Impossibly Fast Quantum Database Search

MATH 4310 Final Paper

Rohen Giralt (rmg296@cornell.edu)

November 21, 2025

1 Introduction

In 1997, Peter Shor developed what have come to be known as “Shor’s Algorithms”, algorithms for solving the prime factorization and discrete log problems.

Definition 1 (Discrete log problem)**.** *Given an abelian group G with a generator g, define a function $f(k) : \mathbb{Z} \to G$ given by $f(k) := g^k$, the discrete log problem asks for an efficient algorithm that, given $f(k)$, can find k.*

Definition 2 (Prime factorization problem)**.** *Given a positive integer n, the prime factorization problem asks for an efficient algorithm to find all prime numbers p such that $p|n$.*

While seemingly innocuous, a vast amount of cryptography relies on the assumption that these problems are hard to compute; i.e., that no efficient algorithm can solve them. When Shor’s paper contradicted this assumption, it set off a frenzy to repair the very foundations of the cryptography we all rely on.

Since then, most discussion of quantum computers has been mired in fear. Is any of our data safe? What if someone is recording our communications to decrypt at a later date, once quantum computers become feasible? Is it even possible to have secure cryptography in the face of quantum computers? These are important questions, and their answers are unknown (though there do exist good candidates for post-quantum cryptography). But what about their positive applications? Are quantum computers nothing more than a specter haunting cryptography? Or can they actually be used for something positive?

Grover’s algorithm provides a hint to an answer. It’s a very simple algorithm for a very simple problem: finding a single element in an unsorted set. It’s a problem that is not even interesting on classical computers, because the optimal solution is so obvious. (We will see that later when we formalize the problem.) And yet Grover’s algorithm manages to be somehow even faster, returning a result in less time than it takes to *even read the input.*

To me, that is incredibly surprising and interesting, as it flies very much in the face of our classical intuition of what a computer can do. Shor’s algorithm is a more technical result without as much intuitive might: if you told the average person that you had an efficient algorithm for factoring numbers, most would be unimpressed. Without having studied the problem, efficient integer factorization doesn’t seem like it should be impossibly hard. But an algorithm that can find an element in a set without even seeing the whole set? I think most would find that truly surprising.

2 Quantum Physics Primer

2.1 Quantum States

In classical physics, there are many quantities that together define the state of a system. For instance, a particle may have a position, a velocity, a mass, a charge, and more. It takes many of these quantities together to form a complete description of the system and predict how it will evolve over time.

In quantum physics, the picture is much simpler: there is only a single "quantum state" that describes everything knowable about a system at a given time.

Definition 3 (Quantum state)**.** *A quantum state $|\psi\rangle$ is a unit vector in some complex Hilbert space $\mathcal{H}$ [1]. It is a complete mathematical representation of the system; every predictable facet of the system can be derived from this state.*

Any given quantum system has an associated Hilbert space in which its state vectors live, but different systems may be associated with different underlying Hilbert spaces.

NB: At this point, it should be evident that linear algebra is intrinsic to the study of quantum physics and quantum computing in particular. We will continue to see this throughout. Essentially everything we care about—quantum states, measurements, quantum gates, etc.—will be phrased in the language of linear algebra.

2.2 Observables

Other quantities, like position and momentum, are no longer fundamental to the system and, in fact, no longer even have physical reality. In quantum physics, these quantities are called "observables". Before being measured, they do not exist.

Definition 4 (Observable)**.** *An observable O is a measurable quantity of a quantum system.*

For instance, the observables of a quantum particle might include its position, momentum, and charge. Observables are a physical concept, not mathematical objects. However, we will later see how they are formalized mathematically.

More unsettlingly, even when a system's quantum state is known, it is not generally possible to predict the exact result of a given measurement. For instance, consider a particle in free space; i.e., in the absence of any gravitational, electromagnetic, or other fields. It is not difficult to compute this particle's precise quantum state. Nonetheless, if one measures the particle's position, it is possible for the particle to appear anywhere in the universe at all. This is not a question of measurement error or incomplete information. There is simply a randomness intrinsic to the measurement that physically cannot be reduced. This is very surprising! Our classical intuition of the world is that objects in a definite state have definite measurable values. For instance, if one places a ball on a table, everyone can agree that the ball is, in fact, on the table. If nobody moves it and no forces act on it, then we expect that the ball will still be on the table next week. It is not the case that every time we blink, the ball magically appears in a different spot. Yet this is what happens in quantum physics!

[1] Although this is in general a Hilbert space, in this report we will generally only consider finite-dimensional Hilbert spaces, so we can just treat it as a regular inner product space.

Knowledge of the quantum state is not entirely useless, however. Although it is impossible to say exactly where a particle is before it is measured, the state allows us to at least derive a probability distribution of where we expect the particle to appear. One can imagine an experiment in which one does the following: first, they put a particle in a particular quantum state. Then, they measure its position. Although the result of each individual experiment is unpredictable, if it is repeated, the distribution of results will match the predicted distribution. We will discuss exactly how to calculate this distribution later on.

2.3 Qubits

For our purposes in quantum computing, our fundamental objects are called qubits. These qubits can be implemented in a variety of ways; for instance, they may be a photon, an electron, or even the state of an entire superconducting circuit. Regardless of their physical instantiation, however, a qubit's state always lives in a two-dimensional Hilbert space.

Definition 5 (Qubit). *A qubit is a quantum system whose state lives in a two-dimensional Hilbert space and which can be manipulated by a quantum computer.*

From the perspective of quantum computing, this abstract definition means we can ignore their physical reality and use only their mathematical description.

Typically, we operate in a standard basis containing two vectors, $\begin{bmatrix}1\\0\end{bmatrix}$ and $\begin{bmatrix}0\\1\end{bmatrix}$. In physics notation, these are $|0\rangle$ and $|1\rangle$, respectively. (To avoid confusion, note that $|0\rangle$ does *not* represent the zero-vector!) Of course, unlike regular bits, qubits are not restricted to only these two states. Instead, they can be in any state with unit norm. If we write the state as $|\psi\rangle$, a general qubit state therefore looks like:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

for some $\alpha, \beta \in \mathbb{C}$ with $|\alpha|^2 = |\beta|^2$. Any state other than $|0\rangle$ or $|1\rangle$ is called a superposition. Sometimes these qubits are described as being "in both the $|0\rangle$ and $|1\rangle$ state at the same time". Mathematically, however, these superposition states are just vectors like any other.

2.4 Measurements and Hermitian Operators

Now that we have discussed a bit of the mathematical basis for quantum states, we can return to the question of measurement. One important fact, which holds for reasons outside the scope of this report, is that every observable can be identified with a particular Hermitian operator. Given an observable O (i.e. position, momentum, energy, etc.), we use the notation $\widehat{O}$ to denote the unique Hermitian operator associated with it.

Definition 6. *A linear operator A is called Hermitian if it is self-adjoint; i.e. $A = A^*$.*

Fact 7. *For every observable quantity O, there exists a unique associated Hermitian operator $\widehat{O}$.*

As mentioned above, most states do not have a definite value of any particular observable. In general, the result of a measurement is unpredictable: multiple measurements of the same state will give different, random, results. However, there are certain special states that *do* have definite values of an observable. Specifically, for any observable O (again, think position, momentum, or energy), there exist certain states for which any measurement of O will always give the same result.

Definition 8. *A state $|\psi\rangle$ is said to have a "definite value" of an observable O if a measurement of O on $|\psi\rangle$ always gives the same value.*

For example, a single photon always has energy $\hbar\omega$, where ω is the frequency of the light and $\hbar$ is a constant. If one were to measure the energy of a single photon, they would always get the same result. We would therefore say that a photon has a definite value of energy, equal to $\hbar\omega$.

It turns out that states like this—with definite values of particular observables—are always eigenstates of the operator associated with the observable. Formally:

Fact 9. *If $|\psi\rangle \in \mathcal{H}$ is the state of some quantum system in its Hilbert space $\mathcal{H}$, O is some observable, and $\widehat{O} \in \mathcal{L}(\mathcal{H})$ is the Hermitian operator associated with O, then:*

$$\widehat{O}\,|\psi\rangle = \lambda\,|\psi\rangle \;\; \textit{for some } \lambda \in \mathbb{R} \iff |\psi\rangle \;\; \textit{has a definite value of } O$$

Furthermore, if this happens, the eigenvalue λ will always be the result of measuring O on $|\psi\rangle$.

Continuing with our photon example above, we know that a photon in state $|\psi\rangle$ has energy $\hbar\omega$. So if we let $\widehat{E}$ be the "energy operator" (the operator associated with the observable energy), we must have:

$$\widehat{E}\,|\psi\rangle = \hbar\omega\,|\psi\rangle$$

With this fact, along with the fact that all observable operators are Hermitian, we can make some observations. For one, we know that the eigenvalues of Hermitian operators are always real. This corresponds to the fact that all physical measurements that can be made are always real-valued. This is certainly what we expect. It would be a confusing world if particles could have a momentum of $2 + i$, for instance!

At this point, one may wonder: what happens if we make a measurement of O on a state $|\psi\rangle$ that is *not* an eigenvector? We know that these non-eigenvector states do not have a definite value of O. This means that the result of the measurement is unpredictable, and can take on a number of possible values. But which values, exactly?

The answer is a bit odd. Consider an arbitrary state $|\psi\rangle$. We know that if $|\psi\rangle$ is an eigenvector of $\widehat{O}$, then the result of the measurement will be the corresponding eigenvalue of $\widehat{O}$. Interestingly, something similar is true even if $|\psi\rangle$ is not an eigenvector:

Fact 10. *For any state $|\psi\rangle$ and observable O, a measurement of O on $|\psi\rangle$ will always result in some eigenvalue λ. It is not possible to measure any value that is not an eigenvalue.*

This leads to some unintuitive conclusions. For instance, in classical physics, we think of energy as a continuum. There is no "smallest amount" of energy a particle can have, nor is there a maximum. Any amount of energy in the range $[0, \inf)$ is theoretically possible. However, in many cases, the quantum energy operator $\widehat{E}$ has only countably many eigenvalues. When this happens, this means there are certain energy values that are simply impossible to achieve. It may be possible to have an energy of 0, 1, or 2 but not 1.5! This is very much not true in classical physics.

With this fact stated, a natural next question arises: when we measure a non-eigenvector state, which eigenvalue results are possible? We know there will be some randomness in the value measured. But how can we describe the distribution of possible measurements?

It turns out that the answer is very simple. Consider an arbitrary operator O, and recall that $\widehat{O}$ must be Hermitian. Since one can always find eigenvectors of a Hermitian operator that form an orthonormal basis, this implies that any arbitrary state $|\psi\rangle$ can always be written in the form:

$$|\psi\rangle = \sum_{i=1}^{n} \alpha_i |\psi_i\rangle$$

where $\{|\psi_i\rangle\}_{i=1}^{n}$ are the eigenvectors of $\widehat{O}$.

Fact 11. *Given a quantum state $|\psi\rangle$ written in the above form, let λ_i be the eigenvalue corresponding to $|\psi_i\rangle$. Then a measurement of O on $|\psi\rangle$ will give λ_i with probability $|\alpha_i|^2$, where α_i is the coefficient of $|\psi_i\rangle$ in the linear combination forming $|\psi\rangle$.*

Because we know that $\{|\psi_i\rangle\}_{i=1}^{n}$ form an orthonormal set, we can conclude the following:

Corollary 12. *Suppose $|\psi\rangle$, $|\psi_i\rangle$, and λ_i are defined as above. Then a measurement of O on $|\psi\rangle$ will give λ_i with probability $|\langle\psi_i|\psi\rangle|^2$, where $\langle\psi_i|\psi\rangle$ is physics notation for the inner product $\langle|\psi\rangle, |\psi_i\rangle\rangle$*

There's one more fact we'll need before returning to quantum computing, essentially the converse of 7:

Fact 13. *For any Hermitian operator $\widehat{O}$, there exists an observable quantity whose possible values are exactly the eigenvalues of $\widehat{O}$.*

This is important to ensure that qubit states are measurable. Consider the operator defined by the matrix

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

in the $\{|0\rangle, |1\rangle\}$ basis. Because this an operator diagonal with respect to an orthonormal basis and with real eigenvalues, it is Hermitian. This implies we can always physically measure the state of a qubit by carrying out the measurement associated with this operator. Our measurement will give 1 or -1, allowing us to "read the value" of the qubit.

2.5 Multi-Qubit Systems

In any useful quantum algorithm, we will want to have more than one qubit. Conveniently, a collection of qubits can be thought of as a new composite quantum system with its own quantum state space. In particular, given a set $\{\mathcal{H}_1, \mathcal{H}_2, \ldots, \mathcal{H}_n\}$ of Hilbert spaces each corresponding to a qubit's state, the whole system of all n qubits can be described by a state vector in $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n$ (here $\otimes$ is the tensor product).

We will typically denote the state of a system with n qubits in one of two ways. The eigenstates will be denoted as $|x_1 x_2 \ldots x_n\rangle$, where each of $x_i \in \{0, 1\}$. So for instance, the state with four qubits, each in the $|0\rangle$ state is denoted as $|0000\rangle$. The non-eigenstates will typically be denoted as a 2^n-dimensional vector, where the first entry is the coefficient of the $|0 \ldots 0\rangle$ state, the second entry is the coefficient of the $|0 \ldots 1\rangle$ state, etc. So for instance, the following state of two qubits:

$$\begin{aligned} |\psi\rangle &= \frac{1}{2}(|0\rangle \otimes |0\rangle) + \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle) + \frac{1}{2}(|1\rangle \otimes |1\rangle) \\ &= \frac{1}{2}|00\rangle + \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{2}|11\rangle \end{aligned}$$

would be denoted as:

$$|\psi\rangle = \left\langle \frac{1}{2}, 0, \frac{1}{\sqrt{2}}, \frac{1}{2} \right\rangle$$

Sometimes we may also use a variation of the first notation, $|x\rangle$. Here, x is a binary string or an integer (represented in binary). This can be interpreted just like the first notation, where each integer represents a particular basis state. For instance, if $x = 3$, we would have $|x\rangle = |101\rangle = \frac{1}{\sqrt{2}}\langle 1, 0, 1\rangle$

2.6 Quantum Gates

Finally, before we can see the algorithm, we must define quantum gates.

Classical computers are built from different gates—AND, OR, NOT, etc.—which each operate on the 0s and 1s stored in the CPU's registers. Quantum computers are conceptually no different.

Definition 14 (Quantum gate)**.** *A quantum gate is a unitary operator $U \in \mathcal{L}(\mathcal{H})$ (not necessarily Hermitian nor related to a measurement!), where $\mathcal{H}$ is the Hilbert space of a system of several qubits.*

A quantum gate simply gets applied to the state of a system of qubits to transform it into a new state. The requirement that it be unitary comes from the fact that quantum states always have unit norm. It must be unitary so that all output states remain properly normalized.

3 Grover's Algorithm

Before we can tackle the algorithm given in the paper—now called Grover's algorithm, after the author—we must define formally the problem it sets out to solve. That problem is called Database Search.

3.1 Database Search

Definition 15 (Database Search)**.** *Suppose there exist a set S, an element $s \in S$, and an efficiently computable function $f : S \to \{0, 1\}$ for which*

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

Then the database search problem asks for an efficient algorithm for finding s given only S and f.

For instance, one could imagine S to be an unsorted database of some records of interest. If s is a particular record in the database, we could use a database search algorithm to find the record.

Alternatively, the setting could be more abstract. Suppose we have any injective function $g : X \to Y$ with finite codomain, as well as some element $y \in Y$ for which we are trying to find the preimage. This is essentially an instance of database search for which $S = Y$ and $f(x) = \begin{cases} 1 \text{ if } g(x) = y \\ 0 \text{ otherwise} \end{cases}$.

Many hard problems in computer science (for instance, the discrete log problem 1) can be reduced to finding the inverses of functions. A very fast algorithm for database search could therefore be applied to solve a very large number of problems.

This problem is thus very general and, without additional information, seemingly very difficult. Notice that we aren't given any information about the set S nor the element s. There is essentially no structure provided by the problem, so we don't have much to go off of in designing an algorithm. Because of this, it should be relatively clear that there is no faster classical algorithm for solving this problem than a simple brute force search:

```
Input: A set $S$, a function $f : S \to \{0, 1\}$
Result: $s \in S$ such that $f(s) = 1$
foreach $s \in S$ do
    if $f(s) = 1$ then
        return $s$
    else
end
```

Algorithm 1: Brute Force Database Search

This algorithm in the worst case takes up to n iterations before finding s. If s happens to be the last element, it will have to iterate through the entire set before finding it. Without any additional information, this is the best we can do on a classical computer.

Intuitively, this should make sense. Because we know nothing about S or f or s, we have no way of determining where s is in the set, so we have to check every element. Yet shockingly, this is not true for quantum computers.

3.2 The Algorithm

With the background out of the way, the algorithm itself is actually fairly simple. It's only six lines and operates on $\lceil \log(n) \rceil$ qubits, where $n = |S|$ is the length of the input:

```
Input: A set $S$, a function $f : S \to \{0, 1\}$
Result: $s \in S$ such that $f(s) = 1$ with constant probability
Initialize the system state $|\psi\rangle$ to $|\psi\rangle = \frac{1}{\sqrt{n}} \underbrace{\langle 1, 1, \ldots, 1 \rangle}_{n \text{ times}}$;
repeat $\lceil \sqrt{2n} \rceil$ times
    $|\psi\rangle \leftarrow U_f \, |\psi\rangle$;
    $|\psi\rangle \leftarrow (-I + 2P) \, |\psi\rangle$;
end
measure each qubit in $|\psi\rangle$ to get a binary string $s$;
return $s$;
```

Algorithm 2: Grover's Algorithm

Of course, to understand it, we will need to understand the U_f and P operators.

Definition 16 (U_f operator)**.** *Given a function f, the operator $U_f \in \mathcal{H}$ is the unitary operator that maps the basis vectors $|x\rangle$ to $(-1)^{f(x)} |x\rangle$. Its action on all other vectors is uniquely determined by linearity.*

Essentially, if $|x\rangle$ is a basis state—i.e., in a non-superposition state—storing the string x, then x is an eigenvector of U_f. If $f(x) = 1$, then it has eigenvalue -1 (i.e. U_f "flips" it), and if $f(x) = 0$, then it has eigenvalue 1 (U_f "leaves it alone").

Given the function f, we can construct the U_f gate. One can think of it as the encoding of f that is usable by a quantum computer.

Definition 17 (P operator)**.** *The unitary operator $P \in \mathcal{L}(\mathcal{H})$ is the operator associated with the following matrix in the standard basis:*

$$\mathcal{M}(P) = \frac{1}{n}\begin{bmatrix} 1 & \dots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \dots & 1 \end{bmatrix}$$

The matrix is called P in the article because $P^2 = P$, so it is a projection matrix. While this is true, it can more intuitively thought of in a different way. Consider the effect of applying P to some state $|\psi\rangle = \langle x_1, x_2, \dots, x_n\rangle$. We have:

$$\begin{aligned} & P\left(\begin{bmatrix} x_1 \\ x_2 \\ \dots \\ x_n \end{bmatrix}\right) \\ =& \frac{1}{n}\begin{bmatrix} 1 & \dots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \dots & 1 \end{bmatrix}\begin{bmatrix} x_1 \\ x_2 \\ \dots \\ x_n \end{bmatrix} \\ =& \frac{1}{n}(x_1 + x_2 + \dots + x_n) \end{aligned}$$

which is just the mean of the components of $|\psi\rangle$! So in some sense, P can be thought of as the "average value" operator.

But what is $-I + 2P$? The article describes it as "inversion about the mean". This is more clear when written differently:

$$-I + 2P = P - (I - P)$$

If we consider any particular component x_i of $|x\rangle$, this operator maps x_i to $\bar{x} - (x_i - \bar{x})$, where $\bar{x}$ is the mean of all the components. $x_i - \bar{x}$ can be thought of as the (signed) distance of x_i from the mean. Thus, $x_i - (x_i - \bar{x})$ "flips" x_i to the value the same distance from the mean but on the other side.

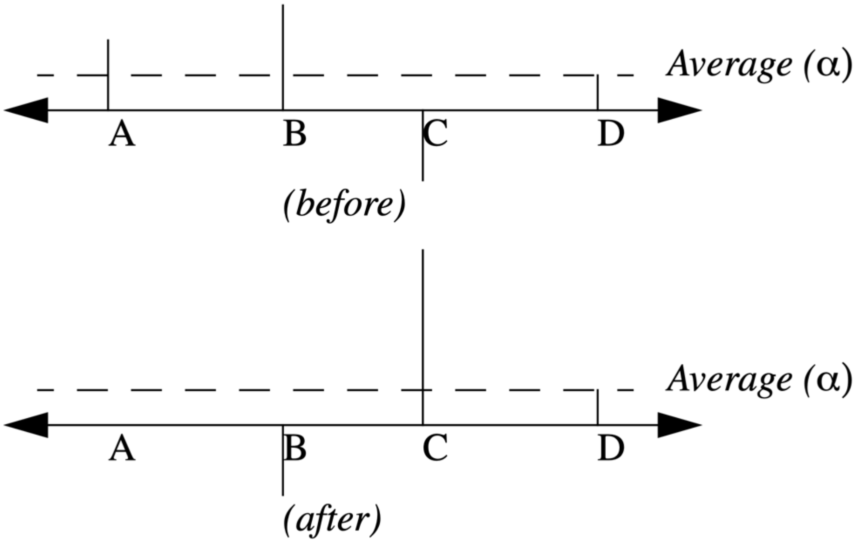

Figure 1: A visualization of the inversion about the mean operation, from the original paper.

3.3 Analysis of the Algorithm

Although the paper provides a formal proof of both the algorithm's correctness as well as its time complexity, I will only give intuition here.

3.4 Time Complexity Analysis

The easiest part of the analysis is the time complexity, a measure of how long an algorithm will run for in the worst case. The algorithm has a fixed loop of $\lceil \sqrt{2n} \rceil$ iterations, so clearly its runtime scales like $O(\sqrt{n})$ (where n is again the size of the search space S).

3.5 Correctness

Understanding the algorithm's behavior and correctness is a bit more difficult. It's useful to consider the steps of the algorithm one by one.

At the start of the algorithm, the state is initialized to be uniform:

$$|\psi\rangle = \frac{1}{\sqrt{n}}\langle 1, 1, \dots, 1\rangle$$

After applying U_f, every component has been flipped to $\frac{-1}{\sqrt{n}}$ except for the single state (call it $|s\rangle$) for which $f(s) = 1$:

$$|\psi\rangle = \frac{1}{\sqrt{n}}\langle -1, -1 \dots, 1, \dots, -1, -1\rangle$$

At this point, especially if n is fairly large, the mean of these components is roughly $\frac{-1}{\sqrt{n}}$. So applying $-I + 2P$ has no effect on any component but $|s\rangle$. Meanwhile, $|s\rangle$ has amplitude $\frac{1}{\sqrt{n}}$. Since the mean is $\frac{1}{\sqrt{n}}$, $|s\rangle$'s amplitude is therefore distance $\frac{2}{\sqrt{n}}$ from the mean. So when it gets inverted, it gets a new amplitude $\frac{-1}{\sqrt{n}} - \frac{2}{\sqrt{n}} = \frac{-3}{\sqrt{n}}$, making the new state approximately following:

$$|\psi\rangle = \frac{1}{\sqrt{n}}\langle -1, -1 \ldots, -3, \ldots, -1, -1\rangle$$

(Note that this state is no longer normalized! This is just a product of our approximation, though. If we were to compute the new state exactly, the non-$|s\rangle$ states would also change slightly to repair the normalization.)

Repeating the loop again, we see a similar phenomenon. After applying U_f, every non-$|s\rangle$ component gets flipped yet again:

$$|\psi\rangle = \frac{1}{\sqrt{n}}\langle 1, 1 \ldots, -3, \ldots, 1, 1\rangle$$

Then, similarly to before, the mean is still roughly $\frac{1}{\sqrt{n}}$. So applying $-I + 2P$ flips the $|s\rangle$ state across the mean. Because the mean is $\frac{1}{\sqrt{n}}$ and $|s\rangle$ has amplitude $\frac{-3}{\sqrt{n}}$, it gets mapped to $\frac{3}{\sqrt{n}} + \frac{2}{\sqrt{n}} = \frac{5}{\sqrt{n}}$:

$$|\psi\rangle = \frac{1}{\sqrt{n}}\langle 1, 1 \ldots, 5, \ldots, 1, 1\rangle$$

It's clear that, as we continue this process, the amplitude of the basis vector $|s\rangle$ will grow by about $\frac{2}{\sqrt{n}}$ each time. After repeating this a few times, we can expect its amplitude to tend towards 1. Based on the growth rate, we would furthermore expect only on the order of $\sqrt{n}$ iterations to be necessary.

Of course, this isn't exactly true due to the approximation we made. In reality, the growth rate is always somewhat less than $\frac{2}{\sqrt{n}}$, and decreases with each iteration. Nonetheless, the paper shows that it still takes only at most $\sqrt{2n}$ iterations to reach an amplitude of $\frac{1}{2}$.

Now recall that the probability of measuring a given eigenvalue is related to its corresponding eigenvector's coefficient in a linear combination. In our case, the measurable eigenvalues are different binary strings, and the coefficient of a state is just its amplitude in the state vector. Thus, because the amplitude of the $|s\rangle$ vector grows in each iteration, so too does the probability of measuring s (the string we want) in the end.

Once the probability reaches $\frac{1}{2}$, we have a $\left|\frac{1}{2}\right|^2 = \frac{1}{4}$ chance of measuring the correct string. While this probability may seem low, it's actually not a problem. Since it's easy to check if the s we got is correct (just plug it into f!) we can easily run the experiment a few times until we get the desired result. With a measurement probability of $\frac{1}{4}$, we only need to run the algorithm four times in expectation before getting the result we're looking for!

References

[1] Tomas A. Arias. Hermitianness, 1995.

[2] Lov K. Grover. A fast quantum mechanical algorithm for database search, 1996.

[3] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, October 1997.