

This is the accepted manuscript made available via CHORUS. The article has been published as:

# One-way quantum repeaters with quantum Reed-Solomon codes

Sreraman Muralidharan, Chang-Ling Zou, Linshu Li, and Liang Jiang

Phys. Rev. A **97**, 052316 — Published 14 May 2018

DOI: [10.1103/PhysRevA.97.052316](https://doi.org/10.1103/PhysRevA.97.052316)

# One way quantum repeaters with quantum Reed-Solomon codes

Sreraman Muralidharan<sup>1,2</sup>, Chang-Ling Zou<sup>3</sup>, Linshu Li<sup>3,4</sup>, and Liang Jiang<sup>3,4\*</sup>

<sup>1</sup>*Department of Electrical Engineering, Yale University, New Haven, CT 06511 USA*

<sup>2</sup>*US Army research laboratory, Adelphi MD 20783 USA*

<sup>3</sup>*Department of Applied Physics, Yale University, New Haven, CT 06511 USA and*

<sup>4</sup>*Yale Quantum Institute, Yale University, New Haven, CT 06520 USA*

(Dated: April 26, 2018)

We show that quantum Reed-Solomon codes constructed from classical Reed-Solomon codes can approach the capacity on the quantum erasure channel of  $d$ -level systems for large dimension  $d$ . We study the performance of one-way quantum repeaters with these codes and obtain a significant improvement in key generation rate compared to previously investigated encoding schemes with quantum parity codes and quantum polynomial codes. We also compare the three generation of quantum repeaters using quantum Reed-Solomon codes and identify parameter regimes where each generation performs the best.

## I. INTRODUCTION

The possibility of transmitting information encoded into quantum states offers unconditional in principle security [1–4] and can potentially lead to a secure quantum internet [5]. There are currently two approaches taken to the transmission of quantum states using single photons [6]. One uses satellite to link remote parties [7, 8], while the other uses fiber based quantum repeaters [9]. Fiber based quantum repeaters have the potential to offer higher bandwidth, larger key generation rates and is tolerant to inclement weather conditions compared to satellite based quantum communication. Long distance classical communication through optical fibers is made possible through establishing intermediate repeater stations, where the optical signal is amplified and retransmitted to the neighboring station to compensate fiber attenuation. However, quantum communication relies on the transfer of quantum states - which unlike classical states, cannot be perfectly amplified or duplicated [10]. Quantum repeaters [11] (QRs) provide the only known approach for long distance quantum communication through optical fibers [12, 13], where loss and operation errors are detected or even actively corrected at the repeater stations.

QRs can be classified into three generations depending on the methods used to overcome loss and operation errors [14, 15]. The first generation QRs [9, 11] relies on heralded entanglement generation [16] between neighboring repeater stations to overcome loss errors and entanglement purification [9, 17] between neighboring and remote repeater stations to correct operation errors. The remote two way classical communication needed between remote stations slows down the key generation rates and requires long lived quantum memories at repeater stations. The second generation QRs relies on heralded entanglement generation between neighboring repeater stations to overcome loss errors and quantum error cor-

rection to overcome operation errors [18–23]. This needs two-way classical communication only between neighboring stations, which can be achieved in parallel. The third generation QR uses only quantum error correction [24–27] to overcome both loss and operation errors [14, 28–37]. The third generation QRs are analogous to classical repeaters because their communication rate depends solely on the time taken to perform local operations and is a completely one-way protocol, with the potential of reaching ultrafast communication rates [33, 37]. Teleportation based error correction (TEC) [38] have been introduced at each repeater station to correct loss and operation errors in the third generation QRs [34]. Similar to quantum teleportation, TEC protocol requires encoded Bell state preparation and measurement of logical  $X$  and  $Z$  operators of the code. TEC for QR has been generalized to accommodate qudit error correcting codes such as quantum polynomial codes [34] using generalized Pauli operators that act on a  $d$ -level system as  $X^l|j\rangle = |j+l\rangle$  and  $Z^l|j\rangle = \omega^{lj}|j\rangle$ ,  $0 \leq i, j \leq d-1$  [39]. The performance of quantum parity codes (QPC) was first studied for one-way QRs [32] and the repeater parameters were optimized using a cost function [33]. It has been shown that quantum polynomial codes (QPyCs) [34, 40], which can correct up to a maximum of 50% photon losses [41], can reduce the cost for low operation errors. Moreover, continuous variable cat codes can also be used for this generation of QRs [42].

So far all proposed third generation QR schemes rely on encoding a single logical qubit (qudit) into a block of physical qubits (qudits). This leads to an interesting question of whether the third generation QR can benefit from error correcting codes encoding multiple logical qubits/qudits, which might enable us to further improve the key generation rates. There are efficient ways to construct qubit and qudit quantum error correcting codes from classical linear codes using the Calderbank-Shor-Steane (CSS) construction [27]. For third generation QRs, we need CSS codes because the encoded CNOT gate required by the TEC protocol has a transversal implementation [27]. For example, a Steane  $[[7, 1, 3]]$  code [27] can be constructed from the  $[[7, 4, 3]]$  classical Ham-

---

\*liang.jiang@yale.edu

ming code and its dual  $[7, 3, 3]$  code.

Reed-Solomon codes introduced in 1960 [43] have found spectacular applications [44, 45] for information transmission in the past few decades and has revolutionized the information technology industry. This motivates us to consider the construction of quantum Reed-Solomon codes from classical Reed-Solomon codes using the CSS construction and consider their usefulness for quantum communication. More specifically, here, we show that quantum Reed-Solomon codes (QRSC) [46, 47] encoding multiple logical qudits can be a promising candidate for the third generation QRs. Since, we encode multiple logical qudits into QRSC, one can expect an increase in data transfer rates compared to encoding schemes where a single logical qubit (qudit) is being encoded.

In the following, we first introduce the construction of QRSC [46, 47] from classical Reed Solomon codes [43–45] using the CSS construction [27]. We then show that QRSC of qudit with dimension  $d$  approaches the capacity of the quantum erasure channel of  $d$ -level systems. We then describe the application of QRSC for QRs and study the improvement compared to QPC and QPyC in terms of the cost coefficient. Finally, we compare the three generations of QRs assuming QRSC for the third generation and identify experimental parameter regimes where each generation performs the best.

## II. CLASSICAL REED-SOLOMON CODES

A classical Reed Solomon code is defined over a Galois field  $GF(d)$ , where  $d$  is a prime, which contains a primitive element  $\alpha$  such that  $\alpha^{d-1} = 1$ .  $GF(d) = \{0, \alpha, \alpha^2, \dots, \alpha^{d-2}, 1\}$ . A Reed Solomon code is defined in the following manner [43–45]: Suppose,  $c = (c_0, c_1, \dots, c_{k-1})$  is a list of information symbols with each element taken from  $GF(d)$ , we define the polynomial function

$$p_c(x) = c_0 + c_1x + \dots + c_{k-1}x^{k-1}, \quad (1)$$

which can generate the codewords

$$c = (c_0, c_1, \dots, c_{k-1}) \mapsto (p_c(0), p_c(\alpha), \dots, p_c(\alpha^{d-1})). \quad (2)$$

We can obtain  $d$  linear equations with  $k$  variables as following

$$p_c(0) = c_0, \quad (3)$$

$$p_c(\alpha^j) = c_0 + c_1\alpha^j + c_2\alpha^{2j} + \dots + c_{k-1}\alpha^{(k-1)j}, \quad (4)$$

where  $j \in \{1, \dots, d-1\}$  and the summation is taken *mod*  $d$ . Without loss of generality, we can use the first  $k$  equations to solve for the codewords, which gives us the  $[d, k, d-k+1]_d$  Reed-Solomon code. We rewrite the above equations in the matrix form

$$(p_c(0), p_c(\alpha), \dots, p_c(\alpha^{d-1})) = c \cdot G, \quad (5)$$

with generator matrix

$$G = \begin{bmatrix} 1 & 1 & \cdot & \cdot & 1 \\ 0 & \alpha & \alpha^2 & \cdot & \alpha^{d-1} \\ 0^2 & \alpha^2 & \alpha^4 & \cdot & \alpha^{2(d-1)} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0^{k-1} & \alpha^{k-1} & \alpha^{2(k-1)} & \cdot & \alpha^{(k-1)(d-1)} \end{bmatrix}, \quad (6)$$

with the corresponding parity check matrix as

$$H = \begin{bmatrix} 1 & 1 & \cdot & \cdot & 1 \\ 0 & \alpha & \alpha^2 & \cdot & \alpha^{d-1} \\ 0^2 & \alpha^2 & \alpha^4 & \cdot & \alpha^{2(d-1)} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0^{d-k-1} & \alpha^{d-k-1} & \alpha^{2(d-k-1)} & \cdot & \alpha^{(d-1)(d-k-1)} \end{bmatrix}. \quad (7)$$

It can be verified that the rows of matrix  $H$  are orthogonal to the rows of  $G$ .  $H$  can also be regarded as the generator matrix of the dual code  $[d, d-k, k+1]_d$  [45].

## III. QUANTUM REED-SOLOMON CODES

A QRSC [46, 47] can be obtained from the CSS construction of two classical Reed-Solomon codes, namely the  $[d, k, d-k+1]_d$  code and its dual  $[d, d-k, k+1]_d$  code, giving us the quantum code  $[[d, 2k-d, d-k+1]]_d$  [48–50] where  $2k-d$  logic qudits of  $d$  levels are encoded into  $d$  physical qudits. So that as long as less than (or equal to)  $d-k$  qudits are lost, the encoded quantum information can be retrieved. Therefore, the classical codes

$$C_1 = \{p_c(0), p_c(\alpha), \dots, p_c(\alpha^{d-1}) | c \in F_d^k\} \quad (8)$$

$$C_2 = \{p_c(0), p_c(\alpha), \dots, p_c(\alpha^{d-1}) | c \in F_d^{d-k}\} \quad (9)$$

fulfil the requirement of CSS construction  $C_1 \subset C_2$  and hence they can yield the quantum code (i.e. QRSC)

$$|s_0, s_1, \dots, s_{2k-d-1}\rangle \mapsto \sum_{c_{d-k+j}=s_j, |c \in F_d^k} |p_c(0)p_c(1)\dots p_c(\alpha^{d-2})\rangle. \quad (10)$$

To understand the above summation, let us consider an example of the  $[[3, 1, 2]]_3$  code with  $d = 3$ ,  $k = 2$  and  $c_{1+j} = s_j$ . The primitive element of  $GF(3)$  is 2. This gives us the codeword

$$|s_0\rangle \mapsto \sum_{c_{1+j}=s_j} |p_c(0)p_c(1)p_c(2)\rangle. \quad (11)$$

For  $s_0 = 0$ , we have  $c_1 = 0$ , for  $s_0 = 1$ , we have  $c_1 = 1$  and for  $s_0 = 2$ , we have  $c_1 = 2$ . The logical states are

given by,

$$\begin{aligned} |0\rangle_L &= \sum_{c_0=0}^2 |c_0\rangle|c_0\rangle|c_0\rangle = \frac{1}{\sqrt{3}}(|000\rangle + |111\rangle + |222\rangle), \\ |1\rangle_L &= \sum_{c_0=0}^2 |c_0\rangle|c_0+1\rangle|c_0+2\rangle = \frac{1}{\sqrt{3}}(|012\rangle + |120\rangle + |201\rangle), \\ |2\rangle_L &= \sum_{c_0=0}^2 |c_0\rangle|c_0+2\rangle|c_0+4\rangle = \frac{1}{\sqrt{3}}(|021\rangle + |102\rangle + |210\rangle). \end{aligned} \quad (12)$$

Note that the addition is performed modulo 3 here. QPyC is related to the special case of QRSC with  $k = (d+1)/2$ , for encoding a single logical qudit. Note that QPyC construction does not require the size of the encoding block to be equal to the dimension of qudit  $d$  [40], so QPyC is not a subset of QRSC. We will now show how to construct the stabilizers and logical operators of QRSC.

*Example 1:  $[[3, 1, 2]]_3$  code*

To construct a  $[[3, 1, 2]]_3$  code, we use two classical codes, namely, the  $[3, 2, 2]_3$  code and the  $[3, 1, 3]_3$  code. The generator and the parity check matrices for the  $[3, 2, 2]_3$  code are given by

$$G = \begin{bmatrix} 1 & 1 & 1 \\ 0 & \alpha & 1 \end{bmatrix}, H = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}$$

respectively. Similarly the generator and parity check matrices of the  $[3, 1, 3]_3$  code are given by  $H$  and  $G$  respectively. The stabilizers of the  $[[3, 1, 2]]_3$  code are given by,  $XXX$  and  $ZZZ$ , while the logical operators are  $X_L = IXX^2$  and  $Z_L = IZ^2Z$ . By multiplying stabilizers we obtain equivalent expressions for logical operators  $X_L = X^2IX$ ,  $XX^2I$  and  $Z_L = ZIZ^2$ ,  $Z^2ZI$ . If the first qudit is erased, we can restore the encoded information based on the logical operators  $X_L = IXX^2$  and  $Z_L = IZ^2Z$ , independent of the first qudit. Similarly, we can restore the encoded information, if the second or third qudit is erased. Therefore,  $[[3, 1, 2]]_3$  code can correct a single erasure error.

*Example 2:  $[[5, 3, 2]]_5$  code*

To construct a  $[[5, 3, 2]]_5$  code, we pick two classical codes, namely  $[5, 4, 2]_5$  code and the  $[5, 1, 5]_5$  code. The generator and parity check matrices of the  $[5, 4, 2]_5$  code is given by

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & \alpha & \alpha^2 & \alpha^3 & 1 \\ 0 & \alpha^2 & 1 & \alpha^2 & 1 \\ 0 & \alpha^3 & \alpha^2 & \alpha & 1 \end{bmatrix}, H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

The stabilizer generators of the code are  $XXXXX$  and  $ZZZZZ$ . The logical operators can also be constructed

from the matrices. For example, the  $X_L$  operators are given by,  $X_L^{(1)} = IXX^2X^3X^4$ ,  $X_L^{(2)} = IX^2X^4X^2X^4$ ,  $X_L^{(3)} = IX^3X^2XX^4$ . Other equivalent logical operators can be obtained by multiplying the stabilizers with these logical operators. The  $Z_L$  operators can be obtained in a similar fashion.

#### IV. CAPACITY OF QUANTUM ERASURE CHANNEL

For erasure probability  $p_l$ , the capacity of qudit erasure channel is  $1 - 2p_l$  dits/channel use [41]. In the following, we show that QRSC can approach this capacity for large  $d$ , which is associated with both the size of the encoding block and the physical dimension of the  $d$ -level system [57]. To justify this claim, we may generally compute the success probability of error correction for the  $[[d, 2k - d, d - k + 1]]_d$  code with prime  $d$  as

$$P_{\text{success}} = \sum_{j=0}^{d-k} \binom{d}{j} p_l^j (1 - p_l)^{d-j}. \quad (13)$$

The failure probability is

$$P_{\text{fail}} = \sum_{j=d-k+1}^d \binom{d}{j} p_l^j (1 - p_l)^{d-j}, \quad (14)$$

which can be rewritten as

$$P_{\text{fail}} = \sum_{j=0}^k \binom{d}{j} p_l^{d-j} (1 - p_l)^j, \quad (15)$$

Let  $k = (1 - p_l)d + x$ , then  $\varepsilon = x/d$  with  $x \ll d$ . We have  $p_l > \frac{d-k}{d}$ . According to the Chernoff-Hoeffding theorem

$$\begin{aligned} P_{\text{success}}|_{1-\frac{k}{d}=p_l-\varepsilon} &\leq \left( \left( \frac{p_l}{p_l-\varepsilon} \right)^{p_l-\varepsilon} \left( \frac{1-p_l}{1-p_l+\varepsilon} \right)^{1-p_l+\varepsilon} \right)^d \\ &= e^{-D(p_l-\varepsilon||p_l)d} \end{aligned} \quad (16)$$

where

$$D(a||b) = a \ln \frac{a}{b} + (1-a) \ln \frac{1-a}{1-b} \quad (17)$$

is the Kullback-Leibler divergence [51]. Taking the Taylor expansion of  $D$ , For  $d \rightarrow \infty$  and letting  $\varepsilon = x/d \ll 1$ , we have

$$P_{\text{success}}|_{p_l} \leq e^{-\varepsilon x/p_l} e^{-\varepsilon x/(1-p_l)} \quad (18)$$

For  $p_l < \frac{d-k}{d}$ , we have

$$P_{\text{success}}|_{1-\frac{k}{d}=p_l+\varepsilon} = 1 - P_{\text{fail}}|_{1-\frac{k}{d}=p_l+\varepsilon}. \quad (19)$$

According to the Chernoff-Hoeffding theorem,

$$P_{\text{fail}}|_{1-\frac{k}{d}=p_l+\varepsilon} \leq \left( \left( \frac{p_l}{p_l+\varepsilon} \right)^{p_l+\varepsilon} \left( \frac{1-p_l}{1-p_l-\varepsilon} \right)^{1-p_l-\varepsilon} \right)^d. \quad (20)$$

For  $d \rightarrow \infty$  and let  $\varepsilon = x/d \ll 1$ , we have

$$P_{\text{success}}|_{p_l=1-\frac{k}{d}-\varepsilon} \geq 1 - e^{-(p_l+\varepsilon)x/p_l} e^{(1-p_l-\varepsilon)x/(1-p_l)}. \quad (21)$$

Therefore, for  $d \rightarrow \infty$ ,  $P_{\text{success}} \approx 1$  for  $p_l - \frac{1-R_c}{2} < O(\frac{1}{\sqrt{d}})$ , and  $P_{\text{success}} = 0$  for  $p_l - \frac{1-R_c}{2} > O(\frac{1}{\sqrt{d}})$ , with  $R_c = \frac{2k-d}{d}$  is the code rate.

## V. ONE-WAY QUANTUM REPEATERS WITH QRSC

One-way QRs use quantum error correction instead of amplification used in classical repeaters to counter photon loss in propagation. Here, the quantum state to be transmitted is encoded into an error correcting code and sent to the neighboring station where a TEC operation is performed to correct both loss and operation errors. After the error correction, the signal is retransmitted to the neighboring station. This is carried out until the encoded quantum state reaches the receiver. We will first study the error model and describe the optimization of QRSC quantum repeaters. There are two kinds of errors that is encountered by QRs which have to be corrected.

1. Photon loss errors: The probability that each photon successfully reaches the neighboring repeater station is  $\eta_c^2 \times e^{-\frac{L_0}{L_{\text{att}}}}$ , where  $L_0$  is the repeater spacing,  $L_{\text{att}} = 20\text{km}$  is the attenuation length of the fiber, and  $\eta_c$  is the coupling efficiency between fiber and matter qudits.
2. Operation errors: These include the gate errors, depolarization errors and measurement errors. Here,  $\epsilon_g$  is the gate error,  $\epsilon_d$  is the depolarization error and  $\epsilon_m$  is the measurement error. The total error measured at the  $X$  and  $Z$  measurements of the TEC circuit is given by  $(3\epsilon_g + 4\epsilon_d + \epsilon_m)$  [34].

If  $x$  photons are lost during the communication, among the rest of the photons that reach the destination,  $y$  photons suffer operation errors, as such, the code can correct up to  $x + 2y \leq (d - k)$  errors [34, 37]. The probability that at least  $(d - k)$  photons are received and the encoded state is decoded correctly is given by

$$P_{\text{correct}(X/Z)} = \sum_{x=0}^{d-k} \sum_{y=0}^{\lfloor \frac{d-k}{2} - \frac{x}{2} \rfloor} \binom{d}{x} \binom{d-x}{y} \times (1-\eta)^x \epsilon_{X/Z}^y (1-p_l)^{d-x} (1-\epsilon_{X/Z})^{d-x-y}. \quad (22)$$

The probability that at least  $(d - k)$  photons are received and the encoded state is decoded incorrectly is given by

$$P_{\text{incorrect}(X/Z)} = \sum_{x=0}^{d-k} \sum_{y=\lceil \frac{d-k}{2} - \frac{x}{2} + 0.5 \rceil}^{(d-k-x)} \binom{d}{x} \binom{d-x}{y} \times (1-\eta)^x \epsilon_{X/Z}^y (1-p_l)^{d-x} (1-\epsilon_{X/Z})^{d-x-y}. \quad (23)$$

By making an assumption that an effective logical error in any one of the QR stations leads to a logical error at the receiver's end, the quantum bit error rate can be defined as [34],

$$Q_{X/Z} = 1 - \frac{[P_{\text{correct}(X/Z)}]^r}{[P_{\text{success}}]^r}, \quad (24)$$

where  $r$  is the number of repeater stations. For the two basis protocol for quantum key distribution, the asymptotic secure key generation rate is [52]

$$R = (2k - d) \frac{[P_{\text{success}}]^r}{t_0} (\log_2 d - 2h(Q)), \quad (25)$$

where  $t_0$  is the time taken for quantum gates and measurement and

$$Q = \left( \frac{Q_X + Q_Z}{2} \right) \\ h(Q) = -Q \log_2 \frac{Q}{d-1} - (1-Q) \log_2 (1-Q). \quad (26)$$

It is worth mentioning that compared to protocols encoding a single logical qudit [34], the boost in the key generation rates comes by the factor  $(2k - d)$  in logical qudit encoding. The two important resources one has to consider for one-way QRs are the number of physical qudits and the time consumption. The cost coefficient which is obtained by taking the product of temporal and physical resources needed for the QR to function provides an excellent tool to compare QR schemes with different error correcting codes [33, 34]. The cost coefficient is the number of qubits required per km to generate one secure bit per unit time  $t_0$ . Since we need to compare schemes based on qubit encoding (e.g. QPC) and qudit encoding (e.g. QPyC and QRSC), we assume that each qudit of  $d$  levels can be mapped into  $\log_2 d$  qubits. Following Ref. [34], we define the cost coefficient for QRSC

$$C' = \frac{2d \log_2 d}{L_0 R}, \quad (27)$$

where  $2d$  is the number of qudits required for TEC,  $L_0$  is the repeater spacing and  $R$  is the secure key generation rate. In Fig. 1, we compare the performances of QRSC with QPyC and QPC in the absence of operation errors. It can be seen that one can obtain a factor of 35 reduction in cost for communication up to  $L_{\text{tot}} = 10,000\text{km}$  by using QRSC instead of QPC.

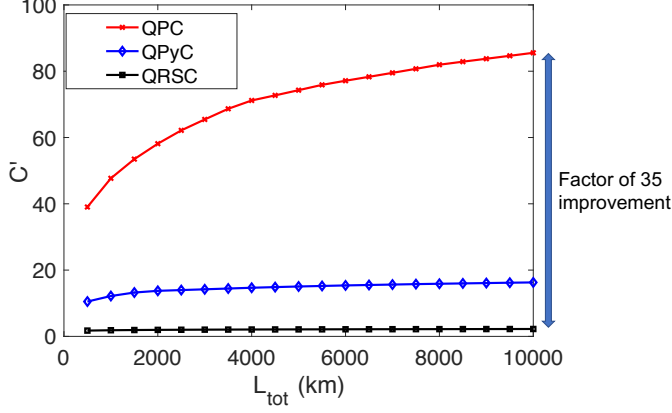


FIG. 1: Comparison between the cost coefficients of quantum Reed Solomon codes (QRSC) (denoted with black  $\square$ ) with quantum polynomial codes (QPyC) (denoted with blue  $\diamond$ ) and quantum parity codes (QPC) (denoted with red  $\times$ ) in the absence of operation errors assuming it takes the same time to create small encoded blocks of qubits (qudits).

## VI. COMPARISON OF DIFFERENT GENERATIONS OF QRS WITH QRSC FOR THE THIRD GENERATION

The cost coefficient provides an effective tool to compare the three generations of QRs. For a given set of experimental parameters, we can identify the quantum repeater generation that yields the minimum cost and conclude that generation to be the optimum for that set of experimental parameters. Following Ref. [15], we choose gate error  $\epsilon_G$ , coupling efficiency (between atom and photon)  $\eta_c$  and operation time  $t_0$  for comparison. For first and second generation QRs, we assume that the initial fidelity of Bell pairs generated is  $(1 - \frac{5}{4}\epsilon_G)$  with entanglement purification [15] and measurement error probability  $\epsilon_m = \frac{\epsilon_G}{4}$  obtained through a measurement with an ancilla qubit [53]. The three generations of QRs have been compared using QPC for the third generation with a maximum of 200 qubits [15]. Here, we expand the comparison by including QRSC for the third generation QRs, with a maximum of  $d = 23$  which corresponds to  $2d \cdot \log_2 d \approx 200$  qubits. This assumes that we use qubits as elementary building blocks for first and second generations of QRs and QRSC of qudits for the third generation QRs. In Fig. 2, it can be seen that QRSC can correct a large fraction of erasure errors up to  $10^{-2}$ . For  $\eta_c \geq 90\%$ , the third generation QRs dominate for all values of  $\epsilon_G$ . For  $\eta_c = 30\%$ , and  $\epsilon_G = 10^{-3}, 10^{-4}$  the third generation QR cannot correct the loss errors and the second generation without (with) encoding comes into play. For  $\epsilon_G = 10^{-2}$ , the errors proliferate for first and second generations of QRs and consequently, the first generation becomes useful here.

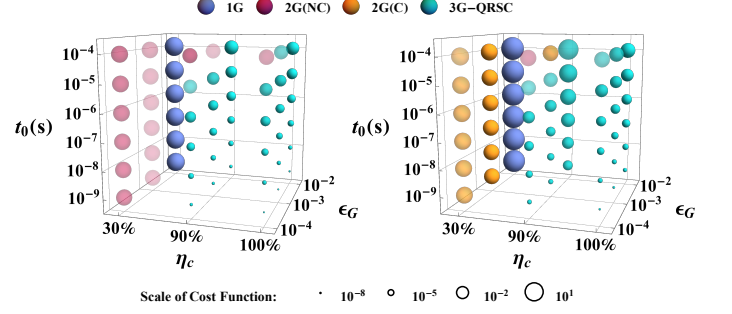


FIG. 2: The bubble plot comparing various QR protocols in the three-dimensional parameter space spanned by  $\eta_c$ ,  $\epsilon_G$ , and  $t_0$ , for a)  $L_{tot} = 1000\text{km}$  and b)  $L_{tot} = 10,000\text{km}$ . The bubble color indicates the associated optimized QR protocol, and the bubble diameter is proportional to the log of the cost coefficient.

Now, we study the variation of cost coefficient with respect to  $d$ . In Fig. 3, the cost function is compared for  $t_0 = 1 \mu\text{s}$ , with  $L_{tot} = 1000\text{ km}$  and  $10,000\text{ km}$  respectively. Here,  $d \geq 3$  corresponds to QRSC while cases with  $d = 2$  corresponds to QPC. The results indicate that for small  $\epsilon_G < 10^{-2}$ , QRSC can outperform QPC with a sufficiently large dimension  $d$ .

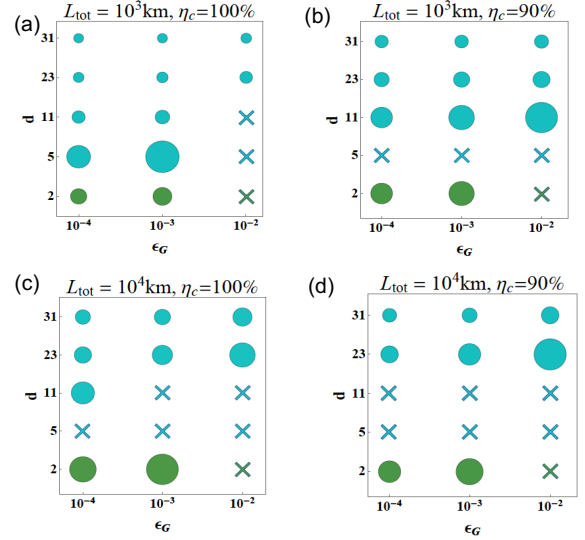


FIG. 3: Bubble plot showing the cost coefficient achievable for various  $\epsilon_G$  as a function of  $d$ .  $d = 2$  corresponds to the case of QPC.  $\times$  corresponds to a region not correctable. To beat the cost coefficient achievable with QPC, one needs to use a QRSC with a large  $d$ .  $d = 23$  corresponds to the maximum  $d$  searched by the optimization algorithm for the bubble plot as it is less than 200 qubits. The cost coefficient does not vary appreciably for  $d > 31$ .

## VII. CONCLUSION

We have investigated quantum Reed-Solomon codes constructed from the CSS construction of classical Reed-Solomon codes for application of the third generation quantum repeater over long distances. We described the construction of stabilizers and logical operators for these codes with examples. The rates of these codes approach channel capacity of the quantum erasure channel for  $d$ -level systems. For channel dominated by photon loss errors (with negligible operation errors), QRSC can achieve a factor of 35 improvement in the cost coefficient compared to QPC. For situations with both loss and operation errors, we compared the three generations of QRs including QRSC for the third generation QRs and identified the dimension  $d$  where these codes begin to perform better than QPC. As proposed in Ref. [34], neutral atoms of multilevel systems trapped by photonic nanocrystal

cavities [54] may provide a potential physical platform to realize qudit based third generation QRs. For future research, it will be interesting to analyze other quantum error correcting codes for one-way QRs such as quantum Reed-Muller codes [55] and quantum polar codes [56] and optimize their performance by systematic comparison.

## Acknowledgments

We thank Vladimir Malinovsky, Jungsang Kim, Kasper Duivenvoorden, Henry Pfister, Hong Tang and Steven Girvin for discussions. This work was supported by the ARL CDQI, Alfred P. Sloan Foundation (BR-2013-049), ARO (W911NF-14-1-0011, W911NF-14-1-0563), ARO MURI (W911NF-16-1-0349), AFOSR MURI (FA9550-14-1-0052, FA9550-15-1-0015), NSF (EFMA-1640959) and Packard Foundation (2013-29-273).

- 
- [1] H. K. Lo and H. F. Chau, *Science* **283**, 2050 (1999).
  - [2] V. Scarani, H. Bechmann-Pasquinucci, N. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, *Rev. Mod. Phys.* **81**, 1301 (2009).
  - [3] N. Gisin and R. Thew, *Nat. Phot.* **1**, 165 (2007).
  - [4] P. W. Shor and J. Preskill, *Phys. Rev. Lett.* **85**, 441 (2000).
  - [5] H. J. Kimble, *Nature* **453**, 1023 (2008).
  - [6] C. Simon, *Nat. Phot.* **11**, 678 (2017).
  - [7] J.-G. Ren, P. Xu, H.-L. Yong, L. Zhang, S.-K. Liao, J. Yin, W.-Y. Liu, W.-Q. Cai, M. Yang, L. Li, et al., *Nature* **549**, 70 (2017).
  - [8] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, et al., *Science* **356**, 1140 (2017).
  - [9] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, *Phys. Rev. A* **59**, 169 (1999).
  - [10] W. K. Wootters and W. H. Zurek, *Nature(London)* **299**, 802 (1982).
  - [11] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, *Phys. Rev. Lett.* **81**, 5932 (1998).
  - [12] M. Takeoka, S. Guha, and M. M. Wilde, *Nat. comm.* **5**, 5235 (2014).
  - [13] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, *Nat. Comm.* **8**, 15043 (2017).
  - [14] R. M. Gingrich, P. Kok, H. Lee, F. Vatan, and J. P. Dowling, *Phys. Rev. Lett.* **91**, 217901 (2003).
  - [15] S. Muralidharan, L. Li, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, *Sci. Rep.* **6**, 20463 (2016).
  - [16] H. Bernien, B. Hensen, W. Pfaff, G. Koolstra, M. S. Blok, L. Robledo, T. H. Taminiau, M. Markham, D. J. Twitchen, L. Childress, et al., *Nature(London)* **497**, 86 (2013).
  - [17] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, *Phys. Rev. Lett.* **76**, 722 (1996).
  - [18] L. Jiang, J. M. Taylor, K. Nemoto, W. J. Munro, R. Van Meter, and M. D. Lukin, *Phys. Rev. A* **79**, 032325 (2009).
  - [19] W. J. Munro, K. A. Harrison, A. M. Stephens, S. J. Devitt, and K. Nemoto, *Nat. Photon.* **4**, 792 (2010).
  - [20] K. Azuma, K. Tamaki, and H.-k. Lo, *Nat. Comm.* **6**, 67897 (2015).
  - [21] M. Pant, H. Krovi, D. Englund, and S. Guha, *arxiv:quantph/1603.01353* (2016).
  - [22] M. Epping, H. Kampermann, and D. Bruß, *Applied Physics B: Lasers and Optics* **122**, 54 (2016).
  - [23] Y. Li, S. D. Barrett, T. M. Stace, and S. C. Benjamin, *New J. Phys.* **15**, 023012 (2013).
  - [24] M. Grassl, T. Beth, and T. Pellizzari, *Phys. Rev. A* **56**, 33 (1997).
  - [25] C. Y. Lu, W.-B. Gao, J. Zhang, X.-Q. Zhou, T. Yang, and J.-W. Pan, *Proc. Natl. Acad. Sci. USA* **105**, 11050 (2008).
  - [26] M. Bergmann and P. van Loock, *Phys. Rev. A* **94**, 012311 (2016).
  - [27] M. A. Nielsen and I. Chuang, *Quantum computation and quantum information* (Cambridge University Press, Cambridge, U.K; New York, 2000).
  - [28] A. G. Fowler, D. S. Wang, C. D. Hill, T. D. Ladd, R. Van Meter, and L. C. L. Hollenberg, *Phys. Rev. Lett.* **104**, 180503 (2010).
  - [29] M. Zwerger, H. J. Briegel, and W. Dür, *Appl. Phys. B* **50**, 122 (2016).
  - [30] M. Zwerger, A. Pirker, V. Dunjko, H. J. Briegel, and W. Dür, *Phys. Rev. Lett.* **120**, 030503 (2018).
  - [31] M. Zwerger, H. J. Briegel, and W. Dür, *Sci. Rep.* **4**, 5364 (2014).
  - [32] W. J. Munro, A. M. Stephens, S. J. Devitt, K. A. Harrison, and K. Nemoto, *Nature Phot.* **6**, 777 (2012).
  - [33] S. Muralidharan, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, *Phys. Rev. Lett.* **112**, 250501 (2014).
  - [34] S. Muralidharan, C. L. Zou, L. Li, J. Wen, and L. Jiang, *New J. Phys.* **19**, 013026 (2017).
  - [35] F. Ewert, M. Bergmann, and P. van Loock, *Phys. Rev. Lett.* **117**, 210501 (2016).
  - [36] R. Namiki, L. Jiang, J. Kim, and N. Lütkenhaus, *Phys. Rev. A* **94**, 052304 (2016).
  - [37] A. N. Glaudell, E. Waks, and J. M. Taylor, *New Jour. of Phys.* **18**, 93008 (2016).
  - [38] E. Knill, *Nature (London)* **434**, 39 (2005).

- [39] D. Gottesman, *Chaos, Solitons & Fract.* **10**, 1749 (1999).
- [40] R. Cleve, D. Gottesman, and H.-K. Lo, *Phys. Rev. Lett.* **83**, 648 (1999).
- [41] C. H. Bennett, D. P. DiVincenzo, and J. A. Smolin, *Phys. Rev. Lett.* **78**, 3217 (1997).
- [42] L. Li, C.-L. Zou, V. V. Albert, S. Muralidharan, S. M. Girvin, and L. Jiang, *Phys. Rev. Lett.* **119**, 030502 (2017).
- [43] I. S. Reed and G. Solomon, *J. Soc. Industrial and Appl. Math* **8**, 300 (1960).
- [44] R. J. McEliece and D. V. Sarwate, *Communications of the ACM* **24**, 583 (1981).
- [45] S. B. Wicker and K. B. Vijay, *Reed-Solomon codes and their applications* (IEEE press, 1999).
- [46] M. Grassl, W. Geiselmann, and T. Beth, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. AAECC. Lecture Notes in Computer Science* p. 231 (1999).
- [47] Z. Li, L. J. Xing, and X. M. Wang, *Phys. Rev. A* **77**, 012308 (2008).
- [48] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, *IEEE transactions on information theory* **52**, 4892 (2006).
- [49] G. G. LaGuardia, *Phys. Rev. A* **80**, 042331 (2009).
- [50] G. G. LaGuardia, *Quant. Info. Proc.* **11**, 591 (2012).
- [51] S. Kullback and R. A. Leibler, *The Annals of Mathematical statistics* **22**, 79 (1951).
- [52] L. Sheridan and V. Scarani, *Phys. Rev. A* **82**, 030301 (2010).
- [53] E. Knill, *Nature* **434**, 39 (2005).
- [54] T. G. Tiecke, J. D. Thompson, N. P. de Leon, L. R. Liu, V. Vuletic, and M. D. Lukin, *Nature(London)* **508**, 241 (2014).
- [55] S. Kumar, R. Calderbank, and H. D. Pfister, *IEEE International Symposium on Information Theory (ISIT)* (2016).
- [56] J. M. Renes, F. Dupuis, and R. Renner, *Phys. Rev. Lett.* **109**, 050504 (2012).
- [57] We cannot claim classical Reed-Solomon codes to be capacity achieving on the classical erasure channel because we have a sequence of codes for various values of  $d$ . However, from our definition of QRSC, there exists a single code for a given value of  $d$ .