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 operators and some initial quantum state. By linking the unitary Lie algebra with the additive group, the classical correspondences of some of these quantum codes can be rendered.

Keywords—Quotient-Algebra Partition, Codeword Spinors, Basis Codewords, Syndrome Spinors

I. INTRODUCTION

WHEN quantum information is transmitted or manipulated in noisy environments, the information gets lost gradually due to the baneful 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 $σ_1 = |0⟩⟨1| + |1⟩⟨0|$, phase error $σ_3 = |0⟩⟨0| - |1⟩⟨1|$ and bit-phase error $σ_2 = -i|0⟩⟨1| + i|1⟩⟨0|$. For a $p$-qubit states, $p ≥ 1$, a set of $N$ encountered errors $ɛ = \{E_0, E_1, \ldots, E_{N-1}\}$ is chosen from the set $G = \{I, σ_1, σ_2, σ_3^{⊗p}\}$ comprising all tensor products of $p$ Pauli matrices, namely $0 ≤ N ≤ p^q$.

Ming-Chung Tsai and Zheng-Yao Su are with the Department of Physics, National Tsing Hua University, Hsinchu, 30076 Taiwan, e-mail: suzertsaigoo@gmail.com.

Kuan-Peng Chen, and Zheng-Yao Su are with the Applied Scientific Computing Division, National Center for High-Performance Computing, Hsinchu, 30076 Taiwan.
Fig. 1. A partition generated by a Cartan subalgebra $\mathfrak{c}_0$ of $su(8)$.

$\mathfrak{c}_0 = W_{000} = \{I \otimes I \otimes I, \sigma_3 \otimes I \otimes I, I \otimes \sigma_3 \otimes I, I \otimes I \otimes \sigma_3, I \otimes I \otimes I, I \otimes I \otimes I, I \otimes I \otimes I, I \otimes I \otimes I\}$;

$W_{001} = \{I \otimes I \otimes \sigma_1, \sigma_3 \otimes I \otimes \sigma_1, I \otimes I \otimes \sigma_2, \sigma_3 \otimes I \otimes \sigma_2, I \otimes \sigma_3 \otimes \sigma_1, I \otimes \sigma_3 \otimes \sigma_2, \sigma_3 \otimes \sigma_3 \otimes \sigma_2\}$;

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

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

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

$W_{101} = \{I \otimes \sigma_1 \otimes I, \sigma_2 \otimes I \otimes \sigma_2, \sigma_2 \otimes I \otimes \sigma_1, I \otimes \sigma_1 \otimes \sigma_2, I \otimes \sigma_1 \otimes \sigma_2, I \otimes \sigma_1 \otimes \sigma_2, I \otimes \sigma_1 \otimes \sigma_2\}$;

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

$W_{111} = \{I \otimes \sigma_1 \otimes \sigma_1, I \otimes \sigma_2 \otimes \sigma_2, I \otimes \sigma_2 \otimes \sigma_2, I \otimes \sigma_2 \otimes \sigma_2, \sigma_3 \otimes \sigma_2 \otimes \sigma_2, \sigma_3 \otimes \sigma_2 \otimes \sigma_2, \sigma_3 \otimes \sigma_2 \otimes \sigma_2\}$

---

### TABLE II

<table>
<thead>
<tr>
<th>Classical Regime</th>
<th>Quantum Regime</th>
</tr>
</thead>
<tbody>
<tr>
<td>A set of errors $E = {\lambda_0, \lambda_1, \cdots, \lambda_{N-1}} \subset \mathbb{Z}_N^p$.</td>
<td>A set of spinor errors $E = {E_0, E_1, \cdots, E_{N-1}} \subset su(2^p)$, $E_i \in \mathcal{W}<em>\lambda$, $0 \leq i &lt; N$ and $su(2^p) = \bigcup</em>{\lambda \in \mathbb{Z}<em>2^p} \mathcal{W}</em>\lambda$.</td>
</tr>
<tr>
<td>A code $[p, K] = {\omega_0, \omega_1, \cdots, \omega_{K-1}}$ satisfying the condition $\lambda_i + \omega_m \neq \lambda_j + \omega_n$, $0 \leq i, j &lt; N$ and $0 \leq m, n &lt; K$, can correct the error set $E$.</td>
<td>A code $[[p, K]] = \text{Span}{S_0</td>
</tr>
<tr>
<td>$[p, K]$ is a linear code if ${\omega_m}$ is a subgroup of $\mathbb{Z}_2^p$.</td>
<td>$[p, K]$ is a code of type-I if $\bigcup_{\omega_m} \mathcal{W}_{\omega_m}$ is a subgroup of $su(2^p)$.</td>
</tr>
<tr>
<td>$[p, K]$ is a nonlinear code if ${\omega_m}$ is not a subgroup of $\mathbb{Z}_2^p$.</td>
<td>$[p, K]$ is a quantum code of type-II if $\bigcup_{\omega_m} \mathcal{W}_{\omega_m}$ is not a subgroup of $su(2^p)$.</td>
</tr>
</tbody>
</table>
$I \otimes \sigma_1 \otimes \sigma_1 \in \mathcal{W}_{011}$ and $\sigma_1 \otimes \sigma_1 \otimes I \in \mathcal{W}_{110}$ must belong to the subspace $\mathcal{W}_{011+100} = \mathcal{W}_{101}$. 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 $\mathcal{E} = \{E_0, E_1, \ldots, E_{N-1}\} \subset G$, a Cartan subalgebra $\mathcal{C} \subset su(2^p)$ is chosen to generate a partition $\{P(\mathcal{C})\} = \{\mathcal{W}_\lambda : \forall \lambda \in Z^p_2\}$ in $su(2^p)$, such that the $N$ errors are distributed to $N$ different subspaces, namely $E_i \in \mathcal{W}_{\lambda_i}$ 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

$$|\psi_0\rangle = \sum_{\mathcal{S} \in \mathcal{E}} S|00\cdots 0\rangle \quad (4)$$

is produced by applying all the spinors of the Cartan subalgebra $\mathcal{C}$ to the $p$-qubit zero state. Being a basis codeword, the initial state is 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, \ldots, S_{K-1}\} \subset G,$n

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

$$\mathcal{B}S = \{|\psi_r\rangle : 0 \leq r < K\} = \{|\psi_r\rangle = S_r|\psi_0\rangle : 0 \leq r < K\}. \quad (5)$$

The set $B_0$ 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 $\mathcal{C}$ is given, a unique partition $\{P(\mathcal{C})\}$ 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 $0 < K \leq 2^p$.

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

$$|\psi_f\rangle = E_i|\psi_i\rangle = E_i \cdot S_j|\psi_0\rangle \quad (7)$$

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 $\mathcal{E}$ if

$$\mathcal{W}_{\tau_1} \neq \mathcal{W}_{\tau_2} \quad \text{for any} \quad E_{i_1} \cdot S_j \in \mathcal{W}_{\tau_1} \quad \text{and} \quad E_{i_2} \cdot S_j \in \mathcal{W}_{\tau_2} \quad (8)$$

here $0 \leq i_1, i_2 < N$, $0 \leq j_1, j_2 < K$ and $\tau_1, \tau_2 \in Z^p_2$.

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 $\mathcal{C}_0$ in Fig. 1. By selecting any spinor in the subspace $\mathcal{W}_{111}$ as a codeword spinor, say $\sigma_1 \otimes \sigma_1 \otimes \sigma_1$, another basis codeword $|\psi_1\rangle = \sigma_1 \otimes \sigma_1 \otimes \sigma_1|\psi_0\rangle = |111\rangle$ 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 $\mathcal{E} = \{I \otimes I \otimes \sigma_1, \sigma_1 \otimes I, \sigma_1 \otimes I \otimes I\}$. In fact, this code can correct any error set that comprises three spinors from the subspaces $\mathcal{W}_{001}, \mathcal{W}_{110}$ and $\mathcal{W}_{100}$ 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 $\mathcal{C}$ is a subgroup of $su(2^p)$ under the multiplication, the set of strings $C = \{\alpha_r \in Z^p_2 ; r = 0, 1, \ldots, 2^p - 1\}$ for the initial state $|\psi_0\rangle = \sum_{\mathcal{S} \in \mathcal{E}} S|00\cdots 0\rangle = \sum_{r=1}^{2^p} (-1)^r|\alpha_r\rangle$ as of Eq. 4 forms a subgroup of the additive group $Z^p_2$. 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>
<th>Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>g</td>
<td>g</td>
<td>additive</td>
</tr>
<tr>
<td>II</td>
<td>g</td>
<td>n.g.</td>
<td>nonadditive</td>
</tr>
<tr>
<td>III</td>
<td>g</td>
<td>n.g.</td>
<td>nonadditive</td>
</tr>
<tr>
<td>IV</td>
<td>n.g.</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 $Z^p_2$ and $P(\mathcal{C})$ 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 $|\psi_0\rangle = \sum_{\alpha \in Z^p_2} (-1)^t|\alpha\rangle$ whose strings is a subgroup $C = \{\alpha_r ; 0 \leq r < 2^k\}$ in $Z^p_2$. Each codeword spinor $S_m$ is included in a subspace $\mathcal{W}_{\omega_m}$, $\omega_m \in Z^p_2$. By Theorem 1, the behavior of the subspaces $\mathcal{W}_{\omega_m}$ in $\{P(\mathcal{C})\}$ is equivalent to that of the strings $\omega_m$ in $Z^p_2$. 

---

This text is from an academic paper discussing quantum codes and their classifications, focusing on the construction of quantum codes from Cartan subalgebras, and the implications of these constructions on the classification of quantum codes. It also includes a table summarizing the types of quantum codes and their classical correspondences.
Since the subspaces \( \{W_{\omega_m}\} \) for the quantum code of type-I is a subgroup of \( \{P(\mathfrak{C})\} \), the set of strings \( \{\omega_m\} \) is a subgroup of \( \mathbb{Z}_2^p \). 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 \( \{P(\mathfrak{C})\} \) and the set of strings \( \{\omega_m\} \) is not a subgroup of \( \mathbb{Z}_2^p \). 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 \( \mathbb{Z}_2^3 \) and there reveals the isomorphism of the partition and \( \mathbb{Z}_2^3 \). The table (Table I) demonstrates the comparison of the quantum codes and classical codes.