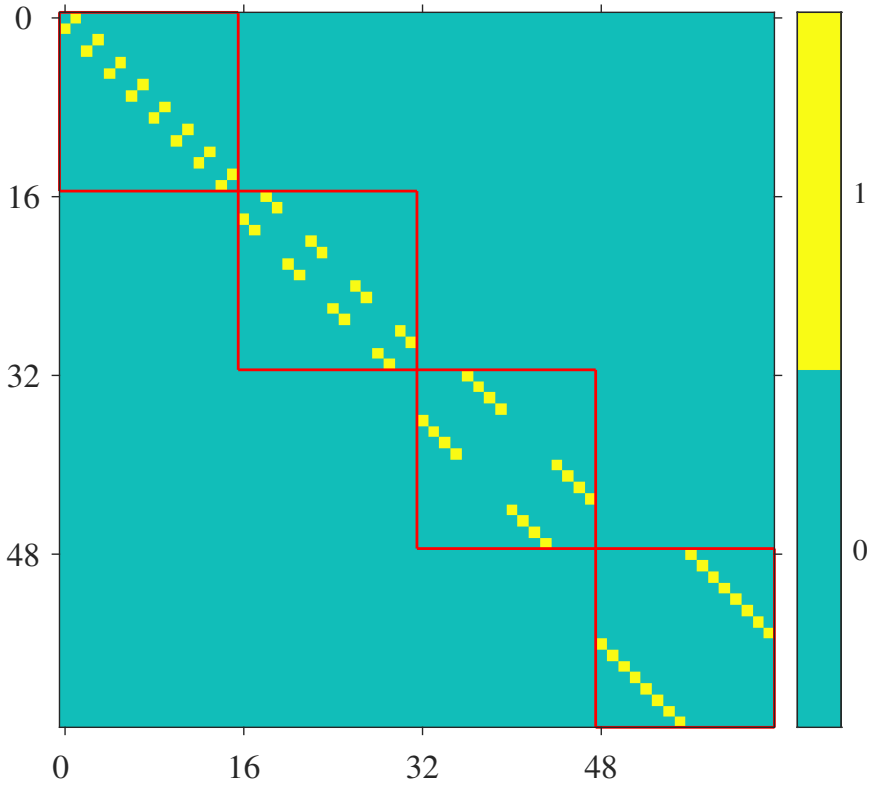

Figure 2.6 Shift operator S^{CS} for $n = 4$. The S_d blocks are delimited by red lines.

diagonal, 2^{n-d} repetitions of a diagonal block consisting of 2^{d-1} coefficients 1 followed by 2^{d-1} coefficients -1, as shown in figure 2.7.

The Fourier transform preserves the block-diagonal character of a matrix. We can therefore construct $\widetilde{S}^{\mathrm{CS}}$ the spatial Fourier transform of S^{CS} made up of $\widetilde{S}_d$ blocks. This is equivalent to defining $\widetilde{S}^{\mathrm{CS}}$ by

$$\widetilde{S}^{\mathrm{CS}} = (I_n \otimes H_N) S^{\mathrm{CS}} (I_n \otimes H_N). \tag{2.57}$$

The shift operator has a simple structure in $\mathcal{H}^{\mathrm{C}} \otimes \mathcal{H}^{\mathrm{S}}$, but we will also need its representation in $\mathcal{H} = \mathcal{H}^{\mathrm{S}} \otimes \mathcal{H}^{\mathrm{C}}$. We can switch from one representation to the other using permutation matrices. We will use the matrix $P_{N,n}$ defined in appendix C. We have

$$S = P_{N,n} S^{\mathrm{CS}} P_{N,n}^{\mathsf{T}}. \tag{2.58}$$

We can then see that the structure of the operator S is more complex in $\mathcal{H}^{\mathrm{S}} \otimes \mathcal{H}^{\mathrm{C}}$ than in $\mathcal{H}^{\mathrm{C}} \otimes \mathcal{H}^{\mathrm{S}}$, as illustrated in figure 2.8, but as the opposite is true for the operator C, there is no representation better than the other. We therefore arbitrarily choose to use

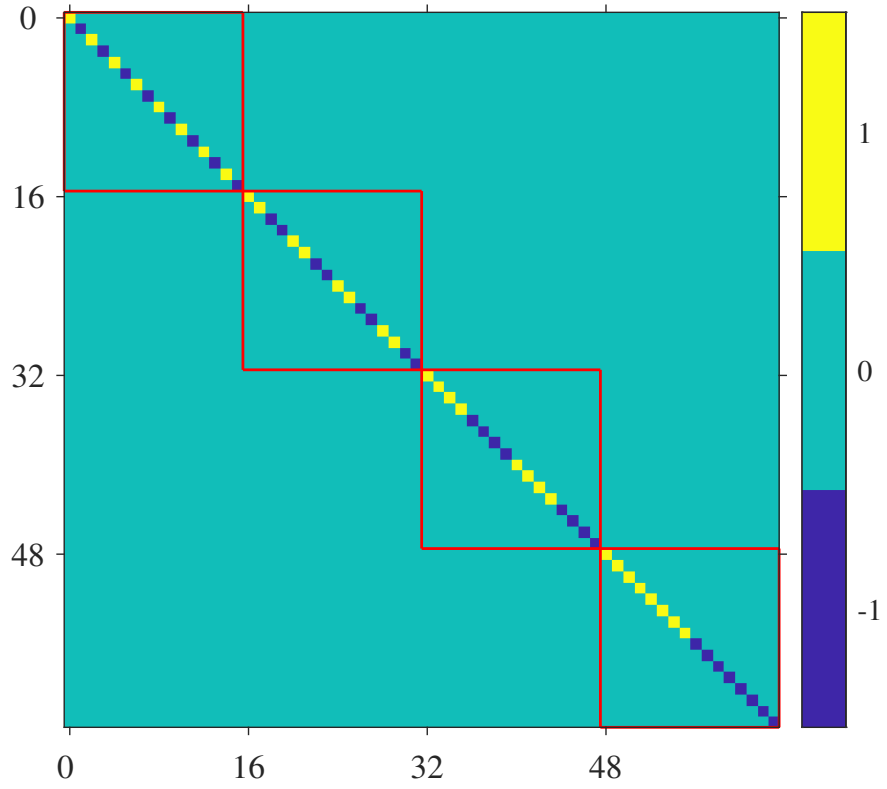

Figure 2.7 Diagonalized shift operator $\widetilde{S}^{\mathrm{CS}}$ for $n = 4$. The $\widetilde{S}_d$ blocks are delimited by red lines.

$\mathcal{H} = \mathcal{H}^{\mathrm{S}} \otimes \mathcal{H}^{\mathrm{C}}$ as the reference space, but it is always possible to switch from one representation to the other.

It is also possible to diagonalize the shift operator in $\mathcal{H}$ by spatial Fourier transform. Let us call F the spatial Fourier transform operator in $\mathcal{H}$, such that

$$F = H_N \otimes I_n. \tag{2.59}$$

The $\widetilde{S} = FSF$ matrix is shown in figure 2.9. This is a diagonal matrix with a remarkable structure that can be split into N diagonal blocks $\widetilde{S}^{(p)}$ containing the terms 1 and -1. If we associate the values 1 and -1 respectively with bits 0 and 1, we can read in each block $\widetilde{S}^{(p)}$ the binary word b associated with position p.

The choice of the coin operator C is more complex for the walk on a hypercube than on an axis. As C has no action in $\mathcal{H}^{\mathrm{S}}$, it can be decomposed into

$$C = I_N \otimes C_0, \tag{2.60}$$

where C_0 is a $n \times n$ matrix acting in $\mathcal{H}^{\mathrm{C}}$. We can lay down two criteria for the operator C_0, namely that it be unitary, but also that it be symmetrical to dimension permutations.

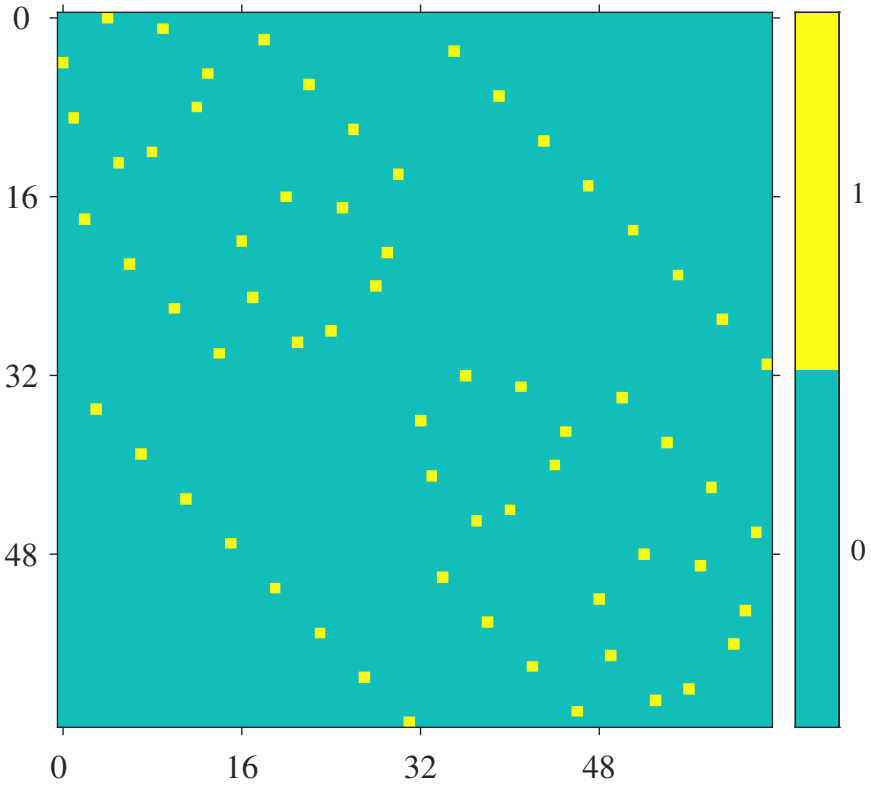

Figure 2.8 Shift operator S for n =4

Indeed, the numbering of the hypercube dimensions is arbitrary, and changing it should not alter the walk. As shown in [MR02], an operator that satisfies these conditions is necessarily of the form

$$C_0 = \begin{bmatrix} a & b & b & \dots & b \\ b & a & b & \dots & b \\ b & b & a & \cdots & b \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b & b & b & \dots & a \end{bmatrix}, \tag{2.61}$$

with $|a|^2 + (n-1)|b|^2 = 1$ and $|a-b|^2 = 1$. Solutions exist only if $1 - 2/n \leqslant |a| \leqslant 1$, with two possible values of b per value of a. Among the matrices in this family, we choose the one that is furthest from a diagonal unit matrix, i.e. that mixes the directions the most. Let cI_n be a diagonal unit matrix with $|c| = 1$. We have

$$\|C_0 - cI_n\| = 2n(1 - \mathrm{Re}(ac^*)), \tag{2.62}$$

$$\geqslant 2n(1 - |a|), \tag{2.63}$$

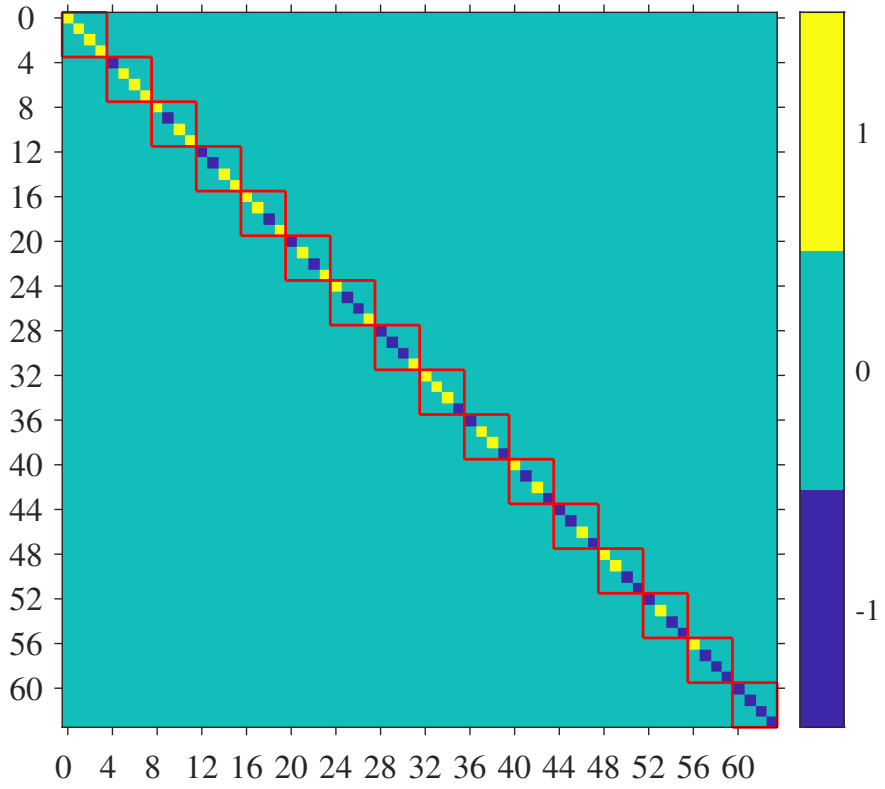

Figure 2.9 Diagonalized shift operator $\widetilde{S}$ for $n = 4$. The $\widetilde{S}^{(p)}$ blocks are delimited by red lines.

where $\|A\| = \mathrm{tr}(A^\dagger A)$ denotes the operator norm of the matrix A. We can see that $2n(1 - |a|)$ is maximized when $|a|$ becomes small. We therefore choose the smallest possible value, $|a| = 1 - 2/n$. This gives us the Grover G diffusion operator, named after Grover's algorithm presented in chapter 3. By choosing a to be a negative real number, we can write this operator as

$$G = 2|u_n\rangle\langle u_n| - I_n, \tag{2.64}$$

where $|u_n\rangle$ is the uniform superposition of all $\mathcal{H}^C$ basis states, that is

$$|u_n\rangle = \frac{1}{\sqrt{n}} \sum_{x=1}^{n} |x\rangle. \tag{2.65}$$

Finally, the expression for the coin operator in $\mathcal{H}$ is

$$C = I_N \otimes G. \tag{2.66}$$

The suitability of a graph for random walks can be gauged by studying certain characteristic times, such as mixing or reaching times. Although these notions are not explored in this work, we may note that Kempe has shown in [Kem05] that the time to go from a vertex to its opposite is polynomial in the dimension of the hypercube, which is exponentially faster than classical walks. This is an encouraging result, suggesting that some classical hypercube walk algorithms could be accelerated by quantum computing.

3. Quantum search algorithm

Introduced in *A Fast Quantum Mechanical Algorithm for Database Search* [Gro96] by Grover, the quantum search algorithm, or simply Grover's algorithm, can find with high probability an element in a database that meets a given criterion faster than a classical algorithm. In a database of N unsorted elements, a classical algorithm requires $\mathcal{O}(N)$ operations to find an element that satisfies any given criterion. For example, if we have 1 000 words scrambled and are looking for one that begins with the letter "A", we need to read them one by one until we find one that matches. In the worst case, there is only one, and it is at the end of the list, so you have to perform 1 000 operations.

Grover's algorithm is able to perform this task in $\mathcal{O}\left(\sqrt{N}\right)$, which represents a quadratic gain in time. Unlike other quantum algorithms, such as Shor's famous algorithm for prime factorization in polynomial time [Sho94], Grover's algorithm offers no exponential gain compared with its classical equivalent. However, such a gain is not negligible, especially when N becomes large. According to Nielsen and Chuang [NC10], Grover's algorithm could speed up the resolution of NP-complete problems. It is also possible to use Grover's algorithm to speed up brute force attacks, as shown in *Grover vs. McEliece* [Ber10].

3.1. Quantum Oracle and Grover iteration

The element at the heart of Grover's algorithm is the oracle, an operator capable of recognizing whether or not an element is a solution to the problem associated with it. Any n-bit problem contains at most $N = 2^n$ elements that can be numbered from 0 to $N - 1$. Let $f(x) = 1$ if x is a solution to the problem and $f(x) = 0$ otherwise, with $x \in \mathbb{Z}_N$. The problem is equivalent to finding the antecedents of 1 by f.

From the function f, we can devise an operator capable of recognizing solutions, the oracle. Let the operator O be such that

$$|x\rangle|q\rangle \xrightarrow{O} |x\rangle|q \oplus f(x)\rangle, \tag{3.1}$$

where $|x\rangle$ is the state corresponding to the element under test, $|q\rangle$ is an arbitrary fixed qubit and $\oplus$ denotes modulo 2 addition . Such an operator O is involutive, meaning that it is its own inverse. Indeed, we have

$$|x\rangle|q \oplus f(x)\rangle \xrightarrow{O} |x\rangle|q \oplus f(x) \oplus f(x)\rangle = |x\rangle|q\rangle. \tag{3.2}$$

Furthermore, we can determine the $2N$ eigenvectors of O, all of the form $|x\rangle|+\rangle$ and $|x\rangle|-\rangle$. We have

$$O\Big(|x\rangle\frac{|0\rangle+|1\rangle}{\sqrt{2}}\Big) = |x\rangle\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \tag{3.3}$$

$$O\Big(|x\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}}\Big) = (-1)^{f(x)}|x\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}}. \tag{3.4}$$

We observe that the eigenvectors $|x\rangle|+\rangle$ are all associated with eigenvalue 1, and that the eigenvectors $|x\rangle|-\rangle$ are associated with eigenvalues 1 or -1 depending on $f(x)$. The distribution of eigenvalues therefore depends on the problem, but the eigenvectors are always the same, and are all orthogonal to each other. We deduce that O is a normal operator as well as being involutive, which means that it is Hermitian and, more importantly, unitary. The oracle O is a valid quantum operator, and can theoretically be implemented.

The case of eigenvectors $|x\rangle|-\rangle$ is especially useful: if we consider that we always initialize with $|q\rangle = |-\rangle$, the action of the oracle becomes

$$|x\rangle|-\rangle \xrightarrow{O} (-1)^{f(x)}|x\rangle|-\rangle, \tag{3.5}$$

and we observe that the qubit $|q\rangle$ remains unchanged. Consequently, it is often omitted, and the action of the oracle can be summarized by

$$|x\rangle \xrightarrow{O} (-1)^{f(x)}|x\rangle. \tag{3.6}$$

The oracle is then able to "mark" solutions to the problem.

We generally denote M the number of solutions to a given problem. We also define $|s\rangle$ the uniform superposition of these M solutions and $|\bar{s}\rangle$ the uniform superposition of the $N-M$ non-solutions. We then have

$$|s\rangle = \frac{1}{\sqrt{M}}\sum_{\substack{x\in\mathbb{Z}_N \\ f(x)=1}}|x\rangle, \tag{3.7}$$

$$|\bar{s}\rangle = \frac{1}{\sqrt{N-M}}\sum_{\substack{x\in\mathbb{Z}_N \\ f(x)=0}}|x\rangle, \tag{3.8}$$

Consider the plane generated by the vectors $|s\rangle$ and $|\bar{s}\rangle$. Once projected into this plane, any state $|\psi\rangle$ can then be expressed as $\alpha|s\rangle + \beta|\bar{s}\rangle$, and the application of the oracle O will result in

$$\alpha|s\rangle + \beta|\bar{s}\rangle \xrightarrow{O} -\alpha|s\rangle + \beta|\bar{s}\rangle, \tag{3.9}$$

which corresponds to a reflection of the $|\psi\rangle$ state with respect to $|\bar{s}\rangle$.

According to its definition, the oracle can be represented by a diagonal matrix consisting of -1 at the positions of the solutions and 1 elsewhere. As an example, the oracle of a problem with $N = 16$ elements and solutions at positions 0,3 and 6, is represented is represented in figure 3.1.

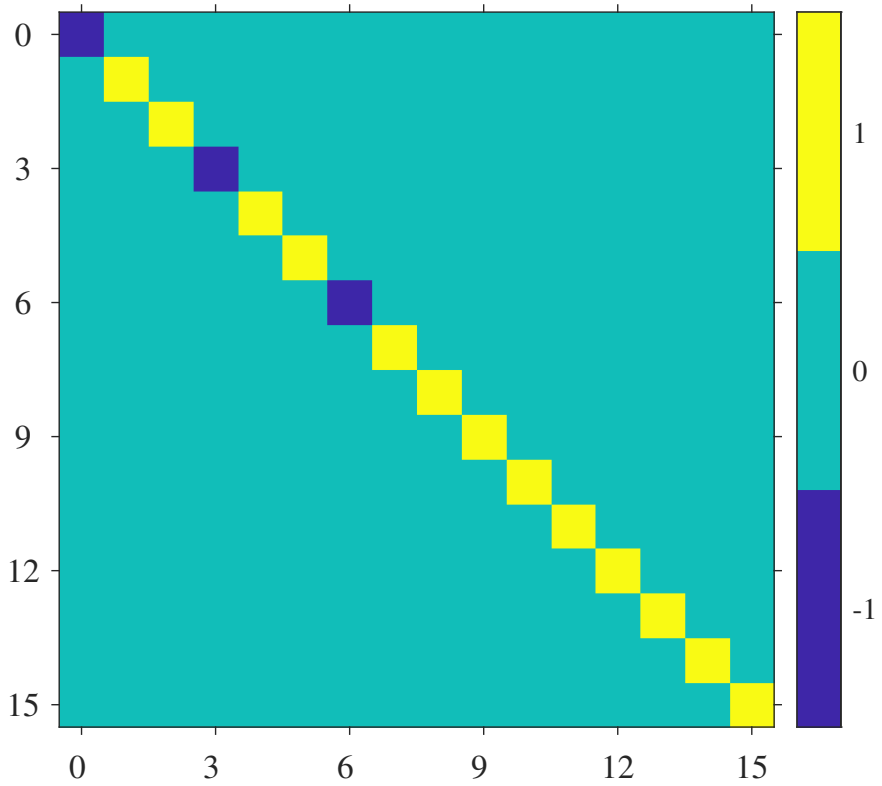

Figure 3.1 Oracle of a $N = 16$ element problem whose solutions are 0, 3 and 6

From the definition of an oracle, we might think that designing one requires prior knowledge of the solutions to the problem it is solving. In reality, it is only necessary to be able to check quickly whether a given element is a solution or not, which is always possible when working on NP problems. The difference with the classical case comes from quantum superposition: if we build a superposition of N elements, then the oracle is capable of evaluating them all at once.

The implementation of an oracle is generally not an easy task, and the number of quantum gates required varies from problem to problem. In this work, we will consider the oracle as a black box, and we will count the number of calls to the oracle to evaluate the complexity of Grover's algorithm.

Grover's algorithm consists of the repeated application of the oracle associated with the problem O followed by the Grover diffusion operator G, defined in the equation (2.64).

A Grover iteration is therefore the application of GO.

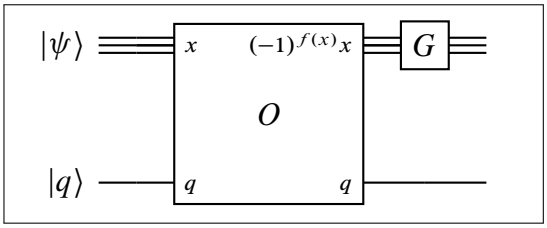

Figure 3.2 Circuit of a Grover iteration. The qubit $|q\rangle$ ignored in the equations is depicted

The effect of the operator G on any state $|\psi\rangle = \sum_x \alpha_x |x\rangle$ is

$$G|\psi\rangle = G \sum_{x\in\mathbb{Z}_N} \alpha_x |x\rangle, \tag{3.10}$$

$$= (2|u_N\rangle\langle u_N| - I_N) \sum_{x\in\mathbb{Z}_N} \alpha_x |x\rangle, \tag{3.11}$$

$$= \sum_{x\in\mathbb{Z}_N} (2|u_N\rangle\langle u_N|\alpha_x - \alpha_x)|x\rangle, \tag{3.12}$$

$$= \sum_{x\in\mathbb{Z}_N} (2\langle\alpha\rangle - \alpha_x)|x\rangle. \tag{3.13}$$

where $\langle\alpha\rangle$ denotes the average value of the α_x coefficients. This term appears because

$$\langle u_N|x\rangle = \frac{1}{\sqrt{N}}, \tag{3.14}$$

therefore

$$\sum_{x\in\mathbb{Z}_N} |u_N\rangle\langle u_N|\alpha_x|x\rangle = \sum_{x\in\mathbb{Z}_N} \frac{\alpha_x}{\sqrt{N}}|u_N\rangle, \tag{3.15}$$

$$= \Big(\sum_{x\in\mathbb{Z}_N} \alpha_x\Big)\frac{1}{\sqrt{N}}|u_N\rangle, \tag{3.16}$$

$$= \sqrt{N}\,\langle\alpha\rangle|u_N\rangle. \tag{3.17}$$

According to equation (2.65), we thus have

$$\sum_{x\in\mathbb{Z}_N} |u_N\rangle\langle u_N|\alpha_x|x\rangle = \langle\alpha\rangle \sum_{x\in\mathbb{Z}_N} |x\rangle. \tag{3.18}$$

We then see that

$$\frac{1}{2}(|\psi\rangle + G|\psi\rangle) = \frac{1}{2}\Big(\sum_{x\in\mathbb{Z}_N}(2\langle\alpha\rangle - \alpha_x)|x\rangle + \sum_{x\in\mathbb{Z}_N}\alpha_x|x\rangle\Big), \tag{3.19}$$

$$= \frac{1}{2}\sum_{x\in\mathbb{Z}_N}(2\langle\alpha\rangle)|x\rangle, \tag{3.20}$$

$$= \langle\alpha\rangle\sum_{x\in\mathbb{Z}_N}|x\rangle, \tag{3.21}$$

$$= \langle\alpha\rangle\sqrt{N}|u_N\rangle, \tag{3.22}$$

which means that $|\psi\rangle$ and $G|\psi\rangle$ are symmetrical with respect to $|u_N\rangle$, and therefore that G applies a reflection with respect to it.

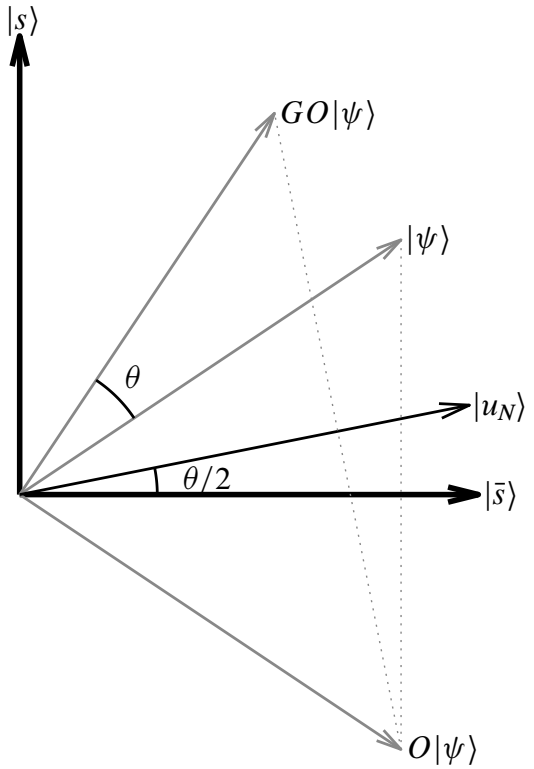

Figure 3.3 Effect of the Grover iteration GO on an arbitrary state $|s\rangle$ in the plane directed by $|s\rangle$ and $|\bar{s}\rangle$

In the plane directed by $|s\rangle$ and $|\bar{s}\rangle$, the Grover iteration GO is therefore the sequence of two reflections: with respect to $|\bar{s}\rangle$ and then with respect to $|u\rangle$. In a plane, the

application of two reflections is equivalent to a rotation, as illustrated in figure 3.3. Each iteration therefore rotates the $|\psi\rangle$ state by a constant angle over the iterations, which will be defined in the next section. When we measure $|\psi\rangle$, the probability of success will be

$$\mathbf{P}(s) = |\langle s|\psi\rangle|^2. \tag{3.23}$$

We need to determine the number of iterations GO that maximizes $\mathbf{P}(s)$, that is, the one that gets the states $|s\rangle$ and $|\psi\rangle$ as close as possible.

3.2. Grover's algorithm execution

For a given n-bit problem, there are $N = 2^n$ elements. We start by constructing a uniform superposition of all these elements. To do this, we initialize n qubits to $|0\rangle$ and apply Hadamard gates to them. We then obtain the initial state $|\psi_0\rangle = H^{\otimes n}|0\rangle^{\otimes n} = |u_N\rangle$.

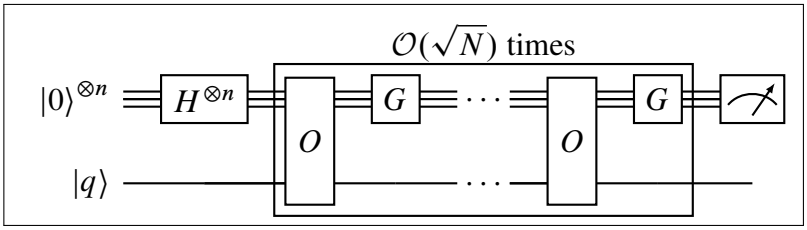

Figure 3.4 Circuit for Grover's algorithm. The $|q\rangle$ qubit ignored in the equations is depicted on the bottom wire

We then apply R Grover iterations to $|\psi_0\rangle$ and measure it. The result of this measurement is $|x_R\rangle$, one of the N states $|x\rangle$. It now remains to determine R to maximize the probability that x_R is a solution.

We can express $|u_N\rangle$ as a superposition of states $|s\rangle$ and $|\bar{s}\rangle$. We have

$$|u_N\rangle = \sqrt{\frac{M}{N}}|s\rangle + \sqrt{\frac{N-M}{N}}|\bar{s}\rangle, \tag{3.24}$$

where M is the number of solutions. We consider only the case where $M < N/2$. We can define an angle θ such that

$$\sin\frac{\theta}{2} = \sqrt{\frac{M}{N}}, \tag{3.25}$$

$$\cos\frac{\theta}{2} = \sqrt{\frac{N-M}{N}}, \tag{3.26}$$

which is equivalent to

$$\sin\theta = \frac{2\sqrt{M(N-M)}}{N}, \tag{3.27}$$

$$\cos\theta = \frac{N-2M}{N}. \tag{3.28}$$

We can then express the $|u_N\rangle$ state as

$$|u_N\rangle = \sin\frac{\theta}{2}|s\rangle + \cos\frac{\theta}{2}|\bar{s}\rangle. \tag{3.29}$$

The state vector $|u_N\rangle$ is therefore oriented at an angle $\theta/2 \in [0, \pi/4]$ with respect to $|\bar{s}\rangle$.

As the oracle O applies a reflection with respect to $|\bar{s}\rangle$, we have

$$O|u_N\rangle = -\sin\frac{\theta}{2}|s\rangle + \cos\frac{\theta}{2}|\bar{s}\rangle, \tag{3.30}$$

and $O|u_N\rangle$ is oriented at an angle $-\theta/2$ with respect to $|\bar{s}\rangle$.

The operator G then applies a reflection with respect to $|u_N\rangle$, of orientation $\theta/2$, yielding $GO|u_N\rangle$ oriented by $3\theta/2$ with respect to $|\bar{s}\rangle$. After the first iteration, we obtain the state

$$|\psi_1\rangle = \cos\Big(\frac{3}{2}\theta\Big)|\bar{s}\rangle + \sin\Big(\frac{3}{2}\theta\Big)|s\rangle. \tag{3.31}$$

By repeating the k operation, we obtain

$$|\psi_k\rangle = \cos\Big(\frac{2k+1}{2}\theta\Big)|\bar{s}\rangle + \sin\Big(\frac{2k+1}{2}\theta\Big)|s\rangle. \tag{3.32}$$

Each iteration rotates the state by an angle θ in the plane directed by $|s\rangle$ and $|\bar{s}\rangle$. According to the equations (3.24) and (3.29), the initial state of the algorithm is oriented by $\theta/2$ with respect to $|\bar{s}\rangle$. To maximize the chances of finding a solution, the state must be orthogonal to $|\bar{s}\rangle$. We therefore need to apply a rotation of $\pi/2 - \theta/2$, i.e. $\arccos\sqrt{M/N}$. The number of iterations to be applied is therefore

$$R = \frac{\arccos\sqrt{\frac{M}{N}}}{\theta}, \tag{3.33}$$

rounded to the nearest integer. We have $\arccos\sqrt{M/N} < \pi/2$. Furthermore, as $\theta \geqslant 0$, we have $\theta/2 \geqslant \sin\theta/2 = \sqrt{M/N}$ and thus

$$R \leqslant \left\lceil \frac{\pi}{4}\sqrt{\frac{N}{M}} \right\rceil, \tag{3.34}$$

where $\lceil x \rceil$ denotes the rounding up of x. This gives an upper bound on the number of iterations R that is easier to interpret than its exact definition. We can therefore confirm that Grover's algorithm makes $\mathcal{O}\left(\sqrt{N}\right)$ calls to the oracle. It is shown that Grover's algorithm is optimal, in the sense that no quantum algorithm can perform the same task in fewer than $\mathcal{O}\left(\sqrt{N}\right)$ calls to an oracle.

In order to estimate the number of iterations R of the algorithm, the number of solutions M must be known in advance, without actually knowing them. Fortunately, there is a "quantum counting" algorithm [BHT98], which makes it possible to estimate the number of solutions to a problem from the oracle. We can therefore consider that M is always known.

If we apply Grover's algorithm when $M \geqslant N/2$, we have $\theta/2 \in [\pi/2, \pi]$, and by applying the equation (3.33), we always find that the number of iterations is zero. This is equivalent to randomly picking one of the N elements, and the probability of finding a solution is $\mathbf{P}(s) = M/N \geqslant 1/2$. One way of increasing the probability of success is to double the number of elements by adding N non-solutions. This ensures that less than half the elements are solutions, but requires the addition of a qubit.

As the state of the system rotates by an angle θ at each iteration, the angle between the state $|\psi_R\rangle$ obtained after R iterations and $|\bar{s}\rangle$ is at most $\theta/2$, meaning $\pi/4$. The probability of success of Grover's algorithm is therefore bounded by

$$\mathbf{P}(s) \geqslant \left|\cos\frac{\pi}{4}\right|^2 = \frac{1}{2}. \tag{3.35}$$

This minimum success probability of $1/2$ is reached when $M = N/2$. Generally speaking, performance is much better. We can show that when $M = N/2$, we have

$$\mathbf{P}(s) \geqslant 1 - \frac{M}{N}. \tag{3.36}$$

The probability of success curve for Grover's algorithm is shown in figure 3.5. The curve maintains the same pattern for all values of N.

Example with a 10-bit problem

Suppose we are looking for the solutions of a problem on $n = 10$ bit elements, that is $N = 1\,024$ elements, having $M = 25$ solutions. We consider the plane directed by $|s\rangle$ and $|\bar{s}\rangle$. The initial state $|\psi_0\rangle$ is

$$|\psi_0\rangle = \sqrt{\frac{25}{1\,024}}|s\rangle + \sqrt{\frac{999}{1\,024}}|\bar{s}\rangle. \tag{3.37}$$

If we now measure, the probability of success is

$$\mathbf{P}_0(s) = |\langle s|\psi_0\rangle|^2 = \frac{25}{1\,024} \approx 0.024. \tag{3.38}$$

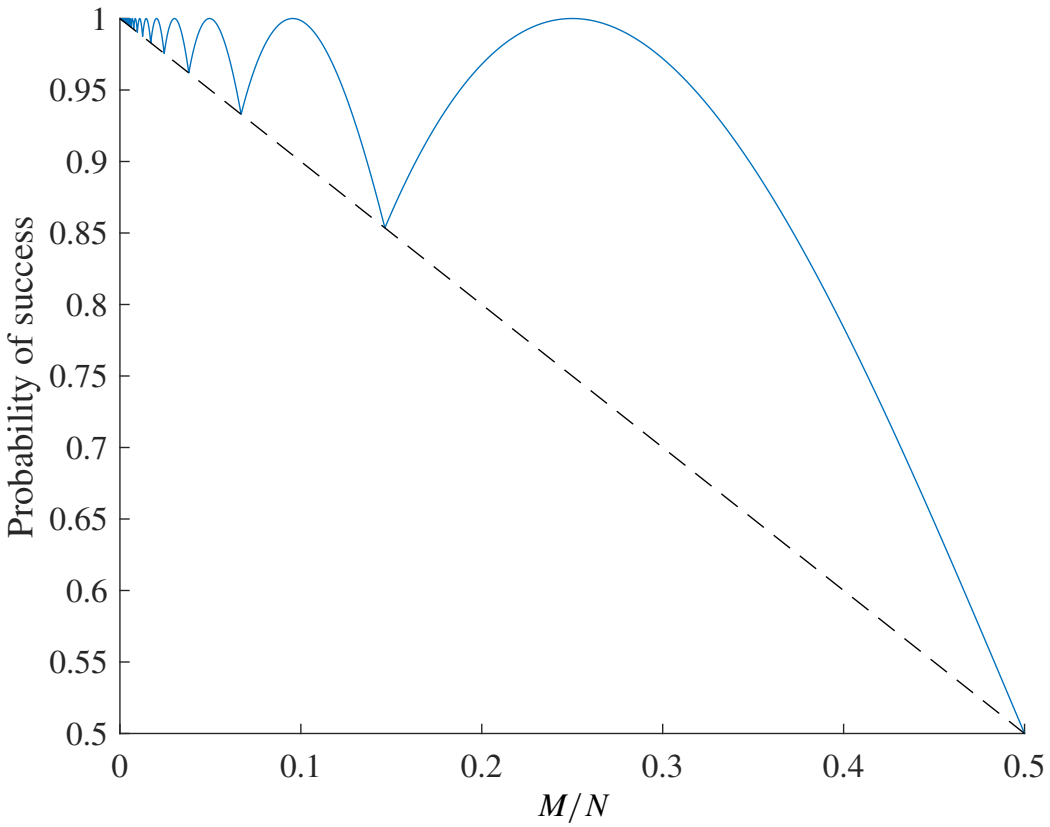

Figure 3.5 Probability of success $\mathbf{P}(s)$ of Grover's algorithm as a function of M/N. The lower bound of the equation (3.36) is drawn in dotted lines

Applying an iteration of Grover GO will produce a rotation in the plane directed by $|s\rangle$ and $|\bar{s}\rangle$ of

$$\theta = \arcsin \frac{2\sqrt{M(N-M)}}{N} \approx 0.314. \tag{3.39}$$

The number of iterations will therefore be

$$R = \frac{\arccos \sqrt{\frac{25}{1\,024}}}{0.314} \approx 4.506, \tag{3.40}$$

which rounds up to $R = 5$ iterations. We can check that this result is correct by adding 5θ to the starting angle $\theta/2$. The result is

$$\left(5 + \frac{1}{2}\right)\theta \approx 0.549\pi, \tag{3.41}$$

which is close to a $\pi/2$ rotation. The resulting state is

$$|\psi_R\rangle = \cos\frac{11}{2}\theta|\bar{s}\rangle + \sin\frac{11}{2}\theta|s\rangle \approx -0.154|\bar{s}\rangle + 0.988|s\rangle, \tag{3.42}$$

and so the probability of obtaining a solution when measuring is

$$\mathbf{P}_R(s) = |\langle s|\psi_R\rangle|^2 = \left(\sin\frac{11}{2}\theta\right)^2 \approx 0.976. \tag{3.43}$$

We observe that the probability of success of the algorithm is very high after only 5 iterations, whereas it would take on average $N/M \approx 41$ evaluations for a classical algorithm to find a solution. Furthermore, this is an unfavorable case, where the chances of error are almost maximal. Indeed, as we round up to $R \approx 5$, we induce an error, as the state vector rotates a little more than necessary in the plane directed by $|s\rangle$ and $|\bar{s}\rangle$. Figure 3.6 illustrates how this example works.

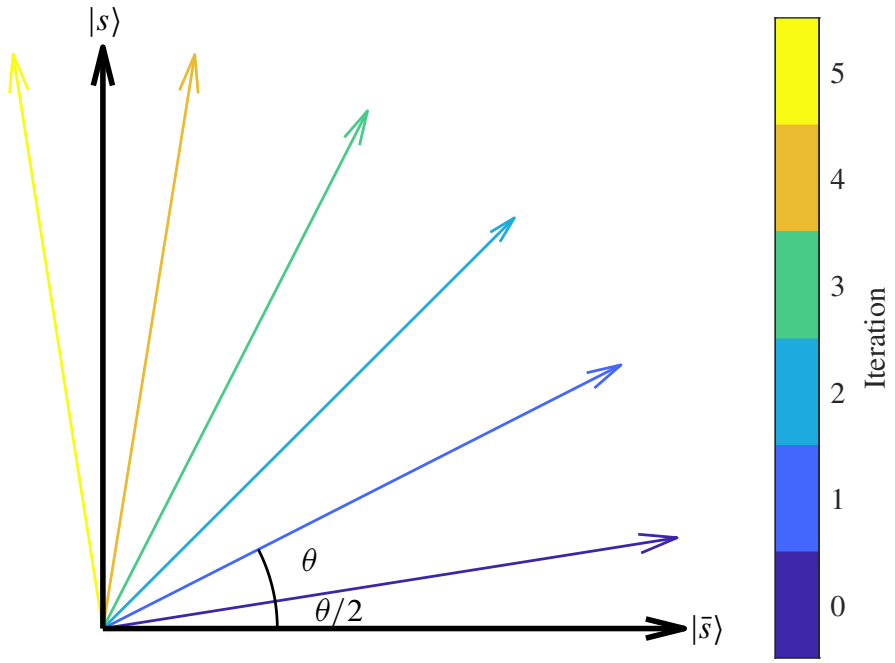

Figure 3.6 Evolution of the system during Grover's algorithm with $N = 1\,024$ and $M = 25$, in the plane directed by $|s\rangle$ and $|\bar{s}\rangle$

3.3. Hypercube search algorithm

The subject of this work is the quantum walk search algorithm on hypercube graphs. As explained in 2.2, uniform walk on hypercube consists in the repeated application of a coin operator C to mix the directions assigned to each vertex of the hypercube, and a shift operator S to move along these directions. In 2003, Shenvi, Kempe and Whaley presented in *A Quantum Random Walk Search Algorithm* [SKW03] the hypercube search algorithm in question, sometimes referred to as the "SKW" algorithm, after the initials of its creators. Note that there are other adaptations of the search algorithm to quantum walks, on other types of graphs, for example star graphs [QMW+22], or in continuous time, such as the Childs and Goldstone's algorithm [CG04], or the more recent Marsh and Wang's algorithm [MW21].

The idea behind this algorithm is to use a C operator that behaves differently on the vertices of the hypercube that correspond to solutions. This operator C' acts on each position p as

$$C' = \begin{cases} I_N \otimes G & \text{if } p \text{ is not solution,} \\ I_N \otimes -I_n & \text{if } p \text{ is solution.} \end{cases} \tag{3.44}$$

This cancels the action of the C operator on the solution vertices, and we can express the new C' operator as

$$C' = I_N \otimes G - \sum_{\substack{p \in \mathbb{Z}_N \\ f(p)=1}} |p\rangle\langle p| \otimes (I_n + G), \tag{3.45}$$

$$= I_N \otimes G - \sum_{\substack{p \in \mathbb{Z}_N \\ f(p)=1}} |p\rangle\langle p| \otimes (2|u_n\rangle\langle u_n|) \tag{3.46}$$

where f is the binary function defined in section 3.1, such that $f(p) = 1$ if p is a solution and $f(p) = 0$ otherwise.

The algorithm is initialized in a uniform state on all vertices and all directions, that is to say

$$|\psi_0\rangle = \frac{1}{nN} \sum_{d=1}^{n} \sum_{p=0}^{N-1} |p\rangle|d\rangle, \tag{3.47}$$

to which we apply the operator $U' = SC'$, repeated R times. The final state is therefore $|\psi_R\rangle = U'^R|\psi_0\rangle$.

Shenvi, Kempe and Whaley have shown that in the case where there is only one solution among the N elements, the probability of success after a number of iterations

$$R = \frac{\pi}{2}\sqrt{\frac{N}{2}} \tag{3.48}$$

is

$$\mathbf{P}_R(s) = \frac{1}{2} - \mathcal{O}\Big(\frac{1}{n}\Big). \tag{3.49}$$

The probability of finding the solution is greater than that of finding another given element. We can therefore obtain an accuracy arbitrarily close to 1 by repeating the algorithm. The evolution of the probability of success over the iterations of the algorithm is shown in Figure 3.7, for a one-solution problem on a hypercube of dimension $n = 6$. We can then verify that the maximum probability of success is close to 0.5 and is reached for the value of $R = (\pi/2)\sqrt{N/2} \approx 9$.

The number of iterations required is equivalent, by a factor, to that of Grover's original algorithm. Since the latter is optimal, we can say that the hypercube quantum search algorithm is too. As in the original algorithm, the probability of success curve shows a sinusoidal trend as a function of the number of iterations, except that it remains constant one iteration out of two. However, this sinusoidal, regular aspect is lost as the number of solutions increases. As an example, consider the hypercube of dimension $n = 6$, for a problem whose solution set is 0, 3, 4, 8, 9, 11 and 16. The probability of success after 9 iterations is about $\mathbf{P}(s) \approx 0.119$. This is hardly better than a random draw, which would give us a probability of success of $\mathbf{P}(s) = 7/64 \approx 0.109$. However, as shown in figure 3.8, it is possible to achieve a probability of success greater than $1/2$. The central problem of this work is to determine the maximum success probability of the hypercube search algorithm, and the number of iterations required to achieve it.

It is possible to transform the uniform direction coin C into its modified analogue for search C' defined in equation (3.44) by product with a block-diagonal matrix O whose structure is reminiscent of Grover's oracle. Indeed, if we have

$$O = I_N \otimes I_n - \sum_{\substack{p\in\mathbb{Z}_N \\ f(p)=1}} |p\rangle\langle p| \otimes (I_n + G), \tag{3.50}$$

we notice that

$$CO = (I_N \otimes G)\Big(I_N \otimes I_n - \sum_{\substack{p\in\mathbb{Z}_N \\ f(p)=1}} |p\rangle\langle p| \otimes (I_n + G)\Big) \tag{3.51}$$

$$= I_N \otimes GI_n - \sum_{\substack{p\in\mathbb{Z}_N \\ f(p)=1}} |p\rangle\langle p| \otimes G(I_n + G), \tag{3.52}$$

$$= I_N \otimes G - \sum_{\substack{p\in\mathbb{Z}_N \\ f(p)=1}} |p\rangle\langle p| \otimes (I_n + G), \tag{3.53}$$

$$= C'. \tag{3.54}$$

We can therefore rewrite the equation of the hypercube search algorithm to show an oracle in the manner of Grover's original algorithm, such that an iteration of the hypercube

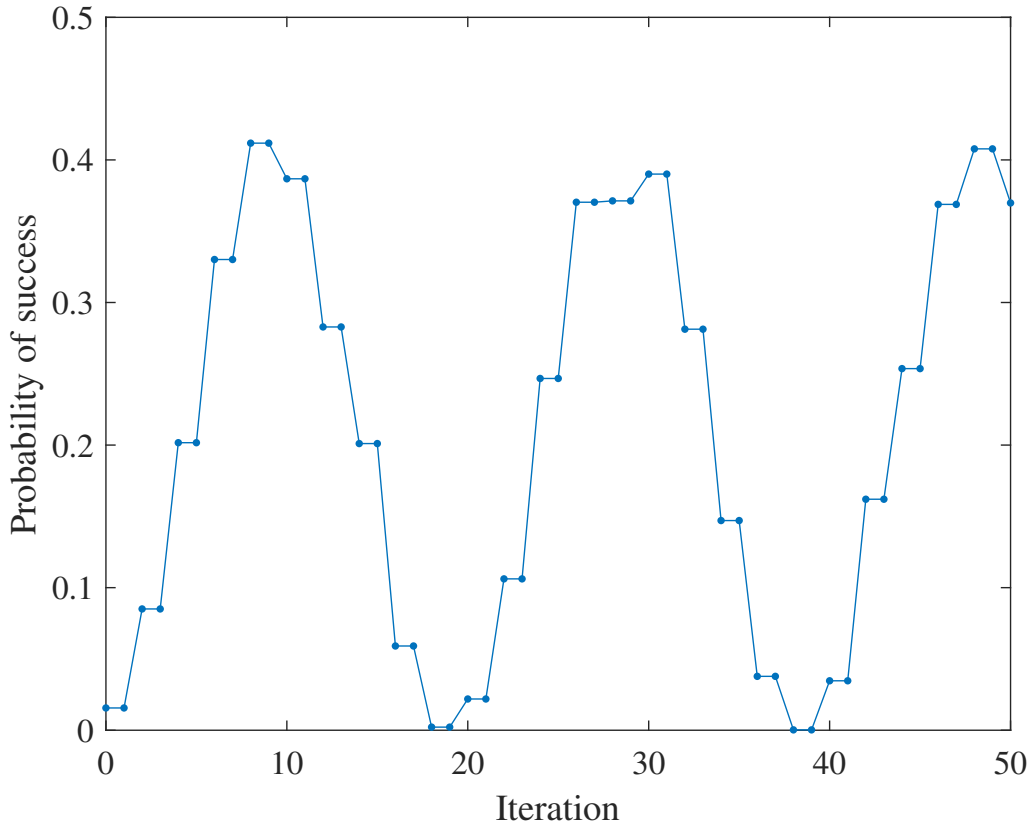

Figure 3.7 Evolution over 50 iterations of the probability of success of the hypercube search algorithm for $n = 6$ with a single solution

search algorithm becomes

$$U' = SCO, \tag{3.55}$$

where O is the oracle of a hypercube search problem. Thus, for a hypercube of a given dimension, the operators S and C are constant for all problems, and only the oracle O changes, as is the case for Grover's algorithm. According to equation (3.50), this oracle is made up of N blocks O_p, such that

$$O_p = \begin{cases} I_n & \text{if } p \text{ is not solution,} \\ -G & \text{if } p \text{ is solution.} \end{cases} \tag{3.56}$$

An example oracle for a search problem on a hypercube of dimension $n = 4$ with solutions 0, 3 and 6 is shown in figure 3.9.

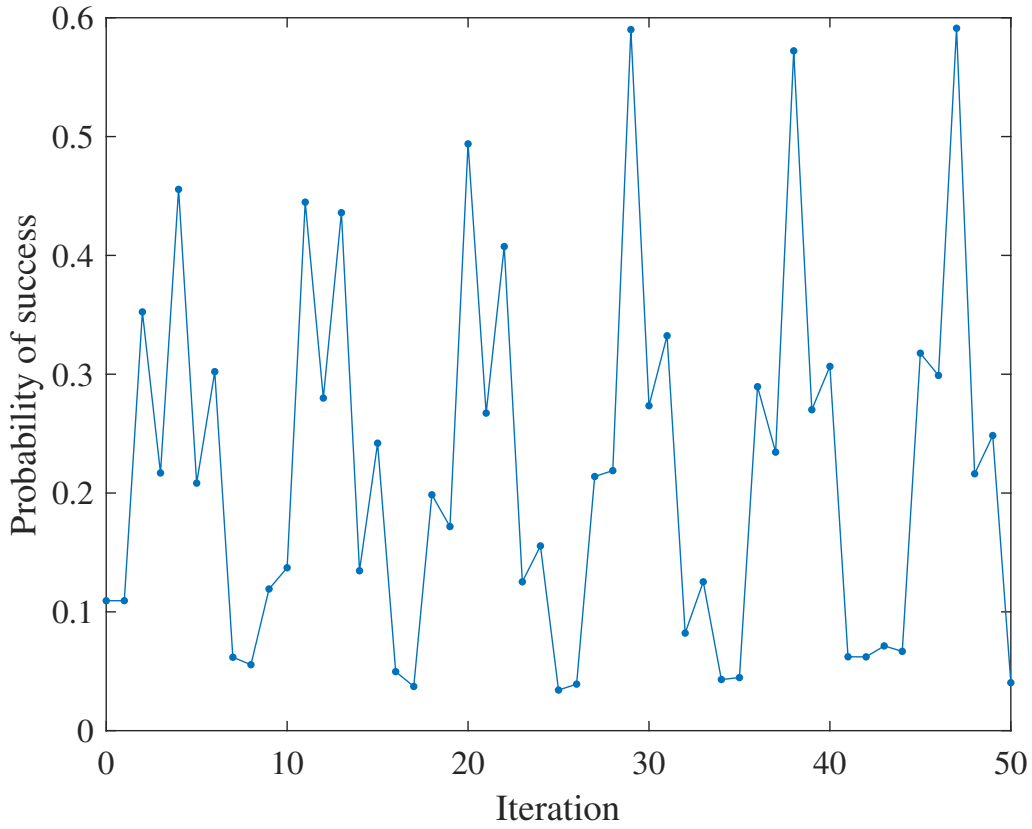

Figure 3.8 Evolution over 50 iterations of the probability of success of the hypercube search algorithm for $n = 6$ with solutions 0, 3, 4, 8, 9, 11 and 16

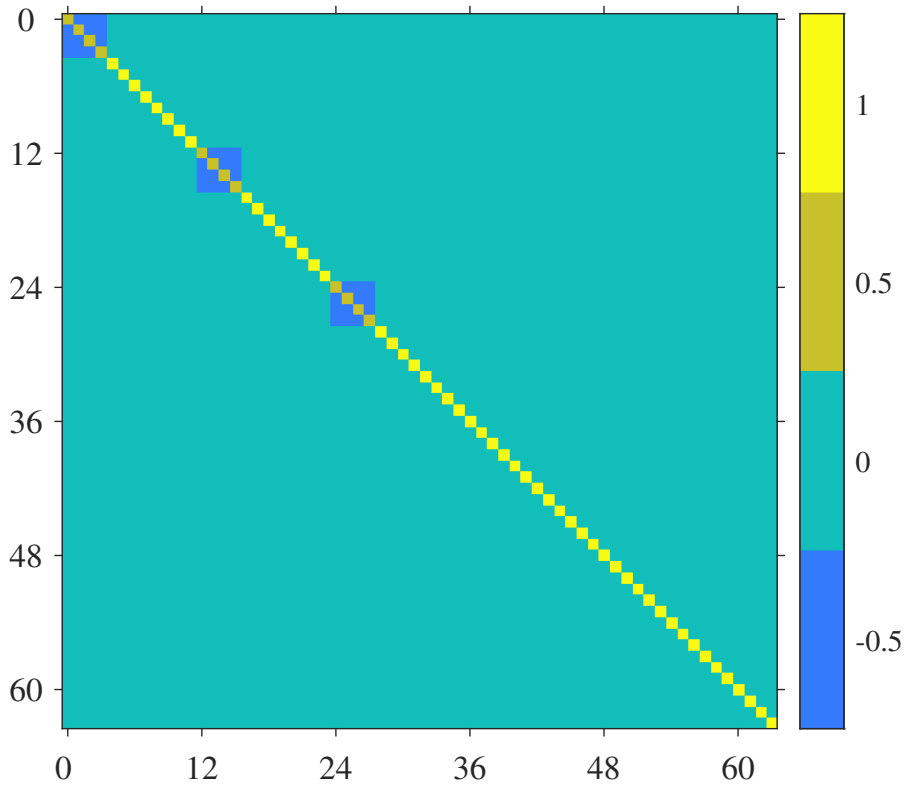

Figure 3.9 Oracle of a search problem on a hypercube of dimension $n = 4$ with solutions 0, 3 and 6

4. Eigenanalysis of the hypercube search algorithm

The iteration of the search algorithm is the sequence of an oracle O and the uniform walk operator U. Let $\overline{\mathcal{E}}$ denote their joint eigenspace, and $O_{\overline{\mathcal{E}}}$ and $U_{\overline{\mathcal{E}}}$ their respective components in this eigenspace. Since two operators commutate in their joint eigenspace, every two iterations in $\overline{\mathcal{E}}$ gives

$$\begin{aligned}(U_{\overline{\mathcal{E}}}O_{\overline{\mathcal{E}}})^2 &= U_{\overline{\mathcal{E}}}O_{\overline{\mathcal{E}}}U_{\overline{\mathcal{E}}}O_{\overline{\mathcal{E}}}, &(4.1)\\ &= U_{\overline{\mathcal{E}}}O_{\overline{\mathcal{E}}}O_{\overline{\mathcal{E}}}U_{\overline{\mathcal{E}}}, &(4.2)\\ &= U_{\overline{\mathcal{E}}}O^2_{\overline{\mathcal{E}}}U_{\overline{\mathcal{E}}}, &(4.3)\\ &= U^2_{\overline{\mathcal{E}}}, &(4.4)\end{aligned}$$

that is, the search algorithm is equivalent to the uniform walk in $\overline{\mathcal{E}}$ without the oracle. Consequently, the effective part of the algorithm takes place in the complement of $\overline{\mathcal{E}}$, which we will denote $\mathcal{E}$. In this section, following the algorithm eigenanalysis, we will show that this space of interest $\mathcal{E}$ is of very small dimension compared to that of the global space $\mathcal{H}$.

In this work, we denote the eigenspace of an operator A associated with the eigenvalue α by

$$E^A_\alpha = \{|a\rangle \in \mathcal{H} \mid A|a\rangle = \alpha|a\rangle\}, \tag{4.5}$$

and the joint eigenspace of two operators A and B associated with the eigenvalues α and β respectively by

$$E^{A,B}_{\alpha,\beta} = E^A_\alpha \cap E^B_\beta. \tag{4.6}$$

For reasons of clarity, the very common ± 1 eigenvalues will only be represented by their signs. For example, we will write $E^{A,B}_{+,-}$ rather than $E^{A,B}_{1,-1}$. We also use the notation $E^A_\pm$ to designate the spaces E^A_+ and E^A_- at the same time. For example, $E^S_\pm = \text{span}(F_\pm)$ is equivalent to $E^S_+ = \text{span}(F_+)$ and $E^S_- = \text{span}(F_-)$, where F_+ and F_- are matrices defined in the next section.

As the analysis presented in this chapter is relatively dense, it is summarized in section 4.6. It may be useful to consult it before or during the reading of this chapter. Readers may also wish to consult beforehand the tables 4.2, 4.3 and 4.4, which contain all the non-empty eigenspaces studied in this chapter.

4.1. Search operator eigenspaces

As seen previously, an iteration of the hypercube search algorithm, represented by the unit operator U', consists of the succession of three operators O, C and S, such that $U' = UO = SCO$. This section is the first step in the analysis of the algorithm itself, in which we will study the eigenvalue and eigenvector decompositions of these three operators.

4.1.1. Shift operator

Defined in section 2.2, the shift operator S is diagonalizable by spatial Fourier transform. Indeed, the matrix $\widetilde{S} = FSF$ is diagonal and has only ± 1 coefficients. As observed earlier, these coefficients are arranged so that all N binary words can be read in ascending order. This ordering of coefficients will be useful later in this work, and we will call them "signatures", which we will define as

$$\varsigma_i = \widetilde{S}_{i,i}, i \in \mathbb{Z}_{nN}. \tag{4.7}$$

We deduce from the diagonalization of $S = F\widetilde{S}F$ that its eigenvalues $\lambda_i^S = \varsigma_i$ are all equal to ± 1 and that its eigenvectors are the columns of F, shown in figure 4.1. Since the sum of the eigenvalues is equal to the trace, and since $\mathrm{tr}(S) = 0$, there are as many eigenvalues -1 and 1. We therefore have

$$\dim(E_+^S) = \dim(E_-^S) = \frac{nN}{2}. \tag{4.8}$$

We define F_+ and F_-, two submatrices of F, respectively constructed by keeping only the columns of F of signatures $\varsigma_i = 1$ and $\varsigma_i = -1$. According to equation (4.8), these two matrices are of size $nN \times nN/2$. We have

$$E_+^S = \mathrm{span}(F_+), \tag{4.9}$$

$$E_-^S = \mathrm{span}(F_-). \tag{4.10}$$

4.1.2. Coin operator

Also introduced in section 2.2, the coin operator C is constructed from the Grover scattering operator G defined in equation (2.64). We can therefore simply link their respective diagonalizations $C = V_C D_C V_C^\dagger$ and $G = V_G D_G V_G^\dagger$. We then have

$$C = I_N \otimes G, \tag{4.11}$$

$$= (I_N I_N I_N^\dagger) \otimes (V_G D_G V_G^\dagger), \tag{4.12}$$

$$= (I_N \otimes V_G)(I_N \otimes D_G)(I_N \otimes V_G)^\dagger, \tag{4.13}$$

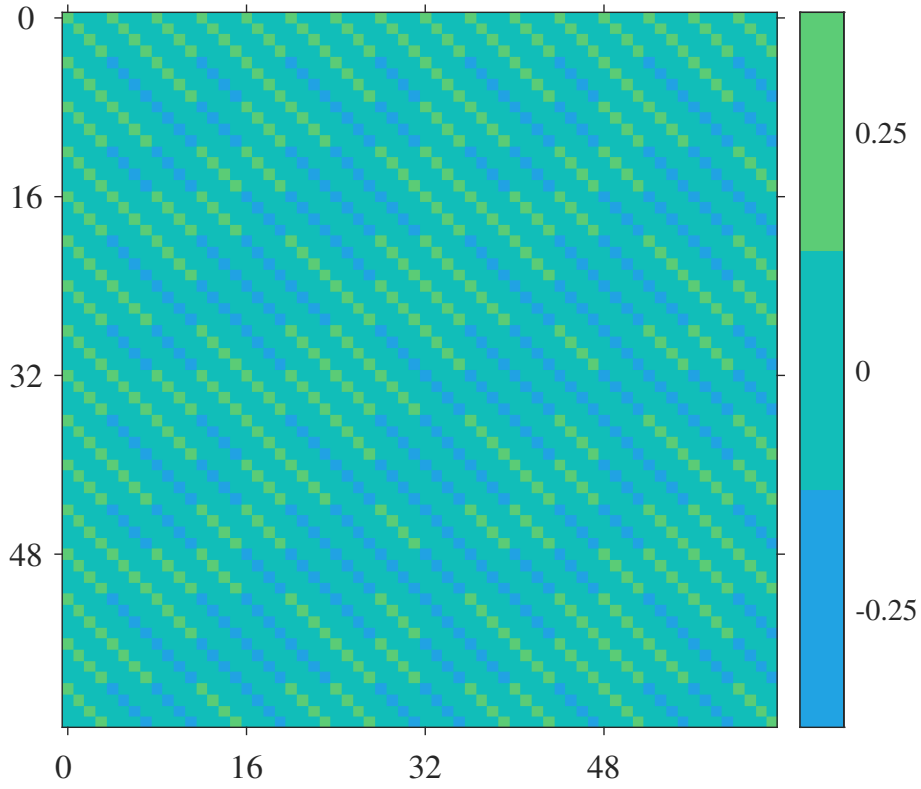

Figure 4.1 Operator of the spatial Fourier transform F in $\mathcal{H}$ for $n = 4$

that is

$$V_C = I_N \otimes V_G, \tag{4.14}$$
$$D_C = I_N \otimes D_G. \tag{4.15}$$

To diagonalize G, we introduce Λ, a $n \times (n-1)$ matrix such that

$$\begin{cases} \langle u_n|\Lambda = 0, \\ \Lambda^\intercal \Lambda = I_{n-1}, \end{cases} \tag{4.16}$$

that is, whose $n-1$ columns form the kernel of $\langle u_n|$. Note that

$$G|u_n\rangle = (2|u_n\rangle\langle u_n| - I_n)|u_n\rangle, \tag{4.17}$$
$$= 2|u_n\rangle\langle u_n|u_n\rangle - |u_n\rangle, \tag{4.18}$$
$$= |u_n\rangle, \tag{4.19}$$

and that

$$G\Lambda = (2|u_n\rangle\langle u_n| - I_n)\Lambda, \tag{4.20}$$
$$= 2|u_n\rangle\langle u_n|\Lambda - I_n\Lambda, \tag{4.21}$$
$$= -\Lambda. \tag{4.22}$$

Consequently, $|u_n\rangle$ is an eigenvector of G associated with eigenvalue 1, and the columns of Λ are $n-1$ eigenvectors associated with eigenvalue -1. We then deduce that the columns of $I_N \otimes |u_n\rangle$ are the eigenvectors of C associated with the 1 eigenvalue and that the columns of $I_N \otimes \Lambda$ are those associated with the -1 eigenvalue, that is to say

$$E_+^C = \text{span}(I_N \otimes |u_n\rangle), \tag{4.23}$$
$$E_-^C = \text{span}(I_N \otimes \Lambda). \tag{4.24}$$

The dimensions of these eigenspaces are

$$\dim(E_+^C) = N, \tag{4.25}$$
$$\dim(E_-^C) = (n-1)N. \tag{4.26}$$

4.1.3. Oracle

As shown in section 3.3, the oracle O is a block-diagonal matrix, made up of N blocks O_p of size $n \times n$, equal to $-G$ at solution positions, and I_n elsewhere. Since we know the eigenvalue and eigenvector decomposition of G, that of O is straightforward.

The blocks I_n are, of course, associated with n eigenvalues equal to 1, and we can choose the columns of I_n as the set of eigenvectors. We can repeat the contents of the previous section for the eigenanalysis of $-G$ blocks. Each of these blocks has eigenvectors $|u_n\rangle$ and columns of Λ, associated with eigenvalues -1 and 1 respectively.

The eigenvectors of the oracle O can be found from those of the blocks O_p by tensor product with $|p\rangle$. The eigenspaces of the oracle O are

$$E_+^O = \mathcal{H} \setminus E_-^O, \tag{4.27}$$
$$E_-^O = \text{span}(\{|p\rangle \otimes |u_n\rangle \mid f(p) = 1\}), \tag{4.28}$$

where $f(p) = 1$ if p is a solution. With M solutions, the dimensions of these eigenspaces are

$$\dim(E_+^O) = nN - M, \tag{4.29}$$
$$\dim(E_-^O) = M. \tag{4.30}$$

4.2. Generator matrices

In this section, we will define a set of matrices and submatrices known as "generators", which will simplify notation in the rest of this work. These are listed in table 4.1.

In particular, we will use several submatrices of I_N and H_N. First, we define $I_N^{(s)}$ and $H_N^{(s)}$, submatrices respectively of I_N and H_N, of size $N \times M$, formed by the columns corresponding to the solutions. From $H_N^{(s)}$, we construct the submatrix $H_N^{(s,w)}$ of size $\binom{n}{w} \times M$, formed by the rows at positions corresponding to binary words with Hamming weights equal to w. In the following, we will refer to the Hamming weight of the binary word associated with a position p as $\mathrm{wt}(p)$. We also define $I_N^{(\bar{s})}$, a submatrix of I_N constructed from columns not corresponding to solutions.

4.2.1. Generators G_1, G_2, G_3

In addition to the columns of the F_+ and F_- matrices, we will use those of three specially constructed matrices to characterize the eigenspaces

$$G_1 = I_N^{(s)} \otimes |u_n\rangle, \tag{4.31}$$
$$G_2 = I_N^{(\bar{s})} \otimes |u_n\rangle, \tag{4.32}$$
$$G_3 = I_N \otimes \Lambda, \tag{4.33}$$

of sizes $nN \times M$, $nN \times (N-M)$ and $nN \times (n-1)N$ respectively. We also define the matrices

$$G_{1,2} = G_1 \dashv\vdash G_2, \tag{4.34}$$
$$G_{2,3} = G_2 \dashv\vdash G_3, \tag{4.35}$$
$$G_{1,3} = G_1 \dashv\vdash G_3, \tag{4.36}$$
$$G_{1,2,3} = G_1 \dashv\vdash G_2 \dashv\vdash G_3, \tag{4.37}$$

where $\dashv\vdash$ denotes the horizontal concatenation of two matrices, so that

$$\mathrm{span}(A \dashv\vdash B) = \mathrm{span}(A) \cup \mathrm{span}(B). \tag{4.38}$$

The matrix $G_{1,2,3}$ is shown in figure 4.2. As $\mathrm{span}(I_N^{(s)} \dashv\vdash I_N^{(\bar{s})}) = \mathcal{H}^{\mathrm{S}}$ and $\mathrm{span}(|u_n\rangle \dashv\vdash \Lambda) = \mathcal{H}^{\mathrm{C}}$, the columns of $G_{1,2,3}$ form an orthonormal basis of $\mathcal{H}$. We can also express the eigenspaces of the operators C and O as

$$E_+^C = \mathrm{span}(G_{1,2}), \tag{4.39}$$
$$E_-^C = \mathrm{span}(G_3), \tag{4.40}$$
$$E_+^O = \mathrm{span}(G_{2,3}), \tag{4.41}$$
$$E_-^O = \mathrm{span}(G_1). \tag{4.42}$$

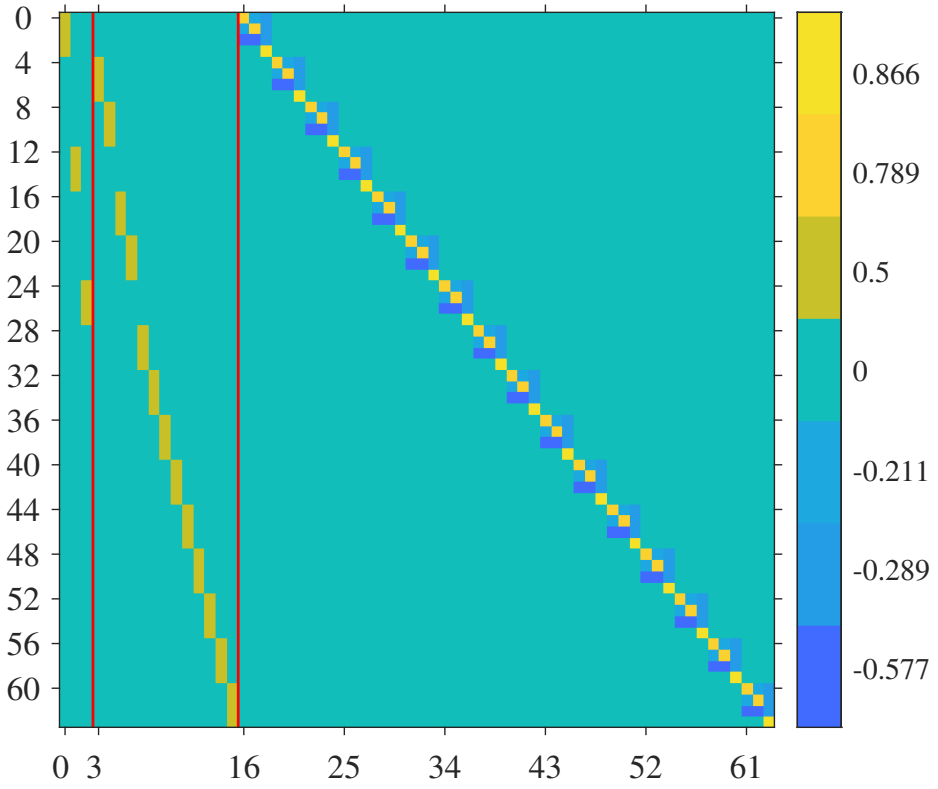

Figure 4.2 Generator matrix $G_{1,2,3}$ of a hypercube search problem of dimension $n = 4$ with solutions 0, 3, and 6. The matrices G_1, G_2 and G_3 are separated by red lines.

We can show that the matrices $G_{1,2}$ and G_3 each generate the same spaces before and after spatial Fourier transform. For example, since $G_3 = I_N \otimes \Lambda$, we have $FG_3 = H_N \otimes \Lambda$. Since we can multiply on the right by any non-singular matrix without changing the vector space generated, we know that $\text{span}(FG_3) = \text{span}(FG_3F) = \text{span}(G_3)$. More generally, this is true for any matrix whose component in $\mathcal{H}^S$ is I_N. The demonstration for $G_{1,2}$ is the same, since $\text{span}(G_{1,2}) = \text{span}(I_N \otimes |u_n\rangle)$. We therefore have

$$\text{span}(FG_3) = \text{span}(G_3), \tag{4.43}$$
$$\text{span}(FG_{1,2}) = \text{span}(G_{1,2}). \tag{4.44}$$

We also define the vector $|g_-\rangle$ as the spatial Fourier transform of the column of $G_{1,2}$ having all its signatures $\varsigma_i = -1$, which corresponds to the last position $p = N - 1$, that is

$$|g_-\rangle = F(|N-1\rangle|u_n\rangle). \tag{4.45}$$

4.2.2. Generator G'_3 and its submatrices

We construct the matrix G'_3, a variant of G_3 in which most of the columns are eigenvectors of $\widetilde{S}$. To do this, we replace each Λ block with a $\Lambda^{(p)}$ block. Each of these blocks is itself the concatenation of three matrices $\Lambda^{(p)}_-$, $\Lambda^{(p)}_+$ and $\Lambda^{(p)}_\circ$, whose sizes depend on the associated position p, and the Hamming weight $w = \mathrm{wt}(p)$ of the corresponding binary word. An example of the G'_3 matrix is shown in figure 4.3.

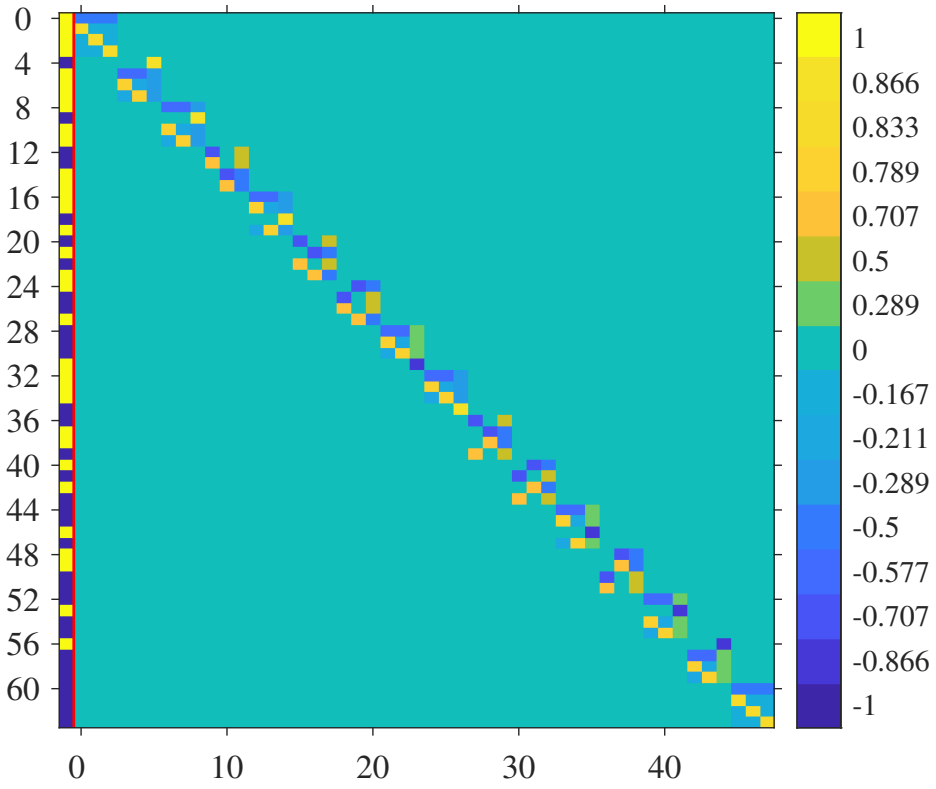

Figure 4.3 Generator matrix G'_3 for $n = 4$. The signatures of each row are attached on the left.

The blocks $\Lambda^{(p)}_-$ are $n \times (w-1)$ matrices with non-zero coefficients only in the w rows of signature $\varsigma_i = -1$. These non-zero coefficients are chosen to form $w-1$ vectors orthogonal to $|u_w\rangle$ and to each other. So the columns of $\Lambda^{(p)}_-$ are all orthogonal to $|u_n\rangle$. If $w \leqslant 1$, then $\Lambda^{(p)}_-$ is an empty matrix.

Similarly, the blocks $\Lambda^{(p)}_+$ are $n \times (n-w-1)$ matrices, with non-zero coefficients only at the $n-w$ rows of signature $\varsigma_i = 1$. These non-zero coefficients are chosen to form $n-w-1$ vectors orthogonal to $|u_{n-w}\rangle$ and to each other. The columns of $\Lambda^{(p)}_+$ are therefore also all orthogonal to $|u_n\rangle$. If $n-w \leqslant 1$, then $\Lambda^{(p)}_+$ is an empty matrix.

If $w = 0$ or $w = n$, $\Lambda_\circ^{(p)}$ is an empty matrix. Otherwise, it is a column vector orthogonal to $|u_n\rangle$ and to the columns of $\Lambda_-^{(p)}$ and $\Lambda_+^{(p)}$ which completes the block $\Lambda^{(p)}$ so that its columns generate the same vector space as those of the original Λ matrix. The elements of such a vector are

$$\begin{cases} \sqrt{\dfrac{n-w}{nw}} & \text{if } \varsigma_i = -1, \\ -\sqrt{\dfrac{w}{n(n-w)}} & \text{if } \varsigma_i = 1. \end{cases} \tag{4.46}$$

The N blocks $\Lambda^{(p)}$ are formed by concatenating the three submatrices

$$\Lambda^{(p)} = \Lambda_-^{(p)} +\!\!+ \Lambda_+^{(p)} +\!\!+ \Lambda_\circ^{(p)}. \tag{4.47}$$

We also define G'_-, G'_+ and $G'_\circ$ as submatrices of G'_3, made up respectively of columns containing the blocks $\Lambda_-^{(p)}$, $\Lambda_+^{(p)}$ and $\Lambda_\circ^{(p)}$. The matrices G'_- and G'_+ are of size $nN \times (nN/2 - N + 1)$ and the matrix $G'_\circ$ is of size $nN \times (N-2)$.

4.3. Joint eigenspaces

Using the generators defined in the previous section, we can characterize the joint eigenspaces of the walk operators S, C and O to prepare the eigenspace analysis of the operators $U = SC$ and $U' = UO$. The table 4.2 at the end of this section summarizes the analysis of the operators S, C and O.

4.3.1. Joint eigenspaces of operators C and O

First we look at the joint eigenspaces of the operators C and O. Recall that $E_+^C = \text{span}(G_{1,2})$, $E_-^C = \text{span}(G_3)$, $E_+^O = \text{span}(G_{2,3})$, and $E_-^O = \text{span}(G_1)$. Thus we have

$$\begin{aligned} E_{+,+}^{C,O} &= E_+^C \cap E_+^O, && (4.48)\\ &= \text{span}(G_{1,2}) \cap \text{span}(G_{2,3}), && (4.49)\\ &= \text{span}(G_2), && (4.50) \end{aligned}$$

$$\begin{aligned} E_{+,-}^{C,O} &= E_+^C \cap E_-^O, && (4.51)\\ &= \text{span}(G_{1,2}) \cap \text{span}(G_1), && (4.52)\\ &= \text{span}(G_1), && (4.53)\\ &= E_-^O, && (4.54) \end{aligned}$$

Table 4.1 Generator matrices

Notation	Dimension	Definition
$I_N^{(s)}$	$N \times M$	Submatrix of the identity matrix I_N obtained by keeping only the columns associated with solutions
$H_N^{(s)}$	$N \times M$	Submatrix of the Hadamard matrix H_N obtained by keeping only the columns associated with solutions
$H_N^{(s,w)}$	$\binom{n}{w} \times M$	Submatrix of $H_N^{(s)}$ obtained by keeping only the rows associated with positions of Hamming weight w
F_-	$nN \times nN/2$	Submatrix of the spatial Fourier transform operator F, obtained by keeping only the columns associated with signatures $\varsigma_i = -1$
F_+	$nN \times nN/2$	Submatrix of the spatial Fourier transform operator F, obtained by keeping only the columns associated with signatures $\varsigma_i = 1$
G_1	$nN \times M$	$I_N^{(s)} \otimes \|u_n\rangle$, generates the space of solution positions
G_2	$nN \times (N - M)$	$I_N^{(\bar{s})} \otimes \|u_n\rangle$, generates the space of non-solution positions
G_3	$nN \times (n-1)N$	$I_N \otimes \Lambda$, generates the complementary space to those generated by G_1 and G_2
G'	$nN \times (n-1)N$	Variant of G_3, generates the same space
G'_-	$nN \times (nN/2 - N + 1)$	Submatrix of G', made up of blocks Λ_-
G'_+	$nN \times (nN/2 - N + 1)$	Submatrix of G', made up of blocks Λ_+
$G'_\circ$	$nN \times (N-2)$	Submatrix of G', made up of blocks $\Lambda_\circ$
$\|g_-\rangle$	$nN \times 1$	$F(\|N-1\rangle\|u_n\rangle)$, spatial Fourier transform of the column of $G_{1,2}$ with all its signatures $\varsigma_i = -1$

$$E^{C,O}_{-,+} = E^C_- \cap E^O_+, \tag{4.55}$$
$$= \mathrm{span}(G_3) \cap \mathrm{span}(G_{2,3}), \tag{4.56}$$
$$= \mathrm{span}(G_3), \tag{4.57}$$
$$= E^C_-, \tag{4.58}$$

$$E^{C,O}_{-,-} = E^C_- \cap E^O_-, \tag{4.59}$$
$$= \mathrm{span}(G_3) \cap \mathrm{span}(G_1), \tag{4.60}$$
$$= \emptyset. \tag{4.61}$$

The dimensions of these joint eigenspaces are directly deduced as

$$\dim(E^{C,O}_{+,+}) = N - M, \tag{4.62}$$
$$\dim(E^{C,O}_{+,-}) = M, \tag{4.63}$$
$$\dim(E^{C,O}_{-,+}) = (n-1)N, \tag{4.64}$$
$$\dim(E^{C,O}_{-,-}) = 0, \tag{4.65}$$

and the eigenvalue and eigenvector decomposition of the CO operator.

$$E^{CO}_+ = E^{C,O}_{+,+} \cup E^{C,O}_{-,-} = G_2, \tag{4.66}$$
$$E^{CO}_- = E^{C,O}_{+,-} \cup E^{C,O}_{+,-} = G_{1,3}. \tag{4.67}$$

4.3.2. Joint eigenspaces of operators S and C

Because of its complex structure, direct analysis of S joint eigenspaces is difficult. We therefore use its spatial Fourier transform $\widetilde{S}$, defined in section 2.2, whose diagonal structure makes eigenanalysis trivial. Note also that the coin operator is invariant under the spatial Fourier transform, since it acts only in $\mathcal{H}^{\mathrm{C}}$. Indeed, we have

$$\widetilde{C} = FCF, \tag{4.68}$$
$$= (H_N \otimes I_n)(I_N \otimes G)(H_N \otimes I_n), \tag{4.69}$$
$$= (H_N I_N H_N) \otimes (I_n G I_n), \tag{4.70}$$
$$= I_N \otimes G, \tag{4.71}$$
$$= C. \tag{4.72}$$

We can therefore determine the spaces $E^{S,C}_{\pm,\pm}$ from the spaces $E^{\widetilde{S},C}_{\pm,\pm}$.

By definition of signatures ς_i, a vector contained in $E^{\widetilde{S}}_{\pm}$ has as non-zero elements only those whose signature is ± 1. Since $E^C_- = \mathrm{span}(G_3) = \mathrm{span}(G'_3)$, we have

$$E^{\widetilde{S},C}_{\pm,-} = \mathrm{span}(F_\pm) \cap \mathrm{span}(G'_3), \tag{4.73}$$
$$= \mathrm{span}(G'_\pm). \tag{4.74}$$

We deduce

$$E^{S,C}_{\pm,-} = \text{span}(FG'_{\pm}), \tag{4.75}$$

and

$$\dim(E^{S,C}_{\pm,-}) = \dim(\text{span}(G'_{\pm})) = \frac{nN}{2} - N + 1. \tag{4.76}$$

We have $E^{C}_{+} = \text{span}(G_{1,2})$ and therefore

$$E^{\tilde{S},C}_{\pm,+} = E^{\tilde{S}}_{\pm} \cap E^{C}_{+}, \tag{4.77}$$

$$= E^{\tilde{S}}_{\pm} \cap \text{span}(G_{1,2}). \tag{4.78}$$

A vector of $E^{\tilde{S}}_{\pm}$ must have non-zero elements only in the rows with signature $\varsigma_i = \pm 1$. The only element of $\text{span}(G_{1,2})$ having only elements with signatures $\varsigma_i = +1$ is the column of $G_{1,2}$ corresponding to the first position $|0\rangle|u_n\rangle$. Similarly, the only element of $\text{span}(G_{1,2})$ having only elements with signatures $\varsigma_i = -1$ is the column of $G_{1,2}$ corresponding to the last position $|N-1\rangle|u_n\rangle$. Therefore

$$E^{\tilde{S},C}_{+,+} = \text{span}(|0\rangle|u_n\rangle), \tag{4.79}$$

$$E^{\tilde{S},C}_{-,+} = \text{span}(|N-1\rangle|u_n\rangle). \tag{4.80}$$

The spatial Fourier transforms of these vectors are

$$F|0\rangle|u_n\rangle = |u_{nN}\rangle, \tag{4.81}$$

$$F|N-1\rangle|u_n\rangle = |g_-\rangle, \tag{4.82}$$

where $|g_-\rangle$ is the vector defined in equation 4.45. We then have

$$E^{S,C}_{+,+} = \text{span}(|u_{nN}\rangle), \tag{4.83}$$

$$E^{S,C}_{-,+} = \text{span}(|g_-\rangle), \tag{4.84}$$

and

$$\dim(E^{S,C}_{+,+}) = \dim(E^{S,C}_{-,+}) = 1. \tag{4.85}$$

4.3.3. Joint eigenspaces of operators S, C and O

Noting that $|u_{nN}\rangle$ and $|g_-\rangle$ contain no zero values, we can conclude that they do not belong to $\text{span}(G_1)$ nor to $\text{span}(G_2)$, we find that the only eigenspace common to the three operators S, C and O is $\text{span}(G_3)$. We have

$$E^{S,C,O}_{\pm,-,+} = E^{S}_{\pm} \cap E^{C,O}_{-,+}, \tag{4.86}$$

$$= E^{S}_{\pm} \cap E^{C}_{-}, \tag{4.87}$$

$$= E^{S,C}_{\pm,-}, \tag{4.88}$$

$$= \text{span}(FG'_{\pm}), \tag{4.89}$$

and all other joint eigenspaces of the three operators are empty.

We therefore have $E_{+,-}^{S,C,O} = E_{+,-}^{S,C}$ and we know that $E_{+,-}^{S,CO} \supseteq E_{+,-}^{S,C}$. In order to find the dimension of $E_{+,-}^{S,CO}$, we switch to the Fourier domain to exploit the diagonal structure of $\widetilde{S}$. We have $E_{+,-}^{\widetilde{S},C} = \mathrm{span}(G'_+)$ and $E_+^{\widetilde{S}} \perp \mathrm{span}(G'_-)$. The eigenvectors that generate the complement of $E_{+,-}^{\widetilde{S},C}$ in $E_{+,-}^{\widetilde{S},CO}$ are therefore of the form

$$|\varepsilon\rangle = FG_1|\varepsilon_1\rangle + G'_\circ|\varepsilon_\circ\rangle, \tag{4.90}$$

where the vectors $|\varepsilon_1\rangle$ and $|\varepsilon_\circ\rangle$ are of lengths M and $N-2$ respectively. Recall that by definition, the first and last rows of $G'_\circ$ are empty, since the blocks $\Lambda_\circ^{(0)}$ and $\Lambda_\circ^{(N-1)}$ are empty.

For the vector $|\varepsilon\rangle$ to belong to $E_+^{\widetilde{S}}$, all its coefficients of signature $\varsigma_i = -1$ must be zero. This means that the n values of the block corresponding to position $p = N-1$ must be zero, since they all have signature -1. As $G'_\circ$ is already zero at this position, we only need to cancel the $|\varepsilon_1\rangle$ component. We define $\langle h|$ as the last row of the matrix $H_N^{(s)}$, that is to say

$$\langle h| = \frac{1}{\sqrt{N}}\begin{bmatrix}(-1)^{w_1} & (-1)^{w_2} & \cdots & (-1)^{w_M}\end{bmatrix}, \tag{4.91}$$

where w_i is the Hamming weight of the binary word associated with the i-th solution. We must have $\langle h|\varepsilon_1\rangle = 0$, and since $\langle h|$ is of length M, we can find $M-1$ orthogonal vectors $|\varepsilon_1\rangle$.

It can also be shown that each vector $|\varepsilon_1\rangle$ corresponds to a unique $|\varepsilon_\circ\rangle$. Consider a column $\Lambda_\circ^{(p)}$ of $G'_\circ$. At each block of position p, the coefficients of signature $\varsigma_i = -1$ have the value $\sqrt{(n-w)/(nw)}$. We also have

$$FG_1|\varepsilon_1\rangle = (H_N^{(s)} \otimes |u_n\rangle)|\varepsilon_1\rangle, \tag{4.92}$$

$$= (H_N^{(s)}|\varepsilon_1\rangle) \otimes |u_n\rangle. \tag{4.93}$$

and $FG_1|\varepsilon_1\rangle$ is a vector of length nN composed of N blocks each associated with a position p, containing n coefficients equal to the p-th value of $H_N^{(s)}|\varepsilon_1\rangle/\sqrt{n}$, which we will denote $(H_N^{(s)}|\varepsilon_1\rangle)(p)/\sqrt{n}$. We must then have

$$\frac{1}{\sqrt{n}}(H_N^{(s)}|\varepsilon_1\rangle)(p) + \sqrt{\frac{n-w}{nw}}|\varepsilon_\circ(p)\rangle = 0, \tag{4.94}$$

that is

$$|\varepsilon_\circ(p)\rangle = -\sqrt{\frac{w}{n-w}}(H_N^{(s)}|\varepsilon_1\rangle)(p), \tag{4.95}$$

and we check that each coefficient of $|\varepsilon_\circ\rangle$ is always uniquely defined for $p \neq 0$ and $p \neq N$ for each of the $M-1$ vectors $|\varepsilon_1\rangle$. We conclude that the dimension of the complement of $E_{+,-}^{\widetilde{S},C}$ in $E_{+,-}^{\widetilde{S},CO}$ is $M-1$. Since $\dim(E_{+,-}^{S,C}) = nN/2 - N + 1$, we have

$$\dim(E_{+,-}^{S,CO}) = \frac{nN}{2} - N + M. \tag{4.96}$$

In a similar way, we prove that

$$\dim(E^{S,CO}_{-,-}) = \frac{nN}{2} - N + M, \tag{4.97}$$

using the $H^{(s)}_N$ row corresponding to $p = 0$, that is $\langle u|$ instead of $\langle h|$.

Table 4.2 Eigenspaces of walk operators

Eigenspace	Generator	Dimension
$E^{S}_{\pm}$	$F_{\pm}$	$nN/2$
E^{C}_{-}	G_3	$nN - N$
E^{C}_{+}	$G_{1,2}$	N
E^{O}_{-}	G_1	M
E^{O}_{+}	$G_{2,3}$	$nN - M$
$E^{C,O}_{-,+}$	G_3	$nN - N$
$E^{C,O}_{+,-}$	G_1	M
$E^{C,O}_{+,+}$	G_2	$N - M$
E^{CO}_{-}	$G_{1,3}$	$nN - N + M$
E^{CO}_{+}	G_2	$N - M$
$E^{S,C}_{\pm,-}$	$FG'_{\pm}$	$nN/2 - N + 1$
$E^{S,C}_{-,+}$	$\|g_-\rangle$	1
$E^{S,C}_{+,+}$	$\|u_{nN}\rangle$	1
$E^{S,C,O}_{\pm,-,+}$	$FG'_{\pm}$	$nN/2 - N + 1$
$E^{S,CO}_{\pm,-}$	$G_{1,3} \perp F_{\mp}$	$nN/2 - N + M$

$\perp F_{\mp}$ denotes an orthogonality constraint

4.4. Eigenanalysis of the uniform walk

4.4.1. Overview of the uniform walk eigenanalysis

In this section, we exploit the analyses of the elementary uniform walk operators S and C to determine the eigenvalues and eigenspaces of the uniform walk operator $U = SC$. As summarized in table 4.2, operators S and C have only eigenvalues ± 1. This is therefore

also the case for their joint eigenspaces, and we have

$$E_{-}^{U} \supseteq E_{+,-}^{S,C} \cup E_{-,+}^{S,C}, \tag{4.98}$$

$$E_{+}^{U} \supseteq E_{-,-}^{S,C} \cup E_{+,+}^{S,C}, \tag{4.99}$$

which allows us to establish an upper bound on the dimension of these spaces:

$$\dim(E_{-}^{U}) \geqslant \frac{nN}{2} - N + 2, \tag{4.100}$$

$$\dim(E_{+}^{U}) \geqslant \frac{nN}{2} - N + 2. \tag{4.101}$$

To find the other eigenvalues of U, we use its spatial Fourier transform $\widetilde{U}$, with a block-diagonal structure much simpler to study. The p-th block of $\widetilde{U}$ is expressed as

$$\widetilde{U}^{(p)} = \widetilde{S}^{(p)} G, \tag{4.102}$$

where $\widetilde{S}^{(p)}$ is the p-th block of the diagonal of $\widetilde{S}$, introduced in 2.2, and G is the Grover diffusion operator. This block-diagonal structure makes it possible to study $\widetilde{U}$ block by block, as the eigenvalues of a block-diagonal matrix are those of each of its blocks.

Since the sum of the eigenvalues of a matrix is equal to its trace, and the trace of each block is known, we determine that in each block there is a pair of complex eigenvalues λ_w and λ_w^*, with

$$\lambda_w = 1 - 2\frac{w}{n} + \mathrm{i}\frac{2}{n}\sqrt{w(n-w)}, \tag{4.103}$$

where w is the Hamming weight of the binary word associated with position p. It can be seen that the eigenvalues of the $\widetilde{U}^{(p)}$ blocks do not depend on position p but only on the associated Hamming weight w. Furthermore, we note that at positions $p = 0$ and $p = N - 1$, we have $\lambda_w = \lambda_w^* = \pm 1$. Since there are $\binom{n}{w}$ words of n bits of Hamming weight w, we have

$$\dim(E_{\lambda_w}^{U}) = \dim(E_{\lambda_w^*}^{U}) = \binom{n}{w}. \tag{4.104}$$

Given that

$$\sum_{w=1}^{n-1} \binom{n}{w} = N - 2, \tag{4.105}$$

with $N = 2^n$, and that we have a total of nN eigenvalues, we determine that

$$\dim(E_{-}^{U}) = \dim(E_{+}^{U}) = \frac{nN}{2} - N + 2, \tag{4.106}$$

and we can then easily determine the eigenspaces of U associated with the eigenvalues ± 1 based on the table 4.2. We have

$$E_-^U = \text{span}(FG'_+ \mathbin{+\!\!+} |g_-\rangle), \tag{4.107}$$
$$E_+^U = \text{span}(FG'_- \mathbin{+\!\!+} |u_{nN}\rangle). \tag{4.108}$$

The eigenvalues λ_w and λ_w^* are associated with eigenvectors $|p\rangle|v_p\rangle$ and $|p\rangle|v_p^*\rangle$, with

$$|v_p\rangle = \frac{1}{\sqrt{2w}}|b\rangle - \mathrm{i}\frac{1}{\sqrt{2(n-w)}}|\bar{b}\rangle, \tag{4.109}$$

where $|b\rangle$ denotes the vector formed by the binary word associated with position p on the hypercube and $|\bar{b}\rangle$ that formed by its negation.

4.4.2. Detail of the eigenanalysis of the uniform walk

The uniform walk without the oracle is represented by the operator $U = SC$, shown in figure 4.4. This gives us

$$E_-^U \supseteq E_{+,-}^{S,C} \cup E_{-,+}^{S,C}, \tag{4.110}$$
$$E_+^U \supseteq E_{-,-}^{S,C} \cup E_{+,+}^{S,C}, \tag{4.111}$$

which implies

$$\dim(E_-^U) \geqslant \frac{nN}{2} - N + 2, \tag{4.112}$$
$$\dim(E_+^U) \geqslant \frac{nN}{2} - N + 2. \tag{4.113}$$

As with the shift operator S, the structure of the operator U is simpler in the Fourier domain. In fact, we have

$$\widetilde{U} = FUF, \tag{4.114}$$
$$= (FSF)(FCF), \tag{4.115}$$
$$= \widetilde{S}\widetilde{C}, \tag{4.116}$$
$$= \widetilde{S}C, \tag{4.117}$$

and we see, as shown in figure 4.5, that $\widetilde{U}$ has a block-diagonal structure, with N blocks $\widetilde{U}^{(p)}$ such that

$$\widetilde{U}^{(p)} = \widetilde{S}^{(p)}G, \tag{4.118}$$

where the blocks $\widetilde{S}^{(p)}$ are those defined in section 2.2. These blocks $\widetilde{S}^{(p)}$ are diagonal matrices containing w coefficients equal to 1 and $n - w$ coefficients equal to -1, where

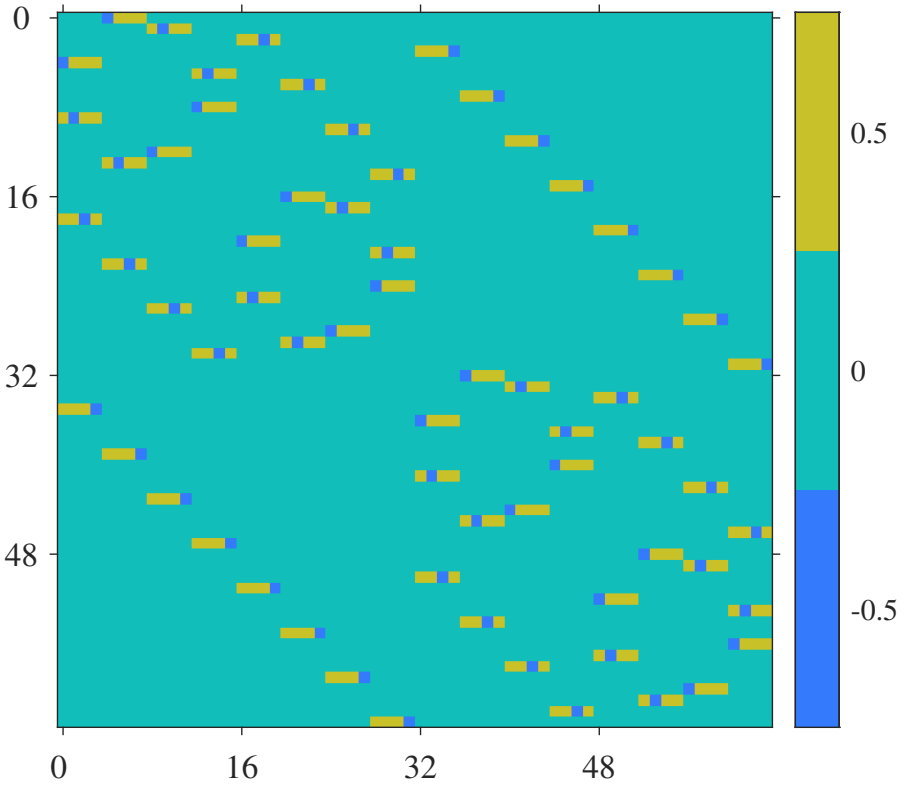

Figure 4.4 Operator of the uniform walk U for $n = 4$

$w = \mathrm{wt}(p)$. At positions $p = 0$ and $p = N - 1$, we have $\widetilde{S}^{(p)} = \pm I_n$, and therefore $\widetilde{U}^{(p)} = \pm G$, which corresponds only to eigenvalues equal to ± 1.

Since all coefficients on the diagonal of G are equal to $-1 + 2/n$, we have

$$\mathrm{tr}(\widetilde{U}^{(p)}) = ((n-w)-w)\Big(-1+\frac{2}{n}\Big), \tag{4.119}$$

$$= (n-2w)\Big(-1+\frac{2}{n}\Big), \tag{4.120}$$

$$= -n + 2w + 2\Big(1 - 2\frac{w}{n}\Big). \tag{4.121}$$

A matrix $\widetilde{U}^{(p)}$ has $n - w - 1$ eigenvalues equal to -1 and $w - 1$ eigenvalues equal to 1, making $n - 2$ eigenvalues, the sum of which is $-n + 2w$. Since the sum of the eigenvalues of a matrix is equal to its trace, the sum of the two remaining eigenvalues is equal to $2(1 - 2w/n)$. Since $\widetilde{U}^{(p)}$ is unitary, all its eigenvalues have modulus equal to 1. We conclude that the two missing eigenvalues λ_w and λ_w^* form a pair of conjugate

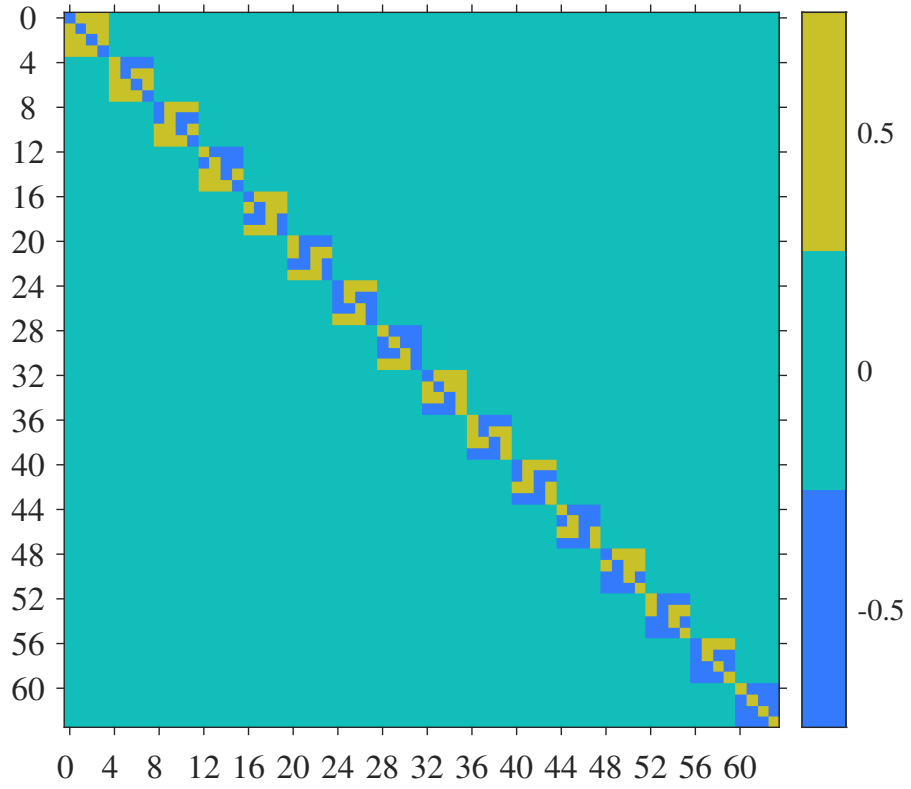

Figure 4.5 Diagonalized uniform walk operator $\widetilde{U}$ for $n = 4$

complex numbers, with

$$\mathrm{Re}(\lambda_w) = 1 - 2\frac{w}{n}. \tag{4.122}$$

We deduce

$$\lambda_w = 1 - 2\frac{w}{n} + \mathrm{i}\frac{2}{n}\sqrt{w(n-w)}. \tag{4.123}$$

We construct the vector

$$|v_p\rangle = \frac{1}{\sqrt{2w}}|b\rangle - \mathrm{i}\frac{1}{\sqrt{2(n-w)}}|\bar{b}\rangle, \tag{4.124}$$

where $|b\rangle$ denotes the vector formed by the binary word associated with position p on the hypercube and $|\bar{b}\rangle$ that formed by its negation. For example, for $n = 4$ and $p = 3$, we have $w = 2$ and

$$\lambda_2 = 1 - 2\frac{2}{4} + \mathrm{i}\frac{2}{4}\sqrt{2(4-2)} = \mathrm{i}, \tag{4.125}$$

and

$$|v_3\rangle = \frac{1}{\sqrt{2\times 2}}\begin{bmatrix}1\\1\\0\\0\end{bmatrix} - \mathrm{i}\frac{1}{\sqrt{2(4-2)}}\begin{bmatrix}0\\0\\1\\1\end{bmatrix} = \frac{1}{2}\begin{bmatrix}1\\1\\-\mathrm{i}\\-\mathrm{i}\end{bmatrix}. \tag{4.126}$$

We will show that $|v_p\rangle$ is the eigenvector of $\widetilde{U}^{(p)}$ associated with the eigenvalue λ_w. We first note that

$$\widetilde{S}^{(p)}|v_p\rangle = -|v_p\rangle^*, \tag{4.127}$$

and that

$$\widetilde{S}^{(p)}|u_n\rangle = \frac{|\bar{b}\rangle - |b\rangle}{\sqrt{n}}. \tag{4.128}$$

We also have

$$\begin{aligned}
\langle u_n|v_p\rangle &= \frac{1}{\sqrt{n}}\Big(\frac{w}{\sqrt{2w}} - \mathrm{i}\frac{n-w}{\sqrt{2(n-w)}}\Big), && (4.129)\\
&= \frac{1}{\sqrt{2n}}(\sqrt{w} - \mathrm{i}\sqrt{n-w}), && (4.130)\\
&= \frac{1}{\sqrt{2n}}(n\frac{1-\lambda_w}{2\sqrt{w}}), && (4.131)\\
&= \frac{1}{2\sqrt{2}}\sqrt{\frac{n}{w}}(1-\lambda_w). && (4.132)
\end{aligned}$$

Thus, we have

$$\begin{aligned}
\widetilde{U}^{(p)}|v_p\rangle &= \widetilde{S}^{(p)}G|v_p\rangle, && (4.133)\\
&= \widetilde{S}^{(p)}(-I_n + 2|u_n\rangle\langle u_n|)|v_p\rangle, && (4.134)\\
&= \Big(-\widetilde{S}^{(p)} + \frac{2}{\sqrt{n}}(|\bar{b}\rangle - |b\rangle)\langle u_n|\Big)|v_p\rangle, && (4.135)\\
&= -\widetilde{S}^{(p)}|v_p\rangle + \frac{2}{\sqrt{n}}\langle u_n|v_p\rangle(|\bar{b}\rangle - |b\rangle), && (4.136)\\
&= \frac{1}{\sqrt{2w}}|b\rangle + \mathrm{i}\frac{1}{\sqrt{2(n-w)}}|\bar{b}\rangle + \frac{1}{\sqrt{2n}}\sqrt{\frac{n}{w}}(1-\lambda_w)(|\bar{b}\rangle - |b\rangle), && (4.137)\\
&= \Big(1 - 2\frac{w}{n} + \mathrm{i}\frac{2}{n}\sqrt{w(n-w)}\Big)\Big(\frac{1}{\sqrt{2w}}|b\rangle - \mathrm{i}\frac{1}{\sqrt{2(n-w)}}|\bar{b}\rangle\Big), && (4.138)\\
&= \lambda_w|v_p\rangle. && (4.139)
\end{aligned}$$

We therefore conclude that for $N-2$ blocks $\widetilde{U}^{(p)}$ with $p \neq 0$ and $p \neq N-1$, we have two eigenvectors $|v_p\rangle$ and $|v_p\rangle^*$. This means that we have $(N-2)$ pairs of eigenvectors

of U associated with the eigenvalues λ_w and λ_w^*, which are of the form $F|p\rangle|v_p\rangle$ and $F|p\rangle|v_p^*\rangle$. Added to the $2(nN/2 - N + 2)$ eigenvectors from the $E_{\pm,\pm}^{S,C}$ spaces, we obtain all nN eigenvectors of U. We can therefore rewrite the equations (4.112) and (4.113) as

$$\dim(E_-^U) = \frac{nN}{2} - N + 2, \tag{4.140}$$

$$\dim(E_+^U) = \frac{nN}{2} - N + 2. \tag{4.141}$$

Moreover, since there are $\binom{n}{w}$ binary words of n bits and Hamming weight w, we have

$$\dim(E_{\lambda_w}^U) = \dim(E_{\lambda_w^*}^U) = \binom{n}{w}. \tag{4.142}$$

We define matrices V_w and V_w^* of size $N \times \binom{n}{w}$, whose columns are the eigenvectors of $\widetilde{U}$ corresponding to the positions where $\mathrm{wt}(p) = w$, that is

$$\mathrm{span}(V_w) = \{|p\rangle|v_p\rangle \mid p \in \mathbb{Z}_N\}, \tag{4.143}$$

$$\mathrm{span}(V_w^*) = \{|p\rangle|v_p^*\rangle \mid p \in \mathbb{Z}_N\}. \tag{4.144}$$

Table 4.3 summarizes the eigenvalue and eigenvector decomposition of the uniform walk operator U.

Table 4.3 Eigenspaces of the uniform walk operator

Eigenspace	Generator	Dimension
E_-^U	$FG'_+ +\!\!+ \|g_-\rangle$	$nN/2 - N + 2$
E_+^U	$FG'_- +\!\!+ \|u_{nN}\rangle$	$nN/2 - N + 2$
$E_{\lambda_w}^U$	FV_w	$\binom{n}{w}$
$E_{\lambda_w^*}^u$	FV_w^*	$\binom{n}{w}$

$+\!\!+$ denotes a horizontal concatenation

4.5. Dimension of the space of interest

4.5.1. Overview of the computation of the dimension of the space of interest

The search algorithm operator U' is defined from the uniform walk operator U and the problem oracle O, such that $U' = UO$. We have shown that the algorithm has no specific effect in the joint eigenspace of U and O, and is therefore only effective in the complement of this eigenspace, a space qualified "of interest", denoted $\mathcal{E}$. In this section, we will define and calculate the dimension of all the eigenspaces associated with U and O, in order to best define $\mathcal{E}$.

We first study the case of joint eigenspaces associated with the eigenvalue -1 of O, and show that this space is always empty, i.e.

$$E^{U,O}_{\lambda,-} = \emptyset. \tag{4.145}$$

Next, we study the eigenspaces associated with the real eigenvalues of U and the eigenvalue 1 of O. We show that

$$E^{U,O}_{\pm,+} = E^{S,C}_{\mp,-}, \tag{4.146}$$

and therefore

$$\dim(E^{U,O}_{\pm,+}) = \frac{nN}{2} - N + 1. \tag{4.147}$$

Finally, we study the eigenspaces associated with the complex eigenvalues of U and the eigenvalue 1 of O. We show that

$$\dim(E^{U,O}_{\lambda_w,+}) = \dim(E^{U,O}_{\lambda^*_w,+}) = \binom{n}{w} - \mathrm{rk}(H_N^{(s,w)}), \tag{4.148}$$

where $H_N^{(s,w)}$ is a submatrix of H_N defined in table 4.1.

This gives us the exact dimension of the space of interest $\mathcal{E}$

$$\dim(\mathcal{E}) = 2 + 2\sum_{w=1}^{n-1} \mathrm{rk}(H_N^{(s,w)}), \tag{4.149}$$

as well as a simpler upper bound

$$\dim(\mathcal{E}) \leqslant 2(n-1)M + 2, \tag{4.150}$$

which shows that the dimension of the space of interest grows linearly with the dimension n of the hypercube.

In the process, we also show that the initial state of the algorithm $|u_{nN}\rangle$ and the solution vector $|s\rangle$ are completely included in the space of interest, allowing us to calculate exactly the probability of success of the algorithm from their components in $\mathcal{E}$.

4.5.2. Detail of the computation of the dimension of the space of interest

The primary aim of the analysis presented in this chapter is to determine the dimension of the space of interest $\mathcal{E}$, in which the operators U and O do not commute, and where the algorithm converges to a solution. To do this, we will calculate the dimension of $\overline{\mathcal{E}}$, the space where the operators U and O commute. We have

$$\overline{\mathcal{E}} = \bigcup_{\lambda_U,\lambda_O} E^{U,O}_{\lambda_U,\lambda_O}, \tag{4.151}$$

and thus

$$\dim(\mathcal{E}) = \dim(\mathcal{H}) - \dim(\overline{\mathcal{E}}), \tag{4.152}$$

$$\dim(\mathcal{E}) = nN - \sum_{\lambda_U,\lambda_O} \dim(E^{U,O}_{\lambda_U,\lambda_O}). \tag{4.153}$$

Case of the joint eigenspaces $E^{U,O}_{\lambda,-}$

We can show that the joint eigenspaces of U and O where $\lambda_O = -1$ are all empty. We showed earlier that $E^O_- \subset E^C_+$, and therefore, for any eigenvalue λ

$$E^{U,O}_{\lambda,-} \subset E^{U,C}_{\lambda,+}. \tag{4.154}$$

Furthermore, since $U = SC$, $E^{U,C}_{\lambda,+} = E^{S,C}_{\lambda,+}$, and we have $E^{U,O}_{\lambda,-} \subset E^{S,C}_{\lambda,+}$, which means that $\lambda = \pm 1$, as S has no other eigenvalues. We then have

$$E^{U,O}_{-,-} \subset E^{S,C}_{-,+}, \tag{4.155}$$

$$E^{U,O}_{+,-} \subset E^{S,C}_{+,+}, \tag{4.156}$$

that is

$$E^{U,O}_{-,-} \subset \text{span}(|g_-\rangle), \tag{4.157}$$

$$E^{U,O}_{+,-} \subset \text{span}(|u_{nN}\rangle), \tag{4.158}$$

As previously mentioned, the vectors $|g_-\rangle$ and $|u_{nN}\rangle$ do not belong to span(G_1), and therefore not to E^O_-. Therefore

$$E^{U,O}_{\lambda,-} = \emptyset. \tag{4.159}$$

Case of the joint eigenspaces $E^{U,O}_{\pm,+}$

We are now looking at the joint eigenspaces of U and O where $\lambda_O = +1$. Consider first the spaces $E^{U,O}_{\pm,+}$. We have

$$E^U_+ = E^{S,C}_{-,-} \cup E^{S,C}_{+,+}, \tag{4.160}$$
$$E^U_- = E^{S,C}_{+,-} \cup E^{S,C}_{-,+}, \tag{4.161}$$

soit

$$E^U_+ = \text{span}(FG'_+) \cup \text{span}(|u_{nN}\rangle), \tag{4.162}$$
$$E^U_- = \text{span}(FG'_-) \cup \text{span}(|g_-\rangle). \tag{4.163}$$

The vectors $|u_{nN}\rangle$ and $|g_-\rangle$ do not belong to G_2 either. Since $\text{span}(FG'_\pm) \subset \text{span}(G_3)$ and $E^O_+ = \text{span}(G_{2,3})$, we have

$$E^{U,O}_{\pm,+} = E^{S,C}_{\mp,-}, \tag{4.164}$$

that is

$$\dim(E^{U,O}_{\pm,+}) = \frac{nN}{2} - N + 1. \tag{4.165}$$

We also note the important fact that $|u_{nN}\rangle$ does not belong to any eigenspace of O, which means that $|u_{nN}\rangle$ is in $\mathcal{E}$, and that the state of the system at any iteration $|\psi_t\rangle = U'^t|u_{nN}\rangle$ remains in $\mathcal{E}$. Moreover, since $|s\rangle$ belongs to G_1, the superposition of solutions is also in $\mathcal{E}$. We will see that these properties enable us to calculate the algorithm probability of success in polynomial time.

Case of the joint eigenspaces $E^{U,O}_{\lambda_w,+}$ and $E^{U,O}_{\lambda^*_w,+}$

The last case to be treated is that of the spaces $E^{U,O}_{\lambda_w,+}$ and $E^{U,O}_{\lambda^*_w,+}$. To do this, we define $\tilde{O}$ as the spatial Fourier transform of O. Since $\mathcal{H} = \text{span}(G_1) \cup \text{span}(G_{2,3})$, we can reformulate $E^O_+ = \text{span}(G_{2,3})$ to $E^O_+ = \ker({G_1}^\intercal)$, and thus

$$E^{\tilde{O}}_+ = \ker((FG_1)^\intercal). \tag{4.166}$$

Since we have

$$FG_1 = (H_N \otimes I_n)(I^{(s)}_N \otimes |u_n\rangle), \tag{4.167}$$
$$= H^{(s)}_N \otimes |u_n\rangle, \tag{4.168}$$

where $H^{(s)}_N$ is the submatrix of H_N of size $N \times M$ defined in section 4.2, formed by keeping only those columns of H_N corresponding to solutions. We then have

$$E^{\tilde{O}}_+ = \ker\big(H^{(s)\intercal}_N \otimes \langle u_n|\big). \tag{4.169}$$

Since $E_{\lambda_w}^{\widetilde{U}} = \mathrm{span}(V_w)$, we have

$$E_{\lambda_w,+}^{\widetilde{U},\widetilde{O}} = \mathrm{span}(V_w) \cap \ker\big(H_N^{(s)\mathsf{T}} \otimes \langle u_n|\big). \tag{4.170}$$

Any vector $|p\rangle|v_w\rangle$ of $\mathrm{span}(V_w)$ can be expressed $V_w|\nu\rangle$, where $|\nu\rangle$ is a unit vector of length $\binom{n}{w}$. Since we work in $\ker\big(H_N^{(s)\mathsf{T}} \otimes \langle u_n|\big)$, we must also have

$$\big(H_N^{(s)\mathsf{T}} \otimes \langle u_n|\big)(V_w|\nu\rangle) = 0, \tag{4.171}$$

that is, $|\nu\rangle$ is orthogonal to all columns of $\big(H_N^{(s)\mathsf{T}} \otimes \langle u_n|\big)V_w$. These columns are

$$\big(H_N^{(s)\mathsf{T}} \otimes \langle u_n|\big)(|p\rangle \otimes |v_w\rangle) = \langle u_n|v_w\rangle\big(H_N^{(s)\mathsf{T}}\big)|p\rangle. \tag{4.172}$$

Here, $\big(H_N^{(s)\mathsf{T}}\big)|p\rangle$ corresponds to the column of $H_N^{(s)\mathsf{T}}$ associated with position p, and $\langle u_n|v_w\rangle$ to a scalar that we will denote α_w, such that

$$\alpha_w = \sqrt{\frac{w}{2}} - \mathrm{i}\sqrt{\frac{n-w}{2}}. \tag{4.173}$$

It follows that

$$\big(H_N^{(s)\mathsf{T}} \otimes \langle u_n|\big)V_w = \alpha_w H_N^{(s,w)\mathsf{T}}, \tag{4.174}$$

where $H_N^{(s,w)}$ is the submatrix of $H_N^{(s)}$ defined in section 4.2, formed by keeping only the rows of $H_N^{(s)}$ corresponding to positions associated with binary words of Hamming weight w. Since $\alpha_w \neq 0$, we must have

$$H_N^{(s,w)\mathsf{T}}|\nu\rangle = 0, \tag{4.175}$$

that is

$$|\nu\rangle \in \ker\big(H_N^{(s,w)\mathsf{T}}\big). \tag{4.176}$$

We therefore deduce

$$E_{\lambda_w,+}^{U,O} = \{F V_w|\nu\rangle \mid |\nu\rangle \in \ker(H_N^{(s,w)})\}, \tag{4.177}$$

$$E_{\lambda_w^*,+}^{U,O} = \{F V_w^*|\nu\rangle \mid |\nu\rangle \in \ker(H_N^{(s,w)})\}, \tag{4.178}$$

and

$$\dim(E_{\lambda_w,+}^{U,O}) = \dim(E_{\lambda_w^*,+}^{U,O}) = \dim\big(\ker\big(H_N^{(s,w)\mathsf{T}}\big)\big), \tag{4.179}$$

$$= \binom{n}{w} - \mathrm{rk}(H_N^{(s,w)}). \tag{4.180}$$

The table 4.4 summarizes the eigenvalue and eigenvector decomposition of the search algorithm operator U'.

Table 4.4 Eigenspaces of the search algorithm operator

Eigenspace	Expression	Dimension
$E^{U,O}_{\pm,+}$	$\mathrm{span}(FG'_{\mp})$	$nN/2 - N + 1$
$E^{U,O}_{\lambda_w,+}$	$\{FV_w\|\nu\rangle \mid \|\nu\rangle \in \ker(H_N^{(s,w)})\}$	$\binom{n}{w} - \mathrm{rk}(H_N^{(s,w)})$
$E^{U,O}_{\lambda_w^*,+}$	$\{FV_w^*\|\nu\rangle \mid \|\nu\rangle \in \ker(H_N^{(s,w)})\}$	$\binom{n}{w} - \mathrm{rk}(H_N^{(s,w)})$

Dimension of the space of interest

We now know all the eigenspaces of $\bar{\mathcal{E}}$ and their respective dimensions. Then

$$\dim(\bar{\mathcal{E}}) = 2\Big(\frac{nN}{2} - N + 1\Big) + 2\sum_{w=1}^{n-1}\left(\binom{n}{w} - \mathrm{rk}(H_N^{(s,w)})\right), \tag{4.181}$$

$$= nN - 2N + 2 + 2(N-2) - 2\sum_{w=1}^{n-1}\mathrm{rk}(H_N^{(s,w)}), \tag{4.182}$$

$$= nN - 2 - 2\sum_{w=1}^{n-1}\mathrm{rk}(H_N^{(s,w)}). \tag{4.183}$$

This gives us the dimension of the space of interest

$$\dim(\mathcal{E}) = nN - \dim(\bar{\mathcal{E}}), \tag{4.184}$$

$$= 2 + 2\sum_{w=1}^{n-1}\mathrm{rk}(H_N^{(s,w)}). \tag{4.185}$$

We know that $\bar{\mathcal{E}} \subseteq E^O_+$, so

$$\dim(\bar{\mathcal{E}}) \leqslant nN - M. \tag{4.186}$$

Moreover, as $1 \leqslant \mathrm{rk}(H_N^{(s,w)}) \leqslant \min(M, \binom{n}{w})$, we have

$$\max(2n, M) \leqslant \dim(\mathcal{E}) \leqslant 2(n-1)M + 2. \tag{4.187}$$

We can see that the dimension of the space of interest $\mathcal{E}$ grows linearly with the dimension of the hypercube n, while the total space $\mathcal{H}$ grows exponentially (remember that $\dim(\mathcal{H}) = n2^n$). For example, in the case of a hypercube of dimension $n = 100$, the total space is of dimension $\dim(\mathcal{H}) = 1.27 \times 10^{32}$, whereas that of the space of interest, in which the algorithm acts, is $\dim(\mathcal{E}) \leqslant 198M + 2$. This doesn't mean that we can simulate the search algorithm on a conventional computer, but we will see that it at least allows us to predict its probability of success as it is iterated.

4.6. Summary of the eigenanalysis

The hypercube quantum search algorithm is an iterative algorithm consisting of the repetition of the same operator U' a certain number of times R, the determination of which is one of the subjects of this work. This operator U' is decomposed into an oracle O, capable of "marking" the solutions of the problem studied, and a uniform walk operator U, depending only on the dimension n of the hypercube. The uniform walk U is itself the combination of two operators, the coin operator that mixes the directions of displacement on the hypercube C, and the shift operator S which moves the particles along these directions. We have

$$U' = UO = SCO. \tag{4.188}$$

In this chapter, we first showed that in the joint eigenspace of U and O, the application of two iterations of the algorithm, that is U'^2, was equivalent to that of two iterations of the walk without the oracle, that is U^2. In this space, the algorithm then has no reason to converge to a solution, and we deduce that its useful component takes place in the complement of this joint eigenspace, which we call $\mathcal{E}$.

By eigenanalysis of the elementary operators S, C and O and of their joint eigenspaces, we find that the dimension of $\mathcal{E}$ grows only linearly in the dimension n of the hypercube, while that of the global space $\mathcal{H}$ grows exponentially. To facilitate this analysis, we use several generator matrices whose columns generate eigenspaces from which we can express the eigenspaces of the operators. These matrices are defined in equations from (4.31) to (4.37). We also use the spatial Fourier transform defined by equation (2.59), which allows us to diagonalize S, and thus obtain a block-diagonal structure when studying the U operator.

Finally, we determine three eigenspaces common to U and O, as well as the dimension of their union in equation (4.183). This gives us an upper bound on the dimension of the space of interest $\mathcal{E}$.

$$\dim(\mathcal{E}) \leqslant 2(n-1)M + 2, \tag{4.189}$$

where M is the number of solutions to the problem.

In addition, we have shown that the states $|u_{nN}\rangle$ and $|s\rangle$ belong to the space of interest $\mathcal{E}$, which will allow us to calculate the probability of success in the next chapter.

5. Search algorithm probability of success calculation

In the previous chapter, we showed that the dimension of the space of interest $\mathcal{E}$ grows linearly in n and that the uniform state $|u_{nN}\rangle$, which serves as the initial state of the algorithm, belongs to $\mathcal{E}$. As each column of G_1 corresponds to a solution position, the uniform superposition of solution elements $|s\rangle$ is the sum of these M columns, that is to say

$$|s\rangle = \frac{1}{\sqrt{M}} \sum_{\substack{p\in\mathbb{Z}_N \\ f(p)=1}} |p\rangle|u_n\rangle. \tag{5.1}$$

Since $\text{span}(G_1) = E_-^O$ and $E_-^O \subset \mathcal{E}$, we have $|s\rangle \in \mathcal{E}$. Furthermore, since

$$|\bar{s}\rangle = \sqrt{\frac{nN}{n(N-M)}}|u_{nN}\rangle - \sqrt{\frac{nM}{n(N-M)}}|s\rangle, \tag{5.2}$$

then we also have $|\bar{s}\rangle \in \mathcal{E}$. The rules of measurement in quantum physics allow us to establish that the probability of success at iteration t is

$$\mathbf{P}_t(s) = \left|\langle s|U'^t|u_{nN}\rangle\right|^2. \tag{5.3}$$

It can be calculated solely from the system component in $\mathcal{E}$. In a basis formed by the eigenvectors of U', we can represent its component in $\mathcal{E}$ by a diagonal matrix $U'_{\mathcal{E}}$ of size $\dim(\mathcal{E}) \times \dim(\mathcal{E})$, whose coefficients are the eigenvalues $\mathrm{e}^{iu\varphi_k}$ of U' in $\mathcal{E}$.

We denote $u(k,l)$ and $s(k,l)$ the components of the vectors $|u_{nN}\rangle$ and $|s\rangle$ in $\mathcal{E}$ associated with the eigenvalue $\mathrm{e}^{\mathrm{i}\varphi_k}$, the parameter l being used to distinguish components associated with the same eigenvalue. The state vector of the system at iteration t being $|\psi_t\rangle = U'^t|u_{nN}\rangle$, its components in $\mathcal{E}$ are

$$\psi_t(k,l) = \mathrm{e}^{\mathrm{i}\varphi_k t} u(k,l). \tag{5.4}$$

We then have

$$\mathbf{P}_t(s) = \left|\sum_{k,l} s(k,l)^* \psi_t(k,l)\right|^2, \tag{5.5}$$

$$= \left|\sum_{k,l} \mathrm{e}^{\mathrm{i}\varphi_k t} s(k,l)^* u(k,l)\right|^2, \tag{5.6}$$

and we can then calculate the algorithm probability of success with only the $\dim(\mathcal{E})$ eigenvalues of U' in $\mathcal{E}$ and the associated components of the $|u_{nN}\rangle$ and $|s\rangle$ vectors.

This chapter, like the previous one, involves a significant amount of mathematical development. A summary of the method for calculating the probability of success is therefore given in section 5.4. It may be useful to use this summary as a guide while reading the chapter.

5.1. Space of interest eigenanalysis

5.1.1. Overview of the space of interest eigenanalysis

In this section, exploiting the results of chapter 4, we study the component of the algorithm operator U' in the space of interest $\mathcal{E}$ to determine its eigenvalues. We denote by $|\varepsilon\rangle$ an eigenvector of U' in $\mathcal{E}$, and represent it by its components in E_+^{CO} and E_-^{CO}, respectively noted $|\varepsilon_+\rangle$ and $|\varepsilon_-\rangle$. We then have

$$|\varepsilon\rangle = |\varepsilon_+\rangle + |\varepsilon_-\rangle. \tag{5.7}$$

We then show that for a given eigenvalue $\lambda_k = \mathrm{e}^{\mathrm{i}\varphi_k}$, we can express $|\varepsilon_+\rangle$ as a function of $|\varepsilon_-\rangle$, and vice versa. We have

$$|\varepsilon_+\rangle = \mathrm{i}\Big(\cot\frac{\varphi_k}{2}P_+^S - \tan\frac{\varphi_k}{2}P_-^S\Big)|\varepsilon_-\rangle, \tag{5.8}$$

$$|\varepsilon_-\rangle = -\mathrm{i}\Big(\tan\frac{\varphi_k}{2}P_+^S - \cot\frac{\varphi_k}{2}P_-^S\Big)|\varepsilon_+\rangle, \tag{5.9}$$

where the matrices P_+^S and P_-^S are projectors into the spaces E_+^S and E_-^S.

We create a matrix $\widetilde{\Gamma}_{\varphi_k}$ which allows the passage between the vectors $|\tilde{\varepsilon}_+\rangle$ and $|\tilde{\varepsilon}_-\rangle$, the spatial Fourier transforms of the vectors $|\varepsilon_+\rangle$ and $|\varepsilon_-\rangle$, defined as

$$\widetilde{\Gamma}_{\varphi_k} = \cot\frac{\varphi_k}{2}\widetilde{P}_+^S + \tan\frac{\varphi_k}{2}\widetilde{P}_-^S. \tag{5.10}$$

We then have

$$|\tilde{\varepsilon}_+\rangle = \mathrm{i}\widetilde{\Gamma}_{\varphi_k}|\tilde{\varepsilon}_-\rangle, \tag{5.11}$$

$$|\tilde{\varepsilon}_-\rangle = -\mathrm{i}\widetilde{\Gamma}_{\varphi_k}^{-1}|\tilde{\varepsilon}_+\rangle. \tag{5.12}$$

From the matrix $\widetilde{\Gamma}_{\varphi_k}$, we create a matrix D_{φ_k}, defined by the inverse of its spatial Fourier transform, the diagonal matrix $\widetilde{D}_{\varphi_k}^{-1}$, whose p-th coefficient is

$$\widetilde{D}_{\varphi_k}^{-1}(p) = \Big(1 - \frac{w}{n}\Big)\tan\frac{\varphi_k}{2} - \frac{w}{n}\cot\frac{\varphi_k}{2}, \tag{5.13}$$

where w denotes the Hamming weight of the binary word associated with position p.

We then create $D^{(s)}_{\varphi_k}$, the submatrix of D_{φ_k} obtained by keeping only the rows and columns associated with solution positions. If $e^{i\varphi_k}$ is an eigenvalue of U' in $\mathcal{E}$, then the matrix $D^{(s)}_{\varphi_k}$ is singular. This means that for any angle θ, if the matrix $D^{(s)}_{\theta}$ is singular, then $e^{i\theta}$ is probably an eigenvalue of U' in $\mathcal{E}$.

Thanks to singular value decomposition (see appendix E), it is easy to test whether a matrix $D^{(s)}_{\theta}$ is singular or not. Indeed, if at least one of the singular values of a matrix is zero, then it is singular. We therefore have a criterion for identifying eigenvalues. We also show that it suffices to test angles θ in the interval $[0, \pi/2[$ to find all the eigenvalues by symmetry. Moreover, in our case, the number of zero singular values tells us the dimension of the eigenspace associated with a given eigenvalue.

5.1.2. Detail of the space of interest eigenanalysis

Expressions for the vectors $|\varepsilon_+\rangle$ and $|\varepsilon_-\rangle$

In this section, we study the component of U' in $\mathcal{E}$ to determine its eigenvalues. Since we have $\mathcal{H} = E^{CO}_+ \cup E^{CO}_-$, any eigenvector $|\varepsilon\rangle$ of U' in $\mathcal{E}$ can be decomposed into a sum of vectors $|\varepsilon_+\rangle$ and $|\varepsilon_-\rangle$ belonging to E^{CO}_+ and E^{CO}_- respectively, that is

$$|\varepsilon\rangle = |\varepsilon_+\rangle + |\varepsilon_-\rangle. \tag{5.14}$$

Let $\lambda_k = e^{i\varphi_k}$ be an eigenvalue of U'. We have

$$U'|\varepsilon\rangle = \lambda_k|\varepsilon\rangle = \lambda_k(|\varepsilon_+\rangle + |\varepsilon_-\rangle), \tag{5.15}$$

but also

$$U'|\varepsilon\rangle = SCO(|\varepsilon_+\rangle + |\varepsilon_-\rangle), \tag{5.16}$$

$$= S|\varepsilon_+\rangle - S|\varepsilon_-\rangle. \tag{5.17}$$

We therefore have

$$S|\varepsilon_+\rangle - S|\varepsilon_-\rangle = \lambda_k(|\varepsilon_+\rangle + |\varepsilon_-\rangle), \tag{5.18}$$

that is, as $S^2 = I_{nN}$,

$$|\varepsilon_+\rangle - |\varepsilon_-\rangle = \lambda_k S(|\varepsilon_+\rangle + |\varepsilon_-\rangle). \tag{5.19}$$

We define P^S_+ and P^S_- as projectors to the spaces E^S_+ and E^S_-, operators with the property

$$\forall|x\rangle \in \mathcal{H}, P^S_\pm|x\rangle \in E^S_\pm. \tag{5.20}$$

Since S is a unit operator such that $S^2 = I_{nN}$, we show

$$P^S_+ = \frac{I_{nN} + S}{2}, \tag{5.21}$$

$$P^S_- = \frac{I_{nN} - S}{2}, \tag{5.22}$$

and

$$P_+^S S = P_+^S, \tag{5.23}$$
$$P_-^S S = -P_-^S. \tag{5.24}$$

We deduce

$$P_+^S|\varepsilon_+\rangle - P_+^S|\varepsilon_-\rangle = \lambda_k P_+^S|\varepsilon_+\rangle + \lambda_k P_+^S|\varepsilon_-\rangle, \tag{5.25}$$
$$-P_-^S|\varepsilon_+\rangle + P_-^S|\varepsilon_-\rangle = \lambda_k P_-^S|\varepsilon_+\rangle + \lambda_k P_-^S|\varepsilon_-\rangle, \tag{5.26}$$

that is

$$(1-\lambda_k)P_+^S|\varepsilon_+\rangle = (1+\lambda_k)P_+^S|\varepsilon_-\rangle, \tag{5.27}$$
$$(1+\lambda_k)P_-^S|\varepsilon_+\rangle = (1-\lambda_k)P_-^S|\varepsilon_-\rangle. \tag{5.28}$$

When $\lambda_k \neq \pm 1$, we have

$$\frac{1-\lambda_k}{1+\lambda_k} = -\frac{\mathrm{e}^{\mathrm{i}\frac{\varphi_k}{2}} - \mathrm{e}^{-\mathrm{i}\frac{\varphi_k}{2}}}{\mathrm{e}^{\mathrm{i}\frac{\varphi_k}{2}} + \mathrm{e}^{-\mathrm{i}\frac{\varphi_k}{2}}} = -\mathrm{i}\tan\frac{\varphi_k}{2}, \tag{5.29}$$

and

$$\frac{1+\lambda_k}{1-\lambda_k} = \mathrm{i}\frac{1}{\tan\frac{\varphi_k}{2}} = \mathrm{i}\cot\frac{\varphi_k}{2}, \tag{5.30}$$

therefore

$$P_+^S|\varepsilon_+\rangle = \mathrm{i}\cot\frac{\varphi_k}{2}P_+^S|\varepsilon_-\rangle, \tag{5.31}$$
$$P_-^S|\varepsilon_+\rangle = -\mathrm{i}\tan\frac{\varphi_k}{2}P_-^S|\varepsilon_-\rangle. \tag{5.32}$$

Since $P_+^S + P_-^S = I_{nN}$, we finally obtain

$$|\varepsilon_+\rangle = \mathrm{i}\Big(\cot\frac{\varphi_k}{2}P_+^S - \tan\frac{\varphi_k}{2}P_-^S\Big)|\varepsilon_-\rangle, \tag{5.33}$$
$$|\varepsilon_-\rangle = -\mathrm{i}\Big(\tan\frac{\varphi_k}{2}P_+^S - \cot\frac{\varphi_k}{2}P_-^S\Big)|\varepsilon_+\rangle. \tag{5.34}$$

We denote $\widetilde{P}_\pm^S$ the spatial Fourier transform of $P_\pm^S$. From the eigenanalysis of S performed in section 4.1, we know that $\widetilde{P}_\pm^S$ is a diagonal matrix whose coefficients of signature $\varsigma_i = \pm 1$ are equal to 1 and the others, of signature $\varsigma_i = \mp 1$, are 0. We define

$$\widetilde{\Gamma}_{\varphi_k} = \cot\frac{\varphi_k}{2}\widetilde{P}_+^S + \tan\frac{\varphi_k}{2}\widetilde{P}_-^S, \tag{5.35}$$

so as to have

$$|\tilde{\varepsilon}_+\rangle = \mathrm{i}\widetilde{\Gamma}_{\varphi_k}|\tilde{\varepsilon}_-\rangle, \tag{5.36}$$

$$|\tilde{\varepsilon}_-\rangle = -\mathrm{i}\widetilde{\Gamma}^{-1}_{\varphi_k}|\tilde{\varepsilon}_+\rangle, \tag{5.37}$$

where $|\tilde{\varepsilon}_+\rangle$ and $|\tilde{\varepsilon}_-\rangle$ are the spatial Fourier transforms of $|\varepsilon_+\rangle$ and $|\varepsilon_-\rangle$.

We have

$$|\varepsilon_+\rangle \in E^{CO}_+ = \mathrm{span}(G_2), \tag{5.38}$$

$$|\varepsilon_-\rangle \in E^{CO}_- = \mathrm{span}(G_{1,3}), \tag{5.39}$$

and since $FG'_\pm$ generates a space orthogonal to $\mathcal{E}$, we have

$$|\varepsilon_-\rangle \in \mathrm{span}(G_1) \cup \mathrm{span}(G'_\circ). \tag{5.40}$$

These vectors can be expressed as

$$|\varepsilon_+\rangle = G_2|\varepsilon_2\rangle, \tag{5.41}$$

$$|\varepsilon_-\rangle = G_1|\varepsilon_1\rangle + FG'_\circ|\varepsilon_\circ\rangle, \tag{5.42}$$

that is

$$|\varepsilon_+\rangle = I_N^{(\bar{s})}|\varepsilon_2\rangle \otimes |u_n\rangle, \tag{5.43}$$

$$|\varepsilon_-\rangle = I_N^{(s)}|\varepsilon_1\rangle \otimes |u_n\rangle + FG'_\circ|\varepsilon_\circ\rangle, \tag{5.44}$$

where $|\varepsilon_1\rangle$, $|\varepsilon_2\rangle$ and $|\varepsilon_\circ\rangle$ are vectors of sizes M, $N-M$ and $(n-1)N$ respectively. We define the vectors

$$|e_+\rangle = I_N^{(\bar{s})}|\varepsilon_2\rangle, \tag{5.45}$$

$$|e_-\rangle = I_N^{(s)}|\varepsilon_1\rangle. \tag{5.46}$$

Since $FG'_\circ|\varepsilon_\circ\rangle$ is a vector made up of N blocks of n values of zero mean, we have

$$|e_\pm\rangle = (I_N \otimes \langle u_n|)|\varepsilon_\pm\rangle. \tag{5.47}$$

We can decompose $\widetilde{\Gamma}^{-1}_{\varphi_k}$ into

$$\widetilde{\Gamma}^{-1}_{\varphi_k} = \widetilde{D}^{-1}_{\varphi_k} \otimes I_n + \Upsilon_{\varphi_k}, \tag{5.48}$$

where $\widetilde{D}^{-1}_{\varphi_k}$ is a diagonal $N \times N$ matrix whose elements are the averages of n blocks of $\widetilde{\Gamma}^{-1}_{\varphi_k}$, and Υ_{φ_k} is another diagonal matrix made up of N blocks of size $n \times n$ and of zero average. The coefficients of the diagonal of $\widetilde{D}^{-1}_{\varphi_k}$ are

$$\widetilde{D}^{-1}_{\varphi_k}(p) = \left(1 - \frac{w}{n}\right)\tan\frac{\varphi_k}{2} - \frac{w}{n}\cot\frac{\varphi_k}{2}, \tag{5.49}$$

with $w = \mathrm{wt}(p)$. Let $|e_+\rangle$ and $|e_-\rangle$ be the spatial Fourier transforms of $|e_+\rangle$ and $|e_-\rangle$. Since all blocks of Υ_{φ_k} have zero mean, we have $\Upsilon_{\varphi_k}(|x\rangle \otimes |u_n\rangle) = 0$ for any $|x\rangle$ vector of size N. According to equation (5.37), we therefore have

$$|\tilde{e}_-\rangle = -\mathrm{i}\widetilde{D}_{\varphi_k}^{-1}|\tilde{e}_+\rangle. \tag{5.50}$$

If none of the coefficients of the diagonal of $\widetilde{D}_{\varphi_k}^{-1}$ is zero, we also have

$$|\tilde{e}_+\rangle = \mathrm{i}\widetilde{D}_{\varphi_k}|\tilde{e}_-\rangle, \tag{5.51}$$

with

$$\widetilde{D}_{\varphi_k}(p) = \left(\left(1 - \frac{w}{n}\right)\tan\frac{\varphi_k}{2} - \frac{w}{n}\cot\frac{\varphi_k}{2}\right)^{-1}. \tag{5.52}$$

We can see that the values of $\widetilde{D}_{\varphi_k}(p)$ are identical for positions associated with binary words of the same Hamming weight w. We denote the value common to these positions by $\widetilde{D}_{\varphi_k}^{(w)}$. The case where $\widetilde{D}_{\varphi_k}^{-1}$ is singular, that is, its diagonal contains zero terms, will be dealt with later in the chapter. Leaving the Fourier domain, we have

$$D_{\varphi_k} = H_N \widetilde{D}_{\varphi_k} H_N, \tag{5.53}$$

and

$$|e_+\rangle = \mathrm{i}D_{\varphi_k}|e_-\rangle. \tag{5.54}$$

We define $D_{\varphi_k}^{(s)}$ the $M \times M$ submatrix of D_{φ_k} obtained from the rows and columns associated with the solutions, that is to say

$$D_{\varphi_k}^{(s)} = H_N^{(s)} \widetilde{D}_{\varphi_k} H_N^{(s)}. \tag{5.55}$$

For each eigenvalue $\mathrm{e}^{\mathrm{i}\varphi_k}$, the vectors $|\varepsilon_1\rangle$ form an orthogonal basis of $\ker(D_{\varphi_k}^{(s)})$. We can therefore find the eigenvalues of $\mathcal{E}$, by constructing matrices $D_\theta^{(s)}$ for different angles $\theta \in [0, 2\pi[$. For each angle θ, we define

$$d_\theta = \dim(\ker(D_\theta^{(s)})). \tag{5.56}$$

If $d_\theta \geqslant 1$, then $\mathrm{e}^{\mathrm{i}\theta}$ is probably an eigenvalue of $\mathcal{E}$, associated with d_θ eigenvectors. As the eigenvalues come in complex conjugate pairs, we can restrict the search to $[0, \pi[$. Furthermore, since we have

$$D_\theta^{(s)} = -D_{-\theta}^{(s)}, \tag{5.57}$$

and that

$$\ker(D_\theta^{(s)}) = \ker(D_{-\theta}^{(s)}), \tag{5.58}$$

research can still be reduced to $[0, \pi/2[$.

We can calculate d_θ using the singular value decomposition, or SVD (see appendix E), of $D_\theta^{(s)}$, since the number of zero singular values of a matrix equals the dimension of its kernel. Since the matrix $D_\theta^{(s)}$ has size $M \times M$, the search for eigenvalues by SVD has polynomial complexity in M, the number of solutions. We denote σ_θ the last, and therefore smallest, singular value of $D_\theta^{(s)}$. By testing a set of angles $\theta \in [0, \pi/2[$, it is unlikely to find a case where at least one singular value is exactly equal to zero. We therefore look for local minima of the function $\sigma_\theta(\theta)$, corresponding to probable eigenvalues of $\mathrm{e}^{\mathrm{i}\theta}$.

5.2. Eigenvalue search in polynomial time

As the method of finding eigenvalues by locating the minima of $\sigma_\theta(\theta)$ is based on the SVD of matrices $D_\theta^{(s)}$ of size $M \times M$, it is feasible in polynomial time provided that we can calculate these matrices quickly. Indeed, equation (5.55) involves $\widetilde{D}_\theta$ and $H_N^{(s)}$, two $N \times N$ matrices, that is, that grow exponentially with respect to the dimension of the hypercube. Direct calculation of $D_\theta^{(s)}$ is therefore impossible when n is large. However, since $\widetilde{D}_\theta$ is diagonal, we have

$$D_\theta^{(s)} = \sum_{w=0}^{n} \widetilde{D}_\theta^{(w)} H_N^{(s,w)\mathsf{T}} H_N^{(s,w)}. \tag{5.59}$$

We define the matrix $\Xi_w = H_N^{(s,w)\mathsf{T}} H_N^{(s,w)}$ of size $M \times M$, so as to have

$$D_\theta^{(s)} = \sum_{w=0}^{n} \widetilde{D}_\theta^{(w)} \Xi_w. \tag{5.60}$$

We define $\bar{H}_N$, the unnormalized Hadamard matrix

$$\bar{H}_N = \sqrt{N} H_N, \tag{5.61}$$

containing only coefficients ± 1, and $|h_i\rangle$ the column of $\bar{H}_N$ corresponding to position i. We have

$$\Xi_w(i,j) = \frac{1}{N}\langle h_i | h_j \rangle, \tag{5.62}$$

$$= \frac{1}{N} \sum_{\substack{p \in \mathbb{Z}_N \\ \mathrm{wt}(p)=w}} h_i(p) h_j(p). \tag{5.63}$$

Let $|b_i\rangle$ be the binary representation of position i. Hadamard matrices have the property

$$\bar{H}_N(i,j) = (-1)^{\langle b_i | b_j \rangle}, \tag{5.64}$$

therefore

$$h_i(p)h_j(p) = (-1)^{\langle b_p|b_i\rangle}(-1)^{\langle b_p|b_j\rangle}, \tag{5.65}$$

$$= (-1)^{\langle b_p|b_i\oplus b_j\rangle}, \tag{5.66}$$

$$= h_{i\oplus j}(p), \tag{5.67}$$

where $i \oplus j$ designates the position associated to the binary word $|b_i \oplus b_j\rangle$.

We define $\eta_i^{(w)}$ as the sum of the elements of $|h_i\rangle$ at positions p where $\mathrm{wt}(p) = w$, that is

$$\eta_i^{(w)} = \sum_{\substack{p\in\mathbb{Z}_N \\ \mathrm{wt}(p)=w}} h_i(p), \tag{5.68}$$

$$= \sum_{\substack{p\in\mathbb{Z}_N \\ \mathrm{wt}(p)=w}} (-1)^{\langle b_p|b_i\rangle}. \tag{5.69}$$

The elements of this sum are positive when $\langle b_p|b_i\rangle$ is even, which happens when $|b_p\rangle$ contains an even number of bits equal to 1 among the Hamming weight positions $w_i = \mathrm{wt}(i)$. We denote this even number $2k$, and there is $\binom{w_i}{2k}$ possible placement for these 1, and $\binom{n-w_i}{w-2k}$ for the remaining $w - 2k$ coefficients equal to 1. The total number of positive terms in the sum is therefore

$$\zeta_i^{(w)} = \sum_k \binom{w_i}{2k}\binom{n-w_i}{w-2k}, \tag{5.70}$$

for all values of k where these two binomial coefficients are defined, that is

$$0 \leqslant k \leqslant \frac{w_i}{2}, \tag{5.71}$$

$$\frac{w_i + w - n}{2} \leqslant k \leqslant \frac{w}{2}. \tag{5.72}$$

In $|h_i\rangle$, there are $\binom{n}{w}$ positions associated with elements of weight w whose $\zeta_i^{(w)}$ coefficients are positive. There are therefore $\binom{n}{w} - \zeta_i^{(w)}$ negative coefficients and the sum of these coefficients is

$$\eta_i^{(w)} = \zeta_i^{(w)} - \left(\binom{n}{w} - \zeta_i^{(w)}\right), \tag{5.73}$$

$$= 2\zeta_i^{(w)} - \binom{n}{w}. \tag{5.74}$$

Note that since $\eta_i^{(w)}$ does not depend on i but on w_i, we can calculate it for several values of i and save calculation time.

In the end

$$\Xi_w(i,j) = \frac{1}{N}\eta_{i\oplus j}^{(w)}, \tag{5.75}$$

and we can calculate $D_\theta^{(s)}$ without using the matrices $\widetilde{D}_\theta$ and $H_N^{(s)}$.

5.3. Vector components in the space of interest

5.3.1. Overview of the vector component calculation

In this section, we compute the components of the vectors $|s\rangle$ and $|u_{nN}\rangle$ in the space of interest $\mathcal{E}$ in order to calculate the exact value of the probability of success of the algorithm from a reduced number of values.

From the results of chapter 4, we show that any eigenvector $|\varepsilon\rangle$ of the algorithm operator U' in $\mathcal{E}$ can be expressed as

$$|\varepsilon\rangle = G_1|\varepsilon_1\rangle + G_2|\varepsilon_2\rangle + FG'_\circ|\varepsilon_\circ\rangle, \tag{5.76}$$

For each eigenvalue $\lambda_k = \mathrm{e}^{\mathrm{i}\varphi_k}$ we have as many vectors $|\varepsilon_1\rangle$ as the associated eigenspace has dimensions, and as $|s\rangle \in \mathrm{span}(G_1)$, for each of these vectors $|\varepsilon_1\rangle$

$$\langle\varepsilon|s\rangle = \langle\varepsilon_1|G_1^\mathsf{T}|s\rangle, \tag{5.77}$$

$$= \langle\varepsilon_1|u_M\rangle. \tag{5.78}$$

Similarly, as $|u_{nN}\rangle \in \mathrm{span}(G_{1,2})$, we show that

$$\langle\varepsilon|u_{nN}\rangle = \sqrt{\frac{M}{N}}\big(1 - \mathrm{i}\cot\frac{\varphi_k}{2}\big)\langle\varepsilon|s\rangle. \tag{5.79}$$

We denote $s(k,l)$ and $u(k,l)$ the components of the vectors $|s\rangle$ and $|u_{nN}\rangle$ associated with the eigenvalue λ_k, where the parameter l is used to distinguish multiple components corresponding to the same eigenvalue associated with an eigenspace of dimension greater than 1. In most cases, we have

$$s(k,l) = \langle\varepsilon_1|u_M\rangle, \tag{5.80}$$

$$u(k,l) = \sqrt{\frac{M}{N}}\big(1 - \mathrm{i}\cot\frac{\varphi_k}{2}\big)s(k,l). \tag{5.81}$$

There are, however, eigenvalues λ_k for which the matrix $D_{\varphi_k}^{(s)}$ is not defined, as $\widetilde{D}_{\varphi_k}^{-1}$ is not invertible. This happens either when $\lambda_k = \pm 1$ or when λ_k is an eigenvalue of the uniform walk operator U.

Of the two real eigenvalues, only $\lambda_k = -1$ is of interest because $\lambda_k = 1$ is always associated with zero components in $\mathcal{E}$. We then show that in this case

$$s(k,l) = \langle \varepsilon_1 | u_M \rangle, \tag{5.82}$$

with

$$|\varepsilon\rangle = G_1|\varepsilon_1\rangle + FG'_\circ|\varepsilon_\circ\rangle, \tag{5.83}$$

where

$$|\varepsilon_\circ(p)\rangle = -\sqrt{\frac{w}{n-w}}(H_N^{(s)}|\varepsilon_1\rangle)(p), \tag{5.84}$$

and

$$u(k,l) = \langle \varepsilon | u_{nN} \rangle = \sqrt{\frac{M}{N}}\langle \varepsilon | s \rangle. \tag{5.85}$$

To deal with the case where λ_k is an eigenvalue of the operator U, we construct the matrix $\widetilde{D}_\theta^{(\bar{p})}$, a variant of $\widetilde{D}_\theta$ where we replace the undefined coefficients on the diagonal (because we have inverted zero values) by 0. This allows us to determine a new vector $|\varepsilon_1\rangle$, from which we can calculate the associated components of the vectors $|s\rangle$ and $|u_{nN}\rangle$.

In cases where an eigenvalue λ_k is associated with an eigenspace of dimension greater than 1, there is no guarantee that the vectors $|\varepsilon_1\rangle$ are orthogonal. One way to overcome this problem is to form a vector $|s(k)\rangle$ with all the $s(k,l)$ values associated with the eigenvalue λ_k, and apply a correction matrix C. This matrix C is defined differently according to the type of eigenvalue.

5.3.2. Detail of the vector component calculation

Typical case

As shown in equation (5.6), we can calculate the probability of success of the hypercube search algorithm from the eigenvalues of U' and the components of the vectors $|s\rangle$ and $|u_{nN}\rangle$ in the space $\mathcal{E}$.

Each eigenvector is of the form

$$|\varepsilon\rangle = G_1|\varepsilon_1\rangle + G_2|\varepsilon_2\rangle + FG'_\circ|\varepsilon_\circ\rangle, \tag{5.86}$$

therefore, as $|s\rangle \in \text{span}(G_1)$,

$$\langle \varepsilon | s \rangle = \langle \varepsilon_1 | G_1^\mathsf{T} | s \rangle, \tag{5.87}$$

$$= \langle \varepsilon_1 | u_M \rangle. \tag{5.88}$$

Similarly, as $|u_{nN}\rangle \in \mathrm{span}(G_{1,2})$,

$$\langle\varepsilon|u_{nN}\rangle = \langle\varepsilon_1|G_1^{\mathsf{T}}|u_{nN}\rangle + \langle\varepsilon_2|G_2^{\mathsf{T}}|u_{nN}\rangle, \tag{5.89}$$

$$= \sqrt{\frac{M}{N}}\langle\varepsilon_1|u_M\rangle + \langle\varepsilon_+|u_{nN}\rangle, \tag{5.90}$$

and as

$$\langle\varepsilon_+|u_{nN}\rangle = \langle e_+ \otimes u_n|u_N \otimes u_n\rangle, \tag{5.91}$$

$$= \langle e_+|u_N\rangle, \tag{5.92}$$

we have

$$\langle\varepsilon|u_{nN}\rangle = \sqrt{\frac{M}{N}}\langle\varepsilon|s\rangle + \langle e_+|u_N\rangle. \tag{5.93}$$

Recall that, as with any vector, $\langle e_+|u_N\rangle = \langle\tilde{e}_+(0)|$, and thus

$$\langle e_+|u_N\rangle = \langle\tilde{e}_+(0)|, \tag{5.94}$$

$$= -\mathrm{i}\widetilde{D}_{\varphi_k}(0)\langle\tilde{e}_-(0)|, \tag{5.95}$$

$$= -\mathrm{i}\cot\frac{\varphi_k}{2}\langle e_-|u_n\rangle, \tag{5.96}$$

$$= -\mathrm{i}\cot\frac{\varphi_k}{2}\sqrt{\frac{M}{N}}\langle\varepsilon_1|u_M\rangle, \tag{5.97}$$

$$= -\mathrm{i}\cot\frac{\varphi_k}{2}\sqrt{\frac{M}{N}}\langle\varepsilon|s\rangle, \tag{5.98}$$

and the equation 5.93 becomes

$$\langle\varepsilon|u_{nN}\rangle = \sqrt{\frac{M}{N}}\Big(1 - \mathrm{i}\cot\frac{\varphi_k}{2}\Big)\langle\varepsilon|s\rangle. \tag{5.99}$$

We can therefore calculate the components of the vectors $|s\rangle$ and $|u_{nN}\rangle$ in $\mathcal{E}$ for all eigenvalues $\lambda_k = \mathrm{e}^{\mathrm{i}\varphi_k}$, with the exception of real eigenvalues and those associated with singular $\widetilde{D}_{\varphi_k}^{-1}$ matrices, which will be dealt with later. For each vector $|\varepsilon_1\rangle$, we have

$$s'(k,l) = \langle\varepsilon_1|u_M\rangle, \tag{5.100}$$

$$u'(k,l) = \sqrt{\frac{M}{N}}\Big(1 - \mathrm{i}\cot\frac{\varphi_k}{2}\Big)s'(k,l). \tag{5.101}$$

Correction matrices

Here, the notations $s'(k,l)$ and $u'(k,l)$ refer exactly to the components of the vectors $|s\rangle$ and $|u_{nN}\rangle$ in $\mathcal{E}$ only if the vectors $|\varepsilon_1\rangle$ form an orthonormal basis. This is usually the

case, as there is often only one vector $|\varepsilon_1\rangle$ per eigenvalue. If not, these coefficients need to be corrected. To do this, we first define the ξ transformation, identical to that presented in equation (5.59), that is to say

$$\xi(A) = \sum_{w=0}^{n} A^{(w)} H_N^{(s,w)\mathsf{T}} H_N^{(s,w)}, \tag{5.102}$$

where A is a diagonal matrix whose coefficients $A(p, p)$ depend only on $\mathrm{wt}(p)$. Since the vectors $|\tilde{\varepsilon}_+\rangle$ and $|\tilde{\varepsilon}_-\rangle$ are orthogonal, for two vectors $|\tilde{\varepsilon}\rangle$ and $|\tilde{\varepsilon}'\rangle$ we have

$$\langle\tilde{\varepsilon}|\tilde{\varepsilon}'\rangle = \langle\tilde{\varepsilon}_+|\tilde{\varepsilon}'_+\rangle + \langle\tilde{\varepsilon}_-|\tilde{\varepsilon}'_-\rangle, \tag{5.103}$$

and so, for each pair of vectors $|\varepsilon_1\rangle$ and $|\varepsilon'_1\rangle$

$$\begin{aligned}
\langle\tilde{\varepsilon}_+|\tilde{\varepsilon}'_+\rangle &= \langle\tilde{e}_+ \otimes u_n|\tilde{e}'_+ \otimes u_n\rangle, && (5.104)\\
&= \langle e_+|e'_+\rangle, && (5.105)\\
&= \langle e_-|\tilde{D}^2_{\varphi_k}|e'_-\rangle, && (5.106)\\
&= \langle\varepsilon_1|H_N^{(s)\mathsf{T}}\tilde{D}^2_{\varphi_k}H_N^{(s)}|\varepsilon'_1\rangle, && (5.107)\\
&= \langle\varepsilon_1|\xi(\tilde{D}^2_{\varphi_k})|\varepsilon'_1\rangle, && (5.108)
\end{aligned}$$

and

$$\begin{aligned}
\langle\tilde{\varepsilon}_-|\tilde{\varepsilon}'_-\rangle &= \langle\tilde{\varepsilon}_+|\tilde{\Gamma}^{-2}_{\varphi_k}|\tilde{\varepsilon}'_+\rangle, && (5.109)\\
&= \langle\tilde{e}_+ \otimes u_n|\tilde{\Gamma}^{-2}_{\varphi_k}|\tilde{e}'_+ \otimes u_n\rangle, && (5.110)\\
&= \langle e_+|T_{\varphi_k}|e'_+\rangle, && (5.111)\\
&= \langle e_-|\tilde{D}_{\varphi_k}T_{\varphi_k}\tilde{D}_{\varphi_k}|e'_-\rangle, && (5.112)\\
&= \langle\varepsilon_1|H_N^{(s)\mathsf{T}}\tilde{D}_{\varphi_k}T_{\varphi_k}\tilde{D}_{\varphi_k}H_N^{(s)}|\varepsilon'_1\rangle, && (5.113)\\
&= \langle\varepsilon_1|\xi(\tilde{D}^2_{\varphi_k}T_{\varphi_k})|\varepsilon'_1\rangle, && (5.114)
\end{aligned}$$

where T_{φ_k} is a diagonal $N \times N$ matrix such that the coefficient $T_{\varphi_k}(p)$ is the average value of the n coefficients of the p-th block of $\tilde{\Gamma}^{-2}_{\varphi_k}$, that is

$$T_\varphi(p) = \left(1 - \frac{w}{n}\right)\tan^2\frac{\varphi_k}{2} + \frac{w}{n}\cot^2\frac{\varphi_k}{2}. \tag{5.115}$$

We finally have

$$\langle\tilde{\varepsilon}|\tilde{\varepsilon}'\rangle = \langle\varepsilon_1|\xi(\tilde{D}^2_{\varphi_k} + \tilde{D}^2_{\varphi_k}T_{\varphi_k})|\varepsilon'_1\rangle. \tag{5.116}$$

For each eigenvalue λ_k associated with several vectors $|\varepsilon_1\rangle$, we define the matrix C_1 whose columns are these vectors $|\varepsilon_1\rangle$. We can construct the correlation matrix

$$C^\dagger C = C_1^\dagger\xi(\tilde{D}^2_{\varphi_k} + \tilde{D}^2_{\varphi_k}T_{\varphi_k})C_1, \tag{5.117}$$

where each column of C is a vector $|\tilde{\varepsilon}\rangle$ of the eigenspace associated with λ_k. We can diagonalize C as

$$C^\dagger C = V_C \Sigma_C^2 V_C^\dagger, \tag{5.118}$$

where Σ_C^2 is a diagonal matrix containing the eigenvalues of $C^\dagger C$. This gives the SVD of the C matrix.

$$C = U_C \Sigma_C V_C^\dagger. \tag{5.119}$$

We therefore have

$$s'(k,l) = \langle c(l)|s\rangle, \tag{5.120}$$

where $|c(l)\rangle$ denotes the l-th column of C. Since the columns of U_C form an orthonormal basis of the eigenspace associated with the eigenvalue λ_k, we have

$$|s(k)\rangle = U_C|s\rangle, \tag{5.121}$$

where $|s(k)\rangle$ is the vector formed by all $s(k,l)$ coefficients associated with the eigenvalue λ_k. However, U_C is a matrix of size $nN \times \dim(\ker(D_{\varphi_k}^{(s)}))$, and is exponentially large with respect to the dimension of the hypercube. Its calculation can be avoided, however, as we also have

$$|s(k)\rangle = \Sigma_C^{-1} V_C^{-1}|s'(k)\rangle, \tag{5.122}$$

and the matrices Σ_C and V_C are of size $\dim(\ker(D_{\varphi_k}^{(s)})) \times \dim(\ker(D_{\varphi_k}^{(s)}))$. Finally, we calculate the components of $|u_{nN}\rangle$ in $\mathcal{E}$

$$u(k,l) = \sqrt{\frac{M}{N}}\big(1 - \mathrm{i}\cot\frac{\varphi_k}{2}\big)s(k,l). \tag{5.123}$$

Case of real eigenvalues

As explained above, this method of calculating the components $s(k,l)$ and $u(k,l)$ only concerns complex λ_k eigenvalues associated with invertible $\widetilde{D}_{\varphi_k}^{-1}$ matrices. When $\lambda_k = 1$, we must have

$$P_-^S|\varepsilon_+\rangle = 0, \tag{5.124}$$
$$P_+^S|\varepsilon_-\rangle = 0, \tag{5.125}$$

and therefore $|\varepsilon_+\rangle \in E_{+,+}^{S,CO}$ and $|\varepsilon_-\rangle \in E_{-,-}^{S,CO}$. Since $\dim(E_{+,+}^{S,CO}) = 0$, we have $|\varepsilon\rangle \in E_{-,-}^{S,CO}$, and we know that the intersection of $E_{-,-}^{S,CO}$ and $\mathcal{E}$ is of dimension $M-1$. Similarly, if $\lambda_k = -1$, we must have

$$P_+^S|\varepsilon_+\rangle = 0, \tag{5.126}$$
$$P_-^S|\varepsilon_-\rangle = 0, \tag{5.127}$$

and therefore $|\varepsilon_+\rangle \in E_{-,+}^{S,CO}$ and $|\varepsilon_-\rangle \in E_{+,-}^{S,CO}$. Since $\dim(E_{-,+}^{S,CO}) = 0$, we have $|\varepsilon\rangle \in E_{+,-}^{S,CO}$, whose intersection with $\mathcal{E}$ is also of dimension $M-1$. In the following, we will not study the case $\lambda_k = 1$, as it is similar to the case $\lambda_k = -1$ and only concerns zero components of $|s\rangle$ and $|u_{nN}\rangle$ in $\mathcal{E}$. We have

$$|\varepsilon\rangle = G_1|\varepsilon_1\rangle + FG'_\circ|\varepsilon_\circ\rangle, \tag{5.128}$$

with constraint $\langle\varepsilon_1|h\rangle = 0$, $\langle h|$ being the last row of the matrix $H_N^{(s)}$ defined in equation (4.91). We also have

$$|\varepsilon_\circ(p)\rangle = -\sqrt{\frac{w}{n-w}}(H_N^{(s)}|\varepsilon_1\rangle)(p). \tag{5.129}$$

Since the vectors $|u_{nN}\rangle$ and $|s\rangle$ do not belong to $G'_\circ$, we have

$$\langle\varepsilon|s\rangle = \langle\varepsilon_1|G_1^\dagger|s\rangle, \tag{5.130}$$
$$= \langle\varepsilon_1|u_M\rangle, \tag{5.131}$$

and

$$\langle\varepsilon|u_{nN}\rangle = \langle\varepsilon_1|G_1^\dagger|u_{nN}\rangle, \tag{5.132}$$
$$= \sqrt{\frac{M}{N}}\langle\varepsilon_1|u_M\rangle, \tag{5.133}$$
$$= \sqrt{\frac{M}{N}}\langle\varepsilon|s\rangle. \tag{5.134}$$

As was the case previously for complex λ_k eigenvalues, the vectors obtained are not orthogonal and a similar correction must be applied. For two vectors $|\varepsilon\rangle$ and $|\varepsilon'\rangle$, we have

$$\langle\varepsilon|\varepsilon'\rangle = \langle\varepsilon_1|\varepsilon'_1\rangle + \langle\varepsilon_\circ|\varepsilon'_\circ\rangle. \tag{5.135}$$

Let W be the diagonal matrix whose coefficients are $W(p) = w/(n-w)$. We have

$$\langle\varepsilon_\circ|\varepsilon'_\circ\rangle = \langle\varepsilon_1|H_N^{(s)\mathsf{T}}WH_N^{(s)}|\varepsilon'_1\rangle, \tag{5.136}$$
$$= \langle\varepsilon_1|\xi(W)|\varepsilon'_1\rangle. \tag{5.137}$$

The correlation matrix obtained is

$$C^\dagger C = C_1^\dagger\xi(I_N + W)C_1, \tag{5.138}$$

where C_1 is defined in the same way as in the previous case. The method for correcting the components of the vectors $|s\rangle$ and $|u_{nN}\rangle$ in $\mathcal{E}$ is the same as in the case of complex eigenvalues, using the new matrix $C^\dagger C$.

Case of eigenvalues of U

It still remains to deal with the case of angles θ associated with singular $\widetilde{D}_\theta^{-1}$ matrices, that is, matrices containing at least one zero coefficient on their diagonals. According to equation (5.49), this happens when

$$\Big(1-\frac{w}{n}\Big)\tan\frac{\theta}{2}-\frac{w}{n}\cot\frac{\theta}{2}=0, \tag{5.139}$$

for a given Hamming weight w that is,

$$\Big(1-\frac{w}{n}\Big)\tan^2\frac{\theta}{2}=\frac{w}{2}, \tag{5.140}$$

$$\Big(1-\frac{w}{n}\Big)\frac{1-\cos\theta}{1+\cos\theta}=\frac{w}{2}, \tag{5.141}$$

meaning

$$\cos\theta=1-\frac{2w}{n}, \tag{5.142}$$

which corresponds to the case where θ is one of the eigenvalues λ_w of U. In this case, the zero terms on the diagonal of $\widetilde{D}_\theta^{-1}$ are those at positions p such that $\mathrm{wt}(p)=w$, and so we have $\widetilde{D}_\theta^{(w)}=0$. This implies that $|\tilde{e}_-(p)\rangle=0$ at these p positions, and since

$$|\tilde{e}_-\rangle=H_N^{(s)}|\varepsilon_1\rangle, \tag{5.143}$$

we have the new constraint on $|\varepsilon_1\rangle$

$$|\varepsilon_1\rangle\in\ker(H_N^{(s,w)}). \tag{5.144}$$

The matrix $H_N^{(s,w)}$ is large, but for any matrix A, we have

$$\ker(A)=\ker(A^\dagger A), \tag{5.145}$$

and therefore

$$|\varepsilon_1\rangle\in\ker(\Xi_w), \tag{5.146}$$

still with $\Xi_w=H_N^{(s,w)\mathsf{T}}H_N^{(s,w)}$.

We will now define a second constraint. We designate by $\bar{p}$ the positions associated with binary words of Hamming weight different from w, that is $\mathrm{wt}(\bar{p})\neq w$. Equation (5.51) is only valid at these positions $\bar{p}$, so

$$|\tilde{e}_+(\bar{p})\rangle=\mathrm{i}\widetilde{D}_\theta(\bar{p})|\tilde{e}_-(\bar{p})\rangle. \tag{5.147}$$

We define $|\tilde{e}_+^{(\bar{p})}\rangle$ the vector whose elements at positions p are zero and those at $\bar{p}$ positions are defined by the above equation. In the same way, we define the matrix $\widetilde{D}_\theta^{(\bar{p})}$, obtained

by replacing the terms of $\widetilde{D}_\theta$ at the positions p by 0. If we denote $|x\rangle$ the vector of length $\binom{n}{w}$ which contains the non-zero elements of $|\tilde{e}_+\rangle$, which are located at positions p, we have

$$|\tilde{e}_+\rangle = |\tilde{e}_+^{(\bar{p})}\rangle + I_N^{(w)}|x\rangle. \tag{5.148}$$

Since$|\tilde{e}_+\rangle \in \text{span}(H_N^{(\bar{s})})$, its M coefficients corresponding to the solutions are zero, and

$$H_N^{(s)\mathsf{T}}|\tilde{e}_+\rangle = 0, \tag{5.149}$$

and

$$\mathrm{i}H_N^{(s)\mathsf{T}}\widetilde{D}_\theta^{(\bar{p})}|\tilde{e}_-\rangle + H_N^{(s,w)\mathsf{T}}|x\rangle = 0, \tag{5.150}$$

$$\mathrm{i}D_\theta^{(s,\bar{p})}|\varepsilon_1\rangle + H_N^{(s,w)\mathsf{T}}|x\rangle = 0. \tag{5.151}$$

We therefore have the constraint

$$\begin{bmatrix}|\varepsilon_1\rangle\\ |x\rangle\end{bmatrix} \in \ker\left(\mathrm{i}D_\theta^{(s,\bar{p})} +\!\!+ H_N^{(s,w)\mathsf{T}}\right). \tag{5.152}$$

As the matrix $H_N^{(s,w)}$ is large, the calculation of $\ker H_N^{(s,w)\mathsf{T}}$ becomes too complex as the hypercube dimension grows. However, if we define the SVD of $H_N^{(s,w)}$ as

$$H_N^{(s,w)} = U_w \Sigma_w V_w^\dagger, \tag{5.153}$$

we have

$$H_N^{(s,w)\mathsf{T}} = V_w \Sigma_w U_w^\dagger, \tag{5.154}$$

and any vector $|a\rangle$ belonging to $\text{span}\left(H_N^{(s,w)\mathsf{T}}\right)$ can be written as

$$|a\rangle = H_N^{(s,w)\mathsf{T}}|b\rangle, \tag{5.155}$$

$$= V_w \Sigma_w U_w^\dagger |b\rangle, \tag{5.156}$$

$$= V_w \Sigma_w |b_\parallel\rangle, \tag{5.157}$$

where $|b_\parallel\rangle$ denotes the component of $|b\rangle$ in $\text{span}(U_w^\dagger)$. Let $|b_\perp\rangle$ denote the component of $|b\rangle$ orthogonal to $\text{span}(U_w^\dagger)$, such that

$$|b\rangle = U_w|b_\parallel\rangle + |b_\perp\rangle. \tag{5.158}$$

Since $|b_\perp\rangle$ has no impact on $|a\rangle$, it can be considered as zero, and we simply have

$$|b\rangle = U_w|b_\parallel\rangle, \tag{5.159}$$

and thus

$$\mathrm{span}\big(H_N^{(s,w)\mathsf{T}}\big) = \mathrm{span}(V_w \Sigma_w). \tag{5.160}$$

Since

$$\Xi_w = V_w \Sigma_w^2 V_w^\dagger, \tag{5.161}$$

matrices V_w and Σ_w can be calculated from the SVD of Ξ_w.

We define the matrix Y_w whose columns form an orthonormal basis of $\ker(\Xi_w)$. We have

$$|\varepsilon_1\rangle = Y_w |\tilde{\varepsilon_1}\rangle. \tag{5.162}$$

The equation (5.152) thus becomes

$$\begin{bmatrix} |\tilde{\varepsilon_1}\rangle \\ |\dot{x}\rangle \end{bmatrix} \in \ker\big(\mathrm{i}D_\theta^{(s,\bar{p})} Y \mathbin{+\!\!+} V_w \Sigma_w\big), \tag{5.163}$$

where $|\dot{x}\rangle = U_w^\dagger |x\rangle$ is a vector of length $\mathrm{rk}(\Xi_w)$. We then have

$$\begin{aligned}
\langle\tilde{\varepsilon}_+|\tilde{\varepsilon}'_+\rangle &= \langle\tilde{e}_+|\tilde{e}'_+\rangle, && (5.164)\\
&= \langle\tilde{e}_+^{(\bar{p})}|\tilde{e}'^{(\bar{p})}_+\rangle + \langle\dot{x}|\dot{x}'\rangle, && (5.165)\\
&= \langle\tilde{e}_-|\widetilde{D}_\theta^{(s,\bar{p})^2}|\tilde{e}'_-\rangle + \langle\dot{x}|\dot{x}'\rangle, && (5.166)\\
&= \langle\varepsilon_1|\xi\big(\widetilde{D}_\theta^{(s,\bar{p})^2}\big)|\varepsilon'_1\rangle + \langle\dot{x}|\dot{x}'\rangle, && (5.167)
\end{aligned}$$

and,

$$\begin{aligned}
\langle\tilde{\varepsilon}_-|\tilde{\varepsilon}'_-\rangle &= \langle\tilde{\varepsilon}_+|\widetilde{\Gamma}_\theta^{-2}|\tilde{\varepsilon}'_+\rangle, && (5.168)\\
&= \langle\tilde{e}_+ \otimes u_n|\widetilde{\Gamma}_\theta^{-2}|\tilde{e}'_+ \otimes u_n\rangle, && (5.169)\\
&= \langle\tilde{e}_+|W_\theta|\tilde{e}'_+\rangle + \langle\dot{x}|I_N^{(w)\mathsf{T}} W_\theta I_N^{(w)}|\dot{x}'\rangle. && (5.170)
\end{aligned}$$

Since $\cos\theta = 1 - 2w/n$,

$$\begin{aligned}
\tan\frac{\theta}{2} &= \sqrt{\frac{w}{n-w}}, && (5.171)\\
\cot\frac{\theta}{2} &= \sqrt{\frac{n-w}{w}}, && (5.172)\\
& && (5.173)
\end{aligned}$$

we have, at each position p

$$\begin{aligned}
W_\theta(p) &= \frac{n-w}{n}\tan^2\frac{\theta}{2} + \frac{w}{n}\cot^2\frac{\theta}{2}, && (5.174)\\
&= \frac{w}{n} + \frac{n-w}{n}, && (5.175)\\
&= 1, && (5.176)
\end{aligned}$$

and therefore

$$\langle \tilde{\varepsilon}_- | \tilde{\varepsilon}'_- \rangle = \langle \tilde{e}_- | \widetilde{D}_\theta^{(\bar{p})} W_\theta \widetilde{D}_\theta^{(\bar{p})} | \tilde{e}'_- \rangle + \langle \dot{x} | \dot{x}' \rangle, \tag{5.177}$$

$$= \langle \varepsilon_1 | \xi \big(\widetilde{D}_\theta^{(\bar{p})^2} W_\theta \big) | \varepsilon'_1 \rangle + \langle \dot{x} | \dot{x}' \rangle. \tag{5.178}$$

We define $\dot{X}$ as the matrix whose columns are the vectors $|\dot{x}\rangle$. The correlation matrix $E^\dagger E$ is

$$E^\dagger E = E_1^\dagger \xi \big(\widetilde{D}_\theta^{(\bar{p})^2} + \widetilde{D}_\theta^{(\bar{p})^2} W_\theta \big) E_1 + 2 \dot{X}^\dagger \dot{X}. \tag{5.179}$$

The computation method for the $s(k,l)$ and $u(k,l)$ components is identical to that of the standard case, with the new definition of the vector $|\varepsilon_1\rangle$ and the correction matrix C.

5.4. Summary of the probability of success calculation

At iteration t, the probability of success can be calculated from the inner product of the system state vector $|\psi_t\rangle$ and the solution vector $|s\rangle$, as determined by equation (5.3). Calculating the probability of success in this way would take too long, since to obtain $|\psi_t\rangle$, we must first calculate U'^t, knowing that U' is a matrix $n2^n \times n2^n$. However, we showed in the previous chapter that the vectors $|\psi_t\rangle$ and $|s\rangle$ belong to the space of interest $\mathcal{E}$ defined in the previous chapter, whose size is linear in n. We can therefore calculate the same inner product by restricting ourselves to the components of $|u_{nN}\rangle$ and $|s\rangle$ in $\mathcal{E}$. To do this, we also need the eigenvalues $\lambda_k = \mathrm{e}^{\mathrm{i}\varphi_k}$ of U' associated with eigenspaces in $\mathcal{E}$.

The first step is to determine these eigenvalues, which will then enable us to calculate the components of the vectors $|u_{nN}\rangle$ and $|s\rangle$ in the $\mathcal{E}$ space. Although we cannot calculate these eigenvalues directly, we can check whether a term $\mathrm{e}^{\mathrm{i}\theta}$ is an eigenvalue or not, by constructing a specific $D_\theta^{(s)}$ matrix as shown in section 5.1. If this matrix is singular, that is, the dimension of its kernel is non-zero, then $\mathrm{e}^{\mathrm{i}\theta}$ is an eigenvalue. We can quickly calculate the dimension of a matrix kernel using its singular value decomposition, or SVD: if at least one of the singular values of $D_\theta^{(s)}$ is zero, then we've found an eigenvalue of U' in $\mathcal{E}$.

Calculating the $D_\theta^{(s)}$ matrix according to its definition involves matrices of exponential size in n, but it is possible to use the properties of Hadamard matrices to restrict ourselves to matrices Ξ_w of size $M \times M$, where M is the number of solutions to the problem under study. We can therefore find the eigenvalues $\mathrm{e}^{\mathrm{i}\theta}$ for $\theta \in [0, \pi/2]$ by testing enough matrices $D_\theta^{(s)}$. We then deduce by symmetry the eigenvalues associated with values of θ in $]\pi/2, 2\pi[$.

Most of the time, the components of $|u_{nN}\rangle$ and $|s\rangle$ are calculated directly from the eigenvalues, according to the equations (5.100) and (5.101). However, some particular eigenvalues need to be treated differently: those equal to ± 1 and those producing singular $\widetilde{D}_{\varphi_k}^{-1}$ matrices.

In addition, each eigenvalue is associated with one or more vectors $|\varepsilon_1\rangle$, one for each dimension of the corresponding eigenspace. If there are several vectors $|\varepsilon_1\rangle$ for the same eigenvalue, their orthogonality must be ensured, which is done by applying a correction matrix C to the vectors formed by all the $|s\rangle$ components associated with the eigenvalue.

6. Results and perspectives

6.1. Probability of success computation procedure

In this section, we will detail the steps of the procedure with the example of a problem on a hypercube with $n = 8$ dimensions, where the solutions are at positions 3 and 6. We therefore have $M = 2$ and

$$|s\rangle = \frac{1}{\sqrt{2}}(|3\rangle + |6\rangle)|u_8\rangle. \tag{6.1}$$

According to equation (4.185), the dimension of the space of interest $\mathcal{E}$ is exactly 30. The upper bound (4.187) gives us $\dim(\mathcal{E}) \leqslant 30$, which is perfectly consistent. Most of the time, the upper bound of $\dim(\mathcal{E})$ is a little higher than the exact dimension, which means that we will be looking for more eigenvalues than necessary. This poses no problem, since any supernumerary eigenvalues outside the space of interest $\mathcal{E}$ have no influence on the calculation of the probability of success. The important point is that we obtain very few eigenvalues compared with the $n2^n = 2048$ required for the direct calculation using the entirety of the U' operator.

The first step in the calculation is to find the eigenvalues of U' associated with eigenspaces in $\mathcal{E}$. To do this, we create the matrices $D_\theta^{(s)}$ in accordance with section 5.2 for a set of angles in $[0, \pi/2]$. Several strategies of choice of the tested angles θ are possible. One that has given good results is a two-pass search, first over the entire interval $[0, \pi/2]$, then around each local minimum. The eigenvalue search in our example is shown in figure 6.1. To obtain the curve shown in figure 6.1, each of the two passes uses 10 000 values of θ, evenly spaced, which is much more than necessary. Generally, 500 values of θ are enough.

Once the eigenvalues whose phases φ_k are in $[0, \pi/2]$ have been identified, we find those whose phases φ_k are in $]\pi/2, \pi]$ then in $]-\pi, 0[$ by symmetry around $\pi/2$ then 0. By adding the 1 and -1 eigenvalues, we obtain a total of 42 eigenvalues, 12 more than the 30 we were looking for. In figure 6.1, we can see three θ values marked with $\sigma_\theta(\theta)$ values above the others, close to 1, which are "false-positives". After the two symmetries, this corresponds to 12 mistakenly identified eigenvalues. As mentioned above, we can choose to keep these few eigenvalues in later calculations, as they correspond to zero components in $\mathcal{E}$.

As shown in section 5.3, if one of the eigenvalues we are looking for is equal to one of the λ_w or λ_w^* eigenvalues of U, we cannot construct the corresponding $D_\theta^{(s)}$ matrix.

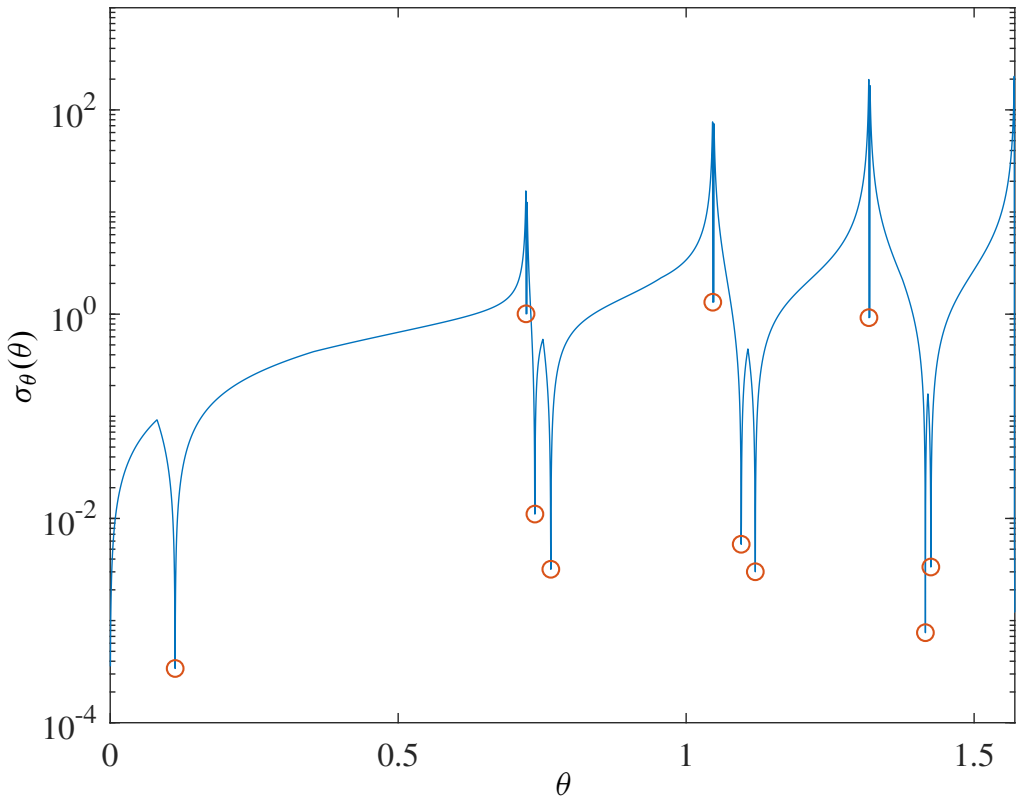

Figure 6.1 Search for the eigenvalues of U' associated with eigenspaces in $\mathcal{E}$ for $\theta \in [0, \pi/2]$. The eigenvalues found are marked by the circles

During the simulations, this case never arose, perhaps because the computational tools at our disposal do not allow us to study high-dimensional cases. As a precaution, we may choose to always include these $2n$ eigenvalues with those found.

Once the 30 eigenvalues have been identified, we calculate the $s(k)$ and $u(k)$ components of the $|s\rangle$ and $|u_{nN}\rangle$ vectors in the space of interest $\mathcal{E}$. Of these 30 eigenvalues, we find that 14 are associated with zero components. This leaves 16 useful eigenvalues, which are presented in table 6.1.

The evolution of the probability of success can then be calculated from equation (5.6). Figure 6.2 shows a comparison between the proposed method and direct simulation using the entire operator U'. Both methods give almost identical results, and the number of iterations that maximizes the probability of success is found to be $R = 12$.

In this example, the maximum probability of success is about 0.4 over the first 50 iterations. We can also find an upper bound on the probability of success. By triangular

Table 6.1 Non-zero components of vectors $|s\rangle$ and $|u\rangle$ in $\mathcal{E}$ with $n = 8$, $M = 2$ solutions at positions 3 and 6.

φ_k	$s(k)$	$u(k)$
0.1127	0.4487	$0.0397 - 0.7033\mathrm{i}$
0.7649	−0.1300	$-0.0115 + 0.0286\mathrm{i}$
1.1200	0.1267	$0.0112 - 0.0179\mathrm{i}$
1.4250	0.1255	$0.0111 - 0.0128\mathrm{i}$
1.7166	−0.1255	$-0.0111 + 0.0096\mathrm{i}$
2.0216	−0.1267	$-0.0112 + 0.0070\mathrm{i}$
2.3766	0.1300	$0.0115 - 0.0046\mathrm{i}$
3.0289	−0.4487	$-0.0397 + 0.0022\mathrm{i}$
−3.0289	−0.4487	$-0.0397 - 0.0022\mathrm{i}$
−2.3766	0.1300	$0.0115 + 0.0046\mathrm{i}$
−2.0216	−0.1267	$-0.0112 - 0.0070\mathrm{i}$
−1.7166	−0.1255	$-0.0111 - 0.0096\mathrm{i}$
−1.4250	0.1255	$0.0111 + 0.0128\mathrm{i}$
−1.1200	0.1267	$0.0112 + 0.0179\mathrm{i}$
−0.7649	−0.1300	$-0.0115 - 0.0286\mathrm{i}$
−0.1127	0.4487	$0.0397 + 0.7033\mathrm{i}$

inequality, we have

$$\mathbf{P}_t(s) = \left|\sum_{k,l} s(k,l)^* \mathrm{e}^{\mathrm{i}\varphi_k t} u(k,l)\right|^2, \tag{6.2}$$

$$\leqslant \left(\sum_{k,l} |s(k,l)^* \mathrm{e}^{\mathrm{i}\varphi_k t} u(k,l)|\right)^2, \tag{6.3}$$

$$\leqslant \left(\sum_{k,l} |s(k,l)||u(k,l)|\right)^2, \tag{6.4}$$

and as from equation (5.123)

$$|u(k,l)| = \sqrt{\frac{M}{N}}\sqrt{1 + \cot^2\frac{\varphi_k}{2}}|s(k,l)|, \tag{6.5}$$

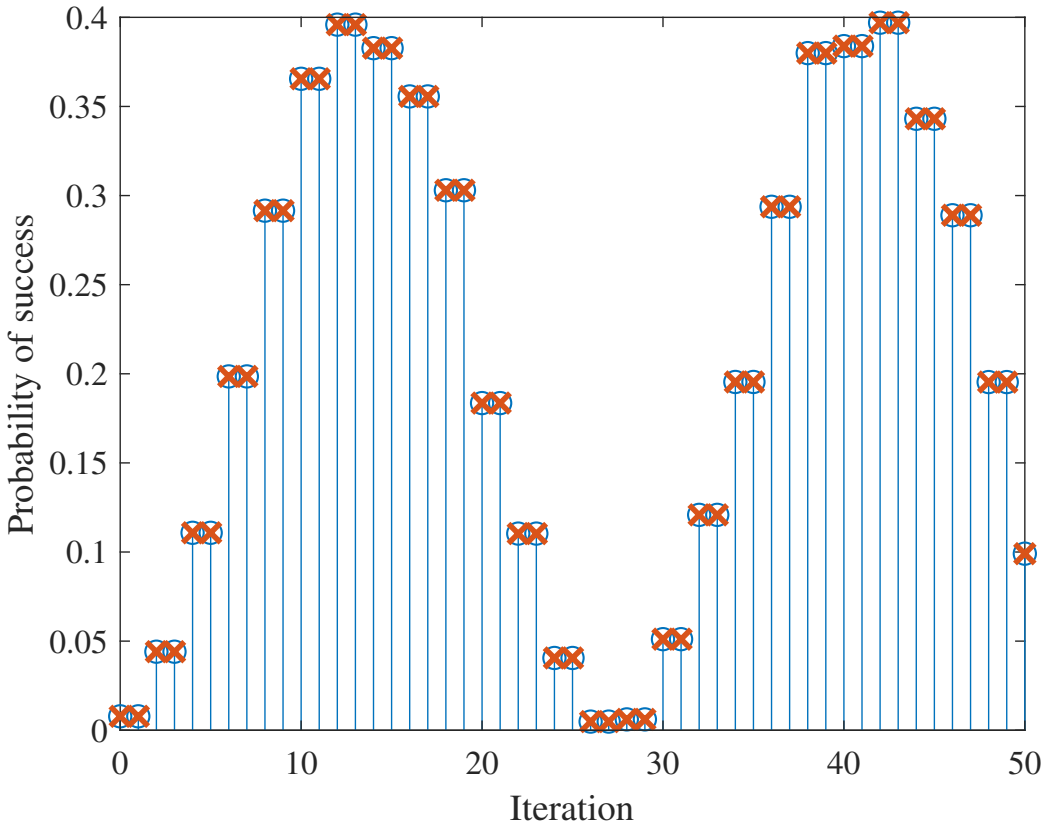

Figure 6.2 Evolution of the probability of success as a function of the number of iterations. Circles correspond to the method proposed in this work, crosses to exact values obtained by direct simulation

we finally have

$$\mathbf{P}_t(s) \leqslant \frac{M}{N}\left(\sum_k \sqrt{1+\cot^2\frac{\varphi_k}{2}}\sum_l |s(k,l)|^2\right)^2. \tag{6.6}$$

In our example, this upper bound is 0.4839, which is an overestimate of around 20 % of the maximum probability of success.

6.2. Improvements and applications

Although the procedure presented produces an excellent approximation of the exact probability of success, there is still room for improvement. Firstly, we need to determine the optimum method for choosing the angles θ to be tested when searching for eigenvalues,

which involves studying how the eigenvalues are distributed according to the problem. Then, the question of the exact complexity of the method could be resolved. It should also be verified that the error between the exact probability and that calculated by the method remains zero, in accordance with theory, as the dimension n of the problem grows.

Practical applications of the method presented are limited by the need to know the solutions in advance before simulating. However, it should be noted that it is sufficient to know the relative positions of the solutions, not the absolute positions. For example, all problems with the same number of bits and two opposite solutions behave in the same way, and we can determine the optimal number of iterations R by testing just one of these problems, chosen arbitrarily. We can therefore deal with families of problems for which we have some prior knowledge of how their solutions are distributed, such as on a face of the hypercube, in a hypersphere of known radius centered on any position, etc.

The proposed method and the algorithm eigenanalysis are mainly of theoretical interest, and provide a slightly more detailed understanding of its functioning. The observation at the root of the method, that the useful part of the algorithm occupies a small subspace of the workspace, could be transposed to other quantum walks, for other algorithms or even other types of graphs, such as planar walks.

It is also planned to study the impact of the number and relative positions of solutions on the probability of success, in order to better understand the phenomenon of "interferences" between solutions related to the graph, which exists neither in classical walks, nor in the original Grover algorithm. Understanding these interferences could help us to understand the globally irregular appearance of the probability of success curve, and thus maximize the probability of success. In particular, in a study prior to this paper, we developed a variant of the hypercube walk search algorithm using a modified oracle. Without going into detail, this version of the algorithm generally gives a much higher probability of success than the original algorithm, at a seemingly low cost in time. Figures 6.3 and 6.4 show a comparison of the two algorithms. However, as it is difficult to simulate realistic cases, with for example a few thousand qubits, with a conventional computer, the proposed eigenanalysis technique could possibly show and quantify the superiority of one of the versions.

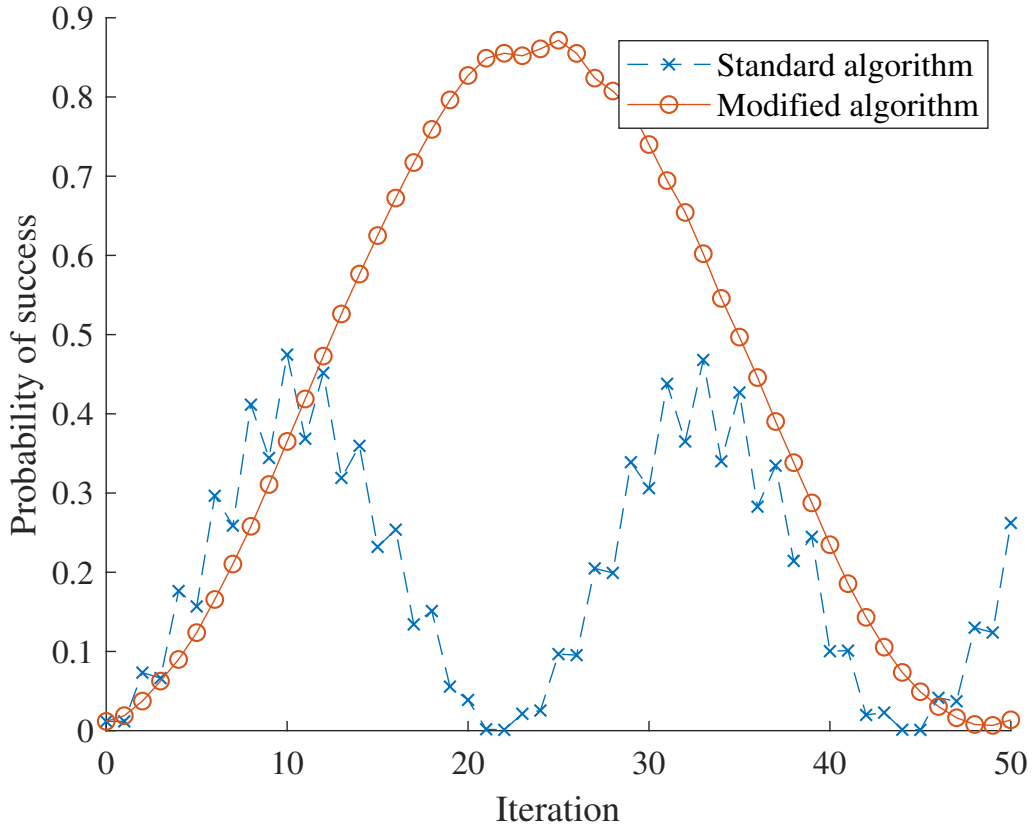

Figure 6.3 Comparison of the original and modified hypercube search algorithms, for $n = 8$, with $M = 3$ solutions, at positions 2, 49, 99

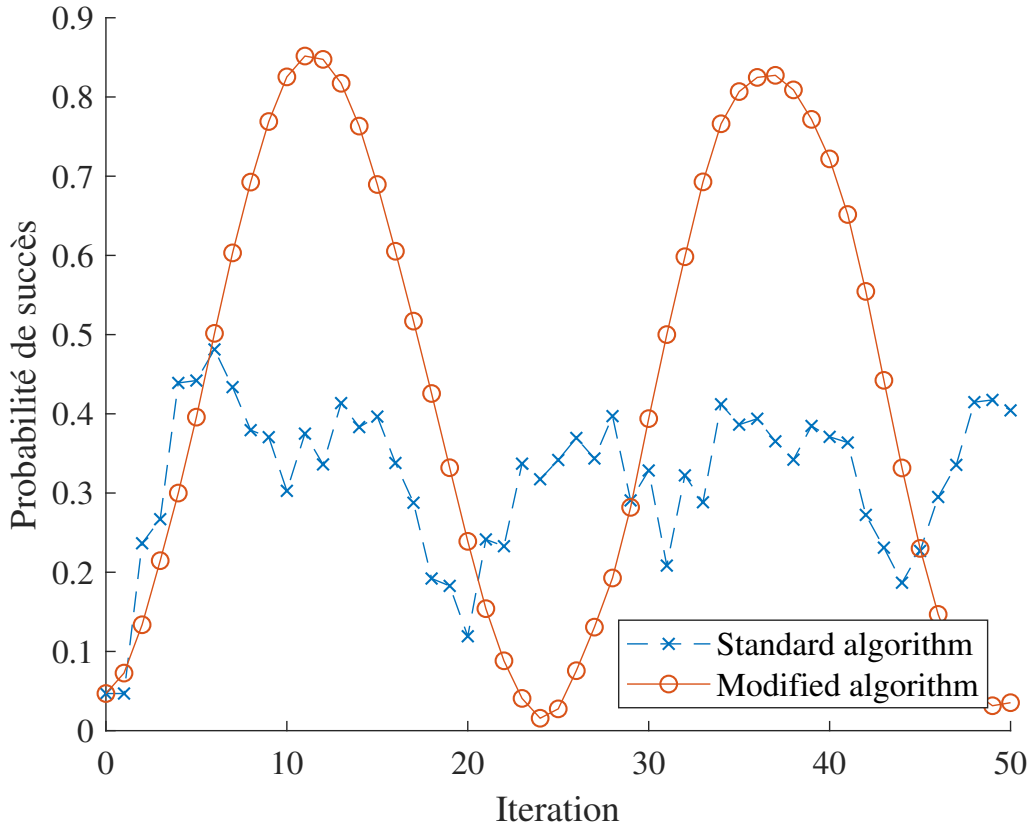

Figure 6.4 Comparison of the original and modified hypercube search algorithms, for $n = 8$, with $M = 12$ solutions, at positions 0, 5, 9, 10, 29, 31, 49, 50, 53, 54, 69, 77

Conclusion

The study of the hypercube quantum walk search algorithm presented in this paper is organized around a simple observation: the algorithm does nothing useful in most of the $\mathcal{H}$ workspace. We therefore began by showing that the useful space $\mathcal{E}$ was of very low dimension (see equation (4.187)), exponentially smaller than that of the workspace. To achieve this result, we carried out a joint eigenanalysis of the three elementary search operators S, C and O in chapter 4, using specially constructed generator matrices and the spatial Fourier transform.

In addition to refining our general understanding of the algorithm, this analysis allows us to show that the initial state of the system $|u_{nN}\rangle$ and the solution state $|s\rangle$ are both part of the space of interest $\mathcal{E}$. This means that at any iteration of the algorithm, the state of the system is completely included in $\mathcal{E}$, and above all, that we can calculate the probability of success of the algorithm from just the few components of the vectors $|u_{nN}\rangle$ and $|s\rangle$ in $\mathcal{E}$. Chapter 5 presents a procedure for calculating the probability of success in polynomial time. This procedure is divided into two phases: finding the eigenvalues of the algorithm operator U' associated with eigenspaces included in $\mathcal{E}$, then calculating the components of the vectors in each eigenspace.

It is not possible to determine analytically the eigenvalues of U' in $\mathcal{E}$, but it is possible to check whether or not a $e^{i\theta}$ term is one of the eigenvalues we are looking for. To do this, we construct matrices $D_\theta^{(s)}$ for a set of values of $\theta \in [0, \pi/2]$. These matrices are small, but are defined from very large matrices. However, in section 5.2, we show that it is possible to exploit the properties of Hadamard matrices to compute efficiently the matrices $D_\theta^{(s)}$. If, for a given value of θ, at least one of the singular values of $D_\theta^{(s)}$ is zero, then $e^{i\theta}$ is one of the eigenvalues we are looking for. By repeating the process with enough values of $\theta \in [0, \pi/2]$, we find all the eigenvalues λ_k located in the upper right quadrant of the complex plane. By symmetry around 0 and $\pi/2$, we deduce the other eigenvalues, to which we add 1 and -1. The $2n$ non-real eigenvalues λ_w and λ_w^* of the uniform walk operator U are potential eigenvalues of U' in $\mathcal{E}$ that do not correspond to a matrix $D_\theta^{(s)}$. For the sake of simplicity, we can choose to include them systematically in the eigenvalues identified. Most of the time, we obtain too many eigenvalues, which is not a problem, as the supernumerary values correspond to zero components in the space of interest $\mathcal{E}$.

Once the eigenvalues have been obtained, all that remains is to calculate the components of the vectors $|u_{nN}\rangle$ and $|s\rangle$. In general, these components can be calculated directly from the equations (5.100) and (5.101). When an eigenvalue is associated with

more than one eigenvector, a correction matrix C defined in section 5.3 must be used. This correction matrix is defined differently for real and λ_w eigenvalues.

All that remains is to calculate the probability of success over the iterations from the equation (5.6). The presented procedure is perfectly equivalent to the direct calculation using the full U' operator, as shown in figure 6.2.

As mentioned in section 6.2, the eigenanalysis of the algorithm that led to the design of the procedure for calculating the probability of success is undoubtedly as interesting a result as the procedure itself. The notion of interest space and the technique of joint eigenspace analysis could be applied to other algorithms or quantum walks on graphs other than the hypercube, to study their behavior, evaluate or compare their performance.

A. Dirac notation

A.1. Definition

Dirac notation, or "bra-ket" notation, is an alternative method for writing quantities of linear algebra using row and column vectors, while avoiding matrices. It is particularly well-suited to the manipulation of vectors containing a very large, or even infinite, number of elements, as seen in quantum physics. Of course, Dirac notation in no way changes the principles of linear algebra. It is based on the use of the brakets"⟨" and "⟩" and the vertical bar "|" to construct "bras" and "kets" (hence the name "bra-ket").

A ket is denoted $|x\rangle$ and mathematically represents a complex vector $\mathbf{x}$ in a Hilbert space V. In quantum information, a ket systematically represents a state vector. If $\mathbf{x} \in \mathbb{C}^n$, it can be written as a column vector.

A bra is denoted by $\langle f|$ and mathematically represents a linear functional, that is $f : V \to \mathbb{C}$. This means that in matrix notation, $\langle x|$ denotes the dual of the vector $\mathbf{x}$, that is, $\langle x| = |x\rangle^\dagger$, where "†" is the Hermitian transpose. If $\mathbf{x} \in \mathbb{C}^n$, we can write it as a row vector whose terms are the complex conjugates of $\mathbf{x}$.

This notation allows us to write the inner product between two vectors $\mathbf{x}$ and $\mathbf{y}$ as $\langle x| \cdot |y\rangle = \langle x|y\rangle$. Consequently, we can express the squared norm of a vector as

$$\|\mathbf{x}\|^2 = \langle x|x\rangle. \tag{A.1}$$

Similarly, we can define an operator which takes the $\mathbf{y}$ component of $\mathbf{x}$ as $|y\rangle\langle x|$. Indeed, we have $|y\rangle\langle x| \cdot |x\rangle = |y\rangle\langle x|x\rangle = \|\mathbf{x}\|^2\mathbf{y}$.

The symbol assigned to a ket or bra is often reused to designate a constant or scalar variable. For example, the spectral decomposition of a normal operator $\widehat{M}$ can be written as

$$\widehat{M} = \sum_m m|m\rangle\langle m|. \tag{A.2}$$

Here, for each eigenvalue m of the operator $\widehat{M}$, we sum the weighted $|m\rangle\langle m|$, where $|m\rangle$ is an eigenvector of $\widehat{M}$.

In quantum information theory, kets are often assigned binary words, such as $|001\rangle$.

A.2. Properties

Bras and kets are objects suitable for linear algebra. Consequently, their manipulation follows the same rules as row and column vectors in $\mathbb{C}^n$.

A linear combination of kets will always result in a ket, and the same applies to bras. For example, if $|x_1\rangle$, $|x_2\rangle$ and $|x\rangle$ are kets, and

$$|y\rangle = c_1|x_1\rangle + c_2|x_1\rangle, \tag{A.3}$$

$$|z\rangle = \int_{-\infty}^{+\infty} f(x)|x\rangle \,\mathrm{d}x, \tag{A.4}$$

with $(c_1, c_2) \in \mathbb{C}^2$ and $f : \mathbb{R} \to \mathbb{C}$, then $|y\rangle$ and $|z\rangle$ are also valid kets.

Since bras are by definition linear functionals, their application to a sum of kets follows the distributive property

$$\langle y|(c_1|x_1\rangle + c_2|x_2\rangle) = c_1\langle y|x_1\rangle + c_2\langle y|x_2\rangle, \tag{A.5}$$

and by duality, the application of a sum of bras to a ket is also distributive, that is

$$(c_1\langle y_1| + c_2\langle y_2|)|x\rangle = c_1\langle y_1|x\rangle + c_2\langle y_2|x\rangle, \tag{A.6}$$

with $(c_1, c_2) \in \mathbb{C}^2$.

Any sequence of multiplication of bras, kets, linear operators and complex scalars can be written without parentheses, as it is an associative operation. For example

$$\langle x|(A|y\rangle) = (\langle x|A)|y\rangle = \langle x|A|y\rangle, \tag{A.7}$$

where A is a linear operator.

The Hermitian transpose, noted "†", is a frequent operation. It is equivalent to transposing and conjugating the terms of a matrix. The rules of Hermitian transpose on bras and kets are as follows:

$$|x\rangle^\dagger = \langle x|, \tag{A.8}$$

$$\langle x|^\dagger = |x\rangle, \tag{A.9}$$

$$(c_1|x_1\rangle + c_2|x_2\rangle)^\dagger = c_1^*\langle x_1| + c_2^*\langle x_2|, \tag{A.10}$$

$$\langle x|y\rangle^\dagger = \langle y|x\rangle, \tag{A.11}$$

$$\langle x|A|y\rangle^\dagger = \langle y|A^\dagger|x\rangle, \tag{A.12}$$

$$(c_1|x_1\rangle\langle y_1| + c_2|x_2\rangle\langle y_2|)^\dagger = c_1^*|y_1\rangle\langle x_1| + c_2^*|y_2\rangle\langle x_2|. \tag{A.13}$$

B. Kronecker tensor product

The tensor product is an operation used to model multilinear mathematical objects in many fields of mathematics and physics. In this paper, we focus on the special case of the Kronecker tensor product. As this is the only tensor product used in this document, it will simply be referred to as a tensor product. This operation makes it possible to represent n-dimensional systems and operations in the form of vectors and matrices, as will be the case for quantum systems. The tensor product between two matrices A and B is denoted by $A \otimes B$. The matrices A and B can be of any or different dimensions.

Let A and B be two matrices of dimensions $m_A \times n_A$ and $m_B \times n_B$ respectively.

$$A = \begin{bmatrix} a_{11} & \cdots & a_{1n_A} \\ \vdots & \ddots & \vdots \\ a_{m_A1} & \cdots & a_{m_An_A} \end{bmatrix}, \; B = \begin{bmatrix} b_{11} & \cdots & b_{1n_B} \\ \vdots & \ddots & \vdots \\ b_{m_B1} & \cdots & b_{m_Bn_B} \end{bmatrix}.$$

The tensor product $A \otimes B$ is defined as

$$A \otimes B = \begin{bmatrix} a_{11}B & \cdots & a_{1n_A}B \\ \vdots & \ddots & \vdots \\ a_{m_A1}B & \cdots & a_{m_An_A}B \end{bmatrix}, \tag{B.1}$$

explicitly

$$\begin{bmatrix} a_{11}b_{11} & \cdots & a_{11}b_{1n_B} & \cdots & a_{1n_A}b_{11} & \cdots & a_{1n_A}b_{1n_B} \\ \vdots & \ddots & \vdots & & \vdots & \ddots & \vdots \\ a_{11}b_{m_B1} & \cdots & a_{11}b_{m_Bn_B} & \cdots & a_{1n_A}b_{m_B1} & \cdots & a_{1n_A}b_{m_Bn_B} \\ \vdots & & \vdots & \ddots & \vdots & & \vdots \\ a_{m_A1}b_{11} & \cdots & a_{m_A1}b_{1n_B} & \cdots & a_{m_An_A}b_{11} & \cdots & a_{m_An_A}b_{1n_B} \\ \vdots & \ddots & \vdots & & \vdots & \ddots & \vdots \\ a_{m_A1}b_{m_B1} & \cdots & a_{m_A1}b_{m_Bn_B} & \cdots & a_{m_An_A}b_{m_B1} & \cdots & a_{m_An_A}b_{m_Bn_B} \end{bmatrix}. \tag{B.2}$$

We can see that the dimensions of the matrix $(A \otimes B)$ are the products of the dimensions of the terms, that is, $m_Am_B \times n_An_B$. We deduce that the tensor product with a scalar is a simple multiplication.

A tensor power can be defined in the same way as a multiplicative power, denoted by

$$A^{\otimes n} = \bigotimes_n A = \underbrace{A \otimes A \otimes A \otimes \cdots \otimes A}_{n \text{ times}}. \tag{B.3}$$

The tensor product is associative, that is

$$(A \otimes B) \otimes C = A \otimes (B \otimes C). \tag{B.4}$$

Moreover, the tensor product is bilinear, that is

$$A \otimes (cB + C) = cA \otimes B + A \otimes C, \tag{B.5}$$

where c is a scalar.

The Kronecker product is not commutative, but we can link $A \otimes B$ and $B \otimes A$ by permutation matrices P and Q (see appendix C):

$$A \otimes B = P(B \otimes A)Q. \tag{B.6}$$

Furthermore, if A and B have the same size, we will have $Q = P^{-1} = P^\intercal$ and therefore

$$A \otimes B = P(B \otimes A)P^\intercal. \tag{B.7}$$

An essential property of the tensor product is its interaction with the matrix product, sometimes called the mixed product:

$$(A \otimes B)(C \otimes D) = AC \otimes BD. \tag{B.8}$$

This is a result that will often come in handy. We can consider $A \otimes B$ to be an object occupying two dimensions, where A occupies the first dimension, and B the second, and similarly for C and D. The matrix product takes place dimension by dimension: AC on the first, BD on the second. From this property, we can deduce the scalar product of tensor products:

$$\langle \vec{a} \otimes \vec{b}, \vec{c} \otimes \vec{d} \rangle = \langle \vec{a}, \vec{c} \rangle \otimes \langle \vec{b}, \vec{d} \rangle = \langle \vec{a}, \vec{c} \rangle \times \langle \vec{b}, \vec{d} \rangle. \tag{B.9}$$

The inverse of a tensor product is the tensor product of inverses, that is

$$(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}. \tag{B.10}$$

Transposition acts in the same way:

$$(A \otimes B)^\intercal = A^\intercal \otimes B^\intercal. \tag{B.11}$$

The trace and rank of a tensor product are the products of the traces and ranks of the product terms, that is

$$\operatorname{tr}(A \otimes B) = \operatorname{tr}(A) \operatorname{tr}(B), \tag{B.12}$$

$$\operatorname{rk}(A \otimes B) = \operatorname{rk}(A) \operatorname{rk}(B). \tag{B.13}$$

C. Permutation matrices

A permutation matrix P is a matrix containing only coefficients equal to 0 or 1, where there is only one 1 per row and column. The columns of a $n \times n$ permutation matrix form the canonical basis of $\mathbb{R}^n$. Consequently, permutation matrices are unitary and therefore compatible with the quantum operations formalism. As the permutation matrices are orthogonal matrices, we have $P^{-1} = P^\intercal$. We can therefore cancel the application of a permutation matrix P with its transpose $P^\intercal$.

Multiplying any matrix A with a permutation matrix P is equivalent to permuting the columns of A if P is on the right, or the rows if P is on the left. For example, let the matrices

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}, \; P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}.$$

We can see that P is indeed a permutation matrix. The matrix products of A and P are

$$AP = \begin{bmatrix} 1 & 3 & 2 \\ 4 & 6 & 5 \\ 7 & 9 & 8 \end{bmatrix}, \; PA = \begin{bmatrix} 1 & 2 & 3 \\ 7 & 8 & 9 \\ 4 & 5 & 6 \end{bmatrix}. \tag{C.1}$$

We can see that AP is identical to the matrix A with columns 2 and 3 inverted. The same applies to PA, but now with the rows.

In this document, we define special permutation matrices $P_{a,b}$ of size $ab \times ab$ to interact with tensor products. For example, the matrix $P_{2,3}$ is a 6×6 matrix created as follows:

1. We place the integers from 1 to ab (here 6) in a $a \times b$ matrix (here 2×3), row by row then column by column:
$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}.$$

2. Next, we read this matrix column by column and then row by row. The result is 1, 4, 2, 5, 3, 6.

3. In the k-th column of the matrix $P_{a,b}$, we place the coefficient 1 in the row

indicated by the k-th integer of the sequence obtained. We then have

$$P_{2,3} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}. \tag{C.2}$$

Note that $P_{a,b}^{\mathsf{T}} = P_{b,a}$. This is the matrix referred to in equation (B.7). It reverses the order of the tensor product. If A and B are matrices of sizes $a \times a$ and $b \times b$ respectively, we have

$$A \otimes B = P_{a,b} \, (B \otimes A) \, P_{b,a}. \tag{C.3}$$

This property allows us to swap the order of quantum walk workspaces to obtain operators that are easier to study, notably in section 2.2.

D. SAT problem

The Boolean satisfiability problem, or SAT, is a central logic problem in theoretical computer science. It consists in determining whether or not there exists, for a given logical formula, at least one n-tuple of variables that induces this formula to be true. This set of variables is said to "satisfy" the proposition. For example, the formula

$$v_1 \wedge v_2 \wedge \neg v_3 \tag{D.1}$$

is satisfiable, as it is true for v_1 true, v_2 true and v_3 false. In contrast, the formula

$$v_1 \wedge \neg v_1 \tag{D.2}$$

is always false, and therefore unsatisfiable.

When manipulating more complex formulas, we use De Morgan's laws to represent formulas in "conjunctive normal form", that is, as the conjunction (concatenation of ANDs) of "clauses". Clauses are themselves disjunctions (OR concatenations) of literals. Literals are either variables or variable negations. If we note the literals l_i, a clause is of the form

$$\bigvee_{i=1}^{n} l_i = l_1 \vee l_2 \vee \ldots \vee l_n. \tag{D.3}$$

For example, the formula

$$(\neg(x_1 \vee x_2) \vee (x_3 \wedge x_4)) \wedge (\neg x_1 \vee x_2) \tag{D.4}$$

becomes, in conjunctive normal form

$$(\neg x_1 \vee x_3) \wedge (\neg x_1 \vee x_4) \wedge (\neg x_2 \vee x_3) \wedge (\neg x_2 \vee x_4) \wedge (\neg x_1 \vee x_2), \tag{D.5}$$

where $(\neg x_1 \vee x_3)$, $(\neg x_1 \vee x_4)$, $(\neg x_2 \vee x_3)$, $(\neg x_2 \vee x_4)$ and $(\neg x_1 \vee x_2)$ are the clauses, whose literals are $\neg x_1$, x_2, $\neg x_2$, x_3 and x_4.

It is possible that by switching to the conjunctive normal form, a logical formula becomes exponentially longer. A typical case is the formula

$$\bigvee_{i=1}^{n} (x_i \wedge y_i) = (x_1 \wedge y_1) \vee (x_2 \wedge y_2) \vee \ldots \vee (x_n \wedge y_n), \tag{D.6}$$

which becomes

$$(x_1 \vee x_2 \vee \ldots \vee x_n) \wedge (y_1 \vee x_2 \vee \ldots \vee x_n) \wedge (x_1 \vee y_2 \vee \ldots \vee x_n) \wedge (y_1 \vee y_2 \vee \ldots \vee x_n) \wedge \ldots \wedge (x_1 \vee x_2 \vee \ldots \vee y_n) \wedge (y_1 \vee x_2 \vee \ldots \vee y_n) \wedge (x_1 \vee y_2 \vee \ldots \vee y_n) \wedge (y_1 \vee y_2 \vee \ldots \vee y_n). \tag{D.7}$$

In conjunctive normal form, this formula contains n literals per clause. Deciding on its satisfiability is therefore an n-SAT problem.

The SAT problem is of paramount importance in algorithmics, because according to Cook's theorem [Coo71] it is NP-complete (except 2-SAT, which is solvable in polynomial time), which means that all NP problems can be reduced to SAT, and even to 3-SAT [Kar72], in polynomial time. We then prove that many algorithms are NP-complete by reducing them to SAT or 3-SAT, such as the Hamiltonian cycle problem, the traveling salesman problem, the graph coloring problem and the knapsack problem.

E. Singular value decomposition

Singular value decomposition, or SVD, is a matrix factorization tool. It is quite similar to the eigenvalue and eigenvector decomposition, which it generalizes to rectangular matrices. For any $m \times n$ matrix M with complex coefficients, we can write the decomposition

$$M = U \Sigma V^\dagger, \tag{E.1}$$

where U is a unitary $m \times m$ matrix, V a unitary $n \times n$ matrix and Σ a diagonal $m \times n$ matrix containing only non-negative real values.

The terms on the diagonal of Σ are the singular values of M. They are denoted σ_i, for i from 1 to $\min(m, n)$. By convention, the singular values are arranged in descending order, and the columns of the matrices U and V are ordered appropriately.

We can prove that the SVD of a matrix always exists. Let M be a $m \times n$ complex matrix. The matrix $M^\dagger M$ is positive semidefinite and thus Hermitian. It can therefore be diagonalized by a unitary matrix V of size $n \times n$ such that

$$V^\dagger M^\dagger M V = \begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix}, \tag{E.2}$$

where D is a diagonal matrix containing $\min(m, n)$ strictly positive real values. We can then decompose V into two parts V_1 of size $n \times \min(m, n)$ and V_2 of size $n \times (n - \min(m, n))$ such that

$$\begin{bmatrix} V_1^\dagger \\ V_2^\dagger \end{bmatrix} M^\dagger M \begin{bmatrix} V_1 & V_2 \end{bmatrix} = \begin{bmatrix} V_1^\dagger M^\dagger M V_1 & V_1^\dagger M^\dagger M V_2 \\ V_2^\dagger M^\dagger M V_1 & V_2^\dagger M^\dagger M V_2 \end{bmatrix} = \begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix}, \tag{E.3}$$

that is

$$V_1^\dagger M^\dagger M V_1 = D, \tag{E.4}$$

$$M V_2 = 0. \tag{E.5}$$

We can then define the matrix $U_1^\dagger = D^{-1/2} V_1^\dagger M^\dagger$, such that

$$U_1^\dagger M V_1 = D^{1/2}. \tag{E.6}$$

We can then find a matrix $U_2^\dagger$ such that $U = \begin{bmatrix} U_1 & U_2 \end{bmatrix}$ is unitary. In the end, we have

$$\begin{bmatrix} U_1^\dagger \\ U_2^\dagger \end{bmatrix} M \begin{bmatrix} V_1 & V_2 \end{bmatrix} = U^\dagger M V = \begin{bmatrix} D^{1/2} & 0 \\ 0 & 0 \end{bmatrix}, \tag{E.7}$$

and we find the expression for SVD

$$M = U \begin{bmatrix} D^{1/2} & 0 \\ 0 & 0 \end{bmatrix} V^\dagger. \tag{E.8}$$

We can see that

$$\Sigma = \begin{bmatrix} D^{1/2} & 0 \\ 0 & 0 \end{bmatrix}, \tag{E.9}$$

which implies that the non-zero singular values of M are the square roots of the non-zero eigenvalues of $M^\dagger M$.

In this work, we use a variant of SVD, labelled "fine", which consists in calculating only the first n columns of U, thus saving time when $m > n$. If $m < n$, the calculation can be performed on the transposed matrix. The fine SVD can be expressed as

$$M = U_n \Sigma_n V^\dagger, \tag{E.10}$$

where U_n is of size $m \times n$ and Σ_n is of size $n \times n$. The M and V matrices are unchanged and all non-zero singular values are preserved.

Among the many properties of SVD, the one that will be used in this paper is the determination of the dimension of the kernel of a matrix. As a reminder, the kernel $\ker(M)$ of a matrix M is the set of vectors $\mathbf{v}$ such that $M\mathbf{v} = 0$. The dimension of the kernel of M is equal to the number of zero eigenvalues, that is

$$\dim(\ker(M)) = \#(i \in [0, \min(m,n)] \mid \sigma_i = 0). \tag{E.11}$$

There are algorithms capable of calculating the SVD in polynomial time. According to Golub and Van Loan [GL13], the R-SVD algorithm can perform this task with complexity $\mathcal{O}(n^3 + nm^2)$. It is also possible to restrict the calculation to singular values, in which case the operation can be performed with complexity $\mathcal{O}(mn^2)$ by the Golub-Reinsch SVD algorithm.

Example of singular value decomposition

Let the matrix

$$M = \sqrt{2} \begin{bmatrix} 1 & 2 \\ -1 & 2 \\ 0 & 1 \end{bmatrix}. \tag{E.12}$$

Its decomposition into singular values is

$$M = U\Sigma V^\dagger, \tag{E.13}$$

$$= \begin{bmatrix} -2/3 & -\sqrt{2} & -\sqrt{2}/6 \\ -2/3 & \sqrt{2} & -\sqrt{2}/6 \\ -1/3 & 0 & 2\sqrt{2}/3 \end{bmatrix} \begin{bmatrix} 3\sqrt{2} & 0 \\ 0 & 2 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}, \tag{E.14}$$

and its fine decomposition is

$$M = U_n \Sigma_n V^\dagger, \tag{E.15}$$

$$= \begin{bmatrix} -2/3 & -\sqrt{2} \\ -2/3 & \sqrt{2} \\ -1/3 & 0 \end{bmatrix} \begin{bmatrix} 3\sqrt{2} & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}. \tag{E.16}$$

Bibliography

[AAMP20] F. Acasiete, F. P. Agostini, J. Khatibi Moqadam, and R. Portugal. Implementation of quantum walks on IBM quantum computers. *Quantum Information Processing*, 19(12):426, November 2020.

[ADZ93] Y. Aharonov, L. Davidovich, and N. Zagury. Quantum random walks. *Physical Review A*, 48(2):1687–1690, August 1993. Publisher: American Physical Society.

[Asp76] Alain Aspect. Proposed experiment to test the nonseparability of quantum mechanics. *Physical Review D*, 14(8):1944–1951, October 1976. Publisher: American Physical Society.

[BB14] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11, December 2014.

[Ben80] Paul Benioff. The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. *Journal of Statistical Physics*, 22(5):563–591, May 1980.

[Ber10] Daniel J. Bernstein. Grover vs. McEliece. In Nicolas Sendrier, editor, *Post-Quantum Cryptography*, Lecture Notes in Computer Science, pages 73–80, Berlin, Heidelberg, 2010. Springer.

[BHT98] Gilles Brassard, Peter Høyer, and Alain Tapp. Quantum counting. In Kim G. Larsen, Sven Skyum, and Glynn Winskel, editors, *Automata, Languages and Programming*, Lecture Notes in Computer Science, pages 820–831, Berlin, Heidelberg, 1998. Springer.

[CG04] Andrew M. Childs and Jeffrey Goldstone. Spatial search by quantum walk. *Phys. Rev. A*, 70(2):022314, August 2004. Publisher: American Physical Society.

[Coo71] Stephen A. Cook. The complexity of theorem-proving procedures. In *Proceedings of the third annual ACM symposium on Theory of computing*, STOC '71, pages 151–158, New York, NY, USA, May 1971. Association for Computing Machinery.

[Cro18] Andrew Cross. The IBM Q experience and QISKit open-source quantum computing software. 2018:L58.003, January 2018. Conference Name: APS March Meeting Abstracts ADS Bibcode: 2018APS..MARL58003C.

[DFK91] Martin Dyer, Alan Frieze, and Ravi Kannan. A random polynomial-time algorithm for approximating the volume of convex bodies. *Journal of the ACM*, 38(1):1–17, January 1991.

[Dir35] P. A. M. Dirac. *The Principles of Quantum Mechanics, Second Edition*. Oxford University Press, oxford at the clarendon press; 2nd edition edition, January 1935.

[DRKB02] W. Dür, R. Raussendorf, V. M. Kendon, and H.-J. Briegel. Quantum walks in optical lattices. *Physical Review A*, 66(5):052319, November 2002. Publisher: American Physical Society.

[Fey82] Richard P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6):467–488, June 1982.

[GL13] Gene H. Golub and Charles F. Van Loan. *Matrix Computations*. JHU Press, February 2013.

[Gro96] Lov K. Grover. A fast quantum mechanical algorithm for database search, November 1996. arXiv:quant-ph/9605043.

[GS22] Walther Gerlach and Otto Stern. Der experimentelle Nachweis der Richtungsquantelung im Magnetfeld. *Zeitschrift für Physik*, 9(1):349–352, December 1922.

[JSV04] Mark Jerrum, Alistair Sinclair, and Eric Vigoda. A polynomial-time approximation algorithm for the permanent of a matrix with nonnegative entries. *Journal of the ACM*, 51(4):671–697, July 2004.

[Kar72] Richard M. Karp. Reducibility among Combinatorial Problems. In Raymond E. Miller, James W. Thatcher, and Jean D. Bohlinger, editors, *Complexity of Computer Computations: Proceedings of a symposium on the Complexity of Computer Computations, held March 20–22, 1972, at the IBM Thomas J. Watson Research Center, Yorktown Heights, New York, and sponsored by the Office of Naval Research, Mathematics Program, IBM World Trade Corporation, and the IBM Research Mathematical Sciences Department*, The IBM Research Symposia Series, pages 85–103. Springer US, Boston, MA, 1972.

[Kem05] Julia Kempe. Discrete Quantum Walks Hit Exponentially Faster. *Probab. Theory Relat. Fields*, 133(2):215–235, October 2005.

[MR02] Cristopher Moore and Alexander Russell. Quantum Walks on the Hypercube. In José D. P. Rolim and Salil Vadhan, editors, *Randomization and Approximation Techniques in Computer Science*, Lecture Notes in Computer Science, pages 164–178, Berlin, Heidelberg, 2002. Springer.

[MW19] S. Marsh and J. B. Wang. A quantum walk-assisted approximate algorithm for bounded NP optimisation problems. *Quantum Inf Process*, 18(3):61, January 2019.

[MW20] S. Marsh and J. B. Wang. Combinatorial optimization via highly efficient quantum walks. *Phys. Rev. Res.*, 2(2):023302, June 2020. Publisher: American Physical Society.

[MW21] S. Marsh and J. B. Wang. Deterministic spatial search using alternating quantum walks. *Phys. Rev. A*, 104(2):022216, August 2021. Publisher: American Physical Society.

[MW22] Edric Matwiejew and Jingbo Wang. QuOp_mpi: A framework for parallel simulation of quantum variational algorithms. *Journal of Computational Science*, 62:101711, May 2022.

[NC10] Michael A. Nielsen and Isaac L. Chuang. Quantum Computation and Quantum Information: 10th Anniversary Edition, December 2010. ISBN: 9780511976667 Publisher: Cambridge University Press.

[NV00] Ashwin Nayak and Ashvin Vishwanath. Quantum Walk on the Line, October 2000. arXiv:quant-ph/0010117.

[PBB+23] Hugo Pillin, Gilles Burel, Paul Baird, El-Houssain Baghious, and Roland Gautier. Hypercube quantum search: exact computation of the probability of success in polynomial time. *Quantum Information Processing*, 22(3):149, March 2023.

[QMW+22] Dengke Qu, Samuel Marsh, Kunkun Wang, Lei Xiao, Jingbo Wang, and Peng Xue. Deterministic Search on Star Graphs via Quantum Walks. *Phys. Rev. Lett.*, 128(5):050501, February 2022. Publisher: American Physical Society.

[QWX+21] Xiaogang Qiang, Yizhi Wang, Shichuan Xue, Renyou Ge, Lifeng Chen, Yingwen Liu, Anqi Huang, Xiang Fu, Ping Xu, Teng Yi, Fufang Xu, Mingtang Deng, Jingbo B. Wang, Jasmin D. A. Meinecke, Jonathan C. F.

Matthews, Xinlun Cai, Xuejun Yang, and Junjie Wu. Implementing graph-theoretic quantum algorithms on a silicon photonic quantum walk processor. *Science Advances*, 7(9):eabb8375, February 2021. Publisher: American Association for the Advancement of Science.

[Sch95] Benjamin Schumacher. Quantum coding. *Physical Review A*, 51(4):2738–2747, April 1995. Publisher: American Physical Society.

[Sch99] T. Schoning. A probabilistic algorithm for k-SAT and constraint satisfaction problems. In *40th Annual Symposium on Foundations of Computer Science (Cat. No.99CB37039)*, pages 410–414, October 1999. ISSN: 0272-5428.

[Sho94] P.W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, November 1994.

[SKW03] Neil Shenvi, Julia Kempe, and K. Birgitta Whaley. Quantum random-walk search algorithm. *Physical Review A*, 67(5):052307, May 2003. Publisher: American Physical Society.

[SMMW21] N. Slate, E. Matwiejew, S. Marsh, and J. B. Wang. Quantum walk-based portfolio optimisation. *Quantum*, 5:513, July 2021. Publisher: Verein zur Förderung des Open Access Publizierens in den Quantenwissenschaften.

[TM02] B. C. Travaglione and G. J. Milburn. Implementing the quantum random walk. *Physical Review A*, 65(3):032310, February 2002. Publisher: American Physical Society.

[Tur37] A. M. Turing. On Computable Numbers, with an Application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society*, s2-42(1):230–265, 1937. _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1112/plms/s2-42.1.230.

COLLEGE MATHSTIC
DOCTORAL BRETAGNE
BRETAGNE OCEANE

Université de Bretagne Occidentale

Titre : Algorithme de recherche par marche quantique sur hypercube — Analyse propre et calcul de la probabilité de succès en temps polynomial

Mots clés : Algorithme quantique, algorithme de Grover, marche quantique, probabilité de succès, calcul en temps polynomial

Résumé : Les algorithmes de marche quantique à temps discret sont les analogues directs des algorithmes de marche aléatoire classiques, une famille importante en informatique. Ils peuvent résoudre une variété de problèmes, dont le problème NP-complet SAT, en un temps relativement court. Ainsi, l'étude des marches quantiques pourrait amener à la conception de nouveaux algorithmes quantiques. Parmi les algorithmes quantiques, l'un des plus étudiés est l'algorithme de recherche de Grover, un processus itératif qui peut trouver un élément parmi N qui répond à un certain critère, avec un gain de temps quadratique par rapport à n'importe quel algorithme classique. Dans cette thèse, on étudie la variante de l'algorithme de recherche de Grover proposée par Shenvi, Kempe et Whaley, basée sur les marches sur les graphes hypercubes. Comme les algorithmes de recherche sont des processus itératifs, il faut calculer le nombre correct d'étapes R avant de lancer la recherche, car la probabilité de succès diminue au-delà d'un certain point. La valeur de R dépend du nombre d'éléments N, mais aussi du nombre de solutions M. Pour l'algorithme de Grover, le nombre optimal d'itérations est bien connu, mais ce n'est pas le cas pour la recherche sur l'hypercube dès qu'il y a plusieurs solutions. Dans cette thèse, on propose une analyse propre exhaustive de l'algorithme de recherche sur l'hypercube, qui conduit à une procédure permettant de calculer la probabilité de succès de l'algorithme de recherche sur l'hypercube sans l'exécuter, en temps polynomial.

Title : Quantum walk search algorithm on hypercube — Eigenanalysis and calculation of the probability of success in polynomial time

Keywords : Quantum algorithm, Grover's algorithm, quantum walk, probability of success, computation in polynomial time

Abstract : Discrete time quantum walk algorithms are the direct analogs of classical random walk algorithms, an important family in theoretical informatics. They can solve a variety of problems, in particular the NPcomplete SAT problem, in a relatively short time. Thus, the study of quantum walks could lead to the conception of new quantum algorithms. Among the quantum algorithms, one of the most extensively studied is Grover's search algorithm, an iterative process that can find one element among *N* that meet a certain criterion, with a quadratic time gain over any classical algorithm. In this thesis, we study the variant of Grover's search algorithm proposed by Shenvi, Kempe and Whaley, based on walks on hypercube graphs. As search algorithms are iterative processes, one has to compute the correct number of steps R before running the search, as the probability of success decreases past a certain point. The value of R depends on the number of elements N, but also the number of solutions M. For Grover's algorithm, the optimal number of iterations is well known, but this is not the case for the search on the hypercube as soon as there are multiple solutions. In this thesis, we propose an extensive eigenanalysis of the hypercube search algorithm, which leads to a procedure that allows us to compute the probability of success of the search algorithm on the hypercube without running it, in polynomial time.