Quantum Information Processing (2024) 23:241
https://doi.org/10.1007/s11128-024-04451-5

RESEARCH

Quantum variations of cyclotomic cosets for cyclic stabiliser codes construction

En Chong Yap[1] · **Kai Lin Ong**[1]

Received: 4 January 2024 / Accepted: 2 June 2024

Abstract
Cyclotomic cosets are intrinsically linked with the design and construction of classical cyclic codes whose properties can be inferred from the coset structures. This paper proposes some new quantum variations of cyclotomic cosets for cyclic stabiliser construction. These variations are governed by several parameters which are devoted to designing the two essential parts: the error part and the position part of these cosets. Criteria on these cosets in generating additive cyclic stabiliser are extensively studied, followed by actual implementation on stabiliser codes construction of several selected classes of length.

Keywords Cyclotomic cosets · Quantum error correction · Stabiliser codes · Quantum cyclotomic cosets

1 Introduction

Quantum computing leverages quantum mechanical properties arising from its unit of information, namely qubits in performing efficient computation. There exist quantum algorithms able to solve certain intricate black box problems. The supremacy of quantum computing is demonstrated when no classical algorithms can solve these problems, even in subexponential time [1]. To date, cutting-edge quantum technologies have been implemented in a wide range of fields. For instance, in enhancing methods and algorithms for calculation of electronic structures in quantum chemistry [2], in developing quantum-resistant cryptosystems in quantum cryptography [3], and speeding up for machine learning algorithms in quantum machine learning [4], etc.

En Chong Yap and Kai Lin Ong have contributed equally to this work

✉ En Chong Yap
yapenchong1@gmail.com

Kai Lin Ong
k.ong@hw.ac.uk

[1] School of Mathematical and Computer Sciences, Heriot-Watt University Malaysia, 1, Jalan Venna P5/2, Precinct 5, 62200 Putrajaya, Wilayah Persekutuan Putrajaya, Malaysia

Published online: 17 June 2024

Despite their advantages over classical computers, quantum systems are not easy to observe without producing uncontrollable disturbances. The current state of quantum computing is referred to as the noisy intermediate-scale quantum (NISQ) era [5]. Officially, our existing quantum processors are capable of manipulating the intermediate scale of qubits to perform computation better than brute force using supercomputers. However, there remains imperfect control over qubits due to the limitation imposed by quantum decoherence [5]. This critical impediment towards practical quantum computation is caused by intrinsic noise in quantum devices as well as the interaction with the environment. Consequently, this could result in information loss in qubits which leads to errors on large scales.

Various methods have been devoted to solving this problem, most notably, quantum error correction (QEC). The idea of QEC extends from its classical counterpart called coding theory. Coding theory is the study that concentrates on transmitting data through a noisy classical channel successfully. The process involves correcting the messages that might have been corrupted by errors in the channel. Let $\mathbf{F}_2 = \{0, 1\}$ be the binary field. Any subset $C \subseteq \mathbf{F}_2^n$ is called a classical code over $\mathbf{F}_2$ of length n. Two important parameters of such a code are its size $|C|$, and minimum distance d. They governs the number of messages the code can represent, and its error-correcting ability, respectively. Algebraic structures embedded in codes could provide an advantageous way of extracting their properties [6]. For instance, the vector space structure of a linear code C allows its dimension $k = log_2(|C|)$ to be that of the row space of its generator matrix and minimum distance to be that of $d = min\{wt(\vec{w})|\vec{w} \in C\backslash\{\vec{0}\}\}$. Linear codes which are closed under the cyclic shift operator are called cyclic codes. Cyclic codes are uniquely defined by a single generator. More precisely, p-ary cyclic codes can be viewed isomorphically as the principal ideal of the polynomial ring $\mathbf{F}_p[x]/(x^n - 1)$ [7], associated with a generator in polynomial form.

Notably, a cyclic code's generator can be designed from the following notions of cyclotomic cosets in multiple aspects.

Definition 1.1 Let $p \nmid n$. The cyclotomic coset of p or cyclotomic-p-coset modulo n containing r is defined as follows:

$$\mathfrak{C}_{p,r} = \{rp^j \ mod \ n \in \mathbb{Z}_n | j \in \mathbb{Z}^+\},$$

where $\mathbb{Z}_n$ is the integer ring. A subset $\{r_1, \ldots, r_t\}$ of $\mathbb{Z}_n$ is called a complete set of representatives of cyclotomic cosets of p modulo n if $\mathfrak{C}_{p,r_1}, \ldots, \mathfrak{C}_{p,r_t}$ are distinct and $\bigcup_{j=1}^{t} \mathfrak{C}_{p,r_j} = \mathbb{Z}_n$. Also, r is known as the representative of $\mathfrak{C}_{p,r}$. Note that $\mathfrak{C}_{p,r}$ is said to be non-trivial if $r \neq 0$.

It is well known that cyclotomic cosets are associated with the minimal polynomial of cyclic codes [6]. In addition, cyclotomic cosets have been proven useful in constructing cyclic codes with designed minimum distance such as BCH codes, while extracting their dimensions [8, 9]. In particular, the smallest representative of cyclotomic cosets has been shown to allow precise estimates of the dimension of BCH and Goppa codes [10]. Moreover, the cyclotomic-2-cosets can be used to design idempotents in both commutative and non-commutative group algebras. This perspective allows the extraction of the properties of group codes involved [11, 12].

Quantum error correction codes (QECCs) of length n are subspaces of a higher dimensional Hilbert space $\mathbb{C}^{2^n}$. Extending classical code construction to QEC normally faced challenges due to its inherent quantum phenomena. One notable example is the no-cloning theorem, which states that for an arbitrary quantum state $|\psi\rangle$, $|\psi\rangle \mapsto |\psi\rangle \otimes |\psi\rangle$ cannot be done due to the linearity of quantum mechanics [13]. A mainstream research direction in QEC is stabiliser codes. Their underlying construction method is called stabiliser formalism, which could be viewed as the task of constructing classical self-orthogonal additive quaternary codes w.r.t. the Hermitian inner product [14]. It is instructive to note that a quaternary code is said to be cyclic additive if it is in the form of $\overline{S} = \text{span}_{\mathbf{F}_2}(\tau^j(\vec{v})|j \in \mathbb{Z}^+)$ for some $\vec{v} \in \mathbf{F}_4^n$, where τ is the cyclic shift operator.

More recently, researchers have extended the applications of cyclotomic cosets into QEC. Defining sets arising from cyclotomic-p-coset modulo n containing r with $gcd(r, n) = 1$ were proven useful for characterising self-orthogonal cyclic codes to construct CSS codes, a specific class of stabiliser codes [15]. Further attempts include using the linkage between cyclotomic 2-cosets and idempotents of binary cyclic group algebras, as established in [16], to design cyclic stabiliser codes. As a result, these idempotent generators have been proven to be useful for extracting the burst minimum distance of the respective cyclic stabiliser codes [17]. However, the research into cyclotomic cosets in designing stabiliser codes remains restrictive and lacks generality.

Therefore, this paper proposes an original framework for constructing cyclic additive stabilisers derived from the new generalised cyclotomic cosets. These new quantum variants of cyclotomic cosets ensure sufficient variations in the coefficients of $\mathbf{F}_4$, an essential criterion for designing effective stabilisers. More precisely, these variations are governed by several parameters dedicated to designing the two essential parts: the error part and the position part of these cosets. Our stabiliser construction framework has notable strengths. Each stabiliser can be effectively described by a set of cyclotomic representatives, and sufficient conditions on these representatives can be developed to guarantee the stabiliser construction. Numerous stabiliser codes with the best known set of code parameters were obtained through this construction.

The outline of the paper is as follows. Section 2 contains an introduction to quantum error correction mainly revolving around the theory of stabiliser codes. Next, Sect. 3 is devoted to introducing the notion of quantum cyclotomic coset and its generalised version, followed by some discussion of their injectivity and self-inverse properties. This formulation is then applied in stabiliser construction of three specific types of lengths $\left(n = p^s \pm 1 \text{ and } n = |\mathfrak{C}_{p,r}| + 1\right)$ in Sect. 4 and the resultant stabiliser codes' parameters were studied.

2 Quantum error correction

This section gives a brief overview of quantum error models, stabiliser codes and their properties. In classical setting, errors occurring in a binary classical channel are called bit-flip errors. This error could technically occur to any position of a string of bits, flipping 0 to 1 or vice versa.

In quantum setting, the basic unit of information is called a qubit. Qubits are either expressed as a superposition of two orthonormal states $\alpha|0\rangle + \beta|1\rangle$ with $\alpha, \beta \in \mathbb{C}$ or interchangeably as a vector $\begin{pmatrix}\alpha\\ \beta\end{pmatrix} \in \mathbb{C}^2$, both subjecting to the ℓ^2-norm normalisation constraint. The complex coefficients $\alpha, \beta \in \mathbb{C}$ describes its wave-like behaviour.

Unlike classical errors, a continuum of possible quantum errors could occur to a qubit state. Besides bit-flip, there also exists phase error which is known as the Z-error which maps $\alpha|0\rangle + \beta|1\rangle$ to $\alpha|0\rangle - \beta|1\rangle$. In addition, if both bit-flip and phase flip errors occur simultaneously, the resultant error is known as the Y-error. These errors are linear operators and, thus can be represented by the Pauli X, Y and Z matrices as follows:

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

Combining the Pauli matrices with the identity matrix, I (i.e. no error occurred), every quantum error can be described by using them as the basis elements. In other words, any linear operator $E \in M_{2\times 2}(\mathbb{C})$ can be expressed as

$$E = \alpha_X X + \alpha_Y Y + \alpha_Z Z + \alpha_I I$$

by some unique combination of $\alpha_X, \alpha_Y, \alpha_Z, \alpha_I \in \mathbb{C}$. This relation suggests that correcting a continuum of possible quantum errors on a qubit state is possible by correcting the Pauli matrices in their basis. In this paper, this basis for error operators is denoted by the set $P = \{X, Y, Z, I\}$.

Quantum errors on an n qubit state can be modelled as an n-fold tensor product of linear operators on $\mathbb{C}^2$. This brings us to the error group model defined below.

Definition 2.1 Consider an overall phase of $\pm 1, \pm i$, the multiplicative group

$$G_n = \{i^j \otimes_{k=1}^n P_k | j \in \{0, 1, 2, 3\}, P_k \in P\}$$

is called the error group model for the quantum error model.

Denote its quotient group as $\bar{G}_n = G_n/\{\pm \bigotimes_{k=1}^n I_k, \pm i \bigotimes_{k=1}^n I_k\}$. The weight of a quantum error $\epsilon \in G_n$, $wt(\epsilon)$ is the total number of tensor component P_k which are non-identity. The algebraic structure of G_n can be inferred from elements of P, which satisfy $[P_i, P_i] = 0$ for $P_i \in P$ and $\{P_i, P_j\} = 0$ for $P_i \neq P_j \in P\backslash\{I\}$. Note that $[P_i, P_j]$ and $\{P_i, P_j\}$ denote the commutator and anti-commutator of P_i and P_j respectively. Therefore, it follows that every pair of elements $\epsilon_1, \epsilon_2 \in G_n$ is having the relation either $[\epsilon_1, \epsilon_2] = 0$ or $\{\epsilon_1, \epsilon_2\} = 0$.

A classical bit-flip error will always result in the sent codeword and received word being different. In contrast, due to the superposition property, an n-qubit quantum state could be invariant under the effect of some $E \in G_n$. This motivates the following definition of stabiliser codes.

Definition 2.2 Let C be a QECC of length n and S be a subgroup of G_n. Then, C is a stabiliser code with stabiliser subgroup S if $C = \left\{|\psi\rangle \in \mathbb{C}^{2^n} | S_i|\psi\rangle = |\psi\rangle, \forall S_i \in S\right\}$.

Table 1 Mapping of φ, from the operators of $\bar{G}_1$ to elements of $\mathbf{F}_4$

Operators of $\bar{G}_1$	Elements of $\mathbf{F}_4$
I	0
X	ω
Z	1
Y	$1+\omega$ or ω^2

A stabiliser code with length, dimension and minimum distance being n, k and d respectively is called a $[[n, k, d]]$-stabiliser code. For C to be non-trivial, the stabiliser subgroup S must be an elementary abelian 2-group, that is S must have a representation with l generators, with $|S| = 2^l$. The dimension and minimum distance of stabiliser codes can be characterised by its stabiliser, summarised in the below proposition.

Proposition 2.1 *Let C be an $[[n, k, d]]$-stabiliser code with the stabiliser S of l generators. Then, $k = n - l$ and $d = min\{wt(\epsilon)|\epsilon \in Z(S)\backslash S\}$.*

Proof The proof can be found in Sect. 3.2 in [14]. □

Stabilisers of stabiliser codes can be viewed as additive quaternary codes via an isomorphism $\varphi : \bar{G}_n \to \mathbf{F}_4^n$ which applies the map in Table 1 on every position.

Define the trace operator $Tr : \mathbf{F}_4 \to \mathbf{F}_2$ as $Tr(\beta) = \beta + \beta^2$ for every $\beta \in \mathbf{F}_4$. This gives rise to the following inner product.

Definition 2.3 The trace Hermitian inner product on $\mathbf{F}_4^n$ is defined by $\langle , \rangle_{th} : \mathbf{F}_4^n \times \mathbf{F}_4^n \to \mathbf{F}_2$ such that $\langle \vec{u}, \vec{v} \rangle_{th} = Tr\left(\sum_{k=1}^{n} u_k \overline{v}_k\right)$, for $\vec{u} = (u_k)$ and $\vec{v} = (v_k)$, where $\overline{v}_k$ denotes the complex conjugate of v_k.

The commutativity of stabiliser elements can be characterized as an orthogonal condition w.r.t to the inner product introduced above.

Theorem 2.2 *Consider a stabiliser $S \subseteq G_n$. Then, $\varphi(S) = \{\varphi(s)|s \in S\}$ must be self-orthogonal w.r.t. the trace Hermitian inner product.*

Lastly, when the stabiliser is cyclic additive, the following theorem gives a sufficient condition for stabiliser formalism. The result was revised from a group algebra approach introduced in [17]. Note that the notion of self-inverse was defined based on the group inverse elements property of the underlying cyclic group with ordered listing $C_n = \{1, x, x^2, \ldots, x^{n-1}\}$ for its generator x.

Theorem 2.3 *Let $\vec{v} = (v_i)_{1 \le i \le n} \in \mathbf{F}_4^n$. Then the cyclic additive code over $\mathbf{F}_4$ generated by $\vec{v}$ is self-orthogonal w.r.t. Hermitian inner product if $\vec{v}$ is self-inverse, that is, for every $i \in \{1, 2, \ldots, n\}$, we have $v_i = v_{n+2-i \,(mod\, n)}$.*

Proof Let τ be the cyclic shift operator. It is sufficient to show that $\vec{v}$ and $\tau^j(\vec{v})$ are orthogonal for every j, then the self-orthogonality naturally follows from the cyclic property.

Let $a \in \mathbb{Z}_n^+$ such that $v_a, \tau^j(\vec{v})_a = v_{a-j}$ are both nonzero. Then, $v_{n+2-a} = \tau^j(\vec{v})_{(n+2-a)+j}, v_{n+2-(a-j)}$ are both nonzero by self-inverse property of $\vec{v}$. In addition, $v_a = \tau^j(\vec{v})_{(n+2-a)+j}$ and $\tau^j(\vec{v})_a = v_{n+2-(a-j)}$.

This means by computing $\langle \vec{v}, \tau^j(\vec{v}) \rangle_{th}$, for any $a \in \mathbb{Z}_n^+$, at position a and $n + 2 - a$, the corresponding summation terms $v_a \overline{\tau^j(v)_a}$ and $v_{n+2-(a-j)} \overline{\tau^j(v)}_{n+2-(a-j)}$ are complex conjugate, which results in the trace of their sum to be 0. Therefore, by linearity property, we have $\langle \vec{v}, \tau^j(\vec{v}) \rangle_{th} = 0$. □

3 Quantum cyclotomical construction

In this section, a general framework of designing the stabiliser using cyclotomic cosets associated with elements of $\mathbf{F}_4$ is proposed. More precisely, the generator of a cyclic additive stabiliser subgroup can be designed by associating a finite union of these (disjoint) cosets to some $\vec{v} \in \mathbf{F}_4^n$. In other words, for such $\vec{v} \in \mathbf{F}_4^n$, its nonzero positions and their associated elements of $\mathbf{F}_4$ are described by the cosets. Some further review on classical cyclotomic cosets is provided first, followed by two subsections devoted to the study of these new cosets.

3.1 Cyclotomic cosets

Extending from Definition 1.1 and its literature review, the following special class of cyclotomic cosets is often of interest.

Definition 3.1 The cyclotomic coset of p modulo n containing r, $\mathfrak{C}_{p,r}$ is said to be a coprime coset if $gcd(r, n) = 1$.

The inverse of a cyclotomic coset is defined as follows.

Definition 3.2 The inverse of cyclotomic coset of p modulo n containing r, $\mathfrak{C}_{p,r}$ is defined as $\mathfrak{C}_{p,n-r} = \{-rp^j \bmod n \in \mathbb{Z}_n | j \in \mathbb{Z}^+\}$.

It can be shown that for certain classes of n and r, the cyclotomic cosets satisfy $\mathfrak{C}_{p,r} = \mathfrak{C}_{p,n-r}$.

Proposition 3.1 *Let $p \nmid n$ and consider a non-trivial $\mathfrak{C}_{p,r}$. Then, $\mathfrak{C}_{p,r} = \mathfrak{C}_{p,n-r}$ with $|\mathfrak{C}_{p,r}| = 2l$ if and only if l is the smallest positive integer satisfying $rp^l \equiv -r \bmod n$.*

Proof The fact that $|\mathfrak{C}_{p,r}|$ is even follows from the fact that each pair of $i, -i \in \mathfrak{C}_{p,r}$ are distinct and $\mathfrak{C}_{p,r}$ is non-trivial, as $j \equiv -j \bmod n$ if and only if $j \equiv 0 \bmod n$.

Let $\mathfrak{C}_{p,r}$ be self-inverse with $|\mathfrak{C}_{p,r}| = 2l$. Then $-r \in \mathfrak{C}_{p,r}$ and there exists a smallest $k \in \mathbb{Z}^+$ such that $rp^k \equiv -r \bmod n$. Since $gcd(p^k, n) = 1$, the equation is equivalent to

$$rp^k p^k \equiv -rp^k \bmod n,$$
$$rp^{2k} \equiv r \bmod n.$$

Hence, this implies that $|\mathfrak{C}_{p,r}| \mid 2k$. Note that we must have $|\mathfrak{C}_{p,r}| = 2k$, otherwise, if $|\mathfrak{C}_{p,r}| < 2k$, then we have $rp^{\frac{|\mathfrak{C}_{p,r}|}{2}} \equiv -r \ mod \ n$, a contradiction. Hence, $k = l$.

Conversely, if l is the smallest positive integer satisfying $rp^l \equiv -r \ mod \ n$, then

$$rp^i p^l \equiv -rp^i \ mod \ n, \text{ for every } i,$$
$$rp^{i+l} \equiv -rp^i \ mod \ n.$$

This implies that for each $i \in \mathbb{Z}^+$, $-rp^i \in \mathfrak{C}_{p,r}$, hence $\mathfrak{C}_{p,r}$ is self-inverse. Next, $|\mathfrak{C}_{p,r}| = 2l$ can be inferred from the fact that $i = l$ is the smallest possible choice that gives $rp^{l+l} \equiv -rp^l \equiv r \ mod \ n$. □

3.2 Quantum cyclotomic-*p*-cosets

Conventional cyclotomic cosets have their limitations in designing stabiliser codes. As stabilisers must possess more than one error type for the existence of error-correcting abilities, further error-type variations is needed to be infused into the coset framework. Hence, the following variants of cyclotomic cosets are introduced to act as the generator of the cyclic additive stabiliser subgroup.

Definition 3.3 Let $p \nmid n$. The quantum cyclotomic-p-coset, $\mathfrak{C}_{p,r}^{\delta,\gamma}$ modulo n is defined as

$$\mathfrak{C}_{p,r}^{\delta,\gamma} = \left\{ (\delta^{j \ mod \ \gamma}, rp^j \ mod \ n) | j \in \mathbb{Z}^+ \right\},$$

where $\delta \in \mathbf{F}_4^*$, $\gamma \in \mathbb{Z}^+$ and p is prime. Each element in the cyclotomic quantum coset can be written as a direct product of an error part and a position part, as follows:

$$\mathfrak{C}_{p,r}^{\delta,\gamma} = \left\{ \underbrace{(\delta^{j \ mod \ \gamma}}_{\text{error part}}, \underbrace{rp^j \ mod \ n)}_{\text{position part}} | j \in \mathbb{Z}^+ \right\}.$$

Remark 3.1 During stabiliser construction, the error part of the coset is used to assign $\mathbf{F}_4^*$ elements with the position part specifying its respective position. Specifically, p is acting as the cyclotomic parameter with r being a representative, which both give variations to the position part generated. Similarly, δ is the cyclotomic parameter with γ as the controlling parameter, together giving variations to the error part generated. In practice, we would set $\delta = \omega$ or $\delta = \omega^2$ to allow variations of the error types.

Note that $\mathfrak{C}_{p,r}^{\delta,\gamma} \subseteq \mathbf{F}_4^* \times \mathfrak{C}_{p,r}$. For abbreviations, we omit the tuple notation when expressing elements of $\mathfrak{C}_{p,r}^{\delta,\gamma}$. The following forms a special class of quantum cyclotomic cosets, which we will be mainly focussing in the subsequent section.

Definition 3.4 A quantum cyclotomic-p-coset, $\mathfrak{C}_{p,r}^{\delta,\gamma}$ is defined as the first representative coset if $r = min\{j \mid j \in \mathfrak{C}_{p,r}\}$.

For each $\mathfrak{C}_{p,r}^{\delta,\gamma}$, define its canonical projection as $\phi : \mathfrak{C}_{p,r}^{\delta,\gamma} \rightarrow \mathfrak{C}_{p,r}$ such that $\phi((\delta^{j \bmod \gamma}, rp^j \bmod n)) = rp^j \bmod n$. Using ϕ, it can be observed that $|\mathfrak{C}_{p,r}| \mid |\mathfrak{C}_{p,r}^{\delta,\gamma}|$. The injectivity of ϕ needs to be guaranteed when designing the generator of additive stabiliser codes. The following proposition holds trivially since ϕ is always surjective.

Proposition 3.2 *Consider a quantum coset $\mathfrak{C}_{p,r}^{\delta,\gamma}$ with its canonical projection $\phi : \mathfrak{C}_{p,r}^{\delta,\gamma} \rightarrow \mathfrak{C}_{p,r}$. Then ϕ is injective if and only if $|\mathfrak{C}_{p,r}^{\delta,\gamma}| = |\mathfrak{C}_{p,r}|$.*

Next, the study of injectivity of ϕ is done by looking at two different cases, $|\mathfrak{C}_{p,r}| \leq \gamma$ and $|\mathfrak{C}_{p,r}| > \gamma$.

Theorem 3.3 *Let $p \nmid n$. Consider a quantum cyclotomic coset $\mathfrak{C}_{p,r}^{\delta,\gamma}$ with its canonical projection $\phi : \mathfrak{C}_{p,r}^{\delta,\gamma} \rightarrow \mathfrak{C}_{p,r}$.*

1. *If $\gamma \leq |\mathfrak{C}_{p,r}|$, then ϕ is injective if and only if $\gamma \mid |\mathfrak{C}_{p,r}|$.*
2. *If $\gamma > |\mathfrak{C}_{p,r}|$, then ϕ is injective if and only if $3 \mid |\mathfrak{C}_{p,r}|$.*

Proof Note that ϕ is injective if and only if for every $j, k \in \mathbb{Z}^+$, $rp^{j+k|\mathfrak{C}_{p,r}^{\delta,\gamma}|}$ give rise to identical error parts. As the forward direction implies $|\mathfrak{C}_{p,r}^{\delta,\gamma}| = |\mathfrak{C}_{p,r}|$ by Proposition 3.2, while $|\mathfrak{C}_{p,r}| \mid |\mathfrak{C}_{p,r}^{\delta,\gamma}|$ holds in general, thus showing $rp^{j+k|\mathfrak{C}_{p,r}|}$ have identical error parts is sufficient to guarantee the theorem's validity.

Therefore, this can be formulated into the congruence equation $j + k|\mathfrak{C}_{p,r}| \equiv j \bmod \gamma$, for every $j, k \in \mathbb{Z}^+$, yielding

$$k|\mathfrak{C}_{p,r}| \equiv 0 \bmod \gamma, \tag{1}$$

for every $k \in \mathbb{Z}^+$.

Thus, if $\gamma \leq |\mathfrak{C}_{p,r}|$, (1) can be satisfied precisely when $\gamma \mid |\mathfrak{C}_{p,r}|$. If $\gamma > |\mathfrak{C}_{p,r}|$ instead, note that (1) can never be fulfilled for $k = 1$. Hence, it must be that the injectivity of ϕ can be inferred from the congruence equation, follows from the fact that $\mathbf{F}_4^*$ is a multiplicative cyclic group of order 3

$$k|\mathfrak{C}_{p,r}| \equiv 0 \bmod 3,$$

which correspond to the condition $3 \mid |\mathfrak{C}_{p,r}|$. □

Recall from Theorem 2.3 that a sufficient condition that a generator of stabiliser subgroup could fulfil is being self-inverse. Hence, the remaining subsection is devoted to studying their constructions using our proposed cosets, starting from the below definitions.

Definition 3.5 Let $p \nmid n$ and $\mathfrak{C}_{p,r}^{\delta,\gamma}$ be a quantum cyclotomic coset, the inverse of $\mathfrak{C}_{p,r}^{\delta,\gamma}$ is defined as

$$\mathfrak{C}_{p,n-r}^{\delta,\gamma} = \left\{ (\delta^{j \bmod \gamma}, (n-r)p^j \bmod n) | j \in \mathbb{Z}^+ \right\},$$

$$= \left\{ \underbrace{(\delta^{j \bmod \gamma}}_{\text{error part}}, \underbrace{-rp^j \bmod n)}_{\text{position part}} \mid j \in \mathbb{Z}^+ \right\}.$$

The existence and uniqueness of the inverse of $\mathfrak{C}_{p,r}^{\delta,\gamma}$ clearly follows from the definition. In particular, certain quantum cyclotomic cosets can be classified as below.

Definition 3.6 A quantum cyclotomic coset $\mathfrak{C}_{p,r}^{\delta,\gamma}$ is said to be self-inverse if $\mathfrak{C}_{p,r}^{\delta,\gamma} = \mathfrak{C}_{p,n-r}^{\delta,\gamma}$.

The necessary and sufficient conditions of a quantum cyclotomic coset being self-inverse are studied by using a similar categorisation of γ.

Theorem 3.4 *Let $p \nmid n$ and $\mathfrak{C}_{p,r}^{\delta,\gamma}$ be a quantum coset with its canonical projection $\phi : \mathfrak{C}_{p,r}^{\delta,\gamma} \to \mathfrak{C}_{p,r}$ being injective.*

1. *If $\gamma \leq \frac{|\mathfrak{C}_{p,r}|}{2}$, then $\mathfrak{C}_{p,r}^{\delta,\gamma}$ is self-inverse if and only if $\mathfrak{C}_{p,r} = \mathfrak{C}_{p,n-r}$ and $\gamma \mid \frac{|\mathfrak{C}_{p,r}|}{2}$.*
2. *If $\gamma > \frac{|\mathfrak{C}_{p,r}|}{2}$, then $\mathfrak{C}_{p,r}^{\delta,\gamma}$ is self-inverse if and only if $\mathfrak{C}_{p,r} = \mathfrak{C}_{p,n-r}$ and $3 \mid \frac{|\mathfrak{C}_{p,r}|}{2}$.*

Proof Note that $|\mathfrak{C}_{p,r}^{\delta,\gamma}| = |\mathfrak{C}_{p,r}| = 2l$ for the smallest $l \in \mathbb{Z}^+$ such that $rp^l \equiv -r \bmod n$ by Proposition 3.1 and Proposition 3.2. To ensure compatibility of error parts, for each $rp^i \in \mathfrak{C}_{p,r}$, since $(rp^i)\,p^l \equiv -rp^i \bmod n$, we must have $l+i \equiv i \bmod \gamma$ for every i, or equivalently

$$l \equiv 0 \bmod \gamma. \tag{2}$$

In the case when $\gamma \leq l$, (2) can be satisfied precisely when $\gamma \mid l$. If $\gamma > l$ instead, then (2) can never be satisfied. Hence, it must be that the injectivity of ϕ can be inferred from the congruence equation

$$l \equiv 0 \bmod 3,$$

which translates to $3 \mid l$. □

At the end of this subsection, we provide an example illustrating explicitly the quantum cyclotomic-2-coset for the length of 31 and its characteristics.

Example 3.1 Let $n = 31$, $p = 2$ and $r = 1$. The classical coset is

$$\mathfrak{C}_{2,1} = \{2^j \bmod 31 | j \in \mathbb{Z}^+\} = \{2, 4, 8, 16, 1\}.$$

Set $\delta = \omega$ and $\gamma = 5$. The quantum coset is

$$\begin{aligned} \mathfrak{C}_{2,1}^{\omega,5} &= \{(\omega^{j \bmod 5}, 2^j \bmod 31) | j \in \mathbb{Z}^+\} \\ &= \{2\omega, 4\omega^2, 8, 16\omega, 1\} \end{aligned}$$

with its inverse as

$$\mathfrak{C}_{2,31-1}^{\omega,5} = \mathfrak{C}_{2,30}^{\omega,5}$$

$$= \{(\omega^{j \bmod 5}, (30)(2^j) \bmod 31) | j \in \mathbb{Z}^+\}$$
$$= \{29\omega, 27\omega^2, 23, 15\omega, 30\}.$$

The construction shows that the underlying ϕ for $\mathfrak{C}_{2,1}^{\omega,5}$ is injective but $\mathfrak{C}_{2,1}^{\omega,5}$ is not self-inverse. This can be inferred from Theorem 3.3 since $\gamma = 5 \leq |\mathfrak{C}_{2,1}| = 5$ with $5 \mid 5$ and Theorem 3.4 since $\gamma = 5 > \frac{|\mathfrak{C}_{2,1}|}{2} = \frac{5}{2}$ but $3 \nmid \frac{5}{2}$.

3.3 Generalised quantum cyclotomic-*p*-cosets

The notion of generalised quantum cyclotomic-p-cosets can be viewed as a generalisation of the quantum cyclotomic-p-cosets, with more flexibility as defined below.

Definition 3.7 Let $p \nmid n$. The generalised quantum cyclotomic-p-coset modulo n is defined as

$$\mathfrak{C}_{p,r,l}^{\delta,\gamma,\kappa} = \left\{(\delta^{\kappa j \bmod \gamma}, rp^{lj} \bmod n) | j \in \mathbb{Z}^+\right\},$$

where $\kappa = 1, 2, \ldots, \gamma - 1$ and $l = 1, 2, \ldots, |\mathfrak{C}_{p,r}| - 1$. Identically, the first part is referred to as the error part and the second part is referred to as the position part.

$$\mathfrak{C}_{p,r,l}^{\delta,\gamma,\kappa} = \left\{ \underbrace{(\delta^{\kappa j \bmod \gamma}}_{\text{error part}}, \underbrace{rp^{lj} \bmod n)}_{\text{position part}} | j \in \mathbb{Z}^+ \right\}.$$

Remark 3.2 It can be seen that $\mathfrak{C}_{p,r,1}^{\delta,\gamma,1} = \mathfrak{C}_{p,r}^{\delta,\gamma}$. Here, l and κ are further controlling parameters of the position and error parts respectively, which gives further variation to the respective parts.

Similarly, we identify conditions that allows the canonical projection $\phi : \mathfrak{C}_{p,r,l}^{\delta,\gamma,\kappa} \rightarrow \mathfrak{C}_{p,r}$ to be injective. Note that in this case, an injective ϕ does not guarantee their cardinalities to be equal.

Proposition 3.5 *Consider a generalised quantum coset, $\mathfrak{C}_{p,r,l}^{\delta,\gamma,\kappa}$ with its canonical projection $\phi : \mathfrak{C}_{p,r,l}^{\delta,\gamma,\kappa} \rightarrow \mathfrak{C}_{p,r}$ being injective. Then $\frac{|\mathfrak{C}_{p,r}|}{|\mathfrak{C}_{p,r,l}^{\delta,\gamma,\kappa}|} = gcd(|\mathfrak{C}_{p,r}|, l)$.*

Proof Note that the smallest $j \in \mathbb{Z}^+$ such that $r(p^{lj}) \equiv r \bmod n$ is $j = |\mathfrak{C}_{p,r,l}^{\delta,\gamma,\kappa}|$. In particular, $j = |\mathfrak{C}_{p,r}|$ also satisfies $r(p^l)^j \equiv r \bmod n$. The smallest such j must be $\frac{|\mathfrak{C}_{p,r}|}{gcd(|\mathfrak{C}_{p,r}|,l)}$. □

The following theorem summarises the criteria of injective ϕ w.r.t. $\mathfrak{C}_{p,r,l}^{\delta,\gamma,\kappa}$.

Theorem 3.6 *Let $p \nmid n$. Consider a generalised quantum coset, $\mathfrak{C}_{p,r,l}^{\delta,\gamma,\kappa}$ with its canonical projection $\phi : \mathfrak{C}_{p,r,l}^{\delta,\gamma,\kappa} \rightarrow \mathfrak{C}_{p,r}$.*

1. *If* $\gamma \leq \frac{\kappa|\mathfrak{C}_{p,r}|}{gcd(|\mathfrak{C}_{p,r}|,l)}$, *then* ϕ *is injective if and only if* $\gamma \mid \frac{\kappa|\mathfrak{C}_{p,r}|}{gcd(|\mathfrak{C}_{p,r}|,l)}$.
2. *If* $\gamma > \frac{\kappa|\mathfrak{C}_{p,r}|}{gcd(|\mathfrak{C}_{p,r}|,l)}$, *then* ϕ *is injective if and only if* $3 \mid \frac{\kappa|\mathfrak{C}_{p,r}|}{gcd(|\mathfrak{C}_{p,r}|,l)}$.

Proof Note that ϕ is injective if and only if for every $j, k \in \mathbb{Z}^+$, $rp^{l\left(j+k\frac{|\mathfrak{C}_{p,r}|}{gcd(|\mathfrak{C}_{p,r}|,l)}\right)}$ give rise to identical error parts. This can be formulated into the congruence equation $\kappa\left(j + k\frac{|\mathfrak{C}_{p,r}|}{gcd(|\mathfrak{C}_{p,r}|,l)}\right) \equiv \kappa j \ mod\ \gamma$, for every $j, k \in \mathbb{Z}^+$, yielding

$$k\kappa \frac{|\mathfrak{C}_{p,r}|}{gcd(|\mathfrak{C}_{p,r}|, l)} \equiv 0 \ mod\ \gamma,$$

for every $k \in \mathbb{Z}^+$.

The remaining of the proof follows analogously from Theorem 3.3 by replacing $|\mathfrak{C}_{p,r}|$ with $\frac{\kappa|\mathfrak{C}_{p,r}|}{gcd(|\mathfrak{C}_{p,r}|,l)}$. □

Under the assumption of injective ϕ, the following theorem further summarises the criteria for self-inverse $\mathfrak{C}^{\delta,\gamma,\kappa}_{p,r,l}$.

Theorem 3.7 *Let* $p \nmid n$ *and* $\mathfrak{C}^{\delta,\gamma,\kappa}_{p,r,l}$ *be a generalised quantum coset with its canonical projection* $\phi : \mathfrak{C}^{\delta,\gamma,\kappa}_{p,r,l} \rightarrow \mathfrak{C}_{p,r}$ *being injective.*

1. *If* $\gamma \leq \frac{\kappa|\mathfrak{C}_{p,r}|}{2gcd(|\mathfrak{C}_{p,r}|,l)}$, *then* $\mathfrak{C}^{\delta,\gamma,\kappa}_{p,r,l}$ *is self-inverse if and only if* $\mathfrak{C}_{p,r} = \mathfrak{C}_{p,n-r}$ *and* $\gamma \mid \frac{\kappa|\mathfrak{C}_{p,r}|}{2gcd(|\mathfrak{C}_{p,r}|,l)}$.
2. *If* $\gamma > \frac{\kappa|\mathfrak{C}_{p,r}|}{2gcd(|\mathfrak{C}_{p,r}|,l)}$, *then* $\mathfrak{C}^{\delta,\gamma,\kappa}_{p,r,l}$ *is self-inverse if and only if* $\mathfrak{C}_{p,r} = \mathfrak{C}_{p,n-r}$ *and* $3 \mid \frac{\kappa|\mathfrak{C}_{p,r}|}{2gcd(|\mathfrak{C}_{p,r}|,l)}$.

Proof Note that $r \in Im(\phi)$ if and only if $-r \in Im(\phi)$. The mutually disjoint property of cyclotomic cosets guarantees that it must be $\mathfrak{C}_{p,r} = \mathfrak{C}_{p,n-r}$.

Note that $|\mathfrak{C}^{\delta,\gamma,\kappa}_{p,r,l}| = \frac{|\mathfrak{C}_{p,r}|}{gcd(|\mathfrak{C}_{p,r}|,l)} = 2t$ for the smallest $t \in \mathbb{Z}^+$ such that $rp^{lt} \equiv -r \ mod\ n$ by Proposition 3.1 and Proposition 3.5. To ensure compatibility of error parts, for each $rp^{li} \in \mathfrak{C}_{p,r}$, since $(rp^{li})p^{lt} \equiv -rp^{li} \ mod\ n$, we must have $\kappa(t + i) \equiv \kappa i \ mod\ \gamma$ for every i, or equivalently

$$\kappa t \equiv 0 \ mod\ \gamma.$$

The remaining proof follows analogously from Theorem 3.4. □

4 Stabiliser construction

The association of quantum cyclotomic cosets to a stabiliser element is done by using the definition below.

Definition 4.1 Let $p \nmid n$ and $\cup_{i=1}^{t} \mathfrak{C}_{p,r_i,l_i}^{\delta,\gamma_i,\kappa_i}$ be a finite union of generalised quantum cyclotomic-p-cosets, with an injective canonical projection. Then its associated vector $\vec{v} = (v_k) \in \mathbf{F}_4^n$ has

$$v_k = \begin{cases} \delta^{\kappa_i j \bmod \gamma_i} & \text{, if } k = r_i p^{l_i j} \bmod n, \text{ for some } i, j \in \mathbb{Z}^+, \\ 0 & \text{, otherwise.} \end{cases}$$

In this paper, the stabiliser subgroups constructed for stabiliser formalism are all in the form of cyclic additive stabiliser, characterised by the following definition.

Definition 4.2 A stabiliser subgroup $S \subseteq G_n$ is said to be a cyclic additive stabiliser generated by $\cup_{i=1}^{t} \mathfrak{C}_{p,r_i,l_i}^{\delta_i,\gamma_i,\kappa_i}$ with an injective canonical projection, if $\overline{S} = \text{span}_{\mathbf{F}_2}(\tau^j(\vec{v}) | j \in \mathbb{Z}^+)$ where $\vec{v}$ is the associated vector of $\cup_{i=1}^{t} \mathfrak{C}_{p,r_i,l_i}^{\delta_i,\gamma_i,\kappa_i}$ and τ is the cyclic shift operator.

Let $p \nmid n$. For each $\mathfrak{C}_{p,r,l}^{\delta,\gamma,\kappa}$, the existence of its inverse pair $\mathfrak{C}_{p,n-r,l}^{\delta,\gamma,\kappa}$ is always guaranteed, hence ensuring stabiliser formalism by Theorem 2.3 and the choice of gamma is critical to ensure injectivity for ϕ. The subsequent study on stabiliser formalism is done on three distinct cases: $n = p^s \pm 1$ and $n = |\mathfrak{C}_{p,r}| + 1$. For each case, the quantum cyclotomic cosets will first be used to generate cyclic additive stabilisers and the constructed stabiliser codes' parameters will be studied. With additional parameters l and κ, the generalised quantum cyclotomic cosets will then be considered in enhancing the code parameters.

4.1 $n = p^s - 1$

The condition $p \nmid n$ always hold here. First, the following proposition gives the cardinality of the coprime cosets.

Proposition 4.1 *Let $n = p^s - 1$. For any coprime cosets $\mathfrak{C}_{p,r}$, $|\mathfrak{C}_{p,r}| = s$.*

Proof Note that $|\mathfrak{C}_{p,r}| = k$ if k is the smallest positive integer such that $rp^{k+1} \equiv rp \bmod (p^s - 1)$. Since $gcd(r, p^s - 1) = 1$, then $p^{k+1} \equiv p \bmod (p^s - 1)$ which is equivalent to $p^k \equiv 1 \bmod (p^s - 1)$. Note that the smallest positive integer j such that $p^j - 1 \equiv 0 \bmod (p^s - 1)$ is $j = s$ as gives that $p^s \equiv 1 \bmod (p^s - 1)$. Thus, k must be equal to s to satisfy $rp^{k+1} \equiv rp \bmod (p^s - 1)$. Hence,

$$|\mathfrak{C}_{p,r}| = s.$$

□

To ensure injectivity of ϕ for $\mathfrak{C}_{p,r}^{\delta,\gamma}$, the choice of γ must satisfy $\gamma \mid s$ when $\gamma \leq s$. Otherwise, we need to ensure that $3 \mid s$. One valid choice of γ for Theorem 3.3 to hold for any $s \in \mathbb{Z}^+$ is $\gamma = s$.

By setting $\gamma = s$, the quantum cyclotomic coset can be rewritten as below

$$\mathfrak{C}_{p,r}^{\delta,s} = \left\{ (\delta^{j \bmod s}, rp^j \bmod p^s - 1) | j \in \mathbb{Z}^+ \right\}.$$

Next, it is shown that $\mathfrak{C}_{p,r}^{\delta,s} = \mathfrak{C}_{p,n-r}^{\delta,s}$ can never fulfil for $r \neq 0$.

Proposition 4.2 *Let $n = p^s - 1$. Then any coprime quantum cyclotomic coset $\mathfrak{C}_{p,r}^{\delta,s}$ cannot be self-inverse.*

Proof Note that from Theorem 3.4, it is sufficient to show that $\mathfrak{C}_{p,r} \neq \mathfrak{C}_{p,n-r}$. Suppose that $\mathfrak{C}_{p,r}$ is self-inverse. This implies

$$rp^j \equiv -r \ mod \ p^s - 1,$$

for some smallest $j \in \mathbb{N}$. Since $gcd(r, n) = 1$, we have

$$p^j \equiv -1 \ mod \ p^s - 1 \tag{3}$$

Note that $|\mathfrak{C}_{p,r}| = s$ by Proposition 4.1, hence $j < s$. The inequality $p^j + 1 < p^s - 1$ holds for most $j < s$ in general, except precisely when

1. $s = 1$ for $p = 2, 3$,
2. $s = 2$ for $p = 2$.

Therefore, if $p^j + 1 < p^s - 1$ holds, there does not exist $j < s$ for (3) to hold, hence contradict to the assumption that $\mathfrak{C}_{p,r}$ is self-inverse. For the remaining cases, indeed, it is possible to find $j < s$ such that (3) holds. However, the condition $3 \mid \frac{|\mathfrak{C}_{p,r}|}{2}$ cannot be satisfied for $|\mathfrak{C}_{p,r}| = s = 1, 2$. Hence, by Theorem 3.4 again, $\mathfrak{C}_{p,r}^{\delta,s}$ can never be self-inverse. □

Based on the proof above, if $\mathfrak{C}_{p,r} \neq \mathfrak{C}_{p,n-r}$, the next theorem can be used to form a stabiliser subgroup of G_n.

Theorem 4.3 *Let $n = p^s - 1$ and $\mathfrak{C}_{p,r}^{\delta,s}$ be a coprime quantum cyclotomic coset with $(s, p) \notin \{(1, 2), (1, 3), (2, 2)\}$. Then, the associated vector of $\mathfrak{C}_{p,r}^{\delta,s} \cup \mathfrak{C}_{p,n-r}^{\delta,s}$ generates a cyclic additive stabiliser subgroup of G_n.*

Proof The proof follows from Proposition 4.2 and Theorem 2.3. □

By the discussion above and Theorem 4.3, MAGMA [18] is used to generate the results for some of the initial $n = 2^s - 1$ and $n = 3^s - 1$ as shown in Table 2, up to $n = 63$. For comparison and display purposes, we let $\delta = \omega$ for the rest of the results shown in the tables and similar procedures can be used to obtain results for $\delta = \omega^2$.

For a concrete understanding of how concatenation is used to generate stabiliser codes, the example below will illustrate the union mechanism used to generate the stabiliser generator.

Example 4.1 Consider the cosets constructed in Example 3.1. Note that $31 = 2^5 - 1$, where the coset and its inverse are a valid set of concatenations to consider by Theorem 4.3, which is

$$\mathfrak{C}_{2,1}^{\omega,5} \cup \mathfrak{C}_{2,30}^{\omega,5} = \{2\omega, 4\omega^2, 8, 16\omega, 1, 29\omega, 27\omega^2, 23, 15\omega, 30\}.$$

Table 2 Parameters of the quantum cyclic codes for $n = p^s - 1$ generated by the union of first representative coprime quantum cyclotomic cosets with its inverse

p	s	γ	Stabiliser Generator	Parameters
2	3	3	$\mathfrak{C}_{2,r}^{\omega,3} \cup \mathfrak{C}_{2,7-r}^{\omega,3}$	[[7,1,3]][1]
	4	4	$\mathfrak{C}_{2,r}^{\omega,4} \cup \mathfrak{C}_{2,15-r}^{\omega,4}$	[[15,1,5]][1]
	5	5	$\mathfrak{C}_{2,r}^{\omega,5} \cup \mathfrak{C}_{2,31-r}^{\omega,5}$	[[31,1,7]]
	6	6	$\mathfrak{C}_{2,r}^{\omega,6} \cup \mathfrak{C}_{2,63-r}^{\omega,6}$	[[63,27,5]]
3	2	2	$\mathfrak{C}_{3,r}^{\omega,2} \cup \mathfrak{C}_{3,8-r}^{\omega,2}$	[[8,2,2]]
	3	3	$\mathfrak{C}_{3,r}^{\omega,3} \cup \mathfrak{C}_{3,26-r}^{\omega,3}$	[[26,2,5]]

[1] Best-known parameters based on [19]

Thus, the associated vector is:

$$(0, 1, \omega, 0, \omega^2, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, \omega, \omega, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, \omega^2, 0, \omega, 1).$$

Setting above as the generator of an additive cyclic code over $\mathbf{F}_4$, this results in a [[31,1,7]] stabiliser code.

Based on Table 2, it can be noted that the quantum cyclic codes generated by all r with $gcd(r, n) = 1$ have the same parameters as listed. This is due to the fact that their underlying congruence equations of modulo n are equivalent, resulting in them having equivalent stabilisers.

Next, the notion of generalised quantum cyclotomic cosets is considered to improve the code parameters of the remaining stabiliser codes, using its flexibility and variation arising from the additional parameters l and κ. By Proposition 4.1 and Theorem 3.6, note that the injectivity of ϕ for $\mathfrak{C}_{p,r,l}^{\delta,\gamma,\kappa}$ holds for the previous choice of $\gamma = s$ if

1. $s \mid \frac{\kappa s}{gcd(s,l)}$ for $\kappa - gcd(s, l) \geq 0$.
2. $3 \mid \frac{\kappa s}{gcd(s,l)}$ for $\kappa - gcd(s, l) < 0$.

as the condition $\frac{\kappa s}{gcd(s,l)} - s = \frac{s(\kappa - gcd(s,l))}{gcd(s,l)}$ and its sign is fully depended on the factor $\kappa - gcd(s, l)$. In particular, the following observation holds.

Corollary 4.4 *Let $n = p^s - 1$ and $\gamma = s$. If $gcd(s, l) = 1$, then the injectivity of ϕ for $\mathfrak{C}_{p,r,l}^{\delta,s,\kappa}$ holds for any κ.*

Proof In this case, $\kappa \geq 1$ and the condition $s \mid \kappa s$ always holds. □

The self-inverse property of $\mathfrak{C}_{p,r,l}^{\delta,s,\kappa}$ for $n = p^s - 1$ is further discussed below.

Proposition 4.5 *Let $n = p^s - 1$. Then any coprime generalised quantum cyclotomic coset $\mathfrak{C}_{p,r,l}^{\delta,s,\kappa}$ cannot be self-inverse.*

Proof The proof is similar to Proposition 4.2. It is sufficient to note that for the following cases:

1. $s = 1$ for $p = 2, 3$.

2. $s = 2$ for $p = 2$.

when $\gamma = |\mathfrak{C}_{p,r}| = s$, $\kappa - 2gcd(s,l) < 0$ for $\kappa, l < |\mathfrak{C}^{\delta,\gamma,\kappa}_{p,r,l}| \leq s$ in the above cases. Therefore, the condition $\gamma > \frac{\kappa|\mathfrak{C}_{p,r}|}{2gcd(|\mathfrak{C}_{p,r}|,l)}$ from Theorem 3.7, or equivalently, $\frac{s(\kappa-2gcd(s,l))}{2gcd(s,l)} < 0$ holds. However, the condition $3 \mid \frac{\kappa s}{2gcd(s,l)}$ can never be fulfilled since $\kappa s < 6$. □

Therefore, by considering inverse pairs the following theorem can be used to construct stabilisers.

Theorem 4.6 *Let $n = p^s - 1$ and $\mathfrak{C}^{\delta,s,\kappa}_{p,r,l}$ be a coprime quantum cyclotomic coset with $(s, p) \notin \{(1, 2), (1, 3), (2, 2)\}$. Then, the associated vector of $\mathfrak{C}^{\delta,s,\kappa}_{p,r,l} \cup \mathfrak{C}^{\delta,s,\kappa}_{p,n-r,l}$ generates a cyclic additive stabiliser subgroup of G_n.*

Next, we proceed by studying the effect of the variation of the error part (varying κ and fixing l) and the position part (varying l and fixing κ) separately. The fixed value that would be chosen for κ and l is 1 which would coincide with the similar position and error part of the quantum cyclotomic coset.

4.1.1 Variation of error part ($\kappa = 1, 2, \ldots, s-1, l = 1$)

For $l = 1$, $gcd(s, l) = 1$ is always true and by Corollary 4.4, any κ chosen could guarantee the injectivity of ϕ for $\mathfrak{C}^{\delta,s,\kappa}_{p,r,1}$. These cosets can never be self-inverse by Proposition 4.5, hence Theorem 4.6 is used to generate cyclic additive stabilisers and the codes parameter are shown in Table 3. Note that the case of $p = 3$ with $s = 2$ is not considered as the only possible value for $\kappa < s = 2$ is 1, results in $\mathfrak{C}^{\omega,2,1}_{3,r,1} = \mathfrak{C}^{\omega,2}_{3,r}$.

Similarly, we provide an example below to demonstrate how the extra parameters affect the elements in the cosets and the generator of the stabiliser.

Example 4.2 Extending from the quantum coset constructed in Example 3.1 by further letting $l = 1$ and $\kappa = 2$, the respective set of concatenations will be

$$\mathfrak{C}^{\omega,5,2}_{2,1,1} \cup \mathfrak{C}^{\omega,5,2}_{2,30,1} = \{2\omega^2, 4\omega, 8\omega, 16, 1, 29\omega^2, 27\omega, 23\omega, 15, 30\}.$$

Note that both quantum cosets are injective, as guaranteed by Proposition 4.4. Note that $(s, p) \notin \{(1, 2), (1, 3), (2, 2)\}$, hence by using Theorem 4.6 the associated vector is:

$$(0, 1, \omega^2, 0, \omega, 0, 0, 0, \omega, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, \omega, 0, 0, 0, \omega, 0, \omega^2, 1).$$

Setting above as the generator of an additive cyclic code over $\mathbf{F}_4$, this results in a [[31,1,9]] stabiliser code.

4.1.2 Variation of position part ($\kappa = 1, l = 1, 2, \ldots, s-1$)

For $\kappa = 1$, the injectivity of ϕ is studied by dividing into $\kappa - gcd(s, l) \geq 0$ and $\kappa - gcd(s, l) < 0$.

Table 3 Parameters of the quantum cyclic codes for $n = p^s - 1$ generated by the union of first representative coprime generalised quantum cyclotomic cosets with its inverse

p	s	γ	l	κ	Stabiliser Generator	Parameters
2	5	5	1	1	$\mathfrak{C}^{\omega,5,1}_{2,r,1} \cup \mathfrak{C}^{\omega,5,1}_{2,31-r,1}$	[[31,1,7]]
				2	$\mathfrak{C}^{\omega,5,2}_{2,r,1} \cup \mathfrak{C}^{\omega,5,2}_{2,31-r,1}$	[[31,1,9]][1]
				3	$\mathfrak{C}^{\omega,5,3}_{2,r,1} \cup \mathfrak{C}^{\omega,5,3}_{2,31-r,1}$	[[31,1,9]][1]
				4	$\mathfrak{C}^{\omega,5,4}_{2,r,1} \cup \mathfrak{C}^{\omega,5,4}_{2,31-r,1}$	[[31,1,7]]
	6	6	1	1	$\mathfrak{C}^{\omega,6,1}_{2,r,1} \cup \mathfrak{C}^{\omega,6,1}_{2,63-r,1}$	[[63,27,5]]
				2	$\mathfrak{C}^{\omega,6,2}_{2,r,1} \cup \mathfrak{C}^{\omega,6,2}_{2,63-r,1}$	[[63,27,5]]
				3	$\mathfrak{C}^{\omega,6,3}_{2,r,1} \cup \mathfrak{C}^{\omega,6,3}_{2,63-r,1}$	[[63,27,1]][2]
				4	$\mathfrak{C}^{\omega,6,4}_{2,r,1} \cup \mathfrak{C}^{\omega,6,4}_{2,63-r,1}$	[[63,27,5]]
				5	$\mathfrak{C}^{\omega,6,5}_{2,r,1} \cup \mathfrak{C}^{\omega,6,5}_{2,63-r,1}$	[[63,27,5]]
3	3	3	1	1	$\mathfrak{C}^{\omega,3,1}_{3,r,1} \cup \mathfrak{C}^{\omega,3,1}_{3,26-r,1}$	[[26,2,5]]
				2	$\mathfrak{C}^{\omega,3,2}_{3,r,1} \cup \mathfrak{C}^{\omega,3,2}_{3,26-r,1}$	[[26,2,5]]

[1] Parameters that have improved as compared to Table 2
[2] The error part of this coset is only having one element, 1 in it. Hence, the codes generated are only stabilised under one type of error which results in $d = 1$

$\kappa - gcd(s, l) \geq 0$ can be true if and only if $gcd(s, l) = 1$, and thus the injectivity of ϕ holds by Corollary 4.4.

When $\kappa - gcd(s, l) < 0$, $gcd(s, l) > 1$. Therefore, the condition of $3 \mid \frac{s}{gcd(s,l)}$ must be satisfied to ensure the injectivity of ϕ. By Proposition 4.5 these cosets are not self-inverse and Theorem 4.6 is used to generate code parameters of cyclic additive stabilisers in Table 4. Similarly, $p = 3$ with $s = 2$ is not considered as the only possible value for $l < s = 2$ is again 1.

4.2 $n = p^s + 1$

Similarly, the condition $p \nmid n$ always holds and the following proposition gives the cardinality of the coprime cosets.

Proposition 4.7 *Let $n = p^s + 1$. For any coprime cosets $\mathfrak{C}_{p,r}$, $\mathfrak{C}_{p,r} = \mathfrak{C}_{p,n-r}$ with $|\mathfrak{C}_{p,r}| = 2s$.*

Proof Note that $m \in \mathbb{Z}^+$ is the smallest positive integer such that $p^m + 1 \equiv 0 \, mod \, (p^s + 1)$, which is equivalent to $rp^m \equiv -r \, mod \, (p^s + 1)$ when $gcd(r, n) = 1$. The results follow from Proposition 3.1 and the fact that $m = s$. □

To preserve the injectivity of ϕ for $\mathfrak{C}^{\delta,\gamma}_{p,r}$ for any n, a similar choice is made, $\gamma = s$. Note that $\gamma = s \leq 2s$ and thus by Theorem 3.3, ϕ must be injective for $\mathfrak{C}^{\delta,\gamma}_{p,r}$ as $\gamma \mid 2s$. The quantum cyclotomic coset can be rewritten as

$$\mathfrak{C}^{\delta,s}_{p,r} = \left\{ (\delta^{j \, mod \, s}, rp^j \, mod \, p^s + 1) | j \in \mathbb{Z}^+ \right\}.$$

Table 4 Parameters of the quantum cyclic codes for $n = p^s - 1$ generated by the union of first representative coprime generalised quantum cyclotomic cosets with its inverse

p	s	γ	κ	l	Stabiliser Generator	Parameters
2	5	5	1	1	$\mathfrak{C}^{\omega,5,1}_{2,r,1} \cup \mathfrak{C}^{\omega,5,1}_{2,31-r,1}$	[[31,1,7]]
				2	$\mathfrak{C}^{\omega,5,1}_{2,r,2} \cup \mathfrak{C}^{\omega,5,1}_{2,31-r,2}$	[[31,1,9]][1]
				3	$\mathfrak{C}^{\omega,5,1}_{2,r,3} \cup \mathfrak{C}^{\omega,5,1}_{2,31-r,3}$	[[31,1,9]][1]
				4	$\mathfrak{C}^{\omega,5,1}_{2,r,4} \cup \mathfrak{C}^{\omega,5,1}_{2,31-r,4}$	[[31,1,7]]
	6	6	1	1	$\mathfrak{C}^{\omega,6,1}_{2,r,1} \cup \mathfrak{C}^{\omega,6,1}_{2,63-r,1}$	[[63,27,5]]
				2	$\mathfrak{C}^{\omega,6,1}_{2,r,2} \cup \mathfrak{C}^{\omega,6,1}_{2,63-r,2}$	[[63,3,-]][2]
				3	$\mathfrak{C}^{\omega,6,1}_{2,r,3} \cup \mathfrak{C}^{\omega,6,1}_{2,63-r,3}$	Not injective
				4	$\mathfrak{C}^{\omega,6,1}_{2,r,4} \cup \mathfrak{C}^{\omega,6,1}_{2,63-r,4}$	[[63,3,-]][2]
				5	$\mathfrak{C}^{\omega,6,1}_{2,r,5} \cup \mathfrak{C}^{\omega,6,1}_{2,63-r,5}$	[[63,27,5]]
3	3	3	1	1	$\mathfrak{C}^{\omega,3,1}_{3,r,1} \cup \mathfrak{C}^{\omega,3,1}_{3,26-r,1}$	[[26,2,5]]
				2	$\mathfrak{C}^{\omega,3,1}_{3,r,2} \cup \mathfrak{C}^{\omega,3,1}_{3,26-r,2}$	[[26,2,5]]

[1] Parameters that have improved as compared to Table 2
[2] The minimum distance of the codes cannot be generated due to the lack of computation power but there is a significant change in the dimension which can be observed and might be caused by lesser elements in the coset

By Theorem 3.4, if $\gamma \leq \frac{|\mathfrak{C}_{p,r}|}{2}$, $\mathfrak{C}^{\delta,s}_{p,r}$ can only be self-inverse if both the conditions are satisfied:

1. $\mathfrak{C}_{p,r} = \mathfrak{C}_{p,n-r}$,
2. $\gamma \mid \frac{|\mathfrak{C}_{p,r}|}{2}$.

Note that 1) is guaranteed by Proposition 4.7 if $\mathfrak{C}_{p,r}$ is coprime, whereas 2) is always true by the choice of $\gamma = s$. This gives the following theorem.

Theorem 4.8 *Let $n = p^s + 1$ and $\mathfrak{C}^{\delta,s}_{p,r}$ be a coprime quantum cyclotomic coset. Then, the associated vector of $\mathfrak{C}^{\delta,s}_{p,r}$ generates a cyclic additive stabiliser subgroup of G_n.*

Proof The proof follows from the fact that $\mathfrak{C}^{\delta,s}_{p,r}$ is self-inverse and Theorem 2.3. □

By the discussion above and Theorem 4.8, MAGMA [18] is used to generate results for some of the initial $n = 2^s + 1$ and $n = 3^s + 1$ as shown in Table 5, up to $n = 65$.

As of Example 4.1, the following example illustrates the difference in stabiliser generator construction $n = p^s + 1$.

Example 4.3 For $n = p^s + 1$, we can consider a single coset in construction as shown in Theorem 4.8. Hence, let $n = 9$, $p = 2, r = 1, \delta = \omega, \gamma = 3$, thus we obtain injective ϕ for $\mathfrak{C}^{\omega,3}_{2,1}$ by Theorem 3.3 and self-inverse $\mathfrak{C}^{\omega,3}_{2,1}$ by Theorem 3.4. The coset is shown below

$$\mathfrak{C}^{\omega,3}_{2,1} = \{2\omega, 4\omega^2, 8, 7\omega, 5\omega^2, 1\},$$

Table 5 Parameters of the quantum cyclic codes for $n = p^s + 1$ generated by the first representative coprime quantum cyclotomic cosets

p	s	γ	Stabiliser Generator	Parameters
2	1	1	$\mathfrak{C}_{2,r}^{\omega,1}$	[[3,1,1]][1]
	2	2	$\mathfrak{C}_{2,r}^{\omega,2}$	[[5,1,3]][1]
	3	3	$\mathfrak{C}_{2,r}^{\omega,3}$	[[9,3,3]][1]
	4	4	$\mathfrak{C}_{2,r}^{\omega,4}$	[[17,1,5]]
	5	5	$\mathfrak{C}_{2,r}^{\omega,5}$	[[33,1,7]]
	6	6	$\mathfrak{C}_{2,r}^{\omega,6}$	[[65,5,9]]
3	1	1	$\mathfrak{C}_{3,r}^{\omega,1}$	[[4,2,1]]
	2	2	$\mathfrak{C}_{3,r}^{\omega,2}$	[[10,2,3]]
	3	3	$\mathfrak{C}_{3,r}^{\omega,3}$	[[28,4,5]]

[1] Best-known parameters based on [19]

where

$$\begin{aligned}\mathfrak{C}_{2,9-1}^{\omega,3} &= \mathfrak{C}_{2,8}^{\omega,3} \\ &= \{(\omega^{j \bmod 3}, (8)(2^j) \bmod 9) | j \in \mathbb{Z}^+\}, \\ &= \{7\omega, 5\omega^2, 1, 2\omega, 4\omega^2, 8\}, \\ &= \mathfrak{C}_{2,1}^{\omega,3}.\end{aligned}$$

Thus, the associated vector is:

$$(0, 1, \omega, 0, \omega^2, \omega^2, 0, \omega, 1)$$

Setting above as the generator of an additive cyclic code over $\mathbf{F}_4$, this results in a [[9,3,3]] stabiliser code.

Similarly, the generalised quantum cyclotomic cosets will be considered to seek improvement of the parameters of the codes generated for the remaining lengths. By Proposition 4.7 and Theorem 3.6, the injectivity of ϕ for $\mathfrak{C}_{p,r,l}^{\delta,\gamma,\kappa}$ holds for the previous choice of $\gamma = s$ if

1. $s \mid \frac{2\kappa s}{gcd(2s,l)}$ for $2\kappa - gcd(2\,s, l) \geq 0$,
2. $3 \mid \frac{2\kappa s}{gcd(2s,l)}$ for $2\kappa - gcd(2s, l) < 0$,

as the condition $\frac{2\kappa s}{gcd(2\,s,l)} - s = \frac{s(2\kappa - gcd(2\,s,l))}{gcd(2\,s,l)}$ and its sign is fully depended on the factor $2\kappa - gcd(2s, l)$. Thus, we have the following corollary.

Corollary 4.9 *Let $n = p^s + 1$ and $\gamma = s$. If $gcd(2s, l) = 1$, then the injectivity of ϕ for $\mathfrak{C}_{p,r,l}^{\delta,s,\kappa}$ holds for any κ.*

Proof Since $\kappa \geq 1$ and the condition of $s \mid 2\kappa s$ always holds. □

Next, the self-inverse property of the coset must also be preserved. By Theorem 3.7 and Proposition 4.7, since ϕ is injective, then the self-inverse structure of coprime $\mathfrak{C}_{p,r,l}^{\delta,s,\kappa}$ is preserved if

1. $s \mid \frac{\kappa s}{gcd(2s,l)}$ for $\kappa - gcd(2s,l) \geq 0$,
2. $3 \mid \frac{\kappa s}{gcd(2s,l)}$ for $\kappa - gcd(2s,l) < 0$,

as the condition $\frac{2\kappa s}{2gcd(2s,l)} - s = \frac{s(\kappa - gcd(2s,l))}{gcd(2s,l)}$ and its sign is fully depended on the factor $\kappa - gcd(2s,l)$. Thus, the following corollary is true.

Corollary 4.10 *Let $n = p^s + 1$, $\gamma = s$ and $\mathfrak{C}_{p,r,l}^{\delta,s,\kappa}$ is coprime. If $gcd(2s,l) = 1$, then the self-inverse property of $\mathfrak{C}_{p,r,l}^{\delta,s,\kappa}$ holds for any κ.*

Proof Since $\kappa \geq 1$ and the condition of $s \mid \kappa s$ always holds. □

Therefore, by considering solely $\mathfrak{C}_{p,r,l}^{\delta,s,\kappa}$ for $n = p^s + 1$, a stabiliser can be constructed as shown in the theorem below.

Theorem 4.11 *Let $n = p^s + 1$ and $\mathfrak{C}_{p,r,l}^{\delta,s,\kappa}$ be a coprime quantum cyclotomic coset. Then, the associated vector of $\mathfrak{C}_{p,r,l}^{\delta,s,\kappa}$ generates a cyclic additive stabiliser subgroup of G_n.*

Proof The proof follows from the fact that $\mathfrak{C}_{p,r,l}^{\delta,s,\kappa}$ is self-inverse and Theorem 2.3. □

4.2.1 Variation of error part ($\kappa = 1, 2, \ldots, s-1, l = 1$)

For $l = 1$, $gcd(2s,l) = 1$ is always true. Thus, Corollary 4.9 and Corollary 4.10 ensure that any κ chosen could guarantee the injectivity of ϕ and self-inverse structure of coprime $\mathfrak{C}_{p,r,1}^{\delta,s,\kappa}$. Theorem 4.11 is used to generate the cyclic additive stabilisers. However, up to length $n = 65$, there is no notable improvement of parameters by considering these generalised cosets as compared to Table 5.

4.2.2 Variation of position part ($\kappa = 1, l = 1, 2, \ldots, 2s-1$)

For $\kappa = 1$, if $2 - gcd(2s,l) \geq 0$, then $s \mid \frac{2s}{gcd(2s,l)}$ must be true to ensure the injectivity of ϕ, else $3 \mid \frac{2s}{gcd(2s,l)}$ must be true to ensure the injectivity of ϕ. Next, the self-inverse property of the coset must be verified also. If $1 - gcd(2s,l) \geq 0$, then $s \mid \frac{s}{gcd(2s,l)}$ can ensure the self-inverse structure, else $3 \mid \frac{s}{gcd(2s,l)}$ can ensure the self-inverse structure. Thus, Theorem 4.11 is used again to generate the cyclic additive stabilisers. Similarly, variation of position part does not result in notable improvement of parameters, up to length $n = 65$.

4.3 $n = |\mathfrak{C}_{p,r}| + 1$

Let $p \nmid n$ and $n = |\mathfrak{C}_{p,r}| + 1$ for some $r \in \mathbb{Z}^+$. The fact that $\mathfrak{C}_{p,r} \cup \mathfrak{C}_{p,0} = \mathbb{Z}_n$ and the coset disjoint property guarantee $\mathfrak{C}_{p,r} = \mathfrak{C}_{p,n-r}$. Therefore, $\mathfrak{C}_{p,r}$ must be a coprime coset, which every $i \in \mathfrak{C}_{p,r}$ has $gcd(i,n) = 1$, thus $n > 2$ must be a prime.

Table 6 Parameters of the quantum cyclic codes for $n = |\mathfrak{C}_{p,r}| + 1$ generated by the first representative quantum cyclotomic cosets

p	γ	Stabiliser Generator	s	$n = 2\gamma s + 1$	Parameters
2	2	$\mathfrak{C}_{2,r}^{\omega,2}$	1	5	[[5,1,3]][1]
			3	13	[[13,1,5]][1]
			7	29	[[29,1,11]][1]
			9	37	[[37,1,11]][1]
3	3	$\mathfrak{C}_{3,r}^{\omega,3}$	1	7	[[7,1,3]][1]
			3	19	[[19,1,7]][1]
			5	31	[[31,1,9]]

[1] Best-known parameters based on [19]

For the case $\gamma \leq \frac{|\mathfrak{C}_{p,r}|}{2}$, the choice of γ must satisfy $\gamma \mid \frac{|\mathfrak{C}_{p,r}|}{2}$ to guarantee both the injectivity of ϕ for $\mathfrak{C}_{p,r}^{\delta,\gamma}$ and its self-inverse property, based on Theorem 3.3 and 3.4. The discussion can be summarised as a necessary condition on n as follows.

Proposition 4.12 *Let $n = |\mathfrak{C}_{p,r}| + 1$ and $\gamma \leq \frac{|\mathfrak{C}_{p,r}|}{2}$. For $\mathfrak{C}_{p,r}^{\delta,\gamma}$ to be self-inverse, n must be a prime in the form of $2\gamma s + 1$ for some $s \in \mathbb{Z}^+$.*

Therefore, the following theorem can be used to generate the stabilisers by $\mathfrak{C}_{p,r}^{\delta,\gamma}$ for $n = |\mathfrak{C}_{p,r}| + 1$.

Theorem 4.13 *Let $n = |\mathfrak{C}_{p,r}|+1$, $\gamma \leq \frac{|\mathfrak{C}_{p,r}|}{2}$, and n is prime in the form of $2\gamma s+1$ for some $s \in \mathbb{Z}^+$. Then, the associated vector of $\mathfrak{C}_{p,r}^{\delta,\gamma}$ generates a cyclic additive stabiliser subgroup of G_n.*

Proof The proof follows from the fact that $\mathfrak{C}_{p,r}^{\delta,\gamma}$ is self-inverse and Theorem 2.3. □

By the discussion above and Theorem 4.13, some initial codes for $p = 2, 3$ are generated as shown in Table 6, up to $n = 37$.

Based on the results shown, quantum cyclotomic cosets are able to generate cyclic stabiliser codes that attain bounds for smaller n. Although larger n codes cannot attain the bounds, improvements are still plausible by considering the generalised version of the cosets. This motivates us to dive deeper into designing the generalised quantum cyclotomic cosets to perfect the result of the cyclic stabiliser codes generated.

Lastly, a substantial amount of our constructed codes are of low rate $\frac{k}{n}$. While computation limitations restrict us from exploring larger length codes, one can obtain higher rate codes by considering different choices of γ. For instance, for $n = 15$, set $\gamma = 2$. The resultant stabiliser generator is $\mathfrak{C}_{2,1}^{\omega,2} \cup \mathfrak{C}_{2,14}^{\omega,2}$, which can be verified to be an inverse pair, forming a [[15, 7, 3]]-code. In addition, Table 7 contains quantum stabiliser codes constructed by our framework for other classes of length, with $\frac{k}{n} > \frac{1}{2}$.

Table 7 Some quantum cyclic codes of other length type with $\frac{k}{n} > \frac{1}{2}$

n	p	γ	Length type (for some prime $\mathfrak{p}$)	Stabiliser Generator	Parameters
16	3	2	$\mathfrak{p}^s$	$\mathfrak{C}_{3,1}^{\omega,2}$	[[16,10,2]]
25	2	2	$\mathfrak{p}^s$	$\mathfrak{C}_{2,1}^{\omega,2}$	[[25,21,2]][1]
41	2	2	$\mathfrak{p}$	$\mathfrak{C}_{2,1}^{\omega,2}$	[[41,21,6]][1]
45	2	2	$(\mathfrak{p}^{s_1}+1)(\mathfrak{p}^{s_2}+1)$	$\mathfrak{C}_{2,1}^{\omega,2}$	[[45,37,2]]
49	3	3	$\mathfrak{p}^s$	$\mathfrak{C}_{3,1}^{\omega,3}$	[[49,43,2]][1]

[1] Best-known parameters based on [19]

5 Conclusion and future outlook

The notion of quantum cyclotomic coset was introduced as a new approach to stabiliser construction. The injectivity and self-inverse properties of these cosets were studied and formulated in a well-structured way. This subsequently allowed criteria for them to serve as the generators of cyclic additive stabilisers being developed. The variation of error part plays a crucial role in ensuring the stabiliser codes constructed by Definition 4.2 are stabilised under more than one error type, otherwise they are restricted to having no error-correcting ability. Certain constructed codes of length $n = p^s \pm 1$ and $n = |\mathfrak{C}_{p,r}| + 1$ are codes with best-known parameters. Some remaining codes can still be improved by further considering the generalised quantum cyclotomic cosets.

Possible future directions include considering further variations of our framework, such as on γ of the existing cases to improve the code parameters. The studies could also potentially be extended to other length type n. In all cases, criteria for cosets to establish certain desirable code properties, such as high rates, could be further developed. With suitable modifications, the framework could also be generalised and applied beyond cyclic codes to design quasi-cyclic and negacyclic stabilisers. Towards implementation, further research involves studying the compatibility of these codes with existing quantum algorithms, particularly focussing on the benefits arising from their cyclotomic properties.

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 not applicable to this article as no datasets were generated or analysed during the current study.

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

References

1. Childs, A.M., et al.: Exponential algorithmic speedup by a quantum walk. Paper presented at the STOC '03: Proceedings of the Thirty-Fifth Annual ACM Symposium on Theory of Computing, San Diego, CA, USA, 9–11 June 2003 (2003)
2. Shao, Y., et al.: Advances in methods and algorithms in a modern quantum chemistry program package. Phys. Chem. Chem. Phys. **8**, 3172–3191 (2006). https://doi.org/10.1039/B517914A
3. Joseph, D., et al.: Transitioning organizations to post-quantum cryptography. Nature **605**, 237–243 (2022). https://doi.org/10.1038/s41586-022-04623-2
4. Zhang, Y., Ni, Q.: Recent advances in quantum machine learning. Quantum Eng. **2**, 34 (2020). https://doi.org/10.1002/que2.34
5. Preskill, J.: Quantum Computing in the NISQ era and beyond. Quantum **2**, 79 (2018). https://doi.org/10.22331/q-2018-08-06-79
6. Ling, S., Xing, C.: Coding Theory: A First Course. Cambridge University Press, Cambridge (2004)
7. Garg, A., Dutt, S.: Cyclic codes of length 2^k over z_8. Open J. Appl. Sci. **2**, 104–107 (2012). https://doi.org/10.4236/ojapps.2012.24B025
8. Aly, S.A., Klappenecker, A., Sarvepalli, P.K.: On quantum and classical BCH codes. IEEE Trans. Inf. Theory **53**, 1183–1188 (2007). https://doi.org/10.1109/TIT.2006.890730
9. Mandelbaum, D.: Two applications of cyclotomic cosets to certain BCH codes (corresp.). IEEE Trans. Inf. Theory **26**, 737–738 (1980). https://doi.org/10.1109/TIT.1980.1056268
10. Yue, D.-W., Feng, G.-Z.: Minimum cyclotomic coset representatives and their applications to bch codes and Goppa codes. IEEE Trans. Inf. Theory **46**, 2625–2628 (2000). https://doi.org/10.1109/18.887870
11. Ong, K.L., Ang, M.H.: On equivalency of zero-divisor codes via classifying their idempotent generator. Des. Codes Crypt. **88**, 2051–2065 (2020). https://doi.org/10.1007/s10623-020-00762-7
12. Ong, K.L., Ang, M.H.: Full identification of idempotens in binary abelian group rings. J. Indones. Math. Soc. **23**, 67–75 (2017). https://doi.org/10.22342/jims.23.2.288.67-75
13. Marinescu, D.C., Marinescu, G.M.: Measurements and quantum information. In: Marinescu, D.C., Marinescu, G.M. (eds.) Classical and Quantum Information, pp. 133–220. Academic Press, Boston (2012)
14. Gottesman, D.: Stabilizer codes and quantum error correction. Preprint at https://arxiv.org/abs/quant-ph/9705052 (1997)
15. La Guardia, G.G., Alves, M.M.S.: On cyclotomic cosets and code constructions. Linear Algebra Appl. **488**, 302–319 (2016). https://doi.org/10.1016/j.laa.2015.09.034
16. Ong, K.L.: Study of idempotents in cyclic group rings over **F2**. AIP Conference Proceedings **1739**(1), (2016). https://doi.org/10.1063/1.4952491
17. Ong, K.L.: Burst error-correcting quantum stabilizer codes designed from idempotents. Quantum Inf. Process. **22**, 158 (2023). https://doi.org/10.1007/s11128-023-03904-7
18. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symbolic Comput. **24**, 235–265 (1997). https://doi.org/10.1006/jsco.1996.0125
19. Grassl, M.: Bounds on the minimum distance of linear codes and quantum codes. Online available at http://www.codetables.de. Accessed on 2024-05-12 (2007)