

Quantum Scrambling Review*

Samuel A. Hopkins

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

(Dated: November 19, 2022)

Abstract Goes Here...

CONTENTS

I. INTRODUCTION	1
II. Background Theory	1
A. Quantum Information and Circuits	1
B. Clifford Circuits and Stabilizer Formalism	3
C. Free-Fermion Circuits	4
III. Operator Scrambling	4
A. Operator Entanglement	4
IV. Further Research	4
References	5

I. INTRODUCTION

II. BACKGROUND THEORY

A. Quantum Information and Circuits

Quantum Information is built upon the concept of quantum bits (qubits for short), represented as a linear combination of states in the standard basis, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where α, β are complex probability amplitudes and the vectors, $|0\rangle, |1\rangle$ are the computational basis states that form the standard basis.

This is easily extended to multi-party or composite systems of n qubits. The total Hilbert space, \mathcal{H} of such a system is defined as the tensor product of n subsystem Hilbert Spaces,

$$\mathcal{H} = \otimes_n \mathcal{H}_n = \mathcal{H}_{n-1} \otimes \mathcal{H}_{n-2} \otimes \cdots \otimes \mathcal{H}_0 \quad (1)$$

Then we may write the computational basis states of this system, as strings of qubits, using the tensor product [1];

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

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. 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 sequence of linear operators acting on a one or more qubits. Some example gate symbols can be seen in Fig. 1.

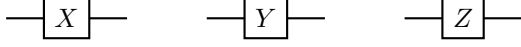


FIG. 1: Gate symbols for the Pauli operators in quantum circuits.

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

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad (2)$$

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. Satisfying the following relations:

$$XY = iZ \quad YZ = iX \quad ZX = iY \quad (3)$$

$$YX = -iZ \quad ZY = -iX \quad XZ = -iY \quad (4)$$

$$X^2 = Y^2 = Z^2 = I \quad (5)$$

Notably, the set of Pauli matrices and the identity form the Pauli group, \mathcal{P}_n , defined as the 4^n n -qubit tensor products of the Pauli matrices (2) 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, \mathcal{P}_1 ;

$$\mathcal{P}_1 \equiv \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}, \quad (6)$$

From this, another group of interest can be defined, namely the Clifford group, \mathcal{C}_n , defined as the set of unitary operators (also called unitaries) that normalise the Pauli group. The elements of this group 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 performed on the other qubit. It's matrix representation is

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad (7)$$

The Phase operator, denoted S is defined as,

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

The CNOT operator is often 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

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

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, $|\Phi^+\rangle$ cannot be written in product form and is said to be entangled. This defines a general condition for a arbitrary state to be entangled. [2]

B. Clifford Circuits and Stabilizer Formalism

Quantum circuits comprised of only quantum gates from the Clifford group are known as *Clifford Circuits*. This family of circuits is of considerable interest as they are classically simulable, that is, circuits of this construction can be efficiently simulated on a classical computer with polynomial effort via the Gottesman-Knill theorem [3]. For this reason, Clifford gates do not form a set of universal quantum gates, meaning a universal quantum computer cannot be constructed using a set of Clifford gates. A set of universal quantum gates allows for any unitary operation to be approximated to arbitrary accuracy by a quantum circuit, constructed using only

the original set of gates.

Stabilizer Formalism. An arbitrary, pure quantum state, $|\psi\rangle$ is *stabilized* by a unitary operator, S if $|\psi\rangle$ is an eigenvector of S , with eigenvalue 1, satisfying:

$$S|\psi\rangle = |\psi\rangle \quad (8)$$

The key idea here is that the quantum state can be described in terms of the unitaries that stabilize it, instead of the state itself. This is due to $|\psi\rangle$ being the unique state that is stabilized by U . [4] This can be seen from considering the Pauli matrices, and the unique states they stabilize. In the one-qubit case these are the +1 eigenstates of the pauli matrices;

$$X(|0\rangle + |1\rangle) = |0\rangle + |1\rangle \quad (9)$$

$$Y(|0\rangle + i|1\rangle) = |0\rangle + i|1\rangle \quad (10)$$

$$Z|0\rangle = |0\rangle \quad (11)$$

If given a group or subgroup of unitaries, \mathcal{U} , the vector space V , of n qubit states is stabilized by \mathcal{U} if every element of V is stable under action from every element of \mathcal{U} . This description is more appealing, as we can exploit mathematical techniques from group theory to describe quantum states and vector spaces. More precisely, the group \mathcal{U} can be described using it's generators. In general, a set of elements g_1, \dots, g_d of a group, \mathcal{G} , generate the group if every element of \mathcal{G} can be written as a product of elements from the set of generators, g_1, \dots, g_d , such that $\mathcal{G} := \langle g_1, \dots, g_d \rangle$. For example, consider the

group $\mathcal{U} \equiv \{I, Z_1 Z_2, Z_2 Z_3, Z_1 Z_3\}$. \mathcal{U} can be compactly written as $\mathcal{U} = \langle Z_1 Z_2, Z_2 Z_3 \rangle$, by recognising $(Z_1 Z_2)^2 = I$ and $Z_1 Z_3 = (Z_1 Z_2)(Z_2 Z_3)$.

This allows for the description of a quantum state, and subsequently it's dynamics, by the generators of a stabilizer group. To see how the dynamics of a state are represented in terms of generators, consider a stabilizer state under the action of a unitary (gate in quantum circuit models):

$$U|\psi\rangle = US|\psi\rangle = USU^\dagger U|\psi\rangle \quad (12)$$

Where S is a generator from an arbitrary stabilizer group. It can be seen that the state, $U|\psi\rangle$ is then stabilized by USU^\dagger , implying the vector space evolved by U , is stabilized by the group USU^\dagger , which can be written in terms of its generators, $US_1 U^\dagger, \dots, US_d U^\dagger$. Thus, only the change in the generators needs to be computed, instead of the change in the whole stabilizer group.

C. Free-Fermion Circuits

III. OPERATOR SCRAMBLING

A. Operator Entanglement

One of the key papers originally investigated, was that of Blake and linden's where they showed

IV. FURTHER RESEARCH

- [1] B. Schumacher and M. Westmoreland, *Quantum Processes Systems, and Information*. Cambridge University Press, 2010.
- [2] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.
- [3] D. Gottesman, “The heisenberg representation of quantum computers,” 1998.
- [4] S. Aaronson and D. Gottesman, “Improved simulation of stabilizer circuits,” *Phys. Rev. A*, vol. 70, p. 052328, Nov 2004.