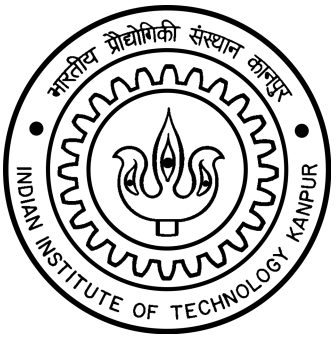


# Quantum Error Correction

Quantum Computing
Semester II, 2015-16
End-term report

*Authors:*
Vishwas Bhargava
Kirtan Padh

*Supervisor:*
Prof. Rajat Mittal

## *Abstract*

Quantum states are usually quite fragile and highly prone to errors. So if we hope to have a practical implementation of a quantum computer, we must have some way of being able to detect and correct such errors. It is the theory of quantum error correcting codes which allows us to do this. We present a very short overview of quantum error correction and stabilizer codes. We also state the laflamme-knill condition and give an intuition of its proof. As an application of quantum error correction, we also present the modified Lo-Chau protocol for quantum key distribution and give an idea of why it is secure.

# Contents

# 1 Introduction

When we describe quantum algorithms, we usually assume that sending the qubits over a channel or storing qubits does not introduce errors. But due to the fragility of quantum states, it is not clear why this is a valid assumption. It is the theory of quantum error correcting codes which allows us to make this assumption. In this chapter we will see some examples of quantum error correcting codes and the Laflamme-Knill condition, which is a necessary and sufficient condition for a code to be a quantum error correcting code.

## 1.1 Error correction

As a motivation for introducing a quantum error correcting code, let us first take a look at a simple classical error correcting code for a single bit. The idea is that if we wish to protect a message $m$ against noise in the channel, then instead of sending $m$ we should send an 'encoded' message $m'$ which has added redundancy. A simple classical is that if we want to send one bit of message, then we can send 000 instead of 0 and 111 instead of 1. So even if one bit flips while sending the message over a noisy classical channel, we can recover the original bit by majority. But it is not so straightforward to do this for quantum computing because of the following hurdles:

- *The no cloning theorem*- We cannot add redundancy by making copies of the qubit.
- *Measurement destroys the state*- Making an observation of what state we have destroys the state. So we cannot look at the state before deciding what to do with it as we did in classical error correction.
- *Errors are continuous*- We had only one kind of error in classical error correction. We now have an infinite number of possible errors.

We look at the example of Shor's 9 qubit code to see how we overcome each of these hurdles.

### 1.1.1 The Shor code

The Shor code corrects an arbitrary error in at most one qubit. The encoding in Shor's code is as follows:

$$|0\rangle \longrightarrow \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$$

$$|1\rangle \longrightarrow \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)$$

We denote the state which $|0\rangle$ maps to as $|0_L\rangle$ and the state which $|1\rangle$ maps to as $|1_L\rangle$. Even before we see how we correct errors using this code, we can see that though the no cloning theorem stops us from copying the qubits, it does not stop us from adding redundancy. We map the basis of the space in which our original qubit lies to a redundant basis in the code space so that the encoding is:

$$\alpha\,|0\rangle + \beta\,|1\rangle \longrightarrow \alpha\,|0_L\rangle + \beta\,|1_L\rangle$$

This gives us the required redundancy in the code space which would allow us to correct the error. We call the space spanned by $|0_L\rangle$ and $|1_L\rangle$ the codespace and its elements codewords. Let us first look at how we correct a single bit flip or phase flip in the encoded qubit.

Denote by $X_i$ and $Z_i$ the pauli matrix $X$ acting on the $i^{th}$ qubit and the pauli matrix $Z$ acting on the $i^{th}$ qubit respectively. But since these are operators on 9 qubits, $Z_1$ for example stands for $Z_1 \otimes I^{\otimes 8}$. So the operator for all positions not mentioned is assumed to be $I$. For example $X_2X_3$ stands for $I \otimes X_1 \otimes X_2 \otimes I^{\otimes 6}$.

Suppose a bit flip occurs on the second qubit in the codeword. Clearly, the error is just $X_2$. The state(obtained after bit flip on the second qubit) will be an eigenvector of $Z_1Z_2$ with eigenvalue $-1$. We can get this eigenvalue by phase estimation, since we know both the operator and eigenvector. This tells us that the error is in the first or second qubit. Similarly, the eigenvalue of $Z_2Z_3$ for the state tells us that the error is in the second or third qubit. We conclude that the error is on the second qubit. We can correct a bit flip on any of the positions in this way. Correcting the error is just a matter of applying $X$ on the qubit on which the error occurred. We took advantage of the fact that though we cannot measure the state, we can measure measure whether two qubits in a state are different. We used this to get around the problem of not being able to measure the codeword.

Similarly for a phase flip, we can figure out in which block the sign change occurred by measuring eigenvalues of $X_1X_2X_3X_4X_5X_6$ and $X_4X_5X_6X_7X_8X_9$ on the state. Suppose the phase flip is in the first block, then $X_1X_2X_3X_4X_5X_6$ will have eigenvalue $-1$ and $X_4X_5X_6X_7X_8X_9$ will have eigenvalue 1, so we know that the phase flip is in the first block. Applying $Z_1Z_2Z_3$ will correct the phase in the first block.

So we have shown that we can correct both phase flip and bit flip errors. Clearly, bit flip and phase flip errors are just the action of $X$ and $Z$ respectively. It is easy to see that the correction of phase flips and bit flips is independent of each other, so we can also correct a combination of both of them, meaning that we can also correct errors of the form $Y_i$, which is the pauli matrix $Y$ acting on the $i^{th}$ qubit. This is because $Y = iXZ$.

Now we will show that the Shor code corrects not just against these distinct set of errors, but any arbitrary error on a single qubit. The most general one qubit error could be some $2 \times 2$ matrix $U$. Since $\{X, Y, Z, I\}$ form a basis for $2 \times 2$ matrices, we can write

$$U = aX + bY + cZ + dI$$

So $U$ acting on $|\psi\rangle$ can be written as

$$U|\psi\rangle = aX|\psi\rangle + bY|\psi\rangle + cZ|\psi\rangle + dI|\psi\rangle$$

Suppose we perform the measuring of error syndrome as described, comparing bits within a block of three, and comparing the signs of blocks of three. This acts as a measurement of which error occurred, causing the state $U|\psi\rangle$ to collapse to $X|\psi\rangle$ with probability $|a|^2$, to $Y|\psi\rangle$ with probability $|b|^2$, to $Y|\psi\rangle$ with probability $|c|^2$ and to $|\psi\rangle$ with probability $|d|^2$. In any of the four cases, we can correct the error as we have shown previously.

So we have shown through the example of the Shor code how we can overcome the apparent difficulties in designing quantum error correcting codes. We now formally define a quantum error correcting code and give a necessary and sufficient condition for a code to be an error correcting code, which is the Laflamme-Knill condition[1].

## 1.2 Laflamme-Knill condition

Quantum states which we want to protect against errors are *encoded* in a *quantum error-correcting code* $C$. If $k$ qubits are being protected by encoding them in $n$ qubits, $C$ will be a subspace of the $2^n$ dimensional hilbert space.

The noise is assumed to be described by a quantum operation $\mathcal{E}$, and the error-correction is effected by a trace-preserving quantum operation $\mathcal{R}$ called the error-correcting operator. In order for error-correction to be considered successful, we require that for any state with density matrix $\rho$ with support in $C$, we must have

$$\mathcal{R}(\mathcal{E}(\rho)) \propto \rho$$

We have proportionality instead of equality because $\mathcal{E}$ might not be trace preserving. We let $\{E_i\}$ to be the operation elements of $\mathcal{E}$ and $\{R_j\}$ to be the operation elements of $\mathcal{R}$. Let $P$ be the projector onto $C$.

**Theorem 1.1** (laflamme-Knill Condition)**.** *$\exists\ \mathcal{R}$ such that $\mathcal{R}(\mathcal{E}(\rho)) \propto \rho$ iff $PE_a^\dagger E_b P = C_{ab}P$ where $C$ is a hermitian matrix.*

We give an intuition of how this can be proved. If we want to distinguish between errors $E_a$ and $E_b$ acting on two different basis states $|\psi_i\rangle$ and $|\psi_j\rangle$ of $C$, then $E_a |\psi_i\rangle$ must be orthogonal to $E_b |\psi_j\rangle$, meaning that:

$$\langle\psi_i|E_a^\dagger E_b|\psi_j\rangle = 0$$

Also, when we make a measurement to find the error, we must learn nothing about the actual state of the code within the coding space. If we did learn something, we would be disturbing superpositions of the basis states, so while we might correct the basis states, we would not be correcting an arbitrary valid codeword. This implies that:

$$\langle\psi_i|E_a^\dagger E_b|\psi_i\rangle = C_{ab}$$

Combining the two conditions, we get:

$$\langle\psi_i|E_a^\dagger E_b|\psi_i\rangle = \delta_{ij} C_{ab}$$

The above arguments show why the above condition is necessary. Note that this condition is the same as $PE_i^\dagger E_j P = C_{ab} P$ where $P = \sum_i |\psi_i\rangle \langle\psi_i|$ as in the statement of the theorem.

To see why this is sufficient, suppose $C_{ab}$ was a diagonal matrix. This would mean that two different errors always act orthogonally and therefore we can always distinguish between them and therefore correct them. So clearly the condition is sufficient when $C_{ab}$ is diagonal. It turns out that we can always find an equivalent representation of errors for which $C_{ab}$ becomes diagonal. We use the fact that $C_{ab}$ is diagonalizable to come up with an equivalent representation of errors which diagonalizes $C_{ab}$. Since this reduction can always be done, the condition is also sufficient.

# 2 Stabilizer Codes

A code which encodes $k$ qubits in $n$ qubits will have $2^k$ basis codewords corresponding to the basis of the original states. Any linear combination of these basis codewords is also a valid codeword, corresponding to the same linear combination of the unencoded basis states. The space $T$ of valid codewords (the coding space ) is therefore a Hilbert space, a subspace of the full $2^n$ dimensional Hilbert space.

As with Shors nine-qubit code, if we can correct errors $E$ and $F$ , we can correct $aE + bF$ , so we only need to consider whether the code can correct a basis of errors. One convenient basis to use is the set of tensor products of Pauli matrices $Z$ and $X$.The set of all these tensor products with a possible overall factor of $\pm 1, \pm i$ forms a group $G_n$(Pauli Group on $n$ qubits ) under multiplication.

Let $S$ be a subgroup of $G_n$ such that $S$ stabilizes all the elements of the codespace $T$.

**Lemma 2.1.** *In order to have a non-trivial codespace, $-I \notin S$ and $S$ should be Abelian.*

*Proof.* If $-I \in S$ then $-I \cdot |\psi\rangle = |\psi\rangle = -|\psi\rangle \implies |\psi\rangle = 0$.
Also if $M, N \in S$ and $MN = -NM \implies MN|\psi\rangle = -NM|\psi\rangle \implies |\psi\rangle = 0$ □

**What is the dimension of the stabilizer subspace?** Well take the first stabilizer generator. This stabilizer generator squares to identity, so has $\pm 1$ eigenvalues. Further, this stabilizer generator has trace zero. Thus $g_1$ must have $2^{n-1}$ eigenvalues $+1$ and $2^{n-1}$ eigenvalues $-1$. So $g_1|\psi\rangle = |\psi\rangle$ splits the Hilbert space of our $n$ qubits in half.
Define

$$P_1 = \frac{1}{2}(I + g_1)$$

Note that $P_1$ is projector onto $+1$ eigenspace of $g_1$. Again we have $Tr(P_1 \cdot g_2) = 0$. Thus we see that for the $2^{n-1}$ dimensional subspace that satisfies $g_1|\psi\rangle = |\psi\rangle$, a subspace of dimension $2^{n-2}$ satisfies $g_1|\psi\rangle = |\psi\rangle$. Continuing inductively, we get the dimension of the space fixed by the stabilizer to be $2^{n-r}$.

**Theorem 2.2.** *[2] Let $E \in G_n$ be an error acting on an element of the codespace. We can detect $E$ iff $E \in \{G_n \setminus N(S)\} \cup \{S\}$ where $N(S)$ is the normalizer of $S$.*

*Proof.* As $E \in G_n$ therefore either error commutes with all the elements in S which means $E \in N(S)$(As here $C(S) = N(S)$ ) or $E$ anti-commutes with atleast one element in $S$(Say

M).Now we will show that this error $E$ will satisfy Laflamme-Knill condition and thus we can detect it. Correction is straightforward once an error has been detected.
Note:

$$\langle\psi_i|E|\psi_j\rangle = \langle(M\psi_i)|E|\psi_j\rangle \implies \langle(\psi_i)|ME|\psi_j\rangle = -\langle(\psi_i)|EM|\psi_j\rangle \implies -\langle(\psi_i)|E|\psi_j\rangle = 0$$

thus Laflamme Knill condition is satisfied.What if $E \in S$? Then it is even more easy as

$$\langle\psi_i|E|\psi_j\rangle = \delta_{ij}$$

. But when $E \in N(S) \setminus S$ then $S$ stabilizes $E|\psi\rangle$ and thus $E$ maps codewords to codewords and thus we can't correct such errors. □

## 2.1 Logical operators for stabilizer codes

Note that $S \trianglelefteq N(S)$
So we claim that

$$N(S)/S \cong G_k$$

One implication of this result is that using this we can relate elements of $N(S)/S$ as logical operators $X$ and $Z$ on our logical $k$ qubits.One can easily see that $N(S) \subset G_k S$ as $N(S)$ takes element from codespace to elements in codespace. Also $|N(S)/S| = 2^{2k} = |G_k|$. Therefore both of them are isomorphic.

## 2.2 Examples

We will now look at some examples of codes defined stabilizers and appreciate the compact representation provided by Stabilizer formalism.

### 2.2.1 The 9 qubit Shor code

The stabilizer for the Shor code has 9-1=8 generators.
Notation: $X_i$ operator is defined as X acting on ith qubit
If we consider any single qubit error like $X_1, Y_3$ then $X_1 \cdot Y_3$ with $Z_1 Z_2$ and thus not in N(S).It can be seen that all other products of two errors from this error set are either in $S$ or else anti-commute with at least one element of $S$ and thus are not in $N(S)$, implying that the Shor code can be used to correct an arbitrary single qubit error.

| Element | Operator |
|---|---|
| $g_1$ | ZZIIIIIII |
| $g_2$ | IZZIIIIII |
| $g_3$ | IIIZZIIII |
| $g_4$ | IIIIZZIII |
| $g_5$ | IIIIIZZI |
| $g_6$ | IIIIIIZZ |
| $g_7$ | XXXXXXIII |
| $g_8$ | XXXIIIXXX |
| $\bar{X}$ | ZZZZZZZZZ |
| $\bar{Z}$ | XXXXXXXXX |

TABLE 2.1: Stabilizer Representation of 9-qubit Shor code

One can easily verify that $\bar{X}$ $\bar{Z}$ acts as logical $X$ and $Z$ on our logical qubits.
We will call an error correcting code **degenerate** if linearly independent correctable error don't produce to linearly independent states. One can note that errors $Z_1$ and $Z_2$ act on codespace identically this implies Shor code is degenerate.

### 2.2.2 5-qubit code

5 is the minimum size for a quantum code which encodes a single qubit so that any error on a single qubit in the encoded state can be detected and corrected[1].

| Element | Operator |
|---|---|
| $g_1$ | XZZXI |
| $g_2$ | IXZZX |
| $g_3$ | XIXZZ |
| $g_4$ | ZXIXZ |
| $\bar{X}$ | XXXXX |
| $\bar{Z}$ | ZZZZZ |

TABLE 2.2: Stabilizera Representation of 5-qubit code

[1]We are just stating as a fact. One can refer it in Section 12.4.3 of [3]

Here we have

$$|0_L\rangle = \sum_{M\in S} |00000\rangle = \frac{1}{4}[|00000\rangle + |10010\rangle + |01001\rangle + |10100\rangle + |01010\rangle - |11011\rangle - |00110\rangle$$
$$- |11000\rangle - |11101\rangle - |00011\rangle - |11110\rangle - |01111\rangle - |10001\rangle - |01100\rangle - |10111\rangle + |00101\rangle]$$

and

$$|1_L\rangle = \bar{X}\,|0_L\rangle = \frac{1}{4}[|11111\rangle + |01101\rangle + |10110\rangle + |01011\rangle + |01010\rangle - |00100\rangle$$
$$- |11001\rangle - |00111\rangle - |00010\rangle - |11100\rangle - |00001\rangle - |10000\rangle - |01110\rangle - |10011\rangle - |01000\rangle + |11010\rangle]$$

Again one can verify following two conditions:
• All products of two errors either lies in $S$ or doesn't lies in $N(S)$.
• $\bar{X}$ ,$\bar{Z}$ acts as logical $X$ and $Z$ on our logical qubits.

### 2.2.3 CSS codes

Calderbank-Shor-Steane code is an important example of stabilizer codes. To describe CSS codes, we must describe linear codes first. We denot be $[n, k]$ a code which encodes $k$ bits in $n$ bits or $k$ qubits in $n$ qubits depending on whether it is a classical code or a quantum code.

#### 2.2.3.1 Linear codes

A linear code is a classical code $C$ encoding $k$ bits of information into an $n$ bit code space and is specified a generator matrix $G \in \mathbb{Z}_2^{n\times k}$. The encoding of a message $m$ is $Gm$. A classical code for which we can have such a generator matrix is called a linear code. We can also simply say that $C \subseteq \mathbb{F}_2^n$ is a linear code if $C$ is a subspace of $\mathbb{F}_2^n$.

An Alternative but equivalent formulation of linear codes is in terms of parity check matrices. In this definition the code is defined to consist of all $n \in Z_2^n$ such that

$$Hx = 0$$

where $H \in \mathbb{Z}_2^{n-k\times n}$ . More precisely the code is defined to be the kernel of $H$. It is easy to see that both these definition are equivalent.

The parity check matrix gives us a natural way to look at error correction for linear codes. Suppose that we encode the message $x$ as $y = Gx$, but an error $e$ due to noise corrupts $y$ giving the corrupted codeword $y' = y + e$. Because $Hy = 0$ for all codewords, it follows that $Hy' = He$. $Hy'$ is called the error syndrome. Clearly, $Hy'$ is equal to 0 in the no error case,

otherwise it is $He$, which is our error syndrome. We look at a simple example to see how we can correct errors. If the error is in just a single position, say $j$, then $Hy'$ is equal to $He_j$, where $e_j$ is the unit vector with 1 in the $j^{th}$ component. If we assume that errors occur on at most one bit, it is therefore possible to perform error-correction by computing the error syndrome $Hy$ and comparing it to the different possible values of $He_j$ to determine which bit needs to be corrected. More involved strategies have to be designed when the error does not have such a simple form.[4]

Suppose $C \subseteq \mathbb{F}^n$ is a linear code encoding $k$ bits, with generator matrix $G$ and parity check matrix $H$. Then we can define another code, the dual of $C$, denoted $C^{\perp}$, to be the code with generator matrix $H^T$ and parity check matrix $G^T$. We now have all definitions necessary to look at $CSS$ codes.

#### 2.2.3.2 CSS codes: Description without stabilizers

Suppose $C_1$ and $C_2$ are $[n, k_1]$ and $[n, k_2]$ classical linear codes such that $C_2 \subset C_1$ and $C_1$ , $C_2^{\perp}$ both correct $t$ errors. We will define an $[n, k_1 - k_2]$ quantum code CSS $(C_1, C_2)$ capable of correcting errors on $t$ qubits, the CSS code of $C_1$ over $C_2$, as follows. Suppose $x \in C_1$ is any codeword in the code $C_1$ . Then we define the quantum state $|x + C_2\rangle$ by

$$|x + C_2\rangle \equiv \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x + y\rangle$$

Observe that

$$|x + C_2\rangle = |x' + C_2\rangle \text{ if } x - x' \in C_2$$

. Thus the state depends on the coset $C_1/C_2$. The number of such cosets $= |C_1|/|C_2| = 2^(k_1 - k_2)$. Therefore $CSS(C_1, C_2)$ is an $[n, k_1 - k_2]$ quantum code. We exploit the classical error-correcting properties of $C_1$ and $C_2^{\perp}$ to detect and correct quantum errors. It is possible to error-correct up to $t$ bit and phase flip errors on $CSS(C_1, C_2)$. The error acts as follows:

$$|x + C_2\rangle \quad \xrightarrow{QuantumErrors} \quad \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(x+y)\cdot e_2} |x + y + e_1\rangle$$

To detect where bit flips occurred, we introduce an all zeros ancilla with sufficient qubits to store the syndrome for the code $C_1$. We can apply the parity matrix $H_1$ for $C_1$(by just using Controlled NOTS). This gives us:

$$|x + y + e1\rangle |0\rangle \, to \, |x + y + e_1\rangle |H_1(x + y + e_1)\rangle = |x + y + e\rangle |H_1 e_1\rangle$$

Knowing the error syndrome $H_1 e_1$ we can infer the error $e_1$ since $C_1$ can correct up to $t$ errors, which completes the error-detection of bit flips and gives us:

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(x+y)\cdot e_2} |x+y\rangle$$

To detect phase flip errors, we apply hadamard on each of the qubits. This gives us:

$$\frac{1}{\sqrt{|C_2|2^n}} \sum_{z} \sum_{y \in C_2} (-1)^{(x+y)\cdot(e_2+z)} |z\rangle$$

Substituting $z' = z + e_2$

$$\frac{1}{\sqrt{|C_2|2^n}} \sum_{z'} \sum_{y \in C_2} (-1)^{(x+y)\cdot(z')} |z' + e_2\rangle$$

So applying hadamard reduced the phase flip errors to bit flip errors which can now be corrected as before.

This gives us a description of CSS codes. Now we see how stabilizers simplify this description and also give us more insight on why this code works.

#### 2.2.3.3 CSS codes: Description by Stabilizers

Suppose we have classical linear codes with parity check matrices $P_1$ and $P_2$. We make a quantum error correcting code to correct just bit flip errors using $P_1$.

We define each row of $P_1$ to be a stabilizer genertor, where we replace the ones by $X$ and the zeros by $I$. The error syndrome for a product of bit flip errors is then equal to the classical error syndrome for the same set of classical bit flip errors. Now we also add in stabilizer generators corresponding to rows of $P_2$, where we replace the ones by $Z$ and the zeros by $I$ for each row in $P_2$. These will identify phase flip errors.

Since the stabilizer must be abelian, we can combine the generators obtained from $P_1$ and $P_2$ in this way if and only if the rows of $P_1$ and $P_2$ are orthogonal by the binary dot product. This is because $X$ and $X$ anti-commute. This means that the dual code of each code must be a subset of the other code. A code formed this way will correct as many bit flip errors as the code for $P_1$ can correct, and as many phase flip errors as the code for $P_2$ can correct. A $Y$ error counts as one of each.

# 3 Modified Lo-Chau protocol

In proving the security of *BB84* protocol over noisy channel the *central idea* is to first prove security of modified Lo-Chau protocol and then systematically simplify this protocol in a series of steps such that each of which provably does not compromise the security of the protocol.

A QKD protocol is called secure if for parameters $s, l > 0$ chosen by Alice and Bob, either the scheme aborts, or it succeeds with probability at least $1 - 2^{-s}$ guarantees Eve's mutual information with the final key is less than $2^{-l}$. Also, the key string that Alice and Bob agree on must be random.

**Theorem 3.1.** *If* $F(\rho, |\beta_{00}\rangle)^2 > 1 - 2^{-s}$*, then* $S(\rho) < (2n + s + 1/ln2)2^{-s} + O(2^{-2s})$.

*Proof.* If $F(\rho, |\beta_{00}\rangle)^2 > 1 - 2^{-s}$, then the largest eigenvalue of $\rho$ must be larger than $1 - 2^{-s}$. Therefore, the maximum possible entropy would be attained when the largest eigenvalue is $1 - 2^{-s}$ , and the remaining eigenvalues are equal. So

$$S(\rho)_{max} = -(1 - 2^{-s}) \log(1 - 2^{-s}) - 2^{-s} \log \frac{2^{-s}}{2^{2n} - 1}$$

. □

By Holevos bound[3], $S(\rho)$ is an upper bound on the information accessible to Eve, resulting from Alice and Bobs measurements of $\rho$. This implies that if a QKD protocol can provide Alice and Bob with EPR pairs of fidelity at least $1 - 2^{-s}$ (with high probability), then it is secure.
But now the question arises that *how we will lower bound the fidelity*? for this we will use following two steps:
• We will randomly select $n$ of the $2n$ EPR pairs to check the bound on errors to be less than some constant(say $t$).
This will imply by Chernoff bound that with very high probability that remaining $n$ qubits will have around $t$ errors. Note that we can do classical probability estimates because the measurements which measure which error (phase or bit flip) occurred commute with the bell basis.
• We will measure the remaining $n$ qubits according to the check matrix for a pre-determined $[n, m]$ quantum code correcting up to $t$ errors. Thus we can compute the syndromes for the

errors, and then correct their state, obtaining m nearly perfect EPR pairs whose fidelity is $1 - 2^{-t}$ which can be thought as probability of more than $t$ errors occurring.

**Modified Lo-Chau protocol**

1. Alice creates $2n$ EPR pairs in the state $|\beta_{00}\rangle^{\otimes 2n}$ .
2. Alice randomly selects $n$ of the $2n$ EPR pairs to serve as checks to check for Eves interference.
3. Alice selects a random $2n$-bit string $b$, and performs a Hadamard transform on the second qubit of each pair for which $b$ is 1.
4. Alice sends the second qubit of each pair to Bob.
5. Bob receives the qubits and publicly announces this fact.
6. Alice announces $b$ and which $n$ qubits are to provide check bits.
7. Bob performs Hadamard on the qubits where $b$ is 1.
8. Alice and Bob each measure their $n$ check qubits in the $|0\rangle$, $|1\rangle$ basis, and publicly share the results. If more than $t$ of these disagree, they abort the protocol.
9. Alice and Bob measure their remaining $n$ qubits according to the check matrix for a pre-determined $[n, m]$ quantum code correcting up to $t$ errors. They share the results, compute the syndromes for the errors, and then correct their state, obtaining $m$ nearly perfect EPR pairs.
10. Alice and Bob measure the m EPR pairs in the $|0\rangle$, $|1\rangle$ basis to obtain a shared secret key.

Further reduction to BB84 is based on an equivalent form of CSS codes called paramatrized CSS codes($CSS_{u,v}(C_1, C_2)$) defined by

$$|x + C_2\rangle \equiv \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{u \cdot y} |x + y + v\rangle$$

The final protocol is obtained by systematically reducing this protocol so that we eliminate the use of entangled pairs as well as quantum error correction without compromising on security [5].

# Bibliography

[1] Emanuel Knill and Raymond Laflamme. Theory of quantum error-correcting codes. *Physical Review A*, 55(2):900, 1997.

[2] Daniel Gottesman. *Stabilizer Codes and Quantum Error Correction.* PhD thesis, California Institute of Technology, 1997.

[3] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition.* Cambridge University Press, New York, NY, USA, 10th edition, 2011. ISBN 1107002176, 9781107002173.

[4] William E. Ryan and Shu Lin. *Channel codes. Classical and modern.* Cambridge: Cambridge University Press, 2009. doi: 10.1017/CBO9780511803253.

[5] Peter W. Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85:441–444, Jul 2000. doi: 10.1103/PhysRevLett.85.441. URL http://link.aps.org/doi/10.1103/PhysRevLett.85.441.