

Optimizing Quantum Search Using a Generalized Version of Grover's Algorithm

Austin Gilliam, Marco Pistoia, and Constantin Gonciulea

JPMorgan Chase

(Dated: May 27, 2020)

Grover's Search algorithm was a breakthrough at the time it was introduced, and its underlying procedure of amplitude amplification has been a building block of many other algorithms and patterns for extracting information encoded in quantum states. In this paper, we introduce an optimization of the inversion-by-the-mean step of the algorithm. This optimization serves two purposes: from a practical perspective, it can lead to a performance improvement; from a theoretical one, it leads to a novel interpretation of the actual nature of this step. This step is a reflection, which is realized by (a) cancelling the superposition of a general state to revert to the original all-zeros state, (b) flipping the sign of the amplitude of the all-zeros state, and finally (c) reverting back to the superposition state. Rather than canceling the superposition, our approach allows for going forward to another state that makes the reflection easier. We validate our approach on set and array search, and confirm our results experimentally on real quantum hardware.

I. INTRODUCTION

The capabilities of quantum computers are evolving at a very fast pace. With half a century of research efforts on theoretical quantum computing, increasingly more researchers are now working on designing and implementing new quantum algorithms that can take advantage of the fast-evolving underlying quantum hardware. While some of such algorithms are meant to address a particular problem in a specific domain, a large body of research has been devoted to the creation of algorithms of general applicability, such as Shor's algorithm [1], Grover's Search [2], and Variational Quantum Eigensolver [3].

Grover's Search algorithm is of particular interest to researchers due to its vast area of applicability, which spans across multiple domains. With high probability, Grover's Search finds an output of interest in an unstructured search space with quadratic speedup compared to classical solutions. The algorithm, introduced by Lov Grover in 1996, has been expanded on several times since its first formulation [4–6].

In this paper, we propose further optimizations of Grover's Search algorithm, as follows:

1. A generalization of the inversion-by-the-mean step,
2. A modified version of the original algorithm formulation, which we describe as *set search*, and
3. A modification of *array search*, which we had introduced in previous work [7].

To the best of our knowledge, these contributions are novel. Additionally, we demonstrate experimentally, on real quantum hardware, that these contributions can lead to more optimal realizations of quantum search.

The modified Grover iterate presented in this paper applies to the search, counting and optimization features of the quantum-dictionary structure [7], as well as to other algorithms that use amplitude amplification.

The remainder of this paper is organized as follows: Section II offers an overview of the standard formulation of Grover's Search algorithm. Section III shows how

our generalization and modification of Grover's Search algorithm can be applied to set search and array search. Section IV demonstrates an experimental validation of our approach on real quantum hardware. Related work around modifications and extensions of Grover's Search algorithm is covered in Section V. Finally, Section VI concludes the paper and discusses potential future directions for this work.

II. STANDARD GROVER'S SEARCH

Grover's Search algorithm [2] was created in the context of unstructured search, where we assume a single state of interest. The algorithm is summarized below:

1. Initialize a quantum system of n qubits to a state of equal superposition.
2. Repeat the following steps $O(\sqrt{2^n})$ times:
 - (a) Apply an oracle O , which recognizes the state of interest and multiplies its amplitude by -1 .
 - (b) Apply an operator that performs an inversion by the mean on all amplitudes. This is typically done by removing the superposition, multiplying the amplitude of the $|0\rangle_n$ state by -1 , and then restoring the superposition.

Step 2 describes the central concept of quantum search. When applied a precise number of times, it incrementally amplifies the magnitude of the amplitudes of the states of interest, thus increasing their probabilities of being measured.

Geometrically, the multiplication of the amplitude of the $|0\rangle_n$ state by -1 is a reflection, which we will denote by M_0 for *mirror*—a convention used in Geometric Algebra and other literature as well [8]. For a given state vector $s = \sum_{j=0}^{2^n-1} \alpha_j |j\rangle$, we define:

$$M_0(s) := \sum_{j \neq 0} \alpha_j |j\rangle_n - \alpha_0 |0\rangle_n \quad (1)$$

In his original paper [2], Grover referred to Step 2b as *diffusion* and the mirror operation as a *rotation*. Note that some authors indicate by *diffusion* only the reflection in $|0\rangle_n$, which is why we choose to use the term *mirror*.

The Hadamard operation is used to create and revert from superposition.

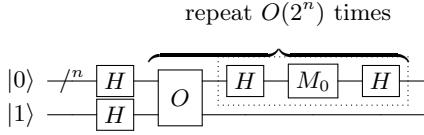


FIG. 1. A circuit representing the simplest case of Grover’s Search algorithm.

The algorithm was later generalized, allowing for any unitary state-preparation operator A (i.e., not necessarily an equal superposition created with the Hadamard operator H) and multiple marked states (sometimes called the *good states*), and is now commonly referred to as *amplitude amplification* [6]. Step 2, known as the *Grover iterate*, takes the form $G = -AS_0A^\dagger O$, where S_0 is the same operator we denote by M_0 . Note that the negative sign can be ignored in the implementation, leading to a small adjustment in the interpretation of measurements. Note also that in some literature, the combination $A^\dagger OA$ is referred to as the *oracle*, but we prefer to keep the definitions of A and O separate.

III. VARIATION OF GROVER’S SEARCH

In this paper, we present a more general form the Grover iterate $G = B^\dagger M_B BO$, where we use operator B and mirroring operator M_B , which depends on B . As we will show, if the implementations of B and M_B are efficient, this generalization can lead to more optimal realizations of quantum search. We retrieve the known form of the Grover iterate by taking $B = A^\dagger$ and $M_B = M_0$.

We will explore a particular case of this generalization, as an optimized alternative to the standard implementation of Grover’s Search, which assumes that before applying the mirror operator we must be in the state $|0\rangle_n$. The mirror operation is implemented as $M_0 = X^{\otimes n} M_1 X^{\otimes n}$, where M_1 is the operator that flips the sign of the all-ones state $|2^n - 1\rangle_n$ i.e., for a given state vector $s = \sum_{j=0}^{2^n-1} \alpha_j |j\rangle$, we have:

$$M_1(s) = \sum_{j \neq 2^n-1} \alpha_j |j\rangle_n - \alpha_{2^n-1} |2^n - 1\rangle_n \quad (2)$$

It is easy to verify that the circuit in Figure 2 is an implementation of M_0 .

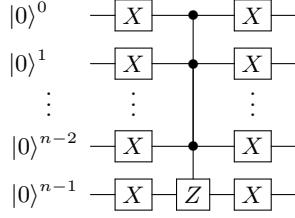


FIG. 2. A circuit implementation of the mirror operator M_0 .

As an algebraic intuition, if we can combine the action of the X gates with the previous operator into a more efficient operator, the result can be more efficient overall.

More formally, if we have an operator B such that $BA = X^{\otimes n}$, then $A^\dagger = X^{\otimes n}B$ and $A = B^\dagger X^{\otimes n}$, and the Grover iterate becomes:

$$\begin{aligned} G &= AM_0A^\dagger O \\ &= B^\dagger X^{\otimes n} M_1 X^{\otimes n} BO \\ &= B^\dagger X^{\otimes n} X^{\otimes n} M_1 X^{\otimes n} X^{\otimes n} BO \\ &= B^\dagger M_1 BO \end{aligned} \quad (3)$$

In this case, $M_B = M_1$, which uses fewer gates than M_0 , as we avoid the X gates on either side of the controls.

A. Set Search

The context in which Grover’s Search algorithm was originally introduced can be described as a *set search*, where we are looking for states of interest in an unstructured collection of data. In this context, the modified version of the algorithm uses $A = R_X(\frac{\pi}{2})$, $B = -iR_X(\frac{\pi}{2})$, and $M_B = M_1$. In many cases, we can ignore the additional rotation added by the $-i$ factor, and use $B = R_X(\frac{\pi}{2})$.

The modification results in a reduction in the total number of gates used in quantum computations that utilize a Grover iterate—which can potentially lead to better overall performance, as confirmed experimentally in Section IV A.

B. Array Search

Many presentations of Grover’s Search algorithm focus on the set search version, where values are put in superposition in a single register before the amplitudes of the desired outcomes are amplified. However, the real power of quantum search is revealed when multiple entangled registers are used.

To show that, we will consider the case of an array search, where values are indexed by a separate register. In general, we do not know how many values are present, or how many times a single value is repeated. In such

situations, one can use *quantum counting* first, revealing the number of times one needs to apply the Grover iterate to find one of the desired values and its index. In [7], we show how to implement quantum search and counting on a quantum dictionary, a pattern for representing key/value pairs as entangled quantum registers. Alternatively, we can use adaptive versions of Grover's algorithm that randomize the number of times the Grover iterate is applied.

In the method described in [7, 9], the values in the array are encoded using an operator of the form $A = PH$, which first puts all indices and possible values in superposition, and then entangles each array index with a corresponding value.

For a given value of interest (in the context of counting or searching), we build a Grover iterate of the form $G = PHM_0HP^\dagger O$.

The modified version uses operators $A = PR_X(\frac{\pi}{2})$ and $B = RX(\frac{\pi}{2})P^\dagger$ (ignoring the $-i$ factor in the cases it can be done), and mirror operator $M_B = M_1$, such that the Grover iterate becomes $G = PR_X(-\frac{\pi}{2})M_1RX(\frac{\pi}{2})P^\dagger O$.

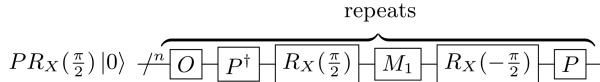


FIG. 3. A circuit implementation of the Grover iterate G used in array search.

A description of P is included in Appendix A, and an example circuit for A is shown in Section IV B.

C. Other Applications

The ideas presented in Section III B are equally applicable to the adaptive versions of Grover's Search algorithm and Amplitude Estimation.

As a general rule, the usages of $R_X(\pi/2)$ within this paper can be replaced by $R_Y(\pi/2)$ —which has a counterpart in the world of probabilistic bits. Thus, the method can also be applied to a probabilistic version of Grover's Search algorithm.

IV. IMPACT OF GATE-COUNT REDUCTION: EXPERIMENTAL RESULTS

In this section, we take a closer look at concrete applications of this generalization, including analyses of performance on real quantum computers.

A. Set Search

Let us compare the standard version of Grover's Search ($A = H$) with the modified version for $n = 2$ qubits, us-

ing 2 (10 in binary representation) as our state of interest (Figure 4).

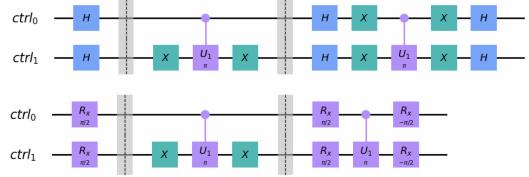


FIG. 4. Circuits for the *standard* (top) and *modified* (bottom) version of Grover's Search, searching for 2 with $n = 2$ qubits. Circuits are generated using Qiskit [10].

The result is a reduction in the number of X gates, as seen in the table below:

Implementation	H	R_X	X	CU_1
Standard	6	0	6	2
Modified	0	6	2	2

The reduction in the gate count continues for $n = 3$ qubits, as shown below. In general, we save $2n$ X gates per mirror operator, and we apply the mirror operator $\lfloor \pi \frac{\sqrt{2^n}}{4} \rfloor$ times [4].

Implementation	H	R_X	X	CCU_1
Standard	15	0	16	4
Modified	0	15	4	4

B. Array Search

Consider the array $[-4, -3, -2, -1, 0, 1, 2, 3]$, whose values are chosen to match the polynomial formula $f(j) = j - 4$ for integer indices $0 \leq j \leq 7$. An efficient way to encode polynomial values in a quantum register is described in [7, 9]. A visual representation of the array is given in Figure 5, where the index register is shown on the horizontal, and the value register on the vertical. Each pixel represents the amplitude of the index/value pair, where the intensity represents the magnitude of the amplitude, and the color is determined by its phase. A more detailed description can be found in Appendix C.

The circuits for encoding such a state with the standard and modified versions are shown in Figure 6.

The modified version reduces the number of X gates, as seen in the table below. Note that nCU_1 denotes an n -controlled U_1 gate, where $n + 1$ is the number of index and value qubits.

Implementation	H	R_X	X	U_1	CU_1	nCU_1
Standard	45	0	36	15	60	4
Modified	0	45	12	15	60	4

The results for both the standard and modified versions are shown in Figure 7, which visualizes each iteration of the search. Note that using $R_X(\frac{\pi}{2})$ leads to different amplitude phases, represented in the color of each pixel.

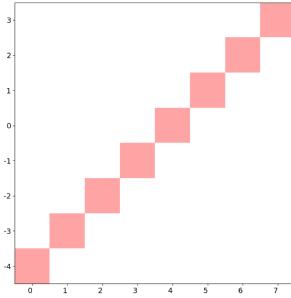


FIG. 5. A visual representation of the quantum state encoding the array described in Section III B. The indices are represented on the horizontal axis, and the values on the vertical.

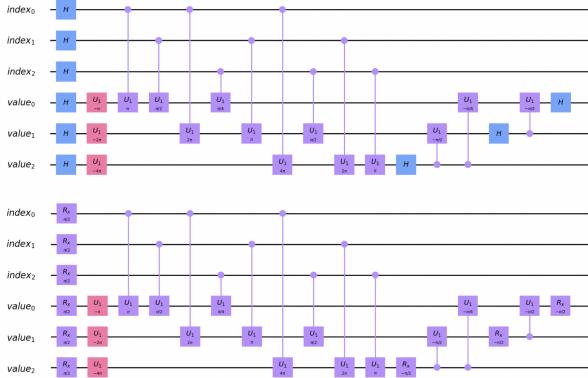


FIG. 6. The circuits representing the operator P for the *standard* (top) and *modified* (bottom) versions of array search. Circuits are generated using Qiskit [10].

C. Real Hardware

As seen in Sections IV A and IV B, the modified version of Grover’s Search decreases the gate count of the circuit. In this section, we present how this affects results on current quantum hardware. Note that the results of any compiled circuit is dependent on the performance of circuit transpilers, which may theoretically make the proposed optimization already. However, it is beneficial to make these optimizations by design, as we show here. Note also that results may differ day by day (due to hardware tuning) and by device, so while we will not always see the same results, a lower gate count offers the potential for improvement. For details on the quantum hardware used in the following examples, see Appendix B.

Returning to the two-qubit examples given in Section IV A, the two versions perform similarly on a high-fidelity quantum computer. However, as the coherence times decrease, the modified version has a notable advantage, as seen in Figures 8 and 9.

We expect the desired value (in this case, 2) to have the highest probability, and stand out among the other outcomes. This is clearly more pronounced with the mod-

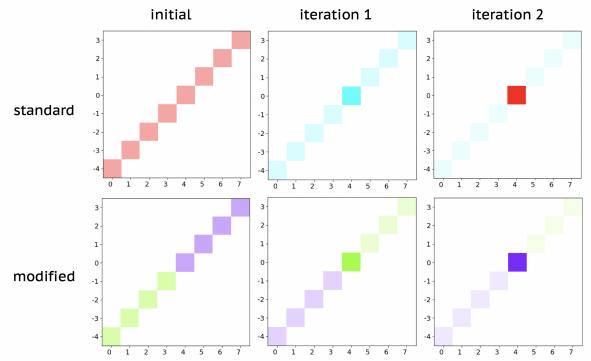


FIG. 7. A visual representation of each iteration of array search, using both the standard and modified versions.

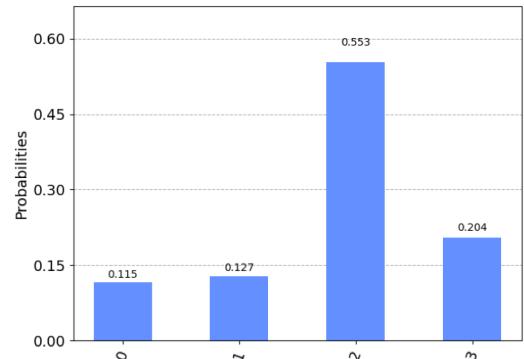


FIG. 8. The aggregated result of running the same circuit three times on IBM’s `ibmq_burlington` backend with 8192 shots, using the *standard* version with $n = 2$ qubits, searching for the value 2.

ified version (see Figure 9), compared to the standard (see Figure 8). Running the experiment multiple times, the modified version resulted in the desired value having a probability that was 15% higher than the one in the standard version.

When using $n = 3$ qubits with a marked value of 5 (shown in Figure 10 and 11), even for a high fidelity computer, we see a difference in the measured results. For $n > 3$ qubits, the circuit depth exceeds the limits regarding the coherence time of the quantum hardware currently used. For example, the results for $n = 4$ qubits are shown in Figures 12 and 13. We receive similar results for the array search example discussed in Section IV B.

V. RELATED WORK

In this section, we cover related work in the area of Grover’s Search algorithm modifications, particularly those that constitute extensions of the general algorithm with the purpose of optimizing it.

Boyer, *et al.* [4] provide a tight analysis of Grover’s Search algorithm and propose a formula for computing

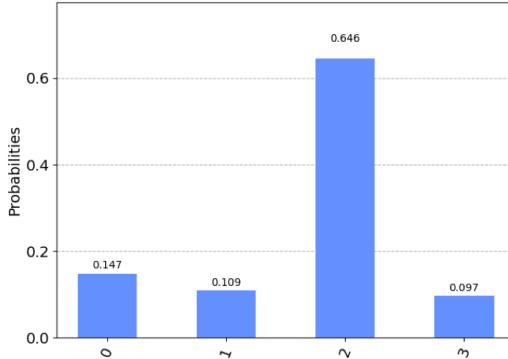


FIG. 9. The aggregated result of running the same circuit three times on IBM’s `ibmq_burlington` backend with 8192 shots, using the *modified* version with $n = 2$ qubits, searching for the value 2.

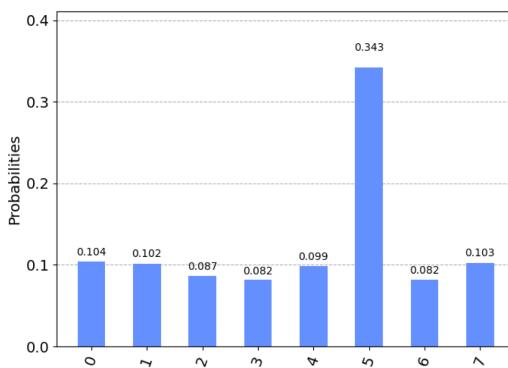


FIG. 10. The result of running a Grover circuit on IBM’s `ibmq_ourense` backend with 8192 shots, using the *standard* version with $n = 3$ qubits, searching for 5.

the probability of finding an element of interest after any given number of iterations of the algorithm. This can in turn lead to predicting the number of iterations needed to find the given element with high probability. Their analysis also include a model of the algorithm in situations in which the element to be found appears more than once. For such situations, they provided a new algorithm that works also when the number of solutions is not known in advance. Furthermore, they introduced a new technique for approximate quantum counting and for estimating the number of solutions. Unlike the solution we present in this paper, their work does not provide an optimization of the inversion-by-the-mean step of Grover’s Search.

Mosca [5] introduces a novel interpretation of the eigenvectors and eigenvalues of the iterate operator of Grover’s Search. Their new interpretation leads to novel, optimised algorithm formulations for searching, approximate counting, and amplitude amplification.

Brassard, *et al.* [6] are also interested in extending Grover’s Search to perform Amplitude Estimation and apply it to approximate counting. Unlike our approach, which is based on optimizing the inversion-by-the-mean

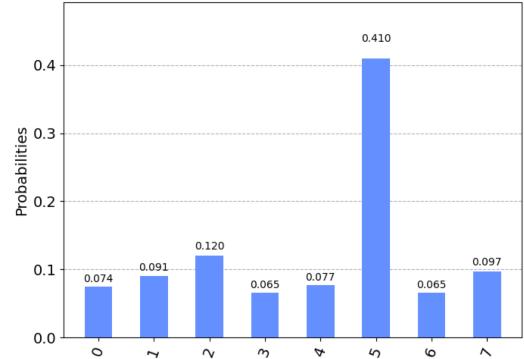


FIG. 11. The result of running a Grover circuit on IBM’s `ibmq_ourense` backend with 8192 shots, using the *modified* version with $n = 3$ qubits, searching for 5.

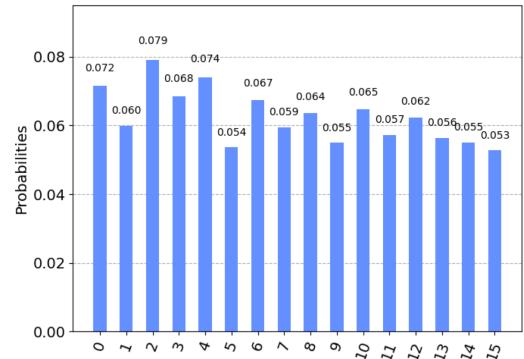


FIG. 12. The result of running a Grover circuit on IBM’s `ibmq_ourense` backend with 8192 shots, using the *standard* version with $n = 4$ qubits, searching for 5.

step, their solution is based on combining ideas from Grover’s and Shor’s quantum algorithms.

VI. CONCLUSION

We have shown variations in the implementation of the building blocks of the Grover’s Search algorithm that use fewer gates, may reduce the number of required iterations, and can lead to overall performance improvements.

For the common case when a circuit prepares a state by starting with an equal superposition, we have shown a general pattern that replaces Hadamard gates with the simpler $R_X(\frac{\pi}{2})$ gate, allowing for the elimination of a number of X gates. We have used set and array search as examples that fall into this category.

In geometric terms, one of the takeaways of this paper should be that the state prepared before applying the Amplitude Amplification procedure does not need to be reverted, but instead can be evolved into another state that makes the reflection easier.

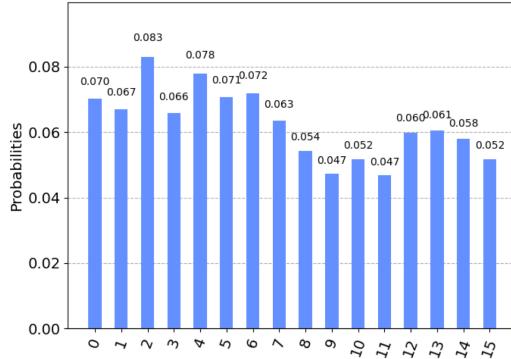


FIG. 13. The result of running a Grover circuit on IBM’s `ibmq_ourense` backend with 8192 shots, using the *modified* version with $n = 4$ qubits, searching for 5.

DISCLAIMER

This paper was prepared for information purposes by the Future Lab for Applied Research and Engineering (FLARE) Group of JPMorgan Chase & Co. and its affiliates, and is not a product of the Research Department of JPMorgan Chase & Co. JPMorgan Chase & Co. makes no explicit or implied representation and warranty, and accepts no liability, for the completeness, accuracy or reliability of information, or the legal, compliance, tax or accounting effects of matters contained herein. This document is not intended as investment research or investment advice, or a recommendation, offer or solicitation for the purchase or sale of any security, financial instrument, financial product or service, or to be used in any way for evaluating the merits of participating in any transaction.

IBM, IBM Q, Qiskit are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product or service names may be trademarks or service marks of IBM or other companies.

APPENDIX

Appendix A: The Encoding Operator for Array Values

The encoding operator for array values is in essence the operator described in the quantum-dictionary pattern. An array is a particular case of a dictionary where the keys are used as array indices.

Without including a full description that can be found in our previous work [7, 9], if the operator U_G is defined by:

$$U_G(\theta)H^{\otimes m}|0\rangle_m = \frac{1}{\sqrt{2^m}} \sum_{k=0}^{2^m-1} e^{ik\theta}|k\rangle_m \quad (\text{A1})$$

then the value encoding operator is of the form PH , where H is the Hadamard operator and P is the composition of the sequence of U_G applications followed by QFT^\dagger , as shown in Figure 14.

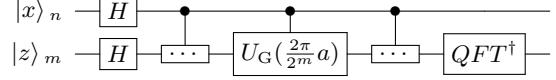


FIG. 14. Circuit for operator A .

Appendix B: Hardware Configuration

In Section IV, we use two quantum devices to run the standard and modified versions of Grover’s Search (introduced in Section III). The configuration and error rates for the devices are listed in Figure 15.

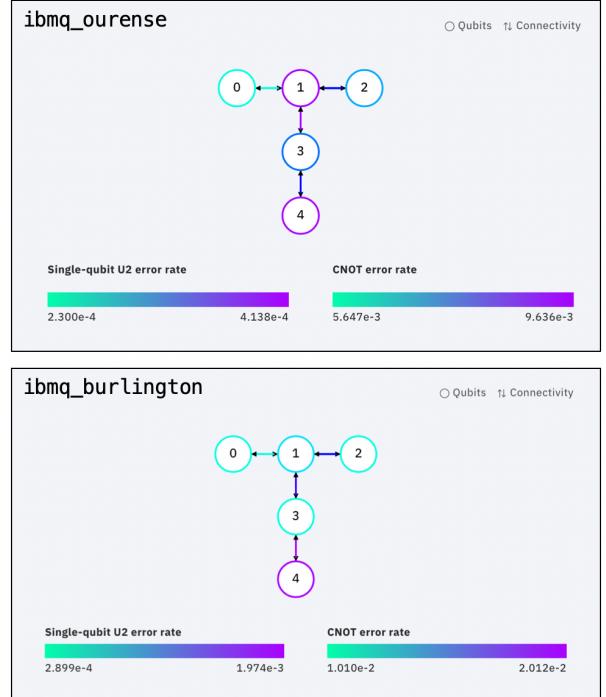


FIG. 15. The configuration and error rates for IBM’s `ibmq_ourense` (top) and `ibmq_burlington` (bottom) backend, taken from the IBM Quantum Experience interface at the time of the experiments.

Appendix C: Pixel-Based Quantum State Visualization

Amplitudes are complex numbers that have a direct correspondence to colors - mapping angles to hues and magnitudes to intensity - as seen in Figure 16.

Using this technique, we can represent the quantum state as a column of pixels, where each pixel corresponds

to its respective amplitude. If the computation contains two entangled registers, such as with a quantum dictionary, the visualization is also useful in a tabular form.

While the mapping of complex numbers to colors is not a new idea (it is commonly used in complex analysis) we find it useful in visualizing quantum state.

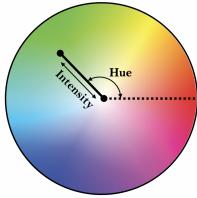


FIG. 16. A complex number represented in polar form, overlaid onto a color wheel. The phase of the amplitude determines the hue, and the magnitude determines the intensity.

REFERENCES

- [1] Peter W Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” *SIAM review* **41**, 303–332 (1999).
- [2] Lov K. Grover, “A fast quantum mechanical algorithm for database search,” in *Proceedings of the Twenty-*

eighth Annual ACM Symposium on Theory of Computing, STOC ’96 (ACM, New York, NY, USA, 1996) pp. 212–219.

- [3] Alberto Peruzzo, Jarrod McClean, Peter Shadbolt, Man-Hong Yung, Xiao-Qi Zhou, Peter J. Love, Alan Aspuru-Guzik, and Jeremy L. O’Brien, “A Variational Eigenvalue Solver on a Photonic Quantum Processor,” *Nature Communications* **5** (2014).
- [4] Michel Boyer, Gilles Brassard, Peter Hoyer, and Alain Tapp, “Tight bounds on quantum searching,” *Fortschritte der Physik* **46**, 493–505 (1998).
- [5] Michele Mosca, “Quantum searching, counting, and amplitude amplification by eigenvector analysis,” (1998).
- [6] Gilles Brassard, Peter Hoyer, Michele Mosca, and Alain Tapp, “Quantum Amplitude Amplification and Estimation,” *Contemporary Mathematics* **305** (2002).
- [7] Austin Gilliam, Charlene Venci, Sreraman Muralidharan, Vitaliy Dorum, Eric May, Rajesh Narasimhan, and Constantin Gonciulea, “Foundational patterns for efficient quantum computing,” (2019), [arXiv:1907.11513 \[quant-ph\]](https://arxiv.org/abs/1907.11513).
- [8] M. Gimeno-Segovia, N. Harrigan, and E.R. Johnston, *Programming Quantum Computers: Essential Algorithms and Code Samples* (O’Reilly Media, Incorporated, 2019).
- [9] Austin Gilliam, Stefan Woerner, and Constantin Gonciulea, “Grover adaptive search for constrained polynomial binary optimization,” (2019), [arXiv:1912.04088 \[quant-ph\]](https://arxiv.org/abs/1912.04088).
- [10] Héctor Abraham et. al., “Qiskit: An open-source framework for quantum computing,” (2019).