Quantum stabilizer codes from Abelian group association schemes

A. Naghipour\textsuperscript{1,2*} M. A. Jafarizadeh\textsuperscript{3} † S. Shahmorad\textsuperscript{2} ‡

\textsuperscript{1}Department of Computer Engineering, University College of Nabi Akram, No. 1283 Rah Ahan Street, Tabriz, Iran
\textsuperscript{2}Department of Applied Mathematics, Faculty of Mathematical Sciences, University of Tabriz, 29 Bahman Boulevard, Tabriz, Iran
\textsuperscript{3}Department of Theoretical Physics and Astrophysics, Faculty of Physics, University of Tabriz, 29 Bahman Boulevard, Tabriz, Iran

22 July 2014

Abstract

A new method for the construction of the binary quantum stabilizer codes is provided, where the construction is based on Abelian group association schemes. Association schemes were originally by Bose and his co-workers in the design of statistical experiments. Since that point of inception, the concept has proved useful in the study of group actions, in algebraic graph theory, in algebraic coding theory, and in areas as far afield as knot theory, numerical integration and construction of quantum stabilizer codes. By using Abelian group association schemes followed by cyclic groups a list of binary stabilizer codes of distance 3 and 4 up to 20 qubits is given in table 4. Moreover, some miscellaneous binary stabilizer codes of distance 5 is presented.

Keywords: Stabilizer codes; Association schemes; Adjacency matrices; Cyclic groups; Quantum Hamming bound; Optimal stabilizer codes

1 Introduction

Quantum error-correcting codes (QECC) \cite{1}-\cite{3} made quantum computing theoretically possible and play an essential role in various quantum information processes. A QECC is just a subspace that corrects certain types of errors. When the subspace is specified by the joint +1 eigenspace of a group of commuting multilocal Pauli operators, i.e., direct products of local Pauli operators, the codes are called as stabilizer codes \cite{4}-\cite{6}. We consider only binary codes here. As usual we shall denote by $[[n, k, d]]_2$ a stabilizer code of length $n$ and distance $d$, i.e., correcting up to $\lfloor \frac{d-1}{2} \rfloor$-qubit errors, that encodes $k$ logical qubits. For stabilizer codes, the error syndrome is obtained by measuring the generators of the stabilizer group. The corresponding quantum measurements can be greatly simplified (and also done in parallel) in low-density parity-check (LDPC) codes which are specially designed to have stabilizer generators of small weight. Recently, several methods for

\*Electronic addresses: naghipour@ucna.ac.ir and a.naghipour@tabrizu.ac.ir
\‡Electronic addresses: jafarizadeh@tabrizu.ac.ir and mjafarizadeh@yahoo.com
\‡Electronic address: shahmorad@tabrizu.ac.ir
constructing good families of quantum codes have been proposed. Presented systematic methods to construct binary quantum codes, called stabilizer codes or additive codes, from classical error-correcting codes. Since then the field has made rapid progress, many good binary quantum codes were constructed by using classical error-correcting codes, such as BCH codes, Reed-Solomon codes, Reed-Muller codes, and algebraic geometric codes [8]-[12]. The theory was later extended to the nonbinary case, since the realization that nonbinary quantum codes can use fault-tolerant quantum computation [13]-[15]. A number of new types of quantum codes, such convolutional quantum codes, subsystem quantum codes studied and the stabilizer method has been extended to these variations of quantum code [16], [17].

Most of the work to date on quantum error-correcting codes (quantum codes) assumes that the quantum channel is symmetric, i.e., the different types of errors are assumed to occur equiprobably. However, recent papers (see [18] and [19], for instance) argue that in many qubit systems, phase-flips (or \(Z\)-type errors) occur more frequently than bit-flips (or \(X\)-type errors). This leads to the idea of adjusting the error-correction to the particular characteristics of the quantum channel and codes that take advantage of the asymmetry are called asymmetric quantum codes (AQCs).

Steane first stated the importance of AQCs in [20]. Since then, the construction of quantum codes have extended to asymmetric quantum channels. In the symmetric framework, Steane’s seminal work [20] and that of Calderbank and Shor [7] provided the connection between a pair of classical codes and a class of quantum stabilizer codes.

Wang et al. presented the construction of nonadditive AQCs as well as constructions of asymptotically good AQCs derived from algebraic-geometry codes [21]. Wang and Zhu [22] presented the construction of optimal AQCs. Ezerman et al. [23] proposed so-called CSS-like constructions based on pairs of nested subfield linear codes. They also used nested codes (such as BCH codes, circulant codes, etc.) over \(F_4\) to construct AQCs in their earlier work [24]. The asymmetry was introduced into topological quantum codes in [25]. Leslie [26] presented a new type of sparse CSS quantum error-correcting code based on the homology of hypermaps. Sarvepalli et al. constructed AQCs using a combination of BCH and finite geometry LDPC codes in [27]. A variety of the constructions of new AQCs were presented in [28], [29]. Our aim in this paper is to construct optimal quantum stabilizer codes of distance 3 and higher based on Abelian group association schemes, e.g., codes with largest possible \(k\) with fixed \(n\) and \(d\). Since in the simplest nontrivial case \(d = 3\), despite many efforts to construct optimal stabilizer codes, a systematic construction for all lengths has not been achieved yet, therefore we applied the Abelian group association schemes for construction of quantum stabilizer codes here.

An association scheme is a combinatorial object with useful algebraic properties (see [30] for an accessible introduction). This mathematical object has very useful algebraic properties which enables one to employ them in algorithmic applications such as the shifted quadratic character problem [31]. A \(d\)-class symmetric association scheme (\(d\) is called the diameter of the scheme) has \(d + 1\) symmetric relations \(R_i\) which satisfy some particular conditions. Each non-diagonal relation \(R_i\) can be thought of as the network \((V, R_i)\), where we will refer to it as the underlying graph of the association scheme \((V, R)\) which is considered as the vertex set of the association scheme. In fact, an association scheme partitions the relationships between pairs of vertices into classes, so that for an arbitrary chosen vertex (referred to as a reference vertex), one can stratify the vertices into distinct classes according to its relationships with all of the other vertices. Moreover, this stratification is independent of the choice of reference vertex. In [32], [33] algebraic properties of association schemes have been employed in order to evaluate the effective resistances in finite resistor networks, where the relations of the corresponding schemes define the kinds of resistances or conductances between any two nodes of networks. In [34], a dynamical system with \(d\) different couplings has been investigated in which the relationships between the dynamical elements (couplings) are given by the relations between the vertexes according to the corresponding association schemes. Indeed, according to the relations \(R_i\), the so-called adjacency matrices \(A_i\) are defined which form a commutative algebra known as Bose-Mesner (BM) algebra. Group association schemes are particular schemes in which the vertices belong to a finite group and the relations are defined based on the conjugacy classes of the corresponding group. Working with these schemes is relatively easy, since almost all of the needed information
about the scheme. We will employ the adjacency matrices \( A_i \) for \( i = 1, \ldots, d \) as one of the known parameters of the corresponding association schemes in order to construct quantum stabilizer codes.

The organization of the paper is as follows. In section 2, we give preliminaries such as quantum stabilizer codes, association schemes, group association schemes and finite Abelian groups. Section 3 is devoted to the construction of quantum stabilizer codes based on Abelian group association schemes. The paper ends with a brief conclusion.

\section{2 Preliminaries}

In this section, we give some preliminaries such as quantum codes and association schemes used through the paper.

\subsection*{2.1 Quantum stabilizer codes}

We recall quantum error correcting codes. For further reading on quantum codes, we direct the reader to the admirably clear accounts in \cite{36}, \cite{42}. A quantum state \( |\psi\rangle \) in a two-dimensional complex vector space \( \mathcal{H}_2 \) which can be written

\[|\psi\rangle = \alpha|0\rangle + \beta|1\rangle\]  

(2.1)

with \( \alpha, \beta \in \mathbb{C} \) and \( |\alpha|^2 + |\beta|^2 = 1 \). \( |\psi\rangle \) is determined up to a phase factor \( e^{i\theta} \), so \( |\psi\rangle \) and \( e^{i\theta}|\psi\rangle \) define the same state. Any operator acting on such an n-qubit state can be represented as a combination of Pauli operators which form the Pauli group \( \mathcal{G}_n \) of size \( 4^{n+1} \) with the phase multiplier \( i^k \):

\[\mathcal{G}_n = i^k \{ I, X, Y, Z \}^\otimes n, \quad k = 0, \ldots, 3,\]  

(2.2)

where \( X, Y \) and \( Z \) are the usual Pauli matrices and \( I \) is the identity matrix. Suppose \( S \) is a subgroup of \( \mathcal{G}_n \) and define \( V_S \) to be the set of \( n \) qubit states which are fixed by every element of \( S \). The \( V_S \) is the vector space stabilized by \( S \), and \( S \) is said to be the stabilizer of the space \( V_S \).

Consider the stabilizer \( S = \langle g_1, \ldots, g_l \rangle \). The check matrix corresponding to \( S \) is a \( l \times 2n \) matrix whose rows correspond to the generators \( g_i \) through \( g_l \). The \( i \)-th row of the check matrix is constructed as follows: If \( g_i \) contains \( I \) on the \( j \)-th qubit then the matrix contain 0 in \( j \)-th and \( n+j \)-th columns. If \( g_i \) contains an \( X \) on the \( j \)-th qubit then the element in \( j \)-th column is 1 and in \( n+j \)-th column is 0. If it contains \( Z \) on \( j \)-th qubit then \( j \)-th column contains 0 and \( n+j \)-th element contains 1. And in the last, if \( g_i \) contains operator \( Y \) on \( j \)-th qubit then both \( j \)-th and \( n+j \)-th columns contain 1.

The check matrix does not contain any information about overall multiplicative factor of \( g_i \). We denote \( r(g) \) to represent a row vector representation of operator \( g \) from check matrix, \( r(g) \) is \( 2n \) elements binary row vector. Denote following \( 2n \times 2n \) matrix as \( \Lambda \):

\[\Lambda = \begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix}\]  

(2.3)

where the \( I \) matrices on the off-diagonals are \( n \times n \). Elements \( g \) and \( g' \) of the Pauli group are easily seen to commute if and only if \( r(g)\Lambda r(g')^T = 0 \). Therefore the generators of stabilizer \( S = \langle g_1, \ldots, g_l \rangle \) with corresponding check matrix \( M \) commute if and only if \( M\Lambda M^T = 0 \). Let \( S = \langle g_1, \ldots, g_l \rangle \) be such that \(-I\) is not an element of \( S \). The generators \( g_i, \; i \in \{1, \ldots, l\} \) are independent if and only if the rows of the corresponding check are linearly independent.
Suppose $C(S)$ is a stabilizer code with stabilizer $S$. We denote $N(S)$ a subset of $G_n$, which is defined to consists of all elements $E \in G_n$ such that $EgE^\dagger \in S$ for all $g \in S$. Following theorem specifies the correction power of $C(S)$.

**Theorem 2.1.** Let $S$ be the stabilizer for a stabilizer code $C(S)$. Suppose $\{E_j\}$ is a set of operators in $G_n$ such that $E_j^\dagger E_k \notin N(S) - S$ for all $j$ and $k$. Then $\{E_j\}$ is a correctable set of errors for the code $C(S)$.

**Proof.** See[36].

Let $V$ denote the vector space $Z_2^n$, and label the standard basis of $C^{2^n}$ by $|\nu\rangle$, $\nu \in V$. Every element $g \in G_n$ can be written uniquely in the form

$$g = i^{k'}X(a)Z(b)$$

(2.4)

where $k' \in \{0, 1, 2, 3\}$, $X(a) : |\nu\rangle \rightarrow |\nu + a\rangle$, $Z(b) : |\nu\rangle \rightarrow (-1)^{b\cdot\nu}|\nu\rangle$, for $a, b \in V$. The element $X(a)Z(b)$ indicates that there are bit errors in the qubits for which $a_j = 1$ and phase errors in the qubits for which $b_j = 1$[5].

An $[[n, k, d]]_2$ stabilizer code $V_S$ is a $2^k$-dimensional subspace of the Hilbert space $H_2^{\otimes n}$ stabilized by an Abelian stabilizer group $S$, which does not contain the operator $-I$ [6]. Explicitly

$$V_S = \{|\psi\rangle : s|\psi\rangle = |\psi\rangle, \forall s \in S\}$$

(2.5)

This code to encode $k$ logical qubits into $n$ physical qubits. The rate of such a code $k/n$. Since codespace has dimension $2^k$ so that we can encode $k$ qubits into it. The stabilizer $S$ has a minimal representation in terms of $n-k$ independent generators $\{g_1, ..., g_{n-k} | \forall i \in \{1, ..., n-k\}, g_i \in S\}$. The generators are independent in the sense that none of them is a product of any other two (up to a global phase).

Each generator $g_i \in S$ is written according to (2.4) in order to obtain the binary check matrix $A = (A_1|A_2)$ in which each row corresponds to a generator, with rows of $A_1$ formed by $a$ and rows of $A_2$ formed by $b$ vectors.

A Pauli error operator $E$ can be interpreted as a binary string $e$ of length $2n$. Our convention is that we reverse the order of the $X$ and $Z$ strings in the error operator, so, for instance the binary string

$$100000001|010000001$$

(with a “|” inserted for interpretational convenience), corresponds to the operator $Z_1X_2Y_9$. With this convention, the ordinary dot product (mod 2) of $e$ with a row of the matrix is zero if $E$ and the stabilizer for that row commute, and 1 otherwise. Thus the quantum syndrome for the noise is exactly the classical syndrome $Ae$, regarding $A$ as a parity check matrix and $e$ as binary noise.

The **weight** of an error $E \in G_n$ is defined to be the number of terms in the tensor product which are not equal to the identity. For example, the weight of $X_1Z_4Y_5$ is three. The distance of stabilizer code $C(S)$ is given by the minimum weight of an element of $N(S) - S$. In terms of the binary vector pairs $(a,b)$, this is equivalent to a minimum weight of the bitwise OR $(a,b)$ of all pairs satisfying the symplectic orthogonality condition,

$$A_1b + A_2a = 0$$

(2.6)

which are not linear combinations of the rows of $A$. By the theorem above a distance $d$ stabilizer code can
fix errors on any \( \left\lfloor \frac{d-1}{2} \right\rfloor \) qubits.

If all errors acting on less than \( d \) qubits can be detected, the codes are non-degenerate or pure. For any pure stabilizer quantum code \([n, k, d]_2\), the quantum Hamming bound is written by

\[
\sum_{j=0}^{\left\lfloor \frac{d-1}{2} \right\rfloor} \binom{n}{j} 3^j 2^k \leq 2^n
\]  

For a pure code of distance 3 all errors happened on up to 2 qubits can be detected. The quantum Hamming bound, e.g.,

\[
n - k \geq \lceil \log_2(3n + 1) \rceil
\]  

for a stabilizer code \([n, k, d]_2\), had been proven initially for non-degenerate codes. It is also valid for degenerate codes of distance 3 and 5 [6].

Optimal quantum stabilizer codes of distance 3 are explicitly constructed for all lengths except for the following four families of lengths \( 8f_m - \{1, 2\} \) and \( f_m+2 - \{2, 3\} \) with \( f_m = \frac{4^m - 1}{3} \) and \( m \geq 2 \) being integer, which codes are of the best parameters known and are only one logical qubit less than the quantum Hamming bound [38].

### 2.2 Association schemes

The theory of association schemes has its origin in the design of statistical experiments [43] and in the study of groups acting on finite sets [35]. Besides, associations schemes are used in coding theory [44], design theory and graph theory. One of the important preferences of association schemes is their useful algebraic structures that enable one to find the spectrum of the adjacency matrices relatively easy; then, for different physical purposes, one can define particular spin Hamiltonians which can be written in terms of the adjacency matrices of an association scheme so that the corresponding spectra can be determined easily. The reader is referred [45] for further information on association schemes.

**Definition 2.2.1.** A d-class association scheme \( \Omega \) on a finite set \( V \) is an order set \( \{R_0, R_1, ..., R_d\} \) of relations on the set \( V \) which satisfies the following axioms:

1. \( \{R_0, R_1, ..., R_d\} \) is a partition of \( V \times V \).
2. \( R_0 \) is the identity relation, i.e., \((x, y) \in R_0\) if and only if \( x = y \), whenever \( x, y \in V \).
3. Every relation \( R_i \) is symmetric, i.e., if \((x, y) \in R_i\) then also \((y, x) \in R_i\), for every \( x, y \in V \).
4. Let \( 0 \leq i, j, l \leq d \). Let \( x, y \in V \) such that \((x, y) \in R_l\), then the number

\[
p^l_{ij} = |\{z \in V : (x, z) \in R_i \text{ and } (z, y) \in R_j\}|
\]

only depends on \( i, j \) and \( l \).

The relations \( R_0, R_1, ..., R_d \) are called the associate classes of the scheme; two elements \( x, y \in V \) are \( i \)-th associates if \((x, y) \in R_i\). The numbers \( p^l_{ij} \) are called the intersection numbers of \( \Omega \). If

\[
R^l_i = R_i \quad \text{for} \quad 0 \leq i \leq d, \quad \text{where} \quad R^l_i = \{(\beta, \alpha) : (\alpha, \beta) \in R_i\}
\]
then the corresponding association scheme is called symmetric. Further, if \( p_{ij}^l = p_{ji}^l \) for all \( 0 \leq i, j, l \leq d \), then \( \Omega = (V, \{R_i\}_{0 \leq i \leq d}) \) is called commutative. Let \( \Omega \) be a commutative symmetric association scheme of class \( d \); then the matrices \( A_0, A_1, \ldots, A_d \) defined by

\[
(A_i)_{\alpha, \beta} = \begin{cases} 
1 & \text{if } (\alpha, \beta) \in R_i \\
0 & \text{otherwise}
\end{cases}
\]  

(2.9)

are adjacency matrices of \( \Omega \) and are such that

\[
A_iA_j = \sum_{l=0}^{d} p_{ij}^l A_l
\]

(2.10)

From (2.10), it is seen that the adjacency matrices \( A_0, A_1, \ldots, A_d \) form a basis for a commutative algebra \( A \) known as the Base-Mesner algebra of \( \Omega \). This algebra has a second basis \( E_0, \ldots, E_d \) primitive idempotents,

\[
E_0 = \frac{1}{n} J, \quad E_iE_j = \delta_{ij}E_i, \quad \sum_{i=0}^{d} E_i = I
\]  

(2.11)

where \( \nu = |V| \) and \( J \) is the \( \nu \times \nu \) all-one matrix in \( A \). In terms of the adjacency matrices \( A_0, A_1, \ldots, A_d \) the four defining axioms of a \( d \)-class association scheme translate to the following four statements \([39]\):

\[
\sum_{l=0}^{d} A_l = J, \quad A_0 = I, \quad A_i = A_i^T \quad \text{and} \quad A_iA_j = \sum_{l=0}^{d} p_{ij}^l A_l
\]  

(2.12)

with \( 0 \leq i, j \leq d \) and where \( I \) denotes the \( \nu \times \nu \) identity matrix and \( A^T \) is the transpose of \( A \). Consider the cycle graph with \( \nu \) vertices by \( C_\nu \). It can be easily seen that, for even number of vertices \( \nu = 2m \), the adjacency matrices are given by

\[
A_i = S^i + S^{-i}, \quad i = 1, 2, \ldots, m - 1, \quad A_m = S^m
\]  

(2.13)

where \( S \) is the \( \nu \times \nu \) circulant matrix with period \( \nu (S^\nu = I_\nu) \) defined as follows:

\[
S = \begin{pmatrix}
0 & 0 & 0 & \ldots & 0 & 0 & 1 \\
1 & 0 & 0 & \ldots & 0 & 0 & 0 \\
0 & 1 & 0 & \ldots & 0 & 0 & 0 \\
\vdots \\
0 & 0 & 0 & \ldots & 1 & 0 & 0 \\
0 & 0 & 0 & \ldots & 0 & 1 & 0
\end{pmatrix}
\]  

(2.14)

For odd number of vertices \( \nu = 2m + 1 \), we have

\[
A_i = S^i + S^{-i}, \quad i = 1, 2, \ldots, m - 1, m
\]  

(2.15)

One can easily check that the adjacency matrices in (2.13) together with \( A_0 = I_{2m} \) (and also the adjacency matrices in (2.15) together with \( A_0 = I_{2m+1} \)) form a commutative algebra.
2.3 Group association schemes

In order to construction of quantum stabilizer codes, we need to study the group association schemes. Group association schemes are particular association schemes for which the vertex set contains elements of a finite group $G$ and the relations $R_i$ are defined by

$$R_i = \{(\alpha, \beta) : \alpha\beta^{-1} \in C_i\}, \quad (2.16)$$

where $\{C_i : 0 \leq i \leq d\}$ are the set of conjugacy classes of $G$, satisfy the $(1)-(4)$ and $(3)'$ conditions, so $\Omega = (G, \{R_i\}_{0 \leq i \leq d})$ becomes a commutative association scheme and it is called the group association scheme of the finite group $G$. It is easy to show that the $i$th adjacency matrix is a summation over elements of the $i$th stratum group. In fact by the action of $\bar{C}_i := \sum_{g \in C_i} g$ (the $i$th class sum) on group elements in the regular representation we observe that $\forall \alpha, \beta, (\bar{C}_i)_{\alpha\beta} = (A_i)_{\alpha\beta}$, so

$$A_i = \bar{C}_i = \sum_{g \in C_i} g, \quad (2.17)$$

Thus due to (2.10),

$$\bar{C}_i\bar{C}_j = \sum_{l=0}^{d} p_{ij}^l \bar{C}_l, \quad (2.18)$$

However the intersection numbers $p_{ij}^l, i, j, l = 0, 1, ..., d$ are given by [41]

$$p_{ij}^l = \frac{|C_i||C_j|}{|G|} \sum_{m=0}^{d} \chi_m(g_i)\chi_m(g_j)\overline{\chi_m(g_l)} \quad (2.19)$$

where $n := |G|$ is the total number of vertices.

2.4 Finite Abelian groups

The classification of finite groups is extremely difficult, but the classification of finite Abelian is not so difficult. It turns out that a fine Abelian group is isomorphic to a product of cyclic groups, and there’s a certain uniqueness to this representation.

2.4.1 Cyclic groups and subgroups

It $a$ is an element of a group $G$, then the subset of $G$ generated by $a$

$$\langle a \rangle = \{a^n | n \in \mathbb{Z}\} \quad (2.20)$$

is a subgroup of $G$. It is called a cyclic subgroup of $G$, or the subgroup generated by $a$. If $G$ is generated by some element $a$, then $G$ is called a cyclic group.

The order of an element $a$ in a group is the smallest positive integer $n$ such that $a^n = 1$. It’s denoted $\text{ord } a$.

An abstract cyclic group of order $n$ is often denoted $C_n = \{1, a, a^2, ..., a^{n-1}\}$ when the operation is written multiplicatively. It is isomorphic to the underlying additive group of the ring $\mathbb{Z}_n$ where an isomorphism is $f : \mathbb{Z}_n \rightarrow C_n$ is defined by $f(k) = a^k$. 
Cyclic groups are all Abelian, since \( a^{n}a^{m} = a^{m+n} = a^{m}a^{n} \). The integers \( \mathbb{Z} \) under addition is an infinite cyclic group, while \( \mathbb{Z}_n \), the integers modulo \( n \), is a finite cyclic group of order \( n \). Every cyclic group is isomorphic either to \( \mathbb{Z} \) or to \( \mathbb{Z}_n \) for some \( n \).

### 2.4.2 Product of groups

Using multiplicative notation, if \( G \) and \( H \) are two groups then \( G \times H \) is a group where the product \((a, b)(c, d)\) is defined by \((ac, bd)\).

The product of two Abelian groups is also called their direct sum, denoted \( G \oplus H \). Since every cyclic group of order \( n \) is given by the modular integers \( \mathbb{Z}_n \) under addition mod \( n \). Hence, to illustrate, an Abelian group of order 1200 may actually be isomorphic to, say, the group \( \mathbb{Z}_{40} \times \mathbb{Z}_6 \times \mathbb{Z}_5 \). Furthermore, the Chinese remainder theorem, as we’ll see, which says that if \( m \) and \( n \) are relatively prime, then \( \mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n \). In the preceding example, we may then replace \( \mathbb{Z}_{40} \) by \( \mathbb{Z}_{23} \times \mathbb{Z}_5 \), and \( \mathbb{Z}_6 \) by \( \mathbb{Z}_2 \times \mathbb{Z}_3 \). Therefore, we will state the fundamental theorem like this: every finite Abelian group is the product of cyclic groups of prime power orders. The collection of these cyclic groups will be determined uniquely by the group \( G \).

**Theorem 2.2** (Chinese remainder theorem for groups). Suppose that \( n = km \) where \( k \) and \( m \) are relatively prime. Then the cyclic group \( C_n \) is isomorphic to \( C_k \times C_m \). More generally, if \( n \) is the product of relatively prime factors, then

\[
C_n \cong C_{k_1} \times \ldots \times C_{k_r} = \prod_{i=1}^{r} C_{k_i}
\]

(2.21)

In particular, if the prime factorization of \( n \) is \( n = p_1^{e_1} \ldots p_r^{e_r} \). Then the cyclic group \( C_n \) factors as the product of the cyclic groups \( C_{p_i^{e_i}} \), that is

\[
C_n \cong \prod_{i=1}^{r} C_{p_i^{e_i}}
\]

(2.22)

**Proof.** See[37].

**Theorem 2.3** (Fundamental theorem of finite Abelian groups). Every finite Abelian group is isomorphic to the direct product of a unique collection of cyclic groups, each having a prime power order.

**Proof.** See[37].

An interesting question follows: Given a positive integer \( n \), how do we determine the number of distinct Abelian group of order \( n \)? We can see a pattern that plays on the exponent of each prime appearing in the factorization of \( n \). For example, the case \( n = 32 = 2^5 \) relies completely upon the different ways we partition the exponent 5 into positive integers. This leads us to the following definition [40].

**Definition.** Where \( n \) ranges through the positive integers, define the partition function \( p(n) \) to stand for the number of different partitions of \( n \) into positive integers.

For instance \( p(5) = 7 \), having seen the seven ways we can partition 5, i.e.,
So, there are seven Abelian group of order 32, i.e.,

\[
\begin{align*}
G_1 &= \mathbb{Z}_{2^5} \\
G_2 &= \mathbb{Z}_{2^4} \times \mathbb{Z}_2 \\
G_3 &= \mathbb{Z}_{2^3} \times \mathbb{Z}_{2^2} \\
G_4 &= \mathbb{Z}_{2^3} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \\
G_5 &= \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_2 \\
G_6 &= \mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \\
G_7 &= \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2
\end{align*}
\] (2.23)

The above function enables us to better express the number of distinct Abelian group of a given order, as follows.

**Theorem 2.4.** Let \( n \) denote a positive integer which factors into distinct prime powers, written \( n = \prod p_k^{e_k} \). Then there are exactly \( \prod p(e_k) \) distinct Abelian group of order \( n \).

In particular, when \( n \) is square-free, i.e., all \( e_k = 1 \) then there is a unique Abelian group of order \( n \) given by \( \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \ldots \times \mathbb{Z}_{p_k} \), which is just the cyclic group \( \mathbb{Z}_n \), if we may borrow Chinese reminder theorem again.

### 3 Construction of stabilizer codes from Abelian group association schemes

To construct a quantum stabilizer code of length \( n \) based on the Abelian group association schemes we need a binary matrix \( A = (A_1|A_2) \) which has \( 2n \) columns and two sets of rows, making up two \( n \times n \) binary matrices \( A_1 \) and \( A_2 \), such that by removing arbitrarily row or rows from \( A \) we can achieve \( n - k \) independent generators. After finding the code distance by \( n - k \) independent generators we can then determine the parameters of the associated code. The parameters \([n, k, d]_2\) of the associated quantum stabilizer are its length \( n \), its dimension \( k \), and its minimum distance \( d \).

Consider the cycle graph \( C_\nu \) with \( \nu \) vertices, as is presented in section 2.2. By setting \( m = 2 \) in view of (2.15), we have

\[
A_0 = I_5, \quad A_1 = S + S^{-1}, \quad A_2 = S^2 + S^{-2}
\] (3.1)

where \( S \) is the \( 5 \times 5 \) circulant matrix with period \( 5(S^5 = I_5) \) defined as follows:
One can see that $A_i$ for $i = 1, 2$ are symmetric and $\sum_{i=0}^{2} A_i = J_5$. Also it can be verified that, $\{A_i, \ i = 1, 2\}$ is closed under multiplication and therefore, the set of matrices $A_0, A_1$ and $A_2$ form a symmetric association scheme.

In view of $A_0, A_1$ and $A_2$ we can write the following cases:

$$A_0, \ A_1, \ A_2, \ A_0 + A_1, \ A_0 + A_2, \ A_1 + A_2, \ A_0 + A_1 + A_2$$ (3.3)

By examining the number of combinations of 2 cases selected from a set of the above 7 distinct cases and consider $B_1 = S + S^{-1}$ and $B_2 = S^2 + S^{-2}$ the binary matrix $B = (B_1 | B_2)$ is written as

$$B = \begin{pmatrix}
0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0
\end{pmatrix}$$ (3.4)

By removing the last row from the binary matrix $B$ we can achieve $n - k = 4$ independent generators. The distance $d$ of the quantum code is given by the minimum weight of the bitwise OR $(a, b)$ of all pairs satisfying the symplectic orthogonality condition,

$$B_1 b + B_2 a = 0$$ (3.5)

Let $a = (x_1, x_2, x_3, x_4, x_5)$ and $b = (y_1, y_2, y_3, y_4, y_5)$. Then by using (3.5), we have

$$\begin{cases}
x_3 + x_4 + y_2 + y_5 = 0 \\
x_4 + x_5 + y_1 + y_3 = 0 \\
x_1 + x_5 + y_2 + y_4 = 0 \\
x_1 + x_2 + y_3 + y_5 = 0
\end{cases}$$ (3.6)

By using (3.6) we can get the code distance $d$ equal to 3. Since the number of independent generators is $n - k = 4$, therefore $k = 1$, thus the $[[5, 1, 3]]_2$ optimal quantum stabilizer code is constructed. It encodes $k = 1$ logical qubit into $n = 5$ physical qubits and protects against an arbitrary single-qubit error. Its stabilizer consists of $n - k = 4$ Pauli operators in table 1.

| Name | Operator |
|------|----------|
| $g_1$ | I X Z Z X |
| $g_2$ | X I X Z Z |
| $g_3$ | Z X I X Z |
| $g_4$ | Z Z X I X |

Table 1: Stabilizer generators for the $[[5, 1, 3]]_2$ code.
Similar to case \( m = 2 \) we obtain quantum stabilizer codes from \( C_\nu, \ \nu = 6, 7, \ldots \). In the case of \( m = 3 \) from \( C_6 \) we can write

\[
A_0 = I_6, \quad A_1 = S^1 + S^{-1}, \quad A_2 = S^2 + S^{-2}, \quad A_3 = S^3 \tag{3.7}
\]

It can be easily seen that \( A_i \) for \( i = 1, 2, 3 \) are symmetric and \( \sum_{i=0}^{3} A_i = J_6 \). By choosing \( B_1 = A_2 + A_3 \) and \( B_2 = A_0 + A_1 + A_2 \) the binary matrix \( B = (B_1|B_2) \) will be in the form

\[
B = \begin{pmatrix}
0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\
0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\
0 & 1 & 1 & 1 & 1 & 0 & 1 & 1
\end{pmatrix} \tag{3.8}
\]

By removing the last row from \( B \) and constituting the system of linear equations the analogue of previous case, we can achieve \( d = 3 \). Since the independent generators is \( n - k = 5 \), therefore the optimal quantum stabilizer code of length 6, that encodes \( k = 1 \) logical qubits, i.e., \([6, 1, 3]_2\) is constructed. This code generated by the \( n - k = 5 \) independent generators in table 2.

| Name | Operator          |
|------|-------------------|
| \( g_1 \) | \( Z \ Z \ Y \ X \ Y \ Z \) |
| \( g_2 \) | \( Z \ Z \ Z \ Y \ X \) |
| \( g_3 \) | \( Y \ Z \ Z \ Y \ X \) |
| \( g_4 \) | \( X \ Y \ Z \ Z \ Y \) |
| \( g_5 \) | \( Y \ X \ Y \ Z \ Z \ Z \) |

Table 2: Stabilizer generators for the \([6, 1, 3]_2\) code.

For construction of quantum stabilizer code from \( C_7 \) by using (2.15), we have

\[
A_0 = I_7, \quad A_1 = S + S^{-1}, \quad A_2 = S^2 + S^{-2}, \quad A_3 = S^3 + S^{-3} \tag{3.9}
\]

One can see that \( A_i \) for \( i = 1, 2, 3 \) are symmetric and \( \sum_{i=0}^{3} A_i = J_7 \). Also it can be easily shown that, \( \{A_i, \ i = 1, 2, 3\} \) is closed under multiplication and therefore, the set of matrices \( A_0, \ldots, A_3 \) form a symmetric association scheme. By choosing \( B_1 \) and \( B_2 \) as follows:

\[
B_1 = A_1, \quad B_2 = A_2 + A_3 \tag{3.10}
\]

We can be seen that \( B_1 B_2^T + B_2 B_1^T = 0 \). So the operators all are commute. On the other hand, since
\[
B = \begin{pmatrix}
0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0
\end{pmatrix}
\]

By removing the last row from it by (3.5) the code distance is \( d = 3 \). And also since the independent generators is \( n - k = 6 \). Therefore, we can obtain the [[7, 1, 3]]_2 quantum stabilizer code. This code generated by 6 the independent generators in table 3.

| Name | Operator |
|------|----------|
| \(g_1\) | I X Z Z Z Z X |
| \(g_2\) | X I X Z Z Z Z |
| \(g_3\) | Z X I X Z Z Z |
| \(g_4\) | Z Z X I X Z Z |
| \(g_5\) | Z Z Z X I X Z |
| \(g_6\) | Z Z Z Z X I X |

Table 3: Stabilizer generators for the [[7, 1, 3]]_2 code.

Applying (2.13) and (2.15), we can obtain quantum stabilizer codes from \( C_\nu(\nu = 8, 9, \ldots) \). A list of quantum stabilizer codes is given in table 4.

**Remark.** Table 4 is a list of quantum stabilizer codes from \( C_\nu(\nu = 8, 9, \ldots) \). In the first column is the cyclic group. In the second column are the \( B_1 \) and \( B_2 \) in terms of \( A_i \), \( i = 0, 1, \ldots, m \). In the third column is the value of the length of quantum stabilizer code. In the fourth column is the value of \( n - k \). The fifth column is a list of the quantum stabilizer codes. In this table \( I_n \) is the \( n \times n \) unit matrix and \( X \) is the Pauli matrix. Also, we will sometimes use notation where we omit the tensor signs. For example \( A_1 I_2 I_2 \) is shorthand for \( A_1 \otimes I_2 \otimes I_2 \). All the optimal quantum stabilizer codes constructed in table 4 lengths labeled by \( l \) having the best parameters known.
### Cyclic group | $B_i(i = 1, 2)$ | $n$ | $n-k$ | $[n,k,d]_2$
---|---|---|---|---
$C_8$ | $B_1 = A_3 + A_4, B_2 = A_2 + A_3$ | 8 | 6 | $[8,2,3]_2$
$C_2 \times C_4$ | $B_1 = I_2 A_2 + X A_1, B_2 = I_2 A_1 + X A_1 + X A_2$ | 8 | 6 | $[8,2,3]_2$
$C_2 \times C_2 \times C_2$ | $B_1 = I_2 I_2 X + X I_2 I_2 + X I_2 X + X X X, B_2 = I_2 I_2 X + I_2 X I_2 + X X I_2 + X X X$ | 10 | 5 | $[8,3,3]_2$
$C_9$ | $B_1 = A_1 + A_2, B_2 = A_2 + A_4$ | 9 | 6 | $[9,3,3]_2$
$C_3 \times C_3$ | $B_1 = I_3 A_1 + SS + S^2 S^2, B_2 = I_3 A_1 + S^2 S + S^2 S$ | 9 | 6 | $[9,3,3]_2$
$C_{10}$ | $B_1 = A_2 + A_4 + A_5, B_2 = A_0 + A_2 + A_3$ | 10 | 6 | $[10,4,3]_2$
$C_{10}$ | $B_1 = A_4, B_2 = A_0 + A_3 + A_5$ | 10 | 9 | $[10,1,6]_2$
$C_{11}$ | $B_1 = A_1 + A_3 + A_4 + A_5, B_2 = A_2 + A_5$ | 11 | 7 | $[11,4,3]_2$
$C_{12}$ | $B_1 = A_2 + A_4 + A_5 + A_6, B_2 = A_2 + A_3 + A_5 + A_6$ | 12 | 6 | $[12,5,3]_2$
$C_{12}$ | $B_1 = A_2 + A_4 + A_5 + A_6, B_2 = A_2 + A_3 + A_5 + A_6$ | 12 | 7 | $[12,5,3]_2$
$C_3 \times C_4$ | $B_1 = I_2 I_2 + I_3 A_1 + A_4, B_2 = A_1 A_1 + A_1 I_4$ | 12 | 10 | $[12,2,3]_2$
$C_3 \times C_2 \times C_2$ | $B_1 = A_1 I_2 I_2 + A_1 I_2 X + A_1 X X, B_2 = I_3 X I_2 + I_3 X X + A_1 I_2 X$ | 12 | 8 | $[12,4,3]_2$
$C_{13}$ | $B_1 = A_1 + A_3 + A_4 + A_5, B_2 = A_2 + A_3 + A_5$ | 13 | 8 | $[13,5,3]_2$
$C_{13}$ | $B_1 = A_1 + A_3 + A_4 + A_5, B_2 = A_2 + A_3 + A_5$ | 13 | 12 | $[13,4,3]_2$
$C_{14}$ | $B_1 = A_0 + A_3 + A_4 + A_6 + A_7, B_2 = A_2 + A_3 + A_5$ | 14 | 8 | $[14,6,3]_2$
$C_{14}$ | $B_1 = A_0 + A_3 + A_4 + A_6 + A_7, B_2 = A_2 + A_3 + A_5$ | 14 | 11 | $[14,3,4]_2$
$C_{15}$ | $B_1 = A_2 + A_3 + A_4 + A_6 + A_7, B_2 = A_1 + A_2 + A_3 + A_5$ | 15 | 9 | $[15,6,3]_2$
$C_{16}$ | $B_1 = A_0 + A_3 + A_4 + A_6, B_2 = A_0 + A_3 + A_4 + A_6$ | 16 | 11 | $[16,5,3]_2$
$C_{16}$ | $B_1 = A_0 + A_3 + A_4 + A_6, B_2 = A_0 + A_3 + A_4 + A_6$ | 16 | 8 | $[16,8,3]_2$
$C_2 \times C_8$ | $B_1 = I_2 A_2 + X A_2 + X A_2 + I_2 A_3 + I_2 A_4 + X A_1, B_2 = I_2 A_2 + X A_3 + I_2 A_3 + I_2 A_4 + I_2 A_4 + X A_1, B_2 = I_2 A_2 + X A_3 + I_2 A_3 + I_2 A_4 + X A_1, B_2 = I_2 A_2 + X A_3 + I_2 A_3 + I_2 A_4 + X A_1$ | 16 | 7 | $[16,9,3]_2$
$C_2 \times C_2 \times C_4$ | $B_1 = I_2 I_2 A_2 + A_1 I_2 A_1 + A_1 A_1 I_4 + I_2 A_1 I_4 + I_2 A_1 A_1 + A_1 A_1 A_1, B_2 = I_2 I_2 A_2 + A_1 I_2 A_1 + A_1 A_1 I_4 + I_2 A_1 I_4 + I_2 A_1 A_1 + A_1 A_1 A_1, B_2 = I_2 I_2 A_2 + A_1 I_2 A_1 + A_1 A_1 I_4 + I_2 A_1 I_4 + I_2 A_1 A_1 + A_1 A_1 A_1, B_2 = I_2 I_2 A_2 + A_1 I_2 A_1 + A_1 A_1 I_4 + I_2 A_1 I_4 + I_2 A_1 A_1 + A_1 A_1 A_1$ | 16 | 8 | $[16,8,3]_2$
$C_4 \times C_4$ | $B_1 = I_4 A_1 + A_1 A_1 + A_1 A_2 + A_2 A_2, B_2 = I_4 A_2 + A_1 A_4 + A_1 A_2 + A_2 A_2 + A_2 A_2 + A_2 A_2$ | 16 | 12 | $[16,4,3]_2$
$C_2 \times C_2 \times C_2 \times C_2$ | $B_1 = I_2 I_2 X I_2 + X I_2 X X + X X X X + I_2 X X X X, B_2 = I_2 I_2 X + X I_2 I_2 X + I_2 I_2 X X + I_2 I_2 X X I_2 + X I_2 X + X X I_2 + X X X I_2$ | 16 | 9 | $[16,7,3]_2$
$C_{17}$ | $B_1 = A_3 + A_4 + A_6 + A_7 + A_8, B_2 = A_2 + A_3 + A_5$ | 17 | 10 | $[17,7,3]_2$
$C_{17}$ | $B_1 = A_3 + A_4 + A_6 + A_7 + A_8, B_2 = A_2 + A_3 + A_5$ | 17 | 14 | $[17,3,4]_2$
$C_{18}$ | $B_1 = A_0 + A_3 + A_4 + A_5 + A_6, B_2 = A_3 + A_5 + A_6 + A_7 + A_8 + A_9$ | 18 | 10 | $[18,8,3]_2$
$C_{19}$ | $B_1 = A_3 + A_4 + A_6 + A_9, B_2 = A_3 + A_5 + A_6 + A_7$ | 19 | 10 | $[19,9,3]_2$
$C_{20}$ | $B_1 = A_3 + A_4 + A_6 + A_9 + A_{10}, B_2 = A_3 + A_5 + A_6 + A_7 + A_8$ | 20 | 8 | $[20,12,3]_2$

Table 4: Quantum stabilizer codes $[[n,k,d]]_2$.

### 3.1 Construction of distance five stabilizer codes from Abelian group association schemes

We can extend the stabilizers of the codes from section 3 to get distance five codes. The parameters of these distance five codes will be $[[n,k,5]]_2$. In the case of $m = 5$ from $C_{11}$ we can write

$$A_0 = I_{11}, \ A_1 = S^1 + S^{-1}, \ A_2 = S^2 + S^{-2}, \ A_3 = S^3 + S^{-3}, \ A_4 = S^4 + S^{-4}, \ A_5 = S^5 + S^{-5} \quad (3.12)$$
where \( S \) is the \( 11 \times 11 \) circulant matrix with period 11 \((S^{11}=I_{11})\). One can easily see that the above adjacency matrices for \( i=1,\ldots,5 \) are symmetric and \( \sum_{i=0}^{5} A_i = J_{11} \). Also, the set of matrices \( A_0,\ldots,A_5 \) form a symmetric association scheme. By choosing \( B_1 = A_1 + A_4 + A_5 \) and \( B_2 = A_2 + A_5 \) the binary matrix \( B = (B_1|B_2) \) will be in the form

\[
B = \left( \begin{array}{ccccccccc}
0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\
1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\
1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\
1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\
1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\
\end{array} \right)
\]

(3.13)

By removing the last row from \( B \) and by considering \( a = (x_0,\ldots,x_{11}) \) and \( b = (y_0,\ldots,y_{11}) \), in view of (3.5) we can achieve \( d = 5 \).

Since the independent generators is \( n-k=10 \), therefore the quantum stabilizer code of length 11, that encodes \( k=1 \) logical qubits, i.e., \([[[11,1,5]]_2\) is constructed. This code generated by the \( n-k=10 \) independent generators in table 5.

| Name | Operator |
|------|----------|
| \( g_1 \) | I X Z I X Y Y X I Z X |
| \( g_2 \) | X I X Z I X Y Y X I Z |
| \( g_3 \) | Z X I X Z I X Y Y X I |
| \( g_4 \) | I Z X I X Z I X Y Y X |
| \( g_5 \) | X I Z X I X Z I X Y Y |
| \( g_6 \) | Y X I Z X I X Z I X Y |
| \( g_8 \) | X Y Y X I Z X I X Z I |
| \( g_9 \) | I X Y Y X I Z X I Z X |
| \( g_{10} \) | Z I X Y Y X I Z X I X |

Table 5: Stabilizer generators for the \([[[11,1,5]]_2\) code.

For construction of distance five quantum stabilizer code from \( C_{13} \) by using (2.15), we have

\[
A_0 = I_{13}, \quad A_1 = S+S^{-1}, \quad A_2 = S^2+S^{-2}, \quad A_3 = S^3+S^{-3}, \quad A_4 = S^4+S^{-4}, \quad A_5 = S^5+S^{-5}, \quad A_6 = S^6+S^{-6}
\]

(3.14)

One can see that \( A_i \) for \( i=1,\ldots,6 \) are symmetric and \( \sum_{i=0}^{6} A_i = J_{13} \). Also it can be easily shown that, \( \{A_i, \ i=1,\ldots,6\} \) is closed under multiplication and therefore, the set of matrices \( A_0,\ldots,A_6 \) form a symmetric association scheme. By choosing \( B_1 \) and \( B_2 \) as follows:

\[
B_1 = A_1 + A_3 + A_4 + A_5, \quad B_2 = A_2 + A_3 + A_5
\]

(3.15)
We can be seen that $B_1B_2^T + B_2B_1^T = 0$. So the operators all are commute. On the other hand, since

\[
B = \begin{pmatrix}
0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\
1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\
1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\
1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\
1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\
0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0
\end{pmatrix}
\]

By removing the last row from $B$ and by considering $a = (x_{01}, ..., x_{13})$ and $b = (y_{01}, ..., y_{13})$, in view of (3.5) we can achieve $d = 5$.

Since the independent generators is $n - k = 12$, therefore the quantum stabilizer code of length 13, that encodes $k = 1$ logical qubits, i.e., $[[13, 1, 5]]_2$ is constructed. This code generated by the $n - k = 12$ independent generators in table 6.

| Name | Operator |
|------|----------|
| $g_1$ | I X Z Y X X I X Y X Y Z X |
| $g_2$ | X I X Z Y X Y I I Y X Y Z |
| $g_3$ | Z X I X Z Y X Y I I Y X Y |
| $g_4$ | Y Z X I X Z Y X Y I I Y X |
| $g_5$ | X Y Z X I X Z Y X Y I I Y |
| $g_6$ | Y X Y Z X I X Z Y X Y I I |
| $g_7$ | I Y X Y Z X I X Z Y X Y I |
| $g_8$ | I I Y X Y Z X I X Z Y X Y |
| $g_9$ | Y I I Y X Y Z X I X Z Y X |
| $g_{10}$ | X Y I I Y X Y Z X I X Z Y |
| $g_{11}$ | Y X Y I I Y X Y Z X I X Z |
| $g_{12}$ | Z Y X Y I I Y X Y Z X I X |

Table 6: Stabilizer generators for the $[[13, 1, 5]]_2$ code.

4 Conclusion

We have developed a new method of constructing binary quantum stabilizer codes from Abelian group association schemes. Using this method, we have constructed good binary quantum stabilizer codes of distance 3 and 4 up to 20. Furthermore, binary quantum stabilizer codes of a large length $n$ with high distance can be constructed. We believe that association schemes will be a good source for constructing good binary quantum stabilizer codes. In a future work, we will use the non-Abelian association schemes to find more quantum stabilizer codes.
References

[1] P. W. Shor, Scheme for reducing decoherence in quantum memory, Phys. Rev. A, 2 (1995) 2493-2496.

[2] E. Knill, and R. Laflamme, A theory of quantum error-correcting codes, Phys. Rev. A, 55 (1997) 900-911.

[3] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Mixed-state entanglement and quantum error correction, Phys. Rev. A, 54 (1996) p. 3824.

[4] A. Calderbank, E. Rains, P. Shor, and N. Sloane, Quantum error correction and orthogonal geometry, Phys. Rev. Lett, 76 (1997) 405-409.

[5] A. Calderbank, E. Rains, P. Shor, and N. Sloane, Quantum error correction via codes over GF(4), IEEE Trans. Inform. Theory, 44 (1998) 1369-1387.

[6] D. Gottesman, Stabilizer codes and quantum error correction, Caltech Ph. D. Thesis, eprint: quant-ph/9705052 (1997).

[7] A. R. Calderbank, and P. W. Shor, Good quantum error-correcting codes exist, Phys. Rev. A, 54 (1996) 1098-1105.

[8] G. Cohen, S. Encheva, and S. Litsyn, On binary constructions of quantum codes, IEEE Trans. Inform. Theory, 45 (1999) 2495-2498.

[9] Z. Li, L. Xing, and X. Wang, Quantum generalized Reed-Solomon codes: Unified framework for quantum maximum-distance separable codes, Phys. Rev. A, 77 (2008) 012308.

[10] A. M. Steane, Quantum Reed-Muller codes, IEEE Trans. Inform. Theory, 45 (1999) 1701-1703.

[11] A. M. Steane, Enlargement of Calderbank-Shor-Steane quantum codes, IEEE Trans. Inform. Theory, 45 (1999) 2492-2495.

[12] H. Chen, S. Ling, and C. Xing, Quantum codes from concatenated algebraic-geometric codes, IEEE Trans. Inform. Theory, 51 (2005) 2915-2920.

[13] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli, On quantum and classical BCH codes, IEEE Trans. Inform. Theory, 53 (2007) 1183-1188.

[14] X. S. Kai, and S. X. Zhu, New quantum MDS codes from negacyclic codes, IEEE Trans. Inform. Theory, 59 (2013) 1193-1197.

[15] X. S. Kai, and S. X. Zhu, Constacyclic codes and some new quantum MDS codes, IEEE Trans. Inform. Theory, 60 (2014) 2080-2-2086.

[16] G. G. La Guardia, On classical and quantum MDS convolutional BCH codes, IEEE Trans. Inform. Theory, 60 (2014) 304-312.

[17] S. A. Aly, and A. Ashikhmin, IEEE Inform. Theory Workshop, (2010) 1-5.

[18] Z. W. E. Evans, A. M. Stephens, J. H. Cole, and L. C. L. Hollenberg, Error correction optimisation in the presence of x/z asymmetry, arXiv: 0709.3875 (2007).

[19] L. Ioffe, and M. M. Mezard, Asymmetric quantum error-correcting codes, Phys. Rev. A, 75 (2007) 032345.
[20] A. Steane, Multiple-particle interference and quantum error correction, *Proc. Roy. Soc. A*, 452 (1996) 2551-2577.

[21] L. Wang, L. Q. Feng, S. Ling, and C. P. Xing, Asymmetric quantum codes: Characterization and constructions, *IEEE Trans. Inform. Theory*, 56 (2010) 2938-2945.

[22] L. Wang, and S. Zhu, On the construction of optimal asymmetric quantum codes, *Int. J. Quantum Inform.*, 12 (2014) 1450017-1450028.

[23] M. F. Ezerman, S. Jitman, S. Ling, and D. V. Pasechnik, CSS-like constructions of asymmetric quantum codes, *IEEE Trans. Inform. Theory*, 59 (2013) 6732-6754.

[24] M. F. Ezerman, S. Ling, and P. Sole, Additive asymmetric quantum codes, *IEEE Trans. Inform. Theory*, 57 (2011) 5536-5550.

[25] A. G. Fowler, Analytic asymptotic performance of topological codes, *Phys. Rev. A*, 87 (2013) 040301.

[26] M. Leslie, Hypermap-homology quantum codes, *Int. J. Quantum Inform.*, 12 (2014) p. 1430001.

[27] P. K. Sarvepalli, A. Klappenecker, and M. Rötteler, Asymmetric quantum codes: Constructions, bounds and performance, *Proc. Roy. Soc.*, 465 (2009) 1645-1672.

[28] G. G. La Guardia, Asymmetric quantum codes: new codes from old, *Quantum Inform. Process*, 12 (2013) 2771-2790.

[29] G. G. La Guardia, On the construction of asymmetric quantum codes, *Int. J. Theor. Phys.*, (2014) doi: 10.1007/s10773-014-2031-y.

[30] C. Godsil, Association scheme, lecture notes, Waterloo University, (2005).

[31] A. M. Childs, On the relationship between continuous and discrete-time quantum walk, *Commun. Math. Phys.*, 294 (2010) 581-603.

[32] M. A. Jafarizadeh, R. Sufiani, and S. Jafarizadeh, Calculating two-point resistances in distance-regular resistor networks, *J. Phys. A: Math. Theor.*, 40 (2007) 4949-4972.

[33] M. A. Jafarizadeh, R. Sufiani, and S. Jafarizadeh, Calculating effective resistances on underlying networks of association schemes, *J. Math. Phys.*, 49 (2008) 073303.

[34] M. A. Jafarizadeh, S. Behnia, E. Faizi, and S. Ahadpour, Generalized N-coupled maps with invariant measure in Bose-Mesner algebra perspective, *Pramana J. Phys.*, 70 (2008) 417-438.

[35] D. G. Higman, Coherent algebras, *Linear Algebra Appl.*, 93 (1987) 109-239.

[36] M. A. Nielsen, and I. L. Chuang, Quantum computation and quantum information, Cambridge University Press, Cambridge, (2000).

[37] D. Joyce, Introduction to modern algebra, Clark University, Version 0.0.6, (2008).

[38] S. Yu, Y. Dong, Q. Chen, and, C. H. Oh, All the optimal stabilizer codes of distance 3, arXiv: quant-ph/0901.1968v1 (2009).

[39] J. Degraer, Isomorph-free exhaustive generation algorithms for association schemes, Gent University Press, (2007).

[40] A. Witno, Finite Abelian groups, WON *Series in Discrete Mathematics and Modern Algebra*, 7 (2012) 1-10.
[41] J. Gordon, L. Martin, Representations and characters of groups, Cambridge University Press, Cambridge, (1993).

[42] H. K. Lo, S. Popescu, and T. Spiller, Introduction to quantum computation and information, World Scientific, (2001).

[43] R. C. Bose, and T. Shimamoto, Classification and analysis of partially balanced incomplete block designs with two associate classes, J. Am. State. Assoc., 47 (1952) 151-184.

[44] P. Delsarte, An algebraic approach to the association schemes of coding theory, Philips Research Reports Suppl., 10 (1973).

[45] R. A. Bailey, Association schemes: Designed experiments, algebra and combinatorics, Cambridge University Press, Cambridge, (2004).