Implementation of quantum Reed–Solomon error detection code on IBM quantum computer and improvement by quantum singular value decomposition

Preprint · June 2019

DOI: 10.13140/RG.2.2.10871.47521

CITATIONS
2

READS
296

4 authors:

Nimish Mishra
Indian Institute of Information Technology, Kalyani
30 PUBLICATIONS **21** CITATIONS
SEE PROFILE

S . Ashutosh
Indian Institute of Science Education and Research Kolkata
2 PUBLICATIONS **2** CITATIONS
SEE PROFILE

Bikash K. Behera
Bikash's Quantum (OPC) Pvt. Ltd.
174 PUBLICATIONS **1,063** CITATIONS
SEE PROFILE

Prasanta K. Panigrahi
Indian Institute of Science Education and Research Kolkata
631 PUBLICATIONS **5,886** CITATIONS
SEE PROFILE

Implementation of quantum Reed-Solomon error detection code on IBM quantum computer and improvement by quantum singular value decomposition

Nimish Mishra

E-mail: nimish_bt18@iiitkalyani.ac.in
First author, Department of Computer Science and Engineering, Indian Institute of Information Technology, Kalyani 741235, West Bengal, India

S. Ashutosh

E-mail: sa17ms105@iiserkol.ac.in
First author, hiIndian Institute of Science Education and Research Kolkata, Mohanpur 741246, West Bengal, India

Bikash K. Behera

E-mail: bkb18rs025@iiserkol.ac.in
Department of Physical Sciences, Indian Institute of Science Education and Research Kolkata, Mohanpur 741246, West Bengal, India

Prasanta K. Panigrahi

E-mail: pprasanta@iiserkol.ac.in
Department of Physical Sciences, Indian Institute of Science Education and Research Kolkata, Mohanpur 741246, West Bengal, India

Abstract. Error detection and correction has been a fundamental branch of quantum information, attempting to minimize decay of information through decoherence. Several error correcting codes have been developed over the years, out of which Reed-Solomon code is one of the most useful ones. We test the reliability of the quantum equivalent of the classical Reed-Solomon code and present the circuit implementation of quantum Reed-Solomon code for encoding-decoding using two approaches; using auxiliary CNOTs as previously established and without auxiliary CNOTs as our improvement to the existing algorithm. We compare the results obtained from these approaches and comment on the general reliability of the quantum Reed-Solomon error correction algorithm for error correction. For the same, we encode a three-qubit GHZ cluster state in IBM 16-qubit quantum computer, manually introduce errors, and analyze cumulative probabilities of error detection. We also discuss possible improvements to the existing quantum Reed-Solomon error detection algorithm using quantum singular value decomposition, interpolation, partial greatest common divisor, and polynomial long division.

Keywords: IBM Quantum Experience, Quantum Reed-Solomon Code, Quantum Singular Value Decomposition

1. Introduction

A quantum error correcting code is a method of transmitting K bits of quantum information using $n(> K)$ qubits, such that if an arbitrary subset of n qubits undergoes arbitrary errors, the transmitted quantum information can be recovered explicitly. Unlike classical computers, which can have only bit-flip errors, quantum computers can have bit-flip, phase-flip and arbitrary phase change errors. Shor first discovered a method for formulating a quantum error correcting code by storing the information of one qubit onto a highly entangled state of nine qubits [1]. Steane achieved the same with seven qubits [2, 3]. Laflamme *et al.* [4] found a class of five-qubit codes which does the same, while having the property of fault-tolerance. A generalization of this concept are the CSS codes, named after their inventors: Calderbank, Shor and Steane. These codes provide a generalized method to obtain quantum analogues of classical codes.

Error detection and correction remains a challenging problem for arbitrary entangled states with large number of qubits. Entangled states have a wide range of applications in quantum information processing tasks. Highly entangled states like Bell states, GHZ states, cluster states and Brown *et al.* states have been widely used for quantum teleportation [5, 6, 7], quantum secret sharing [8, 9, 10] and information splitting [11, 12], making the subject of their error correction of prime importance. Error correction codes for these highly entangled states have been developed for n qudits by Debjit *et al.* [13]. Recently an error detection code for $(2n + 1)$ entangled qubits has been developed by Singh *et al.* [14].

In 1999 Grassl, Geiselmann and Beth published a paper in which they described the encoding procedure of the quantum Reed-Solomon code [15]. Since then it has found applications in various field of quantum information [16, 17]. In this work, we start with the classical Reed-Solomon code in Section 2. In Section 3, we give the theory of quantum error correcting codes. Then in Section 4, we use existing theorems and combine with a linear algebra derivation to derive the quantum Reed-Solomon code. In Section 5, we present the circuit required to correct the bit-flip and the phase-flip errors, and describe the working procedure of the code. In Section 7, we mention the results after simulating the code in the IBM quantum computer. Then finally in Section 8, we discuss the future directions and possible improvements in the existing quantum Reed-Solomon encoding-decoding algorithm.

2. Classical Reed-Solomon Codes

Classical Reed-Solomon codes [18] are polynomial codes over finite fields which have found profound applications in transmitting a message. Spacecrafts like Voyager (1989), Galileo (1991), Mars Global Surveyor (1997) used this code. The reasons behind their

widespread use are that they can efficiently correct both random and burst errors, and there exist efficient decoding algorithms (in $O(n^2)$ and efficient in practice).

A general code denoted by $C = [N, K]$encodes K bits using N bits, with $N > K$. *Encoding* involves mapping a vector in a vector space of dimension K to a vector in a vector space in dimension N, where both vector spaces are defined over finite fields (Galois field). A Galois field exists if and only if it has a prime characteristic p and the number of elements being $q = p^l$, where l is some integer.

A Reed-Solomon code, $C = [N, K]$ is defined over a Galois field F_q with q elements such that $1 \leq K < N \leq q$. To encode K bits of information $(a_0, a_1, ..., a_k)$, Reed and Solomon generated the following polynomial.

$$P(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + ... + a_{k-1} x^{k-1} \tag{1}$$

N elements are selected from F_q and are denoted by $(\alpha_1, \alpha_2, \alpha_3, ..., \alpha_n)$. Some authors [19] refer to the elements selected as general elements, as opposed to [18] approach who took the first element as 0 and the last element as 1. We take the former approach as it has been established that it can offer improvements in classical decoding algorithms [19], the quantum equivalents of which we look to discuss. The encoding proceeds as:

$$c_1 = P(\alpha_1) = a_0 + a_1\alpha_1 + a_2\alpha_1^2 + ... + a_{k-1}\alpha_1^{k-1} \tag{2}$$

$$c_2 = P(\alpha_2) = a_0 + a_1\alpha_2 + a_2\alpha_2^2 + ... + a_{k-1}\alpha_2^{k-1} \tag{3}$$

. .

$$c_n = P(\alpha_n) = a_0 + a_1\alpha_n + a_2\alpha_n^2 + ... + a_{k-1}\alpha_n^{k-1} \tag{4}$$

The generator matrix for the above encoding is given by:

$$A = \begin{pmatrix} 1 & \alpha_1 & .. & .. & .. & \alpha_1^{k-1} \\ 1 & \alpha_2 & .. & .. & .. & \alpha_2^{k-1} \\ 1 & \alpha_3 & .. & .. & .. & \alpha_3^{k-1} \\ .. & .. & .. & .. & .. & .. \\ .. & .. & .. & .. & .. & .. \\ .. & .. & .. & .. & .. & .. \\ 1 & \alpha_n & ... & ... & ... & \alpha_n^{k-1} \end{pmatrix} \tag{5}$$

A is a **Vandermonde matrix** and it generates n equations by operating on the vector $[a_0, a_1, ..., a_{k-1}]$ to yield the encoding $C = [c_1, c_2, ..., c_n]$. It can be shown that a Reed-Solomon code is a linear code, by reducing the above matrix to a Vandermonde determinant form by choosing any k equations. The determinant is:

$$Determinant\, D = \prod_{1 \leq i < j \leq k} (\alpha_i - \alpha_j) \tag{6}$$

Since all α_i are distinct, $D \neq 0$ implying the k equations are linearly independent, which in turn implies k code-words $[c_1, c_2, ..., c_k]$ are linearly independent. It also follows that any k combination shall be linearly independent, concluding that the linear combination of these linear independent code-words shall constitute a new code-word, which is exactly the definition of a linear code. This linear Reed Solomon code has the minimum distance equal to $N - K + 1$, which is the best for any $[N, K]$ linear code [19].

3. Theory of quantum error correcting codes

The theory of quantum error correcting codes arises due to the leakage of information from the considered quantum system into the environment. Since it is practically impossible to completely isolate a quantum system, the environment (or specifically all the degrees of freedom having undesired interactions with the system) interacts with the system and modifies the state of the system, leading to the need of *correcting* the state back to the original state, and thus to the theory of quantum error correcting codes.

The no-cloning theorem [20] prevents the classical *redundant* approach to error correction, but Shor demonstrated the possibility of error correction by spreading the information over several qubits.

The theory is based on the assumption that quantum errors are local, affecting only a small number of qubits. The essence of quantum error correction is that a given state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ (where $|0\rangle$ and $|1\rangle$ constitute the computational basis) can be encoded in a higher dimensional Hilbert space using ancilla qubits (initially prepared in the state $|0\rangle$). The goal of error correction is to find an encoding such that an error maps it into a family of two dimensional sub-spaces preserving the *relative coherence of quantum information* (or the states of the system and the environment are not entangled, therefore making recovery of initially state possible) [21]. Measurement on this two-dimensional non-entangled state can lead to decisions on unitary transformations that can retrieve the original state. We refer to [21] for a detailed overview of environment's interaction with the system and the conditions necessary and/or sufficient for retrieval of the original state.

An error is considered as a unitary transformation on the state of the system. Quantum errors differ from classifications of classical errors due the continuum nature of the states; they are, however, broadly classified into bit–flip errors exchanging the states $|0\rangle$ and $|1\rangle$ corresponding to the Pauli matrix σ_x, phase–flip errors changing the relative phase of $|0\rangle$ and $|1\rangle$ by π corresponding to Pauli matrix σ_z, and their combination corresponding to the Pauli matrix σ_z. It is possible to express any error as an ordered series of these transformations along with the identity transformation.

4. Construction of Quantum Reed-Solomon Code

A quantum Reed-Solomon code is a weakly self dual linear binary code which can be obtained from codes over extension fields according to the CSS construction [22, 23]. The following theorem and definitions are important to construct the QRS code. We give the a definition and a theorem from [22] and then provide a detailed derivation of the properties of the quantum RS code, beginning with very general assumptions about the nature of the fields these codes are based on.

Definition 1 Let C be a weakly self-dual linear binary code i.e., $C \subseteq C^{\perp}$ and let w_j be a *representative* of a left coset in $C^{\perp}/C$ then the basis states of the resultant

quantum code, given by $C = [[N, N-2K]]$ are given by

$$|\psi\rangle = \frac{1}{\sqrt{|C|}} \sum_{c \in C} |c + w_j\rangle \tag{7}$$

where $C^{\perp}/C$ denotes the collection of left cosets of C in $C^{\perp}$ such that a left coset of the *subgroup* C in the *group* $C^{\perp}$ is given by: $w_j C = \{w_j c \,|\, w_j \in C^{\perp}, c \in C\}$ with representative $w_j \in C^{\perp}$.

Theorem 2 Let d be the minimum distance of the dual code $C^{\perp}$ in Definition 1. Then the corresponding quantum code is capable of detecting up to $d-1$ errors or, equivalently, is capable of correcting up to $(d-1)/2$ errors.

Obtaining Weakly self-dual Binary Code From Extension fields

It is possible to derive a quantum RS code from a classical RS code over extension fields, viz. U_{2^k} and U_2 where the subscript denotes the number of finite elements in the field. Since U_{2^k} is the *extension field* of U_2, the operations defined on U_2 are the operations in U_{2^k} restricted to U_2. We take a classical weakly self-dual linear RS code C over U_{2^k} of length $N = 2^k - 1$, dimension $K = N - D + 1$, and $D > \frac{N}{2} + 1$, where the symbols have their usual meanings.

We claim that the binary expansion of C with respect to a self-dual basis B of U_{2^k} over U_2 yields a weakly self-dual linear binary code $C' = [kN, kK, d \geq D]$ according to the discussion below.

Consider the following general transformation schematic in Fig. 1. The discussion stays the same for any arbitrary characteristic > 0, but we consider the characteristic to be 2 for our purpose here. ${}^nU_{2^k}$ and ${}^nV_{2^k}$ are the two vector spaces of dimension n over a finite field of characteristic 2 with 2^k elements such that ${}^nV_{2^k}$ is the dual space of ${}^nU_{2^k}$. T is therefore the dual transformation on a vector in ${}^nU_{2^k}$ to the corresponding vector in dual space ${}^nV_{2^k}$.

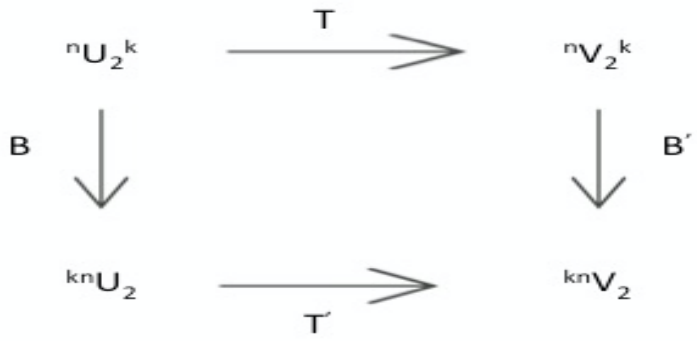

Figure 1. Schematic Representation of the transformations

B is a basis of U_{2^k} over U_2 with dimension k. The binary expansion occurs as follows: $c = a_1 b_1 + a_2 b_2 + ... + a_k b_k$ such that $c \in {}^nU_{2^k}$ and $\{b_1, b_2, ..., b_k\} \in B$, where the length of c (or equivalently the dimension of U_{2^k}) is the constant that multiplies with the initial dimension of the vector space over U_2. Considering the case of length of c as

1, binary expansion can be thought of as a representation of any element in ${}^{1}U_{2^k}$ as a vector in ${}^{k.1}U_2$.

It is therefore established when the classical RS code C of length N undergoes binary expansion through B of dimension k, it transforms as a vector in a vector space of dimension kN. $C^{'}$ therefore has length kN with dimension kK and is capable of encoding kK qubits with kN qubits ($N > K$).

To establish the second part that $C^{'}$ is a self-dual code when C is a self-dual code and B is a self-dual basis and thus proceed to forming the quantum equivalent of $C^{'}$, we begin with the assumption, without loss of generality about the nature of C, that ${}^{n}U_{2^k}$ is a subspace of the vector space W (where W contains all self-dual codes), and that ${}^{n}V_{2^k}$, although the dual of ${}^{n}U_{2^k}$, is not necessarily a subspace of W. The same assumptions are valid for the vector spaces ${}^{kn}U_2$ and ${}^{kn}V_2$ for some vector space $W^{'}$, since all these vector spaces are essentially the binary expansions of ${}^{n}U_{2^k}$, ${}^{n}V_{2^k}$, and W using suitable bases.

Since $C \in {}^{n}U_{2^k}$ is a self-dual code, $C \in {}^{n}V_{2^k}$, as ${}^{n}V_{2^k}$ is the dual space of ${}^{n}U_{2^k}$ and contains the dual of all vectors in ${}^{n}U_{2^k}$. Thus every vector in ${}^{n}U_{2^k}$ is present in ${}^{n}V_{2^k}$ and since dual transformation T is reversible, i.e. $T(T(C)) = C$, it is impossible to find a vector in ${}^{n}V_{2^k}$ that is not in ${}^{n}U_{2^k}$. We conclude, hence, that ${}^{n}V_{2^k}$ is equal to ${}^{n}U_{2^k}$.

Using the second condition that B is a self-dual basis, $B^{'} = B$, where $B^{'}$ is the dual-basis of B, or an endomorphism occurs here. We thus conclude that the binary expansions of C and it's dual using bases B and $B^{'}$ respectively yield codes in the same vector space. Now since it was initially given that C is a self-dual code of length N, the above discussion confirms that $C^{'}$ is also a self-dual code of length kN, where k is the dimension of B.

According to definition 1, the basis of the analogous quantum code of $C^{'}$ is possible to find. The resultant is the quantum RS code $C^{''}$ of length same as that of $C^{'}$ and dimension equal to the difference of length and twice the dimension of $C^{'}$, i.e. $C^{''} = [[kN, kN - 2kK, d \geq K + 1]]$.

The resultant quantum RS code encodes $kN - 2kK$ qubits using kN qubits, with kN evidently being greater than $kN - 2kK$, and thus the extra $2kK$ qubits as inputs in the architecture to preserve reversibility of the transformation.

5. Encoding and Decoding of Messages With Quantum Reed-Solomon Code

5.1. Quantum circuits and Quantum Fourier Transform

Lemma: bit-flip and phase-flip errors are conjugated to each other by Hadamard transform, i.e

$$H\sigma_x H^{-1} = \sigma_z \qquad and \qquad H\sigma_z H^{-1} = \sigma_x \tag{8}$$

The Quantum Fourier Transform (QFT is the quantum analogue of the Discrete Fourier Transform (DFT). DFT transforms a vector $X = (x_0, x_1, ..., x_{N-1}) \in C^N$, where C is

the complex vector space of dimension N, to a vector $Y = (y_0, y_1, ..., y_{N-1}) \in C^N$ by the relation:

$$y_k = \frac{1}{N^{1/2}} \sum_{j=0}^{N-1} x_j e^{\frac{2\pi i}{N} jk} \tag{9}$$

And the inverse discrete Fourier transform is given by the relation:

$$x_k = \frac{1}{N^{1/2}} \sum_{j=0}^{N-1} y_j e^{\frac{2\pi i}{N} j(-k)} \tag{10}$$

The Discrete Fourier Transform can be used to evaluate the values of a function at a given set of points [22], something that is the mathematical framework of the encoding procedure in the classical Reed-Solomon code discussed above and thus the core of our implementation of quantum Reed-Solomon codes.

The quantum equivalent of these transforms is the same relation except that x_i and y_i for $i \in \{0, 1, 2, ..., N-1\}$, are the amplitudes of the state of the system. The state of the system is a vector in a N dimensional Hilbert space given by the basis vectors $|0\rangle$, $|1\rangle$, $|2\rangle$, ..., $|N-1\rangle$ such that vectors X and Y considered in the classical DFT above are given by:

$$X = \sum_{i=0}^{N-1} x_i |i\rangle \quad and \quad Y = \sum_{i=0}^{N-1} y_i |i\rangle \tag{11}$$

The encoding is as follows:

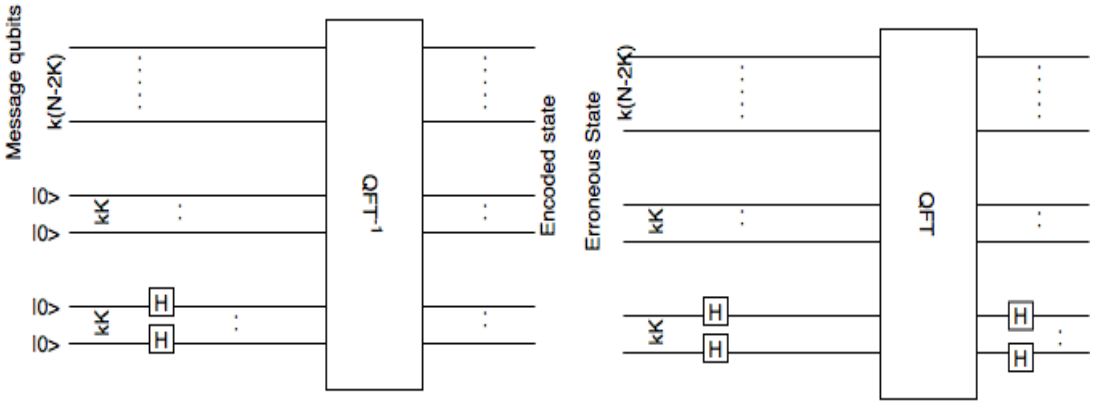

Figure 2. Encoding and decoding circuit for bit-flip and phase flip errors **without** CNOT gates. The second last kK qubits are for bit flip error detection, and the last kK qubits are for phase change error detection.

$$|\psi\rangle = QFT^{-1}[|\psi_1\rangle \otimes |\psi_2\rangle \otimes ...|\psi_{k(N-2K)}\rangle \otimes I^{\otimes kN-2kK}(|0\rangle \otimes |0\rangle \otimes ....|0\rangle) \otimes H^{\otimes kK}(|0\rangle \otimes |0\rangle \otimes ...|0\rangle)] \tag{12}$$

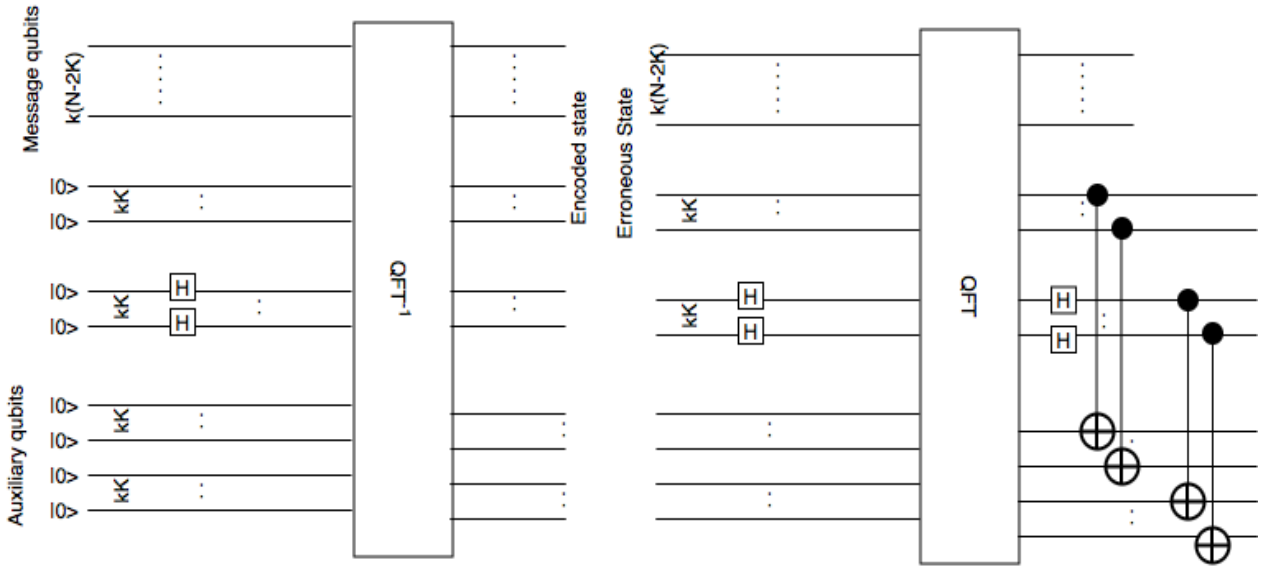

Figure 3. Encoding and decoding circuit for bit-flip and phase flip errors **with** CNOT gates. The second last kK qubits are for bit flip error detection, and the last kK qubits are for phase change error detection.

After decoding as in Fig. 2 and applying Hadamard gates in the last kK qubits we should get back a state as in Eq. (12) with 0's in the last 2kK qubits. We can infer an error has occurred if we get any state that does not have 0 in the last kK qubits.

6. Experimental Results

We encode the 3 qubit cluster state given by

$$|\psi_c\rangle = \frac{1}{\sqrt{2}}(|+\rangle|0\rangle|+\rangle + |-\rangle|1\rangle|-\rangle) \tag{13}$$

We simulate the circuit using a [[9,3]] code(N=3,K=1,k=3), by introducing a bit-flip error in each of the qubits of the encoded state individually. After that, we run the same simulation introducing a phase-flip error in each of the qubits. Then we run the code after introducing arbitrary phase change errors of 90, 45 and 22.5 degrees. The results are tabulated for two cases: without using extra CNOTs gates, in which the requisite qubits were directly measured, and using extra CNOTs gates, which is equivalent to the [24].

Error	Error on 1st qubit				Error on 2nd qubit				Error on 3rd qubit			
	E1	E2	E3	E4	E1	E2	E3	E4	E1	E2	E3	E4
Bit Flip	36.719	54.59	45.997	16.699	39.746	38.281	39.453	22.266	51.66	36.426	44.531	16.699
Phase change 180^o	45.118	45.356	55.469	13.574	57.715	45.215	43.849	12.891	46.874	42.87	48.242	14.453
Phase change 90^o	48.828	47.997	38.769	17.188	-	-	-	-	-	-	-	-
Phase change 45^o	-	-	-	46.094	45.899	48.341	15.332	-	-	-	-	-
Phase change 22.5^o	-	-	-	-	-	-	-	-	48.047	42.383	52.832	14.355

Table 1. Cumulative probabilities of error detection **without** CNOT gates. E1: Cumulative probability of error detection on 1st qubit; E2: Cumulative probability of error detection on 2nd qubit; E3: Cumulative probability of error detection on 3rd qubit; E4: Cumulative probability of no error detection.

Error	Error on 1st qubit				Error on 2nd qubit				Error on 3rd qubit			
	E1	E2	E3	E4	E1	E2	E3	E4	E1	E2	E3	E4
Bit Flip	46.777	56.542	50.391	10.645	47.363	49.512	51.958	12.598	43.067	57.714	45.508	13.672
Phase change 180^o	40.82	46.093	50.488	15.43	48.535	56.933	52.929	10.939	41.602	47.852	54.59	14.16
Phase change 90^o	42.09	42.09	52.833	15.527	-	-	-	-	-	-	-	-
Phase change 45^o	-	-	-	46.68	47.07	42.089	17.48	-	-	-	-	-
Phase change 22.5^o	-	-	-	-	-	-	-	-	67.481	46.974	48.145	9.082

Table 2. Cumulative probabilities of error detection **with** CNOT gates. E1: Cumulative probability of error detection on 1st qubit; E2: Cumulative probability of error detection on 2nd qubit; E3: Cumulative probability of error detection on 3rd qubit; E4: Cumulative probability of no error detection.

7. Further Research Prospects

The present quantum architecture limits the ability to optimize the algorithm discussed above. We hence leave the following discussion as future directions for research on more efficient implementations of quantum Reed-Solomon codes. We discuss here two such potential improvements to this algorithm; the quantum equivalent of [19] and the quantum singular value decomposition as an optimal improvement to quantum Fourier transform [21] improved upon the original classical Reed-Solomon encoding scheme by utilizing the property that RS codes are cyclic codes and can be implemented by generator polynomials. However, the original polynomial encoding had properties that [19] was able to work upon, and come up with a new algorithm for RS encoding with *interpolation*, *partial greatest common divisor*, and *long division* of polynomials using fast Fourier transforms. This algorithm can decode with errors and erasures, and can detect errors outside the decoding radius.

The quantum implementation of Gao's algorithm shall require efficient and implementable algorithms for the above mentioned processes. We note that *interpolation* is essentially approximation of a function using a given set of values, and can be implemented by inverse quantum Fourier transform [25] in their work on elliptic curve arithmetic over binary fields demonstrate the implementation of extended Euclidean algorithm and long division over polynomials in Hilbert spaces which can be converted to our purposes.

While Gao's classical algorithm is an evident winner over the original RS algorithm and doesn't need to find syndromes or calculate the error locations explicitly, the same can't be said for it's quantum equivalent. Considering a Galois field F_{2^k} we find that to implement *long division* (a key component of Gao's algorithm), we need dense quantum circuits $O(2k)$ to find the degree of the polynomials and additional relatively faster *shifting* circuits to divide a polynomial by another. We note this algorithm's implementation is currently constrained by the number of qubits in a quantum register we have at our disposal at present.

A second prospect could be improvements in the approximations by the quantum Fourier transforms used above. Encouraged by the results obtained by [26], we applied quantum singular value decomposition to the Fourier transform we were doing, and obtained a theoretical increase in precision. It remains to be experimentally verified for lack of large enough architecture.

8. Discussion and Conclusion

From the results, we conclude that the quantum RS code has a very low probability of error detection. The quantum RS code is not efficiently implementable in the present day quantum computers due to decoherence. Major sources of decoherence are intrinsic sources like material defects in the superconducting circuit [27, 28]; noise sources like charge; critical current fluctuations [29] and extrinsic sources like inadvertent interactions with the environment. Many approaches have been proposed to minimize the effect of the aforementioned sources - use of transmon qubits which were developed to reduce charge noise sensitivity [30, 31]. Since then transmon qubits have been extensively used to produce qubits with high coherence time [32, 36]. Progress in material science, circuit and program optimizations has also contributed to the development of qubits with high coherence time [35, 36].

From the results, it is also clear that the auxiliary qubit approach (with CNOT gates) of error detection does not lead to any clear improvement over non-auxiliary qubit approach (without CNOT gates), the latter being in general less perceptible to decoherence due to using fewer qubits and no CNOT gates. One of the reasons is the use of extra qubits (6 in case of our implementation) leading to more decoherence in the first approach. Although the non-auxiliary qubit approach destroys the state of qubits that are measured to detect the errors, it leaves the message qubits undisturbed, and hence leaves the scope for error correction without the loss of any information about the message states. So, we propose that the non-auxiliary qubit approach is more efficient than the auxiliary qubit approach for the implementation of higher dimensional quantum RS code to obtain higher fidelity.

We comment that application of quantum Reed-Solomon encoding-decoding algorithm for practical purposes may not be possible due to its unreliability in efficiently indicating the position of the error qubit. To correct the erroneous state, requisite unitary transformations need to be applied based on the measurements made above.

Unreliability in indicating the position of the error qubit decreases the chance of applying the correct unitary transformation, and hence decreases the chance of retrieving the original state. Moreover, there does not exist any protocol to differentiate the type of phase error a qubit has suffered. We conjecture it is still a long way to go before practical applications of quantum Reed-Solomon codes can come up.

Acknowledgement

N.M. acknowledges the hospitality provided by IISER Kolkata during the project work. B.K.B. acknowledges the support of IISER-K institute fellowship. The authors thank Prof. Anil Kumar, IISc Bangalore for his useful suggestions and discussions. We are extremely grateful to IBM team for providing access to IBM Quantum Experience (QE). The discussions and opinions developed in this paper are only those of the authors and do not reflect the opinions of IBM or IBM QE team.

References

[1] P. W. Shor, Scheme for reducing decoherence in quantum computer memory, Phys. Rev. A **52**, R2493 (1995).
[2] A. M. Steane, Error Correcting Codes in Quantum Theory, Phys. Rev. Lett. **77**, 5 (1996).
[3] A. M. Steane, Simple quantum error-correcting codes, Phys. Rev. A **54**, 4741 (1996).
[4] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, Perfect Quantum Error Correction codes, arXiv:quant-ph/9602019.
[5] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels, Phys. Rev. Lett. **70**, 1895 (1993).
[6] S. Choudhury, S. Muralidharan, and P. K. Panigrahi, Quantum teleportation and state sharing using a genuinely entangled six-qubit state, J. Phys. A: Math. Theor. **42**, 115303 (2009).
[7] S. Jain, S. Muralidharan, and P. K. Panigrahi, Secure quantum conversation through non-destructive discrimination of highly entangled multipartite states, Euro. Phys. Lett. **87**, 60008 (2009).
[8] K. Srinivasan, S. Satyajit, B.K. Behera, and P.K. Panigrahi, Efficient quantum algorithm for solving travelling salesman problem: An IBM quantum experience, arXiv:1805.10928 (2018).
[9] B. K. Behera, A. Banerjee, and P. K. Panigrahi, Experimental realization of quantum cheque using a five-qubit quantum computer, Quantum Inf. Process. **16**, 312 (2017).
[10] S. Muralidharan, S. Karumanchi, S. Jain, R. Srikanth, and P. K. Panigrahi, 2N qubit “mirror states" for optimal quantum communication, Eur. Phys. J. D. **61**, 757 (2011).
[11] S. Muralidharan, and P. K. Panigrahi, Quantum-information splitting using multipartite cluster state, Phys. Rev. A **78**, 062333 (2008).
[12] E. S. Prasath, S. Muralidharan, C. Mitra, and P. K. Panigrahi, Multipartite entangled magnon states as quantum communication channels, Quantum Inf. Process. **11**, 397 (2012).
[13] D. Ghosh, P. Agarwal, P. Pandey, B. K. Behera, and P. K. Panigrahi, Automated error correction in IBM quantum computer and explicit generalization, Quantum Inf. Process. **17**, 153 (2018).
[14] R. K. Singh, B. Panda, B. K. Behera, and P. K. Panigrahi, Demonstration of a general fault-tolerant quantum error detection code for (2n+1)-qubit entangled state on IBM 16-qubit quantum computer, arXiv:1807.02883.
[15] M. Grassl, W. Geiselmann, and T. Beth, Quantum Reed–Solomon Codes, In: M. Fossorier, H.

Imai, S. Lin, A. Poli (eds) Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. AAECC 1999. Lecture Notes in Computer Science, vol 1719. Springer, Berlin, Heidelberg.

[16] D. Schlingemann and R. F. Werner, Quantum error-correcting codes associated with graphs, Phys. Rev. A **65**, 012308 (2001).

[17] S Muralidharan, Chang-Ling Zou, Linshu Li, and Liang Jiang,One-way quantum repeaters with quantum Reed-Solomon codes Phys. Rev. A 97, 052316, 2018

[18] I. S. Reed and G. Solomon, Polynomial codes over certain finite fields, J. Soc. Indust. App. Math. **8** 300 (1960).

[19] S. Gao, A New Algorithm for Decoding Reed-Solomon Codes, In: V. K. Bhargava, H. V. Poor, V. Tarokh, S. Yoon (eds), Communications, Information and Network Security (2003), The Springer International Series in Engineering and Computer Science (Communications and Information Theory), vol 712. Springer, Boston, MA.

[20] W. K. Wootters and W. H. Zurek, A single quantum cannot be cloned, Nature **299**, 802 (1982).

[21] D. Gorenstein and N. Zierler, A class of error-correcting codes in p^m symbols, J. Soc. Indust. Appl. Math. **9**, 207 (1961).

[22] E. Knill and R. Laflamme, Theory of quantum error–correcting codes, Phys. Rev. A **55** 900 (1997).

[23] A. Steane, Multiple Particle Interference and Quantum Error Correction, Proc. Roy. Soc. Lond. **A452** 2551 (1996).

[24] M. Grassl, M. Rotteler, and T. Beth, Efficient quantum circuits for non qubit quantum error detecting codes, Int. J. Found. Comput. Sci. **14**, 757 (2003).

[25] P. Kaye and C. Zalka, Optimized quantum implementation of elliptic curve arithmetic over binary fields. *arxiv*. quant-ph:0407095 ,2004.

[26] L. Gyongyosi and S. Imre, An Improvement in Quantum Fourier Transform. arxiv,2012

[27] J. M. Martinis, K. B. Cooper, R. McDermott, M. Steffen, M. Ansmann, K. Osborn, K. Cicak, S. Oh, D. P. Pappas, R. W. Simmonds, and C. C. Yu, Phys. Rev. Lett. **95**, 210503 (2005).

[28] C. M. Quintana *et al.*, Characterization and reduction of microfabrication-induced decoherence in superconducting quantum circuits, Appl. Phys. Lett. **105**, 062601 (2014).

[29] D. J. V. Harlingen, T. L. Robertson, B. L. T. Plourde, P. A. Reichardt, T. A. Crane, and J. Clarke, Decoherence in Josephson-junction qubits due to critical-current fluctuations, Phys. Rev. B **70**, 064517 (2004).

[30] J. Koch, T. M. Yu, J. Gambetta, A. A. Houck, D. I. Schuster, J. Majer, A. Blais, M. H. Devoret, S. M. Girvin, and R. J. Schoelkopf, Charge-insensitive qubit design derived from the Cooper pair box, Phys. Rev. A **76**, 04319 (2007).

[31] J. A. Schreier, A. A. Houck, J. Koch, D. I. Schuster, B. R. Johnson, J. M. Chow, J. M. Gambetta, J. Majer, L. Frunzio, M. H. Devoret, S. M. Girvin, and R. J. Schoelkopf, Suppressing charge noise decoherence in superconducting charge qubits, Phys. Rev. B **77**, 180502 (2008).

[32] H. Paik, D. I. Schuster, L. S. Bishop, G. Kirchmair, G. Catelani, A. P. Sears, B. R. Johnson, M. J. Reagor, L. Frunzio, L. Glazman, S. M. Girvin, M. H. Devoret, and R. J. Schoelkopf, Observation of High Coherence in Josephson Junction Qubits Measured in a Three-Dimensional Circuit QED Architecture, Phys. Rev. Lett. **107**, 240501 (2011).

[33] C. Rigetti, J. M. Gambetta, S. Poletto, B. L. T. Plourde, J. M. Chow, A. D. Corcoles, J. A. Smolin, S. T. Merkel, J. R. Rozen, G. A. Keefe *et al.*, Superconducting qubit in a waveguide cavity with a coherence time approaching 0.1 ms, Phys. Rev. B **86**, 100506 (2012).

[34] R. Barends, J. Kelly, A. Megrant, D. Sank, E. Jeffrey, Y. Chen, Y. Yin, B. Chiaro, J. Mutus, C. Neill et al., Coherent Josephson Qubit Suitable for Scalable Quantum Integrated Circuits. Phys. Rev. Lett. **111**, 080502 (2013).

[35] A. Megrant, C. Neill, R. Barends, B. Chiaro, Y. Chen, L. Feigl, J. Kelly, E. Lucero, M. Mariantoni, P. J. J. O'Malley *et al.*, Planar superconducting resonators with internal quality factors above one million, Appl. Phys. Lett. **100**, 113510 (2012).

[36] Y. Zhang, H. Deng, Q. Li, H. Song, and L. Nie, Optimizing Quantum Programs against Decoherence: Delaying Qubits into Quantum Superposition, arXiv:1904.09041.