On Minimal Universal Quantum Gates

Christopher Gilbert

August 2024

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 ancilla qubits, a zero-controlled dual-axis irrational rotation gate is universal within arbitrary prescision, and for a maximally entangled circuit with no ancillas—a construction more similar to classical universality—the set containing the controlled 90-degree Z-rotation gate and the irrational Y-rotation gate is universal to any prescision.

1 Introduction

1.1 Universal Gates

A logic gate is an operation which acts on bits or qubits. For example, the classical AND gate recieves 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 would be written

$$G : \mathbb{B}^n \to \mathbb{B}^m \text{ where } \mathbb{B} = \{0, 1\}$$

A gate or set of gates is universal if some arrangement of the gates can replicate the behavior of every possible gate.

An example of such a $2 \to 1$ gate for classical universality is the NAND gate, denoted $\overline{\wedge}$, 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 which will be presented later on.

A gate set is said to be minimal if it is the smallest gate set possible to make. For example, $\{\overline{\wedge}\}$ is a minimal universal set because any computation is impossible without at least one operation, and so a set with only a single element is the smallest possible set to be universal.

1.2 Quantum Gates

1.2.1 Quantum Computing

A quantum computer uses the properties of quantum mechanics in order to perform calculations. By creating a superposition of multiple possible inputs, all operations in a circuit are simultaneously done on each input. By canceling out the probabilities of inputs with negative results using quantum phase, an operation can find only the correct inputs with a quadratic improvement over classical computers. For other less generalizable quantum algorithms, notably Shor's algorithm, the speedup over classical computers can be up to exponential.

1.2.2 Quantum State Vectors

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

Quantum states, on the other hand, may be in a superposition of multiple states and so may be represented as a list of probability amplitudes corresponding to each 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 can be fully described by a unit vector in $\mathbb{C}^8$. The state vector must always have a length of 1, because the sum of the squared amplitudes has to be 1, just as the sum of a set of probabilities must always add up to 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.

1.2.3 Quantum Operations

The state vector representation of a classical or quantum state is extremely helpful in formulating universality mathematically using linear algebra. For an n-wire circuit

with $N = 2^n$ states, a matrix

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

will take a classical state vector in the state i to the state vector $\vec{c_i}$. Thus, any operation can be directly described as a matrix of the output state vectors for each input.

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. Some exceptions include state preperation matrices (which are used to mathematically describe extra ancilla wires) and discarding matrices (which remove a 0-state wire from a circuit).

In most cases, an operation is done only on a subset of the wires in a circuit. In order to apply an operation matrix, it first needs to be combined with identity matrices until it achieves the correct dimensions. For a circuit with n wires, in order to operate O on wires a through b, the following matrix M must be applied to the state vector of the entire circuit:

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

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

Each matrix M represents one way that O 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.

The proofs of universality presented in this paper will rely on decomposing each operation in an already proven quantum gate set into operations from a smaller gate set.

2 Classical Universality

2.1 Classical Circuits

Classical circuits are generally presented as electrical circuit diagrams. For example, a demonstration of how an XOR gate can be made from NAND gates is given in Figure 1.

This classical diagram has a number of properties which differ from most quantum circtuits:

- Wires are allowed to cross and move
- Wires may be copied or duplicated

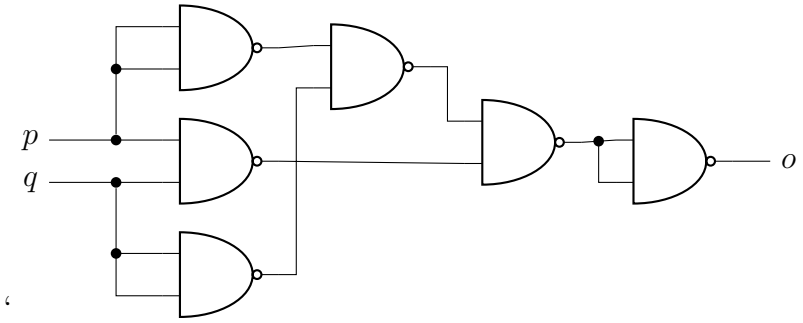

Figure 1: XOR Circuit made from NAND Gates

- Gates may change the number of wires
- No ancilla wires (in the 0 state) are provided

In order to rectify the first disparity, all quantum circuits used to prove universal quantum gate sets will also be allowed to use the SWAP gate, represented with a $\times$ symbol on each wire, which swaps the state of two qubits and so is equivalent to crossing wires in a classical circuit.

The second disparity presents a more significant problem, because the No Cloning Theorem asserts that quantum states cannot be perfectly copied. Instead of directly copying states, another approach is to initialize a circuit with a number of wires in each state. Thus any previously required copying can be acheived throgh duplication of the applied operations.

The third disparity can be prevented by changing the types of classical gates used. Instead of $2 \to 1$ gates like NAND, one can implement $2 \to 2$ gates which replicate the behavior of the original gate on the lower output wire, and then have some other dummy behavior on the upper output wire. Under this new construction, when given an input of (p, q), the modified NAND gate returns $(0, p\overline{\wedge}q)$. This simple example is not entirely accurate as quantum gates must also be reversible for reasons of physics, but this approach can generally be applied.

The final disparity can be solved by just dissallowing any ancilla wires in quantum circuits, but under most formulations of quantum universality, it is assumed that as many ancilla bits are given as are required. This is not so much a mathematical problem as it is a problem with differing definitions of universality. Because of this, this paper will explore both the case where ancilla bits in the 0 state are allowed.

Fig. 2 shows the new implementation of an XOR gate after making the above changes. It only uses modified $2 \to 2$ NAND gates, and it also shows the current state at various positions along the circuit, logically simplified as much as possible.

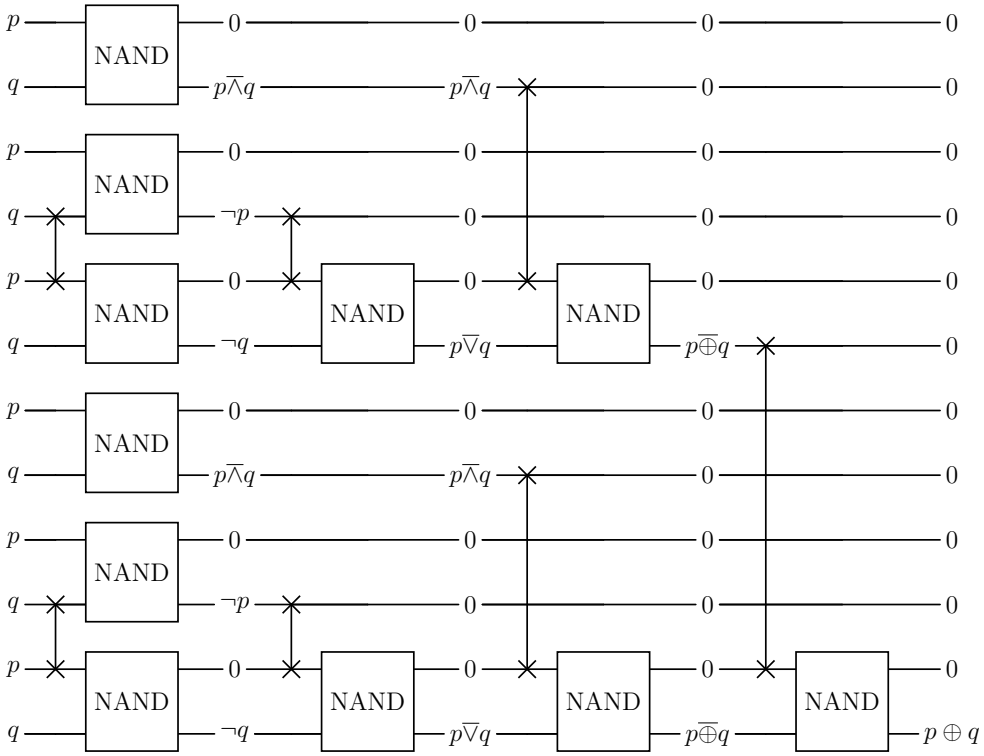

Figure 2: Quantum-Compatible XOR from NAND

2.2 Proof of Classical Universality

The most basic classical gates are the $1 \to 1$ gates: I (Ientity), $\neg$ (NOT), 1 (Constant 1), and 0 (Constant 0). However, as none of these gates can relate one bit to another, none can perform all binary operations (Such as AND), so it is impossible for any 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 regular classical case, without the modifications for implementing it in quantum circutry, this paper will now present a proof that NAND and NOR are the only $2 \to 1$ universal classical quantum gates.

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

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

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 $G(1, 1) = 0$, $G(x, x) = \neg x$. □

Corrolary 1. *Any $2 \to 1$ universal gate can replicate the behavior of the $1 \to 1$ 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, a 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. Therefore, any gate G such that for all inputs p and q, either $G(p, q) = G(!p, q)$ or $G(p, q) = G(p, !q)$ is not universal.

Let U be an oracle which is able to determine if G is universal. Implementing the condition just described into formal logic and simplifying, it becomes:

$$(\forall(p, q), G(p, q) = G(\neg p, q) \vee G(p, q) = G(p, \neg q)) \implies \neg U(G) \tag{1}$$
$$U(G) \implies \neg(\forall(p, q), G(p, q) = G(\neg p, q) \vee G(p, q) = G(p, \neg q)) \tag{2}$$
$$U(G) \implies \exists(p, q), \neg(G(p, q) = G(\neg p, q) \vee G(p, q) = G(p, \neg q)) \tag{3}$$
$$U(G) \implies \exists(p, q), G(p, q) \neq G(\neg p, q) \wedge G(p, q) \neq G(p, \neg q)) \tag{4}$$
$$U(G) \implies \exists(p, q), G(p, \neg q) \neq G(p, q) \neq G(\neg p, q) \tag{5}$$
$$U(G) \implies \exists(p, q), G(p, \neg q) = G(\neg p, q) \tag{6}$$

For the sake of contradiction, when $p = \neg q$, (and thus $q = \neg p$), this statment simplifies to:

$$U(G) \implies \exists(p, q), G(p, p) = G(\neg p, \neg p)$$

which, by Lemma 1, must be false. Therefore, when this condition for universality is met, $p = q$, and therefore:

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

□

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, such as

$$\neg p = p \overline{\wedge} p \tag{7}$$
$$0(p) = (p \overline{\wedge} p) \overline{\wedge} p \tag{8}$$
$$p \wedge q = (p \overline{\wedge} q) \overline{\wedge} (p \overline{\wedge} q) \tag{9}$$
$$p \vee q = (p \overline{\wedge} p) \overline{\wedge} (q \overline{\wedge} q) \tag{10}$$
$$\text{etc.} \tag{11}$$

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 constructable by the Corrolary to Lemma 1), AND (proved above), and OR (proved above). After the inputs have been multiplexed, for each 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 paralell 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 it's universality. Due to lemmas 1 and 2, NAND and NOR are the only possible $2 \to 1$ universal gates, and so the only $2 \to 1$ universal classical gates are NAND and NOR. □

3 Quantum Universality

Just as all classical gates needed to be able to change single bits (i.e., implement the NOT gate, as was proven in the Corrolary to Lemma 1) as well as correlate bits together (as proved in Lemma 2), for a set of quantum gates to be universal, it must be able to make every possible change to an individual qubit's state as well as have some method to correlate or entangle multiple qubits together.

3.1 Bloch Sphere

Recall that a quantum state is represented by a statevector: a linear combination of the possible classical states of the system. This statevector is complex, due to

quantum physics, and has a magnitude of 1, due to the summation of probabilities. Thus, the set of all possible quantum states is isomorphic to a sphere in $\mathbb{R}^4$. However, the complex phase of the $|00\rangle$ (i.e. $\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$) state cannot be physically measured or determined, so it is factored out as a coefficient to the state vector which can then be discarded. This means that a 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.

One of the most commonly used universal quantum gates sets is the Clifford + T set, containing CNOT, H, S, T. However, as S is a /2 rotation about the Z axis of the bloch sphere and as T is a /4 rotation around a bloch sphere, how is an arbitrary Z rotation gate constructed from this universal set? It would seem to me that only rotations by a multiple of /4 around the Z axis would be possible?

For example, how could you construct a RZ(/3) rotation gate solely from the Clifford + T set?