Quantum Scrambling Review*

Samuel A. Hopkins

Level 7 MSci. Laboratory, Department of Physics, University of Bristol.

(Dated: November 18, 2022)

Abstract Goes Here...

CONTENTS

I. INTRODUCTION

II. BACKGROUND THEORY

A. Quantum Information and Circuits

Quantum Information and Quantum Computation is built upon the concept of quantum bits (qubits for short), represented as a computational basis state of either $|0\rangle$ or $|1\rangle$. With this, the quantum state of a system can be completely specified by writing the state as a linear combination, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where α, β are complex numbers. This is easily extended to multi-party quantum systems of n qubits. Then we may write computational basis states as strings of qubits using the tensor product;

$$|x_1\rangle \otimes |x_2\rangle \otimes ... \otimes |x_n\rangle \equiv |x_1 x_2 ... x_n\rangle.$$

The evolution and dynamics of such systems can be represented via quantum circuits, made up of quantum logic gates acting upon the qubits of a system. Analogous to a classical computer which is comprised of logic gates that act upon bit-strings of information. In contrast, quantum logic gates are linear operators acting on qubits, often represented in matrix form. This allows us to decompose a complicated unitary evolution into a sequence of linear transformations on one or more qubits. A common practice is to create diagrams of such evolutions, with each quantum gate having their own symbol, analogous to circuit diagrams in classical computation, allowing the creation of complicated quantum circuitry that can be directly mapped to a string of linear operators acting on a set of qubits. Some example gate symbols can be seen in Fig. 1.

The gates shown in Fig. 1 are known as the Pauli

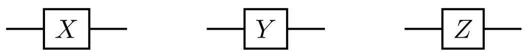

FIG. 1: Gate symbols for the Pauli operators in quantum circuits.

operators, equivalent to the set of Pauli matrices, $P \equiv \{X, Y, Z\}$ for which X, Y and Z are defined in their matrix representation as;

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{1}$$

These gates are all one-qubit gates, as they only act upon a single qubit. The simplest gate is that of the Identity operator (or matrix), I, from which, an algebra can be formed with the Pauli matrices. Notably, the set of Pauli matrices along with the identity form a group known as the Pauli group, P_n, defined as the 4^n n-qubit tensor products of the Pauli matrices (1) and the Identity matrix, I, with multiplicative factors, ± 1 and $\pm i$ to ensure a legitimate group is formed. For clarity, consider the Pauli group on 1-qubit, P_1;

$$P_1 \equiv \{\pm I, \pm iI, \pm X, \pm iX \pm Y, \pm iY, \pm Z, \pm iZ\}, \tag{2}$$

From this, another group of interest can be defined, namely the Clifford group, C_n, for which the elements are the Hadamard, Controlled-Not and Phase operators.

The Hadamard, H, maps computational basis states to a superposition of computational basis states, written explicitly in it's action;

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}},$$
$$H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}},$$

or in matrix form;

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Controlled-Not, $CNOT$, is a two-qubit gate. One qubit acts as a control for an operation to be perfomed on the other qubit. It's matrix representation is

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{3}$$

The Phase gate, denoted S is defined as,

$$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2}} \end{bmatrix}$$

The CNOT gate is used to create entanglement in circuits to generate states that cannot be written in product form. For example, if we prepare a Bell state $|\phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$. We cannot write this as

$$\begin{aligned} |\psi_1\rangle &= [\alpha_0|0\rangle + \beta_0|1\rangle] \otimes [\alpha_1|0\rangle + \beta_1|1\rangle] \\ &= \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle \end{aligned}$$

since the α_0 or β_1 must be zero in order to ensure the $|01\rangle$, $|10\rangle$ vanish. However, this would make the coefficients of the $|00\rangle$ or $|11\rangle$ terms zero, breaking the equality. Thus, $|\psi_1\rangle$ cannot be written in product form and is said to be entangled. This defines a general condition for a arbitrary state to be entangled.

B. Clifford Circuits and Stabilizer Formalism

A notable family of circuits are known as *Clifford circuits*. These are circuits comprised only of unitary operators from the Clifford group, namely the Hadamard, CNOT (Controlled-Not) and the S (phase) gate. In matrix form, these gates are defined as,

Quantum circuits made only of Clifford gates are said to be *classically simulable*, that is, circuits of this construction can be efficiently simulated on a classical computer with polynomial effort via the Gottesman-Knill theorem [1]. For this reason, Clifford gates do not form a set of universal set of quantum gates.

It is useful to extend the gate set to a group, to exploit mathematical techniques from group theory. In this case the set of operators $\{H, CNOT, S\}$ generate the Clifford group C_n. The group, C_n, is defined as the set of operators (also called unitaries) that normalise the Pauli group, P_n. Where P_n is defined

III. OPERATOR SCRAMBLING

A. Operator Entanglement

IV. FURTHER RESEARCH

[1] D. Gottesman, "The heisenberg representation of quantum computers," 1998.