Novel Minimal Universal Quantum Gates

Christopher Gilbert

February 2025

Abstract

This paper investigates the construction of universal classical and quantum gates, and proposes two novel quantum sets which use the fewest types of gates for each of their constructions of universality. For a circuit with maximally entangled ancillas—a formulation similar to classical universality—the set containing the controlled irrational Z-rotation gate and the 90-degree Y-rotation gate is universal to an arbitrary precision.

1 Introduction

1.1 Universal Gates

A logic gate is an operation which acts on bits or qubits. For example, the classical AND gate receives two bits and outputs a 1 if and only if both input bits were 1. Let a gate G that takes in n inputs and returns m outputs be denoted

$$G : n \to m$$

In conventional function notation, this is equivalent to

$$G : \{0,1\}^n \to \{0,1\}^m$$

A gate or set of gates is considered universal if some circuit constructed only from those gates can replicate the behavior of every logic circuit.

An example of such a universal gate is the NAND gate ($\overline{\wedge}$ in logical notation) which outputs a 0 if and only if both of its input bits are 1. The universality of NAND can be proved either by exhaustively showing that every possible $2 \to 1$ gate can be constructed by NAND, or with a more formal proof presented later in the paper.

A minimal universal gate set is the smallest possible set of universal gates. For example, $\{\overline{\wedge}\}$ is minimal and universal because no smaller set of gates exists other than the empty set, which cannot replicate most circuits.

1.2 Quantum Gates

1.2.1 Quantum Computing

A quantum computer uses the properties of quantum mechanics in order to perform calculations. All operations on a quantum circuit can be applied in superposition, and specific output states can be selected with the use of phase.

Generally, for any problem that can be checked in polynomial time but can be solved only in exponential time, quantum computers have a quadratic speedup over classical computers by using Grover's algorithm. For some specific algorithms, notably Shor's algorithm [8] , the speedup over classical computers can be up to exponential.

1.2.2 Quantum State Vectors

The state of a classical logical circuit may be represented as a sequence of bits, where each bit represents a specific wire. By interpreting this bit sequence as a binary integer, every classical state can be represented with a single number.

Quantum systems may be in a superposition of multiple states, and so can be represented by a list of the amplitude of each possible classical state. This list is called the state vector and can accurately represent any possible quantum superposition. Thus a classical state with three wires can be in one of eight states, and a quantum state with three qubits (the quantum equivalent of classical bits) can be fully described by a unit vector in $\mathbb{C}^8$. Because

the probability of getting specific states must always add up to 1, and because the probability is the square of the amplitude, the magnitude of the statevector must be 1.

A classical state with state number n may also be represented as the nth unit vector, because it has a 100% chance to be in the state n, and a 0% chance to be in any other state.

1.2.3 Quantum Operations

The state vector representation of a classical or quantum state is extremely helpful because it can formulate universality in terms of linear algebra. For an n-wire circuit with $N = 2^n$ states, an operation that takes each classical state i to the state $\vec{c_i}$ can be written as the matrix

$$(\vec{c_1} \ \dots \ \vec{c_N})$$

Because operations on superpositions are computed across each classical state, such a matrix can be found for any quantum gate, and matrix multiplication corresponds to application of a gate.

In almost all cases, these matrices are square, because most quantum operations are in-place, meaning they change the state but do not add or delete wires from a quantum circuit. However, they can also describe the addition or removal of a helping qubit, called an ancilla.

Many quantum operations are unary or binary, and so only apply to a subset of the wires in a larger circuit. This can be done by combining a gate matrix with identity matrices: for a circuit with n wires, in order to apply U on wires a through b, the following matrix M must be applied to the state vector of the entire circuit:

$$M_{a,b} = I_{2^a} \otimes U \otimes I_{2^{n-b}}$$

where $\otimes$ is the Kronecker product and I_x is the $x \times x$ identity matrix.

Each matrix M represents one way that U can be applied to a circuit, so the problem of universality can be described in terms of a matrix decomposition of any arbitrary operation into matrices of the form of M.

A simpler route to proving universality is to implement another preexisting universal gate set, and it is what will be used throughout this paper to prove universality.

2 Classical Universality

2.1 Classical Circuits

Classical circuits are generally presented as electrical circuit diagrams. For example, Figure 1 is a circuit demonstrating how a NAND gate can replicate the behavior of an XOR gate.

There are some significant differences between a classical circuit diagram and a quantum one, and in order to write a classical circuit in quantum notation, some changes must first be made to it: classical circuit diagrams allow wires to be moved and change directions and be copied and created and destroyed, none of which are allowed in quantum circuits.

In order to change the vertical ordering of wires, all quantum circuits used to prove universal quantum gate sets will also be allowed to use the SWAP gate, represented with a

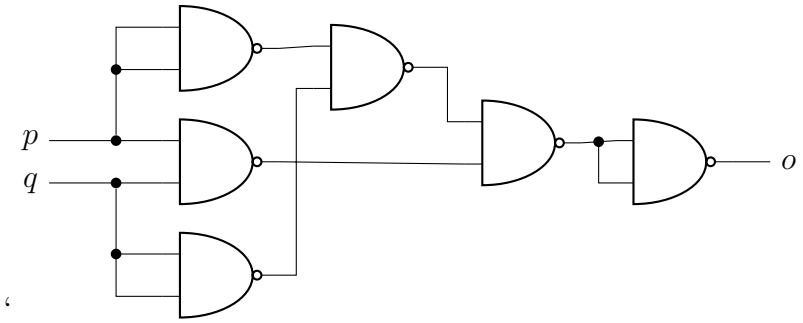

Figure 1: XOR Circuit from NAND Gates

$\times$ symbol on each wire, which swaps the state of two qubits and so is equivalent to crossing wires in a classical circuit.

Because the No Cloning Theorem asserts that quantum states cannot be perfectly copied, one may instead initialize a circuit with a many of wires in each input state. Thus any previously required copying can be achieved through duplication of applied operations.

Because the number of wires in a quantum circuit is, for the most part, constant, instead of $2 \to 1$ gates like NAND, one can implement $2 \to 2$ gates which are still able to replicate the behavior of the original gate. Under this new construction, when given an input of (p, q), one such modified NAND gate may return $(0, p\overline{\wedge}q)$. This simple example is not entirely accurate as quantum gates must also be reversible, but it shows that classical behavior may still be converted into quantum circuitry.

Finally, in most quantum circuits, it is assumed that one may use extra ancilla bits provided in the $|0\rangle$ state. However, this is not the case in classical logic circuitry. If such were the case, a gate like $G(p, q) = \neg p\overline{\wedge}q$ would be universal [1], even though it is not classified as such. This gives rise to a non-trivial difference between "strict" universality, where no extra wires are provided, and "weak" universality, where ancilla qubits are necessary. This paper provides a minimal set for the strict case, but it remains possible to find a smaller set if ancilla qubits are allowed.

After making the above changes, the classical circuit in Figure 1 can be converted into the quantum circuit in Figure 2. For the sake of readability, the state of each wire, logically simplified, is also included after each step.

2.2 Proof of Classical Universality

The most basic classical gates are the $1 \to 1$ gates: I (Identity), $\neg$ (NOT), 1 (Constant 1), and 0 (Constant 0). However, as none of these gates can perform all binary operations (such as AND), so it is impossible for them to be universal. Because of this, a universal gate set must have at least one gate with at least two inputs. With this limitation, the simplest possible gate type that could be universal is $2 \to 1$.

Focusing back to the classical case, without the modifications for implementing it in quantum circuitry, this paper will now present a proof that NAND and NOR are the only $2 \to 1$ universal classical quantum gates. The intuition gained from this proof and the two

[1] For example, it can implement the universal NAND(p, q) with $G(G(0, p), q)$

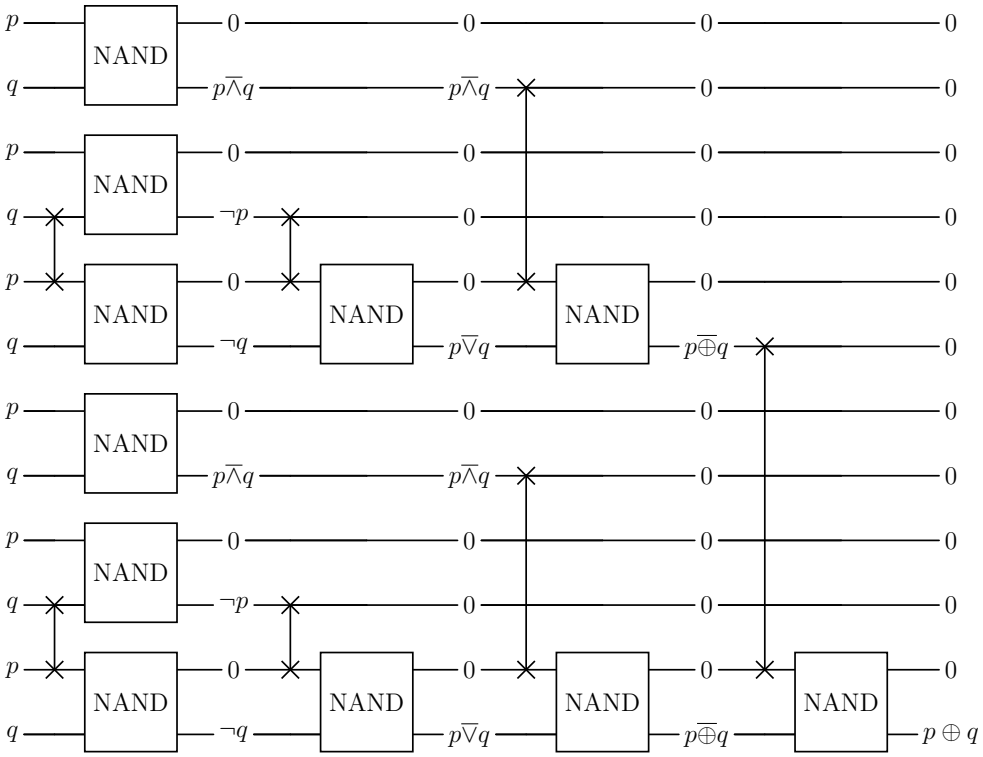

Figure 2: Quantum-Compatible XOR from NAND

conditions for universality that it sets forth will be useful in the following sections of the paper regarding quantum universality.

Theorem 1. *The only* $2 \to 1$ *universal classical gates are NAND and NOR.*

Lemma 1. *For all universal* $2 \to 1$ *gates* G, $G(x, x) = \neg x$ *for all* x.

Proof. All universal $2 \to 1$ gates G must be able to create any other possible gate, including the gate $H(x, y) = 1$.

$H(0, 0) = 1$, so when given an input of $(0, 0)$, G must be able to replicate this output in some way. If $G(0, 0) \neq 1$, then no matter how many times it is applied or the inputs are copied, all wires will be in the 0 state. There would therefore never be any way to get an output in the 1 state. By contradiction, $G(0, 0)$ must equal 1.

By the same logic, when given an input of $(1, 1)$, in order to have any wire in the 0 state, $G(1, 1) = 0$. Therefore, because $G(0, 0) = 1$ and $G(1, 1) = 0$, $G(x, x) = \neg x$. □

Corollary 1. *Any* $2 \to 1$ *universal gate can replicate the behavior of the NOT gate, as any input* x *can be copied to* (x, x)*, onto which* G *can be applied, resulting in* $\neg x$.

Lemma 2. *For all universal* $2 \to 1$ *gates* G, $G(x, \neg x) = G(\neg x, x)$

Proof. In order for a gate to be universal, it must be able to correlate two inputs together. That is, any $2 \to 1$ gate G which can be written as $G(p, q) = H(p)$ or $G(p, q) = H(q)$, for some other $1 \to 1$ gate H, cannot be universal. If G can be represented in such a

way, then the condition holds that it is invariant under at least one input, either because $G(p,q) = G(\neg p, q)$ or $G(p,q) = G(p, \neg q)$ for all p and q. That is,

$$(\forall (p,q), G(p,q) = G(\neg p, q) \vee G(p,q) = G(p, \neg q)) \implies G \text{ is not universal.}$$

By proof of the contrapositive, this statement implies that if G is universal, then the following holds:

$$\neg(\forall (p,q), G(p,q) = G(\neg p, q) \vee G(p,q) = G(p, \neg q)) \tag{1}$$
$$\exists (p,q), \neg(G(p,q) = G(\neg p, q) \vee G(p,q) = G(p, \neg q)) \tag{2}$$
$$\exists (p,q), G(p,q) \neq G(\neg p, q) \wedge G(p,q) \neq G(p, \neg q)) \tag{3}$$
$$\exists (p,q), G(p, \neg q) \neq G(p,q) \neq G(\neg p, q) \tag{4}$$
$$\exists (p,q), G(p, \neg q) = G(\neg p, q) \tag{5}$$

For the sake of contradiction, let $p = \neg q$, (and thus $q = \neg p$),

$$\exists p, G(p,p) = G(\neg p, \neg p)$$

By Lemma 1, this must be false for all universal gates. Therefore, $p = q$, and if G is universal, for all p, it must satisfy

$$G(p, \neg p) = G(\neg p, p)$$

□

Proof. Of the 16 possible $2 \to 1$ gates, only NAND and NOR satisfy both the condition that $G(p,p) = \neg p$ and $G(p, \neg p) = G(\neg p, p)$. Both of these can be exhaustively proved to be universal for all $1 \to 1$ and $2 \to 1$ gates. For example:

$$\neg p = p \overline{\wedge} p \tag{6}$$
$$0(p) = ((p \overline{\wedge} p) \overline{\wedge} p) \overline{\wedge} ((p \overline{\wedge} p) \overline{\wedge} p) \tag{7}$$
$$p \wedge q = (p \overline{\wedge} q) \overline{\wedge} (p \overline{\wedge} q) \tag{8}$$
$$p \vee q = (p \overline{\wedge} p) \overline{\wedge} (q \overline{\wedge} q) \tag{9}$$
$$\text{etc.} \tag{10}$$

In order to prove that NAND and NOR are fully universal (rather than universal for only $2 \to 2$ gates), one can show that it is possible to build a multiplexer to split every possible input state using only NOT (implied to be constructible by the Corollary to Lemma 1), AND (shown above), and OR (shown above). For every possible input, one can select the desired output by either sending the wire w into a $0(w)$ gate for an output of 0, or by sending the wire into an identity gate for an output of 1. Finally, using the OR gate, one can combine all the multiplexed wires back together into a single output. This algorithm is able to create any gate with an arbitrary number of inputs, and multiple $n \to 1$ gates may be put in parallel in order to create an $n \to m$ gate, just as any $f : \mathbb{R}^n \to \mathbb{R}^m$ function may be decomposed as $f(\overrightarrow{x}) = (f_1(\overrightarrow{x}), f_2(\overrightarrow{x}), \ldots, f_m(\overrightarrow{x}))$. Using this approach, any arbitrary gate may be created only from NAND, and thus NAND is universal. The same logic may be applied to NOR to prove its universality. Due to lemmas 1 and 2, these two are the only gates to satisfy both conditions, and so NAND and NOR are the only $2 \to 1$ universal classical gates. □

3 Quantum Universality

Just as in the classical case, all universal gates G must satisfy the two conditions that

- G can implement NOT, and
- G is not independent of one input,

all universal quantum gate sets S must satisfy

- S can implement any single-qubit operation, and
- Some operation in S is not independent of one of its inputs.

In other words, a universal quantum gate set must be able to perform an arbitrary single-qubit rotation (the use of the word rotation for this context will be justified in the next section) and must be able to entangle two qubits together. (The word entanglement refers to a superposition of multiple interconnected states.)

3.1 Bloch Sphere

Recall that a quantum state is represented by a state vector: a linear combination of the possible classical states of the system. This state vector is complex and has a magnitude of 1. Thus, the set of all possible quantum states is isomorphic to a sphere in $\mathbb{R}^4$. However, the complex phase of the $|00\rangle$ state cannot be physically measured or determined, so it is factored out as a coefficient to the state vector as a whole, and largely ignored. This means that a single quantum state is generally visualized as a vector on the unit sphere of $\mathbb{R}^3$, with single-qubit operations corresponding to rotations about the sphere.

3.2 Minimal Universal Quantum Gates

A trivial set of universal quantum gates is the set of all possible rotations plus the entanglement gate CNOT [2]:

$$\{R_X(a) : a \in \mathbb{R}\} \cup \{R_Y(b) : b \in \mathbb{R}\} \cup \{R_Z(c) : c \in \mathbb{R}\} \cup \{\text{CNOT}\}$$

This satisfies the above conditions for universality: it can construct any possible rotation for a single qubit and it can correlate two qubits' states together. Although this set can exactly implement any other possible quantum gate, it contains every possible axis rotation gate, which is far more gates than is necessary.

3.2.1 Irrational Angle Gates

A much smaller universal set can be found after noting the fact that repeated applications of an irrational rotation gate can efficiently approximate arbitrary rotation to within some desired precision.

That is, a gate U, which rotates by an irrational portion of a full rotation θ around an axis, after n applications, results in a total rotation of $n\theta \mod 2\pi$ about that axis. For a

given angle ϕ and any arbitrary precision ε, there is an n such that $|n\theta - \phi \mod 2| < \varepsilon$. This fact can be derived from the Kronecker approximation theorem [5], and a more general result which applies to all possible gates is given by the Solvay-Kitaev theorem [3].

Such irrational angled rotations can be implemented with a sequence of rational rotations in different axes. For example, a rotation by $\pi/4$ in the Z axis followed by a rotation by $\pi/4$ in the X axis results in a rotation angle of

$$\arccos\left(\frac{\sqrt{2}}{2} - \frac{1}{4}\right) \approx 1.09606 \text{ about the axis } \langle 1, 1-\sqrt{2}, 1\rangle.$$

Because of this, the Clifford + T set, consisting of the gates $\{\mathrm{CNOT}, \mathrm{H}, \mathrm{S}, \mathrm{T}\}$, is universal despite the fact that the rotation angle of each single-qubit gate is rational [2].

3.2.2 Reducing the Number of Gates

In the proof of classical universality, two basic properties for universality were established: that any universal set must be able to perform a bit flip on any input, and that it must be able to correlate two wires together. Based on these two properties, one can construct a classically universal set of only two gates, where each performs one action.

The Pauli-Y gate can be used to perform a bit flip, and the CNOT gate can entangle two qubits, and so the set containing those two gates is classically universal.

Although this satisfies the classical requirements, a quantum universal set must also be able to apply a phase-shift to the input. That is, it must be able to impart an arbitrary Z-axis rotation.

Recall that an irrational Z rotation gate $R_Z(2\pi\xi)$ where ξ is irrational can approximate any Z rotation gate. For my gate set, the golden ratio φ will be used as the irrational number, as $n\varphi \mod 1$ is fairly evenly distributed across the unit interval.

In order to transform arbitrary rotation in one axis into arbitrary rotation in any axis, a 90-degree rotation gate can be used. For example, with the 90-degree Y rotation gate (denoted either $R_Y(\pi/2)$ or $Y^{1/2}$), any rotation around the Z-axis may be mapped to a rotation on the X-axis, thus covering the space of all possible rotations around a sphere. Because applying $Y^{1/2}$ twice results in the equivalent of a Y gate, we can replace the Y gate with the the $Y^{1/2}$ gate.

Although our set of CNOT, $Y^{1/2}$, and $R_Z(2\pi\varphi)$ is universal (because it implements arbitrary rotations as well as entanglement), it can be reduced even further by combining gates. Specifically, the CNOT gate can be eliminated by adding a control (meaning that the gate only activates in the $|1\rangle$ state of another qubit) to one of the other gates. If the control is applied to the $Y^{1/2}$, then it would be impossible to bitflip an input only in the $|0\rangle$ state, so the control must be applied to the Z gate.

This logic results in a universal set with only two gates:

$$\{CR_Z(2\pi\varphi), Y^{1/2}\}$$

4 Results

To prove that the proposed set is universal, it must be demonstrated that it can implement any other gate. Since the Clifford + T set is universal, if each gate in this set can be implemented, it follows that the proposed set is also universal. That is, if a gate set can implement gates capable of performing any circuit, it must be able to directly implement any circuit itself, thereby establishing its universality.

4.1 Proof of CNOT

The matrix form of the CNOT gate is

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

which can be implemented with the following circuit (where exponentiation represents repeated application):

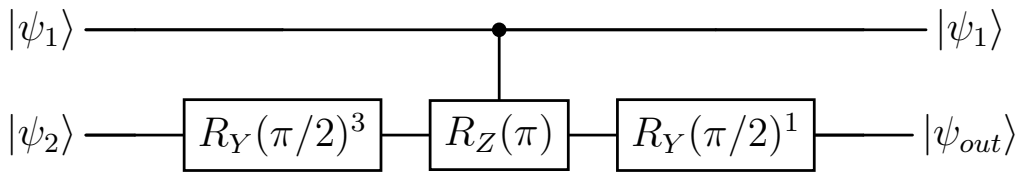

Figure 3: Proof of CNOT Circuit

Multiplying the circuit matrices results in the CNOT matrix, except with a flipped global phase, which is inconsequential. As the arbitrary Z rotation gate has been replaced by the irrational Z rotation gate, $R_Z(\pi)$ must be approximated. With $\varepsilon \leq 10^{-5}$, the approximation comes out to be $R_Z(2\pi\varphi)^{98209}$. This specific exponent was found computationally through a brute force search. The net effect of this circuit is to apply this matrix:

$$\begin{bmatrix} 0.9999999999999997 & 0. & 0. & 0. \\ 0. & 0.9999999999999997 & 0. & 0. \\ 0. & 0. & 0.00000000000957273 - 0.00000357644\mathbf{i} & 0.9999999999904268 + 0.00000357644\mathbf{i} \\ 0. & 0. & 0.9999999999904268 + 0.00000357644\mathbf{i} & 0.00000000000957273 - 0.00000357644\mathbf{i} \end{bmatrix}$$

which approximates CNOT to $\varepsilon = 7.15287 \times 10^{-6}$, within the desired accuracy.[2]

4.2 Proof of T

Implementing the T gate itself is fairly simple, because T is equivalent to $R_Z(\pi/2)$. However, R_Z and CR_Z are considered different gates, so in order to implement a $R_Z(\pi/2)$, a state in

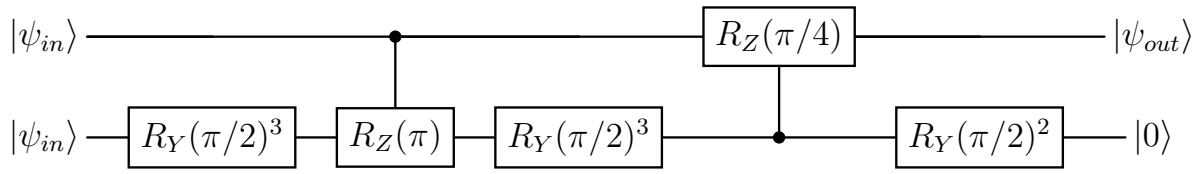

Figure 4: Proof of T Circuit

the $|1\rangle$ state must be prepared. Without the use of an ancilla qubit already in the $|0\rangle$ state, it can be done with the following circuit:

Again, the $R_Z(\pi)$ gate is approximated with $R_Z(2\pi\varphi)^{98209}$, and $R_Z(\pi/4)$ is approximated with $R_Z(2\pi\varphi)^{5796}$. The result of this circuit is to apply the matrix:

$$\begin{bmatrix} 0.9999999999999993 & 0. \\ 0. & 0.7071096086512368 + 0.7071003772806271\mathbf{i} \end{bmatrix}$$

which approximates the T gate to $\varepsilon = 7.00033 \times 10^{-6}$.

4.3 Proof of S

The S gate is equivalent to T^2. By applying the matrix proven above twice, one finds that the resultant matrix

$$\begin{bmatrix} 0.9999999999999991 & 0. \\ 0. & 0.0000029394225792 + 1.0000050578127595\mathbf{i} \end{bmatrix}$$

approximates the S gate to $\varepsilon = 5.84993 \times 10^{-6}$.

4.4 Proof of H

The H gate is the most difficult to implement, as it contains an off-axis rotation (around the line X = Z). This leads to a more complex circuit approximation:

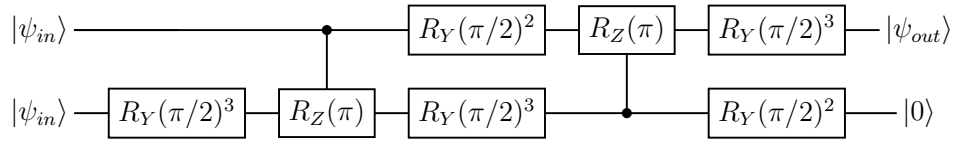

Figure 5: Proof of H Circuit

To keep the final ε less than 10^{-5}, a more presice estimate for $R_Z(\pi)$ must be found. The first exponent which meets this criteria is $R_Z(2\pi\varphi)^{416020}$. The circuit matrix

$$\begin{bmatrix} 0.7071067812048173 - 0.00000119421\mathbf{i} & 0.7071067812048173 - 0.00000119421\mathbf{i} \\ 0.7071067812048173 - 0.00000119421\mathbf{i} & 0.7071067812048173 - 0.00000119421\mathbf{i} \end{bmatrix}$$

is able to approximate the H gate to $\varepsilon = 2.38842 \times 10^{-6}$.

[2]The Solvay-Kitaev theorem [3] is given in terms of the L2 matrix norm, but as the L2 norm bounds the Frobenius norm from below [4], the computationally simpler Frobenius norm is used for epsilon values.

5 Discussion

5.1 Universality

During this paper's discussion of classical universality, it was proven that in order for a gate G to be universal, it must satisfy that $G(p, p) = \neg p$ and that $G(p, \neg p) = G(\neg p, p)$ for all p. This corresponds to the generalizable intuitions that, for every possible input, a universal set must contain a gate that transforms that input in some way, as well as a gate which correlates two outputs together. Not only were these two properties useful in determining universality in the classical case, they also provided the foundational insight that led to the universal set of quantum gates presented above.

5.2 Quantum Gate Sets

Among the infinite possible universal quantum gate sets, some have been found to use very few gates, such as $\{\text{Toffoli}, H\}$ [7] or $\{CC_iR_x(\xi\pi)\}$ [9], but require $|0\rangle$ ancilla qubits or 3-qubit gates (i.e. the Toffoli and Deutsch gate). To my knowledge, the set $\{CR_Z(2\pi\varphi), R_Y(\pi/2)\}$ is the smallest universal set of quantum gates yet found to only use 2-qubit gates and to satisfy strict universality.

In the results section, it was proved that the gate set is truly universal, and it was shown to approximate another universal gate set to within one part in a million.

5.3 Future Work

Following this research, there are many possible extensions, both to the gate set itself and the principles provided within it. For example, it is likely possible to construct a universal gate set with an X rotation gate instead of the Y rotation gate. In the formulation of universality allowing for ancillas in the $|0\rangle$ state, the gate $C_0R_Y(2\pi\xi_1)R_Z(2\pi\xi_2)$—A zero-controlled gate with dual-axis irrational rotation—may be universal so long as $\xi_1 \neq k\xi_2$ for all rational k. This is because it should be able to construct any arbitrary rotation around the sphere, and because it can correlate two qubits together. This is not a proven assertion, but a result of the intuitions given in the paper so far, and a possibly intriguing area of research because it would lead to a 2-qubit gate set consisting of only a single gate.

References

[1] A. Barenco et al. "Elementary gates for quantum computation". In: *Physical Review A* 52.5 (1995), p. 3457.

[2] P. Boykin et al. "A new universal and fault-tolerant quantum basis". In: *Information Processing Letters* 75.3 (2000), pp. 101–107. DOI: 10.1016/s0020-0190(00)00084-3.

[3] Christopher M. Dawson and Michael A. Nielsen. *The Solovay-Kitaev algorithm*. 2005. arXiv: quant-ph/0505030 [quant-ph]. URL: https://arxiv.org/abs/quant-ph/0505030.

[4] R. Geijn and M. Myers. *1.3.3 The Frobenius norm*. Retrieved November 7, 2024, from https://www.cs.utexas.edu/ flame/laff/alaff-beta/chapter01-frobenius-norm.html.

[5] E. Hlawka, R. Taschner, and J. Schoißengeier. "The Kronecker approximation theorem". In: *Geometric and Analytic Number Theory*. 1986, pp. 19–37. DOI: 10.1007/978-3-642-75306-0_2.

[6] M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information*. 10th. Cambridge University Press, 2023.

[7] Y. Shi. "Both Toffoli and Controlled-NOT need little help to do universal quantum computation". In: (2002). Retrieved from https://arxiv.org/abs/quant-ph/0205115.

[8] Peter W. Shor. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". In: *SIAM Journal on Computing* 26.5 (Oct. 1997), pp. 1484–1509. ISSN: 1095-7111. DOI: 10.1137/s0097539795293172. URL: http://dx.doi.org/10.1137/S0097539795293172.

[9] "Universality in Quantum Computation". In: *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences* 449.1937 (June 1995), pp. 669–677. ISSN: 2053-9177. DOI: 10.1098/rspa.1995.0065. URL: http://dx.doi.org/10.1098/rspa.1995.0065.