Bachelor Thesis
Decoding the Color Code

Clemens Schumann,
Advised by Peter-Jan Derks

November 28, 2022

Contents

1 Introduction to the Algebra

In the following we will give an overview of the utilized algebra in quantum information theory.
To this end we must first return to the fundamentals of quantum mechanics.

1.1 Schroedinger and Heisenberg picture

1.1.1 Schroedinger picture

In the Schroedinger picture, we focus on the time evolution of states:

$$|\psi\rangle = |\psi\rangle(t) \tag{1}$$

In this picture we can introduce quantum circuit diagram notation, whereby:

- States progress in time along horizontal parallel lines
- Time goes from left to right
- Gates denoted X,Y,Z are the single qubit pauli operators $\sigma_x, \sigma_y, \sigma_z$
- Gates can act on one or multiple qubits, whereby an X gate on qubit 1 in a 3-qubit system should be interpreted as:
  $(X \otimes \mathbb{I} \otimes \mathbb{I})(|\psi_1\rangle \otimes |\psi_2\rangle \otimes |\psi_3\rangle)$

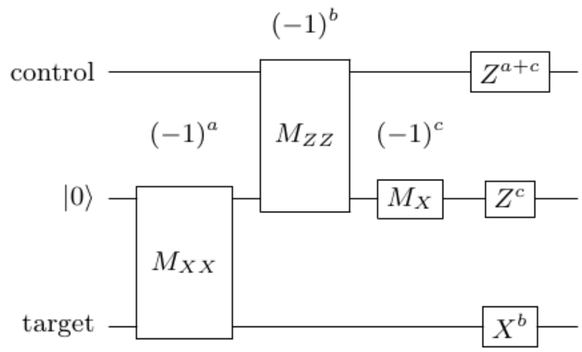

Figure 1: A Quantum Circuit to implement a measurement based Controlled-$X_{|\psi\rangle_{control} \to |\psi\rangle_{target}}$ Gate, where $|0\rangle$ is the +1 eigenstate in σ_z-basis.

As can be seen explicitly calculated in the familiar Schroedinger picture in Appendix 3.1, the circuit from figure 1 implements a CNOT-gate from the control qubit to the target qubit.

We will now analyze this circuit in the Heisenberg picture, finding that it results in an equal output.

1.1.2 Heisenberg Picture

In this picture, we focus on the time evolution of operators instead of states:

$$A = A(t) \tag{2}$$

By considering specifically the operators to which the input state space is part of those operators eigenstatespace, we can compute the output of any circuit:

$$Circuit(|\phi\rangle) = Circuit(A)|\phi\rangle \tag{3}$$

if $|\phi\rangle$ is an eigenstate of A.
This is true because for any unitary operation on a multi-qubit System applying A to a circuit implementing operator B:

$$|\psi\rangle \to^B B|\psi\rangle \tag{4}$$

$$\Rightarrow^A A|\psi\rangle \to^B AB|\psi\rangle = (ABA^\dagger)A|\psi\rangle \tag{5}$$

If $A|\psi\rangle = |\psi\rangle$, this simplifies to:

$$|\psi\rangle \rightarrow (ABA^\dagger)|\psi\rangle \tag{6}$$

Therefore the circuit operator $B \rightarrow (ABA^\dagger)$.

We call an operator/gate A, to which the input state is an eigenvector, a "Stabilizer" of that input state.
The "Stabilizer group" is a generating subset of the set of such operators.
One notable group of operators is the pauli group. It has the feature that it is "complete", in the sense that any transformation of a single qubit states into another can be achieved by sequential application of these transformations.
Also, for each $A \in P_G, n \in \mathbb{N} : A^{2n} = \mathbb{I}$.
We therefore use the Pauli Group as generating set for our stabilizers, so e.g. the input state in figure 1 is only stabilized by $\mathbb{I} \otimes Z \otimes \mathbb{I}$ (and trivially $\mathbb{I} \otimes \mathbb{I} \otimes \mathbb{I}$).
In our case, for the first Measurement in circuit 1 , A is $\mathbb{I} \otimes Z \otimes \mathbb{I}$ and B is $\mathbb{I} \otimes \mathbb{I} \otimes \mathbb{I} \pm \mathbb{I} \otimes X \otimes X$, so depending on wether the measurement result is ± 1 after the first Measurement, to obtain the evolved Operator we need to compute:

$$(\mathbb{I} \otimes Z \otimes \mathbb{I})(\mathbb{I} \otimes \mathbb{I} \otimes \mathbb{I} \pm \mathbb{I} \otimes X \otimes X)(\mathbb{I} \otimes Z \otimes \mathbb{I})^\dagger \tag{7}$$

This notation quickly becomes quite convoluted, so in the following we shall denote the Stabilizer as S, and the measurements as $M_1^\pm, M_2^\pm, M_3^\pm$, where
$M_1^\pm = \mathbb{I} \otimes \mathbb{I} \otimes \mathbb{I} \pm \mathbb{I} \otimes X \otimes X$,
$M_2^\pm = \mathbb{I} \otimes \mathbb{I} \otimes \mathbb{I} \pm Z \otimes Z \otimes \mathbb{I}$ and
$M_3^\pm = \mathbb{I} \otimes \mathbb{I} \otimes \mathbb{I} \pm \mathbb{I} \otimes X \otimes \mathbb{I}$.
After the second measurement the system operator evolves to:

$$M_2^{\dagger\pm} M_2^\pm S M_1^\pm \tag{8}$$

After the third it evolves to:

$$M_3^{\dagger\pm} M_3^\pm M_2^{\dagger\pm} M_2^\pm S M_1^\pm \tag{9}$$

KP THIS NEEDS CLIFFORD STUFF

1.2 The Clifford Gates

It has been proven in *reference source* that operators that take a state stabilized by some member of the Pauli-Group to a state stabilized by another member of the Pauli-Group can be simulated efficiently on a classical computer. The Group of operators that satisfy this condition is called the Clifford-Group.

For the decoder we wish to implement in this thesis it therefore makes sense to focus on those first and foremost, as applying corrective gates is a computationally/ experimentally expensive task that should be put off to the latest possible moment, and the propagation of an error until then can be simulated efficiently.

The Clifford-Group can be generated by:

- The Hadamard-Gate, which performs single qubit basis changes from eigenstates of X to eigenstates of Z and vice-versa:

  $H|+\rangle = |0\rangle$, $H|0\rangle = |+\rangle$, $H|-\rangle = |1\rangle$, $H|1\rangle = |-\rangle$

- The Phase-Gate, which performs single qubit sign flips on the state parts which are $|1\rangle$ in the computational basis:

  $P(\alpha|0\rangle \pm \beta|1\rangle) = \alpha|0\rangle \mp \beta|1\rangle$

- The CNOT-Gate, which on a two qubit system performs an X gate on the second qubit if the first qubit is $|1\rangle$, so takes:

  $\alpha|00\rangle + \beta|01\rangle + \delta|10\rangle + \gamma|11\rangle$
  $\Rightarrow \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$

In the σ_z-basis their matrix representations are:

- $H = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$; $P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$

- $CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

1.3 Error Detection and Correction

One of the big challenges of physically realising a quantum computer is its subjection to noise in the real world. Unlike classical computers, the type of error is not limited to a bitflip, as even single qubit states have a theoretically infinit amount of differing states to it on a bloch sphere, and therefore an infinite amount of types of errors can have occured in the presence of noise such as thermal or electromagnetical noise.

Fortunately, this noise can be modeled as successive pauli gates. Since an identity noise occuring is irrelevant to us, and XY as well as ZY (anti-) commute, we need only correct for X and Z errors occuring.

1.3.1 Repetition Code

In order to correct errors, they must first be detected. From classical computer science there are well known existing codes, such as the repetition code. For this error code information is encoded by repeating the intended message some amount of times, and then decoding it by performing a majority vote on the transmitted message.

A quantum equivalent of the 3-bit repetition code performed on the message $|1\rangle$ is depicted in figure 2, including so-called "Syndrome Extraction". A Syndrome is a message that indicates the location of error occurences in a multi-physical-qubit system. It is crucial that the measurement-based extraction of such Syndromes occurs without harming the actual quantum information stored in the so-called "data-qubits". Therefore two additional "Ancilla-qubits" (both $|0\rangle$) are attached to the circuit via CNOTs.

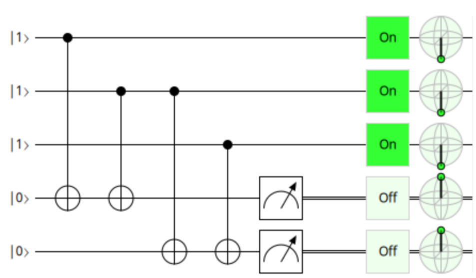

Figure 2: Bitflip Syndrome extractor
+1 measurement result on first Ancilla indicates a bitflip error on qubits 1 or 2, +1 result on second ancilla indicates bitflip on third or fourth qubit

This way of encoding information however leaves two notable issues.

For one, it only detects bitflip, or pauli-X errors occuring on the stored quantum information. While using Hadamard gate one could trivially adapt this code to instead detect pauli-Z errors, it is not possible to use linear codes like the repetition code to *simultaneously* detect pauli-X and pauli-Z errors occuring.

Secondly, it also assumes a noise model of a “Noisy Channel”, which is not compatible with the actually encountered errors in real physical quantum computers.

1.3.2 2D Codes

Again, the previous research in computer science is of immense value to us here, providing a toolset for generating valid codes from existing encoding schemes. According to SUCHANDSUCH a hypergraph product code of two existing codes will always remain a valid detection code. We can therefore form hypergraph product code of two repetition codes for X error detection and Z error detection respectively, obtaining the so-called “Surface-Code” which can detect *both* X and Z errors, and therefore any pauli error happening.

PUT IN A NICE DRAWING OF THE SURFACE CODE.

2 Conclusion

3 Appendix

3.1 Schroedinger picture calculation of CNOT circuit

In the quantum circuit depicted in figure 1 the input state can be written as $|\psi_{control}\rangle \otimes |0\rangle \otimes |\psi_{target}\rangle$ and the measurement in the first timestep can be expressed as $\mathbb{I} \otimes X \otimes X$.

The initial state $|\phi_{t=0}\rangle = |\psi_{control}\rangle \otimes |\psi_{ancilla}\rangle \otimes |\psi_{target}\rangle$
where
$|\psi_{control}\rangle = \alpha|0\rangle + \beta|1\rangle$
$|\psi_{ancilla}\rangle = |0\rangle$
$|\psi_{target}\rangle = \gamma|0\rangle + \delta|1\rangle$
therefore:

$$|\phi_{t=0}\rangle = \alpha\left(\gamma|000\rangle + \delta|001\rangle\right) + \beta\left(\gamma|100\rangle + \delta|101\rangle\right) \tag{10}$$

If the first measurement result is +1, the state becomes:

$$\begin{aligned}|\phi^{+}_{t=1}\rangle &= \frac{1}{2}\left(\mathbb{I}\otimes\mathbb{I}\otimes\mathbb{I} + \mathbb{I}\otimes X\otimes X\right)|\phi_{t=0}\rangle \\ &= \alpha\left(\gamma\left(|000\rangle + |011\rangle\right) + \delta\left(|001\rangle + |010\rangle\right)\right) \\ &+ \beta\left(\gamma\left(|100\rangle + |111\rangle\right) + \delta\left(|101\rangle + |110\rangle\right)\right)\end{aligned}$$

if the result is -1, it becomes:

$$\begin{aligned}|\phi^{-}_{t=1}\rangle &= \frac{1}{2}\left(\mathbb{I}\otimes\mathbb{I}\otimes\mathbb{I} - \mathbb{I}\otimes X\otimes X\right)|\phi_{t=0}\rangle \\ &= \alpha\left(\gamma\left(|000\rangle - |011\rangle\right) + \delta\left(|001\rangle - |010\rangle\right)\right) \\ &+ \beta\left(\gamma\left(|100\rangle - |111\rangle\right) + \delta\left(|101\rangle - |110\rangle\right)\right)\end{aligned}$$

In the case of the +1 Measurement $\rightarrow$ a=0:

$$\begin{aligned}|\phi^{++}_{t=2}\rangle &= \frac{1}{2}\left(\mathbb{I}\otimes\mathbb{I}\otimes\mathbb{I} + Z\otimes Z\otimes\mathbb{I}\right)|\phi^{+}_{t=1}\rangle \\ &= \left(|000\rangle\langle000| + |001\rangle\langle001| + |110\rangle\langle110| + |111\rangle\langle111|\right)|\phi^{+}_{t=1}\rangle \\ &= \alpha\left(\gamma|000\rangle + \delta|001\rangle\right) + \beta\left(\gamma|111\rangle + \delta|110\rangle\right)\end{aligned}$$

$$\begin{aligned}|\phi^{+-}_{t=2}\rangle &= \frac{1}{2}\left(\mathbb{I}\otimes\mathbb{I}\otimes\mathbb{I} - Z\otimes Z\otimes\mathbb{I}\right)|\phi^{+}_{t=1}\rangle \\ &= \left(|010\rangle\langle010| + |011\rangle\langle011| + |100\rangle\langle100| + |101\rangle\langle101|\right)|\phi^{+}_{t=1}\rangle \\ &= \alpha\left(\gamma|011\rangle + \delta|010\rangle\right) + \beta\left(\gamma|100\rangle + \delta|101\rangle\right)\end{aligned}$$

In the case of the -1 Measurement $\rightarrow$ a=1:

$$\begin{aligned}|\phi^{-+}_{t=2}\rangle &= \frac{1}{2}\left(\mathbb{I}\otimes\mathbb{I}\otimes\mathbb{I} + Z\otimes Z\otimes\mathbb{I}\right)|\phi^{-}_{t=1}\rangle \\ &= \alpha\left(\gamma|000\rangle + \delta|001\rangle\right) - \beta\left(\gamma|111\rangle + \delta|110\rangle\right)\end{aligned}$$

$$\begin{aligned}|\phi^{--}_{t=2}\rangle &= \frac{1}{2}\left(\mathbb{I}\otimes\mathbb{I}\otimes\mathbb{I} - Z\otimes Z\otimes\mathbb{I}\right)|\phi^{-}_{t=1}\rangle \\ &= -\alpha\left(\gamma|011\rangle + \delta|010\rangle\right) + \beta\left(\gamma|100\rangle + \delta|101\rangle\right)\end{aligned}$$

Now the applied measurement is $\mathbb{I}\otimes X\otimes\mathbb{I}$, which means:

$$\begin{aligned}|\phi^{+++}_{t=3}\rangle &= \frac{1}{2}\left(\mathbb{I}\otimes\mathbb{I}\otimes\mathbb{I} + \mathbb{I}\otimes X\otimes\mathbb{I}\right)|\phi^{++}_{t=2}\rangle \\ &= \frac{1}{2}((|010\rangle + |000\rangle)\langle 000| + (|011\rangle + |001\rangle)\langle 001| \\ &+ (|000\rangle + |010\rangle)\langle 010| + (|001\rangle + |011\rangle)\langle 011| \\ &+ (|110\rangle + |100\rangle)\langle 100| + (|111\rangle + |101\rangle)\langle 101| \\ &+ (|100\rangle + |110\rangle)\langle 110| + (|101\rangle + |111\rangle)\langle 111|)|\phi^{++}_{t=2}\rangle \\ &= \frac{1}{2}(\alpha\left(\gamma(|000\rangle + |010\rangle) + \delta(|011\rangle + |001\rangle)\right) \\ &+ \beta\left(\gamma(|101\rangle + |111\rangle) + \delta(|100\rangle + |110\rangle)\right))\end{aligned}$$

In this case, a,b and c would each be zero, therefore no further gate would be applied.
As intended, this state is equivalent to $CNOT_{|\psi_{Control}\rangle\rightarrow|\psi_{Target}\rangle}|\phi_{t=0}\rangle$.
If the last measurement result is -1:

$$\begin{aligned}|\phi^{++-}_{t=3}\rangle &= \frac{1}{2}\left(\mathbb{I}\otimes\mathbb{I}\otimes\mathbb{I} - \mathbb{I}\otimes X\otimes\mathbb{I}\right)|\phi^{++}_{t=2}\rangle \\ &= \frac{1}{2}((|010\rangle + |000\rangle)\langle 000| + (|001\rangle - |011\rangle)\langle 001| \\ &+ (|010\rangle - |000\rangle)\langle 010| + (|011\rangle - |001\rangle)\langle 011| \\ &+ (|100\rangle - |110\rangle)\langle 100| + (|101\rangle - |111\rangle)\langle 101| \\ &+ (|110\rangle - |100\rangle)\langle 110| + (|111\rangle - |101\rangle)\langle 111|)|\phi^{++}_{t=2}\rangle \\ &= \frac{1}{2}(\alpha\,(TODOTODOTODOTODOTODO\gamma(|000\rangle + |010\rangle) + \delta(|011\rangle + |001\rangle)) \\ &+ \beta\left(\gamma(|101\rangle + |111\rangle) + \delta(|100\rangle + |110\rangle)\right))\end{aligned}$$

Notably, each measurement sequence has a differing resulting ancilla state, however we do not care since ancillas are meant to be discarded.
For now, the other 7 final computation steps are left as an exercise to the reader, however I probably will still finish that.