Quantum Information Processing (2023) 22:158
https://doi.org/10.1007/s11128-023-03904-7

Burst error-correcting quantum stabilizer codes designed from idempotents

Kai Lin Ong[1]

Received: 19 October 2022 / Accepted: 2 March 2023

Abstract

Certain classical codes can be viewed isomorphically as ideals of group algebras, while studying their algebraic structures help extracting the code properties. Research has shown that this was remarkably efficient in the case when the code generators are idempotents. In quantum error correction, the theory of stabilizer formalism requires classical self-orthogonal additive codes over the finite field $GF(4)$, which, via the lens of group algebras, are essentially F_2-submodules over $GF(4)$. Therefore, this paper provides a classification on idempotents in commutative group algebra $GF(4)G$, followed by a criterion that allows idempotents to generate stabilizer subgroups. Later, the construction of quantum stabilizer codes is done in the case when G is a cyclic group C_n, for $n = 2^m - 1$ and $n = 2^m + 1$. Quantum bounds on their burst error minimum distance are subsequently determined.

Keywords Quantum code · Stabilizer · Group algebra · Idempotents · Burst error

Mathematics Subject Classification 81P73 · 94B20 · 94B65 · 16U40

1 Introduction

In 1982, Feynman proposed the idea of using quantum mechanical system to simulate quantum phenomena to perform computations [1]. Subsequently, extensive works have been done on the design of quantum algorithms to solve intractable classical problems and the quantization of existing classical algorithms [2, 3]. While the research was multi-directional, the most striking instance was the introduction of Shor's algorithm in 1994, a quantum algorithm suggested that prime factorization of large numbers can be done much efficiently using a quantum computer, in which RSA cryptosystem, the

✉ Kai Lin Ong
k.ong@hw.ac.uk

[1] School of Mathematical and Computer Sciences, Heriot-Watt University Malaysia, 62200 Putrajaya, Malaysia

Published online: 22 March 2023

security system of most online transactions, mainly relied on [4]. Quantum phenomena such as quantum parallelism and superposition are core ideas when implementing these quantum algorithms. However, their units of information, quantum bits, are significantly more prone to errors due to decoherence caused by intrinsic noise in quantum devices and interaction with the environment [5]. Hence, quantum error correction is indispensable for quantum computers.

Although the earliest quantum codes, of 9-qubits and 7-qubits, were constructed by Shor and Steane respectively [6, 7], the first notable quantum codes construction 31 framework was introduced by Gottesman [8] generalized from Shor's codes, termed as the stabilizer construction. Using this approach, the challenge of constructing quantum error-correcting codes was transformed to the problem of finding classical additive codes over the finite field $GF(4) = \{0, 1, \alpha, \alpha^2\}$ which are self-orthogonal with respect to the trace Hermitian inner product. The resultant codes are called stabilizer codes [8, 9].

Most theories of quantum error correction are conventionally discussed under the assumption that noises occur in a random manner, known as the "independent qubit decoherence" model [10]. However, in the scenario when decoherence mechanisms of qubits are known, it is often possible to construct quantum codes with greater efficiency [10]. One common decoherence pattern is burst error, or loosely speaking, errors occurred in consecutive positions. Some research has been done in constructing quantum burst error codes such as the quantum interleaver method with no redundant qubits used [11].

A perspective of viewing classical cyclic codes as ideals of a group algebra was introduced by MacWilliam [12], via the ring isomorphism $F_qC_n \cong \dfrac{F_q[x]}{F_q[x](x^n - 1)}$ where F_qC_n is the group algebra of C_n, the cyclic group of order n over F_q, the finite field of q elements. This had induced a more generic way of defining codes as ideal of group algebras F_qG for finite group G, namely group codes. The rich algebraic structures of group codes arose from the dual properties of them being submodules and ideals, as well as having zero-divisors as generators, resulting in various interesting approaches toward problems such as equivalence problem in classical coding theory [13, 14]. Furthermore, through the lens of group algebras, classical additive codes over $GF(4)$ can be viewed isomorphically as F_2-submodules of group algebra over $GF(4)$. This approach was used to study dual-containing classical codes in constructing quantum codes [15].

It is well known that cyclic codes are uniquely characterized by their generator polynomial. For example, generator polynomials with consecutive power of primitive elements as roots generate an important class of cyclic codes with design distance called BCH codes. Setting certain BCH codes as underlying additive codes over $GF(4)$ results in quantum BCH codes having parameter specified in terms of the design distance [16]. An alternative approach is to study cyclic codes via their idempotent polynomials. The discussion is extendable to a more general context of group algebras. Throughout this paper, let F_qG be the group algebra of a finite group G over the finite field of q elements, F_q. An element $e \in F_qG$ is called an idempotent if $e^2 = e$. Group algebras F_qG with $|G|$ being coprime to char(F_q) possess semisimplicity property, hence are expressible as a direct sum of minimal ideals generated by idempotents.

Here, the group codes are direct sum of a subset of those minimal ideals, that is, in the form of $C = \bigoplus_{i=1}^{k} F_q G e_i$ for some $k \in \mathbb{Z}^+$. Each e_i is called a primitive central idempotent generator of C. These primitive central idempotent generators play a crucial role in extracting the parameters and algebraic properties of the group codes [17, 18]. Specifically, for additive codes over $GF(4)$, this approach was used to construct lower bounds of codes' minimum distance and study the duality of classes of additive multivariable codes in [19], extended from the canonical decomposition of additive codes over $GF(4)$ introduced in [20].

This paper is devoted to constructing quantum codes with stabilizers generated by idempotents and studying their burst error-correcting abilities, based on an alternative classification different from the primitive central idempotents approach. The outline of this paper is as follows. In Section 2, a preliminary review of quantum error correction is carried out in detail, followed by a brief introduction to group algebras and their codes. Section 3 gives a classification on idempotents in the group algebra $GF(4)G$ for finite abelian group G. Section 4 inspects the potential of the classified idempotents in generating self-orthogonal cyclic additive codes over $GF(4)$. Lastly, in Section 5, the burst error-correcting abilities of constructed quantum codes of length n are studied for $n = 2^m - 1$ and $n = 2^m + 1$ for $m \in \mathbb{Z}^+$.

2 Quantum error correction and stabilizer formalism

Theories of quantum error correction reviewed in this section can be found in most textbooks and main early research works such as [8, 21]. A single qubit state is often represented mathematically as an element of the Hilbert Space $\mathbb{C}^2$, having a general form of $|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$, subjecting to the normalization constraint $||a||^2 + ||b||^2 = 1$. Quantum errors are modeled as linear operators on $\mathbb{C}^2$, or equivalently elements of $M_{2\times 2}(\mathbb{C})$, in which the set of Pauli operators, P, consists of the following:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

forms a basis.

Generalizing the idea, error operators on n qubits are in the form of n-fold tensor product of linear operators on $\mathbb{C}^2$. With an overall phase of $\pm 1, \pm i$, this gives the multiplicative group $G_n = \{i^j \bigotimes_{k=1}^{n} P_k | j \in \{0, 1, 2, 3\}, P_k \in P\}$. Moreover, every $g \in G_n$ is either of order 2 or 4, thus either $g^2 = 1$ or $g^2 = -1$. Sometimes, the quotient group $\bar{G}_n = G_n / \{\pm \bigotimes_{k=1}^{n} I_k, \pm i \bigotimes_{k=1}^{n} I_k\}$ is considered instead, with $|\bar{G}_n| = 2^{2n}$.

The weight of a quantum error $\epsilon \in G_n$, $wt(\epsilon)$ is the total number of its tensor component P_k which are non-identity. Also, it follows from the property of Pauli operators that for every pair of elements $\epsilon_1, \epsilon_2 \in G_n$, either $[\epsilon_1, \epsilon_2] = 0$ or $\{\epsilon_1, \epsilon_2\} = 0$, where $[\epsilon_1, \epsilon_2]$ and $\{\epsilon_1, \epsilon_2\}$ denote the commutator and anti-commutator of ϵ_1 and ϵ_2, respectively.

The construction of a stabilizer code fully depends on the choice of its stabilizer group S. A stabilizer S of a length n code C is defined to be the set of all possible error operators in G_n that fix each codeword of C. More precisely, S must be an abelian subgroup of G_n, hence it's often termed as the stabilizer group of C. Note that $-1\bigotimes_{k=1}^{n} I_k \notin S$, for every error operator $\epsilon \in S$, $ord(\epsilon) \neq 4$, otherwise $\epsilon^2 = -1\bigotimes_{k=1}^{n} I_k \in S$. Hence, we have $ord(\epsilon) = 2$ or $\epsilon^2 = 1$. Equivalently, S must be an elementary abelian 2-group.

The resultant code C is a subspace of $\mathbb{C}^{2^n}$, such that every codeword in C is invariant under every operator in S. In other words, C is the intersection of the eigenspace of each of the error operator in S with associated eigenvalue 1.

Definition 2.1 Let S be a stabilizer subgroup of G_n. Then, $C \subseteq \mathbb{C}^{2^n}$ is called a stabilizer code with stabilizer S if $C = \{|\psi\rangle \in \mathbb{C}^{2^n} \mid S_i|\psi\rangle = |\psi\rangle, \forall S_i \in S\}$.

A stabilizer code is called an $[[n, k, d]]$-stabilizer code if its length, dimension and minimum distance are n, k and d, respectively. The dimension and minimum distance of a stabilizer code can be determined based on the properties of its stabilizer.

Since S must be an elementary abelian 2-group, $|S| = 2^l$ for some $l \in \mathbb{Z}^+$ and S has a presentation of l generators, that is, $S = \langle S_1, S_2, \ldots, S_l\rangle$. A stabilizer code with $|S| = 2^l$ has dimension $k = n - l$.

The minimum distance of a length n stabilizer code C can be deduced from the set of errors which are detectable or correctable by C. Note that $S \subseteq N(S) \subseteq G_n$, where $N(S)$ is the normalizer of S in G_n. Then, G_n can be partitioned into $G_n = S \cup (N(S) \setminus S) \cup (G_n \setminus N(S))$.

Case 1: $\epsilon \in S$. It can be seen from Definition 2.1 that ϵ has no effect on the codespace C, thus those errors are correctable for C.

Case 2: $\epsilon \in N(S) \setminus S$. Note that since $\epsilon \in N(S)$, then we have $\epsilon S = S\epsilon$. This implies that when ϵ acts on a codeword $|\psi\rangle \in C$, then for every $S_1 \in S$, $S_1(\epsilon|\psi\rangle) = (S_1\epsilon)|\psi\rangle = (\epsilon S_2)|\psi\rangle = \epsilon(S_2|\psi\rangle) = \epsilon|\psi\rangle$ for some $S_2 \in S$. The fact that $\epsilon|\psi\rangle$ is stabilized by each $S_1 \in S$ implies that $\epsilon|\psi\rangle$ is another codeword in C such that $\epsilon|\psi\rangle \neq |\psi\rangle$. Therefore, ϵ is not detectable, hence not correctable.

Case 3: $\epsilon \in G_n \setminus N(S)$. Then, there exists $S_1 \in S$ such that ϵ does not commute with, then it must be $\{\epsilon, S_1\} = 0$, giving $\epsilon S_1 = -S_1\epsilon$. This results in $\epsilon|\psi\rangle = \epsilon(S_1|\psi\rangle) = (\epsilon S_1)|\psi\rangle = (-S_1\epsilon)|\psi\rangle = -S_1(\epsilon|\psi\rangle)$. Since $\epsilon|\psi\rangle = -S_1(\epsilon|\psi\rangle)$, $\epsilon|\psi\rangle$ is not stabilized by $S_1 \in S$; thus, $\epsilon|\psi\rangle$ is not a codeword in C. The error is detectable by C.

Putting all together, this leads to the following theorem and its immediate corollary.

Theorem 2.2 *Let C be a stabilizer code of length n with stabilizer S. Then, C can detect an error operator ϵ if and only if $\epsilon \in S \cup (G_n \setminus N(S))$.*

Corollary 2.3 *Let C be an $[[n, k, d]]$-stabilizer code with stabilizer S consisting of l generators. Then, $k = n - l$ and $d = min\{wt(\epsilon) \mid \epsilon \in N(S) \setminus S\}$.*

Define a group isomorphism, $\varphi : \bar{G}_1 \to GF(4)$ ($GF(4)$ as additive group) such that $\varphi(X) = \alpha$ and $\varphi(Z) = 1$. The complete mapping is depicted in Table 1. For

Table 1 Each Pauli operator and its corresponding field element of $GF(4)$

Pauli operators	Elements of $GF(4)$
I	0
X	α
Z	1
Y	$1+\alpha$ or α^2

convenience, in the remaining of the paper, elements $\epsilon \in \bar{G}_1$ and $\varphi(\epsilon) \in GF(4)$ will be used interchangeably.

Note that not every subgroup S of G_n can act as a stabilizer, as S must be an elementary abelian 2-group according to previous discussion. The commutativity of operators in G_n can be formulated alternatively by the following.

Define the trace operator $Tr : GF(4) \to F_2$ as $Tr(\beta) = \beta + \beta^2$ for every $\beta \in GF(4)$. Note that $Tr(0) = Tr(1) = 0$ and $Tr(\alpha) = Tr(\alpha^2) = 1$.

Definition 2.4 The trace Hermitian inner product on $GF(4)^n$ is defined by $(,)_{th} : GF(4)^n \times GF(4)^n \to F_2$ such that $(x, y)_{th} = Tr\left(\sum\limits_{k=1}^{n} x_k \bar{y}_k\right)$, for $x = (x_k)$ and $y = (y_k)$.

Proposition 2.5 *Let $\epsilon_1, \epsilon_2 \in G_n$. Then, ϵ_1 and ϵ_2 commutes if and only if their trace Hermitian inner product $(\epsilon_1, \epsilon_2)_{th} = 0$.*

The next corollary follows directly from Proposition 2.5.

Corollary 2.6 *Consider a stabilizer $S \subseteq G_n$. Then, S must be self orthogonal w.r.t. the trace Hermitian inner product.*

This section is ended with a review of group algebras and their codes. Consider $GF(4)G = \{\sum\limits_{g\in G} a_g g | a_g \in GF(4)\}$, the set of all formal sums of elements in G with scalars from $GF(4)$, define addition, multiplication and scalar multiplication of elements in $GF(4)G$ as:

$$\sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G} (a_g + b_g) g$$

$$\left(\sum_{g_1\in G} a_{g_1} g_1\right)\left(\sum_{g_2\in G} b_{g_2} g_2\right) = \sum_{g_1 g_2 = h\in G} (a_{g_1} b_{g_2}) h$$

$$\beta(\sum_{g\in G} a_g g) = \sum_{g\in G} (\beta a_g) g$$

Then, $GF(4)G$, with the operations above is called a group algebra of G over $GF(4)$. For every element $u = \sum\limits_{g\in G} a_g g \in GF(4)G$, its support is defined as $\text{supp}(u) = \{g \in G | a_g \neq 0\}$.

With addition and multiplication defined above, $GF(4)G$ forms a ring. Note that $GF(4)G$ is a commutative ring if and only if G is abelian. On the other hand, $GF(4)G$ forms a vector space over $GF(4)$ with addition and scalar multiplication defined above.

Group codes are ideals of group algebras. For $GF(4)G$, every group code of single generator $u \in GF(4)G$ is in the form of $GF(4)Gu = \{wu|w \in GF(4)G\}$. Below is an example of a group code of length 6.

Example 2.7 Let $G = C_6 = \langle x \rangle$. The group algebra is:

$$GF(4)C_6 = \text{span}_{GF(4)}(1, x, x^2, \dots, x^5)$$

Let $u = 1 + x^2 + x^4$, then the resultant group code is:

$$\begin{aligned} GF(4)C_6(1 + x^2 + x^4) &= \{w(1 + x^2 + x^4)|w \in GF(4)C_6\} \\ &= \text{span}_{GF(4)}(1 + x^2 + x^4, x + x^3 + x^5) \end{aligned}$$

follows from that in $GF(4)C_6$, $x^i(1 + x^2 + x^4) = \begin{cases} 1 + x^2 + x^4 & \text{, for even } i \\ x + x^3 + x^5 & \text{, for odd } i \end{cases}$.

For G with $|G| = n$, fix an ordered listing as $G = \{g_1, g_2, \dots, g_n\}$. Define the canonical mapping $T : GF(4)G \to GF(4)^n$ to view any codeword of an additive code over $GF(4)$ as an element of group algebra over $GF(4)$ and vice versa, as follows:

$$(a_i)_{1 \le i \le n} \Longleftrightarrow \sum_{i=1}^{n} a_i g_i$$

where each $a_i \in GF(4)$.

In general, a length n cyclic additive code over GF(4) with generator $u \in GF(4)^n$ can be defined as $F_2C_n(T^{-1}(u))$.

For example, with ordered listing $C_n = \{1, x, x^2, \dots, x^5\}$, $GF(4)C_6(1+x^2+x^4)$ from Example 2.7 can be viewed as $\text{span}_{GF(4)}(101010, 010101)$. In addition, the additive code over $GF(4)$, $\text{span}_{F_2}(101010, 010101)$ can be viewed isomorphically as the group algebra $F_2C_6(1+x^2+x^4)$. Readers who are interested with more details on theories of group algebras and their applications in classical coding theory can refer to [22] and [18], respectively.

3 Idempotents in commutative group algebra over *GF*(4)

This section is mainly devoted to studying the algebraic structure of the set of all idempotents in $GF(4)G$ for finite abelian group G, denoted by $I_{GF(4)}(G)$. Since $\text{char}(GF(4)) = 2 = \text{char}(F_2)$, the approach used in developing the result in this session will be similar to those in [23, 24].

Proposition 3.1 *The set of all idempotents in $GF(4)G$, $I_{GF(4)}(G)$ forms an additive subgroup of $GF(4)G$.*

Proof Let $e_1, e_2 \in I_{GF(4)}(G)$, then $(e_1+e_2)^2 = e_1^2+e_1e_2+e_2e_1+e_2^2 = e_1^2+2e_1e_2+e_2^2 = e_1 + e_2$.

However, $I_{GF(4)}(G)$ need not form a vector subspace of $GF(4)(G)$ as it's not always closed under scalar multiplication over $GF(4)$. An counterexample is given as $e = x + x^2 + x^4 \in I_{GF(4)}(C_7)$ with $\alpha e \notin I_{GF(4)}(C_7)$.

Next, the notion of generated idempotents which forms the basic building blocks of $I_{GF(4)}(G)$ is introduced. □

Definition 3.2 Let $e \in I_{GF(4)}(G)$ with $|\text{supp}(e)| = k$. If $e = \sum\limits_{i=0}^{k-1} (\beta g)^{2^i}$ with $\beta g = (\beta g)^{2^k}$ for some $g \in \text{supp}(e)$ and some coefficient $\beta \in GF(4) \setminus \{0\}$, then e is said to be a generated idempotent in $GF(4)G$ with generator βg and is denoted by $\langle \beta g\rangle_{Id}$.

The explicit construction of generated idempotents is done by studying the generalized cyclotomic 2-cosets. Readers who are interested with the general idea can refer to [23, 24]. Note that a generated idempotent in $I_{GF(4)}(G)$ can have different generators. For instance in $I_{GF(4)}(C_7)$, we have $\langle \alpha x\rangle_{Id} = \langle x\rangle_{Id} = \langle (1+\alpha)x^2\rangle_{Id} = x+x^2+x^4$. The next proposition classifies generated idempotents according to their support sizes.

Proposition 3.3 *Let $\langle g\rangle_{Id}$ be a generated idempotent in $GF(4)G$.*

1. *If $|supp\langle g\rangle_{Id}|$ is odd, then $\langle \beta g\rangle_{Id} = \langle g\rangle_{Id}$ for each $\beta \in \{\alpha, 1+\alpha\}$.*
2. *If $|supp\langle g\rangle_{Id}|$ is even, then $\langle \beta_1 g\rangle_{Id} \neq \langle \beta_2 g\rangle_{Id}$ for every distinct pair of $\beta_1, \beta_2 \in GF(4) \setminus \{0\}$. In addition, $supp\langle \beta_1 g\rangle_{Id} = supp\langle \beta_2 g\rangle_{Id}$.*

Proof Let $|\text{supp}\langle g\rangle_{Id}| = m$ for some $m \in \mathbb{Z}^+$. If m is odd, note that we can expand as follows:

$$\begin{aligned}\langle \beta g\rangle_{Id} &= \beta g + \beta^2 g^{2^1} + \beta g^{2^2} + \cdots + \beta g^{2^{m-1}} + \beta^2 g + \beta g^{2^1} + \cdots + \beta^2 g^{2^{m-1}}\\ &= (\beta+\beta^2)\sum_{k=0}^{m-1} g^{2^k}\\ &= \sum_{k=0}^{m-1} g^{2^k}.\end{aligned}$$

If m is even, we have $(\beta g)^{2^m} = \beta g$ since $\beta^{2^m} = \beta$. Hence, for every distinct pair of $\beta_1, \beta_2 \in GF(4) \setminus \{0\}$:

$$\text{supp}\langle \beta_1 g\rangle_{Id} = \text{supp}\langle \beta_2 g\rangle_{Id} = \{g, g^{2^1}, \ldots, g^{2^{m-1}}\}.$$

In addition, $\langle \beta_1 g\rangle_{Id} \neq \langle \beta_2 g\rangle_{Id}$ since coefficients of g, $\beta_1 \neq \beta_2$. □

Proposition 3.4 *Two generated idempotents $\langle\beta_1 g_1\rangle_{Id}, \langle\beta_2 g_2\rangle_{Id} \in I_{GF(4)}(G)$ must have either equal or disjoint supports.*

Proof Let $\langle\beta_1 g_1\rangle_{Id}, \langle\beta_2 g_2\rangle_{Id} \in I_{GF(4)}(G)$ with distinct supports but not disjoint, then suppose that $h \in \text{supp}\langle\beta_1 g_1\rangle_{Id} \cap \text{supp}\langle\beta_2 g_2\rangle_{Id}$. Then, h must generate a generated idempotent with $\text{supp}\langle\beta_1 g_1\rangle_{Id} = \text{supp}\langle h\rangle_{Id} = \text{supp}\langle\beta_2 g_2\rangle_{Id}$ by Proposition 3.3, which is a contradiction.

Following from Proposition 3.3, note that for generated idempotent $\langle g\rangle_{Id}$ with even $|\text{supp}\langle g\rangle_{Id}|$, we have the following equation:

$$\langle g\rangle_{Id} + \langle\alpha g\rangle_{Id} = \langle(1+\alpha)g\rangle_{Id}$$

Together with Proposition 3.4, this leads to the next corollary. □

Corollary 3.5 *Let G be an abelian group. Suppose that the number of odd and even weight generated idempotents in F_2G are l and m, respectively. Then, there are a total of $l + 2m$ generated idempotents in $GF(4)G$, and thus $|GF(4)G| = 2^{l+2m}$.*

4 Stabilizer formalism with idempotent generators

In this section, the classified idempotents will be served as generators of cyclic additive codes over $GF(4)$. Recall that a stabilizer subgroup S must be abelian, or equivalently the corresponding additive code over $GF(4)$, C must be self-orthogonal w.r.t. the trace Hermitian inner product over $GF(4)$ by Corollary 2.6.

To begin with, we introduce a special class of idempotents which can potentially generate a stabilizer.

Definition 4.1 An idempotent $e \in I_{GF(4)}(G)$ is said to be self-inverse if for every $h \in \text{supp}(e)$, $h^{-1} \in \text{supp}(e)$ with h and h^{-1} having the same coefficients.

Throughout the remaining of this paper, unless stated otherwise, $C_n = \langle x\rangle$, the cyclic group of order n generated by x, is always associated with the ordered listing $C_n = \{1, x, x^2, \ldots, x^{n-1}\}$.

Theorem 4.2 *Let $\langle\beta x^s\rangle_{Id} \in I_{GF(4)}(C_n)$ be self-inverse. Then, the cyclic additive code over $GF(4)$ having generator $\langle\beta x^s\rangle_{Id}$ is self-orthogonal w.r.t. the trace Hermitian inner product over $GF(4)$.*

Proof Define the canonical mapping $T : GF(4)C_n \to GF(4)^n$. It's sufficient to show that $T(\langle\beta x^s\rangle_{Id})$ and $T(x^i\langle\beta x^s\rangle_{Id})$ are orthogonal for every i, then orthogonality naturally follows for $T(x^j\langle\beta x^s\rangle_{Id})$ and $T(x^k\langle\beta x^s\rangle_{Id})$ for any pair of j, k by the cyclical property.

Let $x^a \in \text{supp}(\langle\beta x^s\rangle_{Id}) \cap \text{supp}(x^i\langle\beta x^s\rangle_{Id})$. Note that we can write $a \equiv s2^k \mod (n)$ and $a \equiv s2^{k'} + i \mod (n)$. This implies that for each i:

$$s2^k \equiv s2^{k'} + i \mod (n)$$

$$-s2^k \equiv -s2^{k'} - i \mod (n)$$
$$(-s)2^k + i \equiv (-s)2^{k'} \mod (n)$$

Let $b \equiv (-s)2^{k'} \mod (n)$. Since $\langle \beta x^s \rangle_{Id}$ is self-inverse, we have $x^b \in \text{supp}(\langle \beta x^s \rangle_{Id})$. Also, since $x^b \in \text{supp}(x^i \langle x^{-s} \rangle_{Id})$ and as $\langle \beta x^s \rangle_{Id}$ is self-inverse, $x^b \in \text{supp}(\langle \beta x^s \rangle_{Id}) \cap \text{supp}(x^i \langle \beta x^s \rangle_{Id})$.

As $\langle \beta x^s \rangle_{Id}$ is self-inverse, the coefficient of x^b in $\langle \beta x^s \rangle_{Id}$ is equal to x^a in $x^i \langle \beta x^s \rangle_{Id}$, whereas the coefficient of x^b in $x^i \langle \beta x^s \rangle_{Id}$ is equal to x^a in $\langle \beta x^s \rangle_{Id}$.

Computing $\langle \langle \beta x^s \rangle_{Id}, x^i \langle \beta x^s \rangle_{Id} \rangle_{th}$, at position a and b, the corresponding summation term in Definition 2.4 are complex conjugate, which results in the trace of their sum to be 0. Therefore, by linearity property, we have $\langle \langle \beta x^s \rangle_{Id}, x^i \langle \beta x^s \rangle_{Id} \rangle_{th} = 0$.

The converse of Theorem 4.2 is generally not true, where a counterexample is $1 + \langle x \rangle_{Id} \in I_{GF(4)}(C_{15})$. The next corollary is an implication of Theorem 4.2. □

Corollary 4.3 *Let $e \in I_{GF(4)}(C_n)$ be self-inverse. Then, the cyclic additive code over $GF(4)$ having generator e is self-orthogonal w.r.t. the trace Hermitian inner product over $GF(4)$.*

The remaining section is devoted to further studying self-inverse idempotents of two special cases; when $n = 2^m + 1$ or $n = 2^m - 1$, for $m \in \mathbb{Z}^+$.

4.1 Case: $n = 2^m - 1$

The following proposition determines the weight of certain generated idempotents in $GF(4)C_n$ for $n = 2^m - 1$.

Lemma 4.4 *Let $n = 2^m - 1$ and $\langle x^s \rangle_{Id} \in I_{\langle Id \rangle}(C_n)$ such that $gcd(s, n) = 1$. Then, $|supp\langle x^s \rangle_{Id}| = m$.*

Proof Note that $|\text{supp}\langle x^s \rangle_{Id}| = k$ if and only if k is the smallest positive integer such that $x^{s(2^k)} = x^s$ or equivalently $s(2^k) \equiv s \bmod (n)$. As $\gcd(s, n) = 1$, this results in $2^k \equiv 1 \bmod (n)$. Note that $j = m$ is the smallest positive integer which satisfy $2^j \equiv 1 \bmod (n)$ as for each $1 \leq j < m$, clearly $2^j - 1 < n$.

Using Proposition 3.3, for the case when m is even, we have the following result. □

Corollary 4.5 *Let $n = 2^m - 1$ for some even $m \in \mathbb{Z}^+$ and consider non-trivial $\langle \beta x^s \rangle_{Id} \in I_{GF(4)}(C_n)$ with $gcd(s, n) = 1$. Then, $|supp\langle \beta x^s \rangle_{Id}| = m$.*

The next proposition gives a class of self-inverse idempotents in $I_{GF(4)}(C_n)$ for $n = 2^m - 1$ when m is even. Before that, it's necessarily to recall Lemma 5.6 in [13] as follows.

Lemma 4.6 *For distinct $\langle x^{s_1} \rangle_{Id}, \langle x^{s_1} \rangle_{Id} \in I_{GF(4)}(C_n)$. If $ord(x^{s_1}) = ord(x^{s_2})$, then $|supp\langle x^{s_1} \rangle_{Id}| = |supp\langle x^{s_2} \rangle_{Id}|$.*

The next proposition introduces a class of self-inverse idempotents for $n = 2^m - 1$.

Proposition 4.7 *Let $n = 2^m - 1$ for some $m \in \mathbb{Z}^+$ and consider non-trivial $\langle \beta x^s \rangle_{Id}, \langle \beta x^{-s} \rangle_{Id} \in I_{GF(4)}(C_n)$ with $gcd(s, n) = 1$. Then, $\langle \beta x^s \rangle_{Id} + \langle \beta x^{-s} \rangle_{Id}$ must be a self-inverse idempotent.*

Proof Firstly, $\langle \beta x^s \rangle_{Id} + \langle \beta x^{-s} \rangle_{Id} \in I_{GF(4)}(C_n)$ by Proposition 3.1. To claim that it is self-inverse, note that for each $k \in \mathbb{Z}^+$:

$$(x^{s(2^k)})(x^{-s(2^k)}) = x^{s(2^k)-s(2^k)} = 1.$$

Note that $ord(x^s) = ord(x^{-s})$, results in $|\text{supp}\langle x^s \rangle_{Id}| = |\text{supp}\langle x^{-s} \rangle_{Id}|$ by Lemma 4.6. By Proposition 3.3, we have $|\text{supp}\langle \beta x^s \rangle_{Id}| = |\text{supp}\langle \beta x^{-s} \rangle_{Id}|$. □

4.2 Case: $n = 2^m + 1$

The following proposition determines the weight of certain generated idempotents in $GF(4)C_n$ for $n = 2^m + 1$.

Lemma 4.8 *Let $n = 2^m + 1$ for some $m \in \mathbb{Z}^+$ and consider non-trivial $\langle x^s \rangle_{Id} \in I_{GF(4)}(C_n)$ with $gcd(s, n) = 1$. Then, $|supp\langle x^s \rangle_{Id}| = 2m$.*

Proof Note that $|\text{supp}\langle x^s \rangle_{Id}| = k$ if k is the smallest positive integer such that $(x^s)^{2^k} = x^s$. This is equivalent to k is the smallest positive integer such that $s2^k \equiv s \mod (2^m + 1)$. Since $\gcd(s, n) = 1$, we have $2^k \equiv 1 \mod (2^m + 1)$.

Note that the smallest positive integer j such that $2^j + 1 \equiv 0 \mod (2^m + 1)$ is $j = m$ and this gives

$$2^m \equiv -1 \mod (2^m + 1)$$

Thus, the cyclotomic 2-coset containing 1,

$$\mathfrak{C}_1 = \{1, 2, 2^2, \ldots, 2^m, 2^{m+1}, \ldots, 2^m 2^{a-1}\}$$

for some $a \in \mathbb{Z}^+$ such that $2^m 2^a = 1$. As $a = m$ is the smallest positive integer such that $2^a \equiv -1 \mod (2^m + 1)$, $k = m + a = 2m$ is the smallest positive integer, which is even satisfying $2^k \equiv 1 \mod (2^m + 1)$.

Then, it follows from Proposition 3.3 that the next corollary holds. □

Corollary 4.9 *Let $n = 2^m + 1$ for some $m \in \mathbb{Z}^+$ and consider non-trivial $\langle \beta x^s \rangle_{Id} \in I_{GF(4)}(C_n)$ with $gcd(s, n) = 1$. Then, $|supp\langle \beta x^s \rangle_{Id}| = 2m$.*

In addition, the self-inverse property of $\langle \beta x^s \rangle_{Id}$ is validated as follows.

Proposition 4.10 *Let $n = 2^m + 1$ for some $m \in \mathbb{Z}^+$ and consider non-trivial $\langle \beta x^s \rangle_{Id} \in I_{GF(4)}(C_n)$. Then, $\langle \beta x^s \rangle_{Id}$ is always self-inverse.*

Proof Let $\langle \beta x^s \rangle_{Id} \in F_2 C_n$. For each $s(2^i) \in \mathfrak{C}_s$, to show $(s(2^i))^{-1} \in \mathfrak{C}_s$, we show that there exists $k \in \mathbb{Z}^+$ such that:

$$s(2^i)(2^k) \equiv -s(2^i) \mod (2^m + 1)$$
$$s(2^i)(2^k + 1) \equiv 0 \mod (2^m + 1)$$

Table 2 Orthogonality analysis of burst error ϵ with chosen stabilizers in Proposition 5.2

Components	x^i	x^{i+1}	$\dots$	x^{i+s-1}	x^{i+s}
ϵ	ϵ_1	ϵ_2	$\dots$	ϵ_{s-1}	ϵ_s
$x^{i-s}S_1$	β_{1k}	0	$\dots$	0	0
$x^{i-s}S_2$	β_{2k}	0	$\dots$	0	0

Such k always exist, choose $k = m$ or there might exist smaller $k \in \mathbb{Z}^+$.

Lastly, an immediate consequence of Proposition 4.10 is that, when $n = 2^m + 1$ is prime, each non-trivial generated idempotent in $I_{GF(4)}(C_n)$ is self-inverse. □

5 Burst error correction

The burst length of an error $\epsilon = (\epsilon_i) \in G_n$ is defined as the largest integer $1 \leq l \leq n$ such that $\epsilon_i \neq 0$ and $\epsilon_{i+l-1} \neq 0$ for some $1 \leq i \leq n$, denoted by $bl(\epsilon) = l$. A code C is said to be a l burst error-correcting code if every burst error of length at most l is correctable. An important lower bound, namely the quantum Rieger bound which arose from the no-cloning theorem, was constructed in [25] and is given as follows:

Theorem 5.1 *Given an* $[[n, k]]$ *l burst error-correcting code, then:*

$$n - k \geq 4l$$

The following proposition is required to study the burst error-correcting ability of stabilizer codes.

Proposition 5.2 *Let C be a length n stabilizer code with cyclic additive stabilizer S. Consider $S_1, S_2 \in S$, $S_i = \sum_{j=0}^{n-1} \beta_{ij} x^j$ for $i \in \{1, 2\}$ such that there exists $k \in \{0, 1, \dots, n-1\}$:*

1. *$\beta_{1j} \neq \beta_{2j}$, both nonzero when $j = k$.*
2. *$\beta_{1j} = \beta_{2j} = 0$ for each $j \in \{k+1, k+2, \dots, k+s\}$ for some $s \in \mathbb{Z}^+$.*

Then, for every burst error ϵ with length $l \leq s$, $\epsilon \notin N(S) \setminus S$.

Proof Let the first non-trivial error of ϵ occurs in position x^i, since the stabilizer is cyclic, we can perform cyclic shift on S_1 and S_2 by multiplying x^{i-s}, respectively, to obtain two stabilizer elements, $x^{i-s}S_1$ and $x^{i-s}S_2$, both having s consecutive zero coefficients from x^{i+1} to x^{i+s}, as illustrated in Table 2.

Note that orthogonality between ϵ and $x^{i-s}S_1$, as well as between ϵ and $x^{i-s}S_2$, holds if and only if $Tr(\epsilon_1\bar{\beta}_{1k}) = Tr(\epsilon_1\bar{\beta}_{2k}) = 0$. Since at least one of $\bar{\beta}_{ik} \neq 1$, it must be $\epsilon_1 = \beta_{1k} = \beta_{2k}$, contradicting our assumption. Hence, $\epsilon \notin N(S) \setminus S$.

Using Proposition 5.2, the following theorem illustrates the burst error-correcting abilities of a class of length $n = 2^m - 1$ stabilizer codes. □

Table 3 Orthogonality analysis of burst error ϵ with chosen stabilizers from $F_2C_n(\langle \beta x\rangle_{Id} + \langle \beta x^{-1}\rangle_{Id})$ for $n = 2^m - 1$

Components	x^i	x^{i+1}	$\dots$	$x^{i+2^{m-2}-1}$	$x^{i+2^{m-2}}$
ϵ	ϵ_1	ϵ_2	$\dots$	$\epsilon_{2^{m-2}-1}$	0
S_1	β	0	$\dots$	0	β^2
S_2	β^2	0	$\dots$	0	β

Table 4 Orthogonality analysis of burst error ϵ with chosen stabilizers from $F_2C_{15}(\langle \alpha x\rangle_{Id} + \langle \alpha x^{-1}\rangle_{Id})$

Components	x^i	x^{i+1}	x^{i+2}	x^{i+3}
ϵ	ϵ_1	ϵ_2	ϵ_3	0
S_1	α	0	0	α^2
S_2	α^2	0	0	α

Theorem 5.3 *Let $n = 2^m - 1$ for some even $m > 2$. Consider the quantum stabilizer code C with stabilizer:*

$$S \cong F_2C_n(\langle \beta x\rangle_{Id} + \langle \beta x^{-1}\rangle_{Id})$$

for some $\beta \in \{\alpha, \alpha^2\}$. Then, C can correct any burst errors up to length $\lfloor 2^{m-3} - \frac{1}{2} \rfloor$.

Proof Let ϵ be a burst error with burst length $l \leq 2^{m-2} - 1$. Let the first non-trivial error of ϵ occurs in position x^i, since the stabilizer is cyclic, we can perform cyclic shift on $\langle \beta x\rangle_{Id} + \langle \beta x^{-1}\rangle_{Id}$ by multiplying $x^{i-2^{m-2}}$ and $x^{i-2^{m-1}}$, respectively, to get two stabilizer elements, S_1 and S_2, both having $2^{m-2} - 2$ consecutive zero coefficients from x^{i+1} to $x^{i+2^{m-2}-2}$ as depicted in Table 3.

Therefore, by Proposition 5.2, $\epsilon \notin N(S) \setminus S$, thus concludes our theorem.

The following example illustrates the case when $m = 4$.

Example 5.4 Let $m = 4$ and thus $n = 2^4 - 1 = 15$. We construct the quantum code C with stabilizer $S \cong F_2C_{15}(\langle \alpha x\rangle_{Id} + \langle \alpha x^{-1}\rangle_{Id})$. The idempotent generator $\langle \alpha x\rangle_{Id} + \langle \alpha x^{-1}\rangle_{Id}$ can be expressed explicitly as:

$$\alpha x + \alpha^2 x^2 + \alpha x^4 + \alpha^2 x^7 + \alpha^2 x^8 + \alpha x^{11} + \alpha^2 x^{13} + \alpha x^{14}.$$

Let ϵ be a burst error of length $l \leq 3$, where the first non-trivial error of ϵ occurs in position x^i. Since the stabilizer is cyclic, we can perform cyclic shift on $\langle \alpha x\rangle_{Id} + \langle \alpha x^{-1}\rangle_{Id}$ by multiplying x^{i-4} and x^{i-8}, respectively, to get two stabilizer elements $S_1, S_2 \in S$, as in Table 4. Note that there's no $\epsilon_1 \in GF(4) \setminus \{0\}$ commute with α and α^2, respectively. Hence, $\epsilon \notin N(S) \setminus S$.

We can motivate further by extending the claim to any ϵ' with burst length $l = 4$. Let the first non-trivial error of ϵ' occurs in position x^i. It can be shown that $g(x) = (1 + x^8)(\langle \alpha x\rangle_{Id} + \langle \alpha x^{-1}\rangle_{Id}) \in S$ has summation terms from x^2 to x^6 being:

$$\alpha^2 x^2 + 0x^3 + 0x^4 + 0x^5 + \alpha^2 x^6$$

Table 5 Further orthogonality analysis of burst error ϵ with chosen stabilizers from $F_2C_{15}(\langle \alpha x\rangle_{Id} + \langle \alpha x^{-1}\rangle_{Id})$

Components	x^i	x^{i+1}	x^{i+2}	x^{i+3}
ϵ'	ϵ'_1	ϵ'_2	ϵ'_3	ϵ'_4
S_3	α^2	0	0	0
S_4	0	0	0	α^2

Now, perform cyclic shift on $g(x)$ by multiplying x^{i-2} and x^{i-1}, results in $S_3, S_4 \in S$, respectively, as in Table 5.

Note that orthogonality occurs precisely when $Tr(\epsilon'_1\alpha) = Tr(\epsilon'_4\alpha) = 0$, that is both $\epsilon'_1, \epsilon'_4 \in GF(4) \setminus \{0\}$ equal to α^2. However, such ϵ' anticommutes with S_1 mentioned above. Hence, $\epsilon' \notin N(S) \setminus S$.

Additionally, it can be shown that $\dim(C) = 7$ using MAGMA [26]. Hence, C is a [[15, 7]] code which is capable to correct at least all burst errors of length up to 2. This code attains the quantum Rieger bound.

The later argument in example above can be generalized into the following theorem.

Theorem 5.5 *Let $n = 2^m - 1$ for some even $m > 2$. Consider the quantum stabilizer code C with stabilizer:*

$$S \cong F_2C_n(\langle \beta x\rangle_{Id} + \langle \beta x^{-1}\rangle_{Id})$$

for some $\beta \in \{\alpha, \alpha^2\}$. Then, C can correct any burst errors up to length 2^{m-3}.

Proof We extend the proof of Theorem 5.3 to the case when ϵ has burst length $l = 2^{m-2}$. When m is even, it can be shown that:

$$g(x) = (1 + x^{2^{m-1}})(\langle \beta x\rangle_{Id} + \langle \beta x^{-1}\rangle_{Id}) \in S,$$

has summation terms from $x^{2^{m-3}}$ to $x^{2^{m-2}+2^{m-3}}$ as follows:

$$\beta^2 x^{2^{m-3}} + \sum_{i=2^{m-3}+1}^{2^{m-2}+2^{m-3}-1} 0x^i + \beta^2 x^{2^{m-2}+2^{m-3}}$$

In a similar fashion, let the first non-trivial error of ϵ occurs in position x^i. Perform cyclic shift on $g(x)$ by multiplying $x^{i-2^{m-3}}$ and $x^{i-2^{m-3}+1}$, respectively, to obtain two stabilizer S_1 and S_2, as depicted in Table 6.

Note that orthogonality occurs precisely when both $\epsilon_1, \epsilon_{2^{m-2}} \in GF(4) \setminus \{0\}$ are equal to β^2. However, such ϵ is orthogonal to S_1 mentioned in Theorem 5.3. Hence, $\epsilon \notin N(S) \setminus S$.

Next, the case when $n = 2^m + 1$ is discussed as follows. □

Theorem 5.6 *Let $n = 2^m + 1$ for some even $m > 2$. Consider the quantum stabilizer code C with stabilizer:*

$$S \cong F_2C_n(\langle \beta x\rangle_{Id})$$

Table 6 Further orthogonality analysis of burst error ϵ with chosen stabilizers from $F_2C_n(\langle \beta x\rangle_{Id} + \langle \beta x^{-1}\rangle_{Id})$ for $n = 2^m - 1$

Components	x^i	x^{i+1}	x^{i+2}	$\dots$	$x^{i+2^{m-2}-2}$	$x^{i+2^{m-2}-1}$
ϵ	ϵ_1	ϵ_2	ϵ_3	$\dots$	$\epsilon_{2^{m-2}-1}$	$\epsilon_{2^{m-2}}$
S_1	β^2	0	0	$\dots$	0	0
S_2	0	0	0	$\dots$	0	β^2

Table 7 Orthogonality analysis of burst error ϵ with chosen stabilizers from $F_2C_n(\langle \beta x\rangle_{Id})$ for $n = 2^m + 1$

Components	x^i	x^{i+1}	x^{i+2}	$\dots$	$x^{i+2^{m-2}-1}$	$x^{i+2^{m-2}}$
ϵ	ϵ_1	ϵ_2	ϵ_3	$\dots$	$\epsilon_{2^{m-2}-1}$	0
S_1	β	0	0	$\dots$	0	β^2
S_2	β^2	0	0	$\dots$	0	β

for some $\beta \in \{\alpha, \alpha^2\}$. Then, C can correct any burst errors up to length 2^{m-3}.

Proof For every ϵ with burst length $l \leq 2^{m-1} - 2^{m-2}$, we can find a stabilizer element which is orthogonal to it. Let the first non-trivial error of ϵ occurs in position x^i, since the stabilizer is cyclic, we can perform cyclic shift on $\langle \beta x\rangle_{Id}$ by multiplying $x^{i-2^{m-2}}$ and $x^{i-2^{m-1}+1}$, respectively, to get two stabilizer elements, S_1 and S_2, both having $2^{m-2} - 1$ consecutive zero coefficients from x^{i+1} to $x^{i+2^{m-2}-1}$, where x^i component of S_1, S_2 having different coefficient in $GF(4) \setminus \{0\}$. The case when m is even is illustrated in Table 7. It follows from Proposition 5.2 that $\epsilon \notin N(S) \setminus S$.

Note that the idempotent $1 \in I_{GF(4)}(G)$ is trivially self-inverse, hence for $e \in I_{GF(4)}(G)$ is self-inverse if and only if $1+e \in I_{GF(4)}(G)$ is self-inverse by Proposition 3.1. The below corollaries follow directly from our previous discussion. □

Corollary 5.7 *Let $n = 2^m - 1$ for some even $m > 2$. Consider the quantum stabilizer code C with stabilizer:*

$$S \cong F_2C_n(1 + \langle \beta x\rangle_{Id} + \langle \beta x^{-1}\rangle_{Id})$$

for some $\beta \in \{\alpha, \alpha^2\}$. Then, C can correct any burst errors up to length 2^{m-3}.

Proof The proof works exactly the same as Theorem 5.3 and 5.5, by replacing $\langle \beta x\rangle_{Id} + \langle \beta x^{-1}\rangle_{Id}$ with $1 + \langle \beta x\rangle_{Id} + \langle \beta x^{-1}\rangle_{Id}$. □

Corollary 5.8 *Let $n = 2^m + 1$ for some even $m > 2$. Consider the quantum stabilizer code C with stabilizer:*

$$S \cong F_2C_n(1 + \langle \beta x\rangle_{Id})$$

for some $\beta \in \{\alpha, \alpha^2\}$. Then, C can correct any burst errors up to length 2^{m-3}.

Proof The proof works exactly the same as Theorem 5.6, by replacing $\langle \beta x\rangle_{Id}$ with $1 + \langle \beta x\rangle_{Id}$.

Table 8 Parameters of cyclic quantum codes of length $n = 2^m \pm 1$ for even $m > 2$, up to 65, with self-inverse idempotent as stabilizer generator

Length (n)	Code generator (e)	Row weight	$[[n, k, d]]$	l-burst error correction	Result
15	$\langle \beta x \rangle_{Id} + \langle \beta x^{-1} \rangle_{Id}$	8	[[15,7,3]]	$l \geq 2$	Theorem 5.5
15	$1 + \langle \beta x \rangle_{Id} + \langle \beta x^{-1} \rangle_{Id}$	9	[[15,0,3]]	$l \geq 2$	Corollary 5.7
17	$\langle \beta x \rangle_{Id}$	8	[[17,1,5]]	$l \geq 2$	Theorem 5.6
17	$1 + \langle \beta x \rangle_{Id}$	9	[[17,8,4]]	$l \geq 2$	Corollary 5.8
63	$\langle \beta x \rangle_{Id} + \langle \beta x^{-1} \rangle_{Id}$	12	[[63,19,7]]	$l \geq 8$	Theorem 5.5
63	$1 + \langle \beta x \rangle_{Id} + \langle \beta x^{-1} \rangle_{Id}$	13	[[63,8,7]]	$l \geq 8$	Corollary 5.7
65	$\langle \beta x \rangle_{Id}$	12	[[65,13,7]]	$l \geq 8$	Theorem 5.6
65	$1 + \langle \beta x \rangle_{Id}$	13	[[65,24,?]]	$l \geq 8$	Corollary 5.8

Finally, this section is ended with Table 8 which summarizes the parameters of constructed codes (up to length 65) and their burst error-correcting abilities. Results are computed using MAGMA Calculator [26]. □

6 Conclusion and future directions

A classification of idempotents in commutative group algebras $GF(4)G$ was introduced in this paper, using the generated idempotents as basic building blocks. Viewing cyclic additive codes equivalently as F_2-submodules of group algebra over the same finite field $GF(4)$, we identified an essential criterion for idempotents to generate self-orthogonal cyclic additive codes over $GF(4)$, that is being self-inverse. This led to the successful construction of a few classes of quantum stabilizer codes, where lower bounds on their burst error-correcting abilities were obtained. It was further shown that some constructed quantum stabilizer codes did attain the lower bound. Future directions include self-inverse idempotents in generating stabilizer codes of other length, as well as the study of other properties which enable idempotents to also generate stabilizer codes. Lastly, the potential of idempotents in constructing good entanglement-assisted quantum error-correcting codes (EAQECCs) is also worth exploring.

Acknowledgements This research was supported by EmPOWER Research Grant Scheme (EmRGS) 2022 (MACS/EmRGS/2022/03) provided by School of Mathematical and Computer Sciences, Heriot-Watt University Malaysia (HWUM).

Data availability Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Declarations

Conflict of interest The authors declare that they have no conflict of interest. The authors have no relevant financial or non-financial interests to disclose.

References

1. Feynman, R.: Simulating physics with computers. Int. J. Theor. Phys. **21**(6), 467–488 (1982). https://doi.org/10.1007/BF02650179
2. Grover, L.: A fast quantum mechanical algorithm for database search. In: Annual ACM Symposium on Theory of Computing, Philadelphia, 2–4 May (1996)
3. Lloyd, S., Mohseni, M., Rebentrost, P.: Quantum principal component analysis. Nat. Phys. **10**(9), 631–633 (2014)
4. Shor, P.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput. **26**(5), 1484–1509 (1995)
5. Schlosshauer, M.: Decoherence and the Quantum-to-Classical Transition. Springer, Berlin (2007). https://doi.org/10.1007/978-3-540-35775-9
6. Shor, P.W.: Scheme for reducing decoherence in quantum memory. Phys. Rev. A **52**(4), 2493–2496 (1995)
7. Steane, A.M.: Error correcting codes in quantum theory. Phys. Rev. Lett. **77**(5), 793 (1996)
8. Gottesman, D.: Stabilizer Codes and Quantum Error Correction (1997)
9. Calderbank, A., Rains, E., Shor, P., Sloane, N.: Quantum error correction via codes over GF(4). IEEE Trans. Inf. Theory **44**(4), 1369–1387 (1998)
10. Vatan, F., Roychowdhury, V.P., Anantram, M.: Spatially correlated qubit errors and burst-correcting quantum codes. IEEE Trans. Inf. Theory **45**(5), 1703–1708 (1999)
11. Kawabata, S.: Quantum interleaver: quantum error correction for burst error. J. Phys. Soc. Jpn. **69**(11), 3540–3543 (2000)
12. MacWilliams, M.F.: Binary codes which are ideals in the group algebra of an abelian group. Bell Syst. Tech. J. **49**(6), 987–1011 (1970). https://doi.org/10.1002/j.1538-7305.1970.tb01812.x
13. Ong, K.L., Ang, M.H.: On equivalency of zero-divisor codes via classifying their idempotent generator. Des. Codes Cryptogr. **88**, 2051–2065 (2020). https://doi.org/10.1007/s10623-020-00762-7
14. Ong, K.L., Ang, M.H.: On equivalence of cyclic and dihedral zero-divisor codes having nilpotents of nilpotency degree two as generators. Des. Codes Cryptogr. **90**, 1127–1138 (2022). https://doi.org/10.1007/s10623-022-01025-3
15. Hurley, T.: Self-dual, dual-containing and related quantum codes from group rings. arXiv:0711.3983 (2007)
16. Aly, S.A., Klappenecker, A., Sarvepalli, P.: On quantum and classical BCH codes. IEEE Trans. Inf. Theory **53**, 1183–1188 (2007). https://doi.org/10.1109/TIT.2006.890730
17. Arora, S.K., Pruthi, M.: Minimal cyclic codes of length $2pn$. Finite Fields Appl. **5**(2), 177–188 (1999). https://doi.org/10.1006/ffta.1998.0238
18. Guerreiro, M.: Group algebras and coding theory. São Paulo J. Math. Sci. **10**, 346–371 (2016). https://doi.org/10.1007/s40863-016-0040-x
19. Martínez-Moro, E., Nicolás, A., Rúa, I.: Additive semisimple multivariable codes over $\mathbb{F}_4$. Designs Codes Cryptogr. **69** (2013)
20. Huffman, W.C.: Additive cyclic codes over F4. Adv. Math. Commun. **1**(4), 427–459 (2007)
21. Lidar, D., Brun, T. (Eds.).: Quantum Error Correction. Cambridge: Cambridge University Press (2013) https://doi.org/10.1017/CBO9781139034807
22. Milies, C.P., Sehgal, S.K.: An Introduction to Group Rings. Springer, Berlin (2002)
23. Ong, K.L., Ang, M.H.: Full identification of idempotents in binary Abelian group rings. J. Indones. Math. Soc. **23**, 67–75 (2017)

24. Ong, K.L., Ang, M.H.: Study of idempotents in cyclic group rings over F_2. In: AIP Conference Proceedings 1739 (2016)
25. Fan, J., Hsieh, M., Chen, H., Chen, H.H., Li, Y.: Construction and performance of quantum burst error correction codes for correlated errors. In: 2018 IEEE International Symposium on Information Theory (ISIT), pp. 2336–2340 (2018)
26. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symb. Comput. **24**, 235–265 (1997)