Retracted: Quantum Quasi-Cyclic Low-Density Parity-Check Codes

Dazu Huang¹,², Zhigang Chen¹, Xin Li¹,², and Ying Guo¹

¹ School of Information Science and Engineering, Central South University, Changsha, 410083 China
² Department of Information Management, Hunan College of Finance and Economics, Changsha, 410205, China

Abstract. In this paper, how to construct quantum quasi-cyclic (QC) low-density parity-check (LDPC) codes is proposed. Using the proposed approach, some new quantum codes with various lengths and rates of no cycles-length 4 in their Tanner graph are designed. In addition, the presented quantum codes can be efficiently constructed with large code-word length. Finally, we show the decoding of the proposed quantum QC LDPC.

Keywords: Quantum code, Quasi-cyclic Low-density Parity-check Codes, encoding and decoding, CSS code.

1 Introduction

The first quantum code, introduced by Shor in 1995 [1], encoded one qubit into nine qubits and could correct both bit-flip errors and phase-flip errors. Shortly after, it was shown that QECC can be constructed based on classical block codes. This led to the development of an important class of QECC by Calderbank, Shor and Steane [2, 3], known as CSS codes. Afterwards, a more general quantum codes, i.e., stabilizer quantum code, has been advanced by Gottesman [4]. Currently, almost all of the advanced code constructions may be categorized as these two classes according to the different construction methods and principles.

A class of classical code called LDPC codes was firstly proposed by Gallager [5] and the comeback of more research many years latter [6, 7]. The advantage of LDPC codes are lower decoding complexity, but its disadvantage is higher encoding complexity to get the optimal LDPC codes. LDPC codes are classified into regular and irregular one according to the weight of rows and columns in parity-check matrix. With the development of quantum information, it is necessary to generalize these notions to quantum codes, and has been proposed recently [8]. In 2005, Thomas Camarain et al. [9] proposed a general construction of quantum LDPC codes within the stabilizer formalism. In addition, the decoding of this kind of quantum code evolved pure quantum nature so that it has some novel properties. Furthermore, the quantum rate can be easily adjusted with choosing proper block matrix of generator matrix.
Since CSS code constructed by two classical linear codes, if based on LDPC codes, then it is called quantum LDPC codes. In this paper, the main idea is that: by constructing circulant permutation matrix, we can obtain quantum quasi-cyclic LDPC codes using CSS’s method. Therefore, in Section 2, we propose a method using classical QC LDPC codes for constructing quantum LDPC respectively and analyze the cycle of this kind construction. Finally, the encoding and decoding of constructed quantum QC LDPC codes are studied.

2 Constructions of Classical Codes for QECC

The characteristic of QC LDPC code is that, the parity-check matrix consists of small square blocks which are the zero matrix or circulant permutation matrices. With sum-product decoding, the QC LDPC codes has good performance for short code length. Therefore, the corresponding quantum QC LDPC codes\cite{10,11} have encoding advantage over the other types of quantum codes\cite{12,13}.

To construct the parity check matrices $H_1$ of classical QC LDPC code $C_1$ and $H_2$ of $C_2^\perp$, we should show how to obtain the circulant permutation matrixes which $H_1$ and $H_2$ obtained from.

First, we introduce some notions. A $L \times L$ square matrix $P = (p_{ij})$ is called basic-matrix, which can be denoted as:

\[
p_{ij} = \begin{cases} 
1 & \text{if } i = (j + 1) \text{ mod } L, \\
0 & \text{otherwise}
\end{cases}
\]

where $L$ is a prime. Obviously, the row vectors of basic-matrix form a finite cyclic group. The $mL \times nL$ matrix $G$ called circulant permutation matrix, which can be denoted by $G = (P^{a_{ij}})$, i.e.,

\[
G = \begin{pmatrix}
P^{a_{11}} & P^{a_{12}} & \cdots & P^{a_{1n}} \\
P^{a_{21}} & P^{a_{22}} & \cdots & P^{a_{2n}} \\
\vdots & \vdots & \ddots & \vdots \\
P^{a_{m1}} & P^{a_{m2}} & \cdots & P^{a_{mn}}
\end{pmatrix}
\]

where $a_{ij}$ is the exponent of matrix $P$. If $P^\infty = 0_{L \times L}$, $a_{ij} \in \{0, 1, \cdots, L - 1, \infty\}$, then $E(G) = (a_{ij})$ is called exponent matrix of $G$, i.e.,

\[
E(G) = \begin{pmatrix}
a_{11} & a_{12} & \cdots & a_{1n} \\
a_{21} & a_{22} & \cdots & a_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
a_{m1} & a_{m2} & \cdots & a_{mn}
\end{pmatrix}
\]

When $G$ has full rank, its code rate is given by

\[
R = \frac{Ln - Lm}{Ln} = \frac{n - m}{n} = 1 - \frac{m}{n},
\]