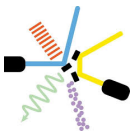
Grover's Algorithm and the Blocks That Count π

Teaching notes (work in progress)

Jovan Markov



Physics 2 Autumn Seminar
Petnica Science Center
November 4, 2026

Contents

Preface **4**

How to Use These Notes **5**
Organization . . . 5
Colors and Notation . . . 5
Prerequisites . . . 5

Introduction **6**

1. **Blocks That Count π** **7**
1.1 The Problem . . . 7
1.2 How to Begin . . . 7
1.3 Conservation Laws and the Collision Equations . . . 8
1.4 The First Few Collisions . . . 9
1.5 The Velocity Plane: An Ellipse . . . 11
1.6 From an Ellipse to a Circle . . . 11
1.7 The Line of Constant Momentum . . . 12
1.8 When the Collisions Stop . . . 13
1.9 From Collisions to a Geometric Problem . . . 14
1.10 Equal Arcs . . . 15
1.11 How Many Arcs Fit Around the Circle? . . . 16
1.12 The Digits of π . . . 19
1.13 Exercises . . . 23

2. **Foundations of Quantum Mechanics and Quantum Computing** **25**
2.1 A Quantum State as a Vector . . . 25
2.2 Superposition and Amplitudes . . . 26
2.3 Measurement and Probabilities . . . 26
2.4 Multiple Qubits . . . 28
2.5 Operators and Unitarity . . . 28
2.6 Quantum Circuits and the X and H Gates . . . 29
2.7 Hadamard Gates on Multiple Qubits . . . 30
2.8 Controlled Quantum Gates: CNOT and CZ . . . 31
2.9 Inner Products, Bras and Projectors . . . 32
2.10 Exercises . . . 35

3. **Grover's Algorithm** **38**
3.1 What Is Quantum Search? . . . 38
3.2 How Many Checks Are Needed? . . . 38
3.3 Algorithmic Complexity . . . 39
3.4 Formulating the Search Problem . . . 40
3.5 What Does the Oracle Know? . . . 40
3.6 Why Does the Oracle Change a Sign? . . . 41
3.7 Why the Oracle Alone Is Not Enough . . . 42
3.8 The Oracle's Action on the Initial State . . . 46
3.9 The Oracle as a Reflection . . . 47
3.10 Diffusion: Reflection about the $|s\rangle$ Axis . . . 49
3.11 Two Reflections Make a Rotation . . . 51
3.12 Why Are Two Dimensions Enough? . . . 53
3.13 How Many Grover Steps Are Needed? . . . 54
3.14 Amplitude Amplification . . . 56
3.15 Grover Search and Classical Unstructured Search . . . 56
3.16 The Quantum Circuit for Grover's Algorithm . . . 57
3.17 Two Qubits, Step by Step . . . 59

3.18 Exercises 61

4. **Two Problems, the Same Geometry** **63**
4.1 The Setup: From Many Balls to Two Blocks 63
4.2 A Shared Plane of States 63
4.3 Collisions as Reflections 64
4.4 Comparing the Mechanical System with Grover's Algorithm 65
4.5 Why Do the Step Counts Differ? 65
4.6 Example: Success on the First Try 66
4.7 Exercises 68

Appendix A. **Counting Collisions with a Ray of Light** **70**

Appendix B. **Radians, Small Angles and the Inscribed-Angle Theorem** **72**

Glossary **74**

Symbols **77**

Further Reading and Viewing **79**

References **79**

Final Answers to the Exercises **80**

Preface

These notes were prepared to accompany a lecture on Grover's algorithm, given at the Physics 2 autumn seminar at Petnica Science Center on November 4, 2026. They are intended primarily for high-school students who would like to learn the basic ideas of quantum computing. They are also written to support independent study.

The starting point of the lecture is that a quantum algorithm can be understood using mathematics familiar from classical mechanics and geometry. We will gradually build a geometric description of Grover's algorithm and show how it connects to an apparently very different problem: the elastic collisions of two blocks.

Our approach draws on the mathematical connection demonstrated by Adam Brown, as well as earlier work on the geometry of collisions and quantum search. These notes aim not only to give the final formulas, but also to explain how they are obtained. New concepts are therefore introduced gradually, and each step in the mathematical derivations is explained.

How to Use These Notes

Organization

In the first chapter, we solve the two-block puzzle. Starting from conservation of energy and momentum, we show why the number of collisions reveals digits of π.

In the second chapter, we introduce the quantum-mechanical and quantum-computing concepts we need: quantum states, superposition, measurement, qubits, operators and quantum circuits. Vectors and geometry will help us explain these new ideas.

In the third chapter, we study Grover's algorithm. We formulate the search problem, explain the actions of the oracle and diffusion, derive the number of steps required and present the corresponding quantum circuit.

The fourth chapter brings the first three together. Drawing on Brown's work, we show how collisions between blocks and Grover's algorithm can be described by the same geometry of reflections and rotations.

Exercises for independent work appear at the end of each chapter, ranging from introductory problems to more challenging ones. Some include brief hints. We leave certain proofs as exercises and refer to them at the appropriate points in the text—for example, "see Exercise 63." Final answers to all exercises, without worked solutions, are provided at the end so that you can check your results.

After the chapters come two appendices with supplementary derivations, a glossary, a list of symbols, suggestions for further reading and viewing, and a bibliography.

Colors and Notation

To make the connection between mechanics and quantum computing easier to follow, we use the same colors for the same concepts throughout the text, both in figures and in formulas.

- **Orange** denotes the small block (m, v, y) and, in Grover's algorithm, the sought element w.
- **Blue** denotes the large block (M, V, x) and the unmarked elements.
- **Red** represents a bounce off the wall or the action of the oracle.
- **Green** represents a collision between the two blocks or the diffusion operation.
- **Purple** denotes the angle $\bar{\theta}$ and the corresponding arcs $2\bar{\theta}$.
- **Gray** is used for auxiliary lines and the region in which no further collisions occur.
- **Gold** denotes the outcome of Grover's algorithm.

Prerequisites

To follow the lecture, a basic familiarity with vectors in a plane, right-triangle trigonometry, probability and mechanics—especially kinetic energy and momentum—is sufficient. No prior knowledge of quantum mechanics is required: we will introduce the necessary concepts as we go.

Introduction

This lecture connects two stories that at first seem entirely unrelated.

The first concerns two blocks sliding on a frictionless surface. The small block is at rest between a wall and a large block approaching it. All collisions are perfectly elastic, including the small block's bounces off the wall. If the large block has 100 times the mass of the small block, there will be 31 collisions. If it is 10,000 times as massive, there will be 314 collisions; if it is a million times as massive, there will be 3,141. These numbers are not random: they contain the leading digits of π. This unusual puzzle was popularized by the *3Blue1Brown* channel in 2019, and featured in another video in 2025 [1].

The second story takes us into the world of quantum computers. Imagine searching among N elements for one that satisfies a given condition. We can check each element, but we have no information that would help us choose promising candidates to try first. A classical computer must then check the elements one by one, taking about $N/2$ checks on average. **Grover's algorithm** allows a quantum computer to find the desired element with high probability using a number of oracle queries that grows as $\sqrt{N}$.

In 2020, Adam Brown showed something surprising: **the same mathematics lies behind these two apparently unrelated stories** [2]. Collisions between the blocks and Grover's algorithm can both be described by the same geometric procedure, using reflections and rotations. **The aim of this lecture is to understand how and why this is possible.**

1. Blocks That Count π

Before turning to Grover's algorithm, we will solve a puzzle from classical mechanics.

1.1 The Problem

Problem setup

Two blocks lie on a horizontal frictionless surface, with a wall to their left. The small block, of mass m, is at rest. The large block, of mass M, moves toward the small block and the wall, with an initial speed $V_0 > 0$. The number of collisions does not depend on that initial speed, only on the ratio of the block masses; we will see why in §1.9. The mass ratio M/m is given and is at least 1. All collisions are perfectly elastic, both between the blocks and when the small block hits the wall (Figure 1.1).

Question: how many collisions occur in total, counting both collisions between the blocks and bounces of the small block off the wall?

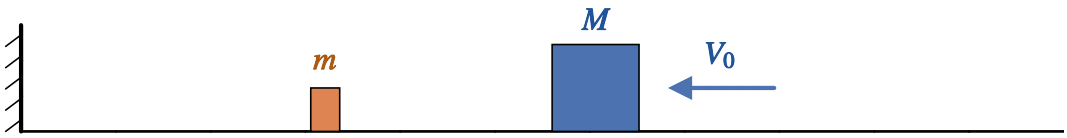


Figure 1.1. At the start, the small block is at rest and the large block moves toward the wall with speed V_0. The sizes of the blocks are not drawn in proportion to their masses.

Here are the answers for seven mass ratios, starting with blocks of equal mass, $M/m = 1$:

Mass ratio M/m	Number of collisions
1	3
100	31
10^4	314
10^6	3141
10^8	31415
10^{10}	314159
10^{12}	3141592

Table 1.1. The number of collisions for seven mass ratios.

The collision counts in the rows give the leading digits of $\pi = 3.14159265\ldots$, without the decimal point. Why does π appear in a problem about two colliding blocks?

1.2 How to Begin

How would you approach this problem? Before reading on, try to think of a possible solution yourself. The following suggestions, also given by *3Blue1Brown* in its video [1], may help:

- Start with a simpler case.
- Consider which physical quantities are conserved.

- Write down the equations that describe the system.
- Look for a symmetry that might simplify the problem.
- Work out a few concrete examples and look for a pattern.
- If you can, make a simple computer simulation.
- Draw a picture.

1.3 Conservation Laws and the Collision Equations

We choose the positive direction to be to the right, away from the wall. We denote the velocity of the small block by v and that of the large block by V. A block's velocity is therefore positive when it moves to the right and negative when it moves to the left. Initially, the small block is at rest and the large block moves toward the wall, so their velocities are $v = 0$ and $V = -V_0$, where $V_0 > 0$.

Because there is no friction and all collisions are perfectly elastic, the blocks' total **kinetic energy** E remains constant. During a collision between the blocks, their total **momentum** p is also conserved: the only horizontal forces acting during the collision are the forces the blocks exert on each other. The system's total kinetic energy and momentum are

$$E = \frac{mv^2}{2} + \frac{MV^2}{2}, \qquad p = mv + MV \tag{1.1}$$

In a perfectly elastic bounce off the stationary wall, the small block reverses direction without changing speed: $v \to -v$. The velocity of the large block does not change. Unlike a collision between the blocks, a bounce off the wall does not conserve their total momentum, because the wall exerts an external force on the system we are considering. We will explain this more fully at the end of the section.

We can use conservation of energy and momentum to determine the blocks' velocities after a collision with each other. Let these be v' and V'. Rewriting conservation of momentum gives

$$m(v - v') = M(V' - V).$$

Factoring the difference of squares in the energy equation gives

$$m(v - v')(v + v') = M(V' - V)(V' + V).$$

The small block's velocity changes in a collision, so $v' \neq v$. We can therefore divide the second equation by the first:

$$v + v' = V + V', \qquad \text{or} \qquad v' - V' = -(v - V).$$

Thus, in a perfectly elastic collision, the blocks' relative velocity changes sign while its magnitude stays the same. Together with conservation of momentum, this gives two linear equations for the unknown velocities v' and V'. Solving them yields

$$v' = \frac{(m - M)\,v + 2MV}{m + M}, \qquad V' = \frac{(M - m)\,V + 2mv}{m + M} \tag{1.2}$$

Equation (1.2) also explains a bounce off the wall. Imagine the wall as a block of mass M_{wall} initially at rest, $V_{\text{wall}} = 0$. Substitute it for the large block in (1.2), and consider what happens as its mass increases without bound, $M_{\text{wall}} \to \infty$.

After the collision, the velocities of the small block and the wall are

$$v' = \frac{m - M_{\text{wall}}}{m + M_{\text{wall}}}\, v \longrightarrow -v, \qquad {V_{\text{wall}}}' = \frac{2mv}{m + M_{\text{wall}}} \longrightarrow 0.$$

In this limit the small block bounces back at the same speed, while the wall's velocity tends to zero. What happens to the momentum? Although the wall's velocity becomes ever smaller, the momentum it receives does not tend to zero:

$$M_{\text{wall}}{V_{\text{wall}}}' = \frac{2M_{\text{wall}}mv}{m + M_{\text{wall}}} \longrightarrow 2mv.$$

The wall's kinetic energy, by contrast, tends to zero:

$$\frac{M_{\text{wall}}{V_{\text{wall}}}'^2}{2} = \frac{(M_{\text{wall}}{V_{\text{wall}}}')^2}{2M_{\text{wall}}} \longrightarrow 0.$$

In the infinite-mass limit, then, the wall receives a finite momentum while its velocity and kinetic energy tend to zero. Thus the two blocks' energy is conserved during the bounce, but their total momentum changes. Before impact the small block moves toward the wall, $v < 0$, so the change in the blocks' momentum is $-2mv = 2m|v|$, directed away from the wall.

1.4 The First Few Collisions

First consider the case in which the blocks have equal masses, $M = m$. Equations (1.2) then give $v' = V$ and $V' = v$: the blocks exchange velocities when they collide. Initially, the small block is at rest and the large block moves toward the wall, so $v = 0$ and $V = -V_0$. The pair of velocities (v, V) changes as follows:

$$(0, -V_0) \xrightarrow{\text{blocks}} (-V_0, 0) \xrightarrow{\text{wall}} (V_0, 0) \xrightarrow{\text{blocks}} (0, V_0).$$

After the first collision, the large block stops, while the small block continues toward the wall. After bouncing off the wall, the small block returns and collides with the large block again. In that collision, the small block stops and the large block moves to the right, away from the wall. The blocks are no longer approaching each other, so there will be no further collisions. **There are three collisions in total.**

Now suppose that the large block is 100 times as massive as the small block, so $M/m = 100$. To make the calculation simpler, choose units in which $m = 1$, $M = 100$ and $V_0 = 1$. For these masses, equations (1.2) become

$$v' = \frac{-99\,v + 200\,V}{101}, \qquad V' = \frac{99\,V + 2\,v}{101},$$

and the energy and momentum in (1.1) become

$$E = \frac{v^2}{2} + 50\,V^2, \qquad p = v + 100\,V.$$

Initially $v = 0$ and $V = -1$, so $E = 50$ and $p = -100$.

The **first collision** is a collision between the blocks. Substituting $v = 0$ and $V = -1$ gives

$$v' = \frac{-99 \cdot 0 + 200 \cdot (-1)}{101} = -\frac{200}{101} \approx -1.98,$$
$$V' = \frac{99 \cdot (-1) + 2 \cdot 0}{101} = -\frac{99}{101} \approx -0.98.$$

Both blocks move toward the wall, but the small block is faster and reaches it first.

The **second collision** is a bounce off the wall. The small block reverses its velocity; the large block keeps its velocity:

$$v' = -\left(-\frac{200}{101}\right) = \frac{200}{101} \approx 1.98,$$
$$V' = V = -\frac{99}{101} \approx -0.98.$$

The small block now moves to the right and the large block to the left, so they approach each other again.

The **third collision** is another collision between the blocks. Substituting the velocities after the second collision gives

$$v' = \frac{-99 \cdot \frac{200}{101} + 200 \cdot \left(-\frac{99}{101}\right)}{101} = -\frac{39600}{10201} \approx -3.88,$$
$$V' = \frac{99 \cdot \left(-\frac{99}{101}\right) + 2 \cdot \frac{200}{101}}{101} = -\frac{9401}{10201} \approx -0.92.$$

Both blocks again move toward the wall. The small block is faster, so it will hit the wall next.

Now let us check the conservation laws. Table 1.2 gives the energy and momentum in each state, with the numerical values substituted into (1.1):

State	Collision	v	V	$E = v^2/2 + 50\,V^2$	$p = v + 100\,V$
Initial		0	-1	$0 + 50 = 50$	$0 - 100 = -100$
After collision 1	blocks	-1.98	-0.98	$1.96 + 48.04 = 50$	$-1.98 - 98.02 = -100$
After collision 2	wall	1.98	-0.98	$1.96 + 48.04 = 50$	$1.98 - 98.02 = -96.04$
After collision 3	blocks	-3.88	-0.92	$7.53 + 42.47 = 50$	$-3.88 - 92.16 = -96.04$

Table 1.2. The first three collisions for $M/m = 100$, with $m = 1$, $M = 100$ and $V_0 = 1$. In the columns for E and p, the first term belongs to the small block and the second to the large block. Values were calculated from the exact fractions and rounded to two decimal places.

Although the blocks' velocities change at each collision, their total kinetic energy remains $E = 50$. Only the way that energy is shared between them changes. For example, after the third collision the kinetic energy of the small block is approximately 7.53, and that of the large block is 42.47.

The blocks' total momentum is conserved during their collisions with each other. It is -100 before and after the first collision, and approximately -96.04 before and after the third. But it changes when the small block bounces off the wall. In the second collision, the small block's velocity changes sign, increasing the system's total momentum by approximately 3.96.

After two collisions between the blocks, the speed of the large block has decreased by only about 8%. If we continued calculating this way, reaching 31 collisions would take a long time, and reaching 314 would be harder still. A computer could readily simulate all the collisions, but simulation alone does not explain why the resulting count contains the digits of π. **Can we represent the problem geometrically and arrive at a simpler solution?**

1.5 The Velocity Plane: An Ellipse

We can represent each pair of block velocities, V and v, by a point in a plane. We plot the velocity of the large block V on the horizontal axis and that of the small block v on the vertical axis. The result is the **velocity plane**, in which each point represents a possible pair of block velocities.

Conservation of kinetic energy gives

$$MV^2 + mv^2 = 2E \tag{1.3}$$

This is the equation of an **ellipse** (Figure 1.2a). Because the blocks' total kinetic energy is conserved, the point (V, v) must always lie on that ellipse. Between collisions the velocities are constant, so the point remains stationary in the velocity plane. At each collision the velocities change, and the point moves to another location on the same ellipse.

We find the ellipse's semiaxes from its intersections with the coordinate axes. For $v = 0$ we obtain $V = \pm\sqrt{2E/M}$, while $V = 0$ gives $v = \pm\sqrt{2E/m}$. The ratio of the vertical to the horizontal semiaxis is therefore $\sqrt{M/m}$. Since $M \geq m$, the ellipse is elongated vertically; for equal masses it becomes a circle.

As the energy increases, both semiaxes grow in proportion to $\sqrt{E}$, while their ratio, and therefore the shape of the ellipse, stays the same.

1.6 From an Ellipse to a Circle

The number of collisions contains π, a number we most often encounter in the geometry of circles. Let us therefore try to turn the ellipse into a circle. Unlike an ellipse with unequal semiaxes, a circle is unchanged by rotation about its center through any angle. This is the symmetry we want to exploit, following the advice in §1.2.

We can turn the ellipse into a circle by rescaling the coordinate axes. Multiplying each block's velocity by the square root of its mass gives the new coordinates

$$x = \sqrt{M}\,V, \qquad y = \sqrt{m}\,v \tag{1.4}$$

Conservation of energy then reads

$$x^2 + y^2 = MV^2 + mv^2 = 2E \tag{1.5}$$

so the point (x, y) lies on a circle of radius $R = \sqrt{2E}$ (Figure 1.2b). Unlike the earlier (V, v) plane, we now use the **scaled-velocity plane**, with coordinates (x, y). From now on, we will represent the collisions in this plane.

Initially $v = 0$ and $V = -V_0$, so $E = MV_0^2/2$ and the circle's radius is

$$R = \sqrt{2E} = \sqrt{M}\,V_0.$$

The circle need not, therefore, be a unit circle. To simplify a drawing we may divide both coordinates by R, obtaining a circle of radius 1. This rescaling changes neither the angles nor the geometric construction; in the equations we continue to use the original coordinates x and y.

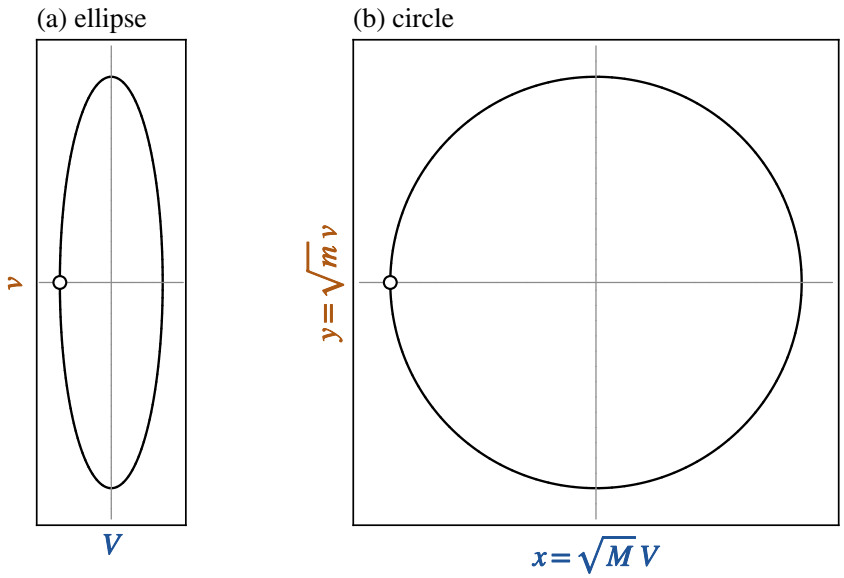


Figure 1.2. $M/m = 16$. (a) In the (V, v) plane, the energy equation $MV^2 + mv^2 = 2E$ describes an ellipse whose vertical semiaxis is four times its horizontal semiaxis. (b) With $x = \sqrt{M}\,V$ and $y = \sqrt{m}\,v$, the same equation describes the circle $x^2 + y^2 = 2E$. The white circle marks the start: the small block is at rest and the large block moves toward the wall.

1.7 The Line of Constant Momentum

Let us see how conservation of momentum looks in the new coordinates. The momentum is

$$MV + mv = \sqrt{M}\,(\sqrt{M}\,V) + \sqrt{m}\,(\sqrt{m}\,v) = \sqrt{M}\,x + \sqrt{m}\,y,$$

so conservation of momentum takes the form

$$\sqrt{M}\,x + \sqrt{m}\,y = p \tag{1.6}$$

For a given value of p, this equation describes a line in the (x, y) plane. Its slope is $-\sqrt{M/m}$. We will call it a **line of constant momentum**, or simply a momentum line.

Both kinetic energy and total momentum are conserved in a collision between the blocks. The points representing the velocities before and after the collision must therefore lie on the same circle and the same line of constant momentum. In a collision that changes the velocities, the line intersects the circle at two distinct points: one represents the velocities before the collision and the other those after it. **To find the velocities after the collision, we need only find the second intersection of the line of constant momentum with the circle.**

Initially, the small block is at rest, $y = 0$, and the large block moves toward the wall, $x < 0$. The initial velocities are therefore represented by the leftmost point on the circle. Draw a line of constant momentum through it. Its second intersection with the circle represents the velocities after the first collision between the blocks (Figure 1.3a).

The next collision is the small block's bounce off the wall. Because it is perfectly elastic, the small block's velocity changes sign, $v \to -v$, while the large block's velocity does not change. In the new coordinates, x stays the same and y changes sign. The velocities before and after the bounce are

therefore represented by two points on the circle that lie on the same vertical line (Figure 1.3b). In the geometric picture we connect them by a vertical line segment.

The procedure then repeats: we represent a collision between the blocks by a segment along a line of constant momentum, and a bounce off the wall by a vertical segment. All the constant-momentum lines have the same slope, $-\sqrt{M/m}$, because it depends only on the mass ratio. Different momentum values give different, parallel lines.

We will see that this slope determines the geometry of the construction and hence the total number of collisions. In Chapter 4 we will connect the same mass ratio with Grover's algorithm.

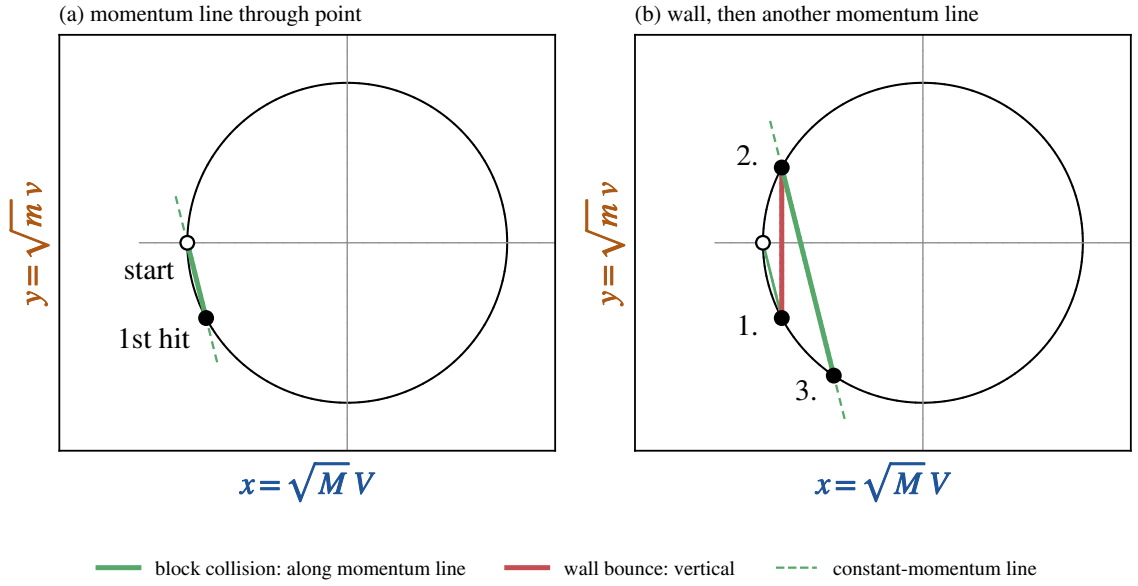


Figure 1.3. $M/m = 16$, circle of radius 1. (a) Collision between blocks: the points before and after the collision are joined by a segment along a line of constant momentum of slope -4. (b) A bounce off the wall changes only y: the corresponding points are joined by a vertical segment. A new line of constant momentum follows. The numbers give the order of the collisions.

1.8 When the Collisions Stop

Because the small block lies to the left of the large block, the rate at which their separation changes is $V - v$. The blocks approach one another when $V < v$ and move apart when $V > v$. If $V = v$, their separation remains constant. A collision with the wall is possible only if the small block moves toward it, $v < 0$.

After a bounce off the wall, the small block moves to the right and cannot hit the wall again until it has collided with the large block. Conversely, the blocks' relative velocity changes sign in an elastic collision (§1.3), so immediately afterward they move apart. Thus, as long as collisions continue, block–block collisions alternate with bounces off the wall.

For there to be no further collision of either kind, the small block must no longer move toward the wall, and the large block must be at least as fast as the small block. Both conditions can be written as one inequality:

$$0 \le v \le V \tag{1.7}$$

In such a state the small block is at rest or moving away from the wall, while the large block moves

to the right at a velocity at least as large as the small block's. No collision of either kind can then occur. We call the set of all such states the **final region**. In the next section we will show what it looks like in the scaled-velocity plane.

1.9 From Collisions to a Geometric Problem

We have seen that collisions stop when condition (1.7), $0 \le v \le V$, holds. Let us see what this condition looks like in the scaled-velocity plane (x, y) (Figure 1.4).

First, the small block must no longer move toward the wall: $v \ge 0$. Since $y = \sqrt{m}\, v$, this means $y \ge 0$. From $V \ge v \ge 0$ it also follows that $x \ge 0$. The final region therefore lies in the upper-right quadrant (Figure 1.4a).

Second, the large block must be at least as fast as the small block: $V \ge v$. On the boundary $V = v$ the blocks move at the same velocity, so their separation remains unchanged. In the ordinary velocity plane (V, v) this is a line of slope 1, at 45° to the horizontal axis (Figure 1.4b).

In the scaled-velocity plane, each velocity is multiplied by the square root of its block's mass. The equal-velocity line therefore becomes

$$V = v \qquad \Longleftrightarrow \qquad y = \sqrt{\frac{m}{M}}\, x.$$

This is the **line of equal velocities** (Figure 1.4c). Since the heavier block's coordinate is multiplied by a larger square root, the line moves closer to the x-axis: its slope is 1/4 for $M/m = 16$, and only 1/10 for $M/m = 100$.

Together, both conditions determine the **final region**: the wedge between the positive horizontal axis and the equal-velocity line,

$$x \ge 0, \qquad 0 \le y \le \sqrt{\frac{m}{M}}\, x.$$

Once the point representing the block velocities enters this wedge, no further collision is possible. Outside the final region, the small block moves toward the wall or the blocks' separation decreases, so at least one more collision will occur. The greater the mass ratio, the narrower the wedge.

We now have everything needed to turn the physical problem into a geometric one. Each collision can be represented by a segment joining the points on the circle immediately before and after the collision. A collision between the blocks corresponds to a segment on a line of constant momentum; a bounce off the wall corresponds to a vertical segment. There is one segment per collision, so the question of the total number of collisions becomes a question of counting segments.

Geometric setup

Start at the leftmost point of the circle. Draw a line of constant momentum through it, with slope $-\sqrt{M/m}$, and join the starting point to the line's other intersection with the circle.

From the new point draw a vertical segment to its other intersection with the circle. Then alternate these two steps until you reach the final region.

Question: how many segments can you draw before reaching the final region? That number is the total number of collisions.

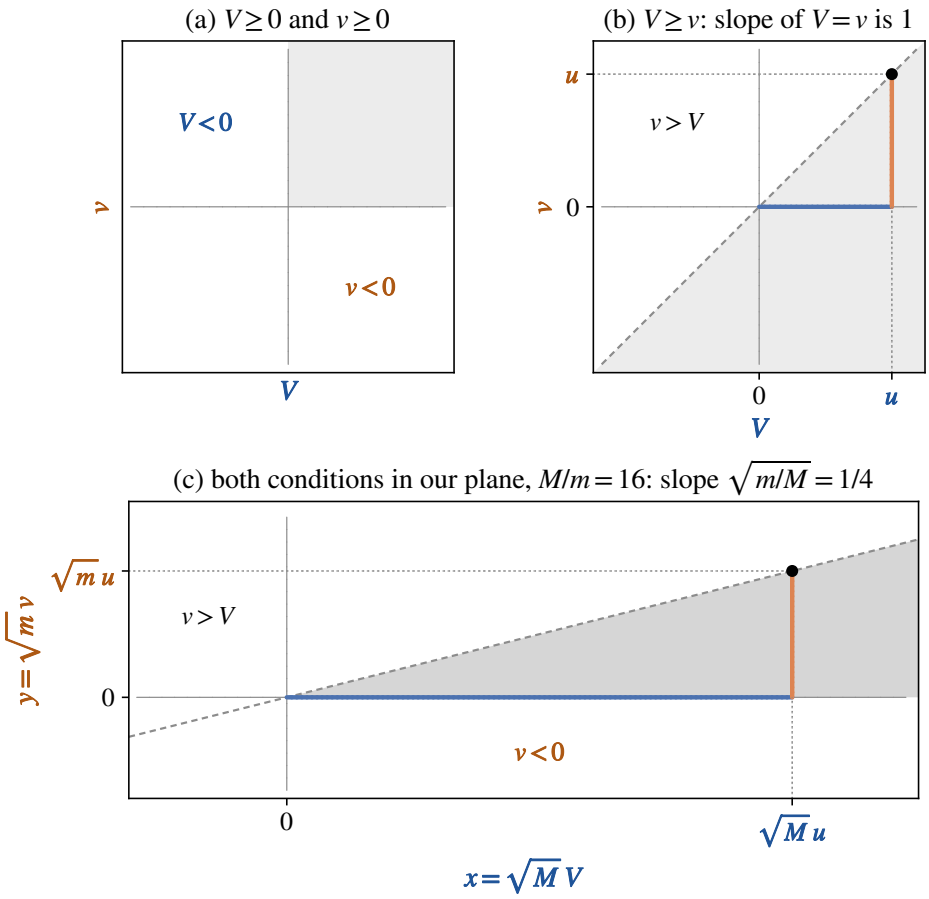


Figure 1.4. Locating the final region. (a) Neither velocity is negative in the upper-right quadrant (light gray); below the axis the small block heads toward the wall, and to the left of the axis the large block does. (b) The large block is no slower than the small one, $V \geq v$, below the line $V = v$. To reach the point where both blocks have velocity u, we move u to the right (blue) and u up (orange), so the slope is 1. (c) In our plane the same point is $(\sqrt{M}\,u, \sqrt{m}\,u)$, so the equal-velocity line has slope $\sqrt{m/M}$, exactly 1/4 when $M/m = 16$. Together the conditions give the narrow gray wedge, the final region in Figure 1.5.

For $M/m = 100$, this construction gives 31 segments, or 31 collisions (Figure 1.5b). The slope of a constant-momentum line depends only on the mass ratio, while the initial speed V_0 determines the circle's radius:

$$R = \sqrt{2E} = \sqrt{M}\,V_0.$$

Changing the initial speed makes the circle larger or smaller, but all angles remain the same. The number of segments we can draw, and hence the number of collisions, therefore remains unchanged. **The total number of collisions depends only on the mass ratio M/m, not on the initial speed.**

1.10 Equal Arcs

We must now count the segments representing collisions. Instead, we will count the arcs of the circle between points obtained by the construction. We will show that each arc we count corresponds to the same central angle $2\bar{\theta}$. Since they all lie on the same circle, equal central angles also mean equal arc lengths; the remaining arc that closes the circle may be shorter (Figure 1.6).

On a circle of radius R, an arc subtending the central angle $\Delta\varphi$ in radians has length $R\Delta\varphi$. Thus an arc subtending $2\bar{\theta}$ has length $2R\bar{\theta}$. In what follows we identify arcs by their central angles; on a unit

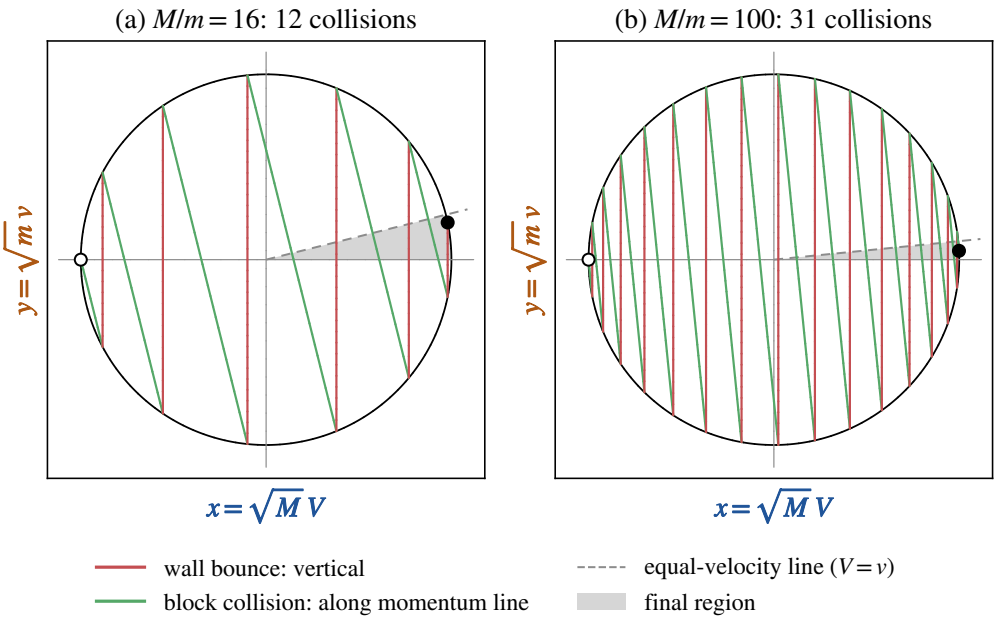


Figure 1.5. All the segments in the scaled-velocity plane. Green represents collisions between the blocks (along momentum lines); red represents bounces off the wall (vertical segments). (a) $M/m = 16$, slope -4: 12 segments. (b) $M/m = 100$, slope -10: 31 segments. The white circle is the start and the black point the end. Gray is the final region, $0 \le v \le V$; the dashed gray line is its upper boundary, the equal-velocity line (Figure 1.4).

circle those numbers are also their lengths.

Why are the angles equal? Each sloping segment lies on a line of slope $-\sqrt{M/m}$, and every other segment is vertical. Every sloping and vertical segment meeting at a point therefore make the **same angle**, which we call $\bar{\theta}$. The angle depends only on the slope, hence on the mass ratio; we calculate it in §1.12.

Take three consecutive points, P_1, P_2 and P_3 (Figure 1.7). At the middle point, P_2, a vertical and a sloping segment meet. Both extend from P_2 in the same direction, either upward or downward, so the angle between them is the acute angle $\bar{\theta}$. Its vertex lies on the circle, making it an **inscribed angle** subtending the arc P_1P_3 that does not contain P_2. By the **inscribed-angle theorem**, the inscribed angle is half the central angle subtending the same arc (proved in Appendix B). Thus arc P_1P_3 subtends $2\bar{\theta}$ for every three consecutive points: each point is $2\bar{\theta}$ farther from the start than the point two collisions earlier. All these arcs are therefore $2\bar{\theta}$, except the arc between the last two points.

The same holds for every arc (Figure 1.8). We number the points in collision order, starting with point 0. Every point except the first and last is the vertex of an inscribed angle $\bar{\theta}$ between the vertical and sloping segments meeting there. That angle subtends the arc between the preceding and following points, so each such arc is $2\bar{\theta}$. Only the first arc, from point 0 to point 1, has no angle of its own, but it too is $2\bar{\theta}$: points 1 and 2 lie on the same vertical line, symmetrically about the x-axis, and the start lies on that axis, so the arcs from the start to points 1 and 2 are equal.

1.11 How Many Arcs Fit Around the Circle?

The arcs with central angle $2\bar{\theta}$ run around the circle on both sides of the starting point until they reach the final region. We get one such arc for each collision, plus an additional arc next to the final region that closes the circle. Collisions stop as soon as the point reaches the final region, including its

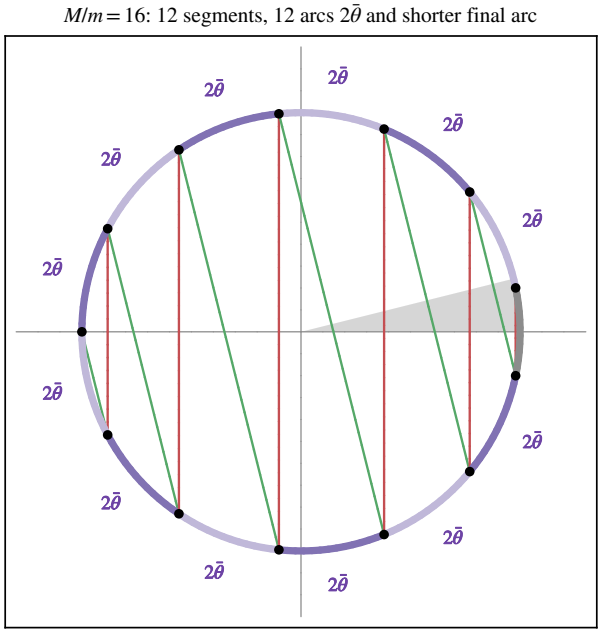


Figure 1.6. $M/m = 16$, slope -4: all 12 segments and their 13 points on the circle. The points divide the circle into 12 equal arcs of $2\bar{\theta}$, shown in two shades of purple, and a shorter final arc, gray, next to the final region.

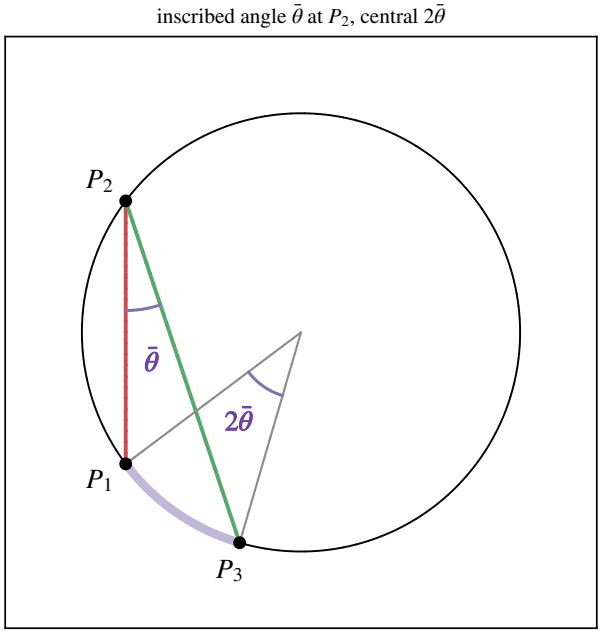


Figure 1.7. Why the arcs are equal. P_1 is the point before a bounce off the wall, P_2 after it, and P_3 after the next collision between the blocks. The inscribed angle at P_2 is $\bar{\theta}$, so the central angle subtending arc P_1P_3 (light purple) is $2\bar{\theta}$. Drawn for $M/m = 9$, where $\bar{\theta} = 18.4°$, to make the angles easier to see.

boundary, so we do not count the remaining arc as a collision. Counting therefore excludes the arc that would close the circle. This strict boundary also follows from the construction in Appendix A: there collisions correspond only to directions $j\bar{\theta}$ strictly between 0 and π; the ray does not cross the direction π.

If the circle has radius R, each counted arc has length $2R\bar{\theta}$ and the circumference is $2\pi R$. The number

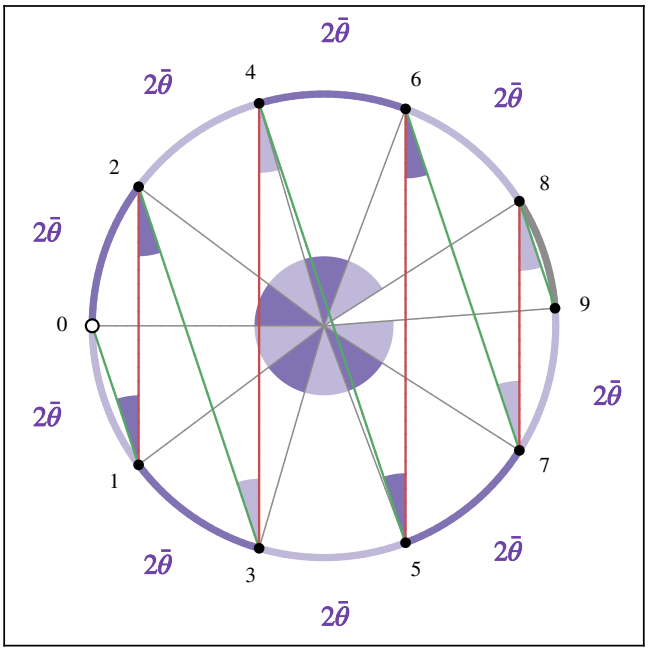


Figure 1.8. The construction in Figure 1.7 applied to every arc, for $M/m = 9$. Points are numbered in collision order, with 0 as the start. At each point from 1 to 8, the small wedge is the inscribed angle $\bar{\theta}$ between the vertical and sloping segments; it subtends the arc between the preceding and following points, colored the same shade of purple. The central angle of that arc, between the two gray radii, has the same shade and equals $2\bar{\theta}$. The first arc, from 0 to 1, equals the arc from 0 to 2 by symmetry; the remaining gray arc can be shorter.

of collisions is the largest number of such arcs that fit before the circle closes. Thus the number of collisions N satisfies

$$N \cdot 2R\bar{\theta} < 2\pi R, \qquad \text{or} \qquad N\bar{\theta} < \pi.$$

Because $R > 0$, the radius cancels: the result does not depend on the size of the circle. We measure angles in radians, so a complete turn is 2π and π radians is 180° (Appendix B). The number of collisions is **the largest integer N for which $N\bar{\theta} < \pi$**. The inequality is strict. For $M = m$, the slope is -1, so the sloping segment makes 45° with the vertical: $\bar{\theta} = \pi/4$ and $4\bar{\theta} = \pi$ exactly. There are 3 collisions, not 4. If $\lceil q \rceil$ denotes the smallest integer not less than q (rounding up), then the number of integers $N \geq 1$ with $N < q$ is $\lceil q \rceil - 1$, because $\lceil q \rceil - 1 < q \leq \lceil q \rceil$. With $q = \pi/\bar{\theta}$:

$$\text{number of collisions} = \left\lceil \frac{\pi}{\bar{\theta}} \right\rceil - 1 \tag{1.8}$$

For $M = m$, $\pi/\bar{\theta} = 4$, giving $\lceil 4 \rceil - 1 = 3$ collisions.

Consider the complete diagram for $M = m$ (Figure 1.9). For simplicity we use a unit circle. The momentum line has slope -1, so it makes a 45° angle with each axis. Hence the angle between a sloping segment and a vertical is $\bar{\theta} = 45°$, and an arc of $2\bar{\theta}$ is a quarter-circle. The point starts at $(-1,0)$: the large block moves toward the wall and the small block is at rest. The first block–block collision is a sloping segment to $(0,-1)$: equal masses exchange velocities, so the large block stops and the small block heads toward the wall. The bounce off the wall is a vertical segment to (0,1): the small block returns at the same speed. The second block–block collision is a sloping segment to (1,0): the small block stops and the large one moves away from the wall. Point (1,0) lies on the

lower boundary of the final region, because the small block is at rest, so the construction stops there. **Three segments, three collisions.**

Counting arcs gives the same result. Four points, 0, 1, 2 and 3, divide the circle into four quarters. Three are laid out from the start, one per collision; the fourth would close the circle. Four collisions would require $4\bar{\theta} < \pi$, but here $4\bar{\theta} = \pi$ exactly: the inequality is strict, so there are 3 collisions, not 4.

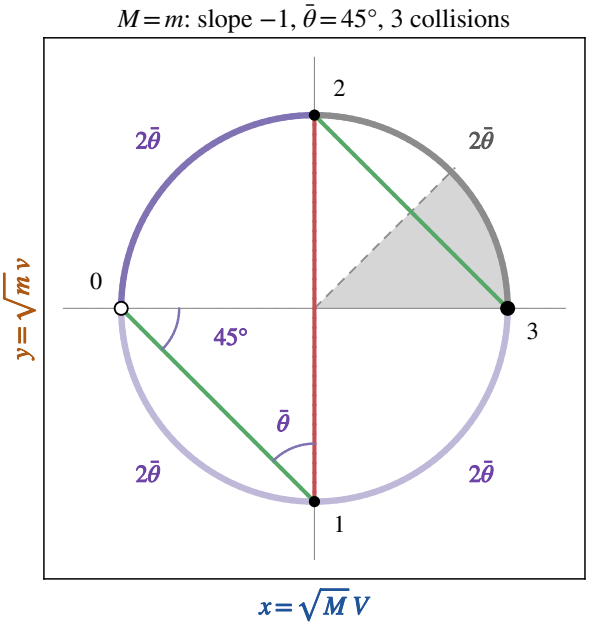


Figure 1.9. $M = m$. The momentum line has slope -1, so the sloping segment makes 45° with the x-axis (at point 0) and $\bar{\theta} = 45°$ with the vertical (at point 1). The point travels from 0 to 1 (block–block collision), from 1 to 2 (bounce off the wall), and from 2 to 3 (another block–block collision), where it reaches the final region. The points divide the circle into four arcs of $2\bar{\theta} = 90°$: three extend from the start (in two shades of purple), and the fourth, gray, would close the circle. Thus there are 3 collisions.

1.12 The Digits of π

We now have all the pieces. By (1.8), the number of collisions depends only on the angle $\bar{\theta}$: how many arcs of $2\bar{\theta}$ fit around the circle. It remains to calculate $\bar{\theta}$ from the masses and see why the answer contains the digits of π. Let us proceed step by step.

The angle from the slope. Consider the right triangle formed by a sloping segment and the vertical and horizontal directions (Figure 1.10a). Its legs have lengths Δy and Δx. The slope is $-\Delta y/\Delta x = -\sqrt{M/m}$. Because $\bar{\theta}$ lies between the sloping segment and the vertical, its tangent is $\Delta x/\Delta y$:

$$\tan\bar{\theta} = \frac{\Delta x}{\Delta y} = \sqrt{\frac{m}{M}} \tag{1.9}$$

Consider two examples from the figures. For $M = m$, $\tan\bar{\theta} = 1$, so $\bar{\theta} = 45° = \pi/4$ and there are 3 collisions (Figure 1.9). For $M/m = 16$, $\tan\bar{\theta} = 1/4$, so $\bar{\theta} \approx 0.2450$, about 14.04°. Then $\pi/\bar{\theta} \approx 12.82$, and (1.8) gives 12 collisions (Figure 1.5a).

A thought experiment: the angle is a power of 10. Suppose for a moment that $\bar{\theta}$ is exactly 0.1.

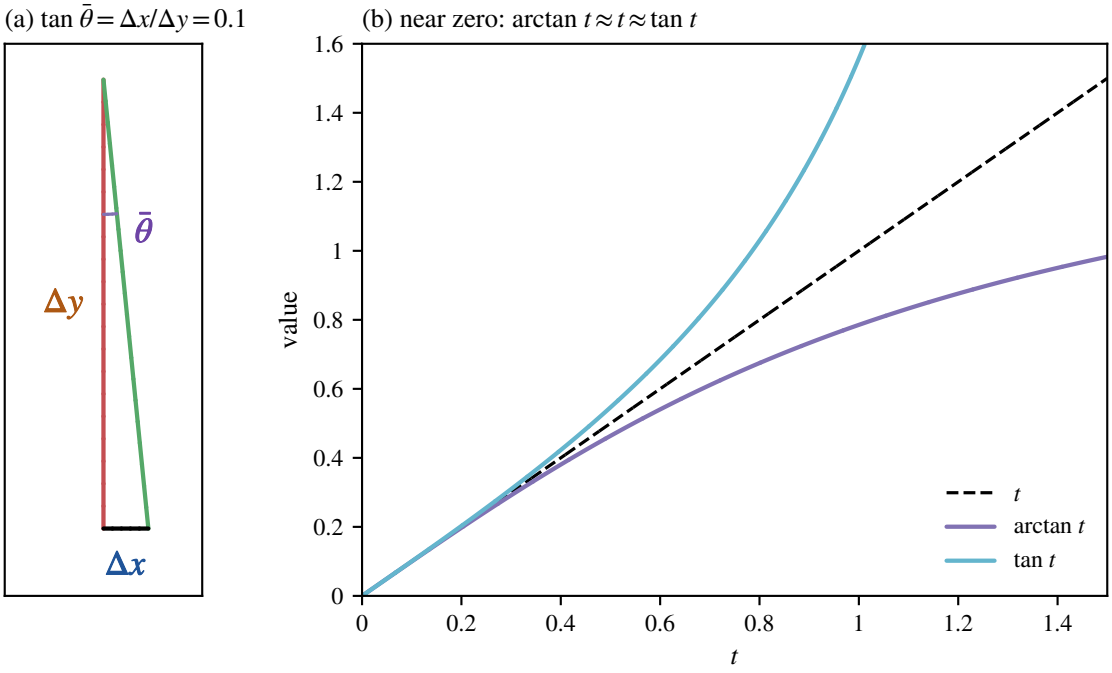


Figure 1.10. (a) For $M/m = 100$, $\tan\bar{\theta} = \Delta x/\Delta y = 0.1$: the narrow triangle between a vertical segment (wall) and a sloping segment (block–block collision). (b) Near zero, $\arctan t$, t and $\tan t$ are nearly equal, so $\bar{\theta} = \arctan 0.1 \approx 0.1$.

The number of collisions is the largest integer N satisfying $N\bar{\theta} < \pi$, or the largest integer less than $\pi/\bar{\theta}$:

$$\frac{\pi}{0.1} = 31.4159\ldots \qquad \Longrightarrow \qquad N = 31.$$

Dividing by 0.1 moves the decimal point one place to the right. Dividing by 0.01 moves it two places, and dividing by 0.001 moves it three:

$$\frac{\pi}{0.01} = 314.159\ldots \implies N = 314, \qquad \frac{\pi}{0.001} = 3141.59\ldots \implies N = 3141.$$

If $\bar{\theta}$ is a power of 10, the collision count is therefore π without its decimal point, truncated after as many decimal places as there are digits after the decimal point in $\bar{\theta}$: these are the **digits of** π. Two questions remain. What mass ratio gives such an angle? And is the angle then really exactly a power of 10?

Which mass ratio? By (1.9), the masses determine the tangent, $\tan\bar{\theta} = \sqrt{m/M}$. For the tangent to be 0.1, we need $m/M = 0.01$, or $M/m = 100$. For it to be 0.01, we need $M/m = 10\,000 = 100^2$. In general, for an integer $D \geq 0$ (the number of digits of π we want after the decimal point), the square root gives

$$\tan\bar{\theta} = 0.1^D \qquad \Longleftrightarrow \qquad \frac{M}{m} = 100^D.$$

The mass ratio must be a power of 100, not 10: the square root halves the exponent. For $M/m = 1000$, $\tan\bar{\theta} = 10^{-1.5} \approx 0.0316$ and there are 99 collisions; for $M/m = 10^5$ there are 993. These are not digits of π, but of $\pi\sqrt{10} = 9.93\ldots$.

The tangent is not the angle. So far we have considered an angle exactly equal to 10^{-D}. The mass ratio, however, determines the tangent, not the angle itself. For $M/m = 100$ it is exactly $\tan\bar{\theta} = 0.1$,

not $\bar{\theta} = 0.1$. The angle is slightly smaller: $\bar{\theta} = \arctan 0.1 = 0.09967\ldots$. Here the **small-angle approximation** helps (Figure 1.10b; see Appendix B). For a small angle t in radians, such as $t = 0.001$,

$$\arctan t \approx t \approx \tan t \tag{1.10}$$

How much smaller is the angle than its tangent, and does it change the collision count? Table 1.3 gives the counts and rounded values of the angle and quotient. For $D \geq 1$ the angle is slightly smaller than the tangent, so $\pi/\bar{\theta}$ is slightly larger than $\pi \cdot 10^D$: 31.52 rather than 31.42; 314.170 rather than 314.159. The excess is about 0.10 for $D = 1$, 0.010 for $D = 2$ and 0.0010 for $D = 3$. In these examples the quotient does not reach the next integer, so the collision counts remain 31, 314 and 3141. The approximation alone, however, does not guarantee this agreement for every D.

M/m	$\tan\bar{\theta}$	$\bar{\theta}$	$\pi/\bar{\theta}$	**collisions**
1	1	0.785398	4	3
100	0.1	0.0996687	31.5204	31
10^4	0.01	0.00999967	314.1697	314
10^6	0.001	0.000999999667	3141.5937	3141

Table 1.3. Tangent, angle and collision count for powers of 100. Collision counts are exact; angle and quotient values are rounded where necessary. In the displayed examples with $D \geq 1$, the angle is slightly smaller than its tangent, making $\pi/\bar{\theta}$ slightly larger than $\pi \cdot 10^D$, but the integer part does not change. For $D = 0$, i.e. $M = m$, the angle is substantially smaller and $\pi/\bar{\theta} = 4$, yet there are 3 collisions because of the strict inequality in §1.11.

Putting it together. From (1.8) and (1.9), the exact collision count is

$$N = \left\lceil \frac{\pi}{\arctan\sqrt{m/M}} \right\rceil - 1.$$

For a large mass ratio the angle is approximately its tangent, $\sqrt{m/M}$, so

$$\text{number of collisions} \approx \pi\sqrt{\frac{M}{m}} \tag{1.11}$$

For $M/m = 100^D$ this is $\pi \cdot 10^D$: a block 100 times as massive gives 31 collisions, 10,000 times gives 314, and a million times gives 3141 (Figure 1.11). The greater the mass ratio, the smaller the arcs $2\bar{\theta}$ and the more fit around the circle. **The arcs write out π, and the collisions count them.**

When the digits do not match. The difference between $\pi/\arctan(10^{-D})$ and $\pi \cdot 10^D$ gets smaller, but that alone does not prove that their integer parts are always equal: the first number can still cross the next integer if the second is close enough to it. In his paper [4], Galperin conjectures that for natural $D \geq 1$, $\lfloor \pi/\arctan(10^{-D}) \rfloor = \lfloor \pi \cdot 10^D \rfloor$. He also considers a related condition involving a string of nines after the Dth decimal place. This remains a conjecture; a small difference does not itself prove agreement of all digits.

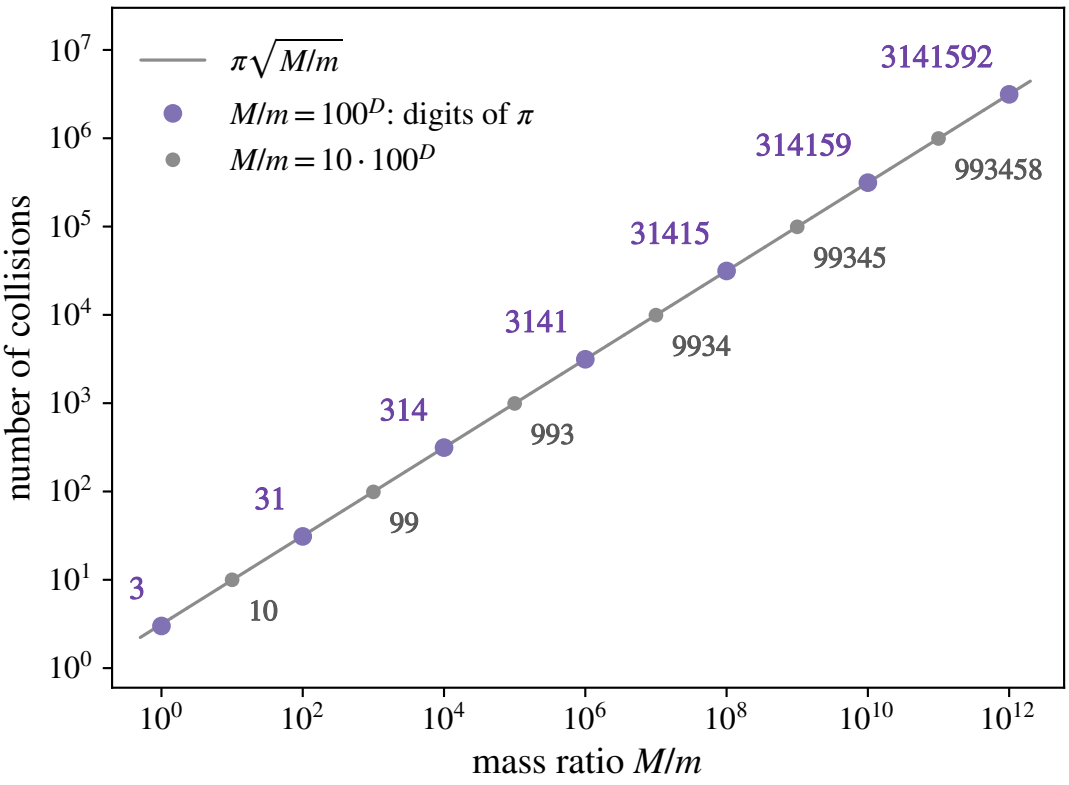


Figure 1.11. Collision counts from simulation for $M/m = 10^k$, $k = 0{,}1, \ldots, 12$, and the line $\pi\sqrt{M/m}$ from (1.11); both axes are logarithmic. Purple points, $M/m = 100^D$, give digits of π: 3, 31, 314, ... Gray points, $M/m = 10 \cdot 100^D$, give digits of $\pi\sqrt{10} = 9.93\ldots$ starting at $M/m = 1000$: 99, 993, 9934, ...

Key Points from This Chapter

1. Conservation laws. The two blocks' kinetic energy is conserved in every collision. Their total momentum is conserved in a collision between the blocks, but not in a bounce off the wall, which exerts an external force:

$$E = \frac{mv^2}{2} + \frac{MV^2}{2}, \qquad p = mv + MV.$$

2. From ellipse to circle. We represent a velocity pair (V,v) by a point on the ellipse $MV^2+mv^2 = 2E$. With $x = \sqrt{M}\,V$ and $y = \sqrt{m}\,v$ we obtain the circle $x^2 + y^2 = 2E$. Its radius is $R = \sqrt{2E} = \sqrt{M}\,V_0$; it need not be a unit circle.

3. Representing collisions. A block–block collision is a segment on the constant-momentum line $\sqrt{M}\,x + \sqrt{m}\,y = p$, of slope $-\sqrt{M/m}$. A bounce off the wall is a vertical segment: y changes sign. The segments connect the points before and after collisions; they are not the blocks' paths.

4. Final region. Collisions stop when $0 \le v \le V$: the small block does not move toward the wall and the large block does not approach it. In the scaled-velocity plane this is the wedge $x \ge 0$, $0 \le y \le \sqrt{m/M}\,x$.

5. Equal arcs. Each collision corresponds to one arc with central angle $2\bar{\theta}$, where $\tan\bar{\theta} = \sqrt{m/M}$. On a circle of radius R, its length is $2R\bar{\theta}$.

6. Exact collision count. The number of collisions N is the largest integer for which $N\bar{\theta} < \pi$, so

$$N = \left\lceil \frac{\pi}{\bar{\theta}} \right\rceil - 1.$$

The radius cancels when arc lengths are compared with the circumference, so the collision count does not depend on the initial speed. For equal masses $\bar{\theta} = \pi/4$ and there are three collisions, because the inequality is strict.

7. Digits of π. For a large mass ratio, $\bar{\theta} = \arctan\sqrt{m/M} \approx \sqrt{m/M}$, so $N \approx \pi\sqrt{M/m}$. For $M/m = 100^D$ we approximately obtain $\pi 10^D$. The approximation alone does not prove that all expected digits agree for every D; Galperin's conjecture was discussed in §1.12.

Key idea: The conservation laws let us represent collisions geometrically and count them using equal arcs. Behind this geometry are reflections that we will later connect to Grover's algorithm.

1.13 Exercises

Exercises for independent study

These exercises practice conservation laws, calculating velocities after elastic collisions and representing them geometrically. We begin with simpler examples involving a few collisions, then move on to the velocity plane, the geometry of the circle and the total number of collisions. The final exercises concern the connection with π and extensions of the problem.

Conservation laws and elastic collisions (§1.1–§1.4)

Exercise 1. Count the collisions for $M = m$ without a formula, then check your answer using (1.8). *Hint: in an elastic collision equal masses exchange velocities.*

Exercise 2. Count the collisions for $M = 3m$ if the small block initially rests and the large one moves toward the wall with initial speed $V_0 = 1$. *Hint: calculate the velocities after each collision using (1.2).*

Exercise 3. Show that (1.2) can be written $v' = 2v_{\text{cm}} - v$ and $V' = 2v_{\text{cm}} - V$, where $v_{\text{cm}} = (mv + MV)/(m + M)$ is the center-of-mass velocity. *Hint: put $2v_{\text{cm}} - v$ over a common denominator.*

Exercise 4. A small block of mass $m = 1$ is at rest; a large block of mass $M = 3$ moves toward it with velocity $V = -4$. Calculate the velocities after their elastic collision and check the total kinetic energy and momentum before and after. *Hint: use (1.2).*

Exercise 5. A small block of mass $m = 2$ hits a stationary wall at velocity $v = -3$ and bounces perfectly elastically. Find its velocity after impact, change in momentum, and kinetic energy before and after impact.

Exercise 6. The small block is between the wall and the large block. For each velocity pair $(v,V) = (-2,1)$, $(2,-1)$ and $(1,2)$, determine whether the next collision is with the wall, between the blocks, or whether there are no further collisions.

The velocity plane and its geometric representation (§1.5–§1.9)

Exercise 7. Let $m = 1$, $M = 4$ and total kinetic energy $E = 8$. Write the equation of the ellipse in the (V,v) plane; find its semiaxes and the radius of the circle in the (x,y) plane. Which point on the circle corresponds to $(V,v) = (-2,0)$?

Exercise 8. For $M/m = 16$, find the slope of the constant-momentum line and the slope of the equal-velocity line in the (x,y) plane. Check that the lines are perpendicular.

Exercise 9. For $m = 1$, $M = 4$ and $(V,v) = (-1,-2)$, calculate E, the coordinates (x,y) and the circle's radius. Which point represents the velocities after the small block bounces off the wall?

Exercise 10. For the velocity pairs $(v,V) = (0,2)$, $(2,1)$, $(-1,3)$ and $(1,1)$, determine which lie in the final region. For the others, say whether the small block moves toward the wall or the blocks approach each other. *Hint: use (1.7).*

Exercise 11. With the masses unchanged, double the large block's initial speed. How do the initial energy, the circle's radius and the collision count change? Explain what happens to the angles in the geometric construction.

Angles, arcs and collision count (§1.10–§1.12)

Exercise 12. How many integers $j \geq 1$ satisfy $0.3\,j < 1$, and how many satisfy $0.25\,j < 1$? Check both answers using the counting rule in §1.11.

Exercise 13. An inscribed angle subtending an arc is $15°$. Find the corresponding central angle and the arc length for a circle of radius $R = 3$. *Hint: express the angle in radians when calculating arc length.*

Exercise 14. Apply the exact formula (1.8) for $\bar{\theta} = \pi/4$, $\pi/6$ and 0.2 radians. Explain why, in the first two cases, the number of collisions is not equal to $\pi/\bar{\theta}$.

Exercise 15. How many collisions occur for $M/m = 16$ and for $M/m = 10^6$? *Hint:* $\tan\bar{\theta}$ *is* $1/4$ *and* 10^{-3}*, respectively; calculate the angle in radians.*

Exercise 16. For $M/m = 100$, compare the exact collision count with the approximation $\pi\sqrt{M/m}$. What is the difference?

Digits of π and further challenges

Exercise 17. For mass ratios $M/m = 100^D$ we obtain the collision counts 3, 31, 314, 3141, ..., containing the leading digits of π in decimal notation (§1.12).

Find a number a such that the mass ratio $M/m = a^D$ similarly gives the leading digits of π in binary, $\pi = (11.001001000011\ldots)_2$. Calculate the collision count for $D = 0,1,2,3$, write it in binary and compare it with the binary expansion of π. Which mass ratio gives the digits in base 3?

Hint: by (1.11), the number of collisions is approximately $\pi\sqrt{M/m}$*. Multiplying by* 10^D *moves the decimal point D places; multiplying by* 2^D *moves the binary point D places.*

Exercise 18. For a number system of base $b \geq 2$, find a mass ratio of the form $M/m = a^D$ that would, according to the approximate formula, shift the expansion of π by D places. Explain why this approximation alone does not guarantee matching digits for every D.

Exercise 19. For $t = 0.1$ calculate $\arctan t$, π/t and $\pi/\arctan t$. Round to four decimal places and compare the integer parts of the latter two numbers.

Exercise 20. *Further challenge.* The numbers 2.999 and 3.001 differ by only 0.002. Find their integer parts and explain why a small difference between $\pi \cdot 10^D$ and $\pi/\arctan(10^{-D})$ does not, by itself, prove that their integer parts are equal.

2. Foundations of Quantum Mechanics and Quantum Computing

To understand how Grover's algorithm works, we must first learn how quantum mechanics describes states and their changes. To begin, vectors, the basic rules for calculating with them, and the concept of probability will suffice. We will represent the operation of a quantum computer as a sequence of operations on state vectors. Once we have learned this language, we will apply it to search in the next chapter.

In this chapter we consider **pure quantum states**, represented by vectors. To make the geometry easier to visualize, we restrict ourselves to real amplitudes. This is sufficient for Grover's algorithm in the form considered here, although amplitudes are complex numbers in quantum mechanics generally, and mixed states also exist.

2.1 A Quantum State as a Vector

We represent a pure quantum state by a vector. For vectors, we use the notation introduced by Paul Dirac [3]. This notation can represent both quantum states and vectors in the mechanical problem; later, it will help us recognize their shared mathematical structure.

A vector in a plane is an arrow from the origin. We describe it by two numbers, its **components**, for example (3,4). We add vectors component by component, $(a,b) + (c,d) = (a + c, b + d)$, and multiply them by numbers, $\lambda(a,b) = (\lambda a, \lambda b)$. By the Pythagorean theorem, the length of (a,b) is $\sqrt{a^2 + b^2}$; the vector (3,4) has length 5. A vector of length 1 is a **unit vector**. None of this depends on having exactly two components. A vector in space has three, and we will also need vectors with N components, where N can be a million. We cannot draw such a vector, but we calculate with it just as in the plane: we add it component by component, multiply it by a number, and find its length by taking the square root of the sum of the squares of all its components.

Dirac writes a vector as $|\psi\rangle$; this is called a **ket**, read "ket psi." Between the vertical bar and the angled bracket is the vector's name, which can be a letter, a number, or a whole word. The symbol $|\psi\rangle$ denotes a vector, just as in school mathematics we might denote a vector by $\vec{\psi}$. The difference is in the notation, not in the rules for addition and multiplication by a number.

The most important vectors in the plane are the two unit vectors along the axes, perpendicular to one another. We call them $|0\rangle$ and $|1\rangle$:

$$|0\rangle = (1,0), \qquad |1\rangle = (0,1).$$

Take care: $|0\rangle$ is not the zero vector. It is the unit vector along the first axis, named "0." We write the zero vector simply as 0.

Every vector in the plane can be built from these two:

$$|\psi\rangle = (a,b) = a\,|0\rangle + b\,|1\rangle \tag{2.1}$$

That is why we say that $|0\rangle$ and $|1\rangle$ form a **basis** for the plane. A vector with N components has a basis of N unit vectors, one along each axis. We label the axes by i, write the basis vectors as $|i\rangle$, and denote the component of $|\psi\rangle$ along axis i by a_i.

Let us see what this mathematical description means in quantum mechanics. Choose a measurement with N possible **outcomes**. We associate a basis vector $|i\rangle$ with each outcome i; different outcomes correspond to different, mutually perpendicular basis vectors. In this chosen basis we represent states and calculate outcome probabilities. The simplest example is a **qubit**: for measurement in the basis $|0\rangle$, $|1\rangle$, the possible outcomes are 0 and 1.

2.2 Superposition and Amplitudes

The state of a system need not be a single basis vector. It can be a sum of basis vectors, each multiplied by its own number:

$$|\psi\rangle = \sum_i a_i \, |i\rangle \tag{2.2}$$

Here $\sum_i$ denotes a sum over all N outcomes. A state that is a sum of several basis vectors is a **superposition** of those vectors: it has more than one nonzero amplitude in the chosen basis. For example, $(|0\rangle + |1\rangle)/\sqrt{2}$ is a superposition of $|0\rangle$ and $|1\rangle$.

Rule 1: we represent a pure quantum state by a unit vector. In our real-valued model, this means $|\psi\rangle = \sum_i a_i|i\rangle$ with $\sum_i a_i^2 = 1$. The components a_i, the numbers in front of the basis vectors, are called **amplitudes**. We will see why the vector must be a unit vector in §2.3.

A qubit state is $a|0\rangle + b|1\rangle$ with $a^2 + b^2 = 1$: a unit vector in the plane, an arrow from the origin to the unit circle (Figure 2.1a).

Amplitudes are not probabilities. A probability is a number between 0 and 1, whereas an amplitude can be **negative**. In general, amplitudes are complex numbers. In our description they are all real. We will see that differences in the signs of amplitudes and their interference are key to how Grover's algorithm works.

2.3 Measurement and Probabilities

Measurement is the most important—and most unusual—part of the story. A quantum state can be a superposition of several basis states, but one measurement in a chosen basis gives only **one** outcome. We do not directly obtain a list of all amplitudes; we obtain a single measurement result.

Rule 2: measurement outcome probabilities are determined by the squares of the amplitudes. Measuring $|\psi\rangle$ yields outcome i with probability

$$P(i) = a_i^2 \tag{2.3}$$

This form of the rule applies to real amplitudes; in general, $P(i) = |a_i|^2$. If we prepare the same state many times and repeat the same measurement, the fraction of trials yielding outcome i approaches its probability $P(i)$. All probabilities must add up to 1, so $\sum_i a_i^2 = 1$: by the Pythagorean theorem, the state is a unit vector. That is why Rule 1 requires unit vectors.

For example, measuring a qubit in the state $0.6\,|0\rangle + 0.8\,|1\rangle$ gives 0 with probability 0.36 and 1 with probability 0.64; the probabilities sum to 1. If we describe the qubit's state arrow by the angle φ it makes with $|0\rangle$, then $|\psi\rangle = \cos\varphi\,|0\rangle + \sin\varphi\,|1\rangle$, so $P(0) = \cos^2\varphi$ and $P(1) = \sin^2\varphi$: the closer the arrow is to the $|1\rangle$ axis, the more likely outcome 1 is (Figure 2.1a). We will return to this picture in Grover's algorithm, where the success probability will be the square of the sine of an arrow's angle.

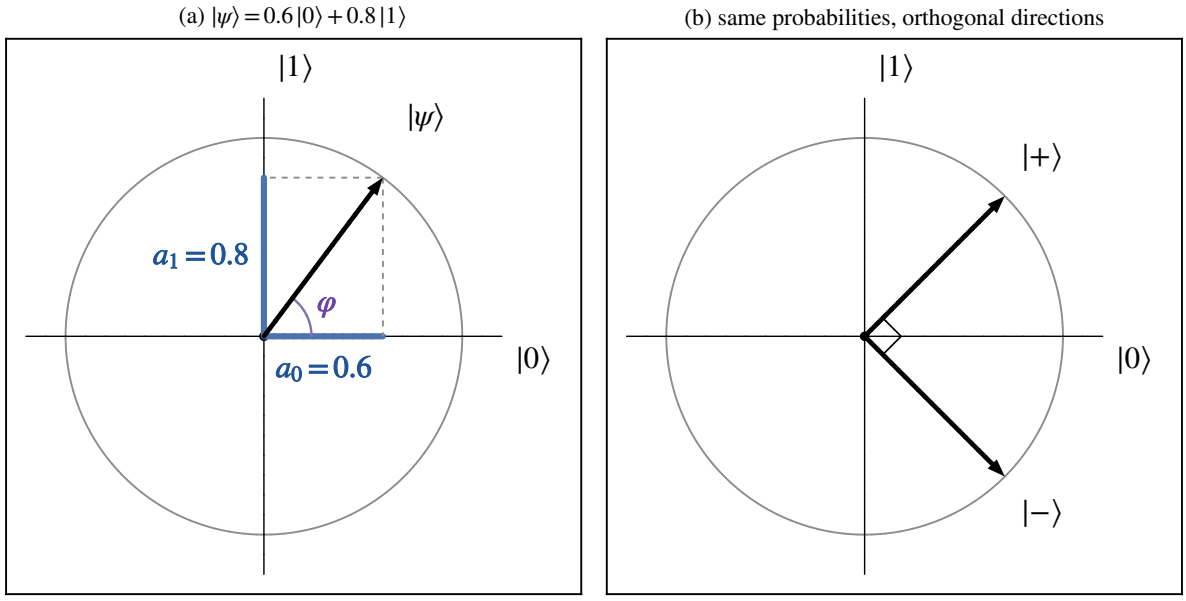


Figure 2.1. (a) A qubit state as an arrow. Its amplitudes are the arrow's projections onto the axes, $a_0 = 0.6$ and $a_1 = 0.8$, so measurement gives 0 with probability 0.36 and 1 with probability 0.64. (b) The states $|+\rangle$ and $|-\rangle$ from §2.6 give the same probabilities, 1/2 and 1/2, yet are perpendicular to each other.

Collapse. If an ideal measurement in the chosen basis yields outcome i, the state after measurement becomes $|i\rangle$: we say the state has **collapsed** to that basis vector. If we immediately repeat the same measurement without an intervening operation, we again obtain outcome i. We cannot read the amplitudes from a single measurement: it gives only one outcome. To estimate a_i^2, we would have to prepare the same state many times and measure it repeatedly. Figure 2.2 shows one state with eight outcomes.

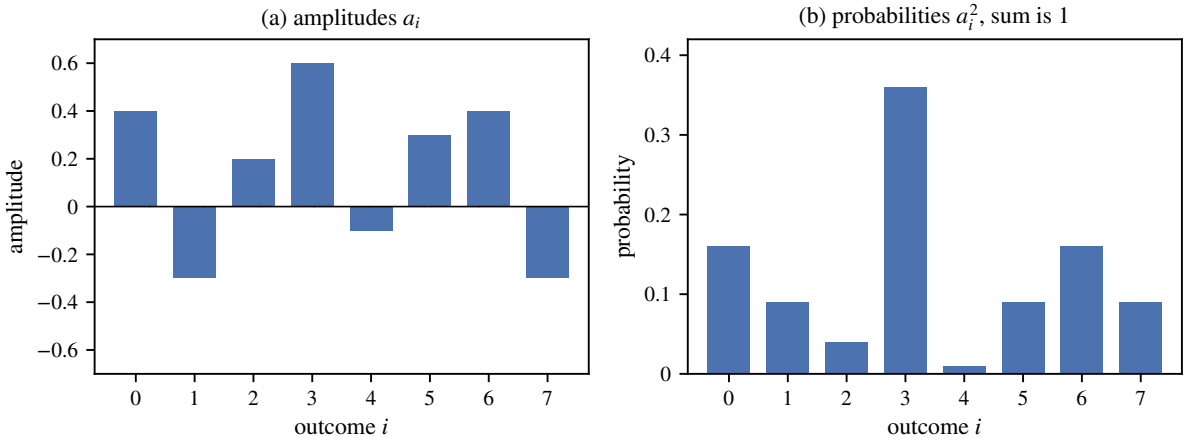


Figure 2.2. A state with eight outcomes. (a) Amplitudes can be negative. (b) Probabilities are the squares of the amplitudes and sum to 1.

Global and relative signs. The vectors $|\psi\rangle$ and $-|\psi\rangle$ represent the same physical state: changing the signs of all amplitudes does not affect the outcomes of any measurement. If, however, we change the sign of only one amplitude, we can obtain a physically different state. Such a change leaves measurement probabilities in the same basis unchanged, but can affect the result after an appropriate quantum operation. We will see an example in §2.6. In quantum mechanics generally, one speaks of global and relative phase.

2.4 Multiple Qubits

When each of n qubits is measured in the basis $|0\rangle$, $|1\rangle$, the outcome is a string of n bits; there are 2^n such outcomes. For two qubits the outcomes are 00, 01, 10 and 11. We can also read a bit string as a number written in binary: $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$ are $|0\rangle$, $|1\rangle$, $|2\rangle$ and $|3\rangle$. A two-qubit state is therefore a vector with four amplitudes:

$$a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle.$$

How do we combine qubits? Suppose two qubits are independently prepared, the first in $a|0\rangle + b|1\rangle$ and the second in $c|0\rangle + d|1\rangle$. Their joint state is the **tensor product** of those states, written with the symbol $\otimes$. We calculate it like a product of two brackets: multiply every term by every other term and join the kets, $|0\rangle \otimes |1\rangle = |01\rangle$:

$$\big(a|0\rangle + b|1\rangle\big) \otimes \big(c|0\rangle + d|1\rangle\big) = ac\,|00\rangle + ad\,|01\rangle + bc\,|10\rangle + bd\,|11\rangle \tag{2.4}$$

The order matters: the first ket supplies the first bit. The product of two unit vectors is a unit vector because $(ac)^2 + (ad)^2 + (bc)^2 + (bd)^2 = (a^2 + b^2)(c^2 + d^2) = 1$.

Entanglement. Not every state of two qubits can be written as a product of the states of the individual qubits. For example, $(|00\rangle + |11\rangle)/\sqrt{2}$ is not such a product: for both ac and bd in (2.4) to be nonzero, a, b, c and d would all have to be nonzero, so neither ad nor bc could be zero. Such states are called **quantum-entangled states**. In §2.8 we will see how gates can produce them.

The number of outcomes grows very quickly. Twenty qubits have $2^{20} = 1\,048\,576$ outcomes, more than a million. Three hundred qubits have $2^{300} \approx 2 \cdot 10^{90}$ outcomes, more than the roughly 10^{80} atoms in the observable universe. The state of n qubits is a vector of $N = 2^n$ amplitudes. A single measurement, however, does not reveal all those numbers: it gives only one outcome. Quantum operations can change the amplitudes and thereby increase the probability of a desired result.

2.5 Operators and Unitarity

A quantum computer changes its state step by step. We can describe a gate by an **operator**: a rule U that assigns a new vector $U|\psi\rangle$ to each vector $|\psi\rangle$. We call $U|\psi\rangle$ the **image** of $|\psi\rangle$. The operators describing these gates are **linear**: the image of a sum of vectors is the sum of their images, and the image of a vector multiplied by a number is its image multiplied by the same number. Therefore it is enough to know what the operator does to the basis vectors:

$$U\Big(\sum_i a_i|i\rangle\Big) = \sum_i a_i\, U|i\rangle.$$

We enter the images of the basis vectors in a table of numbers, a **matrix**: column i of the matrix contains the components of $U|i\rangle$. The operator acts on a vector by multiplying the matrix by the column of vector components: component j of the image is the sum of the products of the entries in row j and the corresponding vector components. An example appears in §2.6.

Rule 3: the quantum gates we consider are described by unitary operators. They are linear and preserve the length of every vector. Thus they turn a unit state into another unit state, and the probabilities continue to add up to 1. In our real model these are orthogonal transformations: **rotations** and **reflections** in a plane, and their generalizations in higher dimensions. In §2.9 we will see that they also preserve angles.

Measurement is a different process: the change of state after measurement is not described by a single unitary gate.

A unitary step never maps two different vectors to the same one. If $U|\varphi\rangle = U|\psi\rangle$, then $U\big(|\varphi\rangle - |\psi\rangle\big)$ would be the zero vector, with length 0. The step preserves lengths, so $|\varphi\rangle - |\psi\rangle$ would also have length 0; hence $|\varphi\rangle = |\psi\rangle$. Every unitary step therefore has an inverse operation that restores the initial state: **unitary gates are reversible**. This will matter in §3.6. By linearity, $|\psi\rangle$ and $-|\psi\rangle$ still differ only by a global sign after any sequence of unitary steps.

2.6 Quantum Circuits and the X and H Gates

We call the unitary steps of a quantum computer **quantum gates**, and a sequence of gates a **quantum circuit**. We draw a circuit as follows (Figure 2.3):

- Each horizontal line represents one qubit.
- Time flows from left to right: the input state is written on the left and the output state on the right.
- A square containing a letter on a line is a gate acting on that qubit.

The X gate is the quantum version of logical NOT: it takes $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $|0\rangle$. Here are its matrix and its action on $a|0\rangle + b|1\rangle$:

$$\mathrm{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 0 \cdot a + 1 \cdot b \\ 1 \cdot a + 0 \cdot b \end{pmatrix} = \begin{pmatrix} b \\ a \end{pmatrix}.$$

The two amplitudes exchange places.

The **Hadamard gate** H takes the basis states $|0\rangle$ and $|1\rangle$ to equal superpositions of them:

$$\mathrm{H}|0\rangle = |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \qquad \mathrm{H}|1\rangle = |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}, \qquad \mathrm{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{2.5}$$

The factor $1/\sqrt{2}$ preserves length: both states are unit vectors, and measuring either yields 0 and 1 with probability $(1/\sqrt{2})^2 = 1/2$ each. The states $|+\rangle$ and $|-\rangle$ therefore give the same probabilities. They differ only in the sign of one amplitude, that of outcome 1.

Applying H twice. What happens if we apply H to $|+\rangle$ again? The gate is linear, so it acts on each term separately:

$$\mathrm{H}|+\rangle = \frac{\mathrm{H}|0\rangle + \mathrm{H}|1\rangle}{\sqrt{2}} = \frac{1}{2}\big(|0\rangle + |1\rangle\big) + \frac{1}{2}\big(|0\rangle - |1\rangle\big) = |0\rangle.$$

The contributions to the amplitude of outcome 0 added, $1/2 + 1/2 = 1$, while those for outcome 1 canceled, $1/2 - 1/2 = 0$. Contributions to the same amplitude add when they have the same sign; with opposite signs they can cancel partly or completely. This is **interference**; water waves behave similarly. For $|-\rangle$ the reverse happens: the contributions for outcome 0 cancel, while those for outcome 1 add:

$$\mathrm{H}|-\rangle = \frac{\mathrm{H}|0\rangle - \mathrm{H}|1\rangle}{\sqrt{2}} = \frac{1}{2}\big(|0\rangle + |1\rangle\big) - \frac{1}{2}\big(|0\rangle - |1\rangle\big) = |1\rangle.$$

Thus:

$$|0\rangle \xrightarrow{\text{H}} |+\rangle \xrightarrow{\text{H}} |0\rangle, \qquad |1\rangle \xrightarrow{\text{H}} |-\rangle \xrightarrow{\text{H}} |1\rangle \tag{2.6}$$

Applying H twice restores the initial state (Figure 2.3c). Consider what happened. Measurement in the basis $|0\rangle$, $|1\rangle$ does not distinguish $|+\rangle$ from $|-\rangle$: both yield 0 and 1 with equal probability. After the H gate, the first certainly yields 0 and the second certainly yields 1. **The relative sign of amplitudes can affect measurement probabilities after a suitable quantum operation.** Here H turns a difference in sign into a difference between two certain outcomes.

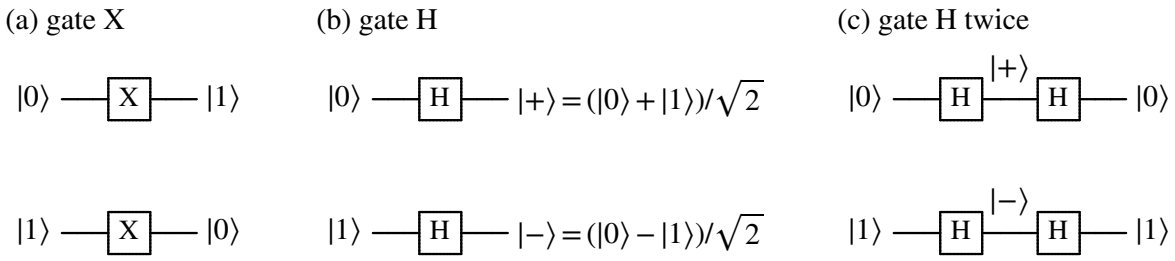


Figure 2.3. Single-qubit circuits: the line is the qubit, time flows from left to right, the input state is on the left and the output on the right. (a) X exchanges $|0\rangle$ and $|1\rangle$. (b) H turns $|0\rangle$ into $|+\rangle$ and $|1\rangle$ into $|-\rangle$. (c) A second H gate restores the initial state.

2.7 Hadamard Gates on Multiple Qubits

Take three qubits, each in $|0\rangle$, and put an H gate on each (Figure 2.4). Gates aligned vertically act in the same step; we call them a **layer**. Each qubit comes out in $|+\rangle$, and the state of all three is their tensor product, as in (2.4):

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{8}}\big(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle\big).$$

We choose one term from each bracket in all $2 \cdot 2 \cdot 2 = 8$ ways, and each product has the factor $(1/\sqrt{2})^3 = 1/\sqrt{8}$. The binary strings are the numbers from 0 to 7, so the result is $\big(|0\rangle+|1\rangle+\cdots+|7\rangle\big)/\sqrt{8}$: **all amplitudes are equal**.

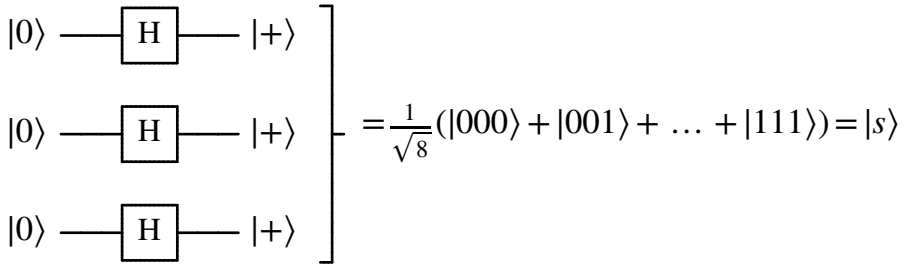


Figure 2.4. A layer of H gates on three qubits. Each qubit comes out in $|+\rangle$, and all three together in $|s\rangle$, where all eight outcomes have the same amplitude, $1/\sqrt{8}$.

The same holds for any n. A layer of n Hadamard gates takes $|0 \dots 0\rangle$ to

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle = \frac{1}{\sqrt{N}} (1, 1, \dots, 1), \qquad N = 2^n \tag{2.7}$$

in which all N outcomes have the same amplitude, $1/\sqrt{N}$. It is a unit vector because the sum of squared amplitudes is $N \cdot (1/N) = 1$. The letter s comes from *superposition*: $|s\rangle$ is the **uniform superposition** of all outcomes. Preparing it requires n Hadamard gates, one on each qubit. Since they act on different qubits, they can be applied in a single layer.

If we measured $|s\rangle$ immediately, each of the N outcomes would have the same probability, $1/N$. This does not help us pick out the desired element: the result is just as random as a random choice.

2.8 Controlled Quantum Gates: CNOT and CZ

A single-qubit gate does not connect qubits. For computation we also need **controlled gates** acting on two or more qubits. Their action is easiest to describe on basis states: if the control qubit is $|0\rangle$, the target operation is not applied; if it is $|1\rangle$, the operation is applied to the target qubit.

Crucially, the control qubit is **not measured**. If it is in superposition, the gate acts linearly on all components of the joint state.

The best-known such gate is CNOT, controlled NOT. We draw it as a dot on the **control** qubit and an $\oplus$ on the **target** qubit, joined by a vertical line (Figure 2.5a). If the control bit is 0, the gate does nothing; if it is 1, the gate applies X to the target. The single-qubit Z gate leaves $|0\rangle$ unchanged and takes $|1\rangle$ to $-|1\rangle$. Thus CZ, controlled Z, changes only the sign of the amplitude of outcome 11; we draw it with a dot on the control and a Z square on the target (Figure 2.5b). The **truth table**, Table 2.1, shows what both gates do to basis vectors. By linearity, they act on a superposition term by term. Both merely move amplitudes or change their signs, so they preserve lengths and are allowed steps.

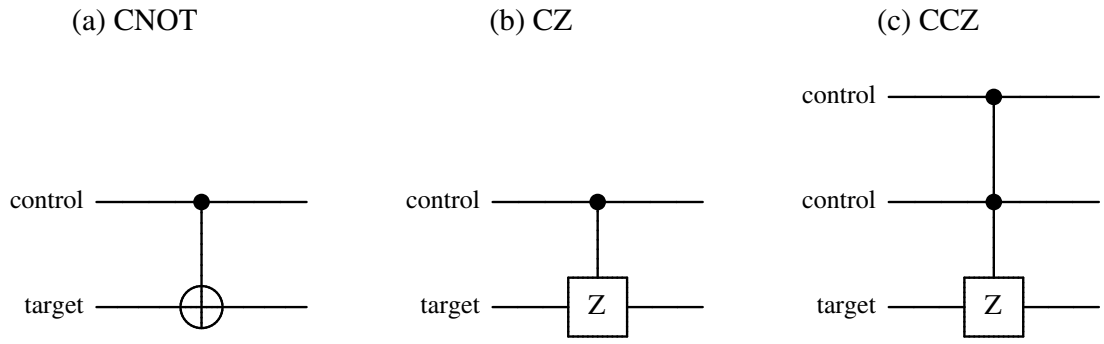


Figure 2.5. Controlled gates; the dot denotes a control qubit. (a) CNOT: if the control bit is 1, the target bit is flipped. (b) CZ: the amplitude changes sign if both bits are 1. (c) CCZ: the sign changes only if all three bits are 1.

Input	CNOT	CZ
$\|00\rangle$	$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|11\rangle$	$\|10\rangle$
$\|11\rangle$	$\|10\rangle$	$-\|11\rangle$

Table 2.1. CNOT and CZ on the four basis vectors of two qubits, with the first qubit as control. CNOT flips the second bit if the first is 1, while CZ changes the sign if both bits are 1.

For example, start from $|00\rangle$. Apply H to the first qubit, then CNOT with the first qubit as control:

$$|00\rangle \xrightarrow{\mathrm{H}\otimes\mathbb{1}} \frac{|00\rangle + |10\rangle}{\sqrt{2}} \xrightarrow{\text{CNOT}} \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

We have obtained the entangled state from §2.4, even though the qubits were independently prepared at the start.

There can also be more than one control qubit. For basis states the target gate is then applied only if **all** control bits are 1. In this way gates implement a check of the form "if the first bit is 1 **and** the second bit is 1 **and** …". For example, CCZ has two controls and one target and changes the sign only of the amplitude of $|111\rangle$ (Figure 2.5c). We will need such gates in Grover's algorithm.

2.9 Inner Products, Bras and Projectors

One final piece of our toolkit remains. You may already have encountered the scalar product at school; let us start from the beginning. In our model, where components are real, the **inner product** of $|\varphi\rangle = \sum_i b_i|i\rangle$ and $|\psi\rangle = \sum_i a_i|i\rangle$ is obtained by multiplying corresponding components and adding the products. Dirac writes it as $\langle\varphi|\psi\rangle$, read "bra phi, ket psi":

$$\langle\varphi|\psi\rangle = \sum_i b_i\, a_i.$$

In the general complex case, the components of the first vector are complex-conjugated: $\langle\varphi|\psi\rangle = \sum_i b_i^* a_i$.

The left half, $\langle\varphi|$, is called a **bra**. A bra and a ket together make a *bracket*, which is the origin of both names. In our real model, we can think of a ket as a column of components and the corresponding bra as a row of the same components; the inner product is then the row multiplied by the column. We write the length of $|\psi\rangle$ as $\|\psi\|$, with two vertical bars on each side. At school you may have written the magnitude of $\vec{a}$ with single bars, $|\vec{a}|$; here we use two because the ket itself already contains a vertical bar. By the Pythagorean theorem, $\|\psi\|^2 = \sum_i a_i^2 = \langle\psi|\psi\rangle$.

The inner product also has a geometric meaning that we will need throughout. Two nonzero, non-parallel vectors $|\varphi\rangle$ and $|\psi\rangle$ **span** a plane: the set of all vectors of the form $\lambda|\varphi\rangle + \mu|\psi\rangle$. Ordinary geometry applies in that plane.

Consider the triangle whose vertices are the origin and the tips of the two vectors. Its sides have lengths $\|\varphi\|$, $\|\psi\|$ and $\|\varphi - \psi\|$; call the angle between the first two γ. Drop a perpendicular from the tip of $|\psi\rangle$ to the line through $|\varphi\rangle$: the signed coordinate of its foot is $\|\psi\|\cos\gamma$ and the perpendicular's length is $\|\psi\|\sin\gamma$. If the angle is obtuse, the foot lies on the other side of the origin, $\cos\gamma$ is negative, and the calculation still holds. By the Pythagorean theorem,

$$\|\varphi - \psi\|^2 = \big(\|\varphi\| - \|\psi\|\cos\gamma\big)^2 + \big(\|\psi\|\sin\gamma\big)^2 = \|\varphi\|^2 + \|\psi\|^2 - 2\,\|\varphi\|\,\|\psi\|\cos\gamma,$$

because $\cos^2\gamma + \sin^2\gamma = 1$. This is the law of cosines, familiar from school. On the other hand, calculating component by component gives

$$\|\varphi - \psi\|^2 = \sum_i (b_i - a_i)^2 = \sum_i b_i^2 + \sum_i a_i^2 - 2\sum_i b_i a_i.$$

Comparing the two expressions gives

$$\langle\varphi|\psi\rangle = \sum_i b_i\, a_i = \|\varphi\|\,\|\psi\|\cos\gamma \tag{2.8}$$

that is, the inner product is the product of the lengths of the vectors and the cosine of the angle between them. The same relation holds for parallel nonzero vectors with angle 0° or 180°; if either vector is zero, both sides are zero and no angle needs to be specified. In the plane this is the familiar dot product.

We will repeatedly use three properties of the inner product.

Length. The inner product of a vector with itself is the square of its length, $\langle\psi|\psi\rangle = \|\psi\|^2$, so a vector is a unit vector if $\langle\psi|\psi\rangle = 1$.

Components. Basis vectors are unit vectors and mutually perpendicular: $\langle i|i\rangle = 1$, while for two different **basis** vectors $|i\rangle$ and $|i'\rangle$, $\langle i|i'\rangle = 0$. Take care: this is true of basis vectors, not of every pair of different states. For example, $\langle 0|+\rangle = 1/\sqrt{2}$, whereas $\langle +|-\rangle = \big(1\cdot 1 + 1\cdot(-1)\big)/2 = 0$: $|+\rangle$ and $|-\rangle$ give the same probabilities but are perpendicular (Figure 2.1b). Taking the inner product with a basis vector extracts one component:

$$\langle i|\psi\rangle = a_i \tag{2.9}$$

so Rule 2 can also be written $P(i) = \langle i|\psi\rangle^2$.

Rules of calculation. In our real model the inner product is symmetric, $\langle\varphi|\psi\rangle = \langle\psi|\varphi\rangle$, and can be calculated term by term: $\langle\varphi|\big(\lambda|\psi\rangle + \mu|\chi\rangle\big) = \lambda\langle\varphi|\psi\rangle + \mu\langle\varphi|\chi\rangle$. In the complex case, $\langle\varphi|\psi\rangle = \langle\psi|\varphi\rangle^*$.

The meaning of the inner product is easiest to see when one vector is a unit vector. If $|u\rangle$ is a unit vector, (2.8) gives $\langle u|\psi\rangle = \|\psi\|\cos\gamma$. This is the signed length of the shadow cast by $|\psi\rangle$ onto the line through $|u\rangle$, negative if the shadow falls in the direction opposite $|u\rangle$. The component $a_i = \langle i|\psi\rangle$ is just such a shadow, on axis i (Figure 2.1a).

Unitary steps also preserve angles. In our real model the inner product can be expressed in terms of lengths:

$$\langle\varphi|\psi\rangle = \frac{\|\varphi+\psi\|^2 - \|\varphi-\psi\|^2}{4}.$$

This follows from $\|\varphi\pm\psi\|^2 = \|\varphi\|^2 \pm 2\langle\varphi|\psi\rangle + \|\psi\|^2$, obtained term by term. A linear step that preserves lengths (§2.5) therefore preserves inner products, and hence angles.

Projector. We can also write a ket and a bra in the opposite order, $|u\rangle\langle u|$. This is no longer a number, but an operator: it waits for a vector on its right. When it acts on $|r\rangle$, the pair on the right becomes an inner product:

$$\big(|u\rangle\langle u|\big)\,|r\rangle = |u\rangle\,\langle u|r\rangle = \langle u|r\rangle\,|u\rangle \tag{2.10}$$

Let $|u\rangle$ be a unit vector. Then $\langle u|r\rangle$ is the signed length of the shadow of $|r\rangle$ on the line through $|u\rangle$, so $\langle u|r\rangle\,|u\rangle$ is a vector on that line. We call it the **projection** of $|r\rangle$ onto the line through $|u\rangle$, and the operator $|u\rangle\langle u|$ a **projector**. The projector leaves $|u\rangle$ unchanged because $\langle u|u\rangle = 1$, and maps every vector perpendicular to $|u\rangle$ to zero. Thus a projector does not generally preserve length and is not a unitary gate; here we use it as a mathematical tool. Projectors also play a role in describing measurement.

The remainder, $|r\rangle - \langle u|r\rangle\,|u\rangle$, is perpendicular to the line: its inner product with $|u\rangle$ is $\langle u|r\rangle - \langle u|r\rangle\,\langle u|u\rangle = 0$. Every vector can therefore be split into two parts, one along the line and one perpendicular to it:

$$|r\rangle = \underbrace{\langle u|r\rangle\,|u\rangle}_{\text{along the line}} + \underbrace{\big(|r\rangle - \langle u|r\rangle\,|u\rangle\big)}_{\text{perpendicular to the line}} .$$

Warm-up. Here is how easily we can calculate with a projector. Let $\mathbb{1}$ be the **identity operator**, which changes nothing, $\mathbb{1}|r\rangle = |r\rangle$, and consider $\mathbb{1} - 2|u\rangle\langle u|$. The projector maps a vector perpendicular to $|u\rangle$ to zero, so that vector remains unchanged. The projector leaves $|u\rangle$ unchanged, so

$$\big(\mathbb{1} - 2|u\rangle\langle u|\big)\,|u\rangle = |u\rangle - 2|u\rangle = -|u\rangle.$$

This operator changes the sign of the component along $|u\rangle$ and leaves everything perpendicular to it unchanged. In the plane, it is reflection about the line perpendicular to $|u\rangle$. If $|u\rangle$ is a basis vector, for example $|2\rangle$, the operator changes only the sign of amplitude a_2. Remember this formula: we will meet it again soon.

Key Points from This Chapter

1. Quantum states and superposition. We represent a pure quantum state by a unit vector

$$|\psi\rangle = \sum_i a_i|i\rangle, \qquad \sum_i a_i^2 = 1.$$

The numbers a_i are **amplitudes**. In our model they are real and may be positive or negative. A state with several nonzero amplitudes in a chosen basis is a superposition of basis states.

2. Measurement and probabilities. Measuring in the chosen basis yields one outcome i, with probability

$$P(i) = a_i^2.$$

After an ideal measurement the state becomes $|i\rangle$. Changing the sign of every amplitude does not change the physical state, but **relative signs of amplitudes** can affect the outcomes of later measurements.

3. Systems of multiple qubits. A state of n qubits has $N = 2^n$ amplitudes. We combine independently prepared states using the **tensor product**, but **entangled states** also exist and cannot be written as products of individual-qubit states.

4. Quantum gates. We describe gates by **unitary operators**: they are linear, preserve lengths and angles between vectors, and have inverses. We do not describe measurement by a single unitary gate.

5. The Hadamard gate and interference. The Hadamard gate H takes basis states to superpositions:

$$\mathrm{H}|0\rangle = |+\rangle, \qquad \mathrm{H}|1\rangle = |-\rangle, \qquad \mathrm{H}^2 = \mathbb{1}.$$

During successive quantum operations, contributions to amplitudes can add or cancel. We call this **interference**. Applying the Hadamard gate to each of n qubits prepared in $|0\rangle$ gives the **uniform**

superposition

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle.$$

6. Controlled gates. CNOT, CZ and CCZ act on multiple qubits. Their action depends on the values of the control bits in basis states, but **the control qubits are not measured**. These gates enable conditional operations, including sign changes of selected amplitudes.

7. Inner products, projectors and reflections. The inner product $\langle\varphi|\psi\rangle$ describes the geometric relationship between two vectors, while $P_u = |u\rangle\langle u|$ projects onto the direction of the unit vector $|u\rangle$. From it we can construct the unitary operator

$$R_u = \mathbb{1} - 2|u\rangle\langle u|,$$

which **changes the sign of the component along** $|u\rangle$, leaving all components perpendicular to that direction unchanged.

Key idea: Quantum algorithms use unitary operations to change amplitudes and allow their interference. In Grover's algorithm, two geometric reflections will combine to increase the probability of obtaining the desired outcome progressively.

2.10 Exercises

Exercises for Independent Work

The exercises in this chapter are designed to practice the basic concepts of quantum mechanics and quantum computing. We begin with simpler calculations involving quantum states, amplitudes and measurement probabilities, then move on to systems of multiple qubits, quantum gates and circuits. The final exercises concern inner products, projectors and geometric transformations that we will need to understand Grover's algorithm.

Unless otherwise stated, use real amplitudes and measure in the computational basis.

States, Normalization and Measurement (§2.1–§2.3)

Exercise 21. Find the positive number λ for which $\lambda(|0\rangle + 2|1\rangle)$ is a unit vector. What are the probabilities of outcomes 0 and 1? *Hint: the condition is* $\langle\psi|\psi\rangle = 1$.

Exercise 22. A four-component vector is given by $|r\rangle = (0, -2, 0, 1)$. Normalize it and write the resulting state in ket notation using $|0\rangle$,$|1\rangle$,$|2\rangle$,$|3\rangle$. Find the probabilities of all four outcomes.

Exercise 23. Write the state $|\psi\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ as a pair of components. Check that it is normalized, determine the probabilities of outcomes 0 and 1, and identify which state from §2.6 it is.

Exercise 24. A qubit is prepared in $|\psi\rangle = (\sqrt{3}\,|0\rangle - |1\rangle)/2$. What are the probabilities of outcomes 0 and 1? If the first ideal measurement yields outcome 1, what is the state immediately after measurement and what will a repeated measurement in the same basis yield?

Exercise 25. Compare the states $|\psi\rangle = (\sqrt{3}\,|0\rangle + |1\rangle)/2$, $-|\psi\rangle$ and $\mathrm{Z}|\psi\rangle$. Which two vectors describe the same physical state? What are the probabilities for measurement in the basis $\{|0\rangle,|1\rangle\}$ for all three vectors? *Hint:* $\mathrm{Z}|0\rangle = |0\rangle$ *and* $\mathrm{Z}|1\rangle = -|1\rangle$.

Exercise 26. Show that the states $|+\rangle$ and $|-\rangle$ from (2.5) give the same probabilities and that $\langle+|-\rangle =$

0. Then rotate both by 45° in the positive mathematical direction and show that a subsequent measurement in the basis $\{|0\rangle,|1\rangle\}$ distinguishes them with certainty. *Hint: $|+\rangle$ lies at an angle of* 45° *and $|-\rangle$ at* $-45°$.

Exercise 27. A qubit is prepared in $|0\rangle$. What is the probability of outcome 0 if it is measured in the basis $\{|0\rangle,|1\rangle\}$? What are the probabilities of outcomes + and − if it is measured in the basis $\{|+\rangle,|-\rangle\}$? *Hint: express $|0\rangle$ in terms of $|+\rangle$ and $|-\rangle$.*

Exercise 28. A state of a system with three possible outcomes has amplitudes $(1,-2,2)/3$. Check normalization. What are the probabilities of outcomes 0, 1 and 2? What is the probability of obtaining outcome 1 **or** outcome 2?

Exercise 29. In each trial a qubit is prepared anew in a state that yields outcome 1 with probability 1/4. We repeat preparation and measurement independently three times. What is the probability of obtaining outcome 1 at least once? *Hint: first calculate the probability of never obtaining it.*

Multiple Qubits and Tensor Products (§2.4)

Exercise 30. Expand the tensor product $|+\rangle \otimes |-\rangle$ in the basis $|00\rangle,|01\rangle,|10\rangle,|11\rangle$ and write its four coefficients as an ordered quadruple.

Exercise 31. Two qubits are in the product state $\big(\sqrt{3}\,|0\rangle + |1\rangle\big)/2 \otimes \big(|0\rangle - |1\rangle\big)/\sqrt{2}$. What are the probabilities of outcomes 00 and 11? What is the probability that the **first** measured bit is 1?

Exercise 32. Consider $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$. Which measurement outcomes are possible, and with what probabilities? Can this state be written as a tensor product of states of the two individual qubits?

Exercise 33. How many computational basis states does a three-qubit system have? For a uniform superposition of all three qubits, calculate the probability of outcome 101 and the probability that the first bit is 1.

Operators and Quantum Gates (§2.5–§2.8)

Exercise 34. Calculate $\mathrm{X}(a|0\rangle + b|1\rangle)$ and $\mathrm{X}|-\rangle$. Is the result in the second case physically different from the initial state?

Exercise 35. An operator R has matrix $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Find $R|0\rangle$ and $R|1\rangle$, then check that $R^T R = \mathbb{I}$, where R^T is the transpose (rows and columns exchanged). Which geometric transformation does R represent?

Exercise 36. Show that H takes $(a,b) = a|0\rangle + b|1\rangle$ to $\big((a+b)/\sqrt{2},(a-b)/\sqrt{2}\big)$ and that applying it twice restores any vector (a,b). *Hint: use (2.5) and the linearity of the gate.*

Exercise 37. On one qubit apply H, then X, then H again. Find the result for input states $|0\rangle$ and $|1\rangle$. Which familiar gate does the whole sequence represent?

Exercise 38. Apply H to $(\sqrt{3}\,|0\rangle + |1\rangle)/2$. Find the two output amplitudes and the probabilities of outcomes 0 and 1 after measurement.

Exercise 39. Apply one H gate to each qubit in $|000\rangle$. Write the result as a sum of computational basis states. What is the probability of outcome 101, and what is the probability that the first bit is 1? How many gates and how many layers are needed?

Exercise 40. Start from $|00\rangle$, apply H to the first qubit, then CNOT with the first qubit as control and the second as target. What is the final state, and what measurement outcomes can occur?

Exercise 41. Apply CZ to $(|00\rangle + |01\rangle + |10\rangle + |11\rangle)/2$. Write the new state and the probabilities of all four outcomes of measurement in the computational basis.

Exercise 42. Apply CNOT with the first qubit as control to $(|00\rangle + |01\rangle + |10\rangle - |11\rangle)/2$. Write all four output amplitudes in the order 00,01,10,11.

Exercise 43. Apply CCZ to the uniform superposition of the eight basis states of three qubits. Which amplitude changes sign? Write the output state and the probability of outcome 111.

Inner Products, Projectors and Reflections (§2.9)

Exercise 44. Let $|s\rangle = (1,1,1,1)/2$ and $|\psi\rangle = (1,1,1,-1)/2$. Calculate $\langle s|\psi\rangle$ and the angle between these vectors. *Hint: use (2.8); both vectors are unit vectors.*

Exercise 45. Calculate $\langle +|-\rangle$, $\langle 0|+\rangle$ and $\langle 1|-\rangle$. Which two of these vectors are mutually orthogonal?

Exercise 46. For $|\psi\rangle = (3|0\rangle + 4|1\rangle)/5$ and $P_0 = |0\rangle\langle 0|$, calculate $P_0|\psi\rangle$ and the remainder $|\psi\rangle - P_0|\psi\rangle$. What is the squared length of the projection?

Exercise 47. Let $P_+ = |+\rangle\langle +|$. Calculate $P_+|0\rangle$ in the basis $\{|0\rangle,|1\rangle\}$ and the squared length of the resulting vector. *Hint: first find* $\langle +|0\rangle$.

Exercise 48. Let $F = \mathbb{I} - 2|+\rangle\langle +|$. Calculate $F|+\rangle$, $F|-\rangle$ and $F|0\rangle$. Which unitary gate is F equal to, up to a possible global sign?

Exercise 49. In four-dimensional space let $|s\rangle = (1,1,1,1)/2$ and $|r\rangle = (1,1,1,-1)/2$. Calculate $D|r\rangle$ for $D = 2|s\rangle\langle s| - \mathbb{I}$. Which measurement result is obtained with certainty? *We will encounter this operator again in the third chapter.*

For the Curious: A First Step Toward Complex Amplitudes

Exercise 50. In general, amplitudes can be complex. Let $i^2 = -1$ and suppose a complex amplitude obeys $P = |a|^2$, with $|1 + i|^2 = |1 - i|^2 = 2$. Compare measurement of $|\psi\rangle = (|0\rangle + i|1\rangle)/\sqrt{2}$ and $|+\rangle$ in the basis $\{|0\rangle,|1\rangle\}$. Then apply H to both states and calculate the measurement probabilities again. *This exercise is optional and is not required for the rest of the handout.*

3. Grover's Algorithm

Now that we know the basic language of quantum states and gates, we can turn to search. We will first compare classical and quantum approaches, then formulate the problem precisely. We will see why the oracle alone is not enough, how diffusion amplifies the amplitude of the sought state, and why the entire algorithm reduces to a sequence of rotations in a plane.

3.1 What Is Quantum Search?

Grover's algorithm is a **quantum search algorithm** [5]. Its goal is to find, among many possibilities, the one that satisfies a given condition, using the rules of quantum mechanics.

Consider a simple example. Imagine the numbers from 0 to 99, exactly one of which is the solution to a problem [6]. We do not know which one. All we can do is check: for each number we can ask "are you the solution?" and obtain a yes-or-no answer. We must find that one number. We will call it the **sought (marked) element** and write it as w. In this example we assume there is exactly one solution. Later we will represent the possibilities by basis states of a quantum register: for n qubits there are $N = 2^n$ such states; the example with 100 numbers is only an introductory illustration.

3.2 How Many Checks Are Needed?

How would we search without a quantum computer? If we know nothing about the possibilities, if they are not ordered, and if there are no "warmer, colder" hints, we can do no better than check them one at a time. This is called **unstructured search**. An everyday example is a four-digit combination lock: there are $N = 10\,000$ possible combinations, and the only way to check one is to try it and see whether the lock opens.

Sometimes we succeed on the first try, sometimes only on the last. Each position in the sequence is equally likely, so if we check in order without repetition, the average number of checks is $(1 + 2 + \cdots + N)/N = (N + 1)/2$, approximately half the possibilities:

$$\text{classically: an average of } \frac{N+1}{2} \text{ checks} \tag{3.1}$$

If the number of possibilities doubles, so does the amount of work.

Grover's algorithm finds w with high probability using far fewer queries to a quantum checker:

$$\text{Grover's algorithm: the number of queries is proportional to } \sqrt{N} \tag{3.2}$$

If the number of possibilities quadruples, only twice as many checks are needed. For $N = 10\,000$, that is on the order of 100 checks rather than about 5,000; for a million possibilities, on the order of a thousand rather than half a million. We will calculate the precise number, including the constant factor before the square root, in §3.13. The number of queries is not the same as running time: actual running time also depends on the complexity of each check, the other gates, and the device on which the circuit runs.

The square root is not new. In Chapter 1, the number of collisions grew as $\sqrt{M/m}$, according to (1.11). We will see in Chapter 4 that this is no coincidence.

3.3 Algorithmic Complexity

Without saying so, we have just begun to discuss **algorithmic complexity**. When comparing the complexity of algorithms, we do not start with their running time in seconds, because that depends on the computer. We ask a different question: **how does the number of steps grow as the problem size N grows?** We express the answer with a capital O. The notation $O(N)$ denotes an asymptotic upper bound: for sufficiently large N, the number of steps is at most a constant multiple of N. If we want to emphasize that it grows at precisely that order, bounded both above and below, we write $\Theta(N)$. We omit constant factors: classical search, with about $N/2$ checks, has complexity $O(N)$, while Grover's algorithm has complexity $O(\sqrt{N})$. Table 3.1 gives several examples.

Complexity	**Example**	**For $N = 10^6$**
$O(1)$, constant	Is a number with N digits even? With direct access to its last digit, we only need to inspect that digit.	1 step
$O(\log N)$, logarithmic	Guessing a number between 1 and N with "higher" and "lower" answers: each question halves the possibilities. This is also how we look up a word in a dictionary.	about 20 questions
$O(\sqrt{N})$, square-root	Grover's algorithm.	on the order of 1,000 checks
$O(N)$, linear	Checking N possibilities one by one, as with the lock.	about 500,000 checks
$O(N^2)$, quadratic	Each of N students shakes hands with every other student: $N(N-1)/2$ handshakes.	about 500 billion
$O(2^N)$, exponential	Trying every configuration of N switches: each additional switch doubles the number of possibilities.	a number with more than 300,000 digits

Table 3.1. Complexity of several procedures. In each row N is the size of the task: the number of digits, numbers, possibilities, students or switches.

We should note a distinction. The complexity in Table 3.1 is a property of an **algorithm**. One problem can have several algorithms of different complexity: for unstructured search, checking in sequence has complexity $O(N)$, while Grover's algorithm has complexity $O(\sqrt{N})$. **Complexity classes**, another much-discussed idea, group **problems** by what a particular kind of computer can do with them quickly: solve them or at least verify their solutions. The two best known are called P and NP. The class P contains decision problems that an ordinary computer can **solve** quickly; NP contains decision problems for which every yes answer can be **verified** quickly using a suitable certificate. Examples include decision versions of generalized Sudoku and three-color map coloring: we ask whether a given instance has a valid solution. If a solution is shown to us, we can check it in a polynomial number of steps [10]. Whether every problem in NP is also in P is the greatest open question in computer science.

Here "quickly" has a precise meaning: the number of steps grows no faster than some power of the **length of the input**, such as n^2 or n^3, where n is the number of digits. There is a subtlety. If a candidate solution is a string of n bits, there are $N = 2^n$ possibilities. Checking them in sequence

then costs $O(N) = O(2^n)$ steps: linear in N but exponential in n, as in the last row of Table 3.1, where N was the number of switches. Grover's algorithm reduces this to $O(\sqrt{N}) = O(2^{n/2})$. The saving is enormous, but this is still exponential in n. Thus a quadratic saving in queries does not by itself turn exponential growth into polynomial growth. Not every problem is an unstructured search, and the actual cost also depends on how the check is implemented.

Where we are going. We have a checker that tells us, for each of N possibilities, whether it is the one sought. In the previous chapter we learned about quantum states, amplitudes, measurement and gates. We can now formulate the search precisely and show how a quantum computer uses two reflections to reach a solution after on the order of $\sqrt{N}$ queries.

3.4 Formulating the Search Problem

We can now state the problem precisely in the language of quantum mechanics.

- **Possibilities.** The computer has n qubits and therefore $N = 2^n$ basis states, $|0\rangle, |1\rangle, \ldots, |N-1\rangle$, with the numbers written in binary. Each basis state is one possibility.
- **Solution.** One of them, $|w\rangle$, is the solution. We do not know which one.
- **Check.** We have a check f that says whether each possibility i is a solution: $f(i) = 1$ if $i = w$, and $f(i) = 0$ otherwise. The function f is a classical rule for checking. We call the corresponding unitary quantum circuit the **oracle**, and each application of that circuit a **query**.
- **Goal.** We start from the state $|0 \ldots 0\rangle$ and may use gates. We want a final measurement to yield w with probability close to 1, using as few queries as possible: about $\sqrt{N}$ rather than about $N/2$. We do not count gates that do not query the oracle, such as a layer of H gates; we count only queries.

3.5 What Does the Oracle Know?

How can we construct a procedure that recognizes a solution when we do not know the solution itself? The key is that **checking a solution does not necessarily require knowing it in advance**.

Imagine a given Sudoku puzzle and a proposed filling of the entire grid. We can check whether the originally given numbers have been preserved and whether the numbers 1 through 9 appear without repetition in every row, column and 3×3 square. This check requires the given grid and the rules, not a previously discovered correct filling. In principle, we can build a reversible quantum circuit from such a check. In a concrete application we must also account for the cost of the gates and auxiliary qubits needed for the check.

Another example is a hash function: given an input, we calculate its hash and compare it with a specified value, without knowing in advance an input that produces that value. There may be more than one such input or none at all; in the main derivation, however, we assume exactly one marked solution.

In theoretical analysis we often use a **black-box model**: the algorithm may apply the oracle, but does not use its internal construction. In this model we compare numbers of queries. If the construction is known, it may reveal additional structure that a classical algorithm can exploit too; a saving in query count alone does not guarantee a speedup in actual running time.

In simple teaching examples we sometimes deliberately construct a check for an answer known in advance. In §3.17 we will construct a circuit that marks 11: since we chose that answer ourselves, the example does not find an unknown solution, but shows how the algorithm works. The description

of such a circuit reveals what is marked, whereas knowing the rules of a Sudoku check does not mean we already know the solved grid.

Thus, we describe an oracle by **what it does to a candidate presented to it**. We can construct it from the conditions a solution must satisfy, without first finding a solution; in a demonstration we can also deliberately build in a known answer.

3.6 Why Does the Oracle Change a Sign?

A classical check is a function: it assigns a bit $f(i)$, either 0 or 1, to each possibility i. Can a quantum computer do the same, converting the state $|i\rangle$ into the one-qubit state $|f(i)\rangle$, either $|0\rangle$ or $|1\rangle$? It cannot when $N \geq 3$. That operation would merge all $N-1$ incorrect possibilities—$N-1$ distinct basis vectors—into the same vector $|0\rangle$. As explained in §2.5, a unitary operation never merges distinct states: $|0\rangle$ would no longer show which possibility it came from, and the operation could not be undone.

The quantum oracle therefore does not replace a possibility with the answer. Two methods are allowed, both leaving the possibility in place: the answer can be written into an additional qubit, or into a **sign**. Grover's algorithm uses the sign: every basis vector stays in place, and the answer is written into its sign:

$$U_w|i\rangle = (-1)^{f(i)}\,|i\rangle \tag{3.3}$$

That is, $U_w|w\rangle = -|w\rangle$, while $U_w|i\rangle = |i\rangle$ for $i \neq w$. In terms of amplitudes, this is

$$a_w \longmapsto -a_w, \qquad a_i \longmapsto a_i \quad \text{for } i \neq w.$$

This is an allowed operation. The operator is linear, and changing the sign of one amplitude preserves the sum of the squares of all amplitudes and therefore the state's length; no two states are merged; applying the oracle twice returns everything to the start. In the notation of §2.9, this is the reflection operator we encountered in the previous chapter, with $|u\rangle = |w\rangle$:

$$U_w = \mathbb{1} - 2|w\rangle\langle w| \tag{3.4}$$

In (3.4), w denotes the unique candidate that passes the check. This notation describes the **action** of the oracle; it does not require us to know w in advance or to construct the circuit by comparing with it. If a Sudoku check has one solution, its phase oracle has exactly this mathematical form even when the solution is unknown to us.

Let us calculate that (3.4) does the same thing as (3.3). Apply U_w to the marked basis vector $|w\rangle$:

$$U_w|w\rangle = |w\rangle - 2|w\rangle\langle w|w\rangle = |w\rangle - 2|w\rangle = -|w\rangle,$$

because $\langle w|w\rangle = 1$. Now apply it to any other basis vector $|i\rangle$, with $i \neq w$:

$$U_w|i\rangle = |i\rangle - 2|w\rangle\langle w|i\rangle = |i\rangle - 0 = |i\rangle,$$

because distinct basis vectors are orthogonal, $\langle w|i\rangle = 0$. The marked vector gets a minus sign, while every other vector is multiplied by 1. The operator acts in the same way on an arbitrary state $|\psi\rangle$: by (2.9), $\langle w|\psi\rangle = a_w$, so

$$U_w|\psi\rangle = |\psi\rangle - 2a_w|w\rangle.$$

We have subtracted the component $a_w|w\rangle$ twice, leaving $-a_w|w\rangle$; the other components do not change.

Geometrically, the oracle is a mirror: it reverses one direction, $|w\rangle$, and leaves everything perpendicular to it unchanged. One application of the oracle is one query. The other allowed method, writing the answer into an additional qubit, acts on $n+1$ qubits: the n candidate qubits and the additional one. We will compare the two methods in §3.7: we will see that they are two faces of the same circuit, and why Grover chooses the sign.

3.7 Why the Oracle Alone Is Not Enough

Let us use the oracle, first as we would on an ordinary computer, by checking one candidate at a time. The oracle is built from the check (§3.5); a check that erases nothing writes its answer into an additional qubit, called the **auxiliary qubit**. We encode a candidate, one of the N possibilities in §3.4, in n qubits as a basis state $|c\rangle$, and set the auxiliary qubit to $|0\rangle$ (Figure 3.1). The joint state is written $|c\rangle|0\rangle$, short for $|c\rangle \otimes |0\rangle$ from §2.4. The oracle is now a circuit on $n+1$ qubits: it leaves the candidate unchanged and writes the answer into the auxiliary qubit:

$$|c\rangle|0\rangle \longmapsto |c\rangle\,|f(c)\rangle.$$

Measuring the auxiliary qubit gives $f(c)$: 1 if c is the sought element, and 0 otherwise. One query therefore checks exactly one candidate, just like an ordinary check. We need as many queries as an ordinary computer, about $N/2$ on average (§3.2). Checking candidates individually gives no quantum speedup in the number of queries.

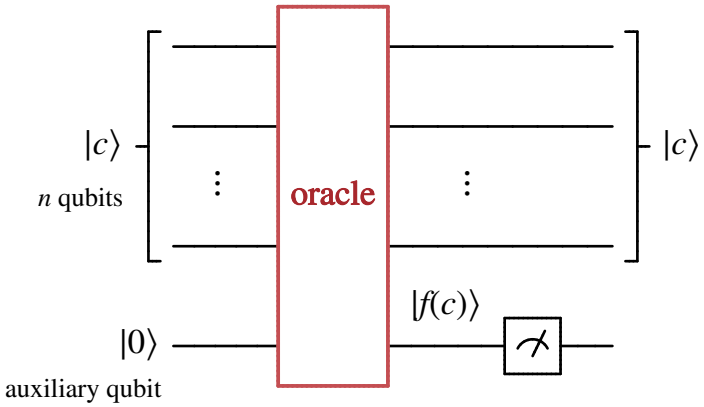


Figure 3.1. Classical use of the oracle. The upper n qubits hold the candidate, a basis state $|c\rangle$, while the lower auxiliary qubit starts in $|0\rangle$. The oracle leaves the candidate unchanged and writes the answer $f(c)$ into the auxiliary qubit. Measuring the auxiliary qubit gives 1 if c is the sought element, and 0 otherwise. The small dial at the end of the line denotes a measurement.

Perhaps the power of a quantum computer lies in superposition? Let us try to make the oracle check all candidates at once. A layer of H gates first prepares $|s\rangle$, in which every candidate has the same amplitude $1/\sqrt{N}$, and we set the auxiliary qubit to $|0\rangle$ as before (Figure 3.2a). The oracle acts on each term separately, so after one query the state is

$$\frac{1}{\sqrt{N}} \sum_{c \neq w} |c\rangle|0\rangle + \frac{1}{\sqrt{N}}\,|w\rangle|1\rangle.$$

It seems as though the oracle has checked every candidate with one query: the auxiliary qubit now shows 1 next to the sought element and 0 next to all others. But what does measurement show?

Measurement gives only one candidate c and its bit $f(c)$, each such pair with probability $(1/\sqrt{N})^2 = 1/N$. The auxiliary qubit shows 1, together with the sought element, only with probability $1/N$—just as if we chose one candidate at random and checked it. If something succeeds with probability $1/N$, it takes about N attempts on average, just as rolling a six takes six throws on average. That is even worse than checking in order, which needs about $N/2$ queries. The oracle has indeed acted on all candidates at once, but that is no help: measurement gives only one random outcome.

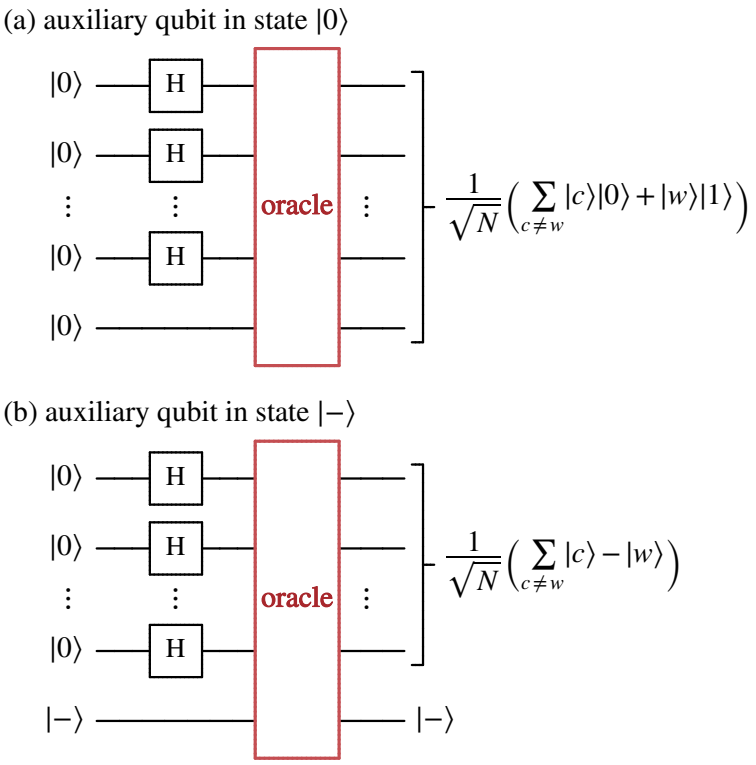


Figure 3.2. The same oracle acting on $|s\rangle$, prepared by a layer of H gates. (a) With the auxiliary qubit in $|0\rangle$, the oracle writes the answer next to each candidate: 1 next to w and 0 next to all others. (b) With the auxiliary qubit in $|-\rangle$, the oracle only changes the sign of the amplitude of w; the auxiliary qubit remains $|-\rangle$. In both cases measurement yields the sought element with probability only $1/N$.

Grover's algorithm prepares the auxiliary qubit in $|-\rangle$, not $|0\rangle$ (Figure 3.2b). The oracle then changes a sign rather than writing the answer, as in (3.3), while the auxiliary qubit itself remains unchanged. How does $|-\rangle$ do this? Let us look closely at the oracle in three steps.

First step: conditionally flipping the auxiliary qubit. Recall the CNOT gate (§2.8). It has a control qubit and a target qubit: it flips the target if the control is 1, and otherwise does nothing. For basis states, $|a\rangle|b\rangle \mapsto |a\rangle|b\oplus a\rangle$, where $\oplus$ is addition modulo 2: $0\oplus 0 = 1\oplus 1 = 0$ and $0\oplus 1 = 1\oplus 0 = 1$. The oracle does the same with the candidate and auxiliary qubit: it flips the auxiliary qubit if the candidate passes the check, and otherwise does nothing. If h is the auxiliary bit,

$$|c\rangle|h\rangle \longmapsto |c\rangle\,|h \oplus f(c)\rangle.$$

This has the same form as CNOT, except that the answer $f(c)$ replaces the control bit a. The smallest example, $N = 2$, makes this clearest. The candidate is one qubit; let the sought element be $w = 1$. The check says yes exactly when the candidate is 1, so $f(c) = c$ and the rule is $|c\rangle|h\rangle \mapsto |c\rangle|h \oplus c\rangle$. This is precisely CNOT: the candidate is the control and the auxiliary qubit is the target. For $w = 0$, the check says yes when the candidate is 0; we therefore put an X gate on the candidate

before and after CNOT, so that the control responds to 0 rather than 1. For two candidate qubits and $w = 11$, the auxiliary qubit must be flipped only when both candidate qubits are 1: this is a CNOT with two controls, the Toffoli gate in §3.17. The same applies to any check that can be built from gates: the circuit computes $f(c)$ without erasing the candidate, the result controls an X gate on the auxiliary qubit, and the circuit then undoes its temporary computation, leaving only the change to the auxiliary qubit. **In general, the oracle is a circuit that conditionally flips the auxiliary qubit; a single** CNOT **suffices only for particular checks.**

Second step: what X **does to the auxiliary qubit.** The X gate exchanges the qubit's two amplitudes, the amplitudes of $|0\rangle$ and $|1\rangle$. What that exchange means depends on the state of the auxiliary qubit (Figure 3.3a–c). The state $|0\rangle$ has amplitudes 1 and 0; after exchange they are 0 and 1, which is the different state $|1\rangle$. The answer has been written into the auxiliary qubit, as in classical checking. The state $|+\rangle$ has two equal amplitudes, $1/\sqrt{2}$, so exchanging them changes nothing: $\mathrm{X}|+\rangle = |+\rangle$. **With the auxiliary qubit in $|+\rangle$, the oracle does nothing:** it neither writes the answer nor changes a sign, so the query reveals nothing. The state $|-\rangle$ has amplitudes $1/\sqrt{2}$ and $-1/\sqrt{2}$; after exchange they are $-1/\sqrt{2}$ and $1/\sqrt{2}$. This is the same state, multiplied by -1:

$$\mathrm{X}|-\rangle = \frac{|1\rangle - |0\rangle}{\sqrt{2}} = -|-\rangle.$$

Thus X does not turn $|-\rangle$ into a different state: it only multiplies it by -1.

Third step: the minus sign passes to the candidate. Put the auxiliary qubit in $|-\rangle$. For the sought element, the oracle flips the auxiliary qubit, so $|w\rangle|-\rangle$ becomes $|w\rangle(-|-\rangle) = -|w\rangle|-\rangle$. For every other candidate c, the state $|c\rangle|-\rangle$ is unchanged. In brief,

$$|c\rangle|-\rangle \longmapsto (-1)^{f(c)}\,|c\rangle|-\rangle.$$

We can attribute the minus sign in front of the product to the candidate: the sought candidate gets a minus sign, while the others do not. If the input is a superposition of candidates, the same happens to each term separately, and the auxiliary qubit remains $|-\rangle$ in every term. The action on the candidates is therefore exactly the oracle (3.3). Figure 3.3d shows this in the smallest example, $N = 2$ and $w = 1$, where the oracle is just CNOT. The state $|+\rangle|-\rangle$ has four amplitudes, $1/2$, $-1/2$, $1/2$ and $-1/2$. CNOT exchanges the two auxiliary-qubit amplitudes only for candidate 1. That pair is $1/2$ and $-1/2$, so exchange gives $-1/2$ and $1/2$: the same as a minus sign on the whole pair. The output is $|-\rangle|-\rangle$: the candidate has acquired a minus sign for w, and the auxiliary qubit remains $|-\rangle$. The sign has "kicked back" from the auxiliary qubit to the candidate; this effect is called *phase kickback*.

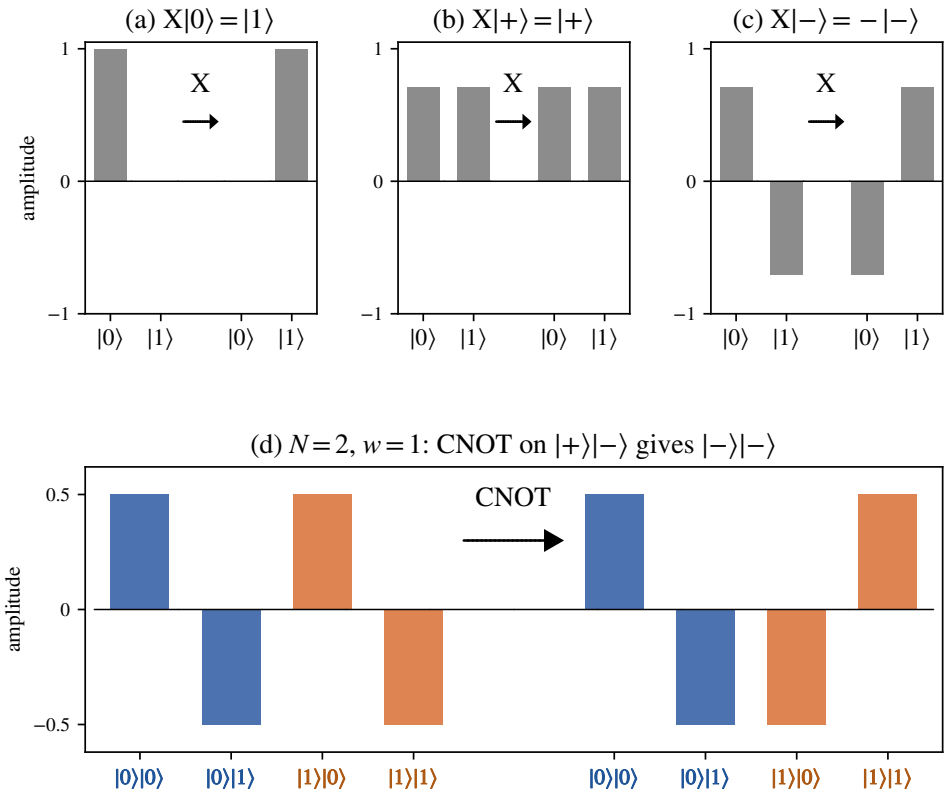


Figure 3.3. How an auxiliary qubit in $|-\rangle$ turns writing an answer into a sign. The X gate exchanges the qubit's two amplitudes (gray, before and after the arrow). (a) $|0\rangle$ becomes a different state, $|1\rangle$: the answer is written. (b) $|+\rangle$ remains unchanged: the oracle does nothing. (c) $|-\rangle$ stays the same except for a minus sign. (d) $N = 2$ and $w = 1$, with CNOT as the oracle: only two of the four amplitudes of $|+\rangle|-\rangle$ are exchanged, those for candidate 1 (orange), equivalent to a minus sign on that pair. The output is $|-\rangle|-\rangle$: the candidate has acquired a minus sign and the auxiliary qubit remains $|-\rangle$.

Why, then, do we prepare the auxiliary qubit in $|-\rangle$ rather than $|0\rangle$? As we have seen, with the auxiliary qubit in $|0\rangle$ the oracle writes the answer $f(c)$ (Figure 3.2a). If the candidate register is in a superposition, it may become entangled with the auxiliary qubit after the query. We can also understand this by writing $|0\rangle = (|+\rangle + |-\rangle)/\sqrt{2}$: the part with $|+\rangle$ remains unchanged, while the part with $|-\rangle$ acquires a sign depending on $f(c)$. Together, the two parts write the answer into the auxiliary qubit. When the latter starts in $|-\rangle$, it can be factored out of the joint state after the query, and the oracle has changed the sign of the marked candidate's amplitude. We can therefore follow only the candidate register in the next step.

What, then, is an oracle? We have considered two related ways to represent the check. The first is a reversible circuit acting on the candidate register and an auxiliary qubit as

$$U_f|c\rangle|h\rangle = |c\rangle|h \oplus f(c)\rangle.$$

With the auxiliary qubit in $|0\rangle$, the result of the check is written into it. If we prepare it in $|-\rangle$, the same operator changes the sign of the amplitude of every candidate for which $f(c) = 1$, while the auxiliary qubit remains in $|-\rangle$. Thus we obtain the action of the phase oracle on the candidate register, $|c\rangle \mapsto (-1)^{f(c)}|c\rangle$. For one marked state this is the operator U_w in (3.3).

This is one way to implement a phase oracle, but not the only one. In simple examples we can also implement it directly, without an auxiliary qubit, as we will see in §3.16. More complicated checks

may need additional work qubits. If we use them for temporary computation, we must return them to their initial states so that they do not remain entangled with the candidate register.

From now on we describe the oracle's action by the phase operator U_w on the candidate space. Its definition says what the operator does, but does not prescribe a unique physical implementation.

After one query the oracle has changed the sign of the amplitude of w, and only that amplitude (Figure 3.4a, b). With one query we have marked the solution! But measurement still does not help. The probability is $(1/\sqrt{N})^2 = 1/N$ for every unmarked possibility and $(-1/\sqrt{N})^2 = 1/N$ for the marked one, just as before the query (Figure 3.4c). Measurement is still a random guess, and repeating the experiment does not help: if we repeat it many times, we see all N outcomes equally often. The minus sign is exactly at w, but measurement cannot see the sign.

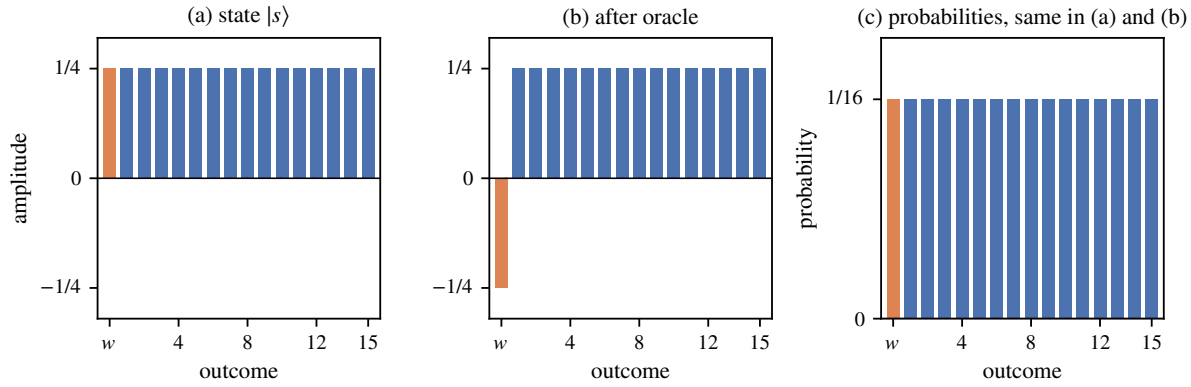


Figure 3.4. Sixteen amplitudes, $N = 16$; the amplitude of the marked element w is orange, the others blue. (a) State $|s\rangle$: all amplitudes are 1/4. (b) After one query the oracle has changed the sign of the amplitude of w. (c) The probabilities are the same in both cases, 1/16: measurement cannot see the sign.

The oracle alone is therefore not enough. We need one more step, which does not query the oracle but uses the sign it left: it increases the amplitude of the marked possibility and decreases the amplitudes of all the others. The probability of measuring w then increases. We have seen that something like this can be done.

Key idea

The states $|+\rangle$ and $|-\rangle$ differ only in the sign of one amplitude, so measurement does not distinguish them. But after another H gate they become $|0\rangle$ and $|1\rangle$, which measurement distinguishes with certainty (§2.6):

$$|+\rangle \xrightarrow{\text{H}} |0\rangle, \qquad |-\rangle \xrightarrow{\text{H}} |1\rangle.$$

The second step, after the oracle, does the same thing, but with all N amplitudes.

To understand both the oracle and this new step, we will look at them geometrically: both turn out to be reflections.

3.8 The Oracle's Action on the Initial State

We now turn to geometry. Grover's algorithm [5] uses two reflections, and all the geometry we saw with the blocks will reappear here.

Return to the oracle in (3.4):

$$U_w = \mathbb{1} - 2|w\rangle\langle w|.$$

It changes the sign only of the part of the state along $|w\rangle$, leaving everything perpendicular to $|w\rangle$ unchanged. Let us see what this means for the state to which we apply it.

We apply the oracle to Grover's initial state $|s\rangle$ from (2.7). A layer of H gates prepares it from $|0\ldots0\rangle$ (§2.7); every element then has the same amplitude, $1/\sqrt{N}$. Let us decompose $|s\rangle$ into two mutually perpendicular parts.

The first is along $|w\rangle$. By (2.9), the component of $|s\rangle$ along $|w\rangle$ is $\langle w|s\rangle = 1/\sqrt{N}$, so that part is $|w\rangle/\sqrt{N}$.

The second part is the remainder: the sum of all the other basis vectors, each with amplitude $1/\sqrt{N}$. The square of its length is the sum of the squares of $N-1$ such amplitudes, $(N-1)/N$. Dividing this remainder by its length, $\sqrt{(N-1)/N}$, gives the unit vector

$$|\bar{s}\rangle = \frac{1}{\sqrt{N-1}} \sum_{i\neq w} |i\rangle,$$

in which all unmarked elements have the same amplitude, and the marked element has amplitude zero. The bar over s reminds us that the marked element is absent. The vectors $|w\rangle$ and $|\bar{s}\rangle$ are orthogonal, $\langle w|\bar{s}\rangle = 0$, because they have no common nonzero component. The initial state is the sum of these two parts:

$$|s\rangle = \frac{1}{\sqrt{N}}|w\rangle + \sqrt{\frac{N-1}{N}}|\bar{s}\rangle = \sin\bar{\theta}\,|w\rangle + \cos\bar{\theta}\,|\bar{s}\rangle, \qquad \sin\bar{\theta} = \frac{1}{\sqrt{N}} \tag{3.5}$$

Draw the plane spanned by $|\bar{s}\rangle$ and $|w\rangle$, with $|\bar{s}\rangle$ horizontal and $|w\rangle$ vertical (Figure 3.5a). We will call the line through $|\bar{s}\rangle$ the $|\bar{s}\rangle$ **axis**, and the line through $|w\rangle$ the $|w\rangle$ axis. In this plane $|s\rangle$ is a unit arrow at an angle $\bar{\theta}$ above the $|\bar{s}\rangle$ axis. Its projection onto the $|\bar{s}\rangle$ axis is $\cos\bar{\theta}$, and onto the $|w\rangle$ axis is $\sin\bar{\theta}$. For large N, the angle $\bar{\theta}$ is small: the initial state is nearly perpendicular to the answer $|w\rangle$. We deliberately used the same letter as for the angle in the block problem (§1.10): in §4.2 we will see that it is the same angle.

Now apply the oracle to $|s\rangle$. By (3.5), $\langle w|s\rangle = \sin\bar{\theta}$, so

$$U_w|s\rangle = |s\rangle - 2\langle w|s\rangle\,|w\rangle = \big(\sin\bar{\theta}\,|w\rangle + \cos\bar{\theta}\,|\bar{s}\rangle\big) - 2\sin\bar{\theta}\,|w\rangle = -\sin\bar{\theta}\,|w\rangle + \cos\bar{\theta}\,|\bar{s}\rangle.$$

The part along the $|\bar{s}\rangle$ axis stays the same, while the part along $|w\rangle$ changes sign. The arrow was at an angle $\bar{\theta}$ above the $|\bar{s}\rangle$ axis; it is now at the same angle below it (Figure 3.5b). Thus $U_w|s\rangle$ is the image of $|s\rangle$ in a mirror placed along the $|\bar{s}\rangle$ axis: **in the plane of $|\bar{s}\rangle$ and $|w\rangle$, the oracle is reflection about the $|\bar{s}\rangle$ axis**.

3.9 The Oracle as a Reflection

In §3.8 we saw what the oracle does to one state, $|s\rangle$. We will now calculate that it does the same to every state in this plane: the oracle really is a reflection about the $|\bar{s}\rangle$ axis.

First let us state exactly what reflection about an axis means. In school this is called axial symmetry: each point moves to a point on the other side of the axis, at the same distance from it. For an

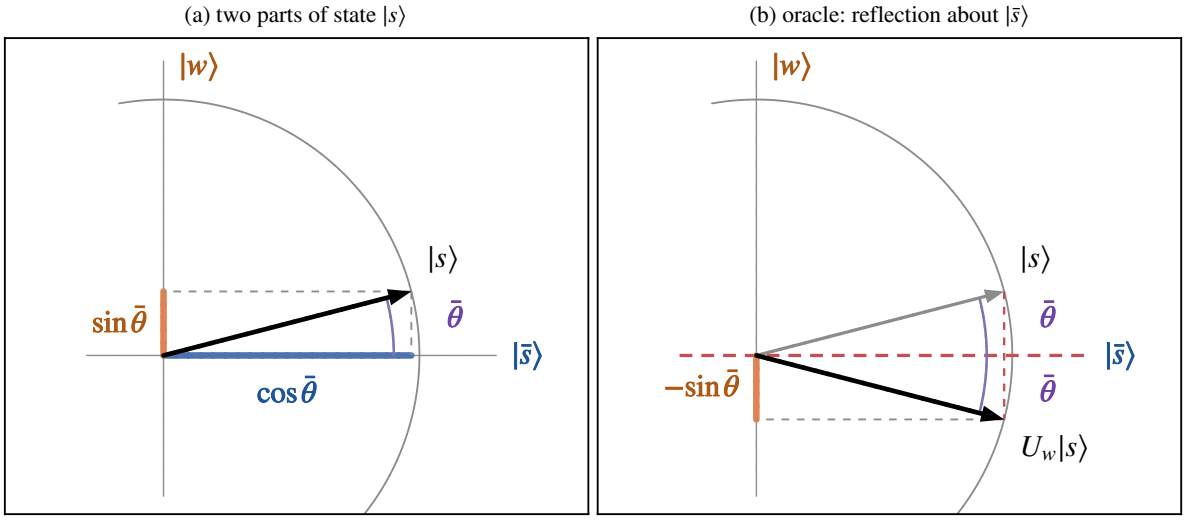


Figure 3.5. The plane spanned by $|\bar{s}\rangle$ and $|w\rangle$, for $N = 16$. (a) The initial state $|s\rangle$ and its two parts: along the $|\bar{s}\rangle$ axis (blue, $\cos\bar{\theta}$) and along the $|w\rangle$ axis (orange, $\sin\bar{\theta}$). (b) The oracle changes the sign of the part along $|w\rangle$ and leaves the part along $|\bar{s}\rangle$ unchanged: $U_w|s\rangle$ is the reflection of $|s\rangle$ in a mirror on the $|\bar{s}\rangle$ axis (red), at an angle $\bar{\theta}$ below it.

arrow this means the following. Decompose the state $|\psi\rangle$ into a part along the axis, $|\psi_\parallel\rangle$, and a part perpendicular to it, $|\psi_\perp\rangle$ (the symbols $\parallel$ and $\perp$ mean "parallel" and "perpendicular"):

$$|\psi\rangle = |\psi_\parallel\rangle + |\psi_\perp\rangle.$$

Reflection retains the part along the axis and changes the sign of the part perpendicular to it:

$$|\psi_\parallel\rangle + |\psi_\perp\rangle \longmapsto |\psi_\parallel\rangle - |\psi_\perp\rangle \tag{3.6}$$

Two properties follow immediately. Applied twice, reflection returns every state to its starting point, because the perpendicular part changes sign twice. Reflection also preserves the state's length. The parts $|\psi_\parallel\rangle$ and $|\psi_\perp\rangle$ are perpendicular, so by Pythagoras the squared length of the state is the sum of their squared lengths, both before and after reflection (see Exercise 56). Reflection is therefore an allowed operation (Rule 3).

Now consider the oracle. Any state in the plane spanned by $|\bar{s}\rangle$ and $|w\rangle$ can be written

$$|\psi\rangle = x\,|\bar{s}\rangle + y\,|w\rangle,$$

where x and y are numbers: the coordinates of the arrow's tip, x along the $|\bar{s}\rangle$ axis and y along the $|w\rangle$ axis. The initial state, for example, has $x = \cos\bar{\theta}$ and $y = \sin\bar{\theta}$ by (3.5). The $|w\rangle$ axis is perpendicular to the $|\bar{s}\rangle$ axis, so the part along $|\bar{s}\rangle$ is $|\psi_\parallel\rangle = x\,|\bar{s}\rangle$ and the perpendicular part is $|\psi_\perp\rangle = y\,|w\rangle$ (Figure 3.6a).

Apply the oracle to $|\psi\rangle$ step by step. First expand:

$$U_w|\psi\rangle = \big(\mathbb{1} - 2|w\rangle\langle w|\big)\big(x\,|\bar{s}\rangle + y\,|w\rangle\big) = x\,|\bar{s}\rangle + y\,|w\rangle - 2|w\rangle\big(x\,\langle w|\bar{s}\rangle + y\,\langle w|w\rangle\big).$$

The final parentheses contain two inner products: $\langle w|\bar{s}\rangle = 0$ because $|w\rangle$ and $|\bar{s}\rangle$ are orthogonal, and $\langle w|w\rangle = 1$ because $|w\rangle$ is a unit vector. The quantity in parentheses is therefore y, giving

$$U_w|\psi\rangle = x\,|\bar{s}\rangle + y\,|w\rangle - 2y\,|w\rangle = x\,|\bar{s}\rangle - y\,|w\rangle.$$

Thus:

$$U_w\big(x\,|\bar{s}\rangle + y\,|w\rangle\big) = x\,|\bar{s}\rangle - y\,|w\rangle, \qquad \text{that is,} \qquad (x, y) \longmapsto (x, -y) \tag{3.7}$$

The part along $|\bar{s}\rangle$ is unchanged, while the perpendicular part changes sign: this is exactly reflection (3.6) about the $|\bar{s}\rangle$ axis (Figure 3.6b). In coordinates, $(x, y) \mapsto (x, -y)$ is reflection in the x-axis, just like a bounce off the wall for the blocks (§1.7). Nowhere did we use that the state is specifically $|s\rangle$, so the oracle reflects every state in this plane about the $|\bar{s}\rangle$ axis. Outside the plane, however, U_w and reflection about that axis are not the same. Reflection about the $|\bar{s}\rangle$ axis changes the sign of everything perpendicular to it, and in N dimensions there are $N-1$ such directions. U_w changes the sign of only one, the direction $|w\rangle$. In the plane they agree because $|w\rangle$ is the only direction perpendicular to $|\bar{s}\rangle$ there. Here is an example with only three directions and no qubits: for $N = 3$ and $w = 0$, the vector $(|1\rangle - |2\rangle)/\sqrt{2}$ is perpendicular to both $|w\rangle$ and $|\bar{s}\rangle = (|1\rangle + |2\rangle)/\sqrt{2}$. U_w leaves it unchanged, while reflection about the $|\bar{s}\rangle$ axis would change its sign. Grover's algorithm never leaves the plane, however (§3.12), so what holds in the plane is enough for us.

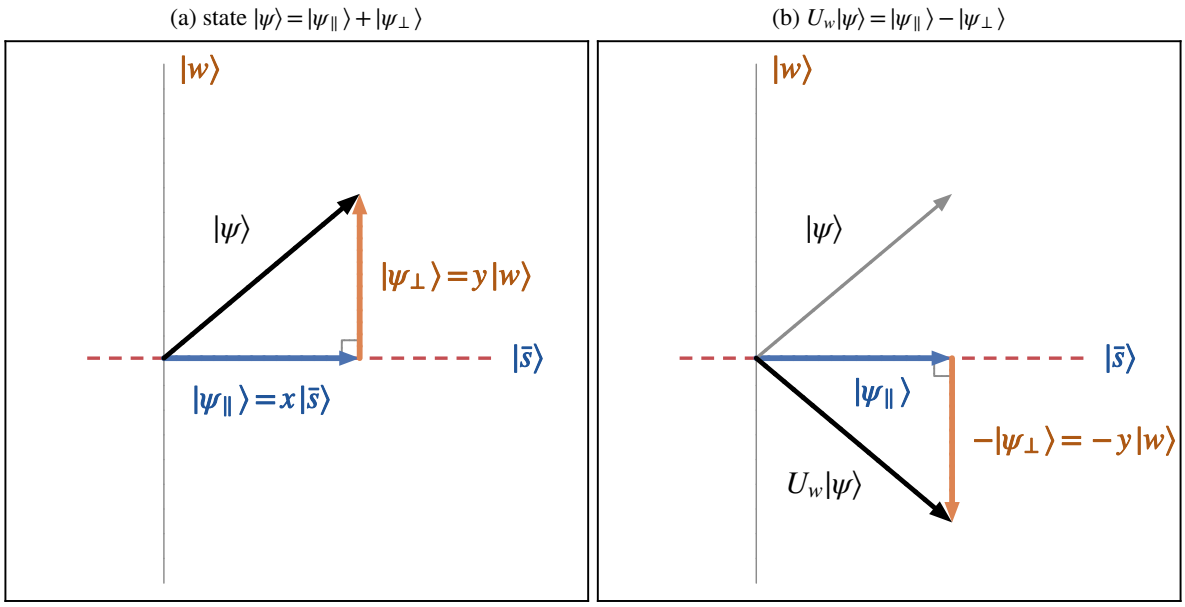


Figure 3.6. The oracle on an arbitrary state $|\psi\rangle = x\,|\bar{s}\rangle + y\,|w\rangle$. (a) The part along the $|\bar{s}\rangle$ axis, $|\psi_\parallel\rangle = x\,|\bar{s}\rangle$ (blue), and the perpendicular part, $|\psi_\perp\rangle = y\,|w\rangle$ (orange). (b) The oracle preserves $|\psi_\parallel\rangle$ and changes the sign of $|\psi_\perp\rangle$: $U_w|\psi\rangle = |\psi_\parallel\rangle - |\psi_\perp\rangle$ is the image of $|\psi\rangle$ in a mirror on the $|\bar{s}\rangle$ axis (red).

3.10 Diffusion: Reflection about the $|s\rangle$ Axis

The oracle alone is not enough (§3.7): after it, measurement still cannot see the sign. We need the missing second operator. It is also a reflection, this time about the axis through the initial state itself, the $|s\rangle$ **axis**:

$$U_s = 2|s\rangle\langle s| - \mathbb{1} \tag{3.8}$$

This operator is called **diffusion**; we will see why at the end of the section.

Let us show by calculation, as we did for the oracle, that U_s is reflection about the $|s\rangle$ axis. Decompose an arbitrary state $|\psi\rangle$ into a part along the $|s\rangle$ axis and a perpendicular part. The part along the axis

is the projection of $|\psi\rangle$ onto $|s\rangle$ (§2.9):

$$|\psi_\parallel\rangle = \langle s|\psi\rangle\,|s\rangle.$$

The perpendicular part is the remainder:

$$|\psi_\perp\rangle = |\psi\rangle - \langle s|\psi\rangle\,|s\rangle.$$

The remainder really is perpendicular to the axis. Its inner product with $|s\rangle$ is zero because $\langle s|s\rangle = 1$:

$$\langle s|\psi_\perp\rangle = \langle s|\psi\rangle - \langle s|\psi\rangle\langle s|s\rangle = \langle s|\psi\rangle - \langle s|\psi\rangle = 0.$$

Apply U_s to $|\psi\rangle$ step by step. First multiply:

$$U_s|\psi\rangle = \big(2|s\rangle\langle s| - \mathbb{1}\big)|\psi\rangle = 2\langle s|\psi\rangle\,|s\rangle - |\psi\rangle.$$

The first term is twice the part along the axis, $2|\psi_\parallel\rangle$, and the second is the whole state, $|\psi\rangle = |\psi_\parallel\rangle + |\psi_\perp\rangle$. Hence

$$U_s|\psi\rangle = 2|\psi_\parallel\rangle - |\psi_\parallel\rangle - |\psi_\perp\rangle = |\psi_\parallel\rangle - |\psi_\perp\rangle.$$

The part along the $|s\rangle$ axis stays the same and the perpendicular part changes sign: that is reflection (3.6) about the $|s\rangle$ axis (Figure 3.7). In particular, a state on the axis stays unchanged, $U_s|s\rangle = |s\rangle$, while a state perpendicular to the axis changes sign.

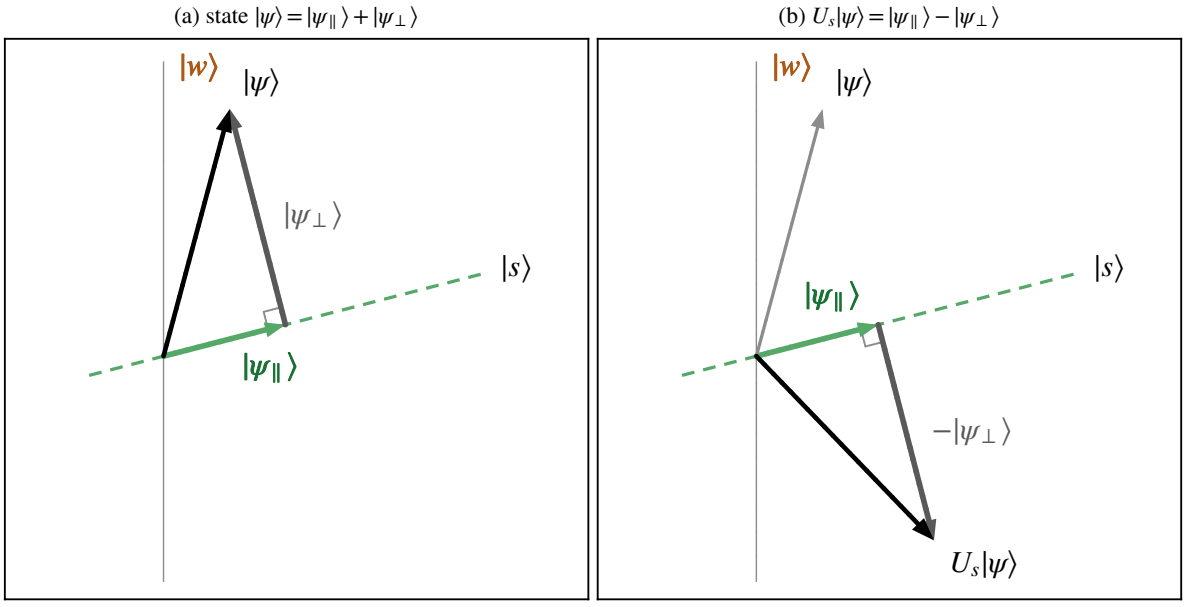


Figure 3.7. Diffusion acting on an arbitrary state $|\psi\rangle$. (a) The part along the $|s\rangle$ axis, $|\psi_\parallel\rangle = \langle s|\psi\rangle\,|s\rangle$ (green), and the remainder $|\psi_\perp\rangle$, perpendicular to the axis (gray). (b) U_s preserves $|\psi_\parallel\rangle$ and changes the sign of $|\psi_\perp\rangle$: $U_s|\psi\rangle = |\psi_\parallel\rangle - |\psi_\perp\rangle$ is the image of $|\psi\rangle$ in a mirror on the $|s\rangle$ axis (the dashed green line).

Nowhere did the calculation use the fact that $|s\rangle$ is the initial state, only that it is a unit vector. The same therefore holds for the axis through any unit vector $|u\rangle$: reflection about the $|u\rangle$ axis is

$$\big(2|u\rangle\langle u| - \mathbb{1}\big)|\psi\rangle = 2\langle u|\psi\rangle\,|u\rangle - |\psi\rangle \tag{3.9}$$

We will meet it again for the blocks (Chapter 4).

Measurement in the computational basis gives one outcome i with probability a_i^2. Let us therefore see how reflection changes amplitudes, and thus the probabilities of possible outcomes. The rule will be very simple, and in §3.14 we will use it to see how the marked element's amplitude grows. Let $|\psi\rangle = \sum_i a_i|i\rangle$. By (2.8), its inner product with $|s\rangle$ is

$$\langle s|\psi\rangle = \frac{1}{\sqrt{N}} \sum_i a_i = \sqrt{N}\,\bar{a},$$

where $\bar{a}$ is the arithmetic mean of the amplitudes, their sum divided by N. The part along the $|s\rangle$ axis is therefore

$$|\psi_\parallel\rangle = \langle s|\psi\rangle\,|s\rangle = \sqrt{N}\,\bar{a} \cdot \frac{1}{\sqrt{N}}\,(1, 1, \ldots, 1) = \bar{a}\,(1, 1, \ldots, 1),$$

a vector whose every component equals the mean. Component i of $U_s|\psi\rangle = 2|\psi_\parallel\rangle - |\psi\rangle$ is therefore $2\bar{a} - a_i$:

$$a_i \longmapsto 2\bar{a} - a_i \tag{3.10}$$

Each amplitude moves to the other side of the mean, the same distance away: if it was 3 above the mean, it is now 3 below. The mean itself does not change (see Exercise 57). We call this **reflection about the arithmetic mean**; for the blocks, the mean will be the center-of-mass velocity (§4.3).

We still need to explain the name. Grover calls this step the "diffusion transformation" and shows that it is reflection about the mean [5], but does not explain the name there. By (3.10), every new amplitude depends on all the old ones through their mean. If initially, for example, all amplitude is on one element, $a_j = 1$, the mean is $1/N$, so after diffusion every other element gets amplitude $2/N$. A small part of the amplitude thus spreads equally over all elements, like a drop of ink in water. Grover himself later explained the name in this way: his step resembles diffusion, in which a little passes from each state to every other state [9]. In Grover's algorithm these small parts add up at the marked element, thanks to the sign supplied by the oracle.

3.11 Two Reflections Make a Rotation

One **Grover step** is the oracle followed by diffusion: $U_s U_w$ (the operator acting first is written on the right). These are reflections about the $|\bar{s}\rangle$ and $|s\rangle$ axes, which make an angle $\bar{\theta}$. Let us show that together two reflections rotate the arrow, through twice the angle between the axes.

We measure angles from the $|\bar{s}\rangle$ axis in the positive, counterclockwise direction. A state at angle φ is $|\psi\rangle = \cos\varphi\,|\bar{s}\rangle + \sin\varphi\,|w\rangle$; by (3.5), the initial state has $\varphi = \bar{\theta}$.

What does reflection do to the angle? Take any reflection axis in this plane—a line through the origin—and let β be the angle **that axis** makes with the $|\bar{s}\rangle$ axis (Figure 3.8a). Take care: β is the angle of the axis itself, not of a state, and does not change from one step to the next. For the oracle the axis is $|\bar{s}\rangle$ itself, so $\beta = 0$; for diffusion it is $|s\rangle$, so $\beta = \bar{\theta}$. The arrow is at angle φ from the $|\bar{s}\rangle$ axis, so its angle from the reflection axis is $\varphi - \beta$: its component along the axis is $\cos(\varphi - \beta)$ and its perpendicular component is $\sin(\varphi - \beta)$. Reflection (3.6) changes the sign of only the second part, taking the arrow the same distance to the other side of the axis, to angle $-(\varphi - \beta)$ measured from that axis (Figure 3.8b). Measured from $|\bar{s}\rangle$, that is $\beta - (\varphi - \beta)$:

$$\varphi \longmapsto 2\beta - \varphi. \tag{3.11}$$

The $|\bar{s}\rangle$ axis has $\beta = 0$, so the oracle sends φ to $-\varphi$; this is $(x, y) \mapsto (x, -y)$ from (3.7). The $|s\rangle$ axis has $\beta = \bar{\theta}$, so diffusion sends φ to $2\bar{\theta} - \varphi$. One Grover step, oracle followed by diffusion, therefore gives

$$\varphi \xrightarrow{U_w} -\varphi \xrightarrow{U_s} 2\bar{\theta} - (-\varphi) = \varphi + 2\bar{\theta}.$$

Every arrow has turned through the same angle, $2\bar{\theta}$, regardless of its initial angle φ: this is a rotation (Figure 3.9).

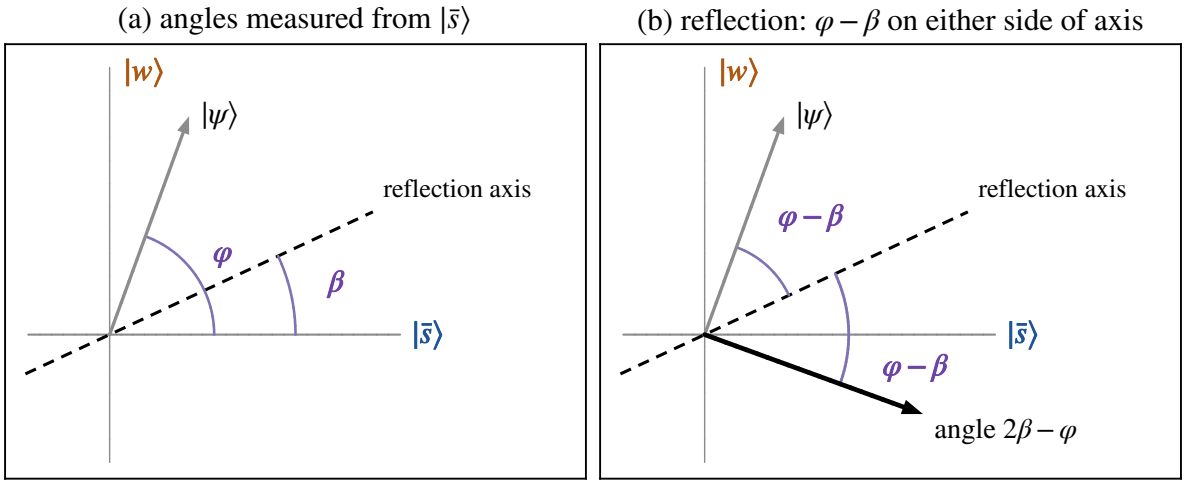


Figure 3.8. What β means. (a) We measure angles from the $|\bar{s}\rangle$ axis: the arrow $|\psi\rangle$ is at angle φ, and the reflection axis, a line through the origin, is at angle β. The angle β belongs to the axis, not the state: for the oracle it is $\beta = 0$, and for diffusion $\beta = \bar{\theta}$. (b) The arrow makes an angle $\varphi - \beta$ with the axis; reflection takes it the same distance to the other side, to angle $2\beta - \varphi$ measured from $|\bar{s}\rangle$.

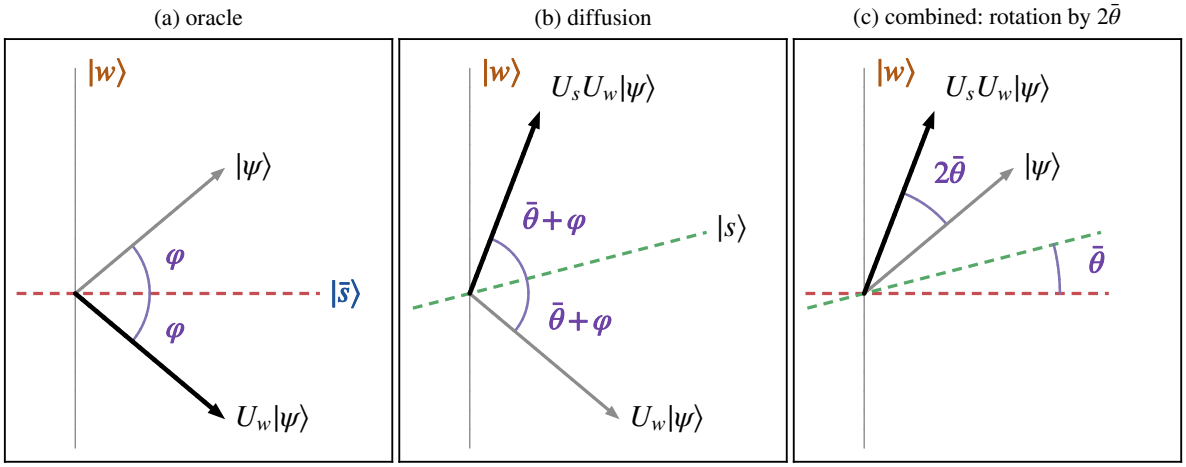


Figure 3.9. Two reflections make a rotation, $N = 16$. (a) The oracle, reflection about the $|\bar{s}\rangle$ axis (red), sends a state at angle φ to angle $-\varphi$. (b) Diffusion, reflection about the $|s\rangle$ axis (green) at angle $\bar{\theta}$, takes it the same distance to the other side of that axis, $\bar{\theta} + \varphi$. (c) Together, the state rotates through $2\bar{\theta}$, twice the angle between the axes.

The same calculation holds for any two axes. If the first makes angle β_1 and the second β_2, reflection about the first followed by reflection about the second gives

$$\varphi \longmapsto 2\beta_1 - \varphi \longmapsto 2\beta_2 - (2\beta_1 - \varphi) = \varphi + 2(\beta_2 - \beta_1).$$

If the axes make an angle $\alpha = \beta_2 - \beta_1$:

$$\text{reflection about the first axis, then about the second} \;=\; \text{rotation through } 2\alpha \tag{3.12}$$

The rotation is twice the angle between the axes. Order matters: reversing it gives a rotation through -2α, in the other direction (see Exercise 63). If the axes nearly coincide, the rotation is small, and many steps are needed to turn the arrow far. That small angle is the source of the square root in both stories.

In Grover's algorithm the axes make an angle $\bar{\theta}$:

$$\text{Grover step} = U_s U_w = \text{rotation through } 2\bar{\theta} \tag{3.13}$$

The axes do not move: at each step we apply the same oracle and the same diffusion. Therefore the state's angle does not double; rather, $2\bar{\theta}$ is added at each step. The initial angle $\bar{\theta}$ becomes $3\bar{\theta}$, then $5\bar{\theta}$, $7\bar{\theta}$, and so on: the arrow turns little by little toward $|w\rangle$.

Key idea

The axes of the two reflections are the initial state $|s\rangle$ and the vector $|\bar{s}\rangle$, which is perpendicular to the marked vector $|w\rangle$ in Grover's plane. The oracle changes the sign of the marked state's amplitude according to the checking rule. The axis $|\bar{s}\rangle$ depends mathematically on w, but the algorithm need not know w or construct that axis separately: applying the oracle is enough. Diffusion, on the other hand, depends on the known initial state $|s\rangle$, not on which element is marked.

The minus sign the oracle adds to the amplitude of w is, geometrically, a reflection; two reflections turn the state step by step toward the solution.

3.12 Why Are Two Dimensions Enough?

The state space has N dimensions, yet we draw a plane. Is that merely a convenient picture? No: the state of Grover's algorithm never leaves the plane spanned by $|\bar{s}\rangle$ and $|w\rangle$. The picture is exact, with no approximation.

Both operators are built only from $|w\rangle$, $|s\rangle$ and the identity operator. Acting on a state $|\psi\rangle$, each gives the same state, possibly with its sign changed, plus a multiple of one of those two vectors:

$$U_w|\psi\rangle = |\psi\rangle - 2\langle w|\psi\rangle\,|w\rangle, \qquad U_s|\psi\rangle = 2\langle s|\psi\rangle\,|s\rangle - |\psi\rangle.$$

If $|\psi\rangle$ is a linear combination of $|w\rangle$ and $|s\rangle$, so is the result. The algorithm starts in $|s\rangle$ itself, so after every step its state is such a combination: it lies in the plane spanned by $|w\rangle$ and $|s\rangle$. This is the same plane spanned by $|w\rangle$ and $|\bar{s}\rangle$, because subtracting the component of $|s\rangle$ along $|w\rangle$ leaves a vector along $|\bar{s}\rangle$:

$$|s\rangle - \frac{1}{\sqrt{N}}\,|w\rangle = \frac{1}{\sqrt{N}} \sum_{i \neq w} |i\rangle = \sqrt{\frac{N-1}{N}}\,|\bar{s}\rangle.$$

After each step, therefore, the state has the form $x\,|\bar{s}\rangle + y\,|w\rangle$, as in §3.9.

The amplitudes tell the same story. Neither $|s\rangle$, the oracle, nor diffusion distinguishes one unmarked element from another: initially all have the same amplitude, the oracle leaves them unchanged, and diffusion reflects each about the same mean. Thus all unmarked elements have the same amplitude at every step and move together as one. The $N-2$ directions in which unmarked amplitudes would differ from each other have zero amplitude throughout.

> **For the curious: a plane in a room.** Let $N = 3$, just three directions without qubits, and let $|w\rangle$ be the room's vertical axis. The two unmarked elements are the floor's two axes, while $|\bar{s}\rangle$ is the floor's diagonal, halfway between them. The vertical axis and that diagonal span a flat sheet: it stands upright and cuts diagonally across the room. The remaining direction, the other floor diagonal, is perpendicular to the sheet, and Grover's algorithm never reaches it: the state rotates within the sheet throughout.

3.13 How Many Grover Steps Are Needed?

Grover's algorithm [5] begins in state $|s\rangle$, repeats the Grover step—the oracle followed by diffusion—k times, and finally measures the state. How many steps do we need?

Let us relate the angle to the number of steps. The initial angle is given by (3.5): $\sin\bar{\theta} = 1/\sqrt{N}$. For large N the angle is small, and a small angle is approximately equal to its sine, by (B.1): $\bar{\theta} \approx 1/\sqrt{N}$. Each step rotates the arrow by $2\bar{\theta}$, so after k steps its angle is $(2k+1)\bar{\theta}$:

$$|\psi_k\rangle = \sin\big((2k+1)\bar{\theta}\big)\,|w\rangle + \cos\big((2k+1)\bar{\theta}\big)\,|\bar{s}\rangle, \qquad P(w) = \sin^2\big((2k+1)\bar{\theta}\big) \tag{3.14}$$

The probability is the square of the amplitude (§2.3), and the amplitude of $|w\rangle$ is the sine of the arrow's angle. As the arrow turns toward $|w\rangle$, the amplitude of the marked element grows and all the others decrease (Figure 3.10).

How many steps bring the arrow to $|w\rangle$? It begins at $\bar{\theta}$, while $|w\rangle$ is at the right angle $\pi/2$. We therefore need $(2k+1)\bar{\theta} = \pi/2$, or $k = q - 1/2$, where $q = \pi/(4\bar{\theta})$. The number of steps must be an integer; an integer closest to $q - 1/2$ is $\lfloor q \rfloor$, the greatest integer not exceeding q (rounding down). Indeed, $\lfloor q \rfloor \le q < \lfloor q \rfloor + 1$, so $q - 1/2$ lies between $\lfloor q \rfloor - 1/2$ and $\lfloor q \rfloor + 1/2$. One choice of step count at which the arrow is first closest to $|w\rangle$ is therefore

$$k^* = \left\lfloor \frac{\pi}{4\bar{\theta}} \right\rfloor \approx \frac{\pi}{4}\sqrt{N} \tag{3.15}$$

If q is an integer, both $q-1$ and q are equally close to the first maximum; the formula selects q. For example, when $N = 2$ the initial probability is already $1/2$, and one step does not increase it. Further maxima can occur later, so this choice need not be unique among all step counts. The approximate value follows from $\bar{\theta} \approx 1/\sqrt{N}$. After k^* steps the arrow is at most $\bar{\theta}$ from $|w\rangle$, so the success probability is at least $1 - 1/N$; this is a lower bound, not necessarily the exact value: $P(w) \ge \cos^2\bar{\theta} = 1 - 1/N$ (see Exercise 64).

The larger N is, the smaller the $|w\rangle$ component of the initial state, $1/\sqrt{N}$, and the smaller $\bar{\theta}$ becomes; more steps are needed, proportional to $\sqrt{N}$. For $N = 4$, $\bar{\theta} = 30°$ and one step brings the arrow exactly to $|w\rangle$, since $3\bar{\theta} = 90°$, giving $P(w) = 1$ (we will also see this in the circuit, §3.17); for $N = 8$, $k^* = 2$

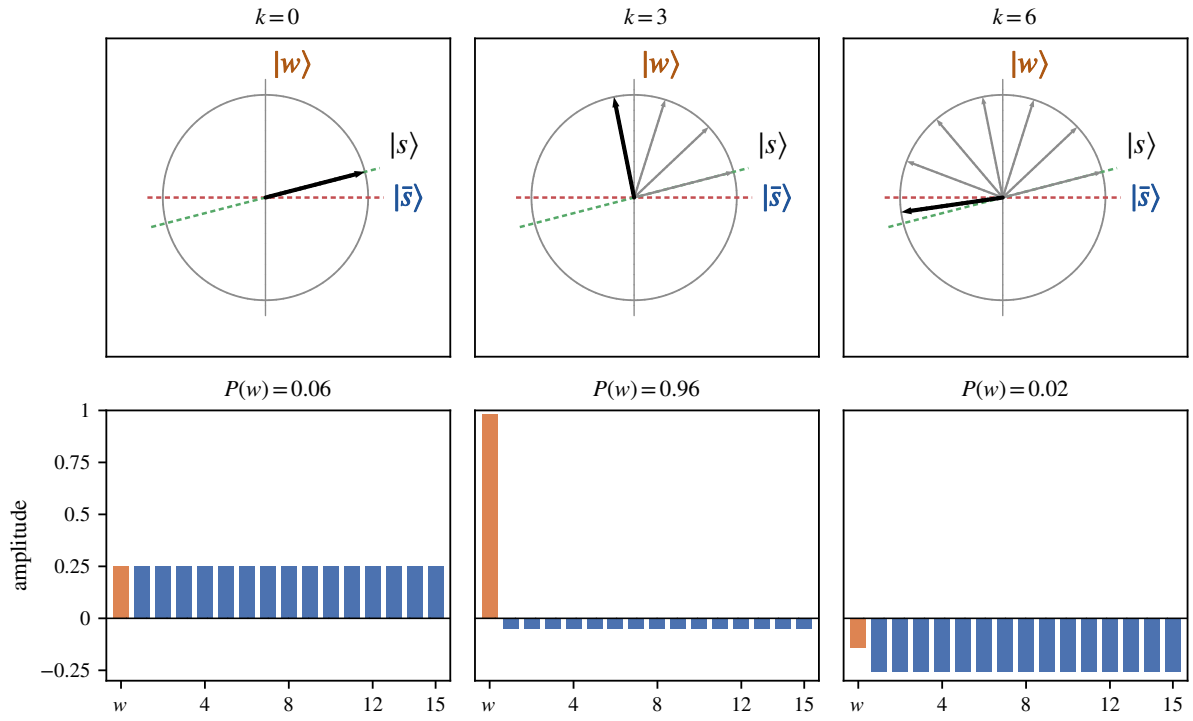


Figure 3.10. $N = 16$, after $k = 0$, 3 and 6 steps. Above: the state arrow in the $|\bar{s}\rangle$, $|w\rangle$ plane (gray arrows show earlier steps). Below: the sixteen amplitudes, marked in orange and unmarked in blue. After $k^* = 3$ steps the arrow is closest to $|w\rangle$ and $P(w) = 0.96$; after six steps it has passed that direction and $P(w)$ is small again.

and $P(w) = 121/128 \approx 0.945$ (Exercise 66); for $N = 16$, $\bar{\theta} = 14.5°$, $k^* = 3$ and $P(w) = 0.96$; for $N = 2^{20} = 1\,048\,576$ states, $k^* = 804$.

Taking more steps immediately after k^* is not better. The rotation does not stop on its own: if we continue, the arrow passes $|w\rangle$, the probability begins to decrease, and amplitude returns to the unmarked elements (Figure 3.11). In the basic version considered here, we choose the number of steps before measuring, using the known number of marked elements. When that number is unknown, a different procedure is needed to choose the number of steps [11]. After another half-turn the arrow again passes close to the direction of $|w\rangle$, now on the other side, sometimes even closer than after k^* steps; but that requires about three times as many queries.

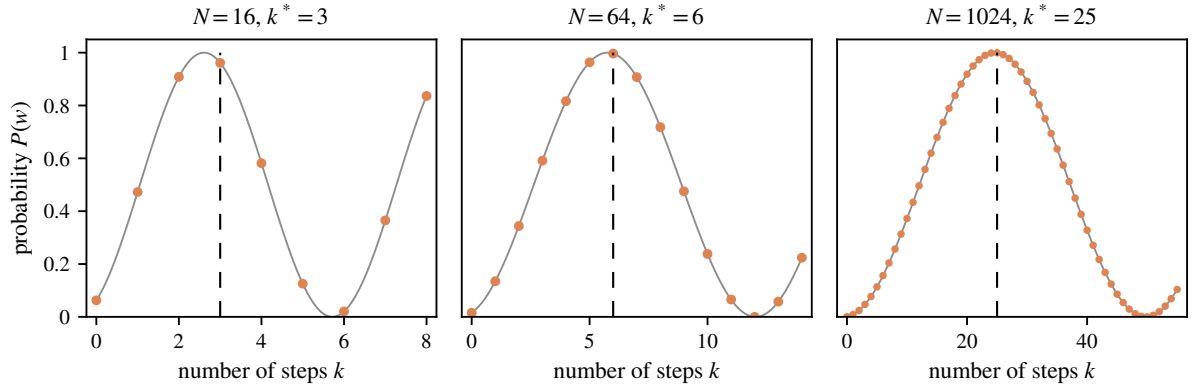


Figure 3.11. Probability $P(w)$ after k steps, for $N = 16$, 64 and 1024. Points show integer step counts; the gray curve is $\sin^2((2k+1)\bar{\theta})$ for continuous k. The dashed line marks k^*: the larger N, the farther along it is.

3.14 Amplitude Amplification

The arrow in the plane showed how a Grover step rotates the state and how many steps are needed. Measurement, however, gives outcomes whose probabilities are determined by amplitudes, so let us examine the same step in terms of amplitudes, bar by bar. We need the rule from §3.10: diffusion reflects each amplitude about their arithmetic mean $\bar{a}$. By (3.10), $a_i \mapsto 2\bar{a} - a_i$. A bar below the mean moves equally far above it; one above it moves equally far below.

Start with $|s\rangle$, where all amplitudes are $1/\sqrt{N}$. The oracle changes the sign of amplitude w to $-1/\sqrt{N}$. This also lowers the mean. The mean is the sum of the amplitudes divided by N; there are now $N-1$ amplitudes $1/\sqrt{N}$ and one $-1/\sqrt{N}$, so

$$\bar{a} = \frac{1}{N}\Big[(N-1)\cdot\frac{1}{\sqrt{N}} - \frac{1}{\sqrt{N}}\Big] = \frac{N-2}{N\sqrt{N}},$$

which for large N is slightly below $1/\sqrt{N}$ (Figure 3.12a). Diffusion reflects each amplitude about this mean. The amplitude of w lies below it by $\bar{a} + 1/\sqrt{N}$, so it moves equally far above:

$$a_w \longmapsto 2\bar{a} + \frac{1}{\sqrt{N}} = \frac{3N-4}{N\sqrt{N}} \approx \frac{3}{\sqrt{N}}.$$

The other amplitudes change under diffusion as $a_i \mapsto 2\bar{a} - 1/\sqrt{N} = (N-4)/(N\sqrt{N})$. For large N they remain close to $1/\sqrt{N}$, while the amplitude of w is approximately three times its initial value. The success probability is then approximately nine times larger, or about $9/N$. For small N we must use the exact formula.

Consider the small example $N = 4$. The mean after the oracle is $1/4$, so the amplitude of w jumps to $2\cdot 1/4 + 1/2 = 1$ and the others fall to $2\cdot 1/4 - 1/2 = 0$: one step finds w with certainty, as in §3.13. For $N = 16$ the amplitude of w rises from $1/4$ to $11/16$ and the others fall from $1/4$ to $3/16$ (Figure 3.12b). The probability of measuring w rises from $1/16$ to $121/256$, nearly one half.

We then repeat the step. It is easy to see what a whole step does to the amplitude of w. Let it be a_w before the step. The oracle changes it to $-a_w$; call the mean after the oracle $\bar{a}$. Diffusion then sends $-a_w$ to $2\bar{a} - (-a_w)$, so

$$a_w \longmapsto a_w + 2\bar{a}.$$

Thus the full step adds twice the mean calculated after the oracle to the amplitude of w. While this mean is positive, the marked amplitude increases step by step and the other amplitudes decrease each time: this is **amplitude amplification**. The bars and the arrow show the same thing: the amplitude of w is the sine of the arrow's angle, $\sin((2k+1)\bar{\theta})$, by (3.14). This is also visible in Figure 3.10, where amplitudes are drawn below each black arrow.

Amplification does not last forever. For sufficiently large N, after k^* steps the other amplitudes are near zero and the amplitude of w is near 1. The next oracle changes it to nearly -1, making the mean negative (Figure 3.12c). The step still adds twice the mean to the marked amplitude, but the mean is now negative, so the amplitude after the step is smaller than before it. For $N = 16$ the marked amplitude after three steps is 0.98. The fourth oracle changes it to -0.98, and diffusion raises it only to 0.76, less than before the oracle (Figure 3.12d). This is the overshoot of §3.13, seen in the bars.

3.15 Grover Search and Classical Unstructured Search

Classical search takes about $N/2$ queries, Grover's algorithm about $(\pi/4)\sqrt{N}$ (Figure 3.13). Can we do better? No: it has been proved that no quantum algorithm can find the marked element with

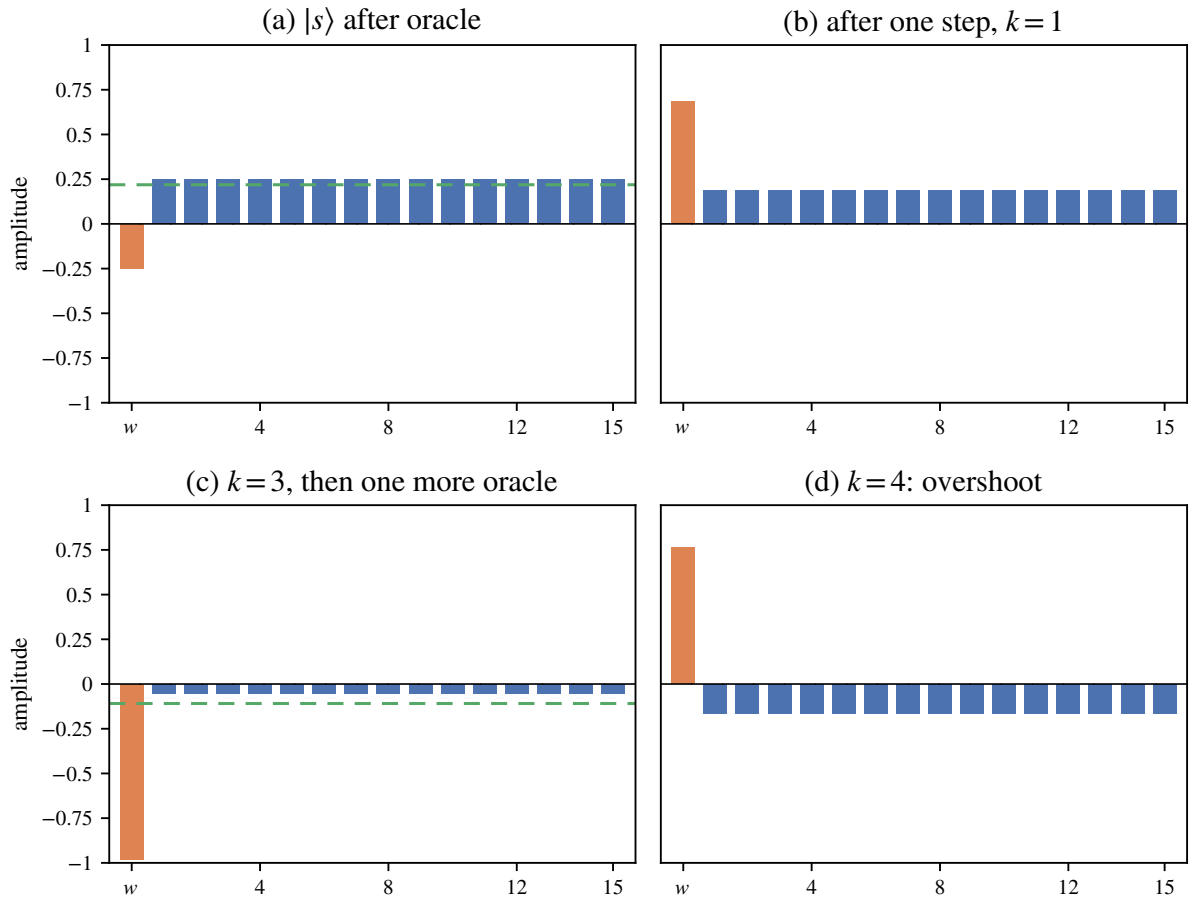


Figure 3.12. Amplitude amplification, $N = 16$. The amplitude of w is orange, the others blue, and the dashed green line is the mean $\bar{a}$. (a) State $|s\rangle$ after the oracle: w is below zero, the mean slightly below 1/4. (b) After one step w has jumped to 11/16 and the others fallen to 3/16. (c) After three steps and another oracle, the mean is negative. (d) The fourth step: reflection about the negative mean raises w only to 0.76, lower than before the fourth oracle (0.98); this is overshooting.

constant success probability using asymptotically fewer than $\sqrt{N}$ queries [7]. Grover's algorithm is therefore optimal in how its query count grows with N. A better algorithm could reduce that count only by a constant factor, however large N becomes.

We should assess the speedup soberly. It is **quadratic**, not exponential: $\sqrt{N}$ instead of N, not, for example, $\log N$ instead of N. It also applies to search without any order. If the problem has structure, such as alphabetical order, classical algorithms can also be much faster than $N/2$.

3.16 The Quantum Circuit for Grover's Algorithm

We now have all the pieces and can draw the complete circuit (Figure 3.14). The computer has n candidate qubits and one auxiliary qubit, as in §3.7. The circuit has three parts.

1. **Initialization.** A layer of H gates takes $|0 \ldots 0\rangle$ to $|s\rangle$ (§2.7). The auxiliary qubit starts in $|0\rangle$; an X gate changes it to $|1\rangle$ and an H gate to $|-\rangle$, by (2.5).

2. **The Grover step, repeated k^* times.** First comes the oracle: with the auxiliary qubit in $|-\rangle$, the check changes the sign only of the amplitude of w and leaves the auxiliary qubit in $|-\rangle$ (§3.7). Then comes diffusion: an H layer, an X layer, a gate that changes only the sign of the amplitude of $|1 \ldots 1\rangle$, and another X layer followed by an H layer.

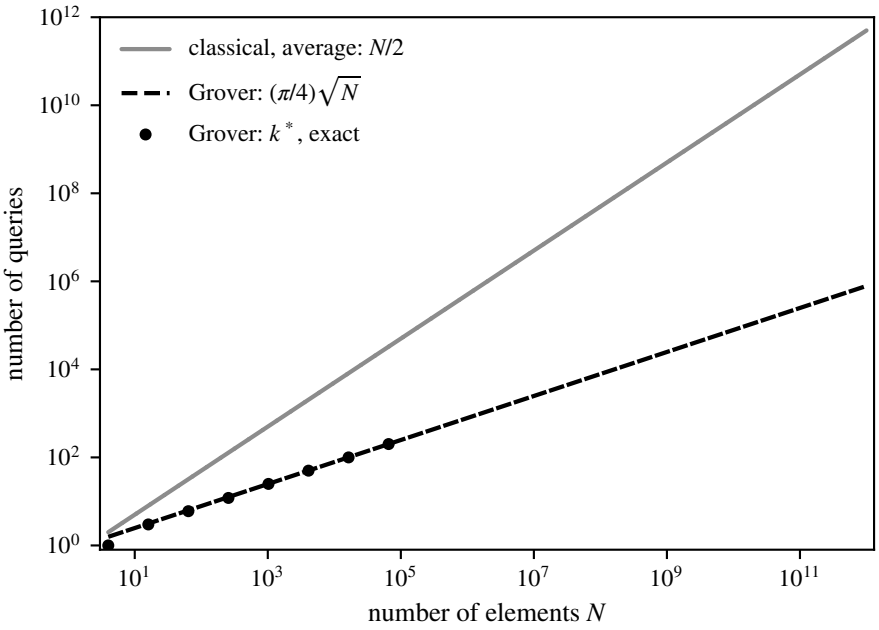


Figure 3.13. Number of queries against the number of elements N: classically $N/2$ on average, for Grover's algorithm $(\pi/4)\sqrt{N}$. Points show the exact values of k^*.

3. **Measurement.** Measuring the candidate qubits gives w with probability $\sin^2\big((2k^*+1)\bar{\theta}\big)$, by (3.14).

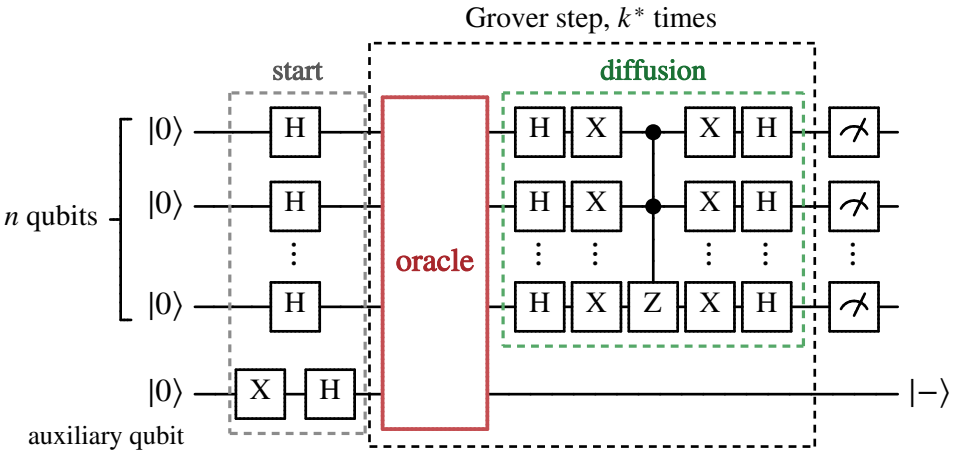


Figure 3.14. Grover's circuit for n candidate qubits (the dots stand for qubits between the second and last) and an auxiliary qubit. Dashed boxes mark initialization, diffusion, and the complete Grover step—oracle then diffusion—repeated k^* times. The gate with dots on every candidate qubit except the last and a square Z on the last changes the sign only of $|1\ldots1\rangle$'s amplitude.

Why does diffusion look like this? A layer of H gates takes $|0\ldots0\rangle$ to $|s\rangle$ (§2.7), and applying it twice has no effect: this holds for each H gate (§2.6), and gates on different qubits do not interfere with each other. The H layer therefore also takes $|s\rangle$ back to $|0\ldots0\rangle$. It preserves lengths and angles (§2.9), so a vector perpendicular to $|s\rangle$ becomes one perpendicular to $|0\ldots0\rangle$. Now consider three steps: an H layer, reflection about the $|0\ldots0\rangle$ axis—the operator $2|0\ldots0\rangle\langle0\ldots0| - \mathbb{I}$ from (3.9)—and another H layer. The first layer takes $|s\rangle$ to $|0\ldots0\rangle$, the reflection leaves it unchanged, and the second layer returns it to $|s\rangle$. A vector perpendicular to $|s\rangle$ is taken perpendicular to $|0\ldots0\rangle$, has its sign changed

by the reflection, and is returned by the second layer to its original direction with its sign changed. The three steps thus leave $|s\rangle$ unchanged and change the sign of everything perpendicular to it. This is reflection about $|s\rangle$, the operator U_s from (3.8):

$$U_s = 2|s\rangle\langle s| - \mathbb{I} = \mathrm{H}\big(2|0\ldots0\rangle\langle 0\ldots0| - \mathbb{I}\big)\,\mathrm{H} \tag{3.16}$$

Here H denotes the whole layer, $\mathrm{H}^{\otimes n}$. Reflection about $|s\rangle$ is thus reflection about $|0\ldots0\rangle$ enclosed by two H layers.

The central reflection keeps only $|0\ldots0\rangle$ unchanged and changes the signs of all other basis vectors. The circuit does the reverse. An X layer flips every bit in each label, moving the amplitude of $0\ldots0$ to $1\ldots1$. A Z gate on the last qubit, controlled by all the others, changes only the sign of $|1\ldots1\rangle$; for $n = 2$ it is CZ, for $n = 3$ it is CCZ (§2.8). A second X layer restores the amplitudes to their places. The circuit therefore changes only the sign of $|0\ldots0\rangle$, leaving the rest: it is $\mathbb{I} - 2|0\ldots0\rangle\langle 0\ldots0|$, the required reflection multiplied by -1, since $\mathbb{I} - 2|0\ldots0\rangle\langle 0\ldots0| = -\big(2|0\ldots0\rangle\langle 0\ldots0| - \mathbb{I}\big)$. Thus the shown circuit gives $-U_s$: in this algorithm it is physically equivalent to U_s, because the resulting states differ only by a global sign (§2.3).

The diffusion circuit is the same for every search problem. Only the oracle depends on the problem.

In this circuit the auxiliary qubit converts a reversible check into a phase oracle (§3.7). If, for a particular problem, we know how to change the sign of the amplitude of w directly, that auxiliary qubit is not needed. For $n = 2$ and $w = 11$, the CZ gate alone does it, and textbooks often draw the circuit this way.

3.17 Two Qubits, Step by Step

Let us follow the circuit for $n = 2$ and $w = 11$, column by column (Figure 3.15). The check "is the candidate 11?" asks whether both bits are 1. The oracle is therefore an X gate on the auxiliary qubit, controlled by both candidate qubits: a two-control CNOT called a **Toffoli gate**. The auxiliary qubit is in $|-\rangle$, so, as in §3.7, the gate changes only the sign of the amplitude of $|11\rangle$. In this teaching example we chose the marked string 11 in advance; the circuit is not used to discover an unknown answer, but to follow the gates' action. In other problems an oracle can be built from the rules of a check without knowing the solution beforehand, as in the Sudoku example (§3.5).

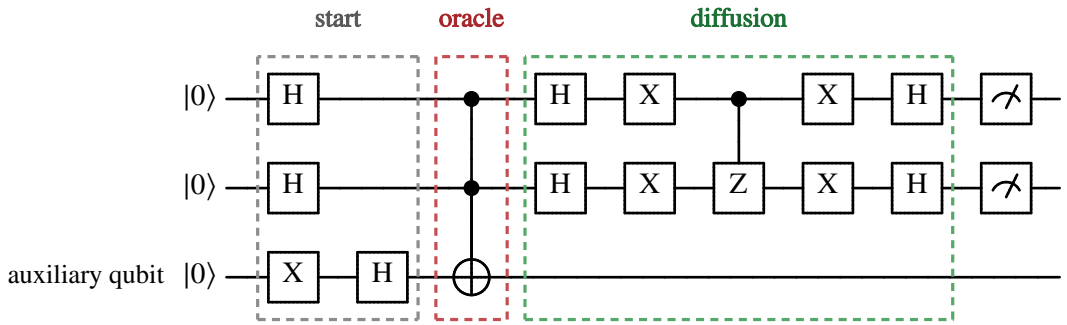


Figure 3.15. Grover's circuit for $n = 2$ and $w = 11$, with an auxiliary qubit and one step. The oracle is a Toffoli gate: it flips the auxiliary qubit if both candidate bits are 1. Dashed boxes mark initialization, the oracle, and diffusion.

Read the circuit as in §2.6, with qubit 1 at the top. Gates directly above one another form one circuit

column. The final symbol on the candidate lines, a small dial with a pointer, denotes measurement; the auxiliary qubit is not measured.

To calculate the state after each column, we need a rule for how a gate on one qubit acts on a multi-qubit state. This is the **pair rule**: the gate divides the amplitudes into pairs whose labels differ only in that qubit's bit, and acts on every pair in the same way, as on a vector in a plane. For $n = 2$, a gate on qubit 1 acts on (a_{00}, a_{10}) and (a_{01}, a_{11}); a gate on qubit 2 acts on (a_{00}, a_{01}) and (a_{10}, a_{11}). An X gate swaps the amplitudes in a pair, while H takes (a,b) to $\big((a+b)/\sqrt{2},(a-b)/\sqrt{2}\big)$, by (2.5) (Exercise 36). A controlled gate acts only on pairs whose control bits are 1; hence CZ changes only the sign of a_{11}.

For $N = 4$, $\bar{\theta} = 30°$, so $k^* = \lfloor \pi/(4\bar{\theta}) \rfloor = \lfloor 1.5 \rfloor = 1$: one step is enough. Table 3.2 gives the candidate amplitudes $(a_{00},a_{01},a_{10},a_{11})$ after every circuit column. After initialization, the auxiliary qubit remains in $|-\rangle$ throughout, so it is omitted from the table.

After	Candidate amplitudes
Input	$(1,0,0,0)$
H H (initialization)	$(1,1,1,1)/2$
Toffoli gate (oracle)	$(1,1,1,-1)/2$
H H	$(1,1,1,-1)/2$
X X	$(-1,1,1,1)/2$
CZ	$(-1,1,1,-1)/2$
X X	$(-1,1,1,-1)/2$
H H	$(0,0,0,-1)$

Table 3.2. Candidate amplitudes after each column of the circuit in Figure 3.15. The final five columns are diffusion.

Measurement gives 11 with probability $(-1)^2 = 1$: success on the first step, as in §3.13. The final minus is the sign of the whole vector discussed in §3.16; it is not observable.

Key Points from This Chapter

1. Unstructured search. With one marked solution among N possibilities, classical sequential checking requires $(N + 1)/2$ checks on average. Grover's algorithm uses on the order of $\sqrt{N}$ oracle queries with high success probability. Running time also depends on the cost of each query.

2. Oracle. The function $f(i)$ checks whether i is a solution. The phase oracle changes the sign of the marked amplitude:

$U_w|i\rangle = (-1)^{f(i)}|i\rangle$, or $U_w = \mathbb{I} - 2|w\rangle\langle w|$.

3. Why the oracle alone is not enough. A sign change alone does not alter measurement probabilities in the computational basis. Interference is also needed to redistribute amplitudes.

4. Diffusion. The operator $U_s = 2|s\rangle\langle s| - \mathbb{I}$ reflects the state about $|s\rangle$. It reflects each amplitude about the mean: $a_i \mapsto 2\bar{a} - a_i$.

5. The algorithm's plane. The initial state and every subsequent state lie in the plane spanned by $|w\rangle$ and the uniform superposition of unmarked states $|\bar{s}\rangle$. In that plane the oracle is reflection about $|\bar{s}\rangle$.

6. Two reflections. One Grover step is the oracle followed by diffusion. In the algorithm's plane it rotates the state through $2\bar{\theta}$, where $\sin\bar{\theta} = 1/\sqrt{N}$.

7. Steps and success. After k steps, the probability of the sought measurement outcome is $P_k(w) =$

$\sin^2((2k+1)\bar{\theta})$. For the first maximum choose $k^* = \lfloor \pi/(4\bar{\theta}) \rfloor \approx (\pi/4)\sqrt{N}$; then $P_{k^*}(w) \geq 1 - 1/N$. Too many steps can decrease the probability again.

This geometry of two reflections will allow us to compare the algorithm with colliding blocks in the next chapter.

3.18 Exercises

Exercises for Independent Study

These exercises practice the mathematical description of Grover's algorithm: from checking and the oracle, through diffusion and rotation, to step counts and quantum circuits. The last group presents further challenges. You need not solve all of them at once; choose according to what you want to practice.

Search, checks and the oracle

Exercise 51. Among $N = 100$ possibilities, the position of the sole solution is uniformly distributed and we check without repetition. How many checks are needed on average? What changes if there are 100 times as many possibilities?

Exercise 52. Let $N = 4$ and the marked state be $|10\rangle$. Write the function $f(i)$ and the phase-oracle matrix in the basis $|00\rangle$,$|01\rangle$,$|10\rangle$,$|11\rangle$. Apply the oracle to $|s\rangle$ and compare the probabilities of all outcomes before and afterward.

Exercise 53. A reversible check acts as $|c\rangle|h\rangle \mapsto |c\rangle|h \oplus f(c)\rangle$. For $f(c) = 1$, find the output when the auxiliary qubit is in $|0\rangle$, $|+\rangle$ and $|-\rangle$ in turn. What are the outputs for $f(c) = 0$?

Exercise 54. For $N = 8$ and $w = 101$, write $|\bar{s}\rangle$, find the angle between $|s\rangle$ and $|\bar{s}\rangle$, and apply the phase oracle to $|s\rangle$.

Exercise 55. If the number of possibilities grows 100-fold, approximately how do the numbers of classical checks and Grover steps change for large N? Must the actual running time change by the same factors?

Diffusion, projectors and reflections

Exercise 56. Show that reflection (3.6) preserves the state's length. *Hint: $|\psi_\parallel\rangle$ and $|\psi_\perp\rangle$ are perpendicular; calculate the squared length of $|\psi_\parallel\rangle \pm |\psi_\perp\rangle$ term by term.*

Exercise 57. Show that reflection about the arithmetic mean, (3.10), leaves the mean unchanged and that two applications restore the original numbers. *Hint: calculate the mean of $2\bar{a} - a_i$.*

Exercise 58. Apply diffusion to $(-1,1,1,1)/2$. *Hint: first calculate the mean amplitude.*

Exercise 59. For $N = 8$, start from $|s\rangle$. Calculate the mean amplitude after the oracle, then the marked and unmarked amplitudes after diffusion and the success probability.

Exercise 60. In the orthonormal basis $\{|\bar{s}\rangle,|w\rangle\}$, write the oracle and diffusion matrices. Multiply them in the correct order and show that a Grover step is a rotation through $2\bar{\theta}$.

Rotations and the number of Grover steps

Exercise 61. For $N = 16$, calculate $\bar{\theta}$, the number of steps to the first maximum and the success probabilities for $k = 0,1,2,3,4$. Draw a graph and explain what happens after the third step.

Exercise 62. For $N = 2$, calculate the success probability before and after the first Grover step. Compare both choices with the formula for k^*.

Exercise 63. Show that reflection about the second axis followed by reflection about the first gives a rotation through -2α, with the axes as in (3.12). *Hint: track the angle using (3.11).*

Exercise 64. Show that after k^* steps the arrow is at most $\bar{\theta}$ from $|w\rangle$, so $P(w) \geq \cos^2\bar{\theta} = 1 - 1/N$. *Hint:* $k^* \leq \pi/(4\bar{\theta}) < k^* + 1$ *implies* $2k^*\bar{\theta} \leq \pi/2 < 2k^*\bar{\theta} + 2\bar{\theta}$.

Exercise 65. How many Grover steps are needed for $N = 2^{20}$, and what is the success probability then? *Hint: for a small angle,* $\bar{\theta} \approx \sin\bar{\theta}$.

Exercise 66. Calculate the success probability for $n = 3$ after two steps using only fractions. *Hint: begin with amplitudes* $1/\sqrt{8}$ *and twice apply the oracle followed by reflection about the mean.*

Quantum circuits

Exercise 67. Follow the circuit in Figure 3.15 using the pair rule and compare your results with Table 3.2.

Exercise 68. In Table 3.2, check that the last five columns—the diffusion circuit—give $-(2\bar{a} - a_i)$, that is, diffusion with the signs of all amplitudes reversed. *Hint: before diffusion the state is* $(1,1,1,-1)/2$*; calculate the mean.*

Exercise 69. Construct an oracle for $w = 01$ along the lines of §3.17, using a Toffoli gate and X gates, with the auxiliary qubit in $|-\rangle$. Check that it changes only the sign of the amplitude of $|01\rangle$. *Hint: the candidate is 01 if qubit 1's bit is 0 and qubit 2's bit is 1. An* X *on qubit 1 before the Toffoli gate turns the first condition into "bit is 1"; the same gate afterward restores the candidate.*

Exercise 70. Construct a phase oracle for $w = 01$ and apply it to the uniform initial state of two qubits, then apply diffusion U_s. What state and measurement outcome do you obtain?

Exercise 71. Show that the layers H, X, controlled Z, X, H in §3.16 realize $-U_s$. How does that sign affect measurement probabilities?

Further challenges

Exercise 72. Suppose two of $N = 16$ elements are marked, w_1 and w_2, and the oracle changes both amplitudes' signs. Show that the account in §3.8–§3.13 remains the same if $|w\rangle$ is replaced by $(|w_1\rangle + |w_2\rangle)/\sqrt{2}$ and $|\bar{s}\rangle$ by a vector with equal amplitudes on the other 14 elements, and that $\sin\bar{\theta} = \sqrt{2/16}$. How many steps are needed, and with what probability will measurement yield one of the two marked elements? *Hint: for a state where* w_1 *and* w_2 *have equal amplitudes, the oracle changes the sign only of the component along the new* $|w\rangle$*. Then use (3.14) and (3.15).*

Exercise 73. If $M = 4$ of $N = 64$ states are marked, use $\sin\bar{\theta} = \sqrt{M/N}$. How many steps would you choose to reach the first maximum, and what is the probability of obtaining one of the marked states?

Exercise 74. One Grover step uses one oracle query of 400 gates and 40 other gates. How many gates do 100 such steps require in total? Does the number of queries alone determine that cost?

Exercise 75. For $N = 4$, compare the success probabilities after one step when one state is marked and when two are marked. What does this example say about choosing the number of steps if the number of marked states is unknown?

4. Two Problems, the Same Geometry

In the first chapter we counted the collisions between two blocks; in the third we derived Grover's algorithm. Both results involve π and a square root: approximately $\pi\sqrt{M/m}$ collisions, and approximately $(\pi/4)\sqrt{N}$ Grover queries. This is no coincidence. Let us see how the same geometric reflections underlie both problems.

4.1 The Setup: From Many Balls to Two Blocks

Our collision problem had two blocks and two velocities; a quantum state was described by N amplitudes. How can we connect the two descriptions? We will use a construction in which the large block consists of identical balls moving together.

Imagine N identical balls, each of mass 1, arranged in a line next to a wall. Glue $N-1$ of them together into one large block of mass $M = N-1$; they move together at velocity V. The remaining ball is the small block, with mass $m = 1$ and velocity v. The velocities of all N balls form the vector

$$|a\rangle = (v, V, V, \dots, V),$$

with one component for each ball. For a simpler notation, we placed the small ball's velocity first. If the marked element $|w\rangle$ occupies a different position, the component v goes in that position and the remaining components are V. The squared length is $v^2+(N-1)V^2 = 2E$. Set the total kinetic energy to $E = 1/2$: then $|a\rangle$ is a unit vector, just like the state of a system with N possible outcomes. The small ball corresponds to the marked element w, and the balls in the large block to the unmarked elements. As before, velocities are positive to the right, away from the wall.

Since the large block's balls are joined, only two velocities, v and V, are independent. We can also normalize the velocity vector for any energy $E > 0$ by dividing by $\sqrt{2E}$. This change of scale leaves angles and collision order unchanged. Choosing $E = 1/2$ simply makes the notation easier.

4.2 A Shared Plane of States

In Grover's plane, $|w\rangle$ is the marked basis vector, and $|\bar{s}\rangle$ is the normalized sum of the $N-1$ unmarked vectors. Each of its nonzero components is $1/\sqrt{N-1}$, so multiplying it by $\sqrt{N-1}V$ gives a component V in every unmarked position.

The vector $|a\rangle$ has component v at w and the same component V in all $N-1$ other positions. By the definition of $|\bar{s}\rangle$ in §3.8,

$$|a\rangle = v\,|w\rangle + \sqrt{N-1}\,V\,|\bar{s}\rangle = y\,|w\rangle + x\,|\bar{s}\rangle \tag{4.1}$$

because, by (1.4), $x = \sqrt{M}\,V = \sqrt{N-1}\,V$ and $y = \sqrt{m}\,v = v$. The scaled-velocity plane is therefore more than merely similar to Grover's plane: the point (x, y) represents the blocks' velocity vector in the plane spanned by $|\bar{s}\rangle$ and $|w\rangle$. Its horizontal axis is $|\bar{s}\rangle$ (the large block) and its vertical axis is $|w\rangle$ (the small block). The angle is the same too: $\tan\bar{\theta} = \sqrt{m/M} = 1/\sqrt{N-1}$ implies $\sin\bar{\theta} = 1/\sqrt{N}$, since a right triangle with legs 1 and $\sqrt{N-1}$ has hypotenuse $\sqrt{N}$.

For a normalized vector, $x^2 + y^2 = 1$; for arbitrary energy, $x^2 + y^2 = 2E$. The velocities are not physical quantum amplitudes: we identify coordinates and mathematical operations, while the physical

systems are different. Two blocks describe only this two-dimensional plane, not an arbitrary state with N independent components.

4.3 Collisions as Reflections

Bounce off the wall. Only the small ball hits the wall. Its velocity changes sign while the large block's velocity stays the same: $(x,y) \mapsto (x, -y)$. This is precisely the action of the phase oracle $U_w = \mathbb{I} - 2|w\rangle\langle w|$ in our plane, by (3.3).

Collision between the blocks. Consider it in a frame moving at the center-of-mass velocity:

$$v_{\text{cm}} = \frac{mv + MV}{m + M}.$$

Total momentum is conserved in the collision, so v_{cm} is the same before and after it. In the center-of-mass frame, total momentum is zero: the blocks' momenta have equal magnitudes and opposite directions. Total kinetic energy is also conserved. It equals the square of that momentum magnitude multiplied by $1/(2m) + 1/(2M)$, so the magnitude of each momentum stays the same.

After a one-dimensional elastic collision the blocks move apart. In the center-of-mass frame both momenta, and hence both velocities, therefore reverse direction. For the small block, $v' - v_{\text{cm}} = -(v - v_{\text{cm}})$, and the same holds for the large one. Returning to the floor frame gives

$$v' = 2v_{\text{cm}} - v, \qquad V' = 2v_{\text{cm}} - V \tag{4.2}$$

Each velocity is reflected about the center-of-mass velocity (the same result follows from (1.2); see Exercise 3). For N balls of mass 1, the center-of-mass velocity is simply the arithmetic mean of all their velocities:

$$v_{\text{cm}} = \frac{v + (N-1)\,V}{N} = \bar{a} \tag{4.3}$$

Each ball acquires velocity $2\bar{a} - a_i$. Diffusion, $U_s = 2|s\rangle\langle s| - \mathbb{I}$, acts on amplitudes by the same rule, according to (3.10). Within this plane it is the same linear operator, not merely a similar picture. The two-block model does not physically realize quantum states outside that plane. Thus:

$$\text{wall bounce} = \text{oracle}, \qquad \text{block collision} = \text{diffusion} \tag{4.4}$$

4.4 Comparing the Mechanical System with Grover's Algorithm

We can now compare the corresponding concepts in the mechanical problem and Grover's algorithm (Table 4.1).

Blocks	**Grover**
small ball, mass 1	marked element w
large block, mass $N-1$	$N-1$ unmarked elements
vector of ball velocities	vector of real amplitudes, in the same mathematical notation
$2E=1$ for the normalized velocity vector	sum of probabilities, 1
bounce off the wall	oracle
collision between blocks	diffusion
both blocks move toward the wall at the same speed	initial state: $-\lvert s\rangle$, the same quantum state as $\lvert s\rangle$
small block at rest, large block moving toward the wall	$-\lvert \bar{s}\rangle$
all energy in the small block	answer, $\pm\lvert w\rangle$

Table 4.1. A correspondence between the blocks and Grover's algorithm, after [2].

In the quantum description, reversing the global sign does not change the physical state; for the blocks, reversing the signs of all velocities reverses their motion.

4.5 Why Do the Step Counts Differ?

Compare the total number of collisions C in the original puzzle with the number of Grover queries k^*. For $m=1$ and $M=N-1$, both problems have the same angle $\bar{\theta}$, but different starting points and stopping conditions:

$$C=\left\lceil \frac{\pi}{\bar{\theta}} \right\rceil - 1, \qquad k^*=\left\lfloor \frac{\pi}{4\bar{\theta}} \right\rfloor, \qquad \bar{\theta}=\arctan\frac{1}{\sqrt{N-1}}=\arcsin\frac{1}{\sqrt{N}}.$$

For large N, the first formula gives $C \approx \pi\sqrt{N-1}$ and the second gives $k^* \approx (\pi/4)\sqrt{N}$, so C/k^* tends to four. This is not an exact equality for every N: collision and step counts are integers, and the initial conditions differ too. For example, at $N=4$ the original puzzle has five collisions and Grover's algorithm has one step.

Where does the approximate factor of four come from? We can understand it as two factors of two:

1. **What is counted.** One Grover step corresponds to a pair of collisions: a bounce off the wall, then a collision between the blocks. Grover's query count includes the oracle, not diffusion. Two collisions therefore correspond to one query in the mechanical representation of a Grover step.

2. **When we stop.** Grover stops near the marked direction after approximately a quarter of a circle. In the original puzzle collisions continue until the blocks move apart; the point travels approximately half a circle.

The starting points differ (Figure 4.1). In the original puzzle the small block is at rest and the large one moves toward the wall: the normalized vector is $-\lvert \bar{s}\rangle$. To represent Grover's starting state mechanically, both blocks move toward the wall at the same speed: the vector is $-\lvert s\rangle$. In the quantum description $-\lvert s\rangle$ and $\lvert s\rangle$ represent the same state, but for the blocks changing both velocity signs reverses their motion. That is why we choose negative velocities for the mechanical representation.

In this second setup the small block is closer to the wall and hits it first; a collision between the blocks follows. This pair acts as $U_s U_w$, like one Grover step, and the same order holds for subsequent pairs while physical collisions remain possible (Figure 4.2). The original puzzle uses the same reflections but starts from a different state, so its total collision count need not be a whole number of such pairs.

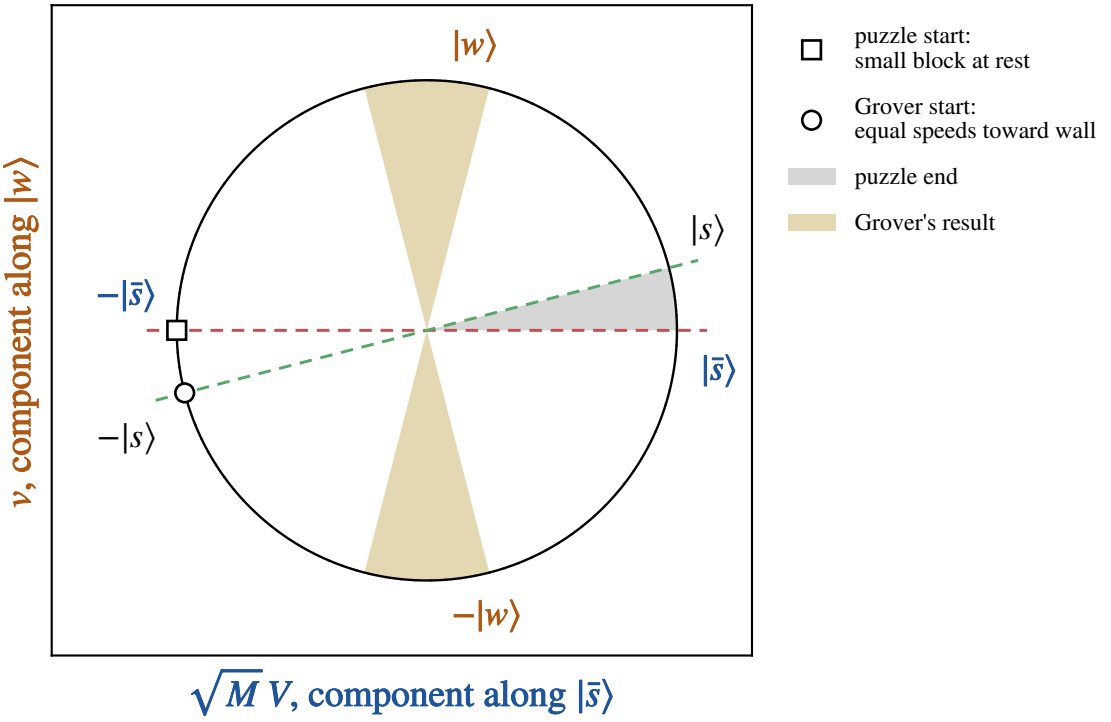


Figure 4.1. $M = 15$, $N = 16$, on the same circle. The square is the puzzle's starting point ($-|\bar{s}\rangle$: the small block is at rest and the large block moves toward the wall); the circle marks Grover's starting point in the block system ($-|s\rangle$: equal velocities toward the wall). The gray region is where the puzzle ends (no more collisions), between $|\bar{s}\rangle$ and $|s\rangle$. The gold regions are Grover's answer (within $\bar{\theta}$ of $|w\rangle$ or $-|w\rangle$, the same quantum state but opposite block velocities). The dashed red and green lines are the axes of the two reflections, the oracle and diffusion.

4.6 Example: Success on the First Try

For $N = 4$, Grover's algorithm finds w in one step (§3.13). In the block system, $M = 3$. The four balls' initial velocities are $(-1/2, -1/2, -1/2, -1/2)$: all move toward the wall at the same speed, and the energy is $4 \cdot (1/2)^2/2 = 1/2$. The small ball hits the wall: $v = 1/2$. The mean velocity is now $(1/2 - 3 \cdot 1/2)/4 = -1/4$, so the collision between the blocks gives $v' = 2 \cdot (-1/4) - 1/2 = -1$ and $V' = 2 \cdot (-1/4) + 1/2 = 0$. **The large block is at rest**, and all the energy is in the small one. This is the state $-|w\rangle$, the same quantum state as $|w\rangle$: success on the first try, on the blocks' side. The blocks would continue colliding, but Grover stops here.

In this last example, the minus sign on the velocity vector shows that the small block moves toward the wall. On the quantum side, a global minus sign does not change measurement probabilities.

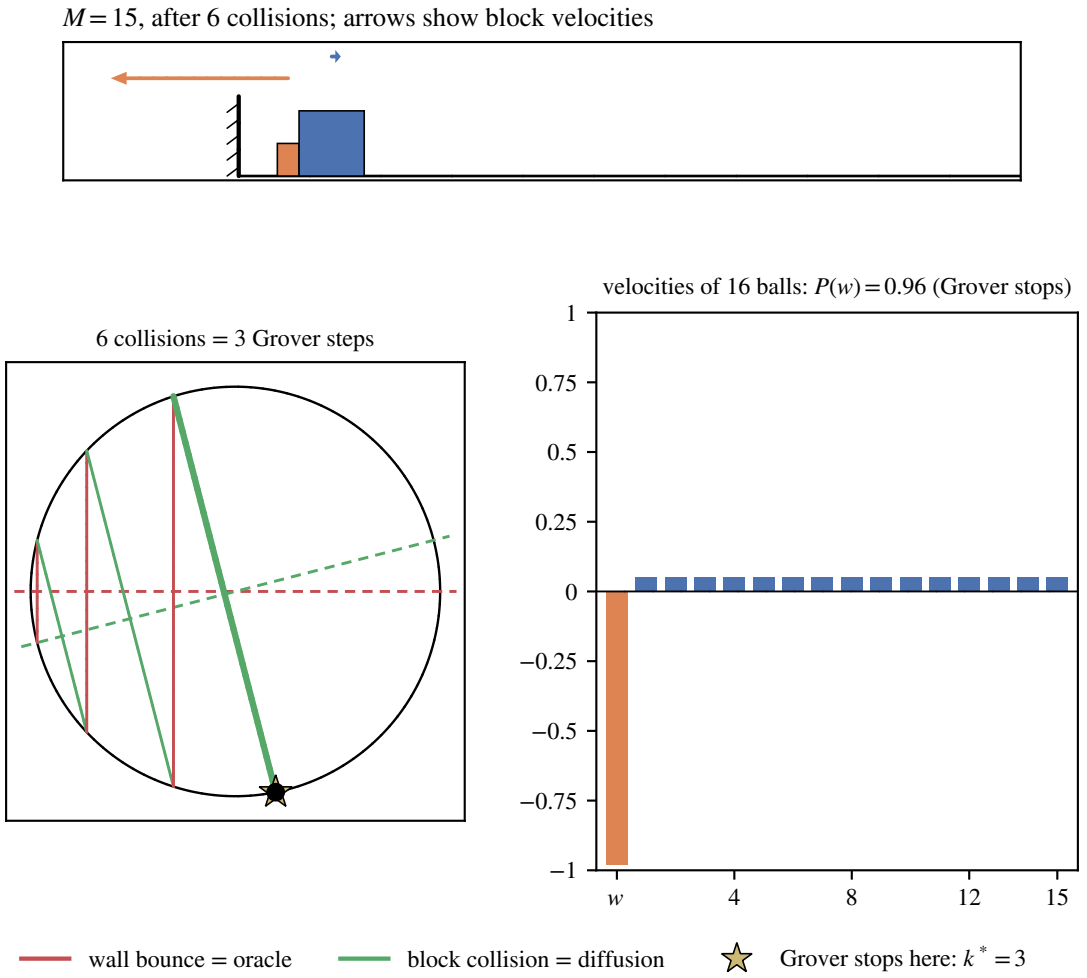


Figure 4.2. The moment at which Grover stops. Top: the blocks for $M = 15$ after 6 collisions; arrows show their velocities: the small block moves rapidly toward the wall, while the large block slowly moves away. Left: their point on the circle; 6 collisions make 3 Grover steps, and the star marks where Grover stops. Right: velocities of the 16 balls at the same moment, i.e. Grover's amplitudes with the sign of the entire vector reversed; $P(w) = 0.96$. The blocks would continue until their point had travelled roughly halfway around the circle, by which point Grover would have missed the target.

Key Points from This Chapter

1. From velocities to a vector. For $m = 1$ and $M = N - 1$, the balls' velocities are the components of $(v, V, \ldots, V)$. Its squared length is $2E$; dividing by $\sqrt{2E}$ gives a unit vector.

2. The same plane. The velocity vector has only two independent coordinates, $x = \sqrt{N-1}V$ and $y = v$. These are coordinates in the $|\bar{s}\rangle, |w\rangle$ plane, and the shared angle satisfies $\sin\bar{\theta} = 1/\sqrt{N}$.

3. Wall and oracle. A bounce off the wall changes y to $-y$: in this plane the phase oracle has the same action.

4. Collision and diffusion. The center-of-mass velocity is the mean velocity of the balls. A collision between the blocks maps each velocity a_i to $2\bar{a} - a_i$, just like diffusion.

5. Two collisions and a Grover step. A wall bounce followed by a block collision gives $U_s U_w$: a rotation by $2\bar{\theta}$. This holds for the corresponding order of collisions in the shared plane.

6. Starting and stopping matter. The original puzzle and the mechanical representation of Grover start differently and stop at different times. For large N, the total number of collisions is approximately four times the number of Grover queries; for finite N the ratio need not be exactly four.

The same mathematical operators describe two different physical systems. Their shared geometry lets us understand a conclusion from one problem in the context of the other.

4.7 Exercises

Exercises for independent work

These exercises connect block velocities to quantum states, and collisions to the oracle and diffusion. We then compare initial conditions and counts of collisions and Grover steps. The final exercises include a concrete example and additional challenges.

From Velocities to Quantum States

Exercise 76. For $N = 4$, determine the blocks' masses and write the velocity vector. Decompose it in the basis $\{|w\rangle,|\bar{s}\rangle\}$, first for arbitrary velocities v,V and then with the small block at rest.

Exercise 77. For $N = 8$, $v = 1$ and $V = 2$, calculate $2E$ and normalize the velocity vector. Write the result in the basis $\{|w\rangle,|\bar{s}\rangle\}$.

Exercise 78. Show that $\tan\bar{\theta} = 1/\sqrt{N-1}$ implies $\sin\bar{\theta} = 1/\sqrt{N}$. Why does the same angle occur in Grover's plane?

Exercise 79. Compare the mechanical starting points $-|\bar{s}\rangle$ and $-|s\rangle$: how do the blocks move, and which collision comes first? What would reversing the sign of the whole vector mean for their motion?

Collisions as Quantum Operators

Exercise 80. Derive (1.2) from the reflection (3.9). *Hint: for* $|r\rangle = (\sqrt{M}\,V, \sqrt{m}\,v)$ *and the unit vector* $|u\rangle = (\sqrt{M}, \sqrt{m})/\sqrt{M+m}$ *along the equal-velocity line (§1.9),* $\langle u|r\rangle = (MV + mv)/\sqrt{M+m}$*; divide the first component of the reflected vector by* $\sqrt{M}$ *and the second by* $\sqrt{m}$*.*

Exercise 81. For $m = 1$, $M = 3$ and arbitrary velocities v,V, calculate the velocities after a collision using both the elastic-collision formulas and reflection about the mean of four velocities. Compare the results.

Exercise 82. In the basis $\{|\bar{s}\rangle,|w\rangle\}$, write the matrices for a wall bounce and a collision between blocks for $m = 1$, $M = N-1$. Multiply them in the order wall first, then blocks, and determine the rotation angle.

Collision Counts and Grover Steps

Exercise 83. For $N = 4$, compare the total collision count in the original puzzle, the number of Grover steps, and the number of collisions in the mechanical representation up to Grover's stopping point. Is the ratio of the first two counts exactly four?

Exercise 84. Let $M = 15$ and $m = 1$, i.e. $N = 16$. How many collisions occur if the small block is initially at rest? After how many collisions does Grover stop if the blocks begin from Grover's starting state? *Hint:* $\sin\bar{\theta} = 1/4$*; use (1.8) and (3.15).*

Examples and Further Challenges

Exercise 85. Explain why for $N = 4$ one Grover step finds w with certainty, and why, for $M = 3$, when both blocks start toward the wall with the same velocity, the large block stops after two collisions. *Hint:* $3 \cdot 30° = 90°$.

Exercise 86. For $N = 16$, start with equal normalized velocities toward the wall. Find the small- and large-block velocities after three pairs of collisions, and the fraction of energy in the small block. Compare it with Grover's success probability.

Exercise 87. Further challenge: r of N elements are marked, with $0 < r < N$. If the balls in each group are joined into a separate block, what are the blocks' masses and the angle $\bar{\theta}$? In particular, calculate the angle and the number of Grover steps to the first maximum for $N = 8$, $r = 2$. Denote the masses of the marked and unmarked groups by m and M respectively; do not assume $M \geq m$.

Exercise 88. Explain why mathematical equality between the collision operators and Grover's operators in this plane does not mean that two classical blocks constitute a general-purpose quantum computer.

Appendix A. **Counting Collisions with a Ray of Light**

This is a side note rather than part of the main argument: we can also see the same collision count by drawing positions instead of velocities. Let d_1 be the distance of the large block from the wall and d_2 that of the small block. Assume the blocks are small enough to be treated as points. Define

$$\xi = \sqrt{M}\, d_1, \qquad \eta = \sqrt{m}\, d_2.$$

We multiply the distances by the square roots of the masses so that the point's velocity components are $\dot{\xi} = \sqrt{M}\, V$ and $\dot{\eta} = \sqrt{m}\, v$. Their sum of squares is therefore twice the kinetic energy.

The point (ξ, η) in the **position plane** moves as the blocks move. The small block cannot pass through the wall, so $d_2 \geq 0$, or pass the large block, so $d_2 \leq d_1$. The point therefore stays in the wedge between $\eta = 0$ and $\eta/\xi = \sqrt{m/M}$. By (1.9), the angle of this wedge is exactly $\bar{\theta}$.

At the boundary $d_1 = d_2$, $\eta/\xi = \sqrt{m/M}$, so the wedge angle is $\bar{\theta} = \arctan\sqrt{m/M}$: the same angle as in the scaled-velocity plane. The condition $0 \leq d_2 \leq d_1$ describes the ordering of the blocks in this point-particle idealization.

Velocities are positive away from the wall, and distances increase away from it, so the point's velocity is $(\sqrt{M}\, V, \sqrt{m}\, v) = (x, y)$: precisely the point in the scaled-velocity plane. Two things follow. First, the squared speed is $x^2 + y^2 = 2E$, so **the point's speed is constant**. Its direction changes at a collision; we can therefore compare its path geometrically with a ray of light. Second, collisions change (x, y) exactly as in §1.7. A bounce changes the sign of y, a reflection about the x-axis. A block collision moves the point to the other intersection of the momentum line with the circle. The momentum line is perpendicular to the equal-velocity line, and a diameter perpendicular to a chord bisects that chord, so this is reflection about the equal-velocity line. These are exactly the directions of the wedge's two sides. When the point hits a side, its velocity is reflected about that side, like a ray in a mirror: the angle of incidence equals the angle of reflection. **The point's path is like that of a light ray between two mirrors at an angle $\bar{\theta}$.**

Unfolding the wedge does not change the mechanical system: we reflect the geometric picture of its path. In a reflected copy, the incident and reflected portions form one straight line, and crossing a shared side corresponds to exactly one collision.

Here is the trick. Instead of reflecting the ray, reflect the entire wedge across the side the ray strikes, and let the ray continue straight. It passes through a fan of copies of the wedge, each with angle $\bar{\theta}$, and each reflection becomes a crossing of one fan line (Figure A.1). The lines emerge from the vertex at angles $\bar{\theta}, 2\bar{\theta}, 3\bar{\theta}, \ldots$, measured from the side $\eta = 0$. Initially the small block is at rest, so the ray moves parallel to that side. Viewed from the vertex, a line parallel to the side passes through all directions with angles strictly between 0 and π, and therefore crosses exactly those fan lines for which $j\bar{\theta} < \pi$. By the counting rule in §1.11, there are $\lceil \pi/\bar{\theta} \rceil - 1$ such lines: again (1.8).

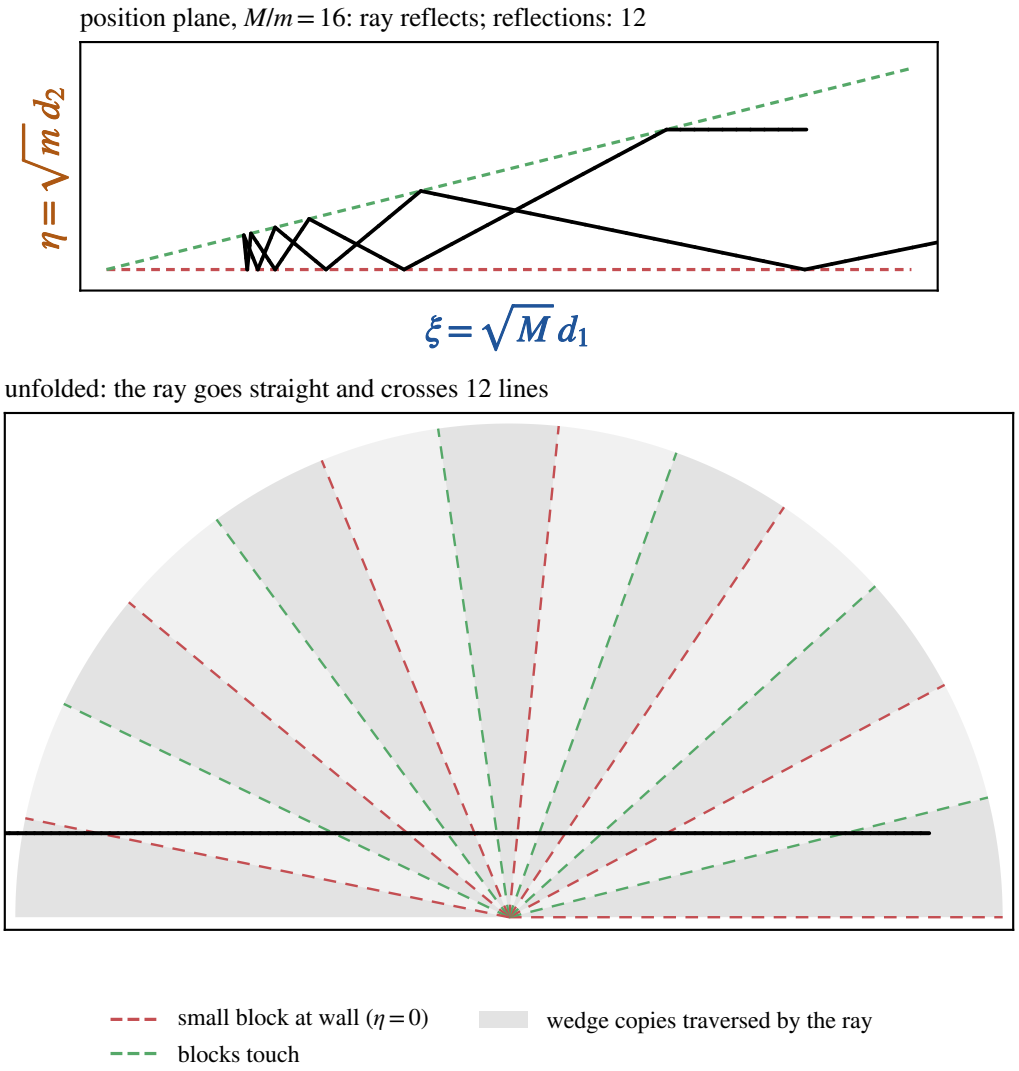


Figure A.1. $M/m = 16$. Top: the ray reflects 12 times in the wedge. Bottom: the same ray, unfolded, travels straight through a fan of wedge copies and crosses 12 lines.

Appendix B. **Radians, Small Angles and the Inscribed-Angle Theorem**

Radians and arc length

For a central angle φ in radians and a circle of radius R, the arc length is $\ell = R\varphi$. Only for a unit circle is $\ell = \varphi$: then the number of radians equals the length of the corresponding arc. The unit circle has circumference 2π, so π radians equals 180° and a right angle is $\pi/2$. In this text, an angle written without ° is in radians. Without radians, π would not appear in the collision count: in degrees the answer would be "180° divided by the angle"; the collision count would be unchanged, but π would not be visible in the formula.

The small-angle approximation

For a small angle t, an arc of length t lies between two line segments in Figure B.1a: the sine, which is a little shorter, and the tangent, which is a little longer. This follows by comparing three areas. The triangle with vertices at the circle's center, (1,0), and the end of the arc has base 1 and height $\sin t$, hence area $(\sin t)/2$. The circular sector is the fraction of the area π proportional to its angle, so its area is $t/2$. The right triangle with legs 1 and $\tan t$ has area $(\tan t)/2$. Each figure contains the preceding one, so for $0 < t < \pi/2$ we have $\sin t < t < \tan t$. For small angles, all three numbers are nearly equal:

$$\sin t \approx t \approx \tan t \qquad \text{for small } t. \tag{B.1}$$

For example, $\sin 0.1 = 0.0998$ and $\tan 0.1 = 0.1003$. The reverse also holds: an angle whose tangent is a small number t is approximately t, i.e. $\arctan t \approx t$, and is slightly less than t because the tangent is slightly greater than the angle.

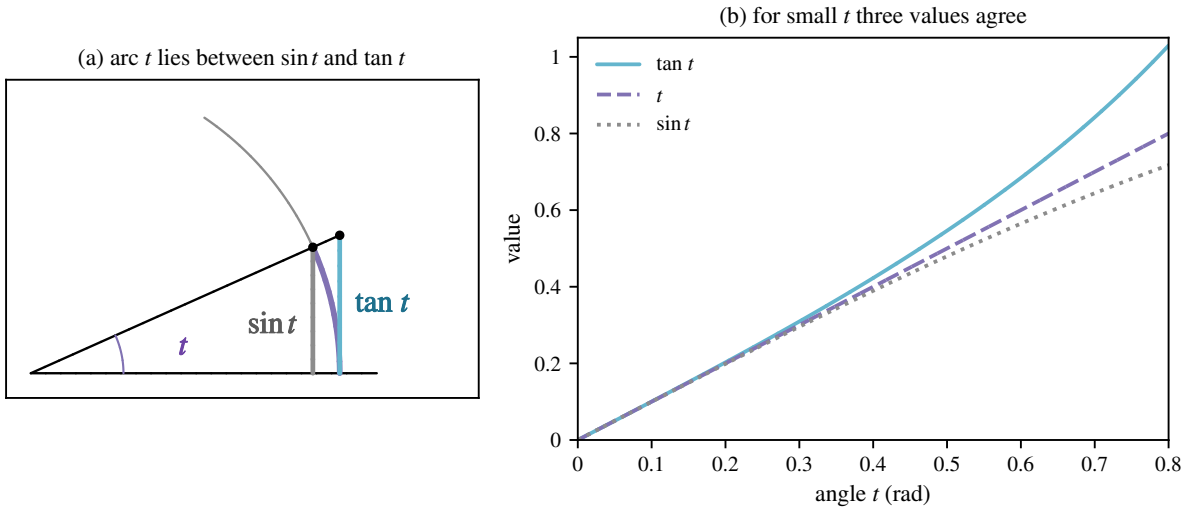


Figure B.1. (a) On a circle of radius 1, the arc of length t lies between $\sin t$ and $\tan t$. (b) The three values as functions of angle: they nearly coincide for small angles.

The central- and inscribed-angle theorem. In §1.10 we use the fact that an inscribed angle is half the central angle subtending the same arc. Here is a standard school proof (Figure B.2).

Let O be the center of a circle and A, B and C points on it. Angle BAC has its vertex A on the circle and its rays pass through B and C: it is the **inscribed angle** subtending the arc BC that does not

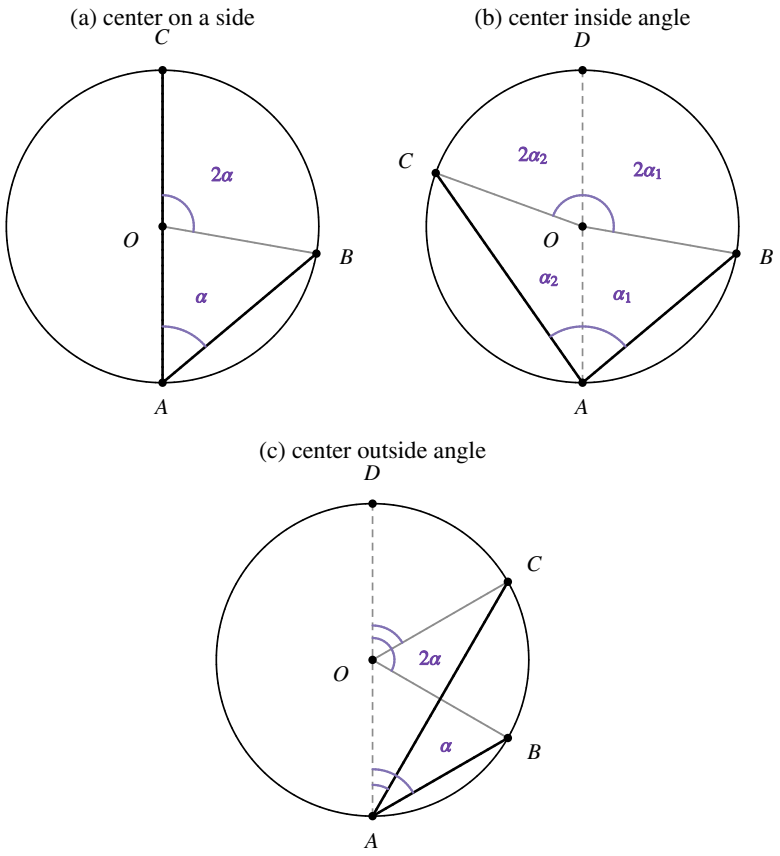


Figure B.2. The central- and inscribed-angle theorem. (a) The center O lies on the ray AC: triangle AOB is isosceles, so the central angle BOC is 2α. (b) Center inside the angle: diameter AD divides both angles into two parts of case (a), $\alpha_1 = \angle BAD$ and $\alpha_2 = \angle DAC$, so the central parts are $2\alpha_1$ and $2\alpha_2$ and add. (c) Center outside the angle: the parts from case (a) are subtracted. Arcs at A mark angles DAB and DAC; arcs at O mark DOB and DOC. Their differences are α and 2α.

contain A. The angle BOC subtending that same arc, which may be greater than 180°, is the **central angle**. We claim that $\angle BOC = 2\angle BAC$.

First consider the special case in which the center lies on ray AC, i.e. AC is a diameter (Figure B.2a). Segments OA and OB are radii, so triangle AOB is isosceles and its base angles at AB are equal. Call them α; one is the inscribed angle BAC. The angles in a triangle sum to π, so $\angle AOB = \pi - 2\alpha$. Points A, O and C lie on a straight line, so $\angle AOB + \angle BOC = \pi$. Hence $\angle BOC = \pi - (\pi - 2\alpha) = 2\alpha$.

The general case reduces to the special case. Draw diameter AD. If the center lies inside angle BAC (Figure B.2b), the diameter divides both angles into two: $\angle BAC = \angle BAD + \angle DAC$ and $\angle BOC = \angle BOD + \angle DOC$. Each is a special case because one ray is the diameter AD: $\angle BOD = 2\angle BAD$ and $\angle DOC = 2\angle DAC$. Adding gives $\angle BOC = 2\angle BAC$. If the center lies outside angle BAC (Figure B.2c), both rays are on the same side of the diameter and the angles are subtracted: $\angle BAC = \angle DAB - \angle DAC$ and $\angle BOC = \angle DOB - \angle DOC$; again $\angle BOC = 2\angle BAC$.

The inscribed angle $\bar{\theta}$ in §1.10 corresponds to the central angle $2\bar{\theta}$. On a circle of radius R the arc has length $2R\bar{\theta}$, and on the unit circle its length is numerically equal to $2\bar{\theta}$. This is an ancient theorem: Proposition 20 of Book III of Euclid's *Elements*.

Glossary

Amplitude – a component of a state in a chosen basis, $a_i = \langle i|\psi\rangle$. In our real model $P(i) = a_i^2$; for complex amplitudes $P(i) = |a_i|^2$.

Amplitude amplification – a procedure in which unitary operations increase the probability of marked outcomes. In Grover's algorithm, after too many steps the probability decreases again (§3.14).

Ancilla qubit – an additional qubit into which the check writes its result. In the state $|-\rangle$ it transfers a sign to the candidate's amplitude while remaining unchanged itself.

Basis – mutually perpendicular unit vectors from which all vectors can be built by addition and multiplication by numbers; in a plane these are $|0\rangle$ and $|1\rangle$.

Bounce off the wall – the small block hits the wall and reverses direction, $v \to -v$. In the scaled-velocity plane this is reflection about the x-axis, and in Grover's algorithm it corresponds to the oracle.

Bra – the left half of an inner product, $\langle\varphi|$; together with the ket $|\psi\rangle$ it gives the number $\langle\varphi|\psi\rangle$.

Collapse – the change of state after measurement; in an ideal measurement in the basis used here, the state becomes the basis vector for the observed outcome.

Collision between blocks – an elastic collision between the small and large blocks. In the scaled-velocity plane it is reflection about the equal-velocity line; in Grover's algorithm it corresponds to diffusion.

Complexity – how the number of steps of an algorithm grows with problem size N; written $O(\ldots)$, for example $O(N)$ or $O(\sqrt{N})$.

Complexity class – a set of decision problems classified by the computational resources needed to solve them. In P an answer can be found in polynomial time; in NP a yes-answer can be verified in polynomial time given a suitable certificate (§3.3).

Conservation law – a statement that a quantity, such as energy or momentum, remains unchanged during the motion.

Controlled gate – a gate that acts only on those pairs of amplitudes whose labels have control-qubit bit 1.

Diffusion – the reflection in Grover's algorithm that does not use the oracle: reflection about the axis $|s\rangle$. It reflects each amplitude about the arithmetic mean of all amplitudes, $a_i \to 2\bar{a} - a_i$.

Elastic collision – a collision in which the total kinetic energy of the colliding bodies is conserved.

Equal-velocity line – the line in the scaled-velocity plane on which $V = v$. It makes an angle $\bar{\theta}$ with the x-axis, by (1.9), and bounds the final region (§1.9). A collision between blocks is reflection about it (Appendix A, Exercise 80).

Final region – the set of states from which no further collision can occur, specified by $0 \le v \le V$. In the scaled-velocity plane it is the wedge between the positive x-axis and the equal-velocity line.

Grover's algorithm – quantum search: start in $|s\rangle$, perform $k^* \approx (\pi/4)\sqrt{N}$ Grover steps, then measure.

Grover step – the oracle followed by diffusion. In the $|\bar{s}\rangle$, $|w\rangle$ plane this is a rotation through $2\bar{\theta}$.

Hadamard gate – the single-qubit gate H, $(a, b) \to \big((a+b)/\sqrt{2}, (a-b)/\sqrt{2}\big)$: reflection about a line at 22.5°. It takes $|0\rangle$ to $|+\rangle$ and $|1\rangle$ to $|-\rangle$.

Hash function – a function mapping data to a fixed-length digest. Cryptographic hash functions are intended to make the digest easy to calculate but finding an input for a given digest computationally hard.

Identity operator – the operator $\mathbb{1}$, which leaves every vector unchanged.

Inner product – the number $\langle\varphi|\psi\rangle$; for real vectors it equals the sum of products of corresponding components, and the product of the lengths and the cosine of the angle between them.

Inscribed angle – an angle with its vertex on a circle and sides intersecting the circle; it equals half the central angle subtending the same arc (the inscribed-angle theorem, proved in Appendix B).

Interference – the addition and cancellation of contributions to amplitudes when a step mixes amplitudes; for example, H returns $|+\rangle$ to $|0\rangle$.

Ket – Dirac's notation for a vector, $|\psi\rangle$.

Layer – gates drawn vertically aligned in a circuit and acting in the same step (§2.7).

Line of constant momentum – the line in the scaled-velocity plane whose points have the same total momentum, (1.6); its slope is $-\sqrt{M/m}$. Points before and after a collision between blocks lie on the same line (§1.7).

Marked element – the element w we are looking for.

Matrix – a table of numbers representing a linear operator: column i is the image of the basis vector $|i\rangle$.

Measurement – a process with possible outcomes; in our model an ideal measurement in the chosen basis yields outcome i with probability a_i^2.

Momentum – mass times velocity. In a collision between two blocks, their total momentum does not change.

Operator – a rule assigning a vector to every vector; the steps of a quantum computer are linear operators.

Oracle – a checking procedure or a corresponding quantum operator accessed by the algorithm through queries. A phase oracle changes the sign of the amplitudes of marked states and leaves the others unchanged (§3.5).

Outcome – one of the possible results of a measurement. Each outcome i corresponds to a basis vector $|i\rangle$.

Pair rule – a single-qubit gate acts in the same way on each pair of amplitudes whose labels differ only in that qubit's bit.

Perpendicular – making a right angle. Two vectors are perpendicular if their inner product is zero.

Position plane – the plane in which the positions of the two blocks are represented by a point $(\sqrt{M}\,d_1, \sqrt{m}\,d_2)$.

Projection – the part of $|r\rangle$ along a unit vector $|u\rangle$, namely $\langle u|r\rangle\,|u\rangle$.

Projector – an operator that extracts the projection onto a subspace. For a unit vector $|u\rangle$, the projector onto its direction is $|u\rangle\langle u|$.

Quantum circuit – a sequence of quantum gates.

Quantum gate – a unitary operator acting on one or more qubits.

Qubit – a quantum system with a two-dimensional state space; its computational basis consists of $|0\rangle$ and $|1\rangle$.

Query – one use of the oracle.

Radian – a measure of angle: the length of the arc cut off by the angle on a circle of radius 1. An angle of π radians is 180°.

Reflection – a transformation that keeps the part of a state along the reflection axis and changes the sign of the part perpendicular to it, (3.6); in a plane this is the familiar reflection about a line. Reflection about the axis through a unit vector $|u\rangle$ is $2|u\rangle\langle u| - \mathbb{1}$, (3.9).

Reflection about the arithmetic mean – the transformation $a_i \to 2\bar{a} - a_i$: each component moves to the other side of the mean, the same distance from it. In Grover's algorithm it is called diffusion.

Rotation – turning all vectors about the origin through the same angle.

Scaled-velocity plane – the plane with coordinates $(x,y) = (\sqrt{M}\,V, \sqrt{m}\,v)$; for constant energy the possible velocities lie on a circle (§1.6).

Small-angle approximation – for a small angle t measured in radians, $\sin t \approx t \approx \tan t$ and $\arctan t \approx t$, (1.10) and (B.1).

State – a unit vector $|\psi\rangle = \sum_i a_i |i\rangle$ describing a quantum system.

Sum modulo 2 – the bit operation $\oplus$: $0 \oplus 0 = 1 \oplus 1 = 0$ and $0 \oplus 1 = 1 \oplus 0 = 1$.

Superposition – a linear combination of basis vectors; we generally use the term when more than one amplitude is nonzero in the chosen basis.

Tensor product – the operation used to combine spaces and states of systems; for example, $|0\rangle \otimes |1\rangle = |01\rangle$. Entangled states cannot be written as products of the states of the individual qubits.

Toffoli gate – an X gate on one qubit controlled by two others, i.e. CNOT with two controls (§3.17).

Truth table – a table giving the output of a gate for each input basis vector.

Uniform superposition – a state in which all possibilities have the same amplitude, such as $|s\rangle$ in (2.7).

Unit vector – a vector of length 1.

Unitary operator – a linear operator that preserves inner products and has an inverse. Quantum gates are unitary; measurement is a different process.

Unstructured search – search without useful structure that would identify promising candidates; classically, we check them one by one (§3.2).

Velocity plane – the plane with coordinates (V,v), the velocities of the large and small blocks; for constant energy the possible velocities lie on an ellipse (§1.5).

Symbols

Quantum states and operators

$|\psi\rangle$, $\langle\varphi|$, $\langle\varphi|\psi\rangle$ – ket, bra and inner product (§2.1, §2.9).

$\|\psi\|$ – the length of $|\psi\rangle$.

λ, μ – numbers used to multiply vectors.

$|0\rangle$, $|1\rangle$ – the basis vectors of the plane, associated with qubit outcomes 0 and 1.

$|i\rangle$, a_i – the basis vector for outcome i and the amplitude of that outcome, $a_i = \langle i|\psi\rangle$.

$\sum_i$ – the sum over all N outcomes i.

γ – the angle between two vectors, (2.8).

$P(i)$ – the probability that measurement yields outcome i.

$O(\ldots)$ – an asymptotic upper bound on growth; $O(N)$ means that, for sufficiently large N, the number of steps is bounded by a constant multiple of N (§3.3).

$\otimes$ – tensor product (§2.4).

$|+\rangle$, $|-\rangle$ – the states $(|0\rangle + |1\rangle)/\sqrt{2}$ and $(|0\rangle - |1\rangle)/\sqrt{2}$, (2.5).

$|r\rangle$ – an arbitrary vector that we split into its projection and remainder (§2.9, Exercise 80).

$|u\rangle$ – a unit vector: projector $|u\rangle\langle u|$ (§2.9) and reflection axis (§3.10).

$|\psi_\parallel\rangle$, $|\psi_\perp\rangle$ – the components of a state along and perpendicular to the reflection axis (§3.9).

φ, α – the angle of the state, measured from the $|\bar{s}\rangle$ axis; the angle between two reflection axes (§3.11).

β, β_1, β_2 – the angle of a reflection axis, measured from $|\bar{s}\rangle$; the angles of two axes (§3.11).

$|s\rangle$ – the vector whose components are all equal, (2.7).

$\bar{a}$ – the arithmetic mean of the components (§3.10, §3.14).

$|a\rangle$ – a vector with components a_i; in chapter 4, the vector of velocities of all the balls (§4.1).

$\lfloor q \rfloor$, $\lceil q \rceil$ – rounding down (§3.13) and up (§1.11).

Mechanics and geometry

m, M – masses of the small and large blocks.

v, V – velocities of the small and large blocks, positive when the block moves to the right, away from the wall.

V_0 – the initial speed of the large block: initially $V = -V_0$ (§1.4).

E, p – kinetic energy and momentum.

x, y – coordinates in the scaled-velocity plane, $x = \sqrt{M}\,V$ and $y = \sqrt{m}\,v$; in Grover's algorithm, coordinates of the state in the $|\bar{s}\rangle$, $|w\rangle$ plane (§3.9).

Δx, Δy – the legs of the narrow triangle along an oblique segment in the scaled-velocity plane, (1.9).

$\bar{\theta}$ – for the blocks, the angle between a vertical and an oblique segment in the scaled-velocity plane, $\tan\bar{\theta} = \sqrt{m/M}$; for Grover's algorithm, the angle between $|\bar{s}\rangle$ and $|s\rangle$, $\sin\bar{\theta} = 1/\sqrt{N}$.

j – the index of a collision or a line in the fan (Appendix A).

M_{wall}, V_{wall} – mass and velocity of the wall, when imagined as a block of enormous mass (§1.3).

D – the integer $D \geq 0$ in the mass ratio $M/m = 100^D$.

t – a small angle or a small number (§1.12, Appendix B).

u – the velocity of both blocks when their velocities are equal (§1.9).

d_1, d_2 – the distances of the large and small blocks from the wall.

ξ, η – coordinates in the position plane, $\xi = \sqrt{M}\, d_1$ and $\eta = \sqrt{m}\, d_2$.

Search and quantum circuits

N, w, n – in search, the number of possibilities, the marked element and the number of qubits, $N = 2^n$; in §1.11, N denotes the number of collisions.

$|w\rangle$, $|\bar{s}\rangle$ – the basis vector of the marked element; the state in which all unmarked elements have equal amplitudes and the marked element has amplitude zero.

k – the number of Grover steps (§3.13).

$|\psi_k\rangle$ – the state after k steps, (3.14).

k^*, $P(w)$ – the selected number of steps near the first maximum and the probability of the marked outcome. In a tie, the neighboring step count can be equally good (§3.13).

H, X, Z, CZ – the gates from §2.6 and §2.8, written in upright letters.

CNOT, CCZ – controlled gates (§2.8).

$\mathbb{1}$, $|u\rangle\langle u|$ – the identity operator and a projector (§2.9).

U_w, U_s – the oracle and diffusion as operators, (3.3) and (3.8).

f, c, h, $\oplus$ – the check, a candidate, the ancilla qubit's bit and addition modulo 2 (§3.4, §3.7).

v_{cm} – center-of-mass velocity, $(mv + MV)/(m + M)$, (4.2).

C – the total number of collisions in the original mechanical puzzle (§4.5).

r – the number of marked elements in the extension of the search to multiple solutions (Exercise 87).

ℓ, R – arc length and circle radius; $\ell = R\varphi$ for an angle φ in radians (Appendix B).

Further Reading and Viewing

- Adam Brown, the paper connecting the blocks and Grover's algorithm [2]: a research paper for readers who want to compare these derivations with the original.
- Two educational 3Blue1Brown videos: one on the blocks [1] and one on Grover's algorithm [6].
- Nielsen and Chuang, chapter 6 [8]: a standard textbook on quantum computing; it requires more mathematical preparation.

References

[1] 3Blue1Brown, "The most unexpected answer to a counting puzzle" (2019). 3blue1brown.com/lessons/clacks · "Why colliding blocks compute pi" (2025). youtu.be/6dTyOl1fmDo

[2] A. R. Brown, "Playing Pool with $|\psi\rangle$: from Bouncing Billiards to Quantum Search", *Quantum* **4**, 357 (2020). doi:10.22331/q-2020-11-02-357 · arXiv:1912.02207

[3] P. A. M. Dirac, "A new notation for quantum mechanics", *Mathematical Proceedings of the Cambridge Philosophical Society* **35**, 416–418 (1939). doi:10.1017/S0305004100021162

[4] G. Galperin, "Playing pool with π (the number π from a billiard point of view)", *Regular and Chaotic Dynamics* **8**(4), 375–394 (2003). doi:10.1070/RD2003v008n04ABEH000252

[5] L. K. Grover, "Quantum mechanics helps in searching for a needle in a haystack", *Phys. Rev. Lett.* **79**, 325–328 (1997). doi:10.1103/PhysRevLett.79.325

[6] 3Blue1Brown, "But what is quantum computing? (Grover's Algorithm)" (2025). youtu.be/RQWpF2Gb-gU

[7] C. H. Bennett, E. Bernstein, G. Brassard, U. Vazirani, "Strengths and weaknesses of quantum computing", *SIAM J. Comput.* **26**, 1510–1523 (1997). doi:10.1137/S0097539796300933 · arXiv:quant-ph/9701001

[8] M. A. Nielsen, I. L. Chuang, *Quantum Computation and Quantum Information*, 10th Anniversary Edition, ch. 6 (Cambridge University Press, 2010). Cambridge University Press

[9] L. K. Grover, "From Schrödinger's equation to the quantum search algorithm", *Am. J. Phys.* **69**, 769–777 (2001). arXiv:quant-ph/0109116

[10] Massachusetts Institute of Technology, *Introduction to Algorithms*, Lecture 19: Complexity (2020). MIT OpenCourseWare

[11] M. Boyer, G. Brassard, P. Høyer, A. Tapp, "Tight bounds on quantum searching", *Fortschritte der Physik* **46**, 493–505 (1998). arXiv:quant-ph/9605034

Final Answers to the Exercises

Only **final answers** are given here, without worked solutions. They are grouped by chapter. For exercises asking for a proof, the result to be established is given, not the proof itself. Expressions differing only by a global sign can describe the same quantum state; where relevant, we retain the sign that follows from the specified gate sequence.

Chapter 1 — Blocks That Count π

1. 3 collisions.

2. 5 collisions.

3. $v' = 2v_{\mathrm{cm}} - v$; $V' = 2v_{\mathrm{cm}} - V$.

4. $v' = -6$, $V' = -2$; before and after the collision $E = 24$, $p = -12$.

5. $v' = 3$; $\Delta p = 12$; kinetic energy before and after impact is 9.

6. Respectively: wall collision; block collision; no further collisions.

7. $4V^2 + v^2 = 16$; semiaxes 2 along V and 4 along v; $R = 4$; $(x,y) = (-4,0)$.

8. The constant-momentum line has slope -4 and the equal-velocity line $1/4$; their product is -1.

9. $E = 4$; $(x,y) = (-2,-2)$; $R = \sqrt{8}$; after the bounce $(x,y) = (-2,2)$.

10. (0,2) and (1,1) are in the final region. For (2,1) the blocks approach each other; for $(-1,3)$ the small block moves toward the wall.

11. Energy quadruples and the radius doubles; the angles and collision count remain unchanged.

12. 3; 3.

13. The central angle is $30° = \pi/6$; arc length $\pi/2$.

14. 3, 5 and 15 collisions, respectively. In the first two cases $\pi/\bar{\theta}$ is an integer, so the strict inequality requires subtracting 1.

15. For $M/m = 16$: 12 collisions; for $M/m = 10^6$: 3141 collisions.

16. Exactly 31 collisions; approximation $10\pi \approx 31.4159$; difference $10\pi - 31 \approx 0.4159$.

17. Binary: $a = 4$; for $D = 0,1,2,3$ the counts are 3,6,12,25, or $(11)_2$, $(110)_2$, $(1100)_2$ and $(11001)_2$. For base 3: $a = 9$.

18. $a = b^2$, or $M/m = b^{2D}$; the approximate count is πb^D, but the approximation alone does not guarantee equal integer parts.

19. $\arctan(0.1) \approx 0.0997$; $\pi/0.1 \approx 31.4159$; $\pi/\arctan(0.1) \approx 31.5204$. Both integer parts are 31.

20. $\lfloor 2.999 \rfloor = 2$ and $\lfloor 3.001 \rfloor = 3$; a small difference can cross an integer boundary.

Chapter 2 — Fundamentals of Quantum Mechanics and Quantum Computing

21. $\lambda = 1/\sqrt{5}$; $P(0) = 1/5$, $P(1) = 4/5$.

22. $|\psi\rangle = (-2|1\rangle + |3\rangle)/\sqrt{5}$; $(P_0,P_1,P_2,P_3) = (0,4/5,0,1/5)$.

23. $(1,-1)/\sqrt{2} = |-\rangle$; $\|\psi\| = 1$; $P(0) = P(1) = 1/2$.

24. $P(0) = 3/4$, $P(1) = 1/4$; after outcome 1 the state is $|1\rangle$ and a repeat measurement gives 1 with certainty.

25. $|\psi\rangle$ and $-|\psi\rangle$ represent the same physical state, while $\mathrm{Z}|\psi\rangle$ is different; for all three vectors $(P_0,P_1) = (3/4,1/4)$.

26. Both have $(P_0,P_1) = (1/2,1/2)$; $\langle +|-\rangle = 0$; a +45° rotation gives $|+\rangle \mapsto |1\rangle$ and $|-\rangle \mapsto |0\rangle$.

27. In the $\{|0\rangle,|1\rangle\}$ basis: $P(0) = 1$; in the $\{|+\rangle,|-\rangle\}$ basis: $P(+) = P(-) = 1/2$.

28. $\|\psi\| = 1$; $(P_0,P_1,P_2) = (1/9,4/9,4/9)$; $P(1 \text{ or } 2) = 8/9$.

29. 37/64.

30. $|+\rangle \otimes |-\rangle = (|00\rangle - |01\rangle + |10\rangle - |11\rangle)/2$; amplitudes $(1,-1,1,-1)/2$.

31. $P(00) = 3/8$; $P(11) = 1/8$; $P(\text{first bit} = 1) = 1/4$.

32. $P(00) = P(11) = 1/2$; $P(01) = P(10) = 0$; the state is not a product state—it is entangled.

33. 8 basis states; $P(101) = 1/8$; $P(\text{first bit} = 1) = 1/2$.

34. $\mathrm{X}(a|0\rangle + b|1\rangle) = b|0\rangle + a|1\rangle$; $\mathrm{X}|-\rangle = -|-\rangle$, the same physical state.

35. $R|0\rangle = |1\rangle$; $R|1\rangle = -|0\rangle$; $R^T R = \mathbb{I}$; rotation by +90°.

36. $\mathrm{H}(a,b) = ((a+b)/\sqrt{2},(a-b)/\sqrt{2})$; $\mathrm{H}^2 = \mathbb{I}$.

37. $|0\rangle \mapsto |0\rangle$; $|1\rangle \mapsto -|1\rangle$; $\mathrm{HXH} = \mathrm{Z}$.

38. Amplitudes: $((\sqrt{3}+1)/(2\sqrt{2}),(\sqrt{3}-1)/(2\sqrt{2}))$; probabilities: $P(0) = (2+\sqrt{3})/4$, $P(1) = (2-\sqrt{3})/4$.

39. $|s\rangle = \frac{1}{\sqrt{8}} \sum_{i=0}^{7} |i\rangle$; $P(101) = 1/8$; $P(\text{first bit} = 1) = 1/2$; 3 gates in one layer.

40. $(|00\rangle + |11\rangle)/\sqrt{2}$; outcomes 00 and 11, each with probability 1/2.

41. $(|00\rangle + |01\rangle + |10\rangle - |11\rangle)/2$; all four outcomes have probability 1/4.

42. Output amplitudes in the order 00,01,10,11: $(1,1,-1,1)/2$.

43. Only the amplitude of $|111\rangle$ changes sign; $\left(\sum_{i=0}^{6} |i\rangle - |111\rangle\right)/\sqrt{8}$; $P(111) = 1/8$.

44. $\langle s|\psi\rangle = 1/2$; $\gamma = 60°$.

45. $\langle +|-\rangle = 0$; $\langle 0|+\rangle = 1/\sqrt{2}$; $\langle 1|-\rangle = -1/\sqrt{2}$; $|+\rangle$ and $|-\rangle$ are orthogonal.

46. $P_0|\psi\rangle = (3/5)|0\rangle$; $|\psi\rangle - P_0|\psi\rangle = (4/5)|1\rangle$; $\|P_0|\psi\rangle\|^2 = 9/25$.

47. $P_+|0\rangle = (|0\rangle + |1\rangle)/2$; $\|P_+|0\rangle\|^2 = 1/2$.

48. $F|+\rangle = -|+\rangle$; $F|-\rangle = |-\rangle$; $F|0\rangle = -|1\rangle$; $F = -\mathrm{X}$.

49. $D|r\rangle = |11\rangle = (0,0,0,1)$; measurement gives 11 with certainty.

50. Before H: for both states $(P_0,P_1) = (1/2,1/2)$. After H: for $|\psi\rangle$ the probabilities remain (1/2,1/2); for $|+\rangle$ they are (1,0).

Chapter 3 — Grover's Algorithm

51. 50.5 checks; for $N = 10\,000$ the average is 5000.5.

52. $f(10) = 1$, $f = 0$ otherwise; $U_w = \mathrm{diag}(1,1,-1,1)$; after the oracle $(1,1,-1,1)/2$; all probabilities before and after are 1/4.

53. For $f(c) = 1$: $|c\rangle|1\rangle$, $|c\rangle|+\rangle$, $-|c\rangle|-\rangle$; for $f(c) = 0$ all three input states are unchanged.

54. $|\bar{s}\rangle = (\sum_{i\neq 101} |i\rangle)/\sqrt{7}$; $\bar{\theta} = \arcsin(1/\sqrt{8}) \approx 20.7°$; $U_w|s\rangle = (\sum_{i\neq 101} |i\rangle - |101\rangle)/\sqrt{8}$.

55. Classical checks increase approximately 100-fold; Grover steps approximately 10-fold. Actual time also depends on query cost and other operations.

56. $\|\psi_\parallel + \psi_\perp\|^2 = \|\psi_\parallel - \psi_\perp\|^2 = \|\psi_\parallel\|^2 + \|\psi_\perp\|^2$.

57. The mean remains $\bar{a}$; two applications restore each a_i.

58. Mean 1/4; after diffusion (1,0,0,0) = $|0\rangle$.

59. Mean after the oracle $3/(4\sqrt{8})$; marked amplitude $5/(2\sqrt{8})$, the others $1/(2\sqrt{8})$; probability 25/32.

60. In the stated basis order, $U_w = \mathrm{diag}(1, -1)$ and $U_s = \begin{pmatrix} \cos 2\bar{\theta} & \sin 2\bar{\theta} \\ \sin 2\bar{\theta} & -\cos 2\bar{\theta} \end{pmatrix}$. The product $U_s U_w$ is a rotation by $2\bar{\theta}$.

61. $\bar{\theta} = \arcsin(1/4) \approx 14.48°$, $k^* = 3$; probabilities 1/16, 121/256, 3721/4096, 63001/65536, 609961/1048576, respectively. The probability decreases at the fourth step.

62. Before and after one step, $P(w) = 1/2$; the formula gives $k^* = 1$, but $k = 0$ gives the same success probability.

63. Rotation by -2α.

64. $|\Delta\varphi| \leq \bar{\theta}$; $P(w) \geq \cos^2\bar{\theta} = 1 - 1/N$.

65. $k^* = 804$; $P(w) \approx 0.999999757$.

66. After two steps $P(w) = 121/128$.

67. Final state $-|11\rangle = (0,0,0,-1)$; outcome 11 has probability 1.

68. The final five columns implement $-U_s$; for input $(1,1,1,-1)/2$ the result is $(0,0,0,-1)$.

69. X gates on the first qubit before and after the Toffoli gate; the phase action on candidates is $\mathrm{diag}(1,-1,1,1)$.

70. After the oracle $(1,-1,1,1)/2$, after U_s the state $|01\rangle$; outcome 01 with probability 1.

71. The middle layers give $\mathbb{I} - 2|0\cdots 0\rangle\langle 0\cdots 0|$; surrounded by H layers they give $\mathbb{I} - 2|s\rangle\langle s| = -U_s$. The global sign does not change probabilities.

72. $\sin\bar{\theta} = 1/\sqrt{8}$; $k^* = 2$; the probability of a marked outcome is $121/128 \approx 0.9453125$.

73. $\sin\bar{\theta} = 1/4$; $k^* = 3$; $P = 63001/65536 \approx 0.9613$.

74. $100(400 + 40) = 44\,000$ gates; the query count does not determine the cost without the cost of the oracle and other operations.

75. One marked state: $P = 1$; two: $P = 1/2$. The number of marked states affects the step count; when it is unknown, the basic formula cannot be applied directly.

Chapter 4 — Two Problems, the Same Geometry

76. $m = 1$, $M = 3$; $(v,V,V,V) = v|w\rangle + \sqrt{3}V|\bar{s}\rangle$; at $v = 0$ only $\sqrt{3}V|\bar{s}\rangle$ remains.

77. $2E = 29$; normalized state $(|w\rangle + 2\sqrt{7}|\bar{s}\rangle)/\sqrt{29}$.

78. $\cos\bar{\theta} = \sqrt{N-1}/\sqrt{N}$ and $\sin\bar{\theta} = 1/\sqrt{N}$; the equal-velocity line and $|s\rangle$ have the same coordinates.

79. For $-|\bar{s}\rangle$ the small block is at rest and the first collision is between blocks; for $-|s\rangle$ both move toward the wall and the small block hits it first. Reversing the overall sign reverses both velocities.

80. $v' = \big((m-M)v + 2MV\big)/(m+M)$; $V' = \big((M-m)V + 2mv\big)/(m+M)$.

81. $v' = (3V - v)/2$; $V' = (v+V)/2$; both methods agree.

82. Wall: diag(1, − 1); collision: $\begin{pmatrix} (N-2)/N & 2\sqrt{N-1}/N \\ 2\sqrt{N-1}/N & -(N-2)/N \end{pmatrix}$; the product is a rotation by $2\bar{\theta}$.

83. Respectively, 5 collisions, 1 Grover step and 2 collisions; the ratio of the first two is 5.

84. For $M/m = 15$ with the small block initially at rest: 12 collisions; from Grover's starting point: 3 steps, or 6 collisions before the algorithm stops.

85. Grover for $N = 4$: one step, $P(w) = 1$; with equal initial velocities $v = V = -u$ and $M = 3m$, a wall collision followed by a block collision gives $V' = 0$, $v' = -2u$.

86. $v = -251/256$, $V = 13/256$; the fraction of energy in the small block is $63001/65536 \approx 0.9613$, equal to the success probability.

87. $m = r$, $M = N - r$, $\sin\bar{\theta} = \sqrt{r/N}$; for $N = 8$, $r = 2$: $\bar{\theta} = 30°$, one step and success probability 1. Here m and M are the marked and unmarked group masses; for $r > N/2$, $m > M$.

88. The mathematical operators agree on a particular two-dimensional plane; block velocities and quantum states have different physical meanings, and the blocks do not implement arbitrary quantum operations or quantum measurement.