Quantum error correction assisted by two-way noisy communication

Zhuo Wang[1,2⋆], Sixia Yu[2,3⋆], Heng Fan[1⋆], C.H. Oh[2]

[1] *Institute of Physics, Chinese Academy of Sciences, Beijing 100190, China*

[2] *Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543*

[3] *Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics of University of Science and Technology of China, Hefei, Anhui 230026, China*

⋆*e-mail: wangzhuo@iphy.ac.cn; yusx@nus.edu.sg; hfan@iphy.ac.cn*

Supplemental Material

Non-binary quantum system. A p-level qudit is a particle with p dimensions defined on the ring $\mathbb{Z}_p = \{0, 1 \ldots, p-1\}$. The computational basis of the qudit is denoted by $\{|l\rangle | l \in \mathbb{Z}_p\}$, and the bit-shift and phase-shift operators are defined as

$$X = \sum_{l \in \mathbb{Z}_p} |l+1\rangle\langle l|, \quad Z = \sum_{l \in \mathbb{Z}_p} \omega^l |l\rangle\langle l|, \quad \left(\omega = e^{i\frac{2\pi}{p}}\right), \tag{1}$$

which satisfy $ZX = \omega XZ$ and $X^p = Z^p = I$. The group $\langle X, Z\rangle$ with X, Z being the generators forms an error basis of the qudit. Another important basis $\{|\theta_j\rangle | j \in \mathbb{Z}_p\}$ should be considered, which reads

$$|\theta_j\rangle = \frac{1}{\sqrt{p}} \sum_{l \in \mathbb{Z}_p} \omega^{-lj} |l\rangle, \tag{2}$$

leading to $X|\theta_j\rangle = \omega^j |\theta_j\rangle$ and $Z|\theta_j\rangle = |\theta_{j-1}\rangle$. In the theory of quantum error-correcting codes (QECCs), state $|\theta_0\rangle = \frac{1}{\sqrt{p}} \sum_{l \in \mathbb{Z}_p} |l\rangle$ is important because it is the initial state of all qudits prior to encoding except for the input qudits. In the binary case, $|\theta_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ is specially labeled by $|+\rangle$.

For a stabilizer QECC, three types of quantum gates are sufficient for forming the encoding circuit, i.e., the Hadamard gate, controlled-phase gate and controlled-NOT gate. The p-level Hadamard gate is defined as

$$H = \frac{1}{\sqrt{p}} \sum_{j,k \in \mathbb{Z}_p} \omega^{-jk} |j\rangle\langle k|. \tag{3}$$

The p-level controlled-phase gate is defined as

$$U_{CP} = \sum_{j,k \in \mathbb{Z}_p} \omega^{jk} |j, k\rangle\langle j, k|. \tag{4}$$

The p-level controlled-NOT gate is defined as

$$U_{CN} = \sum_{j,k\in\mathbb{Z}_p} |j, k + j\rangle\langle j, k| \tag{5}$$

with j indicating the source qudit and k indicating the target qudit.

Consider an n-qudit system. A $\mathbb{Z}_p$-weighted graph $G = (V, \Gamma)$ is composed of a set V of n vertices and a set of weighted edges specified by the *adjacency matrix* $\Gamma \in \mathbb{Z}_p^{n\times n}$, i.e., an $n \times n$ matrix with zero diagonal entries and the matrix element $\Gamma_{ab} \in \mathbb{Z}_p$ indicating the weight of the edge connecting vertices a and b. Denote by $\mathbb{Z}_p^V$ the set of all the vectors $\boldsymbol{s} = (s_1, s_2, \cdots, s_n)$ with n components $s_a \in \mathbb{Z}_p$ $(a \in V)$, then the graph state of this weighted graph reads

$$|\Gamma\rangle = \frac{1}{\sqrt{p^n}} \sum_{\boldsymbol{s}\in\mathbb{Z}_p^V} \omega^{\frac{1}{2}\boldsymbol{s}\cdot\Gamma\cdot\boldsymbol{s}}|\boldsymbol{s}\rangle = \prod_{a,b\in V} (\mathcal{U}_{ab})^{\Gamma_{ab}}|\theta_0\rangle^V, \tag{6}$$

in which $|\boldsymbol{s}\rangle$ is the computational basis of this system, $|\theta_0\rangle^V = |\theta_0\rangle_1 \otimes |\theta_0\rangle_2 \otimes \ldots |\theta_0\rangle_n$ and $\mathcal{U}_{ab}$ is the p-level controlled-phase gate U_{CP} between qudits a and b. Because $X_a^l\mathcal{U}_{ab} = Z_b^{-l}\mathcal{U}_{ab}X_a^l$ and $|\theta_0\rangle^V$ is the joint $+1$ eigenstate of X_a, $X_a|\Gamma\rangle = (\prod_{b\in V} Z_b^{-\Gamma_{ab}})|\Gamma\rangle$. Thus, for an error $X^{\boldsymbol{s}}Z^{\boldsymbol{t}}$ $(\boldsymbol{s}, \boldsymbol{t} \in \mathbb{Z}_p^V)$ of the n-qudit system,

$$X^{\boldsymbol{s}}Z^{\boldsymbol{t}}|\Gamma\rangle = \omega^{-\frac{1}{2}\boldsymbol{s}\cdot\Gamma\cdot\boldsymbol{s}}Z^{\boldsymbol{t}-\boldsymbol{s}\cdot\Gamma}|\Gamma\rangle, \tag{7}$$

indicating that any error acting on a graph state can be replaced by a phase error for some phase factors. Thus, the stabilizer group of this graph state containing n generators takes the following form:

$$\langle g_a := X_a \prod_{b\in V} Z_b^{\Gamma_{ab}} \big| a \in V\rangle \tag{8}$$

with any element written as

$$g^{\boldsymbol{s}} \equiv \prod_{a\in V} (g_a)^{s_a} = \omega^{\frac{1}{2}\boldsymbol{s}\cdot\Gamma\cdot\boldsymbol{s}} X^{\boldsymbol{s}} Z^{\boldsymbol{s}\cdot\Gamma}. \tag{9}$$

The evolution of quantum errors in quantum circuit. The evolution of quantum errors in the circuit depends on the transformation of errors through the quantum gates. For example, for a p-level controlled-NOT gate and an X error on the source qudit,

$$\begin{aligned} U_{CN}(X\otimes I)U_{CN}^{\dagger} &= \sum_{j,k\in\mathbb{Z}_p} |j,k+j\rangle\langle j,k| \cdot \sum_{j,k\in\mathbb{Z}_p} |j+1,k\rangle\langle j,k| \cdot \sum_{j,k\in\mathbb{Z}_p} |j,k-j\rangle\langle j,k| \\ &= \sum_{j,k\in\mathbb{Z}_p} |j+1,k+1\rangle\langle j,k| \\ &= X\otimes X, \end{aligned} \tag{10}$$

indicating that an X error on the source qudit through a controlled-NOT gate will be transformed into a two-qudit error $X\otimes X$. The transforming properties of the p-level quantum errors through the p-level quantum gates are listed in Table S1.

QECCs over mixed alphabets. A QECC over mixed alphabets is a code with different qudits being of different dimensions. We consider only a special 2-alphabet case denoted by $((n,K,d))_{(p^2)^{n_1}p^{n_2}}$, which means that the system is composed of n_1 p^2-level qudits and n_2 p-level qudits with $n_1+n_2=n$ to encode K logical states so that an arbitrary error on up to $\lfloor\frac{d-1}{2}\rfloor$ qudits can be corrected. The system can also be regarded as a p-level subsystem of n qudits, whose first n_1 qudits are combined with another p-level subsystem of n_1 qudits to form the p^2-level qudits. Hence,

$$\{\mathcal{E}\} = \{\mathcal{E}\otimes\mathcal{E}'\} = \{X^{\boldsymbol{s}\otimes\boldsymbol{s}'} Z^{\boldsymbol{t}\otimes\boldsymbol{t}'} \big| \boldsymbol{s},\boldsymbol{t}\in\mathbb{Z}_p^{\otimes n}, \boldsymbol{s}',\boldsymbol{t}'\in\mathbb{Z}_p^{\otimes n_1}\} \tag{11}$$

forms a nice error basis of the mixed-alphabet system. Given a $\mathbb{Z}_p$-weighted graph $G = (V+V_1, \Gamma)$ for these two subsystems, in which the $V_1 \subset V$ indicates the first n_1 vertices of a set V containing n vertices, then

$$\{Z^{\boldsymbol{c}\otimes\boldsymbol{c}'}|\Gamma\rangle\Big|\boldsymbol{c} \in \mathbb{Z}_p^V, \boldsymbol{c}' \in \mathbb{Z}_p^{V_1}\} \tag{12}$$

defines a basis of the mixed-alphabet system, and the stabilizers of the graph state $|\Gamma\rangle$ read

$$\langle g^{\boldsymbol{s}\otimes\boldsymbol{s}'} := X^{\boldsymbol{s}\otimes\boldsymbol{s}'} Z^{(\boldsymbol{s}\otimes\boldsymbol{s}')\cdot\Gamma}\Big|\boldsymbol{s} \in \mathbb{Z}_p^V, \boldsymbol{s}' \in \mathbb{Z}_p^{V_1}\rangle. \tag{13}$$

Any $(< d)$-bit error can be regarded as two errors on two subsystems, i.e.,

$$|\mathcal{E}| = |\mathcal{E} \cup \mathcal{E}'| = |\widehat{\boldsymbol{s}} \cup \widehat{\boldsymbol{t}} \cup \widehat{\boldsymbol{s}'} \cup \widehat{\boldsymbol{t}'}| < d, \tag{14}$$

in which $\widehat{\boldsymbol{s}} = \{j \in V | s_j \neq 0\}$ is the support of a vector $\boldsymbol{s} \in \mathbb{Z}_p^V$, and $|C|$ indicates the number of elements in $C \subseteq V$. Graph states have the advantage that any error can be replaced by a phases error, which allows us to introduce a *composite coding clique* for the mixed-alphabet system as follows.

We define the *d-uncoverable set* as

$$\mathbb{D}_d = \mathbb{Z}_p^V \otimes Z_p^{V_1} - \{(\boldsymbol{t} \otimes \boldsymbol{t}') - (\boldsymbol{s} \otimes \boldsymbol{s}') \cdot \Gamma\Big|0 < |\widehat{\boldsymbol{s}} \cup \widehat{\boldsymbol{t}} \cup \widehat{\boldsymbol{s}'} \cup \widehat{\boldsymbol{t}'}| < d\} \tag{15}$$

and the *d-purity set* as

$$\mathbb{S}_d = \{\boldsymbol{s} \otimes \boldsymbol{s}' \in \mathbb{Z}_p^V \otimes Z_p^{V_1}\Big||\widehat{\boldsymbol{s}} \cup \widehat{\boldsymbol{s} \cdot \Gamma} \cup \widehat{\boldsymbol{s}'} \cup \widehat{\boldsymbol{s}' \cdot \Gamma}| < d\}. \tag{16}$$

A composite coding clique $\mathbb{C}_d^K$ is a collection of K different vectors $\{\boldsymbol{c}_j \otimes \boldsymbol{c}'_j | j = 1, \cdots, K\}$ in $\mathbb{Z}_p^V \otimes Z_p^{V_1}$ that satisfy the following:

(i) $\mathbf{0} \in \mathbb{C}_d^K$;

(ii) $\boldsymbol{s} \cdot \boldsymbol{c} + \boldsymbol{s}' \cdot \boldsymbol{c}' = 0$ for all $\boldsymbol{s} \otimes \boldsymbol{s}' \in \mathbb{S}_d$ and $\boldsymbol{c} \otimes \boldsymbol{c}' \in \mathbb{C}_d^K$;

(iii) $(\boldsymbol{c}_j - \boldsymbol{c}_k) \otimes (\boldsymbol{c}'_j - \boldsymbol{c}'_k) \in \mathbb{D}_d$ for all $\boldsymbol{c}_j \otimes \boldsymbol{c}'_j, \boldsymbol{c}_k \otimes \boldsymbol{c}'_k \in \mathbb{C}_d^K$.

Then, the subspace spanned by the basis

$$\{Z^{\boldsymbol{c}\otimes\boldsymbol{c}'}|\Gamma\rangle \Big| \boldsymbol{c} \otimes \boldsymbol{c}' \in \mathbb{C}_d^K\} \tag{17}$$

defines a mixed-alphabet QECC $((n, K, d))_{(p^2)^{n_1}p^{n_2}}$, which comprises a stabilizer code if the composite coding clique $\mathbb{C}_d^K$ forms a group.

The construction of the 2WNC-assisted codes $[[4, 1, 3; \widetilde{1}]]_4$ **and** $[[2, \frac{1}{2}, 3; \widetilde{2}]]_4$**.** According to the method described, constructing a 2WNC-assisted QECC $[[4, 1, 3; \widetilde{1}]]_4$ is mathematically equivalent to constructing a mixed-alphabet stabilizer QECC $((6, 4, 3))_{4^4 2^2}$. This mixed-alphabet system can be regarded as the composite of a 6-qubit subsystem and a 4-qubit subsystem. Given a 2-weighted graph of 10 vertices $|\Gamma_{10}\rangle$, as shown in FIG. S1(A), the best composite coding clique is a group containing two generators that reads

$$\mathbb{C}_3^4 = \langle 111110 \otimes 0000, 000001 \otimes 1111\rangle. \tag{18}$$

Then, the subspace spanned by the basis $\{Z^{\boldsymbol{c}\otimes\boldsymbol{c}'}|\Gamma_{10}\rangle \Big| \boldsymbol{c} \otimes \boldsymbol{c}' \in \mathbb{C}_3^4\}$ defines a $((6, 4, 3))_{4^4 2^2}$ code. An 8-generator subgroup of the group $\langle g^{\boldsymbol{s}\otimes\boldsymbol{s}'} := X^{\boldsymbol{s}\otimes\boldsymbol{s}'} Z^{(\boldsymbol{s}\otimes\boldsymbol{s}')\cdot\Gamma_{10}} \Big| \boldsymbol{s} \in \mathbb{Z}_2^V, \boldsymbol{s}' \in \mathbb{Z}_2^{V_1}\rangle$, which commutes to the group $\langle Z^{\boldsymbol{c}\otimes\boldsymbol{c}'}\rangle$, forms the stabilizer of this code. Regarding vertices 5 and 6 in the figure as the "partially noisy" qudit 0, and vertices 1 and $1'$, 2 and $2'$, 3 and $3'$, 4 and 4' as qudits

1,2,3,4, respectively, then the subgroup becomes the stabilizer of the $[[4, 1, 3; \widetilde{1}]]_4$ code, as shown in Table I.

Constructing a 2WNC-assisted QECC $[[2, \frac{1}{2}, 3; \widetilde{2}]]_4$ is mathematically equivalent to constructing a mixed-alphabet stabilizer QECC $((6, 2, 3))_{4^2 2^4}$. This mixed-alphabets system can be regarded as the composite of a 6-qubit subsystem and a 2-qubit subsystem. Given a 2-weighted graph of 8 vertices $|\Gamma_8\rangle$, as shown in FIG. S1(B), the best composite coding clique is a group containing one generator that reads

$$\mathbb{C}_3^2 = \langle 011111 \otimes 11 \rangle. \tag{19}$$

Then, the basis $\{Z^{\boldsymbol{c}\otimes\boldsymbol{c}'}|\Gamma_8\rangle \big| \boldsymbol{c} \otimes \boldsymbol{c}' \in \mathbb{C}_3^2\}$ defines a $((6, 2, 3))_{4^2 2^4}$ code. A 7-generator subgroup of the group $\langle g^{\boldsymbol{s}\otimes\boldsymbol{s}'} := X^{\boldsymbol{s}\otimes\boldsymbol{s}'} Z^{(\boldsymbol{s}\otimes\boldsymbol{s}')\cdot\Gamma_8} \big| \boldsymbol{s} \in \mathbb{Z}_2^V, \boldsymbol{s}' \in \mathbb{Z}_2^{V_1}\rangle$, which commutes to the group $\langle Z^{\boldsymbol{c}\otimes\boldsymbol{c}'}\rangle$ forms the stabilizer of this code. Regarding vertices 3 and 4, 5 and 6 as the "partially noisy" qudits 0 and 1, respectively, and vertices 1 and 1', 2 and 2' as qudit 2 and 3, respectively, then the subgroup becomes the stabilizer of the $[[2, \frac{1}{2}, 3; \widetilde{2}]]_4$ code, as shown in Table II. The following list contains the syndromes of all single-bit errors for this code:

$$S(X_0) = 0100011, \quad S(Z_0) = 1000000, \quad S(Y_0) = 1100011,$$

$$S(X_0') = 0101011, \quad S(Z_0') = 0100000, \quad S(Y_0') = 0001011$$

$$S(X_1) = 0001101, \quad S(Z_1) = 0010000, \quad S(Y_1) = 0011101,$$

$$S(X_1') = 1111101, \quad S(Z_1') = 0001000, \quad S(Y_1') = 1110101$$

$$S(X_2) = 0110000, \quad S(Z_2) = 0000100, \quad S(Y_2) = 0110100,$$

$$S(X_2') = 1001000, \quad S(Z_2') = 0000010, \quad S(Y_2') = 1001010,$$

$$S(X_2X_2') = 1111000, \quad S(X_2Z_2') = 0110010, \quad S(X_2Y_2') = 1111010,$$

$$S(Z_2X_2') = 1001100, \quad S(Z_2Z_2') = 0000110, \quad S(Z_2Y_2') = 1001110,$$

$$S(Y_2X_2') = 1111100, \quad S(Y_2Z_2') = 0110110, \quad S(Y_2Y_2') = 1111110,$$

$$S(X_3) = 1010000, \quad S(Z_3) = 0000001, \quad S(Y_3) = 1010001,$$

$$S(X_3') = 0101000, \quad S(Z_3') = 1101111, \quad S(Y_3') = 1000111,$$

$$S(X_3X_3') = 1111000, \quad S(X_3Z_3') = 0111111, \quad S(X_3Y_3') = 0010111,$$

$$S(Z_3X_3') = 0101001, \quad S(Z_3Z_3') = 1101110, \quad S(Z_3Y_3') = 1000110,$$

$$S(Y_3X_3') = 1111001, \quad S(Y_3Z_3') = 0111110, \quad S(Y_3Y_3') = 0010110.$$

Technical details for bringing an encoding circuit into the standard form. In general, the encoding circuit of a mixed-alphabet stabilizer QECC is typically not in the standard form of the corresponding 2WNC-assisted QECC, namely, the encoding operator acts trivially on the idle qudits. Then how to bring it into the standard form after drawing the encoding circuit of the mixed-alphabet code?

First, move the controlled-phase gates U_{CP}, if there are any, between the idle qudits and the corresponding flying qudits to the beginning of the circuit. In the case of absence of a U_{CP} between one pair of idle and flying qudits, choose an arbitrary U_{CP} between the idle qudit and another qudit, which always exists, moving it to the beginning of the circuit and applying the transformation shown in FIG. S2(A). Then, a U_{CP} will act on the pair of idle and flying qudits.

Second, move all quantum gates acting on the idle qudits to the front of the circuit immediately after those U_{CP} gates. Note that the exchange of quantum gates may yield new quantum gates in the circuit; thus, care should be taken in the moving process.

Third, for each idle qudit, since U_{CP} exists between it and the flying qudit, apply the transformation shown in FIG. S2(B) to all other U_{CP} gates on it, and apply the transformation as shown in FIG. S2(C) to all the U_{CN} gates on it. Then, any quantum gate acting on this idle qudit could be replaced by another quantum gate acting on the corresponding flying qudit.

Finally, we are able to bring the encoding circuit into the standard form. Although all 2WNC-assisted codes we have constructed by now could get their circuits transformed into standard forms by using this algorithm, here we must declare that this algorithm has still not been proved to always work.

$Gate$	$Input$	$Output$
U_{CN}	X_1	$X_1 \otimes X_2$
	X_2	X_2
	Z_1	Z_1
	Z_2	$Z_1^\dagger \otimes Z_2$
U_{CP}	X_1	$X_1 \otimes Z_2$
	X_2	$Z_1 \otimes X_2$
	Z_1	Z_1
	Z_2	Z_2
H	X	$Z^\dagger$
	Z	X

Table S1: The transformation of the quantum errors through the quantum gates. Subscript "1" indicates the source qudit and subscript "2" indicates the target qudit.

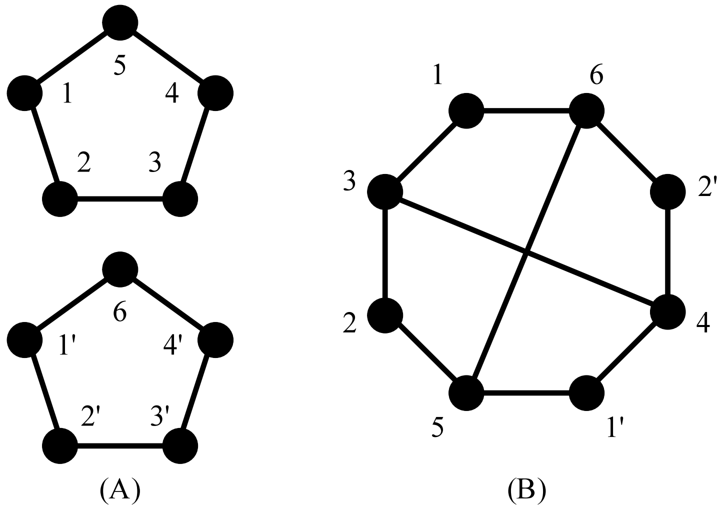

Figure S1: Graphs of the mixed-alphabet codes (A) $((6,4,3))_{4^4 2^2}$ **and (B)** $((6,2,3))_{4^2 2^4}$**.**

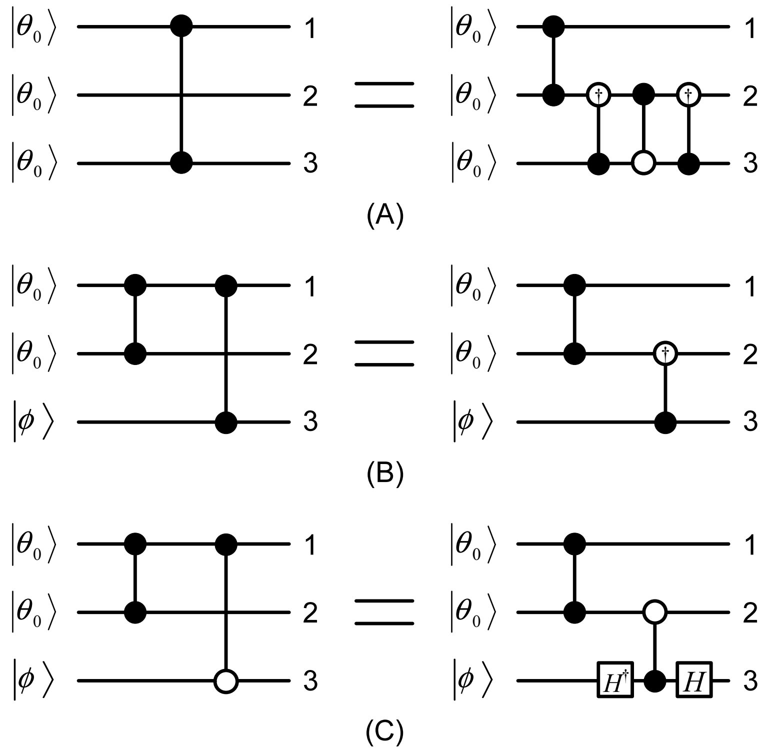

Figure S2: The transformation of the quantum gates. All qudits are of p levels; $|\phi\rangle$ is an arbitrary state; qudits 1,2, and 3 represent the idle qudit, the flying qudit, and a third qudit, respectively; the "†" represents the conjugate of the gates. (A), A U_{CP} between the idle and a third qudit can be replaced by a U_{CP} between the idle and the flying qudit and a swapping gate between the flying and the third qudit. (B), With the aid of U_{CP} between the idle and flying qudit, a U_{CP} between the idle and a third qudit can be replaced by a $U_{CN}^{\dagger}$ between the flying (target) and the third (source) qudit; (C), With the aid of U_{CP} between the idle and flying qudit, a U_{CN} between the idle (source) and a third (target) qudit can be replaced by a U_{CN} between the flying (target) and the third (source) qudit with two more Hadamard gates H and $H^{\dagger}$ on the third qudit.