On Minimal Universal Quantum Gates

Christopher Gilbert

August 2024

Abstract

This paper investigates the construction of universal classical and quatum 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, 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.

1 Introduction

1.1 Universal Gates

A logic gate is an operation which acts on bits or qubits. For example, the classical AND gate, denoted $\wedge$, takes in 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 $G : n \to m$. 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, $\overline{\wedge}$, which outputs a 0 if and only if both of it's input bits are 1. The universality of $\overline{\wedge}$ can be proved either by exhaustively showing that every possible $2 \to 1$ gate can be constructed by $\overline{\wedge}$, 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, $\wedge$ is a minimal universal set because an 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 Statevectors

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 represetned with a single number.

Quantum states, on the other hand, may be in a superposition of multiple states. and so may be represented as list of probability amplitudes corresponding to each classical state. This list is called the statevector, 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 normal vector in $\mathbb{C}^8$. The statevector 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 statevector representation of a classical or quantum state is extremely helpful in formulating universality mathematically using linear algebra. For a n-wire circuit with $N = 2^n$ states, a matrix $(\vec{c_1} \ \dots \ \vec{c_N})$ will take a classical statevector in the state i to the statevector $\vec{c_i}$. Thus, any operation can be directly described as a matrix of the output statevectors for each input.

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 identiy matrixes until it acheives 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

statevector 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 matrixes 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