Algebraic Quantum Error Correction Codes

Ming-Chung Tsai, Post doc., NTHU Kuan-Peng Chen, Assistant Researcher, NCHC, and Zheng-Yao Su

Abstract—A systematic and exhaustive method based on the group structure of a unitary Lie algebra is proposed to generate an enormous number of quantum codes. With respect to the algebraic structure, the orthogonality condition, which is the central rule of generating quantum codes, is proved to be fully equivalent to the distinguishability of the elements in this structure. In addition, four types of quantum codes are classified according to the relation of the codeword and the elements in this structure. In particular, the group structure of the Lie algebra su(2\(^p\)) is proved to be fully equivalent to the distinguishability of quantum codes in the set of the group structure of the Lie algebra su(2\(^p\)).

I. INTRODUCTION

When quantum information is transmitted or manipulated in noisy environments, the information gets lost gradually due to the beneficent interaction with the environment. To protect the fragile quantum states, error-correction codes are essential to safeguard the quantum data during the processes of quantum computation and communication. In this report, a systematic method based on the group structure of a unitary Lie algebra su(2\(^p\)), called quotient-algebra partition [1], is proposed to exhaustively generate quantum codes. According to the linking of the group structure in su(2\(^p\)) and admissible quantum codes, we are able to construct additive (stabilizer) quantum error correction codes as well as non-additive ones. Furthermore, the generated quantum codes can be classified into four types by relating the quantum states and codeword operators. We have found a new category of non-additive quantum error correction codes that is still under search by [2]. Of interest is that two types of these codes disclose their classical correspondences during the construction. The scheme introduced in this article helps the discovery of new types of quantum codes that may have higher efficiency or ability to error correction.

II. QUOTIENT-ALGEBRA PARTITION IN A UNITARY LIE ALGEBRA

A single qubit state can suffer three types of errors respectively represented by the Pauli matrices: the bit error \(\sigma_1 = |1\rangle\langle 1|\) or \(|0\rangle\langle 0|\), the phase error \(\sigma_2 = |1\rangle\langle 0| - |0\rangle\langle 1|\), and the bit-phase error \(\sigma_3 = -i|1\rangle\langle 1| + i|0\rangle\langle 0|\). For a p-qubit states, \(p \geq 1\), a set of \(N\) encountered errors \(\xi = \{E_0, E_1, \ldots, E_{N-1}\}\) is chosen from the set \(G = \{1, \sigma_1, \sigma_2, \sigma_3\}\) comprising all tensor products of p Pauli matrices, namely \(E_{0\leq i < N} = \sigma_{i_1} \otimes \sigma_{i_2} \cdots \otimes \sigma_{i_p} \in G\) for the identity \(I = \sigma_0\) and \(0 \leq i_1, i_2, \ldots, i_p \leq p\). Note that the operator \(I \otimes I \otimes \cdots \otimes I\) indicates that no errors occur. A quantum code, denoted as \([|p, K]\), is a subspace with the code length \(p\) and dimension \(K\) of the Hilbert space \(\mathcal{H}_{2p}\). We generate such codes in this section by investigating the structure of the Lie algebra su(2\(^p\)).

By writing all the 2\(^p\) generators (including the identity) of the Lie algebra su(2\(^p\)) in terms of the spinors in the set \(G\), the algebra su(2\(^p\)) forms a group under the multiplication. That is, a generator \(S = \sigma_{i_1} \otimes \sigma_{i_2} \otimes \cdots \sigma_{i_p}\) of su(2\(^p\)) is a tensor product of \(p\) Pauli matrices and \(S_1 \cdot S_2 = S_3 \in su(2p)\) for all \(S_1, S_2 \in su(2p)\), \(0 \leq i_1, i_2, \ldots, i_p \leq p\). Let the set \(\mathcal{E} = \{S_i : \forall S_i, S_j \in G, 0 \leq i, j \leq 2^p, [S_i, S_j] = S_i \cdot S_j - S_j \cdot S_i = 0\}\)

be a maximal abelian subalgebra of su(2\(^p\)), which is called the Cartan subalgebra and spanned by all the commuting spinors of \(G\). Up to the sign factor, it is easy to check that the subalgebra \(\mathcal{E}\) containing in total 2\(^3\) generators is a subgroup of su(2\(^p\)) under the same group operation, namely \(S_1 \cdot S_2 = S_3 \in \mathcal{E}\) for all \(S_1, S_2 \in \mathcal{E}\). An example of a Cartan subalgebra \(\mathcal{E}_0\) is shown in Fig. 1 which consists of all diagonal generators.

As described in [1], the subalgebra \(\mathcal{E}\) can generate a partition, denoted as \(\{\mathcal{P}(\xi)\}\), in su(2\(^p\)) consisting of 2\(^p\) subspaces \(\{W_i : i = 0, 1, \ldots, 2^p - 1\} \text{ and } \mathcal{W}_0 = \mathcal{E}\) satisfying the rule:

\[
\forall S_i \in W_i, S_j \in W_j, \exists l, s.t., S_i \cdot S_j = S_l \in W_l,
\]

for all \(0 \leq i, j, l < 2^p\). It is instructive to redenote the subscripts of these subspaces by \(p\)-digit binary strings of the additive group \(Z_2^p\). Thus the rule of Eq. 2 can be rephrased as:

\[
\forall S_i \in W_\zeta, S_j \in W_\eta, S_i \cdot S_j = S_l \in W_{\zeta + \eta},
\]

here \(\zeta, \eta\) being a \(p\)-digit binary string of the additive group \(Z_2^p\) under the bitwise addition and \(\mathcal{W}_0 = \mathcal{E}\). Under this notation, the isomorphism between the Lie algebra su(2\(^p\)) and the group can be rendered.

Theorem 1: The partition \(\{\mathcal{P}(\xi)\}\) generated by a Cartan subalgebra \(\mathcal{E}\) of the Lie algebra su(2\(^p\)) is isomorphic to the additive group \(Z_2^p\).

The detailed proof via a constructive procedure is made in [1]. The Cartan subalgebra \(\mathcal{E}\) is regarded as a "subgroup" and the subspace \(W_\zeta\) a "coset" of the partition \(\{\mathcal{P}(\xi)\}\).

As depicted in Fig. 1, the Cartan subalgebra \(\mathcal{E}_0\) uniquely can generate the quotient-algebra part partition \(\{\mathcal{P}(\xi)\}\) = \(\{W_\zeta : \zeta \in Z_2^3\}\) in the Lie algebra su(8). The generators of these eight subspaces \(W_\zeta, \zeta \in Z_2^3\), are related by the 3-digit binary strings. For instance, the multiplication \(I \otimes I \otimes I \otimes I = \sigma_0 \otimes I \otimes I \otimes I\) of the two spinors

\[
\sigma_1 \otimes \sigma_2 \cdots \otimes \sigma_p \in G
\]
\[ \mathcal{C}_0 = W_{000} = \{ I \otimes I \otimes I, \sigma_3 \otimes I \otimes I, I \otimes \sigma_3 \otimes I, I \otimes I \otimes \sigma_3, \sigma_3 \otimes I \otimes \sigma_3, I \otimes \sigma_3 \otimes \sigma_3, \sigma_3 \otimes \sigma_3 \otimes \sigma_3 \}; \]

\[ W_{001} = \{ I \otimes I \otimes \sigma_1, \sigma_3 \otimes I \otimes \sigma_1, I \otimes \sigma_3 \otimes \sigma_1, \sigma_3 \otimes I \otimes \sigma_1, I \otimes \sigma_3 \otimes \sigma_1, I \otimes \sigma_3 \otimes \sigma_1, I \otimes \sigma_3 \otimes \sigma_1, I \otimes \sigma_3 \otimes \sigma_1 \}; \]

\[ W_{010} = \{ I \otimes \sigma_1 \otimes I, \sigma_3 \otimes \sigma_1 \otimes I, I \otimes \sigma_2 \otimes I, \sigma_3 \otimes \sigma_2 \otimes I, I \otimes \sigma_3 \otimes \sigma_3, \sigma_3 \otimes \sigma_3 \otimes \sigma_3, \sigma_3 \otimes \sigma_3 \otimes \sigma_3 \}; \]

\[ W_{011} = \{ I \otimes \sigma_1 \otimes \sigma_1, I \otimes \sigma_2 \otimes \sigma_1, I \otimes \sigma_2 \otimes \sigma_1, I \otimes \sigma_1 \otimes \sigma_2, \sigma_3 \otimes \sigma_2 \otimes \sigma_1, \sigma_3 \otimes \sigma_2 \otimes \sigma_1, \sigma_3 \otimes \sigma_1 \otimes \sigma_2 \}; \]

\[ W_{100} = \{ \sigma_1 \otimes I \otimes I, \sigma_3 \otimes I \otimes I, \sigma_2 \otimes I \otimes I, \sigma_3 \otimes I \otimes I, \sigma_3 \otimes I \otimes I, \sigma_3 \otimes I \otimes I, \sigma_3 \otimes I \otimes I \}; \]

\[ W_{101} = \{ \sigma_1 \otimes I \otimes \sigma_1, \sigma_2 \otimes I \otimes \sigma_1, \sigma_2 \otimes I \otimes \sigma_1, \sigma_3 \otimes \sigma_2 \otimes \sigma_1, \sigma_3 \otimes \sigma_2 \otimes \sigma_1, \sigma_3 \otimes \sigma_1 \otimes \sigma_2 \}; \]

\[ W_{110} = \{ \sigma_1 \otimes \sigma_1 \otimes I, \sigma_2 \otimes \sigma_2 \otimes I, \sigma_2 \otimes \sigma_1 \otimes I, \sigma_1 \otimes \sigma_2 \otimes I, \sigma_1 \otimes \sigma_3 \otimes I, \sigma_2 \otimes \sigma_2 \otimes I, \sigma_2 \otimes \sigma_3 \otimes I, \sigma_1 \otimes \sigma_3 \otimes I \}; \]

\[ W_{111} = \{ \sigma_1 \otimes \sigma_1 \otimes \sigma_1, \sigma_2 \otimes \sigma_2 \otimes \sigma_1, \sigma_2 \otimes \sigma_2 \otimes \sigma_1, \sigma_2 \otimes \sigma_1 \otimes \sigma_1, \sigma_1 \otimes \sigma_2 \otimes \sigma_1, \sigma_2 \otimes \sigma_2 \otimes \sigma_1, \sigma_2 \otimes \sigma_1 \otimes \sigma_2, \sigma_1 \otimes \sigma_1 \otimes \sigma_2 \}; \]

**Fig. 1.** A partition generated by a Cartan subalgebra \( \mathcal{C}_0 \) of \( su(8) \).

**TABLE II**

**Error correction codes in classical and quantum regimes.**

<table>
<thead>
<tr>
<th>Classical Regime</th>
<th>Quantum Regime</th>
</tr>
</thead>
</table>
| A set of errors \( E = \{ \lambda_0, \lambda_1, \ldots, \lambda_{N-1} \} \subset \mathbb{Z}_N^P \). | A set of spinor errors \( E = \{ E_0, E_1, \ldots, E_{N-1} \} \subset su(2P) \), \( E_i \in \mathbb{W}_\lambda \), \( 0 \leq i < N \) and su(2P) = \( \bigcup_{\lambda \in \mathbb{Z}_N^P} \mathbb{W}_\lambda \).
| \[ [p, K] \] is a linear code if \( \{ \omega_m \} \) is a subgroup of \( \mathbb{Z}_N^P \). | A code \( [p, K] = \text{Span} \{ S_0|\psi_0\rangle, S_1|\psi_0\rangle, \ldots, S_{K-1}|\psi_0\rangle \} \) satisfying the condition \( E_i S_m|\psi_0\rangle \neq E_j S_m|\psi_0\rangle \), \( 0 \leq i, j < N \) and \( 0 \leq m, n < K \), can correct the error set \( E \). Here \( S_m \in \mathbb{W}_{\omega_m} \) for \( \omega_m \in \mathbb{Z}_N^2 \).
| \[ [p, K] \] is a nonlinear code if \( \{ \omega_m \} \) is not a subgroup of \( \mathbb{Z}_N^P \). | \[ [p, K] \] is a code of type-I if \( \bigcup_{\omega_m} \mathbb{W}_{\omega_m} \) is not a subgroup of \( su(2P) \).
| \[ [p, K] \] is a code of type-II if \( \bigcup_{\omega_m} \mathbb{W}_{\omega_m} \) is a subgroup of \( su(2P) \). |
$I \otimes \sigma_1 \otimes \sigma_1 \in W_{011}$ and $\sigma_1 \otimes \sigma_1 \otimes I \in W_{110}$ must belong to the subspace $W_{011+101} = W_{011}$. Thanks to the existence of the group structure in $su(2^p)$, a scheme can be designed to acquire quantum codes.

III. CONSTRUCTING QUANTUM CODES

For a given error set $E = \{E_0, E_1, \cdots, E_{N-1}\} \subset G$, a Cartan subalgebra $\mathfrak{c} \subset su(2^p)$ is chosen to generate a partition $\mathcal{P}(\mathfrak{c}) = \{W_\lambda : \forall \lambda \in Z_{R}^p\}$ in $su(2^p)$, such that the $N$ errors are distributed to $N$ different subspaces, namely $E_i \in W_{\lambda_i}$ and $\lambda_i \neq \lambda_j$ if $E_i \neq E_j$, here $0 \leq i < N$ and $E_0 = I^{\otimes p}$. Then an initial state

$$|\psi_0\rangle = \sum_{S \in \mathfrak{c}} S|00\cdots0\rangle \quad (4)$$

is produced by applying all the spinors of the Cartan subalgebra $\mathfrak{c}$ to the $p$-qubit zero state. Being a basis codeword, the initial state is a seed to search other codewords to generate the required code subspace. A set of $K$ codeword spinors

$$\mathcal{B} = \{S_0, I^{\otimes p}, S_1, \cdots, S_{K-1}\} \subset G, \quad (5)$$

respectively chosen from the $K$ subspaces, are applied to the initial state $|\psi_0\rangle$ to generate the set of $K$ states

$$BS = \{|\psi_r\rangle : 0 \leq r < K \} = \{|\psi_r\rangle = S_r|\psi_0\rangle : 0 \leq r < K\}. \quad (6)$$

The set $BS$ comprising $K$ basis codewords forms a generating set of a code subspace $[p, K]$ with the length $p$ and dimension $K$. As long as a Cartan subalgebra $\mathfrak{c}$ is chosen, a unique partition $\mathcal{P}(\mathfrak{c})$ is generated and there produce an enormous number of quantum codes.

**Theorem 2:** Every Cartan subalgebra of the Lie algebra $su(2^p)$ can decide quantum codes $[[p, K]]$ with the code length $p$ and dimension $0 < K < 2^p$.

An implication of this theorem is that, for a given error set, one can always find its error-correction code by choosing appropriate Cartan subalgebra; referring [3] for the more detail.

The corrupted state

$$|\psi_{ij}\rangle = E_i|\psi_j\rangle = E_i \cdot S_j|\psi_0\rangle \quad (7)$$

is produced by applying the error operator $E_i$ to a basis codeword $|\psi_j\rangle = S_j|\psi_0\rangle$, $0 \leq i < N$ and $0 \leq j < K$. We say that the code $[[p, K]]$ has the ability to correct the error set $E$ if

$$W_{r_1} \not\subset W_{r_2} \text{ for any } E_{i_1} \cdot S_{j_1} \in W_{r_1} \text{ and } E_{i_2} \cdot S_{j_2} \in W_{r_2}. \quad (8)$$

here $0 \leq i_1, i_2 < N$, $0 \leq j_1, j_2 < K$ and $r_1, r_2 \in Z_{R}^p$. Each corrupted state indicates a syndrome during the process of error-correction and the result of Eq. 8 implies that all the syndromes are distinguishable. There have in total $MN$ syndromes listed here and the code $[[p, K]]$ obeys the so-called quantum Hamming bound $MN \leq 2^p$.

Up to the normalization, the state $|\psi_0\rangle = |000\rangle$ is the initial state created by applying the spinors of the Cartan subalgebra $\mathfrak{c}_0$ in Fig. 1. By selecting any spinor in the subspace $W_{111}$ as a codeword spinor, say $\sigma_1 \otimes \sigma_1 \otimes \sigma_1$, another basis codeword $|\psi_1\rangle = \sigma_1 \otimes \sigma_1 \otimes \sigma_1|\psi_{00}\rangle = |111\rangle$ is produced. The set $\{|\psi_0\rangle = |000\rangle, |\psi_1\rangle = |111\rangle\}$ is a basis to generate a quantum code $[[3, 2]]$ with the length 3 and dimension 2, which can correct an error set such as $E = \{I \otimes \sigma_1, \sigma_1 \otimes I, \sigma_1 \otimes \sigma_1\}$. In fact, this code can correct any error set that comprises three spinors from the subspaces $W_{001}, W_{110}$ and $W_{100}$ respectively.

IV. CLASSIFICATION OF QUANTUM CODES

Following the procedure of construction in the last section, a basis codeword is created by applying a codeword spinor to an initial state. Since a Cartan subalgebra $\mathfrak{c}$ is a subgroup of $su(2^p)$ under the multiplication, the set of strings $C = \{\alpha_r \in Z_{R}^p : r = 0, 1, \cdots, 2^p - 1\}$ for the initial state $|\psi_0\rangle = \sum_{S \in \mathfrak{c}} S|00\cdots0\rangle = \sum_{r=1}^{2^p} (-1)^r |\alpha_r\rangle$ as of Eq. 4 forms a subgroup of the additive group $Z_{2^p}$ for a fixed initial state, there produce two types of quantum codes according to whether or not the set of codeword spinors $\mathcal{B}$ is a subgroup of $su(2^p)$ under the multiplication. Yet for a fixed $\mathcal{B}$, there admit the other two types of quantum codes. It is instructive to classify the generated quantum codes by the different options of $|\psi_0\rangle$ and $\mathcal{B}$, as shown in Table I.

<table>
<thead>
<tr>
<th>Type</th>
<th>B</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>$I$</td>
<td>g</td>
<td>additive</td>
</tr>
<tr>
<td>$II$</td>
<td>g</td>
<td>nonadditive</td>
</tr>
<tr>
<td>$III$</td>
<td>n.g</td>
<td>nonadditive</td>
</tr>
<tr>
<td>$IV$</td>
<td>n.g</td>
<td>nonadditive</td>
</tr>
</tbody>
</table>

Four types of quantum codes are generated. The quantum code of type-$I$ in Table I, which is an additive code (stabilizer code), corresponds to both $B$ and $C$ being a subgroup of $Z_{2^p}$ and $\mathcal{P}(\mathfrak{c})$ respectively. The remaining codes are nonadditive codes. For the code of type-$II$, the set $B$ is not a subgroup but $C$ is. The set $B$ is a subgroup yet $C$ is not for the code of type-$III$. Neither of $B$ and $C$ is a subgroup in the last type of code. It is noted that the codes like type-$III$ or type-$IV$ are the new categories that have never been discovered so far [2].

V. CLASSICAL CORRESPONDENCES OF QUANTUM CODES

The quantum codes of types $I$ and $II$ have obvious classical correspondences, as shown in Table II in Appendix A. The former type refers to the classical linear code and the latter to the nonlinear one. Both the type-$I$ and type-$II$ codes are created by a set of codeword spinors $\mathcal{B} = \{S_m \in su(2^p) : 0 \leq m < K\}$ in $su(2^p)$, $0 \leq t \leq p$, and by an initial state $|\psi_0\rangle = \sum_{\alpha_r} (-1)^r |\alpha_r\rangle$ whose strings is a subgroup $C = \{\alpha_r : 0 \leq r < 2^p\}$ in $Z_{2^p}$. Each codeword spinor $S_m$ is included in a subspace $W_{\omega_m}$, $\omega_m \in Z_{2^p}$, of the partition $\mathcal{P}(\mathfrak{c})$ generated by a Cartan subalgebra $\mathfrak{c} \subset su(2^p)$. Owing to the isomorphism of the partition $\mathcal{P}(\mathfrak{c})$ and the additive group $Z_{2^p}$ by Theorem 1, the behavior of the subspaces $W_{\omega_m}$ in $\mathcal{P}(\mathfrak{c})$ is equivalent to that of the strings $\omega_m$ in $Z_{2^p}$.
Since the subspaces \( \{W_{\omega m}\} \) for the quantum code of type-I is a subgroup of \( \{P(4)\} \), the set of strings \( \{\omega_m\} \) is a subgroup of \( Z_p^p \). This indicates this type of quantum code has a linear correspondence in classical codes. While the subspaces \( \{W_{\omega m}\} \) for the code of type-II is not a subgroup of \( \{P(4)\} \) and the set of strings \( \{\omega_m\} \) is not a subgroup of \( Z_p^p \). A such type of quantum code thus has a nonlinear correspondence in classical regime.

VI. CONCLUSION

With the group structure of the Lie algebra \( su(2^p) \), we can design a scheme to systematically generate an exhaustive set of quantum codes \([p, K]\) with the code length \( p \) and dimension \( 1 \leq K \leq 2^p \). In addition, we classify these generated quantum codes according to the relations of codeword spinors and a given initial quantum state. New types of quantum codes can be discovered for the purpose of searching higher efficient quantum codes.

REFERENCES


APPENDIX

A figure and a table are listed in next page. The figure (Fig. 1) is a partition of the Lie algebra \( su(8) \), a 3-qubit system. The 64 generators of \( su(8) \) are divided into eight disjoint subspaces by the subgroup, a Cartan subalgebra \( \mathfrak{c}_0 \). These disjoint subspaces are related by the binary strings of the additive group \( Z_2^3 \) and there reveals the isomorphism of the partition and \( Z_2^3 \). The table (Table I) demonstrates the comparison of the quantum codes and classical codes.