World Academy of Science, Engineering and Technology
International Journal of Nuclear and Quantum Engineering
Vol:6, No:3, 2012

Algebraic Quantum Error Correction Codes

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

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 $\sigma_1 = |0\rangle\langle 1| + |1\rangle\langle 0|$, phase error $\sigma_3 = |0\rangle\langle 0| - |1\rangle\langle 1|$ and bit-phase error $\sigma_2 = -i|0\rangle\langle 1| + i|1\rangle\langle 0|$. For a p-qubit states, $p \geq 1$, a set of N encountered errors $\mathcal{E} = \{E_0, E_1, \cdots, E_{N-1}\}$ is chosen from the set $G = \{I, \sigma_1, \sigma_2, \sigma_3\}^{\otimes p}$ comprising all tensor products of p Pauli matrices, namely $E_{0\leq r<N} = \sigma_{i_1} \otimes \sigma_{i_2} \otimes \cdots \otimes \sigma_{i_p} \in G$ for the identity $I = \sigma_0$ and $0 \leq i_1, i_2, \cdots, i_p \leq p$. 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 $\mathcal{H}_{2^p}$. We generate such codes in this section by investigating the structure of the Lie algebra $su(2^p)$.

By writing all the 2^{2p} 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 $S_1 \cdot S_2 = S_3 \in su(2^p)$ for all $S_1, S_2 \in su(2^p)$, $0 \leq i_1, i_2, \cdots, i_p \leq p$. Let the set

$$\mathfrak{C} = \{S_i : \forall\, S_i, S_j \in G, 0 \leq i, j < 2^p, \\ [S_i, S_j] = S_i \cdot S_j - S_j \cdot S_i = 0\} \quad (1)$$

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 $\mathfrak{C}$ containing in total 2^p generators is a subgroup of $su(2^p)$ under the same group operation, namely $S_1 \cdot S_2 = S_3 \in \mathfrak{C}$ for all $S_1, S_2 \in \mathfrak{C}$. An example of a Cartan subalgebra $\mathfrak{C}_0$ is shown in Fig. 1 which consists of all diagonal generators.

As described in [1], the subalgebra $\mathfrak{C}$ can generate a partition, denoted as $\{\mathcal{P}(\mathfrak{C})\}$, in $su(2^p)$ consisting of 2^p subspaces $\{\mathcal{W}_i; i = 0, 1, \cdots, 2^p - 1$ and $\mathcal{W}_0 = \mathfrak{C}\}$ satisfying the rule:

$$\forall\, S_1 \in \mathcal{W}_i, S_2 \in \mathcal{W}_j,\ \exists!\, l, s.t., S_1 \cdot S_2 = S_3 \in \mathcal{W}_l, \quad (2)$$

here $0 \leq i, j, l < 2^p$. It is instructive to redenoting 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,

$$\forall\, S_1 \in \mathcal{W}_\zeta, S_2 \in \mathcal{W}_\eta,\ S_1 \cdot S_2 = S_3 \in \mathcal{W}_{\zeta+\eta}, \quad (3)$$

here ζ, η being a p-digit binary string of the additive group Z_2^p under the bitwise addition and $\mathcal{W}_\mathbf{0} = \mathfrak{C}$. Under this notation, the *isomorphism* between the Lie algebra $su(2^p)$ and the group can be rendered.

Theorem 1: The partition $\{\mathcal{P}(\mathfrak{C})\}$ generated by a Cartan subalgebra $\mathfrak{C}$ 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 $\mathfrak{C}$ is regarded as a "subgroup" and the subspace $\mathcal{W}_\zeta$ a "coset" of the partition $\{\mathcal{P}(\mathfrak{C})\}$.

As depicted in Fig. 1, the Cartan subalgebra $\mathfrak{C}_0$ uniquely can generate the quotient-algebra part partition $\{\mathcal{P}(\mathfrak{C})\} = \{\mathcal{W}_\zeta; \zeta \in Z_2^3\}$ in the Lie algebra $su(8)$. The generators of these eight subspaces $\mathcal{W}_\zeta$, $\zeta \in Z_2^3$, are related by the 3-digit binary strings. For instance, the multiplication $I \otimes \sigma_1 \otimes \sigma_1 \cdot \sigma_1 \otimes \sigma_1 \otimes I = \sigma_1 \otimes I \otimes \sigma_1$ of the two spinors

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

$$\begin{aligned}
\mathfrak{C}_0 =&\mathcal{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\sigma_3\otimes I, \sigma_3\otimes I\otimes\sigma_3, I\otimes\sigma_3\otimes\sigma_3, \sigma_3\otimes\sigma_3\otimes\sigma_3\};\\
&\mathcal{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, \sigma_3\otimes\sigma_3\otimes\sigma_1, I\otimes\sigma_3\otimes\sigma_2, \sigma_3\otimes\sigma_3\otimes\sigma_2\};\\
&\mathcal{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, \sigma_3\otimes\sigma_1\otimes\sigma_3, I\otimes\sigma_2\otimes\sigma_3, \sigma_3\otimes\sigma_2\otimes\sigma_3\};\\
&\mathcal{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_1, \sigma_3\otimes\sigma_1\otimes\sigma_2\};\\
&\mathcal{W}_{100} = \{\sigma_1\otimes I\otimes I, \sigma_1\otimes\sigma_3\otimes I, \sigma_2\otimes I\otimes I, \sigma_2\otimes\sigma_3\otimes I, \sigma_1\otimes I\otimes\sigma_3, \sigma_1\otimes\sigma_3\otimes\sigma_3, \sigma_2\otimes I\otimes\sigma_3, \sigma_2\otimes\sigma_3\otimes\sigma_3\};\\
&\mathcal{W}_{101} = \{\sigma_1\otimes I\otimes\sigma_1, \sigma_2\otimes I\otimes\sigma_2, \sigma_2\otimes I\otimes\sigma_1, \sigma_1\otimes I\otimes\sigma_2, \sigma_1\otimes\sigma_3\otimes\sigma_1, \sigma_2\otimes\sigma_3\otimes\sigma_2, \sigma_2\otimes\sigma_3\otimes\sigma_1, \sigma_1\otimes\sigma_3\otimes\sigma_2\};\\
&\mathcal{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_1\otimes\sigma_3, \sigma_2\otimes\sigma_2\otimes\sigma_3, \sigma_2\otimes\sigma_1\otimes\sigma_3, \sigma_1\otimes\sigma_2\otimes\sigma_3\};\\
&\mathcal{W}_{111} = \{\sigma_1\otimes\sigma_1\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_1\otimes\sigma_2, \sigma_1\otimes\sigma_2\otimes\sigma_2, \sigma_1\otimes\sigma_1\otimes\sigma_2, \sigma_2\otimes\sigma_2\otimes\sigma_2\}
\end{aligned}$$

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

TABLE II
ERROR CORRECTION CODES IN CLASSICAL AND QUANTUM REGIMES.

Classical Regime	Quantum Regime
A set of errors $\mathcal{E} = \{\lambda_0, \lambda_1, \cdots, \lambda_{N-1}\} \subset Z_2^p$.	A set of spinor errors $E = \{E_0, E_1, \cdots, E_{N-1}\} \subset su(2^p)$, $E_i \in \mathcal{W}_{\lambda_i}$, $0 \le i < N$ and $su(2^p) = \bigcup_{\lambda\in Z_2^p} \mathcal{W}_\lambda$.
A code $[p, K] = \{\omega_0, \omega_1, \cdots, \omega_{K-1}\}$ satisfying the condition $\lambda_i + \omega_m \neq \lambda_j + \omega_n$, $0 \le i, j < N$ and $0 \le m, n < K$, can correct the error set $\mathcal{E}$.	A code $[[p, K]] = Span\{S_0\|\psi_0\rangle, S_1\|\psi_0\rangle, \cdots, S_{K-1}\|\psi_0\rangle\}$ satisfying the condition $E_iS_m\|\psi_0\rangle \neq E_jS_n\|\psi_0\rangle$, $0 \le i, j < N$ and $0 \le m, n < K$, can correct the error set $\mathcal{E}$, here $S_m \in \mathcal{W}_{\omega_m}$ for $\omega_m \in Z_2^p$.
$[p, K]$ is a linear code if $\{\omega_m\}$ is a subgroup of Z_2^p.	$[[p, K]]$ is a code of type-I if $\bigcup_{\omega_m} \mathcal{W}_{\omega_m}$ is a subgroup of $su(2^p)$.
$[p, K]$ is a nonlinear code if $\{\omega_m\}$ is not a subgroup of Z_2^p.	$[[p, K]]$ is a quantum code of type-II if $\bigcup_{\omega_m} \mathcal{W}_{\omega_m}$ is not a subgroup of $su(2^p)$.

$I \otimes \sigma_1 \otimes \sigma_1 \in \mathcal{W}_{011}$ and $\sigma_1 \otimes \sigma_1 \otimes I \in \mathcal{W}_{110}$ must belong to the subspace $\mathcal{W}_{011+101} = \mathcal{W}_{101}$. 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 $\mathcal{E} = \{E_0, E_1, \cdots, E_{N-1}\} \subset G$, a Cartan subalgebra $\mathfrak{C} \subset su(2^p)$ is chosen to generate a partition $\{\mathcal{P}(\mathfrak{C})\} = \{\mathcal{W}_\lambda : \forall\, \lambda \in Z_2^p\}$ 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

$$|\psi_0\rangle = \sum_{S \in \mathfrak{C}} S|00\cdots 0\rangle \tag{4}$$

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*

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

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

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

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 given, 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 $0 < K \leq 2^p$.

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*

$$|\psi_{ij}\rangle = E_i|\psi_j\rangle = E_i \cdot S_j|\psi_0\rangle \tag{7}$$

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

$$\mathcal{W}_{\tau_1} \neq \mathcal{W}_{\tau_2} \text{ for any } E_{i_1} \cdot S_{j_1} \in \mathcal{W}_{\tau_1} \text{ and } E_{i_2} \cdot S_{j_2} \in \mathcal{W}_{\tau_2}, \tag{8}$$

here $0 \leq i_1, i_2 < N$, $0 \leq j_1, j_2 < K$ and $\tau_1, \tau_2 \in Z_2^p$. 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 $\mathcal{W}_{111}$ 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 $\mathcal{W}_{001}$, $\mathcal{W}_{010}$ 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 $\mathfrak{C}$ is a subgroup of $su(2^p)$ under the multiplication, the set of strings $C = \{\alpha_r \in Z_2^p; r = 0, 1, \cdots, 2^k - 1\}$ for the initial state $|\psi_0\rangle = \sum_{S \in \mathfrak{C}} S|00\cdots 0\rangle = \sum_{r=1}^{2^k} (-1)^{\epsilon_r} |\alpha_r\rangle$ 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 I
The classification of quantum codes generated by the scheme in this report; here g. (n.g.) indicates that $\mathcal{B}$ and C are (not) a subgroup of Lie algebra $su(2^p)$ and the additive group Z_2^p respectively.

Type	$\mathcal{B}$	C	
I	g.	g.	additive
II	n.g.	g.	nonadditive
III	g.	n.g.	nonadditive
IV	n.g.	n.g.	nonadditive

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 C and $\mathcal{B}$ 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 $\mathcal{B}$ is not a subgroup but C is. The set $\mathcal{B}$ is a subgroup yet C is not for the code of *type-III*. Neither of $\mathcal{B}$ 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 $|\psi_0\rangle = \sum_{r=1}^{2^k} (-1)^{\epsilon_r} |\alpha_r\rangle$ whose strings is a subgroup $C = \{\alpha_r; 0 \leq r < 2^k\}$ in Z_2^p. Each codeword spinor S_m is included in a subspace $\mathcal{W}_{\omega_m}$, $\omega_m \in Z_2^p$, of the partition $\{\mathcal{P}(\mathfrak{C})\}$ generated by a Cartan subalgebra $\mathfrak{C} \in su(2^p)$. 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 $\mathcal{W}_{\omega_m}$ in $\{\mathcal{P}(\mathfrak{C})\}$ is equivalent to that of the strings ω_m in Z_2^p.

Since the subspaces $\{\mathcal{W}_{\omega_m}\}$ for the quantum code of type-I is a subgroup of $\{\mathcal{P}(\mathfrak{C})\}$, the set of strings $\{\omega_m\}$ is a subgroup of Z_2^p. This indicates this type of quantum code has a linear correspondence in classical codes. While the subspaces $\{\mathcal{W}_{\omega_m}\}$ for the code of type-II is not a subgroup of $\{\mathcal{P}(\mathfrak{C})\}$ and the set of strings $\{\omega_m\}$ is not a subgroup of 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

[1] Z.-Y. Su (2006), quant-ph/0603190.
[2] I. L. Chuang, et al. (2008), quant-ph/0803.3232.
[3] M.-C. Tsai, K.-P. Chen, W.-C. Su and Z.-Y. Su., "Additive and Nonadditive Quantum Codes", to appear.

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.